(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 104252636 B
(45)授权公告日 2017.04.12

(21)申请号 201410290243.3

(22)申请日 2014.06.25

(65)同一申请的已公布的文献号
申请公布号 CN 104252636 A

(43)申请公布日 2014.12.31

(30)优先权数据
13174078.9 2013.06.27 EP

(73)专利权人 恩智浦有限公司
地址 荷兰艾恩德霍芬

(72)发明人 弗朗西斯科斯·皮特鲁斯·韦德索文
菲特·霍恩·恩古耶恩

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波

(51)Int.Cl.
G06K 19/073(2006.01)
G06F 21/75(2013.01)
H01L 23/58(2006.01)

(56)对比文件
US 2009086404 A1,2009.04.02,
CN 101617319 A,2009.12.30,
US 2010176920 A1,2010.07.15,
CN 102104480 A,2011.06.22,
CN 101421971 A,2009.04.29,

审查员 曹根千

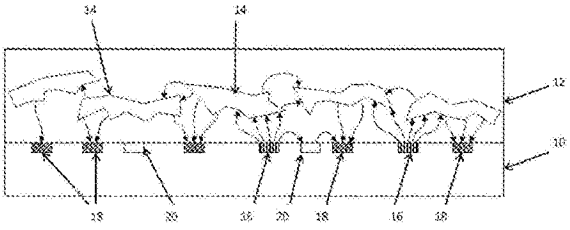
权利要求书2页 说明书6页 附图2页

(54)发明名称

具有电容式安全屏蔽的设备

(57)摘要

本发明提供了一种半导体设备，该半导体设备包括电容式安全屏蔽结构，该电容式安全屏蔽利用形成在介质层内的一组随机分布的介电粒子或导电粒子。一组电极能够被配置为至少两组，其中第一组用于测量电容特性，第二组被配置为非测量组。可以改变电极配置以使得可以获得多个测量。



CN 104252636 B

1.一种半导体设备，其特征在于，该半导体设备包括电容式安全屏蔽，该电容式安全屏蔽包括：

形成在介质层(12)内的一组随机分布的介电粒子或导电粒子(14)；

形成在一层中的一组电极(16,18,20;30,32,34)，所述一组随机分布的介电粒子或导电粒子形成在这一层之上；以及

控制器(52)，

控制器(52)适用于将电极配置为至少两组，其中第一组(16)用于测量电容特性，第二组(18,20)被配置为非测量组，控制器还适用于将电极重新配置成不同的第一组和第二组，被重新配置的第一组用于测量重新配置的电容特性。

2.如权利要求1所述的半导体设备，其特征在于，第二组包括接地的电极(18)。

3.如权利要求1或2所述的半导体设备，其特征在于，第二组包括处于悬浮电位的电极(20)。

4.如权利要求1所述的半导体设备，其特征在于，第二组包括被施加有调制电压的电极。

5.如权利要求4所述的半导体设备，其特征在于，第一组包括被施加有调制电压的电极，第二组的电极具有相同的调制信号。

6.如权利要求4或5所述的半导体设备，其特征在于，第一组(16)包括被施加有调制电压的电极，第二组的电极具有反相的调制信号。

7.如权利要求1所述的半导体设备，其特征在于，包括存储器(50)，存储器(50)存储有一系列不同的电极配置。

8.如权利要求1所述的半导体设备，其特征在于，电极(16,18,20;30,32,34)的面积等于或小于100μm^2。

9.如权利要求1所述的半导体设备，其特征在于，粒子(14)的最大长度尺寸小于30μm。

10.一种卡，其特征在于，包括在前的任意一项权利要求所述的半导体设备。

11.一种安全芯片，其特征在于，包括在前的任意一项权利要求所述的半导体设备。

12.一种RFID标签，其特征在于，包括在前的任意一项权利要求所述的半导体设备。

13.一种从半导体设备提取数据的方法，其特征在于，该半导体设备包括应用在物理不可克隆功能中的结构，该结构包括形成在介质层(12)内的一组随机分布的介电粒子或导电粒子(14)；形成在一层中的一组电极，所述一组随机分布的介电粒子或导电粒子形成在这一层之上；

