(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 103034818 B
(45)授权公告日 2017.04.12

(21)申请号 201210311768.1

(22)申请日 2012.08.29

(65)同一申请的已公布的文献号
申请公布号 CN 103034818 A

(43)申请公布日 2013.04.10

(30)优先权数据
13/220,012 2011.08.29 US

(73)专利权人 马克西姆综合产品公司
地址 美国加利福尼亚州

(72)发明人 J·马 S·U·郭 I·A·乔杜里

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 21/72(2013.01)

(56)对比文件
US 2009212945 A1,2009.08.27,
CN 101258552 A,2008.09.03,
US 6646565 B1,2003.11.11,
CN 1689367 A,2005.10.26,
US 2009146267 A1,2009.06.11,

审查员 马璐璐

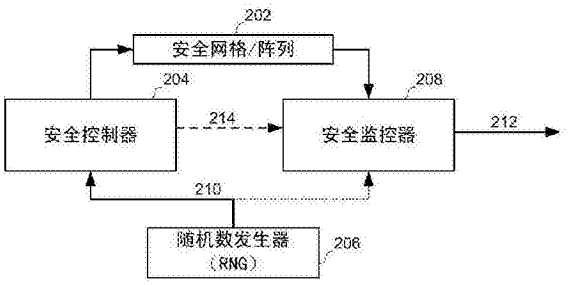
权利要求书3页 说明书9页 附图8页

(54)发明名称

用于检测和阻碍对安全系统的未授权访问和恶意攻击的系统和方法

(57)摘要

本发明的各个实施例涉及通过以下方式检测篡改和防止未授权访问的系统、设备和方法：将可编程性和随机性并入到对布置在安全系统中的敏感区域之上的导电线进行耦合、驱动和感测的过程中。这样的篡改检测系统包括安全网格网络、随机数发生器、安全控制器和安全监控器。该安全网格网络包含由导线制成的多个安全元件。该安全控制器选择安全元件的子集，形成安全阵列，以及产生驱动激励。该安全监控器选择SENSE节点，监控SENSE节点处的输出，以及产生指示篡改企图出现的标志信号。经由随机数将可编程性和随机性引入到包含阵列配置、驱动激励、SENSE节点以及检测模式的系统参数中的至少一项。



CN 103034818 B

1.一种安全系统中的篡改检测系统,包括:

包括多个安全元件的安全网格网络,每个安全元件是由位于集成电路的敏感区域之上的导电金属线制成的;

产生多个随机数的随机数发生器;

耦合在所述随机数发生器和所述安全网格之间的安全控制器,所述安全控制器通过以下方式对所述安全网格网络进行随机化:根据至少一个随机数选择所述多个安全元件的子集,根据阵列配置形成安全阵列,以及产生驱动激励以在至少一个FORCE节点处驱动所述安全阵列;以及

耦合至所述安全网格网络和所述安全控制器的安全监控器,所述安全监控器选择至少一个SENSE节点,根据检测模式监控所述SENSE节点处的输出,以及产生指示是否检测到篡改企图的标志信号,所述检测模式是与所述驱动激励相关联的。

2.根据权利要求1所述的篡改检测系统,其中,当所述多个随机数在两个连续检测周期之间改变时,所述安全阵列的所述阵列配置、所述至少一个SENSE节点和至少一个FORCE节点中的至少一个相应地由所述多个随机数确定。

3.根据权利要求1所述的篡改检测系统,其中,所述检测模式是根据从所述多个随机数中选择的随机数而从模拟检测模式、数字检测模式和混合检测模式中选择的。

4.根据权利要求1所述的篡改检测系统,其中,所述安全控制器和所述安全监控器包括用于访问所述安全元件的末端节点的模拟开关,使得这些末端节点能够被耦合以形成所述安全阵列,并且能够被选择作为所述SENSE节点和FORCE节点。

5.根据权利要求1所述的篡改检测系统,其中,所述检测模式为数字检测模式,使得所述安全控制器还包括数字激励产生器,所述数字激励产生器产生数字驱动激励以在所述FORCE节点处驱动所述安全阵列,并且所述安全监控器还包括数字检测电路,所述数字检测电路检测所述安全阵列的开路或短路状况。

6.根据权利要求1所述的篡改检测系统,其中,所述检测模式为模拟检测模式,使得所述安全控制器产生模拟驱动激励以驱动所述安全阵列,并且所述安全监控器还包括模拟检测电路,所述模拟检测电路检测所述安全阵列的电阻变化。

7.根据权利要求6所述的篡改检测系统,其中,所述模拟驱动激励是从电流和电压中选择的,并且所述安全控制器还包括从电流源和电压发生器中选择的模拟激励产生器。

8.一种检测安全系统中的集成电路中的篡改企图的方法,包括以下步骤:

(1)产生多个随机数;

(2)对安全网格网络进行随机化以形成安全阵列,所述安全网格网络包括布置在所述集成电路的敏感区域之上的多个安全元件;

(3)产生驱动激励以驱动所述安全阵列;

(4)从所述安全阵列中的末端节点和中间节点中选择SENSE节点;

(5)根据与所述驱动激励相关联的检测模式监控SENSE节点处的输出;以及

(6)输出指示是否检测到篡改企图的标志信号。

9.根据权利要求8所述的检测篡改企图的方法,其中,对安全网格网络进行随机化以形成安全阵列还包括以下步骤:

(a)根据至少一个随机数选择所述多个安全元件的子集,所述多个安全元件包含在覆

盖所述集成电路的敏感区域的安全网格网络中；

(b)根据阵列配置将所选择的安全元件串联耦合以形成安全阵列。

10.根据权利要求9所述的检测篡改企图的方法，其中，所述多个随机数在两个连续检测周期之间改变，所述安全阵列的所述阵列配置和至少一个SENSE节点相应地由所述多个随机数确定。

11.根据权利要求8所述的检测篡改企图的方法，其中，所述SENSE节点是根据从所述多个随机数中选择的第一随机数选择的。

12.根据权利要求8所述的检测篡改企图的方法，其中，所述检测模式是根据从所述多个随机数中选择的第二随机数而从模拟检测模式、数字检测模式和混合检测模式中选择的。

13.根据权利要求8所述的检测篡改企图的方法，其中，所述检测模式为数字检测模式，使得所述驱动激励包括数字数据序列，并且所述SENSE节点处的输出是与所述安全阵列的开路或短路状况相关联的。

14.根据权利要求8所述的检测篡改企图的方法，其中，所述检测模式为模拟检测模式，使得产生模拟驱动激励以驱动所述安全阵列，并且所述SENSE节点处的输出是与所述安全阵列的电阻变化相关联的。

15.根据权利要求14所述的检测篡改企图的方法，其中，所述模拟驱动激励是从电流和电压中选择的。

16.根据权利要求8所述的检测篡改企图的方法，其中，所述检测模式为混合检测模式，使得所述驱动激励是从由数字数据序列、电压和电流组成的组中选择的，并且监控所述输出以指示从所述安全阵列的开路电路、短路电路和电阻变化中选择的状况。

17.根据权利要求8所述的检测篡改企图的方法，其中，所述驱动激励是根据所述多个随机数中的另一随机数子集产生的。

18.一种安全系统中的篡改检测系统，包括：

包括多个安全元件的安全网格网络，每个安全元件是由位于集成电路的敏感区域之上的导电金属线制成的；

产生多个随机数的随机数发生器；

耦合在所述随机数发生器和所述安全网格网络之间的安全控制器，所述安全控制器通过以下方式对所述安全网格网络进行随机化：根据至少一个随机数选择所述多个安全元件的子集，根据阵列配置形成安全阵列，以及产生驱动激励以在至少一个FORCE节点处驱动所述安全阵列；以及

耦合至所述安全网格网络和所述安全控制器的安全监控器，所述安全监控器选择至少一个SENSE节点，根据混合检测模式监控所述SENSE节点处的输出，以及产生指示是否检测到篡改企图的标志信号，所述混合检测模式是与所述驱动激励相关联的。

