8620

证书号第1674623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的偏振补偿实现方法

发明人：房坚;黄端;何广强;曾贵华

专利号：ZL 2012 1 0389008.2

专利申请日：2012年10月12日

专利权人：上海交通大学

授权公告日：2015年05月20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10月12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05月20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 102916807 A
(43)申请公布日 2013.02.06

(21)申请号 201210389008.2

(22)申请日 2012.10.12

(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 房坚 黄端 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)
H04B 10/85(2013.01)

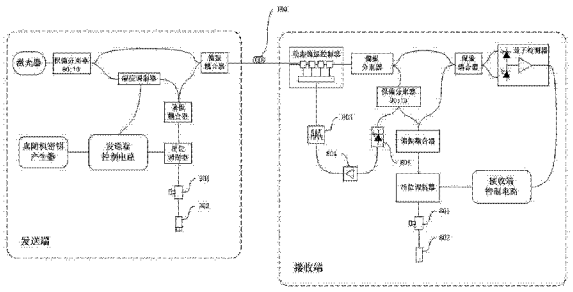
权利要求书 1 页 说明书 5 页 附图 1 页

(54)发明名称

连续变量量子密钥分发系统的偏振补偿实现方法

(57)摘要

本发明公开一种连续变量量子密钥分发系统的偏振补偿实现方法，具体为：发送端采用偏振复用的方式将信号光与本振光通过一根光纤进行传输，接收端通过偏振分束器将信号光与本振光分离，其中的偏振反馈控制方法分为两个阶段：在分光检测阶段，连续变量量子密钥分发的接收端分出一部分本振光，并通过转换电路将其转换为直流反馈电压信号；在偏振校正阶段，接收端根据直流反馈电压，用反馈算法控制动态偏振控制器，完成偏振校正。本发明提出了一种全新的连续变量量子密钥分发系统的偏振反馈控制实现方法，有效地抑制了在光纤通信过程中连续变量量子信号的偏振状态受到的环境干扰，提高了系统的稳定性，推进了连续变量量子密码的实用化。



CN 102916807 A

1. 一种连续变量量子密钥分发系统的偏振补偿实现方法，其特征在于，具体为：

在发送端：将激光器产生的脉冲激光经衰减器衰减后通过保偏分束器分为信号光和本振光两束；令信号光经过幅度调制和相位调制后，通过衰减器衰减到量子水平，然后与本振光一起通过偏振耦合器进入光纤中传输至接收端；

在接收端：令光纤中传输来的信号经动态偏振控制器后，通过偏振分束器分为信号光与本振光两束；令信号光直接进入保偏耦合器；令本振光先通过保偏分束器分为两束，其中，偏振反馈控制单元接收并根据其中的一束向动态偏振控制器输出偏振反馈控制信号，另一束通过相位调制器完成相位补偿，与信号光一起通过偏振耦合器进入量子检测器做相干检测。

2. 根据权利要求 1 所述的连续变量量子密钥分发系统的偏振补偿实现方法，其特征在于，在接收端：偏振反馈控制单元包括依次连接的光电二极管、放大器、以及有效值转换电路，其中，通过光电二极管将本振光通过保偏分束器分出的一束由光脉冲转化为电脉冲，然后通过放大器放大电脉冲，再令放大后的电脉冲经有效值转换电路转化为直流反馈电压输出到动态偏振控制器。

3. 根据权利要求 2 所述的连续变量量子密钥分发系统的偏振补偿实现方法，其特征在于，动态偏振控制器通过改变其内部的四个光纤挤压器上的电压对偏振态进行控制，使直流反馈电压达到最大值，具体包括如下步骤：

步骤（1）：动态偏振控制器采集直流反馈电压；

步骤（2）：选择第一个光纤挤压器的控制电压；

步骤（3）：适当地增加控制电压，采集此时反馈回来的直流反馈电压；

步骤（4）：如果直流反馈电压增大，则返回步骤（3），否则进入步骤（5）；

步骤（5）：适当地减小控制电压，采集此时的直流反馈电压；

步骤（6）：如果直流反馈电压增大，则返回步骤（5），否则进入步骤（7）；

步骤（7）：选择下一个光纤挤压器的控制电压，进入步骤（3）。

4. 根据权利要求 2 所述的连续变量量子密钥分发系统的偏振补偿实现方法，其特征在于，有效值转换电路采用有效值直流转换器来计算脉冲信号的真有效值，有效值直流转换器进行实时测量，完成脉冲电压到直流电压的实时转换。

