(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101040483 B
(45)授权公告日 2011.10.05

(21)申请号 200580029585.9
(22)申请日 2005.09.01
(30)优先权数据
60/606,793 2004.09.02 US
(85)PCT申请进入国家阶段日
2007.03.02
(86)PCT申请的申请数据
PCT/IB2005/002622 2005.09.01
(87)PCT申请的公布数据
WO2006/024939 EN 2006.03.09
(73)专利权人 ID量子技术股份有限公司
地址 瑞士卡鲁日
(72)发明人 尼古拉斯·基辛 格雷戈瑞·瑞博迪 雨果·兹宾登
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 郭思宇
(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
CN 1384621 A,2002.12.11, 全文.
CN 1447558 A,2003.10.08, 全文.
WO 2004/047359 A1,2004.06.03, 全文.

审查员 胡锐先

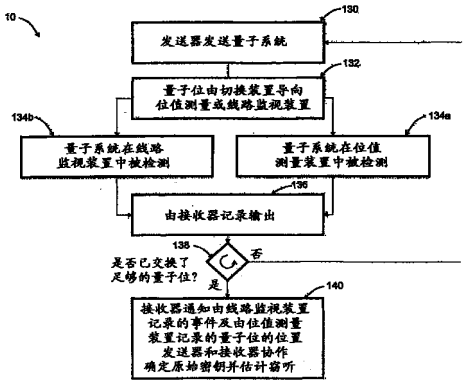
权利要求书 7 页 说明书 10 页 附图 7 页

(54)发明名称

带有用于窃听器检测的量子位内和之间干涉的两非正交状态量子密码学方法及设备

(57)摘要

使用两个非正交状态实现安全量子密码系统的设备和方法。对于每一量子位,发送器站在两个非正交量子状态之一制备一个量子系统,以时间基编码位值。然后使用量子位内部和之间的干涉揭示窃听企图。使用证据状态帮助揭示穿越量子系统分离进行的攻击。



CN 101040483 B

1. 一种用于在由量子信道和传统信道连接的发送器站与接收器站之间分配符号序列的设备，其中该设备评估对这两种信道访问的窃听者可能已获得的关于该序列的信息量，该设备包括：

-a) 一个发送器站，具有控制装置使得发送器站能够命令并控制其自身的与接收器站相关的组件协作的组件，以及一个量子源，用来产生量子系统流，量子系统在位于流附近位置的系统之间具有相干的相位关系，

o 其中一些量子系统在属于第一组量子状态的量子状态中制备，这组包括至少两个非正交量子状态，且这第一组的量子状态与符号值相关联，

o 其中发送器站适于在属于第二组量子状态的一量子状态中产生某些量子系统，这第二组包括至少一个状态，这第二组的状态与第一组的一些状态非正交，这第二组的状态与第一组的一些状态不重叠，选择第二组的状态，使得它们被一测量扰动，该测量当施加于在属于第一组的量子状态中制备的量子系统时，适于至少在一些情形下确定这一量子系统是在什么状态中制备的；

-b) 一个量子信道，适于从发送器站向接收器站传送量子系统；以及

-c) 一个接收器站，通过一量子信道和传统信道连接到发送器站，接收器站具有：

o 控制装置，用来控制接收器站的操作，并与发送器站协调操作和通信，以使接收器站能够命令并控制其自身的与发送器站相关组件协作的组件；

o 一个切换装置，适于用来把量子系统指向至少两个测量子系统之一；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于用来对一些量子系统进行第一测量，这第一测量允许在某些情形下确 定量子系统是在什么量子状态由发送器站制备的；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于对至少两个量子系统的组进行第二测量，这第二测量能够获得关于由接收器站接收的两个量子系统之间现有相位关系的相干程度的信息；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于对量子系统进行第三测量，这第三测量当施加到在属于第二组的一状态中制备的量子系统时，至少在一些情形下允许确定它们是否在发送器与接收器站之间受到测量，该测量当施加到在属于第一组的状态中制备的量子系统时，适于至少在一些情形下确定这一量子系统是在什么状态被制备的；以及

o 通信装置，能够与发送器站进行数据通信，适于通知发送器站

• 至少一些量子系统的流中的位置，在其上这第一测量产生确定的结果，从而允许确定特定的量子系统在第一组的什么量子状态被制备，以及由发送器站已发送什么符号，以及

• 第二测量和第三测量的至少某些测量结果，通信装置还允许发送器站和接收器站协作以估计在量子信道上的窃听强度。

2. 如权利要求 1 的设备，其中测量子系统至多包括两个集成的测量子系统，它们适于进行第一，第二和第三测量中的一个或多个。

3. 如权利要求 1 的设备，其中发送器站的量子系统源适于：

产生电磁场的至少两个弱相干状态的组，每一个弱相干状态在持续时间 t 的时间箱中，每一弱相干状态的中心与其最近的邻居的中心分开时间 T1，T1 大于 t，一个这样的组的

最后的弱相干状态的中心与下一个组的第一弱相干状态的中心分开时间 T2，T2 大于 t，其中一组中任何两个弱相干状态是相位相干的，且一组中的弱相干状态与另一邻近组的至少一些弱相干状态是相位相干的；

对被传送的序列的每一符号产生一个量子系统，该量子系统包括在时间箱之一中有非零振幅的一个这种弱相干状态，以及在其它时间箱中有零振幅的弱相干状态；

在与符号相关联的一些量子系统之间，插入带有在至少两个时间 箱中有非零振幅的至少两个弱相干状态的量子系统；以及

通过适当的量子信道向接收器站发送量子系统。

4. 如权利要求 3 的设备，其中发送器站的量子系统源包括一个模式锁定的激光器，它由适当的光学通路连接到一振幅调制器。

5. 如权利要求 3 的设备，其中发送器站的量子系统源包括一个连续波激光器，它由适当的光学通路连接到一振幅调制器。

6. 如权利要求 3 的设备，其中源包括一个可变光学衰减器。

7. 如权利要求 3 的设备，其中接收器站的切换装置包括一个带有选择的反射 / 传送比的光纤耦合器。

8. 如权利要求 3 的设备，其中接收器站的切换装置包括一个带有选择的反射 / 传送比的光束分割器。

9. 如权利要求 3 的设备，其中接收器站的切换装置包括一个光学开关。

10. 如权利要求 3 的设备，其中接收器站的切换装置是从包括有源和无源装置的装置组选择的。

11. 如权利要求 3 的设备，其中接收器站包括一个第一检测器单元，该第一检测器单元由一适当的光学通路连接到切换装置，并电连接到接收器站中的控制装置，这一第一检测器单元允许以小于 T1 并小于 T2 的分辨率确定光子到达的时间，并从而适于至少在一些情形下确定量子系统由发送器站在什么量子状态被制备的。

12. 如权利要求 11 的设备，其中第一检测器单元包括一个工作在盖革模式的雪崩光电二极管。

13. 如权利要求 11 的设备，其中第一检测器单元包括一个光学频率上转换装置，该光学频率上转换装置由一适当的光学通路连接到一第二检测器单元。

14. 如权利要求 3 的设备，其中接收器站包括一个光学装置，该光学装置由适当的光学通路连接到切换装置，并适于光学重叠不同时间箱的至少两个弱相干状态，使得它们如果是相位相干的则破坏性地干扰，并把重叠的状态引向至少一个第一检测器单元，该至少一个第 一检测器单元能够以小于 T1 并小于 T2 的分辨率确定光子到达的时间。

15. 如权利要求 14 的设备，其中光学装置包括一个干涉仪。

16. 如权利要求 15 的设备，其中干涉仪是 Mach-Zehnder 干涉仪。

17. 如权利要求 15 的设备，其中干涉仪是带有至少一个法拉第镜的自动补偿干涉仪。

18. 如权利要求 14 的设备，其中一个第一检测器单元或多个第一检测器单元包括工作在盖革模式的雪崩光电二极管。

19. 如权利要求 14 的设备，其中一个第一检测器单元或多个第一检测器单元包括一个光学频率上转换装置，它由一适当的光学通路连接到一第二检测器单元。

20. 一种接收器站，用于与一发送器站共同操作，当发送器站和接收器站由一量子信道和传统信道相互连接时，用来在发送器站和接收器站之间分配符号序列，并评估已访问这两种信道的窃听者可能已获得的关于该序列的信息量，接收器站包括：

o 控制装置，用来控制接收器站的操作，并与发送器站协调操作和通信，以使接收器站能够命令并控制其自身的与发送器站相关组件协作的组件，发送器站有一个量子源，用来产生量子系统流，量子系统在位于流附近位置的系统之间具有相干的相位关系，并在携带符号序列时，在第一组量子状态中所选择的一状态被制备，这第一组包括至少两个非正交状态；

o 一个切换装置，适于用来把量子系统指向至少两个测量子系统之一；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于用来对一些量子系统进行第一测量，这第一测量允许在一些情形下确定量子系统是在什么量子状态由发送器站制备的；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于对至少两个量子系统的组进行第二测量，这第二测量能够获得关于由接收器站接收的两个量子系统之间现有相位关系的相干程度的信息；

o 一个测量子系统，由适当的光学通路连接到切换装置，并适于对量子系统进行第三测量，这第三测量允许，当施加到在属于第二组量子状态的一状态制备的量子系统时，这第二组包括至少一个状态，这第二组状态对第一组的某些状态是非正交的，这第二组的状态不是第一组某些状态的重叠，这第二组状态的选择方式使得它们被一种测量扰动，该测量在施加到在属于第一组的状态中制备的量子系统时，适于至少在一些情形下确定这一量子系统是在什么状态中制备的；至少在一些情形下确定，在发送器和接收器站之间它们是否被测量，该测量在施加到在属于第一组的状态中制备的量子系统时，适于确定至少在一些情形下这一量子系统是在什么状态中制备的；以及

o 通信装置，能够与发送器站进行数据通信，适于通知发送器站

• 至少一些量子系统的流中的位置，在其上这第一测量产生确定的结果，从而允许确定特定的量子系统在第一组的什么量子状态被制备，以及由发送器站已发送什么符号，

• 第二测量和第三测量的至少一些测量结果，通信装置还允许发送器站和接收器站协作以估计在量子信道上的窃听强度。

21. 如权利要求 20 的接收器站，其中接收器站的切换装置包括一个带有被选择的反射 / 传送比的光纤耦合器。

22. 如权利要求 20 的接收器站，其中接收器站的切换装置包括一个带有被选择的反射 / 传送比的光束分割器。

23. 如权利要求 20 的接收器站，其中接收器站的切换装置包括一个光学开关。

24. 如权利要求 20 的接收器站，其中接收器站的切换装置是从包括有源和无源装置的装置组选择的。

25. 如权利要求 20 的接收器站，其中，

发送器站的量子系统源适于：产生电磁场的至少两个弱相干状态的组，每一弱相干状态在持续时间 t 的时间箱中，每一弱相干状态的中心与其最近的邻居的中心分开时间 T1，T1 大于 t，一个这样的组的最后的弱相干状态的中心与下一个组的第一弱相干状态的中心