19.根据权利要求18所述的篡改检测系统，其中，所述安全控制器包括至少一个数字激励产生器和至少一个模拟激励产生器，并且所述安全监控器包括至少一个数字检测电路和至少一个模拟检测电路，所述至少一个数字检测电路检测所述安全阵列的开路或短路状况，所述至少一个模拟检测电路检测所述安全阵列的电阻变化。

20.根据权利要求19所述的篡改检测系统，其中，所述至少一个数字激励产生器和所述

至少一个模拟激励产生器都耦合至所述随机数发生器，并且所述驱动激励是根据由所述随机数发生器产生的另一随机数子集产生的。

用于检测和阻碍对安全系统的未授权访问和恶意攻击的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2011年8月29日提交的题目为“Systems and Methods for Detecting and Thwarting Unauthorized Access and Hostile Attacks on Secured Systems”的美国专利申请No.13/220,012的优先权，在此以引用的方式将其主题并入本文。

技术领域

[0003] 本发明通常涉及安全系统，尤其涉及通过以下方式检测篡改和阻止未授权访问的系统、设备和方法：在对布置在安全系统中的敏感区域之上的导线进行耦合、驱动和感测的过程中并入可编程性和随机性感测。

背景技术

[0004] 安全系统一般指一种电子系统，该电子系统用于涉及在可信环境中对宝贵资产进行可信操作的应用。该电子系统可以包括集成电路，所述集成电路包含用于在安全系统中处理、存储或传输敏感数据的中央处理单元(CPU)核心、存储器以及输入/输出(I/O)外围设备。这种敏感数据可以包含账号、访问码、私有信息、金融交易/结余、权利管理、计量数据(例如，能量，单位)、程序算法和其他信息。迄今为止，安全系统已广泛地应用于安全关键应用(例如电子银行、商业交易和付费电视访问控制)或任意要求敏感资产保护的应用。

[0005] 小偷或黑客可能企图通过篡改集成电路(例如，CPU核心，存储器和I/O外围设备)的敏感区域来访问安全系统中的敏感数据。敏感区域一般由涂层材料的屏蔽层覆盖，另外，包含敏感区域的集成电路可以包装在屏蔽封装中。在未授权访问期间，为了获得对敏感区域和敏感数据的访问，黑客不得不刺穿屏蔽层或屏蔽封装。

[0006] 为了检测未授权访问，传统安全系统包含基于屏蔽层的篡改检测系统，该屏蔽层被配置成覆盖敏感区域的导线迹线(trace)。图1示出了由导线迹线覆盖的集成电路。力电路和感测电路集成在底层的集成电路中。所选迹线的一端可以由已知激励(例如，逻辑高或逻辑低)驱动，同时该迹线的另一端由感测电路监控。当检测到的电平与已知激励不符时，该迹线被认为是损坏的或短路至另一迹线，并且检测到屏蔽层的篡改。

[0007] 然而，这种检测容易绕过，并且可能无法满足随着使用了最新技术的安全系统而出现的严格安全要求。上述篡改检测方法仅仅检测屏蔽层中导电迹线的开路或短路。此外，黑客可以破译已知激励的模式，并且通过直接在用于感测的末端应用感测激励来绕过迹线。更直截了当地，黑客甚至可以使迹线的两端短路以避免篡改检测。由于黑客技术变得越来越精密，这样简单的篡改检测方法不能满足目的，不得不以相对低的成本引进竞争性的防篡改方法以阻止对安全系统的未授权访问，尤其是对于涉及不菲交易的那些安全系统更是如此。

发明内容

[0008] 本发明的各个实施例涉及通过以下方式检测篡改和阻止未授权访问的系统、设备和方法：在对布置在安全系统中的敏感区域之上的导线进行耦合、驱动和感测的过程中并入可编程性和随机性感测。经由随机数将可编程性和随机性引入包含阵列配置、驱动激励、SENSE节点以及检测模式在内的系统参数中的至少一项。

[0009] 本发明的一个方面为包括安全网格网络、随机数发生器、安全控制器和安全监控器的篡改检测系统。安全网格网络还包括多个安全元件，并且每个安全元件是由一条导电金属线制成的。随机数发生器产生多个随机数。安全控制器被耦合于随机数发生器和安全网格网络之间，根据从多个随机数中选择的至少一个随机数而从安全网格网络中选择安全元件子集，根据阵列配置形成安全阵列，以及产生驱动激励以驱动安全阵列。安全监控器被耦合至安全网格网络和安全控制器；并被用于选择至少一个SENSE节点，根据检测模式监控在SENSE节点处的输出，并产生指示是否检测到篡改企图的标志信号。

[0010] 本发明的另一方面为包括安全网格网络、随机数发生器、安全控制器和安全监控器的篡改检测系统。具体地，安全监控器是基于混合检测模式的，在该混合检测模式中可以以模拟检测模式或数字检测模式驱动和感测安全阵列。

[0011] 本发明的一个方面为检测安全系统中的篡改企图的方法。产生多个随机数。根据从多个随机数中选择的至少一个随机数而从多个安全元件中选择安全元件子集，并且所述多个安全元件包含在安全网格网络中，所述安全网格网络覆盖安全系统中的集成电路的敏感区域。所选安全元件根据阵列配置串联耦合以形成安全阵列。随后产生驱动激励以驱动安全阵列。从安全阵列中的末端节点和中间节点中选择SENSE节点，并根据与驱动激励相关联的检测模式监控在该SENSE节点处的输出。输出用于指示是否检测到篡改企图的标志信号。

[0012] 已经在该概要部分中概括地描述了本发明的某些特征和优点；然而，附加特征、优点和实施例在本文中给出或者鉴于其附图、说明书和权利要求对于本领域普通技术人员将会更加明显。因此，应当理解，本发明的范围不应由该概要部分中公开的特定实施例来限定。

附图说明

[0013] 将参考本发明的实施例，在附图中示出了这些实施例的例子。这些图旨在是说明性的，而非限制性的。虽然通常在这些实施例的上下文中描述本发明，但是应当理解，并非旨在将本发明的范围限于这些特定实施例。

[0014] 图(“FIG.”)1示出了由导线迹线覆盖的集成电路。

[0015] 图2示出了根据本发明各个实施例的在安全系统中的篡改检测系统的示例性框图。

[0016] 图3A示出了根据本发明各个实施例的集成电路块中的敏感区域的示例性横剖面。

[0017] 图3B示出了根据本发明各个实施例的第一集成电路的示例性横剖面，该第一集成电路包含由第二集成电路覆盖的敏感区域。

[0018] 图3C示出了根据本发明各个实施例的集成电路的示例性横剖面，该集成电路包含封装在两个印刷电路板(PCB)之间的敏感区域。

[0019] 图4A示出了根据本发明各个实施例的安全网格网络的示例性图。

[0020] 图4B示出了根据本发明各个实施例的安全网格网络或阵列202中的安全元件的示例性图。

[0021] 图5A至图5C示出了根据本发明各个实施例的安全阵列的三个示例性阵列配置。

[0022] 图6A示出了根据本发明各个实施例的基于数字检测模式的篡改检测系统的示例性框图。

[0023] 图6B示出了根据本发明各个实施例的以模拟模式驱动安全阵列的安全控制器的示例性框图。

[0024] 图6C示出了另一根据本发明各个实施例的以模拟模式驱动安全阵列的安全控制器的示例框图。

[0025] 图6D为根据本发明各个实施例的模拟检测电路的示例性框图，该模拟检测电路可以包含在处于模拟模式的安全监控器中。

[0026] 图7A示出了根据本发明各个实施例的安全阵列的示例性阵列配置，其包括被驱动用于模拟检测模式的两个安全元件。

[0027] 图7B示出了根据本发明各个实施例的安全阵列的示例性阵列配置，其中，安全元件被篡改。

[0028] 图8示出了根据本发明各个实施例的篡改检测方法的示例性流程图。

具体实施方式

[0029] 在以下描述中，为了解释的目的，给出了具体的细节以提供对本发明的理解。然而，对于本领域的技术人员来说很明显的是，可以在不具有这些细节的情况下实施该发明。本领域的技术人员将认识到以下描述的本发明的实施例可以以多种方式以及使用各种结构来执行。本领域的技术人员还将认识到另外的修改、应用以及实施例也落在其范围之内，本发明也可以在其它领域中提供应用。因此，以下描述的实施例用于说明本发明的特定实施例以及要避免使本发明模糊。

