(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105122722 A
(43)申请公布日 2015.12.02

(21)申请号 201480013393.8
(22)申请日 2014.01.10
(30)优先权数据
13/739,429 2013.01.11 US
13/838,853 2013.03.15 US
(85)PCT国际申请进入国家阶段日
2015.09.09
(86)PCT国际申请的申请数据
PCT/US2014/011064 2014.01.10
(87)PCT国际申请的公布数据
WO2014/110384 EN 2014.07.17
(71)申请人 威瑞斯蒂公司
地址 美国北卡罗来纳州
(72)发明人 威廉·埃利·撒克
罗伯特·弗朗西斯·滕采尔
迈克尔·克林顿·霍克
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张焕生 谢丽娜
(51)Int.Cl.
H04L 9/00(2006.01)
H04L 9/06(2006.01)

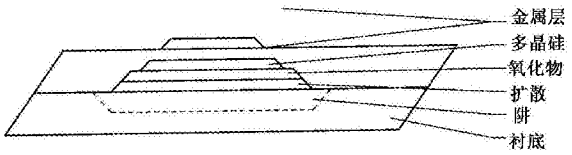
权利要求书2页 说明书30页 附图33页

(54)发明名称

用于防止逆向工程的安全半导体器件

(57)摘要

加密电路用于接收第一数字密钥和纯文本数据的输入，所述加密电路用于数学地操纵数字密钥和纯文本数据以把纯文本数据加密成加密数据，其中加密电路的至少一部分包括IBG电路。解密电路用于接收第二数字密钥和加密数据的输入，所述解密电路用于数学地操纵数字密钥和加密数据以把加密数据解密成纯文本数据，其中解密电路的至少一部分包括IBG电路。



CN 105122722 A

1. 一种数字安全系统，包括：

加密电路，其用于接收第一数字密钥和纯文本数据的输入，所述加密电路用于数学地操纵所述数字密钥和所述纯文本数据，以把所述纯文本数据加密成加密数据，

其中，所述加密电路的至少一部分包括用于 IBG 电路的装置。

2. 根据权利要求 1 所述的数字安全系统，还包括：

解密电路，其用于接收第二数字密钥和所述加密数据的输入，所述解密电路用于数学地操纵所述数字密钥和所述加密数据，以把所述加密数据解密成所述纯文本数据，

其中，所述解密电路的至少一部分包括用于 IBG 电路的装置。

3. 根据权利要求 2 所述的数字安全系统，其中，所述第一数字密钥等于所述第二数字密钥。

4. 根据权利要求 3 所述的数字安全系统，其中，所述第一数字密钥和所述第二数字密钥中的至少一个是公开密钥。

5. 根据权利要求 1 所述的数字安全系统，其中，所述加密电路适于形成数字签名。

6. 根据权利要求 1 所述的数字安全系统，其中，所述加密电路包括私有算法。

7. 根据权利要求 2 所述的数字安全系统，其中，所述解密电路包括私有算法。

8. 根据权利要求 2 所述的数字安全系统，其中，所述第一数字密钥不等于所述第二数字密钥。

9. 根据权利要求 8 所述的数字安全系统，其中，所述第一数字密钥和所述第二数字密钥中的至少一个是公开密钥。

10. 根据权利要求 9 所述的数字安全系统，其中，所述加密电路包括私有算法。

11. 根据权利要求 2 所述的数字安全系统，其中，所述加密电路和所述解密电路中的至少一个被置于成像盒芯片中。

12. 根据权利要求 2 所述的数字安全系统，其中，所述加密电路和所述解密电路中的至少一个被置于成像装置中。

13. 一种数字安全系统，包括：

解密电路，其用于接收数字密钥和加密数据的输入，所述解密电路用于数学地操纵所述数字密钥和所述加密数据，以把所述纯文本数据解密成所述纯文本数据，

其中，所述解密电路的至少一部分包括用于 IBG 电路的装置。

14. 根据权利要求 13 所述的数字安全系统，其中，所述解密电路被置于成像盒芯片中。

15. 根据权利要求 13 所述的数字安全系统，其中，所述解密电路被置于成像装置中。

16. 根据权利要求 13 所述的数字安全系统，其中，所述解密电路包括私有算法。

17. 一种形成数字安全电路的方法，所述方法包括：

设计加密算法；

形成集成电路，该集成电路包括用于执行所述加密算法的器件，

其中，所述器件的至少一部分包括用于 IBG 电路的装置。

18. 权利要求 17 所述的方法，其中，所述加密算法是私有算法。

19. 一种形成数字安全电路的方法，所述方法包括：

设计解密算法；

形成集成电路，该集成电路包括用于执行所述解密算法的器件，

其中，所述器件的至少一部分包括用于 IBG 电路的装置。

20. 根据权利要求 19 所述的方法，其中，所述加密算法是私有算法。

用于防止逆向工程的安全半导体器件

[0001] 本申请要求2013年3月15日提交的美国专利申请US13/838,853的优先权，该美国专利申请是2013年1月11日提交的美国专利申请US 13/739,429的部分连续案，是2011年7月29日提交的美国专利申请序列号US 13/194,452的分案，要求2011年6月7日提交的美国临时专利申请序列号US 61/494,172的权益，这些专利申请的全部内容以引用方式并入本文中。

技术领域

[0002] 设计一种难以进行逆向工程从而保护电路设计的电子芯片。已知的逆向工程技术包括用于拆解芯片各层以暴露逻辑器件的方法。

背景技术

[0003] 半导体拆解技术通常涉及把器件层成像、去除器件层、将下一层成像、去除该下一层等等，直到实现半导体器件的完整表现。通常，使用光学或电子显微镜实现层成像。可通过使用诸如研磨或抛光的物理手段，通过蚀刻特定化合物的化学手段，通过使用激光器或聚焦离子束技术(FIB)，或者通过任何能够去除各层的其它已知方法，进行层去除。图1示出通过拆解逆向工程技术成像的半导体层和区域中的一些。

[0004] 一旦半导体器件拆解完成并且收集到成像信息，就可使用扩散、多晶硅、限定用于形成逻辑门的MOS器件的阱区、限定逻辑门如何互连的金属层，重新构造半导体器件的逻辑功能。图2示出半导体层如何限定MOS器件。

[0005] 美国专利US 7,711,964公开了一种保护逻辑配置数据的方法。逻辑器件的配置数据被加密并且使用硅密钥加密解密密钥。被加密的解密密钥和配置被传递到逻辑器件。硅密钥用于解密随后用于解密配置数据的解密密钥。这种方法带来的一个问题是，芯片没有受到保护而免于遭受如上所述的物理逆向工程。

[0006] 许多其它密码学技术是已知的。但是，所有密码学技术易受到传统拆解技术的攻击。

[0007] 公开了一种用于设计对抗这些技术的半导体器件的方法。该半导体器件包括没有明确表征器件功能的物理几何形状。例如，设计其中两种或更多种类型的逻辑器件具有相同物理几何形状的半导体器件。当执行拆解方法时，两个或更多个器件将表现出相同的物理几何形状，但是这两个或更多个器件具有不同的逻辑功能。这样防止有人执行逆向工程用观察器件几何形状的已知方法确定逻辑功能。

[0008] 采用所公开的方法和器件将迫使逆向工程采用更困难的技术。这些技术更耗时，成本更高，更有可能有误差。

发明内容

[0009] 本发明的方法和器件表现出难以使用已知技术进行逆向工程的半导体器件。

[0010] 在本发明的一个方面，一种安全装置包括：加密电路，其用于接收第一数字密钥和

纯文本数据的输入，所述加密电路用于数学地操纵所述数字密钥和所述纯文本数据，以将所述纯文本数据加密成加密数据，其中，所述加密电路的至少一部分包括 IBG 电路。在本发明的另一个方面，一种安全装置包括：解密电路，其用于接收第二数字密钥和加密数据的输入，所述解密电路用于数学地操纵所述数字密钥和所述加密数据，以将所述加密数据解密成所述纯文本数据，其中，所述解密电路的至少一部分包括 IBG 电路。

[0011] 根据应依照附图阅读的以下实施例的详细描述，将更充分地理解本发明的这些和其它特征和目的。

[0012] 在这点上，在详细说明本发明的至少一个实施例之前，应理解，本发明的应用不限于说明书中阐述或附图中示出的构造的细节和组件的布置。本发明能够具有其它实施例并且以各种方式实践和执行。另外，应理解，本文中采用的措辞和术语以及摘要是出于描述的目的，不应该被视为限制。

[0013] 如此，本领域的技术人员将理解，作为本公开基础的构思可容易地用作设计用于执行本发明的许多目的的其它结构、方法和系统的基础。因此，重要的是，权利要求可视为包括这种等同构造，只要它们不脱离本发明的精神和范围。

附图说明

[0014] 附图并入且形成本说明书的部分，示出本发明的实施例，与描述一起用于说明本发明的原理，其中

[0015] 图 1 示出通过拆解逆向工程技术成像的半导体层和区域；

[0016] 图 2 示出半导体层如何限定 MOS 器件；

[0017] 图 3 示出对抗传统逆向工程技术的电路；

[0018] 图 4 示出使用比较器的电路构造；

[0019] 图 5 示出使用比较器的第二构造；

[0020] 图 6 示出没有比较器的电路构造；

[0021] 图 7 示出没有比较器的第二电路构造；

[0022] 图 8 示出具有六个有源器件的电路构造；

[0023] 图 9A 示出使用公开技术的多路复用器；

[0024] 图 9B 示出使用本公开技术的多路复用器的第二实施例；

[0025] 图 10 示出“NAND”逻辑功能的实现方式；

[0026] 图 11 示出“NOR”逻辑功能的实现方式；

[0027] 图 12 示出“INVERT”逻辑功能的实现方式；

[0028] 图 13 示出“BUFFER”逻辑功能的实现方式；

[0029] 图 14 示出“XOR”逻辑功能的实现方式；

[0030] 图 15 示出“XNOR”逻辑功能的实现方式；

[0031] 图 16A 示出具有有源组件的 IBG 器件；

[0032] 图 16B 示出具有有源组件的 IBG 器件的替代实施例；

[0033] 图 17 示出包括电阻器的电路；

[0034] 图 18 示出具有有源器件的硅晶圆的侧视图；

[0035] 图 19 示出按照本发明一个方面的两晶体管 (2T) IBG ROM 电路；

[0036] 图 20 示出按照本发明的 2T IBG ROM 的 2×2 阵列；

[0037] 图 21 示出按照本发明的 2T 体系结构 ROM 系统的功能框图；

[0038] 图 22 示出按照本发明的 2T IBG ROM 电路的替代实施例；

[0039] 图 23 示出按照本发明的一方面的三晶体管 (3T) IBG ROM 比特对电路；

[0040] 图 24 示出按照本发明的 3T 体系结构 ROM 系统的功能框图；

[0041] 图 25 示出按照本发明的包括至少一个 IBG 器件的成像盒芯片的框图；

[0042] 图 26 示出按照本发明的包括与成像盒 (imaging cartridge) 附接的至少一个 IBG 器件的成像盒芯片的透视图；

[0043] 图 27 示出按照本发明的包括 IBG 器件的示例性 CMOS 对的侧剖视图；

[0044] 图 28 示出图 27 的示例性 CMOS 对的顶部平面图；

[0045] 图 29A 和图 29B 示出按照本发明的 IBG 构造的剖视图，示出晶体管源 / 漏区和相关的注入互连；

[0046] 图 30 和图 31 示出按照本发明的 IBG 比特内容如何可被编程以改变示例性基本逻辑块的逻辑功能的示例；

[0047] 图 32A 是表现为场效应晶体管 (FET) 的半导体器件的平面图；

[0048] 图 32B、图 32C 和图 32D 是图 32A 的半导体器件的剖视图；

[0049] 图 33A 和图 33B 示出现有技术的器件；

[0050] 图 34 描绘按照本发明的 IBG 器件的硅化物层的伪造边缘；

[0051] 图 35 示出按照本发明的 IBG 电路；

[0052] 图 36 至图 38 示出按照本发明的 IBG 加密和解密系统的框图；

[0053] 图 39 示出按照本发明的 IBG 受保护安全视频传输系统；

[0054] 图 40 示出按照本发明的 IBG 受保护智能卡系统；

[0055] 图 41 示出按照本发明的 IBG 受保护 RFID 系统；

[0056] 图 42 示出按照本发明的形成 IBG 受保护安全系统的方法；

[0057] 图 43 示出发送被加密数据并且解密数据。

具体实施方式

[0058] 包含逻辑功能的许多半导体工艺提供了用于不同环境的不同类型的金属氧化物半导体 (MOS) 器件。例如，一个器件可只在较低电压下操作并且可被调整尺寸使得具有最小几何形状。另一个器件可在较高电压下操作并且无法被调整尺寸以具有最小几何形状。使用这种类型的器件允许半导体器件连接到外部信号，相比于内部最小尺寸的器件，这些外部信号的电压较高。

[0059] 前述例子中的那种类型的 MOS 器件通常受扩散材料的电特性控制。通过利用离子注入剂量和能量略微更改此材料的原子结构，改变这些特性。这个过程一般被描述为“掺杂”。无法通过传统的逆向工程拆解技术检测电特性的这种略微变化。

[0060] 为了提供对抗这些逆向工程技术的器件，开发出隐形偏置发生器 (IBG)。IBG 可被定义为具有至少两个内部器件的电子器件，其中，无法使用内部器件的物理几何形状确定 IBG 的操作特性。

[0061] IBG 的一个示例是内部器件二者具有相同几何形状但以不同方式操作的器件。例

如，第一器件可以是在第一电压电平下操作的晶体管并且第二器件是在不同电压电平下操作的晶体管。在另一个示例中，第一器件是硅化物电阻器而第二器件是非硅化物电阻器。在另一个示例中，导电墨水用于形成电子电路并且对于这些元件中的两个，墨水中导电材料的量是变化的。

[0062] IBG 的另一个示例是其中两个内部器件具有不同几何形状而具有相同操作特性的器件。例如，第一器件可以是以第一特性操作的晶体管，并且第二器件较大，是以相同特性操作的晶体管。在另一个示例中，第一器件是硅化物电阻器而第二器件是非硅化物电阻器。在另一个示例中，导电墨水用于形成电子电路并且对于这些元件中的两个，墨水中导电材料的量是变化的。

[0063] IBG 电路的另一个示例包括具有多种可能的几何形状和多种可能的操作特性的器件，在给定几何形状和操作特性之间不存在明显的相关性。

[0064] 图 3 示出有效制止半导体器件拆解技术的示例性 IBG 电路 300。电路 300 包括第一 IBG 器件，第一 IBG 器件包括串联连接在电源 (VCC) 和地之间的 P 沟道器件 301 和 N 沟道器件 303。第二 IBG 器件包括也串联连接在 VCC 和地之间的 P 沟道器件 302 和 N 沟道器件 304。在本发明的一个方面，器件 301 至 304 可包括 MOS 晶体管。在优选实施例中，器件 301 至 304 也可表现出相同的器件几何形状。P 沟道器件 301、302 上的栅是悬浮的，因为它们没有被提供输入信号（悬浮栅）并且被借助漏泄电流充电至大致 VCC 减去器件 301 和 302 的阈值电压得到的电压电平，各阈值电压是不相关的。N 沟道器件 303、304 上的栅也是悬浮栅并且被借助漏泄电流充电至大致地加上器件 303 和 304 的阈值电压得到的电压电平。

[0065] 各器件 301 至 304 可包括器件的源和漏之间的导通沟道。通过器件 301 至 304 的栅的扩散（也被称为注入）区的掺杂水平，确定导通沟道的深度，进而确定 P 和 N 沟道器件结上的电压电平（在图 3 中被标记为 VA 和 VB）。在本发明的一个方面，器件 301 至 304 在保持相同的器件几何形状的同时，形成有对于器件 301 至 304 中的至少一些而言不同的掺杂水平（也被称为杂质水平），从而导致器件结 VA 和 VB 具有不同的电压电平。比较器 310 检测 VA 和 VB 的电压电平并且基于这些电压偏置电平的差异，输出逻辑“1”和“0”。VA 和 VB 可以是任何电压电平，因比较器 310 的逻辑判据是基于这些电压的差异。在优选实施例中，图 3 的电路包含对于 P 和 N 沟道器件 301 至 304 而言相同的几何形状，从而造成器件 301 至 304 之间有掺杂水平差异以控制器件结 VA 和 VB 的电压电平的差异。例如，如果器件 301 和 303 被掺杂以形成低压 MOS 晶体管（如 2.5V）并且如果器件 302 和 304 被不同地掺杂以形成高压 MOS 晶体管（如 3.3V），则器件结 VA 处于比器件结 VB 高的电压，比较器的输出将是逻辑“1”。又如，如果器件 301 和 304 被掺杂以形成低压 MOS 晶体管并且如果器件 302 和 303 被掺杂以形成高压 MOS 晶体管，则器件结 VA 处于比器件结 VB 低的电压，比较器的输出将是逻辑“0”。在进行逆向工程拆解技术时，该电路的逻辑功能是隐形的，因为器件结 VA 和 VB 的操作电压是受掺杂水平控制的并且不能通过传统技术确定这些掺杂水平。

[0066] 对于提供不同类型的 MOS 器件（诸如，上述的高压器件和低压器件）的半导体技术，IBG 电路的优点在于，可用当前方法容易地构造 IBG 电路。另外，按照本发明的一个方面的 IBG 电路可用于通过变化高压器件和低压器件的数量，形成多个不同的逻辑单元。

[0067] 图 4 示出按照本发明的一个方面的示例性电路 420，电路 420 包括 IBG 和产生逻辑“1”或高输出的电平移位器电路。电路 420 的 IBG 部分包括均具有悬浮栅输入的晶体管

401、402、405 和 406。P 沟道晶体管 401 与 N 沟道晶体管 405 串联连接于输出节点 401A，P 沟道晶体管 402 与 N 沟道晶体管 406 串联连接于输出节点 402A。电路的 IBG 部分的各晶体管可以是 P 型或 N 型器件。另外，各晶体管可以是高压器件或低压器件。在优选实施例中，高压器件在 3.3V 下操作，而低压器件在 2.5V 下操作。在示例性实施例中，晶体管 402 是低压 P 型器件，晶体管 401 是高压 P 型器件，晶体管 405 是低压 N 型器件，晶体管 406 是高压 N 型器件，从而导致输出节点 402A 处的电压电平高于输出节点 401A 处的电压电平。例如，晶体管 401 和 405 可在输出节点 401A 处产生大约 100mV 的电压电平并且晶体管 402 和 406 可在输出节点 402A 处产生大约 1.5V 的电压电平。这些输出电平达不到 VCC 和地，这是由于晶体管 401、402、405 和 406 没有因被漏泄电流充电的其悬浮栅上的电荷而完全导通或截止。晶体管 401、402、405 和 406 被选择成确保输出节点 401A 和 402A 的电压电平使得一个电压电平高于晶体管 407 和 408 的阈值电压而另一个电压电平低于晶体管 407 和 408 的阈值电压，如下所述。

[0068] 由于晶体管 401、402、405 和 406 的栅的电压电平，导致 IBG 电路的输出节点 401A 和 402A 的电压电平不足以与数字逻辑直接相互作用。为了与数字逻辑正确相互作用，来自输出节点 401A 和 402A 的信号被输入到包括晶体管 403、404、407 和 408 的电平移位电路。晶体管 403 和 404 可包括低压 P 型器件并且晶体管 407 和 408 可包括低压 N 型器件。与电平移位电路的 N 沟道晶体管 408 的栅和 IBG 电路的输出节点 402A 连接的 IBG 电路的输出节点 401A 连接到电平移位电路的 N 沟道晶体管 407 的栅。在示例性实施例中，N 沟道晶体管可具有大约 700mV 的阈值电压。因此，输入到晶体管 408 的栅的节点 401A 的 100mV 电压电平将使晶体管 408“截止”并且输入到晶体管 407 的栅的 1.5V 电压电平将使晶体管 407“导通”。因此，晶体管 403 将“截止”并且晶体管 404 将“导通”，从而导致电平移位电路的输出是逻辑“1”或高 (HI)。

[0069] 图 4 还示出按照本发明的一个方面的示例性电路 430，示例性电路 430 包括 IBG 和产生逻辑“0”或低输出的电平移位电路。电路 420 的 IBG 部分包括均具有悬浮栅输入的晶体管 409、410、413 和 414。P 沟道晶体管 409 与 N 沟道晶体管 413 串联连接于输出节点 409A，P 沟道晶体管 410 与 N 沟道晶体管 414 串联连接于输出节点 410A。电路的 IBG 部分的各晶体管可以是 P 型或 N 型器件。另外，各晶体管可以是高压器件或低压器件。在优选实施例中，高压器件在 3.3V 下操作，而低压器件在 2.5V 下操作。在示例性实施例中，晶体管 409 是低压 P 型器件，晶体管 410 是高压 P 型器件，晶体管 413 是高压 N 型器件，晶体管 414 是低压 N 型器件，从而导致输出节点 409A 处的电压电平高于输出节点 410A 处的电压电平。例如，晶体管 410 和 414 可在输出节点 410A 处产生大约 100mV 的电压电平并且晶体管 409 和 413 可在输出节点 409A 处产生大约 1.5V 的电压电平。晶体管 409、410、413 和 414 被选择成确保输出节点 409A 和 410A 的电压电平使得一个电压电平高于晶体管 415 和 416 的阈值电压而另一个电压电平低于晶体管 415 和 416 的阈值电压，如下所述。

[0070] 由于晶体管 409、410、413 和 414 的栅的电压电平，导致 IBG 电路的输出节点 409A 和 410A 的电压电平不足以与数字逻辑直接相互作用。为了与数字逻辑正确相互作用，来自输出节点 409A 和 410A 的信号被输入到包括晶体管 411、412、415 和 416 的电平移位电路。晶体管 411 和 412 可包括低压 P 型器件并且晶体管 415 和 416 可包括低压 N 型器件。与电平移位电路的 N 沟道晶体管 416 的栅和 IBG 电路的输出节点 410A 连接的 IBG 电路的输

出节点 409A 连接到电平移位电路的 N 沟道晶体管 415 的栅。在示例性实施例中，N 沟道晶体管可具有大约 700mV 的阈值电压。因此，输入到晶体管 416 的栅的节点 409A 的 1.5V 电压电平将使晶体管 416 “导通”并且输入到晶体管 415 的栅的 100mV 电压电平将使晶体管 415 “导通”。因此，晶体管 412 将“截止”并且晶体管 411 将“导通”，从而导致电平移位电路的输出是逻辑“0”或低 (LO)。

[0071] 如上所述，电路 420 提供“高 (HI)”电压输出而电路 430 提供“低 (LO)”电压输出。电路 420 的 IBG 晶体管 401、402、405 和 406 的几何形状和大小可与电路 430 的 IBG 晶体管 409、410、413 和 414 的几何形状和大小相同。两个器件之间唯一可分辨的差异是高压晶体管和低压晶体管的掺杂水平。因为电路 420 的 IBG 晶体管的大小和几何形状可与电路 430 的 IBG 晶体管相同，所以不可使用传统逆向工程拆解技术确定这两个器件之间的差异。

[0072] 图 5 示出输出“高 (HI)”或“低 (LO)”输出的 IBG 电路和电平移位电路的第二示例。类似于图 4 中示出的实施例，存在 16 个晶体管器件 (501 至 516)。晶体管中的每个可以是 P 型或 N 型器件。另外，各器件可以是高压器件或低压器件。在优选实施例中，高压器件在 3.3V 下操作，而低压器件在 2.5V 下操作。在示例性实施例中，晶体管 502、503、504、509、511 和 512 是低压 P 型器件。晶体管 501 和 510 是高压 P 型器件。晶体管 505、507、508、514、515 和 516 是低压 N 型器件。晶体管 506 和 513 是高压 N 型器件。器件 520 提供“高 (HI)”电压输出，而器件 530 提供“低 (LO)”电压输出。器件 520 的 IBG 晶体管 501、502、505 和 506 的几何形状和大小可与器件 530 的 IBG 晶体管 509、510、513 和 514 的几何形状和大小相同。这两个器件之间唯一可分辨的差异是高压晶体管和低压晶体管的掺杂水平。因为器件 520 的 IBG 晶体管的大小和几何形状与器件 530 的 IBG 晶体管的大小和几何形状相同，所以不可能使用传统逆向工程拆解技术确定这两个器件之间的差异。

[0073] 如果半导体芯片包含如图 4 或图 5 中描述的 IBG，则有人尝试使用拆解技术进行逆向工程来确定布置在芯片上的 IBG 器件的功能是极其困难的，因为内部器件的几何形状是相同的。

[0074] 图 6 和图 7 示出电路的输出的电压电平足以直接与芯片上的器件相互作用的 IBG 的示例。在图 6 中，器件 601 是高压 P 型器件 (诸如，3.3V)，器件 602 是低压 P 型器件 (诸如，2.5V)，器件 603 是低压 N 型器件并且 604 是高压 N 型器件。通过将器件 601 的栅连接到器件 602 的栅，这些器件共用漏泄电流，从而导致高压器件 601 完全截止并且低电压器件 602 完全导通。类似地，通过将器件 603 的栅连接到器件 604 的栅，这些器件共用漏泄电流，从而导致低压器件 603 完全导通并且器件 604 完全截止。输出节点 601A 将足以接近地以用作逻辑“0”并且与其它 CMOS 器件直接连接并且输出节点 602A 将足以接近 VCC 以用作逻辑“1”并且与其它 CMOS 器件直接连接。

