(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111699470 B
(45)授权公告日 2025.03.04

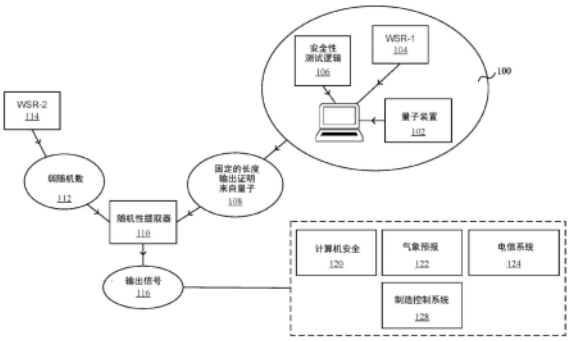
(21)申请号 201880088555.2
(22)申请日 2018.11.30
(65)同一申请的已公布的文献号
申请公布号 CN 111699470 A
(43)申请公布日 2020.09.22
(30)优先权数据
62/607,719 2017.12.19 US
(85)PCT国际申请进入国家阶段日
2020.08.04
(86)PCT国际申请的申请数据
PCT/US2018/063481 2018.11.30
(87)PCT国际申请的公布数据
WO2019/125733 EN 2019.06.27
(73)专利权人 量子有限公司
地址 英国伦敦
(72)发明人 费尔南多·瓜达卢佩·多斯桑托斯·林斯·布兰道
大卫·约翰·沃洛
西蒙尼·塞韦里尼
(74)专利代理机构 北京汇思诚业知识产权代理有限公司 11444
专利代理师 刘晔 王刚
(51)Int.Cl.
G06F 7/58(2006.01)
G06F 7/00(2006.01)
H04L 9/00(2022.01)
H04L 9/06(2006.01)
(56)对比文件
F.Brandao等.Realistic noise-tolerant randomness amplification using finite number of devices.《Nature Communications》.2016,第1-6页.
审查员 余祖澔
权利要求书2页 说明书28页 附图17页

(54)发明名称

放大、生成或证明随机性

(57)摘要

安全性测试逻辑系统可以包括被配置为存储来自测量设备的测量值的非暂时性存储器,测量输出包括是否存在重合的指示,其中在重合时基本上同时在多于一个的检测器处检测到粒子,检测器位于与粒子源不同的通道的端部处并且具有基本相同的长度。该系统可以包括处理器,该处理器被配置为由所存储的测量值来计算测试统计量。测试统计量可以表示贝尔不等式,并且系统可以将测试统计量与阈值进行比较。处理器可以被配置为如果所计算的测试统计量的值超过阈值,则生成并输出证明测量值来自量子系统的凭证。



CN 111699470 B

1.一种用于生成随机位串的系统,其特征在于,所述系统包括:

弱随机性源,其被配置为重复生成第一位串和第二位串,在一个情形中生成的所述第一位串和所述第二位串不必定具有与在另一情形中生成的所述第一位串和所述第二位串相同的值;

量子装置,其被配置为接收一个或多个所述第二位串,并且针对所述量子装置接收的一个或多个所述第二位串中的每一个而输出相关联的第三位串,其中,所述量子装置包括多个量子系统;

安全性测试设备,其被配置为:针对所述量子装置接收的一个或多个所述第二位串中的每一个,使用所述第二位串和所述相关联的第三位串来计算测试统计量;

所述安全性测试设备被配置为至少部分地基于所计算的测试统计量来确定是接受还是拒绝所述相关联的第三位串,并且确定所述多个量子系统是否是近似无信号的;和

两源提取器,其被配置为:如果所述安全性测试设备接受所述相关联的第三位串,则接收基于一个或多个所述第一位串的串和基于一个或多个所述相关联的第三位串的位串,并生成所述随机位串。

2.根据权利要求1所述的系统,其中,所述量子装置包括光学设备。

3.根据权利要求1所述的系统,其中,所述多个量子系统包括2个或4个量子系统,其中,所述2个或4个量子系统中的每一个包括量子位。

4.根据权利要求3所述的系统,其中,每个量子系统包括测量装置,所述测量装置被配置为对所述量子位执行测量并且输出包括测量结果的位。

5. 根据权利要求1所述的系统,其中,所述安全性测试设备被配置为计算:

第一测试,在所述第一测试中,测量对贝尔不等式的违反;和

第二测试,用于确定所述多个量子系统是否是近似无信号的;并且响应于所述贝尔不等式的违反而接受所述相关联的第三位串并且确定所述多个量子系统是近似无信号的。

6.根据权利要求1所述的系统,其中,所述弱随机性源和所述量子装置被配置为提供:

量子生成器,其被配置为生成一对纠缠的粒子a和a';

第一状态扩展设备,其被配置为生成包括a和b的纠缠状态;

第二状态扩展设备,其被配置为生成包括a'和 b'的纠缠状态;并且

所述安全性测试设备被配置为提供:第一测量设备,所述第一测量设备被配置为执行与ab或$a'b$或ab'或$a'b'$的双重重合有关的重合测量;和第二测量设备,所述第二测量设备被配置为测量对贝尔不等式的违反;并且

所述两源提取器被配置为接收来自所述第二测量设备的输入并为所述随机位串输出随机位。

7.一种用系统生成随机位串的方法,其特征在于,所述方法包括:

配置弱随机性源,以重复地生成第一位串和第二位串,在一个情形中生成的所述第一位串和所述第二位串不必定具有与在另一情形中生成的所述第一位串和所述第二位串相同的值;

配置量子装置,以接收一个或多个所述第二位串,并且针对所述量子装置接收的一个或多个所述第二位串中的每一个而输出相关联的第三位串,其中,所述量子装置包括多个

量子系统;

配置安全性测试设备,以针对所述量子装置接收的一个或多个所述第二位串中的每一个,使用所述第二位串和所述相关联的第三位串来计算测试统计量;

配置所述安全性测试设备,以基于所计算的测试统计量来确定是接受还是拒绝所述相关联的第三位串,并且确定所述多个量子系统是否是近似无信号的;和

配置两源提取器,以:如果所述安全性测试设备接受所述量子装置的输出,则接收基于一个或多个所述第一位串的串和基于所述相关联的第三位串的串,并生成所述随机位串。

8.根据权利要求7所述的方法,其中,所述方法包括配置所述安全性测试设备,以从所述测试统计量计算贝尔不等式,从而基于所计算的测试统计量来确定是接收还是拒绝所述相关联的第三位串。

9. 根据权利要求8所述的方法,其中,所述贝尔不等式包括CHSH(Clauser Horne Shimony Holt)不等式。

10.根据权利要求7所述的方法,其中,所述量子装置包括光学设备。

11.根据权利要求7所述的方法,其中,所述多个量子系统包括2个或4个量子系统,并且其中,所述2个或4个量子系统中的每一个包括量子位。

12.根据权利要求11所述的方法,其中,所述方法包括配置所述量子装置以包括测量装置,从而对所述量子位执行测量并且输出包括测量结果的位。

13. 根据权利要求7所述的方法,其中,所述方法包括配置所述安全性测试设备以计算:

第一测试,在所述第一测试中,测量对贝尔不等式的违反;和

第二测试,用于确定所述多个量子系统是否是近似无信号的。

14.根据权利要求7所述的方法,其中,所述方法包括:

配置所述弱随机性源和所述量子装置以提供:

量子生成器,其被配置为生成一对纠缠的粒子a和a';

第一状态扩展设备,其被配置为生成包括a和b的第一纠缠状态; 和

第二状态扩展设备,其被配置为生成包括a'和 b'的第二纠缠状态;

配置所述安全性测试设备以提供第一测量设备,所述第一测量设备被配置为执行与ab或$a'b$或ab'或$a'b'$的双重重合有关的重合测量;和第二测量设备,所述第二测量设备被配置为测量对贝尔不等式的违反;和

配置所述两源提取器以接收来自所述第二测量设备的输入并为所述随机位串输出随机位。

放大、生成或证明随机性

[0001] 相关申请的交叉引用

[0002] 本申请要求于2017年12月19日提交的申请号为US 62/607,719标题为“用于放大、生成或证明随机性的系统和方法(Systems and Methods for Amplifying,Generating,or Certifying Randomness)”的美国临时专利申请的优先权权益,其全部内容通过引用并入本文。

背景技术

[0003] 在计算机安全中使用的加密和认证使用随机位生成器,因为随机数在生成构成加密和认证过程一部分的对称密钥和新鲜值(nonces)中很重要。生成随机位序列的方式典型地分为三种不同的类型,包括:确定性随机位生成器,其使用软件生成伪随机位序列;基于经典物理学的不确定性随机数生成器;以及基于量子系统的不确定性随机数生成器。

发明内容

[0004] 以下是本公开的高级概述,在某些方面进行了简化,作为稍后提出的更详细描述的序言。该概述并非旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用于限制要求保护的主题的范围。

[0005] 在一个实施例中,一种安全性测试逻辑系统具有被配置为存储来自测量设备的测量值的非暂时性存储器,该测量输出包括是否存在重合的指示,其中在重合时,基本上同时在多于一个的检测器处检测到粒子,检测器位于与粒子源不同的通道的端部处,并且具有基本相同的长度。该系统包括处理器,该处理器被配置为由所存储的测量值来计算测试统计量。测试统计量可以表示贝尔不等式,并且系统可以将测试统计量与阈值进行比较。处理器可以被配置为如果所计算的测试统计量的值例如低于阈值则生成并输出证明测量值来自量子系统的凭证凭证。贝尔不等式可以包括用于确定一组测量值是否符合量子力学或符合经典物理学的任何不等式。Bell不等式包括Bell原始不等式、CHSH不等式(Clauser Horne Shimony Holt不等式)或任何其他此类不等式中的任何一种。违反Bell不等式表明该测量值符合量子力学规则并且符合经典物理学规则。

[0006] 通过参考以下结合附图考虑的详细描述,将更好且更容易地理解许多随附的特征。

附图说明

[0007] 根据参照附图阅读的以下详细描述,将更好地理解本说明书。

[0008] 图1是用于证明已经由量子装置产生了数的装置的示例以及被配置为生成用于各种下游应用的随机数的随机性提取器的示例的示意图。

[0009] 图2A是可以在图1的装置中使用的四设备量子装置的示例的示意图。

[0010] 图2B是图2A的四设备量子装置的另一示意图。

[0011] 图2C是诸如图2A或图2B所示的四设备量子装置的示例性操作方法的流程图;

[0012] 图3A是可以在图1的装置中使用的两设备量子装置的示例的示意图。

[0013] 图3B是可以在图1的装置中使用的两设备量子装置的示例的另一示意图。

[0014] 图3C是诸如图3A或图3B所示的两设备量子装置的示例性操作方法的流程图。

[0015] 图4是在四设备情况下的示例性安全性测试A的流程图。

[0016] 图5是示例性安全性测试B的流程图。

[0017] 图6是在两设备情况下的示例性安全性测试A的流程图。

[0018] 图7是诸如在图1的布置中的随机性提取器的示例性操作方法的流程图。

[0019] 图8是光学状态扩展器的波导的示例的立体视图。

[0020] 图9是安装在壳体中且省略盖子的图8的波导的立体视图。

[0021] 图10是通过图8的波导的示意性纵向截面。

[0022] 图11A是解释图8的波导的操作的示意图。

[0023] 图11B与图8相同,但以附图标记表示气隙。

[0024] 图12是可以在图2A的装置中使用的一对示例性测量设备的示意图。

[0025] 在附图中,相同的附图标记用于表示相同的部分。提供的附图不一定按比例绘制,并且被提供以示出本文描述的示例性实施例,并且不旨在限制本公开的范围。

具体实施方式

[0026] 以下结合附图提供的具体实施方式旨在作为对本示例的描述,而并非旨在表示构造或利用本示例的唯一形式。该描述阐述了示例的功能以及用于构造和操作示例的操作顺序。然而,可以通过不同的示例来实现相同或等同的功能和序列。

[0027] 随机位具有太多应用,无法枚举,从密码学到科学计算。但是,传统的随机数生成器基于确定性的经典物理学。因此,在没有另外的假设的情况下,就无法信任输出的随机性,因为表观上的随机性是基于可能没有被对手分享的无知(ignorance)。由于这种原因,由任何种类的确定性软件生成的随机数原则上都容易受到黑客的攻击。量子力学本质上是概率性的,因此可以用来生成随机性。利用量子力学生成随机数可允许基于一种基于不确定性原理的安全性;例如,在正确的条件下,在量子位(qubit)没有被立即摧毁的情况下,对手可能无法观察到量子位。

[0028] 当考虑一种据称基于量子力学产生随机输出的设备时,只有当人们信任或假定量子设备在正确运行时,人们才可以相信该输出是随机的。一旦系统已经生成了随机数,通常就没有简单的方法来证明该随机数已经由量子系统产生。为了确定所谓的量子系统是否实际上利用了量子现象来产生其输出,操作人员通常不仅需要是该领域的专家,而且还需要目视检查所谓的量子系统的内部结构(包括机械装置)并且甚至独立地测试系统。

[0029] 以下描述的实施例不限于解决用于放大、生成或证明随机性的已知技术中的任何或全部的缺点的实施方式。例如,不同的实施例可以解决与放大、生成或证明随机性有关的不同的缺点或挑战。

[0030] 尽管存在产生所谓的随机位商业化的量子系统,但即使对于能够访问该设备的内部工作的专家而言,要验证这种设备正按预期工作仍将是困难的任务。那么将更优选的是,在不了解设备的内部工作的情况下,仅通过考虑输出就可以将设备的输出验证为真实的。此特性称为设备独立性。

[0031] 在以下详细的描述中,描述了随机性放大过程的各种非限制性示例以及实现该过程的示例的现实世界系统的各种实施例。这些示例和实施例旨在示例而不是限制本公开的范围。

[0032] 图1是用于证明量子装置102已经以独立的方式产生了数的装置100的示例以及被配置为生成用于各种下游应用120、122、124、128中的随机数116的示例随机性提取器110的示意图。随机性提取器接收来自弱随机性源114(这里和在图中表示为WSR-2)的输入,弱随机性源114可以是用于计算伪随机数的经典装置。另外,装置100还具有弱随机源104(这里和在图中表示为WSR-1),其可以是用于计算伪随机数的经典装置。

[0033] 弱随机性源是指由于或基于量子效应的存在而无法证明随机性的随机性源。术语"弱"本身并不意味着随机性源在某种程度上不适合或不足以满足随机性的行业标准。在一些实施方式中,弱随机性源可以是至少部分不确定的,或者甚至是完全不确定的。因此,弱随机性源包括输出无法证明的不确定性随机数的源。弱随机性源有时简称为随机性源。

[0034] 量子装置102包括用于生成多个量子位并准备处于特定量子态的量子位的装置,以及用于以至少两个不同基准中测量量子位的设备。装置100具有安全性测试逻辑106,用于自动证明给定的多个量子位测量值108违反了Bell不等式。

[0035] 如本文中所使用的,Bell不等式通常是指与量子或经典系统的测量相关联的任何不等式,其中违反该不等式意味着该测量值符合量子力学的规则(例如,纠缠或非局域性)而不符合经典物理学的规则(例如,局域实在论或隐变量)。Bell不等式包括始终由两方的测量结果的任一局部概率分布满足的不等式,其是当每一方的设备具有其自身的内部状态时可以实现的不等式。Bell不等式包括约翰·斯图尔特·贝尔(John Stewart Bell)推导的任何原始不等式以及其他人推导的不等式,例如CHSH不等式(Clauser Horne Shimony Holt不等式)、Leggett不等式、Leggett-Garg不等式等。如本文进一步描述的,对Bell不等式的违反保证了量子装置102的输出是来源于量子效应,并且因此独立于其他源,包括例如经典的弱随机性源。

[0036] 证明量子位测量值108违反了Bell不等式,表明量子位测量值是已经由于量子效应而不是经典效应而产生了,并且还表明量子位测量值108独立于与任何其他经典的弱随机性源,例如图1中的WSR-2 114和WSR-1 104。在这个意义上,证明来自量子效应已经产生了量子位测量值108证明了量子位测量值108是真正随机的。该证明允许用户信任输出的随机性而无需访问量子装置102的内部(因此,例如,无需安排专家来检查量子装置102的内部结构并对其进行测试)。

[0037] 可以使用以下一项或多项的任意组合来实施安全性测试逻辑106:软件、固件或硬件逻辑组件。例如但不限于,可选择使用的示例性类型的硬件逻辑组件包括现场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、系统级芯片系统(SOC)、复杂可编程逻辑设备(CPLD)、图形处理单元(GPU)、中央处理单元(CPU)或任何其他类型的硬件处理器。

[0038] 在图1所示的实施例中,量子位测量值108的集合具有可能不适合在下游应用120、122、124、128中使用的固定尺寸。因此,在一些实施例中,使用随机性提取器来计算多个适当的尺寸/长度。一旦获得多个量子位测量值108并证明其是由量子效应产生的,则将测量值108输入到随机性提取器110。可以使用经典的随机性提取器,例如Trevisan提取器。在一

些这样的实施例中,随机性提取器110将来自弱随机性源114的伪随机数112以及经证明的量子位测量值108作为输入。随机性提取器计算可以是任何指定长度的数作为输出。与伪随机数112相比,由随机性提取器110产生的数具有放大的随机性,并且是真正随机的,因为如以下更详细解释的,随机性提取器的输入被证明是相互独立的。

[0039] 在一些实施例中,具有放大的随机性的数116被输入到一个或多个下游应用。下游应用示例的非穷举列表包括:计算机安全120,其中随机数通常用作在实体之间预先共享并用于加密的一次性密钥(OTP);气象预报122,其中有时生成随机数并将其用于初始化天气系统模型的参数值;电信系统124,其中有时生成随机数并将其用于资源分配方案;以及制造控制系统128,其中有时生成随机数并将其用于对传感器读数中存在的噪声建模。

[0040] 根据诸如Santha和Vazirani于1986年在计算机与系统科学学报,33,I(1):75-87中"从微随机源生成准随机序列(Generating quasi-random sequences from slightly-random sources)"得出的结果,随机数生成的经典方法典型地假设访问两个独立的随机源,并使用随机性提取器来计算接近理想的随机位。但是,两个随机性源是独立的主张通常必须依赖进一步的假设。这是这种经典方法的主要缺点之一;通常不可能保证两个弱随机性源是独立的,因此这种经典方法不是独立于设备的。

[0041] 相反,本技术能够保证量子装置102与WSR-2,即经典的弱随机性源114的独立性。对Bell不等式的违反保证了量子装置102的输出是来自量子效应,并因此独立于包括WSR-2(即经典的弱随机性源114)的其他源。因此,随机性提取器110从被证明是不相关源的两个源中获取输入。从该意义上,随机性提取器的输出信号116是真正随机的。

[0042] 商业化的量子随机性生成器迄今尚未显示出可证明的设备独立性,因为操作人员需要检查随机性生成器并确认其正在使用量子力学。这样的设备使用量子准备和测量方案来利用量子力学的操作概率性质来创建随机数串,该串在许多方面都比经典的伪随机数生成方法更可取。商业化的量子随机性生成器在单个量子背景中以使其不适用于与独立于设备的实现的方式来执行测量。现有的量子随机性生成器无法保证任何安全性,并且即使对于专家而言,要验证设备正按规定工作也可能很困难。例如,在某些以前开发的基于光子学的系统中,鉴于在光子入射到检测器上时对光子系统的测量破坏光子,因此很难验证所报告的测量结果是真实的:在无法保证所报告的测量结果是来自量子效应引起的,该设备可能会产生对手已知的预先生成的、但显然是随机的位串。

[0043] 许多现有的基于量子的随机性生成器提供了安全性保证,其中只有在每轮测量之后丢弃设备,或者仅当并行使用大量设备(随产生的随机位的数目而增加)时,该保证才是有效的。这些方法对商业设备来说不是好的选择。

[0044] 许多现有的量子随机性生成器不能容忍来自可行的量子设备的实际噪声水平,因此对实际应用来说不是好的选择。

[0045] 装置100的一个有利方面是其对噪声的鲁棒性:仅当构成该量子设备的量子态和量子测量值具有低水平的噪声时,安全性测试逻辑才能正确地工作(并且不会中止)。特别地,即使量子装置102的不同量子系统仅是大致无信号(non-signaling)而不是严格地无信号,装置100也能够操作并证明其输出。在单个设备中实施严格地无信号的量子系统不太可能。