[0030] 说明书中对“一个实施例”或“实施例”的提及意味着结合该实施例描述的特定特征、结构、特性或功能包含在本发明的至少一个实施例中。在说明书的各个地方中出现短语“在一个实施例中”、“在实施例中”等未必都是指相同的实施例。

[0031] 此外，图中组件之间的或方法步骤之间的连接不限于直接实现的连接。相反，图中示出的组件之间的或方法步骤之间的连接可以通过向其增加中间组件或方法步骤而被修改或改变，而不背离本发明的教导。

[0032] 并不是使用可预测激励驱动的导电迹线，本发明引入了由可编程激励驱动的并且在可编程模式下被检测的可编程网格网络。可编程网格网络包括安全元件阵列，每个安全元件由位于敏感区域中的子区域之上的导电迹线形成。根据阵列配置选择并布置多个安全元件以形成安全阵列。该阵列可以由某个激励驱动，并根据从包括模拟模式、数字模式和混合模式的组中选择的检测模式在所选择的节点处被感测。因此，本发明的各个实施例涉及基于可编程性(尤其是阵列配置、驱动激励、感测节点和检测模式的可编程性)的防篡改系统、设备和方法感测。这样的可编程性增强了安全系统的安全级别并减少了安全系统被篡改的机会。

[0033] 图2示出了根据本发明各个实施例的在安全系统中的篡改检测系统的示例性框

图。该篡改检测系统包括安全网格网络或阵列202、安全控制器204、随机数发生器(RNG)206以及安全监控器208。根据由RNG 206提供的至少一个数在安全控制器204和安全监控器208中引入该篡改检测系统的可编程性，以使得以随机的方式来配置、驱动或感测安全网格网络或阵列202感测，从而向任意的黑客篡改企图施加挑战。

[0034] 安全网格网络或阵列202包括安全元件阵列，该安全元件阵列覆盖可以处理或存储敏感数据的敏感区域。在某个实施例中，每一安全元件可以与一导线相关联，因此，安全网格网络或阵列202中的每个安全元件可以模型化为电阻器，该电阻器在该网络上具有基本恒定的电阻R_{SE}。

[0035] RNG 206产生多个随机数210，所述多个随机数210包含用于选择至少一个安全元件的至少一个随机数。在本发明的各个实施例中，可以在一个检测周期期间由RNG 206产生多个随机数210以与多个安全元件相关联。此外，除了指定安全元件之外，随机数210也可以用于设定在安全控制器204和安全监控器208中使用的参数，并且包含驱动激励、SENSE(感测)节点和检测模式在内的这些参数确定篡改检测系统的可编程性。

[0036] 安全控制器204耦合于RNG 206和安全网格网络或阵列202之间。在某个检测周期期间，安全控制器204从RNG 206接收多个随机数210，选择安全网格网络204中的多个安全元件，形成安全阵列，并用驱动激励驱动安全阵列。结果，安全网格网络或阵列202在它的组织、驱动位置或驱动方法方面被安全控制器204进行随机化和编程。

[0037] 根据随机数210选择安全元件是，并且通过根据阵列配置布置这些安全元件来形成安全阵列。阵列配置不仅指所选择的用于形成安全阵列的安全元件，而且也指这些元件形成安全阵列的顺序。在某些实施例中，这些元件的顺序是从RNG 206产生用于选择安全元件的这些随机数210的顺序。

[0038] 驱动激励可以从数字数据序列和模拟电压/电流电平中进行选择，并被应用在安全阵列中的力节点。在一个实施例中，数字数据序列和模拟电平都是根据由RNG 206提供的随机数210产生的。在另一实施例中，该驱动激励是在安全控制器204中内部地确定的。

[0039] 安全监控器208耦合至安全网格网络或阵列202，从安全阵列中选择至少一个SENSE节点，监控在SENSE节点处的输出，并产生标志信号212。具体地，安全监控器208根据从模拟检测模式、数字检测模式和混合检测模式中选择的检测模式来监控输出。在本发明的各个实施例中，SENSE节点和检测模式的选择也可以由RNG 206产生的随机数210确定。由于检测模式和SENSE与阵列配置和驱动激励一致，因此安全监控器208可以接收到由安全控制器204提供的相关联的安全模式信号214。

[0040] 可以从数字模式、模拟模式和混合模式中选择检测模式。安全控制器208中的检测模式与由安全控制器204产生的驱动激励一致。在数字模式中，驱动激励与包括逻辑高和逻辑低的数字数据序列相关联，并被应用于安全阵列中的至少一个FORCE(力)节点。对至少一个SENSE节点而非FORCE节点处的输出进行感测，并将其与激励相比较。在模拟模式中，驱动激励可以与电流、电源电压V_{DD}或变化的电压电平相关联。在还将激励应用于安全阵列中的至少一个FORCE节点上的同时，基于该激励的时机电压电平对至少一个SENSE节点的输出进行分析，并且该输出用于确定是否存在由于篡改而引起的诸如开路或短路之类的电属性改变。模拟模式特别用于在只有安全元件的一部分被绕过时检测部分短路情况中的篡改企图。在混合模式中，在一个安全系统内，在不同检测周期中使用模拟模式和数字模式的。

[0041] SENSE节点不限于包含在包括所选安全元件的安全阵列中的节点。位于安全阵列上的SENSE节点处的输出依赖于驱动激励，并且标志信号212与这种依赖性的有效性相关联。然而，当SENSE节点并非位于安全阵列上时，输出与驱动激励并不相关，并且标志信号212与这种非相关性的有效性相关联。

[0042] 结果，标志信号指示是否检测到篡改和未授权访问。在检测到篡改时，集成电路可以进一步使用标志信号来使能一系列动作，包括擦除敏感数据、触发不可屏蔽的中断、在标志寄存器中写值、重置电路以及运行专用代码。

[0043] 随机数210还可以用另外的方式标识阵列配置。随机数210不是与安全元件相关联，而是直接与阵列配置相关联，即特定安全元件的特定组合。例如，随机数210与第一行安全元件从左至右串联耦合的阵列配置相关联。RNG 206每次产生与阵列配置相关联的一个随机数。安全控制器204直接连接与该阵列配置相关联的多个安全元件。结果，安全控制器204还可以包括存储器，该存储器存储将每个随机数与多个安全元件相关联的查找表以及连接这些安全元件的配置。

[0044] 在本发明的各个实施例中，安全控制器204和安全监控器208都包括多个用于访问安全元件的末端节点的模拟开关，以使得这些末端节点可以耦合以形成安全阵列并分别被选择作为感测节点或力节点。

[0045] 可以在包含敏感区域的集成电路的同一衬底上或封装上制造安全网格网络或阵列202。如下，基于该系统的示例性横剖面公开了制造篡改检测系统的三种示例性方法。

[0046] 图3A示出了根据本发明各个实施例的集成电路块中的敏感区域的示例性横剖面300。集成电路块构建在包含晶体管304和晶体管306的集成电路(IC)衬底302上。安全控制器204和安全监控器208以及RNG 206是由这些晶体管制成的。从而，在IC衬底302上连续地制造多个多晶硅层(例如多晶硅1，多晶硅2)和金属层(例如，金属1-5)，以作为晶体管304和306的栅和/或互连。安全网格网络或阵列202可以集成到金属层之中，并且安全网格网络或阵列202中的安全元件经由中间金属层耦合至底层的电子器件。本领域的技术人员知道安全网格网络或阵列202优选地是使用顶部金属层形成的，然而，安全网格网络或阵列202可以由顶部金属层下部的任意金属层形成。

[0047] 图3B示出了根据本发明各个实施例的第一集成电路342的示例性横剖面340，该第一集成电路342包含由第二集成电路344覆盖的敏感区域。安全网格网络或阵列202可以由第二集成电路中的金属层制造，该第二集成电路位于包含于第一集成电路中的敏感区域顶上。安全控制器204和安全监控器208以及RNG 206可以集成在第一集成电路342和第二集成电路344中的任一个上。然而，当安全网格网络或阵列202和篡改检测电路的其余部分位于两个分离的衬底上时，需要安排互连的路径以通过两个衬底342和344之间的接口346和348。

