(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 106295408 B
(45)授权公告日 2020.06.02

(21)申请号 201610621693.5

(22)申请日 2011.02.28

(65)同一申请的已公布的文献号
申请公布号 CN 106295408 A

(43)申请公布日 2017.01.04

(30)优先权数据
10-2011-0013269 2011.02.15 KR

(62)分案原申请数据
201180070008.X 2011.02.28

(73)专利权人 ICTK控股有限公司
地址 韩国京畿道

(72)发明人 金东奎 崔秉德

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 张全文

(51)Int.Cl.
G06F 21/72(2013.01)
H04L 9/00(2006.01)

(56)对比文件
US 2008/0044010 A1,2008.02.21,说明书第0044-0049段,说明书附图图3-4.
US 2008/0044010 A1,2008.02.21,说明书第0044-0049段,说明书附图图3-4.
US 2006/0131575 A1,2006.06.22,说明书第0003,0056-0064,0119段,说明书附图图1-11.
US 5559889 A,1996.09.24,全文.
JP 特开平10-116326 A,1998.05.06,全文.
JP 特开2011-10218 A,2011.01.13,全文.
CN 1777097 A,2006.05.24,全文.
US 2009/0080647 A1,2009.03.26,全文.
US 2010/0031065 A1,2010.02.04,全文.

审查员 朱江岩

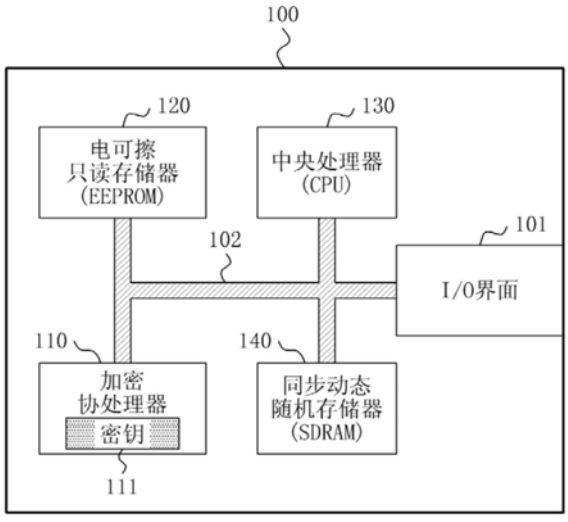
权利要求书1页 说明书11页 附图10页

(54)发明名称

集成电路及加密方法

(57)摘要

提供一种集成电路,包括:密钥模块,用于产生密钥。同时还提供一种加密的方法,包括:产生密钥;以及使用该密钥执行加密算法。



CN 106295408 B

1.一种集成电路,包括:

密钥模块,用于生成密钥;以及

加密模块,用于使用该密钥来执行加密算法,所述加密模块包括多个所述密钥模块,所述多个密钥模块分散设置于多个标准单元布局中的任意位置处,所述多个标准单元被包括在所述加密模块内。

2.如权利要求1所述的集成电路,其中所述多个密钥模块与其他标准单元相似地分散设置。

3.如权利要求1所述的集成电路,其中该密钥模块包括节点和根据节点之间是否短路生成密钥。

4.如权利要求1所述的集成电路,其中,该密钥模块包括多个单元结构,每个单元结构根据半导体制备工程变化来生成1比特的数字值。

5.如权利要求1所述的集成电路,其中,该密钥模块包括多个差分放大器,

其中第一差分放大器的两个输入端短路时,根据半导体制备工程变化该第一差分放大器的两个输出端的逻辑电平互不相同,该密钥模块根据两个输出端的逻辑电平生成对应于第一差分放大器的1比特的数字值。

6.一种加密的方法,包括:

将多个密钥模块分散设置于多个标准单元布局中的任意位置处,所述多个标准单元被包括在所述加密模块内;

生成密钥;以及

使用该密钥执行加密算法。

7.如权利要求6所述的方法,其中,加密模块使用该密钥执行加密算法,该方法还包括:

防止密钥从加密模块泄露;以及

防止额外的密钥流入加密模块。

8.如权利要求6所述的方法,其中,根据半导体的导电层之间是否产生短路来生成该密钥。

9.如权利要求6所述的方法,其中,生成密钥包括根据半导体制备工程变化由多个单元结构的每个单元结构生成1比特的数字值。

10.如权利要求6所述的方法,其中,生成密钥包括根据差分放大器的两个输出端的逻辑电平生成对应于该差分放大器的1比特的数字值,

其中当差分放大器的两个输入端短路时,根据半导体制备工程变化该差分放大器的两个输出端的逻辑电平互不相同。

集成电路及加密方法

技术领域

[0001] 本发明涉及数字保安领域，特别是，涉及一种管理密钥的加密装置及方法，使智能卡等IC保安模块中可防止物理攻击。

技术背景

[0002] 智能卡作为信用卡大小的塑料卡，其包含可加工处理数据的集成电路 IC(Integrated Circuit)。与现有的磁卡相比，该智能卡具有多种优点，其自身具数据存储容量，并具有与微处理器一起的协处理器(co-processor)等的处理单元。

[0003] 因此，为获取用于识别身份(Identification)的个人信息及金融结算信息等，利用加密算法来自动执行加密演算(encryption)。

[0004] 此外，随各IT技术的发展，智能卡被广泛应用，同时对于智能卡的多种保安侵犯也在不断增加。

[0005] 在这种情况下，类似利用IC芯片的逆向工程(Reverse Engineering)技术来读取IC芯片的信息的物理性攻击在保安中存在较大的问题。

[0006] 根据硬件保安模块中所使用的电可擦只读存储器EEPROM和只读存储器 ROM的存储特征及数据存储方式，已知的几个物理性攻击为总线探测(Bus probing)、测试模式探测(test-mode probing)、只读存储器ROM或电可擦只读存储器EEPROM的重写(overwriting)等攻击方式。

发明内容

[0007] 技术课题

[0008] 提供一种加密装置及方法，可强力防止对于智能卡的物理性攻击。

[0009] 特别是，提供一种加密装置及方法，不直接从存储器中提取生成或存储的密钥。此外，提供一种不会通过智能卡的IC芯片内的总线(bus)被泄漏的加密装置及方法。

[0010] 技术方案

[0011] 根据本发明的一个侧面，提供一种接收将要加密的输入数据，执行利用密钥的加密算法的加密装置，所述加密装置包括：加密模块，将提供密钥的密钥模块包含在内部，利用所述密钥模块所提供的密钥来执行所述加密算法。

[0012] 所述加密模块分别包含在用于提供不同密钥的多个密钥模块的内部。在这种情况下，所述加密模块可包括：密钥模块选择单元，选择所述多个密钥模块中的任何一个；和加密单元，利用所述选择的密钥模块所提供的密钥来执行所述加密算法。

[0013] 此外，所述密钥模块选择单元，选择所述多个密钥模块中对应于预先被附于识别索引的密钥模块。

[0014] 根据本发明的一个实施例，所述加密模块包括多个标准单元，所述多个密钥模块被配置在所述加密模块中包含的多个标准单元布局的任意位置中。标准单元可以是用于体现加密模块的规格化元件或功能块。

[0015] 如上所述的集成电路，其中，所述加密模块，利用所述加密模块内部包含的所述密钥模块所提供的密钥，来执行所述加密算法，且所述密钥模块所提供的密钥不泄露至所述加密模块的外部，且为执行所述加密算法，其他附加的密钥不泄露至所述加密模块。

[0016] 根据本发明的一个实施例，所述密钥模块是将预先生成的所述密钥存储的非易失性存储模块。

[0017] 根据本发明的另一个实施例，所述密钥模块是生成并提供所述密钥的非存储模块。

[0018] 在这种情况下，所述密钥模块，违反半导体工程中所提供的设计规定，概率性地来确定所述密钥模块内的节点之间是否短路，且所述密钥模块，可根据读取所述节点之间是否短路的结果来生成并提供所述密钥。

[0019] 在此，所述密钥模块内的节点为半导体的导电层，且所述设计规定，与所述半导体的导电层之间所形成的接点或通路的尺寸有关，且所述密钥模块，利用所述半导体的导电层之间所形成的接点或通路致使所述导电层短路与否，来生成所述密钥。

[0020] 此外，所述密钥模块，违反半导体工程中所提供的设计规定，使所述半导体的导电层之间所形成的所述接点或通路(via)致使所述导电层短路的概率与不短路的概率的差异保持在一定的误差范围内，并具所述接点或通路(via) 的尺寸。

[0021] 根据本发明的一个实施例，所述密钥模块，具有N个利用一对导电层和连接其之间的一个接点或通路来生成1比特的数字值的单元结构，并将通过所述N个的单元结构所生成的N比特的数字值生成为所述密钥，其中，N 为自然数。

