8052

证书号第1816072号

北京市海淀区地方税务局 印花税 代扣专用章 国家知识产权局

发明专利证书

发明名称：连续变量量子密钥分发系统及其相位补偿方法

发明人：申泽源；肖俊俊；代文超；何广强；曾贵华

专利号：ZL 2012 1 0310637.1

专利申请日：2012年08月28日

专利权人：上海交通大学

授权公告日：2015年10月14日

本发明经过本局依照中华人民共和国专利法进行审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为二十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年08月28日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

中华人民共和国国家知识产权局

2015年10月14日

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102868520 A
(43)申请公布日 2013.01.09

(21)申请号 201210310637.1

(22)申请日 2012.08.28

(71)申请人 上海交通大学
地址 200240 上海市闵行区东川路 800 号

(72)发明人 申泽源 肖俊俊 代文超 何广强 曾贵华

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中

(51)Int.Cl.
H04L 9/08(2006.01)

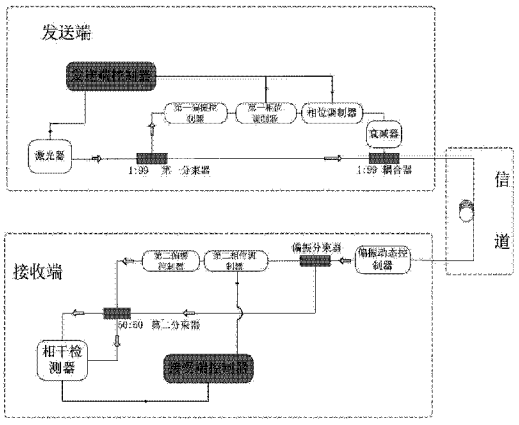
权利要求书 2 页 说明书 7 页 附图 1 页

(54)发明名称

连续变量量子密钥分发系统及其相位补偿方法

(57)摘要

本发明涉及一种连续变量量子密钥分发系统及其相位补偿方法，该方法包括以下步骤：发送端确定发送相位补偿帧及相位补偿帧的插入信号中的频率 A 的取值；发送端发送一个相位补偿帧，且接(A-1)个信号帧；接收端从相干检测器输出信号中采样，提取出相位补偿帧；根据相位补偿帧计算需要补偿的电压值，通过第二相位调制器把补偿电压值补偿到(A-1)个密钥帧相位上去，实现消去环境和系统噪声，并将补偿后的(A-1)个密钥帧储存至原始密钥文件中；接收端接收到下一个相位补偿帧，并提取出相位补偿帧，重复上述操作；发送端发送中断传输信号，接收端接收到中断传输信号后，停止接收，密钥分发完成。本发明具有误码率低、通信可靠的优点。



CN 102868520 A

1. 一种连续变量量子密钥分发系统，包括发送端和接收端，所述发送端包括发送端光路部分和发送端控制器模块，所述接收端包括接收端光路部分和接收端控制器模块，其特征在于，

所述发送端光路部分包括：依次连接的激光器、第一分束器、第一偏振控制器、幅度控制器、第一相位调制器、衰减器和耦合器，其中，所述分束器还与所述耦合器连接；所述激光器用以产生激光，激光出来后经过第一分束器分成2束，1束信号光和1束本振光，一束信号光经过偏振控制器、幅度控制器、相位控制器和衰减器，衰减后的信号光与另外1束本振光在耦合器相遇并耦合成1束激光发送至传输信道；

所述发送端控制器模块包括：真随机密钥产生器、模拟电压输出控制电路和触发时钟电路，所述真随机密钥产生器用以产生真随机密钥，所述第一模拟电压输出控制电路分别与所述真随机密钥产生器、幅度调制器和第一相位调制器连接，用以将所述真随机密钥产生器产生的密钥发送至所述幅度调制器和第一相位调制器，由幅度调制器和相位调制器将密钥调制到激光脉冲上，并根据所述第一相位调制器的调节范围，计算相位补偿帧，随机将相位补偿帧发送至所述第一相位调制器，由所述第一相位调制器将所述相位补偿帧调制到激光脉冲上，然后通过衰减器衰减到量子级别的光脉冲。；

所述触发时钟电路与所述激光器连接，用以触发所述激光器；

所述接收端光路部分包括：偏振动态控制器、偏振分束器、第二相位调节器、第二偏振控制器、第二分束器和相干检测器，所述偏振动态控制器用以消除信号光和本振光在光纤中传输后受到环境的干扰而产生的偏振漂移，偏振分束器将消除偏振漂移的激光脉冲分成2束，1束经过第二相位调制器和第二偏振控制器进行失真补偿，然后与另1束一起进入第二分束器后分为两束分别进入相干检测器进行相干检测，所述相干检测器通过本振光和信号光的干涉作用，把量子级别的信号光的值检测出来；