该方法包含：

将电极配置为至少两组；

利用第一组(16)测量电容特性，第二组(18,20)被配置为非测量组，

将电极重新配置为至少两组的不同组合；

利用第一组(16)测量重新配置的电容特性，第二组(18,20)被配置为非测量组。

14.如权利要求13所述的方法，其特征在于，包括将第二组电极的电压设置为：

接地；和/或

悬浮电位；和/或

调制电压或反相调制电压。

15.如权利要求14所述的方法，其特征在于，包括通过对第一组电极施加调制电压以及对第二组电极施加相同的信号来测量电容特性。

16.如权利要求14或15所述的方法，其特征在于，包括通过对第一组电极施加调制电压以及对第二组电极施加相反的调制信号来测量电容特性。

17.如权利要求13所述的方法用于认证过程。

具有电容式安全屏蔽的设备

技术领域

[0001] 本发明涉及包括电容式安全屏蔽的设备。该防护可以基于电容值实现物理不可克隆功能。

背景技术

[0002] 应用于诸如智能卡、RFID标签、付费电视芯片和类似设备的集成电路(IC)通常包含保密的安全密钥,实现保密功能。IC必须是安全的,能够抵抗来自外部的意欲从其获取数据的攻击。

[0003] 集成电路可能会经受前侧攻击和后侧攻击。半导体设备的“正面”被定义为在半导体设备上设置电路的一侧。半导体设备的“背面”被定义为与正面相反的一侧。

[0004] 正面攻击可以包括打开封装的芯片,并记录芯片与外部探测器的电信号。背面攻击可以包括各种分析技术,诸如光子发射检测,热红外检测,液晶检测,电压或电场检测,以及电磁检测方法。

[0005] 通常,这些方法与入侵攻击结合使用,入侵攻击诸如是晶圆减薄,激光切割和加热,聚焦离子束(FIB)技术。也从背面使用光或激光闪光方法,以迫使信号反相。

[0006] 为了对抗这些攻击,已经提出了各种用于正面和背面的篡改保护方案。

[0007] 当篡改保护方案与密码技术结合时,篡改保护方案会变得更加强大。物理不可克隆功能(PUF)是由帕普等人于2001年3月在麻省理工学院的物理单向函数(Physical One-Way Functions)”中提出的。这篇文章提出了将PUF作为生成密钥的有效方法,该密钥用于加密目的。

[0008] PUF是体现在物理结构中的功能,PUF很容易评估,但难以表征。包含PUF的物理结构包括至少一个随机分量。该随机分量在制造过程中被引入,并且不易于被控制。PUF被描述为用作哈希函数,用于认证的目的。因为通过PUF,类似密钥的数据实质上是存储在材料中,而不是存储在电路中,该技术还可以用作需要认证的设备的一部分,诸如篡改检测传感器。

[0009] 许多进一步的发展集中在开发不同类型的PUF上。PUF的应用集中在,基于响应的独特性以及PUF的不可克隆性这些PUF的非常有用的特性,利用PUF作为智能卡(指纹识别)和信用卡的唯一标识符,或者作为两个主体之间用于密钥生成的廉价来源(通常是随机的)。

[0010] 用于PUF的物理结构的一个重要方面是,它的物理性能使得能够从其得到诸如电容或电阻的电特性,它是不(容易)再现的。这意味着各个电特性的行为是随机的,即在单个半导体设备(具有多个物理结构)内变化,在单个批次的半导体设备内变化,以及在多个批次之间变化。

