

7333

证书号第 1568226 号



# 发明专利证书

发明名称: 连续变量量子密钥分发系统及其同步实现方法

发明人: 申泽源; 肖俊俊; 何广强; 曾贵华

专利号: ZL 2012 1 0181340.X

专利申请日: 2012 年 06 月 04 日

专利权人: 上海交通大学

授权公告日: 2015 年 01 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 06 月 04 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

申长雨





## (12) 发明专利申请

(10) 申请公布号 CN 102724036 A

(43) 申请公布日 2012. 10. 10

(21) 申请号 201210181340. X

(22) 申请日 2012. 06. 04

(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 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)

H04L 27/26 (2006. 01)

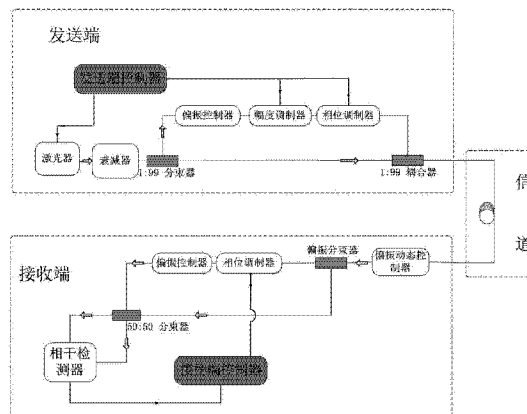
权利要求书 2 页 说明书 7 页 附图 1 页

### (54) 发明名称

连续变量量子密钥分发系统及其同步实现方法

### (57) 摘要

本发明公开一种连续变量量子密钥分发系统及其同步实现方法,连续量子密钥分发系统由光路部分和电路控制部分组成,光路部分主要由激光器、衰减器、分束器、偏振控制器、幅度控制器、相位控制器、耦合器等组成。控制部分是发送端控制器模块,由真随机密钥产生器、模拟电压输出、触发时钟输出组成。同步方法包括位同步和帧同步两个阶段。本发明提出了一种全新的基于连续变量量子在光纤中特性的同步实现方案,推进了连续变量量子密钥分发系统的实用化,同时有效的克服了在光通信过程中连续变量量子受到环境的影响对同步实现的干扰。





5. 根据权利要求 4 所述的连续变量量子密钥分发系统同步实现方法,其特征在于所述标志帧的设计:标志帧的数据长度为一帧,数据个数为  $10N_1$ ,分为 10 节,每一节的数据个数是  $N_1$ ,第一节和第二节选用  $-V_1$ 、 $+V_1$  的交替数据,即交替数据的个数为  $2N_1$ ,后面 8 节数据为 0;标志帧为:  $(-V_1, +V_1, -V_1, +V_1, \dots -V_1, +V_1), (-V_1, +V_1, -V_1, +V_1, \dots -V_1, +V_1), (0, 0, \dots, 0, ) \dots (0, 0, \dots, 0, )$ 。

6. 根据权利要求 3 所述的连续变量量子密钥分发系统同步实现方法,其特征在于所述检测字符同步帧,检测步骤如下:

(1). 选取检测到交替数据  $(-V_1, +V_1, \dots -V_1, +V_1)$  的判决门限,接收端接收的数据来源于相干检测器后的数据,若调制的范围  $(-V_1 \sim +V_1)$ ,则检测输出的范围  $(-V_3 \sim +V_4)$ ,选取的判决门限为  $\text{Thr}$ :  $\text{Thr} = \alpha * |-v_3 - (+v_4)|$ ,其中  $\alpha$  为系统噪声涨落水平,  $\alpha \in (0.5 \sim 1)$ ;