[0022] 在这种情况下，所述密钥模块，将所述生成的N比特的数字值以k个单位进行分组，并在被分组的多个组中比较第1组和第2组，当所述第1组中包含的k个数字比特所构成的值大于所述第2组中包含的k个数字比特所构成的值时，将代表所述第1组和所述第2组的数字值确定为1，且相反时，将代表所述第1组和所述第2组的数字值确定为0，从而将N/k比特的数字值生成为所述密钥，其中，k为自然数。

[0023] 根据本发明的另一个实施例，所述密钥模块内的节点为半导体的导电层，且所述设计规定，与所述半导体的导电层之间的间隔(gap)有关，且所述密钥模块，利用所述半导体的导电层之间的短路与否，来生成并提供所述密钥。

[0024] 根据本发明的又另一个实施例，所述密钥模块，包括：N个的单位晶格，分别输出1比特的数字值，N为自然数，且所述N个的单位晶格，分别基于半导体制备工程变差(Process variation)来生成1比特的数字值，从而所述密钥模块生成并提供N比特的密钥。

[0025] 在这种情况下，所述N个的单位晶格中第1单位晶格包括：具第1逻辑阈值的第1逆变器；和具第2逻辑阈值的第2逆变器，且所述第1逆变器的输入端和所述第2逆变器的输出端与第1节点连接，且所述第1逆变器的输出端和所述第2逆变器的输入端与第2节点连接，形成反馈结构，且所述第1逻辑阈值和所述第2逻辑阈值，基于半导体制备工程变差互不相同，根据所述第1节点的逻辑电平和所述第2节点的逻辑电平，来确定对应于所述第1单位晶格的1比特数字值。

[0026] 此外，根据本发明的又另一个实施例，所述密钥模块，包括：N个的差分放大器，N为自然数，且所述N个的差分放大器中的第1差分放大器，当所述第1差分放大器的两个输入端被短路时，所述第1差分放大器的两个输出端的逻辑电平基于半导体制备工程变差互不相

同,根据所述两个输出端的逻辑电平,来确定对应于所述第1差分放大器的1比特数字值,且所述密钥模块生成并提供N比特的密钥。

[0027] 根据本发明的另一个侧面,提供一种加密方法,包括以下步骤:接收将要加密的数据,输入至内部包含有提供密钥的密钥模块的加密模块中;以及利用所述密钥模块所提供的密钥,来执行所述加密算法,从而来加密所述数据。

[0028] 根据本发明的又另一个侧面,提供一种接收将要加密的输入数据,执行利用密钥的加密算法的IC芯片,所述IC芯片包括:加密模块,其内部包含有提供密钥的密钥模块,利用所述密钥模块所提供的密钥来执行所述加密算法。

[0029] 在这种情况下,所述IC芯片被内藏在智能卡中,在应用所述智能卡时可执行所述加密算法。

[0030] 技术效果

[0031] 由于不是在加密模块外部生成密钥来存储在存储器中或通过总线来传输密钥,因此,对于非易失性存储器的攻击或总线探测(bus probing)等物理性攻击具安全性。

[0032] 由于密钥模块在模块内部与其他标准单元(standard cell)相似地被分散配置,因此,较难直接发现,对于通过物理性攻击来提取存储器内容的攻击具安全性。

[0033] 由于不需要存储密钥的非易失性存储器,因此,可改善空间和电力的使用量。

附图说明

[0034] 图1是示出根据本发明的一个实施例的加密装置的示图。

[0035] 图2是示出根据本发明的一个实施例的加密模块的示图。

[0036] 图3是示出根据本发明的一个实施例的加密模块的示例性结构的框图。

[0037] 图4是用于说明根据本发明的一个实施例,利用工程变差来生成密钥的物理防克隆功能PUF(Physical Unclonable Functions)形式的密钥模块的单位晶格的概念的示例性电路图。

[0038] 图5是用于理解图4的实施例的参照图表。

[0039] 图6是示出根据本发明的一个实施例的密钥模块的的示例性体现的框图。

[0040] 图7是示出根据本发明的一个实施例,利用差分放大器的工程变差来生成数字值的密钥模块的单位晶格的示图。

[0041] 图8是根据本发明的一个实施例,示出密钥模块被体现的示例性电路图。

[0042] 图9是根据本发明的一个实施例,用于说明违反半导体设计规定来生成密钥模块的原理的概念图。

[0043] 图10是根据本发明的一个实施例,用于说明违反半导体设计规定的密钥模块的结构的图表。

[0044] 图11是根据本发明的一个实施例,用于说明调整导电层之间的间隔来生成密钥模块的过程的概念图。

[0045] 图12是示出根据本发明的一个实施例,用于体现密钥模块的半导体层中所形成的通路或接点阵列的示例性结构的概念图。

[0046] 图13是根据本发明的一个实施例,用于说明不直接将图12的实施例中所生成的数字值作为密钥来使用,而是为了0和1的平衡进行后处理的该过程的概念图。

具体实施方式

[0047] 以下，参照附图对本发明的一部分实施例进行详细地说明。但是，本发明并不受实施例限制或局限，各附图中所示出的相同符号表示相同的部件。

[0048] 图1是示出根据本发明的一个实施例的加密装置100的示图。

[0049] 根据一个例子，加密装置100可以是包含在智能卡的IC芯片中的结构，具有存储数据的电可擦只读存储器(EEPROM)120、中央处理器(CPU) 130、及可选择的同步动态随机存储器(SDRAM)140，并可通过I/O界面101与外部通信。

[0050] 加密装置100中包括加密模块110，例如，加密模块110可以是用于加密的协处理器(Crypto co-processor)。

[0051] 以下，根据包含智能卡或智能卡的IC芯片的加密装置100的应用实例，电可擦只读存储器(EEPROM)120、中央处理器(CPU)130、及可选择的同步动态随机存储器(SDRAM)140中的至少一部分可被省略，并在不超出本发明的思想范围下可进行多种改变或应用，在此不作详细说明。

[0052] 此外，不管是接触式和/或非接触式的方式，I/O界面101为将数据输出及输入加密装置100的输出入线路，在此不作详细说明，

[0053] 此外，根据本发明的一个实施例的加密装置100的加密模块110可在执行加密算法的过程中使用密钥。该密钥可以是公开密钥和保密密钥等概念。

[0054] 现有技术中，将用于执行加密算法的密钥以数字值的形式存储在加密模块110外部，从而加密模块110执行加密算法，在将数据加密和/或解码的过程中通过总线102来接收密钥。

[0055] 但是，该方法，在打算识别加密算法和/或密钥的物理性攻击中较脆弱。

[0056] 该物理性攻击可在电可擦只读存储器(EEPROM)120等存储器中直接攻击具密钥的区域，以类似探测(probing)或存储器扫描的方法来提取存储器内的密钥。此外，由于可执行逆向工程来获取IC芯片中总线102的位置，因此，将特定的命令语人为地来执行，并在该情况下执行利用微探针(Micro- probe)的总线探测(Bus probing)的话可提取密钥。

[0057] 根据本发明的一个实施例，加密模块110中所包含的密钥模块111将直接生成和/或预先生成的密钥在密钥模块111中存储一段时间后，在加密模块 110执行加密算法时来提供密钥。

[0058] 因此，根据上述实施例，加密模块110在执行加密算法的过程中，不将使用的密钥以数字值的形式存储在加密模块110的外部，且由于密钥不会通过总线102被传输，因此，可防止对于加密模块110的加密算法的物理性攻击。

[0059] 生成和/或存储密钥从而在加密模块110的加密算法执行时进行提供的密钥模块111，其可物理性地包括在加密模块110中，有关其结构和运作的一些示例性实施例将参照图2进行说明。

[0060] 图2是示出根据本发明的一个实施例的加密模块110的示图。

[0061] 如图1中所示出的，加密模块110在加密装置100中可通过其他结构与总线102连接。

[0062] 根据本发明的一个实施例，加密模块110中包括至少一个的密钥模块 210、220、230、240、250。

[0063] 如示例的图所示，密钥模块210、220、230、240、250各自独立或互相关联，生成和/或存储执行加密算法时所需的密钥，并提供给加密模块110。

[0064] 在一些实施例中，加密模块110中可能只包括一个密钥模块，但是，在其他是实施例中如图2所示，包括多个密钥模块。

[0065] 此外，当加密模块110中包括多个密钥模块时，多个密钥模块210、220、230、240、250中的至少一部分可能是实际上不提供密钥的虚拟 (dummy)。

[0066] 在体现密钥模块210、220、230、240、250的实施例中，密钥模块210、220、230、240、250可以是存储装置(memory device)和非存储装置(non- memory device)两种情况。

[0067] 当然，也可以是密钥模块210、220、230、240、250中的一部分为存储装置，且另一部分为非存储装置，本发明并不仅局限于该一部分实施例。

[0068] 示例性地，在密钥模块210、220、230、240、250为存储装置的实施例中，预先生成的数字值形式的密钥被单纯地存储在作为存储装置的密钥模块 210、220、230、240、250一段时间后，在加密模块110执行加密算法的过程中需要时进行读取(read)并使用。

