(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117289898 A
(43)申请公布日 2023.12.26

(21)申请号 202311122169.X

(22)申请日 2023.09.01

(71)申请人 南京大学
地址 210008 江苏省南京市鼓楼区汉口路22号

(72)发明人 张涵 夏可宇 蒙朝英 蔡淼 杨毓芳 李丰沛

(74)专利代理机构 南京苏高专利商标事务所(普通合伙) 32204
专利代理师 冯艳芬

(51)Int.Cl.
G06F 7/58(2006.01)
G06N 10/20(2022.01)
H04L 9/08(2006.01)
H04B 10/70(2013.01)
H04B 10/61(2013.01)

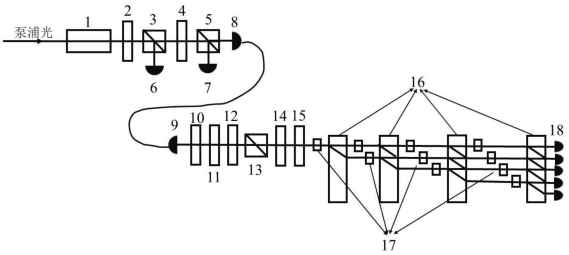
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种基于光量子行走的量子随机数产生系统及方法

(57)摘要

本发明公开了一种基于光量子行走的量子随机数产生系统及方法,包括:泵浦光源;非线性晶体;单光子性能测量模块,用于测量系统单光子性能,提取信号光子延迟后作为预报,并透射闲频光子;光纤传输模块,用于将闲频光子通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位;偏振态形成模块,用于将相位补偿后的闲频光子制备为所需偏振态的闲频光子;量子行走网络,具备多个输出端,实现闲频光子的相干概率分布;单光子探测器,量子行走网络每个输出端连接一个单光子探测器,用于将单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子进行符合测量,当符合测量成功时,将此时输出端标识数作为随机数输出。本发明可以实现按需分布、且高保真低噪声。



CN 117289898 A

1.一种基于光量子行走的量子随机数产生系统,其特征在于,包括:

泵浦光源,用于发射泵浦光;

非线性晶体,用于将入射泵浦光生成一对偏振正交的参量光子,即信号光子和闲频光子;

单光子性能测量模块,用于测量系统单光子性能,提取信号光子延迟后作为预报,并透射闲频光子;

光纤传输模块,用于将闲频光子通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位;

偏振态形成模块,用于将相位补偿后的闲频光子制备为所需偏振态的闲频光子;

量子行走网络,具备多个输出端,用于将所需偏振态的闲频光子按照目标概率分布从各输出端输出;

单光子探测器,量子行走网络每个输出端连接一个单光子探测器,用于将单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子进行符合测量,当符合测量成功时,将此时输出端标识数作为随机数输出。

2.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述非线性晶体具体为具有畴周期反转结构的II型准相位匹配的PPKTP晶体,位于泵浦光束腰处。

3.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述非线性晶体之后还放置有长通滤波片。

4.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述单光子性能测量模块包括第一偏振分束器、第一二分之一波片、第二偏振分束器、第一光纤耦合器、第二光纤耦合器、第三光纤耦合器,所述第一二分之一波片位于所述第一偏振分束器透射端,所述第一光纤耦合器位于所述第一偏振分束器反射端,所述第二偏振分束器位于所述第一二分之一波片后方,所述第二光纤耦合器、第三光纤耦合器依次位于所述第二偏振分束器的反射端、透射端。

5.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述光纤传输模块包括单模光纤、连接在单模光纤接收端并按照光路传播方向依次设置的第四光纤耦合器、第一四分之一波片、第二二分之一波片和第二四分之一波片。

6.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述偏振态形成模块包括按照光路传播方向依次设置的第三偏振分束器、第三二分之一波片和第三四分之一波片。

7.根据权利要求1所述的基于光量子行走的量子随机数产生系统,其特征在于:所述量子行走网络包括n步量子行走分支和n+1个输出端,其中,第i步量子行走分支包括1个光束偏移器和i个二分之一波片,i个二分之一波片分别位于上一步量子行走分支射出的i个光束后方,光束偏移器位于i个二分之一波片后方,从而将从i个二分之一波片透射的光束偏移后形成i+1个光束;i＝1,…,n,n为大于等于1的正整数;所述量子行走网络中每两个相邻光束偏移器之间的平行四边形光路是1个M-Z干涉仪,且每个M-Z干涉仪的上下两臂光程相等。

8.根据权利要求7所述的基于光量子行走的量子随机数产生系统,其特征在于:所述系统还包括:

分光比计算模块,用于按照预设算法计算出所述量子行走网络每个二分之一波片的最优分光比,该最优分光比使得所述量子行走网络输出量子随机数符合目标概率分布。

9.根据权利要求8所述的基于光量子行走的量子随机数产生系统,其特征在于:所述分光比计算模块在执行时用于实现如下步骤:

步骤A:建立量子行走网络第i个输出端的概率分布P_i关于每个二分之一波片分光比$\{\theta_j\}$的函数关系:$P_i=F(\{\theta_j|j=1,\cdots,m\})$,$i=1,..,n+1$,m为二分之一波片的数量;

步骤B:在0到1范围内随机取值,作为量子行走网络中二分之一波片的分光比θ_j的初始值;

步骤C:利用步骤A中建立的函数关系,根据当前的二分之一波片的分光比计算量子行走网络的概率分布$\{P_i|i=1,\cdots,n+1\}$;

步骤D:计算目标概率分布$\{T_i\}$与当前量子行走网络的概率分布$\{P_i\}$之间的损失

$$L=\frac{1}{2}\sum_1^{n+1}(T_i-P_i)^2;$$

步骤E:根据误差梯度下降过程的原理,将每个二分之一波片的分光比的值更新为:$[\theta_j-\eta\cdot\nabla_{\theta_j}(L)]$,其中$\eta$为学习率,取值范围在0到1之间,$\nabla_{\theta_j}(L)$为损失L关于每个二分之一波片的分光比的导数,通过链式求导公式得出;

步骤F:迭代重复执行步骤C至步骤E,直到损失小于设定值时,停止迭代过程,并将此时的二分之一波片的分光比作为最优分光比输出。

10.一种基于光量子行走的量子随机数产生方法,其特征在于,包括:

步骤1:泵浦光入射非线性晶体,小部分泵浦光子生成一对偏振正交的参量光子,即信号光子和闲频光子,透射非线性晶体之后的长通滤波片,大部分泵浦光子被长通滤波片反射滤除;

步骤2:在长通滤波片之后放置单光子性能测量模块,用于测量系统单光子性能,提取信号光子延迟后作为预报,并透射闲频光子;

步骤3:将闲频光子通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位;

步骤4:将相位补偿后的闲频光子制备为所需偏振态的闲频光子;

步骤5:采用量子行走网络将所需偏振态的闲频光子按照目标概率分布从各输出端输出,量子行走网络具备多个输出端;

步骤6:在量子行走网络输出端上分别用单光子探测器收集闲频光,并做单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子的符合测量,当符合测量成功时,将此时输出端标识数作为随机数输出。

一种基于光量子行走的量子随机数产生系统及方法

技术领域

[0001] 本发明涉及光学量子信息处理技术,尤其涉及一种基于光量子行走的量子随机数产生系统及方法。

背景技术

[0002] 随机数是一种重要资源,从密码学、彩票、仿真到计算机应用程序等,不同程度地需要产生随机数。当经典的算法生成器产生随机数序列时,它们是完全确定的,并且表现出巨大且有限的周期,被认为是一种伪随机数。相反,量子随机数产生器是利用量子物理体系的波动性和其内禀的随机性来产生随机数,是由量子力学的态叠加原理和测量原理所保证的,是真正的随机数。产生量子随机数有多种方法,包括:基于放射性衰变的量子随机数产生器、基于噪声的量子随机数产生器和光学量子随机数产生器等,在光学量子随机数产器中,又有基于激光相位噪声、基于光子到达时间和基于路径分支的量子随机数产生器等,其中,基于路径分支的量子随机数产生器由于其构造简单、稳定可靠和易于实现而被广泛应有。然而一般基于多分束器的路径分支量子随机数产生器会有多个内置的M-Z干涉仪,分束器分束比的不确定性以及M-Z干涉仪两臂之间光学长度随外界环境的变化都会导致干涉仪噪声较高、保真度较低,难以产生满足实际需求的量子随机数序列。此外,量子随机数产生器需要有考虑多种概率分布,包括量子秘钥分发常用的均匀分布,以及蒙特卡洛和噪声模拟应用所需要的高斯分布等,如何在技术上解决这些问题是进一步扩展量子随机数产生器应用的关键所在。

发明内容

[0003] 发明目的:本发明针对现有技术存在的问题,提供一种可以按需分布、且高保真低噪声的基于光量子行走的量子随机数产生系统及方法。

[0004] 技术方案:本发明所述的基于光量子行走的量子随机数产生系统包括:

[0005] 泵浦光源,用于发射泵浦光;

[0006] 非线性晶体,用于将入射泵浦光生成一对偏振正交的参量光子,即信号光子和闲频光子;

[0007] 单光子性能测量模块,用于测量系统单光子性能,提取信号光子延迟后作为预报,并透射闲频光子;

[0008] 光纤传输模块,用于将闲频光子通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位;

[0009] 偏振态形成模块,用于将相位补偿后的闲频光子制备为所需偏振态的闲频光子;

[0010] 量子行走网络,具备多个输出端,用于将所需偏振态的闲频光子按照目标概率分布从各输出端输出;

