(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 110380849 A
(43)申请公布日 2019.10.25

(21)申请号 201910625485.6

(22)申请日 2019.07.11

(71)申请人 上海循态信息科技有限公司
地址 200241 上海市闵行区东川路555号丙楼1139室

(72)发明人 黄鹏 李登文 曾贵华

(74)专利代理机构 上海段和段律师事务所 31334
代理人 李佳俊 郭国中

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

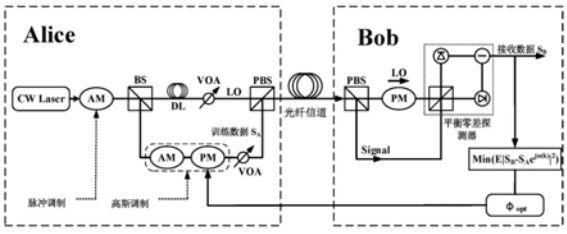
权利要求书2页 说明书7页 附图1页

(54)发明名称

CVQKD系统下针对高速漂移的离线相位补偿方法及存储介质

(57)摘要

本发明提供了一种CVQKD系统下针对高速漂移的离线相位补偿方法及存储介质，包括：步骤A：训练数据与有效数据的设定与传输；步骤B：误差函数的构造及其最优值求解；步骤C：最优补偿角度的求解与补偿实施。本发明可以在相位漂移速度较快时提高基于高斯调制相干态的CVQKD系统的相位补偿精度至0.0001rad。



CN 110380849 A

1.一种CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,包括如下步骤:

步骤A:训练数据与有效数据的设定与传输,具体为:在有效数据的传输中间插入被Alice和Bob已知的训练数据,并通过量子信道进行传输,且Bob端预设补偿角度;

步骤B:根据步骤A得到的补偿模型和预设补偿角度确立误差函数,这里的误差函数采用平方误差;并通过确立搜索方向和搜索步长再利用搜索迭代算法找出最小平方误差;

步骤C:Bob根据步骤B得到的误差函数,找出对应于最小平方误差的补偿角度即为最优补偿角度;Alice发送端把最优补偿角度加载到其相位调制器上进行相位补偿。

2.根据权利要求1所述的CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,所述步骤A包括如下步骤:

步骤A1:在相位漂移速度较快时,即每一帧中的多组有效数据的相漂角度均不一致,将每一帧中的多组有效数据中间均插入长度为1000的训练数据S;

步骤A2:Alice将有效数据与训练数据一并传输给Bob;

步骤A3:对训练数据做后处理操作;根据训练数据S确立通信两端的相应传输数据;Alice端的训练数据S_A=S,Bob端接收的训练数据S_B=T·S+E;其中,T为信道的透过率,E为信道的加性高斯白噪声;

步骤A4:Bob端预设角度u(0)作为初始迭代补偿角度。

3.根据权利要求1所述的CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,所述步骤B包括如下步骤:

步骤B1:确立Alice和Bob两端数据误差ER(0);其中$ER(0)=S_B-S_A\cdot e^{ju(0)}$;

其中,e为自然对数的底,j代表虚数单位;

步骤B2:平方误差$MSE(0)=E[|ER(0)|^2]=R(0)f(u(0))+\sigma^2$;其中R(0)为S的自相关函数,$f(u(0))=E[|Te^{j\phi}-e^{ju(0)}|^2]$,Φ为实际的相位漂移角度,$\sigma^2$为信道加性噪声E的方差;

其中,E[ ]代表取括号内函数的均值;

步骤B3:求解最小平方误差min{MSE(0)}等效于求解f(u(0))的最小值;梯度$\nabla f(u(0))=2Tsin(u(0)-\phi)$,搜索方向$d_0=-\nabla f(u(0))=-2Tsin(u(0)-\phi)$;找出最小迭代次数对应的步长λ作为最优迭代步长;进行第一次补偿角度迭代$u(1)=u(0)+\lambda d_0$;