[0048] 图3C示出了根据本发明各个实施例的集成电路382的示例性横剖面380，该集成电路382包含被封装在两个印刷电路板(PCB)384和386之间的敏感区域。该集成电路安装在PCB 386的衬底上，并且经由线392和线394超声地接合至PCB 386。PCB 384在接口388和接口390处耦合至PCB 386以封装集成电路382。可以在PCB 384的金属层中制造安全网格网络或阵列202，而篡改检测电路的其余部分集成在集成电路382的衬底上。

[0049] 在本发明的各个实施例中，安全网格网络或阵列202可以但不限制于形成在单个

金属层之中。安全网格网络可以形成在多于一个的金属层上，并且需要某种布线方案以将安全网格网络或阵列202耦合至安全控制器204和安全监控器208。

[0050] 图4A示出了根据本发明各个实施例的安全网格网络或阵列202的示例性图。安全网格网络或阵列202包括以x列和y行布置的N个相同安全元件402。安全元件402包括可以在单个层或多于一个的金属层上实现的导电金属线。导电金属线可以为沿着元件的行、列或对角线方向被布线在元件上的直线，并且导电金属线也可以布置为多种形状。

[0051] 图4B示出了根据本发明各个实施例的安全网格网络或阵列202中的安全元件402的示例性图。安全元件402包括一段蜷曲形状的金属线和两个末端节点。该两个末端节点为节点A和节点B，节点A和节点B可以被耦合用于安全元件402的驱动和感测或者可以耦合至其它安全元件的末端节点。

[0052] 不管其配置如何，每个安全元件与电阻R_{SE}相关联。篡改一般涉及移除部分或整个安全网格网络或阵列202或直接刺穿安全网格网络或阵列202以访问敏感区域。结果，在篡改时，对于被旁路、被损坏或部分短路的安全元件，电阻R_{SE}分别改变到0、无穷大或不同的值。

[0053] 根据由RNG 206产生的随机数选择安全网格网络或阵列202中的安全元件，并根据阵列配置形成安全阵列。图5A-图5C示出了根据本发明各个实施例的安全阵列的三个示例性阵列配置502、504和506。在阵列配置502中，安全阵列包括一个安全元件。在阵列配置504中，安全阵列包括行R_1中的所有安全元件和行R_2中的几个安全元件。这些元件串联耦合，并且具体地，行R_1中的安全元件从左至右连接，而行R_2中的那些安全元件从右至左连接。行R_2中的元件在行R_1中的那些元件之后，并且安全阵列在行R_2的开始处结束。在阵列配置506中，安全阵列包括从所有行R_1至R_y选择的安全元件，并且至少一个所选择的安全元件与每一行相关联。这些元件串联耦合，并且未选择的安全元件C_2可以位于两个所选择的元件(例如，C_1和C_X)之间。可以通过经由除了用于元件C_2的金属层以外的金属层进行布线来绕过该元件C_2。

[0054] 上述安全阵列采用串联电阻串的优选阵列配置。在该优选配置中，每个安全阵列可以模型化为一系列电阻器，每个电阻器表示一安全元件。安全阵列具有两个末端节点，并且这两个末端节点之间的电阻为包含在该安全阵列之中的安全元件电阻的总和。在阵列配置504和506中，中间节点位于每两个串联安全元件之间。

[0055] 在本发明的各个实施例中，阵列配置502至506可以与二元状态检测模式相关联。安全控制器204在一个FORCE节点上传递驱动激励，安全监控器206监控来自另一SENSE节点的输出。FORCE节点是从两个末端节点和中间节点中选择的。SENSE节点与FORCE节点不同，并且可以不限制于末端节点或中间节点。

[0056] 二元状态检测模式是一种数字检测模式，并且具体地，驱动激励是与时变二元模式相关联的数字信号。当从末端节点或中间节点中选择SENSE节点时，所检测到输出与时变二元模式相一致；否则，当SENSE节点不在电阻串的路径中时，所检测到输出可能不符合该模式。当检测到意外输出时，由标志信号对错误进行标记。

[0057] 图6A示出了根据本发明各个实施例的基于数字检测模式的篡改检测系统的示例性框图600。在篡改检测系统600中，安全控制器204和安全监控器208分别连接至安全网格网络或阵列202的FORCE节点和SENSE节点。安全控制器204用数字激励来驱动安全网格网络

或阵列202，安全监控器208验证SENSE节点处的数据有效性。

[0058] 安全控制器204包括复用器610。根据由RNG 206提供的随机数210，由复用器610选择并耦合安全阵列中的安全元件。复用器610包含被安全控制器204和安全监控器208使用的模拟开关，以使得安全阵列中的末端节点和中间节点是可访问的，从而形成安全阵列并输出标志信号。

[0059] 安全控制器204还包括数字激励产生器612，该数字激励产生器612还包括状态机602、随机比特产生器604和缓冲器606。状态机602对控制器204中的操作序列进行控制。随机比特产生器604耦合至状态机602，并根据状态机602产生随机比特(即，逻辑高或逻辑低)的数字序列。随机比特产生器604也可以包含在随机数发生器206中。缓冲器606耦合至随机比特产生器604以适当地驱动安全网格网络或阵列202。

[0060] 安全控制器204包括耦合至安全网格网络或阵列202的SENSE节点的数字检测电路。该数字检测电路检测安全阵列的开路或短路状况。在某个实施例中，数字检测电路为XOR逻辑，当SENSE节点处的输出与数字序列中的随机比特不一致时该逻辑输出逻辑高。

[0061] 图6B示出了根据本发明各个实施例的以模拟模式驱动安全网格网络或阵列202的安全控制器的示例性框图620。安全网格网络或阵列202的两个末端节点分别接地以及由包括电流源622的安全控制器204驱动。电流源622耦合至电压源，并产生电流I_{DR}以注入安全网格网络或阵列202。在一个实施例中，电流源622基于由RNG 206控制的数模转换器(DAC)，并且所产生的电流I_{DR}的大小也由RNG 206产生的随机数指定。

[0062] 可以在SENSE节点处监控输出，该感测节点是从耦合至电流源622的末端节点FORCE-1(力-1)和安全网格网络或阵列202中的中间节点选择的。假定SENSE节点和地之间的电阻为R_{AN}，输出电压可以由$I_{DR} \times R_{AN}$表示。在一个实施例中，安全网格网络或阵列202包含一个安全元件，在注入电流I_{DR}的相同末端节点处的输出电压简单地为$I_{DR} \times R_{SE}$。

[0063] 图6C示出了根据本发明各个实施例的以模拟模式驱动安全网格网络或阵列202的安全控制器的另一示例性框图640。安全网格网络或阵列202包括串联布置的多个安全元件。安全控制器204包含两个缓冲器642和644，这两个缓冲器可以分别将两个末端节点FORCE-1(力-1)和FORCE-2(力-2)耦合至电源电压V_{DD}和地。在一些实施例中，安全控制器204还可以包括电压发生器，该电压发生器产生除了电源电压V_{DD}以外的电压V_{DR}以驱动安全阵列。电压发生器可以基于DAC，该DAC根据由RNG 206提供的随机数输出电压V_{DR}。

[0064] 可以在从安全网格网络或阵列202中的中间节点中选择的SENSE节点处监控输出。在一个实施例中，安全网格网络或阵列202包含两个串联的安全元件，在它们之间的中间节点处测试输出电压。因此，在没有篡改企图的情况下，SENSE节点处的输出电压大约为$1/2V_{DD}$，然而，在存在这样的企图时，输出电压向V_{DD}或地移位。

[0065] 图6D为根据本发明各个实施例的模拟检测电路的示例性框图660，该模拟检测电路可以包含在处于模拟模式的安全监控器208中。模拟检测电路660包括参考信号发生器662和比较器664，并检测安全阵列中的电阻变化。参考信号发生器662被耦合以接收由安全控制器204提供的安全模式信号214，并根据阵列配置产生参考电压V_{REF}。安全模式信号214也用于选择感测节点，并允许根据感测节点的位置产生电压V_{REF}。在模拟模式中，比较器664可以由使能信号使能以将感测节点处的输出与参考电压V_{REF}进行比较。