[0069] 在其他实施例中，当密钥模块210、220、230、240、250为非存储装置时，密钥模块210、220、230、240、250的至少一部分可通过物理防克隆功能PUF(Physical Unclonable Functions)来实现。

[0070] 在密钥模块210、220、230、240、250由类似PUF的非存储装置构成的实施例中，体现PUF的实施例具多种方式，例如，可违反半导体制备工程上的设计规定或利用半导体制备工程的工程变差来实现。

[0071] 对于该实施例，将参照图4至图13进行更详细地说明。

[0072] 图3是示出根据本发明的一个实施例的加密模块110的示例性结构的框图。

[0073] 当进行加密的数据可通过总线102等被输入至数据输入单元310时，便开始执行加密算法。

[0074] 参照图2，如上所述，被物理性地包含在加密模块110中的密钥模块 320可以是一个或多个。

[0075] 例如，当密钥模块01 321至密钥模块N322存在时，密钥模块选择单元330选择密钥模块，用于提供加密算法中将使用的密钥，其中，N为自然数。

[0076] 该选择，可以是用于识别密钥模块320的索引中实际被选择的密钥模块的索引信息，或是密钥模块320与加密模块110一起被设计，并可在被制备的过程中，通过接线(wiring)被预先设置。

[0077] 通过该过程设定密钥后，加密单元340利用该密钥执行加密算法，从而将输入的数据加密，并经由数据输出单元350通过总线102传输至其他结构。

[0078] 以上，虽然只对数据加密过程进行了详细地说明，但利用加密算法的解码过程也与此相似。本发明的实施例并仅不局限于加密或解码的任何一方。

[0079] 由此，密钥的管理在加密模块110中自动形成，因此，密钥不会被传输至加密模块110的外部，或是从外部传输至加密模块110中，从而物理性攻击成功的可能性较低。特别是，探测总线102的物理性攻击成功的可能性十分低。

[0080] 以上参照图1至图2对密钥模块为存储装置时进行了说明，以下，参照图4至图13，对密钥模块由非存储装置的PUF被体现的实施例进行说明。

[0081] 作为参考，本发明中所提到的PUF不可执行物理性复制，在一次性制备后，生成至少理论上不会变化的密钥。

[0082] 以下，对密钥模块由非存储装置的PUF被体现的多种实施例进行说明，图4至图8对应于利用半导体工程(Semiconductor Process)中的工程变差来生成密钥的密钥模块的实施例。

[0083] 此外，图9至图13对应于设计电路时违反设计规定从而生成密钥模块的实施例。

[0084] 图4是用于说明根据本发明的一个实施例，利用工程变差来生成密钥的物理防克隆功能PUF形式的密钥模块的单位晶格的概念的示例性电路图。

[0085] 在图4的实施例中，示出第1逆变器410和第2逆变器420。

[0086] 在半导体工程中，工程变差经多种原因而发生。例如，在制备晶体管时，有效栅(gate)长度、半导体掺杂物密度相关指数、氧化层厚度相关指数、或阈值电压等参数都可能成为工程变差的原因。

[0087] 一般情况下，认为较小的半导体制备工程其工程变差较为优秀，但是，在物理性特征上，可使工程变差尽可能化小但不可能完全消除。

[0088] 在本实施例中，第1逆变器410可具有第1逻辑阈值，且第2逆变器 420具有第2逻辑阈值。逻辑阈值(logic threshold)为逆变器的输入电压和输出电压具相同的值时的电压值，以下将参照图5来进行说明。

[0089] 逆变器的逻辑阈值可被检测为使运作中的逆变器的输出端和输入端短路(short)时的电压值。

[0090] 在相同的工程中被制备的逆变器，理论上被设计为具有相同的逻辑阈值，但如上所述，由于在实际的制备工程中存在工程变差，因此，任何的两个逆变器不可能具有完全相同的逻辑阈值。

[0091] 根据本发明的一个实施例，所述第1逆变器410和所述第2逆变器420 在相同的制备工程中被制备，因此，具有因工程变差的逻辑阈值的差异性。

[0092] 所述逻辑阈值的差异虽然根据工程工程而不同，但可能相差数毫伏至数十毫伏的差异。因此，由于检测上的误差，利用另外的比较器电路来检测所述第1逆变器410的逻辑阈值和所述第2逆变器420的逻辑阈值并不准确。

[0093] 因此，需要一种可相对性地比较两个逆变器的逻辑阈值(即，不使用另外的比较器电路来进行检测)的方法。在本发明的一些实施例中，将两个逆变器之间的逻辑阈值进行相对性地(不使用另外的比较器电路而是自动地) 比较，从而可判断哪一方的逻辑阈值较大。

[0094] 假设第2逆变器420不存在，当第1逆变器410的输入端和输出端短路时，第1逆变器410的输出电压与所述第1逆变器410的逻辑阈值相同。

[0095] 此外，假设第1逆变器410不存在，当第2逆变器420的输入端和输出端短路时，第2逆变器420的输出电压与所述第2逆变器420的逻辑阈值相同。

[0096] 但是，如图4所示，第1逆变器410的输入端和第2逆变器420的输出端被短路，通过第1节点被连接时，且第1逆变器410的输出端和第2逆变器420的输入端被短路，通过第2节点被连接时，具有与上述不同的结果。

[0097] 利用开关430使所述第1节点和所述第2节点短路时，被短路的所述两个节点的电压值为所述第1逆变器410的逻辑阈值和所述第2逆变器420的逻辑阈值的中间值(可能为平

均值以下)。

[0098] 与所述两个逆变器的逻辑阈值中哪一方的值较高无关,在所述开关430 关闭期间,输出电压的值为所述两个逆变器的逻辑阈值的中间值。

[0099] 此外,之后将开关430打开,在使所述第1节点和所述第2节点开路 (open)时,所述第1节点和所述第2节点中任何一个的电压值的逻辑电平 (logical level)为“0”,且另一个的逻辑电平为“1”。

[0100] 例如,假设当第1逆变器410的逻辑阈值比所述第2逆变器420的逻辑阈值低时,所述开关430被关闭,第1节点(输出Out的相反节点)和第2 节点(输出Out节点)被短路期间的第1节点的电压比所述第1逆变器410 的逻辑阈值要高。

[0101] 因此,所述开关430重新打开,所述第1节点和所述第2节点开路后,第1逆变器410将(自身的输入端)第1节点的电压识别为高(High)逻辑电平,因此,第1逆变器210的输出端第2节点的电压为低(Low)逻辑电平。

[0102] 在这种情况下,第2逆变器420将(自身的输入端)第2节点的电压识别为低逻辑电平,因此,第2逆变器420的输出端第1节点的电压为高逻辑电平。

[0103] 结果,图4的输出端("Out")第2节点的电压为高(High)逻辑电平。

[0104] 相反,假设第1逆变器410的逻辑阈值比所述第2逆变器420的逻辑阈值高时,所述开关430关闭,第1节点和第2节点被短路期间的第1节点的电压比所述第1逆变器410的逻辑阈值低。

[0105] 因此,所述开关430重新打开,所述第1节点和所述第2节点开路后,第1逆变器410将(自身的输入端)第1节点的电压识别为低逻辑电平,因此,第1逆变器410的输出端第2节点的电压为高逻辑电平。

[0106] 在这种情况下,第2逆变器420将(自身的输入端)第2节点的电压识别为高逻辑电平,因此,第2逆变器420的输出端第1节点的电压为低逻辑电平。

[0107] 结果,图4的输出端("Out")第2节点的电压为低逻辑电平。

[0108] 如上所述,根据第1逆变器410的逻辑阈值和第2逆变器420的逻辑阈值中哪一方较高,来决定开关430的短路-开路后的输出端("Out")的逻辑电平为高(或是“1”)还是低(或是“0”)。

[0109] 但是,在相同的制备工程中所制备的所述第1逆变器410和第2逆变器 420中,哪一方的逻辑阈值较高具随机性(random),概率性地两个逆变器中一方的逻辑阈值比另一方的逻辑阈值高的概率约为50%。

[0110] 此外,制备后,较难改变所述逻辑阈值较高一方为哪一方。

[0111] 结果,通过图4的实施例,可生成1比特的数字值(为“1”或“0”的概率虽然相同,但一旦决定后较难改变)。

[0112] 参照图5时,上述过程将会更清楚地被理解。

[0113] 图5是用于理解图4的实施例的参照图表。

[0114] 在本示例性参照图表中,示出图4的第1逆变器410的逻辑阈值比第2 逆变器420的逻辑阈值低时的电压特性(voltage characteristic)。