[0011] 各个电特性的变化越大,包含在PUF中的信息就越多。

[0012] 已知PUF的问题是各个电特性的变化是有限的。

发明内容

[0013] 根据本发明，提供一种半导体设备，该半导体设备包括电容式安全屏蔽，该电容式安全屏蔽包括：

[0014] 形成在介质层内的一组随机分布的介电粒子或导电粒子；

[0015] 形成在一层中的一组电极，一组介电粒子或导电粒子形成在这一层之上；以及

[0016] 控制器，

[0017] 其中控制器适用于将电极配置为至少两组，其中第一组用于测量电容特性，第二组被配置为非测量组，控制器还适用于将电极重新配置成不同的第一组和第二组，被重新配置的第一组用于测量重新配置的电容特性。

[0018] 这种配置提供了用于不同电极配置的多种电容测量。这样提高了电容函数的随机性，使得克隆变得更加难。

[0019] 第二组包括接地电极、和/或悬浮电极、和/或施加有调制电压的电极。因此，第二组电极可以被分成具有子集，其中一些是接地的，一些是悬浮的，一些是调制的。第二组电极可以都是相同的，或者它们可以被分成两个或多个子集。第二组可以被认为是对电极组，虽然可以有对对电极功能起作用的其他导电体。

[0020] 第一组包括被施加有调制电压用于它们的电容测量的电极。当调制电压被施加到第二组电极，可以使用相同的调制频率和相位，或者是相同调制频率和相反相位。通常，可以使用任何相位。为了提高随机性或熵，可以选择可再现的随机相位。

[0021] 该设备可以包括存储器，存储器存储有一系列不同配置的电极。存储器信息被用于定义电容测量是如何发生的。存储器可以是受电容式安全屏蔽保护的设备的一部分。

[0022] 在一组非限制性的例子中，电极的面积等于或小于100μm^2。小的电极能够检测由小的外部有源探测设备引发的电极电容中的小的变化。

[0023] 电极阵列可以具有数十个或数千个电极。电极阵列通常是规则的电极阵列，然而粒子是在制造过程中随机分布的。例如，粒子的最大长度尺寸小于30μm。

[0024] 该设备可以被用在智能卡或RFID标签中。

[0025] 本发明提供了一种从半导体设备提取数据的方法，该半导体设备包括应用在物理不可克隆功能中的结构，该结构包括形成在介质层内的一组随机分布的介电粒子或导电粒子；以及形成在一层中的一组电极，一组介电粒子或导电粒子形成在这一层之上；

[0026] 该方法包含：

[0027] 将电极配置为至少两组；

[0028] 利用第一组测量电容特性，第二组被配置为对电极组；

[0029] 将电极重新配置为至少两组的不同组合；

[0030] 利用第一组测量重新配置的电容特性，第二组被配置为对电极组。

附图说明

[0031] 图1示出了本发明的设备；

[0032] 图2示出了如何将该设备重新配置成用于多种测量的不同配置；和

[0033] 图3示出了如何使用该设备的示例。

具体实施方式

[0034] 本发明提供包含电容式安全屏蔽结构的半导体设备，该电容式安全屏蔽结构使用一组形成在介电层内的随机分布的介质粒子或导电粒子。该组电极可以被配置为至少两组，其中，第一组被用于测量电容特性，第二组被配置为对电极组。可以改变电极配置以使得可以获得多个测量。

[0035] 在这种方式中，本发明基于一组单电极边缘电容，这组单电极边缘电容分布在芯片区域上(特别是分布在需要被保护以防止攻击的部分上)。各电容器通过测量其电极板与所有物体和材料之间的扩散电容来感测它的本地环境，其中这些物体和材料位于源自电极板的电场线内。

