



(12) 发明专利申请

(10) 申请公布号 CN 114080781 A

(43) 申请公布日 2022. 02. 22

(21) 申请号 202080049795.9

(74) 专利代理机构 北京市柳沈律师事务所
11105

(22) 申请日 2020.06.17

代理人 李芳华

(30) 优先权数据

10-2019-0071799 2019.06.17 KR

10-2019-0120521 2019.09.30 KR

(51) Int.Cl.

H04L 9/08 (2006.01)

H04B 10/70 (2013.01)

(85) PCT国际申请进入国家阶段日

2022.01.07

(86) PCT国际申请的申请数据

PCT/KR2020/007846 2020.06.17

(87) PCT国际申请的公布数据

W02020/256408 KO 2020.12.24

(71) 申请人 株式会社KT

地址 韩国京畿道

(72) 发明人 申定桓 李京云 李旻洙

权利要求书2页 说明书10页 附图6页

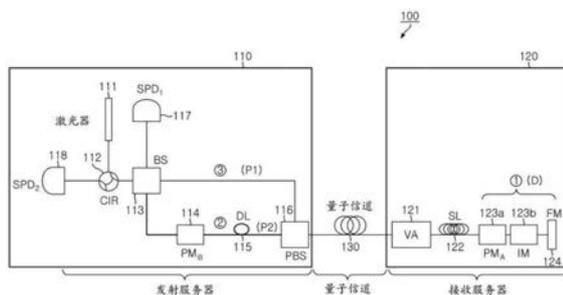
(54) 发明名称

量子密钥分配方法、装置和系统

(57) 摘要

本发明涉及一种量子密钥分配方法、装置和系统,并特别涉及一种能够利用一次性连续控制信号控制在量子密钥分配系统的接收机中提供的偏振相关元件的量子密钥分配方法、装置和系统,以独立于偏振进行驱动。本发明涉及一种量子密钥分配方法、装置和系统,并特别涉及一种能够利用一次性连续控制信号控制在量子密钥分配系统的接收机中提供的偏振相关元件的量子密钥分配方法、装置和系统,以独立于偏振进行驱动。公开了一种量子密钥分配系统(100),用于向发射机(110)和接收机(120)分配量子密钥,该量子密钥分配系统(100)的特征在于包括:发射机(110),其将光信号分成穿过第一路径(P1)的第一光信号和穿过比所述第一路径(P1)长的第二路径(P2)的第二光信号,并且依次传送所述第一和第二光信号;和接收机(120),其中通过量子信道(130)入射的第一光信号和第二光信号在穿过偏振相关元件(123)后被法拉第镜(124)反

射,向回穿过偏振相关元件(123),并然后通过量子信道(130)被传送到发射机(110),其中所述发射机(110)中的第一路径(P1)的长度(L_{P1})和第二路径(P2)的长度(L_{P2})之间的差($dL=L_{P2}-L_{P1}$)具有等于或大于偏振相关元件(123)与法拉第镜(124)之间的距离(= D)的两倍的值($dL \geq 2D$)。



1. 一种量子密钥分配系统(100),用于向发射机(110)和接收机(120)分配量子密码密钥,该量子密钥分配系统(100)包括:

发射机(110),被配置为将光信号分成穿过第一路径(P1)的第一光信号和穿过比所述第一路径(P1)长的第二路径(P2)的第二光信号,并且依次传送所述第一光信号和所述第二光信号;和

接收机(120),被配置为接收通过量子信道(130)入射的所述第一光信号和所述第二光信号,并在穿过偏振相关元件(123)、被法拉第镜(124)反射、并再次穿过偏振相关元件(123)后,穿过所述量子信道(130)将所述第一光信号和所述第二光信号传送回所述发射机(110),

其中所述发射机(110)中的第一路径(P1)的长度(L_{P1})和第二路径(P2)的长度(L_{P2})之间的差($dL=L_{P2}-L_{P1}$)等于或大于偏振相关元件(123)与法拉第镜(124)之间的距离(= D)的两倍($dL \geq 2D$)。

2. 如权利要求1所述的量子密钥分配系统,其中,所述发射机(110)包括被配置为生成光信号的光源(111)和被配置为将所述光信号分成所述第一光信号和所述第二光信号、将所述第一光信号输出到第一路径(P1)、并将所述第二光信号输出到第二路径(P2)的分束器(113)。

3. 如权利要求2所述的量子密钥分配系统,其中在所述第二路径(P2)中提供延伸所述第二光信号的传播路径的延迟线(115)。

4. 如权利要求1所述的量子密钥分配系统,其中在所述发射机(110)中提供偏振分束器(116)以将通过第一路径(P1)行进的第一光信号偏振为具有第一偏振,并且将通过第二路径(P2)行进的第二光信号偏振为具有与第一偏振正交的第二偏振。

5. 如权利要求4所述的量子密钥分配系统,其中所述偏振分束器(116)使从接收机(120)传送的所述第一光信号行进到所述第二路径(P2),并使所述第二光信号行进到所述第一路径(P1)。

6. 如权利要求1所述的量子密钥分配系统,其中,在所述接收机(120)中,当第一光信号或第二光信号穿过偏振相关元件(123)、在法拉第镜(124)上反射、并然后再次穿过偏振相关元件(123)时,施加一次性连续控制信号作为用于控制所述偏振相关元件(123)的操作的控制信号。

7. 如权利要求1所述的量子密钥分配系统(100),其中所述接收机(120)包括多个偏振相关元件(123),并且

所述第一路径(P1)的长度(L_{P1})和所述第二路径(P2)的长度(L_{P2})之间的差($dL=L_{P2}-L_{P1}$)等于或大于远离所述法拉第镜(124)的所述偏振相关元件(123)之一与所述法拉第镜(124)之间的距离(= D)的两倍($dL \geq 2D$)。

8. 如权利要求7所述的量子密钥分配系统,其中所述多个偏振相关元件(123)包括第一相位调制器(123a)和强度调制器(123b),并且

所述第一相位调制器(123a)仅调制所述第二光信号的相位。

9. 如权利要求7所述的量子密钥分配系统,其中所述多个偏振相关元件(123)包括第一相位调制器(123a)和强度调制器(123b),并且

所述强度调制器(123b)调制所述第一光信号的强度和所述第二光信号的强度。

10. 一种在量子密钥分配系统(100)中提供的发射机(110),用于与接收机(120)分配量子密码密钥,所述发射机(110)包括:

光源(111),被配置为生成光信号;

分束器(113),被配置为将所述光信号分为第一光信号和第二光信号,将所述第一光信号输出到第一路径(P1),并将所述第二光信号输出到第二路径(P2);和

延迟线(115),被提供在所述第二路径(P2)中以延伸所述第二光信号的传播路径,

其中所述第一路径(P1)的长度(L_{P1})和所述第二路径(P2)的长度(L_{P2})之间的差($dL = L_{P2} - L_{P1}$)等于或大于接收机(120)中提供的偏振相关元件(123)与法拉第镜(124)之间的距离(=D)的两倍($dL \geq 2D$)。

11. 一种在量子密钥分配系统(100)中提供的接收机(120),用于与发射机(110)分配量子密码密钥,所述接收机(120)包括:

偏振相关元件(123),具有取决于光信号的偏振而变化的工作特性;和

法拉第镜(124),被配置为通过将进入光信号的偏振旋转90度,来反射所述光信号,

其中,所述发射机(110)生成光信号,将光信号分成穿过第一路径(P1)的第一光信号和穿过比所述第一路径(P1)长的第二路径(P2)的第二光信号,并且向所述接收机120依次传送所述第一光信号和所述第二光信号,所述接收机120接收通过量子信道(130)入射的所述第一光信号和所述第二光信号,并在穿过偏振相关元件(123)、被法拉第镜(124)反射、并再次穿过偏振相关元件(123)后,通过所述量子信道(130)将所述第一光信号和所述第二光信号传送回所述发射机,并且

所述发射机(110)中的第一路径(P1)的长度(L_{P1})和第二路径(P2)的长度(L_{P2})之间的差($dL = L_{P2} - L_{P1}$)等于或大于偏振相关元件(123)与法拉第镜(124)之间的距离(=D)的两倍($dL \geq 2D$)。

量子密钥分配方法、装置和系统

技术领域

[0001] 本公开涉及一种量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统,尤其涉及这样的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统,用于使用一次性连续控制信号,来控制量子密钥分配系统的接收机中提供的偏振相关元件以独立于偏振驱动该元件。

背景技术

[0002] 近来,个人或国家已遭受由其间的搭线窃听和窃听而导致的损害,并且存在对于安全性的显著增长的关注。然而,典型的安全通信具有通信内容可能被外部攻击暴露的严重风险。为了补偿典型安全通信方法的不足,量子密码通信作为下一代安全技术已被引入并备受关注。量子密码理论上可以保证很高的安全性。

[0003] 因此,关于量子密码通信技术之中的量子密钥分配已经积极进行了许多研究。量子密钥分配(QKD)是一种利用光子的量子力学属性在远程用户之间分配和共享加密密钥的技术。如果攻击者试图获取在用户之间分配的密码密钥信息,由于量子力学属性,密码密钥信息可能会发生变化。因此,交换密码密钥的用户可以检测到攻击者的存在。

[0004] 具体而言,量子密钥分配(QKD)使用具有量子属性的单光子(或与单光子类似的水平的准单光子)传送信息,以使用量子状态分配密码密钥,并使用光子的各种量子属性之中的偏振和相位安全地共享防止窃听的密码密钥。

[0005] 因此,量子密钥分配(QKD)系统包括各种光学元件,并且量子密钥分配(QKD)系统中包括的各种光学元件通常具有偏振相关的操作特性。因此,发生在量子密钥分配(QKD)系统中的光子偏振变化对量子密钥分配(QKD)系统的性能具有重大影响。

[0006] 例如,量子密钥分配(QKD)系统通常使用相位来分配密码密钥。量子密钥分配(QKD)系统采用相位调制器(PM)将密码密钥信息加载到光子上。相位调制器(PM)通常具有相位调制特性根据光子的偏振状态而变化的偏振相关特性。

[0007] 也就是说,相位调制器(PM)是使用电压或电流控制光子的相位、并根据偏振相关特性通过输入偏振来改变相位控制值的装置。因此,当输入到相位调制器(PM)的光子的偏振改变时,难以精确地控制相位。此外,由于偏振引起的相位误差,量子密钥分配(QKD)系统无法正确生成/分配密码密钥。

[0008] 强度调制器(IM)用于生成诱饵(decoy)数据,用于检测量子密钥分配(QKD)系统中的攻击者的存在。这种强度调制器通常也是偏振相关的。因此,当进入强度调制器(IM)的光子的偏振发生变化时,强度调制器(IM)难以生成准确的诱饵数据(诱饵状态),这限制了量子密钥分配(QKD)系统的稳定操作。

[0009] 一种单向量子密钥分配(QKD)系统包括生成单光子的发射机和检测单光子的接收机。因此,发射机和接收机通常都配置有光链路和能够保持适当偏振的元件,以便控制偏振相关器件的特性。此外,接收机具有单独的偏振校正功能,以校正发生在量子信道(通过其传送单光子的光链路)中的偏振失真。

[0010] 一种双向量子密钥分配 (QKD) 系统包括发射机,用于生成、传送单光子,并检测由接收机反射的光子。双向量子密钥分配 (QKD) 系统被配置为将发射机产生的光信号传送到接收机,并通过同一链路将光信号返回到发射机,以校正量子信道中发生的偏振失真。因此,在从发射机到接收机的传送中发生的偏振失真被校正为与在通过相同链路传送到发射机期间最初发生在发射机中的偏振相同的偏振。

[0011] 在双向量子密钥分配 (QKD) 系统中,可以使用相同光链路通过偏振校正来确保设置在发射机中的干涉仪的稳定操作。但是,接收机需要使用从发射机接收的光信号来校正在使用调制器 (PM) 和强度调制器 (IM) 时由偏振引起的误差,以生成其中在光信号的相位中对密码密钥信息进行编码的单光子。

[0012] 为了校正双向系统中的误差,接收机通过使用生成与输入光信号的偏振失真程度成正比的误差的元件,对进入接收机的光信号和从接收机存在的光信号重复对该元件控制两次,以便控制偏振失真。

[0013] 如上所述的这种典型方法需要生成高速操作的两个控制信号,并且需要在进入光信号和出射光信号不重叠的时候高速控制偏振相关器件两次。

发明内容

[0014] 技术问题

[0015] 因此,已经鉴于上述问题提出本公开,并且本公开的一个方面在于提供一种量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统,用于当在其中光信号来回穿过与双向结构相同的光链路的量子密钥分配 (QKD) 系统中使用偏振相关元件配置装置时,通过使用一次性连续控制信号来控制偏振相关元件,来校正由于偏振相关特性导致的误差。

[0016] 本技术领域的专家或研究人员通过以下将要描述的详细内容将清楚地标识和理解本公开的其他具体方面。

[0017] 技术方案

[0018] 根据本公开的一个实施例,一种用于向发射机110和接收机120分配量子密码密钥的量子密钥分配系统100包括:所述发射机110,被配置为将光信号分成穿过第一路径P1的第一光信号和穿过比所述第一路径P1长的第二路径P2的第二光信号,并且依次传送所述第一光信号和所述第二光信号;和所述接收机120,被配置为接收通过量子信道130入射的所述第一光信号和所述第二光信号,并在穿过偏振相关元件123、被法拉第镜124反射、并再次穿过偏振相关元件123后,通过所述量子信道130将所述第一光信号和所述第二光信号送回所述发射机110,其中所述发射机110中的第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于偏振相关元件123与法拉第镜124之间的距离(= D)的两倍($dL \geq 2D$)。

[0019] 所述发射机110可包括:光源111,生成光信号;和分束器113,将所述光信号分成所述第一光信号和所述第二光信号,将所述第一光信号输出到第一路径P1,并将所述第二光信号输出到第二路径P2。

[0020] 可以在所述第二路径P2中提供延伸所述第二光信号的传播路径的延迟线115。

[0021] 可以在所述发射机110中提供偏振分束器116,以将通过第一路径P1行进的第一光信号偏振为具有第一偏振,并且将通过第二路径P2行进的第二光信号偏振为具有与第一偏

振正交的第二偏振。

[0022] 偏振分束器116可以使从接收机120传送的所述第一光信号能够行进到所述第二路径P2,并使所述第二光信号能够行进到所述第一路径P1。

[0023] 在所述接收机120中,当第一光信号或第二光信号穿过偏振相关元件123、在法拉第镜124上反射、并再次穿过偏振相关元件123时,可以施加一次性连续控制信号作为用于控制所述偏振相关元件123的操作的控制信号。