[0075] 在图 7 中，器件 701 是诸如 2.5V 的低压 P 型器件，器件 702 是诸如 2.5V 的高压 P 型器件，器件 704 是低压 N 型器件并且 703 是高压 N 型器件。通过将器件 701 的栅连接到器件 702 的栅，这些器件共用漏泄电流，从而导致低压器件 701 完全导通并且高压器件 702 完全截止。类似地，通过将器件 703 的栅连接到器件 704 的栅，这些器件共用漏泄电流，从而导致高压器件 703 完全截止并且低压器件 704 完全导通。输出节点 701A 将足以接近 VCC 以用作逻辑“1”并且与其它 CMOS 器件直接连接并且输出节点 702A 将足以接近地以用作逻辑“0”并且与其它 CMOS 器件直接连接。

[0076] IBG 晶体管 601、602、603 和 604 的几何形状和大小可与 IBG 晶体管 701、702、703 和 704 的几何形状和大小相同。IBG 晶体管 601、602、603 和 604 的几何形状和大小可彼此不同。IBG 晶体管 701、702、703 和 704 的几何形状和大小可彼此不同。另外，栅相连晶体管的栅处的电压电平相等。两个器件之间唯一可分辨的差异是高压晶体管和低压晶体管的掺杂水平。因为图 6 的 IBG 晶体管的大小和几何形状可与图 7 的器件的 IBG 晶体管相同，所以不可能使用传统逆向工程拆解技术确定这两个器件之间的差异。图 6 中示出的 IBG 具有与图 7 中示出的 IBG 相同的几何形状，唯一的差异是晶体管中的一些的掺杂水平。因此，如果使用图 6 中示出的 IBG 和图 7 中示出的 IBG 设计芯片，则确定因各设计造成的器件功能差异是非常困难的。

[0077] 图 6 中示出的 IBG 可包括不同的构造。在一个示例中，器件 601 是低压 P 型器件，器件 602 是高压 P 型器件，器件 603 是低压 N 型器件并且 604 是高压 N 型器件。在另一个示例中，器件 601 是高压 P 型器件，器件 602 是低压 P 型器件，器件 603 是高压 N 型器件并且 604 是高压 N 型器件。在另一个示例中，器件 601 是高压 P 型器件，器件 602 是低压 P 型器件，器件 603 是低压 N 型器件并且 604 是低压 N 型器件。在另一个示例中，器件 601 是高压 P 型器件，器件 602 是低压 P 型器件，器件 603 是低压 N 型器件并且 604 是高压 N 型器件。四个器件 IBG 可能存在总共十六个构造。

[0078] 图 8 示出 IBG 电路的另一个实施例。器件 801、802、803 被示出为 P 型器件并且可以是高压器件或低压器件的任何组合。器件 804、805、806 被示为 N 型器件并且可以是高压器件或低压器件的任何组合。然而，示出的六个器件可以是 P 型器件和 N 型器件的任何组合。六个器件 IBG 具有总共 64 个可能的构造。此外，IBG 可包括任何数量的有源器件，具有 2 的“n”次方种组合，其中，n 是有源器件的数量。

[0079] 图 9A 和图 9B 示出包括多路复用器的 IBG 电路。因为 IBG 电路可用于选择逻辑功能，所以与将两个输入中的一个有效引导到其输出的数字多路复用器相结合地实现这些电路是方便的。这些基于 IBG 的多路复用器仅仅基于 IBG 功能选择输入。在图 9A 中，晶体管 901、902、905 和 906 包括 IBG 电路并且晶体管 903、904、907 和 908 包括多路复用器。在图 9B 中，晶体管 911、912、915 和 916 包括 IBG 电路并且晶体管 917、918、913 和 914 包括多路复用器。在图 9A 中，器件 901 和 906 是 3.3V 器件，而器件 902、903、904、905、907 和 908 是 2.5V 器件。反相器 910 提供输入 A 的反相和输入 B 的反相。在图 9B 中，器件 912 和 915 是 3.3V 器件，而器件 911、913、914、916、917 和 918 是 2.5V 器件。反相器 920 提供输入 A 的反相和输入 B 的反相。基于 IBG 晶体管 901、902、905 和 906 的输出，图 9A 中示出的多路复用器选择 B 输入，而基于 IBG 晶体管 911、912、915 和 916 的输出，图 9B 中示出的多路复用器选择 A 输入。两个器件之间唯一可分辨的差异是高压晶体管和低压晶体管的掺杂水平。因为图 9A 的晶体管的大小和几何形状可与图 9B 的晶体管相同，所以不可以使用传统逆向工程拆解技术确定这两个器件之间的差异。图 9A 中示出的 IBG 可具有与图 9B 中示出的 IBG 相同的几何形状，唯一的差异是晶体管中的一些的掺杂水平。因此，如果使用图 9A 中示出的电路和图 9B 中示出的电路设计芯片，则确定因各设计造成的器件功能差异是非常困难的。这些电路之间的唯一差异是 3.3V 和 2.5V 器件的构造。

[0080] 图 10 代表“NAND”逻辑功能的实现方式，图 11 示出“NOR”逻辑功能的实现方式。在图 10 中，NAND 门 1010 和 NOR 门 1011 的输出通向基于 IBG 的多路复用器 1012（诸如，图

9A 中示出的 IBG 电路多路复用器），以选择 NAND 门 1010 的输出。在图 11 中，NAND 门 1110 和 NOR 门 111 的输出通向基于 IBG 的多路复用器 1112（诸如，图 9B 中示出的 IBG 电路多路复用器），以选择 NOR 门 1111 的输出。在进行逆向工程期间，这两种实现方式看上去是一样的，因为这些构造之间的差异是 IBG 电路。在没有得知 IBG 电路的情况下，这些构造的逻辑功能是不明确的。

[0081] 图 12 示出包括反相器 1201 和被实现为选择反相输入的基于 IBG 的多路复用器 1202（诸如，图 9A 中示出的 IBG 电路多路复用器）的逻辑功能“INVERT”的实现方式。图 13 示出包括反相器 1301 和被实现为选择非反相输入的基于 IBG 的多路复用器 1302（诸如，图 9B 中示出的 IBG 电路多路复用器）的逻辑功能“BUFFER”的实现方式。图 14 示出包括异或门 1401、反相器 1403 和被实现为选择门 1401 的输出的基于 IBG 的多路复用器 1402（诸如，图 9A 中示出的 IBG 电路多路复用器）的逻辑功能“XOR”的实现方式。图 15 示出包括同门 (exclusive nor gate)1501、反相器 1503 和被实现为选择反相器 1503 的输出的基于 IBG 的多路复用器 1502（诸如，图 9B 中示出的 IBG 电路多路复用器）的逻辑功能“XNOR”的实现方式。如同之前的示例，对具有图 12 的“INVERT”和图 13 的“BUFFER”二者的芯片进行逆向工程将难以执行，因为“INVERT”和“BUFFER”将具有相同的外观。对具有图 14 的“XOR”和图 15 的“XNOR”二者的芯片进行逆向工程是困难的，因为“XOR”和“XNOR”具有相同的外观。如上所述，在没有得知基于 IBG 电路的多路复用器的逻辑操作情况下，每对实现方式都是不明确的。

[0082] 抗逆向工程遏制的高电压 / 低电压方法的一个优点是，大部分过程支持这个区分。许多实现方式被设计成使用低电压内部电压，因为随着特征的大小减小，内部电压减小。但是，芯片外部的许多器件以较高电压操作并且芯片必须能够与这些器件连接。因此，使用较高电压的器件仍然在被使用并且正在开发中。可以使用 P 器件和 N 器件之间的小掺杂变化来实现低电压装置和高电压装置之间的差异。

[0083] 上述 IBG 器件包括使用掺杂水平来控制器件特性的有源器件。举例来说，已知在特定工艺中，2.5V 和 3.3V 器件之前的掺杂浓度差异是大约 8×E16 原子 /cm^3。掺杂密度差异低于 1×E17 的结构是 IBG 设计的候选结构。在图 16 中的是 IBG 的示例。

[0084] 除了 2.5V 器件和 3.3V 器件，器件的许多其它组合也是可以的。例如，2.5V 可与 5V 器件一起使用。1.8V 器件、1.5V 器件或 1.2V 可与 3.3V 器件一起使用。1.2V 器件可与 1.8V 或 2.5V 器件一起使用。1.0V 器件可与 1.8V 器件、2.5V 器件或 3.3V 器件一起使用。0.85V 器件可与 1.8V 器件、2.5V 器件或 3.3V 器件一起使用。这个清单只是示例性的并且可使用可用相同物理几何形状制成的器件的任何组合。

[0085] 之前的示例示出使用有源器件的 IBG 期间的可能实现方式中的一些。另一种实现 IBG 器件的方式是使用无源器件。可使用硅化物多晶硅电阻器和非硅化物多晶硅电阻器制成 IBG。第一器件用于将第一偏置电压设置为有源偏置电压并且第二器件用于将第二偏置电压设置为有源偏置电压。硅化物多晶硅电阻器和非硅化物多晶硅电阻器之间的差异对于传统逆向工程技术而言将并不明显，因为电阻器具有相同的几何形状。图 16A 示出 IBG 器件的示例。图 16B 示出 IBG 器件的其它示例。

[0086] 多晶硅具有相当高的电阻，大约几百 μΩ-cm。多晶硅电阻器件承受这种高电阻，因为随着器件尺寸缩小，多晶硅本地互连的电阻增大。这个增大的电阻造成功耗增大和较

长的RC时间延迟。在多晶硅器件中添加硅化物，因为硅化物的添加使电阻减小并且使器件速度提高。可使用比多晶硅具有小得多电阻的任何硅化物。硅化钛($TiSi_2$)和硅化钨(WSi_2)是公共使用的两种硅化物。

[0087] 接下来，描述形成硅化物器件的一种方法。传统上，使用自对准硅化物工艺形成硅化钛。初始地，使用化学溶液清洁晶圆表面，以去除污染物和颗粒。接下来，使用氩气在真空腔室中溅射晶圆，以从晶圆表面去除原生氧化物。接下来，溅射晶圆表面的层，以在晶圆表面上沉积钛层。这导致晶圆具有暴露于源/漏和多晶硅栅顶部的硅。接下来，通过使用热退火工艺，在多晶硅上形成硅化钛。例如，可在快速热工艺中执行退火，以在多晶硅顶部和源/漏的表面上形成硅化钛。因为钛没有与二氧化硅反应，所以只在多晶硅直接接触钛的地方形成硅化物。接下来，通过使用湿蚀刻工艺去除未经处理的钛，以使未反应的钛接触双氧水(H_2O_2)和硫酸(H_2SO_4)的混合物。最后，将晶圆退火，以增大硅化钛的粒径。增大的粒径提高了晶圆的导电性并且减小了晶圆的接触电阻。

[0088] 可在IBG器件中控制的另一种特性是阈值电压。可通过阈值调节注入控制MOS晶体管的阈值。使用离子注入工艺确保电子系统的电源电压可将IC芯片中的MOS晶体管导通和截止。阈值调节注入是低能量且低电流注入工艺。通常，在栅氧化物生长之前，执行阈值调节注入。对于CMOS IC芯片，需要两个阈值调节注入工艺，一个针对p型，一个针对n型。

[0089] 在IBG器件中，上述工艺可用于制造具有相同物理尺寸并且具有不同电阻的电阻器。相反地，该工艺可用于制造具有不同几何形状和相同电阻的电阻器。

[0090] 图17示出用硅化物电阻器实现的IBG器件的示例。电压源VCC连接到具有电阻器1701、1702、1703、1704的电路。在所有电阻器都具有相同物理几何形状的情况下，可通过上述方法设置电阻器的电阻，使其具有两个不同的电阻大小。例如，电阻器1701和1704可以是非硅化物电阻器，而电阻器1702和1703是硅化物电阻器。在这个示例中，如果Va小于Vb，则器件的输出是逻辑“1”。如果Va大于或等于Vb，则器件的输出是逻辑“0”。

[0091] 在另一个实施例中，可使用导电墨水形成器件。导电墨水用于在各种衬底材料上印刷电路。导电墨水包含诸如粉末状或薄片状银材料的导电材料。

[0092] 导电墨水可用于实现IBG电路，因为用于印刷电路的导电墨水的性质可有所变化，以形成具有不同性质的器件。例如，可使用具有一定量导电材料的导电墨水，印刷一些器件。那么，具有更多（或更少）导电材料的导电墨水用于印刷电路的另一部分。那么，电路可具有看上去近似并且以不同方式操作或者看上去不同并且一样操作的器件。

[0093] 对IBG电路进行逆向工程的一种可能方法是物理地测量电路中的器件。可使用探针进行这个操作以测量电路产生的实际电压。为了挫败这种逆向工程方法，IBG单元被随机放置，在整个设计中间隔开。这样使得更难以探测对该设计进行逆向工程所需的大量IBG电路。

[0094] 在替代实施例中，所使用的那些类型的IBG电路是随机分布的。例如，使用IBG电路实现每个第三“AND”门，而使用IBG电路实现每个第四“NAND”门。随着IBG电路实现的器件的数量增加，对芯片进行逆向工程的难度增大。另外，随着IBG电路实现的逻辑器件的类型的数量增加，对芯片进行逆向工程的难度增大。

[0095] 在另一个实施例中，可制成其中具有逻辑器件的逻辑块。在各逻辑块内，IBG被随

机分布在逻辑块内。结果，各逻辑块内的不同类型的逻辑器件包括 IBG 器件。

[0096] 在另一个实施例中，制成具有逻辑器件的逻辑块。设计者确定逻辑块的临界点并且使用 IBG 实现临界点。临界点是逻辑块内的必须得知功能或输出值以确定逻辑块功能的点。用 IBG 实现逻辑块内的临界点是有利的，因为这确保了 IBG 在防止逆向工程方面的效果最强。不能确定临界点的值一定会阻碍逆向工程人员确定逻辑块的正确功能。

[0097] 例如，如果逻辑块是加法器 (ADDER)，则取代输出中的数字可使得不可以确定加法器的功能。这是因为，尝试对芯片进行逆向工程从而监测逻辑块功能的人员将预料加法器的特定输出。当被取代的数字没有提供预期结果时，确定逻辑块没有正用作加法器。

[0098] 所公开系统和方法的另一个优点是可使用标准工具和技术设计该芯片。在下面的段落中描述设计芯片的方法。

[0099] 设计者创造芯片和芯片内的逻辑块的整体设计。以诸如 Verilog 或 VHDL 的已知硬件设计语言创造设计。接着，设计被合成为标准逻辑，以将设计转换成优化的门级。可使用诸如 Talus Design、Encounter RTL Designer 和 Design Complier 的标准合成工具执行合成。该合成使用供应商提供的标准单元库 (standard cell library) 将逻辑块映射到标准逻辑。接下来，使用布局布线工具形成设计的物理实现方式。这个步骤涉及形成平面布置图、电网、布置标准单元、实现时钟树并且铺设单元和输入 / 输出引脚之间的连接。布局布线工具的一些示例是 Talus Vortex、Encounter Digital Implementation 和 IC Compiler。使用这个过程，存在使用 IBG 器件设计芯片的各种方式。一种方式是创建和表征一个或多个新标准单元库并且在该过程开始时使用一个或多个新标准单元。另一种方法是在布局布线步骤中布置 IBG 器件，无论是自动还是手动的。

[0100] 设计芯片的另一种方法是设计者使用示意性输入工具创造设计。设计者用手创建包括基础逻辑门的电路。设计者可使用卡诺图 (Karnaugh-map) 优化逻辑功能。使用布局输入工具形成设计的物理实现方式。设计者绘出多边形来代表用硅实现的实际层。使用这种方法，设计者将 IBG 器件放置在任何所需位置。

[0101] 因为上述器件导致难以使用传统拆解技术进行逆向工程的设计，所以可实现另一种方法对芯片进行逆向工程。逆向工程的另一种已知方法是探测启用时的器件，以建立内部器件的操作值。为了执行这些方法，逆向工程必须去除晶圆的一些层以暴露器件的输出接触件。使这种技术更难以进行的一种方式是如上所述随机布置逻辑器件。另一种技术是设计物理上对抗这些技术的芯片。

[0102] 图 18 示出对抗芯片电子测试的硅晶圆的各层。晶圆具有包括扩散层的基体层 1801。氧化物层 1802 在扩散层 1801 的顶部上。多晶硅层 1803 位于氧化物层的顶部上，使金属层 1 1804 位于其上。在金属层 1 1804 中形成信号输出。金属层 2 1805 位于金属层 1 1804 的顶部上。在金属层 2 1805 中形成栅连接件。用这个布局，必须去除金属层 2 1805 的一部分，以探测位于金属层 1 1804 中的信号输出。去除金属层 2 1805 的一部分破坏了器件的栅连接件，进而禁用器件。因此，尝试探测器件的逆向工程人员将在进行逆向工程过程期间破坏器件的功能。

[0103] 在上述技术中的一些中，使用器件的输出电压电平确定器件的操作。但是，可使用器件的任何其它操作特性。例如，可在 IBG 中使用器件的上升时间、消耗的电流或操作温度。另外，器件的不止一种物理特性可发生变化。例如，可控制几何形状和掺杂水平以实现

IBG。

[0104] 公开的系统和方法的另一个优点是，它可用任何类型的电子器件实现。例如，可用上述技术实现只读存储器 (ROM) 并且通过 IBG 电路的物理实现方式保护存储器的内容。这使得在不需要复杂加密技术的情况下，启用受保护的存储器器件。

[0105] IBG ROM 电路可以是对硬件反向工程技术极具抵抗力的掩模型存储器技术。IBG ROM 电路可以是基于比特对的 N 和 P 沟道器件，这些沟道器件的掺杂密度差异太小，以致不能通过光学区分技术确定。IBG ROM 使用光学逆向工程工艺增加读取存储器的复杂度和成本，从而产生存储在 IBG ROM 中的数据的安全环境。

[0106] 图 19 示出按照本发明一个方面的两晶体管 (2T) IBG ROM 电路 1900。2T IBG ROM 电路 1900 包括第一 N 沟道晶体管 1902，第一 N 沟道晶体管 1902 具有与第一 N 沟道晶体管 1902 的源端连接的输出节点 1904。第一 N 沟道晶体管 1902 被选择成使器件几何形状和包括掺杂特性的器件特性适于在第一 N 沟道晶体管 1902 连接到 P 沟道器件时将输出节点 1904 偏置成指示二进制 1 的预定电压电平或指示二进制 0 的预定电压电平，以下更详细进行描述。二进制 1 和二进制 0 之间的掺杂特性差异太小，以致通过光学技术检测不到。第一 N 沟道晶体管 1902 的栅端是悬浮栅，因此没有连接到输入信号。第一 N 沟道晶体管 1902 的漏端连接到地。2T IBG ROM 电路 1900 还包括连接在输出节点 1904 和数据总线 1908 之间的第二 N 沟道晶体管 1906。字线 1910 连接到第二 N 沟道晶体管 1906 的栅。第二 N 沟道晶体管 1906 像通道晶体管一样操作并且通过字线 1910 被导通。当通道晶体管 1906 通过字线 1910 被导通时，通道晶体管将输出节点 1904 的预定电压电平传递到数据总线 1908。

[0107] 公共 P 沟道电路 1910 也连接到数据总线并且提供漏泄电流以当通道晶体管 1906 导通时为第一 N 沟道晶体管 1902 中的悬浮栅充电。公共 P 沟道电路 1910 包括串联连接的 P 沟道晶体管 1912 和虚设 P 和 N 晶体管对 1914。P 沟道晶体管 1912 和虚设 P 晶体管的栅相连，从而当通道晶体管 1906 导通时，形成第一 N 沟道晶体管 1902 正常操作所需的漏泄分布。预定电压电平在通过晶体管 1906 导通时将只存在于输出节点 1904，从而将公共 P 沟道电路 1910 连接到晶体管 1902，以提供用于操作 N 沟道晶体管 1902 的漏泄电流。

[0108] 图 20 示出按照本发明的 2T IBG ROM 2000 的 2×2 阵列。2×2IBG ROM 包括四个 N 沟道晶体管 2002、2004、2006 和 2008 及其相关的通道晶体管 2012、2014、2016 和 2018。这四个 N 沟道晶体管 2002、2004、2006 和 2008 具有输出节点 2003、2005、2007 和 2009。N 沟道晶体管 2002、2004、2006 和 2008 被选择成使器件几何形状和包括掺杂特性的器件特性适于在 N 沟道晶体管 2002、2004、2006 和 2008 连接到 P 沟道器件时将输出节点 2003、2005、2007 和 2009 偏置成指示二进制 1 的预定电压电平或指示二进制 0 的预定电压电平，以下更详细进行描述。二进制 1 和二进制 0 之间的掺杂特性差异太小，以致通过光学技术检测不到。晶体管 2002 和 2004 均是第一字的部分，它们的通道晶体管 2012 和 2014 通过被第一字线 2020 导通。晶体管 2006 和 2008 均是第二字的部分，它们的通道晶体管 2016 和 2018 通过第二字线 2022 被导通。通道晶体管 2012 和 2016 的输出连接到第一数据总线 2030 并且通道晶体管 2014 和 2018 的输出连接到第二数据总线 2032。

[0109] 当字线 2020 被断言时，通道晶体管 2012 和 2014 导通并且通道晶体管 2012 和 2014 将输出节点 2003 和 2005 的预定电压电平传递到数据总线 2030 和 2032。当字线 2022 被断言时，通道晶体管 2016 和 2018 导通并且通道晶体管 2016 和 2018 将输出节点 2007 和 2008

的预定电压电平传递到数据总线 2030 和 2032。

[0110] 第一公共 P 沟道电路 2040 连接到第一数据总线 2030 并且像晶体管 2002 和 2006 的公共 P 沟道一样操作，第二公共 P 沟道电路 2042 连接到第二数据总线 2032 并且像晶体管 2014 和 2018 的公共 P 沟道一样操作。预定电压电平在通道晶体管 2012 和 2014 导通时将只存在于输出节点 2003 和 2005，从而将公共 P 沟道电路 2040 连接到晶体管 2002 和 2004，以提供用于操作 N 沟道晶体管 2002 和 2004 的漏泄电流。类似地，预定电压电平在通道晶体管 2016 和 2018 导通时将只存在于输出节点 2007 和 2009，从而将公共 P 沟道电路 2042 连接到晶体管 2006 和 2008，以提供用于操作 N 沟道晶体管 2006 和 2008 的漏泄电流。

[0111] 图 21 示出按照本发明的 2T 构造 ROM 系统的功能框图 2100。地址解码单元 2102 接收从外部系统读取的地址并且解码该地址，以选择与将从 IBG N 沟道器件阵列 2104 读取的数据的字对应的字线。公共 P 沟道器件 2106 连接到各数据线输出 2104。读放大器 2108 放大输出的数据的字，以将数据的字从阵列 2104 输出的电压电平转换成与数字逻辑电路中的逻辑“1”和逻辑“0”对应的电平。读放大器在数据总线 2110 上发送放大的数据。

[0112] 图 22 示出按照本发明的 2T IBG ROM 电路 2200 的替代实施例。相比于图 20 中示出的 2T IBG ROM 电路 2000，N 沟道 IBG 晶体管 2002 和 2004 的栅和 N 沟道 IBG 晶体管 2006 和 2008 的栅以比特对方式连接。相比于 2T IBG ROM 电路 2000，连接这些 N 沟道栅使晶体管 2002、2004、2006 和 2008 的栅电容和漏泄电流增大。这允许具有较小几何形状的较小几何 IBG 单元正确操作且更快安定。

[0113] 图 23 示出按照本发明的一个方面的三晶体管 (3T) IBG ROM 比特对电路 2300。3T IBG ROM 比特对电路 2300 包括第一晶体管对，第一晶体管对具有通过输出节点 2306 与 N 沟道晶体管 2304 串联连接的 P 沟道晶体管 2302。第二晶体管对具有通过输出节点 2312 与 N 沟道晶体管 2310 串联连接的 P 沟道晶体管 2308。晶体管 2302 的栅连接到晶体管 2308 的栅，从而允许这些器件共用漏泄电流。类似地，晶体管 2304 的栅连接到晶体管 2310 的栅，从而允许这些器件也共用漏泄电流。晶体管 2302 和 2304 被选择成使器件几何形状和包括掺杂特性的器件特性适于将输出节点 2306 偏置成指示二进制 1 的预定电压电平或指示二进制 0 的预定电压电平。二进制 1 和二进制 0 之间的掺杂特性差异太小，以致通过光学技术检测不到。

[0114] N 沟道晶体管 2314 连接在输出节点 2306 和数据总线 2316 之间。N 沟道晶体管 2318 连接在输出节点 2312 和数据总线 2320 之间。字线 2322 连接到像通道晶体管一样操作并且通过字线 2322 被导通的 N 沟道晶体管 2314 的栅。字线 2322 还连接到像通道晶体管一样操作并且通过字线 2322 被导通的 N 沟道晶体管 2318 的栅。当字线 2322 被断言时，通道晶体管 2314 和 2318 将输出节点 2306 和 2312 的预定电压电平传递到数据总线 2316 和 2320。

[0115] 图 24 示出按照本发明的 3T 构造 ROM 系统的功能框图 2400。地址解码单元 2402 接收从外部系统读取的地址并且解码该地址，以选择与将从 IBG P 和 N 沟道器件阵列 2404 读取的数据的字对应的字线。读放大器 2408 放大输出的数据的字，以将数据的字从阵列 2104 输出的电压电平转换成与数字逻辑电路中的逻辑“1”和逻辑“0”对应的电平。读放大器在数据总线 2410 上发送放大后的数据。

[0116] 在本发明的另一个方面，将安全防护与 IBG ROM 电路阵列一起利用。IBG ROM 电

路阵列可包括以蜿蜒方式敷设在该阵列表面上方以得到包括该阵列的器件的地 (GND) 连接的顶部金属迹线或跑线 (run)。例如，安全防护可布置在图 18 的第二金属层 1805 上方。任何切割安全防护对阵列进行逆向工程的尝试将造成 IBG ROM 电路失效，从而使操作期间的任何电路测量变复杂。在被修复后，切割将表现出增大的 DC 电阻，从而限制可成功完成的修复的数量。