[0036] 图1示出了电极层10，介电层12形成在电极层10上，随机分散的粒子14嵌入在介电层12中。

[0037] 电极层10可以是IC的顶部金属层，并且与各电极具有独立的连接，然后路由到IC内的处理电路。

[0038] 图1示意性地示出了形成的电场线，省略了通到底层的电场线。

[0039] 该电极被分成两组。第一组包括有源电极16，第二组包括对电极，其中一些是接地电极18，另外一些是悬浮电极20。

[0040] 图1示出了通过这些电极的横截面。电极在垂直于附图的平面的方向上的尺寸与其在附图的平面上的尺寸差不多，从而使电极例如通常为圆形或方形。

[0041] 在这个例子中，仅使用了接地电极和悬浮电极。虽然只能看到一行电极，但实际上使用的是二维电极阵列。

[0042] 在图1的例子中，芯片被介电层覆盖，具有不规则形状的导电粒子随机分布在介电层中。如果攻击者去除掉介电层的一部分，或者是去除、损坏或置换一个或多个导电粒子，则被攻击位置附近的有源电极的电容会发生变化。如果材料的去除或置换是在芯片上电之前完成的，则会感应到这种变化。

[0043] 粒子的实例是：

[0044] 不规则形状的导电粒子，像金属、半导体、石墨等薄片；或

[0045] 不规则形状的介电粒子，具有的介电常数不同于其所嵌入的介电层12的介电常数。

[0046] 当芯片接收电力供应时，选择电极的子集(第一组有源电极)来测量其电容响应。

[0047] 所有有源电极的电容被单独测量。通常通过例如以逻辑门作为开关元件，对电极的电容反复地进行充电和放电，并测量平均充电/放电电流，以此来测量电容。在以逻辑门作为开关元件的情况下，逻辑门的动态功耗与电极的电容和逻辑门的寄生电容的总和成正比。

[0048] 其余的未被选择的电极(第二组对电极)以特定的连接方式与集中分布的对电极连接，电力线源自于有源电极端。电力线的终端也可以位于附近的其他导体上。在这些对电极中，第一子集可以接地，第二子集可以是悬浮的，第三子集可以被连接到与有源电极具有相同频率和相位的调制电压上，第四子集可以被连接到与有源电极具有相同频率和相反相位的调制电压上。

[0049] 这定义了具有四个子集的方法。然而，在最简单的实现方式中，第二组的所有电极可以是相同的，例如所有都是接地的或所有都是悬浮的。对电极(第二组)的划分可以按照希望的更复杂。甚至可以超过上述确定的四个子集。

[0050] 因此，可以通过删除、添加或修改有源电极或对电极的子集来创建不同的连接方式。

[0051] 在下面的描述中，有源电极和对电极的特定配置被称为物理连接方式。

[0052] 图2示出了全扫描的四个(1至4)连续的物理连接方式的示例(表示芯片的一部分的俯视图)。

[0053] 有源电极30显示为一个填充图案(这些是第一组)。接地的对电极32显示为另一个填充图案(这些是第二组的第一子集)，悬浮的对电极34显示为不同的填充图案(这些是第二组的第二子集)。不规则形状的图形是导电粒子(或介质粒子)。

[0054] 每一类电极中只有一个电极用参考标号进行了标注，但是相同类型的所有电极都显示为具有相同的填充图案。

[0055] 对整个芯片表面的全扫描可以通过对一组替代的物理连接方式重复多次电容测量来实现。在最简单的版本中，有两个测量阶段。在测量阶段之间，一些先前未选择的电极被激活，一些或全部先前的有源电极被添加到接地的、悬浮的等对电极的子集中。

[0056] 以这种方式，可以创建和测量一系列不同的物理连接方式。图2示出了全扫描的四个可能的物理连接方式即4个测量阶段的示例。

[0057] 所需的测量阶段的数量取决于测量所需的随机性、芯片区域以及测量处理的并行数。更多的并行提供了更快的扫描，但需要芯片上更多的硬件资源。

[0058] 在极端的情况下，具有1,000-10,000个电极的芯片的电极对在差分测量中顺序地进行比较，可以是500-5,000个测量阶段。在更实际的情况下，可能有几十到上百个阶段。对高度安全芯片非常精确的测量，可以通过重新配置未选择的电极的状态使用更多阶段。阶段的数量还取决于可用于篡改检测的总时间。