分开时 间 T2，T2 大于 t，其中一组中任何两个弱相干状态是相位相干的，且一组中的弱相干状态与另一邻近组的至少一些弱相干状态是相位相干的，

接收器站包括一个第一检测器单元，该第一检测器单元由一适当的光学通路连接到切换装置，并电连接到控制装置，这一第一检测器单元允许以小于 T1 并小于 T2 的分辨率确定光子到达的时间，并从而适于至少在一些情形下确定量子系统由发送器站在什么量子状态制备。

26. 如权利要求 25 的接收器站，其中第一检测器单元包括一个工作在盖革模式的雪崩光电二极管。

27. 如权利要求 25 的接收器站，其中第一检测器单元包括一个光学频率上转换装置，由一适当的光学通路连接到一第二检测器单元。

28. 如权利要求 20 的接收器站，其中，

发送器站的量子系统源适于：产生电磁场的至少两个弱相干状态的组，每个弱相干状态在持续时间 t 的时间箱中，每一弱相干状态的中心与其最近的邻居的中心分开时间 T1，T1 大于 t，一个这样的组的最后的弱相干状态的中心与下一个组的第一弱相干状态的中心分开时间 T2，T2 大于 t，其中一组中任何两个弱相干状态是相位相干的，且一组中的弱相干状态与另一邻近组的至少一些弱相干状态是相位相干的，

接收器站包括一个光学装置，该光学装置由适当的光学通路连接到切换装置，并适于光学重叠不同时间箱的至少两个弱相干状态，使得它们如果是相位相干的则破坏性地干扰，并把重叠的状态引向接收器站中的至少一个第一检测器单元，该至少一个第一检测器单元允许以小于 T1 并小于 T2 的分辨率确定光子到达的时间。

29. 如权利要求 28 的接收器站，其中光学装置包括一个干涉仪。

30. 如权利要求 29 的接收器站，其中干涉仪是 Mach-Zehnder 干涉仪。

31. 如权利要求 29 的接收器站，其中干涉仪是带有至少一个法拉 第镜的自动补偿干涉仪。

32. 如权利要求 25 或 28 的接收器站，其中一个第一检测器单元或多个第一检测器单元包括工作在盖革模式的雪崩光电二极管。

33. 如权利要求 25 或 28 的接收器站，其中一个第一检测器单元或多个第一检测器单元包括一个光学频率上转换装置，由一适当的光学通路连接到一第二检测器单元。

34. 一种发送器站，用于与权利要求 20 的接收器站协作，以便当由量子信道和传统信道连接时在该发送器站和接收器站之间分配符号序列，并评估已访问这两种信道的窃听者可能已获得的关于序列的信息量，该发送器站包括：

-a) 控制装置，以便使发送器站能够命令并控制其自身的与接收器站相关组件协作的组件；以及

-b) 一个量子源，用来产生量子系统流，量子系统在位于流附近位置的系统之间具有相干的相位关系，

o 其中某些量子系统在属于第一组量子状态的一个量子状态被制备，这第一组包括至少两个非正交量子状态，且这第一组的量子状态与符号值相关，

o 其中发送器站适于在属于第二组量子状态的一个量子状态中产生一些量子系统，这第二组量子状态包括至少一个状态，这第二组的状态对第一组的一些状态为非正交，这第

二组的状态不是第一组某些状态的重叠，第二组的状态的选择方式使得它们被一种测量干扰，该测量在施加到在属于第一组的状态被制备的量子系统时，适于至少在一些情形下确定这一量子系统是在什么状态制备的。

35. 如权利要求 34 的发送器站，其中发送器站的量子系统源适于用来：

产生电磁场的至少两个弱相干状态的组，每一弱相干状态在持续时间 t 的时间箱中，每一弱相干状态的中心与其最近的邻居的中心分开时间 T1，T1 大于 t，一个这样的组的最后的弱相干状态的中心与下一个组的第一弱相干状态的中心分开时间 T2，T2 大于 t，其中一组中 的任何两个弱相干状态是相位相干的，且一组中的弱相干状态与另一邻近组的至少某些弱相干状态是相位相干的；

对被传送的序列的每一符号产生一个量子系统，其包括在时间箱之一中有非零振幅的一个这种弱相干状态，以及在其它时间箱中有零振幅的弱相干状态；

在与符号相关联的某些量子系统之间，插入带有在至少两个时间箱中有非零振幅的至少两个弱相干状态的量子系统；以及

通过适当的量子信道向接收器站发送量子系统。

36. 如权利要求 34 的发送器站，其中发送器站的量子系统源包括一个模式锁定的激光器，它由适当的光学通路连接到一振幅调制器。

37. 如权利要求 34 的发送器站，其中发送器站的量子系统源包括一个连续波激光器，它由适当的光学通路连接到一振幅调制器。

38. 如权利要求 34 的发送器站，其中量子源包括一个可变光学衰减器。

39. 一种用于分配符号序列及估计窃听者可能知道的关于从符号序列产生的密钥的信息的方法，该方法包括以下步骤：

-a) 通过发送器站发送由量子系统源产生的量子系统流，该量子系统在位于流附近位置的系统之间具有相干相位关系，且其中量子系统在属于第一组量子状态的量子状态被制备，这第一组包括至少两个非正交量子状态，且这第一组量子状态与符号值相关联，

-b) 在与符号相关联的一些量子系统之间插入属于第二组量子状态的量子系统，这第二组量子状态包括至少一个状态，这第二组的状态与第一组的某些状态是非正交的，这第二组的状态不是第一组某些状态的重叠，这第二组的状态是以这样的方式选择的，使得它们被一测量干扰，该测量当施加到在属于第一组的状态中制备的量子系统时，至少在一些情形下适于确定这一量子系统是在什么状态制备的，

-c) 通过接收器站对一些量子系统进行第一测量，以试图确定它们由发送器站在什么量子状态制备的，

-d) 由接收器站对至少两个量子系统的组进行第二测量，这第二 测量能够获得关于由接收器站收到的两个量子系统之间现有的相位关系的相干程度的信息；

-e) 由接收器站对量子系统进行第三测量，这第三测量当施加到属于第二组量子状态的状态中制备的量子系统时，允许至少在一些情形下确定它们是否在发送器站与接收器站之间已被测量，该测量在施加到属于第一组的状态中制备的量子系统时，适于至少在一些情形下确定这一量子系统是在什么状态制备的；以及

-f) 通知发送器站在至少一些量子系统的流中第一测量在其上产生确定结果的位置，从而允许确定一特定量子系统是在第一组的什么量子状态被制备的，并确定由发送器站发

送了什么符号，以及第二测量和第三测量的至少一些测量结果，以及

-g) 通过发送器站和接收器站协作以评估对量子信道窃听的强度。

40. 一种用于分配符号序列并估计窃听者可能知道的关于从符号序列产生的密钥的信息的方法，该方法工作在权利要求 1 的设备上，其中发送器站的量子系统源，对于通过量子信道要传送到接收器站的序列的每一符号，产生一量子系统，该量子系统在从至少两个状态的第一组选择的一个量子状态中被制备，所述状态由一组电磁场的至少两个弱相干状态组成，每一弱相干状态位于持续时间 t 的时间箱中，组中这种弱相干状态的中心以时间 T1 与其最近的邻居的中心分开，T1 大于 t，一个这种组的最后的弱相干状态的中心与由源发射的下一个弱相干状态的中心分开时间 T2，T2 大于 t，该组的一个弱相干状态具有非零振幅，而其它组具有零振幅，且其中一组的任何两个弱相干状态是相位相干的，且一个组的弱相干状态与另一邻接组的任何弱相干状态相位相干。

41. 如权利要求 40 的方法，其中发送器站向接收器站通过适当的量子信道发送量子系统。

42. 如权利要求 41 的方法，其中接收器站把某些接收的量子系统导向检测器单元，该检测器单元允许以小于 T1 并小于 T2 的分辨率确 定光子到达的时间，从而在某些情形下允许确定量子系统是在什么量子状态由发送器站制备的。

43. 如权利要求 42 的方法，其中接收器站通知发送器站以上测量在其上产生确定结果的至少一些量子系统在流中的位置，从而指示发送器站什么符号可能对原始密钥有贡献。

44. 如权利要求 43 的方法，其中接收器站把接收的某些量子系统导向一光学装置，该装置通过重叠来自不同量子系统的至少两个弱相干状态测量量子系统，使得它们如果是相位相干的则破坏性地干扰，并向接收器站中的至少一个检测器单元发送重叠的状态，该至少一个检测器单元允许以小于 T1 并小于 T2 的分辨率确定光子到达的时间。

45. 如权利要求 44 的方法，其中接收器站通知以上测量的至少一些测量结果，从而允许发送器站和接收器站协作以估计窃听者知道的关于原始密钥的信息量。

46. 如权利要求 45 的方法，其中发送器站在第一组中的一个状态中制备的一些量子系统之间插入一个量子系统，该量子系统包括至少两个弱相干状态，该至少两个弱相干状态在至少两个时间箱中有非零振幅。

47. 如权利要求 46 的方法，其中接收器站把一些接收的量子系统导向一光学装置，该光学装置通过以如下方式重叠来自单个量子系统的至少两个弱相干状态来测量量子系统，该方式为如果它们是相位相干则破坏性干扰，并向接收器站中的至少一个检测器单元发送该重叠状态，该至少一个检测器单元允许以小于 T1 并小于 T2 的分辨率确定光子到达的时间。