[0066] 篡改企图一般与至少一个安全元件的开路电路、完全短路或部分短路相关联。安

全元件的电阻会改变。相应地，SENSE节点处的输出电压从参考电压V_{REF}漂移。因此，比较器664用于检测输出电压的漂移以及因此由篡改努力引起的电阻变化。

[0067] 在本发明的各个实施例中，比较器664检测大于容许电压V_{TH}的输出电压漂移。该电压V_{TH}足够大以适应由制造工艺引起的漂移，同时被控制以检测较小的篡改努力。

[0068] 图7A示出了根据本发明各个实施例的安全阵列的示例性阵列配置700，其包括被驱动用于模拟检测模式的两个安全元件702和704。这两个安全元件是根据由RNG 206提供的两个随机数选择的，并且它们可以物理地互相邻近或间隔开。安全阵列700包括两个末端节点FORCE-1(力-1)和FORCE-2(力-2)以及一个中间节点SENSE(感测)。

[0069] 阵列配置700与中间状态检测模式相关联，该中间状态检测模式为模拟检测模式。安全控制器204分别以高电压和低电压(例如，V_{DD}和地)驱动两个末端节点(即，FORCE-1(力-1)和FORCE-2(力-2))，并且安全监控器206监控来自感测节点的输出。未被篡改的安全阵列700与基本上为高电压和低电压的平均值的输出相关联。

[0070] 在某些实施例中，元件702在篡改后是损坏的、部分或完全短路。结果，在感测节点处监控的输出从未被篡改的安全阵列中的高电压和低电压的平均电平分别变化至低电压(例如，地)、升高的电压或高电压(例如，V_{DD})。如果输出在平均电平窗口之外，那么检测到篡改。

[0071] 安全网格网络或阵列202的某个阵列配置可以与安全控制器208中的模拟检测模式和数字检测模式之间的优选检测模式相关联。图7B示出了根据本发明各个实施例的安全元件702被篡改的安全阵列的示例阵列配置750。黑客刺穿该安全元件702，并创建开路电路。虽然数字模式和模拟模式都可以被采用，但是优选的是模拟模式。在二元状态检测模式中，将驱动激励应用到节点FORCE-1(力-1)或FORCE-2(力-2)。如果黑客可以使用一条线来使节点FORCE-1(力-1)和SENSE(感测)短路，从而绕过开路电路区域，那么安全监控器208可能无法检测到这种未授权访问。然而，在中间状态检测模式中，分别在节点FORCE-1和FORCE-2上应用高电压和低电压。因此，当黑客绕过该安全元件702中的整个或部分线时，安全监控器208检测到节点SENSE处的输出从高电压和低电压的平均值向高电压偏移。

[0072] 模拟检测模式和数字检测模式具有精确和节能的各自优点。在模拟模式中，输出电压的漂移一般直接与某种篡改企图引起的破坏或影响相关联。模拟模式允许更好的精确度，并且甚至检测到数字模式不适用的篡改企图(图7B)。然而，模拟模式与静态功耗相关联，该静态功耗不仅是由驱动安全网格网络或阵列202的需要引起的而且还是由使用模拟电路单元(例如，电流源622)的倾向引起的。相反地，数字模式一般与动态功耗相关联，可以通过使用减慢的时钟减小该动态功耗。可以在一个篡改检测系统中对模拟检测模式和数字检测模式进行组合以保持两者的优点。

[0073] 混合检测模式基于模拟检测模式和数字检测模式的组合。在一个实施例中，在一个时钟周期中采用模拟检测模式，接着数字检测模式用于随后的时钟周期。结果，在该混合检测模式中组合了精确和节能的这两个优点。

[0074] 图8示出了根据本发明各个实施例的篡改检测方法的示例性流程图。在步骤802，篡改检测过程开始。作为篡改检测周期中的第一步骤，在步骤804，随机数发生器产生至少一个随机数。在步骤806，在安全网格网络中选择至少一个安全元件，以及在步骤808，根据阵列配置将所选安全元件串联耦合以形成安全阵列。在步骤806和808中，安全网格网络被

随机化成安全阵列。

[0075] 在步骤810，用驱动激励驱动安全阵列，该驱动激励可以是逻辑高或逻辑低的数字序列、模拟电压或电流。在步骤812，从安全阵列选择输出并根据检测模式监控该输出。在步骤814，检查所选节点处的输出的有效性。当有效性得到确认，重复包括步骤810-814的下一个检测周期，然而，当有效性检查失败时，检测周期终止以标志检测到篡改企图。

[0076] 可以从由模拟模式、数字模式或混合模式组成的组中选择检测模式。阵列配置、驱动激励和所选用于驱动和感测的节点是与检测模式相关联的。此外，在每个检测周期期间，这些变量可以由RNG 206随机产生的随机数确定。

[0077] 在本发明的各个实施例中，可编程性和随机性增强了篡改检测系统的灵敏性，因此增强了由安全网格网络保护的敏感区域的安全级别。篡改检测系统并入了包含阵列配置、驱动激励、感测节点选择和检测模式在内的变量。这些变量将可编程性和随机性引入到安全网格网络，包含物理位置、驱动信号、检测位置和检测方法。即使采用这些变量中的一些变量而不是全部变量，本发明也能够得到黑客很少或没有机会闯入的高度不可预知网格网络。

[0078] 虽然本发明易受各种修改和替换形式的影响，但是在附图中已经示出了本发明的具体例子并且在本文中对其进行了详细描述。然而，应当理解，本发明并不限于所公开的具体形式，相反地，本发明将覆盖落入所附权利要求的范围内的所有修改、等价形式和替换形式。

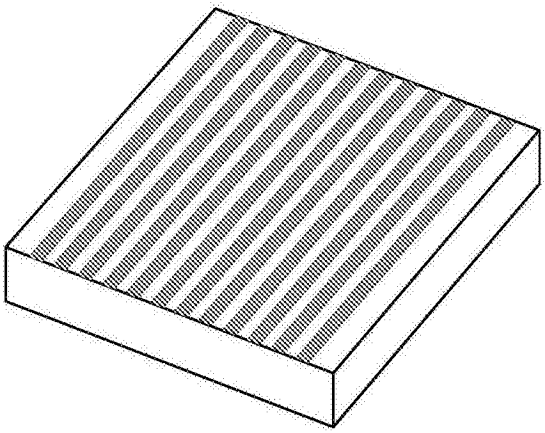


图1(现有技术)