[0046] 在该文件中描述的四设备和两设备量子装置102的各种实施例在其设计和应用方

面是独特的。他们使用量子系统来获得使用经典源不可行的结果。本文描述的实施例对于实际的日常使用是现实可实现的。实施例使用小的固定数量的量子设备，并且能够容忍量子设备中的实际噪声水平。另外，量子态是由仅需几个门且具有低电路深度的量子电路产生的。

[0047] 能够生成真正随机性并且还能够以独立于设备的方式证明其正按预期工作并产生随机位的装置100在对手对随机位攻击的可能性极小的任何环境中提供了相对于弱随机性源的独特优势。另外，出于金融行业中的法律原因，证明随机数的能力也很重要。当使用蒙特卡洛模拟模型来计算预测时，通常必须将当前使用的最初伪随机种子提交给监管机构，但是以前没有有效的方法来证明这些种子确实是随机选择的，并且例如没有被选择来以特定方式影响结果。本装置100产生所需的随机位以及量子效应的存在的凭证108，并且在这种意义上还产生真正随机性的凭证。我们描述了使用量子力学系统将任何弱随机性源放大成几乎理想的随机性源的过程的各种非限制性示例。该过程具有以下关键的区别特征：

[0048] 装置102的好处是设备独立，这意味着用户不必信任设备的内部工作。这是因为对设备的输入/输出执行统计测试的安全性测试逻辑向用户证明输出位108、116确实是随机的。除了提供随机性凭证之外，装置102在输出位108、116对于用户以外的任何人都是未知的意义上是额外安全的。装置100给出的安全性或正确性不依赖于任何计算复杂性假设，并且至少在这种意义上是无条件的。用于证明装置100的某些实施例的正确性和安全性的唯一假设是，从设备到非信任方(例如窃听者)不能有任何信令。在适当情况下，可以通过屏蔽设备来保证这一点。与早期的设备独立的随机性产生的工作形成鲜明对比，设备100避免了在设备的不同方之间进行无信号假设的需要。这是通过引入新的测试(安全性测试B)来实现的，即使当各个量子系统仅是大致无信号时，该测试也可通过。该设备可选地与经典随机数生成器或经典伪随机生成器一起使用。由于输出位完全独立于宇宙中的任何其他随机性源，因此可以选择将它们用作经典随机性提取器的种子，以生成更大的随机位序列。这允许明显更高的位速率。

[0049] 装置100在最终位串的长度上以大约线性运行时间操作。在各种示例中，该装置使用2个或4个分离的(大致无信号的)量子设备来产生任意数量的随机位。

[0050] 图2A是用作图1的量子装置102的示例四设备量子装置的示意图。也可以使用两设备的量子装置(例如，参见图3A)作为图1的量子装置102。本实施例中的四设备量子装置的优点在于，它可以可靠地抵御对手使用Popescu-Rohrlich(PR)盒和局部分布的凸混合物的攻击，而两设备量子装置则不是这样。在至少一些实施例中，四设备量子装置使用比两设备量子装置更简单的安全性测试。而且，在至少一些两设备实施例中，与在至少在一些四设备实施例的四设备量子装置中相比，两设备量子装置准备量子位进入不同的量子态。在至少一些两设备实施例中，两设备量子装置给出可被证明为是来自量子效应的传感器测量值，其中量子力学的正确性被假定为用于计算证明的过程的公理。在至少一些四设备实施例中，凭证的有效性不依赖于量子力学作为公理的正确性。

[0051] 参考图2A中所示的示例实施例，有用于发射量子位的能量源200，并且有从能量源200接收输入的四个量子系统202、204、206、208。每个量子系统包括一个状态扩展器210，该状态扩展器210使量子位准备进入指定的量子态。每个量子系统包括以一个或多个测量基

础检测量子位的测量设备212。测量设备212的测量基础可以由驱动器216根据弱随机性源218生成的测量设备设置的伪随机值来配置。测量设备212经由相应的状态扩展器210检测从源200接收的量子位。

[0052] 源200产生成对的量子位,每对量子位沿不同的通道发送。通道可以包括从源200穿过状态扩展器210到测量设备212中的检测器的路径。这些路径的长度基本相同,从而量子位沿着每个路径行进所花的时间基本相同。

[0053] 在测量设备212中的检测器处检测到来自每个路径的出现信号,并且识别重合(coincidences)。重合可以包括基本上同时在多于一个的检测器处检测到量子位。例如,重合可以包括在指定时间段内在两个或更多个检测器处检测到量子位。指定的时间段可以至少部分取决于由源200产生的成对的量子位的通量。指定的时间段可倾向于与通量成反向关联,例如,当成对的量子位的通量较大时(例如,每单位时间可能有很多检测),指定的时间段可以更短,并且当成对的量子位的通量较小时(例如,每单位时间可能有较少的检测),指定的时间段可倾向于更长。在一些实施例中,指定的时间段在从约1ns到1μs、从1μs到1ms、从1ms到0.1s的范围内,或者在其他范围内。例如,时间段可以在5到15ns的范围内,例如大约10ns。

[0054] 在一些实施例中,其中检测到量子位的事件由1(一)表示,而未检测到量子位的事件由0(零)表示。以这种方式,测量设备212生成包括位串的输出信号214。然而,使用二进制表示不是必需的,并且在一些实施例中,其他表示方法可用于输出信号214。

[0055] 使用安全性测试A 220和可选的安全性测试B来检查输出信号214。在优选实施例中,由于硬件通常比软件或固件更安全,因此使用硬件来实现安全性测试A和B。但是,仅使用硬件来实施安全性测试A和B并不是必需的。

[0056] 安全性测试A通过对违反Bell不等式的测试来检查输出信号214是来自量子效应还是来自经典效应。如果通过了安全性测试A,则证明226输出信号214是来自量子效应,并且这个意义上是真正随机的。如果安全性测试A失败224,则没有证明,并且输出信号214被丢弃。因为源200和量子系统202、204、206、208可能受到噪声的影响,所以在量子系统中准备的粒子可能并不总是量子位,且有时可能是经典粒子。因此,安全性测试A特别有益,这是因为,除了具有在不需要检查量子系统202、204、206、208的内部的情况下证明输出信号214是否是量子的能力之外,它还对噪声具有鲁棒性(因为它是对测量设备的检测器处对粒子检测的许多观察结果进行的统计测试)。

[0057] 安全性测试A涉及监视来自每个通道的出现信号。对于每个检测器,存在量子位从源200到检测器可以沿着的唯一路径或通道,并且路径被布置成基本相同的长度,使得状态叠加中的纠缠量子位将同时到达检测器中的多个指定的检测器。路径被配置为仅接受特定偏振和/或模式下的量子位。通过比较粒子在检测器处检测到粒子的次数,可以推断出粒子是否是具有纠缠和叠加的量子位,或者粒子是否是经典的。更正式地说,在至少一些实施例中,安全性测试A包括通过观察在不同的检测器处检测到粒子的次数来测量对Bell不等式的违反。

[0058] 现在将在接下来的几段中描述一些四设备实施例,而不在每个步骤处重复诸如“在一些实施例中”的短语。四个量子系统202、204、206、208是四个空间上分开的各方,具有测量设置$\{u_1,u_2,u_3,u_4\}$和相应的结果$\{x_1,x_2,x_3,x_4\}$。四个量子系统中的每一个都有一个特

定的二维希尔伯特子空间,其服从量子控制;每个系统能够存储一个量子位。量子位及其测量设备的物理实现遵循包括线性光学、离子阱和超导量子位的许多可能的设计之一。

[0059] Bell不等式包括对于两方的测量结果的任何局部概率分布总是满足的不等式,当每一方的设备具有其自己的内部状态时可以实现这一不等式。此状态可能与另一方保持的状态相关,但是它们拥有的每个系统都有其自己单独的描述,而无需整体描述这对系综(ensemble)。这意味着从原理上讲,通过测量一个子系统所发现的表观随机性可以被认为是源于对子系统事实上处于何种状态的无知。但是,量子力学中的纠缠状态会产生非局部的概率分布。由于这种分布不能被认为是由对每个子系统处于何种状态的无知引起的,因为根本不能说子系统事实上处于任何状态:必须对状态进行整体描述。这为真正随机性的可能性打开了大门,因此,本技术试图测量对Bell不等式的违反,以便能够证明随机位被输出为来自测量设备的测量。虽然不可能经典地违反Bell不等式,但对于特定选择的测量,可以发现纯纠缠的量子态没有任何漏洞地违反其中一个。

[0060] 安全性测试B是可选的,并且其检查量子系统是否是无信号的(即,量子系统202、204、206、208不会相互影响)。安全性测试B在安全性测试A之后执行,因为安全性测试B与量子系统的在其作为量子系统运行时的无信号性质有关,而与由于噪声而经过量子系统的任何经典粒子无关。安全性测试B包括使用测量设备212进行重复测量,以及进行测试以查看测量结果是否在量子系统之间相关,即使在以在测量设备之间部分相关的方式设置测量基准的情况下。

[0061] 图2B是图2A的四设备量子装置的另一示意图。四个状态扩展器被描绘为框210,并且这些框接收作为输入的由正方形内部的圆表示的量子粒子。每个状态扩展器210均附接到测量设备212。

[0062] 一种在图2B的四设备量子装置处的操作方法包括:在操作A中,通过准备状态扩展器中的量子粒子的状态,使附接到每个测量设备的状态扩展器相互作用。这在图2B中由框210周围的虚线表示。这可以是概率性的相互作用而不是确定性的相互作用,在这种情况下,准备状态的过程不具有固定的长度。

[0063] 在操作B中,一旦准备了正确的纠缠量子态,就将输入U_i提供给四个测量设备,并测量量子系统。输入U_i是使用弱随机性源选择并且用于在测量设备212处设置测量基准的测量设置。如图2B中的符号X_i所示的测量结果由测量设备212输出(操作C)。

[0064] 重复图2B中所示的操作A至C。输入U_i和输出X_i之间的框之间没有相互作用。请注意,在操作A和操作B之间,系统处于无法被描述为由其子系统的各个状态组成的状态:因此,系统在操作A和操作B之间被整体描述。

[0065] 图2C是图2A与图2B的四设备量子装置的操作方法的流程图。在诸如四个量子系统的多个量子系统中生成230量子位。例如,如以下等式3所示,以指定的纠缠量子态准备232量子位。这可以使用状态扩展器来完成。准备四个量子位,因而它们相互作用,以便为设备产生指定的量子态,其是称为纠缠状态的类型的量子态。这利用了二量子位相互作用和单量子位相互作用这两者。使用来自弱随机性源的输入来配置234测量设备的设置。弱随机性源用于为每个测量设备212独立配置设置。这些设置是从操作方法中使用的测量基准中得出的。例如,弱随机性源可以用于为四个测量设备212中的每一个从两个测量基准(例如,计算基准和Hadamard基准,其可以各自具有两个基本状态或基本向量)中选择测量设置。测量

设置用于配置234测量设备的设置。四个量子位中的每一个均根据其测量设置进行测量。根据量子设备的精确实现,这可能包括对检测器的设置进行更改或对测量设备的通道上的量子位进行转换。然后,测量量子位。值得注意的是,这有效地破坏了量子态。然后,检测器将输出包含测量结果x_i的位,然后开始下一轮测量。在一个示例中,设置包括两个可能的正交偏振(例如水平和竖直)和两个可能的量子位模式。一旦配置了这些设置,测量设备中的检测器开始感应在从源到每个检测器的路径上接收的检测到的粒子。测量过程236在测量时产生测量结果,将测量结果与测量设备的设置的相关值一起存储238。检查240是否重复以获得更多测量结果。该检查包括检查标准,例如是否经过了指定时间,是否经过了指定数量的测量迭代或存储测量结果的存储器是否已满。一旦在操作240处的检查指示不需要进一步的重复,则输出242存储的测量结果。

[0066] 现在给出至少某四个量子设备实施例的其他细节。

[0067] 考虑由以下给出的测量设置的两个串:

[0068] U_0={{0001},{0010},{0100},{1000}}和

[0069] U_1={{0111},{1011},{1101},{1110}},

[0070] 其中,U_0是四种可能的测量设置的集合,并且U_1是四种可能的测量设置的不同集合。

[0071] 该实施例中使用的Bell不等式如下:

[0072] $$\boldsymbol{B}\cdot\{P(\boldsymbol{x}|\boldsymbol{u})\}=\sum_{\boldsymbol{x},\boldsymbol{u}}B(\boldsymbol{x},\boldsymbol{u})\,P(\boldsymbol{x}|\boldsymbol{u})\geq 2, \qquad (1)$$

[0073] 其中,B是Bell不等式的指标向量,且P(x|u)是结果或测量值x给定输入或测量设置值u的条件概率分布。

[0074] 在一些实施例中,B是具有$2^4\times 2^4$个条目的指标向量:

[0075] $$B(\boldsymbol{x},\boldsymbol{u})=\mathbb{1}_{\oplus_{i=1}^{4}x_i=1}\mathbb{1}_{\boldsymbol{u}\in U_0}+\mathbb{1}_{\oplus_{i=1}^{4}x_i=0}\mathbb{1}_{\boldsymbol{u}\in U_1} \qquad (2)$$

[0076] 其中,如果表达式E为真,则指标函数$\mathbb{1}_E$等于1,否则等于0。

[0077] 在一些实施例中,Bell不等式指标函数B使用其条目分别为零或一的16×16阵列或矩阵来实现。阵列的列代表检测器的可能配置,阵列的行代表在检测器处的可能观察。在一些实施例中,由于存在四个测量设备,每个测量设备具有四个检测器,所以存在16种可能的检测器配置。代替阵列或矩阵,还可以使用许多其他的数据结构,例如位图、哈希表、查找表或搜索树。在一些实施例中,允许快速搜索或查找的数据结构是优选的,因为在一些实施例中,阵列或数据结构被用作查找机制,其中四个输入位和四个输出位的组合被有效地用作关键字来查找Bell不等式指标函数的值。

[0078] 阵列的示例被给出如下:使设备的四个输入位为$V_1,\ldots,V_4$和四个输出$S_1,\ldots,S_4$。然后函数B(V,S)被定义为如下,其中⊕表示XOR(排斥或)操作:

[0079] $$B(\boldsymbol{V},\boldsymbol{S})=\begin{cases}0 \text{ 如果 } \boldsymbol{V}\in U_0 \text{ and } S_1\oplus S_2\oplus S_3\oplus S_4=0\\ 1 \text{ 如果 } \boldsymbol{V}\in U_0 \text{ and } S_1\oplus S_2\oplus S_3\oplus S_4=1\\ 0 \text{ 如果 } \boldsymbol{V}\in U_1 \text{ and } S_1\oplus S_2\oplus S_3\oplus S_4=1\\ 1 \text{ 如果 } \boldsymbol{V}\in U_1 \text{ and } S_1\oplus S_2\oplus S_3\oplus S_4=0\\ \text{否则 } 0\end{cases}$$

[0080] 其中,U_0和U_1如上所定义。虽然有检测器设置的值的16种可能组合,但是为清楚起见在该示例中仅使用8种。如果函数B(V,S)被实施为阵列或矩阵,则检测器设置中的剩余8个值可以用零填充。

[0081] 使V^i和S^i为协议的第i轮的输入/输出的向量。安全性测试将计算:

[0082] $$B'=\frac{1}{n}\sum_{i=1}^{n}B(\boldsymbol{V}^i,\boldsymbol{S}^i)$$

[0083] Bell不等式指标向量的使用提供了一种有效且准确的方式来评估在检测器处观察到的重合。如果在同一测量设备中不同通道上的检测器处观察到重合,则该重合为经典噪声。如果在一对测量设备的不同测量设备中的检测器处发现重合,则该重合来自量子效应。安全逻辑使用阵列(或类似数据结构)和观察到的重合来执行重合评估,以查看对于每个可能的配置设置的结果是否均小于2。由于存在16种可能的配置设置,因此安全逻辑将寻找小于八分之一(即2除以16)的重合评估结果。

[0084] 该协议中使用的量子态为:

[0085] $$|\Psi\rangle=\frac{1}{\sqrt{2}}\left(|\phi_-\rangle|\tilde{\phi}_+\rangle+|\psi_+\rangle|\tilde{\psi}_-\rangle\right) \qquad (3)$$

[0086] 其中,

[0087] $$|\phi_-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle)$$

[0088] $$|\psi_+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)$$

[0089] $$|\tilde{\phi}_+\rangle=\frac{1}{\sqrt{2}}(|0\rangle|+\rangle+|1\rangle|-\rangle)$$

[0090] $$|\tilde{\psi}_-\rangle=\frac{1}{\sqrt{2}}(|0\rangle|-\rangle-|1\rangle|+\rangle)$$

[0091] 其中,在至少一些实施例中,{|0>,|1>}是计算基准(有时称为标准基准),并且在至少一些实施例中,{|+>,|->}是由$|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$和$|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$给出的Hadamard或Fourier基准。

[0092] 在该示例中的量子态|Ψ>是两个量子态($|\phi_-\rangle|\tilde{\phi}_+\rangle$和$|\psi_+\rangle|\tilde{\psi}_-\rangle$)的均匀线性组合,这两个量子态是两个量子位的最大纠缠状态。有几种产生状态|Ψ>的方式。例如,一种

可能性是实施将直积态|0>|0>|0>|0>映射到|Ψ>的量子幺正。为了实施该示例幺正,可以使用Solovay-Kitaev构造将其分解为更简单的一量子位幺正和两量子位幺正。

[0093] 输入u_i=0对应于X基准(或Hadamard或Fourier基准)上的测量,而输入u_i=1对应于Z基准(或计算基准)上的测量(对于输入i∈{1,2,3,4}中的每个)。为了测量Z基准,例如,可以首先应用旋转到Hadamard或Fourier基准的单量子位幺正,然后在计算基准上测量。在理想条件下,使用这种纠缠状态和量子测量的上述贝尔测试的实施给出B·{P(x|u)}=0。

[0094] 现在参照图4正式描述用于四量子设备实施例的安全性测试A。

[0095] 来自弱随机源w_2的串用于选择上述贝尔实验中的测量值输入;例如,对于实验的n次实现中的每次来说,可以使用来自w_2的4位来选择$(u_i)_j$,j范围从1到n。然后收集输出$(x_i)_j$,这些输出连在一起形成串w_3。根据串w_3中输出的值来计算400测试统计量。统计测试包括计算函数:

[0096] $$L_n \equiv \frac{1}{n}\sum_{j=1}^{n} B(\boldsymbol{x}_j, \boldsymbol{u}_j), \qquad (4)$$

[0097] 其可以用文字表示为:测试统计量被计算为测量次数的倒数,乘以为Bell不等式指标向量的、来自16乘16值的阵列(或类似的数据结构)的适当条目的测量次数的总和。使用观察到的测量值和用于观察测量值的检测器设置来查找适当的阵列条目。

[0098] 如果测试统计量L_n的计算值小于阈值b(参见图4中的检查402),则处理过程继续进行404。否则,过程失败406并返回至图2C的操作408。

[0099] 总的来说,除非L_n<b,否则过程中止,其中b是根据初始弱随机源218的质量选择的自由参数;增量越小,协议可容忍的噪声就越小,但另一方面,它可以放大弱随机源的随机性。对于实际的实现,可以选择例如b=0.01,其给出输出随机位,该输出随机位与真正随机位(在变分距离上)相差最多0.0001(其在大多数应用中可以忽略不计)。同时,b=0.01的值意味着即使使用线性光学设备、离子阱和超导系统中达到的准确电流(以约为99.2%的精确度测量),也可以成功运行协议。在另一个实施例中,b=0.125和针对其测试的Bell不等式是上面的方程1。但是,在某些情况下,其他阈值b可以与上述方程的Bell不等式或其他Bell不等式一起使用。

[0100] 量子力学显示出一种称为无信号的特性,这意味着尽管存在产生非局部概率分布的纠缠状态,但无法利用这种非局部性来提供拥有量子系统的各方之间的即时通信。许多Bell不等式的性质是存在其他物理理论,虽然它们仍遵守无信号原理,但导致比量子力学更大的贝尔违背。CHSH不等式就是一个著名的例子,与为2的经典值相比,它容许为$2\sqrt{2}$的量子最大值;但是,允许实施Popescu-Rohrlich(PR)盒的无信号理论实现为4的值。如果量子力学的正确性不被当作当前技术的附加公理,那么看到CHSH计算值为$2\sqrt{2}$不能被看作完全安全的,因为量子系统可能已被PR盒和局部分布的凸混合物所代替。从理论上讲,这可能导致对手知道29%的随机位。尽管可能不太可能发生此类攻击,但采用四设备程序对抗它们是安全的。这是因为,在一些实施例中,所使用的Bell不等式具有以下特性:不存在任何允许比量子力学更大的违背的无信号理论,因此基于替代物理理论的攻击是不可行的。这是量子可访问的最大非局部性的一个示例;它是逻辑上非局部性的量子可访问的一个示