5. 根据权利要求 1 所述的连续变量量子密钥分发系统的偏振补偿实现方法，其特征在于，在发送端，将信号光与本振光通过偏振复用的方式在同一根光纤中传输；在接收端，通过偏振分束器将偏振复用的本振光与信号光分成两路后，对本振光进行分光。

连续变量量子密钥分发系统的偏振补偿实现方法

技术领域

[0001] 本发明涉及一种量子密码通信领域的技术，具体地说，是一种连续变量量子密钥分发系统的偏振补偿实现方法。

背景技术

[0002] 随着经济的发展和科学的进步，信息化、数字化进程不断加快，信息传递和互换越来越频繁，因此对信息传达过程的安全性和可靠性有越来越高的要求。如何安全地传递信息已经成为现代通信领域的重要问题。应用密码学由此应运而生，尤其在第二次世界大战中的广泛使用，更加体现出了密码学的重要性。到目前为止，密码学在政治、军事、经济、文化等社会生活的各个方面都起着重要的作用。

[0003] 经典密码通信可以分为两大类：非对称密码系统和对称密码系统。非对称密码系统又称为公开密钥系统，如现在广为采用的 RSA 算法。接收方先选择一组只有他知道的专用密钥，依次计算出相应的公开密钥，再将公开密钥分给所以人用来加密信息。非对称密码系统的安全性依赖于计算的复杂度。一旦量子计算机研制出世，计算的速度将会极大提升，破解非对称密码系统的难度将会显著降低；对称密码系统又称为专用密钥系统，如公认绝对安全的一次一密包（One-Time-Pad），发送方与接收方拥有相同的密钥。密钥只用一次，并且密钥长度不小于信息长度。这样安全性就得到了保证，代价是降低了密码的使用效率。

[0004] 量子密码通信与经典密码通信不同，其安全性基于量子物理的基本特性而非计算的复杂性。它不是单纯利用计算复杂性使窃听者在有限时间内不能破译密码，而是利用量子力学的基本原理和特性来发现是否有窃听者存在，以此确立合法通信者与窃听者之间对比出的信息优势，从而确保通信的安全。因此，在量子计算不断发展的今天，研究并实现量子密码技术是非常必要的。

[0005] 经过这二十几年的发展，量子密码通信已从理论研究逐步走向实际应用。根据实现方式的不同，主要分为离散变量量子密钥分发系统和连续变量量子密钥分发系统。其中离散变量量子密钥分发通过单光子的方式来实现。由于现在还无法使用理想的单光子源，因此主要是通过将相干光进行衰减，使得每个脉冲的平均光子数小于 1。激光源的光子数服从泊松分布，除了含有单光子脉冲之外还含有多光子脉冲。这些多光子脉冲被窃听之后不会被察觉，从而影响密码系统的安全性。使用诱骗态（Decoy State）可以很大程度上解决这个问题，但是增加了实际系统的复杂程度。

[0006] 连续变量量子密码起步比离散变量要晚一些，直到 1999 年 Ralph 首先提出利用连续变量进行量子密钥分发的概念。与离散变量不同，连续变量将信息编码在连续的正则分量上（如正则位置 X 和正则动量 P），在每个比特上能够比离散变量编码更多的信息。采用的光源可以是相干态、压缩态或者纠缠态。考虑到实验上的方便，一般都采用相干激光作为光源。连续变量量子密钥分发采用 Homodyne 检测器作为量子检测器，与离散变量相比，具有成本上的优势。因此连续变量量子密钥分发有着很好的实用化发展前景。

[0007] 目前，连续变量量子密钥分发系统均采用的双不等臂干涉结构。此种结构很容易

受到各种因素的影响。这些因素包括但不限于：

[0008] 1. 温度变化：铌酸锂材质的电光调制器本身对于温度的变化比较敏感，不稳定的环境温度会在调制时产生较大的偏差。

[0009] 2. 系统所受到的机械振动，机械振动会在光纤中产生应力，导致折射率发生改变，使得在光纤中传输的光偏振态产生漂移。

[0010] 3. 空气流动的影响。空气流动会对未紧致固定的光纤产生扰动，导致偏振态发生漂移。

[0011] 4. 电磁辐射场的影响：电磁辐射（诸如手机信号、交流电产生的电磁波）会对系统的电路部分产生比较明显的干扰，收到的干扰最明显就是量子检测器部分。

[0012] 为了解决这些问题，让连续变量量子密钥分发系统能够具有较高的稳定性，我们需要对环境的影响进行监测，并通过反馈的方式来校准，使得系统对于环境干扰具有抵抗能力，并能够长时间连续工作。