[0115] 曲线510为第1逆变器410的电压特征曲线,且曲线520为第2逆变器 420的电压特征曲线。根据本发明的一个实施例,当第1逆变器410和第2 逆变器420在相同的制备工程中

被制备时，曲线510和曲线520虽然基本一致，但由于工程变差的原因具有一点差异。

[0116] 在找到曲线510和倾斜的1条直线530的交点时，可确定第1逆变器 410的逻辑阈值V1。此外，在找到曲线520和直线530的交点时，可确定第2逆变器420的逻辑阈值V2。

[0117] 在本实施例中V1比V2低，因此，图4的开关430关闭，当第1节点和第2节点被短路时(也称为“Reset”)，第1节点和第2节点的电压(VReset) 为V1和V2之间的任何值。

[0118] 此外，所述开关430重新打开，所述第1节点和所述第2节点开路后，第1逆变器410将第1节点的电压(VReset)识别为高逻辑电平，因此，第1 逆变器410的输出端第2节点的电压为低逻辑电平。

[0119] 在这种情况下，第2逆变器420将第2节点的电压(VReset)识别为低逻辑电平，因此，第2逆变器420的输出端第1节点的电压为高逻辑电平。

[0120] 因此，图4的输出端("Out")第2节点的电压为高逻辑电平。

[0121] 如图4所示，单位晶格为1比特的数字值时，将该单位晶格集成N个时，N比特的数字值可生成密钥。

[0122] 根据本发明的一些实施例，密钥模块320可通过该方式被体现。

[0123] 密钥模块可如以下图6所示的结构被体现，通过利用半导体工程变差的逆变器装置的逻辑阈值差异来生成数字值形式的密钥。

[0124] 图6是示出根据本发明的一个实施例的密钥模块600的的示例性体现的框图。

[0125] 在本实施例中，密钥模块600包括：逆变器611至逆变器615的5个逆变器、选择单元620、和比较单元630。

[0126] 选择单元620可选择图6中所示出的5个逆变器中的任何两个，例如，可选择逆变器612和逆变器613。

[0127] 在这种情况下，比较单元630比较逆变器612的逻辑阈值和逆变器613 的逻辑阈值，并根据比较结果，向输出(Out)端提供输出电压。此外，可根据所述输出(Out)端的输出电压的逻辑电平来生成1比特的数字值。

[0128] 此外，当选择单元620选择另外的两个逆变器时，所述比较单元630可重新生成1比特的数字值。

[0129] 如上所述，选择单元620可选择5个逆变器(611至615)中的两个，且当比较单元630将选择的两个逆变器的逻辑阈值进行比较来生成数字值时，最多可获取10比特的数字值。

[0130] 在本实施例中，虽然包括5个逆变器，但本发明并不局限于，用关生成的数字值的比特数、电路的面积等都可进行多种改变。

[0131] 此外，当半导体芯片内可集成的比较单元630的面积比逆变器(611至 615)的面积大时，在本实施例中，多个逆变器和一个比较单元630通过选择单元620被连接。但是，在其他应用实施例中，每两个逆变器可与一个比较单元形成对来生成N比特的数字值。

[0132] 此外，利用半导体工程变差的逆变器装置的逻辑阈值差异来生成数字值形式的密钥的密钥模块也可通过如图7所示的结构被体现。

[0133] 图7是示出根据本发明的一个实施例，利用差分放大器的工程变差来生成数字值的密钥模块的单位晶格700的示图。

[0134] 单位晶格700为差分放大器电路。由晶体管和电阻中的至少一个所构成的差分放大器电路单位晶格700，其将第1输入端711和第2输入端712的电压差异扩大，作为第1输出

端721和第2输出端722之间的电压差异来提供。

[0135] 因此，当所述第1输入端711和第2输入端712短路时，理论上，输出电压值第1输出端721和第2输出端722之间的电压差异应该为0。

[0136] 但是，由于半导体工程变差，装置之间具电器特征差异，因此，第1输出端721的电压和第2输出端722的电压不可能完全一样。

[0137] 因此，在图6的实施例中，通过类似将逆变器的逻辑阈值进行比较的方法，在比较两个输出端中哪个输出端的电压较高时，可生成1比特的数字值。

[0138] 例如，在使第1输入端711和第2输入端712短路的情况下，当第1输出端721的电压值高于第2输出端722的电压值时，识别为数字值“1”，且在相反的情况下，可识别为数字值“0”

[0139] 因此，当该差分放大器单位晶体700被集成N个时，可通过N比特的数字值形式来提供密钥，从而根据本发明的一些实施例的密钥模块可被体现。该体现在图8中被示出。

[0140] 图8是根据本发明的一个实施例，示出密钥模块800被体现的示例性电路图。

[0141] 在图示的实施例中，密钥模块800包括：6个差分放大器(811至816)；用于选择所述6个差分放大器中的任何一个的选择单元820；和比较器830，比较经所述选择单元820被选择的差分放大器的两个输出电压，来生成1 比特的数字值。

[0142] 在这种情况下，所述6个差分放大器(811至816)的整个输入端被短路，具有相同的电压。

[0143] 根据本发明的一个实施例，选择单元820可以是6:1多路复用器(6:1 MUX)。但是，其仅仅是用于体现本发明的一个实施例，本发明并不局限于该特定实施例。

[0144] 因此，MUX装置的输入/输出端口的个数可改变，进一步，选择单元820可以是其他装置而不是MUX装置，所述6:1MUX装置将通过12个输入端输入的6个差分放大器的输出电压向两个输出端输出。此外，该两个输出端与比较器830的两个输入端连接。

[0145] 在所述实施例中，密钥模块800可生成6比特的数字值密钥。

[0146] 以上，参照图4至图8对利用半导体工程的工程变差来体现密钥模块的实施例进行说明。

[0147] 以下，参照图9至13，对违反半导体设计规定从而来体现密钥模块的实施例进行说明。

[0148] 图9是根据本发明的一个实施例，用于说明违反半导体设计规定来生成密钥模块的原理的概念图。

[0149] 通常，接点或通路被设计用来使导电层之间连接，通常，确定接点或通路尺寸来使导电层短路。此外，在常规的设计规定(rule)中，规定有最起码的接点或通路尺寸来确保导电层之间短路。

[0150] 但是，在根据本发明的一个实施例的密钥模块的体现中，使接点或通路的尺寸比设计规定中所指定要小，从而一部分的接点或通路使导电层之间短路，且其他一部分的接点或通路不会使导电层之间短路，该导电与否被概率性地确定。

[0151] 在现有的半导体工程中，当接点或通路不能使导电层之间短路时，为工程上的失败，但可利用其来生成具随机数的密钥。

[0152] 参照图9，示出在半导体制备工程中，金属1层902和金属2层901之间通路被形成。

[0153] 在根据设计规定使通路尺寸较大的组910中，所有通路使金属1层902 和金属2层901短路，将短路与否以数字值来表示时，都为0。

[0154] 此外，在通路尺寸较小的组930中，所有通路没有使金属1层902和金属2层901短路。因此，将短路与否以数字值来表示时，都为1。

[0155] 此外，在通路尺寸为组910和组930之间的组920中，一部分通路使金属1层902和金属2层901短路，且其他一部分的通路没有使金属1层902 和金属2层901短路。

[0156] 根据本发明的一个实施例，为实现密钥模块，如组920所示，一部分通路使金属1层902和金属2层901短路，且其他一部分通路被设定通路尺寸来构成，从而不会使金属1层902和金属2层901短路。

[0157] 有关通路尺寸的设计规定根据半导体制备工程有所不同。例如，在0.18 微米(um)的互补金属氧化物半导体CMOS(Complementary metal oxide semiconductor)，当通路的设计规定为0.25微米时，在根据本发明的一个实施例的密钥模块的体现中，违反设计规定，将通路尺寸设置为0.19微米，从而使金属层之间的短路与否概率性的分布。

[0158] 优选是，该短路与否的概率分布具有50％的短路概率，在根据本发明的一个实施例的密钥模块的体现中，使概率分布最大限度地接近50％来设置并构成通路尺寸。在该通路尺寸设置中，可通过工程试验来确定通路尺寸。

[0159] 图10是根据本发明的一个实施例，用于说明违反半导体设计规定的密钥模块的结构的图表。

[0160] 在图表中，通路尺寸越大，金属层之间的短路概率可为接近于1。根据设计规定的通路尺寸Sd，是充分确保金属层之间短路的值。

[0161] 此外，S_m是理论上金属层的短路概率为0.5的通路尺寸，如上所述，根据工程，值不同时，可通过试验获取最大相似值，但较难获取准确的S_m。

[0162] 因此，在根据本发明的一个实施例的密钥模块的体现中，根据具体的试验，金属层之间的短路与否可设置在0.5中具一定许可误差的Sx1和Sx2范围内(所述Sx1和Sx2虽然没有另外示图，但可以是图示的Sx附近的具一定边缘的区域)。