(2). 计算一帧里面连续的交替数据个数  $T_{\text{num}}$ ,从收到的帧的第一个数据开始,每一个数据都和后一个数据做差值并取绝对值,如果差值的绝对值大于判决门下  $\text{Thr}$ ,那么  $\text{Temp}$  加 1,若其中有一个差值绝对值小于  $\text{Thr}$ ,如果  $\text{Temp}$  大于  $T_{\text{num}}$ ,那么把  $\text{Temp}$  赋值给  $T_{\text{num}}$ ,并使  $\text{Temp}$  为 0;如果  $\text{Temp}$  小于  $T_{\text{num}}$ ,那么使  $\text{Temp}$  为 0;一帧扫描计算结束后,得到  $T_{\text{num}}$  值为  $N_3$ ;

(3). 判断字符同步是否成功,如果  $T_{\text{num}}$  的值  $N_3$  等于  $N_2$ ,那么就找到了字符的开始时刻,字符同步成功,结束操作;如果  $T_{\text{num}}$  的值  $N_3$  不等于  $N_2$ ,那么帧的选取移一节,然后重复上面操作,直到字符同步成功为止,若在时间  $T_1$  时刻之前一直都没找到,则通信失败。

7. 根据权利要求 3 所述的连续变量量子密钥分发系统同步实现方法,其特征在于所述检测标志帧,检测步骤如下:

(1). 选取检测到交替数据  $(-V_1, +V_1, \dots -V_1, +V_1)$  的判决门限,选用第一阶段的判决门限  $\text{Thr}$  作为本阶段的判决门限;

(2). 统计一帧里面交替数据个数  $\text{Tagnum}$ ,从收到的帧的第一个数据开始,每一个数据都和后一个数据做差值并取绝对值,如果差值的绝对值大于判决门下  $\text{Thr}$ ,那么  $\text{Tagnum}$  加 1,一帧扫描计算结束后,得到  $\text{Tagnum}$  值为  $N_4$ ;

(3). 判断这帧是否为标志帧,首先需要设置一个判断标志帧的判决门限值  $N_5$ ,判决门限值  $N_5$  的选取与通信系统环境造成的噪声  $\beta$  有关,  $\beta \in (0.75 \sim 1)$ ,选取的判决门限值  $N_5$ :  $N_5 = \beta * (10 * N_1)$ ;若  $\text{Tagnum}$  值  $N_4$  大于  $N_5$ ,则确定此帧为标志帧,那么这帧结束后的第一个字符为帧头开始时刻;若  $\text{Tagnum}$  值  $N_4$  小于  $N_5$ ,那么此帧不是标志帧,通信失败。

## 连续变量量子密钥分发系统及其同步实现方法

### 技术领域

[0001] 本发明涉及一种光纤通信技术领域的技术,具体地说,涉及的是一种连续变量量子密钥分发系统及其同步实现方法。

### 背景技术

[0002] 1999 年 Ralph 首先从实验角度提出了利用连续变量进行量子密钥分发的概念并分析其安全性,连续变量量子密钥分配迅速得到发展,各种方案相继被提出。M. Hillery 在 2000 年从理论的角度上提出了基于压缩态的量子密钥分配方案。2001 年,D. Gottesman 和加州理工大学的 J. Preskill 采用连续变量纠错码的概念证明了他们提出的基于压缩态的量子密钥分配方案的安全性,这是第一次证明了连续变量量子密钥分配的安全性。法国科学家 N. J. Cerf 提出了一种改进的方案,实现了全连续态的量子密钥分配,这也是第一个真正意义上的连续变量量子密钥分配方案。N. J. Cerf 的方案极大提高的密钥传输的速率,但是其实验方案实现难度却非常大。

[0003] 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,这种不涉及光场的任何非经典性质的 QKD 方案具有极大的意义,由于它的实现非常容易,该方案引起了学术界的极大关注。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。实验表明,在无损耗的量子信道上,密钥传输速率为 1.7M/s;当信道损耗为 3.1dB 时,密钥传输速率为 75k/s。该实验采用的量子信号为平均光子数为 250 个的相干光脉冲。由于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。基于相干态高斯调制的连续变量量子密钥分发方案的安全性证明相继被提出。

[0004] 经过各国科学家的不断努力,研究人员逐渐掌握了连续量子密钥分发实验方案所需要的核心技术,主要包括以下几个方面:

[0005] 1、连续变量量子信号发生器

[0006] 目前连续变量量子信号发生器主要分三类:相干激光脉冲源、压缩态光量子、纠缠光量子。现在国际上主流都采用衰减后的微弱相干激光脉冲作为连续变量量子信号,这是因为相干激光脉冲源技术已经成熟、相干光制备比较容易实现。

[0007] 2、连续变量量子信号的检测技术

[0008] 连续变量量子信号检测采用相干检测,检测装置为一对光电二极管,通过差分电路降低检测器噪声与本振光抖动,得到较高的灵敏度。这种检测方式的最大优点是可以在常温下工作,并且量子效率比单光子检测器的效率要高得多,在 1550nm 电信光纤通信窗口波长上可以达到 50% 以上。

[0009] 3、连续变量量子密钥分发系统流程设计

[0010] 连续变量量子信号的产生是相干激光脉冲经过衰减后得到连续变量量子信号,基本上在 1 个相干光脉冲内,光子数小于 250 个。由于相干光脉冲衰减到了量子级别,在光通信过程中,特别容易受到环境的影响,比如温度、湿度、声音等。这些环境因素造成的影响主

要体现在对光脉冲相位扰动上,从通信的角度看,这些影响使得误码率大大的增加。然而,传统的强光通信中,这些问题对光通信系统的影响基本上可以忽略不计。这也使得传统的光通信方面的一系列协议、流程设计在连续变量量子密钥分发系统中并不实用。从通信层面上来看,一个系统需要通信,必须先实现系统之间的载波同步、位同步(码元同步)、帧同步(群同步),在连续变量量子密钥分发系统中,同步问题也是必须先实现的问题。

[0011] 量子变量量子密钥分发研究是一个结合密码学、光纤通信、量子光学、和网络通信等多个学科的前沿课题。目前这个方面的技术正受到国际学术界的关注,并且开始应用于现实生活中。

[0012] 经检索发现,中国发明专利申请号:201010108798.3,公开号为101800636A,该发明专利提供一种用于量子密钥分发的同步装置及同步方法,其中:

[0013] “一种用于量子密钥分发的同步装置,其特征在于:用于同步信号产生和编码的同步信号编码模块信号输出端与用以产生同步激光的同步激光发射模块信号输入端连接;所述同步激光发射模块的信号输出端通过光纤与用于光电转换的光探测器和用于甄别的比较器电路模块信号输入端连接;光探测器和比较器电路模块的信号输出端分别与用于产生门控信号并且可调延时的可调延时电路模块和使用一个帧计数器进行计数,对同步信息进行编码的同步检出和编码模块的信号输入端连接。”

[0014] “用于量子密钥分发同步装置的同步方法,其特征在于包括以下步骤:(1)使用同步信号编码模块对信号进行编码,产生同步光激光器的驱动信号;(2)所述驱动信号进入同步光激光发射模块,进行电平转换,对信号整形,并将同步激光发射;(3)发射的同步光和信号光耦合到同一根光纤中,从发送方传送到接收方;(4)在接收方,使用同步光探测和甄别模块中的光电二极管完成同步光的接收和光电转换,并使用高性能比较器完成信号的甄别;(5)使用独立可调延时电路,对步骤(4)采集到的信号进行延时,作为门控信号输给单光子探测器;(6)对步骤(4)采集到的信号进行同步检出,并结合单光子探测器得到的信号计数进行编码。”

[0015] 但是上述的同步装置及同步方法不能适用于连续变量量子密钥分发。

## 发明内容

[0016] 本发明的目的在于针对连续变量量子密钥分发系统同步方案的空白,提出了一种连续变量量子密钥分发系统及其同步实现方法,推进了连续变量量子密钥分发系统的实用化,同时有效的克服了在光通信过程中连续变量量子受到环境的影响对同步实现的干扰。

[0017] 为实现上述目的,本发明采用的技术方案如下:

[0018] 本发明所述的连续变量量子密钥分发系统,由光路部分和电路控制部分构成,其中:

[0019] 所述光路部分主要由激光器、衰减器、分束器、偏振控制器、幅度控制器、相位控制器和耦合器组成,激光器产生激光,激光出来后经过衰减器,衰减后的激光被分束器分成2束,1束经过偏振控制器、幅度控制器、相位控制器,然后与另外1束在耦合器相遇并耦合成为1束激光;

[0020] 所述电路控制部分主要由真随机密钥产生器、模拟电压输出控制电路和触发时钟电路组成,真随机密钥产生器产生密钥,然后由模拟电压输出控制电路传递给光路器件,触

发时钟电路是单独用来触发激光器的；

[0021] 发送端, 触发时钟信号产生触发电平来触发激光器发出激光脉冲, 激光脉冲经过衰减器后大幅度衰减成准单光子信号; 准单光子信号经过 1:99 的分束器分成 2 束信号, 1 束信号作为信息信号经过偏振控制器来调整光子的偏振, 然后通过幅度控制器、相位控制器。幅度控制器和相位控制器把真随机密钥调制到光子载体上, 然后与另外 1 束光在耦合器里面耦合成 1 束光传送至光纤里面。

[0022] 接收端, 光纤中的信号通过动态偏振控制器调整偏振, 然后通过偏振分束器分成 2 束, 1 束经过相位调制器和偏振调制器进行失真补偿; 最后这 1 束激光与另 1 束一起进入分束器进行相干检测。

[0023] 本发明所述的连续变量量子密钥分发系统同步实现方法,包括位同步和帧同步两个阶段,所述位同步阶段是为了能从弱光光脉冲中准确的提取出调制信息;所述帧同步阶段在位同步基础上,准确的找出信号中一个字符、一个帧的开始时刻。

[0024] 1、位同步阶段

[0025] 位同步阶段:连续变量量子信号检测采用相干检测,检测装置输出的是一个的弱光脉冲,然后通过 A/D 采样,在采样序列中提取出调制信息,也就是弱光脉冲上调制的密钥信息。

[0026] 位同步方案:要得到连续变量密钥,需从相干检测器输出信号中采样,并且提取出调制的那1个信息,光脉冲中调制信息最准确的体现是在光脉冲的峰值上,所以需要提取每一个脉冲的峰值。

[0027] 2、帧同步阶段

[0028] 帧同步阶段：帧同步第一个阶段是找到第一个字符的开始时刻，第二个阶段是在第一个阶段上，准备找到每一个帧头的开始时刻。

[0029] 找字符开始时刻,由于相干光脉冲衰减到了量子级别,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。为了消去相位扰动需要相位补偿模块,而相位补偿模块又需要先同步,然后才能从相位补偿帧中提取出需要补偿的电压值。所以,在帧同步阶段,必须考虑这些环境因素带来的极高误码率对通信的影响。

[0030] 第一阶段:找字符开始时刻

[0031] 发送端中分发密钥端调制器件调制范围 $(-V_1 \sim +V_1)$ ,设计一种特殊帧——字符同步帧来进行寻找到字符准确的开始时刻。字符同步帧结构:取 $N_1$ 个点作为第一节,前 $N_2$ 个点设计为 $-V_1$ 、 $+V_1$ 的交替数据,后 $(N_1-N_2)$ 个点的数据取为0,这里必须 $N_1$ 大于 $N_2$ ,第二节至第十节,每一节取 $N_1$ 个点,并且每个点的数据都为0。这十节数据组成一个字符同步帧,即字符同步帧 $(-V_1, +V_1, -V_1, +V_1, \dots, -V_1, +V_1, 0, 0, 0, 0, \dots, 0, ), (0, 0, \dots, 0, ) (0, 0, \dots, 0, ) \dots (0, 0, \dots, 0, )$ 。

[0032] 发送端一直重复发送字符同步帧,直到接收端准确确认了字符同步帧后,并且检测到字符同步帧的开始时刻才停止。

[0033] 接收端在位同步基础上,开始检测字符同步帧,检测的时候也是一帧一帧的检测,发送端字符同步帧的数据长度为  $10N_1$ ,所以在接收端选取的帧长度也是  $N_1$ 。