[0024] 所述接收机120可以包括多个偏振相关元件123,并且所述第一路径P1的长度 L_{P1} 和所述第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于远离所述法拉第镜124的所述偏振相关元件123之一与所述法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0025] 所述多个偏振相关元件123可以包括第一相位调制器123a和强度调制器123b,并且所述第一相位调制器123a可以仅调制所述第二光信号的相位。

[0026] 所述多个偏振相关元件123可以包括第一相位调制器123a和强度调制器123b,并且所述强度调制器123b可以调制所述第一光信号的强度和所述第二光信号的强度。

[0027] 根据本公开的另一实施例,一种在量子密钥分配系统100中提供的发射机110,用于与接收机120分配量子密码密钥,所述发射机110包括:光源111,被配置为生成光信号;分束器113,被配置为将所述光信号分为第一光信号和第二光信号,将所述第一光信号输出到第一路径P1,并将所述第二光信号输出到第二路径P2;和延迟线115,被提供在所述第二路径P2中以延伸所述第二光信号的传播路径,其中所述第一路径P1的长度 L_{P1} 和所述第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于接收机120中提供的偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0028] 根据本公开的另一实施例,一种在量子密钥分配系统100中提供的接收机120,用于与发射机110分配量子密码密钥,所述接收机120包括:偏振相关元件123,具有取决于光信号的偏振而变化的工作特性;和法拉第镜124,被配置为通过将进入光信号的偏振旋转90度,来反射所述光信号,其中,当所述发射机110生成光信号、将光信号分成穿过第一路径P1的第一光信号和穿过比所述第一路径P1长的第二路径P2的第二光信号、并且向所述接收机120依次传送所述第一光信号和所述第二光信号时,所述接收机接收通过量子信道130入射的所述第一光信号和所述第二光信号,并在穿过偏振相关元件123、被法拉第镜124反射、并再次穿过偏振相关元件123后,通过所述量子信道130将所述第一光信号和所述第二光信号传回所述发射机,并且所述发射机110中的第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0029] 发明的有益效果

[0030] 通过根据本公开的实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统,通过在其中光信号来回穿过与双向结构相同的光链路的量子密钥分配(QKD)系统中使用一次性连续控制信号控制偏振相关元件,来校正由于偏振相关特性导致的误差。

[0031] 也就是说,根据本公开,可以控制在双向量子密钥分配(QKD)系统中使用的偏振相关元件不受到用于在装置内部和外部传送光的周期中发生的偏振失真的影响。

[0032] 因此,在本公开中,可能在使用偏振相关元件的双向量子密钥分配(QKD)系统中控制光信号,而不管偏振失真如何。

[0033] 具体地,根据本公开的量子密钥分配(QKD)系统包括接收机120,其控制偏振相关元件,例如相位调制器(PM)和强度调制器(IM)。因此,可能使用一次性连续控制信号独立于偏振来控制偏振相关元件。

附图说明

[0034] 作为详细描述的一部分以帮助理解本公开的附图提供本公开的实施例,并结合详细描述来描述本公开的技术精神,其中:

[0035] 图1和图2图示了根据本公开实施例的量子密钥分配系统100;

[0036] 图3详细图示了根据本公开实施例的量子密钥分配系统100;

[0037] 图4A和图4B是图示了根据本公开的实施例的量子密钥分配系统100中的用于控制偏振相关元件的控制信号的曲线图;

[0038] 图5图示了根据本公开实施例的量子密钥分配系统100中的接收机120的偏振相关元件123的布置;和

[0039] 图6和图7图示了根据本公开实施例的量子密钥分配系统100中的发射机110和接收机120。

具体实施方式

[0040] 本公开可以进行各种修改,并且可以包括各种实施例。下面将结合附图对具体实施例进行详细描述。

[0041] 提供以下实施例是为了全面理解这里描述的方法、装置和/或系统。然而,提供这些实施例仅用于说明,并且本公开不限于此。

[0042] 当在描述本公开的实施例时确定关于与本公开相关的已知技术的详细描述使得本公开的主旨不清楚时,将在这里省略该详细描述。此外,下面使用的术语是鉴于本公开中的功能而定义的,并因此可以取决于用户、操作者的意图、或习惯而改变。因此,这些术语应该基于本说明书的以下总体描述来定义。详细描述中使用的术语仅用于描述本公开的实施例,而不意欲限制本公开。除非按照别的方式明确使用,否则单数形式旨在包括复数形式。应当理解,当在本说明书中使用时,表述“包括”或“包含”指定所阐述的特征、整数、步骤、操作、元素、或其一些或组合的存在,但不排除存在或添加一个或多个其他特征、整数、步骤、操作、元素、或其一些或组合。

[0043] 虽然术语“第一”、“第二”等可用于描述各种组件,但这些组件不应受这些术语的限制。这些术语仅用于将一个组件与另一个组件区分开来。

[0044] 在下文中,将参照附图详细描述本公开的示例性实施例。

[0045] 图1图示了根据本公开的实施例的量子密钥分配系统100。

[0046] 如图1所示,根据本公开的实施例的量子密钥分配系统100可以包括发射机110、接收机120和量子信道130。发射机110和接收机120通过经由量子信道130交换光信号,而生成并共享量子密码密钥。

[0047] 这里,发射机110和接收机120可以是服务器、连接到服务器的客户端或终端、诸如网关或路由器的通信装置、或具有移动性的便携式装置。发射机110和接收机120可以使用能够通过生成和共享量子密钥进行通信的各种装置来配置。

[0048] 量子信道130提供在发射机110和接收机120之间以传送光信号。虽然量子信道130可以使用光纤来配置,但是本公开不一定限于此,并且可以使用能够传送光信号的任何介质来配置量子信道130。

[0049] 因此,发射机110和接收机120可以根据各种协议,例如BB84协议,使用光信号的相位、偏振等来交换生成量子密码密钥所必需的信息。此外,发射机110和接收机120可以生成并共享量子密码密钥,从而有效地防止攻击者140窃取量子密码密钥并试图破解量子密码密钥。

[0050] 此外,量子密码通信系统可以在使用在量子密钥分配系统100中生成的量子密码密钥执行加密和解密的同时执行通信,从而增强通信系统的安全性。

[0051] 图2是图示了根据本公开的实施例的量子密钥分配系统100的框图。如图2所示,根据本公开的实施例的量子密钥分配系统100将量子密码密钥分配给发射机110和接收机120。量子密钥分配系统100可以包括i) 发射机110,其将光信号划分为穿过第一路径P1的第一光信号、和穿过比第一路径P1更长的第二路径P2的第二光信号,并依次传送光信号,和ii) 接收机120,其在第一光信号和第二光信号通过量子信道130入射、穿过偏振相关元件123、在法拉第镜124上反射、并然后再次穿过偏振相关元件123之后,通过量子信道130向发射机110传送第一光信号和第二光信号。

[0052] 这里,在根据本公开的实施例的量子密钥分配系统100中,发射机110中的第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于偏振相关元件123和法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0053] 在其中光信号来回穿过与双向结构相同的光链路的量子密钥分配系统100中,根据本公开的实施例,接收机120使用偏振相关元件123来配置,并且可以使用一次性连续控制信号来控制偏振相关元件123。因此,没有必要执行非连续控制信号两次或更多次。因此,根据本公开的实施例的量子密钥分配系统100校正由偏振相关特性引起的误差。