例。值得注意的是,爱因斯坦的狭义相对论和广义相对论都肯定了无信号原理。因此,在四量子设备装置中使用的方法是通过一般物理原理来保证的,而不是必须依赖于量子力学的绝对正确性。

[0101] 在四量子设备实施例(和二量子设备实施例)中,安全性测试B的示例被正式描述如下:

[0102] 安全性测试B包括检查4个不同的量子系统之间是否近似无信号。为了精确地解释彼此之间无信号的含义,请考虑以输入$u_1,\ldots,u_4$为条件的输出$x_1,\ldots,x_4$的概率分布:

[0103] $p(x_1,x_2,x_3,x_4|u_1,u_2,u_3,u_4)$

[0104] 对于首次使用设置$u_1,\ldots,u_4$且另一次使用u'_2,u'_3,u'_4的任意对的测量设备,并且同样对于成对测量设备的三种其他组合,近似无信号条件表达为:

[0105]
$$\sum_{x_2,x_3,x_4} p(x_1,x_2,x_3,x_4|u_1,u_2,u_3,u_4) \approx \sum_{x_2,x_3,x_4} p(x_1,x_2,x_3,x_4|u_1,u'_2,u'_3,u'_4)$$

[0106] 即,任何测量设备的边缘分布几乎不受其他测量设备中的测量选择的影响(在技术上假定所有边缘的变分距离与某个小误差ε是相同的,小误差ε是测试的参数且在上述讨论的实施例被认为是例如ε=0.02)。弱随机源用于生成$(u_i)_j$,这是其被输入到测量设备以配置检测器设置。测得的输出是$(x_i)_j$。然后,装置基于获得的频率计算经验分布$q(x_1,x_2,x_3,x_4|u_1,u_2,u_3,u_4)$。对于任何$u_1,\ldots,u_4$和$u'_2,u'_3,u'_4$,并且同样对于其他量子系统2、3和4,除非满足以下,否则过程中止:

[0107]
$$\| \sum_{x_2,x_3,x_4} p(x_1,x_2,x_3,x_4 \mid u_1,u_2,u_3,u_4) - \sum_{x_2,x_3,x_4} p(x_1,x_2,x_3,x_4 \mid u_1,u'_2,u'_3,u'_4) \|_1 \leq \varepsilon。 \quad (5)$$

[0108] 总而言之,参考图5,安全性测试B包括使用诸如WSR-1之类的弱随机性源104来配置装置的所有测量设备的装置的测量设置(方框500)。对于502每个测量设备,安全性测试B过程针对测量设备的设置的每种可能配置进行重复地测量504。针对每个测量设备存储506基线直方图,其示出对于测量设置的每种配置的粒子的检测频率。

[0109] 对于测量设置508的每种组合,过程篡改其中一个设置以使其与来自另一测量设备的设置匹配。重复进行测量并将结果存储512在测试直方图中。

[0110] 进行检查514以查看测量设备的任何测试直方图是否与该测量设备的基线直方图显著不同。如果存在显著差异,则采取警报或中止步骤516,因为在测量设备之间存在某种程度的相互作用,其表明它们不是无信号的。否则,过程继续进行518以证明测量设备为近似无信号的。

[0111] 图3A示出了在一些实施例中用作图1的量子装置102的示例性两设备量子装置的示例。在两设备量子装置中,有两个量子系统302、304,每个系统包括状态扩展器310和测量

设备312。量子位的源连接到每个状态扩展器310并产生量子位。量子位行进到状态扩展器310中,并且当量子位行进通过状态扩展器310时,量子位的状态准备进入指定状态。量子位的准备好的状态在下面正式列出。测量设备312每个都包含多个检测器,这些检测器检测量子位,并且可以根据弱随机性源318生成的设置值被配置成一种或多种配置。弱随机性源318生成随机位串(或其他随机数)并将其输入到驱动器316。驱动器316驱动测量设备312中的检测器的配置,以便改变偏振的值和/或检测器的模式的值。

[0112] 所准备的量子位从状态扩展器310行进到测量设备312中。每个测量设备具有粒子能够遵循的多个可能路径。每条路径都从状态扩展器到检测器。这些路径的长度基本相同,因此量子位沿着每个路径行进所花费的时间大致相同。在每个检测器上几乎同时进行测量,并产生输出信号314,在一些示例中,输出信号314为位串的形式,每个检测器一位,其中位为1表示检测到的粒子,0表示未检测到粒子。输出信号314被输入到执行安全性测试A的部件320。部件320从弱随机性源318接收信息,使得部件320知道用于获得输出信号314的测量设备312的配置设置。

[0113] 在一些实施例中,由部件320实施的安全性测试A不同于四设备量子装置的安全性测试A,因为它实施了表示安全性测试C的附加测试。

[0114] 如果安全性测试A通过,则可选地使用部件322执行安全性测试B。在一些实施例中,安全性测试B与以上针对四设备量子装置所描述的相同。输出信号326包括输出信号314和安全性测试A(以及可选地,安全性测试B)已经通过的信息。因此,下游系统具有证明输出信号326是由量子系统生成的信息,因此具有真正随机性。

[0115] 图3B是用于图1的装置中的示例性两设备量子装置的另一示意图。图3B示出了状态扩展器310和测量设备312。将量子位(由正方形内的圆表示)输入到状态扩展器310,并且状态扩展器相互作用,从而使量子位纠缠并重叠放置(由下面给出的两设备装置中的状态扩展器310准备的量子位的状态)。检测器设置u_1和u_2被输入到测量设备312,以根据来自弱随机性源的输入来设置测量设备中的检测器的配置。测量设备测量到达检测器的粒子并输出信号x_1,x_2。

[0116] 在示例性的两设备量子系统的情况下,操作方法与上述示例性的四个装置的设备量子系统的操作方法非常相似。然而,在至少一些实施例中,在操作A中形成的状态是不同的,并且检测器设置在数量和清晰度(definition)上都不同。现在将在接下来的几段中进一步描述一些两设备实施例,而无需在每个步骤中重复诸如“在一些实施例中”的短语。

[0117] 图3A和3B的两设备量子装置涉及测量四个量子位:两个位于两个物理设备中的每一个处(与具有四个物理设备的示例性四设备量子装置不同)。参照图3C,在两设备量子装置处的过程如下:在两个量子设备310内的多个量子系统中生成330量子位。两个量子设备310相互作用以形成纠缠的量子态。如以下方程式10中所定义的,准备332纠缠的量子态。

[0118] 弱随机性源用于为每个测量设备312独立配置设置。这些设置是从操作方法中可用的测量基准中得出的。例如,弱随机性源可以用于为两个测量设备312中的每一个从九个测量基准中选择测量设置。测量设置用于334配置测量设备的设置。

[0119] 在两个测量设备处执行测量336,并且将测量结果与测量基准(设置)的值一起存储338。该过程在操作340处检查是否需要重复,如果是,则该过程从操作330重复。如果在操作340处的检查指示不要重复所存储的测量结果,则输出342相关联的设置。使用诸如以下

一项或多项的标准在操作340处做出是否重复的决定:时间间隔、重复次数、存储的测量结果的数量,用于存储测量结果的可用内存的量。

[0120] 针对Bell不等式检查输出测量结果。如果违反了Bell不等式,则得知输出测量结果来自量子效应,并且将其输入到如参考图1所解释的随机性提取器中。如果满足Bell不等式,则得知输出测量结果来自经典效应,并拒绝该输出测量结果。可选地,完成另一检查(安全性测试B),如下所述。

[0121] 待测试的Bell不等式可以表示为:

[0122] $$B \cdot \{P(\boldsymbol{x}|\boldsymbol{u})\} = \sum_{\boldsymbol{x},\boldsymbol{u}} B(\boldsymbol{x},\boldsymbol{u})\, P(\boldsymbol{x}|\boldsymbol{u}) \geq 4 \qquad (6)$$

[0123] 其中,B是指标向量,包括用于集合S_B的指标函数。指标函数被定义为:

[0124] $$B(\boldsymbol{x},\boldsymbol{u}) = \begin{cases} \text{如果}(\boldsymbol{x},\boldsymbol{u}) \in S_B\ ,\ 1 \\ \text{否则}\ 0 \end{cases} \qquad (7)$$

[0125] 其可以用文字表示为:如果测量值和测量设定值在集合S_B中,则给定测量值x和相关联的测量设置值u的指标函数B的值等于1;否则指标函数的值为零。

[0126] 该集合S_B包括以下18个量子态的集合,这18个量子态在此被表示为非归一化的量子态,该非归一化的量子态被集合到以下表示为M_1到M_9的9个不同的基准中在此示例中,每个通道是一个量子位从源到检测器可以沿着的路径,并且通道的长度基本相同。

[0127]
$$\begin{aligned}
|v_1\rangle &= |0\rangle & |v_2\rangle &= |1\rangle \\
|v_3\rangle &= |2\rangle + |3\rangle & |v_4\rangle &= |2\rangle - |3\rangle \\
|v_5\rangle &= |0\rangle - |1\rangle & |v_6\rangle &= |0\rangle + |1\rangle - |2\rangle - |3\rangle \\
|v_7\rangle &= |0\rangle + |1\rangle + |3\rangle + |4\rangle & |v_8\rangle &= |0\rangle - |1\rangle + |2\rangle - |3\rangle \\
|v_9\rangle &= |0\rangle - |2\rangle & |v_{10}\rangle &= |1\rangle - |3\rangle \\
|v_{11}\rangle &= |0\rangle + |2\rangle & |v_{12}\rangle &= |0\rangle + |1\rangle - |2\rangle + |3\rangle \\
|v_{13}\rangle &= -|0\rangle + |1\rangle + |2\rangle + |3\rangle & |v_{14}\rangle &= |0\rangle + |1\rangle + |2\rangle - |3\rangle \\
|v_{15}\rangle &= |0\rangle + |3\rangle & |v_{16}\rangle &= |1\rangle - |2\rangle \\
|v_{17}\rangle &= |1\rangle + |2\rangle & |v_{18}\rangle &= |3\rangle
\end{aligned} \qquad (8)$$

[0128] $M_1 = \{|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle\}$

[0129] $M_2 = \{|v_4\rangle, |v_5\rangle, |v_6\rangle, |v_7\rangle\}$

[0130] $M_3 = \{|v_7\rangle, |v_8\rangle, |v_9\rangle, |v_{10}\rangle\}$

[0131] $M_4 = \{|v_{10}\rangle, |v_{11}\rangle, |v_{12}\rangle, |v_{13}\rangle\}$

[0132] $M_5 = \{|v_{13}\rangle, |v_{14}\rangle, |v_{15}\rangle, |v_{16}\rangle\}$

[0133] $M_6 = \{|v_{16}\rangle, |v_{17}\rangle, |v_{18}\rangle, |v_1\rangle\}$

[0134] $M_7 = \{|v_2\rangle, |v_9\rangle, |v_{11}\rangle, |v_{18}\rangle\}$

[0135] $M_8 = \{|v_3\rangle, |v_5\rangle, |v_{12}\rangle, |v_{14}\rangle\}$

[0136] $M_9 = \{|v_6\rangle, |v_8\rangle, |v_{15}\rangle, |v_{17}\rangle\}$ (9)

[0137] 因此,当测量设备被配置用于测量基准M_1时,它只能在通道1、2、3和4上接收。当测量设备被配置用于测量基准M_2时,它只能在通道4,5、6和7上接收;并且对于其他测量基准以此类推。

[0138] 对每个可能的测量值的与上下文无关的隐藏变量赋值将意味着对每个向量赋值0和1,以使在每个测量基准中恰好有一个赋值为1的向量。有9个测量基准,因此总共有奇数个1赋值。但是,请注意,每个向量出现在恰好两个测量值中,因此,将对向量的0和1的任意赋值必然导致在测量基准内包含偶数个1。因此,这样的与上下文无关的赋值是不可能的:这被称为情境域(contextuality)证明。请注意,没有必要考虑得到任何测量结果的实际概率,甚至不必考虑到它们的可能性:这是最大的情境域的一个示例,它以状态独立的方式表现其自身。

[0139] 两个测量设备312使全部的九个测量基准M_i对它们可用,并且在它们之间随机选择。这样,对u的估值就存在八十一种不同的可能性,对u的估值表示测量设备设置。如果在u_1中的结果x_1正比于u_2中的结果x_2,则将该对(x,u)定义为在S_B中。选择纠缠状态:

[0140] $$|\Psi\rangle = \frac{1}{2}\sum_{i=0}^{3} |i\rangle \otimes |i\rangle \qquad (10)$$

[0141] (其可以用文字表达为:以下总和的一半:|0>与其自身的张量积加上|1>与其自身的张量积加上|2>与其自身的张量积加上|3>与其自身的张量积;|i>可以表示通道i)上的一个量子位)得到集合S_B中的每个测量结果是不可能的,从而Bell不等式的左侧为0(例如,上面的方程式6)。因此,相对于该组无信号物理设备的集合存在最大量的非定域性。

[0142] 现在参照图6描述用于两设备量子装置实施例的安全性测试。通过在操作600处计算测试统计量L_n来完成安全性测试A。安全性测试A与以上参考四设备量子装置实施例所描述的相同。如果在检查602处测试统计量L_n低于阈值,则过程继续进行到安全性测试C,从而计算610测试统计量$S_n(x,u)$。使用数学符号描述安全性测试A,该装置计算由以下定义的测试统计量:

[0143] $$L_n \equiv \frac{1}{n}\sum_{j=1}^{n} B(\boldsymbol{x}_j, \boldsymbol{u}_j), \qquad (11)$$

[0144] 除非$L_n < b$,该装置中止(参见图6的失败框606)该过程,其中b是针对初始弱随机源318的质量选择的自由参数。在一个实施例中,b=0.125。

[0145] 如果测试统计量L_n小于阈值b,则过程继续进行以执行称为安全性测试C的附加的安全性测试。安全性测试C包括为任何固定的测量设置u^*将随机变量定义为$D(x_j,u_j)$:

[0146] $$D_j^u(x) = D(\boldsymbol{x}_j, \boldsymbol{u}_j) = \begin{cases} \text{如果}(\boldsymbol{x}_j = \boldsymbol{x}^* \wedge \boldsymbol{u}_j = \boldsymbol{u}^*),\ 1 \\ \text{否则 } 0 \end{cases} \qquad (12)$$

[0147] 其中x^*是测量结果,u^*是优先选择的测量设置。用语言表达,如果观察到的测量值等于指定的测量结果并且测量设置是固定的测量设置,则对于观察到的测量值和相应的检测器设置的随机变量D等于1;否则D为零。可以从零和一的数组中查找随机变量的值,其中该阵列具有用于测量设置的每种组合的一列以及用于每个测量值组合的一行。使用与本文档前面所述的四量子系统设备实施例相同的原理填充阵列。和以前一样,也可以使用其他数据结构,例如哈希表。

[0148] 安全性测试C的测试统计量被定义为:

[0149] $$S_n(x,u)=\frac{1}{n}\sum_{j=1}^{n}D(\boldsymbol{x}_j,\boldsymbol{u}_j)$$

[0150] 它可以用语言表达为安全性测试C的测试统计量等于所进行的测量数目的倒数乘以所进行的测量数目对应于观察到的测量值和测量设置的对应值的随机变量D的值的总和。在一些实施例中,如上所述,在提供查找机制的阵列或其他数据结构中查找随机变量D的值。

[0151] 将参数μ固定在大于零(μ>0)的值处,并进行检查612安全性测试C的测试统计量是否大于或等于参数μ的值,其数学表达为$S_n(x,u)\geq\mu$。当测试接受时(例如,安全性测试C的测试统计量大于参数μ的值),这作为测量设备312正在正确地产生输入设置u^*的随机性以及过程继续进行614的保证。但是,如果测试未通过(例如,安全性测试C的测试统计量小于参数μ的值),则过程中止并返回到图2C的操作230,如图6的框608所示。

[0152] 总之,在两设备的实施例中,安全性测试A和C作为Bell不等式的测试。如果这些测试通过,则检测器的测量结果被证明是由量子位而不是由经典粒子产生的。

[0153] 在另一个实施例中,图1的量子装置102可以包括具有四个自由模式的仅两个量子位的量子系统,并且具有测量设备,该测量设备获取针对每个量子系统的仅两个不同的量子测量值。在这种情况下,安全性测试A可以实施CHSH测试。贝尔定理的证明中可以使用CHSH不等式。

[0154] 现在给出关于图1的随机性提取器110的更多细节。通常,随机性提取器110是确定性函数,其获取一个或多个随机位串作为输入,并产生完全随机的位序列作为其输出信号116。一个或多个随机位输入串可以是一串或多串弱随机位(例如,弱随机位串可以具有接近0的偏差,而不是均匀随机的)。不可证明的不确定性随机数是弱随机数的一个示例。通常,除非有两个或更多个源(尽管它们本身可能不是完全随机,但彼此独立),否则随机抽取是不可能的。典型地,这不可能以设备独立的方式实现;然而,本技术证明由测量结果给出的输出串108独立于弱随机数112(由WSR-2、即弱随机性源114提供),该弱随机数112也被发送至随机性提取器110。WSR-2可以看作是Santha-Vazirani源的假设足以证明量子装置102的测量结果108完全独立于直接从WSR-2发送到经典随机性提取器110的弱随机数112。量子噪声的存在并没有弱化这一事实,以致它不再适用:即使考虑到噪声,测量结果也形成极低的最小熵的随机源。

[0155] 这意味着随机性提取器110仅必须在经典设置中操作,对于该经典设置,存在提取真正随机串的已知方法。虽然经典上不可能保证两个输入108、112相对于随机性提取器110的独立性,但是这种保证通过利用量子装置102中纠缠量子系统的非定域测量特性已成为可能。有许多这样的经典随机提取器110,其包括但不限于:冯·诺依曼提取器、混沌机器、加密哈希函数。一个示例是Li的随机性提取器(“两源提取器的改进结构(Improved constructions of two-source extractors)”,Xin Li,2015年8月5日arXiv:1508.01115),它为协议提供了一种实用的选择。其他合适的示例随机性提取器包括如Ma等人“用于量子随机数生成器的后处理:熵评估和随机性提取(Postprocessing for quantum random-number generators:entropy evaluation and randomness extraction)”arXiv:1207.1473v2,2013年6月22日所述的Trevisian的随机性提取器和/或Toeplitz哈希提取器

的实施。

[0156] 图7是诸如在图1的布置中的随机性提取器110的示例性操作方法的流程图。在700处,如果由量子装置执行的测量通过了安全性测试,则由量子装置输出的测量串可证明是由量子效应产生的。测量串可以包括参考图1描述的输出串108。如本文所述,安全性测试可以包括(例如,针对两设备量子装置的)安全性测试A、可选的安全性测试B或安全性测试C中的一个或多个。参见,例如,参照图2A和图3A的安全性测试的描述。在702处,将测量串传递到两源提取器。在704处,两源提取器从第二弱随机性源(例如,WSR-2 114)接收输入。因为安全性测试在700处通过,所以可以肯定地知道,测量串和第二弱随机性源是独立的。两源提取器将这些输入进行组合,并且在706处输出随机数。随机数可以包括如参照图1的输出信号116、图2A的输出信号226或图3A的输出信号326所描述的完全且可证明的随机位序列。

[0157] 到目前为止,在本文中已经使用通用语言对该技术进行了描述,以从量子位、测量、通道、量子态等方面解释了该技术。这是为了强调该技术可在各种不同的物理平台中实施。现在给出适合于实施该技术的三种特定平台。以下三种平台旨在示例而非限制该技术的示例实施。

[0158] 光学器件:

[0159] 在用于量子信息处理的光学系统中,被称为光子的给定模式下的光单位用于表示量子位。通过光学元件(分束器、镜和移相器)的操作用于在量子位上实施量子门。为了准备许多光子量子位的状态,使用完善的光学参量下转换程序。在光学参量下转换中,光束被发送通过非线性晶体,非线性晶体然后输出其偏振(或动量)纠缠的双光子。另一种方法是生成定义明确的量子态的单光子。同样,这可以使用光学元件来完成。可以用于实施一般量子电路的另一个元件是量子门(一个或多个光子的量子态的转换)。基本原理是,使用分束器和/或移相器可以构建任何任意的1量子位幺正操作。对于两个量子位的门,可以像Kerr非线性方案那样使用光学设备(例如,具有Kerr非线性)或使用测量值来模拟非线性。光子的测量可以用包括将光子转换成电流的p-n结的工业制造的光电检测器来执行。