[0034] 所述检测字符同步帧,检测步骤如下:

[0035] (1). 选取检测到交替数据 $(-V_1, +V_1, \dots, -V_1, +V_1)$ 的判决门限。接收端接收的数



据来源于相干检测器后的数据,若调制的范围 $(-V_1 \sim +V_1)$ ,则检测输出的范围 $(-V_3 \sim +V_4)$ 。本发明选取的判决门限为 Thr:  $\text{Thr} = \alpha * |-v_3 - (+v_4)|$ , 其中  $\alpha$  为系统噪声涨落水平,根据实际情况选取,  $\alpha \in (0.5 \sim 1)$ 。

[0036] (2). 计算一帧里面连续的交替数据个数 Tnum。从收到的帧的第一个数据开始,每一个数据都和后一个数据做差值并取绝对值,如果差值的绝对值大于判决门下 Thr, 那么 Temp 加 1, 若其中有一个差值绝对值小于 Thr, 如果 Temp 大于 Tnum, 那么把 Temp 赋值给 Tnum, 并使 Temp 为 0; 如果 Temp 小于 Tnum, 那么使 Temp 为 0。一帧扫描计算结束后, 得到 Tnum 值为  $N_3$ 。

[0037] (3). 判断字符同步是否成功。如果 Tnum 的值  $N_3$  等于  $N_2$ , 那么就找到了字符的开始时刻, 字符同步成功, 结束操作; 如果 Tnum 的值  $N_3$  不等于  $N_2$ , 那么帧的选取移一节, 然后重复上面操作, 直到字符同步成功为止, 若在时间  $T_1$  时刻之前一直都没找到, 则通信失败。

[0038] 第二个阶段: 找帧头开始时刻

[0039] 在找字符同步成功的基础上, 开始寻找帧头开始时刻。当发送端接到接收端发送过来的找字符时刻成功的信号后, 发送一个用来寻找帧头时刻的特殊帧—标志帧。接收端当检测出这个标志帧后, 就能得到每一帧的确切开始时刻。

[0040] 标志帧的设计和检测必须能适应连续量子在相位校正之前出现的高误码率情况, 标志帧的设计: 标志帧的数据长度为一帧, 数据个数为  $10N_1$ , 分为 10 节, 每一节的数据个数是  $N_1$ , 第一节和第二节选用  $-V_1$ 、 $+V_1$  的交替数据, 即交替数据的个数为  $2N_1$ , 后面 8 节数据为 0。标志帧为:  $(-V_1, +V_1, -V_1, +V_1, \dots, -V_1, +V_1), (-V_1, +V_1, -V_1, +V_1, \dots, -V_1, +V_1), (0, 0, \dots, 0, ) \dots (0, 0, \dots, 0, )$ 。

[0041] 接收端检测时, 交替数组的判决门限是第一阶段的判决门限 Thr, 检测方式与第一阶段略有不同, 第一阶段里面是检测字符同步帧里面连续交替数据的个数, 而在这里, 是检测标志帧里面出现的交替数据个数。

[0042] 所述检测标志帧, 检测步骤如下:

[0043] (1). 选取检测到交替数据  $(-V_1, +V_1, \dots, -V_1, +V_1)$  的判决门限。选用第一阶段的判决门限 Thr 作为本阶段的判决门限。

[0044] (2). 统计一帧里面交替数据个数 Tagnum。从收到的帧的第一个数据开始, 每一个数据都和后一个数据做差值并取绝对值, 如果差值的绝对值大于判决门下 Thr, 那么 Tagnum 加 1, 一帧扫描计算结束后, 得到 Tagnum 值为  $N_4$ 。