发明内容

[0013] 针对现有技术中的缺陷，本发明的目的在于针对连续变量量子密钥分发系统偏振反馈控制方案的空白，提出了一种全新的偏振反馈控制方案，推进了连续变量量子密码的实用化，同时有效地抑制了在量子通信过程中连续变量量子信号的偏振受到的环境干扰。

[0014] 根据本发明的一个方面，提供一种连续变量量子密钥分发系统的偏振补偿实现方法，具体为：

[0015] 在发送端：将激光器产生的脉冲激光经衰减器衰减后通过保偏分束器分为信号光和本振光两束；令信号光经过幅度调制和相位调制后，通过衰减器衰减到量子水平，然后与本振光一起通过偏振耦合器进入光纤中传输至接收端；

[0016] 在接收端：令光纤中传输来的信号经动态偏振控制器后，通过偏振分束器分为信号光与本振光两束；令信号光直接进入保偏耦合器；令本振光先通过保偏分束器分为两束，其中，偏振反馈控制单元接收并根据其中的一束向动态偏振控制器输出偏振反馈控制信号，另一束通过相位调制器完成相位补偿，与信号光一起通过偏振耦合器进入量子检测器做相干检测。

[0017] 优选地，在接收端：偏振反馈控制单元包括依次连接的光电二极管、放大器、以及有效值转换电路，其中，通过光电二极管将本振光通过保偏分束器分出的一束由光脉冲转化为电脉冲，然后通过放大器放大电脉冲，再令放大后的电脉冲经有效值转换电路转化为直流反馈电压输出到动态偏振控制器。

[0018] 优选地，动态偏振控制器通过改变其内部的四个光纤挤压器上的电压对偏振态进行控制，使直流反馈电压达到最大值，具体包括如下步骤：

[0019] 步骤（1）：动态偏振控制器采集直流反馈电压；

[0020] 步骤（2）：选择第一个光纤挤压器的控制电压；

[0021] 步骤（3）：适当地增加控制电压，采集此时反馈回来的直流反馈电压；

[0022] 步骤（4）：如果直流反馈电压增大，则返回步骤（3），否则进入步骤（5）；

[0023] 步骤（5）：适当地减小控制电压，采集此时的直流反馈电压；

[0024] 步骤（6）：如果直流反馈电压增大，则返回步骤（5），否则进入步骤（7）；

[0025] 步骤(7):选择下一个光纤挤压器的控制电压,进入步骤(3)。

[0026] 优选地,有效值转换电路采用有效值直流转换器(RMS-DC)来计算脉冲信号的真有效值,有效值直流转换器进行实时测量,完成脉冲电压到直流电压的实时转换。

[0027] 优选地,在发送端,将信号光与本振光通过偏振复用的方式在同一根光纤中传输;在接收端,通过偏振分束器将偏振复用的本振光与信号光分成两路后,对本振光进行分光。

[0028] 更为具体地,为实现上述目的,本发明的一个优选的实施例所采用的技术方案如下:

[0029] 本发明所述的具有偏振反馈功能的连续变量量子密钥分发系统,包含发送端和接收端两部分,发送端和接收端均由各自的光路部分和电路部分组成。其中所述光路部分主要由激光器、衰减器、保偏分束器、保偏耦合器、法拉第镜、可调延时线、偏振耦合器、偏振分束器、动态偏振控制器、幅度调制器和相位调制器组成;所述电路部分由真随机密钥产生器、发送端和接收端的控制电路、量子检测器和偏振反馈控制单元组成。

[0030] 发送端:激光器产生脉冲激光,经衰减器衰减后被 10:90 保偏分束器分为两束,10% 的一束作为信号光,90% 的一束作为本振光。信号光经过幅度调制和相位调制后,通过衰减器衰减到量子水平,然后与本振光一起通过偏振耦合器进入光纤中传输。