[0160] 在使用光学器件的示例中,通过使用参量下转换产生四对,并检测来自每一对的一个光子以便预示(herald)另一个,来创建四个单独的光子。然后,使用Knill、Laflamme和Milburn的方案“利用线性光学器件进行高效量子计算的方案(A scheme for efficient quantum computation with linear optics)”Nature,409(6816):46-52,使光子相互作用。可替代地,使光子通过具有如Pritchard,Weatherill and Adams的“使用冷Rydberg原子的非线性光学器件(Non-linear optics using cold Rydberg atoms),”Annual review of cold atoms and molecules,1(301),2013所描述的很大三阶非线性磁化率$x^{(3)}$值的非线性光学介质相互作用。如果需要,可以重复进行此操作,直到相互作用的结果为所需状态为止。四个测量设备中的每一个都接收输入位$i\in\{1,2,3,4\}$,它选择特定的测量设置。当每个检测器已接收其输入信号时,其将一个半波片添加到入射光子的路径中,或者不执行任何操作。然后,使用雪崩光电二极管进行测量,并输出结果(已看到光子,或还没有)作为测量结果x_i。在下一轮中将重复这些步骤。

[0161] 离子阱:

[0162] 装置可以是被俘获的原子的线性阵列(例如,通过电磁驻波)。每个离子在两个基态超精细能级中存储一个量子位。超精细量子位的寿命非常长(例如,数千到数百万年的衰

减时间),并且在相位和频率上稳定(因此传统上用于原子频率标准)。使用众所周知的光泵浦的过程,将离子的量子位状态准备成特定的量子位状态。

[0163] 可以如下完成测量。激光被施加到仅一个耦合量子位状态的离子。当离子在测量过程中塌陷到此状态时,激光将激发它,从而使得当离子从激发态衰减时释放出光子。衰减后,离子被激光连续激发并重复发射光子。这些光子可以通过光电倍增管(PMT)或电荷耦合器件(CCD)相机收集。如果离子塌陷到另一个量子位状态,则它不与激光相互作用,也不发射光子。通过计数收集的光子的数量,可以以非常高的精度(例如,大于约99.9%)确定离子的状态。

[0164] 量子门可以如下实施。可以使用用于超精细量子位的磁偶极子跃迁或受激拉曼跃迁和用于光学量子位的电四极跃迁来实现单个量子位门。通过将离子的电子状态耦合到集体分子上可以实现两个量子位门。使用Cirac-Zoller方案,可以生成四个纠缠离子。在Cirac,J.I.、Zoller,P.(1995-05-15)的“具有冷陷获离子的量子计算(Quantum Computations with Cold Trapped Ions)”(Physical Review Letters.74(20):4091-4094)中阐述了Cirac-Zoller方案。

[0165] 在使用离子阱的示例中,产生四个纠缠离子,图2A的量子装置的四个测量设备中的每一个接收输入位u_i,$i\in\{1,2,3,4\}$,其选择特定的测量设置。为了测量存储在离子中的四个量子位中的每个量子位,该装置使用CCD相机对其进行检测(如果$u_i=0$且希望在计算基础上进行测量),或者首先该装置应用激光以将量子位旋转至Fourier基础,然后进行测量用CCD相机测量离子(如果$u_i=1$)。然后,检测器输出包含测量结果x_i的位。在下一轮中重复这些步骤。

[0166] 超导电路:

[0167] 随机性生成协议也可以在超导电路中实施。

[0168] 使用光学系统的量子装置的示例

[0169] 现在参考图8至图12描述详细的实施例,在图8至图12中,使用光学系统来实施量子装置102。以下详细描述旨在示出参考图8至图12描述的实施例,但不限制该装置的范围或设计。

[0170] 常规激光可用于产生光子,其中一些光子是经典的,而另一些是纠缠的量子光子。来自激光的光子被输入到一对或两对参数下变频波导,从而使纠缠的量子光子在波导中具有多于一条的路径可循,并从而使量子光子相互作用。参数下变频波导使至少一些光子相互作用,这是因为在该实施例中使用了Knill、Laflamme和Milburn的“一种采用线性光学器件的有效量子计算的方案(A scheme for efficient quantum computation with linear optics)”(参见Nature,409(6816):46-52)的方案。结果,波导的输出包括一个光子流,其中一些光子是经典光子,而有些则根据Knill Laflamme Milburn方案是纠缠的并在量子态中相互作用。

[0171] 光子流进入多个测量设备。每个测量设备具有光子可遵循的多个可能路径,每个路径在雪崩光电二极管或其他光子检测器中结束。路径长度相同。因此,处于叠加状态的量子光子将沿其可用的所有路径行进,并同时到达这些路径末端处的每个光子检测器。通过在检测器处查找重合(多个检测器同时检测光子),可以找到量子光子叠加的证据。经典光子还可以沿测量设备中的路径行进,但不叠加。因此,通过查看检测器处的输出模式,也可

以找到经典光子的证据。更改检测器的测量设置,以便提高安全性并避免恶意方知道测量设置并篡改结果的任何风险。在一些实施方式中,可以进行数百万次测量,并且在做出关于测量设备的输出是否来自量子系统的决定之前,可以汇总支持和反对存在量子光子的证据。

[0172] 在该示例中,图2A的状态扩展器210具有两个光波导810,并且图8是一个这样的光波导的立体图。波导810适用于其他类型的量子装置以及图2A的量子装置。

[0173] 在光学情况下,状态扩展器210可以利用纠缠光子的量子叠加。状态扩展器210可具有至少一对波导,每个波导810包括散布有多个偏振修改器802的多个光移位材料块800。波导810具有输入端804,以从源(例如激光)接收一对纠缠的光子。光子通过波导传输,并由块800偏转,并由偏振修改器802偏振。波导有两个输出端806、808,每个输出端用于两个相互正交的偏振中的每一个。

[0174] 该对纠缠的光子中的每个成员具有相对于该对中的另一个成员相互正交的偏振。输入端804连接到该对波导(尽管在图8中仅示出了一个波导),使得每个波导接收该对纠缠的光子中的一个,并通过光移位材料块800和偏振修改器802在该波导内引导纠缠的光子以产生光子的量子叠加,由此在波导内有多个光子所遵循的路径,偏振沿着该路径变化。在图10中更详细地示出了多个可能的路径。

[0175] 每个波导810的尺寸和形状被确定为使得对于每个纠缠的光子,无论纠缠的光子的相互正交的偏振如何,光子通过波导所行进的路径的长度基本相同。

[0176] 每个波导810具有一对输出光纤806、808,一对中的每个输出光纤806、808被配置为接受以相互正交的偏振中一个而偏振的光并且丢弃以另一个相互正交的偏振而偏振的光。

[0177] 图9示出了在壳体(也称为外壳)900中的波导810,该壳体具有纵向通道902,该纵向通道的尺寸和形状被设置为容纳该波导,从而使光移位材料块800靠着通道902的侧面而装配。壳体900具有可移除的盖,一旦波导在通道内部,该可移除的盖在则封盖住通道902。外壳壳体900和盖起到保护波导免受诸如湿度、灰尘、运动、温度变化和其他环境变化之类的环境条件的影响。外壳可以由减小大气压力、振动、湿度对波导的影响的材料形成。

[0178] 图10是通过图8的波导810的示意性纵向截面。在该示例中,有六个光移位材料块800,尽管在其他示例中使用了其他数量的块。在该示例中,存在六个偏振修改器802,尽管在其他示例中使用了其他数量的偏振修改器。在此示例中,在波导802的输出端有一个偏振修改器,其他五个偏振修改器分别位于两个不同的块800之间。进入波导的水平偏振光子(用H表示)被偏转,以具有通过波导的两个可能路径1000、1006。进入波导的竖直偏振光子(用V表示)被偏转以具有通过波导的两个可能的路径1002、1004。注意,通过波导的多个路径的具有基本相同的长度,因为所有路径都穿过固定长度的波导。

[0179] 如图11A所示,该光移位材料块800包括由使光在第一方向上移位的材料形成的至少一个块1100(如图11A的块1100中的向上箭头所示)以及由使光在与第一方向不同的第二方向上移位的材料形成的至少一个块1102(如图11A的块1102中的向下箭头所示)。图11A示出了重复的波导,以帮助理解该技术。图11A中的波导中的上部波导示出了水平偏振光子,其在路径1000上进入波导并且被块偏转/移位,使得光子(其是从激光输出的纠缠光子)能够同时沿着两个可能的路径1000和1006通过波导。图11B中的波导中的下部波导示出了进

入波导的竖直偏振光子的相同情况。注意,实际上,图11B的上部和下部波导是相同的波导,并且路径1000、1002、1004、1006穿过如图10所示的单个波导。

[0180] 在第一方向上使光移位的至少一个块1100由上空气晶体(up-air crystal)制成,并且使光在第二方向上移位的至少一个块1102由下空气晶体(down-air crystal)制成。以这种方式,促进了光子的移位,这使得创建了供来自激光的纠缠光子遵循的多个可能的路径,上空气晶体使光沿第一方向远离波导的纵向轴线移位。下空气晶体使光在第二方向上远离波导的纵向轴线并且与第一方向基本相反地移位。

[0181] 优选地,多个光移位材料块800由相同材料制成,因为这便于制造。但是,使用相同的材料不是必需的。制成块800的材料的示例的非穷举列表是方解石或铌酸锂中的一种或多种。在优选的示例中,波导810包括六块光移位材料,因为这给出了相对容易制造的实际工作解决方案。然而,在其他示例中使用其他数量的块800。

[0182] 在图11A中,波导810被示出为具有六块由上空气晶体和下空气晶体制成的光移位材料块,其从波导的输出端到波导的输入端按以下顺序布置:下空气晶体、上空气晶体、上空气晶体、下空气晶体、下空气晶体、上空气晶体。发现该布置对于为具有适合于图2A的实施例的量子态和/或如以上方程式3所定义的量子位提供多个光学路径而言特别有效。

[0183] 在图11A和图11B的示例中,偏振修改器按以从波导的输出端到波导的输入端以下列顺序布置的光移位材料块的顺序放置并且具有或没有以下气隙:偏振修改器1124、气隙1122、下空气晶体、偏振修改器1120、上空气晶体、气隙1118、偏振修改器1116、气隙1114、上空气晶体、偏振修改器1112、下空气晶体、气隙1110、偏振修改器1108、气隙1106,下空气晶体、偏振修改器1104、上空气晶体。

[0184] 偏振修改器可以是半波片,其中一些偏振修改器通过气隙与相邻的光移位材料块的偏振修改器隔开。其他的偏振修改器中的可以与相邻的光移位材料块的偏振修改器接触。通过选择气隙的位置或大小,促进了光子在波导内衍射或移位的能力。

[0185] 至少一个偏振修改器包括区域1126,不改变偏振的情况下,光穿过区域1126。该区域被配置为使得光透射而没有偏振变化。在图11B的示例中,区域1126位于从波导的输出端起的第三偏振修改器1116中。

[0186] 在一些示例中,存在冷却室,该冷却室容纳波导并且被配置为在操作期间将波导的温度降低至大约二十摄氏度,因为这减少了所生成的量子位中的噪声(即,波导810生成更高比例的与经典光子相反的所需状态的量子位)。

[0187] 在刚刚描述的光学实施例中的状态扩展器从诸如激光器的生成器接收一对纠缠的光子,该对光子中的每个成员具有相对于该对中的另一个成员相互正交的偏振。状态扩展器将纠缠的光子输入到一对波导,使得每个波导810接收该对纠缠的光子中的一个,并在波导内沿其长度引导纠缠的光子以产生光子的量子叠加,从而存在多个在波导中光子所遵循的可能路径,偏转沿着该路径发生变化。每个波导的尺寸和形状被确定为使得对于每个纠缠的光子,不管纠缠的光子的相互正交的偏振如何,光子通过波导行进的路径的长度基本相同。

[0188] 图12是用于测量从状态扩展器810接收的粒子的一对测量设备1200和1202的示例的示意图。在该示例中,测量设备1200和1202是光学的,并且量子位是使用如参照图8至11B所述的光子形成的。注意,尽管实际上在图2A的装置中可以有四个这样的测量设备,单图12

仅示出一对测量设备1200和1202。话虽如此,在图3A的示例中,只有两个这样的测量设备。

[0189] 每个测量设备1200、1202具有光子可以遵循的多个可能路径,每个路径在雪崩光电二极管或其他光子检测器中结束。路径具有基本相同的长度。因此,处于叠加状态的量子光子将沿着其可用的所有路径行进,并基本上同时到达这些路径末端的每个光子检测器。通过在检测器处查找重合模式(多个检测器同时检测光子),可以找到量子光子叠加的证据,其给出违反Bell不等式的证据。经典光子还能够沿着测量设备中的路径行进,但不重合,并且在检测器处呈现与量子光子不同的模式。可以更改检测器的测量设置,以提高安全性。可以进行数以百万计的测量,并且可以汇总支持或范围量子光子存在的证据以决定是否违反了Bell不等式。

[0190] 图12中的一对测量设备1200和1202是用于检测纠缠的光子对的装置的一部分,该纠缠的光子对在包括纠缠的光子对和经典光子的光子流中叠加。每个测量设备1200、1202具有多个检测器(用于测量设备1200的1204、1206、1208和1210以及用于测量设备1202的1212、1214、1216和1218),每个检测器布置成检测单个光子。每个测量设备1200、1202具有检测器配置装置,以根据控制参数的值为每个检测器自动配置检测器的测量基准。在图12的示例中,测量设备1200中的检测器配置装置包括偏振修改器1240、1244和光学模式设置器1232。测量设备1202中的检测器配置装置包括偏振修改器1242、1246和光学模式设置器1234。

[0191] 每个测量设备1200、1202都有一个来自相应状态扩展器810的光子输入。每个光子输入都有两个光子路径:一个用于两个可能相互正交的光子偏振(例如,水平(H)和竖直(V))中一个,每个光子路径行进到一个不同的检测器,并且其中单个测量设备中的光子路径的长度基本相同。在图12中,输入到测量设备1200的光子用A表示,输入到测量设备1202的光子用A'表示。使用竖直条指示光子的偏振状态;例如,A|H代表光子A的水平偏振状态,而A'|V表示光子A'的竖直偏振状态。

[0192] 此外,对中的测量设备的光子路径具有基本相同的长度。即,从源到测量设备1200中的检测器的距离与从源到测量设备1202中的检测器的距离基本相同,并且对于为清楚起见图12中未示出的其他两个测量设备也是如此。

[0193] 每个测量设备包括两个偏振分束器(PBS)1228、1224、1230、1226以及一个或多个镜子1236、1238。当竖直偏振的光子A(图12中的光子A|V)进入测量设备1200,它被传输到分束器(BS)1220,通过该分束器,从镜子反射并通过(根据光学模式设置器1232的设置如何)潜在地改变光子的光学模式的光学模式修改器1232,从另一个镜子1236反射回到分束器1220,并从另一个镜子反射到偏振修改器1244中。由于光子已经竖直偏振,如果偏振修改器1244不做任何操作,则竖直偏振的光子将在被检测器1210检测到而没有被检测器1208检测到之前进入偏振分束器1224。如果偏振滤波器1244被配置为改变通过它的光子的偏振,则光子变为水平偏振,并由检测器1208检测。来自状态扩展器810的给出水平偏振的光子(A|H)的输入沿着具有可配置的偏振修改器1240并且通过可配置的光学模式设置器1232到达检测器1204、1206的路径。当作用在偏振装态A'|H或A'|V的光子A'上时,测量设备1202的功能大体上类似于针对设备1200所描述的功能。

[0194] 测量设备检测重合,该重合是基本上同时在检测器处检测到量子位。如本文档前面更详细所述,对重合进行了评估,以查看是否违反了Bell不等式。如果一对测量设备中的

第一个测量设备中的检测器在第一时间处检测到光子并且该对测量设备中的另一个测量设备中的检测器在第一时间的指定时间内检测到光子(重合),则检测到的光子有可能是叠加的纠缠光子。例如,指定的时间段可以在5到15ns的范围内,例如大约10ns。

[0195] 但是,如果单个测量设备中的检测器在第一时间处检测到光子,且单个测量设备中的另一个检测器在第一时间的指定时间内检测到光子(重合),则检测到的光子可能是经典光子。再次,例如,指定时间段可以在5到15ns的范围内,例如大约10ns。

[0196] 在每个测量设备1200、1202中,有四个检测器,包括:用于两个相互正交的偏振的每一个的第一对检测器(测量设备1200中的1204、1206;测量设备1202中的1212、1214),以及用于两个相互正交的偏振中的每一个第二对检测器(测量设备1200中的1208、1210;测量设备1202中的1216、1218);其中第一对检测器操作用于第一光学模式,第二对检测器操作用于第二光学模式。如参考图12所描述的,两个相互正交的偏振可以是水平(H)偏振和竖直(V)偏振。

[0197] 检测器配置装置包括用于在两个指定值(例如π弧度和π/2弧度,或者是正交的另一对相移)之间改变相移(也称为光学模式)的弧度数的装置,并在两个指定值(例如水平和竖直或零度和22.5度,或另一对偏振值)之间改变多个偏振度,以供各个检测器使用。检测器配置装置经由设备驱动器1250从第一随机性弱源104接收控制参数的值。

[0198] 在示例中,检测器配置装置接收为四位的控制参数的值,因为这特别有效。但是,在其他示例中使用其他位数。

[0199] 在示例中,测量设备的输出包括:对于每个测量设备的两个位,每个位表示是否以给定的测量基准检测到光子。在一个示例中,有四个测量设备,并且使用查找表将测量设备的所得的8位输出转换为4位输出。

[0200] 在一些实施例中,存在图3A和图3C的示例的两设备光子学实现。在这种情况下,图3A的源300可以是发射光子的激光器,其中一些光子是经典的,而一些是纠缠的量子光子。如图3A所示,存在两个量子物理装置302、304,与图2A的实施例不同,每个量子装置能够存储两个量子位。装置302包括状态扩展器310,该状态扩展器310包括两个波导,使得它能够存储两个量子位。装置304还包括状态扩展器310,该状态扩展器310包括两个波导,使得它能够存储两个量子位。可以如参考图8至图11A和图11B所描述的那样来实现波导。在两设备光子学实施例中的存储在状态扩展器310中的至少一些光子的量子态不同于以上在不限于任何特定类型的量子位实施的示例中描述的四设备的光子学实施例的量子态。

[0201] 在两设备光子学实施例中,有如图3A所示的两个测量设备312。测量设备通常如图12所示,但是可被修改为针对每个检测器使用九个不同的测量基准。这可以通过使用九种不同的偏振和/或光学模式设置来完成。

[0202] 使用与四设备光子学实施例相同的原理,通过在光子检测器处的许多测量记录测量设备的光子检测器处的检测事件的模式。检测事件的模式被用作支持或反对存在量子位且违反Bell不等式的证据。可选地,如上所述,完成进一步的检查(安全性测试B)。

[0203] 作为本文所述其他示例的替代或补充,示例包括以下各项的任意组合:

[0204] 条款1:一种生成随机位串的方法,该方法包括:提供弱随机性源;

[0205] 提供量子设备,该量子设备被配置为使处于量子态的多个量子粒子纠缠;以两个不同的基准测量该多个粒子中的每个粒子;

[0206] 确定违反Bell不等式的程度;

[0207] 至少部分地基于所确定的违反程度来确定是接受还是中止;

[0208] 通过两源提取器提取随机位串。通过确定违反Bell不等式的程度,可以确定包括被测粒子的量子设备的输出是来自经典效应还是来自量子效应。如果输出来自经典效应,则该过程可中止。如果该过程接受,则已知量子设备的输出来自量子效应,而无需人工视觉或手动检查量子设备本身。当过程接受时,输出包括量子效应的测量值,并且两源提取器使用此不确定性输出来根据下游过程(如加密或认证过程或使用随机位串的其他下游过程)所要求的需求来生成随机位串。由于两源提取器的输入是已知来自量子源的随机位串,因此,两源提取器的输出是随机的。