[0045] (3). 判断这帧是否为标志帧。首先需要设置一个判断标志帧的判决门限值  $N_5$ , 判决门限值  $N_5$  的选取与通信系统环境造成的噪声  $\beta$  有关,  $\beta \in (0.75 \sim 1)$ 。这选取的判决门限值  $N_5$ :  $N_5 = \beta * (10 * N_1)$ 。若 Tagnum 值  $N_4$  大于  $N_5$ , 则确定此帧为标志帧, 那么这帧结束后的第一个字符为帧头开始时刻。若 Tagnum 值  $N_4$  小于  $N_5$ , 那么此帧不是标志帧, 通信失败。

[0046] 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。采用上述技术方案, 本发明有效的克服了在光通信过程中连续变量量子受到环境的影响对同步实现的干扰, 误码率大大的降低。

## 附图说明

[0047] 图 1 为连续量子密钥分发系统的框图。



[0048] 图 2 为字符同步帧和标志帧的帧结构。

### 具体实施方式

[0049] 下面对本发明的实施例作详细说明,本实施例以本发明技术方案为前提进行实施,给出了详细的实施方式和具体的操作过程,但本发明的保护范围不限于下述的实施例。

#### [0050] 实施例 1

[0051] 如图 1 所示,本实施例提供一种连续变量量子分发系统,发送端包括光路部分和电路控制部分,光路部分主要由激光器、衰减器、分束器、偏振控制器、幅度控制器、相位控制器、耦合器等组成。电路控制部分是发送端控制器模块,由真随机密钥产生器、2 路模拟电压输出、1 路时钟触发构成。真随机密钥产生器是为了产生真随机密钥,2 路模拟电压输出是通过控制振幅调制器和相位调制器把密钥调制到光脉冲上,1 路时钟信号是用来触发激光光源。

[0052] 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,动态偏振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  $100 R_1$  (bit/s)。

#### [0053] 实施例 2

[0054] 本实施例提供一种连续变量量子密钥分发系统同步实现方法,具体步骤如下:

[0055] (1)、连续变量量子密钥分发端依据偏振控制器、幅度控制器的调节范围,发送字符同步序列帧。

[0056] (2)、连续变量量子密钥接收端从相干检测器输出信号中采样,并且提取提取每一个脉冲的峰值。进行位同步。

[0057] (3)、在位同步成功的基础上,连续变量量子密钥接收端根据噪声涨落水平,选择交替数据判决门限,开始找字符开始时刻。对发送端发来的同步序列帧进行判断。如果位同步没有成功,继续执行步骤(2)。

[0058] (4)、若找到字符开始时刻,接收端向发送端发送字符同步帧成功信号,并且开始检测标志帧。接收端接收到信号后,停止发送字符同步帧,转而发送标志帧,然后进去步骤(5)。若没有找到字符开始时刻,继续执行步骤(3)。

[0059] (5)、若检测到标志帧,则连续变量量子密钥分发系统同步成功,通信开始。若没有

检测到标志帧,则通信失败,重步骤(1)重新开始。

[0060] 如图2所示,发送端中分发密钥端调制器件调制范围 $(-V_1 \sim +V_1)$ ,设计字符同步帧来进行寻找到字符准确的开始时刻。字符同步帧结构:取 $N_1$ 个点作为第一节,前 $N_2$ 个点设计为 $-V_1$ 、 $+V_1$ 的交替数据,后 $(N_1-N_2)$ 个点的的数据取为0,这里必须 $N_1$ 大于 $N_2$ ,第二节至第十节,每一节取 $N_1$ 个点,并且每个点的数据都为0。这十节数据组成一个字符同步帧,即字符同步帧 $(-V_1, +V_1, -V_1, +V_1, \dots -V_1, +V_1, 0, 0, 0, 0, \dots, 0, )$ ,  $(0, 0, \dots, 0, )$   $(0, 0, \dots, 0, ) \dots (0, 0, \dots, 0, )$ 。