48. 如权利要求 47 的方法，其中接收器站通知以上测量的至少一些结果，从而允许发送器站和接收器站协作以估计窃听者知道的关于原始密钥的信息量。

49. 一种使用符号值的时间编码及电磁场在时间箱中的脉动弱相干状态来产生符号流的设备，该设备包括 ：

a. 一个发送器站，具有一量子系统源，适于在非正交状态制备量 子系统，其特征是在邻近的量子系统之间有相干的相位关系，并在其中插入证据状态，该证据状态帮助揭示跨越量子系统分离进行的攻击，以及

b. 一个接收器站，具有通过适当的光学信道与其连接的检验装置，该检验装置适于检验一些量子系统对存在相干的相位关系，并适于检测证据状态，以帮助揭示跨越量子系统分离进行的攻击。

50. 一种使用符号值的时间编码及电磁场在时间箱中的脉动弱相干状态产生符号流的方法，该方法包括以下步骤：

a. 在一个发送器站中，在具有与邻近的量子系统有相干的相位关系的非正交状态中制备量子系统，并在其中插入证据状态，该证据状态帮助揭示跨越量子系统分离进行的攻击，

b. 使用量子信道，把这些量子系统传送到接收器站，接收器站具有通过适当的光学信道与其连接的检验装置，

c. 在一个接收器站中，对某些量子系统对检验存在相干的相位关系；以及

d. 在接收器站，检测证据状态，以帮助揭示跨越量子系统分离进行的攻击。

带有用于窃听器检测的量子位内和之间干涉 的两非正交状态量子密码学方法及设备

技术领域

[0001] 本发明一般涉及量子密码学领域，并具体涉及允许两个用户交换位序列并确认其保密的设备和方法。

背景技术

[0002] 如果两个用户拥有共享的随机保密信息（以下称为“密钥”），他们以可证实的安全性能够实现以下两个密码学目标：1）使得他们的消息对于窃听者不能理解，以及 2）区分出合法的消息与伪造的和改动的消息。一次填充密码算法实现了第一个目标，而 Wegman-Carter 鉴别实现了第二个目标。遗憾的是这两个密码学方案消耗密钥资料而使其不适于使用。这样对于希望保护他们以这些密码技术之一或两者交换的消息的双方，必须发明一种方法以便交换最新的密钥资料。一种可能性是一方生成密钥并在其到达第二方之前刻录在物理介质上（盘，cd-rom，rom）。这一方法的问题是密钥的安全性与这样的事实相关，即在其整个生命期，从其产生到其使用，直到最终放弃都要受到保护。此外，这是不实际的并很繁琐。

[0003] 因为这些困难，在许多应用中，人们另外诉诸纯粹的数学方法允许双方同意通过非安全通信信道共享机密。遗憾的是，所有这类对于密钥协议的数学方法依靠的是未证实的假设，诸如分解大整数成因式的困难。这样它们的安全性只是有条件的，并且是有问题的。进一步的数学上的发展可能会证明它们完全是不安全的。

[0004] 量子密码术 (QC) 是这样一种方法，其允许在远程的两方，即发送器与接收器之间，以可证实的绝对安全性交换保密密钥。该方法的说明可在 Nicolas Gisin，Grégoire Ribordy，Wofgang Tittel，and HugoZbinden，“Quantum Cryptography”，Rev.of Mod. Phys.74，(2002) 中找到，其内容在此结合以资对比。一方 - 发送器关于量子系统诸如光子，通过在对应的的量子态制备这一量子系统，对密钥的每一二进制数字或位的值编码。携有密钥位的量子系统称为量子位 (qubit)。量子位通过量子信道诸如光学滤波器向另一方即接收器发送，其进行量子测量以确定每一量子位是在什么量子态制备的。这些测量结果被记录并用来产生密钥。这一方法的安全性来源于以下著名的事实，即未知量子系统的量子态的测量引起这一系统的修改。这意味着在量子信道上的间谍窃听在不向发送器与接收器之间被交换的密钥引入差错情形下，不能获得关于密钥的信息。换言之，QC 的安全性是因为量子力学的非克隆理论：间谍不能复制被传送的量子系统并向接收器转发完好的拷贝。

[0005] 有几种 QC 协议。这些协议描述了在量子系统上如何使用量子态组对位值编码，及发送器和接收器如何协同产生保密的密钥。这些协议最常使用的，也是第一个要提及的，是由 Charles Bennett 和 GillesBrassard 在 Proceedings IEEE Int.Conf.On Computers，Systems andSignal Processing，Bangalore，India(IEEE，New York，1984)，pp.175-179 中公开的所谓 Bennett-Brassard 84 协议 (BB84)，其内容在此结合以资参考。发送器对他想发送的每一位在两个水平的量子系统上编码，以制备量子位。每一量子位可或者作为

σ_x(|+x >对“0”编码及 |-x >对“1”编码）的本征态，或者作为 σ_y(|+y >或 |-y >，使用相同的惯例）的本征态制备。可以说位是以两个不兼容的基被编码的。对于每一位，发送器使用一个适当的随机数产生器产生信息的两个随机位，它们用来确定位值（一个随机位）和基信息（一个随机位）。每一量子位通过量子信道被发送到接收器，接收器以这两个基之一对其进行分析，即测量 σ_x 或 σ_y。接收器使用适当的随机数产生器产生确定测量基（基信息）的信息的随机位。对每一量子位，测量基础是被随机选择的。在交换大量的量子系统之后，发送器和接收器进行称为基调和的过程。发送器通过普通的或公共通信信道向接收器通知其中制备了每一量子位的基 x 或 y（σ_x 或 σ_y 的本征态）。当接收器使用了与发送器用于这一测量相同的基时，他知道他已测量的位值必定是由发送器发送过来的位值。他公开指出这一条件对哪些量子位被满足。对应的的位构成所谓原始密钥。使用了错误的基的测量被简单地抛弃。在没有间谍的情形下，被共享的位的顺序是没有错误的。虽然想获得关于被交换的量子位顺序的某些信息的间谍，能够在几种攻击之间选择，但量子物理的定律保证了他不能在密钥中不引入可觉察的微扰之下这样作。BB84 协议的安全性依赖于这样的事实，即由发送器发送的量子位是在属于不兼容基的量子态制备的。对于给定的量子位，这就使得窃听者不能有绝对把握确定其量子态。更一般来说，BB84 协议属于一类协议，其中在至少两个不兼容的基中至少使用两个量子态。

[0006] 实际上，人们不得不使用不完美的设备，这意味着在位序列中存在某些错误，即使窃听者与量子位没有相互作用。为了仍然允许产生保密密钥，协议的基协调部分补以其它步骤。这整个的过程称为密钥精化 (distillation)。发送器和接收器检验关于位顺序样本的微扰程度，这也称为量子位错率 (QBER)，以便评估传输的保密性。如果这一差错率不很大，则不妨碍安全密钥的精化，区别于原始密钥也称为精化的密钥。在两方采用把窃听者能够获得的信息量降低到任意低水平的所谓秘密放大算法之前，确实能够纠正差错。

[0007] 已提出几种其它的量子密码协议。在 1992 年，Charles Bennett 在 Phys. Rev. Lett. 68, 3121 (1992) 中证明，在两个非正交状态之一足以制备量子位，并公开了所谓 B92 协议，该文献内容在此结合以资参考。这种情形下，发送器重复发送非正交的两个纯状态 $|u_1>$ 或 $|u_2>$ 之一的量子位。接收器不能在它们之间作出明确的区分。然而他能够进行一个广义的测量，这也称为正算子值测量，其有时不能给出答案，但在所有其它时候可给出正确的答案（形式上这一测量是一组两个射影算子 $P_1 = 1-|u_2><u_2|$ 或 $P_2 = 1-|u_1><u_1|$）。关于量子位这一测量的结果用来产生密钥位。只需要两个状态这一事实意味着，这一协议实际中比较容易实现。然而重要的是要意识到，窃听者还可能进行广义的测量。当他获得一个答案时，他能够因此转发一个制备好的量子位，而当结果是非决定性的时就不进行。这一攻击在实际的设备中特别有力，其中因为量子信道的衰减和有限的检测器效率，接收器预期只检测由发送器发送的量子位的一小部分。然而当使用混合状态 ρ_1 和 ρ_2 而非纯状态 $|u_1>$ 或 $|u_2>$ 时，实际中就是这种状态，通过保证选择的混合状态 ρ_1 和 ρ_2 跨过希尔伯特空间的两个非交子空间，能够挫败这一攻击。这允许接收器找出两个算子 P_1 和 P_2，使得 P_1 消灭 ρ_2 而 P_2 消灭 ρ_1，但任何状态都不会被两个算子消灭。这可保证，如果窃听者发送空状态而非混合状态 ρ_1 和 ρ_2 之一，则接收器仍然能够记录确定性的测量结果，其引入有非零概率的差错。当考虑大量的量子位时，这一非零概率产生可测量的差错率。

[0008] 在过去十年，使用光子作为量子位及光学滤波器作为量子信道，已实现了几种 QC

设备的验证。对于实际使用的这些验证，尽管有当前的技术限制，重要的是它们简单，并如果可能允许高速率的密钥交换。这一考虑影响着 QC 设备和其在其中制备量子位的量子态组的选择。尽管电磁场的极化状态代表着为实现 QC 自然的候选，但当光纤携带量子位时实际中它们难以使用。光纤通常确实引起极化状态的转换。反之，定时信息特别稳定并能够用来实现简单的 QC 设备。在 Physical Review A 70,042306(2004) 中 Debuisschert 等人已提出一族时间编码协议，该文献在此结合以资参考。这些协议最简单的协议中，发送器对每一位发送一个单个的光子脉冲。位值之一，比如“0”通过一个非延迟的脉冲编码，而“1”由一个延迟脉冲编码。延迟值小于脉冲持续时间。接收器相对于基准时间测量光子到达时间，并定义三组事件。第一组事件包含检测只能来自非延迟脉冲并被计数为“0”值位。第二组包含检测只能来自延迟脉冲并被计数为“1”值位。最后，第三组包含检测既来自非延迟又来自延迟的脉冲。它们对应于非确定的结果并被抛弃。接收器有时还向干涉仪发送脉冲，以对它们的持续时间进行干涉测量。这一协议的安全性来自这样的事实，即只要窃听者获得确定的结果，则他必定猜测向接收器转发什么状态并具有引入差错的非零概率。脉冲持续时间的干涉测量防止了窃听者发送大大短于原始脉冲的脉冲，强制接收器的测量结果。使用两个附加的不携带信息的延迟脉冲，对窃听者强加附加的对称抑制，这防止他利用量子信道衰减。