所述接收端控制器模块包括：模拟电压输入控制电路和第二模拟电压输出控制电路，所述模拟电压输入控制电路与相干检测器相连接，用于接收相干检测后的电信号；所述第二模拟电压输出控制电路与第二相位调制器相连接，通过提取相位补偿帧然后计算得出需要补偿的电压，然后输出这个电压值到第二相位调制器进行相位补偿。

2. 一种连续变量量子密钥分发系统相位补偿方法，其特征在于，包括以下步骤：

（1）连续变量量子密钥分发系统发送端依据相位调制器的调节范围，确定发送相位补偿帧；

（2）根据系统所处的环境，确定相位补偿帧的插入信号中的频率A的取值；

（3）连续变量量子密钥分发系统发送端发送一个相位补偿帧，且接（A-1）个信号帧；

（4）连续变量量子密钥分发系统接收端从相干检测器输出信号中采样，并且提取出相位补偿帧；

（5）连续变量量子密钥分发系统接收端通过提取出的相位补偿帧，根据相位补偿帧的结构计算需要补偿的电压值；

（6）接收端计算出补偿电压值后，通过控制接收端的第二相位调制器把补偿电压值补偿到（A-1）个密钥帧相位上去，实现消去环境和系统噪声；

（7）接收端接收到补偿后的（A-1）个密钥帧，并储存至原始密钥文件中；

（8）接收端接收到下一个相位补偿帧，并提取出相位补偿帧，重复步骤（5）至步骤（7）

的操作；

（9）发送端已完成密钥的分发，发送中断传输信号，接收端接收到中断传输信号后，停止接收，密钥分发完成。

3. 根据权利要求 2 所述的连续变量量子密钥分发系统相位补偿方法，其特征在于，步骤（1）中，相位补偿帧的最佳效果确定为：设所述第一相位控制器的调制范围为：$-V_1$ ～ $+V_1$，取 N 个点作为一帧，N 个点设计为从 $-V_1$ 到 $+V_1$ 的等差数组，相邻 2 个点的差值为（$2V_1$/(N-1)），则相位补偿帧为：

（$-V_1$，$-V_1$+（$2V_1$/(N-1)），$-V_1$+2*（$2V_1$/(N-1)），……，$-V_1$+(N-2)*（$2V_1$/(N-1)），$+V_1$）。

4. 根据权利要求 2 所述的连续变量量子密钥分发系统相位补偿方法，其特征在于，步骤（1）中，相位补偿帧的最简单结构确定为：设所述第一相位控制器的调制范围为：$-V_1$ ～ $+V_1$，取 N 个点作为一帧，N 个点设计为固定一个电压值 V_2，则相位补偿帧为：

（V_2，V_2，V_2，……，V2）。

5. 根据权利要求 2 所述的连续变量量子密钥分发系统相位补偿方法，其特征在于，所述发送端相位补偿帧是按照间隔为 A 的取值循环插入到密钥分发中，相位补偿帧的插入重复频率为 A，即发送端发送了（A-1）个帧的明文后，紧接着发送 1 帧相位补偿帧，相应的，引入相位补偿帧带来的通信额外开销为（1/A）。

6. 根据权利要求 3、4、5 所述的连续变量量子密钥分发系统相位补偿实现方法，其特征在于，所述 N 和 A 的取值选定根据环境条件和系统时钟频率来确定，若环境引起的相位抖动范围为 10~1000 之间，系统时钟频率为 B(MHz)，则 N 和 A 的取值必须符合：$\frac{B\times10^6}{N\times A}\geq1000$。

7. 根据权利要求 3 所述的连续变量量子密钥分发系统相位实现方法，其特征在于，接收端检测到相位补偿帧后，根据相位补偿帧的结构计算需要补偿的电压值，具体计算公式为：

$$\psi=\frac{N_1\times(2\times V_1)}{N}-V_1;$$

其中，N_1 是计算出正弦曲线平移后最大值所在的数组位置。

8. 如权利要求 4 所述的连续变量量子密钥分发系统相位实现方法，其特征在于，接收端检测到相位补偿帧后，根据相位补偿帧的结构计算需要补偿的电压值，具体计算公式为：