步骤B4:重复步骤B2和步骤B3并把其中的u(0)替换为当前迭代后的角度值,不断迭代,直至补偿角度与实际相位漂移角度误差小于0.0001rad。

4.根据权利要求1所述的CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,所述步骤C包括如下步骤:

步骤C1:将步骤B中的最后迭代角度作为实际的最优相位补偿角度;

步骤C2:Bob将最优相位补偿角度通过经典信道传输给Alice,并由Alice加载Alice端的相位调制器PM上进行相位补偿。

5.根据权利要求2所述的CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,步骤A1中每一帧中的有效数据与训练数据为多组,且每一组有效数据对应一组训练数据,通过计算训练数据的相位漂移来判断其对应有效数据的相位漂移。

6.根据权利要求4所述的CVQKD系统下针对高速漂移的离线相位补偿方法,其特征在于,步骤C2中Bob是在量子信号传输完毕后经数据处理得到补偿角度再传给Alice,Alice对

其有效数据单独实施调相操作，并不做传输处理，其实施的相位补偿为离线补偿。

7.根据权利要求2所述的CVQKD系统下针对高速漂移的离线相位补偿方法，其特征在于，步骤A4中的预设角度u(0)能够随机任意设置，即最优补偿角度的求解与预设角度u(0)无关。

8.根据权利要求2所述的CVQKD系统下针对高速漂移的离线相位补偿方法，其特征在于，步骤A1中，在每一帧的帧头和有效数据之间插入训练数据S。

9.根据权利要求3所述的CVQKD系统下针对高速漂移的离线相位补偿方法，其特征在于，S_B为Bob端用探测器对传输的训练数据S的实际测量值，包括引入的信道衰减与噪声；搜索方向d_0选取梯度的负方向；所述CVQKD系统下针对高速漂移的离线相位补偿方法能够通过控制搜索步长λ在保证精度为0.0001rad情况下达到最少的迭代次数。

10.一种存储有计算机程序的计算机可读存储介质，其特征在于，所述计算机程序被处理器执行时实现权利要求1至9中任一项所述的CVQKD系统下针对高速漂移的离线相位补偿方法的步骤。

CVQKD系统下针对高速漂移的离线相位补偿方法及存储介质

技术领域

[0001] 本发明涉及量子密钥分发的相位补偿技术领域，具体地，涉及一种CVQKD系统下针对高速漂移的离线相位补偿方法及存储介质，尤其涉及一种利用反馈优化迭代的离线补偿方法，即通过求解最小均方误差来求解最优相位补偿角度，再经过经典信道传输给Alice端并由Alice进行补偿的离线高精度补偿技术。

背景技术

[0002] 随着信息技术的迅速发展，人们对安全性的要求越来越高，基于量子力学的量子保密通信具有物理上的无条件安全性，成为了人们关注的焦点。

[0003] 如专利文献CN106533565A公开的一种量子保密通信方法和装置，技术方案为：在量子保密通信的发送端和接收端配置中继设备，并采用多芯光纤作为连接链路。中继设备通过与直连的上游设备和F游设备分别进行量于密钥协商，并根据分别与直连的上游设备和T游设备协商的量子密钥，以及上游设备发来的密钥中继处理信号执行密钥中继处理和传输，实现端到端的通信密钥共享和量子密钥通信。

[0004] 量子密钥分发作为量子保密通信的核心技术，提供了一种相距很远的两端共享安全密钥的方法，它的安全性基于海森堡定理、量子不可克隆定理和测不准原理。量子密钥分发可分为离散变量的量子密钥分发和连续变量的量子密钥分发，二者各有优缺点，离散变量的量子密钥分发传输的距离远，但整体信息传输速率较低，而连续变量虽然传输的距离有待突破，但信息传输速率较高。我们主要对连续变量量子密钥分发进行研究。连续变量量子密钥分发可分为四个阶段：密钥传输、参数估计、秘密协商、保密增强。

