



(12)发明专利

(10)授权公告号 CN 106656491 B

(45)授权公告日 2019.08.09

(21)申请号 201611254402.X

H04B 10/50(2013.01)

(22)申请日 2016.12.30

H04B 10/524(2013.01)

(65)同一申请的已公布的文献号

H04B 10/548(2013.01)

申请公布号 CN 106656491 A

H04B 10/80(2013.01)

(43)申请公布日 2017.05.10

(73)专利权人 北京信息科学技术研究院

地址 100878 北京市西城区府右街10号

专利权人 安徽问天量子科技股份有限公司

(72)发明人 王宇 张启发 景传明 李晨曦

黄敦峰

(74)专利代理机构 北京连城创新知识产权代理

有限公司 11254

代理人 郝学江

(56)对比文件

CN 106100837 A,2016.11.09,

CN 102739394 A,2012.10.17,

CN 103178954 A,2013.06.26,

CN 103199994 A,2013.07.10,

CN 103929300 A,2014.07.16,

CN 101324441 A,2008.12.17,

US 2005078827 A1,2005.04.14,

EP 1742408 A2,2007.01.10,

审查员 刘永辉

(51)Int.Cl.

H04L 9/08(2006.01)

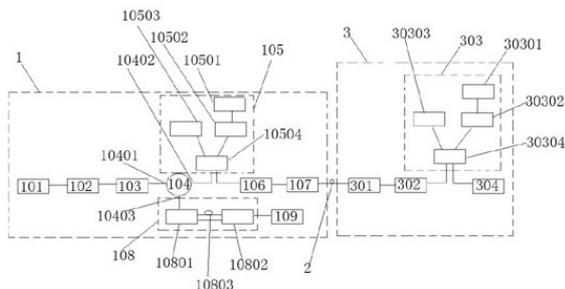
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种量子密钥分配系统中相位调制器半波电压的补偿方法

(57)摘要

本发明属于量子密码技术领域,具体涉及一种量子密钥分配系统中相位调制器半波电压的补偿方法,装置包括:发送端和接收端,其中,所述发送端包括:DFB激光器、光强调制器、电控衰减器、光环形器、马赫曾德干涉仪、光电探测器、FPGA、法拉第迈克尔逊干涉仪、光隔离器和波分复用器,所述接收端包括:波分复用器、光隔离器、法拉第迈克尔逊干涉仪和单光子探测器;方法:先得到发送端相位调制器的相位与电压加载关系,再进行量子密钥分配发送两干涉仪技术探测,再FPGA提取计数分析归纳,再根据相位电压关系进行补偿。本发明通过闭环监测实时跟踪相位调制器的电压-相位关系漂移的问题,并实时进行补偿,提高了半波电压的测量精度。



1. 一种基于量子密钥分配系统对相位调制器半波电压进行补偿的装置,包括:发送端和接收端,其中,所述发送端包括:DFB激光器、光强调制器、电控衰减器、法拉第迈克尔逊干涉仪、光隔离器和波分复用器,其中,所述DFB激光器与所述光强调制器相连,用于产生光脉冲,所述光强调制器分别与所述DFB激光器和电控衰减器相连,用于对光脉冲进行信号态和诱骗态调制变为光脉冲信号,所述电控衰减器分别与所述光强调制器和光环形器相连,用于将所述光脉冲信号衰减成单光子信号,所述法拉第迈克尔逊干涉仪分别与所述光环形器和光隔离器相连,用于对单光子信号产生干涉,所述光隔离器分别与所述法拉第迈克尔逊干涉仪和波分复用器相连,用于使单光子信号单向导通,其特征在于,

所述发送端还包括:光环形器、马赫曾德干涉仪、光电探测器和FPGA,其中,所述光环形器包括第一端口、第二端口和第三端口,所述第一端口与第二端口形成第一通道,所述第二端口和第三端口形成第二通道,所述第一端口与所述电控衰减器相连,所述第二端口与所述法拉第迈克尔逊干涉仪中的光分束器相连,所述第三端口与所述马赫曾德干涉仪相连,用于使经所述第一通道传输至所述法拉第迈克尔逊干涉仪中进行干涉的单光子信号再经所述第二通道传输至所述马赫曾德干涉仪中再次进行光子干涉,所述马赫曾德干涉仪包括:第一光分束器和第二光分束器,所述第一光分束器和第二光分束器通过光纤延时线相连,用于对单光子信号进行延时处理,所述光电探测器分别与所述第二光分束器和FPGA相连,用于对单光子信号进行探测且转换成电信号。