[0163] 在图9至图10中，虽然对违反有关通路尺寸的设计规定来体现密钥模块的实施例进行了说明，但根据本发明的其他一些实施例，也可通过违反有关导电层之间的间隔(gap)的设计规定来体现密钥模块。

[0164] 图11是根据本发明的一个实施例，用于说明调整导电层之间的间隔来生成密钥模块的过程的概念图。

[0165] 如上所述，根据本发明的实施例，调整金属线之间的间隔，从而来概率性地确定金属线之间的短路与否。

[0166] 在为充分确保金属线之间的短路，金属线间隔较小的组1110中，在所有的情况下金属线都被短路。

[0167] 此外，金属线间隔较大的组1130中，在所有的情况下金属线没有被短路。

[0168] 在本实施例中，为实现密钥模块，如组1120所示，设置用于概率性地形成短路的金属线间隔，从而使金属线中的一部分被短路，且一部分没有被短路。

[0169] 图12是示出根据本发明的一个实施例，用于体现密钥模块1200的半导体层中所形成的通路或接点阵列的示例性结构的概念图。

[0170] 半导体基板(substrate)中被积层的金属层之间形成有横向M个,纵向N 个(但M和N为自然数),总共M*N个通路。

[0171] 密钥模块1200根据M*N个的通路各自使金属层之间短路(数字值为0) 或不短路(数字值为1)的与否,来生成M*N比特(bit)的密钥。

[0172] 图13是根据本发明的一个实施例,用于说明不直接将图12的实施例中所生成的数字值作为密钥来使用,为了0和1的平衡进行后处理的过程的概念图。

[0173] 根据本发明的一个实施例,密钥模块1200中所生成的M*N比特的数字值被集聚成所定的k个单位,且k为自然数。

[0174] 当然,图13中所示出的集聚是便于说明的示例性附图,在实际的体现中,可使用将密钥模块1200内的晶体管或触发器进行集聚的方法。

[0175] 因此,通过将数字值集聚等方法来执行0和1的平衡的过程可由本领域的普通技术人员通过多种变形和应用来执行,且不超出本发明的范围。

[0176] 在图13的实施例中,4个数字值被集聚成一个组。

[0177] 密钥模块1200将组1310和组1320各自生成的4比特的数字值的大小进行比较。此外,当组1310的4比特数字值比组1320的4比特数字值大时,代表所述组1310和组1320的数字值为1。

[0178] 相反,当组1310的4比特数字值比组1320的4比特数字值小时,代表所述组1310和组1320的数字值为0。

[0179] 在其他实施例中,可比较组之间的数字值1的个数来选择代表组的数字值。

[0180] 根据本发明的实施例的方法可通过多种计算机手段以可执行的程序命令形式记录在计算机可读媒体中。该计算机可读媒体可包括独立的或结合的程序指令、数据文件、数据结构等。该媒体记录的程序指令可专门为本发明的目的设计和创建,或为计算机软件技术人员熟知而应用。计算机可读媒体的例子包括:磁媒体(magnetic media),如硬盘、软盘和磁带;光学媒体(optical media),如CD ROM、DVD;磁光媒体(magneto-optical media),如光盘 (floptical disk);和专门配置为存储和执行程序指令的硬件设备,如只读存储器(ROM)、随机存取存储器(RAM)等。程序指令的例子,既包括机器代码,如由编译器产生的,也包括含有可由计算机使用解释程序执行的更高级代码的文件。所述硬件设备可配置为作为一个以上软件模块运行以执行上面所述的本发明的运作,反之亦然。

[0181] 如上所示,本发明虽然已参照有限的实施例和附图进行了说明,但是本发明并不局限于所述实施例,在本发明所属领域中具备通常知识的人均可以从此记载中进行各种修改和变形。

[0182] 因此,本发明的范围不受说明的实施例的局限或定义,而是由后附的权利要求范围以及权利要求范围等同内容定义。

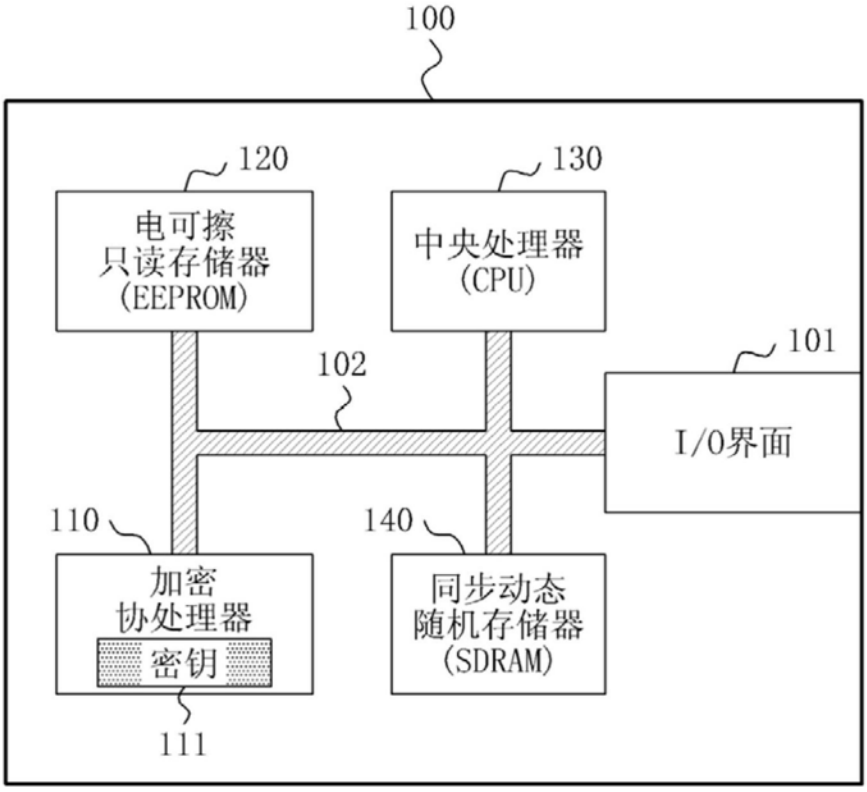

100
120
电可擦
只读存储器
(EEPROM)
130
中央处理器
(CPU)
101
102
I/O界面
110
加密
协处理器
密钥
111
140
同步动态
随机存储器
(SDRAM)