[0209] 条款2:根据条款1所述的方法,其中,Bell不等式包括CHSH(Clauser Horne Shimony Holt)不等式。其中在使用CHSH不等式时,存在一种准确有效的方法来确定测量的输出是来自量子效应还是来自经典效应。

[0210] 条款3:条款1或条款2所述的方法,其中,多个量子粒子是2个或4个。通过使用成对的量子粒子,可以以特别有效的方式评估Bell不等式。

[0211] 条款4:根据条款1-3中任一项所述的方法,其中,确定是接受还是中止包括确定量子设备是否满足无信号标准。通过确定量子设备是否满足无信号标准,提高了准确性和质量。这是因为检测到量子设备内的量子系统相互影响的情况,并且在这些情况下过程中止。

[0212] 条款5:根据条款4所述的方法,其中,无信号标准包括近似无信号的标准。发现使用近似无信号的标准以实用有效的方式给出准确的工作结果。在量子设备仅需要是近似无信号的情况下,制造实施该方法的系统更为实用。

[0213] 条款6:一种用于生成随机位串的系统,该系统包括:

[0214] 弱随机性源,其被配置为重复生成第一位串和第二位串;

[0215] 量子设备,其被配置为接收第二位串并输出相关联的第三位串;

[0216] 安全性测试设备,其被配置为通过针对每个第二位串和相关联的第三位串来比较第二位串和第三位串从而计算测试统计量;安全性测试设备,其被配置为基于所计算的测试统计量来确定是接受还是拒绝量子设备的输出;和

[0217] 两源提取器,其被配置为如果安全性测试设备接受量子设备的输出则接收第一位串和第三位串,并生成随机位串。该系统的优点是能够生成真正随机的位串,因为仅使用通过安全性测试并因此已知来自量子效应的量子设备的输出。

[0218] 条款7:根据条款6所述的系统,其中,所述量子设备包括光学设备、离子阱或超导电路。这样,各种不同类型的技术可用于实施该系统。

[0219] 条款8:根据条款6或条款7所述的系统,其中,该量子设备包括2或4个量子系统,每个量子系统包括量子位。通过使用成对的量子系统,可以准确地评估Bell不等式。

[0220] 条款9:根据条款8所述的系统,其中,所述量子系统包括测量装置,所述测量装置被配置为对量子位执行测量并输出包括所述测量结果的位。测量装置输出形成随机位串的位。

[0221] 条款10:根据条款6-9中任一项所述的系统,其中,安全性测试包括:

[0222] 第一测试,其中测量对Bell不等式的违反;和

[0223] 第二测试,用于确定量子设备是否满足无信号标准。通过使用两个测试,可以确定

来自量子设备的输出质量来自于量子效应,并且也来自于在量子设备内互不影响的量子系统。Bell不等式可以包括Clauser Horne Shimony Holt(CHSH)不等式。

[0224] 条款11:根据条款10所述的系统,其中,无信号标准包括用于近似无信号标准。使用近似无信号标准是高效且有效的。

[0225] 条款12:一种配置为输出随机位的系统,该系统包括:

[0226] 量子生成器,其被配置为生成一对纠缠的粒子a和a';

[0227] 第一状态扩展设备,其被配置为生成包括a和b的纠缠状态;

[0228] 第二状态扩展设备,其被配置为生成包括a'和b'的纠缠状态;

[0229] 第一测量设备,其被配置为执行与ab或a'b或ab'或a'b'的双重重合有关的重合测量;

[0230] 第二测量设备,其被配置为测量对Bell不等式的违反并确定纠缠状态是否为无信号;和

[0231] 两源提取器,其被配置为接收来自第二测量设备的输入并输出随机位。该系统是一种实用的装置,其输出已知是从量子系统生成的随机位,而无需手动检查系统本身的内部运作。

[0232] 条款13:一种安全性测试逻辑,其具有:

[0233] 存储器,其存储来自测量装置的测量值,测量输出包括是否存在重合的指示,其中基本上同时在多于一个的检测器处检测到粒子,该检测器位于与粒子源不同的通道的末端,并具有基本相同的长度;

[0234] 处理器,其被配置为由存储的测量值计算表示Bell不等式的测试统计量,并将该测试统计量与阈值进行比较;

[0235] 所述处理器被配置为:如果所计算的测试统计量的值低于所述阈值,则生成并输出证明测量值来自量子系统的凭证。安全性测试逻辑是一种实用且有效的装置,其可以自动证明测量值来自量子系统,而无需手动检查量子系统的运行情况。

[0236] 条款14:根据条款13所述的安全性测试逻辑,其中,处理器被配置为通过计算测量数目的倒数乘以测量数目个保存二进制数值的阵列中适当条目的总和,当进行各次测量时,根据量子测量装置中使用的检测器的测量设置的值在阵列中查找该适当条目。由于阵列易于操作,因此安全性测试逻辑能够以高效、准确的方式计算测试统计量。

[0237] 条款15:根据条款14所述的安全性测试逻辑,其中,该阵列用于评估重合,所述重合作为支持或反对具有已生成的各个测量值的量子效应的证据。该阵列易于使用和存储,并使安全性测试逻辑变得高效。

[0238] 条款16:根据条款13至15中任一项所述的安全性测试逻辑,其中,通道承载处于以下量子态中的任一状态的量子位:等于二的平方根的倒数乘以两对量子位的量子态的总和的量子态,其中这两对量子位的量子态是纠缠并叠加的;或等于从0到3的i个具有相同量子位的通道i上的量子位的张量积的总和的一半的量子态。通过使用这些量子态,可以以有效的方式评估Bell不等式。Bell不等式可以包括Clauser Horne Shimony Holt(CHSH)不等式。

[0239] 条款17:根据条款13至16中任一项所述的安全性测试逻辑,其中,处理器还被配置为通过由测量值创建基线直方图并将基线直方图与从测量装置获得的测量值的一个或多

个测试直方图比较来测试测量装置内的各个测量设备之间的相互作用。以这种方式,以高效且有效的方式来检测测量设备之间的相互作用。

[0240] 条款18:根据条款13至17中任一项所述的安全性测试逻辑,其中,处理器还被配置为计算第二测试统计量并在决定是否生成凭证之前将第二测试统计量考虑在内。第二测试统计量使得能够获取准确且高质量的结果。

[0241] 条款19:一种用于形成光子的量子叠加的装置,包括:

[0242] 至少一对波导,每个波导包括散布有多个偏振修改器的多个光移位材料块;接收一对纠缠的光子的输入端,该对中的每个成员具有相对于该对中的另一个成员相互正交的偏振,该输入端连接到该对波导,使得每个波导接收该对纠缠的光子中的一个并在波导内引导纠缠的光子通过光移位材料块和偏振修改器,以形成光子的量子叠加,从而具有光子在波导中遵循的多个可能的路径,偏振沿着该多个可能的路径发生变化;并且

[0243] 其中,每个波导的尺寸和形状被设计成使得:对于每个纠缠光子,无论纠缠光子的相互正交的偏振如何,光子通过波导行进的路径的长度基本上相同。该装置是实际可部署的,并且能够以稳健和准确的方式产生光子的量子叠加。

[0244] 条款20:根据条款19所述的装置,对于每个波导包括一对输出光纤,一对中的每个输出光纤配置为接受以相互正交的偏振中的一个而偏振的光并丢弃以另一个相互正交的偏振而偏振的光。以这种方式,输出光纤提供适合于输入到量子测量设备的输出,以用于评估Bell不等式。

[0245] 条款21:根据条款19或条款20所述的装置,其中,多个光位移材料块包括:由使光在第一方向上移位的材料形成的至少一个块,以及由使光在不同于第一方向的第二方向上移位的材料形成的至少一个块。以此方式,光沿不同方向移位,以产生光子的量子叠加。

[0246] 条款22:根据条款21所述的装置,其中,使光在第一方向上移位的至少一个块是由上空气晶体制成的,并且使光在第二方向上移位的至少一个块是由下空气晶体制成的。以这种方式使用晶体有助于产生光子的量子叠加。

[0247] 条款23:根据条款19至22中任一项所述的装置,其中,所述多个光移位材料块由相同材料制成。使用相同的材料降低了制造成本,并促进了装置的方便制造和/或维修。

[0248] 条款24:根据条款19至22中任一项所述的装置,其中,光移位材料块由方解石、铌酸锂中的一种或多种制成。使用这些材料便于制造,因为这些材料适合在指定的公差内切割或形成为指定的尺寸和形状。

[0249] 条款25:根据条款19至24中任一项所述的装置,包括由6个光移位材料块。发现使用6个光移位材料块在产生光子的量子叠加方面具有特别好的效果。

[0250] 条款26条:根据条款25所述的装置,其中,六个光移位材料块从波导的输出端到波导的输入端按以下顺序布置的上空气晶体和下空气晶体制成:下空气晶体、上空气晶体、上空气晶体、下空气晶体、下空气晶体、上空气晶体。发现这种布置在产生光子的量子叠加方面具有特别好的结果。

[0251] 条款27:根据条款26所述的装置,其中,所述偏振修改器从光波导的输出端到光波导的输入端按照以下顺序以光移位材料块的序列放置并且具有或不具有以下气隙:偏振修改器、气隙、下空气晶体、偏振修改器、上空气晶体、气隙、偏振修改器、气隙、上空气晶体、偏振修改器、下空气晶体、气隙、偏振修改器、气隙、下空气晶体、偏振修改器、上空气晶体。发

现这种布置在产生光子的量子叠加方面具有特别好的结果。

[0252] 条款28:根据条款19至27中任一项所述的装置,其中,偏振修改器是半波片。使用半波片可获得良好的结果,同时简化了装置的制造。

[0253] 条款29:根据条款19至28中任一项所述的装置,其中,多个偏振修改器通过气隙与相邻的所述光移位材料块分离。使用气隙是一种重量轻、低成本的解决方案。

[0254] 条款30:根据条款19至29中任一项所述的装置,其中,第二多个偏振修改器与相邻的光移位材料块接触。使用"接触"布置易于制造,并且具有紧凑的布置。

[0255] 条款31:根据条款19至30中任一项所述的装置,其中,偏振修改器中的至少一个包括光在不改变偏振的情况下穿过的区域。以这种方式使用区域是使光在不改变的情况下通过的有效方法。

[0256] 条款32:根据项19至31中任一项所述的装置,还包括:容纳该装置的外壳,所述外壳由减小大气压力、振动、湿度对所述波导的影响的材料形成。使用外壳有利于装置的实际部署。

[0257] 条款33:根据条款19至32中任一项所述的装置,还包括:冷却室,其容纳波导并且被配置为将所述波导的温度降低至大约负二十摄氏度。使用冷却室有助于减少经典噪音。

[0258] 条款34:一种用于产生状态叠加的方法,该方法包括:

[0259] 从生成器接收一对纠缠的光子,该对中的每个成员具有相对于该对的另一个成员相互正交的偏振,

[0260] 将纠缠的光子输入到一对波导,使得每个波导接收该对纠缠的光子中的一个,并在波导中沿其长度引导纠缠的光子,以产生光子的量子叠加,从而存在光子在波导内所遵循的多个可能的路径,偏振沿该多个可能的路径变化,并且

[0261] 其中,每个波导的尺寸和形状被设计成使得:对于每个纠缠光子,不论纠缠光子的相互正交的偏振如何,光子通过波导行进的路径的长度基本上相同。该方法是产生状态叠加的实用且有效方法。该方法适用于与检测纠缠的光子对的装置一起使用,以评估Bell不等式的存在与否。

[0262] 条款35:一种用于检测在光子流中叠加的纠缠光子对的装置,该装置包括纠缠光子对和经典光子,该装置包括:

[0263] 至少一对测量设备,每个测量设备包括:

[0264] 多个检测器,每个检测器布置成检测单个光子;

[0265] 检测器配置装置,用于针对每个检测器根据控制参数的值来自动配置检测器的测量基准;

[0266] 光子输入端,其具有两个光子路径,每个光子路径用于两个可能的相互正交的光子偏振中的每一个,每个光子路径行进到所述检测器中的一个不同的检测器,并且其中单个测量设备内的光子路径的长度基本相同;并且其中,该对中的测量设备的光子路径的长度基本相同。该装置是用于检测纠缠的光子对的实用设备。

[0267] 条款36:根据条款35所述的装置,包括:安全性测试逻辑,用于评估在检测器处检测到的重合,该重合是在指定时间间隔内在多于一个的检测器处检测到的光子,并且其中,安全性测试逻辑进行检查一对测量设备中的第一测量设备中的检测器是否在第一时间处检测到光子,且该对测量设备中的另一个测量设备中的检测器是否在第一时间的指定时间

内检测到光子,从而使得被检测到的光子有可能是叠加的纠缠光子。以这种方式,该装置能够收集关于在测量设备处检测到的粒子是来自量子效应还是来自经典效应的证据。

[0268] 条款37:根据条款36所述的装置,其中,安全性测试逻辑检查重合,在重合时,光子在单个测量设备内的检测器处被检测到,使得如果单个测量设备内的检测器在第一时间处检测到光子,且单个测量设备内的另一个检测器在第一时间的指定时间内检测到光子,则检测到的光子有可能是经典光子。以这种方式,该装置能够收集关于在测量设备处检测到的粒子是来自量子效应还是来自经典效应的证据。

[0269] 条款38:根据条款35至37中任一项所述的装置,其中,在每个测量设备中具有四个检测器,其包括用于两个相互正交的偏振中的每一个的第一对检测器,以及用于两个正交的偏振中的每一个的第二对检测器;其中第一对检测器针对第一光学模式进行操作,第二对检测器针对第二光学模式进行操作。通过这种方式,检测器能够检测处于叠加状态的量子粒子。

[0270] 条款39:根据条款35至38中任一项所述的装置,其中,检测器配置装置包括用于在两个指定值之间改变相移的弧度数并且在两个指定值之间改变偏振度数的装置,以供各个检测器使用。该配置装置的优点是能够容易地改变各个检测器检测到的内容。

[0271] 条款40:根据条款35至39中任一项所述的装置,其中,所述检测器配置装置从第一弱随机性源接收所述控制参数的值。这提供了配置检测器的简单有效的方法。

[0272] 条款41:根据条款35至39中任一项所述的装置,其中,所述检测器配置装置接收为四个位的所述控制参数的值。这为配置检测器提供了紧凑的信号。

[0273] 条款42:根据条款35至39中任一项所述的装置,其中,监视装置的输出对于每个测量设备包括两个位,每个位表示是否以给定的测量基准检测到光子。这给出了与模拟输出相反的数字测量输出。数字输出便于与下游数字过程一起使用。

[0274] 条款43:一种用于提供随机数的装置,该装置包括:

[0275] 被配置为输出量子位的能量源;

[0276] 与能量源通信的多个量子系统,多个量子系统中的每一个包括:

[0277] 状态扩展器,其被配置为产生处于纠缠的量子态的量子位;和

[0278] 测量设备,其被配置为以至少一个测量基准来检测量子位;

[0279] 驱动器,其被配置为从随机性源接受第一输入并且至少部分地基于第一输入来调节每个测量设备的至少一个测量基准;

[0280] 硬件处理器,其被配置为:

[0281] 分析测量设备的量子位检测;

[0282] 确定发生对Bell不等式的违反;

[0283] 确定多个量子系统满足无信号条件;

[0284] 根据所分析的量子位检测输出量子可证明串;并且

[0285] 根据量子可证明串和来自随机性源的第二输入,提取随机数。

[0286] 条款44:根据条款43所述的装置,其中,能量源包括激光器。

[0287] 条款45:根据条款43或44所述的装置,其中,该状态扩展器包括一对波导。

[0288] 条款46:根据条款43至45中任一项所述的装置,其中,所述多个量子系统包括两个量子系统。

[0289] 条款47:根据条款46所述的装置,其中,所述至少一个测量基准包括两个测量基准。

[0290] 条款48:根据条款43至45中任一项所述的装置,其中,所述多个量子系统包括四个量子系统。

[0291] 条款49:根据条款48所述的装置,其中,至少一个测量基准包括九个测量基准。

[0292] 条款50:根据条款43至49中任一项所述的装置,其中,所述随机性源包括弱随机性源或不可证明的不确定性随机数源。

[0293] 条款51:根据条款43至50中任一项所述的装置,其中,为了确定发生了对Bell不等式的违反,硬件处理器被配置为确定测试统计量低于阈值,其中,测试统计量包括:应用于由测量设备检测到的重合的Bell指标向量。

[0294] 条款52:根据条款43至51中任一项所述的装置,其中,为了确定所述多个量子系统满足无信号条件,所述硬件处理器被配置为将以测量设备在第一时间处的测量设置为条件的测量设备的输出的第一概率分布与以测量设备在第二时间处的测量设置为条件的测量设备的输出的第二概率分布进行比较。

[0295] 条款53:根据条款43至52中任一项所述的装置,其中,为了确定发生了对Bell不等式的违反,所述硬件处理器被配置为评估与测量设备的观察到的测量值相对应的随机变量的值和测量设备的测量设置的对应值。

[0296] 条款54:根据条款43至53中任一项所述的装置,其中,所述硬件处理器被配置为输出所述随机数是量子效应的产物的凭证。

[0297] 条款55:根据条款43至54所述的装置,还包括:配置为接收随机数的应用程序,该应用程序包括计算机安全应用程序、气象预报应用程序、电信应用程序或制造控制应用程序。

[0298] 术语“计算机”或“基于计算的设备”在本文中用于指代具有处理能力以使其执行指令的任何设备。本领域技术人员将意识到,这种处理能力被结合到许多不同的设备中,因此术语“计算机”和“基于计算的设备”分别包括个人计算机(PC),服务器、移动电话(包括智能电话)、平板电脑计算机、机顶盒、媒体播放器、游戏机、个人数字助理、可穿戴计算机和许多其他设备。

[0299] 在一些示例中,本文所述的方法通过在有形的非暂时性存储介质上以机器可读形式(例如,以计算机程序的形式)的软件执行,计算机程序包括计算机程序代码,当程序在计算机上运行时,计算机程序代码适于执行本文所述的一个或多个方法的操作,并且其中计算机程序可实施在非临时计算机可读介质上。该软件适合于在并行处理器或串行处理器上执行,使得可以以任何合适的顺序或同时执行方法操作。

[0300] 这承认软件是一种有价值的、可单独交易的商品。它旨在涵盖在“哑”或标准硬件上运行或控制“哑”或标准硬件的软件,以执行所需的功能。它还旨在涵盖“描述”或定义如设计硅芯片或配置通用可编程芯片中所使用的硬件配置的软件,例如HDL(硬件描述语言)软件,以执行所需功能。

[0301] 本领域技术人员将认识到,用于存储程序指令的存储设备可选地跨网络分布。例如,远程计算机能够存储描述为软件的过程的示例。本地或终端计算机能够访问远程计算机并下载部分或全部软件来运行该程序。替代地,本地计算机可以根据需要下载软件的片

段,或者在本地终端处执行一些软件指令并且在远程计算机(或计算机网络)处执行一些软件指令。本领域技术人员还将认识到,通过利用本领域技术人员已知的常规技术,所有或部分软件指令可以由专用电路(例如数字信号处理器(DSP)、可编程的逻辑阵列等)执行。

[0302] 如对本领域技术人员将显而易见的是,可以在不丧失寻求的效果的情况下扩展或改变本文给出的任何范围或设备值。

[0303] 尽管已经用特定于结构特征和/或方法动作的语言描述了主题,但是应该理解,所附权利要求书中定义的主题不必限于上述特定特征或动作。相反,上述特定特征和动作被公开为实施权利要求的示例形式。

[0304] 将理解的是,上述益处和优点可以涉及一个实施例或可以涉及若干实施例。实施例不限于解决任何或所有所述问题的实施例或具有任何或所有所述益处和优点的实施例。对于每个实施例来说,没有单个特征或单组特征是必要的或必不可少的。

[0305] 这里使用的条件语言,例如“能够”,“可以”,“可能”,“可”,“例如”等,除非另有明确说明,否则在上下文中应理解为使用,通常意在传达某些实施例包括而其他实施例不包括某些特征、元件和/或步骤。因此,这样的条件语言通常不旨在暗示一个或多个实施例以任何方式要求的特征、元件和/或步骤,或者一个或多个实施例必须包括用于在有或没有作者输入或提示的情况下决定这些特征、元件和/或步骤是否包括在内或将在任何特定实施例中执行。术语“包括”,“包含”,“具有”等是同义词,以开放式方式包含性地使用,并且不排除其他元件、特征、动作、操作、块等。同样,术语“或”以其包含的含义使用(而不是以其排他的含义使用),因此,例如在用于连接元件列表时,术语“或”表示列表中的一个、一些或全部的元件。另外,在本申请和所附权利要求书中使用的冠词“一”,“一个”和“该”应被解释为表示“一个或多个”或“至少一个”,除非另有说明。