[0061] 标志帧的设计和检测必须能适应连续量子在相位校正之前出现的高误码率情况,标志帧的设计:标志帧的数据长度为一帧,数据个数为 $10N_1$ ,分为10节,每一节的数据个数是 $N_1$ ,第一节和第二节选用 $-V_1$ 、 $+V_1$ 的交替数据,即交替数据的个数为 $2N_1$ ,后面8节数据为0。标志帧为: $(-V_1, +V_1, -V_1, +V_1, \dots -V_1, +V_1)$ ,  $(-V_1, +V_1, -V_1, +V_1, \dots -V_1, +V_1)$ ,  $(0, 0, \dots, 0, ) \dots (0, 0, \dots, 0, )$ 。

[0062] 连续变量量子密钥分发开始前,必须进行端与端的同步,本实施例把同步分为2个阶段,第一个阶段是位同步阶段,第二个阶段为帧同步阶段,帧同步阶段又细分为2个步骤,第一个步骤是找字符开始时刻,第二个步骤是找帧头开始时刻。

[0063] 位同步阶段的具体步骤如下:连续变量密钥发送端分发速率为 $R_1$ (bit/s),接收端控制器的A/D采样速率为 $100 R_1$  (bit/s),则需要从100个数值中提取出信号值。光脉冲的信号调制值为脉冲的峰值,因此位同步过程就是提取峰值过程。提取峰值的操作可以视为提取数组的最大值操作,即从100个值组成的数组中提取最大值,取出的最大值即是信号调制的值。经过提取调制信息这个阶段,最终成码率为 $R_1$ (bit/s)。

[0064] 帧同步阶段的具体步骤如下:在位同步基础上,发送端发送字符同步帧,在没有接收到接收端发来的已完成字符同步信号,一直发送字符同步帧。接收端方面先根据实际噪声环境情况,先选取交替数组的判决门限,然后开始检测字符同步帧并且进行判决。先计算一帧里面连续的交替数据个数 $T_{num}$ ,若 $T_{num}$ 的值 $N_3$ 等于 $N_2$ ,那么就找到了字符的开始时刻,字符同步成功,结束操作;若 $T_{num}$ 的值 $N_3$ 不等于 $N_2$ ,那么帧的选取移一节,然后重复上面操作,直到字符同步成功为止,若在时间 $T_1$ 时刻之前一直都没找到,则通信失败。在字符同步成功的基础上,进行第二阶段找帧头开始时刻。接收端字符同步成功后给发送端发送字符同步成功信号,接收端在接收到字符同步成功的信号,停止发送字符同步帧,发送标志帧,然后开始发送密钥数据,进入密钥分发阶段。接收端发送完字符同步成功信号后,进入检测标志帧阶段,标志帧检测时,选用位同步中交替数组判决门限为本次门限,根据实际噪声环境情况确定标志帧的判决门限 $N_5$ 。开始统计每一帧里面交替数据个数 $Tag_{num}$ ,当 $Tag_{num}$ 值 $N_4$ 大于 $N_5$ ,则确定此帧为标志帧,那么这帧结束后的第一个字符为数据帧头开始时刻,进入密钥分发数据阶段。若 $Tag_{num}$ 值 $N_4$ 小于 $N_5$ ,那么此帧不是标志帧,接着判断下一帧,若经过一段时间一直都没找到标志帧,则通信失败,从位同步阶段开始重试。

[0065] 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。本发明上述的同步实现方案,是完全能克服上面这些环境的影响。

