

一种量子密钥分发方法、装置和系统

本申请要求于 2023 年 3 月 31 日提交中国国家知识产权局、申请号为 2023103418969、
申请名称为“一种量子密钥分发方法、装置和系统”的中国专利申请的优先权，其全部内
5 容通过引用结合在本申请中。

技术领域

本发明涉及量子通信领域，尤其涉及一种量子密钥分发方法、装置和系统。

10 背景技术

量子密钥分发 (Quantum Key Distribution, QKD)，是利用量子力学特性来保证通信安全性，从而使通信的双方能够产生并分享一个随机的、安全的密钥，来加密和解密消息的技术，在实用密码学、信息安全、国防等领域、以及各种安全通信环境中有着广泛的应用。

15 量子密钥分发系统的一个主要问题是如何基于光学设备实现更实用、稳定且低成本的量子密钥分发。然而，目前绝大多数的量子密钥分发系统出于安全性考虑，发送的信号光强都控制在单光子水平，加上光纤等信道的衰减，在测量端通常使用的是高灵敏度的单光子探测器，这类探测器往往成本高昂，且由于暗计数、死时间等问题导致探测效率较低，错误率较高。

20 因此，需要一种新的量子密钥分发方案。

发明内容

本发明实施例提供一种量子密钥分发的方法、装置和系统。利用该方法，使得量子密钥分发的接收方可以利用相干探测器进行信号光测量，而无需使用高灵敏度且昂贵的单光子探测器。从而，使得测量设备相较现有技术方案成本更低，且可以有效的避免高灵敏度单光子探测器带来的暗计数、死时间可以降低测量效率的问题。

25 本发明为解决上述技术问题采用的技术方案为，一方面提供一种量子密钥分发方法，所述量子密钥分发的参与方包括第一方和第二方，所述方法包括：

30 第一方制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定；

第二方接收所述相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，其中，所述第二光强大于所述第一光强，所述第二相位根据第二随机值确定；

35 第二方将所述测量结果与预设的第一阈值相对比，所述第一阈值由所述第一方和第二方预先约定；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述

第二方对应的第二密钥位，并向第一方公开所述第二随机值；

第一方根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

优选地，所述方法还包括：

若所述测量结果与所述第一阈值满足不满足预设关系，则放弃确定第一密钥位在所述

5 第二方对应的第二密钥位。

优选地，所述第一光强根据预先设定的多个光强值随机确定。

优选地，所述第一相位可以表示为：

$$\phi_i = \phi_1^a + \pi \kappa_a^i$$

其中， ϕ_i 表示第一相位， ϕ_1^a 表示第一随机值， κ_a^i 表示第一密钥位；

优选地，所述第一随机值可以由第一方从 $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D-1$; D 为正自然数)中随机

10 确认，所述第二随机值可以由第二方从 $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D-1$; D 为正自然数)中随机确认。

优选地，所述第一阈值大于0；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，包括：若所述测量结果大于所述第一阈值，则确定所述第二密钥位为0。

15 优选地，所述第一阈值大于0；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，包括：若所述测量结果小于所述第一阈值的负值，则确定所述第二密钥位为1。

优选地，第一方根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转，包括：

20 若第一随机值和第二随机值之差的绝对值属于预设区间，则将所述第一密钥位进行翻转。

第二方面，提供一种量子密钥分发方法，所述量子密钥分发的参与方包括第一方和第二方，所述方法由第一方执行，所述方法包括：

制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定；

25 获取第二方公开的第二随机值；

根据所述第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

第三方面，提供一种量子密钥分发方法，所述量子密钥分发的参与方包括第一方和第二方，所述方法由第二方执行，所述方法包括：

30 接收第一方发送的相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，其中，所述第二光强大于所述相干光脉冲的第一光强，所述第二相位根据第二随机值确定；将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果；

将所述测量结果与预设的第一阈值相对比，若所述测量结果与所述第一阈值满足预设关系，则确定出第二密钥位并向第一方公开所述第二随机值，其中，所述第一阈值由所述

第一方和第二方预先约定。

第四方面，提供一种量子密钥分发系统，包括作为参与方的第一方和第二方，其中：

第一方，配置为，制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密
5 钥位确定；

第二方，配置为，接收所述相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，其中，所述第二光强大于所述第一光强，所述第二相位根据第二随机值确定；