[0005] 在密钥传输的过程中，由于光纤的抖动、温度等因素的影响会使得传输的量子信号的相位发生漂移，从而引入相位噪声。这会对整个系统的过噪声造成不可忽视的影响，进而也会影响密钥率。为了消除相位漂移的对整个系统的影响，需要进行相位补偿操作。

[0006] 相位补偿可以减少由于相位漂移引起的相位噪声，其补偿精度会极大影响整个密钥分发系统的性能。当前的相位补偿方案大致分为两种，一种是通过把整个相位区间等分，然后通过相位-电压转换的方法来对最接近实际漂移的等分点进行判断，从而获得补偿角度；另一种方法是通过求解两端数据的互相关量来求解相位漂移角度。但这两种方法所能处理的漂移速度有限，当相位漂移速度过快时很难进行精确补偿，并且达到的精度都比较有限，实时补偿的效率也很难进一步提高。因此，设计出能处理快速相位漂移的高精度的相位补偿算法来提升整个量子密钥分发系统的性能尤为重要。

发明内容

[0007] 针对现有技术中的缺陷，本发明的目的是提供一种CVQKD系统下针对高速漂移的离线相位补偿方法及存储介质。

[0008] 根据本发明提供的一种CVQKD系统下针对高速漂移的离线相位补偿方法，包括如下步骤：

[0009] 步骤A:训练数据与有效数据的设定与传输,具体为:在有效数据的传输中间插入被Alice和Bob已知的训练数据,并通过量子信道进行传输,且Bob端预设补偿角度;

[0010] 步骤B:根据步骤A得到的补偿模型和预设补偿角度确立误差函数,这里的误差函数采用平方误差;并通过确立搜索方向和搜索步长再利用搜索迭代算法找出最小平方误差;

[0011] 步骤C:Bob根据步骤B得到的误差函数,找出对应于最小平方误差的补偿角度即为最优补偿角度;Alice发送端把最优补偿角度加载到其相位调制器上进行相位补偿。

[0012] 优选地,所述步骤A包括如下步骤:

[0013] 步骤A1:在相位漂移速度较快时,即每一帧中的多组有效数据的相漂角度均不一致,将每一帧中的多组有效数据中间均插入长度为1000的训练数据S;

[0014] 步骤A2:Alice将有效数据与训练数据一并传输给Bob;

[0015] 步骤A3:对训练数据做后处理操作;根据训练数据S确立通信两端的相应传输数据; Alice端的训练数据S_A=S,Bob端接收的训练数据S_B=T·S+E;其中,T为信道的透过率,E为信道的加性高斯白噪声;

[0016] 步骤A4:Bob端预设角度u(0)作为初始迭代补偿角度。

[0017] 优选地,所述步骤B包括如下步骤:

[0018] 步骤B1:确立Alice和Bob两端数据误差ER(0);其中$ER(0)=S_B-S_A\cdot e^{ju(0)}$;

[0019] 其中,e为自然对数的底,j代表虚数单位;

[0020] 步骤B2:平方误差$MSE(0)=E[|ER(0)|^2]=R(0)f(u(0))+\sigma^2$;其中R(0)为S的自相关函数,$f(u(0))=E[|Te^{j\Phi}-e^{ju(0)}|^2]$,Φ为实际的相位漂移角度,$\sigma^2$为信道加性噪声E 的方差;

[0021] 其中,E[ ]代表取括号内函数的均值;

[0022] 步骤B3:求解最小平方误差min{MSE(0)}等效于求解f(u(0))的最小值;梯度$\nabla f(u(0))=2Tsin(u(0)-\phi)$,搜索方向$d_0=-\nabla f(u(0))=-2Tsin(u(0)-\phi)$;找出最小迭代次数对应的步长λ作为最优迭代步长;进行第一次补偿角度迭代$u(1)=u(0)+\lambda d_0$;

[0023] 步骤B4:重复步骤B2和步骤B3并把其中的u(0)替换为当前迭代后的角度值,不断迭代,直至补偿角度与实际相位漂移角度误差小于0.0001rad。

[0024] 优选地,所述步骤C包括如下步骤:

[0025] 步骤C1:将步骤B中的最后迭代角度作为实际的最优相位补偿角度;

[0026] 步骤C2:Bob将最优相位补偿角度通过经典信道传输给Alice,并由Alice加载Alice 端的相位调制器PM上进行相位补偿。

[0027] 优选地,步骤A1中每一帧中的有效数据与训练数据为多组,且每一组有效数据对应一组训练数据,通过计算训练数据的相位漂移来判断其对应有效数据的相位漂移。

[0028] 优选地,步骤C2中Bob是在量子信号传输完毕后经数据处理得到补偿角度再传给Alice,Alice对其有效数据单独实施调相操作,并不做传输处理,其实施的相位补偿为离线补偿。

[0029] 优选地,步骤A4中的预设角度u(0)能够随机任意设置,即最优补偿角度的求解与预设角度u(0)无关。

[0030] 优选地,步骤A1中,在每一帧的帧头和有效数据之间插入训练数据S。

[0031] 优选地,S_B为Bob端用探测器对传输的训练数据S的实际测量值,包括引入的信道

衰减与噪声;搜索方向d_0选取梯度的负方向;所述CVQKD系统下针对高速漂移的离线相位补偿方法能够通过控制搜索步长λ在保证精度为0.0001rad情况下达到最少的迭代次数。

[0032] 根据本发明提供的一种存储有计算机程序的计算机可读存储介质,所述计算机程序被处理器执行时实现上述的CVQKD系统下针对高速漂移的离线相位补偿方法的步骤。

[0033] 与现有技术相比,本发明具有如下的有益效果:

[0034] 1、本发明提供的CVQKD系统下针对高速漂移的离线相位补偿方法,具有步骤清晰直接,计算效率高、补偿精度高的优点;

[0035] 2、本发明提供的CVQKD系统下针对高速漂移的离线相位补偿方法,通过反馈优化求解最小均方误差使预设相位补偿角度逐步迭代逼近实际相位漂移角度,可以在相位漂移速度较快时提高基于高斯调制相干态的CVQKD系统的相位补偿精度至 0.0001rad;

[0036] 3、本发明提供的CVQKD系统下针对高速漂移的离线相位补偿方法,为了使得系统能够对较高速的相位漂移进行补偿,系统采用一帧中多组训练数据和有效数据一一对应的帧结构,并进行线下的相位补偿算法,并不耽误光纤中数据的传输,从而有效避免了系统实时性的问题;

[0037] 4、本发明提供的CVQKD系统下针对高速漂移的离线相位补偿方法,利用反馈优化并不断迭代求解两端数据的最小平方误差,找出其对应的最优补偿角度,并通过改变步长来控制迭代次数与提高补偿精度。

[0038] 5、本发明提供的CVQKD系统下针对高速漂移的离线相位补偿方法,能够处理高速的相位漂移,解决了补偿速度跟不上漂移速度的问题,且精度水平相较于先前的相位补偿方法提高了20倍,从而为连续变量量子密钥分发系统的有效性与精确性做出贡献。

附图说明

[0039] 通过阅读参照以下附图对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

[0040] 图1为CVQKD系统帧结构。

[0041] 图2为针对高速漂移的离线相位补偿算法原理图。

[0042] 图中:

[0043] CWLaser表示激光器;

[0044] AM、PM分别为幅度调制器、相位调制器;

[0045] BS、PBS分别为分束器、偏振分束器;

[0046] DL为延时线;

[0047] LO、Signal分别为本振光、信号光;

[0048] VOA为衰减器;

[0049] φ_{opt}为最优补偿角。

具体实施方式

[0050] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明,但不以任何形式限制本发明。应当指出的是,对本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变化和改进。这些都属于本发明

的保护范围。

[0051] 根据本发明提供的一种CVQKD系统下针对高速漂移的离线相位补偿方法，包括如下步骤：

[0052] 步骤A：训练数据与有效数据的设定与传输，具体为：在有效数据的传输中间插入被Alice和Bob已知的训练数据，并通过量子信道进行传输，且Bob端预设补偿角度；