[0117] 在成像行业，再造和翻新诸如调色剂盒、鼓盒、喷墨盒等各种类型的可更换成像盒的市场日益增大。例如，这些成像盒用于诸如激光打印机、经典印刷复印件、喷墨打印机、传真机等成像装置。成像盒一旦被用完，就不可用于它们最开始意图的目的。在没有翻新工艺的情况下，这些盒将只是被丢弃，即使盒本身仍然还可能有寿命。结果，专门开发出解决这个问题的技术。这些工艺可需要例如拆开盒的各种结构、更换调色剂或墨水、清洁、调节或更换任何用坏的组件并且重新组装成像盒。例如，如果成像盒包括诸如有机光导体 (OPC) 鼓的鼓或辊，则该鼓或辊可被更换或翻新。

[0118] 一些调色剂盒可例如包括带有存储器装置的芯片，该存储器器件用于存储与诸如打印机的和或成像装置相关的数据。成像装置可使用直接接触方法或利用射频 (RF) 通信的广播技术与芯片通信。诸如打印机的成像装置读取存储在盒存储器装置中的数据，以确定一定打印参数并且将信息传达给用户。例如，存储器可存储成像盒的型号编号，使得打印机可识别成像盒是与该特定成像装置兼容的成像盒。另外，举例来说，盒存储器可存储在成像盒的生命周期期间可预期从成像盒打印出的多页和其它可用数据。成像装置还可将某个数据写入存储器装置，诸如，关于盒中剩余调色剂的量的指示。存储在存储器装置中的其它数据可涉及调色剂盒的使用历史。

[0119] 这种芯片通常被安装在盒上的诸如槽的位置，以允许当盒被安装在打印机中时打印机和调色剂盒之间正确进行通信。当正在再造调色剂盒时，如上所述，原始设备制造商 (OEM) 提供的芯片 (诸如，Hewlett-Packard 或 Lexmark) 可能需要被更换为第三方开发的兼容芯片。期望保护成像盒的芯片的电路设计。因此，包括难以进行逆向工程的一个或多个 IBG 器件的成像盒芯片将是极为有利的。

[0120] 图 25 示出包括本申请中更详细描述的一个或多个 IBG 器件的按照本发明的成像盒芯片 2500 的功能框图。成像盒芯片 2500 可适宜地包括输入和输出 (I/O) 接口电路 2502、控制器 2504 和存储器 2506。I/O 接口电路 2502 与控制器 2504 通信连接并且提供用于控制器 2504 的合适电子电路以与诸如打印机的成像装置通信。举例来说，对于利用射频 (RF) 进行通信的成像装置，I/O 接口电路 2502 可包括射频 (RF) 天线和电路，并且为了与成像装置直接有线连接，I/O 接口电路 2502 可包括一个或多个接触焊盘等和接口电路。

[0121] 控制器 2504 控制成像盒芯片 2500 的操作并且为存储器 2506 提供功能界面，包括通过打印机控制从存储器 2506 读取数据以及将数据写入存储器 2506。从成像盒芯片 2500 读取并且写入成像盒芯片 2500 的数据可包括打印机类型、盒序列号、有机光导体 (OPC) 鼓执行的转数 (鼓计数)、制造日期、打印的页数 (页计数)、调色剂剩余百分比、产量 (预期的页数)、颜色指示符、调色剂用完指示符、调色剂量低指示符、未使用盒指示符 (盒之前是否已经被再造)、作业计数 (打印的页数和页类型)、可存储在存储器 2506 上的任何其它数据或程序指令。

[0122] 控制器 2504 可合适地被实现为定制或半定制集成电路、可编程门阵列、来自存储

器 2506 或其它存储器的微处理器执行指令、微控制器等。另外，控制器 2504、存储器 2506 和 / 或 I/O 接口电路 2502 可被分开或组合于一个或多个物理模块。这些模块可被合适安装到印刷电路板，形成成像盒芯片 2500。可使用本文中详细描述的一个或多个 IBG 器件实现控制器 2504、存储器 2506、I/O 接口电路 2502 和任何其它电路中的一个或多个，以保护电路的操作免于遭受逆向工程。图 26 示出按照本发明的安装在成像盒 2600 上的成像盒芯片 2500 的示例性实施例的透视图。

[0123] 图 27 和图 28 示出按照本发明的 IBG 器件的替代实施例，该 IBG 器件可被适当地注入成像盒芯片中，如上述的成像盒芯片。图 27 示出典型 CMOS 对的侧剖视图。图 28 示出典型 CMOS 对的顶部平面图。在 P 衬底 2700 中，形成 N 阱 2702。借助注入，在 N 阱 2702 中形成 p+ 源 / 漏 2704 和 p+ 源 / 漏 2706。在 P 衬底 2700 中，还存在通过注入形成的 n+ 源 / 漏 2708 和 n+ 源 / 漏 2710。还存在通过注入形成的连接到 Vcc 源的 n+ 区 2712 和 2714 和通过注入形成的连接到 Vss 源的 p+ 区 2716 和 2718。

[0124] 多晶硅栅 2720 形成待形成的任何所需源和漏之间的沟道。硅化物层 2722（为了图示，以夸大的厚度比例示出并且被示出为“侵蚀了”衬底表面）形成在 n+ 区 2712 和 2714、p+ 区 2716 和 2718、p+ 源 / 漏 2704 和 2706 和 n+ 源 / 漏 2708 和 2710 上方。按照本发明，通过包括将 n+ 区 2712 和 p+ 源 / 漏 2704 互连的选定硅化物层 2740，形成 IBG 器件。与 n+ 区 2017 和 p+ 源 / 漏 2704 上方的硅化物层 2722 合并的硅化物层 2740 在硅化物 2722 形成的同时形成。一个或多个其它硅化物层可用于互连诸如在 n+ 区 2710 和 p+ 区 2718 之间的其它或所有有源区（如需要互连的电路设计组件将确定的并且设计者将优先掩饰的）。设计者可根据需要选择硅化物层 2740 的范围，使得用硅化物层互连替换标准的上层互连，以挫败潜在的逆向工程努力。硅化物层 2740 可能薄，诸如 100 埃，因此难以检测通过硅化物层 2740 进行的任何连接。在优选实施例中，硅化物层可形成在电路有源区中的至少一个有源区上方和用于通过硅化物区将有源区与其它区域互连的选定衬底区上方。另外，区域硅化物层可形成在至少第一有源层上方和用于通过硅化物将第一有源层和第二有源层互连的至少第二有源层上方。

[0125] 在本发明的另一个方面，IBG 电路提供掩饰的数字 IC，进行逆向工程非常困难的 IC 的制造方法可在没有任何另外的制造步骤的情况下实现并且与计算机辅助设计 (CAD) 系统兼容，CAD 系统允许方便构造许多不同种类的逻辑电路。为了实现这些目标，对于同一晶体管类型，使各单元内的晶体管的大小和内部几何形状相同，不同的逻辑单元将它们的晶体管布置成基本相同的空间图案，使得不能根据晶体管图案辨别出逻辑功能，这些晶体管被一齐以均一阵列布置在衬底上，使得不同逻辑单元之间的边界是类似地、不可辨别的。逆向工程师难以检测的导电的、重掺杂注入互连提供了各单元内的晶体管之间的互连，其中，互连的图案确定单元的逻辑功能。优选地，提供衬底上的所有晶体管之间的互连的均一图案，其中，通过添加相反导电类型沟道阻断注入，断开一些互连，使这些互连显现（它们看上去是导电连接，但实际是不导电的），从而实现不同的逻辑功能。沟道阻断比它们所断开的互连短得多，优选地，使尺寸大致等于 IC 的最小特征尺寸。为了达到逆向工程师可分辨互连的程度，因为将检测不到沟道阻断，所以互连将都看上去是相同的，从而增强了电路掩饰。还通过在晶体管阵列上方提供金属引线的均一图案，阻碍逆向工程。形成重掺杂注入塞的均一图案，用于使各种晶体管与引线连接。通过与显现的晶体管间互连中采用的沟道

阻断类似的沟道阻断来阻挡一些塞，使这些塞显现。因此，逆向工程师将不能够根据金属化或塞图案确定不同单元之间的边界或识别不同的单元类型。金属化优选地在多层中实现，其中，上层遮蔽下层和下伏 IC 之间的连接。优选地，通过同时注入互连和晶体管中具有相同导电类型的那些部分，并且还同时注入沟道阻断和晶体管中与沟道阻断具有相同导电类型的那些部分，制造这种掩饰电路。

[0126] 图 29A 和图 29B 示出这种 IBG 构造 2900 的剖视图，示出晶体管源 / 漏区和相关的注入互连，包括使一些互连件显现而非有功能的沟道阻断。这些器件形成在半导体 38 中，出于例证目的，半导体 38 是硅，但可以是某种其它所需的半导体材料。在衬底 38 被示出为具有 n 掺杂的情况下，形成略微更重掺杂的 p 阱 40。氧化物掩模 42 被放在衬底上方，在源和漏的所需位置带有开口。在按照本发明的可通过离子注入将源 12S 和漏 12D 互连的 n 沟道 FET 12 的情况下，提供单个连续的掩模开口 44，以注入漏 12D、源 12S、外部源塞 ST 和内部漏塞 DT、连接件 C1。然后，优选地，用诸如砷的合适 n 掺杂离子的泛光束（用标号 46 指示），执行注入。不可用的沟道阻断部位 CS 1 以与它们各自的塞和连接件相同的掺杂导电类型留下，而有源沟道阻断 CSO 被注入达到相反导电类型。这可以通过以下步骤来进行：在注入源和漏期间在 CSO 部位上方提供掩模并且在注入 p 沟道晶体管期间注入沟道阻断，或者通过将沟道阻断 n+ 连同 n 沟道晶体管的剩余部分一起注入并且之后（或之前）执行受沟道阻断限制的双剂量 p+ 注入。可按与之前不保险过程相同的方式执行该注入，唯一的不同是，现在是通过包括注入塞和连接件以及 FET 源和漏但不包括沟道阻断的各掩模中的较大开口进行注入。如传统处理中一样，单独的注入掩模 48 用于 p 沟道器件。单个连续开口 50 设置在塞和连接件和它们所连接的晶体管元件的掩模中；这些被示出为 p 沟道 FET 源 2S、漏 2D、漏塞 DT、源塞 ST 和连接件 C1。优选地，用诸如硼的合适 p 型掺杂物的用标号 52 指示的泛光束执行注入。需要处理时间或技术无差异，操作人员甚至不需要知道提供电路安全的掩模。然后，以传统方式完成这些电路，其中，FET 沟道中进行阈值注入，以设置晶体管特性。场氧化物按常规放置，然后通过扩散或离子注入沉积和掺杂多晶硅，以形成沟道和互连。接下来，沉积电介质并且添加金属化层以建立输入、输出、偏置线和任何必要的单元联接。最后，将保护玻璃或其它合适的介电涂层放置在整个芯片上方。由于制造过程中唯一需要的变化是改造离子注入掩模的开口，因此可提供具有改造开口的新标准掩模集合并且将其用作电路设计过程的标准元件。这使得本发明尤其适于 CAD 系统，使设计者仅仅从这种门的库中选择所需的安全逻辑门设计。

[0127] 在本发明的另一个方面，公开了逻辑结构块和使用结构块针对 IBG CMOS ASIC 设计逻辑单元库的方法。用与下述相同的结构块构建的不同逻辑门将具有相同的晶体管连接示意并且还具有相同的物理布局，使得它们在光学或电子显微镜下看起来是物理上相同的。用这种逻辑单元的库设计的 ASIC 对于逆向工程努力极具抵抗力。

[0128] 图 30 示出按照本发明的一方面的 IBG 比特内容如何可被编程以改变示例性基本逻辑块 3020 的逻辑功能的示例。本领域的普通技术人员将容易理解基本逻辑块 3020 的操作并且将不再详细进行描述。在图 30 中使用两个掩饰连接件 3031、3032 连接到基本逻辑块 3020 的输入 C。IBG 掩饰连接件 3031 和 3032 是可被编程为连接或隔离的 CMOS 技术中的结构，但通过逆向工程进行检测是非常困难的。IBG 掩饰连接件包括可以连接或隔离的 CMOS 技术中的结构，并且当遭受逆向工程攻击时这种结构的连接和隔离之间没有任何明显

的成像差异。

[0129] 在图30中，一个IBG掩饰连接件3031将输入C连接到被标记为C1的节点，另一个IBG掩饰连接器3032连接在输入C和被标记为C2的节点之间。节点C1和C2可被电源电压Vdd、Vss驱动，或者被来自其它逻辑单元的其它有源输出信号驱动，或者甚至被作为反馈信号的逻辑块的自身输出Z驱动。当顶部掩饰连接器3032被编程为与连接到Vdd的节点C2连接时，虽然底部掩饰连接件3031被编程为是隔离的，但输入C将接收逻辑状态“1”并且逻辑块表现得像输入A和B的“OR”门一样。在这种情况下，节点C1可连接到任何信号，因为底部掩饰连接件31被隔离。

[0130] 如果顶部掩饰连接件3032被编程为是隔离的，则虽然底部掩饰连接件3031被编程为使节点C1连接到Vss的连接件，但输入C处的逻辑状态是“0”并且逻辑块执行“A AND B bar”(Z = A B)的逻辑函数。在这种情况下，节点C2可连接到任何信号，因为顶部掩饰连接件被隔离。

[0131] 图31中示出IBG掩饰连接件的示例（例如，诸如，连接件3031）。图31中的顶部图示出用N型扩展注入（也称为NLDD(N型轻掺杂漏）注入）实现的连接。为了制成这种掩饰连接件，硅化物窗口敞口于有源硅区中的PN结上方以避免PN结通过硅化物直接短路。硅化物有时被称为硅化金属（自对准硅化物），是通过出于减小硅注入区的薄膜电阻的目的在硅表面上沉积金属（例如，钛）薄层而形成的金属硅化合物。当用NLDD注入来注入带有硅化物窗口的这个PN结的中心部分时，由于借助顶部上的硅化物从N+区到NLDD区和进一步从NLDD区到P+区的导通路径，导致PN结的两个端子将被短接。在CMOS制造过程中，NLDD注入是的标准注入之一。相比于源和漏N+/P+注入，掺杂注入较轻。其作用是减轻CMOS N型器件的短沟道效应。在CMOS制造中，P型扩展或PLDD注入是与P型器件的类似种类的注入。将图31的顶部结构中的NLDD切换成PLDD注入将把该结构变成作为反向偏置PN结的隔离。这在图31的顶部图中示出的。存在场氧化物(F.O.)是为了将掩饰连接件与其它有源电路隔离。相比于源和漏N+/P+注入，NLDD和PLDD注入的浓度较轻并且深度较浅，因此逆向工程师会发现在它们位于重掺杂N+/P+区旁边时难以辨别它们。有利的是，使用尽可能多的不同技术实现掩饰连接件，因为掩饰连接件的样式越多，将越难以对设计成具有这些掩饰连接件的ASIC进行逆向工程。

[0132] 在本发明的另一个方面，通过具有受控外形和受控厚度的多个材料层，形成IBG集成电路结构。在所述多个层之间设置厚度受控制的电介质材料层，从而致使集成电路结构不能有意操作。这种技术将使得逆向工程更加难以进行，特别地讲，将迫使逆向工程师非常细致地研究可能的硅-栅多晶线，以查看它们是否是真实情况。据信，这将使得逆向工程师的一切努力更艰难，因为为了对采用本发明的芯片进行逆向工程是非常耗时的并且有可能使得逆向工程师对采用本发明的芯片进行逆向工程是极其不切实际的（如果并非不可能），如以下关于图32-32C描述的。图32是看上去是场效应晶体管(FET)的半导体器件的平面图。然而，如从图32A、图32B和图32C中描绘的剖视图中看到，半导体器件是伪晶体管。图32A描绘本发明可如何有意“断开”接触以形成伪晶体管。类似地，图32B示出本发明可如何有意“断开”栅结构以形成伪晶体管。图32C是栅区3212和有源区3216、3218二者的剖视图，本发明有意“断开”与有源区3218的接触以形成伪晶体管。本领域的技术人员将理解，尽管这些图描绘了增强模式型器件，但伪晶体管还可以是耗散模式型器件。本发

明有意“断开”栅、源或漏接触。在耗散模式型晶体管的情况下，如果栅接触被“断开”，则在向控制电极施加标称电压时，器件将“导通”。如果源或漏接触被“断开”，则在向控制电极施加标称电压的情况下，伪耗散模式型晶体管将基本上“截止”。

[0133] 双多晶半导体工艺优选地包括两个多晶硅层 3224-1、3224-2 并且还可具有两个硅化金属层 3226-1、3226-2。可使用双多晶硅处理实现图 32、32A、32B 和 32C 中示出的结构。

[0134] 图 32 用平面图示出伪 FET 晶体管，但本领域的技术人员将理解，双极性晶体管的金属接触与描绘的源 / 漏接触极为类似。图 32A 是与被逆向工程师（从顶图看，参见图 32）看上去是 CMOS FET 的有源区金属层 3230、3231 有关的伪晶体管的侧视图。可供选择地，器件可以是垂直双极性晶体管，在这种情况下，逆向工程师看到的金属层 3320、3231 可以是发射极接触。如图 32A 中描绘的，对于 CMOS 结构，使用场氧化物 3220 作为区域边界，以传统方式形成有源区 3218。通过栅氧化物 3222（参见图 32C）注入有源区 3218，随后，栅氧化物 3222 被从有源区上方剥离下来并且可选地被随后烧结的硅化物金属替代，从而产生硅化物层 3226-1。接下来，沉积电介质层 3228。在优选实施例中，电介质层是二氧化硅层 3228。另外，可在二氧化硅层 3228 上方沉积多晶硅层 3224-2。在双多晶硅过程中，多晶硅层 3224-2 优选地是第二多晶硅层。接着，在多晶硅层 3224-2 上方形成可选硅化物层 3226-2。沉积并且蚀刻第二二氧化硅层 3229，以允许包括金属塞 3231 和金属接触件 3230 的金属层形成在可选硅化物层 3226-2 上方并且接触多晶硅层 3224-2（如果没有用到硅化物层 3226-2）。氧化物层 3228 和氧化物层 3229 优选地包括相同材料（可能具有不同密度），如此，当被堆叠地放置时，逆向工程师不能将其彼此区分开。

[0135] 在形成多晶硅层 3224-2 和金属塞 3231 时使用不同的掩模。为了保持多晶硅层 3224-2 和金属塞 3231 之间的对准，在与半导体衬底 3210 的主表面 3211 平行的方向上的多晶硅层 3224-2 的横截面优选地被设计成在工艺对准容差内基本上是与同一方向上截取的金属塞 3231 的横截面相同大小。如此，多晶硅层 3224-2 至少被金属塞 3231 部分掩饰。在图 32、图 32A、图 32B 和图 32C 中，多晶硅层 3224-2 被描绘为比金属塞 3231 大得多；然而，仅仅为了清晰起见，这些图被夸张。优选地，多晶硅层 3224-2 被设计成确保金属塞 3231 的横截面与多晶硅层 3224-2 的横截面或可选硅化物层 3226-2（如果使用的话）的横截面对准，但足够小，以致在显微镜下看到是极其困难的。另外，金属塞 3231 的底部优选地完全接触多晶硅层 3224-2 或可选硅化物层 3226-2（如果使用的话）。

[0136] 逆向工程师无法容易地得到正视图。事实上，逆向工程师将得到正视图的典型方式将是在各可能的接触或非接触处拍摄个体横截面扫描电子显微照片。在各可能的接触或非接触处拍摄显微照片的过程是过分耗时且昂贵的。逆向工程师当从顶部看时将看到金属接触件 3230 的顶部。氧化物 3228 与多晶硅层 3224-2 和可选的硅化物层 3226-2 的接触失效层将至少被电路结构的特征（即，金属接触件 3230 和金属塞 3231）掩饰。

[0137] 逆向工程过程经常涉及将半导体器件分层，以将各层从硅衬底 3210 拆除下来，然后从与硅衬底 3210 的主表面 3211 垂直的方向观察半导体器件。在这个过程期间，逆向工程师将去除本发明中为了停用接触件而使用的氧化物层 3228 的迹线。

[0138] 另外，逆向工程师可选择只从半导体区去除金属接触件 3230 的更高成本的方法。多晶硅层 3224-2 的横截面优选地在工艺对准容差内与金属塞 3231 的横截面基本上相同。

氧化物层 3228、3229 实际是透明的，可选硅化物层 3226-2 和多晶硅层 3224-2 的厚度小。可选硅化物层 3226-2 的典型厚度是 100-200 埃，多晶硅层 3224-2 的典型厚度是 2500-3500 埃。因此，逆向工程师当从顶部观察器件时，将认为金属塞 3231 接触硅化物层 3226-1，从而不正确地认为器件是能操作的。另外，当使用可选硅化物层 3226-2 时，一旦金属塞 3231 被去除，逆向工程师在看器件时会进一步混淆。在看到硅化物层 3226-2 剩下的闪亮残留物时，逆向工程师将不正确地认为闪亮残留物是金属塞 3231 留下的。因此，逆向工程师将再次不正确地认为用到接触件。

[0139] 图 32B 是图 32 的伪晶体管的栅接触件的侧视图。如可从图 32 看到的，沿着剖面线 32B--32B 截取的图 32B 的视图贯穿栅氧化物层 3222，贯穿第一多晶硅层 3224-1 并且贯穿第一硅化物层 3226-1，栅氧化物层 3222、第一多晶硅层 3224-1 和第一硅化物层 3226-1 形成在有源区 3216 和 3218 之间的半导体衬底 3210（典型地，硅）中的场氧化物区 3220 和栅区 3212 上方（参见图 323C）。第一多晶硅层 3224-1 将用作导电层，如果该器件正常发挥作用，则该导电层影响因施加控制电压形成的贯穿栅区 3212 的导通。使用传统加工技术形成有源区 3216、3218 和 3212、栅氧化物 3222、第一多晶硅层 3224-1 和第一硅化物层 3226-1。对于正常发挥作用的器件，通过金属层 3230、3231 形成的控制电极将接触场氧化物 3220 上方的硅化物层 3226-1 的层。硅化物层 3226-1 接着将用作正常发挥作用的器件的控制层。为了形成伪晶体管，沉积至少一个电介质层，例如，氧化物层 3228。接下来，在氧化物层 3228 上方沉积第二多晶硅层 3224-2 和可选的第二硅化物层 3226-2。在一些制造过程中，可省去描绘的在多晶硅层 3224-2 和金属塞 3231 之间的硅化物层 3226-2，因为一些双多晶硅处理技术只利用了一个硅化物层（当使用这种处理技术时，将只使用一个硅化物层 3226-1 或 3226-2）。在任一种情况下，氧化物层 3228 妨碍了栅正常发挥作用。

[0140] 在与半导体衬底 3210 的主表面 3211 平行的方向上的第二多晶硅层 3224-2 的横截面优选地在工艺对准容差内基本上与同一方向上截取的金属塞 3231 的横截面是相同大小。如此，第二多晶硅层 3224-2 部分被金属塞 3231 掩饰。在图 32、图 32A、图 32B 和图 32C 中，多晶硅层 3224-2 被描绘为比金属塞 3231 大得多；然而，仅仅为了清晰起见，夸大了这些图。优选地，多晶硅层 3224-2 被设计成确保金属塞 3231 的横截面与多晶硅层 3224-2 的横截面或可选硅化物层 3226-2（如果使用的话）的横截面完全对准，但足够小，以致在显微镜下看到是极其困难的。另外，金属塞 3231 的底部优选地完全接触多晶硅层 3224-2 或可选硅化物层 3226-2（如果使用的话）。

[0141] 添加的氧化物层 3228 和多晶硅层 3224-2 被布置成使它们出现在将出现金属 - 多晶硅接触的垂直平面上，如当从平面图上看时出现的。该布置使金属层 3230、3231 至少部分掩饰添加的氧化物层 3228 和 / 或多晶硅层 3224-2，使得布局看上去垂直于逆向工程师。逆向工程师将蚀刻掉金属层 3230、3231，查看多晶硅层 3224-2 和可选硅化物层 3226-2（如果使用的话）可能的残留物。在看到可选硅化物层 3226-2 的闪亮残留物时，逆向工程师会不正确地认为闪亮残留物是来自金属塞 3231。逆向工程师将没有任何理由相信形成了与多晶硅层 3224-1 或可选硅化物层 3226-1 的接触。另外，当没有使用可选硅化物层 3226-2 时，在从与硅衬底 3210 的主表面 3211 的垂直方向上观察接触时，没有明确看到氧化物层 3228 和多晶硅层 3226-2 的小厚度，因此，逆向工程师将得出结论，他或她正在看的是正常发挥作用的多晶硅栅 FET 晶体管。

[0142] 在使用时，图 32A、32B 和 / 或 32C 的逆向工程保护技术仅仅需要保守地使用，但优选地与其它逆向工程技术（如以上子标题“相关技术”下讨论的技术）相结合地使用。这些相关技术和本文中公开的技术的基本目的是，使得弄清如何实现电路（使得它可被成功复制）是非常耗时的，这使逆向工程师的努力受挫。因此，对于现代 IC 中的成千上万的器件，其中只有少部分将采用本文中描述的并且图 32A、图 32B 和图 32C 中描绘的伪晶体管来掩饰电路。因此，除非逆向工程师能够确定这些伪晶体管，否则逆向工程师确定的所得电路将是不正确的。