图1

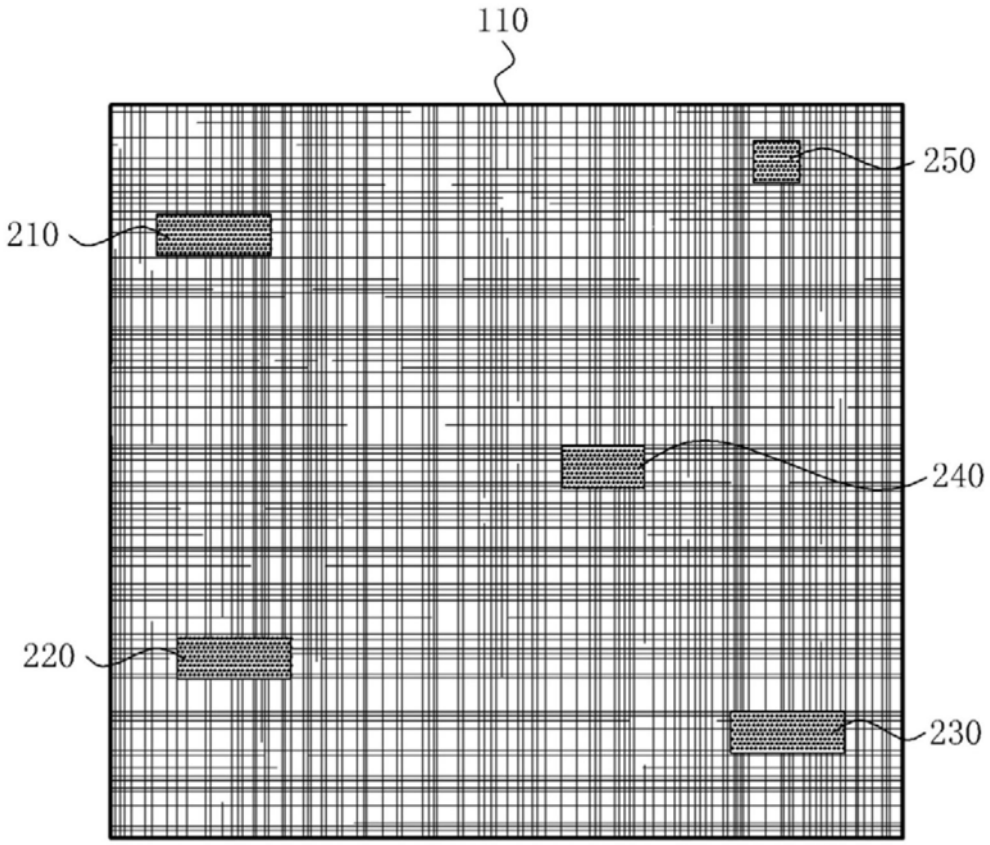


图2

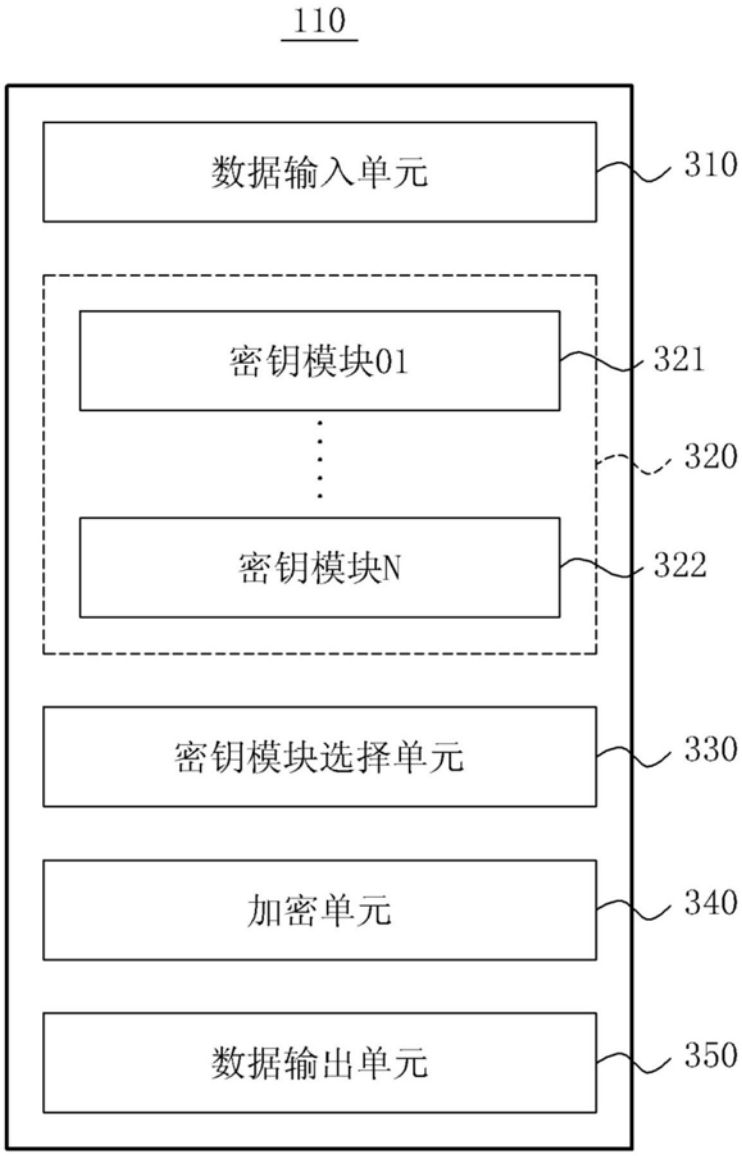

110
数据输入单元
310
密钥模块01
321
320
密钥模块N
322
密钥模块选择单元
330
加密单元
340
数据输出单元
350

图3

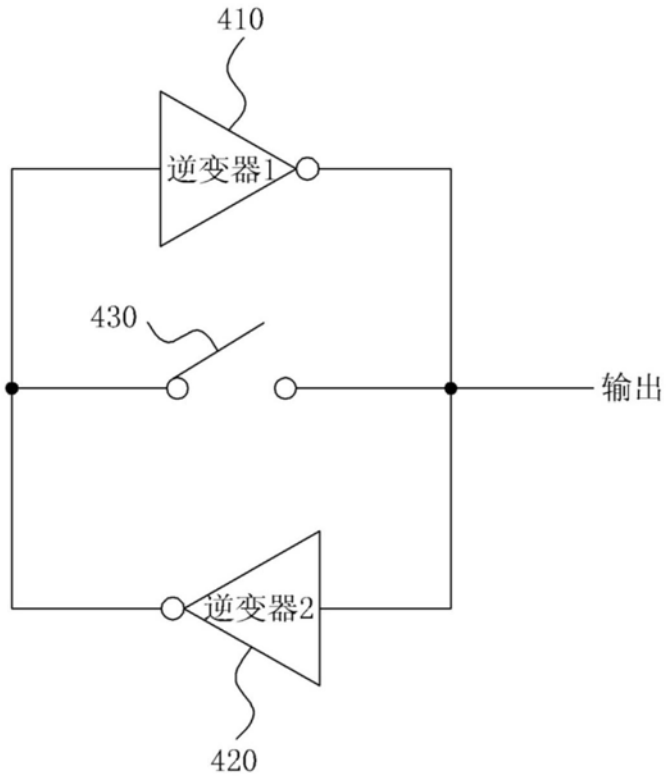

410
逆变器1
430
输出
逆变器2
420

图4

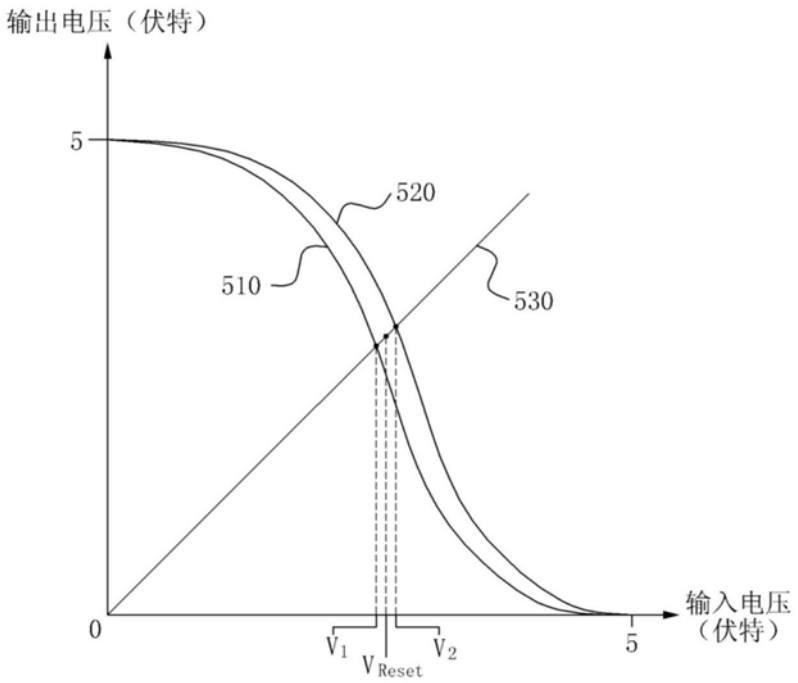