[0011] 单光子探测器,量子行走网络每个输出端连接一个单光子探测器,用于将单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子进行符合测量,当符合测量成

功时,将此时输出端标识数作为随机数输出。

[0012] 进一步的,所述非线性晶体具体为具有畴周期反转结构的II型准相位匹配的PPKTP晶体,位于泵浦光束腰处。

[0013] 进一步的,所述非线性晶体之后还放置有长通滤波片。

[0014] 进一步的,所述单光子性能测量模块包括第一偏振分束器、第一二分之一波片、第二偏振分束器、第一光纤耦合器、第二光纤耦合器、第三光纤耦合器,所述第一二分之一波片位于所述第一偏振分束器透射端,所述第一光纤耦合器设置于所述第一偏振分束器反射端,所述第二偏振分束器位于所述第一二分之一波片后方,所述第二光纤耦合器、第三光纤耦合器依次位于所述第二偏振分束器的反射端、透射端。

[0015] 进一步的,所述光纤传输模块包括单模光纤、连接在单模光纤接收端并按照光路传播方向依次设置的第四光纤耦合器、第一四分之一波片、第二二分之一波片和第二四分之一波片。

[0016] 进一步的,所述偏振态形成模块包括按照光路传播方向依次设置的第三偏振分束器、第三二分之一波片和第三四分之一波片。

[0017] 进一步的,所述量子行走网络包括n步量子行走分支和n+1个输出端,其中,第i步量子行走分支包括1个光束偏移器和i个二分之一波片,i个二分之一波片分别位于上一步量子行走分支射出的i个光束后方,光束偏移器位于i个二分之一波片后方,从而将从i个二分之一波片透射的光束偏移后形成i+1个光束;i=1,…,n,n为大于等于1的正整数;所述量子行走网络中每两个相邻光束偏移器之间的平行四边形光路是1个M-Z干涉仪,且每个M-Z干涉仪的上下两臂光程相等。

[0018] 进一步的,所述系统还包括:

[0019] 分光比计算模块,用于按照预设算法计算出所述量子行走网络每个二分之一波片的最优分光比,该最优分光比使得所述量子行走网络输出量子随机数符合目标概率分布。

[0020] 进一步的,所述分光比计算模块在执行时用于实现如下步骤:

[0021] 步骤A:建立量子行走网络第i个输出端的概率分布P_i关于每个二分之一波片分光比$\{\theta_j\}$的函数关系:$P_i=F(\{\theta_j|j=1,\cdots,m\})$,i=1,..,n+1,m为二分之一波片的数量;

[0022] 步骤B:在0到1范围内随机取值,作为量子行走网络中二分之一波片的分光比θ_j的初始值;

[0023] 步骤C:利用步骤A中建立的函数关系,根据当前的二分之一波片的分光比计算量子行走网络的概率分布$\{P_i|i=1,\cdots,n+1\}$;

[0024] 步骤D:计算目标概率分布$\{T_i\}$与当前量子行走网络的概率分布$\{P_i\}$之间的损失$L=\frac{1}{2}\sum_1^{n+1}(T_i-P_i)^2$;

[0025] 步骤E:根据误差梯度下降过程的原理,将每个二分之一波片的分光比的值更新为:$[\theta_j-\eta\cdot\nabla_{\theta_j}(L)]$,其中$\eta$为学习率,取值范围在0到1之间,$\nabla_{\theta_j}(L)$为损失L关于每个二分之一波片的分光比的导数,通过链式求导公式得出;

[0026] 步骤F:迭代重复执行步骤C至步骤E,直到损失小于设定值时,停止迭代过程,并将此时的二分之一波片的分光比作为最优分光比输出。

[0027] 本发明还提供一种基于光量子行走的量子随机数产生方法,包括:

[0028] 步骤1:泵浦光入射非线性晶体,小部分泵浦光子生成一对偏振正交的参量光子,即信号光子和闲频光子,透射非线性晶体之后的长通滤波片,大部分泵浦光子被长通滤波片反射滤除;

[0029] 步骤2:在长通滤波片之后放置单光子性能测量模块,用于测量系统单光子性能,提取信号光子延迟后作为预报,并透射闲频光子;

[0030] 步骤3:将闲频光子通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位;

[0031] 步骤4:将相位补偿后的闲频光子制备为所需偏振态的闲频光子;

[0032] 步骤5:采用量子行走网络将所需偏振态的闲频光子按照目标概率分布从各输出端输出,量子行走网络具备多个输出端;

[0033] 步骤6:在量子行走网络输出端上分别用单光子探测器18收集闲频光,并做单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子的符合测量,当符合测量成功时,将此时输出端标识数作为随机数输出。