[0054] 在下文中,将参照图3详细描述根据本公开的实施例的量子密钥分配系统100。

[0055] 首先,如图3所示,发射机110可以包括光源111和分束器BS 113。光源111生成光信号。分束器BS 113将光信号分成第一光信号和第二光信号,将第一光信号输出到第一路径P1,并将第二光信号输出到第二路径P2。

[0056] 可以在第二路径P2中提供延伸第二光信号的传播路径的延迟线DL 115。

[0057] 此外,如图3所示,偏振分束器PBS 116可以设置在发射机110中,使得通过第一路径P1行进的第一光信号可以被偏振为具有第一偏振,并且通过第二路径P2行进的第二光信号可以被偏振为具有与第一偏振正交的第二偏振。

[0058] 这里,偏振分束器116可以使从接收机120传送的第一光信号行进到第二路径P2,并且使第二光信号行进到第一路径P1。

[0059] 如图3所示,在接收机120中,当第一光信号或第二光信号穿过偏振相关元件123(例如,第一相位调制器123a和强度调制器123b)、在法拉第镜124上反射、并然后再次穿过偏振相关元件123时,可以应用一次性连续控制信号作为用于控制偏振相关元件123的操作的控制信号。

[0060] 如图3所示,接收机120可以包括多个偏振相关元件123。在这种情况下,第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)可以等于或大于远离法拉第镜

124的偏振相关元件123中的一个(例如,第一相位调制器123a)与法拉第镜124之间的距离($=D$)的两倍($dL \geq 2D$)。

[0061] 接收机120可以包括第一相位调制器123a和强度调制器123b作为多个偏振相关元件123,并且第一相位调制器123a可以仅调制第二光信号的相位。

[0062] 另外,参考图3,当第二相位调制器 PM_B 114位于第一路径P1上时,接收机120中的第一相位调制器123a可以仅调制第一光信号的相位。

[0063] 接收机120可以包括第一相位调制器123a和强度调制器123b作为多个偏振相关元件123,并且强度调制器123b可以调制第一光信号的强度和第二光信号的强度。

[0064] 在下文中,关于根据本公开的实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统100,将参考图3详细描述每个单独组件的操作。

[0065] 首先,如图3所示,在根据本公开的实施例的发射机110中,在诸如激光发生装置的光源111中生成的光信号可以经由准确地控制第一光信号和第二光信号,同时快速转换用于第一相位调制器 PM_A 123a的控制信号器CIR112输入到分束器BS 113。

[0066] 分束器113可以将输入光信号分成第一光信号和第二光信号,将第一光信号传送到作为短路径的第一路径P1(图3的③),并且将第二光信号传送到具有延迟线DL的第二路径P2(图3的②)。

[0067] 第一光信号和第二光信号经由偏振分束器PBS 116输入到量子信道130。

[0068] 这里,由于第一路径P1的长度 L_{P1} 和包括延迟线115的第二路径P2的长度 L_{P2} 之间的差异,经由第二路径P2的第二光信号按照第二路径P2的长度 L_{P2} 与第一路径P1的长度 L_{P1} 之间的差($dL = L_{P2} - L_{P1}$)的间隔被输出到量子信道130。

[0069] 此外,偏振分束器PBS 116使得已经由第一路径P1的第一光信号的输出具有垂直(V)偏振,并且使得经由第二路径P2的第二光信号的输出具有与第一光信号的偏振正交的水平(H)偏振。

[0070] 通过量子信道130到达接收机120的第一光信号和第二光信号在穿过量子信道130时分别失真为具有任意偏振 V' 和 H' 。输入到接收机120的第一光信号和第二光信号经由存储线SL、第一相位调制器 PM_A 123a、和强度调制器IM 123b到达法拉第镜FM 124。

[0071] 因此,由于法拉第镜FM 124通过将入射的第一光信号和第二光信号旋转90度来反射入射的第一光信号和第二光信号的偏振,因此首先入射的第一光信号的偏振 V' 被反射为变为 H' ,而随后入射的第二光信号的偏振 H' 被反射为变为 V' 。

[0072] 从法拉第镜FM 124反射的第一光信号和第二光信号被输入到强度调制器IM 123b和第一相位调制器 PM_A 123a。因此,强度调制器IM 123b调整光信号的强度以生成诱饵数据(诱饵状态)。

[0073] 这里,强度调制器IM 123b可以调制第一光信号的强度和第二光信号的强度两者以生成诱饵数据(诱饵状态)。

[0074] 第一相位调制器 PM_A 123a可以仅改变入射的光信号中的第二光信号的相位以生成密码密钥。因此,经由第一相位调制器 PM_A 123a的第二光信号的相位从 V' 变为 $V'a$ 。

[0075] 随后,第一光信号和第二光信号经由可变衰减器VA 121被转换成单光子(或伪单光子),然后通过量子信道130将其传送回发射机110。

[0076] 因此,由于传送到发射机110的单光子级的第一光信号和第二光信号通过与第一

次传送到接收机120时使用的光信道相同的路径向回传送,因此按照从发射机110到接收机120的传送中的相同程度的偏振失真,发生偏振失真。因此,在量子信道130中发生的偏振失真被抵消以消失。

[0077] 结果,第一光信号再次到达发射机110,偏振 H' 被校正为 H ,并且第二光信号再次到达发射机110,偏振 $V'a$ 被校正为 Va 。

[0078] 随后,首先通过具有发射机110的延迟线DL的第二路径P2传送的第二光信号具有由法拉第镜FM 124旋转90度的偏振,并因此由偏振分束器PBS116穿行第一路径P1,而通过第一路径P1传送的第一光信号由偏振分束器PBS 116经由延迟线DL 115穿行第二路径P2。结果,第一光信号信号和第二光信号相对于发射机110的分束器BS 113行进相同的距离,从而同时到达分束器BS 113,并根据第一相位调制器 PM_A 123a和第二相位调制器 PM_B 114的相变引起干扰。

[0079] 这里,在量子密钥分配系统100的接收机120中,与偏振相关的第一相位调制器 PM_A 123a和强度调制器(IM) 123b在入口和出口的每一个处执行两个相位控制以校正偏振相关特性。因此,由于进入第一相位调制器 PM_A 123a和强度调制器(IM) 123b的光信号和从其离开的光信号由法拉第镜(FM) 124引起的90度的偏振差,因此可以通过两个相位控制校正由于偏振引起的相位控制误差。

[0080] 然而,在量子密钥分配系统100中,从发射机110传送的第一光信号和第二光信号按照第一路径P1的长度 L_{P1} 与第二路径P2的长度 L_{P2} 之间的差值($dL=L_{P2}-L_{P1}$)的间隔进入接收机120。

[0081] 如图3所示,接收机120的电路可以通过依次布置存储线SL122、第一相位调制器 PM_A 123a、强度调制器IM 123b、和法拉第镜FM 124来配置。

[0082] 这里,偏振相关元件123可以不考虑顺序地布置。即,当偏振相关元件123和法拉第镜FM 124在存储线SL122(图3的①)之后连续配置时,如果此配置中的包括接收机120的第一相位调制器 PM_A 123a、强度调制器IM 123b、和法拉第镜FM 124的距离被定义为D,并且D被配置为dL的1/2或更短,则直到第一光信号穿过第一相位调制器 PM_A 123a、在法拉第镜FM 124上反射、并然后再次穿过第一相位调制器 PM_A 123a,第二光信号才到达第一相位调制器 PM_A 123a。