[0009] 虽然原始的 QC 提议要求使用单个的光子作为量子位对密钥编码，但它们的产生是困难的且良好的单光子源也不存在。而是因为简单的考虑，许多的实现依赖于发送器与接收器之间弱相干状态的交换，作为对理想量子位的逼近。相干状态由光子状态的相干重叠组成。换言之，在相干状态内部不同的光子状态成分之间存在一种固定的相位关系。为了描述这种状态，只要知道其振幅和全程相位即可。相干状态当其振幅小时被称为是弱的。弱相干状态可通过衰减激光脉冲产生。

[0010] 在实际实现中使用弱相干状态而不是单个光子这一事实意味着，窃听者可以进行一种非常有力的攻击，称为光子数分割 (PNS) 攻击。窃听者进行量子非破坏性测量，以测量每一弱脉冲中存在的光子数。当脉冲恰好只包含一个光子时，窃听者阻挡该光子。当脉冲包含两个光子时，窃听者提取一个光子并将其存储在量子存储器中，同时向接收器转发另一光子。在协议的基协调步骤之后，窃听者最后测量他已存储的光子的量子状态。在这一阶段，窃听者知道他必须进行哪种测量，以便获得关于已由发送器发送的量子状态的完全的信息。因为有被阻挡的部分脉冲，可通过降低接收器检测速率揭示其存在，为了隐藏其存在，窃听者可使用优秀的无损信道 - 记住在 QC 中窃听者是由物理学而不是技术限制的 - 向接收器转发他从其去除了一个光子的多光子脉冲。PNS 攻击在实际中是特别有力的，其中接收器预期只检测一小部分光子，因为量子信道衰减和有限的检测器效率。因而对于 QC 设备和协议重要的是阻止这些攻击。

[0011] 已经提出几种方法降低窃听者进行 PNS 攻击的可能性。HwangW.Y. 在 Physical Review Letters 91,057901(2003) 中，Hwang X.B. 在 Physical Review Letters 94,230503(2005) 中，以及 Lo H.K. 等人在 Physical Review Letters 94,230504(2005) 中已提出使用引诱状态，这些文献在此结合以资参考。已提出对 PNS 攻击有弹性的新的协议。在 H.Takesue 等人标题为“在 105km 光纤上差分相移量子密钥分布的实验”，quant-oh/0507110 中，其内容在此结合以资参考。Takesue 等人提出这样一种协议，其使用

在无限流中持续时间为 t 并以时间 T 分开的两个相邻弱相干状态之间的二进制相位差对位值编码，其中 t 小于 T。在这流中，相邻的弱相干状态认为是相位相干的。接收器进行干涉测量以确定这一差分相位差，并从而建立位值。这一协议的安全性来自这样的事实，即对应于每一差分相位值的两个量子状态是非正交的。试图测量位值的窃听者有时获得不确定的结果。这些情形下，他必须猜测要转发哪个状态并以非零概率引入差错。如果当他获得一个不确定结果时他选择不向接收器转发任何东西，则他抑制了对相邻弱相干状态的干扰，这引起有非零概率的差错。在这协议中，关于各弱相干状态的 PNS 攻击明显是无用的，因为位值是按相邻状态之间的相位差编码的。一个有效的 PNS 攻击将必须测量在两个相邻弱相干状态中的光子数。然而这将破坏与其它相邻状态的相位相干，并引入有非零概率的差错。

发明内容

[0012] 提供了一种设备和方法，用于在发送器和接收器之间交换位序列，又称为原始密钥，并允许发送器和接收器估计窃听者能够获得的关于原始密钥的最大信息量。随后这一原始密钥通过一适当的密钥精化过程可被精化为一个安全的密钥。

[0013] 该方法包括几个步骤。在第一步骤，该方法通过一个发送器发送由量子位源产生的量子位流，流中两个相邻的量子位具有固定的相位关系，且其中每一量子位在两个量子状态之一制备，其中量子状态是非正交的。在第二步骤中，该方法通过接收器对某些量子位进行第一类测量，一个正的算子值测量，以确定它们通过发送器在什么量子状态制备的。在第三步骤中，该方法通过接收器对量子位对进行第二类测量，以估计它们之间现有相位关系的相干程度。在第四步骤，该方法通过接收器通知什么量子位产生了正算子值测量的确定的结果，使得它们能够对原始密钥有贡献。在第六步骤，该方法通过传统信道的通信以及发送器与接收器之间的协作，评估流的量子位之间的相干程度，以估计窃听者关于原始密钥的信息量。

[0014] 这一量子密码设备和方法的第一个优点在于，它们可简单地实现。这一简单性源于这样的事实，即量子位只需在两个非正交状态制备。此外，该设备和方法允许使用量子位值的时间编码。位值之一通过在两个时间箱的第一个中制备由非空弱相干状态组成的量子位而被编码，同时保持第二个时间箱为空，每一个时间箱比它们之间时间短。其它位值关于空和非空时间箱被交换的量子位编码。此外，由发送器发送的两个量子位必须有固定的相位关系（它们必须是相位相干的）。这种情形下，允许在两个状态之间进行区分的优化的正算子值测量之一，涉及以光子计数检测器测量光子到达的时间。这一测量的进行非常简单。此外，这些状态对量子信道中的环境干扰是非常鲁棒性的。例如极化波动不会诱导差错。最后，这一简单性还意味着，即使使用现有的技术也能够进行高速率密钥交换。通过由接收器所作的两个量子位的两个时间箱之间相位相干的相干估计，监视窃听。

[0015] 这一量子密码设备和方法的第二个优点在于，它们对于 PNS 攻击是鲁棒性的。这一属性来自这样的事实，即由窃听者去除量子位结果是明显的扰动。如果量子位之一被去除且接收器试图测量这一特定量子位与另一量子位的相干性，则测量所得结果将以非零概率指出这一去除。

附图说明

[0016] 从以下参照附图的说明，本发明其它的目的和优点将明显可见，其中通过说明和示例，公开了本发明的实施例。

[0017] 附图的简要说明

[0018] 图 1 是密钥分布过程的高级流程图。

[0019] 图 2 是本发明设备的示意图。

[0020] 图 3 是由发送器产生的量子位流的图示。

[0021] 图 4 发送器源的实施例的示意图。

[0022] 图 5 是表示在正交空间中由发送器产生的非正交状态的图示。

[0023] 图 6 是接收器的光子系统的示意图。

[0024] 图 7 的图示表示在接收器的光学子系统的相干测量器输出端口之一中的量子系统，及由窃听者去除和交换这些量子系统之一的值的效果。

具体实施方式

[0025] 现在参见图 1 和 2，提供了方法 10 和设备 12，用于在发送器站 14 和接收器站 16 之间交换关于图 3 中所示量子系统（即量子位）20 的流 22 被编码的符号序列，用来传送原始密钥（数据串，诸如 10110010100111100100101O...01010100），并允许发送器站和接收器站估计窃听者 24 可能已获得关于原始密钥的最大信息量。这一原始密钥随后可通过适当的业内已知的密钥精化过程被精化为一安全密钥（比粗数据串较少数字的精化数据串，诸如 10011000...1100）。

[0026] 发送器站 14 和接收器站 16 通过量子信道 26 和传统的信道 30 连接。符号值通过在特定的量子状态也称为数据状态制备量子系统而被编码。以下在发送器站 14 和接收器站 16 之间被交换的量子系统称为量子位，不论所使用的符号的符号集大小如何。

[0027] 所使用的量子状态是非正交的。这意味着，根据量子物理定律，制备量子位部分忽略的状态不能以 100％的概率对其确定。可能作的最好的是进行广义测量，这给出概率 $p < 1$ 的确定的结果和概率 $1-p$ 的非确定结果。这样接收器站 16 只能确定状态的一部分－且也是符号一部分－由发送器站 14 发送的。对于窃听者 24 也是这样。当获得一个非确定的结果时，窃听者 24 将有选择，或者猜测发送的是什么状态，或者不发送任何东西。

[0028] 如果窃听者 24 猜测他所发送的状态，他将在通过测量流 22 的量子位 20 所产生的符号 20 序列中引入有非零概率的差错。发送器站 14 和接收器站 16 在所谓密钥精化阶段能够协作检测出这些差错。如果窃听者 24 只是选择不发送任何东西代替非确定结果，则情形变得更为困难。确实不能区分这些情形与量子位由有损耗的量子信道吸收的情形。这样就必须添加一种机制，以允许发送器和接收器站 14 和 16 注意这类攻击。为实现这一点，发送器站 14 保证其位置在量子位流 22 中充分靠近的流 22 的两个量子位 20 之间存在相干相位关系。这时接收器将有时通过进行适当的测量（例如相干测量），检验两个随机选择的量子系统之间仍然存在相干相位关系。量子位 20 的去除或相位关系的破坏将产生显著的非零概率的干扰。

[0029] 遗憾的是，窃听者 24 仍然有另外的可能。他能够穿越两个量子位之间的分离，进行用来编码符号值的量子性质的相干测量。使用这种攻击，他将不破坏量子位之间的相干，这就不会触发警报，同时获得几乎全部的信息。这样必须添加一种机制，允许发送器和接收

器站 14 和 16 注意到这类攻击。为实现这一点，发送器站 14 在数据状态制备的某些量子位之间，插入在称为证据状态的一种状态中制备的量子系统，它与数据状态不正交并且不是这些状态的叠加。在证据状态中制备的这些量子系统以下也将称为量子位。这时至少存在一种测量，允许当在证据状态进行时确定这一状态是否已受到测量，当施加到在数据状态制备的量子位 20 时其允许确定这一数据状态是什么。这时接收器站 16 能够对某些量子位 20 随机进行这一测量。这些量子位 20 的某些将在证据状态制备，并这样将允许对穿越量子位分离的攻击的识别。

[0030] 总之，本发明的方法 10 和设备 12 基于三个原理：首先使用在非正交状态制备的量子位 20，并刻画与邻近的相干相位关系；其次，检验关于仍然存在相干相位关系的某些量子位对；第三，使用在所谓证据状态制备的量子位，帮助揭示穿越量子系统分离进行的攻击。以下将展示本发明的方法 10 和设备 12 的一个实施例，其使用符号值的时间编码，并使用电磁场在时间箱 (time bin) 中脉动弱相干状态。