[0034] 有益效果:本发明与现有技术相比,其显著优点是:(1)采用多步量子行走网络,通过设置量子行走网络的不同参数可产生任意所需概率分布,包括均匀分布(见图4)和高斯分布(见图5)等,调节方法十分简洁;(2)仅仅利用线性光学元件可以实现高保真低噪声的量子随机数产生器,方法便捷、稳定可靠,例如:均匀分布,左旋圆偏振保真度为95.8%(见图4),右旋圆偏振保真度为96.5%(见图4);高斯分布,左旋圆偏振保真度为95.8%(见图5),右旋圆偏振保真度为94.1%(见图5);(3)设置分光比计算模块,可以计算出量子行走网络的最优参数值(每个二分之一波片的最优分光比),使得所述量子行走网络输出的量子随机数与目标概率分布的符合度增大。

附图说明

[0035] 图1是本发明提供的基于光量子行走的量子随机数产生系统的结构示意图;

[0036] 图2是二阶时间关联函数g^2的图,符合时间3ns,g^2函数最小值是0.02860±0.00001;

[0037] 图3是4种偏振光经过4步量子行走网络后的概率分布图,柱状图顺序从左到右依次为水平偏振、垂直偏振、右旋圆偏振和左旋圆偏振光,柱状图上的横线为理论值;

[0038] 图4是以均匀分布为目标概率分布时,将右旋圆偏振光和左旋圆偏振光经4步量子行走网络后输出的量子随机数序列的概率分布图;

[0039] 图5是以高斯分布为目标概率分布时,将右旋圆偏振光和左旋圆偏振光经4步量子行走网络后输出的量子随机数序列的概率分布图。

具体实施方式

[0040] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0041] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别

不同对象,而不是用于描述特定顺序。在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本发明的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0042] 本实施例提供一种基于光量子行走的量子随机数产生系统,如图1所示,包括:用于发射泵浦光的泵浦光源;用于将入射泵浦光生成一对偏振正交的参量光(信号光和闲频光)的非线性晶体;用于测量系统单光子性能、提取信号光子延迟后作为预报,并透射闲频光子的单光子性能测量模块;用于将闲频光通过光纤传输,实现光束整形,并补偿闲频光子在光纤中产生的相位的光纤传输模块;用于将相位补偿后的闲频光制备为所需偏振态的闲频光的偏振态形成模块;具备多个输出端,用于将所需偏振态的闲频光子按照目标概率分布从各输出端输出的量子行走网络;用于将单光子性能测量模块提取的信号光子和量子行走网络输出端输出的闲频光子进行符合测量的单光子探测器,当符合测量成功时,将此时输出端标识数作为随机数输出;用于按照预设算法计算出量子行走网络每个二分之一波片的最优分光比的分光比计算模块。下面对每一模块进行详细阐述。

[0043] 泵浦光源发射脉冲泵浦光,本实施例是波长为397.49nm的脉冲光。

[0044] 非线性晶体具体是具有畴周期反转结构的II型准相位匹配的PPKTP非线性晶体1,结构周期8.8μm,位于泵浦光束腰处。脉冲泵浦光正入射PPKTP非线性晶体1产生自发参量下转换过程,生成一对偏振正交的参量光,即信号光子和闲频光子。PPKTP非线性晶体1前后两个端面均镀有泵浦光与参量光的增透膜,透过率均大于99.8%。参量光的中心波长均为794.98nm。

[0045] 非线性晶体之后还放置有长通滤波片2,用于滤除未参与自发参量下转换的泵浦光。

[0046] 单光子性能测量模块包括第一偏振分束器3、第一二分之一波片4、第二偏振分束器5、第一光纤耦合器6、第二光纤耦合器7、第三光纤耦合器8,第一二分之一波片4位于第一偏振分束器3透射端,第一光纤耦合器6设置于第一偏振分束器3反射端,第二偏振分束器5位于第一二分之一波片4后方,第二光纤耦合器7、第三光纤耦合器8依次位于第二偏振分束器5的反射端、透射端。第一偏振分束器3反射垂直偏振的信号光,透射水平偏振的闲频光子,信号光子被第一光纤耦合器6收集,延时59ns后,作为预报信号,第一偏振分束器3和第二偏振分束器5的前后端面均镀有参量光的增透膜,透射率均大于99.5%,第一二分之一波片4前后端面均镀有参量光的增透膜,透过率均大于99.8%。实验上通过电子学系统可以精确测量单个光子到达探测器的时间,如果信号光子和闲频光子同时被探测到,即两个光子到达探测器的时间差在3ns内,被认为是一个两体符合事例,并被电子学系统记录下来。预报单光子源是指精确测量信号光子的到达时间就可以预报闲频光子在时间或空间上的位置,从而产生一个单光子的序列,其单光子性用二阶时间关联函数来表征,用单光子性能测量模块来实现。二阶时间关联函数又称为g^2函数:$g^2=P(678)P(6)/[P(67)P(68)]$,这里P(678)是指光纤耦合器6、7、8同时探测到光子的三体符合事例的概率,P(6)是指第一光纤耦合器6探测到光子单体事例的概率,P(67)、P(68)分别是指6、7和6、8探测到光子两体符合事例的概率。在延迟时间$\tau=0$处,g^2函数值越接近0,表示单光子性越好(见图2)。