[0143] 另外，伪晶体管优选地没有用于完全禁用用到它们的多个晶体管电路，而是致使晶体管电路以意料不到或非直观的方式发挥作用。例如，被逆向工程师看上去是 OR 门的部分有可能实际上是用作 AND 门。或者，看上去是反相输入的部分有可能实际上是非反相的。可能性几乎无穷无穷，几乎肯定致使逆向工程师特别沮丧以致他或她放弃，这与逆向工程师力求发现利用了这些技术的集成电路器件截然相反。

[0144] 另外，根据本发明，当逆向工程师蚀刻掉金属 3230、3231 时，他和她应该优选地“看到”正常意料中的层，而无论接触是否被阻挡。因此，如果逆向工程师期望在蚀刻掉金属之后看到硅化物，则即使接触被阻挡时，他或她也应该看得到。如果他 / 她期望在蚀刻掉金属之后看到多晶硅，则即使接触被阻挡时，他或她也应该看得到。

[0145] 在另一个方面，按照本发明的 IBG 电路使用当用其它逆向工程检测防止技术制造逆向工程前时逆向工程师会看到的硅化物层的伪造边缘。更具体地讲，为了进一步混淆逆向工程师，在制造半导体器件期间，使用导电层阻挡掩模。

[0146] 在上述逆向工程检测防止技术中，使用沟道阻挡结构来迷惑逆向工程师。如图 33B 中所示，沟道阻挡结构 3327 具有与沟道区 3323、3325 不同的掺杂物类型并且在上覆硅化物中具有障碍物 3330。在使用诸如 CMP 的逆向工程过程之后，硅化物层的伪造边缘 3328 可显露给逆向工程师，使用沟道阻挡结构 3324、3327 中断两个沟道区 3323、3325 之间的电连接，如通过比较图 33A 和图 33B 看到的。在大多数逆向工程过程中，逆向工程师不容易得到沟道区和沟道阻挡结构中使用的掺杂物的类型。因此，迫使逆向工程师依赖于诸如硅化物层的伪造边缘 3328 的其它方法来确定导电沟道中是否具有沟道阻断。

[0147] 图 34 描绘按照本发明制造的 IBG 器件的硅化物层的伪造边缘 3328。硅化物块掩模优选地被改造，以防止硅化物成完全覆盖伪沟道阻挡结构 3329。沟道阻挡结构 3329 与沟道区 3323、3325 具有相同的导电类型；因此，是否存在连接沟道区 3323、3325 的硅化物层并没有对贯穿沟道的导电性产生影响。然而，通过改造硅化物阻挡掩模以防止硅化物层完全覆盖伪沟道阻挡结构 3329，对于逆向工程师，伪造边缘 3328 与障碍物 3330 一起看上去是指示沟道没有电连接，即，图 34 的伪造边缘 3328 与图 33B 的伪造边缘 3328 相同。因此，逆向工程师在观察伪造边缘 28 时将立即不正确地认定下伏沟道的连接性。

[0148] 为了进一步掩饰电路，可在形成轻掺杂漏 (LDD) 的同时形成沟道阻挡结构 3329 中使用的掺杂物类型。因此，即使使用染色蚀刻工艺，相比于剂量高得多的源 / 漏注入物 3322、3326，逆向工程师也将花多得多的时间来辨别两种类型的注入 (N 型与 P 型）之间的差异。另外，通过用 LDD 过程形成伪沟道阻挡结构 3329，因为考虑到击穿，所以可使沟道阻挡结构 3329 的尺寸较小。

[0149] 在制造本发明的优选方法中，半导体芯片制造商的设计规则被修改，以允许有未

被硅化的注入区。另外，设计规则还可被修改，以允许沟道阻挡结构 3329 小并且被轻掺杂（通过使用 LDD 注入），以进一步防止被逆向工程师检测到。

[0150] 在修改设计规则时，重要的是确保如图 34 中所示的实际导电沟道的伪造边缘匹配如图 33B 中所示的非导电沟道的伪造边缘的布置。为了图示，图 33B 中的伪造边缘 3328 匹配图 34 的伪造边缘 3328。本领域的技术人员可理解，伪造边缘 3328 不一定如图 33B 或图 34 中具体示出的。替代地，伪造边缘可沿着沟道出现在几乎任何地方。然而，重要的是，(1) 硅化物层没有提供电连接（即硅化物层没有完全覆盖其中带有意图块或伪块的沟道）和 (2) 用于电连接（即真实连接）的伪造边缘 3328 用于非电连接（即假连接）的伪造边缘 3328 相对相同。如此，虽然可建议包括全在单个集成电路装置上的图 33A、图 33B 和图 34 中示出的类型的导通和非导通沟道，但使用将使逆向工程师走投无路的参照图 33B 和图 34 示出和描述的那些类型的沟道的混合物。

[0151] 在本发明的另一个方面，IBG 电路可包括诸如电容器的其它无源器件。因为理想的电容器阻挡所有电流，所以这致使理想电容器划分器输出到 DC 电源的未知状态。电容器的 DC 方程是 i（电流）＝ C（电容）×dV/dT（电压变化的速率）。除非输入电压正在变化，否则理想电容器不可用于限定可用于 IBG 电路的电压。因此，电路中的电压将在为电路供电时初始地变化。另外，所有电容器都具有可通过电阻器建模的一定量的漏泄电流。参见图 35，图 35 示出被作为与电阻器 R1 和 R2 并联的理想电容器 C1 和 C2 建模的实际电容器。

[0152] 在具有电容器的 IBG 电路的情况下，这些电容器可基于当向电路供电时的初始电压变化，充当非易失性电压存储装置。电容值将确定初始电压电平，并且建模真实电容器的泄漏的电阻器将确定这个电压电平如何衰减。在向图 35 的分压器电路供应电力 (Vcc) 之后，如果 R1 和 R2 的电阻值大，则主要通过电容器划分器对节点 V 进行初始充电。在一定时间段内，输出 V 的 DC 电压电平将衰减至通过 R1 和 R2 确定的电压值。只要 R1 和 R2 大，时间量就会非常大，大约是数年。在这种情况下，电容值接着确定 V 的 DC 电平。

[0153] 通过面积（通常是金属）、电容器节点之间的间隔（电介质）和介电常数实际确定电容值。在 MOS 过程中，金属几何形状、电介质厚度或电介质材料可发生变化，以改变电容值。其中，电介质材料出于逆向工程目的进行确定是非常困难的。因此，诸如图 35 的电容器对的电容器可发生偏置，以用作 IBG 电路并且妨碍逆向工程师。

[0154] 在本发明的另一个方面，IBG 器件可用于提供多个实体之间的安全数字通信。两个器件之间的许多交易（如借助互联网在商业交易期间发生的）需要进行安全数据传递，使得信用卡、密码、银行账户或其它敏感信息无法被非法拦截和使用。还可使用安全数据传递认证器件或人员的身份。编码纯文本以形成密文的过程被称为加密并且解码密文以产生纯文本的过程被称为解密。为了保障数据交易，通过利用算法在两个通信实体之间的通信链路上使用加密，这些算法允许纯文本数据被发送实体加密并且被接收实体解密。另外，可使用加密和解密来鉴权诸如打印装置的消息或装置。

[0155] 传统上，密码使用秘密的解码密钥中包含的信息加密和解密消息。现代电子密码系统使用已知是数字密钥和算术算法的比特串来加密和解密信息。存在两种类型的加密：对称密钥（私有密钥）加密和不对称密钥（公开密钥）加密。对称密钥和私有密钥加密经常结合起来使用，以提供网络和信息安全的各种安全功能。

[0156] 对称密钥加密算法使用相同的密钥来加密信息和解密信息。对称密钥也被称为私

有密钥，因为它被保持为信息的发送方和接收方之间的共享秘密。因为加密和解密算法通常不是秘密，所以必须将对称密钥保密，以保护该信息。

[0157] 图 36 示出按照示例性实施例的私有密钥系统 3600 的框图。私有密钥系统 3600 允许发送方 3602 向接收方 3606 发送纯文本数据 3604，并且知道，即使被拦截，接收方之外的其他人不能看到纯文本数据 360。发送方 3602 使用不公开的私有密钥 3608 加密纯文本数据 3604。私有密钥 3608 与加密算法 3610 一起用于将纯文本数据 3604 安全加密成加密数据 3612。加密算法 3610 通常不是秘密。纯文本数据 3604 可以是诸如电子邮件消息（电子邮件）的文本或诸如照片的任何其它数字信息、或仅仅是二进制数据。一旦被加密，加密数据 3612 就可在诸如互联网或任何其它通信链路的网络 3614 上发送，确信只有接收方 3606 才能够看到纯文本数据 3604。当被接收方 3606 接收时，使用私有密钥 3608 和解密算法 3614 将加密数据 3612 解密。接收方 3606 此时可看到纯文本数据 3604。

[0158] 对称密钥加密比公开密钥加密快得多，经常快 100 倍至 1000 倍。因为相比于对称密钥加密，公开密钥加密给计算机处理器带来的计算负担重得多，所以对称密钥技术通常用于为信息的整体加密和解密提供保密。

[0159] 对称密钥一般按安全协议被用作可信在线通信的会话密钥。例如，传输层安全 (TLS) 和网际协议安全 (IPSec) 协议将对称会话密钥与标准加密算法一起用于加密和解密各方之间的秘密通信。不同的会话密钥用于各秘密通信会话并且会话密钥有时按指定时间间隔被更新。

[0160] 对称密钥一般被提供诸如电子邮件消息和文献文件的持久性数据的整体加密的技术使用。例如，安全 / 多用途互联网邮件扩展 (S/MIME) 使用对称密钥加密秘密邮件的消息，加密文件系统 (EFS) 使用对称密钥加密要保密的文件。

[0161] 相比于对称密钥加密，不对称算法针对加密信息和解密信息使用不同的密钥。公开的不对称密钥被发送方用来加密信息并且对应的私有不对称密钥被接收方作为秘密保持并且用于解密通过不对称公开密钥加密的信息。加密和解密算法通常不是秘密，因此，私有对称密钥彼此保密，以保护信息。用户的公开密钥可在目录中公开，使得它能被其他人获得，而不包括安全性。两个密钥是不同的，但数学上以函数相关联。可只用一组对应的私有密钥解码用公开密钥加密的信息。密钥本身不能同时用于执行加密和解密两个功能。

[0162] 图 37 示出按照示例性实施例的不对称公开密钥系统 3700 的框图。公开密钥系统 3700 允许发送方 3702 向接收方 3706 发送纯文本数据 3704，而知道，即使被拦截，接收方之外的其他人不能看到纯文本数据 3704。发送方 3702 使用公知的公开密钥 3708 加密纯文本数据 3704。公开密钥 3708 通常是由接收方 3706 提供的。公开密钥 3708 与加密算法 3710 一起用于将纯文本数据 3704 安全加密成加密数据 3712。加密算法 3710 通常不是秘密。纯文本数据 3704 可以是诸如电子邮件消息（电子邮件）的文本或诸如照片的任何其它数字信息、或仅仅是二进制数据。一旦被加密，加密数据 3612 就可在诸如互联网或任何其它通信链路的网络 3714 上发送，确信只有接收方 3606 才能够看到纯文本数据 3704。当被接收方 3706 接收时，使用私有密钥 3716 和解密算法 3714 将加密数据 3712 解密。接收方 3706 此时可看到纯文本数据 3704。

[0163] 已知为 RSA 数字签名过程的加密方法还使用私有密钥加密信息以形成数字签名。对于 RSA 数字签名，只有公开密钥可解密通过一组对应的私有密钥加密的信息。此过程可

用于验证另一方或装置的可靠性。

[0164] 现今，公开密钥加密在内部网和因特网上提供强的可升级安全性方面扮演越来越重要的角色。公开密钥加密一般用于执行以下功能，例如：在通过网络进行交换期间或者在被操作系统使用、存储或缓存的同时，加密对称密钥以保护对称密钥；形成数字签名，以得到在线实体的鉴权和不可抵赖性；形成数字签名，以得到电子文件和文档的数据完整性。

[0165] 当传输的一方不能访问时，公开密钥加密最有效。例如，公开密钥的产生得到完全保护，如果产生公开密钥是在安全互联网站点（不包括站点攻击）上执行的。如果对于独立的点对点通信利用的是不对称加密，则公开密钥和私有密钥产生算法驻于可被分层和颠倒的硅内。这允许开发重复器件并且解密发送的数据。

[0166] 已知的不对称和对称加密算法可被足够强大的超级计算机破解，从而产生公开密钥和私有密钥。这就是为什么这些算法的复杂度不断增加。另外，公开密钥和私有密钥的传输需要对抗攻击（如动态力或电磁发射分析）的其它保护，以保护数据交易。

[0167] 按照本发明的一个方面，IBG 器件可用于保护信息从一个实体到另一个实体的安全发送，包括加密和解密算法。执行这些算法的电路可包括 IBG 器件，从而防止对算法的细节进行逆向工程。在这种基于 IBG 的器件中，不必保持一个或多个加密密钥的保密，因为算法是保密的。另外，针对基于 IBG 的安全系统的动态力和电磁攻击将不会成功。用基于 IBG 的安全系统，不对称加密的重要性降低并且对称加密现在可即刻用于需要安全的低成本应用。

[0168] 图 38 示出按照本发明的受 IBG 保护的安全系统 3800 的框图。受 IBG 保护的安全系统 3800 允许发送方 3802 向接收方 3806 发送纯文本数据 3804，并且知道，即使被拦截，接收方之外的其他人不能看到纯文本数据 3804。发送方 3802 使用密钥 3808 加密纯文本数据 3804。有利地，密钥 3808 可以是公知的或私有的。密钥 3808 与加密算法 3810 一起用于将纯文本数据 3804 安全加密成加密数据 3812。加密算法 3810 是私有算法，至少部分包括使加密算法免于遭受逆向工程并且保持保密的 IBG 电路。纯文本数据 3804 可以是诸如电子邮件消息（电子邮件）的文本或诸如照片、视频或仅仅二进制数据的任何其它数字信息。一旦被加密，加密数据 3812 就可在诸如互联网或任何其它通信链路的网络 3814 上发送，确信只有接收方 3806 才能够看到纯文本数据 3804。当被接收方 3806 接收时，使用密钥 3816 和解密算法 3814 将加密数据 3812 解密。接收方 3806 此时可看到纯文本数据 3804。解密算法 3814 至少部分包括使解密算法免于遭受逆向工程并且保持保密的 IBG 电路。在优选实施例中，加密和解密方案是对称的，因此用于解密的密钥 3816 与用于加密的密钥 3808 相同。在替代实施例中，解密和解密是不对称的并且用于解密的密钥 3816 不同于用于加密的密钥 3808。有利地，密钥 3816 可以是公知的或私有的。IBG 电路还可用于构造这些系统的其它部分。例如，IBG ROM 可用于安全地存储供加密和解密系统使用的数据。

[0169] 在各种系统中可采用受 IBG 保护的加密和解密器件。例如，图 39 示出按照本发明的视频的安全传输的系统 3900。例如，安全视频系统 3900 可用于通过有线 TV 或卫星 TF 提供商发送视频。视频发送芯片 3902 加密视频数据流，然后，例如，使用诸如卫星或电缆的介质将视频流发送到可位于用户机顶盒中的视频接收芯片 3904。发送视频芯片 3902 可包括使用 IBG 电路实现的加密电路。类似地，视频接收芯片 3904 可包括也使用 IBG 电路实现的解密电路。虽然加密 / 解密方案可以是不对称的，但在优选实施例中，解密和解密方案是对

称的，从而导致执行加密和解密的计算负担减小。

[0170] 又如，图 40 示出系统 4000 的框图，该系统用于受 IBG 保护的智能卡 4002 和将加密数据发送到智能卡 4002 并且从智能卡 4002 接收加密数据的受 IBG 保护的智能卡读取器 4004。智能卡通常是内嵌电子电路的口袋大小的卡，但可用多种形式实施。例如，智能卡 4200 可提供识别、鉴权、数据存储、应用处理和其它功能。在优选实施例中，智能卡读取器 4004 包括使用 IBG 电路实现的不对称公开密钥加密和解密电路 4006。智能卡 4002 包括使用 IBG 电路实现的不对称公开密钥加密和解密电路 4008。例如，还可使用诸如 ROM 的 IBG 电路实现智能卡 4002 和读智能卡器 4004 的电路的其它部分。例如，这种受 IBG 保护的智能卡电路可用于护照、ID 卡和驾驶证。

[0171] 图 41 示出受 IBG 保护的 RFID 标签 4102 和将加密射频数据发送到 RFID 标签 4102 并且从 RFID 标签 4102 接收加密视频数据的受 IBG 保护的 RFID 读取器 / 写入器 4104 的系统 4000 的框图。在优选实施例中，智能卡读取器 / 写入器 4104 包括使用 IBG 电路实现的对称公开密钥加密和解密电路 4106。RFID 标签 4102 包括使用 IBG 电路实现的对称公开密钥加密和解密电路 4108。例如，还可使用诸如 ROM 的 IBG 电路实现智能标签 4102 和读卡器 / 写卡器 4104 的电路的其它部分。这种 RFID 标签可用于产品信息、诸如收费公路的运费交易和需要安全交易或认证的其它环境。

[0172] 如以上相对于图 25 和图 26 描述的，可使用本文中详细描述的一个或多个 IBG 器件实现诸如控制器 2504、存储器 2506、I/O 接口电路 2502 和任何其它电路的成像盒芯片的电路组件，以保护电路的操作免于遭受逆向工程。在本发明的一个方面，附接到成像盒的成像盒芯片可包括使用 IBG 电路实现的加密或解密电路。与该成像盒兼容的诸如打印机的成像装置还可包括使用 IBG 电路实现的加密或解密电路。当成像盒被安装在成像装置中时，成像芯片和成像装置可安全地通信，从而允许信息被交换并且允许成像装置验证成像盒的真实性。

[0173] 图 42 示出将 IBG 电路结合到集成电路中的示例性方法的流程图。在第一步骤 4202 中，消费者或顾客提供关于集成电路功能的高级设计 (HDL) 描述。在本发明的一个方面，HDL 包括定制加密和 / 或解密电路。在第二步骤 4204 中，DHL 设计经过产生晶体管级设计描述的合成过程。IBG 标准单元库 4205 的一些部分可被并入保护设计的部分或全部的这个设计描述中。IBG 标准单元库可包括例如使用 IBG 电路实现的、诸如逻辑门、缓冲器和存储器的器件。在步骤 4206 中布置和敷设这个晶体管级设计之后，消费者将验证设计的操作。接着，在步骤 4208 中，消费者可制造经验证的设计。

[0174] 图 43 示出使用可构造的加密 / 解密引擎。在这个示例中，硬件加密 / 解密引擎由产生 32 比特随机序列 4301 的 32 比特线性反馈移位寄存器 (LFSR) 组成。这 32 比特随机序列被初始化并且与加密阶段 4302 中发送的数据进行异或并且被发送到接收方 4303。进而进行初始化并且与解密阶段 4304 中接收的数据进行异或。加密 / 解密密钥由在移位操作期间使用的两个 32 比特字段 (32 比特初始化值和 32 比特 LFSR 异或值) 组成。这个 64 比特密钥形成唯一性随机序列并且可以 IBG 形式在内部实现。

[0175] LFSR 是通过有效扰动数据比特的 160IBG 单元构造的。这个扰动施加到用于 64 比特密钥中的 32 比特。如果需要进一步扰动，则可使用另外的 160 个 IBG 单元扰动密钥的剩余 32 比特。以下是用于这个加密 / 解密引擎的硬件描述语言 (HDL) 的示例。

[0176] 以下的 Verilog 代码定义了硬件加密 / 解密引擎。

[0177] // 简单定制加密算法

[0178] // 使用 32 比特线性反馈移位寄存器作为异或源

[0179] module simple_encryption(

[0180] i_key,//64 比特秘钥

[0181] i_rst,// 初始化线性反馈移位寄存器

[0182] i clk,// 数据时钟

[0183] o_data// 线性反馈移位寄存器输出

[0184]) ;

[0185] input wire[63:0]i_key ;// 加密秘钥 - 异或反馈

[0186] input wire i_rst ;//LFSR 初始化

[0187] input wire i clk ;// 数据时钟

[0188] output wire[31:0]o_data ;//LFSR 输出

[0189] //IBG 规范块 - 由 IBG 单元 32x 5 = 160IBG 单元设置的值

[0190] parameter IBG0 = 5'h0 ;

[0191] parameter IBG1 = 5'h1 ;

[0192] parameter IBG2 = 5'h2 ;

[0193] parameter IBG3 = 5'hf ;

[0194] parameter IBG4 = 5'h4 ;

[0195] parameter IBG5 = 5'h5 ;

[0196] parameter IBG6 = 5'h1c ;

[0197] parameter IBG7 = 5'h7 ;

[0198] parameter IBG8 = 5'h8 ;

[0199] parameter IBG9 = 5'h9 ;

[0200] parameter IBG10 = 5'ha ;

[0201] parameter IBG11 = 5'hb ;

[0202] parameter IBG12 = 5'hc ;

[0203] parameter IBG13 = 5'hd ;

[0204] parameter IBG14 = 5'he ;

[0205] parameter IBG15 = 5'h3 ;

[0206] parameter IBG16 = 5'h10 ;

[0207] parameter IBG17 = 5'h11 ;

[0208] parameter IBG18 = 5'h12 ;

[0209] parameter IBG19 = 5'h16 ;

[0210] parameter IBG20 = 5'h14 ;

[0211] parameter IBG21 = 5'h15 ;

[0212] parameter IBG22 = 5'h13 ;

[0213] parameter IBG23 = 5'h17 ;

[0214] parameter IBG24 = 5'h18 ;

[0215] parameter IBG25 = 5'h19 ;

[0216] parameter IBG26 = 5'h1a ;

[0217] parameter IBG27 = 5'h1b ;

[0218] parameter IBG28 = 5'h6 ;

[0219] parameter IBG29 = 5'h1d ;

[0220] parameter IBG30 = 5'h1e ;

[0221] parameter IBG31 = 5'h1f ;

[0222] reg[31:0]data ;//LFSR

[0223] wire[31:0]data_mux ;// 配置基于 IBG 的 LFSR 的数据乘子

[0224] // 由 IBG 单元数据驱动的数据多路器

[0225] LFSR_multiplex LM0(

[0226] .i_data(data),

[0227] .i_addr(IBG0),

[0228] .o_data(data_mux[0])) ;

[0229] LFSR_multiplex LM1(

[0230] .i_data(data),

[0231] .i_addr(IBG1),

[0232] .o_data(data_mux[1])) ;

[0233] LFSR_multiplex LM2(

[0234] .i_data(data),

[0235] .i_addr(IBG2),

[0236] .o_data(data_mux[2])) ;

[0237] LFSR_multiplex LM3(

[0238] .i_data(data),

[0239] .i_addr(IBG3),

[0240] .o_data(data_mux[3])) ;

[0241] LFSR_multiplex LM4(

[0242] .i_data(data),

[0243] .i_addr(IBG4),

[0244] .o_data(data_mux[4])) ;

[0245] LFS_multiplex LM5(

[0246] .i_data(data),

[0247] .i_addr(IBG5),

[0248] .o_data(data_mux[5])) ;

[0249] LFSR_multiplex LM6(

[0250] .i_data(data),

[0251] .i_addr(IBG6),

[0252] .o_data(data_mux[6])) ;