[0306] 如本文中所使用的,指项目列表中的“至少一个”的短语是指那些项目的任何组合,包括单个成员。例如,“A,B或C中的至少一个”旨在涵盖:A;B;C;A和B;A和C;B和C;以及A,B和C。除非另有明确说明,否则使用诸如短语“X,Y和Z中的至少一个”之类的连接语言时应结合上下文理解,通常用于传达项、术语等可以是X、Y或Z中的至少一个。因此,这种连接语言通常并不意在暗示某些实施例要求X,Y或Z中的至少一个各自都存在。

[0307] 本文描述的方法的操作可以以任何合适的顺序执行,或者在适当的情况下同时执行。另外,在不脱离本文描述的主题的范围的情况下,可以从任何块中删除单独的块,将其与其他块组合或在任何方法中将其重新布置。可以将上述任何示例的方面与所描述的任何其他示例的方面相结合以形成其他示例,而不会失去所寻求的效果。

[0308] 将理解,以上描述仅以示例的方式给出,并且本领域技术人员可以进行各种修改。上面的说明书、示例和数据提供了示例性实施例的结构和使用的完整描述。尽管以上已经以某种程度的特殊性或参考一个或多个单独的实施例描述了各种实施例,但是本领域技术人员可以在不脱离本说明书的范围的情况下对所公开的实施例进行多种改变。

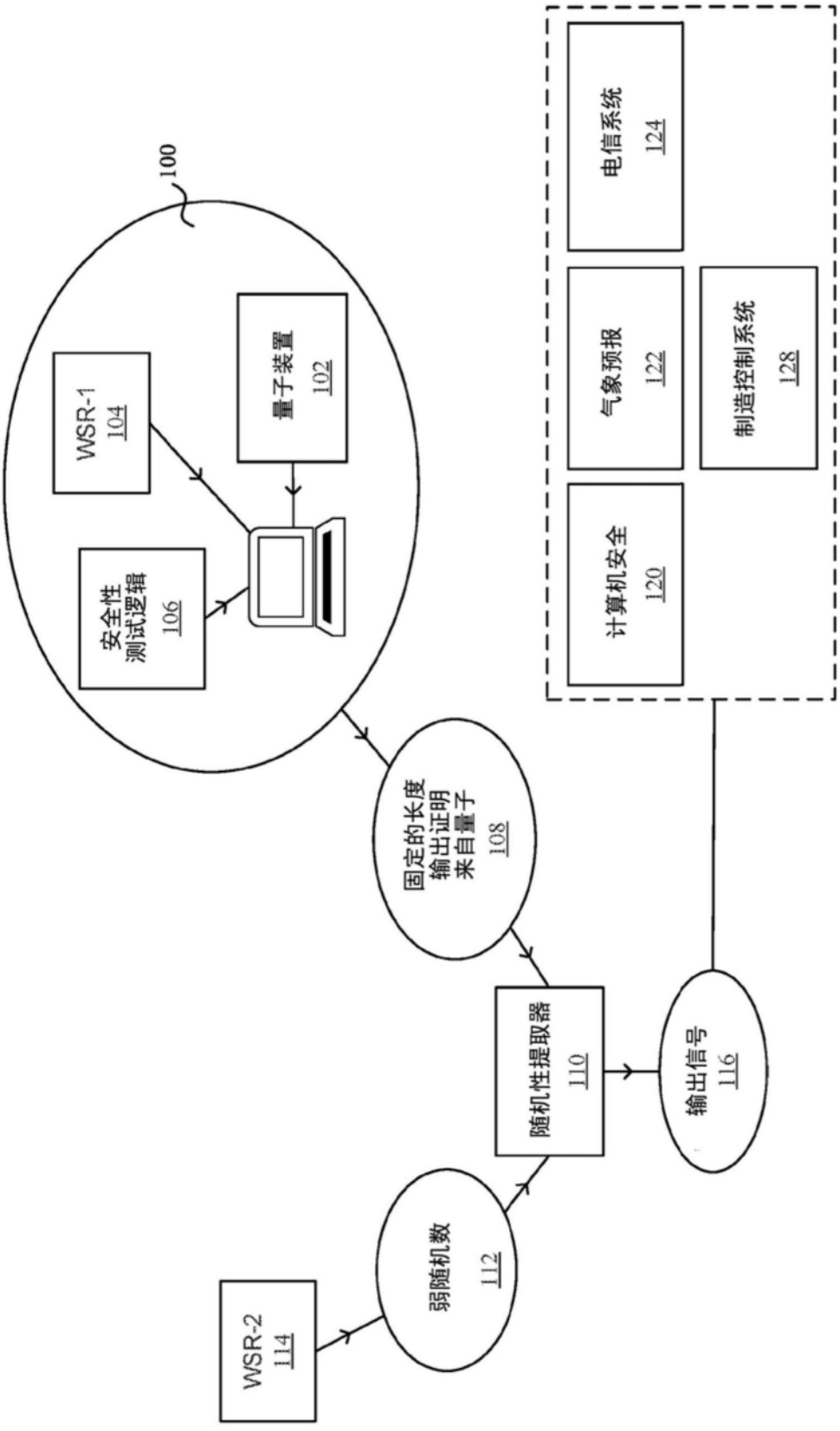

100
WSR-1
104
量子装置
102
安全性
测试逻辑
106
固定的长度
输出证明
来自量子
108
随机性提取器
110
弱随机数
112
WSR-2
114
输出信号
116
计算机安全
120
气象预报
122
电信系统
124
制造控制系统
128

图1

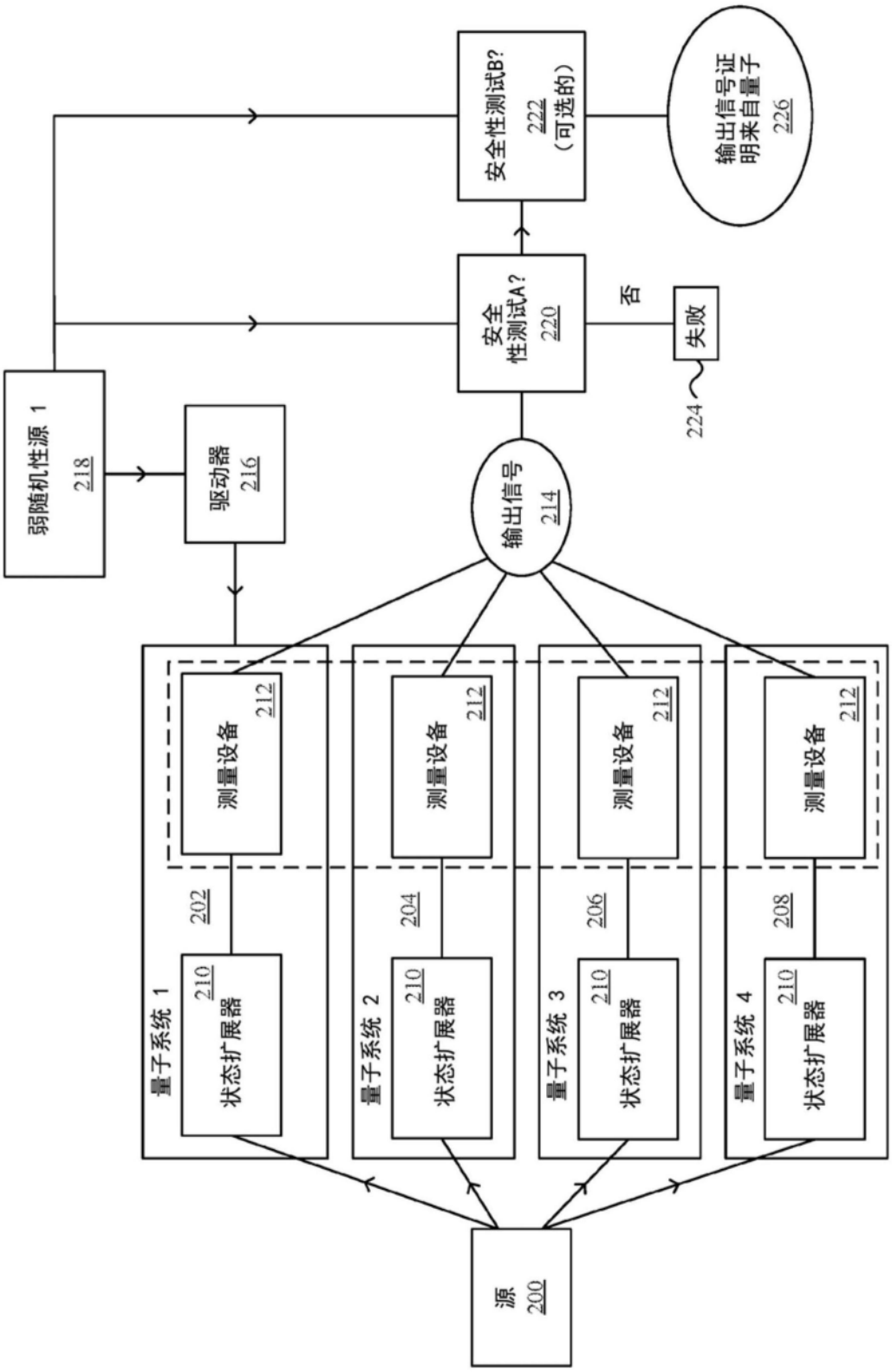

源
200
量子系统 1
量子系统 2
量子系统 3
量子系统 4
202
204
206
208
210
状态扩展器
212
测量设备
输出信号
214
弱随机性源 1
218
驱动器
216
安全性测试A?
220
否
失败
224
安全性测试B?
222
(可选的)
输出信号证明来自量子
226

图2A

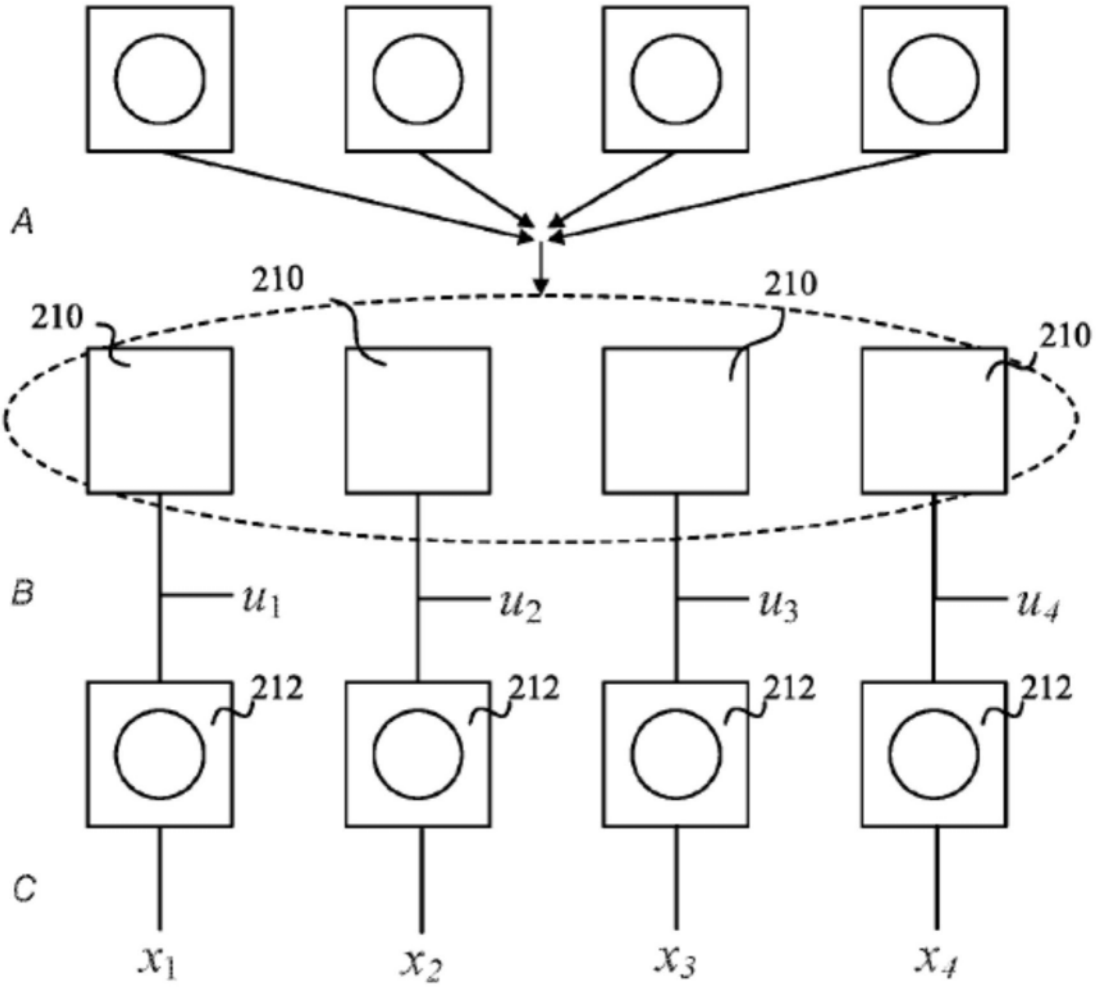


图2B

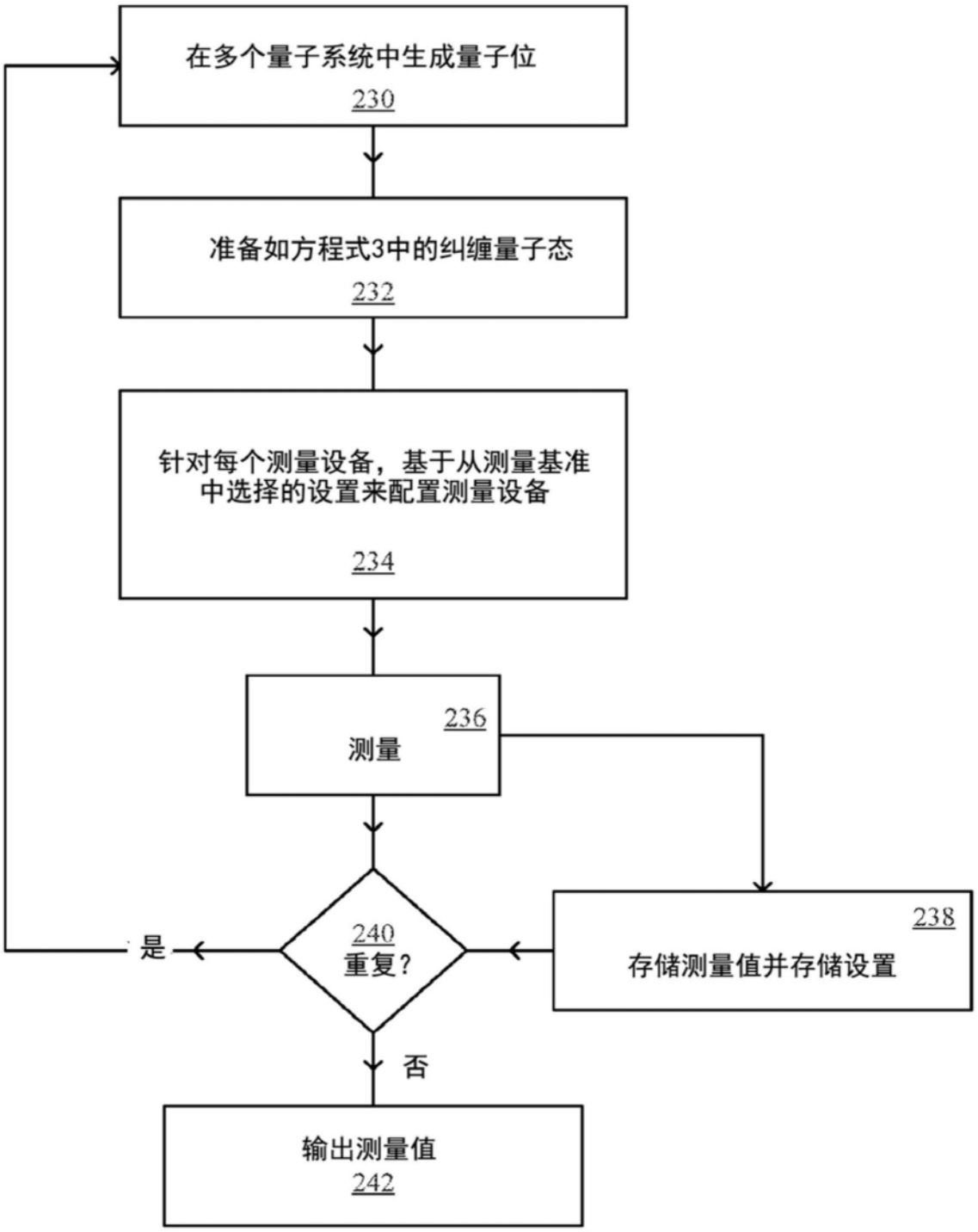

在多个量子系统中生成量子位
230
准备如方程式3中的纠缠量子态
232
针对每个测量设备，基于从测量基准中选择的设置来配置测量设备
234
测量
236
240
重复？
是
否
238
存储测量值并存储设置
输出测量值
242

图2C

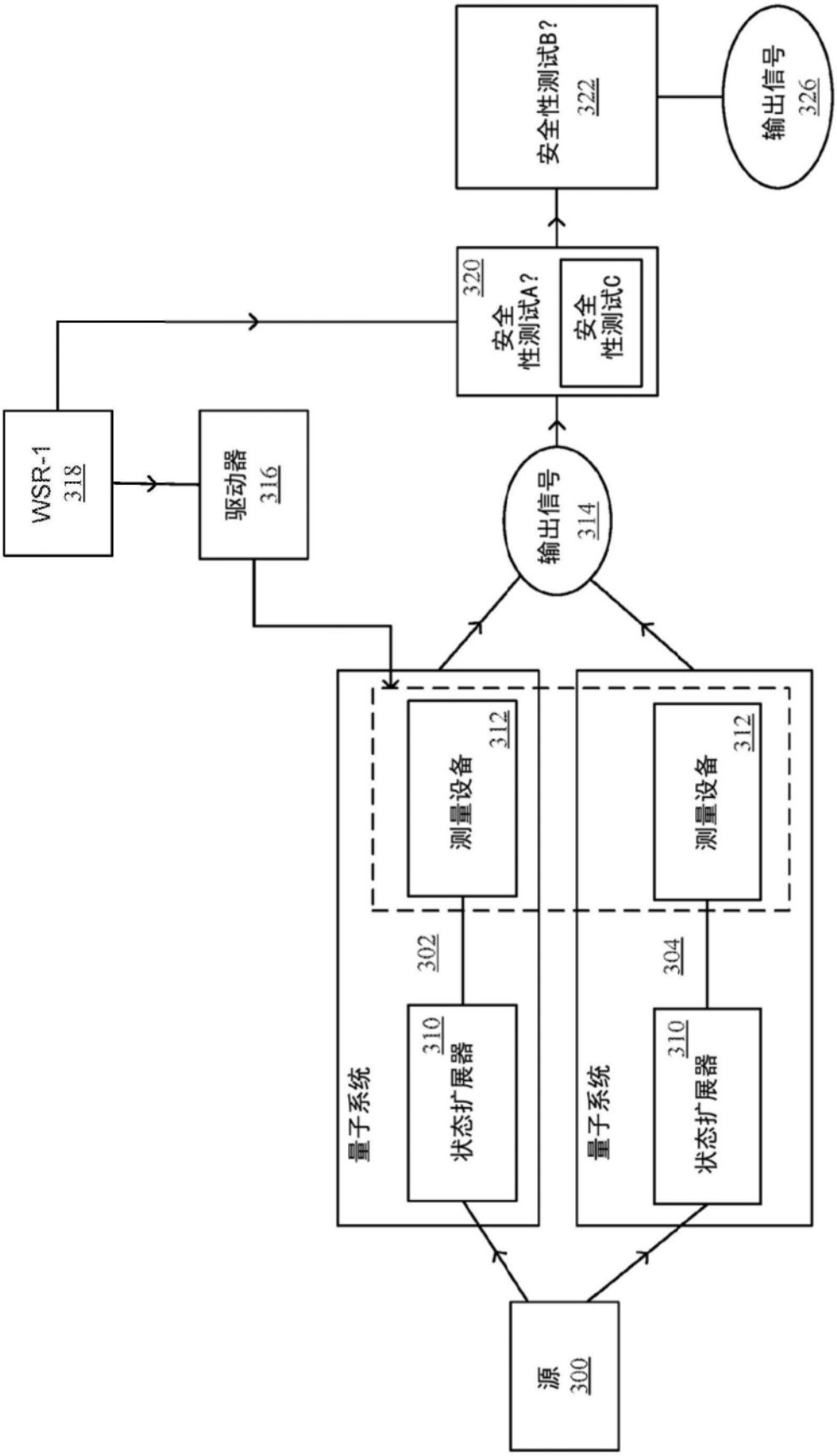

源
300
量子系统
302
304
状态扩展器
310
测量设备
312
输出信号
314
驱动器
316
WSR-1
318
安全性测试A?
320
安全性测试C
安全性测试B?
322
输出信号
326