[0047] 光纤传输模块包括单模光纤和连接在单模光纤接收端按照光路传播方向依次设置的第四光纤耦合器9、第一四分之一波片10、第二二分之一波片11、第二四分之一波片12，单模光纤可以实现闲频光的光束整形，第一四分之一波片10、第二二分之一波片11、第二四分之一波片12组合用于补偿闲频光在单模光纤中产生的相位。上述三个波片前后端面均镀有参量光的增透膜，透过率均大于99.8％。

[0048] 偏振态形成模块包括按照光路传播方向依次设置的第三偏振分束器13、第三二分之一波片14和第三四分之一波片15。可以转动第三二分之一波片14和第三四分之一波片15角度使偏振分束器13出射的水平偏振态转化为任意偏振态(包括水平偏振、垂直偏振、左旋圆偏振和右旋圆偏振态)。第三偏振分束器13的前后端面均镀有参量光的增透膜，透射率均大于99.5％，第三二分之一波片14和第三四分之一波片15前后端面均镀有参量光的增透膜，透过率均大于99.8％。

[0049] 量子行走网络包括n步量子行走分支和n+1个输出端，其中，第i步量子行走分支包括1个光束偏移器和i个二分之一波片，i个二分之一波片分别位于上一步量子行走分支射出的i个光束后方，光束偏移器位于i个二分之一波片后方，从而将从i个二分之一波片透射的光束偏移后形成i+1个光束；i＝1，…，n，n为大于等于1的正整数；量子行走网络中每两个相邻光束偏移器之间的平行四边形光路是1个M-Z干涉仪，且每个M-Z干涉仪的上下两臂光程相等。如图1所示为一个4步量子行走网络，有5个输出端，共包括10个二分之一波片和4个光束偏移器，左起第1个二分之一波片17和第1个光束偏移器16组成第1步量子行走分支，第2、3个二分之一波片17和第2个光束偏移器16组成第2步量子行走分支，第4、5、6个二分之一波片17和第3个光束偏移器16组成第3步量子行走分支，第7、8、9、10个二分之一波片17和第4个光束偏移器16组成第4步量子行走分支，继续增加二分之一波片17和光束偏移器16数量可扩展成更多步数的量子行走网络。光束偏移器16分别使垂直偏振光和水平偏振光透射，水平偏振光相对于垂直偏振光有约4mm的侧移，二分之一波片17中心波片孔径约5mm，其余为玻璃基底，可实现对单束光的偏振操控，光束偏移器16和二分之一波片17组合后可调节垂直偏振光和水平偏振光的分光比，10个二分之一波片17前后端面均镀有参量光增透膜，透过率均大于99.8％，4个光束偏移器16前后端面均镀有参量光增透膜，透过率均大于99.2％。4步量子行走网络中，每两个相邻光束偏移器之间的平行四边形光路是1个M-Z干涉仪，4步量子行走网络共形成6个M-Z干涉仪，通过倾斜光束偏移器和干涉仪内放置的二分之一波片使每个M-Z干涉仪的上下两臂光程相等。

[0050] 分光比计算模块用于按照预设算法计算出所述量子行走网络每个二分之一波片的最优分光比，该最优分光比使得所述量子行走网络输出量子随机数符合目标概率分布；在执行时用于实现如下步骤：步骤A：建立量子行走网络第i个输出的概率分布P_i关于每个二分之一波片分光比$\{\theta_j\}$的函数关系：$P_i=F(\{\theta_j|j=1,\cdots,m\})$，i＝1，..，n+1，m为二分之一波片的数量；步骤B：在0到1范围内随机取值，作为量子行走网络中二分之一波片的分光比θ_j的初始值；步骤C：利用步骤A中建立的函数关系，根据当前的二分之一波片的分光比计算量子行走网络的概率分布$\{P_i|i=1,\cdots,n+1\}$；步骤D：计算目标概率分布$\{T_i\}$与当前量子行走网络的概率分布$\{P_i\}$之间的损失$L=\frac{1}{2}\sum_1^{n+1}(T_i-P_i)^2$；步骤E：根据误差梯度下降过程的原理，将每个二分之一波片的分光比的值更新为：$[\theta_j-\eta\cdot\nabla_{\theta_j}(L)]$，其中$\eta$为学习率，取值范

围在0到1之间，$\nabla_{\theta_j}(L)$为损失L关于每个二分之一波片的分光比的导数，通过链式求导公式得出；步骤F：迭代重复执行步骤C至步骤E，直到损失小于设定值时，停止迭代过程，并将此时的二分之一波片的分光比作为最优分光比输出。最优分光比计算完成后，通过旋转量子行走网络中每个二分之一波片角度来设置偏振状态，之后通过光束偏移器的垂直偏振和水平偏振光的分光比就达到所述最优分光比。