[0031] 接收端:光纤中的信号通过动态偏振控制器后,被偏振分束器分为信号光与本振光两束。信号光直接进入保偏耦合器,本振光先通过 10:90 的保偏分束器分为两束,10% 的一束用来做为偏振反馈控制信号,其余通过相位调制器完成相位补偿,与信号光一起做相干检测。通过调节可调延时线使得双不等臂干涉结构达到平衡。

[0032] 本发明提出的偏振反馈控制实现方法分为两个阶段,分光检测阶段和偏振校正阶段。方案如下:

[0033] 分光检测阶段:连续变量量子密钥分发的接收端将收到的信号用偏振耦合器进行偏振解复用,之后将得到的本振光分出一部分,通过脉冲转换电路将脉冲光信号转换为直流电压信号。

[0034] 脉冲转换电路采用光电二极管将光脉冲转化为电脉冲。由于用于分光检测的光强很小,电脉冲信号很微弱,因此需要使用放大器进行放大。放大后的电脉冲用有效值转换器(RMS-DC)进行处理,将其转化为直流电压。

[0035] 偏振校正阶段:将脉冲转化电路输出的直流电压反馈给接收端的动态偏振控制器,动态偏振控制器对直流反馈电压进行采样,并通过下述的偏振反馈控制算法来持续调节动态偏振控制器,使得直流反馈电压保持最大值。

[0036] 动态偏振控制器通过改变其内部的四个光纤挤压器上的电压对偏振态进行控制。偏振反馈算法的主要步骤如下:

[0037] 步骤(1):动态偏振控制器采集直流反馈电压;

[0038] 步骤(2):选择第一个光纤挤压器的控制电压;

[0039] 步骤(3):适当地增加电压,采集此时反馈回来的直流反馈电压;

[0040] 步骤(4):如果直流反馈电压增大,则返回步骤(3),否则进入步骤(5);

[0041] 步骤(5):适当地减小电压,采集此时的直流反馈电压;

[0042] 步骤(6):如果直流反馈电压增大,则返回步骤(5),否则进入步骤(7);

[0043] 步骤(7):选择下一个光纤挤压器的控制电压,进入步骤(3)。

[0044] 通过以上过程，可以将直流反馈电压一直保持在最大值状态。此时对应的本振光的强度最强，即实现了偏振反馈控制的功能。

[0045] 与现有技术相比，本发明的主要优点如下：

[0046] 1、安全性方面：由于在本发明中，偏振反馈控制采用分出部分本振光的方法，没有对于信号光进行分光和测量，根据量子密钥分发的分析理论，本发明对密钥的安全性不会造成任何影响。

[0047] 2、连续变量量子密钥分发的量子信号由于达到了量子级别，因此在光纤信道的传输过程中特别容易受到环境干扰，造成偏振漂移，进而造成系统的误码率的增加。本发明中的接收端通过偏振分束器，将本振光和信号光分开；之后对一部分本振光进行检测，以得知偏振漂移的程度；这部分本振光强度越小，说明漂移的程度越严重；这部分本振光强度达到最大时，即为偏振得到补偿的状态。从而能够有效抑制在量子密钥分发过程中的环境干扰，使得偏振持续处于稳定状态，降低了误码率，增强了系统的稳定性。

附图说明

[0048] 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：

[0049] 图 1 为根据本发明提供的连续变量量子密钥分发系统的偏振补偿实现方法的框图。

[0050] 图中：100 为光纤信道，901 为发送端的可调衰减器，902 为发送端的法拉第镜，801 为接收端的可调衰减器，802 为法拉第镜，803 为真有效值转换电路，804 为放大器，805 为光电二极管。

具体实施方式

[0051] 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，还可以做出若干变形和改进。这些都属于本发明的保护范围。

[0052] 在本实施例中，所述连续变量量子密钥分发系统偏振补偿实现方法，具体步骤如下：

[0053] (1) 分光检测阶段：连续变量量子密钥分发系统的接收端将量子信号通过偏振分束器，根据光的偏振理论及偏振耦合器的性质，如果偏振无漂移，则本振光将会和信号光完全分开。在存在偏振漂移的情况下，本振光会泄露一部分到信号光端，使得本振光自身能量降低。通过对分出的一部分本振光进行检测，可以得知偏振的漂移程度。在偏振匹配的情况下，本振光的强度达到最大。此时即为最佳的偏振状态。