[0059] 因为每个单独的芯片上覆盖着不同的独特图案的粒子，因此对于每个不同的芯片，给定的一系列物理连接方式将产生独特的一系列测量的电容值。这使得它难以使用所收集的关于一个特定芯片中的粒子分布的信息来预测另一个芯片上测量的电容。

[0060] 如果电极做得足够小，则它们的电容将会小于典型的金属探测器尖端的扩散电容，金属探测器尖端被放置在介电层之上足够接近介电层，以便能够感应芯片上的电位。所以，如果有人试图检测由有源电极或由芯片上的其它电路产生的电信号图形，则将其作为邻近该金属探测器尖端的有源电极的电容的变化来感应，其中芯片上的其它电路是通过例如将微小的金属探测器尖端正好放在受保护的芯片表面上受到电容式安全屏蔽保护的。

[0061] 通过举例的方式，电极的尺寸可以是侧边为1至5μm的正方形，类似直径的圆形，或者是具有类似面积的线。该区域通常小于100μm^2，以使得可以检测到由小的外部探测器导致的电容变化。粒子可以具有0.3μm到30μm的最大线性尺寸。粒子尺寸和粒子密度是一起选择的，以获得电容功能的所需灵敏度。

[0062] 利用由连接到局部有源读取电极的微小金属尖端构成的有源电场探测器，可以检测源自于芯片的非常小的电边缘场。然而，对于足够的信噪比，这通常需要长的集成时间。因此，通过使用非常高的调制频率以快速测量有源电极的电容，使得这样的攻击是很难的

或者甚至是不可能的，因为芯片上的电容测量可以进行的很快，以致外部有源探测器在存在特定的物理连接方式的时间内不能获得所需的信噪比。

[0063] 电容测量所需的时间依赖于噪声，以及来自于芯片上的其他信号的串扰。它也依赖于电容测量所需的灵敏度。对于单个电容测量，需要0.03ms-3ms。

[0064] 在攻击者能够检测到源自于芯片的信号之前，利用小电极和快速高频测量的组合，可以由芯片检测到任何试图利用外部探测器检测源自于芯片的信号的行为。当检测到这种攻击时，可以使芯片停止工作或者使芯片断电，这样可以使攻击者不能利用持续时间长的测量来积累信息。

[0065] 然而，攻击者可以通过调查一些芯片(例如，通过反向工程)来揭露固定的一系列物理连接方式，然后利用这些信息来对另一个芯片进行准备的攻击。可以通过例如利用片上的SRAM PUF或类似部件将固定的一系列逻辑地址映射到一系列芯片专用的物理连接方式来防止这样的攻击。其结果是，每个芯片将具有自己独特的一系列物理连接方式。以这种方式，不可能在准备的攻击中利用从其他芯片获得的关于物理连接方式的先前信息以及它们与逻辑地址的关系。

[0066] 为了避免通过SRAM PUF进行的映射被反向工程，可以利用上述电容式安全屏蔽来保护SRAM PUF。

[0067] 在生产之后，要在安全终端中读取出每个受保护芯片的响应图形并将其存储在数据库中。部分数据库可以被存储在芯片外(例如，当它被用于验证时)，部分数据库可以被存储在非易失性的片上存储器中(当它被用于防止攻击时)。这可以通过提供一系列逻辑地址(在PUF的情况中通常被称为“询问”)，并记录从有源电容器的序列中读取出的相应电容值来实现。