2. 根据权利要求1所述的装置,其特征在于,所述接收端包括:波分复用器、光隔离器、法拉第迈克尔逊干涉仪和单光子探测器,所述接收端的波分复用器与所述发送端的波分复用器通过公共信道相连,用于将发送端的不同波长的单光子信号进行合束后传输至接收端,所述光隔离器分别与所述波分复用器和法拉第迈克尔逊干涉仪相连,所述单光子探测器与所述法拉第迈克尔逊干涉仪相连,用于对单光子信号进行探测。

3. 根据权利要求1-2中任一项所述的装置,其特征在于,所述接收端中的法拉第迈克尔逊干涉仪与所述发送端的法拉第迈克尔逊干涉仪结构相同,均包括:第一法拉第反射镜、相位调制器、第二法拉第反射镜和光分束器,其中,所述第一法拉第反射镜与所述相位调制器相连,用于对单光子信号进行反射,所述相位调制器分别与所述第一法拉第反射镜和光分束器相连,用于对单光子信号进行相位调制,所述第二法拉第反射镜与所述光分束器连接,所述发送端的光分束器分别与所述发送端的第二法拉第反射镜、相位调制器、光环形器和光隔离器相连,所述接收端的光分束器分别与所述接收端的第二法拉第反射镜、相位调制器、光隔离器和单光子探测器相连,均用于对一束单光子信号按比例分束。

4. 根据权利要求1所述的装置,其特征在于,所述装置频率为50M,所述光脉冲信号间隔时间为20ns,所述延时时间为20ns,所述电信号为电压信号。

5. 一种利用权利要求1-4中任一项所述的装置进行补偿的方法,其特征在于,包括以下步骤:

第一步:通过DFB激光器发出的前一光脉冲传输至所述发送端的相位调制器时,将所述发送端的相位调制器的电压固定为0V,后一脉冲传输至所述发送端的相位调制器时,所述发送端的相位调制器的电压在0V至 $V_0$ 范围内变化,每隔0.1V变化一次,具体步骤为固定一个在0V至 $V_0$ 范围内变化的电压扫描N个点,扫描完成一个电压,得到计数值,然后在0V至 $V_0$ 范

围内固定下一个电压进行扫描,然后根据干涉计数比例公式  $y = [1 + \cos(\Delta\varphi)]/2$ , 计算出相应的  $\Delta\varphi$  值,由此得到所述发送端的相位调制器的相位电压加载关系,其中,所述  $y$  表示为:每个固定电压值扫描得到的计数值与前一光脉冲和后一光脉冲传输至所述发送端的相位调制器均加载0V时的计数值之比的比例值,  $\Delta\varphi$  表示干涉的两个光子的相位差;

第二步:所述装置进行量子密钥分配,在量子密钥分配的过程中,所述发送端的相位调制器每隔20ns随机加载相位为 $0\pi$ 、 $\pi/2$ 、 $\pi$ 、 $3\pi/2$ 中的一个相位,所述DFB激光器发出的前、后光脉冲经所述光强调制器变为前、后光脉冲信号,再经过所述电控衰减器,将所述前、后光脉冲信号衰减成所述前、后单光子信号,所述前、后单光子信号经所述光环形器的第一通道传输至所述发送端的法拉第迈克尔逊干涉仪进行干涉,干涉后的前、后单光子信号一部分经所述光隔离器和波分复用器传输至所述接收端的法拉第迈克尔逊干涉仪进行量子密钥分配,另一部分经所述光环形器的第二通道传输至所述马赫曾德干涉仪进行干涉,经过所述马赫曾德干涉仪干涉后的单光子,传输至所述光电探测器进行计数,所述FPGA对探测的信息进行提取分析,根据所述发送端相位调制器加载的相位进行归类,提取出前、后脉冲加载相位差分别为 $\pi/2$ 和 $3\pi/2$ 的计数值 $N_{a=1,2,3,4,5,6,7,8}$ ,对计数值进行计算;