[0054] 用于连续变量量子密钥分发系统所使用的本振光强度很小，每个脉冲约有 10^8 个光子，在时钟触发频率为 1MHz 的情况下，功率只有 -48.9dBm。分出的光占本振光能量的 10%，即每个脉冲有约 10^7 光子，在 1MHz 的时钟频率下功率为 -58.9dBm。经过光电二极管转换后，得到的电流非常微弱(约为 1uA)，因此需要放大器对其进行放大。放大器将微弱电流放大到峰值为 500mV 的脉冲电压信号。

[0055] 放大后的脉冲电压信号通过脉冲转换电路转换为直流反馈电压。本发明采用有效值直流转换器 (RMS-DC) 来计算脉冲电压的真有效值，输出直流电压。有效值直流转换器在很宽的输入频率范围内可以进行实时测量，完成脉冲信号到直流信号的转换。

[0056] (2) 偏振校正阶段：脉冲转化电路输出的直流电压反馈给接收方的动态偏振控制器，动态偏振控制器对反馈电压进行采样，并通过下述的偏振反馈控制算法来持续调节动态偏振控制器，使得直流反馈电压保持最大值。

[0057] 动态偏振控制器通过改变其内部的四个光纤挤压器上的电压 V1、V2、V3、V4 对偏振态进行控制，电压调节范围为 -12V 到 +12V 之间。光的偏振态用邦加球上的点来描述，斯托克斯参量 S1、S2、S3 对应着邦加球的坐标轴。如果增加电压 V1 或 V3，则偏振态会绕着 S1 轴顺时针旋转；相反，如果减少 V1 或 V3，则偏振态会绕着 S1 轴逆时针旋转。另一方面，如果增加电压 V2 或 V4，则偏振态会绕着 S2 轴顺时针旋转，如果降低 V2 或 V4，偏振态则会绕着 S2 轴逆时针旋转。由此，只要输入光的偏振态与 S1 和 S2 的方向都不垂直，那么输入光的偏振态都可以通过操作最少 2 个电压改变到任意一个偏振态。

[0058] 由此，一个优选的偏振反馈算法的具体流程如下：

[0059] 步骤 (1)：动态偏振控制器的单片机对直流反馈电压采样并记录数据；

[0060] 步骤 (2)：四个光纤挤压器的控制电压都置为 0V，选择第一个光纤挤压器控制电压；

[0061] 步骤 (3)：适当地增加控制电压，此时偏振态会在邦加球上绕着对应的矢量轴做顺时针转动，采集此时的直流反馈电压，如果电压已经达到了 +12V，则跳至步骤 (7)；

[0062] 步骤 (4)：如果直流反馈电压增大，则返回步骤 3，否则进入步骤 (5)；

[0063] 步骤 (5)：适当地减小控制电压，此时偏振态会在邦加球上绕着对应的矢量轴做逆时针转动，采集此时的直流反馈电压，如果电压已经达到了 -12V，则跳至步骤 (7)；

[0064] 步骤 (6)：如果直流反馈电压增大，则返回步骤 (5)，否则进入步骤 (7)；

[0065] 步骤 (7)：选择下一个光纤挤压器的控制电压，进入步骤 (3)。

[0066] 通过以上过程，可以将直流反馈电压一直保持在最大值状态。根据上面的分析，这时对应的本振光强度最强，即本振光没有发生泄漏，偏振达到最佳状态。

[0067] 安全性方面：由于在本发明中，偏振反馈控制采用分出部分本振光的方法，没有对于信号光进行分光和测量，根据量子密钥分发的分析理论，本发明对密钥的安全性不会造成任何影响。

[0068] 连续变量量子密钥分发的量子信号由于达到了量子级别，因此在光纤信道的传输过程中特别容易受到环境干扰，造成偏振漂移，进而造成系统的误码率的增加。本发明采用上述技术方案，有效抑制了在量子密钥分发过程中的环境干扰，使得偏振持续处于稳定状态，降低了误码率，增强了系统的稳定性。