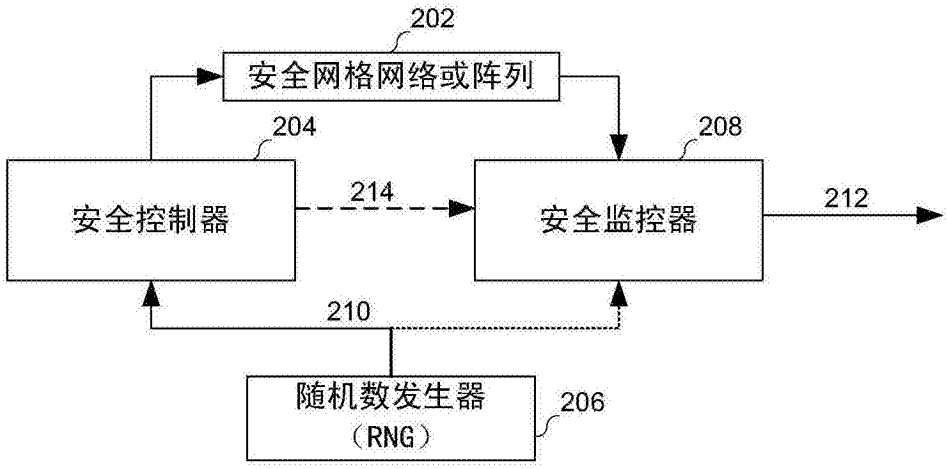


图2

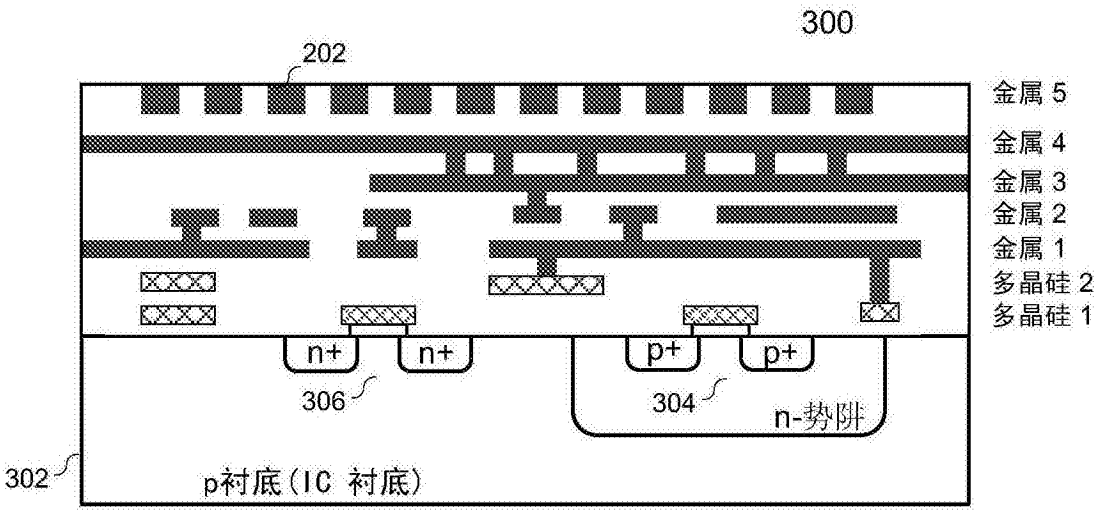


图3A

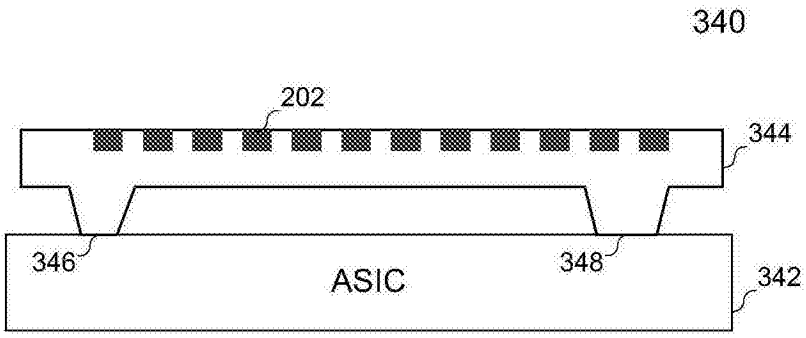

340
202
344
346
ASIC
348
342

图3B

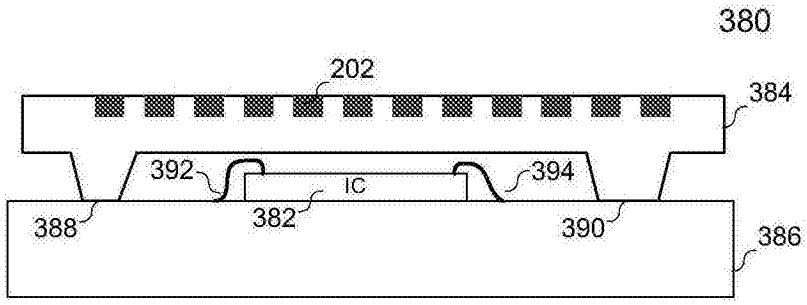

380
202
384
392
IC
394
388
382
390
386

图3C

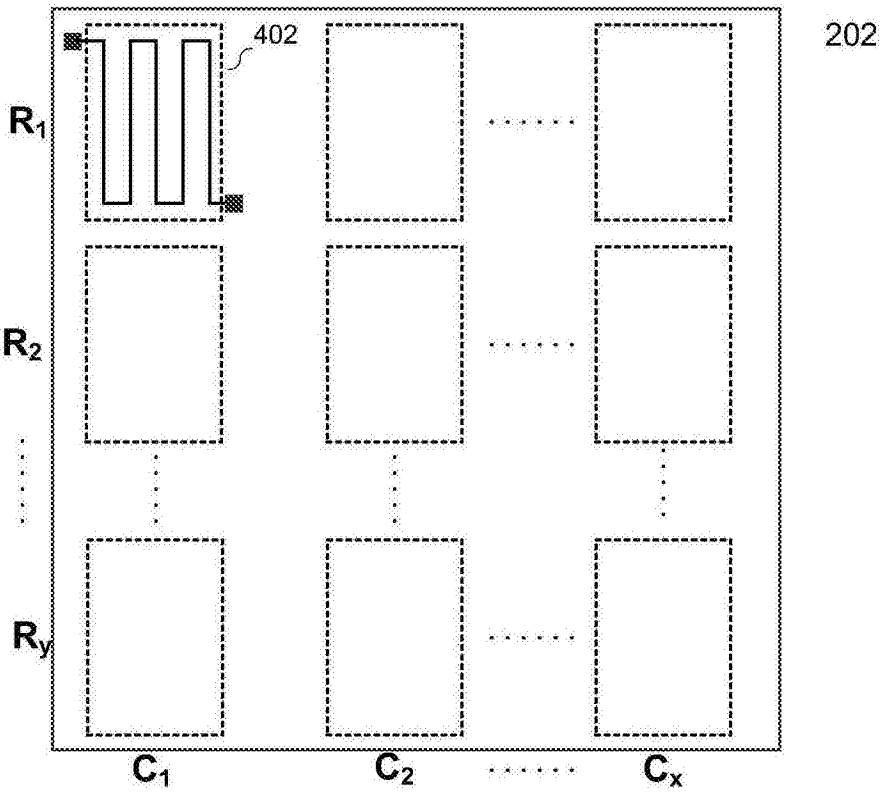

202
402
R1
R2
Ry
C1
C2
Cx