第二方，还配置为，将所述测量结果与预设的第一阈值相对比，所述第一阈值由所述
10 第一方和第二方预先约定；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值；

第一方，还配置为，根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

第五方面，提供一种量子密钥分发装置，所述量子密钥分发的参与方包括第一方和第
15 二方，所述装置设置于第一方，所述设置包括：

制备单元，配置为，制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定；

获取单元，配置为，获取第二方公开的第二随机值；

20 确定单元，配置为，根据所述第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

第六方面，提供一种量子密钥分发装置，所述量子密钥分发的参与方包括第一方和第二方，所述装置设置于第二方，所述装置包括：

25 测量单元，配置为，接收第一方发送的相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，其中，所述第二光强大于所述相干光脉冲的第一光强，所述第二相位根据第二随机值确定；将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果；

确定单元，配置为，将所述测量结果与预设的第一阈值相对比，若所述测量结果与所述第一阈值满足预设关系，则确定出第二密钥位并向第一方公开所述第二随机值，其中，所述第一阈值由所述第一方和第二方预先约定。

30

附图说明

为了更清楚说明本发明实施例的技术方案，下面将对实施例描述中所需使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

35 图1是量子密钥分发中使用单光子探测器的方案的示意图；

图 2A 为本发明实施例提供的一种量子密钥分发方案的示意图；

图 2B 为本发明实施例一种相干探测模块的结构示意图；

图 3 为本发明实施例提供的一种量子密钥分发方法的流程图；

图 4 为本发明另一实施例提供的一种量子密钥分发方法的流程图；

5 图 5 为本发明又一实施例提供的一种量子密钥分发方法的流程图；

图 6 为本发明实施例提供的一种量子密钥分发系统的结构图；

图 7 为本发明实施例提供的一种量子密钥分发装置的结构图；

图 8 为本发明另一实施例提供的一种量子密钥分发装置的结构图。

10 具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，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做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

15 如前所述，目前绝大多数的量子密钥分发系统出于安全性考虑，发送的信号光强都控制在单光子量级，加上光纤等信道的衰减，测量端所接受到的信号强度往往非常弱，所以测量端通常使用的是高灵敏度的单光子探测器对接收的信号进行测量。图 1 是量子密钥分发中使用单光子探测器的方案的示意图。如图 1 所示，可以由发送端（例如为 Alice 端）通过光源产生单光子量级的光信号，并将密钥信息编码进光信号。然后，通过传输信道（例如为光纤）发送给接收端。接收端（例如为 Bob 端）接收光信号，例如可以对光信号进行光学预处理（例如分束）后，通过单光子探测器进行测量，并根据测量结果确定密钥信息。但是这种方案存在如下问题：一方面，单光子探测器往往十分昂贵，导致密钥分发的成本较高；另一方面，使用单光子探测器还会因为暗计数、死时间等问题导致探测效率较低，且探测错误率较高。所谓暗计数，是指由于单光子探测器的高灵敏度，杂散光（非信号光）和电噪声容易被单光子探测器认为是有效光信号，这种误判被称作暗计数。所谓死时间，是指单光子探测器在探测完一个光子后，通常需要固定时间（例如，20ns）来排空电容电荷，以继续探测下一个光子，这个固定时间被称为死时间（Dead Time）。由于在死时间内无法探测光子，可能导致测量数据的遗漏。

25 针对上述问题，本说明书实施例提供一种新的量子密钥分发方案。图 2A 为本发明实施例提供的一种量子密钥分发方案的示意图。如图 2A 所示，可以由发送端 Alice 端通过相干光源产生相干光信号，并将密钥信息编码进相干光信号。然后，通过传输信道发送给接收端。接收端（例如为 Bob 端）接收相干光信号，并制备对应的本振光脉冲。可以对光信号进行光学预处理后，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，然后根据测量结果确定密钥信息。图 2B 示出相干探测模块的结构示意。如图中所示，输入的信号光与本振光分别进入分束器，在其中干涉后分别进入两个探测器，探测器得到经