$$\psi=360\times\frac{V_3-V_2}{2\times V_1};$$

其中，V_3 是相位抖动值附加到整个帧内所引起的变化后的固定值。

9. 根据权利要求 2 所述的连续变量量子密钥分发系统相位实现方法，其特征在于，步骤（6）中所述的（A-1）个密钥帧是紧接着上一个相位补偿帧的。

10. 根据权利要求 2 所述的连续变量量子密钥分发系统相位实现方法，其特征在于，所述中断传输信号为一段全零数据帧。

连续变量量子密钥分发系统及其相位补偿方法

技术领域

[0001] 本发明涉及光纤量子通信技术领域，具体涉及一种连续变量量子密钥分发系统及其相位补偿方法。

背景技术

[0002] 量子密码学是基于经典密码体制和量子物理体制的新型密码体制，这种密码体制的安全性由量子自身的内秉属性所保证，具体来说，是由量子不可克隆定理和海森堡测不准原理保证了量子密码具有无条件安全性和对窃听的可检测性，使得量子密码具有良好的性能和前景。

[0003] 1969 年，由 S.Wiesner 首先提出量子密码思想，但并没有受到人们的重视。1984 年，美国科学家 C.H.Bennett 和加拿大密码学家 G..Brassard 提出国际上第一个量子密钥分发协议——BB84 协议，这个协议得到了广泛的认可，不久由 Bennett 和 Brassard 采用微弱激光脉冲作为量子信号发生器首次实现基于 BB84 协议的自由空间中的量子密钥分发实验。从此，进入了由经典密码体系进入量子密码体系的时代，量子密码学成为国际上普遍关注的课题之一，各国学者和科学家在理论和实验上从不同的角度开展量子密码研究，并且得到了各国政府的重视和鼎力支持。因此，量子密码学发展迅速，内容得到了极大的扩充，涉及了量子密钥分发、量子密钥验证、量子数据加密、量子秘密共享、量子身份认证、量子签名、量子比特承诺、量子不经意传输、量子多方计算以及量子密码的信息理论。

[0004] 量子密钥分发可以分为离散变量量子密钥分发和连续变量量子密钥分发，BB84 协议是基于离散变量的量子密钥分发实验，所以刚开始，国际上绝大多数的学者目光是对准的是离散变量量子密钥分发的研究，并且得到了很多技术上的突破。但是连续变量量子密钥分发也有着自己的优势，因此，慢慢的人们目光开始转移到连续变量量子密钥上的研究。

[0005] Ralph 在 1999 年首先从实验角度提出连续变量进行量子密钥分发的概念并分析其安全性，从此开启了连续变量量子密钥分配的研究大幕，并且各种方案相继被提出。例如 :基于压缩态的量子密钥分配方案 ;基于压缩态的连续变量纠错码 ;全连续态的量子密钥分配等等。

[0006] 2003 年，F.Grosshans 提出了基于相干态高斯调制的连续变量量子密钥分发方案，该方案引起了学术界的极大关注，因为这种方案实现比较容易，并且后来这个方案的安全性得到了严格的证明。在该方案中，量子态的检测采用的是零差检测，不需要单光子探测器。相比于压缩光，相干光制备比较容易，所以该实验方案的可重复性较高，也是目前各个研究机构重视和采用最多的一种方案。

[0007] 连续变量量子密钥分发作为量子密码学的一个核心的分支，连续变量量子密钥分发从物理上是无条件安全的，经典加密方法一次一密也是绝对安全的，那么，连续变量量子密钥分发后可以采用一次一密加密明文或者采用量子方法加密明文，这两者都是绝对安全的。从这可以看出连续变量量子密钥分发系统在量子密码学中的重要地位。

[0008] 与传统光纤通信中的相位补偿相比较，在连续变量量子密钥分发系统中，有着极

大的不同，传统光纤通信中所有的光源都是强光，无论是频率，相位，时间调制等，环境对相位变化影响有限，主流是用锁相环来消除环境带来的相位扰动。但是连续变量量子密钥分发系统中，信号光的强度在量子级别上的非常小，非常容易收到环境因素和系统噪声带来的影响，产生非常大的随即的相位漂移，而这是不能通过任何锁相环来消除的，必须寻找另外的方法来实现。

[0009] 本发明的目的在于针对连续变量量子密钥分发系统相位补偿方案的空白，提出了一种全新的基于连续变量量子在光纤中特性的相位补偿实现方案，是连续变量量子密钥分发系统实用化中一个关键技术，克服了在光通信过程中连续变量量子受到环境的影响对相位的干扰。

发明内容

[0010] 本发明的目的在于提供一种连续变量量子密钥分发系统，以解决现有技术中连续变量量子密钥分发系统存在容易受环境因素影响产生相位漂移的技术问题。

[0011] 本发明的另一目的在于提供一种连续变量量子密钥分发系统相位补偿方法，以解决现有连续变量量子密钥分发系统存在的受环境因素影响产生相位漂移的技术问题。

[0012] 为达到上述目的，本发明的目的在于提供一种连续变量量子密钥分发系统，包括发送端和接收端，发送端包括发送端光路部分和发送端控制器模块，接收端包括接收端光路部分和接收端控制器模块，其中，