图4A

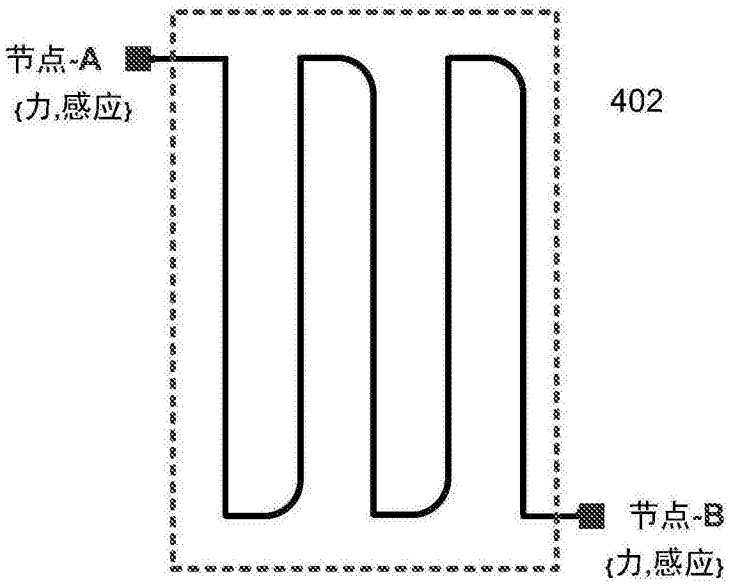


图4B

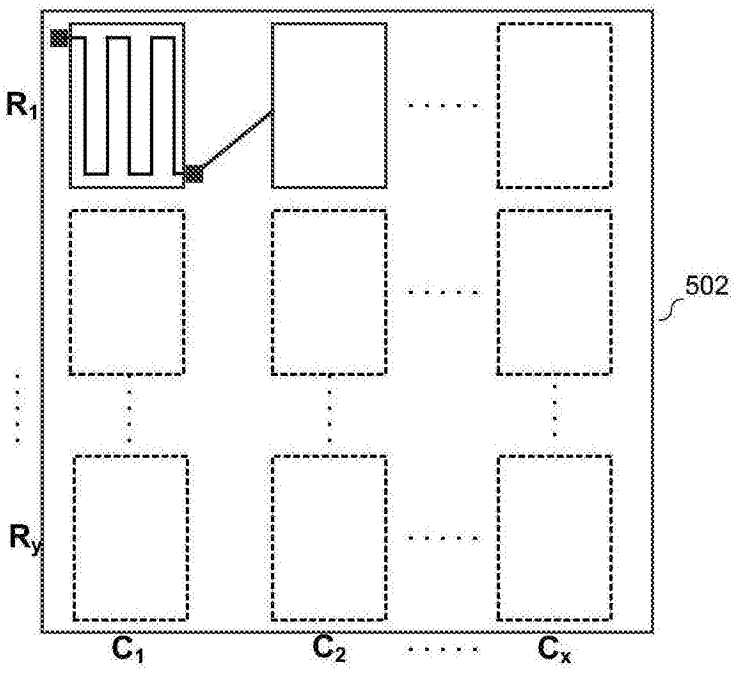


图5A

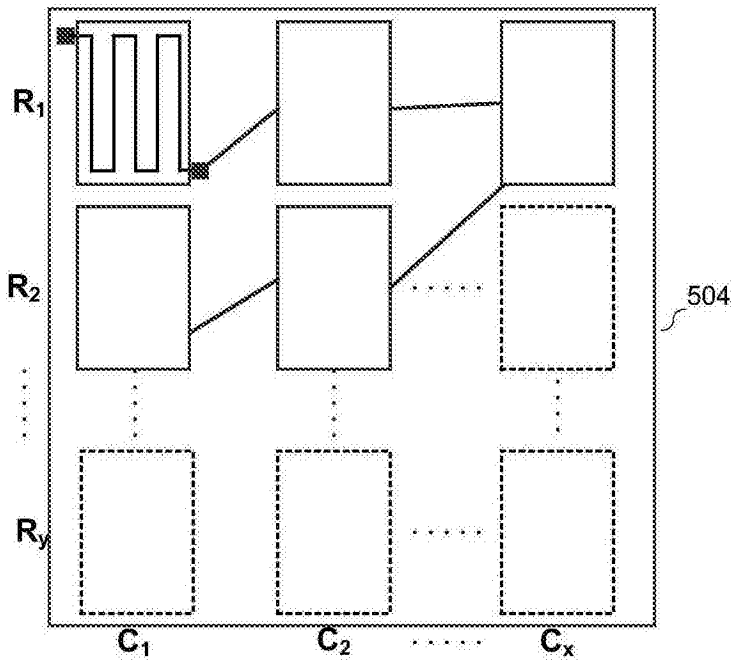


图5B

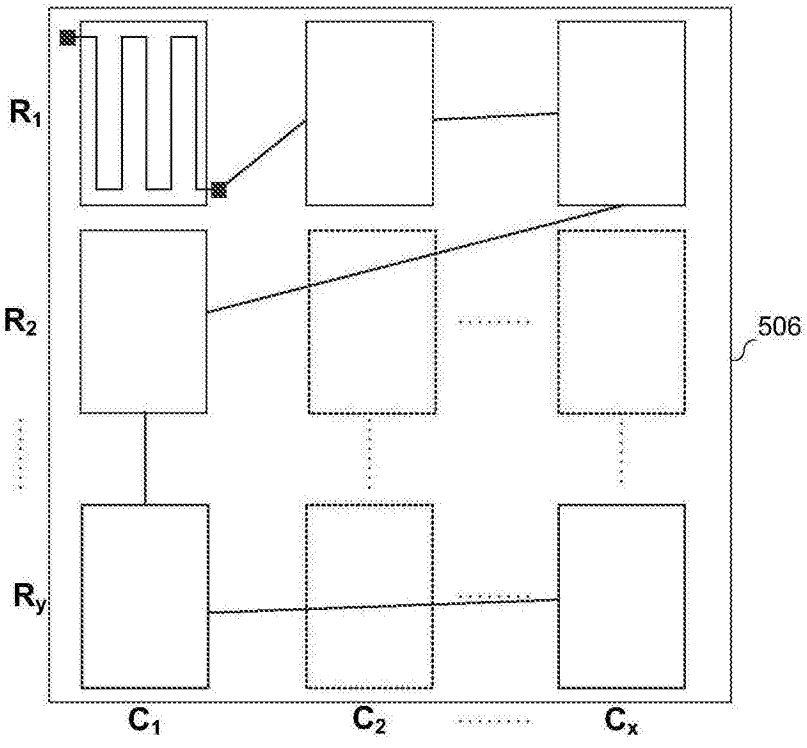


图5C

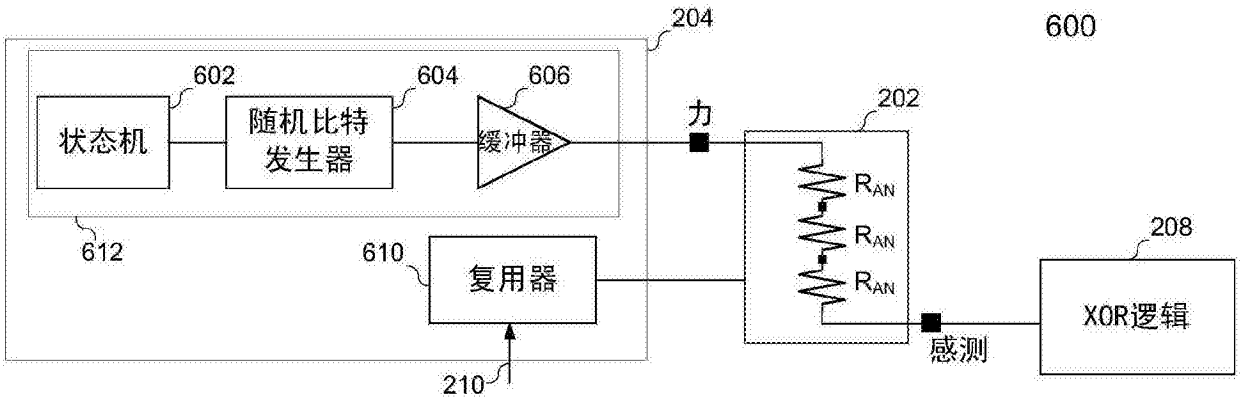

204
600
602
604
606
状态机
随机比特发生器
缓冲器
力
202
R_{AN}
R_{AN}
R_{AN}
208
612
610
复用器
XOR逻辑
感测
210