[0068] 这种配置可以使用被埋在划伤保护层或其他上层之下的电极。闪存或EEPROM存储器可用于本地数据库，存储器受电容式安全屏蔽本身保护。

[0069] 图3示出了本发明的设备的可能使用。

[0070] 该集成电路包括嵌入式存储器50，被保护的主集成电路52和电容式安全屏蔽结构。

[0071] 在芯片的生产过程中，表示电容式安全屏蔽54的预期评估结果的值被存储在芯片内部的非易失性存储器50中。例如在芯片的反向工程情况下尝试去除钝化层将不可逆地损坏电容式安全屏蔽(即粒子的随机结构)，电容式安全屏蔽的评价结果将永久地偏离预期结果。

[0072] 因此，该芯片可以通过电容感测来评估电容式安全屏蔽，并将评价结果与一组参考值进行比较，以确定钝化层是否已被去除。

[0073] 如果钝化层被去除和/或替换，则可以通过芯片以相对简单的方式自主地检测到这种变化。本发明的电容式安全屏蔽，利用在芯片的钝化层中随机分布的导电粒子，可以结合相对简单的检测方案来保护芯片的表面。

[0074] 通过使用逻辑地址到物理电极配置的映射，为每个芯片提供了独特的指纹，以致不能使用对非功能芯片的反向工程来篡改另一个功能芯片。

[0075] 为了使用该芯片，嵌入式的非易失性存储器50的逻辑地址被访问。这定义了配置方式。该配置方式是由集成电路52(其因此用作控制器)实现的。对于该配置方式，基于询问

和响应，从保护电容式安全屏蔽54获得一组电容测量。

[0076] 感测到的数据被输出并基于所存储的数据被验证(或者可以在外部进行验证)。

[0077] 电极通常是具有5-25μm间隔的电极，该间隔取决于电极的尺寸和形状，以及所需的灵敏度。通常，所有的逻辑区域和存储器外围设备(如地址译码器)会受到电容式安全屏蔽保护。可选地，其它电路也可以受到保护。在安全芯片中，存储器的内容通常是加密的，因此并不一定需要由电容式安全屏蔽进行保护，但对地址解码器等进行保护是有利的。

[0078] 本发明对加密功能以及对保护半导体装置不被篡改都是有益的，这里所说的篡改是指尝试获取存储在例如智能卡或RFID标签等半导体设备中的数据。特别是，当有加密密钥存储在半导体设备中时，黑客可能要尝试找到密钥以获得有效数据。

[0079] 根据本发明的物理结构可以有利地被应用(即沉积)在半导体设备的互连堆叠的顶部上，该半导体设备包括具有安全数据的电子电路。当试图从正面接入半导体设备时，电容值发生改变，这会影响所提取的加密密钥。换句话说，变得难以找到存储在半导体设备中的有效数据。

[0080] 本发明可以被应用在各种应用领域。例如，本发明可以用于智能卡、RFID标签、付费电视芯片等的数据安全。这类芯片通常包含保密的安全密钥(加密密钥)，实现保密功能。可以从根据本发明的半导体设备中的物理结构有利地提取出加密密钥。

[0081] 本发明还可以用于通过内部的安全密钥确保与例如移动电话的通信安全。本发明可以替代经由SIM卡的身份识别，因为SIM卡是很容易被复制的。

[0082] 被保护的半导体设备可以利用任何已知的形式。

[0083] 应该注意的是，术语“物理不可克隆功能”并不意味着是绝对不可克隆的。它只是意味着物理结构的复杂性使得在物理上复制该结构或计算模仿该结构是不可行的。

[0084] 应当指出的是，上述实施例是用来说明而非限制本发明，并且本领域的技术人员将能够设计许多替代实施例而不脱离所附权利要求的范围。在权利要求中，置于括号之间的任何标号不应被解释为限制权利要求。某些措施被记载在不同的从属权利要求中并不意味着这些措施的组合不能被有利地使用。各种修改对于本领域技术人员来说将是显而易见的。