[0253] LFSR_multiplex LM7(

```
[0254]  .i_data(data),
[0255]  .i_addr(IBG7),
[0256]  .o_data(data_mux[7]));
[0257]  LFSR_multiplex LM8(
[0258]  .i_data(data),
[0259]  .i_addr(IBG8),
[0260]  .o_data(data_mux[8]));
[0261]  LFSR_multiplex LM9(
[0262]  .i_data(data),
[0263]  .i_addr(IBG9),
[0264]  .o_data(data_mux[9]));
[0265]  LFS_multiplex LM10(
[0266]  .i_data(data),
[0267]  .i_addr(IBG10),
[0268]  .o_data(data_mux[10]));
[0269]  LFSR_multiplex LM11(
[0270]  .i_data(data),
[0271]  .i_addr(IBG11),
[0272]  .o_data(data_mux[11]));
[0273]  LFSR_multiplex LM12(
[0274]  .i_data(data),
[0275]  .i_addr(IBG12),
[0276]  .o_data(data_mux[12]));
[0277]  LFSR_multiplex LM13(
[0278]  .i_data(data),
[0279]  .i_addr(IBG13),
[0280]  .o_data(data_mux[13]));
[0281]  LFSR_multiplex LM14(
[0282]  .i_data(data),
[0283]  .i_addr(IBG14),
[0284]  .o_data(data_mux[14]));
[0285]  LFSR_multiplex LM15(
[0286]  .i_data(data),
[0287]  .i_addr(IBG15),
[0288]  .o_data(data_mux[15]));
[0289]  LFS_multiplex LM16(
[0290]  .i_data(data),
[0291]  .i_addr(IBG16),
[0292]  .o_data(data_mux[16]));
```

```
[0293]  LFSR_multiplex LM17(
[0294]  .i_data(data),
[0295]  .i_addr(IBG17),
[0296]  .o_data(data_mux[17]));
[0297]  LFSR_multiplex LM18(
[0298]  .i_data(data),
[0299]  .i_addr(IBG18),
[0300]  .o_data(data_mux[18]));
[0301]  LFSRjmultiplex LM19(
[0302]  .i_data(data),
[0303]  .i_addr(IBG19),
[0304]  .o_data(data_mux[19]));
[0305]  LFSR_multiplex LM20(
[0306]  .i_data(data),
[0307]  .i_addr(IBG20),
[0308]  .o_data(data_mux[20]));
[0309]  LFS jTiultiplex LM21(
[0310]  .i_data(data),
[0311]  .i_addr(IBG21),
[0312]  .o_data(data_mux[21]));
[0313]  LFSR_multiplex LM22(
[0314]  .i_data(data),
[0315]  .i_addr(IBG22),
[0316]  .o_data(data_mux[22]));
[0317]  LFSR_multiplex LM23(
[0318]  .i_data(data),
[0319]  .i_addr(IBG23),
[0320]  .o_data(data_mux[23]));
[0321]  LFSR_multiplex LM24(
[0322]  .i_data(data),
[0323]  .i_addr(IBG24),
[0324]  .o_data(data_mux[24]));
[0325]  LFSR_multiplex LM25(
[0326]  .i_data(data),
[0327]  .i_addr(IBG25),
[0328]  .o_data(data_mux[25]));
[0329]  LFSR_multiplex LM26(
[0330]  .i_data(data),
[0331]  .i_addr(IBG26),
```

```
[0332]  .o_data(data_mux[26]));
[0333]  LFS_multiplex LM27(
[0334]  .i_data(data),
[0335]  .i_addr(IBG27),
[0336]  .o_data(data_mux[27]));
[0337]  LFSR_multiplex LM28(
[0338]  .i_data(data),
[0339]  .i_addr(IBG28),
[0340]  .o_data(data_mux[28]));
[0341]  LFSR_multiplex LM29(
[0342]  .i_data(data),
[0343]  .i_addr(IBG29),
[0344]  .o_data(data_mux[29]));
[0345]  LFSR_multiplex LM30(
[0346]  .i_data(data),
[0347]  .i_addr(IBG30),
[0348]  .o_data(data_mux[30]));
[0349]  LFSR_multiplex LM31(
[0350]  .i_data(data),
[0351]  .i_addr(IBG31),
[0352]  .o_data(data_mux[31]));
[0353]  assign o_data = data;// 指派输出给 LFSR
[0354]  always@(posedge i elk or negedge i_rst)begin
[0355]  // 对每个数据时钟或初始化脉冲
[0356]  if(! i_rst)begin
[0357]   data<= i_key[31:0];// 初始化成秘钥值
[0358]   end
[0359]  else begin
[0360]   data<= {data_mux[30:0]^i_key[62:32],(i_key[63]^data_mux[31])};
[0361]  // 基于秘钥和 IBG 加扰的数据的 XOR 反馈
[0362]   end
[0363]  end
[0364]  endmodule
[0365]  // 数据多路器 32 至 1 定义
[0366]  module LFSR_multiplex(
[0367]    i_data,//32 比特数据输入
[0368]    i_addr,//5 比特选择
[0369]    o_data//1 比特输出
[0370]  );
```

```
[0371]  input wire[31:0]i_data;
[0372]  input wire[4:0]i_addr;
[0373]  output o_data;
[0374]  //多路器指派
[0375]  assign o_data = i_addr == 5'h0 ? i_data[0]:
[0376]                  i_addr == 5'h1 ? i_data[1]:
[0377]                  i_addr == 5'h2 ? i_data[2]:
[0378]                  i_addr == 5'h3 ? i_data[3]:
[0379]                  i_addr == 5'h4 ? i_data[4]:
[0380]                  i_addr == 5'h5 ? i_data[5]:
[0381]                  i_addr == 5'h6 ? i_data[6]:
[0382]                  i_addr == 5'h7 ? i_data[7]:
[0383]                  i_addr == 5'h8 ? i_data[8]:
[0384]                  i_addr == 5'h9 ? i_data[9]:
[0385]                  i_addr == 5'ha ? i_data[10]:
[0386]                  i_addr == 5'hb ? i_data[11]:
[0387]                  i_addr == 5'hc ? i_data[12]:
[0388]                  i_addr == 5'hd ? i_data[13]:
[0389]                  i_addr == 5'he ? i_data[14]:
[0390]                  i_addr == 5'hf ? i_data[15]:
[0391]                  i_addr == 5'h10 ? i_data[16]:
[0392]                  i_addr == 5'h11 ? i_data[17]:
[0393]                  i_addr == 5'h12 ? i_data[18]:
[0394]                  i_addr == 5'h13 ? i_data[19]:
[0395]                  i_addr == 5'h14 ? i_data[20]:
[0396]                  i_addr == 5'h15 ? i_data[21]:
[0397]                  i_addr == 5'h16 ? i_data[22]:
[0398]                  i_addr == 5'h17 ? i_data[23]:
[0399]                  i_addr == 5'h18 ? i_data[24]:
[0400]                  i_addr == 5'h19 ? i_data[25]:
[0401]                  i_addr == 5'h1a ? i_data[26]:
[0402]                  i_addr == 5'h1b ? i_data[27]:
[0403]                  i_addr == 5'h1c ? i_data[28]:
[0404]                  i_addr == 5'h1d ? i_data[29]:
[0405]                  i_addr == 5'h1e ? i_data[30]:i_data[31];
[0406]  endmodule
```

[0407] 以上是使用 IBG 结构确保安全的 32 比特加密 / 解密引擎的示例。可理解，加密 / 解密引擎可以是所需的任何长度。例如，对应成本关键的基本应用而言，可使用诸如 8 比特加密 / 解密引擎的较短加密 / 解密。相反，在安全关键的应用中，可使用诸如 128 比特加密

/解密引擎的较长加密/解密引擎。可选择加密/解密引擎来平衡器件的成本、大小和安全性。

[0408] 根据详细的说明书，已清楚本发明的许多特征和优点。因此，权利要求书涵盖落入本发明的真实精神和范围内的本发明的所有这种特征和优点。另外，由于本领域的技术人员将容易想到众多修改形式和变形形式，因此不期望将本发明限于示出和描述的精确构造和操作。因此，所有合适的修改形式和等同形式可被包括在本发明的范围内。

[0409] 尽管已经参照具体实施例例证了本发明，但本领域的技术人员应该清楚，可进行明确落入本发明的范围内的各种变化和修改。本发明应广义地在权利要求书的精神和范围内受到保护。