[0031] 参见图 2，设备 12 的一个实施例包括由量子信道 26 和传统信道连接的一个发送器站 14 和一个接收器站 16。量子信道 26 例如可以是专用的光纤，或波长分割多路复用光学通信系统中的信道。传统通信信道 30 例如可以是因特网或携带明亮光脉冲的第二光纤。

[0032] 发送器站 14 包括一个由处理单元 36 控制的量子位源 34。处理单元 36 例如可以是一计算机，其具有存储器，输入 / 输出端口，管理输入、存储器和关于它的操作的中央处理器，以产生所需的输出，以及数据传送和通信机制，允许与设备的其它组件通信。量子位源 34 通过传送线路 40 连接到处理单元 36。这一传送线路 40 例如可以由携带电子信号的导线或电缆制成。随机数产生器 42 连接到处理单元 36。

[0033] 现在参见图 4，量子位源 34 包括一个光源 44，其由一光学通路 46 连接到振幅调制器 48。光源 44 例如可由模式锁定的激光器或连续波激光器制成。源 34 还可以包括一个可变光学衰减器 50，通过一个光学通路 52 连接到振幅调制器 46，以调节量子位 20 总振幅。光学通路 46 和 52 例如可包括光纤或自由空间光纤通路。量子位源 34 的输出连接到量子信道 26，使得发送的光投入到量子信道。

[0034] 再来参见图 3，这一源 34 产生量子位 20 的一个流 22。每一量子位 20，在持续时间的时间箱 60 和 62 中，由电磁场的一对脉动的弱相干状态 56 例如衰减的激光脉冲的对 54 组成。在给定的量子位 20 中，时间箱 60 和 62 的中心由时间 T1 分离，t 小于 T1。量子位 20 的第二脉动弱相干状态 72 与随后的量子位 20 的第一脉动弱相干状态 66 的中心分离时间 T2，t 小于 T2。原则上，T1 不需要等于 T2。然而为了简单起见，以下我们将认为 T1 ＝ T2 ＝ T。携带“0”位值的量子位 74 由在第一时间箱 60 中非空弱相干状态 71，其平均包含 μ 个光子，μ 的选择要保证协议的安全性，以及在第二时间箱 62 中空的 (μ ＝ 0) 弱相干状态 72 组成。类似地，携带“1”位值的量子位 76 由量子位 76 的第一时间箱 60 中的空的 (μ ＝ 0) 弱相干状态 66，和量子位 76 的第二时间箱 62 中非空弱相干状态 64 组成，其平均包含 μ 个光子，μ 的选择要保证协议的安全性。注意，尽管图 3 只示出量子位 74 的第一时间箱 60 和第二时间箱 62 这一事实，但流 72 的每一量子位都具有第一时间箱 60 和第二时间箱 62。

[0035] 现在参见图 5，其中示出对于两个时间箱 60 和 62 的正交空间，对应于量子位 20 的两个值每一个的量子状态重叠，因而是非正交的。

[0036] 在正式的记法中，量子位 q 可写为 |q ＞＝ | β ；α ＞。方程式的第二个“右矢”中每一位置代表一个模式。以上所描述的状态对应于时间编码。这种情形下，每一模式是非重叠的时间箱。字母 α 和 β 指示每一时间箱中相干状态的振幅。在这一记法中，可以通过 | α^2| 在第一时间中并通过 | β^2| 在第二时间中计算光子的平均数。这样 0 的量子位值记为 |0 ＞＝ |0 ；α ＞，而 1 的量子位值记为 |1 ＞＝ | α ；0 ＞，其中非空弱相干状态中平均光子数目 μ 等于 | α^2|。

[0037] 量子位源 34 还可产生称为证据状态 80 的序列 |d ＞＝ | δ_2 ；δ_1 ＞。其由非空弱相干状态 82 和 84 组成，在第一和第二时间箱中分别有平均光子数 | δ_1^2| 和 | δ_2^2|。引诱序列 80 不对位值编码，但用来防止一定的窃听者攻击。

[0038] 源 34 一个重要的性质在于，两个相邻的弱相干状态，不论是在特定量子位 20 的两个时间箱 60 或 62 中，还是邻近量子位的时间位 62 或 86，必定有一个固定相位关系。同样地，可以说流 22 中的相邻的弱相干状态必须是相位相干的。箭头 88 和 89 表示相邻弱相干状态，例如 66 和 72 或 71 和 72 之间固定的相位关系。这意味着，两个这种弱相干状态如果重叠则相干干扰。可通过从连续波激光束使用振幅调制器 48 切割出脉冲，产生呈现这种相位相干的脉动弱相干状态的流 22。

[0039] 对于流 22 的每一量子位 20，发送器站 14 的处理单元 36 使用由随机数产生器 42 提供的随机数，选择在量子信道 26 上应当发送“0”- 量子位，“1”- 量子位或证据状态 80。对于每一量子位 20，处理单元 36 记录该选择。对于每一可能性的各概率不必是相等的。它们的选择要使密钥交换速率最大化。

[0040] 现在参见图 2，接收器 16 包括一个光学子系统 90 和一个处理单元 92。处理单元 92 例如可以是一个计算机，其具有存储器，输入 / 输出端口，中央处理器，它管理输入，存储器和在其上的操作，以产生所需的输出，以及允许与设备其它组件通信的数据传送和通信机制。光学子系统 90 通过传送线路 94 连接到处理单元 92。这一传送线路 94 例如可以包括携带电子信号的导线或电缆。

[0041] 现在参见图 6，光学子系统 90 具有一切换装置 96，其带有至少一个输入端口 98 和至少两个输出端口 100 及 102。这一装置 96 例如可以是带有适当的反射 / 传送率的耦合器。它还可以是一个由处理单元 92 随机触发的光学开关。切换装置 96 的输入端口 98 连接到量子信道 26。其第一个输出端口 100 连接到位值测量装置 106 的一个检测器单元 104，它用来进行时间基的测量。第二输出端口 102 连接到线路监视装置 114 的不平衡干涉仪 112 的输入端口 110。切换装置 96 的作用是使用光学通路 116 或 118 把进入的量子位 20 或者指向位值测量装置 106，或者指向线路监视装置 114。光学通路 116 和 118 例如可包括光纤或自由空间光通路。干涉仪 112 例如可以是包含时间延迟 T 的不平衡 Mach-Zehnder 干涉仪。其作用是重叠或者来自单个量子位 (71 和 72) 或者来自两个相邻量子位 (66 和 72) 的相邻弱相干状态。当重叠的状态 71 和 72 来自单个量子位 74 的两个时间箱 60 和 62 时，这可称为内部重叠，其作用是检验内部量子位的相干。当它们来自相邻量子位例如 66 和 72 时，可称为交叉重叠，其作用是检验内部量子位相干。两个检测器单元 120 和 122 连接到干涉仪 112 的输出端口 124 和 126。当非空弱相干状态出现在两个相邻脉冲中时，这一干涉仪 112 的非平衡被调节，以便在连接到一个检测器单元 120 或 122 例如检测器单元 122 的输出端口 124 或 126 之一中产生破坏性的干涉。这就是对于证据状态 80 的情形（因为内部重

叠）并在“1”-量子位后随“0”-量子位的情形下（因为交叉重叠）。检测器单元 104，120 和 122 例如由光子计数检测器构成，其定时分辨率小于 T，足以允许它们在由源 34 产生的量子状态 20 的两个时间箱例如 60 或 62 之间辨别。这些光子计数检测器 104，120 和 122 例如可包括盖革模式下的雪崩光电二极管，或采用非线性过程的装置，以便上转换输入信号。检测器单元 104，120 和 122 由传送线路 124 连接到处理单元 92。这些传送线路 124 例如可由携带电子信号的导线或电缆构成。

[0042] 位值测量装置 106 包括检测器单元 104，允许一个光子在到达第一时间箱 60 或第二时间箱 62 之间区别。这意味着要进行正算子值测量，以便在非正交状态之间区分。由于每量子位 20 的平均光子数低，位值测量装置 106 有时不能记录在时间箱 60 或 62 中的检测。当这发生时，测量是非确定的。当检测器单元 104 记录到一个检测时，它由处理单元 92 记录。

[0043] 线路监视装置 114 使得能够监视两个不同量子位 74 或 76（量子位之间相干）或证据状态 80 内（量子位内部相干）相邻时间箱 60 或 62 的相邻弱相干状态 66 和 72 之间的相位相干程度。两个弱相干状态通过干涉仪 112 重叠，且干涉被记录。

[0044] 现在参见图 7，在左侧可以看到，如果量子位值 n 和 n+1 的子序列为“11”或“00”，则记录干涉时间窗口中计数的概率对于两个检测器单元 122 和 120 都是非零的。当非空弱相干状态与空状态重叠，不发生干涉，且光子概率地选择干涉仪的输出端口 124 或 126。如果该子序列为“10”，则检测器单元 122 和 120 应当不记录干涉窗口中的计数，因为两个贡献是空的。最后如果子序列为“01”，因为破坏性干涉，检测器单元 122 也应当不记录计数，而检测器单元 120 具有记录计数的非零概率。

[0045] 现在看中心列，可以看到，在“01”序列情形下并如果窃听者去除量子位之一，则它破坏了干涉。然后检测器单元 122 记录有非零概率的干涉时间窗口中的计数。这些计数以下称为警告计数。这意味着要去除一定量子位 20 的窃听者 24，例如当他获得一个不确定结果时，将引起明显的干扰。明显地，如果窃听者 24 为防止这些非干扰事件出现而阻挡所有量子位 20，他就中断了通信，这将由发送器和接收器注意到。

[0046] 看右侧的列，看到一个量子位值的交换将类似地引起在干涉时间窗口中计数，其中没有预期的。将随机猜测未知量子位值的窃听者 24，会以 50％的概率选择错误的值。在这些情形下，他将有非零的概率引入警告计数。注意，这种由窃听者 24 的干涉也将诱导在位值测量装置 106 中被检测的序列中有非零概率的错误。