[0083] 这里,第一相位调制器 PM_A 123a和强度调制器IM 123b的位置可以改变。因此,当首先定位强度调制器IM 123b时,直到第一光信号穿过强度调制器IM 123b、在法拉第镜FM 124上反射、并然后再次穿过强度调制器IM123b,第二光信号才到达强度调制器IM 123b。

[0084] 在接收机120中,第一相位调制器 PM_A 123a可以仅针对第二光信号操作。因此,当D被配置为dL的1/2或更短时,直到第二光信号穿过第一相位调制器 PM_A 123a、在法拉第镜FM 124上反射、并然后再次穿过第一相位调制器 PM_A 123a,第一光信号才位于第一相位调制器 PM_A 123a和法拉第镜FM124之间。

[0085] 因此,为了控制第二光信号的相位并使用一次性连续控制信号校正由偏振失真引起的误差,当在第一光信号离开第一相位调制器 PM_A 123a之后、控制信号被施加到第一相位调制器 PM_A 123a达到时间T时,第二光信号在进入第一相位调制器 PM_A 123a、在法拉第镜FM 124上反射、并再次经过第一相位调制器 PM_A 123a达到时间T的时候受到两次相位控制,从而抵消由于偏振引起的相位误差。

[0086] 这里,T可以通过等式1计算。

[0087] [等式1]

[0088] $T=2N/c+E$ (c:光链路中的光速)

[0089] 此外,为了在接收机120中生成诱饵数据(诱饵状态),强度调制器IM 123b需要针对第一光信号和第二光信号两者操作。因此,当在第一光信号和第二光信号穿过强度调制器IM 123b、在法拉第镜FM 124上反射、并然后再次穿过强度调制器IM 123b的同时施加一次性连续控制信号时,第一光信号和第二光信号经受两次控制,由此抵消由于偏振引起的相位误差。

[0090] 执行本发明的方式

[0091] 更具体地说,图4A和图4B图示了根据本公开实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统中的光信号和用于控制偏振相关元件的控制信号。

[0092] 首先,如图4A所示,在相关技术中,由于第一光信号在i) 第二光信号输入到接收机120并经过偏振相关元件123的时间S21、和ii) 第二光信号在法拉第镜124上反射并再次穿过偏振相关元件123的时间S22之间穿过偏振相关元件123 (S12),因此需要使用单独的高速控制信号C11和C12个别控制S21和S22。

[0093] 然而,在根据本公开的实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统中,如图4B所示,第一光信号不位于i) 第二光信号输入到接收机120并经过偏振相关元件123的时间S21、和ii) 第二光信号在法拉第镜124上反射并再次穿过偏振相关元件123的时间S22之间。因此,可能根据实施例使用单个低速控制信号C11组合控制S21和S22。

[0094] 在下文中,结合图3、图4A、和图4B对根据本公开的实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统进行更详细的描述。

[0095] 在下文中,虽然为了说明而描述了其中提供相位调制器 PM_A 123a作为接收机120中的偏振相关元件123的情况,但是本公开不必限于此。

[0096] 首先,在相关技术中,当如图3所示将第二相位调制器 PM_B 114布置在第二路径P2上时,如图4A所示,在第一光信号进入接收机120之后(图4A的S1),在第二光信号经过第一相位调制器 PM_A 123a时施加第一控制信号,从而调制第二光信号的相位(图4A的S21)。

[0097] 另外,当第二光信号在法拉第镜FM 124上反射并然后再次穿过第一相位调制器 PM_A 123a时,再次施加第一控制信号,从而调制第二光信号的相位(图4A的S22)。因此,第二光信号在经过第一相位调制器 PM_A 123a时经受两次相位控制,从而校正由偏振引起的相位误差。

[0098] 然而,如图4A所示,在第一光信号穿过第一相位调制器 PM_A 123a并在法拉第镜FM 124上反射之后、再次到达第一相位调制器 PM_A 123a之前,第二光信号可到达第一相位调制器 PM_A 123a(图4A的S21)。

[0099] 因此,在相关技术中,对于第一相位调制器 PM_A 123a,需要在时间S21施加用于第二光信号的第一控制信号,并然后去除第一控制信号,并且在时间S22施加用于第二光信号的第二控制信号,并然后去除第二控制信号。因此,为了适当地控制第一光信号和第二光信号,需要准确地控制第一光信号和第二光信号,同时快速转换用于第一相位调制器 PM_A 123a的控制信号。

[0100] 然而,在根据本公开实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥

分配系统中,第一路径P1的长度 L_{p1} 和第二路径P2的长度 L_{p2} 之间的差($dL=L_{p2}-L_{p1}$)等于或大于偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。因此,可以使用一次性连续控制信号来控制偏振相关元件123,并且可以校正由偏振相关特性引起的误差。

[0101] 更具体地说,如图4B所示,在本公开中,在进入接收机120的第一光信号穿过第一相位调制器 PM_A 123a(图4B的S11)、在法拉第镜FM 124上反射、并然后再次穿过第一相位调制器 PM_A 123a(图4B的S12)之前,第二光信号不到达相位调制器 PM_A 123a。

[0102] 因此,由于在第二光信号进入接收机120时第一光信号已经穿过第一相位调制器 PM_A 123a,所以可以使用图4B所示的用于第二光信号的一次性连续控制信号来控制第一相位调制器 PM_A 123a,从而有效地校正由偏振相关特性引起的误差(图4B的C11)。

[0103] 在下文中,虽然为了说明而描述了提供强度调制器IM 123b作为接收机120中的偏振相关元件123的情况,但是本公开不必限于此。

[0104] 首先,在相关技术中,如图4A所示,当第一光信号进入接收机120时(图4A的S1),在第一光信号穿过强度调制器IM 123b时施加第一控制信号,从而调制第一光信号的强度(图4A的S11)。

[0105] 另外,当第一光信号在法拉第镜FM 124上反射并然后再次穿过强度调制器IM 123b时,再次施加第一控制信号,从而调制第一光信号的强度(图4A的S12)。因此,第一光信号在穿过强度调制器IM 123b时经受两次相位控制,从而校正由偏振引起的相位误差。

[0106] 然而,如图4A所示,在第一光信号穿过强度调制器IM 123b并在法拉第镜FM 124上反射之后、再次到达强度调制器IM 123b之前,第二光信号可到达强度调制器IM 123b(图4A的S21)。

[0107] 因此,在相关技术中,对于强度调制器IM 123b,需要在图4A的时间S11施加用于第一光信号的第一控制信号,并然后去除第一控制信号,并且在图4A的时间S21施加用于第二光信号的第二控制信号,并然后去除第二控制信号。因此,为了适当地控制第一光信号和第二光信号,需要准确地控制第一光信号和第二光信号,同时快速转换用于强度调制器IM 123b的控制信号。

[0108] 然而,在根据本公开实施例的量子密钥分配方法、量子密钥分配装置、和量子密钥分配系统中,发射机110中的第一路径P1的长度 L_{p1} 和第二路径P2的长度 L_{p2} 之间的差($dL=L_{p2}-L_{p1}$)等于或大于偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。因此,可以使用一次性连续控制信号来控制偏振相关元件123,并由此根据实施例可以校正由偏振相关特性引起的误差。