[0013] 发送端光路部分包括：依次连接的激光器、第一分束器、第一偏振控制器、幅度控制器、第一相位调制器、衰减器和耦合器，其中，分束器还与耦合器连接；激光器用以产生激光，激光出来后经过第一分束器分成 2 束，1 束信号光和 1 束本振光，一束信号光经过偏振控制器、幅度控制器、相位控制器和衰减器，衰减后的信号光与另外 1 束本振光在耦合器相遇并耦合成 1 束激光发送至传输信道；

[0014] 发送端控制器模块包括：真随机密钥产生器、模拟电压输出控制电路和触发时钟电路，真随机密钥产生器用以产生真随机密钥，第一模拟电压输出控制电路分别与真随机密钥产生器、幅度调制器和第一相位调制器连接，用以将真随机密钥产生器产生的密钥发送至幅度调制器和第一相位调制器，由幅度调制器和相位调制器将密钥调制到激光脉冲上，并根据第一相位调制器的调节范围，计算相位补偿帧，随机将相位补偿帧发送至第一相位调制器，由第一相位调制器将相位补偿帧调制到激光脉冲上，然后通过衰减器衰减到量子级别的光脉冲。；

[0015] 触发时钟电路与激光器连接，用以触发激光器；

[0016] 接收端光路部分包括：偏振动态控制器、偏振分束器、第二相位调节器、第二偏振控制器、第二分束器和相干检测器，偏振动态控制器用以消除信号光和本振光在光纤中传输后受到环境的干扰而产生的偏振漂移，偏振分束器将消除偏振漂移的激光脉冲分成 2 束，1 束经过第二相位调制器和第二偏振控制器进行失真补偿，然后与另 1 束一起进入第二分束器后分为两束分别进入相干检测器进行相干检测，相干检测器通过本振光和信号光的干涉作用，把量子级别的信号光的值检测出来；

[0017] 接收端控制器模块包括：模拟电压输入控制电路和第二模拟电压输出控制电路，模拟电压输入控制电路与相干检测器相连接，用于接收相干检测后的电信号；第二模拟电

压输出控制电路与第二相位调制器相连接，通过提取相位补偿帧然后计算得出需要补偿的电压，然后输出这个电压值到第二相位调制器进行相位补偿。

[0018] 为达到上述目的，本发明还提供一种连续变量量子密钥分发系统相位补偿方法，包括以下步骤：

[0019] (1)连续变量量子密钥分发系统发送端依据相位调制器的调节范围，确定发送相位补偿帧；

[0020] (2)根据系统所处的环境，确定相位补偿帧的插入信号中的频率 A 的取值；

[0021] (3)连续变量量子密钥分发系统发送端发送一个相位补偿帧，且接(A-1)个信号帧；

[0022] (4)连续变量量子密钥分发系统接收端从相干检测器输出信号中采样，并且提取出相位补偿帧；

[0023] (5)连续变量量子密钥分发系统接收端通过提取出的相位补偿帧，根据相位补偿帧的结构计算需要补偿的电压值；

[0024] (6)接收端计算出补偿电压值后，通过控制接收端的第二相位调制器把补偿电压值补偿到(A-1)个密钥帧相位上去，实现消去环境和系统噪声；

[0025] (7)接收端接收到补偿后的(A-1)个密钥帧，并储存至原始密钥文件中；

[0026] (8)接收端接收到下一个相位补偿帧，并提取出相位补偿帧，重复步骤(5)至步骤(7)的操作；

[0027] (9)发送端已完成密钥的分发，发送中断传输信号，接收端接收到中断传输信号后，停止接收，密钥分发完成。

[0028] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，步骤(1)中，相位补偿帧的最佳效果确定为：设第一相位控制器的调制范围为：$-V_1 \sim +V_1$，取 N 个点作为一帧，N 个点设计为从 $-V_1$ 到 $+V_1$ 的等差数组，相邻 2 个点的差值为$(2V_1/(N-1))$，则相位补偿帧为：

[0029] $(-V_1, -V_1+(2V_1/(N-1)), -V_1+2*(2V_1/(N-1)), \cdots\cdots, -V_1+(N-2)*(2V_1/(N-1)), +V_1)$。

[0030] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，步骤(1)中，相位补偿帧的最简单结构确定为：设第一相位控制器的调制范围为：$-V_1 \sim +V_1$，取 N 个点作为一帧，N 个点设计为固定一个电压值 V_2，则相位补偿帧为：