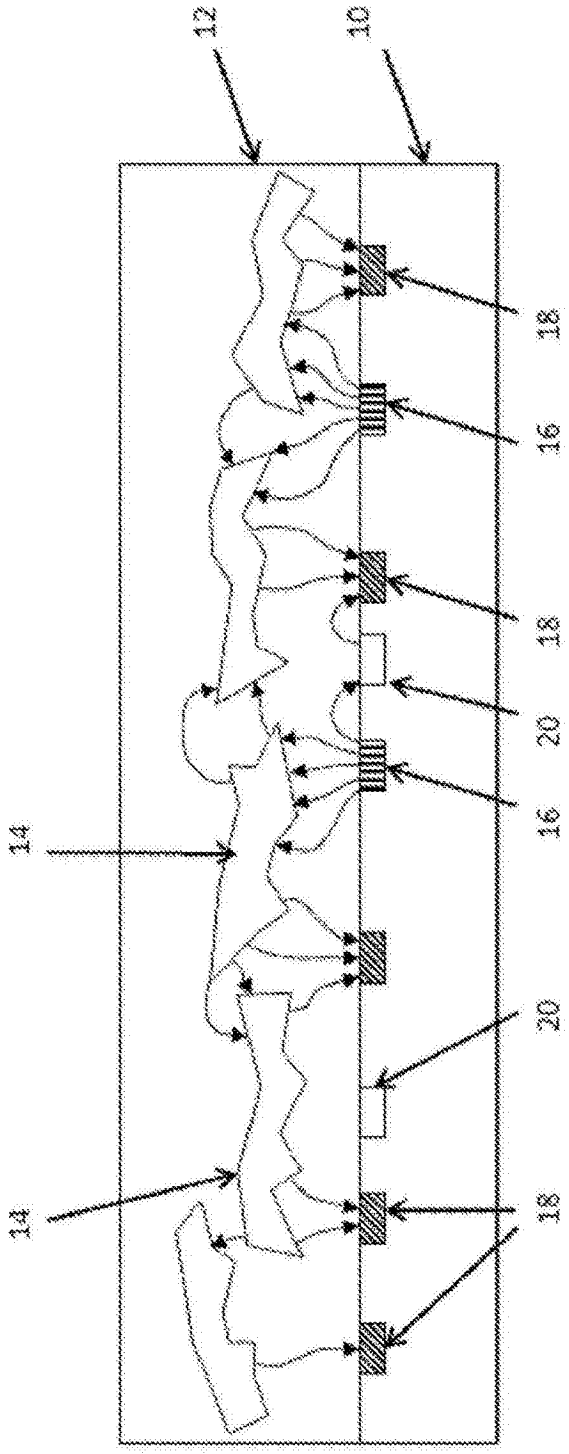


图1

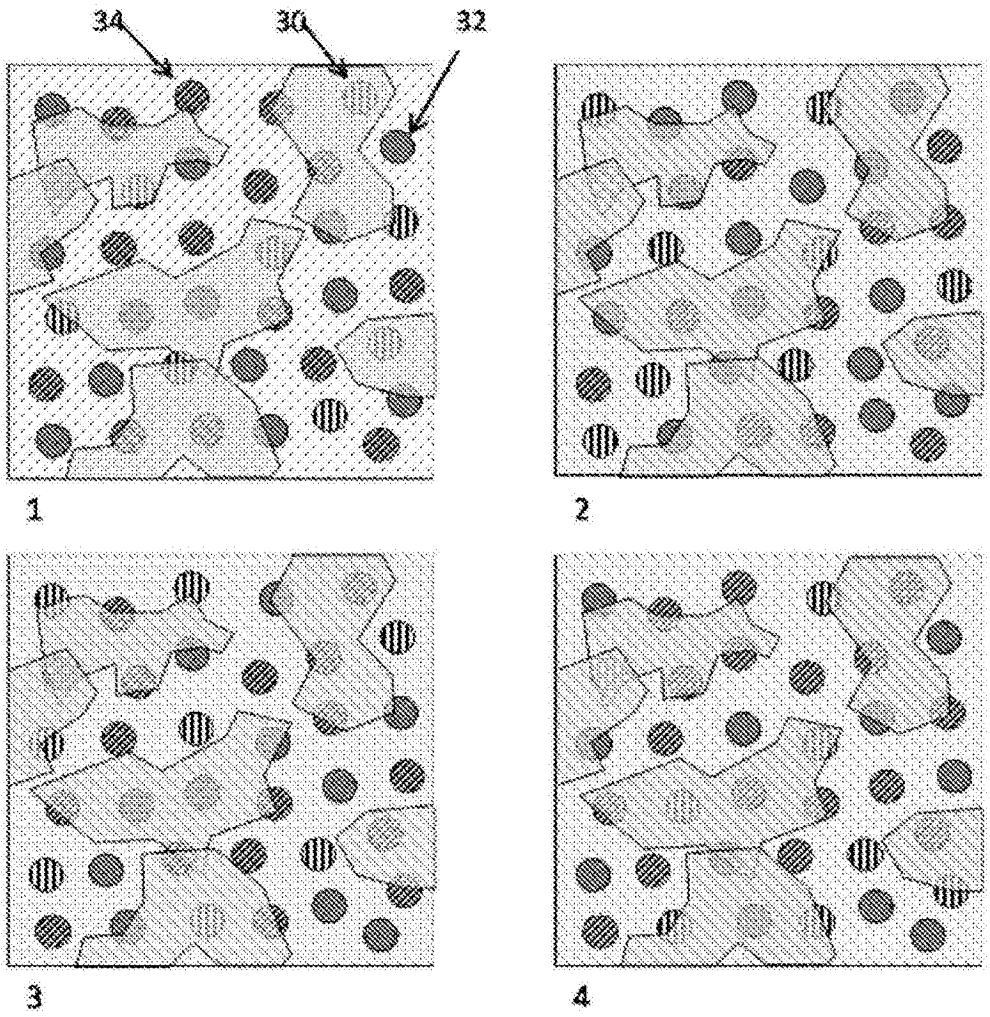

34
30
32
1
2
3
4