[0109] 因此,在根据本公开的双向量子密钥分配系统100中,接收机120和发射机110被设计为使得例如通过调整布置于发射机110中的干涉仪的延迟线DL 115的长度、以及布置于接收机120中的法拉第镜FM 124与第一相位调制器 PM_A 123a和强度调制器IM 123b之间的间隔,发射机110传送的第一光信号和第二光信号中的第一光信号被法拉第镜FM 124反射,并然后在第二光信号到达接收机120的第一相位调制器 PM_A 123a之前可以离开接收机120的第一相位调制器 PM_A 123a,从而第一光信号不受影响而第二光信号受到第一相位调制器 PM_A 123a和强度调制器IM 123b的影响。

[0110] 尽管已经描述了例如使用第一相位调制器123a和强度调制器123b来控制第一光信号和第二光信号的情况,但是本公开不必限于此,并且可以采用各种其他偏振相关元件

123。

[0111] 此外,在根据本公开的实施例的量子密钥分配系统100中,虽然接收机120的多个偏振相关元件123可以如图3所示连续地布置(图3的第一相位调制器123a和强度调制器123b),但是多个偏振相关元件123可以以各种形式配置,例如使用光学元件(例如分束器BS(图5的(a))或环行器(图5的(b)))分开布置,以分离光链路或改变方向,如图5所示。这里,每个偏振相关元件123可以取决于目的单独调制第一光信号和第二光信号,或者可以调制第一光信号和第二光信号两者。

[0112] 图6图示了根据本公开的实施例的量子密钥分配系统100的发射机110,而图7图示了根据本公开的实施例的量子密钥分配系统100的接收机120。

[0113] 由于在根据本公开的实施例的量子密钥分配系统100的前述描述中已经详细解释了发射机110和接收机120,因此下面将描述根据本公开的实施例的量子密钥分配系统100的发射机110和接收机120的配置和操作的要义。

[0114] 首先,如图6所示,发射机110可与接收机120分配量子密码密钥。发射机110可包括 i) 光源111,用于生成光信号, ii) 分束器113,用于将光信号分成第一光信号和第二光信号,将第一光信号输出到第一路径P1,并将第二光信号输出到第二路径P2,以及 iii) 延迟线115,提供在第二路径P2中以延伸第二光信号的传播路径。

[0115] 这里,第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于既然手机120中提供的偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0116] 如图7所示,接收机120可以与发射机110分配量子密码密钥。接收机120可以包括 i) 偏振相关元件123,其操作特性取决于光信号的偏振而改变,以及 ii) 法拉第镜124,其通过将光信号的偏振旋转90度来反射进入的光信号。这里,当在发射机110中生成的光信号被分成穿过第一路径P1的第一光信号和穿过比第一路径P1长的第二路径P2的第二光信号、并依次传送第一光信号和第二光信号时,通过量子信道130入射的第一光信号和第二光信号经由偏振相关元件123在法拉第镜124上反射,再次穿过偏振相关元件123,并且然后通过量子信道130传送到发射机110。

[0117] 这里,发射机110中第一路径P1的长度 L_{P1} 和第二路径P2的长度 L_{P2} 之间的差($dL=L_{P2}-L_{P1}$)等于或大于偏振相关元件123与法拉第镜124之间的距离(=D)的两倍($dL \geq 2D$)。

[0118] 根据该实施例,接收机120在量子密钥分配系统100中使用偏振相关元件123配置,其中光信号来回穿过与双向结构相同的光链路。因此,根据实施例的量子密钥分配系统100可以使用一次性连续控制信号来控制偏振相关元件123,从而校正由偏振相关特性引起的误差。

[0119] 提供上述描述仅用于解释本公开的技术思想,并且对于本公开所属领域的普通技术人员显而易见的是,可以在本公开中进行各种修改和变化而不背离本公开的必要性。提供在此公开的实施例不是为了限制而是为了描述本公开的技术思想,并且不限制本公开的范围。本公开的范围应理解为由所附权利要求限定,并且在所附权利要求及其等同物内的任何技术思想均应理解为包括在本公开的范围之内。