输出电压（伏特）
5
520
510
530
0
输入电压
（伏特）
5
V_1
V_2
V_{Reset}

图5

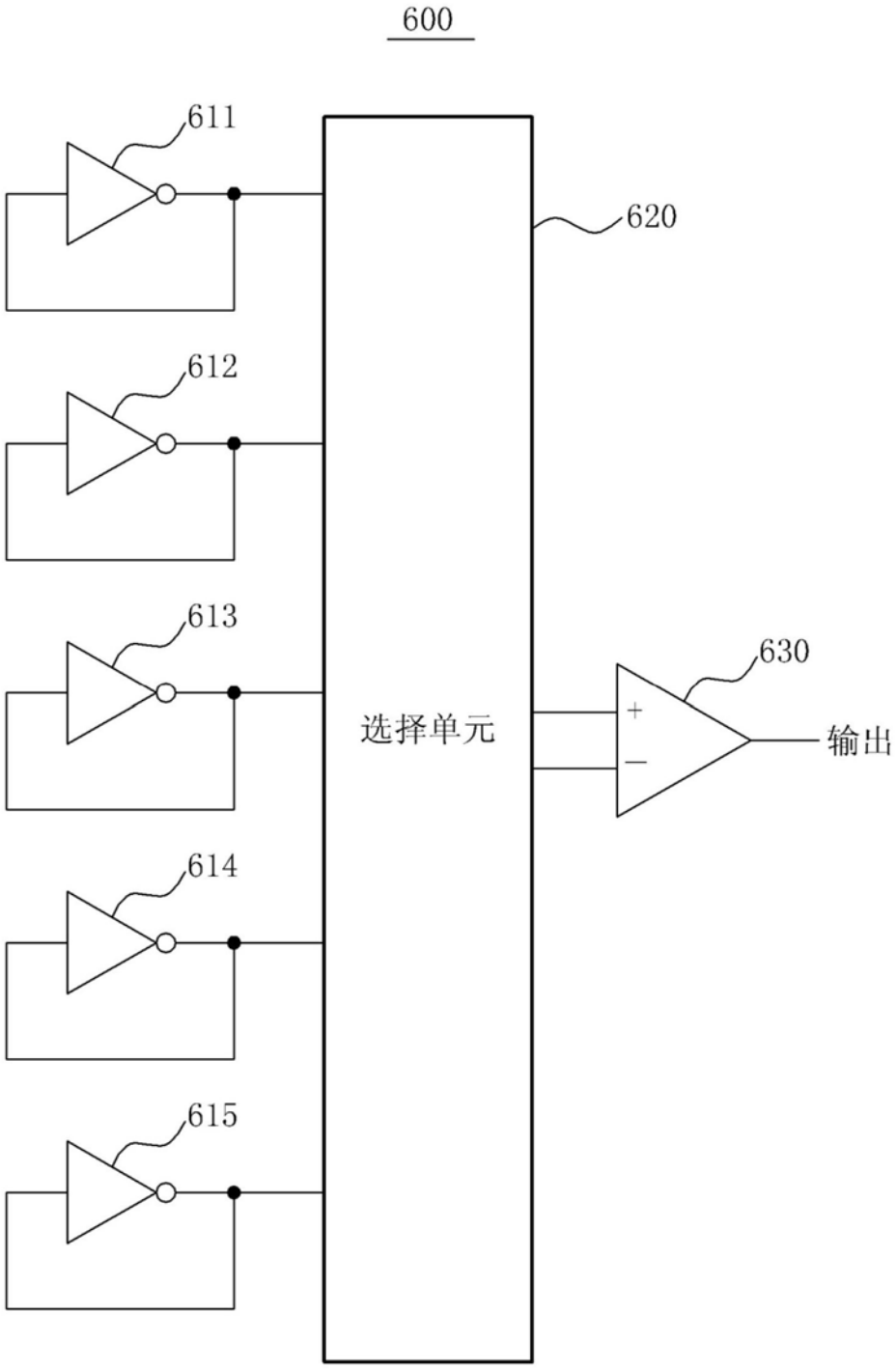


图6

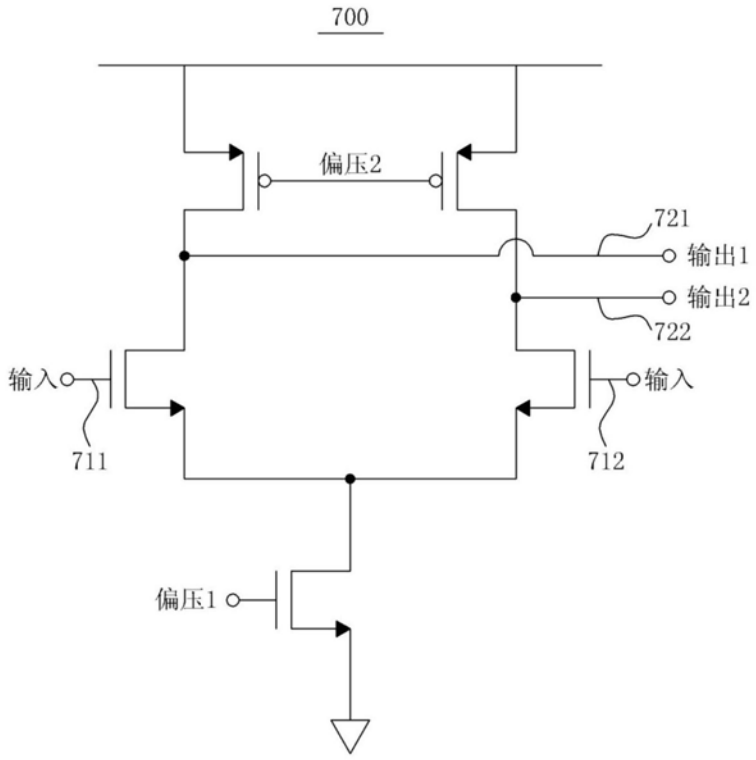

700
偏压2
721
输出1
输出2
722
输入
711
输入
712
偏压1

图7

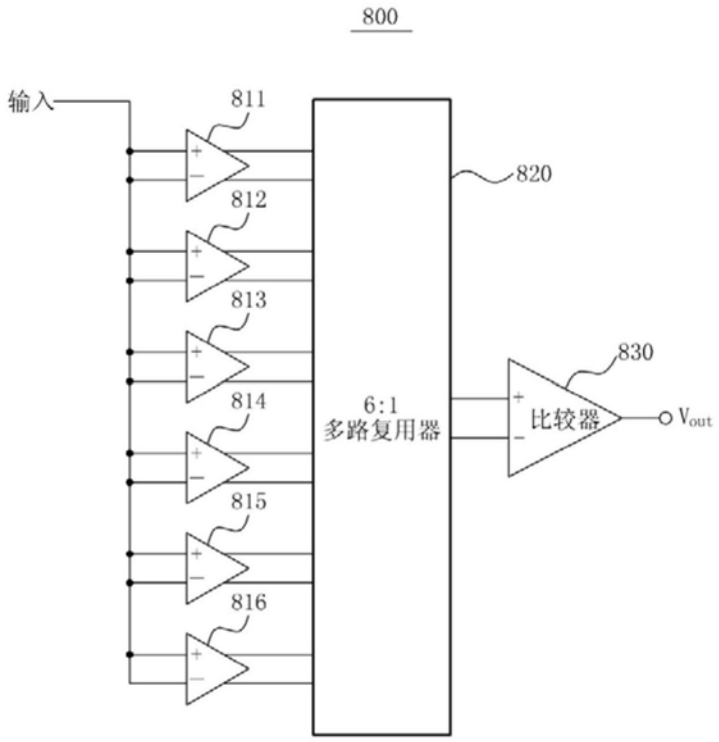

800
输入
811
812
813
814
815