[0053] 步骤B：根据步骤A得到的补偿模型和预设补偿角度确立误差函数，这里的误差函数采用平方误差；并通过确立搜索方向和搜索步长再利用搜索迭代算法找出最小平方误差；

[0054] 步骤C：Bob根据步骤B得到的误差函数，找出对应于最小平方误差的补偿角度即为最优补偿角度；Alice发送端把最优补偿角度加载到其相位调制器上进行相位补偿。

[0055] 所述步骤A包括如下步骤：

[0056] 步骤A1：在相位漂移速度较快时，即每一帧中的多组有效数据的相漂角度均不一致，将每一帧中的多组有效数据中间均插入长度为1000的训练数据S；

[0057] 步骤A2：Alice将有效数据与训练数据一并传输给Bob；

[0058] 步骤A3：对训练数据做后处理操作；根据训练数据S确立通信两端的相应传输数据；Alice端的训练数据S_A＝S，Bob端接收的训练数据S_B＝T·S+E；其中，T为信道的透过率，E为信道的加性高斯白噪声；

[0059] 步骤A4：Bob端预设角度u(0)作为初始迭代补偿角度。

[0060] 所述步骤B包括如下步骤：

[0061] 步骤R1：确立Alice和Bob两端数据误差ER(0)；其中$ER(0)=S_B-S_A\cdot e^{ju(0)}$；

[0062] 其中，e为自然对数的底，j代表虚数单位；

[0063] 步骤B2：平方误差$MSE(0)=E[|ER(0)|^2]=R(0)f(u(0))+\sigma^2$；其中R(0)为S的自相关函数，$f(u(0))=E[|Te^{j\Phi}-e^{ju(0)}|^2]$，Φ为实际的相位漂移角度，$\sigma^2$为信道加性噪声E 的方差；

[0064] 其中，E[ ]代表取括号内函数的均值；

[0065] 步骤B3：求解最小平方误差min{MSE(0)}等效于求解f(u(0))的最小值；梯度$\nabla f(u(0))=2Tsin(u(0)-\phi)$，搜索方向$d_0=-\nabla f(u(0))=-2Tsin(u(0)-\phi)$；找出最小迭代次数对应的步长λ作为最优迭代步长；进行第一次补偿角度迭代$u(1)=u(0)+\lambda d_0$；

[0066] 步骤B4：重复步骤B2和步骤B3并把其中的u(0)替换为当前迭代后的角度值，不断迭代，直至补偿角度与实际相位漂移角度误差小于0.0001rad。

[0067] 所述步骤C包括如下步骤：

[0068] 步骤C1：将步骤B中的最后迭代角度作为实际的最优相位补偿角度；

[0069] 步骤C2：Bob将最优相位补偿角度通过经典信道传输给Alice，并由Alice加载Alice 端的相位调制器PM上进行相位补偿。

[0070] 步骤A1中每一帧中的有效数据与训练数据为多组，且每一组有效数据对应一组训练数据，通过计算训练数据的相位漂移来判断其对应有效数据的相位漂移。

[0071] 步骤C2中Bob是在量子信号传输完毕后经数据处理得到补偿角度再传给Alice，Alice对其有效数据单独实施调相操作，并不做传输处理，其实施的相位补偿为离线补偿。

[0072] 步骤A4中的预设角度u(0)能够随机任意设置，即最优补偿角度的求解与预设角度u(0)无关。

[0073] 步骤A1中，在每一帧的帧头和有效数据之间插入训练数据S。

[0074] S_B为Bob端用探测器对传输的训练数据S的实际测量值，包括引入的信道衰减与噪声；搜索方向d_0选取梯度的负方向；所述CVQKD系统下针对高速漂移的离线相位补偿方法能够通过控制搜索步长λ在保证精度为0.0001rad情况下达到最少的迭代次数。