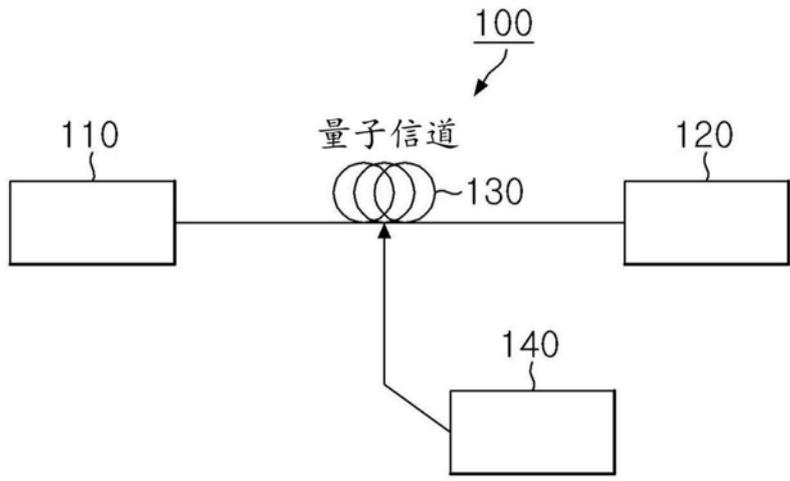


图1

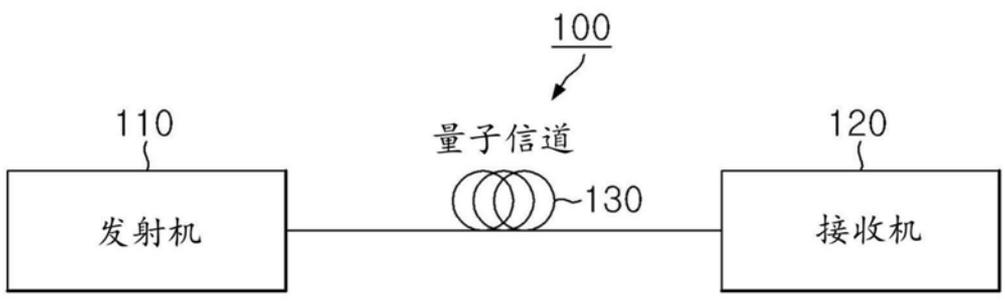


图2

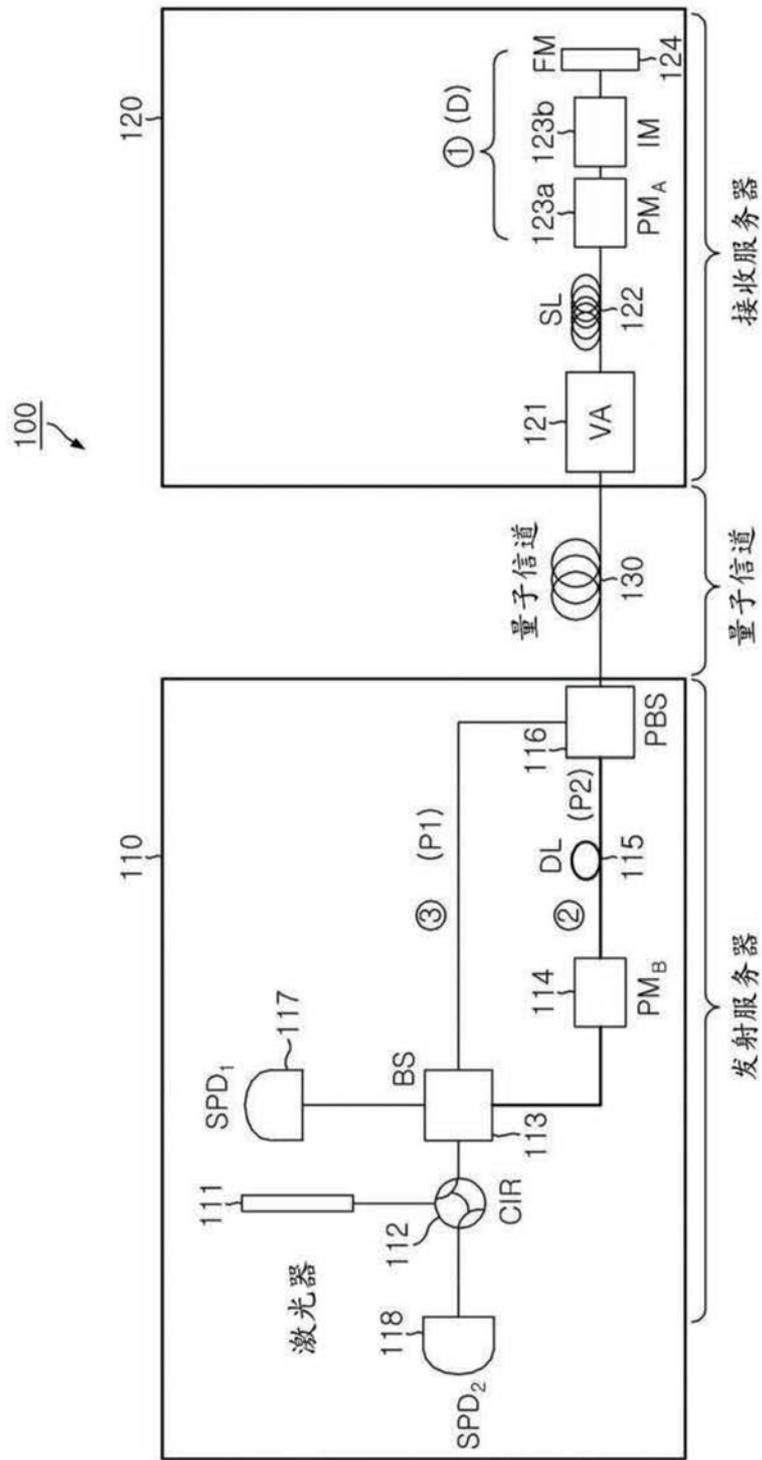


图3

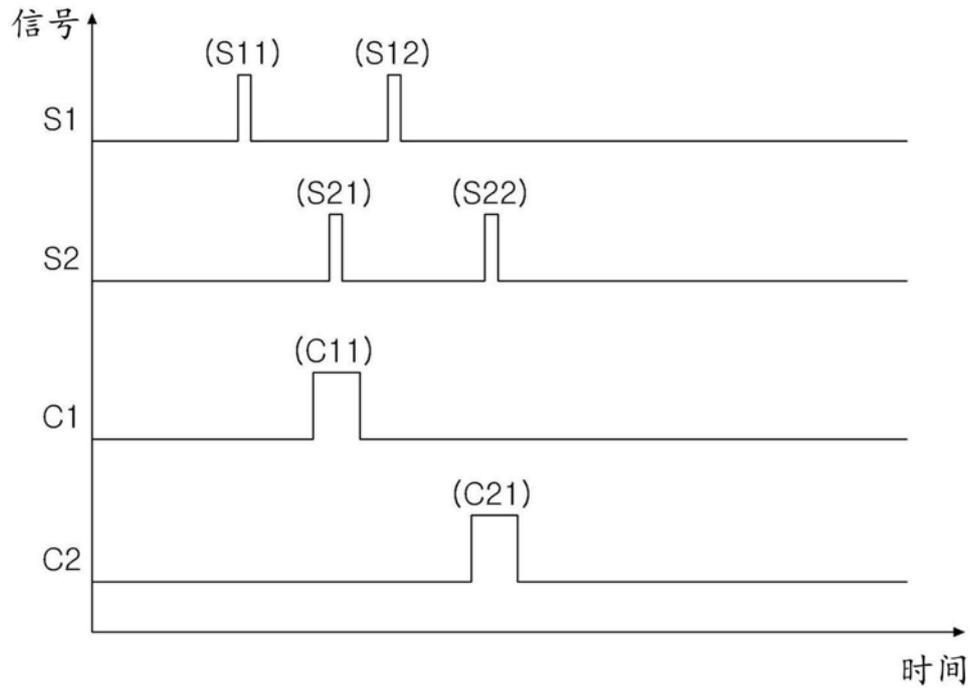


图4A