30

35

典的测量结果后，将结果输入至后处理模块进行一定运算得到最终测量结果。此处的后处理通常为减法运算。需要强调的是，这里所使用的探测器并不需要为高灵敏度单光子探测器，一般探测器即可。

- 5 以上示出的量子密钥分发方案的优点在于，可以通过基于相干光的信息编码与密钥提取，以及将测量器件由单光子探测器替换为相干探测模块，降低测量结果的错误率。并且，相关探测模块可以使用成本更加低廉的探测器，从而降低量子密钥分发的费用。

下面详细介绍本说明书实施例提供的量子密钥分发方案。图3为本发明实施例提供的一种量子密钥分发方法的流程图。量子密钥分发的参与方包括第一方和第二方，如图3所示，该方法至少包括如下步骤：

- 10 步骤31，第一方制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定；

- 15 步骤32，第二方接收所述相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，其中，所述第二光强大于所述第一光强，所述第二相位根据第二随机值确定；

步骤33，第二方将所述测量结果与预设的第一阈值相对比，所述第一阈值由所述第一方和第二方预先约定；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值；

- 20 步骤34，第一方根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。首先，在步骤31，第一方制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方。

在一个实施例中，第一方例如可以通过量子相干光源产生相干态脉冲，并通过强度和相位调制，得到第一光强和第一相位的相干光脉冲，并将调制后的相干光脉冲通过传输信道传送给第二方。

- 25 在不同的实施例中，第一光强的值可以不同。在一个实施例中，第一光强可以根据预先设定的多个光强值随机确定。在一个具体的实施例中，例如可以从 $0, \nu, \mu$ 三个值中进行随机选择($0 < \nu < \mu$)。

第一相位可以根据第一随机值和第一方的原始密钥中包括的第一密钥位确定。在不同的实施例中，第一相位的确定方式可以不同。在一个实施例中，第一相位可以表示为：

$$\phi_i = \phi_i^a + \pi \kappa_a^i$$

- 30 其中， ϕ_i 表示第一相位， ϕ_i^a 表示第一随机值， $\kappa_a^i \in \{0,1\}$ 表示第一密钥位，其为第一方所持有的、待分发的原始密钥中的一个比特位。

在一个具体的实施例中，第一随机值 ϕ_i^a 可以由第一方从 $\frac{2\pi}{D}k$ ($k = 0,1, \dots, D-1$; D 为正自然数)中随机确定。

在一个实施例中，在步骤31之前，第一方和第二方可以对信道的通信时钟和初始相

位进行校准, 以及进行双方的身份认证。

各参与方可以通过其终端执行本方步骤, 终端并非专指一个参与方例如为一台工作站的终端设备, 其可以是参与方用于进行计算处理的任意计算设备, 包括但不限于服务器、工作站、小型机、移动处理终端等, 也可以是参与方的多个计算设备的协调工作。由于量子密钥分发的过程可以包括量子操作部分和后处理部分, 因此, 在一些实施例中, 参与方的终端也可以包括量子经典混合服务器, 所述量子经典混合服务器中包括量子处理器和经典处理器, 可以由所述量子处理器执行量子操作部分, 由所述经典处理器执行后处理部分。

然后, 在步骤 32, 第二方可以接收所述相干光脉冲, 并制备具有第二光强和第二相位的本振光脉冲, 将相干光脉冲和本振光脉冲输入相干探测模块, 得到测量结果。第二相位根据第二随机值确定。

该步骤中, 第二方例如可以根据第二随机值确定第二相位, 并用本振光光源制备相应相位的第二光强的本振光, 将接收到的信号光、以及制备的本振光输入相干测量模块进行测量, 得到测量结果。

理论上, 第二光强可以远大于第一光强。因此, 在一个实施例中, 第二光强可以大于第一光强。在一个实施例中, 第二光强可以大于第一光强的预设倍数。在不同的具体实施例中, 预设倍数可以是不同的具体倍数。

第二相位可以根据第二随机值确定。在一个实施例中, 第二随机值 ϕ_i^b 可以由第二方从 $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D-1$; D 为正自然数) 中随机确定。