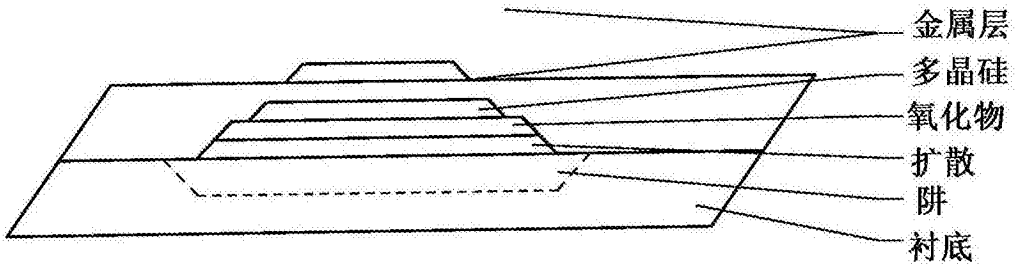


图 1

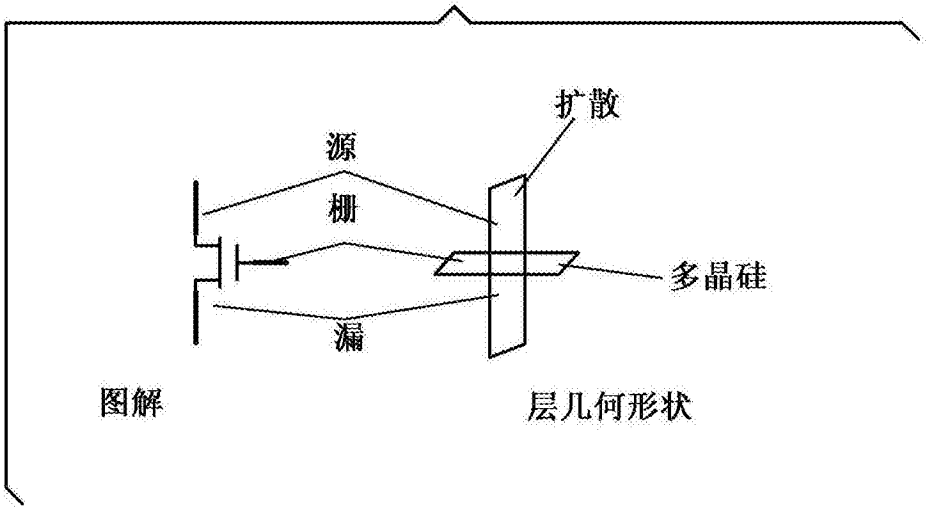


图 2

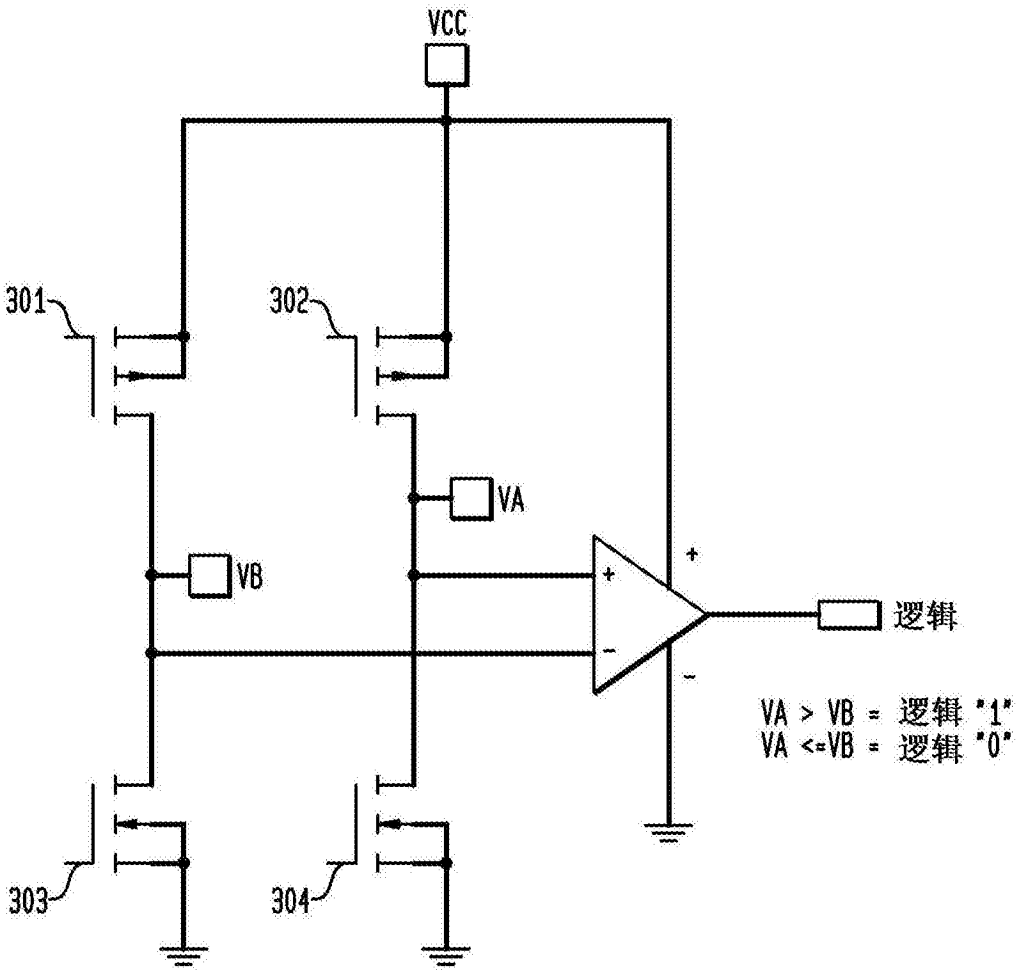


图 3

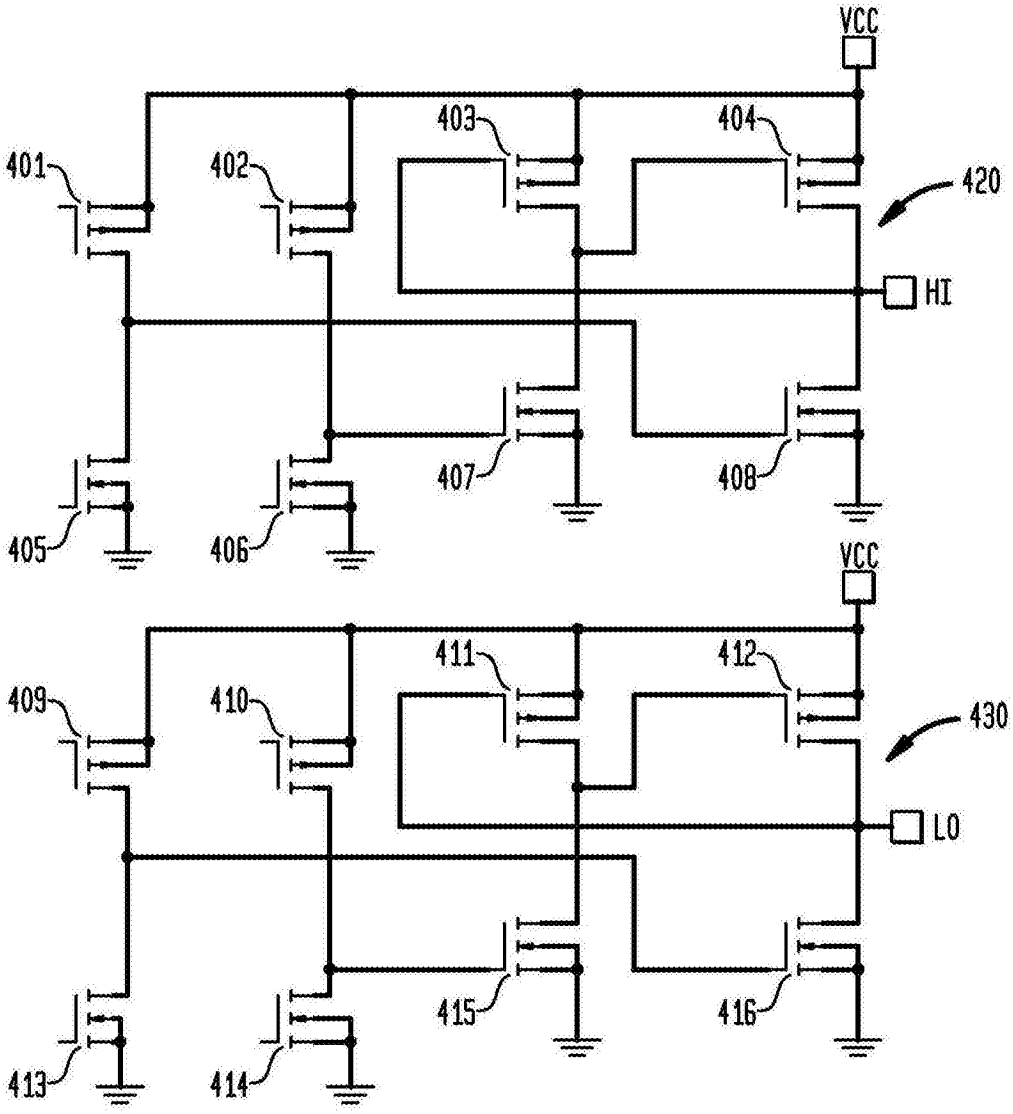

VCC
401
402
403
404
420
HI
405
406
407
408
VCC
409
410
411
412
430
LO
413
414
415
416

图 4

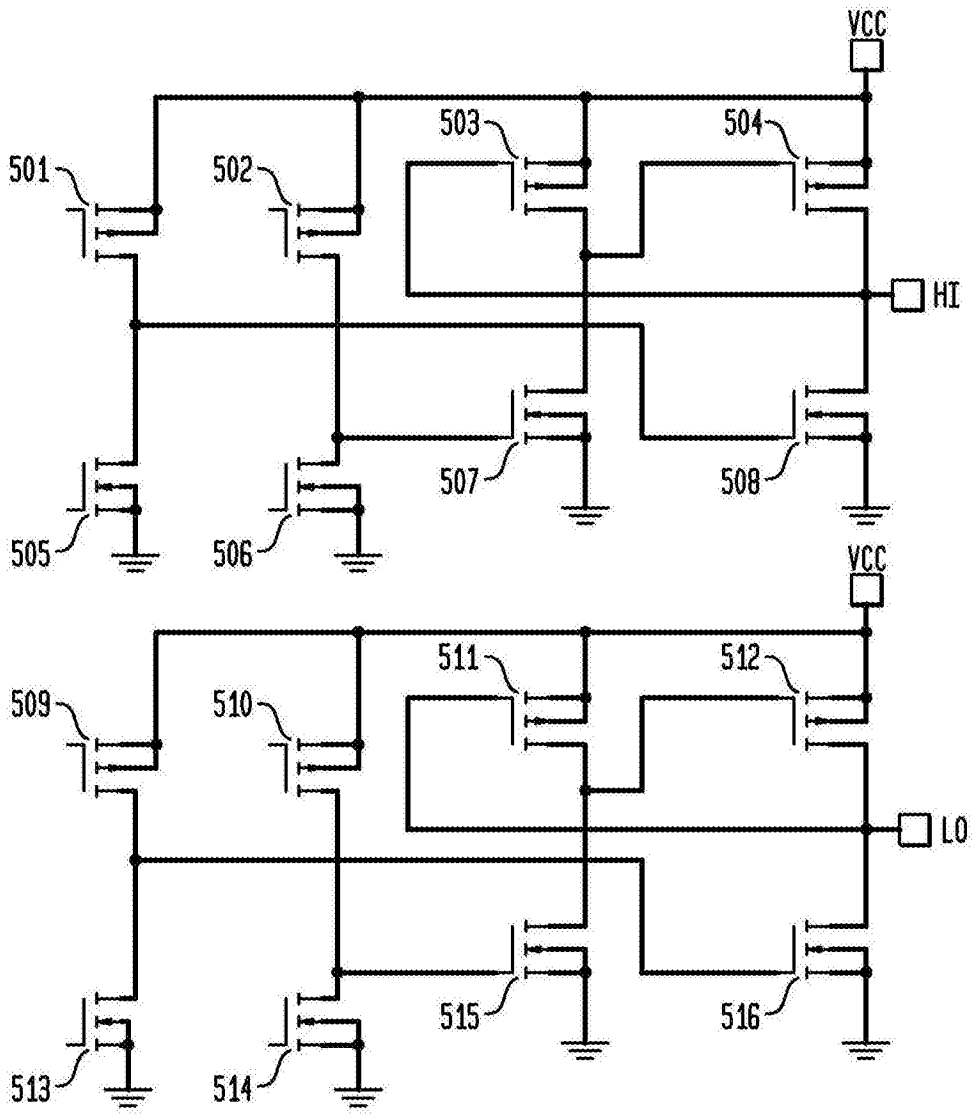

VCC
501
502
503
504
HI
505
506
507
508
VCC
509
510
511
512
LO
513
514
515
516

图 5

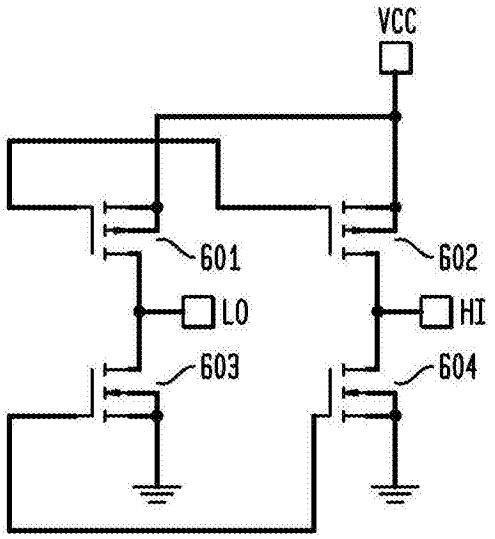

VCC
601
602
LO
HI
603
604

图 6

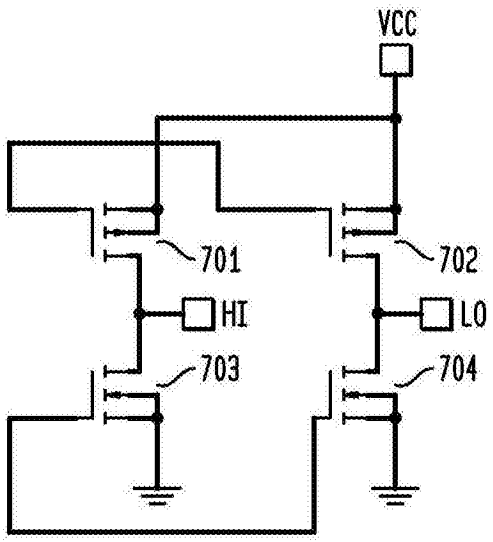

VCC
701
702
HI
LO
703
704

图 7

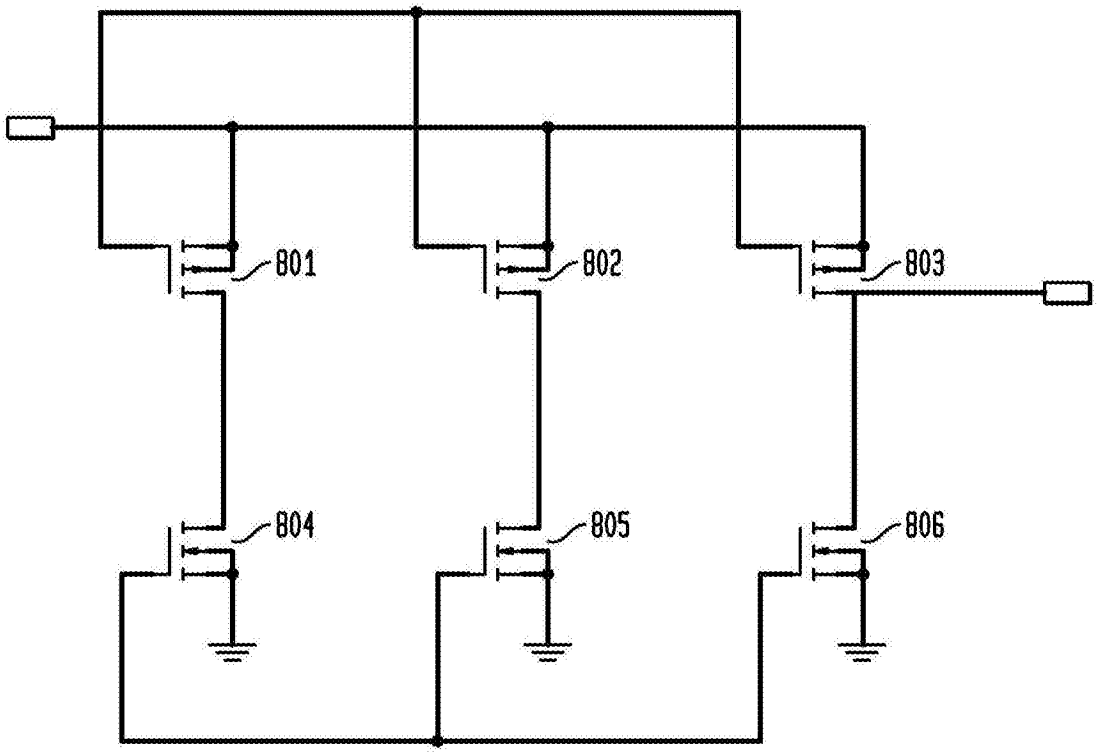

801
802
803
804
805
806

图 8

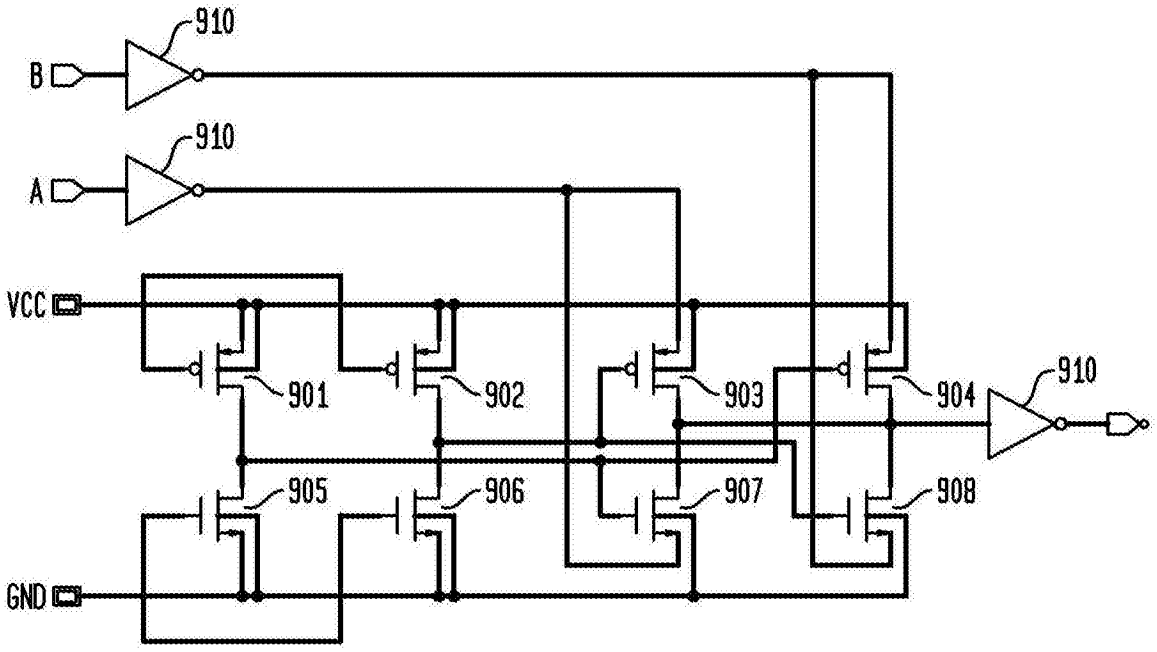

910
B
910
A
VCC
901
902
903
904
910
905
906
907
908
GND

图 9A

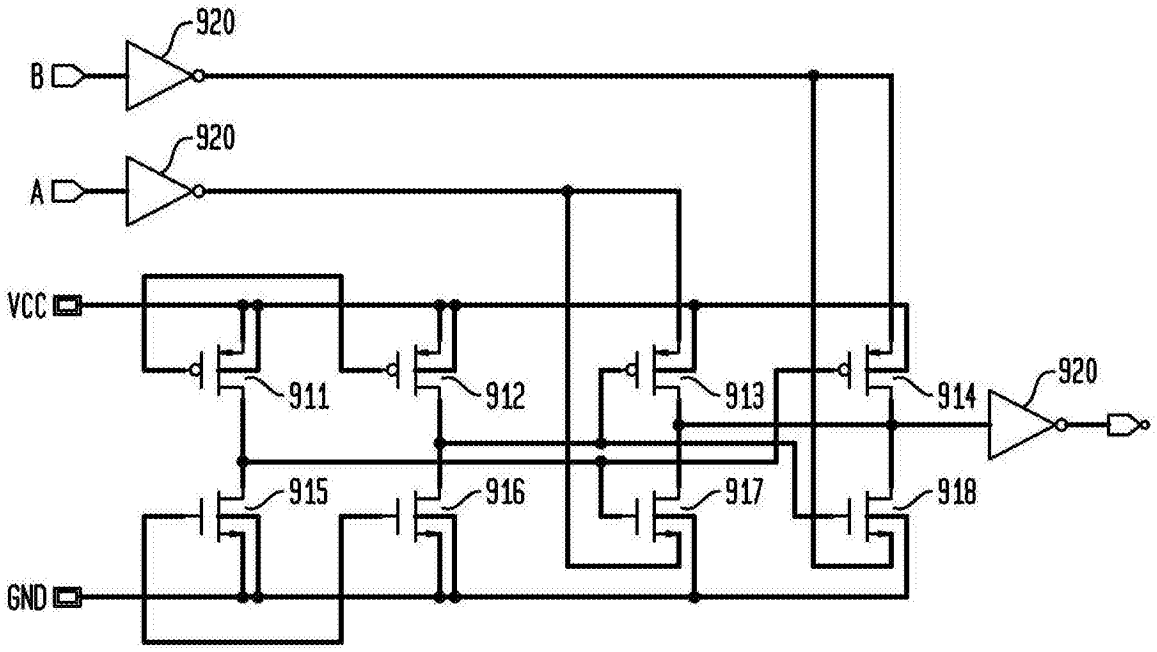

920
B
920
A
VCC
911
912
913
914
920
915
916
917
918
GND

图 9B

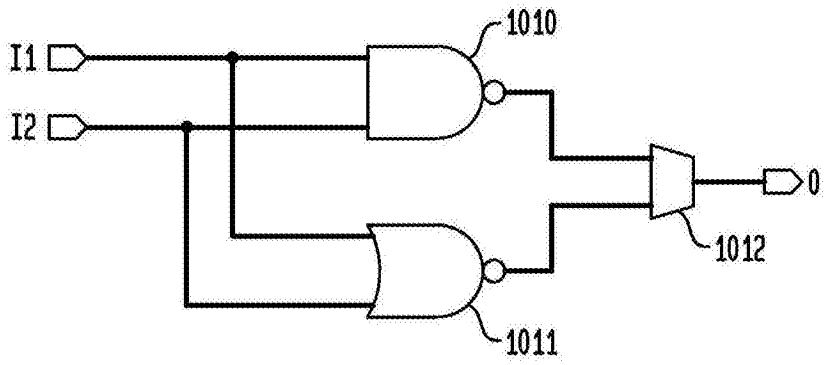


图 10

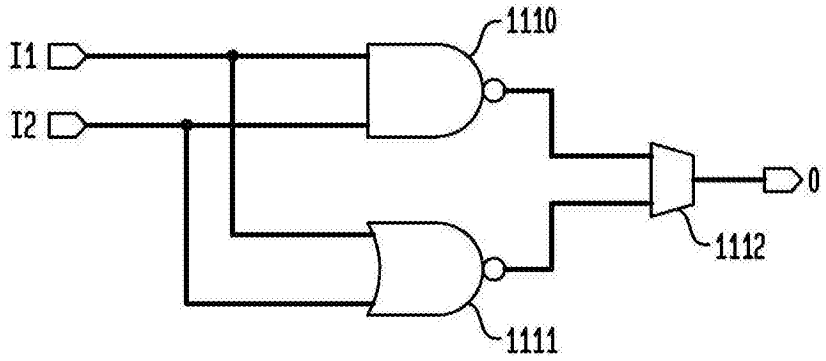


图 11

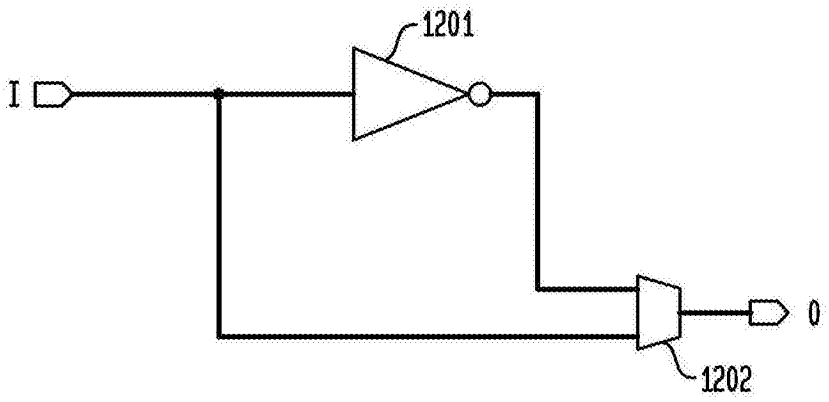


图 12

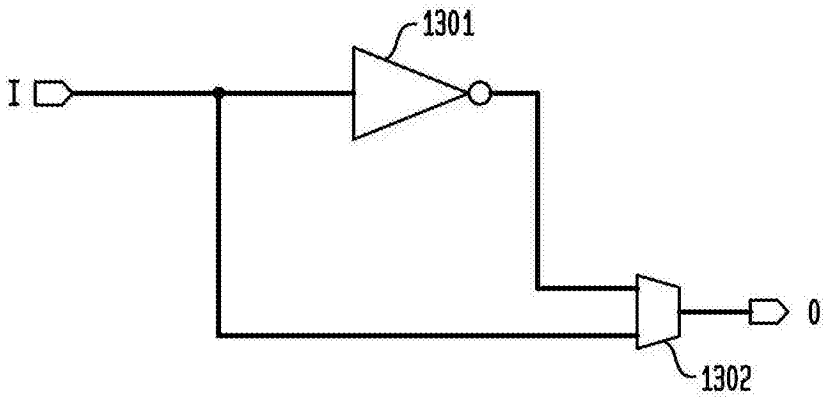


图 13

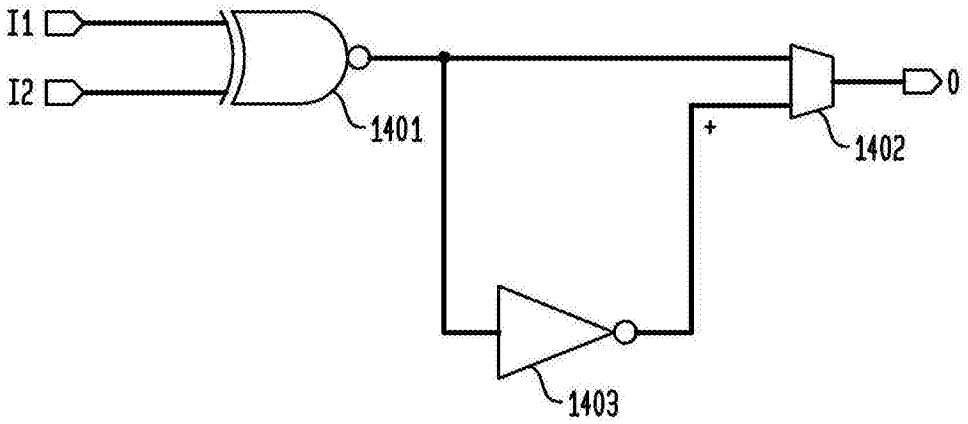


图 14

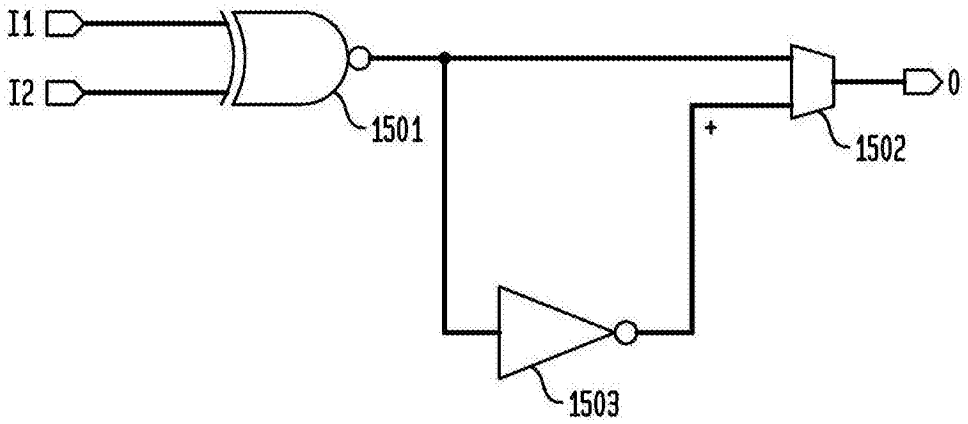


图 15

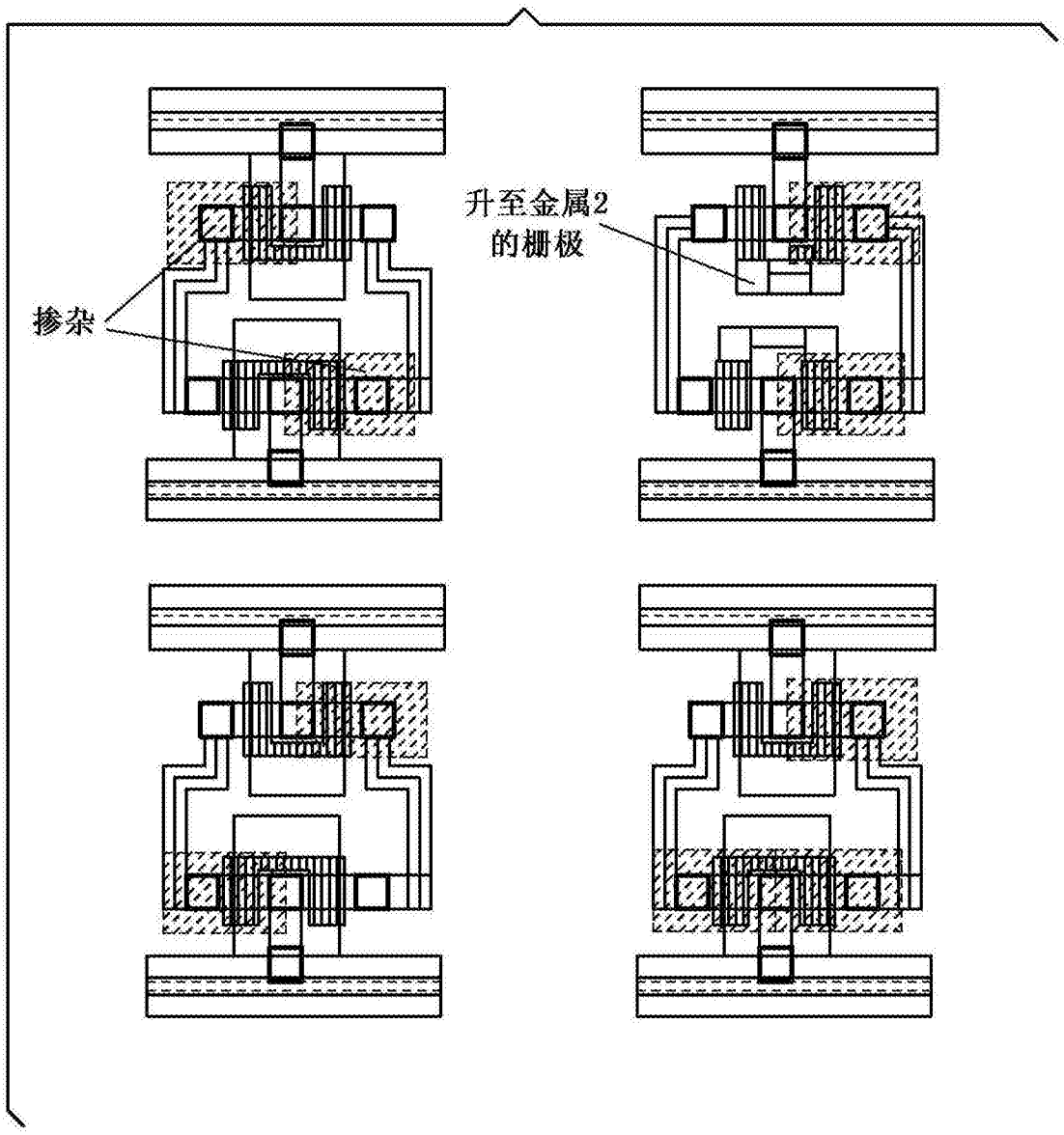


图 16A

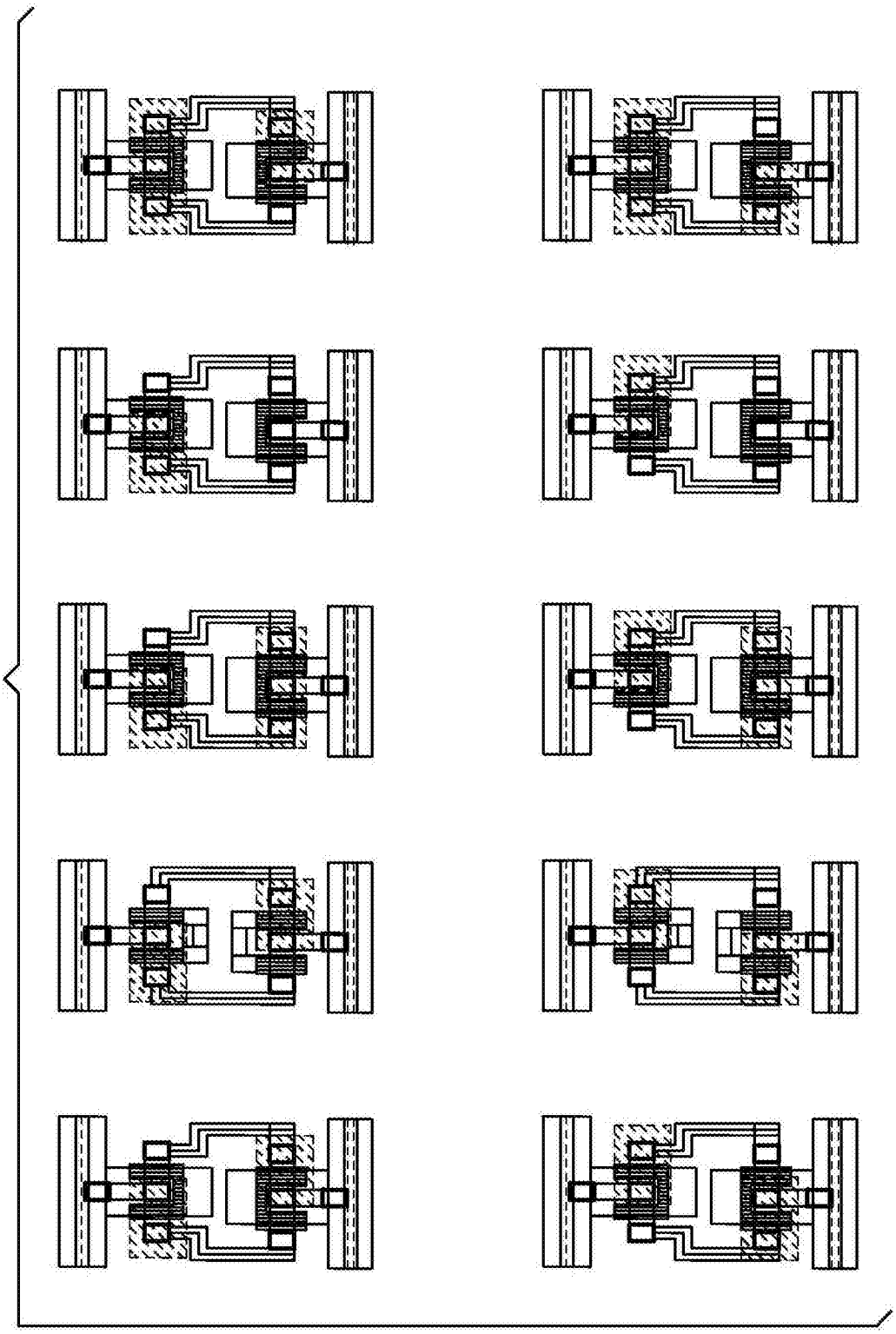


图 16B

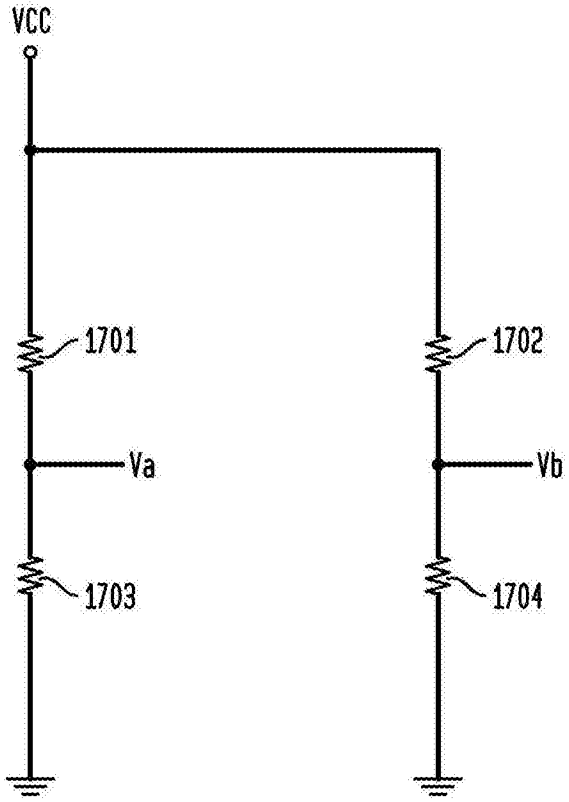


图 17

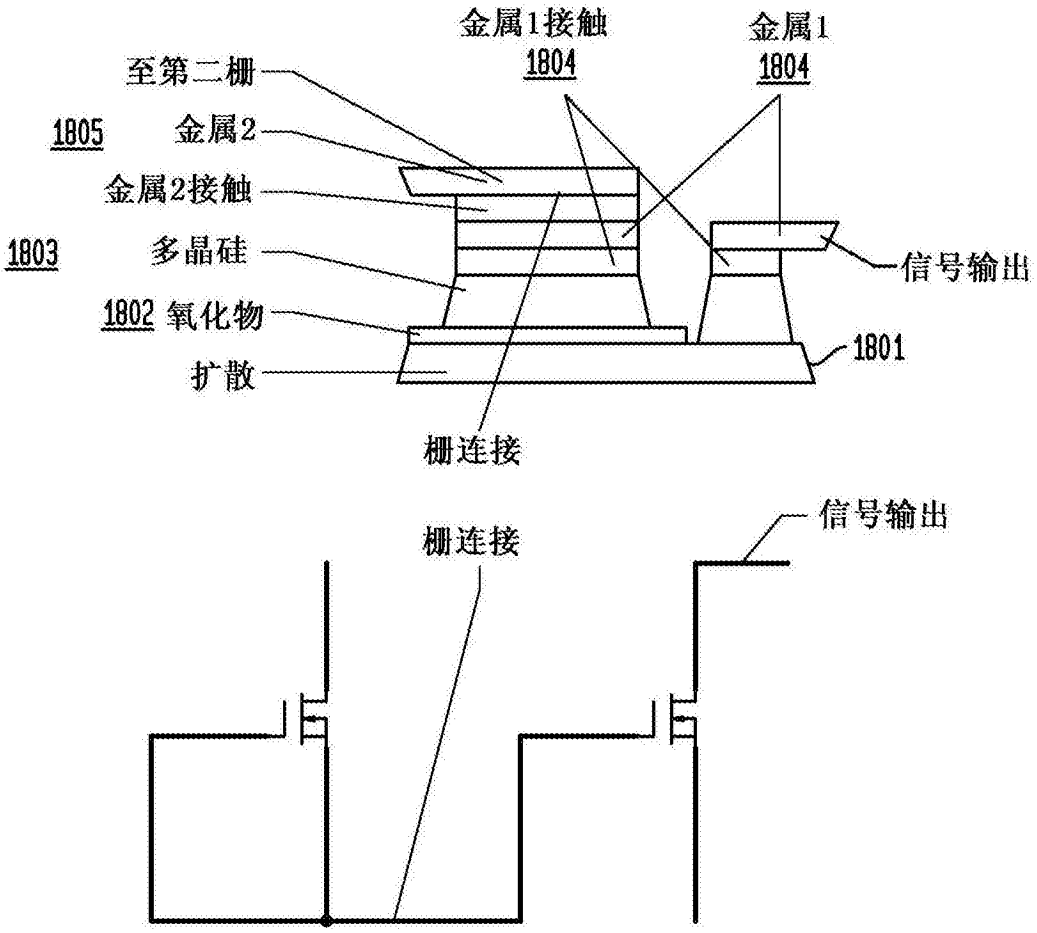

金属1接触
1804
金属1
1804
至第二栅
1805
金属2
金属2接触
1803
多晶硅
1802
氧化物
扩散
信号输出
1801
栅连接
栅连接
信号输出

图 18

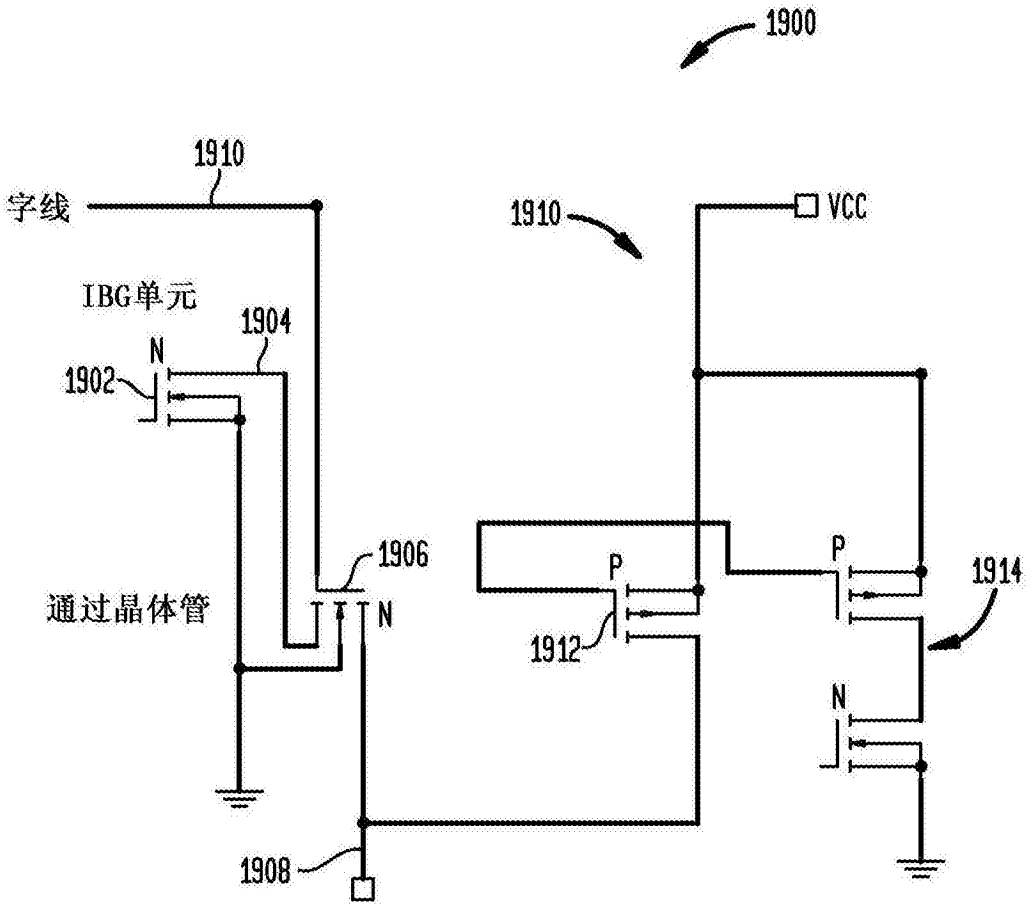

1900
1910
字线
1910
VCC
IBG单元
1904
N
1902
1906
通过晶体管
N
P
P
1914
1912
N
1908

图 19

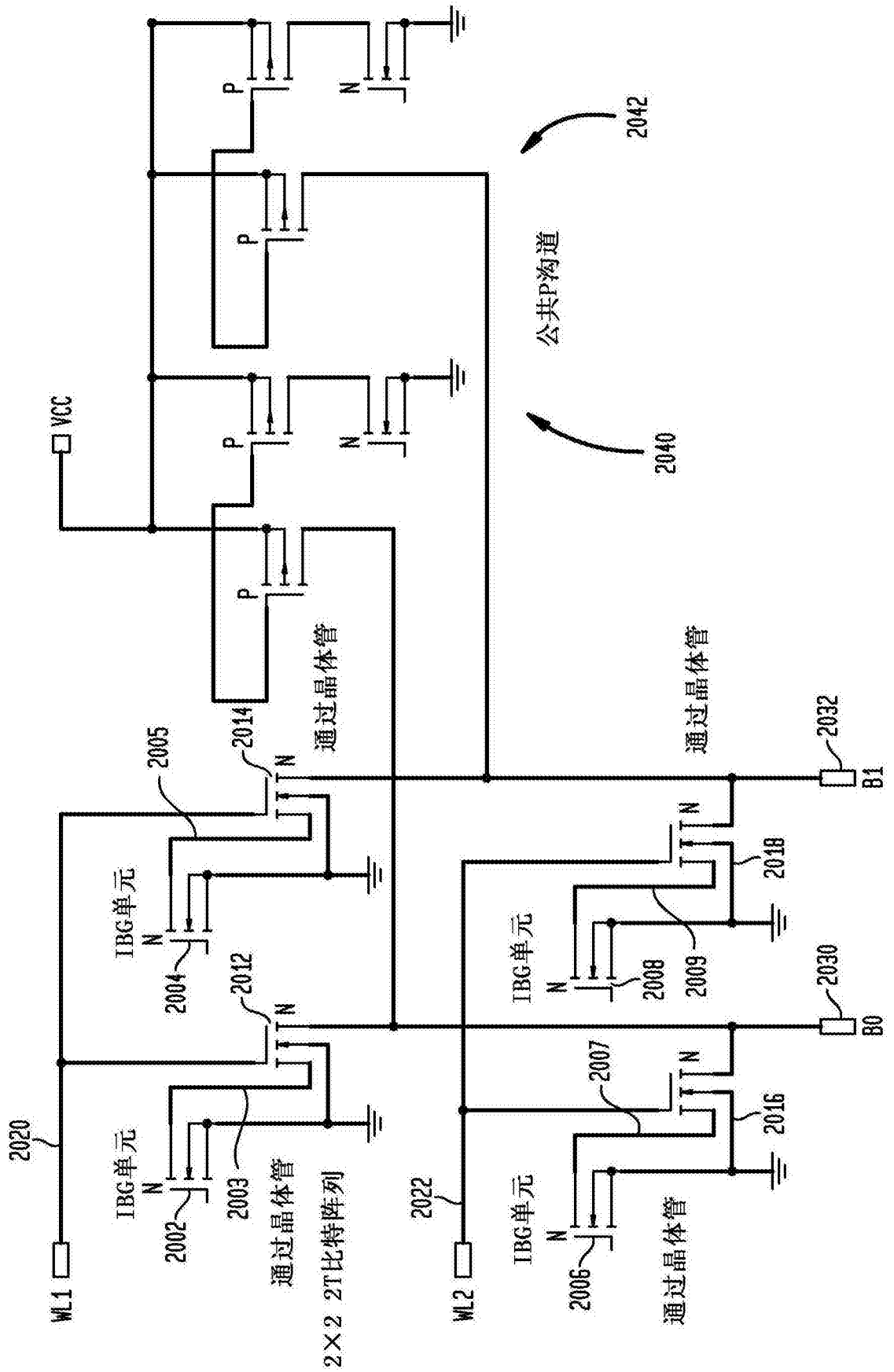

2×2 2T比特阵列
WL1
WL2
2020
2022
VCC
P
N
2042
2040
公共P沟道
通过晶体管
IBG单元
2002
2003
2004
2005
2006
2007
2008
2009
2012
2014
2016
2018
2030
2032
B0
B1