[0047] 最后，跨越两个弱相干状态例如属于单个量子位例如 74 的 71 和 72 的量子非破坏测量，破坏与相邻弱相干状态的相位相干，并于是当被攻击的量子位的一个弱相干状态与相邻的量子位的一个弱相干状态重叠时，将诱导有非零概率的警告计数。类似地，对两个弱相干状态，例如属于两个不同量子位 76 和 74 的 66 和 72 的量子非破坏测量，将破坏这两个弱相干状态与它们各自量子位的第二弱相干状态的相位相干。于是当对证据状态进行攻击时，也将诱导警告计数。如果量子非破坏攻击覆盖多于两个弱相干状态，相位相干将类似地被破坏，并诱导警告计数。检测器单元 120 和 122 的检测由处理单元 92 记录。

[0048] 在大量量子位 20 交换之后，接收器站 16 通过传统信道 30 公开通知，在该情形下他在他的位值测量装置 106 中获得了确定的结果。发送器站 14 检验并通知接收器站 16 什么情形对应于证据状态 80 及什么情形不对应。对应于证据状态的情形被抛弃，因为它们对

于符号值不编码。其它的情形被添加到原始密钥。接收器站 16 还通过传统信道 30 通知发送器站 14，在什么情形下他在线路监视装置 114 的检测单元 120 和 122 记录检测。发送器站 14 在所发送的量子位 20 的列表中检验这些检测是否预期的或是否不是。警告计数的出现概率允许发送器站 14 和接收器站 16 降低窃听进行的强度，并于是降低窃听者 24 能够获得的关于密钥的信息量。这一估计允许他们把密钥精化过程的步骤充分参数化，例如包括纠错及秘密放大，这从原始密钥产生安全的最终密钥。

[0049] 在设备 12 的另一实施例中，设备 12 的发送器站 14 与接收器站 16 分开装但与之一同使用。

[0050] 再次参见图 1，本发明的密钥交换方法 10 包括以下步骤。

[0051] 在第一步骤 130，发送器站 14 使用其量子位源 34 产生量子位 20，并将其向接收器站 16 通过量子信道 26 发送。

[0052] 在第二步骤 132，量子位 20 通过切换装置 96（图 6 中所示），其中或者指向位值测量装置 106，或者指向线路监视装置 114，其中对各每一量子位流进行相关的测量。

[0053] 在第一可替代子步骤 134a，对于因而由切换装置 96 指向位值测量装置 106 的量子位 20，测量光子到达的时间。

[0054] 在第二可替代子步骤 134b，以干涉方式测量由切换装置 96 因而指向线路监视装置 114 的量子位 20 的内部－量子位相位相干或相邻量子位之间的量子位之间的相位相干。子步骤 134 和 134b 是相互排斥的。

[0055] 在第四步骤 136，测量的输出由接收器站 16 的处理单元 92 记录。

[0056] 在第五步骤 138，方法 10 进行一个回路，重复先前方法步骤 130，132，134a，134b 和 136，直到足够数目量子位 20 的流 22 已被交换。

[0057] 在第六步骤 140，一旦足够数目量子位 20 已被交换，发送器站 14 和接收器站 16 交换相关信息，以便通过估计来自步骤 134b 的测量的输出的内部和相互量子位相位相干程度，评估交换期间窃听的强度。发送器站 14 和接收器站 16 还合作确定在步骤 134a 进行的哪一个测量产生了原始密钥位。

[0058] 原始密钥以及窃听者可能已获得的关于这一原始密钥的信息的估计，构成了密钥交换方法 10 的产品。

[0059] 这一量子密码设备 12 和方法 10 的一种优点是实现起来简单。这一简单来自这样的事实，即量子位 20 必须只在两个非正交状态制备。

[0060] 设备 12 和方法 10 的另一优点是允许使用量子位 20 的值的时间编码。通过制备一个量子位，例如由两个时箱 60 的第一个中的非空弱相干状态 71 组成的 74，编码一个位值，同时保持第二时间箱 62 为空，每一时间箱短于他们之间的时间。其它位值关于量子位例如 76 被编码，其中空的和非空的时间箱被交换。这种情形下，允许在两个状态之间区分的优化的正算子值测量之一，涉及使用光子计数检测器测量光子到达的时间。这一测量可特别简单地进行。

[0061] 此外另一优点是，所使用的状态对量子信道 26 中的环境干扰是特别鲁棒的。例如极化波动不会诱导差错。

[0062] 另一优点是，本发明的简单意味着即使使用现有的技术，也能够进行高速率密钥交换。

[0063] 这一量子密码设备 12 和方法 10 的另一优点在于，他们对窃听是鲁棒的，通过某量子位例如 74 内的两个时间箱例如 60 和 62 之间，以及某些量子位对 76 和 74 之间的两个时间箱例如 86 和 62 的相位相干的干涉仪评估，窃听被监视。特别地，这一设备 12 和方法 10 对 PNS 攻击是非常鲁棒的。这一属性源于这样的事实，即由窃听者 24 进行的量子位 20 的去除结果是明显的扰动。如果量子位 20 之一被去除，且接收器站 16 试图测量这一特定量子位与另一个的相互的相干，测量输出将以非零概率指示这一去除。

[0064] 在这里所述的本发明的实施例中可以有各种变化和修改。虽然已展示并描述了本发明一定的示例性实施例，在以上的公开中预期会有范围广泛的修改，变化，和替换。在明显情形下，会采用本发明的明显特性，而没有对应的使用其它特性。因而应当理解，以上的描述应被广义地解释，并理解为只是通过示例和例子的方式给出的，本发明的精神和范围只以所附权利要求为限。

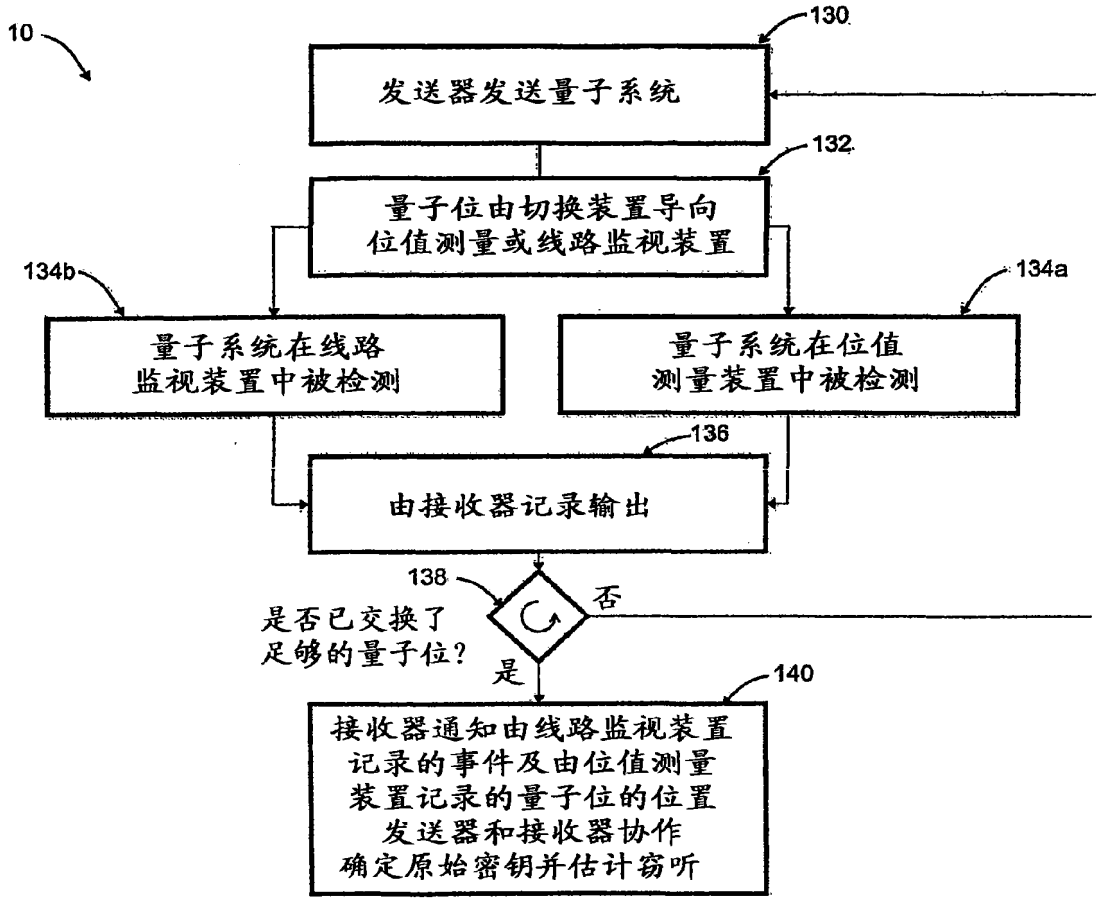

10
130
发送器发送量子系统
132
量子位由切换装置导向
位值测量或线路监视装置
134b
134a
量子系统在线路
监视装置中被检测
量子系统在位值
测量装置中被检测
136
由接收器记录输出
138
是否已交换了
足够的量子位?
否
是
140
接收器通知由线路监视装置
记录的事件及由位值测量
装置记录的量子位的位置
发送器和接收器协作
确定原始密钥并估计窃听