第三步:选取 $N_{a=1,2,7,8}$ 计数值,设半波电压相位漂移角度为 $2\theta$ ,

则:  $\frac{[1 + \cos(\frac{\pi}{2} - \theta)]}{2} = (N_1 + N_8)/(N_1 + N_2 + N_7 + N_8)$  计算出 $\theta$ 的值,得到所述半波

电压漂移角度 $2\theta$ 的值,然后根据所述步骤一中得到的相位电压加载关系得到需补偿的电压值,其中, $N_1$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi/2$ 且发送端相位调制器后一脉冲加载的相位为0时的计数值, $N_2$ 为所述发送端相位调制器前一脉冲加载的相位为 $3\pi/2$ 且发送端相位调制器后一脉冲加载的相位为0时的计数值, $N_7$ 为所述发送端相位调制器前一脉冲加载的相位为0且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值, $N_8$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi$ 且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值。

6. 根据权利要求5所述的方法,其特征在于,所述步骤一中, $N$ 为10000。

## 一种量子密钥分配系统中相位调制器半波电压的补偿方法

### 技术领域

[0001] 本发明属于量子密码技术领域,具体涉及一种基于量子密钥分配系统对相位调制器半波电压进行补偿的装置及方法。

### 背景技术

[0002] 基于法拉第迈克尔逊(F-M)干涉环的量子密钥分配系统中,相位调制器的相位加载准确与否,直接影响到系统的整体性能。当相位调制器加载的半波电压值有所波动时,造成系统的误码率升高,降低密钥生成率,并且严重影响成码的随机性。针对半波电压值的波动,对发送端和接收端均实时进行扫描,会降低系统的效率。实际的设备运行时,通过采用固定发送端半波电压值不变,实时扫描接收端相位电压。针对半波电压值的波动,通常是通过扫描模式,采用极值法寻找相位调制器的半波电压,固定一端的相位调制器加载电压,扫描另一端,通过最大值和最小值来确定相位调制器的半波电压。此方法是基于发送端相位调制器电压-相位关系稳定的前提,但该电压-相位关系存在漂移现象,因此接收端和发送端任何一方存在漂移现象都会引入误差;而且采用极值法只能粗略的测量相位调制器的半波电压,导致发送端相位电压加载存在误差,无法实现更高的精度。因此如何设计一种对相位电压进行补偿,提高相位电压精度的装置及方法成为本领域亟需解决的技术问题。

### 发明内容

[0003] 针对现有技术的不足,本发明提出了基于量子密钥分配系统对相位调制器半波电压进行补偿的装置及方法,本发明对通过对单端相位调制系统进行改进,提高了量子密钥分配中相位调制的半波电压加载精度,同时在量子密钥分配过程中,通过闭环监测实时跟踪相位调制器的电压-相位关系漂移的问题,并实时进行补偿,实现了单端相位纠偏。

[0004] 为解决上述技术问题,本发明采取的技术方案为:本发明提出了一种基于量子密钥分配系统对相位调制器半波电压进行补偿的装置,根据本发明的实施例,包括:发送端和接收端,其中,所述发送端包括:DFB激光器、光强调制器、电控衰减器、法拉第迈克尔逊干涉仪、光隔离器和波分复用器,其中,所述DFB激光器与所述光强调制器相连,用于产生脉冲光,所述光强调制器分别与所述DFB激光器和电控衰减器相连,用于对脉冲光进行信号态和诱骗态调制变为脉冲光信号,所述电控衰减器分别与所述光强调制器和光环形器相连,用于将所述光脉冲信号衰减成单光子信号,所述法拉第迈克尔逊干涉仪分别与所述光环形器和光隔离器相连,用于对单光子信号产生干涉,所述光隔离器分别与所述法拉第迈克尔逊干涉仪和波分复用器相连,用于使单光子信号单向导通,所述发送端还包括:光环形器、马赫曾德干涉仪、光电探测器和FPGA,其中,所述光环形器包括第一端口、第二端口和第三端口,所述第一端口与第二端口形成第一通道,所述第二端口和第三端口形成第二通道,所述第一端口与所述电控衰减器相连,所述第二端口与所述法拉第迈克尔逊干涉仪中的光分束器相连,所述第三端口与所述马赫曾德干涉仪相连,用于使经所述第一通道传输至所述法拉第迈克尔逊干涉仪中进行干涉的单光子信号再经所述第二通道传输至所述马赫曾德干