图2

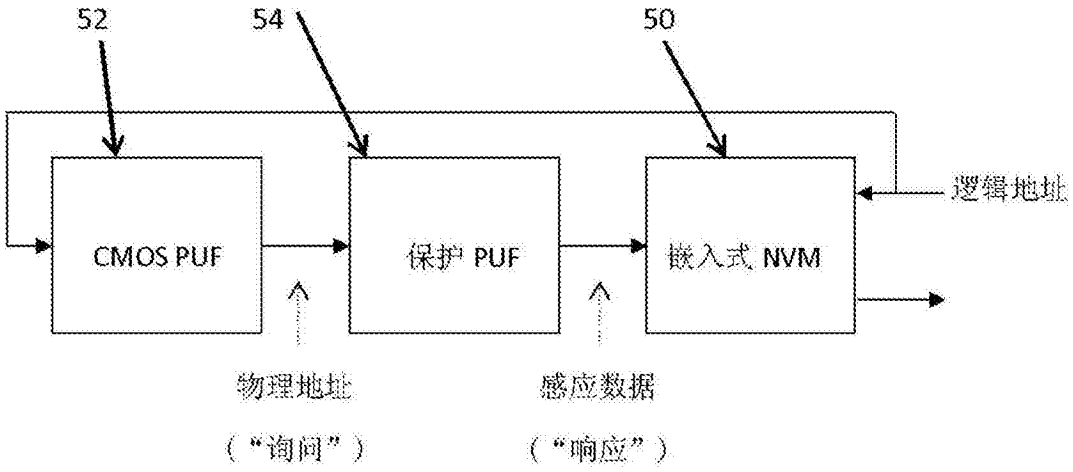

52
54
50
CMOS PUF
保护 PUF
嵌入式 NVM
逻辑地址
物理地址
（“询问”）
感应数据
（“响应”）

图3