图3A

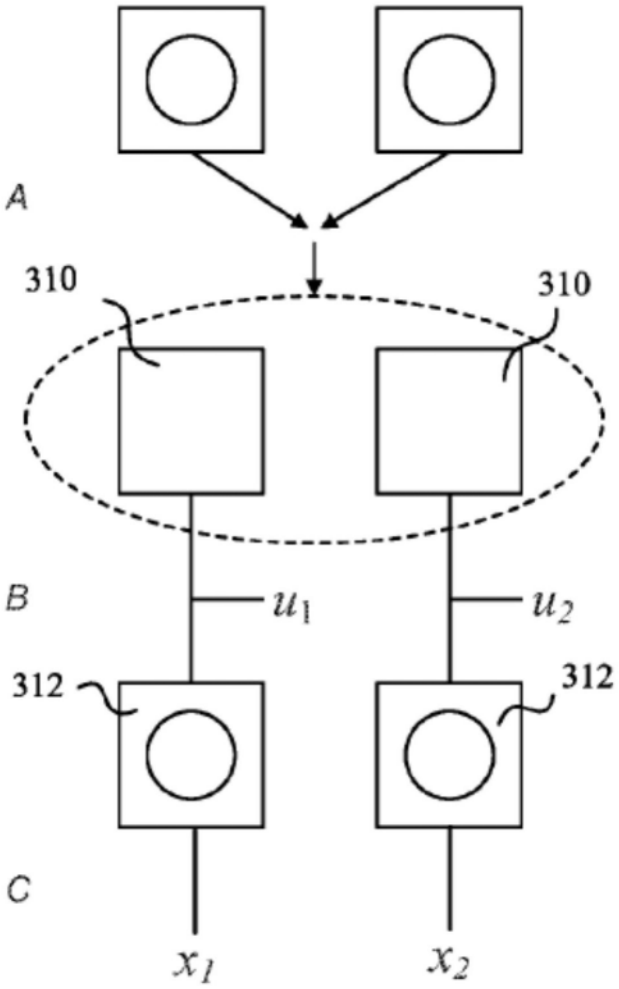


图3B

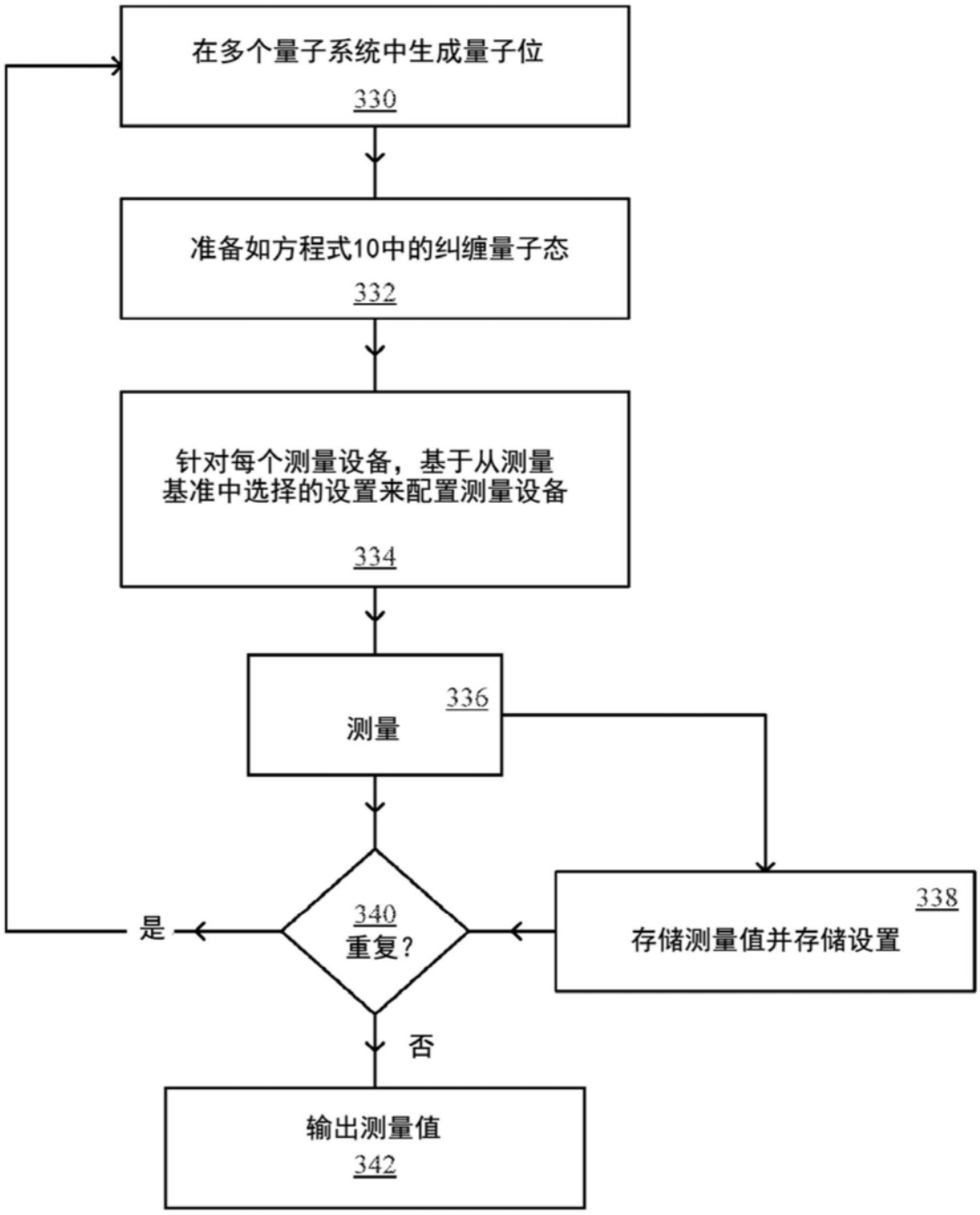

在多个量子系统中生成量子位
330
准备如方程式10中的纠缠量子态
332
针对每个测量设备，基于从测量基准中选择的设置来配置测量设备
334
测量
336
存储测量值并存储设置
338
重复？
340
是
否
输出测量值
342

图3C

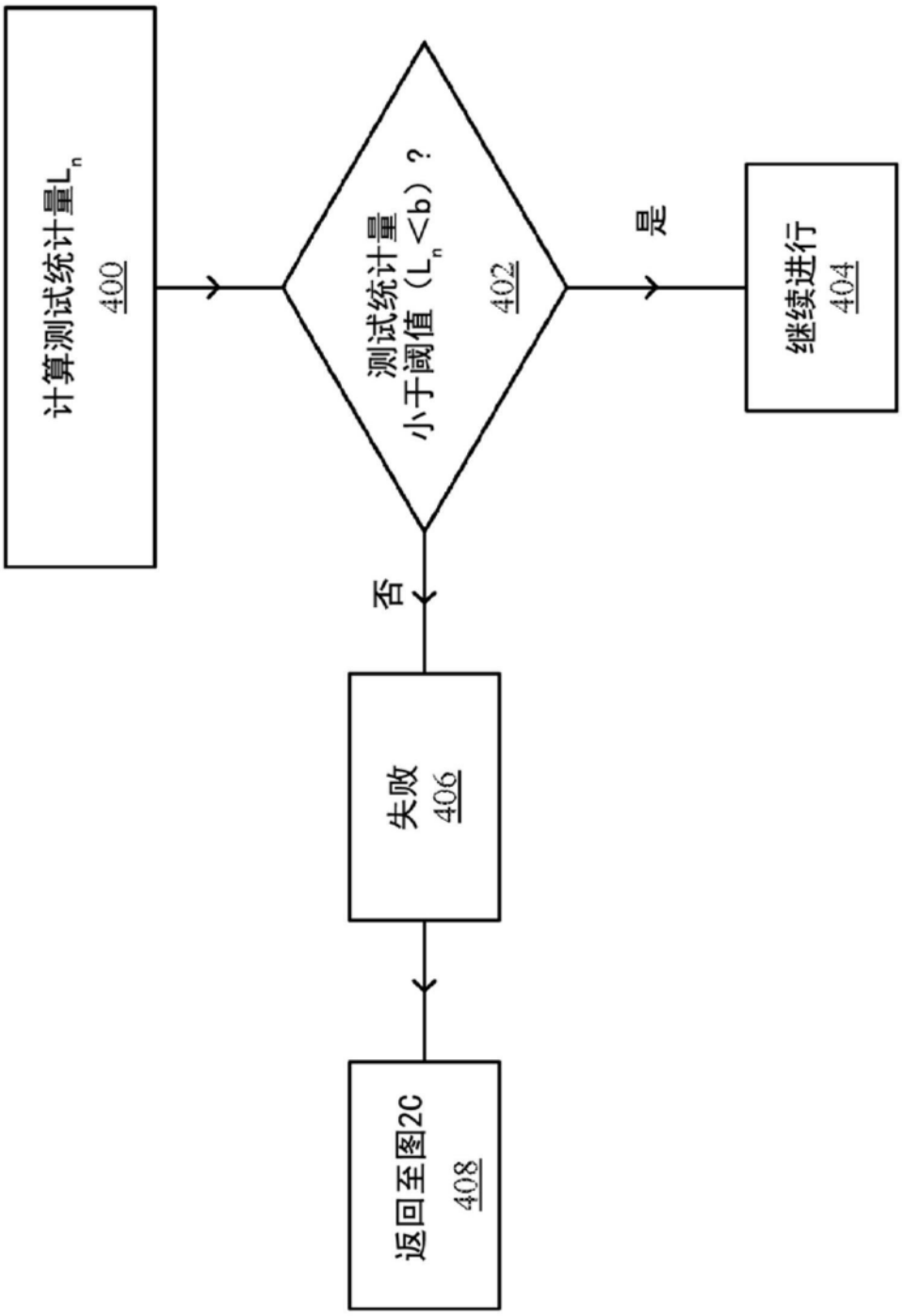

计算测试统计量L_n
400
测试统计量
小于阈值（L_n<b）？
402
是
继续进行
404
否
失败
406
返回至图2C
408

图4

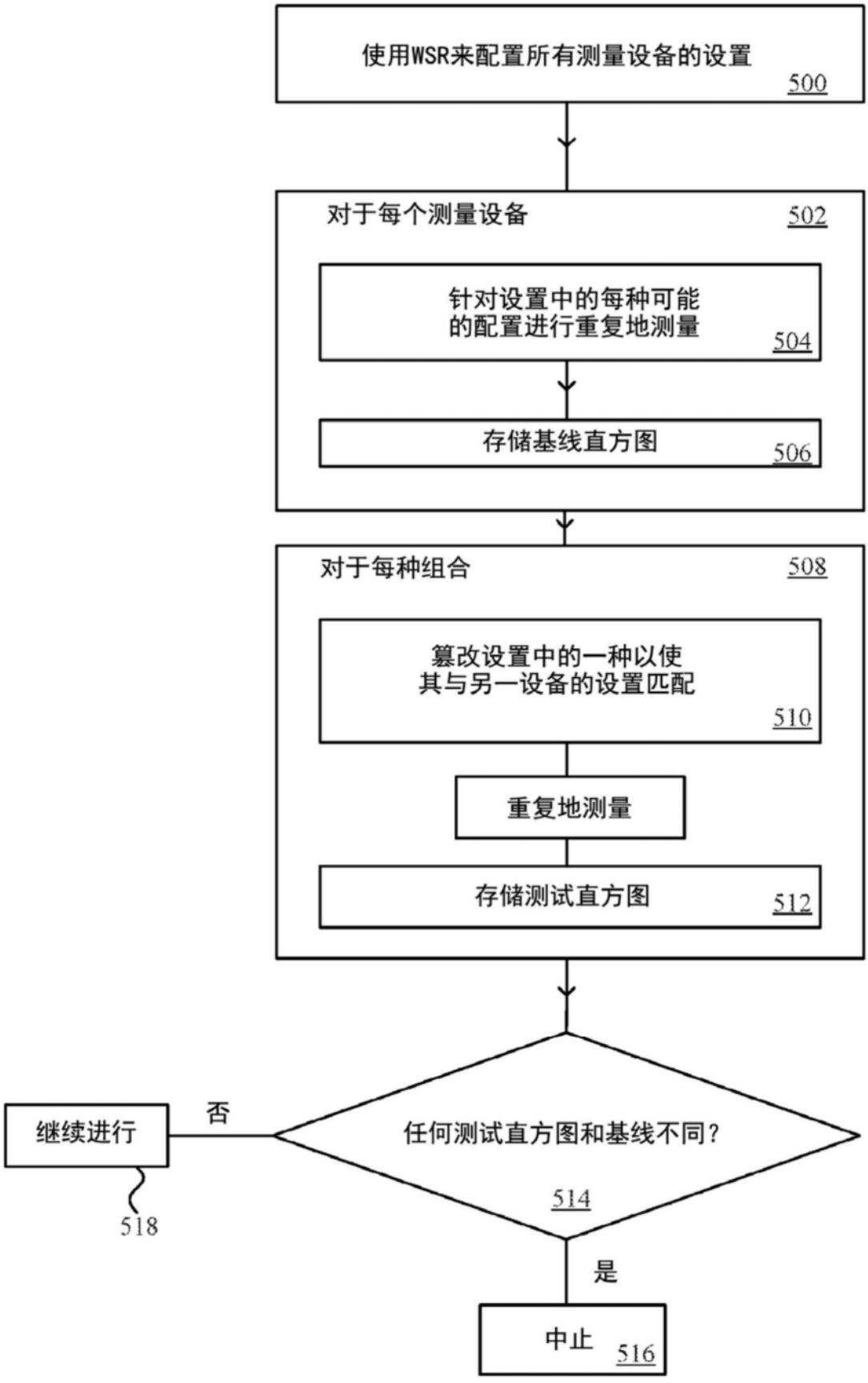

使用WSR来配置所有测量设备的设置
500
对于每个测量设备
502
针对设置中的每种可能的配置进行重复地测量
504
存储基线直方图
506
对于每种组合
508
篡改设置中的一种以使其与另一设备的设置匹配
510
重复地测量
存储测试直方图
512
任何测试直方图和基线不同？
514
否
继续进行
518
是
中止
516

图5

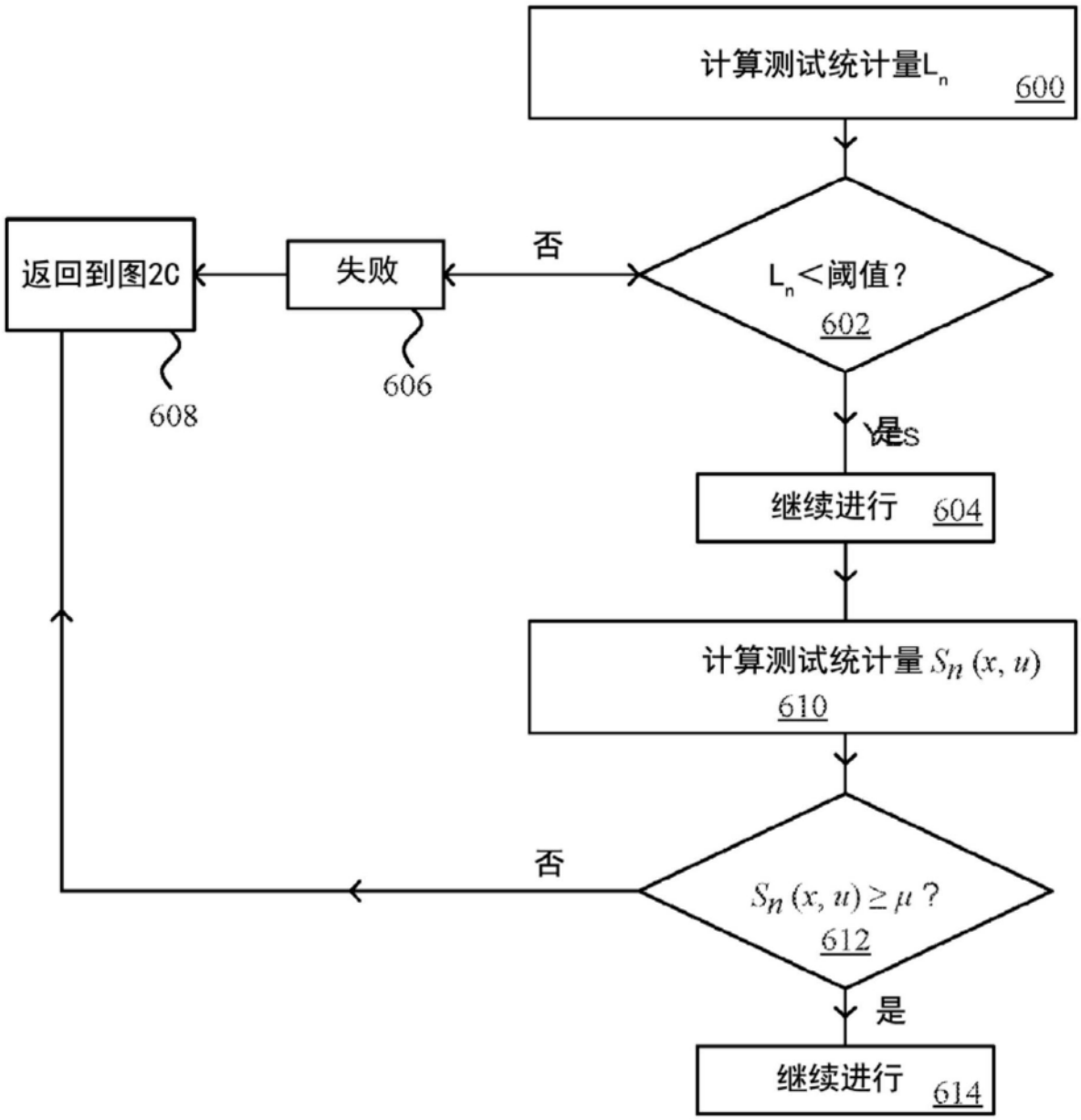

计算测试统计量L_n
600
L_n<阈值?
602
否
失败
606
返回到图2C
608
是
继续进行 604
计算测试统计量 $S_n(x,u)$
610
$S_n(x,u) \geq \mu$?
612
否
是
继续进行 614