[0031] $(V_2, V_2, V_2, \cdots\cdots, V2)$。

[0032] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，发送端相位补偿帧是按照间隔为 A 的取值循环插入到密钥分发中，相位补偿帧的插入重复频率为 A，即发送端发送了(A-1)个帧的明文后，紧接着发送 1 帧相位补偿帧，相应的，引入相位补偿帧带来的通信额外开销为(1/A)。

[0033] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，上述的 N 和 A 的取值选定根据环境条件和系统时钟频率来确定，若环境引起的相位抖动范围为 10~1000 之间，系统时钟频率为 B(MHz)，则 N 和 A 的取值必须符合：$\frac{B\times10^6}{N\times A}\geq1000$。

[0034] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，接收端

检测到相位补偿帧后，根据相位补偿帧的最佳效果结构计算需要补偿的电压值，具体计算公式为：

[0035] $$\psi = \frac{N_1 \times (2 \times V_1)}{N} - V_1$$；

[0036] 其中，N_1 是计算出正弦曲线平移后最大值所在的数组位置；

[0037] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，接收端检测到相位补偿帧后，根据相位补偿帧的最简单结构计算需要补偿的电压值，具体计算公式为：

[0038] $$\psi = 360 \times \frac{V_3 - V_2}{2 \times V_1}$$；

[0039] 其中，V_3 是相位抖动值附加到整个帧内所引起的变化后的固定值。

[0040] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，步骤（6）中的（A-1）个密钥帧是紧接着上一个相位补偿帧的。

[0041] 依照本发明较佳实施例所述的连续变量量子密钥分发系统相位补偿方法，中断传输信号为一段全零数据帧。

[0042] 由于量子信号容易受到环境因素的影响，产生不规则的扰动，并且幅度很大，这是传统通信上不存在的现象，所以传统意义上的相位补偿方法都不能适用于量子密钥分发，本发明通过引入额外开销实现连续变量密钥分发系统相位补偿。由以上可以看出，本发明提供的基于连续变量量子在光纤中特性的相位补偿方案，通过引入相位补偿帧克服在光通信过程中连续变量量子受到环境的影响对相位的干扰，有效降低了误码率，提高了通信质量，通信可靠性高。因此，与现有技术相比，本发明具有误码率低、通信可靠的优点。

附图说明

[0043] 图 1 为本发明连续变量量子密钥分发系统的结构原理框图；

[0044] 图 2 为本发明实施例的相位补偿帧的最优结构示意图；

[0045] 图 3 为本发明实施例的相位补偿帧的最简单结构示意图。

具体实施方式

[0046] 以下结合附图，具体说明本发明。

[0047] 请参阅图 1，一种连续变量量子密钥分发系统，包括发送端和接收端，发送端包括发送端光路部分和发送端控制器模块，接收端包括接收端光路部分和接收端控制器模块，其中，

[0048] 发送端光路部分包括：依次连接的激光器、第一分束器、第一偏振控制器、幅度控制器、第一相位调制器、衰减器和耦合器，其中，分束器还与耦合器连接；激光器用以产生激光，激光出来后经过第一分束器分成 2 束，1 束信号光和 1 束本振光，一束信号光经过偏振控制器、幅度控制器、相位控制器和衰减器，衰减后的信号光与另外 1 束本振光在耦合器相遇并耦合成 1 束激光发送至传输信道；

[0049] 发送端控制器模块包括：真随机密钥产生器、模拟电压输出控制电路和触发时钟电路，真随机密钥产生器用以产生真随机密钥，第一模拟电压输出控制电路分别与真随机

密钥产生器、幅度调制器和第一相位调制器连接，用以将真随机密钥产生器产生的密钥发送至幅度调制器和第一相位调制器，由幅度调制器和相位调制器将密钥调制到激光脉冲上，并根据第一相位调制器的调节范围，计算相位补偿帧，随机将相位补偿帧发送至第一相位调制器，由第一相位调制器将相位补偿帧调制到激光脉冲上，然后通过衰减器衰减到量子级别的光脉冲。；

[0050] 触发时钟电路与激光器连接，用以触发激光器；

[0051] 接收端光路部分包括：偏振动态控制器、偏振分束器、第二相位调节器、第二偏振控制器、第二分束器和相干检测器，偏振动态控制器用以消除信号光和本振光在光纤中传输后受到环境的干扰而产生的偏振漂移，偏振分束器将消除偏振漂移的激光脉冲分成 2 束，1 束经过第二相位调制器和第二偏振控制器进行失真补偿，然后与另 1 束一起进入第二分束器后分为两束分别进入相干检测器进行相干检测，相干检测器通过本振光和信号光的干涉作用，把量子级别的信号光的值检测出来；