[0075] 根据本发明提供的一种存储有计算机程序的计算机可读存储介质，所述计算机程序被处理器执行时实现上述的CVQKD系统下针对高速漂移的离线相位补偿方法的步骤。

[0076] 进一步地，本发明优选例提供了一种连续变量量子密钥分发系统离线相位补偿方法，包括：步骤A：训练数据与有效数据的设定与传输；步骤B：误差函数的构造及其最优值求解；步骤C：最优补偿角度的求解与补偿实施。本发明可以在相位漂移速度较快时提高基于高斯调制相干态的CVQKD系统的相位补偿精度至0.0001rad。

[0077] 本发明优选例的目的是提供一种针对高速漂移的离线相位补偿算法，是通过反馈优化求解最小均方误差使预设相位补偿角度逐步迭代逼近实际相位漂移角度并由Alice端进行离线补偿的方法。

[0078] 根据本发明优选例提供的一种CVQKD系统下针对高速漂移的离线相位补偿方法，包括如下步骤：

[0079] 步骤A：训练数据与有效数据的设定与传输，具体为：在有效数据的传输中间插入被Alice和Bob已知的训练数据，并通过量子信道进行传输，且Bob端预设补偿角度；

[0080] 步骤B：根据步骤A得到的补偿模型和预设补偿角度确立误差函数，这里的误差函数采用平方误差。并通过确立搜索方向和搜索步长再利用搜索迭代算法找出最小平方误差；

[0081] 步骤C：Bob根据步骤B得到的误差函数，找出对应于最小平方误差的补偿角度即为最优补偿角度。Alice发送端把最优补偿角度加载到其相位调制器上进行相位补偿。

[0082] 所述步骤A包括如下步骤：

[0083] 步骤A1：在相位漂移速度较快时，即每一帧中的多组有效数据的相漂角度均不一致，将每一帧中的多组有效数据中间均插入长度为1000的训练数据S；

[0084] 步骤A2：Alice将有效数据与训练数据一并传输给Bob；

[0085] 步骤A3：对训练数据做后处理操作。根据训练数据S确立通信两端的相应传输数据。Alice端的训练数据$S_A=S$，Bob端接收的训练数据$S_B=T\cdot S+E$。其中，T为信道的透过率，E为信道的加性高斯白噪声；

[0086] 步骤A4：Bob端预设角度u(0)作为初始迭代补偿角度。在每一帧的帧头和有效数据之间插入训练数据S。通过训练数据的相位漂移判断有效数据的相位漂移。为使得补偿结果稳定在精度范围要求以内，每次都采取1000点的训练数据作为样本。

[0087] 步骤A1中每一帧中的有效数据与训练数据为多组，且每一组有效数据对应一组训练数据，通过计算训练数据的相位漂移来判断其对应有效数据的相位漂移，如图1所示。

[0088] 步骤A4中的预设角度u(0)可以随机任意设置。即最优补偿角度的求解与预设角度u(0)无关。

[0089] 所述步骤B如下：

[0090] 步骤B：根据步骤A得到的补偿模型和预设补偿角度确立误差函数，这里的误差函数采用平方误差。并通过确立搜索方向和搜索步长再利用搜索迭代算法找出最小平方误

差；

[0091] 所述步骤B包括如下步骤：

[0092] 步骤R1：确立Alice和Bob两端数据误差ER(0)。其中ER(0)＝S_B-S_A·$e^{ju(0)}$。

[0093] 步骤B2：平方误差MSE(0)＝E[|ER(0)|^2]＝R(0)f(u(0))+σ^2。其中R(0)为S的自相关函数，f(u(0))＝E[|$Te^{j\Phi}$-$e^{ju(0)}$|^2]，Φ为实际的相位漂移角度，σ^2为信道加性噪声E 的方差。