[0066] 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。

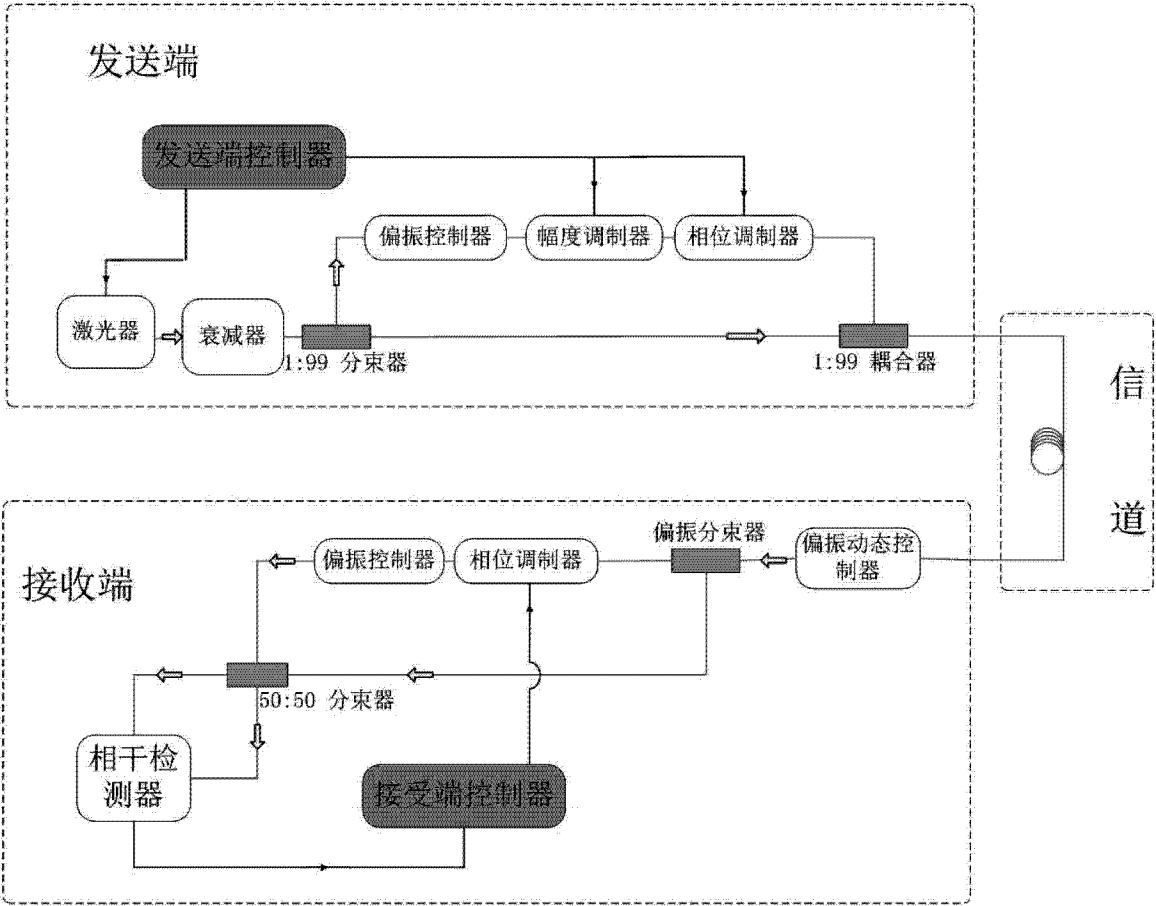


图 1

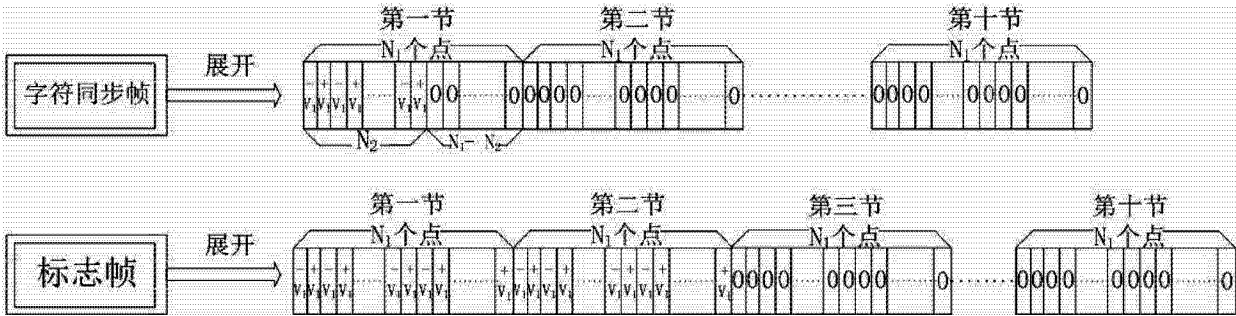


图 2