[0052] 接收端控制器模块包括：模拟电压输入控制电路和第二模拟电压输出控制电路，模拟电压输入控制电路与相干检测器相连接，用于接收相干检测后的电信号；第二模拟电压输出控制电路与第二相位调制器相连接，通过提取相位补偿帧然后计算得出需要补偿的电压，然后输出这个电压值到第二相位调制器进行相位补偿。

[0053] 本实施例系统将从半导体激光器发出的激光脉冲大幅度衰减产生的准单光子作为信息载体——激光光源属相干光源，其光子数分布满足泊松分布，将脉冲激光衰减到平均每个脉冲 0.1 个光子时，每个脉冲含 1 个以上光子的概率仅为 0.5%，此时的光脉冲表现出不可克隆等量子属性，本发明把这种由激光器和衰减器构成的准单光子源作为量子信号发生器。激光器的输出频率由触发时钟频率决定，若连续变量密钥发送端分发速率为 R_1(bit/s)，那么为了使得 1 个光脉冲调制 1 个信息，触发时钟频率则为 R_1(Hz)。光脉冲通过 1/99 分束器，1 的那路是信号光，通过偏振控制器使得与 99 本振光偏振相差 90 度，然后密钥通过幅度调制器或者是相位调制器调制到信号光脉冲上，为了把密钥信息调制准确调制到光脉冲上，那么 2 路模拟电压输出频率也为 R_1(Hz)。调制好后通过耦合器耦合本振光输出到信道上。经过信道后，偏振动态控制器的作用是消除信道噪声对光脉冲的偏振影响，通过偏振分束器后，把信号光与本振光分开，信号光通过相位控制器来选择测量的分量，在经过偏振控制器的微调，使得相干检测器的输出为调制输入信号。检测输出的弱光脉冲的频率为 R_1(Hz)，为了能更准备得到调制信息，接收端控制器的 A/D 采样速率选取 $100R_1$(bit/s)。

[0054] 为达到上述目的，本发明还提供一种连续变量量子密钥分发系统相位补偿方法，包括以下步骤：

[0055] (1)连续变量量子密钥分发系统发送端依据相位调制器的调节范围，确定发送相位补偿帧。

[0056] 发送端中分发密钥端调制器件调制范围 $-V_1 \sim +V_1$，设计相位补偿帧来进行相位补偿，消除环境和系统噪声等造成的相位扰动。相位补偿帧的结构可以多种多样，本发明提供 2 种结构，一种是最佳结构，效果最好；另一种是最简单结构，最容易实现。

[0057] 如图 2 所示，最佳相位补偿帧结构为：取 N 个点作为一帧，N 个点设计为从 $-V_1$ 到 $+V_1$ 的等差数组，相邻 2 个点的差值为($2V_1$/(N-1))，即相位补偿帧($-V_1$，$-V_1$+ ($2V_1$/

(N-1)),$-V_1$+2*(2V_1/(N-1)),……,$-V_1$+(N-2)*(2V_1/(N-1)),+V_1)。这样设置的相位补偿帧调制到相位控制器上,输出的信号是正弦波形,容易计算出环境和系统引入的噪声值。

[0058] 如图 3 所示,最简单的相位补偿帧结构为:取 N 个点作为一帧,N 个点设计为固定一个电压值 V_2,即相位补偿帧(V_2,V_2,V_2,……,V2)。采用最简单的相位补偿帧结构也可以实现相位补偿的目的,不过可视性和容错率上不如最佳结构的相位补偿帧。

[0059] (2)根据系统所处的环境,确定相位补偿帧的插入信号中的频率 A 的取值。

[0060] 发送端相位补偿帧是按照间隔为 A 的取值循环插入到密钥分发中,相位补偿帧的插入重复频率为 A,即发送端发送了(A-1)个帧的明文后,紧接着发送 1 帧相位补偿帧,相应的,引入相位补偿帧带来的通信额外开销为(1/A)。

[0061] 具体的 N 和 A 的取值选定根据环境条件和系统时钟频率来确定,若环境引起的相位抖动范围为 10~1000 之间,系统时钟频率为 B(MHz),则 N 和 A 的取值必须符合:$\frac{B\times10^6}{N\times A}\geq1000$。