第二方在制备好以上所述的本振光的基础上, 将接收到的相干光脉冲, 以及本方制备的本振光脉冲输入相干探测模块。结合图 2B, 相关光脉冲与本振光脉冲通过分束器干涉后分别进入两个探测器, 两个探测器分别得到经典测量结果后, 由后处理模块对两份经典测量结果进行例如减法运算的运算操作, 将运算结果作为测量结果 n_i 。

接着, 在步骤 33, 第二方将所述测量结果与预设的第一阈值相对比, 所述第一阈值由所述第一方和第二方预先约定; 若所述测量结果与所述第一阈值满足预设关系, 则确定出第一密钥位在所述第二方对应的第二密钥位, 并向第一方公开所述第二随机值。

该步骤中, 测量结果 n_i 与第一阈值 n_{th} 满足预设关系, 可以表示第一密钥位传输的正确性较高, 所以, 可以确定第一密钥位在第二方对应的密钥位 (第二密钥位), 即第二方接收的密钥位。具体的, 在不同的实施例中, 第一阈值 n_{th} 、以及预设关系可以不同。在一个实施例中, 第一阈值 n_{th} 例如可以大于 0。若所述测量结果大于所述第一阈值, 即 $n_i > n_{th}$, 则确定所述第二密钥位为 0。在另一个实施例中, 若所述测量结果小于所述第一阈值的负值, 即 $n_i < -n_{th}$, 则确定所述第二密钥位为 1。

测量结果 n_i 与第一阈值 n_{th} 不满足预设关系, 可以表示第一密钥位传输的正确性较低, 所以, 可以放弃确定第一密钥位在第二方对应的密钥位 (第二密钥位), 即第二方接收的密钥位。因此, 在一个实施例中, 若所述测量结果与所述第一阈值不满足预设关系, 则放弃确定第一密钥位在所述第二方对应的第二密钥位。

在第二方确定出第二密钥位后，可以向第一方公开第二随机值。由于第一方的原始密钥中可以包括多个密钥位，因此在实施例1中，步骤31~33可以（针对多个密钥位）执行多个轮次。因此，在一个实施例中，可以在执行所述多个轮次后，由第二方向第一方公开各个未放弃确认本方对应密钥位的轮次，以及这些轮次对应的第二随机值。

5 此后，在步骤34，第一方根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

在实际场景中，如果第一方和第二方分别选取的第一随机值和第二随机值之间的差别处于特定区间，则在第二方确定的第二密钥位常常不是第一密钥位的原值，而是其翻转值（例如，0变为了1，0变为了1）。所以，在第一方获取第二方公开的第二随机值后，可以比较两者的差别是否处于上述特定区域。并根据比较结果，确定是否对本方原有的第一密钥位也进行翻转，从而和第二方确定的第二密钥位保持一致。在一个实施例中，若第一随机值和第二随机值之差的绝对值属于预设区间，则将所述第一密钥位进行翻转操作（将0变为1，将0变为1）。在不同的实施例中，预设区间可以不同。在一个具体的实施例中，预设区间可以为 $[\frac{1}{2}\pi, \frac{3}{2}\pi)$ 。即若 $|\phi_1^a - \phi_1^b| \in [\frac{1}{2}\pi, \frac{3}{2}\pi)$ ，则将第一密钥位进行翻转操作，否则不对第一密钥位进行翻转操作。

10 15

如前所述，步骤31~33可以（针对多个密钥位）执行多个轮次。因此，在一个实施例中，第一方可以根据多个轮次中各个第二方未放弃确认本方对应密钥位的轮次，以及这些轮次对应的第二随机值，确定是否翻转这些轮次中本方的第一密钥位。进而，第一方和第二方，可以根据各个未放弃轮次各方分别确定的密钥位，确定各方保留的密钥。

20 为了提高双方保留的密钥的准确度，以及加强密钥分发的安全性，在一个实施例中，第一方和第二方还可以根据双方的密钥，进行进一步的信息协商（Information Reconciliation）和/或隐私放大（Privacy Amplification）。信息协商，主要用于保证各个用户所持有的密钥是相同的，即密钥的一致性。隐私放大，主要用于使得潜在的窃听者无法获得密钥信息，即保证密钥的安全性。在不同的具体实施例中，第一方和第二方进行信息协商和/或隐私放大的具体方式可以不同，本说明书对此不做限制。