涉仪中再次进行光子干涉,所述马赫曾德干涉仪包括:第一光分束器和第二光分束器,所述第一光分束器和第二光分束器通过光纤延时线相连,用于对单光子信号进行延时处理,所述光电探测器分别与所述第二光分束器和FPGA相连,用于对单光子信号进行探测且转换成电信号。

[0005] 发明人发现,通过本发明所述的装置和方法,在量子密钥分配过程中,通过闭环监测实时跟踪相位调制器的电压-相位关系漂移的问题,并实时进行补偿,实现了单端相位纠缠,同时不会对系统引入性能上的负面影响,也不会对系统造成效率下降,提高了半波电压的测量精度,同时量子密钥分配系统更稳定,对环境的适应性更强。

[0006] 根据本发明的实施例,所述接收端包括:波分复用器、光隔离器、法拉第迈克尔逊干涉仪和单光子探测器,所述接收端的波分复用器与所述发送端的波分复用器通过公共信道相连,用于将发送端的不同波长的单光子信号进行合束后传输至接收端,所述光隔离器分别与所述波分复用器和法拉第迈克尔逊干涉仪相连,所述单光子探测器与所述法拉第迈克尔逊干涉仪相连,用于对单光子信号进行探测。

[0007] 根据本发明的实施例,所述接收端中的法拉第迈克尔逊干涉仪与所述发送端的法拉第迈克尔逊干涉仪结构相同,均包括:第一法拉第反射镜、相位调制器、第二法拉第反射镜和光分束器,其中,所述第一法拉第反射镜与所述相位调制器相连,用于对单光子信号进行反射,所述相位调制器分别与所述第一法拉第反射镜和光分束器相连,用于对单光子信号进行相位调制,所述第二法拉第反射镜与所述光分束器连接,所述发送端的光分束器分别与所述发送端的第二法拉第反射镜、相位调制器、光环形器和光隔离器相连,所述接收端的光分束器分别与所述接收端的第二法拉第反射镜、相位调制器、光隔离器和单光子探测器相连,均用于对一束单光子信号按比例分束。

[0008] 根据本发明的实施例,所述装置频率为50M,所述光脉冲信号间隔时间为20ns,所述延时时间为20ns,所述电信号为电压信号。

[0009] 在本发明的另一方面,提出了一种利用前面所述装置进行补偿的方法,根据本发明的实施例,包括以下步骤:第一步:通过DFB激光器发出的前一光脉冲传输至所述发送端的相位调制器时,将所述发送端的相位调制器的电压固定为0V,后一脉冲传输至所述发送端的相位调制器时,所述发送端的相位调制器的电压在0V至 $V_0$ 范围内变化,每隔0.1V变化一次,具体步骤为固定一个在0V至 $V_0$ 范围内变化的电压扫描N个点,扫描完成一个电压,得到计数值,然后在0V至 $V_0$ 范围内固定下一个电压进行扫描,然后根据干涉计数比例公式  $y = [1 + \cos(\Delta\phi)]/2$ ,然后计算出相应的 $\Delta\phi$ 值,由此得到所述发送端的相位调制器的相位电压加载关系,其中,所述y表示为:每个固定电压值扫描得到的计数值与前一光脉冲和后一光脉冲传输至所述发送端的相位调制器均加载0V时的计数值之比的比例值, $\Delta\phi$ 表示干涉的两个光子的相位差;第二步:所述装置进行量子密钥分配,在量子密钥分配的过程中,所述DFB激光器发出的前、后脉冲光经所述光强调制器变为前、后脉冲光信号,再经过所述电控衰减器,将所述前、后脉冲光信号衰减成所述前、后单光子信号,所述前、后单光子信号经所述光环形器的第一通道传输至所述发送端的法拉第迈克尔逊干涉仪进行干涉,干涉后的前、后单光子信号一部分经所述光隔离器和波分复用器传输至所述接收端的法拉第迈克尔逊干涉仪进行量子密钥分配,另一部分经所述光环形器的第二通道传输至所述马赫曾德干涉仪进行干涉,经过所述马赫曾德干涉仪干涉后的单光子,传输至所述光电