[0062] (3)连续变量量子密钥分发系统发送端发送一个相位补偿帧,且接(A-1)个信号帧。

[0063] (4)连续变量量子密钥分发系统接收端从相干检测器输出信号中采样,并且提取出相位补偿帧。

[0064] (5)连续变量量子密钥分发系统接收端通过提取出的相位补偿帧,根据相位补偿帧的结构计算需要补偿的电压值。

[0065] 接收端检测到相位补偿帧后,根据相位补偿帧的结构计算需要补偿的电压值,如果选取的最佳相位补偿帧的结构,那么具体计算公式为:

[0066] $$\psi=\frac{N_1\times(2\times V_1)}{N}-V_1;$$

[0067] 其中,N_1 是计算出正弦曲线平移后最大值所在的数组位置;

[0068] 如果选取的最简单的相位补偿帧的结构,则具体计算公式为:

[0069] $$\psi=360\times\frac{V_3-V_2}{2\times V_1};$$

[0070] 其中,V_3 是相位抖动值附加到整个帧内所引起的变化后的固定值。

[0071] (6)接收端计算出补偿电压值后,通过控制接收端的第二相位调制器把补偿电压值补偿到(A-1)个密钥帧相位上去,实现消去环境和系统噪声。其中,的 (A-1) 个密钥帧是紧接着上一个相位补偿帧的。

[0072] (7)接收端接收到补偿后的(A-1)个密钥帧,并储存至原始密钥文件中;

[0073] (8)接收端接收到下一个相位补偿帧,并提取出相位补偿帧,重复步骤(5)至步骤(7)的操作;

[0074] (9)发送端已完成密钥的分发,发送中断传输信号,接收端接收到中断传输信号后,停止接收,密钥分发完成。具体的,中断传输信号为一段全零数据帧。

[0075] 除以上外,连续变量量子密钥分发开始前,必须进行端与端的同步,同步完后,则进入系统初始化阶段,确定相位补偿帧的结构,然后开始通信。本实施例额外的帧开销来实现相位补偿,也就是引入相位补偿帧来消除环境引入的噪声。

[0076] 相位补偿的具体步骤如下：连续变量量子密钥发送端密钥随机的通过幅度调制器和第一相位调制器调制到量子光信号载体上，相位补偿帧通过第一相位调制器调制到信号光载体上。发送端发送顺序为：先把 1 个相位补偿帧通过第一相位调制器调制到信号光载体上，然后（A-1）个密钥帧通过幅度调制器或者第一相位调制器调制到光子载体上，选择幅度或者第一相位调制器是完全随机的。发送端就这样循环发送相位补偿帧和密钥，直到密钥分发结束的时候。连续变量量子密钥接受端，提取出相位补偿帧，然后通过与相位补偿帧相对应的结构选择相位补偿的计算公式，计算出应该补偿的相位电压值。然后把这个相位电压值通过接受端的第二相位调制器加到接受的信号上，实现相位补偿。每当提取出一个相位补偿帧，计算得到当前的相位扰动值，在加到后面的（A-1）密钥信息上，实现实时的自发相位补偿。

[0077] 相干光脉冲衰减到了量子级特别容易受到环境的影响，造成强烈的相位扰动，这些影响使得误码率大大的增加。本发明上述的相位补偿方案，是完全能克服上面这些环境的影响，才能进行有效的量子密钥分发。

[0078] 尽管本发明的内容已经通过上述优选实施例作了详细介绍，但应当认识到上述的描述不应被认为是对本发明的限制。在本领域技术人员阅读了上述内容后，对于本发明的多种修改和替代都将是显而易见的。因此，本发明的保护范围应由所附的权利要求来限定。