图 1

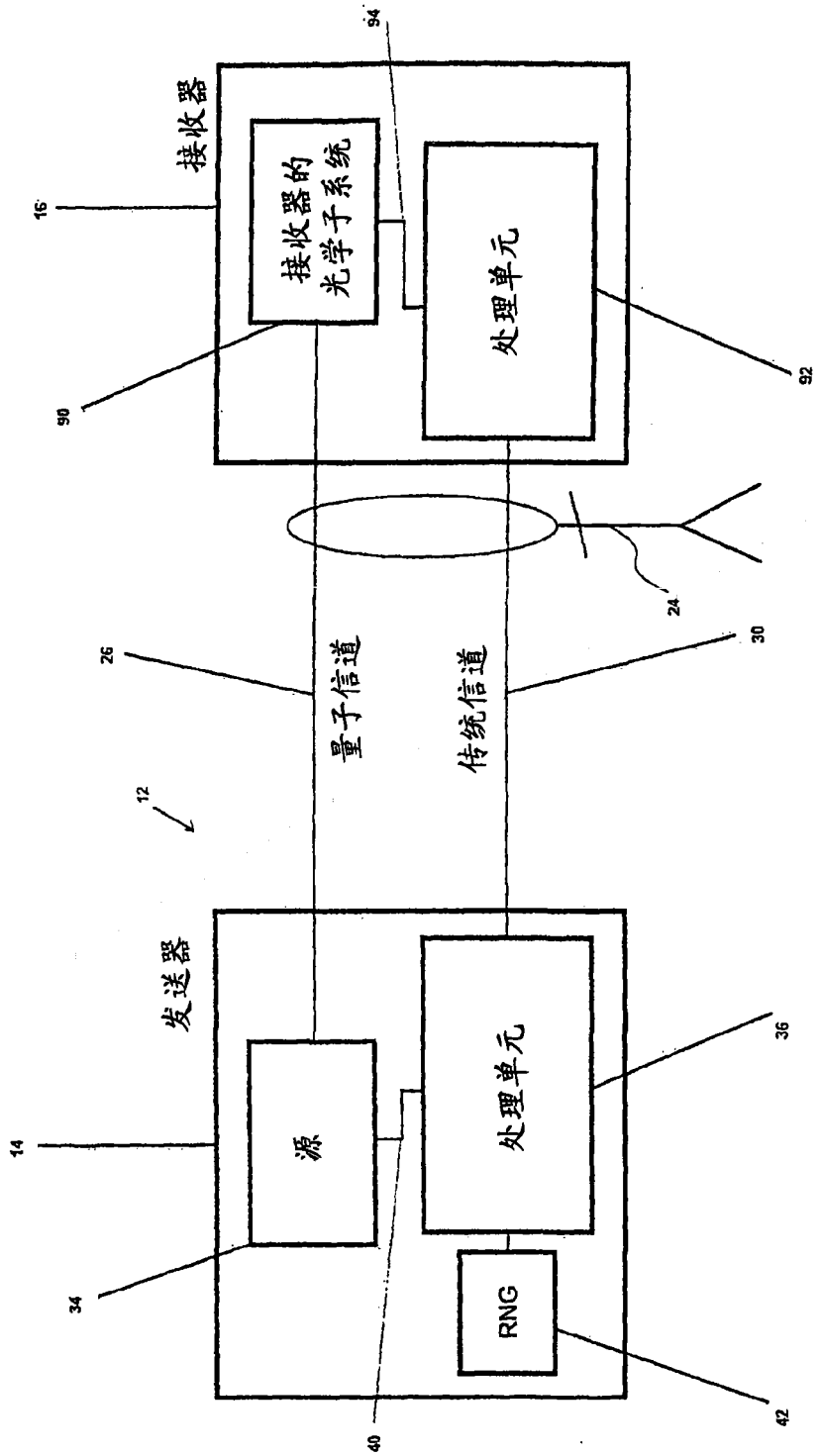

接收器
16
接收器的光学子系统
处理单元
90
92
94
24
量子信道
传统信道
26
30
12
发送器
源
处理单元
RNG
14
34
36
40
42

图2

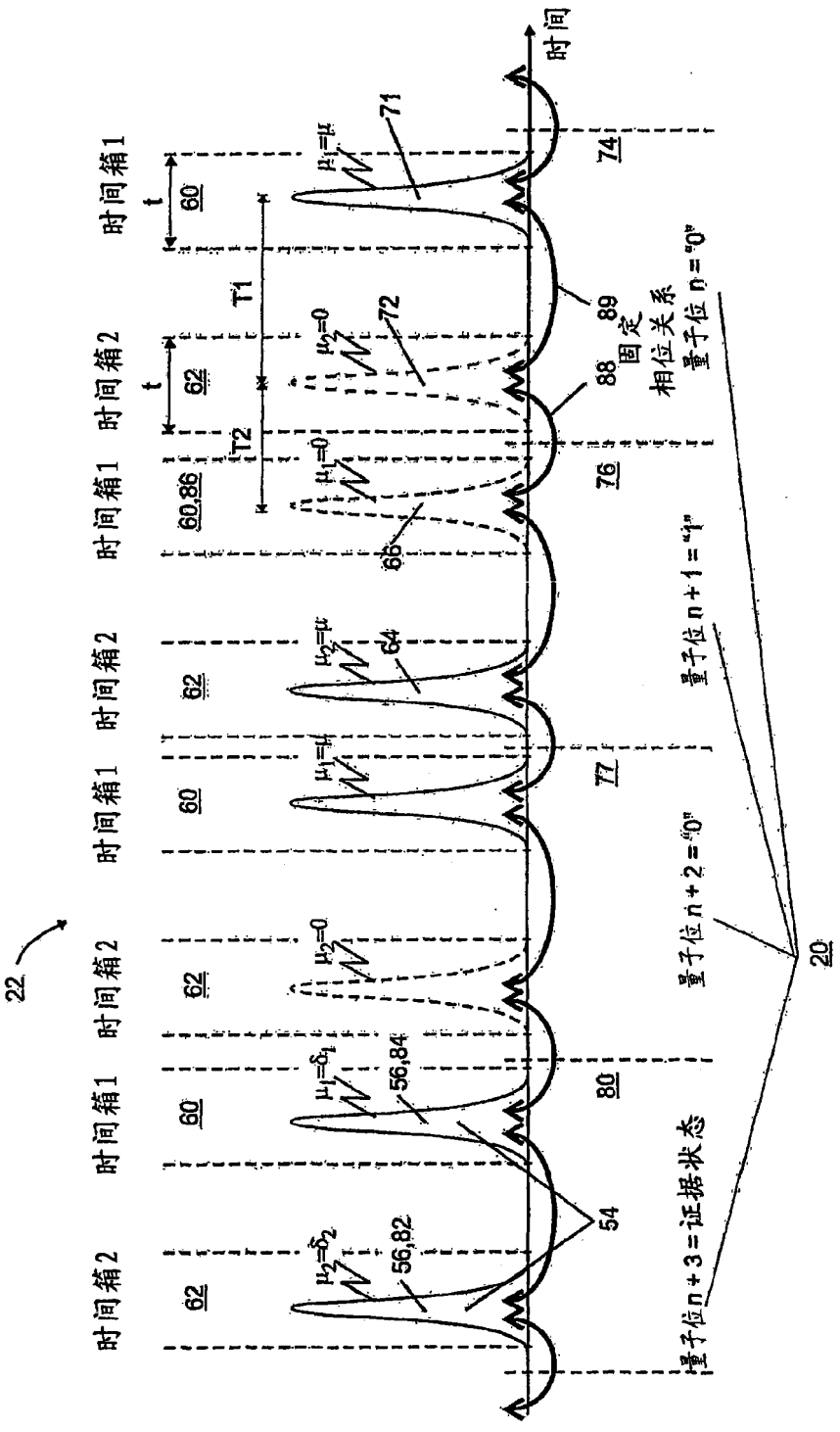

22
时间箱2
时间箱1
时间箱2
时间箱1
时间箱2
时间箱1
时间箱2
时间箱1
时间
t
T1
T2
60
62
60,86
54
56,82
56,84
64
66
71
72
74
76
77
80
88
89
固定
相位关系
量子位 n = "0"
量子位 n + 1 = "1"
量子位 n + 2 = "0"
量子位 n + 3 = 证据状态
20