[0094] 步骤B3：求解最小平方误差min{MSE(0)}等效于求解f(u(0))的最小值。梯度$\nabla f(u(0)) = 2Tsin(u(0)-\phi)$，搜索方向$d_0 = -\nabla f(u(0)) = -2Tsin(u(0)-\phi)$。找出最小迭代次数对应的步长λ作为最优迭代步长。进行第一次补偿角度迭代u(1)＝u(0)+ λd_0。

[0095] 步骤B4：重复步骤B2和步骤B3并把其中的u(0)替换为当前迭代后的角度值，不断迭代，直至补偿角度与实际相位漂移角度误差小于0.0001rad。

[0096] S_B为Bob端用探测器对传输的训练数据S的实际测量值，包含了信道的衰减与噪声的引入。

[0097] 由于S的自相关函数R(0)≥0且σ^2≥0，因此求解最小平方误差min{MSE(0)}等效于求解f(u(0))的最小值。

[0098] 由于梯度方向为函数增长最快的方向，而目标函数为平方误差的最小值，因此搜索方向d_0选取梯度的负方向。

[0099] 通过控制搜索步长λ使得整个补偿算法在保证精度为0.0001rad情况下达到最少的迭代次数。

[0100] 所述步骤C如下：

[0101] 步骤C：Bob根据步骤B得到的误差函数，找出对应于最小平方误差的补偿角度即为最优补偿角度。Alice发送端把最优补偿角度加载到其相位调制器上进行相位补偿。

[0102] 步骤C包括如下步骤：

[0103] 步骤C1：将步骤B中的最后迭代角度作为实际的最优相位补偿角度；

[0104] 步骤C2：在量子信号传输结束后Bob将最优相位补偿角度通过经典信道传输给Alice，并由Alice加载Alice端的相位调制器PM上进行相位补偿。

[0105] 系统的相位为本振光与信号光的相对相位差。将最优补偿角加载到接收端Bob的本振光相位调制器PM上调节本振光的实际相位相当于调节本振光与信号光的相对相位差。

[0106] 步骤C2中Bob是在量子信号传输完毕后经数据处理得到补偿角度再传给Alice，Alice对其有效数据单独实施调相操作，并不做传输处理，其实施的相位补偿为离线补偿。

[0107] 更进一步地，本发明优选例提为了使得系统能够对较高速的相位漂移进行补偿，系统采用一帧中多组训练数据和有效数据一一对应的帧结构，并进行线下的相位补偿算法，并不耽误光纤中数据的传输，从而有效避免了系统实时性的问题。除此之外，利用反馈优化并不断迭代求解两端数据的最小平方误差，找出其对应的最优补偿角度，并通过改变步长来控制迭代次数与提高补偿精度。最终运用本发明的方法能够处理高速的相位漂移，解决了补偿速度跟不上漂移速度的问题，且精度水平相较于先前的相位补偿方法提高了20倍，从而为连续变量量子密钥分发系统的有效性与精确性做出贡献。

[0108] 为实现上述目的，本发明优选例采用的技术方案如下：

[0109] 首先在每一帧数据的帧头之后的每一组有效数据之前均插入1000点的训练数据S，其中训练数据为Alice和Bob已知，如图1所示。

[0110] 在量子信道中传输训练数据S，Alice端的数据S_A＝S，Bob端的数据S_B为Bob对传输训练数据的测量值。

[0111] Bob端预设角度u(0)作为初始迭代补偿角度。

[0112] 计算通信两端数据的误差ER(0)＝S_B-S_A•$e^{ju(0)}$。

[0113] 计算平方误差MSE(0)＝E[|ER(0)|^2]＝R(0)f(u(0))+σ^2。

[0114] 选择搜索方向$d_0 = -\nabla f(u(0)) = -2Tsin(u(0)-\phi)$。选取最小迭代次数对应的步长λ作为最优迭代步长。进行第一次补偿角度迭代u(1)＝u(0)+λd_0。

[0115] 不断迭代直至误差小于0.0001rad即为求解f(u(0))＝E[|$Te^{j\Phi}$-$e^{ju(0)}$|^2]的最小值。

[0116] 在量子信号传输完毕后Bob将最后迭代角度作为最优相位补偿角度通过经典信道传输给Alice，并加载到Alice端的相位调制器PM上进行相位补偿。

[0117] 在本申请的描述中，需要理解的是，术语“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本申请和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本申请的限制。