[0051] 量子行走网络每个输出端连接一个单光子探测器18，用于将单光子性能测量模块提取的信号光子(第一光纤耦合器6输出)和当前输出端输出的闲频光子进行符合测量，当符合测量成功时，将此时输出端标识数作为随机数输出。

[0052] 本发明系统形成了一种预报单光子源，每次输出一对光子(信号光子和闲频光子)，一个信号光子被第一光纤耦合器6提取作为预报信号，另一个闲频光子进入量子行走网络后，最终会选择多个输出端中一个输出端出来。每个输出端连接一个单光子探测器18，做信号光子和闲频光子的符合测量，若信号光子和闲频光子被探测到的间差在3ns内，被认为是符合测量成功，之后将当前测量成功的输出端标识数作为随机数输出，例如，图1所示5个输出端，输出端标识数从上倒下依次可以标记为1,2,3,4,5，若闲频光子选择第3个输出端(位置标记为3)输出，被单光子探测器探测到且符合测量成功后，则输出随机数3，并被电子学系统记录下来，预报单光子源会连续发送光子对，这样会连续记录一组数据，例如;3,2,5,2,2,3,5,...，这就是量子随机数序列。因为量子行走网络的输出端概率分布符合目标概率分布，因此，量子随机数序列也符合目标概率分布。

[0053] 本实施例还提供一种基于光量子行走的量子随机数产生方法，该方法采用上述系统实现，具体包括：

[0054] 步骤1：选用波长为397.49nm的脉冲泵浦光入射PPKTP非线性晶体1，小部分泵浦光子生成一对偏振正交的参量光子，即信号光子和闲频光子，透射PPKTP非线性晶体1之后的长通滤波片2，参量光子的中心波长均为794.98nm，大部分泵浦光子被长通滤波片2反射滤除。

[0055] 步骤2：在长通滤波片2之后放置单光子性能测量模块，用于测量系统单光子性能，提取信号光子延迟后作为预报，并透射闲频光子。单光子性能测量模块包括依次放置的第一偏振分束器3、第一二分之一波片4和第二偏振分束器5，第一光纤耦合器6设置于第一偏振分束器3反射端，第二光纤耦合器7、第三光纤耦合器8依次位于第二偏振分束器5的反射端、透射端，组合后用于测量预报单光子源的二阶时间关联函数。

[0056] 步骤3：将闲频光子通过光纤传输，实现光束整形，并补偿闲频光子在光纤中产生的相位。具体实施时，闲频光子经过单模光纤整形后通过第四光纤耦合器9放出，在第四光纤耦合器9后依次放置第一四分之一波片10、第二二分之一波片11和第二四分之一波片12构成的组合波片，用于补偿闲频光子在单模光纤中产生的相位。

[0057] 步骤4：将相位补偿后的闲频光子制备为所需偏振态的闲频光子。具体可以采用第三偏振分束器13、第三二分之一波片14和第三四分之一波片15组合产生任意偏振态。

[0058] 步骤5：采用量子行走网络将所需偏振态的闲频光子按照目标概率分布从各输出端输出，量子行走网络具备多个输出端。量子行走网络根据目标概率分布使用预设算法计算出量子行走网络中每个二分之一波片的分光比，并按照分光比设置每个二分之一波片角度，使得将所需偏振态的闲频光子按照目标概率分布从各输出端输出。

[0059] 步骤6:在量子行走网络输出端上分别用单光子探测器18收集闲频光,并做单光子性能测量模块提取的信号光子和当前输出端输出的闲频光子的符合测量,当符合测量成功时,将此时输出端标识数作为随机数输出。

[0060] 对本发明进行测量,利用第三二分之一波片14和第三四分之一波片15分别产生水平偏振、垂直偏振、右旋圆偏振和左旋圆偏振光入射到量子行走网络,依次产生四种量子行走分布,见图3从左到右。以右旋圆偏振和左旋圆偏振光入射到量子行走网络,当目标概率分布为均匀分布时,本发明输出的量子随机数序列见图4,可以看出符合均匀分布,当目标概率分布为高斯分布时,本发明输出的量子随机数序列见图5,可以看出,符合高斯分布。由此可知,本发明输出的量子随机数序列符合目标概率分布。