图 3

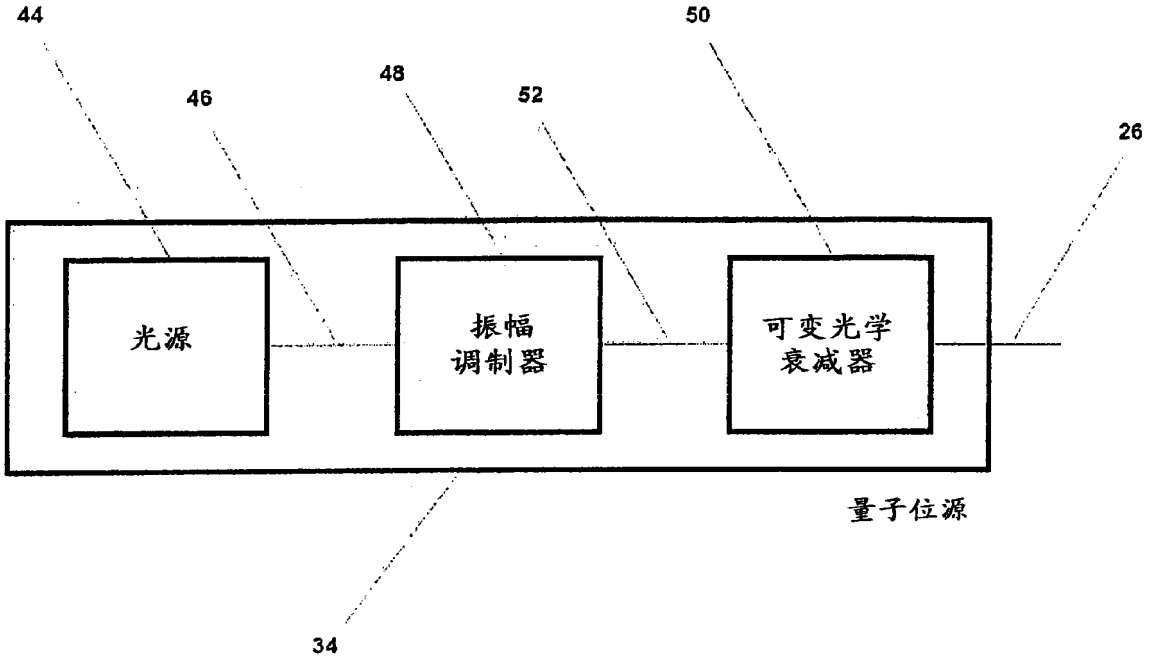


图 4

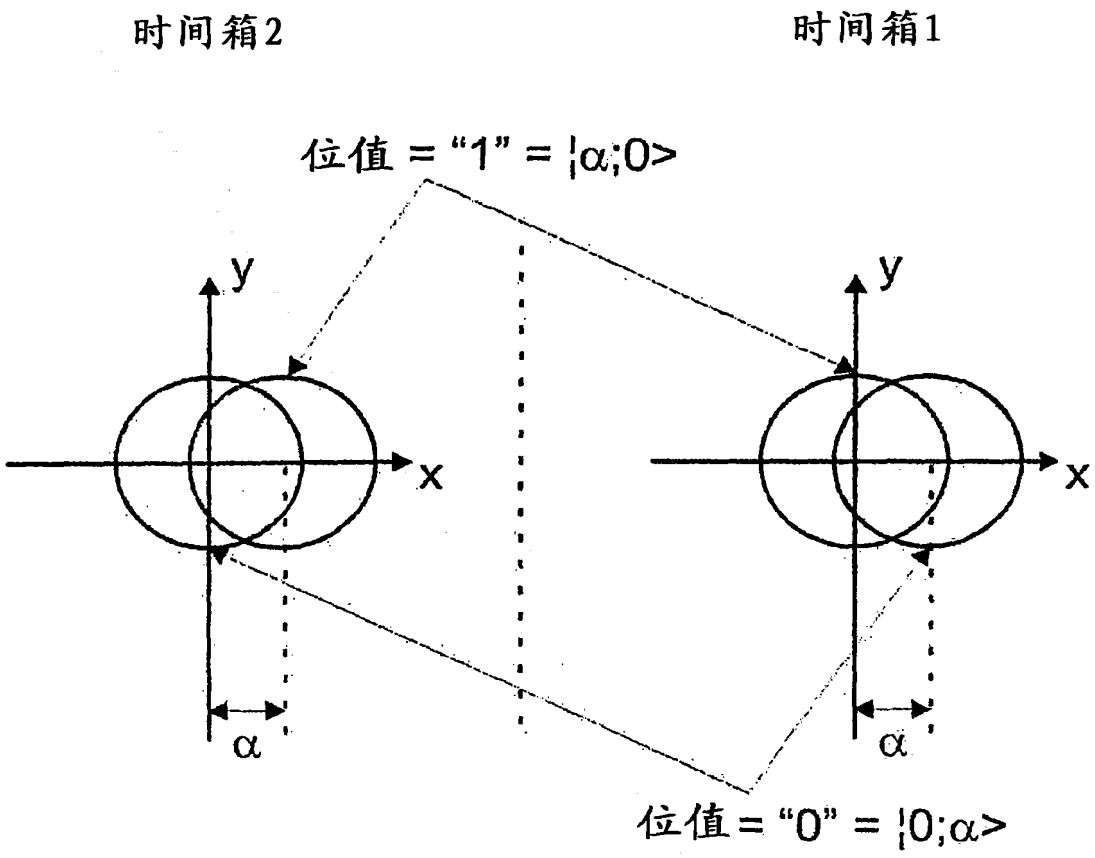


图 5

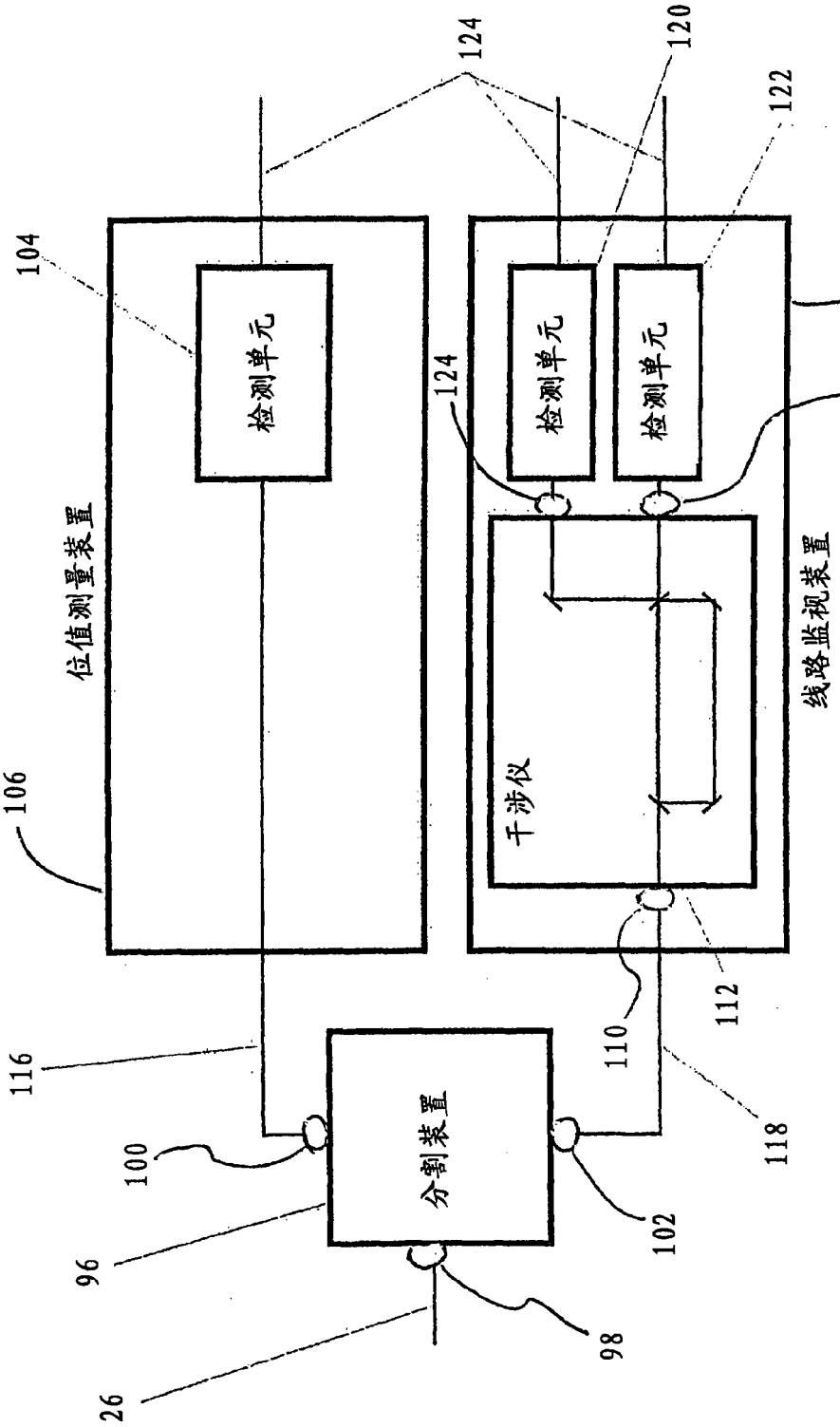

124
120
122
104
检测单元
位值测量装置
114
检测单元
检测单元
124
126
106
干涉仪
线路监视装置
112
110
116
分割装置
118
100
102
96
98
26

图 6

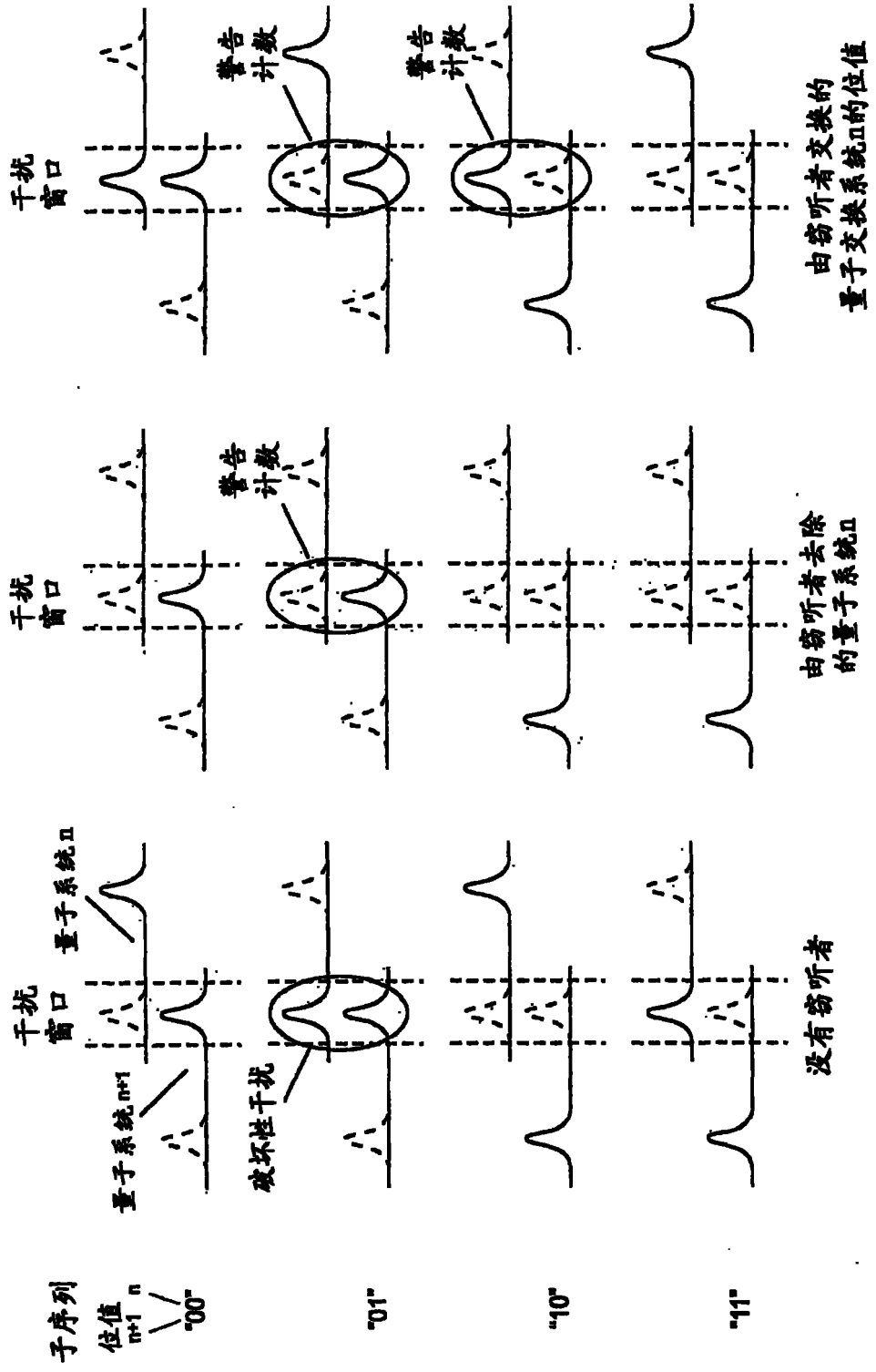

子序列
位值 n+1 n
"00"
"01"
"10"
"11"
干扰
窗口
量子系统n
量子系统n+1
破坏性干扰
没有窃听者
警告
计数
由窃听者去除
的量子系统n
由窃听者交换的
量子交换系统n的位值

图7