图 20

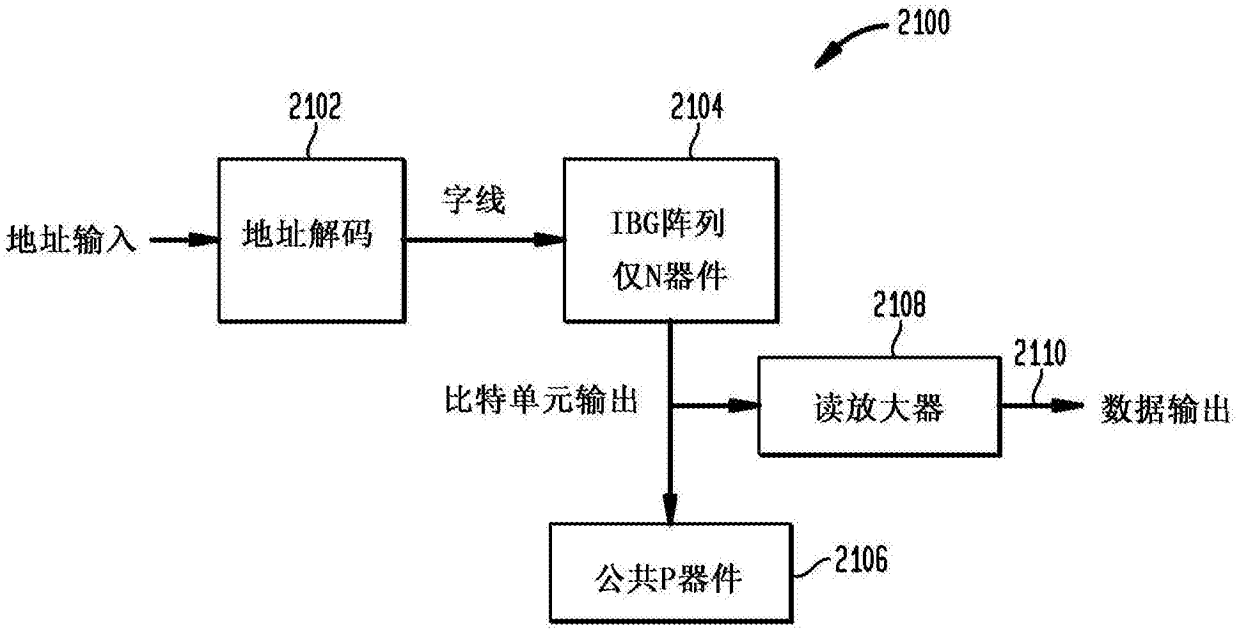

IBG ROM 2T体系结构
2100
2102
2104
地址输入
地址解码
字线
IBG阵列
仅N器件
2108
2110
比特单元输出
读放大器
数据输出
公共P器件
2106

图 21

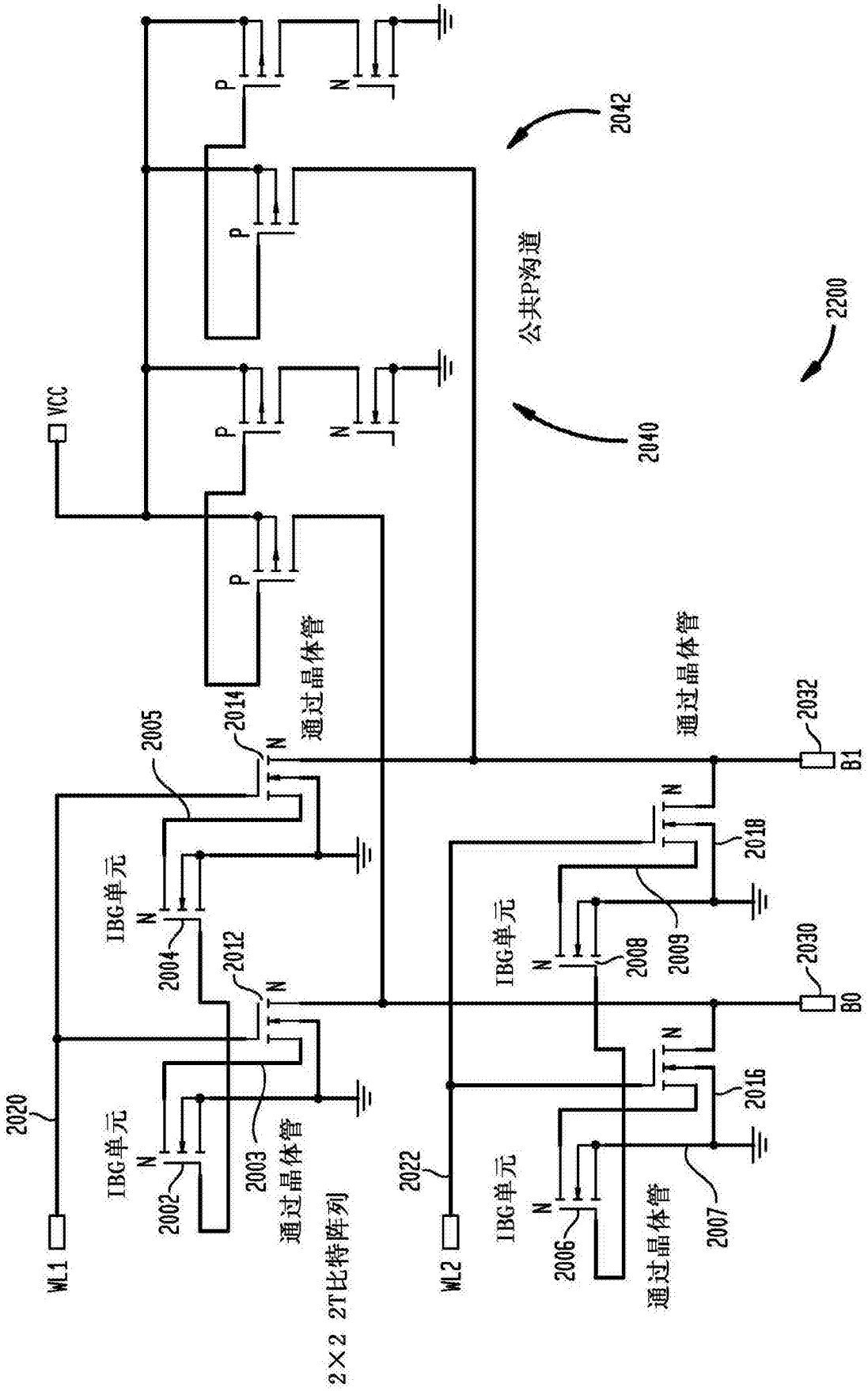

2200
2042
公共P沟道
2040
VCC
P
N
2014
2005
通过晶体管
2032
B1
2018
2030
B0
2016
2020
2022
WL1
WL2
IBG单元
2004
2012
2002
2003
2008
2009
2006
2007
2×2 2T比特阵列

图 22

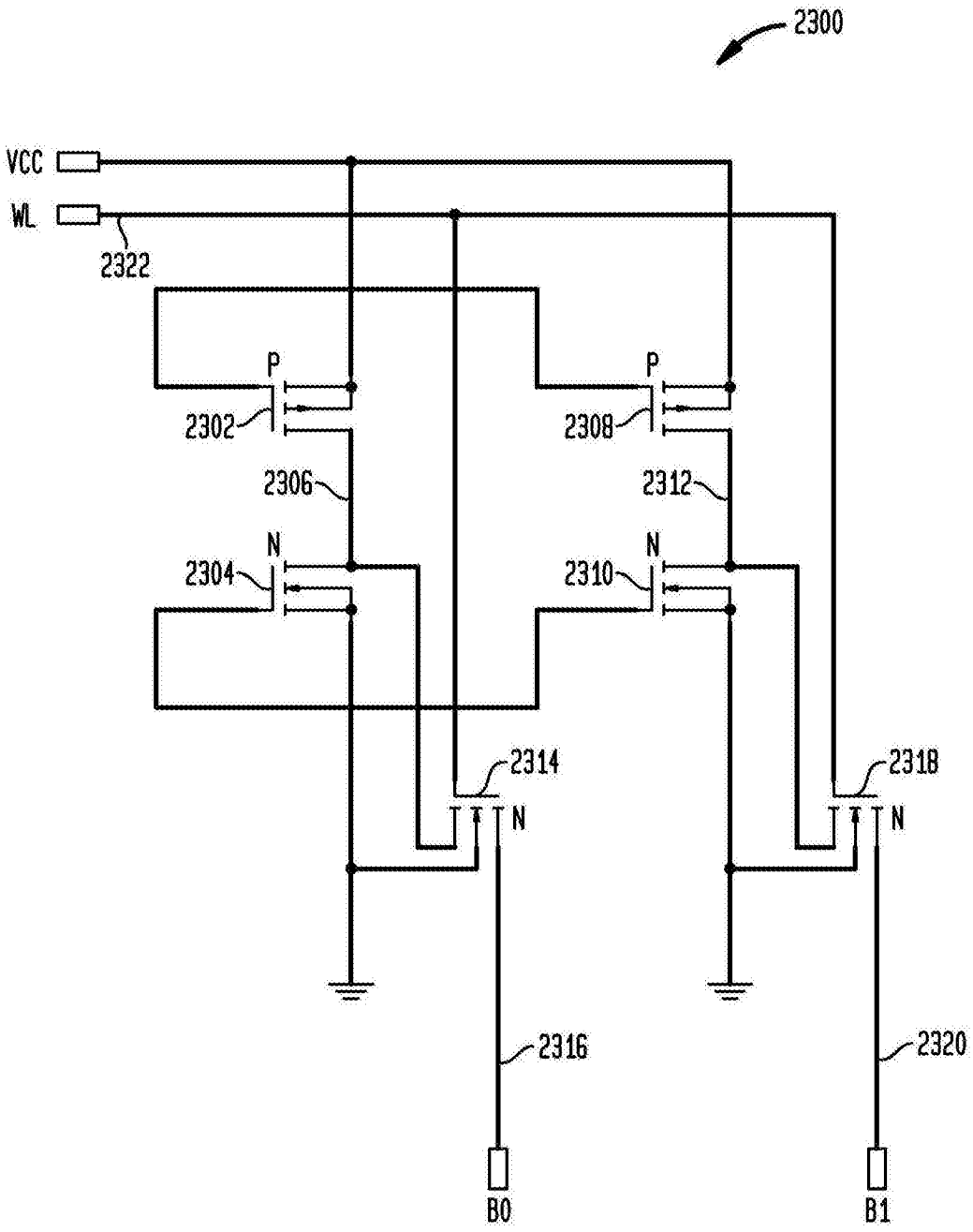

2300
VCC
WL
2322
P
2302
2306
N
2304
P
2308
2312
N
2310
2314
N
2318
N
2316
2320
B0
B1

图 23

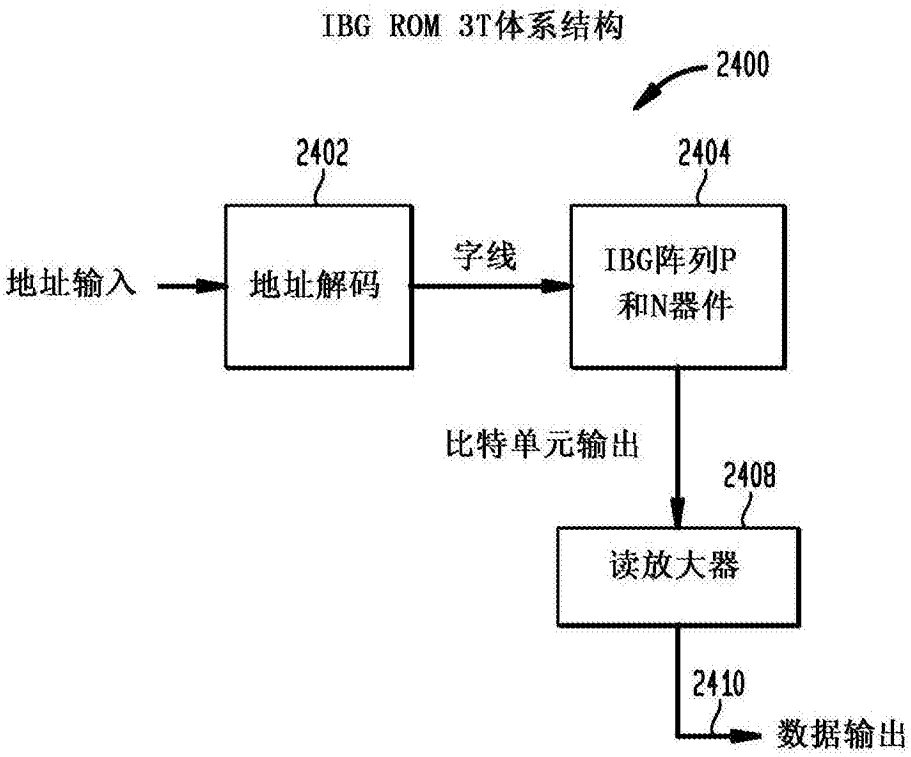

IBG ROM 3T体系结构
2400
2402
2404
地址输入
地址解码
字线
IBG阵列P
和N器件
比特单元输出
2408
读放大器
2410
数据输出

图 24

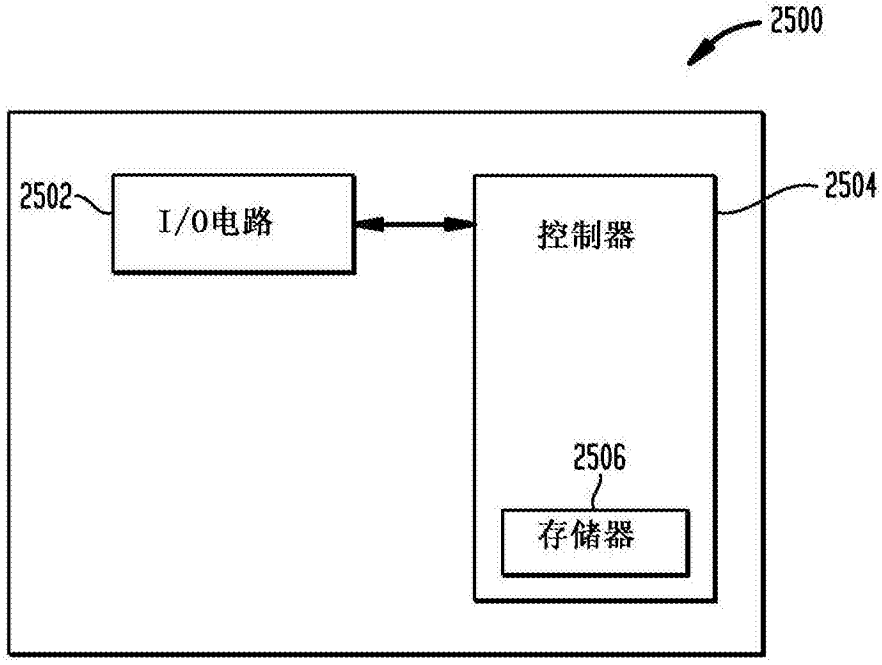

2500
2502
I/O电路
2504
控制器
2506
存储器

图 25

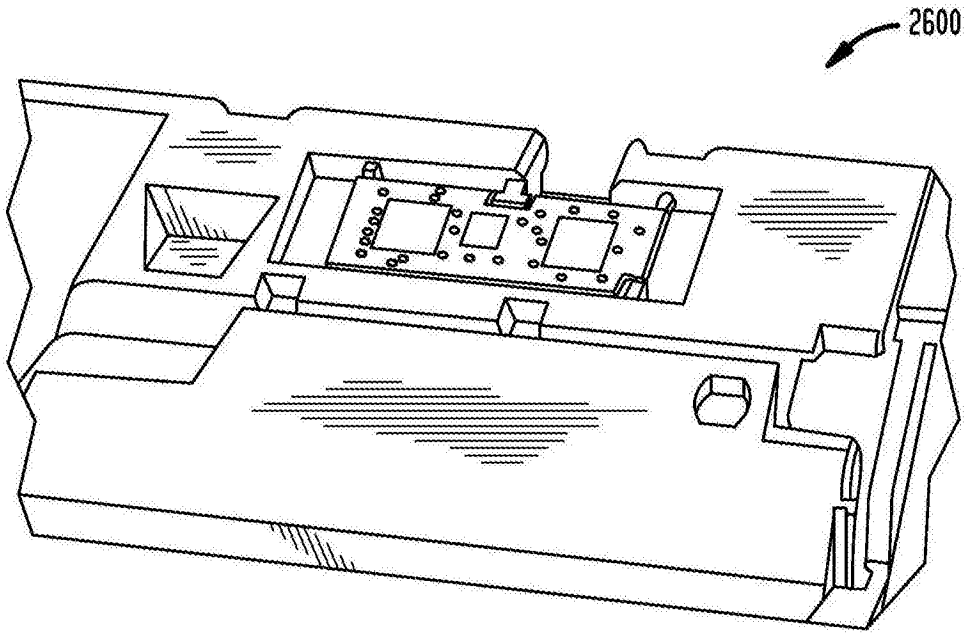


图 26

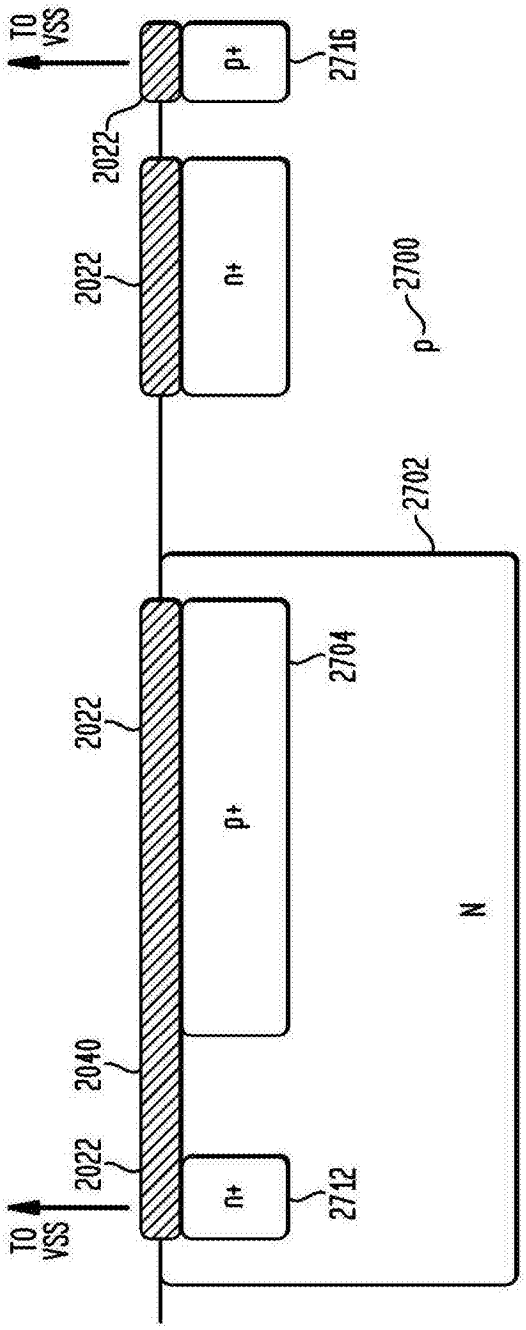

TO VSS
2716
p+
2022
2022
n+
2700
p
2702
2704
2022
p+
N
2040
2022
TO VSS
n+
2712

图 27

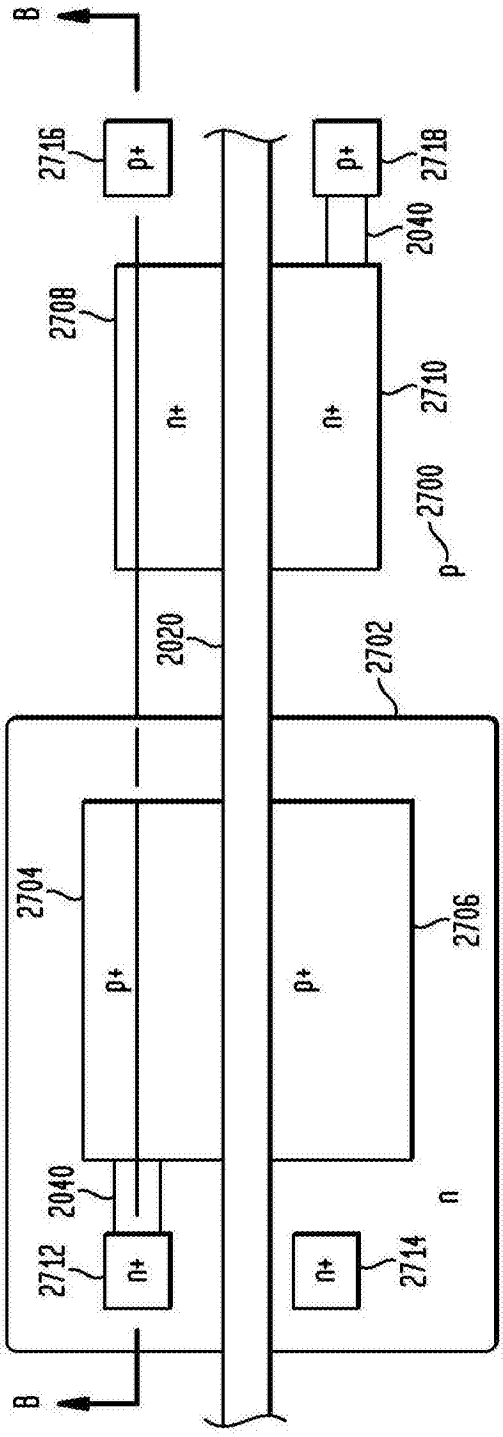

B
2716
p+
2718
p+
2040
2708
n+
n+
2710
2700
p
2020
2702
2704
p+
p+
2706
2040
n
2712
n+
n+
2714
B