816
820
6:1
多路复用器
830
比较器
Vout

图8

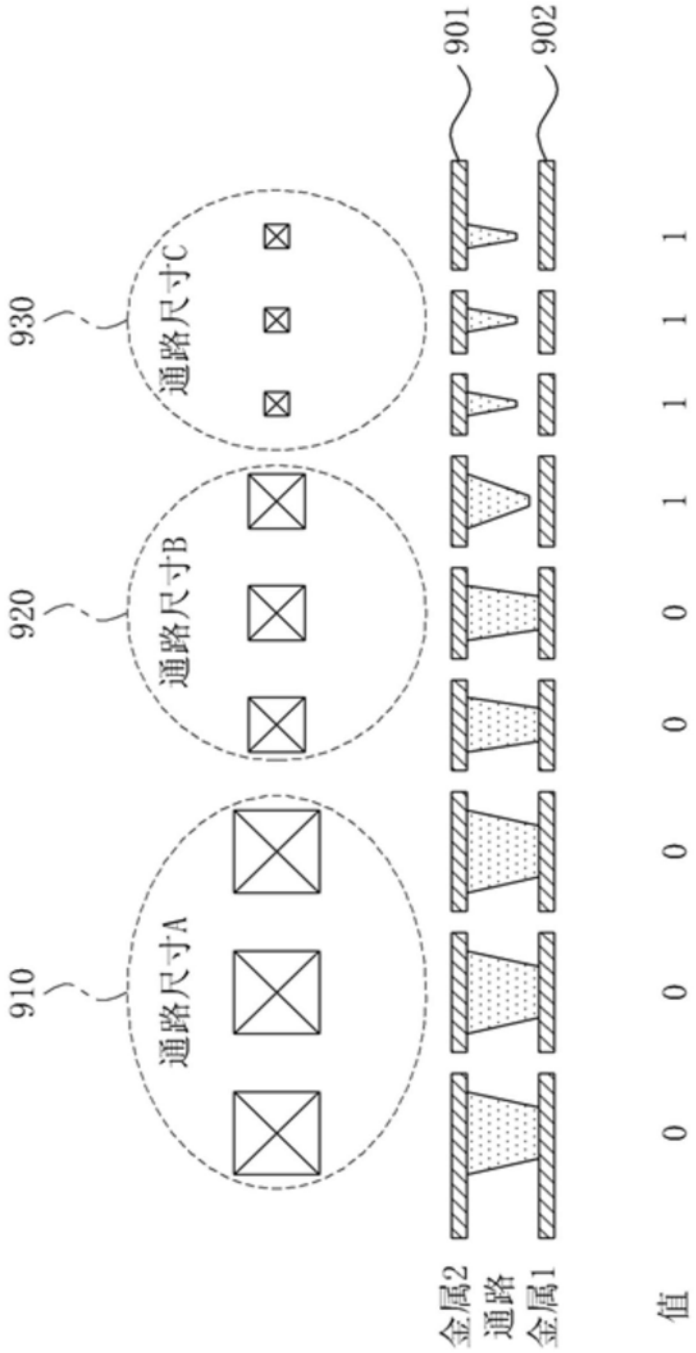


图9

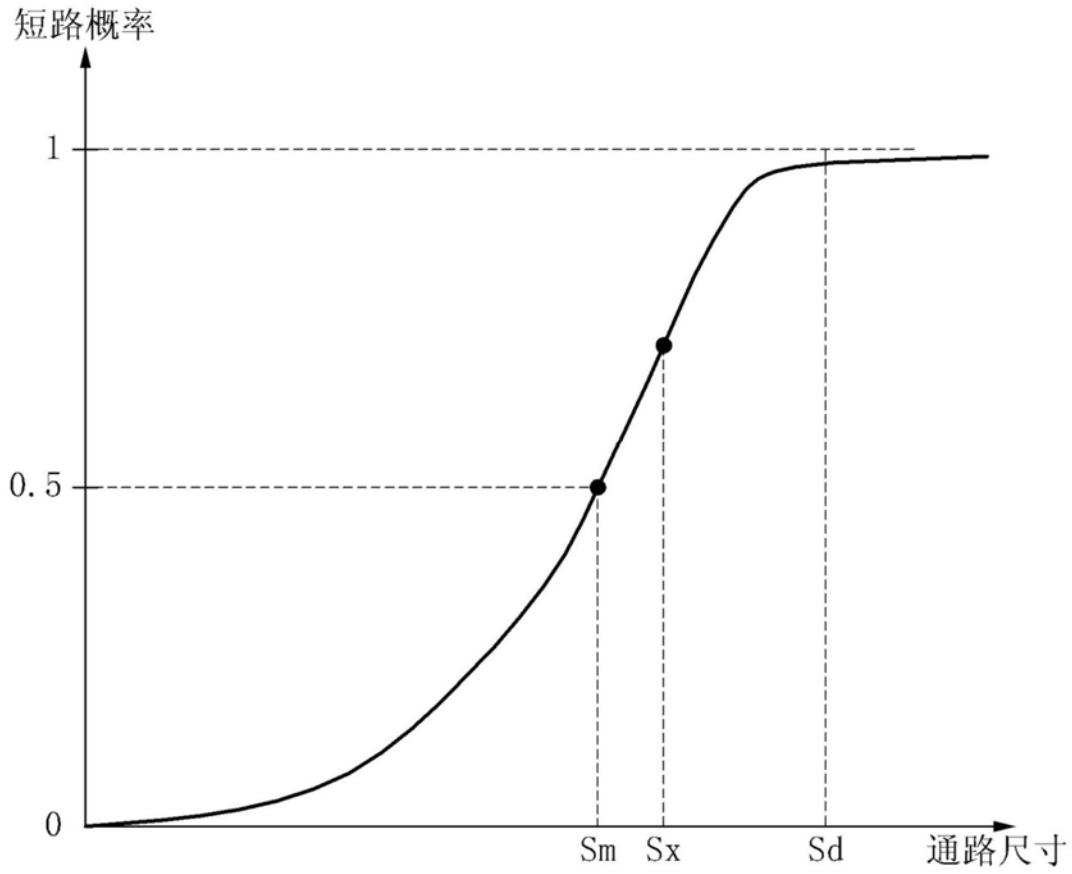


图10

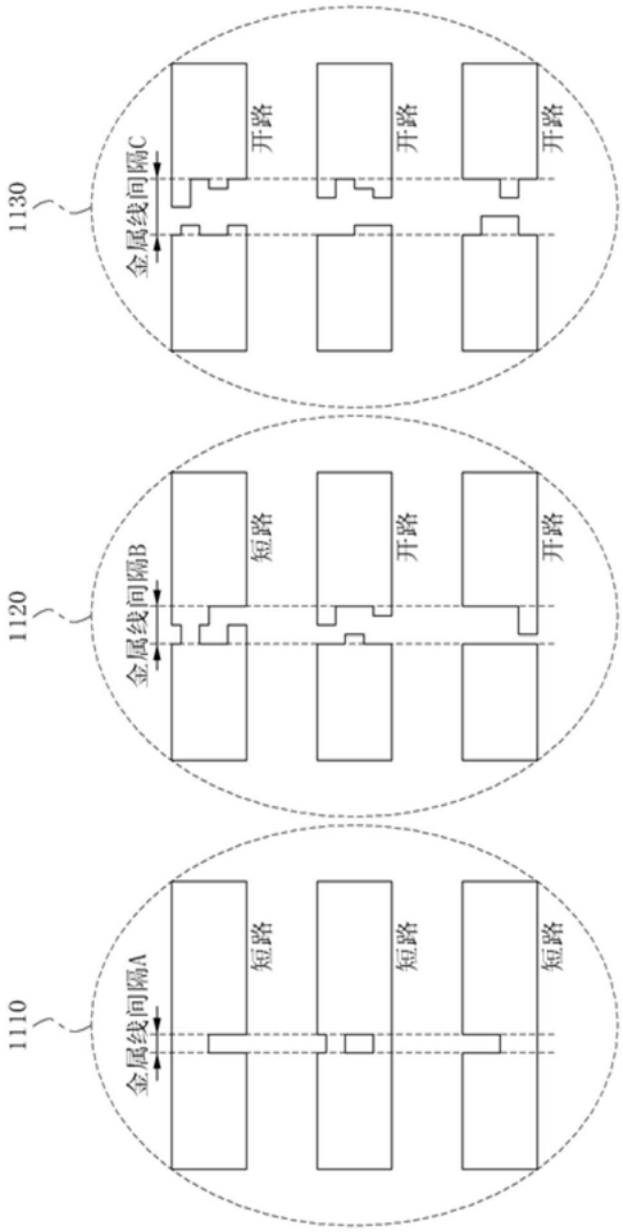


图11

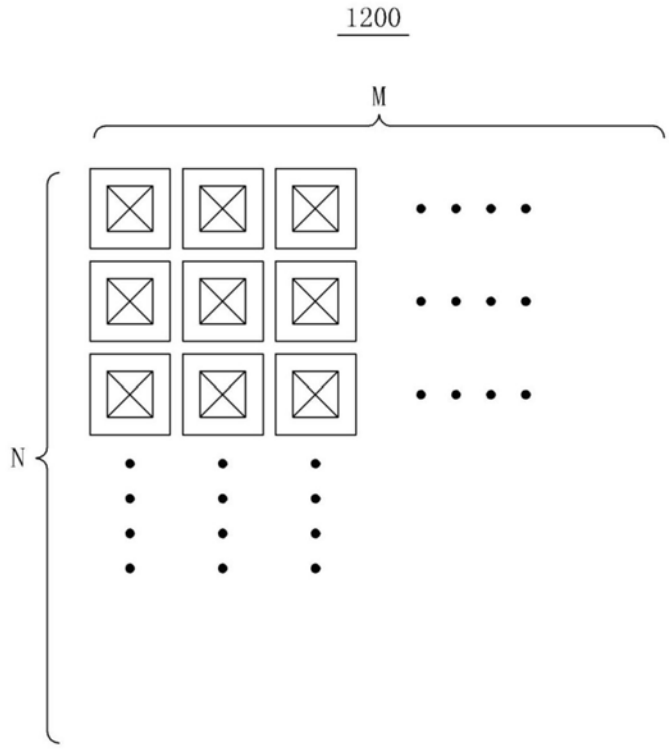


图12

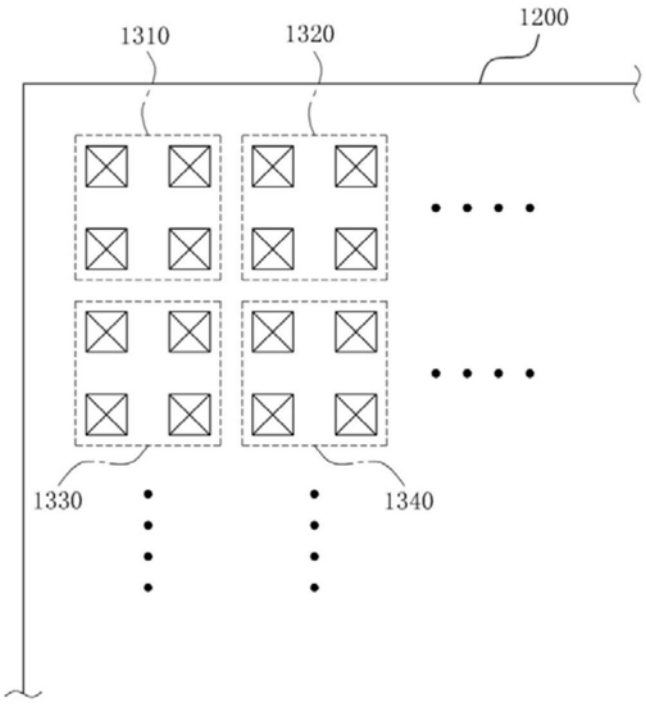


图13