探测器进行计数,所述FPGA对探测的信息进行提取分析,根据所述发送端相位调制器加载的相位进行归类,提取出前、后脉冲加载相位差分别为 $\pi/2$ 和 $3\pi/2$ 的计数值 $N_{a=1,2,3,4,5,6,7,8}$ ,对计数值进行计算;第三步:选取 $N_{a=1,2,7,8}$ 计数值,设半波电压相位漂移角度为 $2\theta$ ,则:

$$\frac{[1+\cos(\frac{\pi}{2}-\theta)]}{2} = (N_1 + N_8)/(N_1 + N_2 + N_7 + N_8), \text{计算出}\theta\text{的值,得到所述半波电压漂}$$

移角度 $2\theta$ 的值,然后根据所述步骤一中得到的相位电压加载关系得到需补偿的电压值,其中, $N_1$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi/2$ 且发送端相位调制器后一脉冲加载的相位为 $0$ 时的计数值, $N_2$ 为所述发送端相位调制器前一脉冲加载的相位为 $3\pi/2$ 且发送端相位调制器后一脉冲加载的相位为 $0$ 时的计数值, $N_7$ 为所述发送端相位调制器前一脉冲加载的相位为 $0$ 且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值, $N_8$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi$ 且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值。

[0010] 根据本发明的实施例,所述步骤一中, $N$ 为10000。

[0011] 根据本发明的实施例,所述步骤二中,在量子密钥分配的过程中,所述发送端的相位调制器每隔20ns随机加载相位为 $0\pi$ 、 $\pi/2$ 、 $\pi$ 、 $3\pi/2$ 中的一个相位。

[0012] 本发明至少包括以下有益效果:通过本发明所述的装置和方法,在量子密钥分配过程中,通过闭环监测实时跟踪相位调制器的电压-相位关系漂移的问题,并实时进行补偿,实现了单端相位纠偏,同时不会对系统引入性能上的负面影响,也不会对系统造成效率下降,提高了半波电压的测量精度,同时量子密钥分配系统更稳定,对环境的适应性更强。

## 附图说明

[0013] 图1为本发明基于量子密钥分配系统对相位调制器半波电压进行补偿的装置结构示意图。

[0014] 其中,发送端1,DFB激光器101,光强调制器102,电控衰减器103,光环形器104,光环形器第一端口10401,光环形器第二端口10402,光环形器第三端口10403,法拉第迈克尔逊干涉仪105,第一法拉第反射镜10501,相位调制器10502,第二法拉第反射镜10503,光分束器10504,光隔离器106,波分复用器107,马赫曾德干涉仪108,第一光分束器10801,第二光分束器10802,光纤延时线10803,光电探测器109,公共信道2,接收端3,波分复用器301,光隔离器302,法拉第迈克尔逊干涉仪303,第一法拉第反射镜30301,相位调制器30302,第二法拉第反射镜30303,光分束器30304,单光子探测器304。

## 具体实施方式

[0015] 为了使本领域技术人员更好地理解本发明的技术方案,下面结合具体实施例对本发明作进一步的详细说明。下面描述的实施例是示例性的,仅用于解释本发明,而不能理解为对本发明的限制。

[0016] 本发明提出了一种基于量子密钥分配系统对相位调制器半波电压进行补偿的装置,图1为本发明基于量子密钥分配系统对相位调制器半波电压进行补偿的装置结构示意图,参照图1所示,根据本发明的实施例,本发明所述装置包括:发送端1和接收端3,其中,所述发送端包括:DFB激光器101、光强调制器102、电控衰减器103、光环形器104、法拉第迈克尔