图6

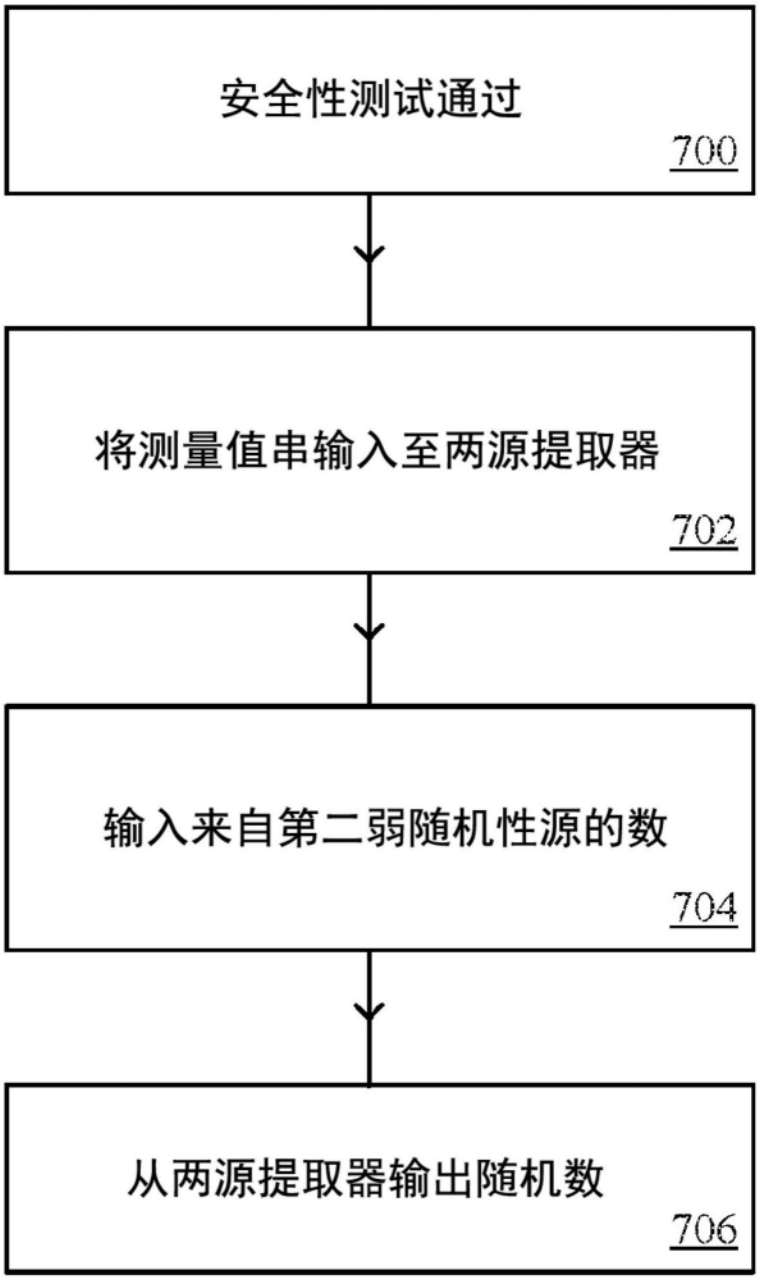

安全性测试通过
700
将测量值串输入至两源提取器
702
输入来自第二弱随机性源的数
704
从两源提取器输出随机数
706

图7

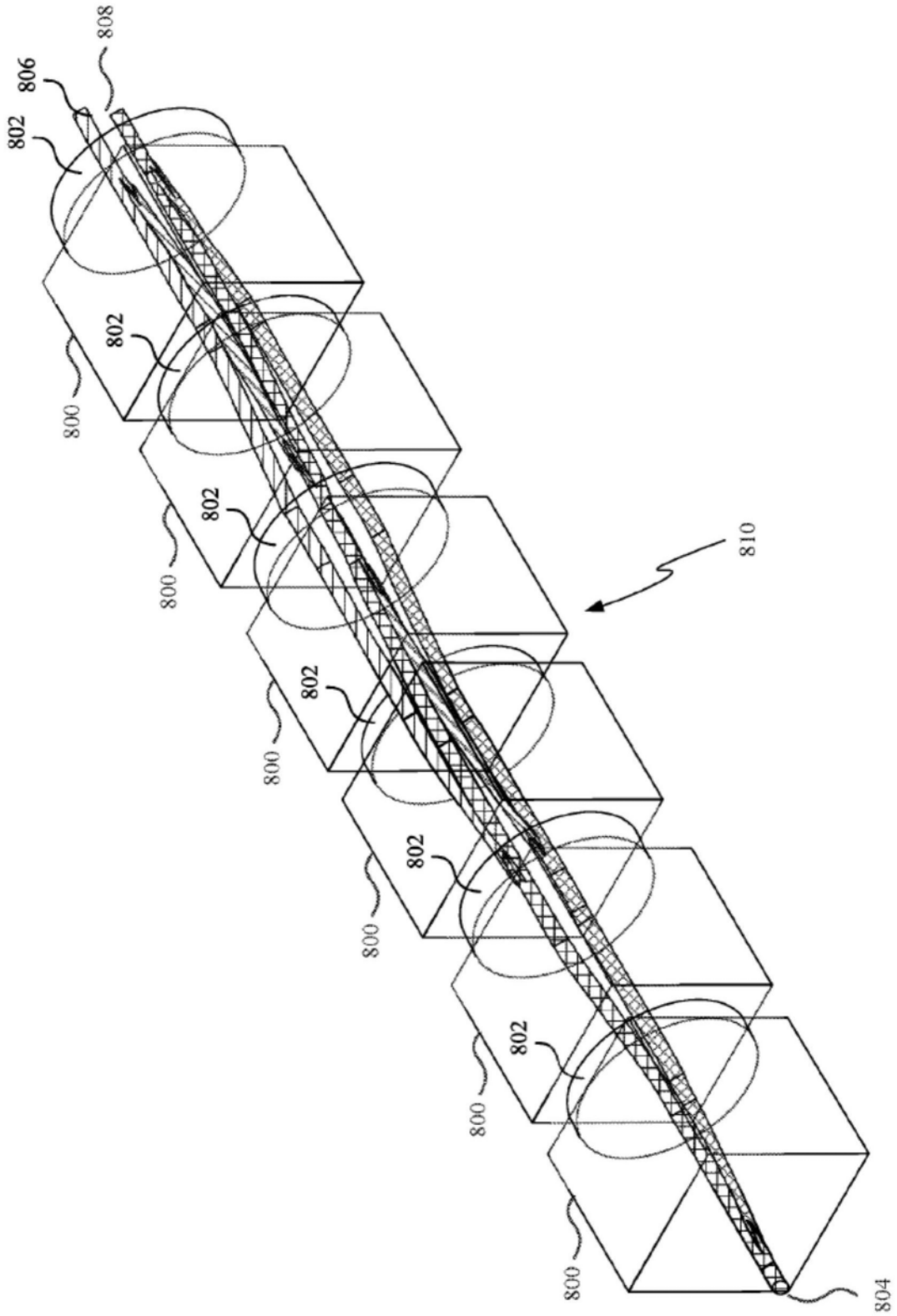


图8

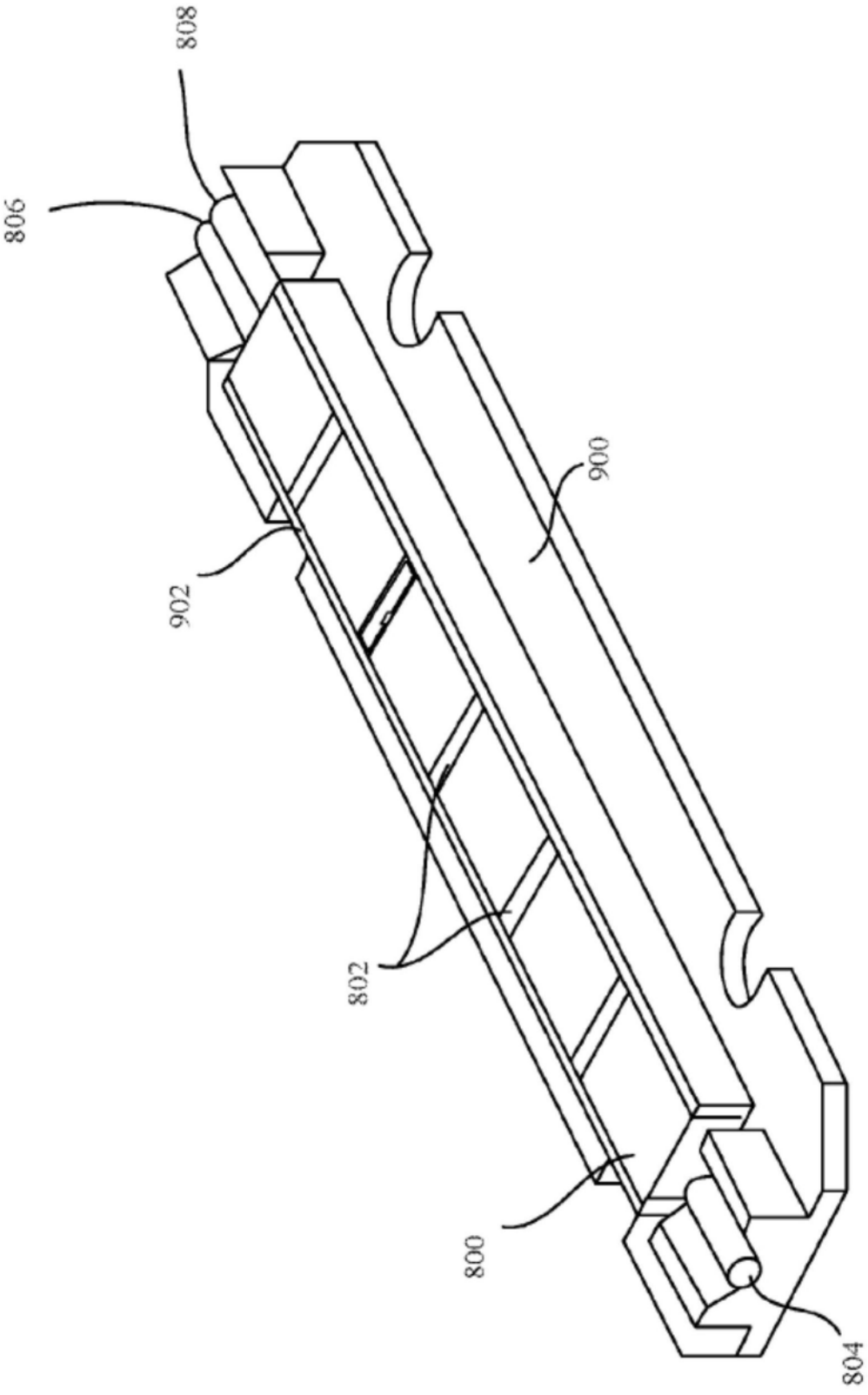


图9

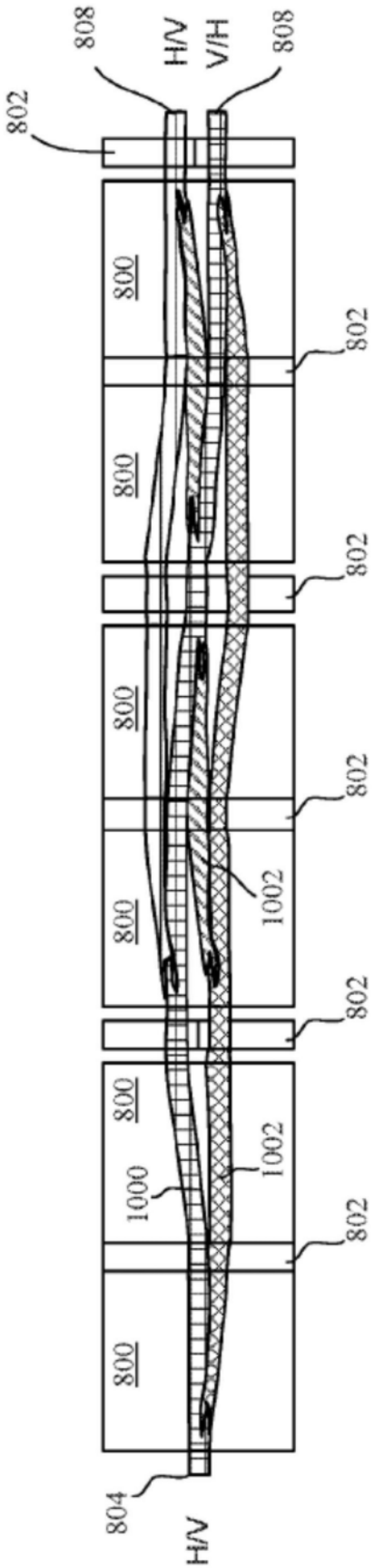

808
H/V
V/H
808
802
800
802
800
802
800
1002
802
800
1000
1002
802
800
804
H/V

图10

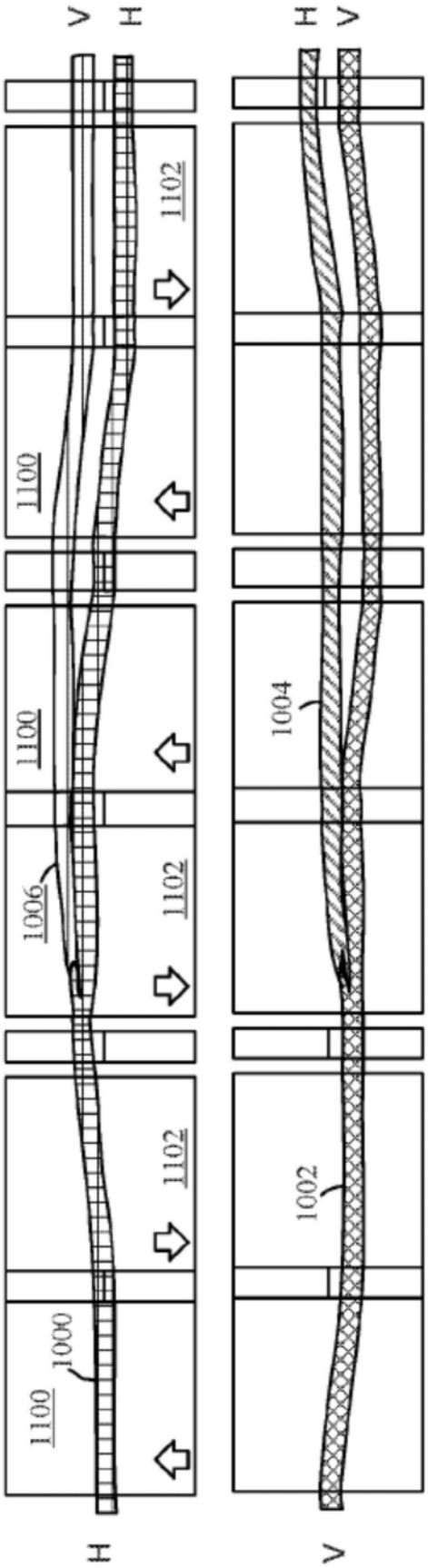


图11A

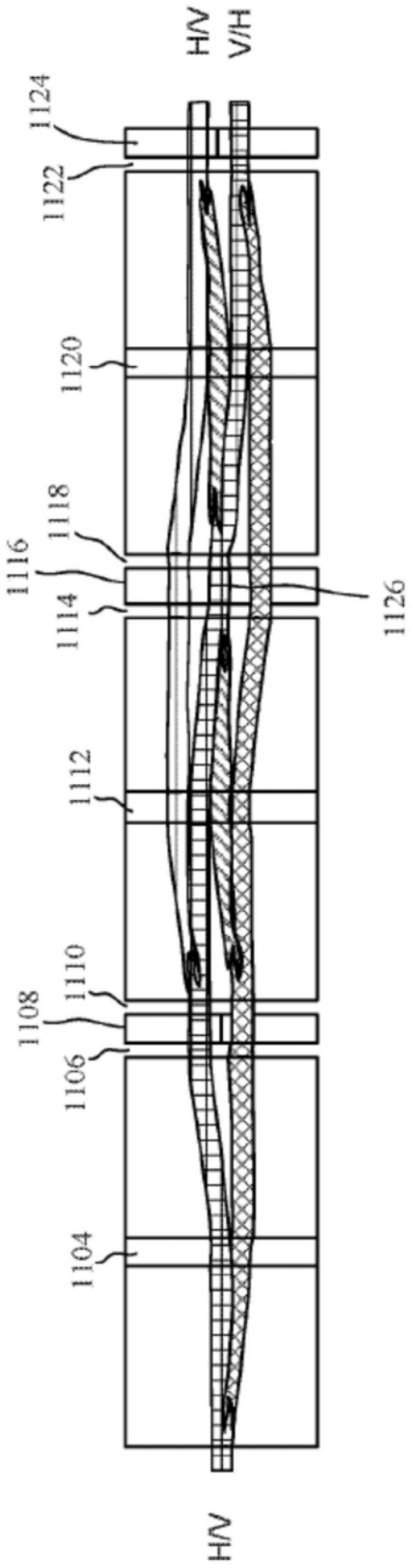

H/V
V/H
1124
1122
1120
1118
1116
1114
1126
1112
1110
1108
1106
1104
H/V

图11B

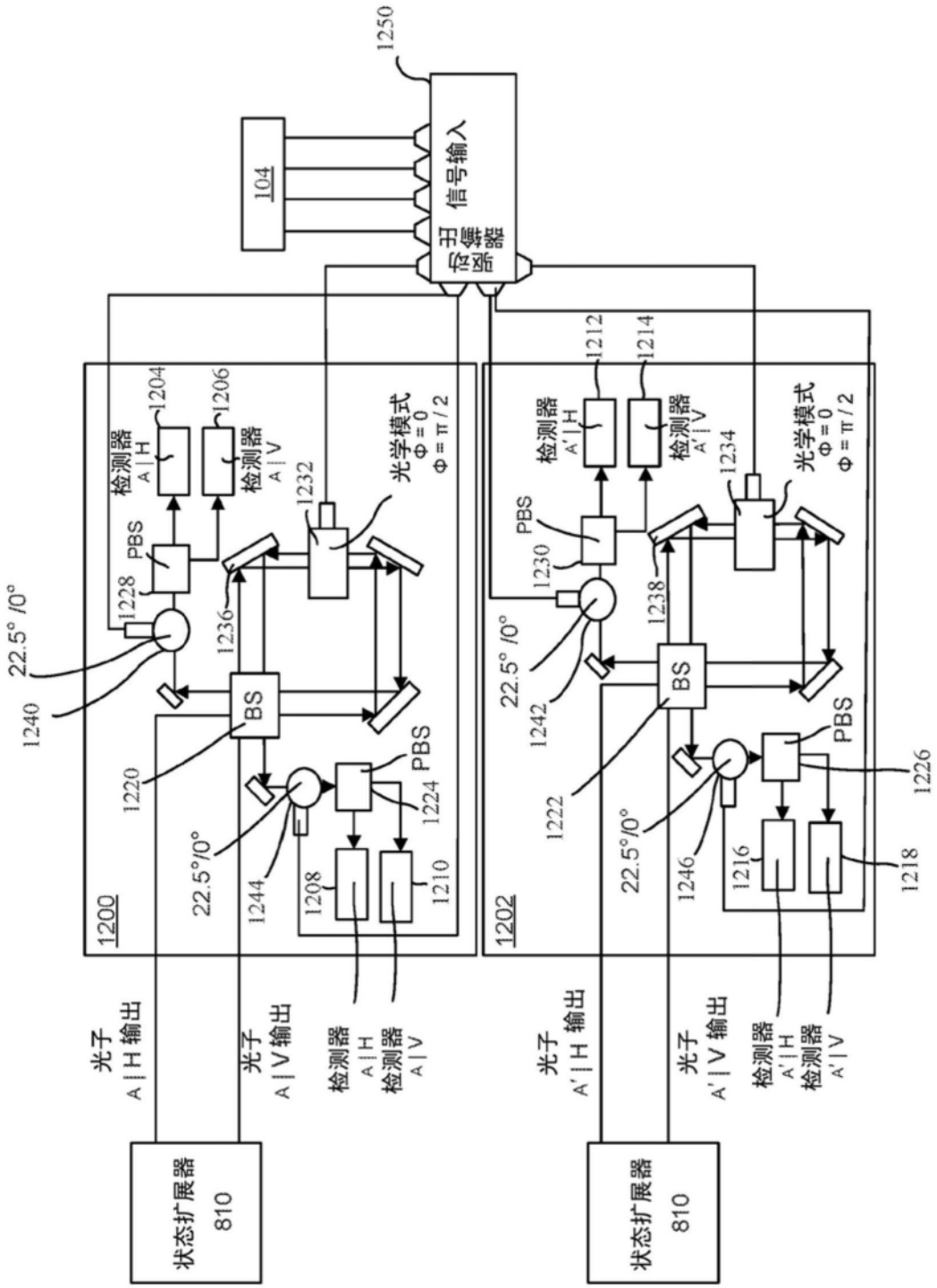

1250
驱动器和信号输入
104
1200
1202
检测器 A|H
检测器 A|V
光学模式 Φ=0 Φ=π/2
PBS
BS
22.5°/0°
1204
1206
1208
1210
1212
1214
1216
1218
1220
1222
1224
1226
1228
1230
1232
1234
1236
1238
1240
1242
1244
1246
光子 A|H 输出
光子 A|V 输出
检测器 A|H
检测器 A|V
光子 A'|H 输出
光子 A'|V 输出
检测器 A'|H
检测器 A'|V
状态扩展器 810
状态扩展器 810

图12