图6A

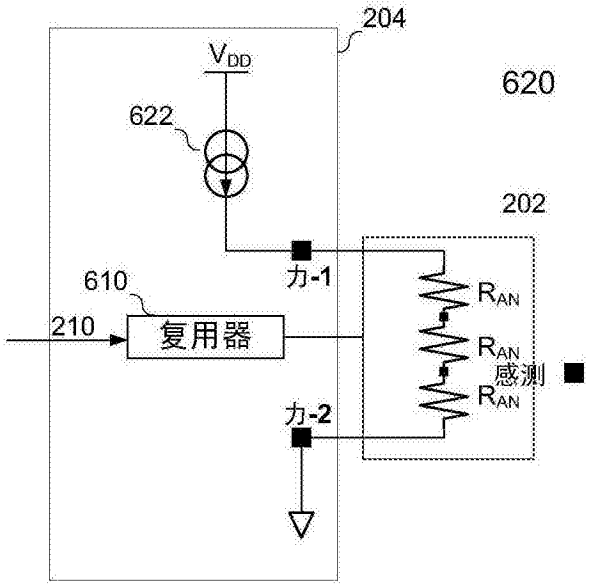

204
V_{DD}
620
622
202
力-1
610
210
复用器
R_{AN}
R_{AN}
感测
R_{AN}
力-2

图6B

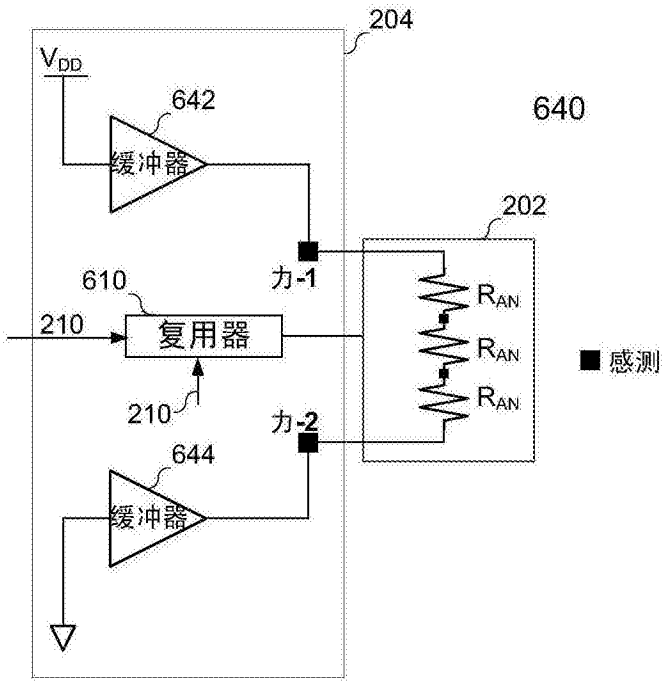


图6C

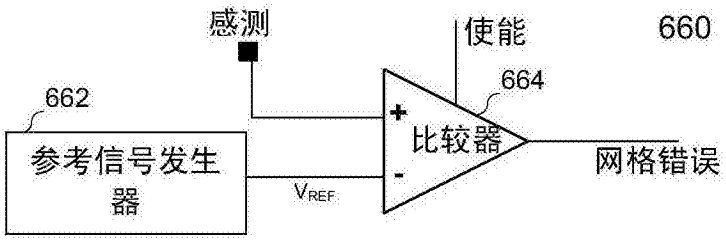


图6D

700

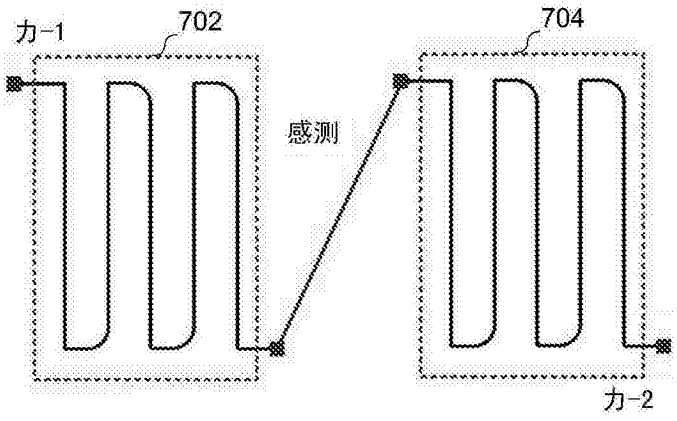


图7A

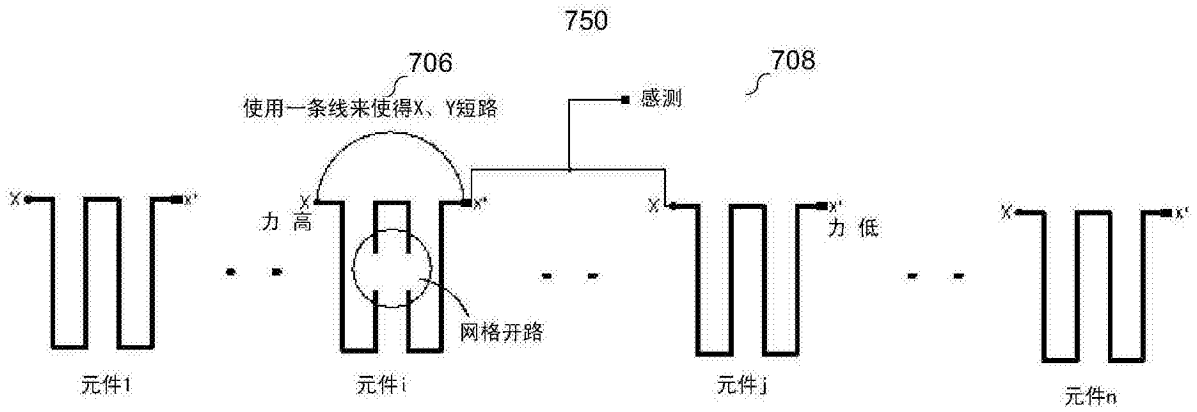


图7B

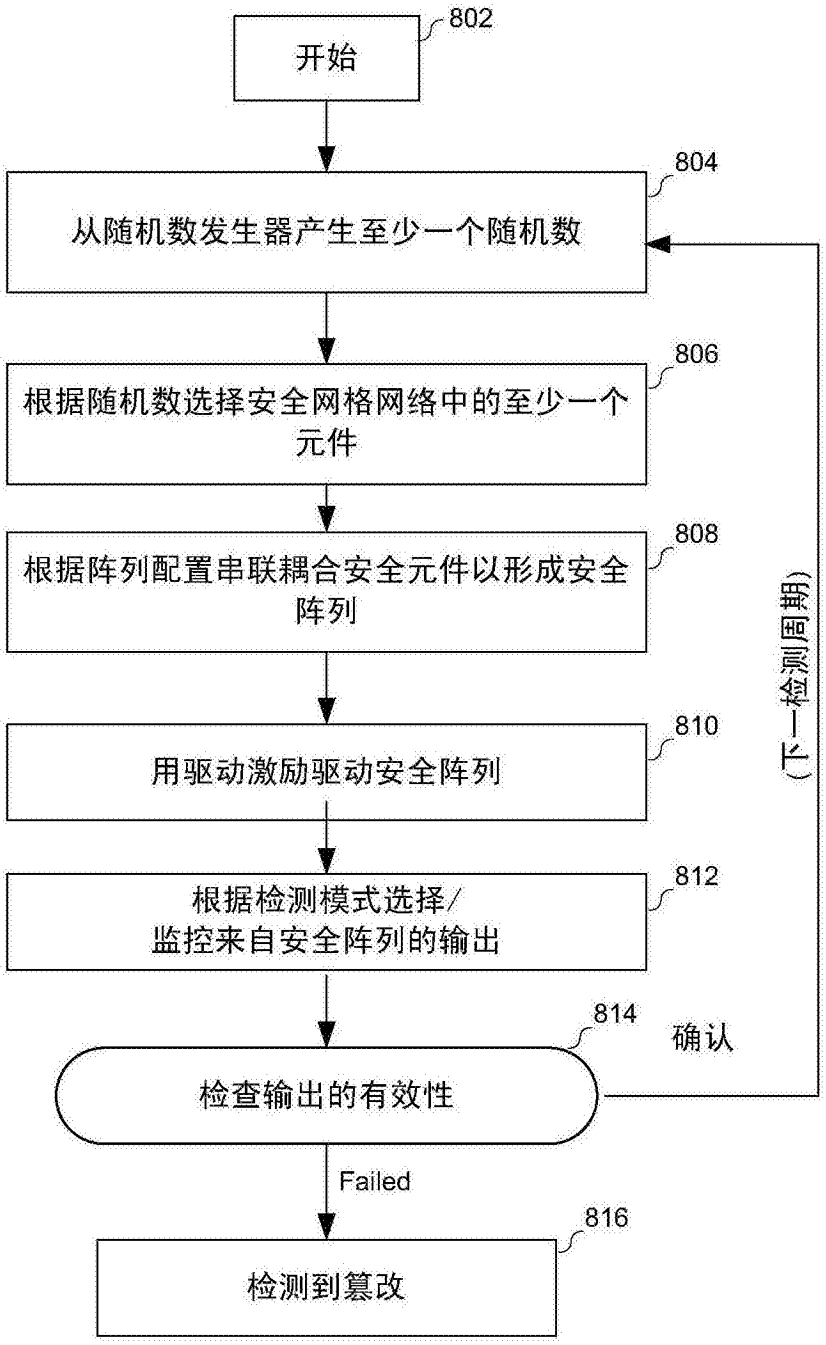

开始
802
从随机数发生器产生至少一个随机数
804
根据随机数选择安全网格网络中的至少一个元件
806
根据阵列配置串联耦合安全元件以形成安全阵列
808
用驱动激励驱动安全阵列
810
根据检测模式选择/监控来自安全阵列的输出
812
检查输出的有效性
814
确认
(下一检测周期)
Failed
检测到篡改
816

图8