[0069] 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形或修改，这并不影响本发明的实质内容。

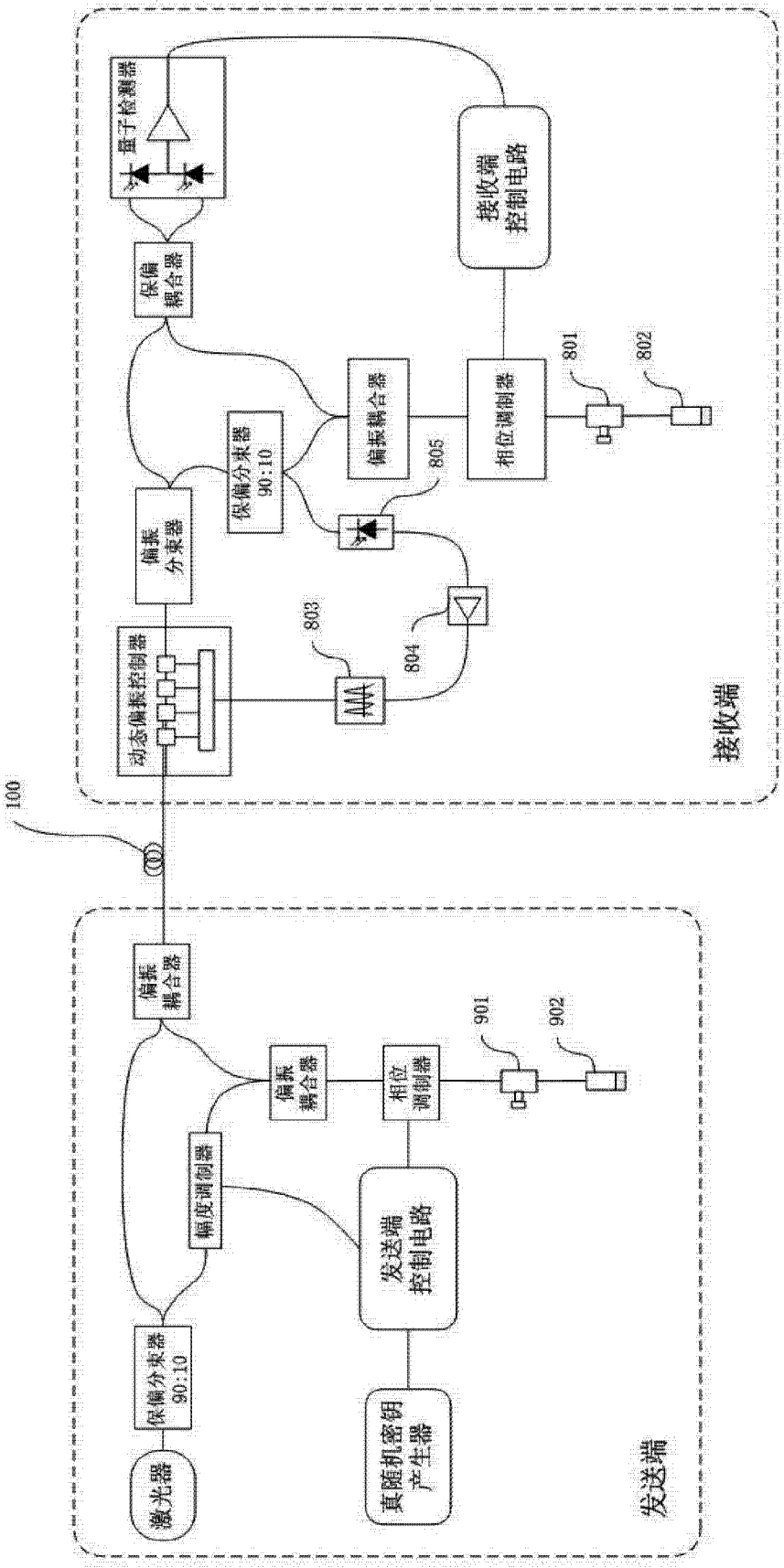

量子检测器
保偏耦合器
接收端控制电路
801
802
偏振耦合器
相位调制器
保偏分束器 90:10
805
偏振分束器
803
804
动态偏振控制器
接收端
100
偏振耦合器
901
902
偏振耦合器
相位调制器
幅度调制器
发送端控制电路
保偏分束器 90:10
激光器
真随机密钥产生器
发送端

图 1