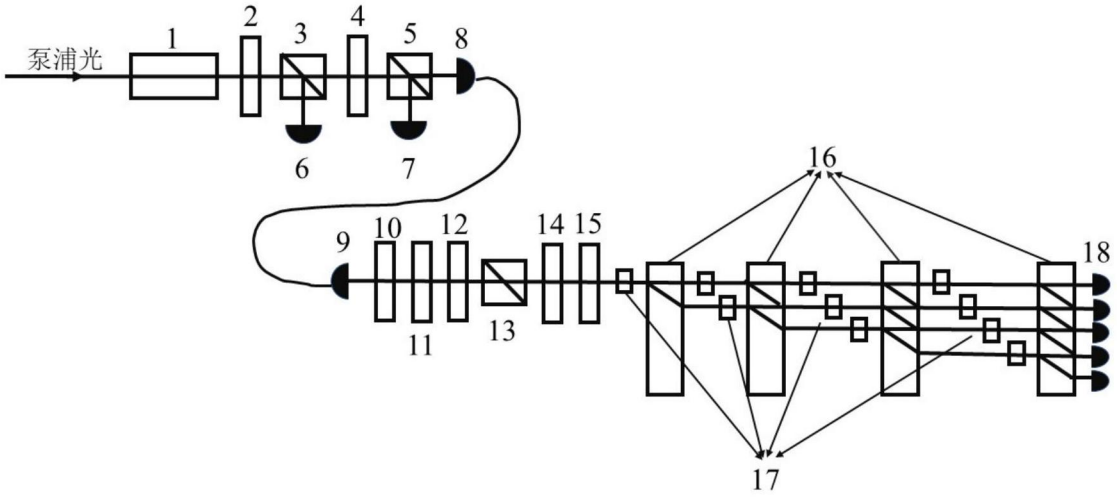

泵浦光
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

图1

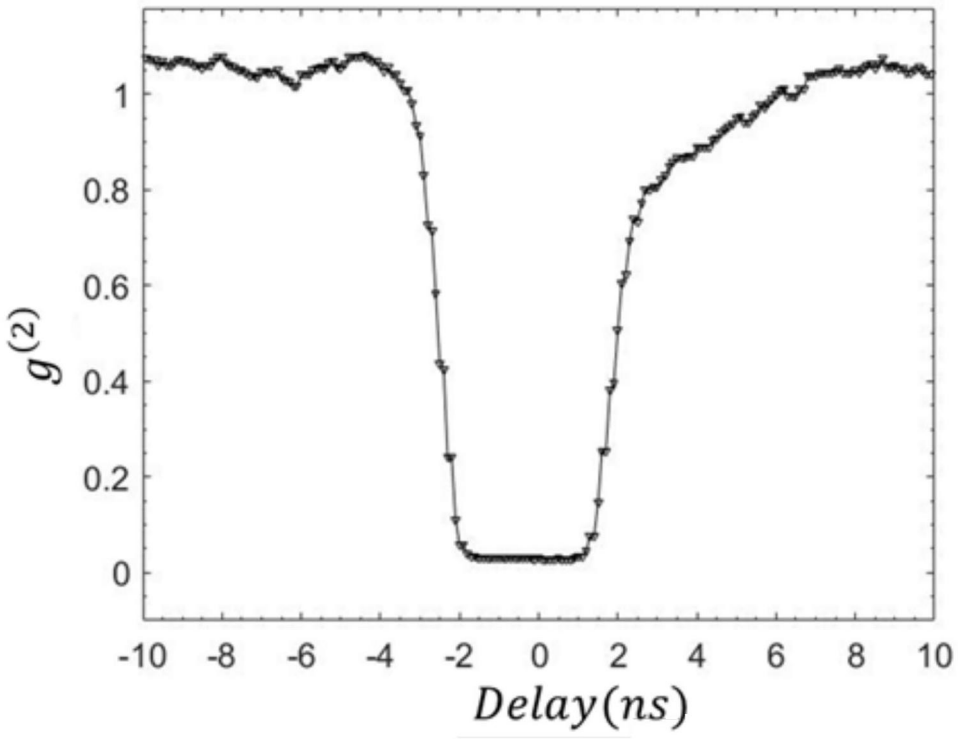

$g^{(2)}$
1
0.8
0.6
0.4
0.2
0
-10
-8
-6
-4
-2
0
2
4
6
8
10
Delay(ns)