尔逊干涉仪105、马赫曾德干涉仪108、光电探测器109、FPGA、光隔离器106和波分复用器107,其中,所述DFB激光器与所述光强调制器相连,用于产生脉冲光,所述光强调制器分别与所述DFB激光器和电控衰减器相连,用于对脉冲光进行信号态和诱骗态调制变为脉冲光信号,所述电控衰减器分别与所述光强调制器和光环形器相连,用于将所述光脉冲信号衰减成单光子信号,所述光环形器包括第一端口10401、第二端口10402和第三端口10403,所述第一端口与第二端口形成第一通道,所述第二端口和第三端口形成第二通道,所述第一端口与所述电控衰减器相连,所述第二端口与所述法拉第迈克尔逊干涉仪中的光分束器相连,所述第三端口与所述马赫曾德干涉仪相连,用于使经所述第一通道传输至所述法拉第迈克尔逊干涉仪中进行干涉的单光子信号再经所述第二通道传输至所述马赫曾德干涉仪中再次进行光子干涉,所述法拉第迈克尔逊干涉仪分别与所述光环形器和光隔离器相连,用于对单光子信号产生干涉,其包括:第一法拉第反射镜10501、相位调制器10502、第二法拉第反射镜10503和光分束器10504,其中,所述第一法拉第反射镜与所述相位调制器相连,用于对单光子信号进行反射,所述相位调制器分别与所述第一法拉第反射镜和光分束器相连,用于对单光子信号进行相位调制,所述第二法拉第反射镜与所述光分束器连接,所述发送端的光分束器分别与所述发送端的第二法拉第反射镜、相位调制器、光环形器和光隔离器相连,所述马赫曾德干涉仪包括:第一光分束器10801和第二光分束器10802,所述第一光分束器和第二光分束器通过光纤延时线10803相连,用于对单光子信号进行延时处理,所述光电探测器分别与所述第二光分束器和FPGA相连,用于对单光子信号进行探测且转换成电信号,所述光隔离器分别与所述法拉第迈克尔逊干涉仪和波分复用器相连,用于使单光子信号单向导通。

[0017] 根据本发明的实施例,参照图1所示,所述接收端3包括:波分复用器301、光隔离器302、法拉第迈克尔逊干涉仪303和单光子探测器304,所述接收端的波分复用器与所述发送端的波分复用器通过公共信道2相连,用于将发送端的不同波长的单光子信号进行合束后传输至接收端,所述光隔离器分别与所述波分复用器和法拉第迈克尔逊干涉仪相连,所述单光子探测器与所述法拉第迈克尔逊干涉仪相连,用于对单光子信号进行探测。

[0018] 根据本发明的实施例,参照图1所示,所述接收端中的法拉第迈克尔逊干涉仪与所述发送端的法拉第迈克尔逊干涉仪结构相同,均包括:第一法拉第反射镜30301、相位调制器30302、第二法拉第反射镜30303和光分束器30304,其中,所述第一法拉第反射镜与所述相位调制器相连,用于对单光子信号进行反射,所述相位调制器分别与所述第一法拉第反射镜和光分束器相连,用于对单光子信号进行相位调制,所述第二法拉第反射镜与所述光分束器连接,所述接收端的光分束器分别与所述接收端的第二法拉第反射镜、相位调制器、光隔离器和单光子探测器相连,均用于对一束单光子信号按比例分束。

[0019] 根据本发明的一些实施例,本发明所述装置的频率为50M,所述光脉冲信号间隔时间为20ns,所述延时时间为20ns,所述电信号为电压信号。

[0020] 在本发明的另一方面,提供了一种利用前面所述的装置进行补偿的方法,根据本发明的实施例,包括以下步骤:第一步:通过DFB激光器发出的前一光脉冲传输至所述发送端的相位调制器时,将所述发送端的相位调制器的电压固定为0V,后一脉冲传输至所述发送端的相位调制器时,所述发送端的相位调制器的电压在0V至 $V_0$ 范围内变化,每隔0.1V变化一次,具体步骤为固定一个在0V至 $V_0$ 范围内变化的电压扫描10000个点,扫描完成一个电