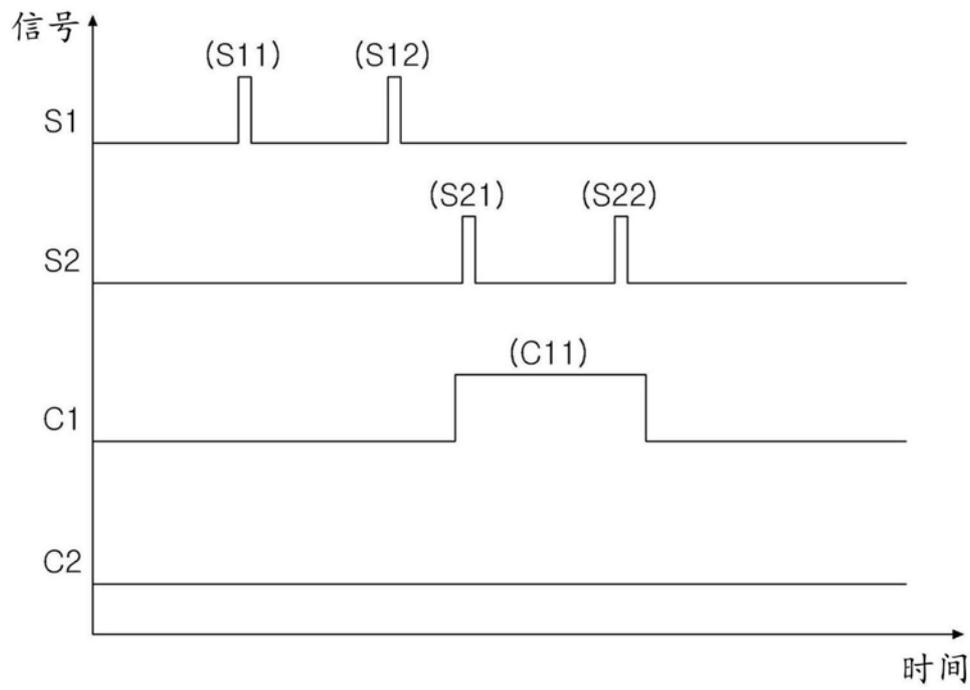


图4B

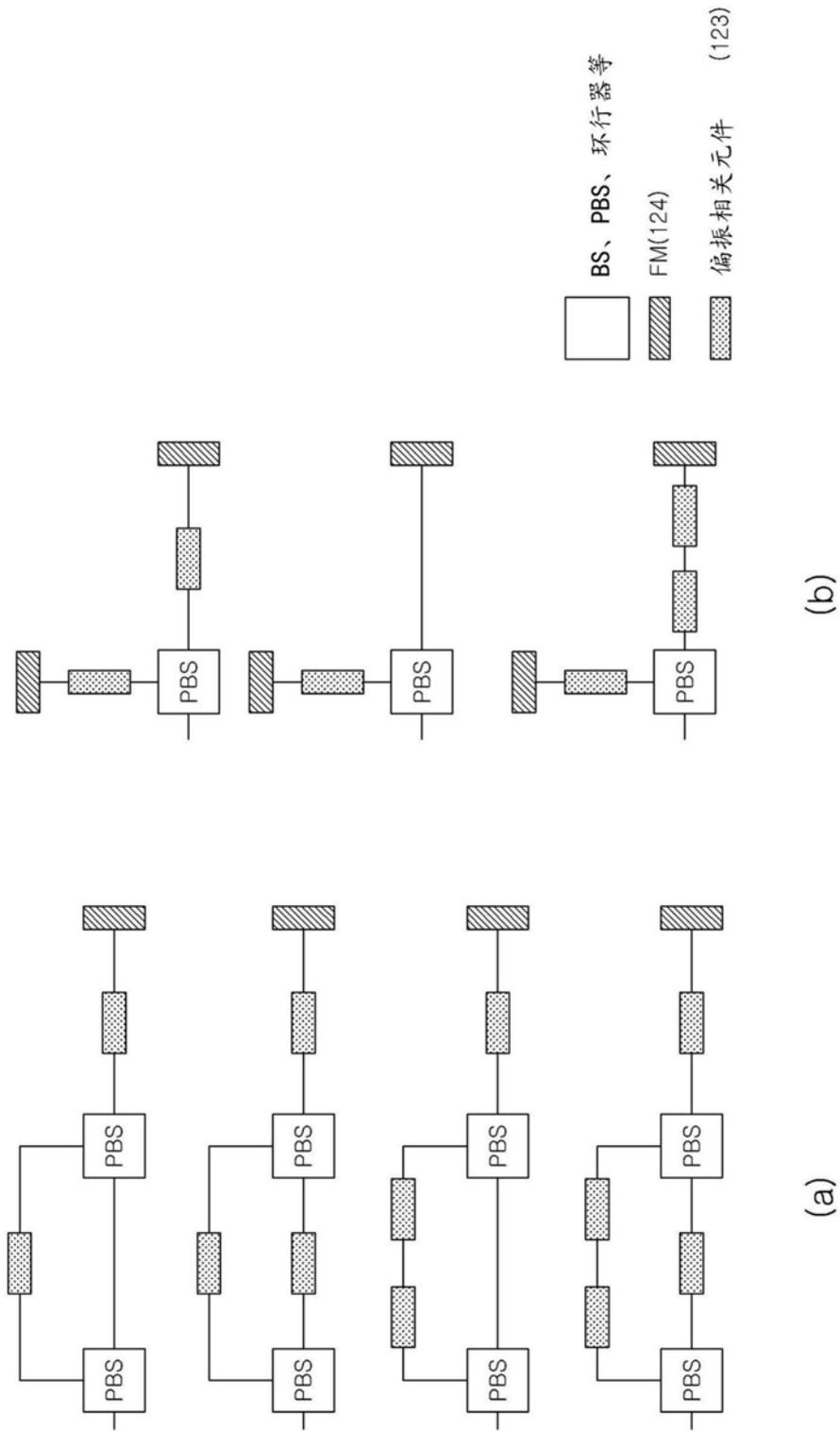


图5

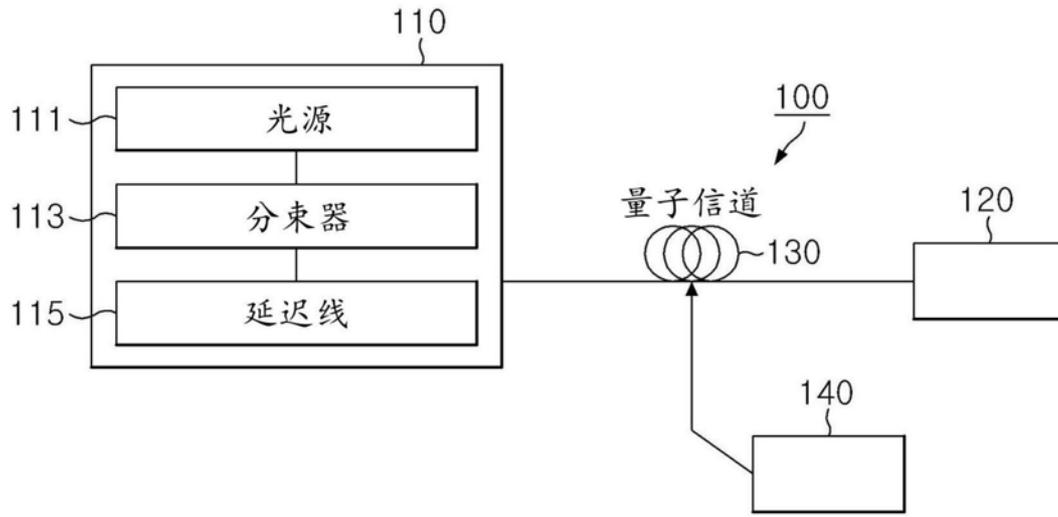


图6

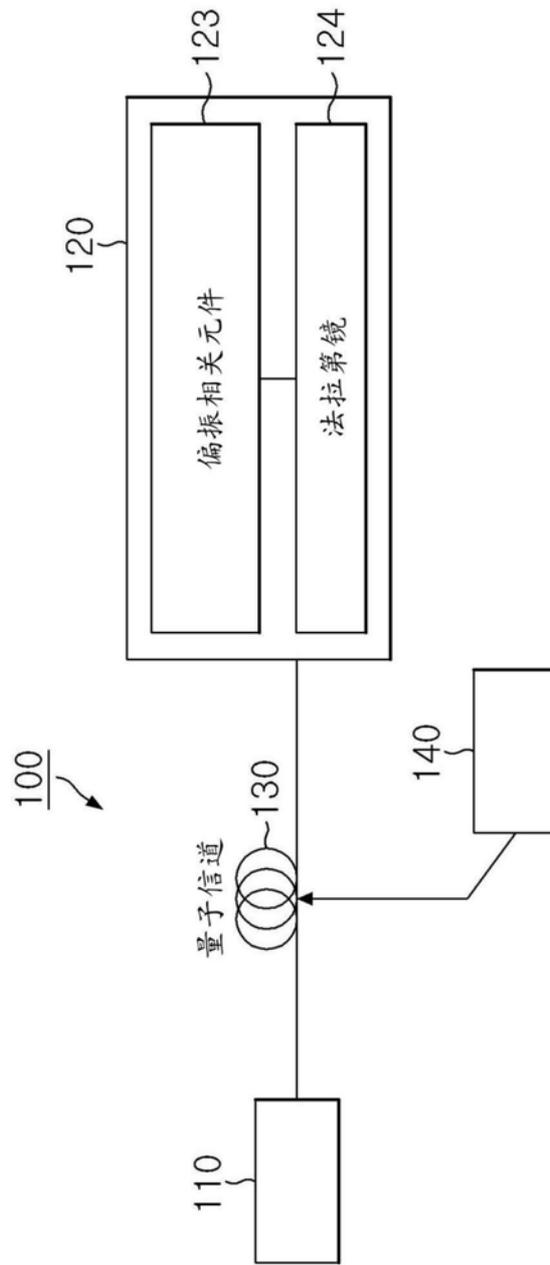


图7