25

综上所述，本发明实施例提供的一种量子密钥分发方法，可以通过基于相干光的信息编码、光信号传输和密钥提取，将测量器件由单光子探测器替换为相干探测模块。一方面，显著降低光信号测量的错误率，提高测量效率。另一方面，相对于常规方案中使用昂贵的单光子探测器进行光信号测量，本方法可以使用成本低廉的普通光探测器进行光信号测量，也显著降低了量子密钥分发的成本。

30

图4为本发明另一实施例提供的一种量子密钥分发方法的流程图。量子密钥分发的参与方包括第一方和第二方，该方法由第一方执行。如图4所示，该方法至少包括如下步骤：

步骤41，制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定；

35

步骤 42, 获取第二方公开的第二随机值; 该第二随机值是在第二方确定测量结果与第一阈值满足预设关系的情况下公开的, 所述测量结果是第二方将其制备的具有第二光强和第二相位的本振光脉冲, 以及所述相干光脉冲输入相干探测模块得到的, 其中所述第二光强大于所述第一光强, 所述第二相位根据所述第二随机值确定; 所述第一

5 阈值由所述第一方和第二方预先约定;

步骤 43, 根据所述第一随机值和第二随机值, 确定是否对所述第一密钥位进行翻转。

图 5 为本发明又一实施例提供的一种量子密钥分发方法的流程图。量子密钥分发的参与方包括第一方和第二方, 该方法由第一方执行。如图 5 所示, 该方法至少包括如下步骤:

步骤 51, 接收第一方发送的具有第一光强和第一相位的相干光脉冲, 其中所述第一

10 相位根据第一方持有的第一随机值和第一方的原始密钥中包括的第一密钥位确定; 制备具有第二光强和第二相位的本振光脉冲, 其中, 所述第二光强大于所述相干光脉冲的第一光强, 所述第二相位根据第二随机值确定; 将相干光脉冲和本振光脉冲输入相干探测模块, 得到测量结果;

步骤 52, 将所述测量结果与第一方和第二方预先约定的第一阈值相对比, 若所述测

15 量结果与所述第一阈值满足预设关系, 则确定出所述第一密钥位在所述第二方对应的第二密钥位, 并向第一方公开所述第二随机值, 使其根据第一随机值和第二随机值, 确定是否对所述第一密钥位进行翻转。

根据又一方面的实施例, 还提供了一种量子密钥分发系统。图 6 为本发明实施例提供一种量子密钥分发系统的结构图。如图 6 所示, 该系统包括作为参与方的第一方 61 和

20 第二方 62, 其中:

第一方 61, 配置为, 制备具有第一光强和第一相位的相干光脉冲, 并将所述相干光脉冲发送到第二方, 其中, 所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定;

第二方 62, 配置为, 接收所述相干光脉冲, 并制备具有第二光强和第二相位的本振光

25 脉冲, 将相干光脉冲和本振光脉冲输入相干探测模块, 得到测量结果, 其中, 所述第二光强大于所述第一光强, 所述第二相位根据第二随机值确定;

第二方 62, 还配置为, 将所述测量结果与预设的第一阈值相对比, 所述第一阈值由所述

30 第一方和第二方预先约定; 若所述测量结果与所述第一阈值满足预设关系, 则确定出第一密钥位在所述第二方对应的第二密钥位, 并向第一方公开所述第二随机值;

第一方 61, 还配置为, 根据第一随机值和第二随机值, 确定是否对所述第一密钥位进行

35 翻转。

根据又一方面的实施例, 还提供了一种量子密钥分发系统。图 7 为本发明实施例提供一种量子密钥分发系统的结构图。如图 6 所示, 该系统 600 包括作为参与方的第一方 610

和 620, 其中:

35 第一方 610, 配置为, 制备具有第一光强和第一相位的相干光脉冲, 并将所述相干光

脉冲发送到第二方，其中，所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定；

5 第二方 620，配置为，接收所述相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，其中，所述第二光强大于所述第一光强，所述第二相位根据第二随机值确定；