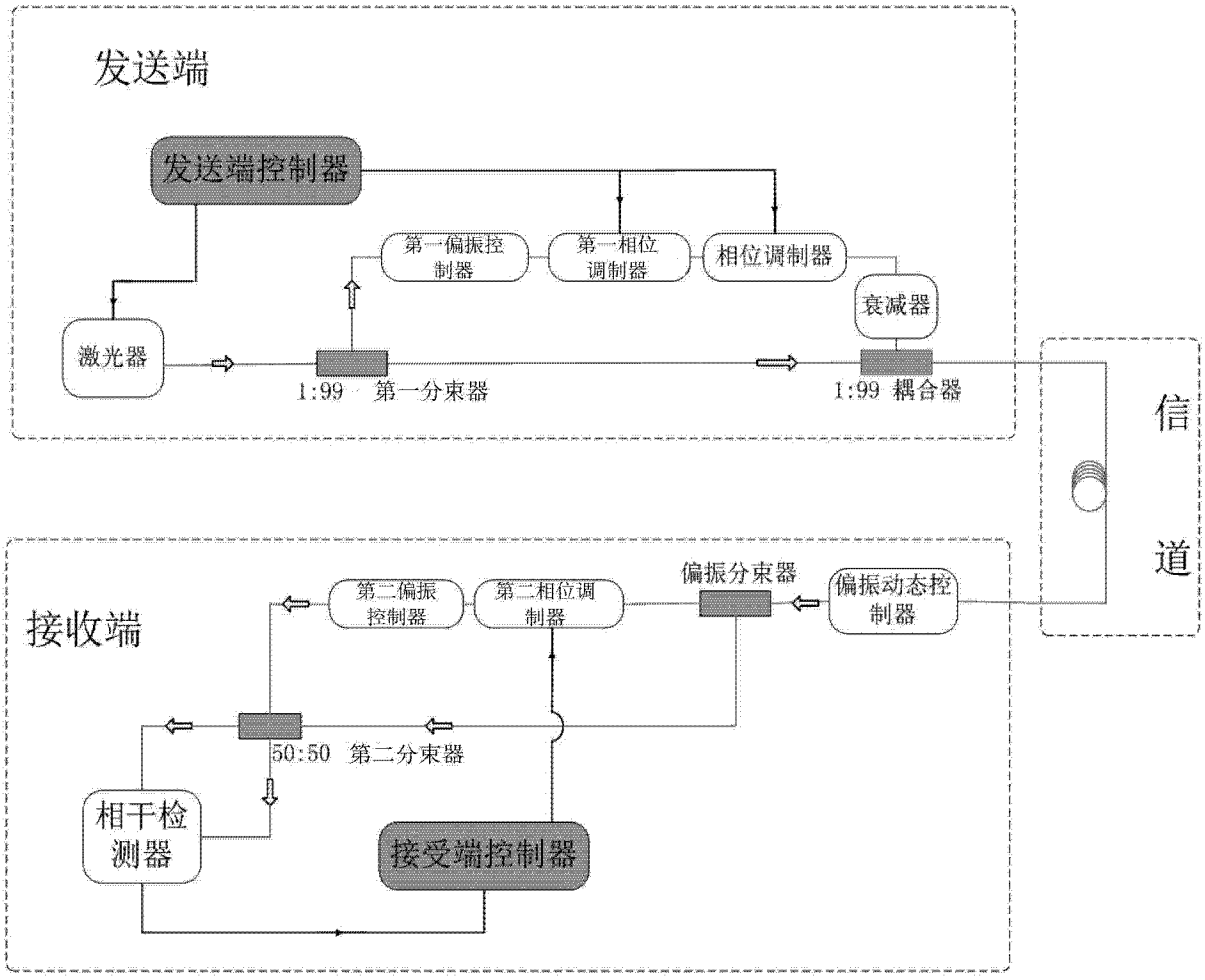

发送端
发送端控制器
第一偏振控制器
第一相位调制器
相位调制器
衰减器
激光器
1:99 第一分束器
1:99 耦合器
信道
接收端
第二偏振控制器
第二相位调制器
偏振分束器
偏振动态控制器
50:50 第二分束器
相干检测器
接受端控制器

图 1

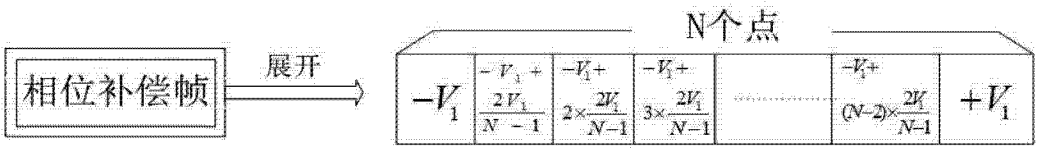

相位补偿帧
展开
N个点
$-V_1$
$+V_1$

图 2

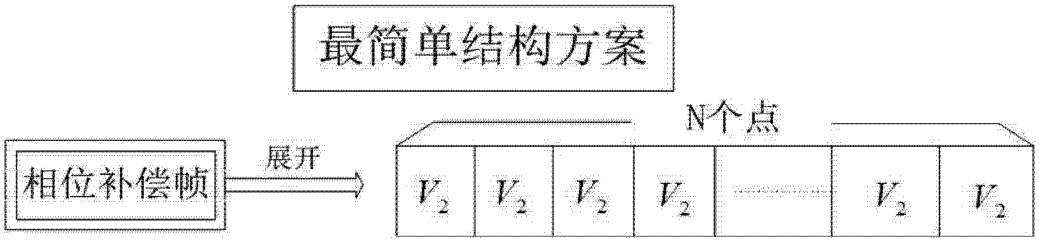

最简单结构方案
相位补偿帧
展开
N个点
V_2

图 3