[0118] 本领域技术人员知道，除了以纯计算机可读程序代码方式实现本发明提供的系统、装置及其各个模块以外，完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系统、装置及其各个模块以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同程序。所以，本发明提供的系统、装置及其各个模块可以被认为是一种硬件部件，而对其内包括的用于实现各种程序的模块也可以视为硬件部件内的结构；也可以将用于实现各种功能的模块视为既可以是实现方法的软件程序又可以是硬件部件内的结构。

[0119] 以上对本发明的具体实施例进行了描述。需要理解的是，本发明并不局限于上述特定实施方式，本领域技术人员可以在权利要求的范围内做出各种变化或修改，这并不影响本发明的实质内容。在不冲突的情况下，本申请的实施例和实施例中的特征可以任意相互组合。

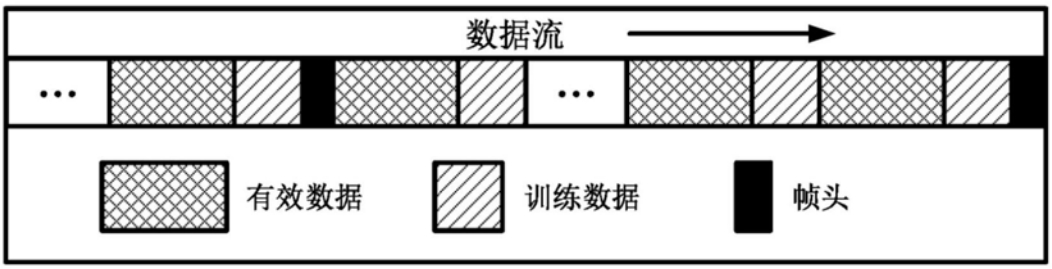

数据流
有效数据
训练数据
帧头

图1

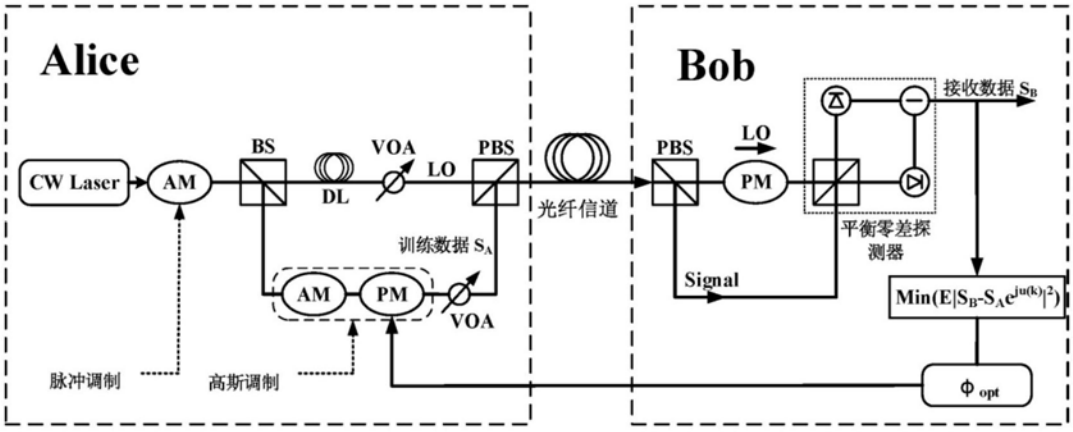

Alice
Bob
CW Laser
AM
BS
DL
VOA
LO
PBS
光纤信道
训练数据 S_A
AM
PM
VOA
脉冲调制
高斯调制
PBS
LO
PM
接收数据 S_B
平衡零差探测器
Signal
$Min(E|S_B-S_Ae^{ju(k)}|^2)$
ϕ_{opt}

图2