第二方 620，还配置为，将所述测量结果与预设的第一阈值相对比，所述第一阈值由所述第一方和第二方预先约定；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值；

10 第一方 610，还配置为，根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

在一个实施例中，第一方 610 可以包括量子密钥分发装置。如图 7 所示，该装置包括：

制备单元 611，配置为，制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定；

15 获取单元 612，配置为，获取第二方在确定测量结果与第一阈值满足预设关系的情况下公开的第二随机值，所述测量结果是第二方将其制备的具有第二光强和第二相位的本振光脉冲，以及所述相干光脉冲输入相干探测模块得到的，其中所述第二光强大于所述第一光强，所述第二相位根据所述第二随机值确定；所述第一阈值由所述第一方和第二方预先约定；

20 确定单元 613，配置为，根据所述第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

在一个实施例中，第二方 620 可以包括量子密钥分发装置。如图 8 所示，该装置包括：

25 测量单元 621，配置为，接收第一方发送的具有第一光强和第一相位的相干光脉冲，其中所述第一相位根据第一方持有的第一随机值和第一方的原始密钥中包括的第一密钥位确定；制备具有第二光强和第二相位的本振光脉冲，其中，所述第二光强大于所述相干光脉冲的第一光强，所述第二相位根据第二随机值确定；将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果；

30 确定单元 622，配置为，将所述测量结果与第一方和第二方预先约定的第一阈值相对比，若所述测量结果与所述第一阈值满足预设关系，则确定出所述第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值，使其根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

根据又一方面的实施例，还提供一种计算机可读介质，包括存储于其上的计算机程序，所述计算机在运行时执行上述的方法。

35 根据又一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述的方法。

上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

5 专业人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专
10 业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、
15 或技术领域内所公知的任意其它形式的存储介质中。

以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种量子密钥分发方法,所述量子密钥分发的参与方包括第一方和第二方,所述方法包括:

第一方制备具有第一光强和第一相位的相干光脉冲,并将所述相干光脉冲发送到第二方,其中,所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定;

第二方接收所述相干光脉冲,并制备具有第二光强和第二相位的本振光脉冲,将相干光脉冲和本振光脉冲输入相干探测模块,得到测量结果,其中,所述第二光强大于所述第一光强,所述第二相位根据第二随机值确定;

第二方将所述测量结果与预设的第一阈值相对比,所述第一阈值由所述第一方和第二方预先约定;若所述测量结果与所述第一阈值满足预设关系,则确定出第一密钥位在所述第二方对应的第二密钥位,并向第一方公开所述第二随机值;

第一方根据第一随机值和第二随机值,确定是否对所述第一密钥位进行翻转。

2、根据权利要求1的方法,还包括:

若所述测量结果与所述第一阈值满足不满足预设关系,则放弃确定第一密钥位在所述第二方对应的第二密钥位。

3、根据权利要求1的方法,其中,所述第一光强根据预先设定的多个光强值随机确定。

4、根据权利要求1的方法,其中,所述第一相位表示为:

$$\phi_i = \phi_i^a + \pi \kappa_a^i$$

其中, ϕ_i 表示第一相位, ϕ_i^a 表示第一随机值, κ_a^i 表示第一密钥位。

5、根据权利要求1的方法,其中,所述第一随机值由第一方从 $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D-1$; D 为正自然数) 中随机确定,所述第二随机值由第二方从 $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D-1$; D 为正自然数) 中随机确定。

6、根据权利要求1的方法,其中,所述第一阈值大于0;

若所述测量结果与所述第一阈值满足预设关系,则确定出第一密钥位在所述第二方对应的第二密钥位,包括:

若所述测量结果大于所述第一阈值,则确定所述第二密钥位为0。

7、根据权利要求1的方法,其中,所述第一阈值大于0;

若所述测量结果与所述第一阈值满足预设关系,则确定出第一密钥位在所述第二方对应的第二密钥位,包括:

若所述测量结果小于所述第一阈值的负值,则确定所述第二密钥位为1。

8、根据权利要求1的方法,其中,第一方根据第一随机值和第二随机值,确定是否对所述第一密钥位进行翻转,包括:

若第一随机值和第二随机值之差的绝对值属于预设区间，则将所述第一密钥位进行翻转。

9、一种量子密钥分发方法，所述量子密钥分发的参与方包括第一方和第二方，所述方法由第一方执行，所述方法包括：

制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定；

获取第二方在确定测量结果与第一阈值满足预设关系的情况下公开的第二随机值，所述测量结果是第二方将其制备的具有第二光强和第二相位的本振光脉冲，以及所述相干光脉冲输入相干探测模块得到的，其中所述第二光强大于所述第一光强，所述第二相位根据所述第二随机值确定；所述第一阈值由所述第一方和第二方预先约定；

根据所述第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

10、一种量子密钥分发方法，所述量子密钥分发的参与方包括第一方和第二方，所述方法由第二方执行，所述方法包括：

接收第一方发送的具有第一光强和第一相位的相干光脉冲，其中所述第一相位根据第一方持有的第一随机值和第一方的原始密钥中包括的第一密钥位确定；

制备具有第二光强和第二相位的本振光脉冲，其中，所述第二光强大于所述相干光脉冲的第一光强，所述第二相位根据第二随机值确定；将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果；

将所述测量结果与第一方和第二方预先约定的第一阈值相对比，若所述测量结果与所述第一阈值满足预设关系，则确定出所述第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值，使其根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

11、一种量子密钥分发系统，包括作为参与方的第一方和第二方，其中：

第一方，配置为，制备具有第一光强和第一相位的相干光脉冲，并将所述相干光脉冲发送到第二方，其中，所述第一相位根据第一随机值和第一方的原始密钥中包括的第一密钥位确定；

第二方，配置为，接收所述相干光脉冲，并制备具有第二光强和第二相位的本振光脉冲，将相干光脉冲和本振光脉冲输入相干探测模块，得到测量结果，其中，所述第二光强大于所述第一光强，所述第二相位根据第二随机值确定；

第二方，还配置为，将所述测量结果与预设的第一阈值相对比，所述第一阈值由所述第一方和第二方预先约定；若所述测量结果与所述第一阈值满足预设关系，则确定出第一密钥位在所述第二方对应的第二密钥位，并向第一方公开所述第二随机值；

第一方，还配置为，根据第一随机值和第二随机值，确定是否对所述第一密钥位进行翻转。

12、一种量子密钥分发装置,所述量子密钥分发的参与方包括第一方和第二方,所述装置设置于第一方,所述装置包括:

制备单元,配置为,制备具有第一光强和第一相位的相干光脉冲,并将所述相干光脉冲发送到第二方,其中,所述第一相位根据第一随机值和所述第一方的原始密钥中包括的第一密钥位确定;

获取单元,配置为,获取第二方在确定测量结果与第一阈值满足预设关系的情况下公开的第二随机值,所述测量结果是第二方将其制备的具有第二光强和第二相位的本振光脉冲,以及所述相干光脉冲输入相干探测模块得到的,其中所述第二光强大于所述第一光强,所述第二相位根据所述第二随机值确定;所述第一阈值由所述第一方和第二方预先约定;

确定单元,配置为,根据所述第一随机值和第二随机值,确定是否对所述第一密钥位进行翻转。

13、一种量子密钥分发装置,所述量子密钥分发的参与方包括第一方和第二方,所述装置设置于第二方,所述装置包括:

测量单元,配置为,接收第一方发送的具有第一光强和第一相位的相干光脉冲,其中所述第一相位根据第一方持有的第一随机值和第一方的原始密钥中包括的第一密钥位确定;制备具有第二光强和第二相位的本振光脉冲,其中,所述第二光强大于所述相干光脉冲的第一光强,所述第二相位根据第二随机值确定;将相干光脉冲和本振光脉冲输入相干探测模块,得到测量结果;

确定单元,配置为,将所述测量结果与第一方和第二方预先约定的第一阈值相对比,若所述测量结果与所述第一阈值满足预设关系,则确定出所述第一密钥位在所述第二方对应的第二密钥位,并向第一方公开所述第二随机值,使其根据第一随机值和第二随机值,确定是否对所述第一密钥位进行翻转。