压,得到计数值,然后在0V至 $V_0$ 范围内固定下一个电压进行扫描,然后根据干涉计数比例公式 $y = [1 + \cos(\Delta\varphi)]/2$ ,然后计算出相应的 $\Delta\varphi$ 值,由此得到所述发送端的相位调制器的相位电压加载关系,其中,所述y表示为:每个固定电压值扫描得到的计数值与前一光脉冲和后一光脉冲传输至所述发送端的相位调制器均加载0V时的计数值之比的比例值, $\Delta\varphi$ 表示干涉的两个光子的相位差。

[0021] 根据本发明的实施例,第二步:所述装置进行量子密钥分配,在量子密钥分配的过程中,所述DFB激光器发出的前、后脉冲光经所述光强调制器变为前、后脉冲光信号,再经过所述电控衰减器,将所述前、后脉冲光信号衰减成所述前、后单光子信号,所述前、后单光子信号经所述光环形器的第一通道传输至所述发送端的法拉第迈克尔逊干涉仪进行干涉,干涉后的前、后单光子信号一部分经所述光隔离器和波分复用器传输至所述接收端的法拉第迈克尔逊干涉仪进行量子密钥分配,另一部分经所述光环形器的第二通道传输至所述马赫曾德干涉仪进行干涉,经过所述马赫曾德干涉仪干涉后的单光子,传输至所述光电探测器进行计数,所述FPGA对探测的信息进行提取分析,根据所述发送端相位调制器加载的相位进行归类,提取出前、后脉冲加载相位差分别为 $\pi/2$ 和 $3\pi/2$ 的计数值 $N_{a=1,2,3,4,5,6,7,8}$ ,对计数值进行计算。

[0022] 根据本发明的实施例,在量子密钥分配的过程中,所述发送端的相位调制器每隔20ns随机加载相位为 $0\pi$ 、 $\pi/2$ 、 $\pi$ 、 $3\pi/2$ 中的一个相位。

[0023] 根据本发明的实施例,所述发送端包括:DFB激光器、光强调制器、电控衰减器、光环形器、法拉第迈克尔逊干涉仪、马赫曾德干涉仪、光电探测器、FPGA、光隔离器和波分复用器,其中,所述DFB激光器与所述光强调制器相连,用于产生脉冲光,所述光强调制器分别与所述DFB激光器和电控衰减器相连,用于对脉冲光进行信号态和诱骗态调制变为脉冲光信号,所述电控衰减器分别与所述光强调制器和光环形器相连,用于将所述光脉冲信号衰减成单光子信号,所述光环形器包括第一端口、第二端口和第三端口,所述第一端口与第二端口形成第一通道,所述第二端口和第三端口形成第二通道,所述第一端口与所述电控衰减器相连,所述第二端口与所述法拉第迈克尔逊干涉仪中的光分束器相连,所述第三端口与所述马赫曾德干涉仪相连,用于使经所述第一通道传输至所述法拉第迈克尔逊干涉仪中进行干涉的单光子信号再经所述第二通道传输至所述马赫曾德干涉仪中再次进行光子干涉,所述法拉第迈克尔逊干涉仪分别与所述光环形器和光隔离器相连,用于对单光子信号产生干涉,所述马赫曾德干涉仪包括:第一光分束器和第二光分束器,所述第一光分束器和第二光分束器通过光纤延时线相连,用于对单光子信号进行延时处理,所述光电探测器分别与所述第二光分束器和FPGA相连,用于对单光子信号进行探测且转换成电信号,所述光隔离器分别与所述法拉第迈克尔逊干涉仪和波分复用器相连,用于使单光子信号单向导通。

[0024] 根据本发明的实施例,实际传输过程中发送端PD采集数据计数统计如下所示:

	发送端 PM 前一脉冲				
	发送端 PM	0	$\pi/2$	$\pi$	$3\pi/2$
	后一脉冲				
[0025]	0		N1		N2
	$\pi/2$	N3		N4	
	$\pi$		N5		N6
	$3\pi/2$	N7		N8	

[0026] 第三步:选取 $N_{a=1,2,7,8}$ 计数值,设半波电压相位漂移角度为 $2\theta$ ,

[0027] 则:  $\frac{1+\cos(\frac{\pi}{2}-\theta)}{2} = (N_1 + N_8)/(N_1 + N_2 + N_7 + N_8)$ ,计算出 $\theta$ 的值,得到所述

半波电压漂移角度 $2\theta$ 的值,然后根据所述步骤一中得到的相位电压加载关系得到需补偿的电压值,提高半波电压的测量精度,其中, $N_1$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi/2$ 且发送端相位调制器后一脉冲加载的相位为0时的计数值, $N_2$ 为所述发送端相位调制器前一脉冲加载的相位为 $3\pi/2$ 且发送端相位调制器后一脉冲加载的相位为0时的计数值, $N_7$ 为所述发送端相位调制器前一脉冲加载的相位为0且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值, $N_8$ 为所述发送端相位调制器前一脉冲加载的相位为 $\pi$ 且发送端相位调制器后一脉冲加载的相位为 $3\pi/2$ 时的计数值。

[0028] 发明人发现,通过本发明所述的装置和方法,在量子密钥分配过程中,通过闭环监测实时跟踪相位调制器的电压-相位关系漂移的问题,并实时进行补偿,实现了单端相位纠偏,同时不会对系统引入性能上的负面影响,也不会对系统造成效率下降,提高了半波电压的测量精度,同时量子密钥分配系统更稳定,对环境的适应性更强。

[0029] 在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示意性实施例”、“示例”、“具体示例”或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0030] 在本发明的描述中,需要说明的是,除非另有明确的规定和限定,术语“相连”和“连接”应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或一体地连接;可以是机械连接,也可以是点连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本发明中的具体含义。

[0031] 尽管上面已经示出和描述了本发明的实施例,可以理解的是,上述实施例是示例性的,不能理解为对本发明的限制,本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型,同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处。

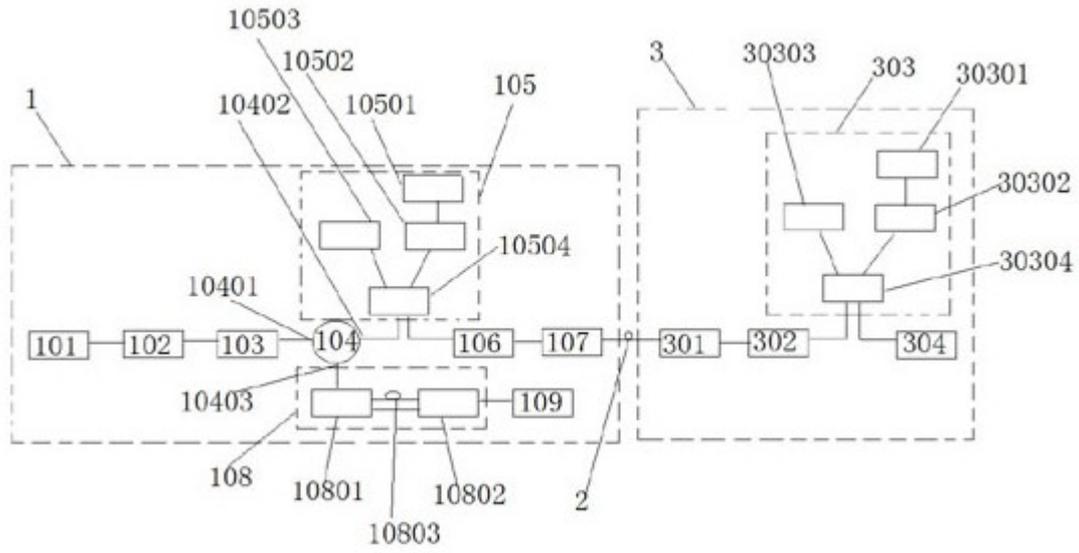


图1