图2

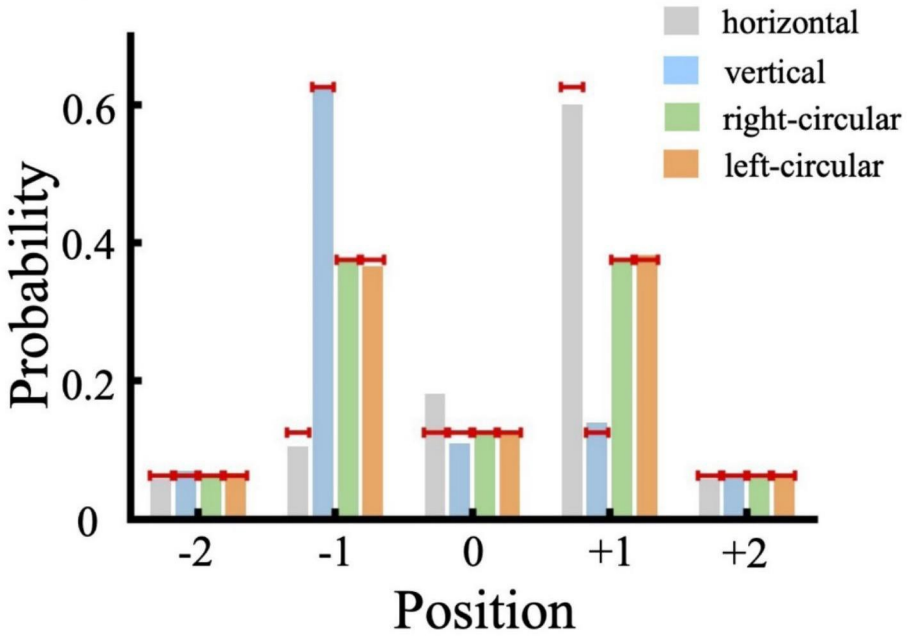

horizontal
vertical
right-circular
left-circular
Probability
0.6
0.4
0.2
0
-2
-1
0
+1
+2
Position

图3

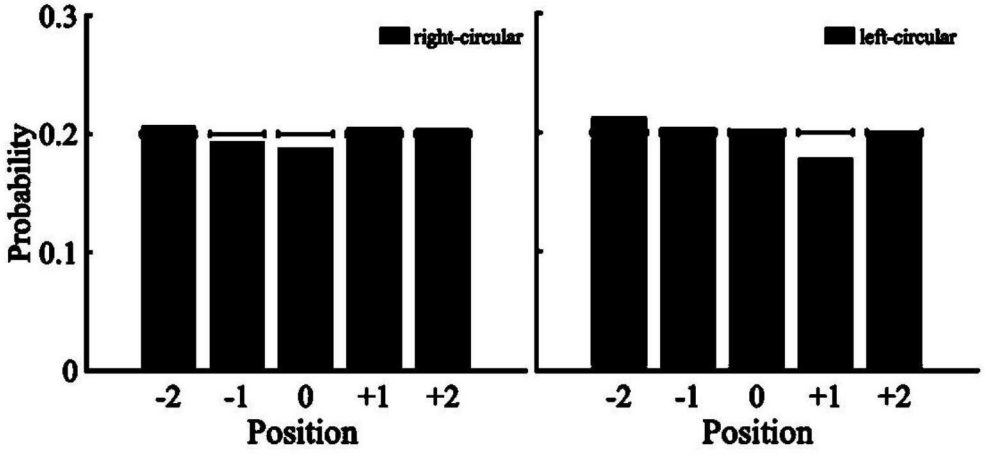

right-circular
left-circular
Probability
0.3
0.2
0.1
0
-2
-1
0
+1
+2
Position
-2
-1
0
+1
+2
Position

图4

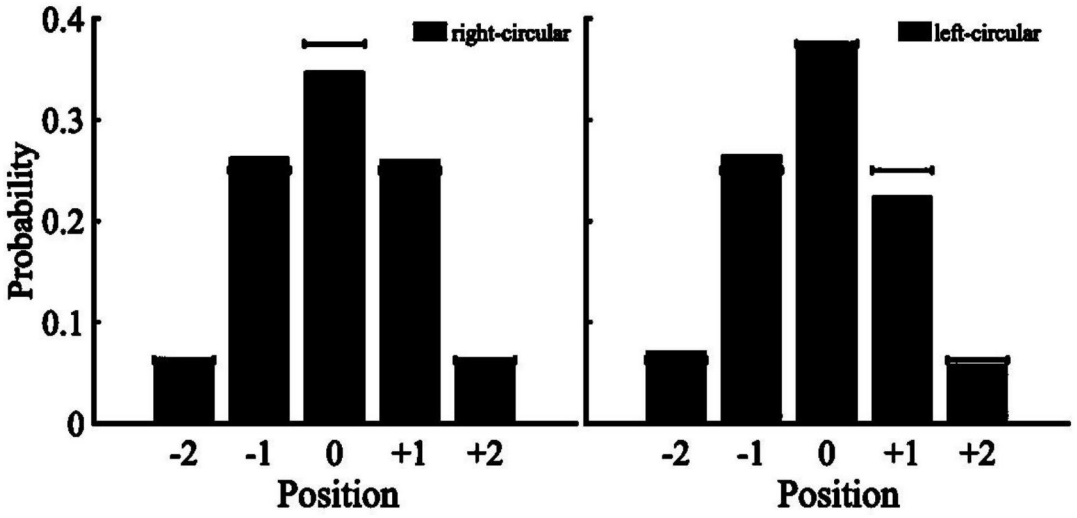

0.4
0.3
0.2
0.1
0
Probability
right-circular
-2
-1
0
+1
+2
Position
left-circular
-2
-1
0
+1
+2
Position

图5