图 28

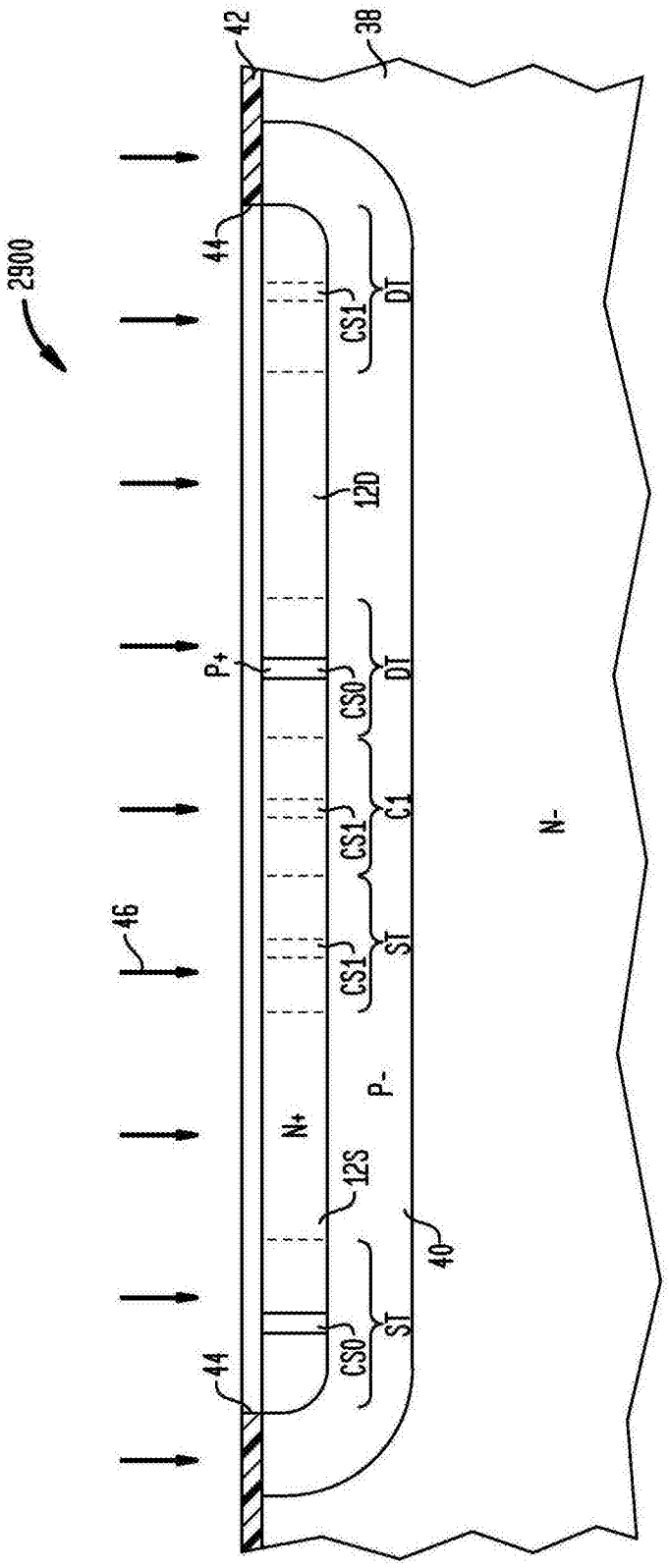

2900
42
38
44
CS1
DT
120
P+
CS0
DT
CS1
C1
N-
46
CS1
ST
P-
N+
120
40
CS0
ST
44

图 29A

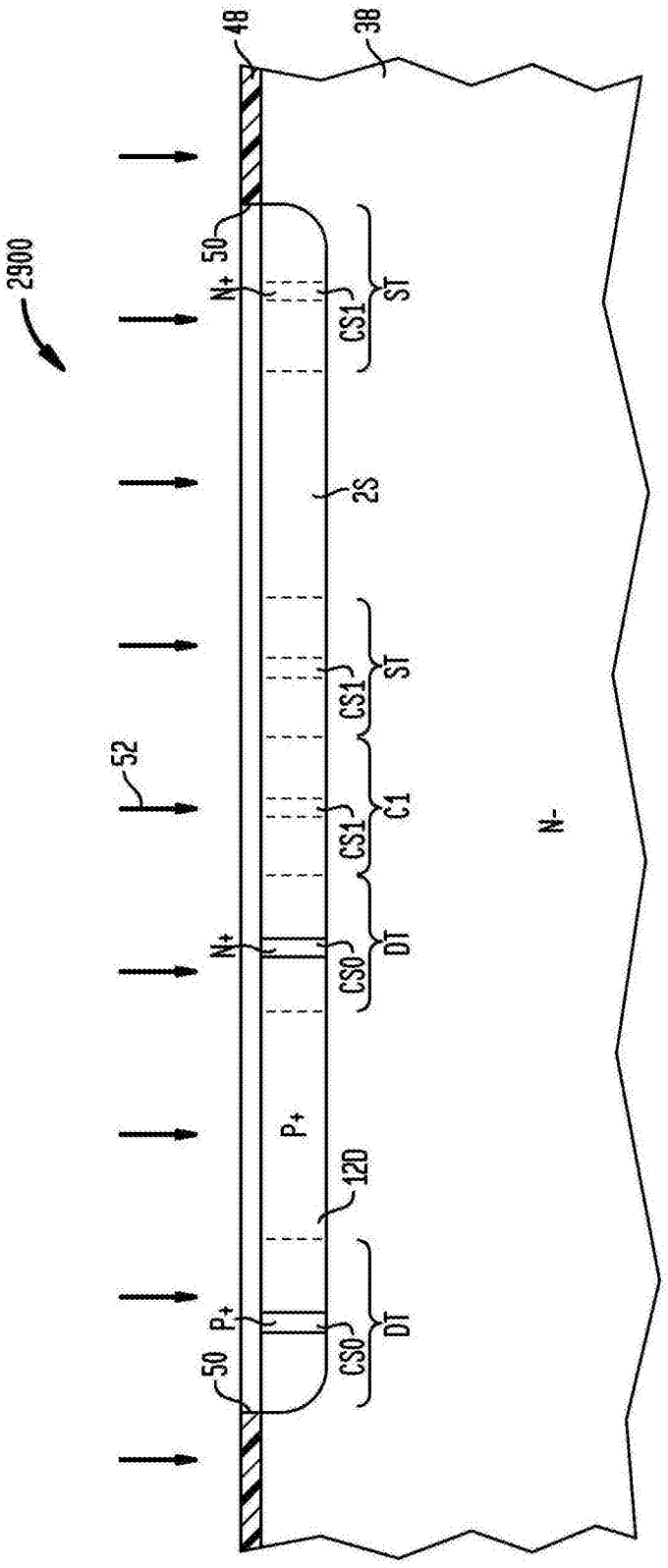

2900
48
38
50
N+
CS1
ST
2S
CS1
ST
52
CS1
C1
CS1
N+
CS0
DT
N-
P+
120
P+
50
CS0
DT

图 29B

具有掩饰的基本逻辑块的逻辑编程

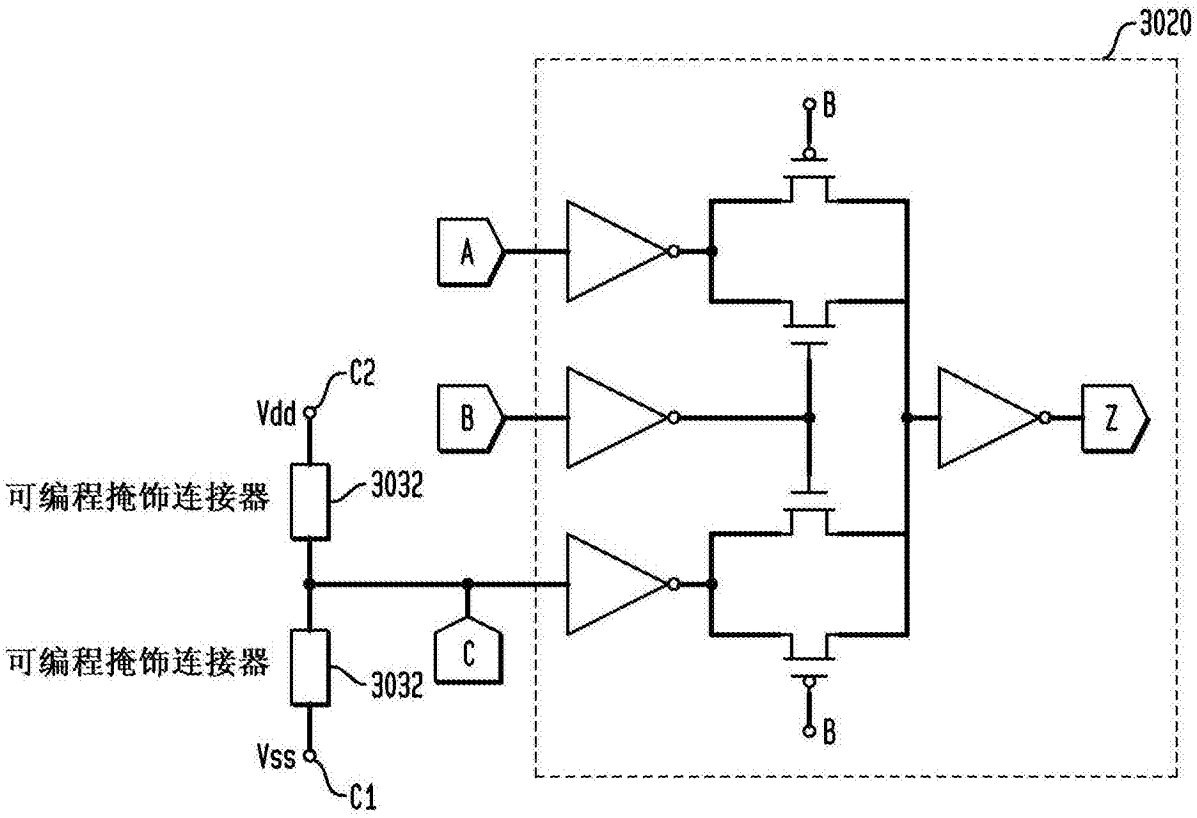
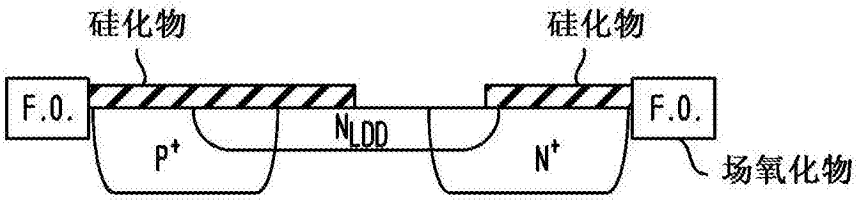


图 30

在以LDD编程的硅中的掩饰连接器

NLDD注入中的连接



NLDD注入中的隔离

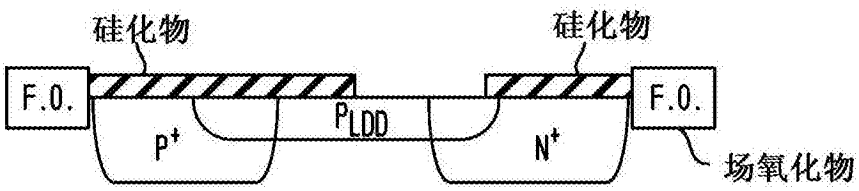


图 31

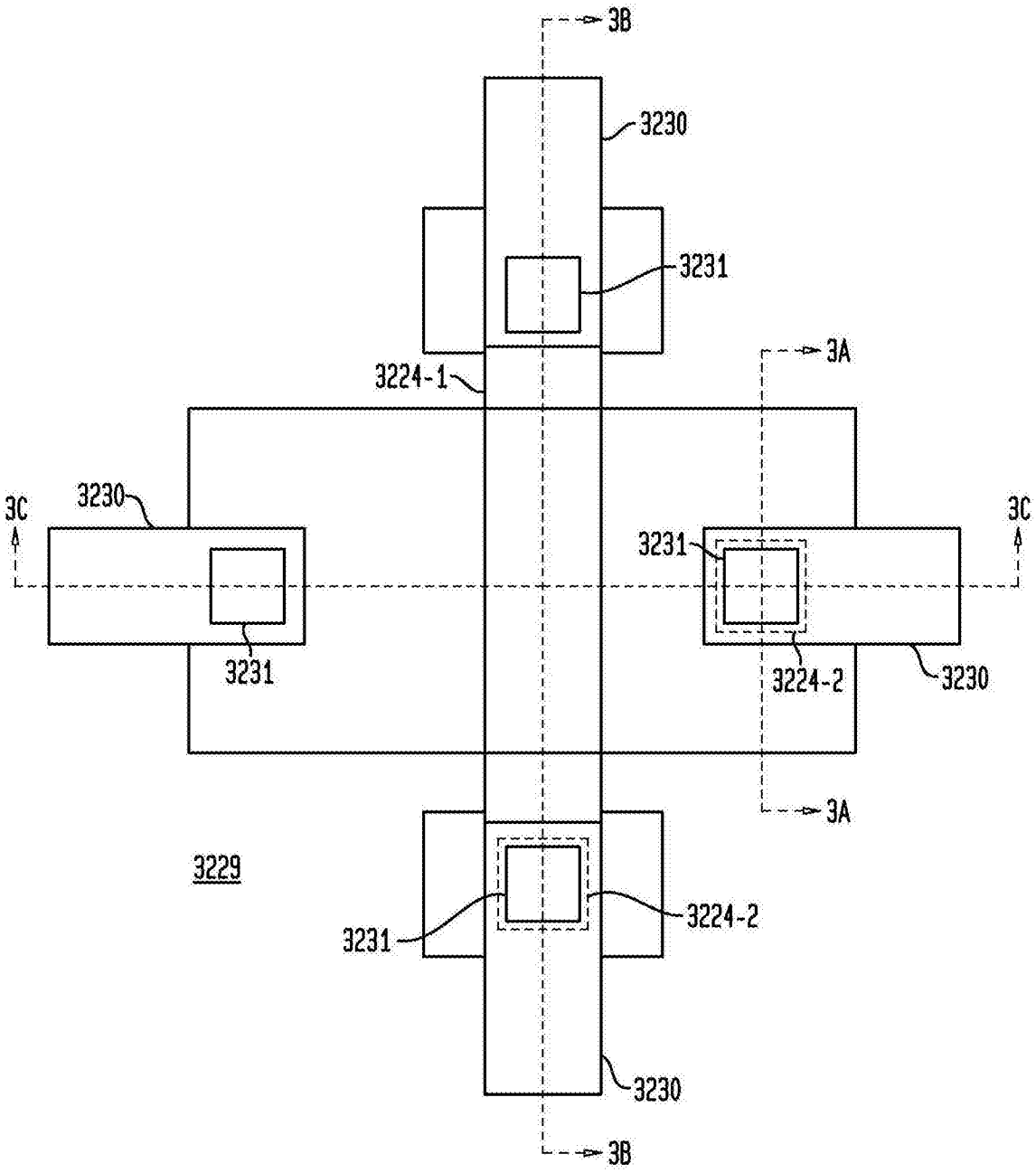

3B
3230
3231
3A
3224-1
3C
3230
3231
3C
3231
3224-2
3230
3A
3229
3231
3224-2
3230
3B

图 32

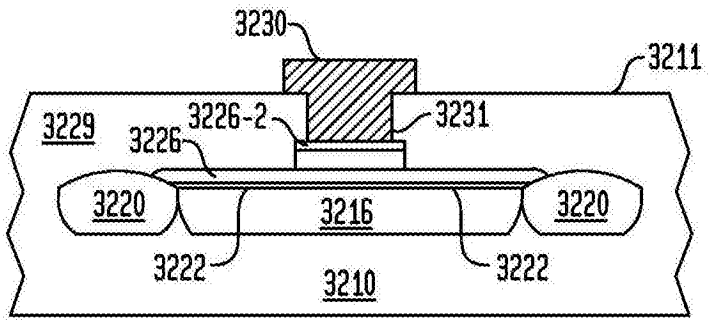


图 32A

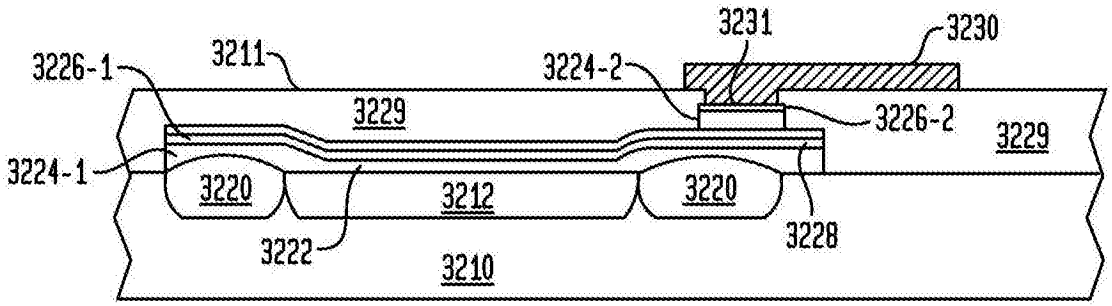


图 32B-1

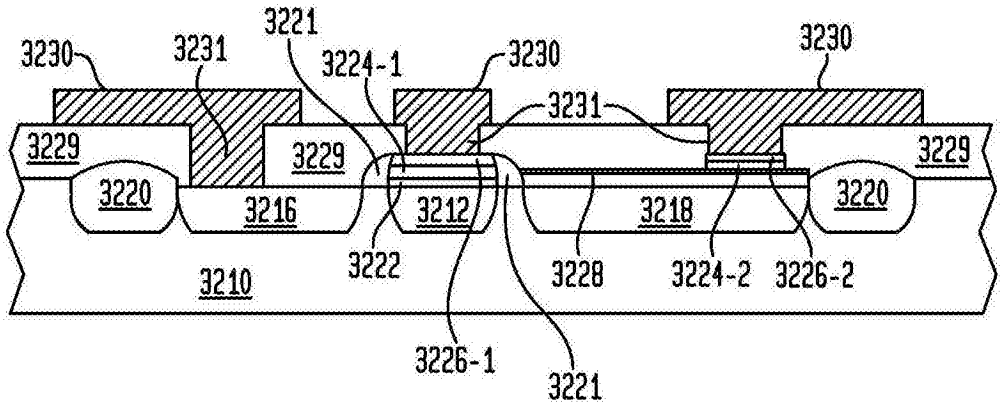
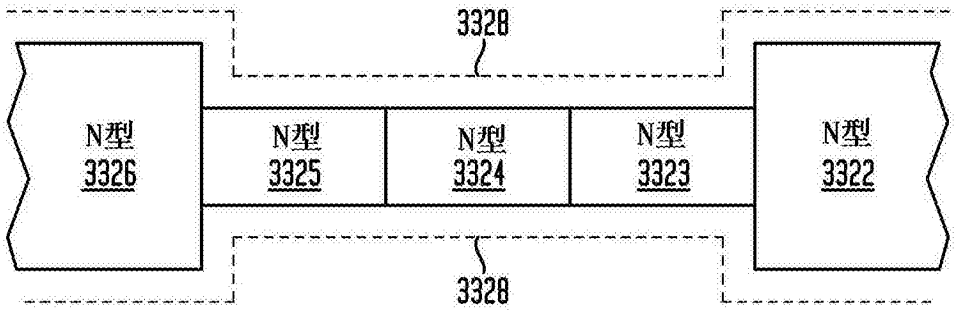
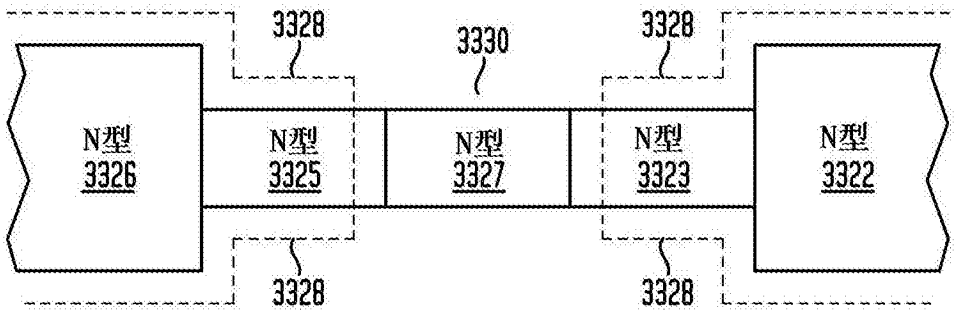


图 32B-2



（现有技术）

图 33A



（现有技术）

图 33B

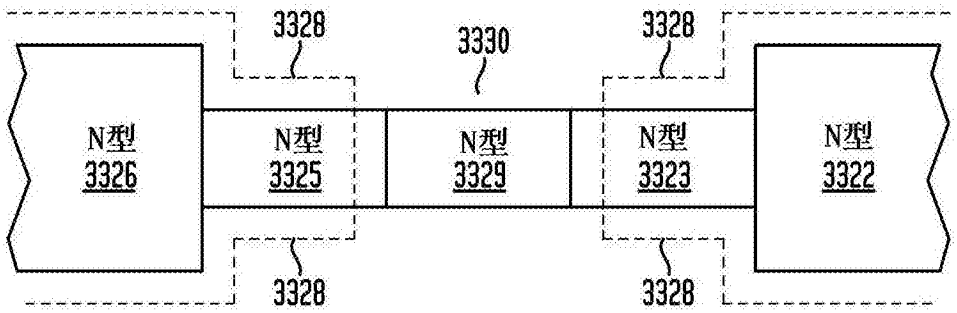


图 34

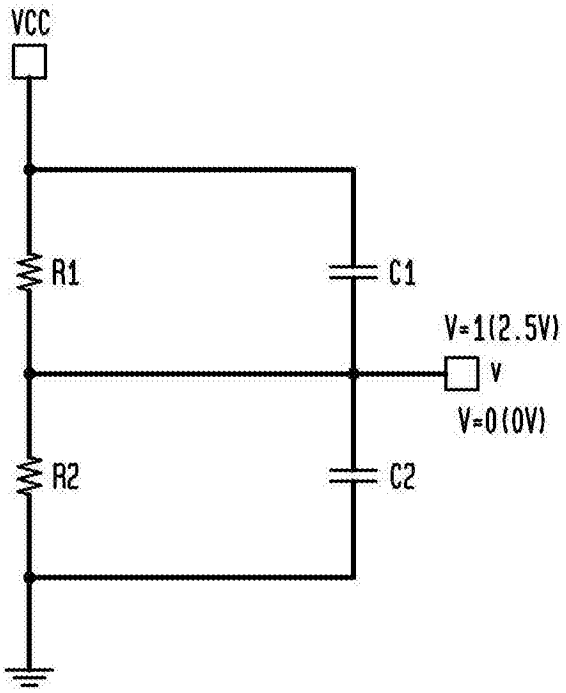


图 35

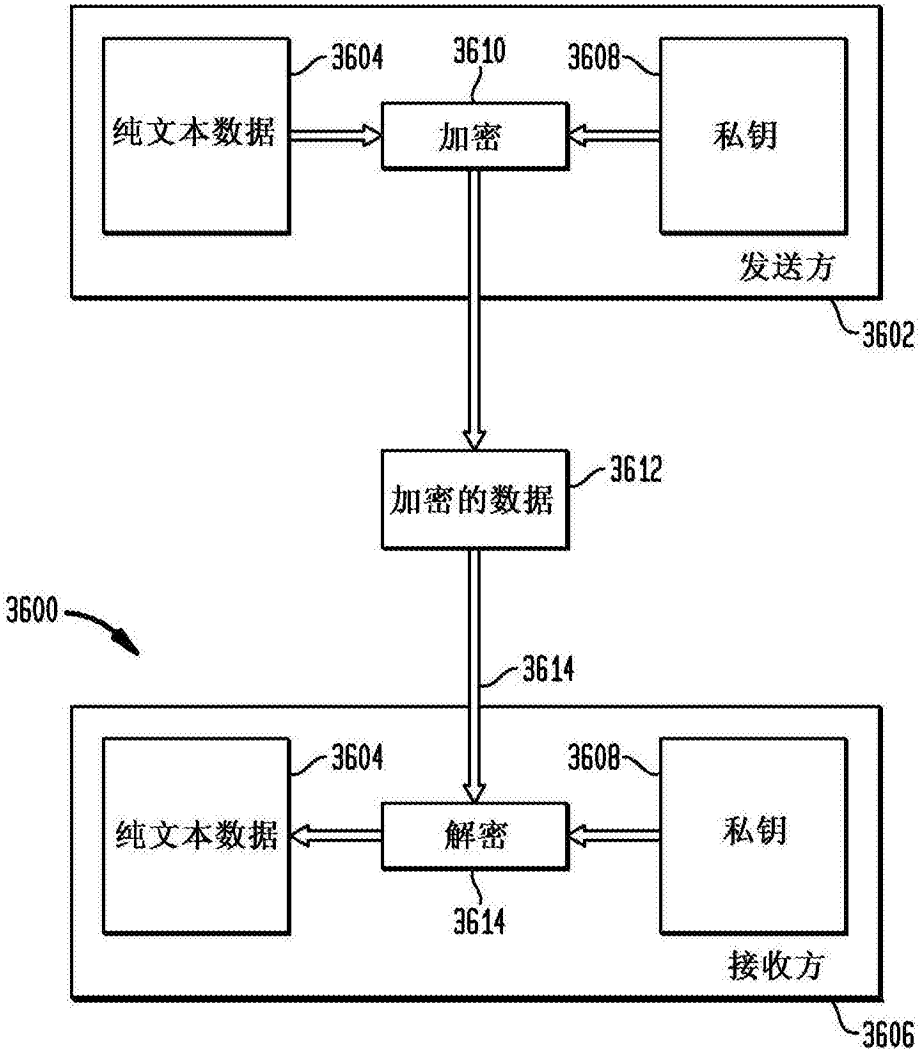

3604
3610
3608
纯文本数据
加密
私钥
发送方
3602
加密的数据
3612
3600
3614
3604
3608
纯文本数据
解密
私钥
3614
接收方
3606

图 36

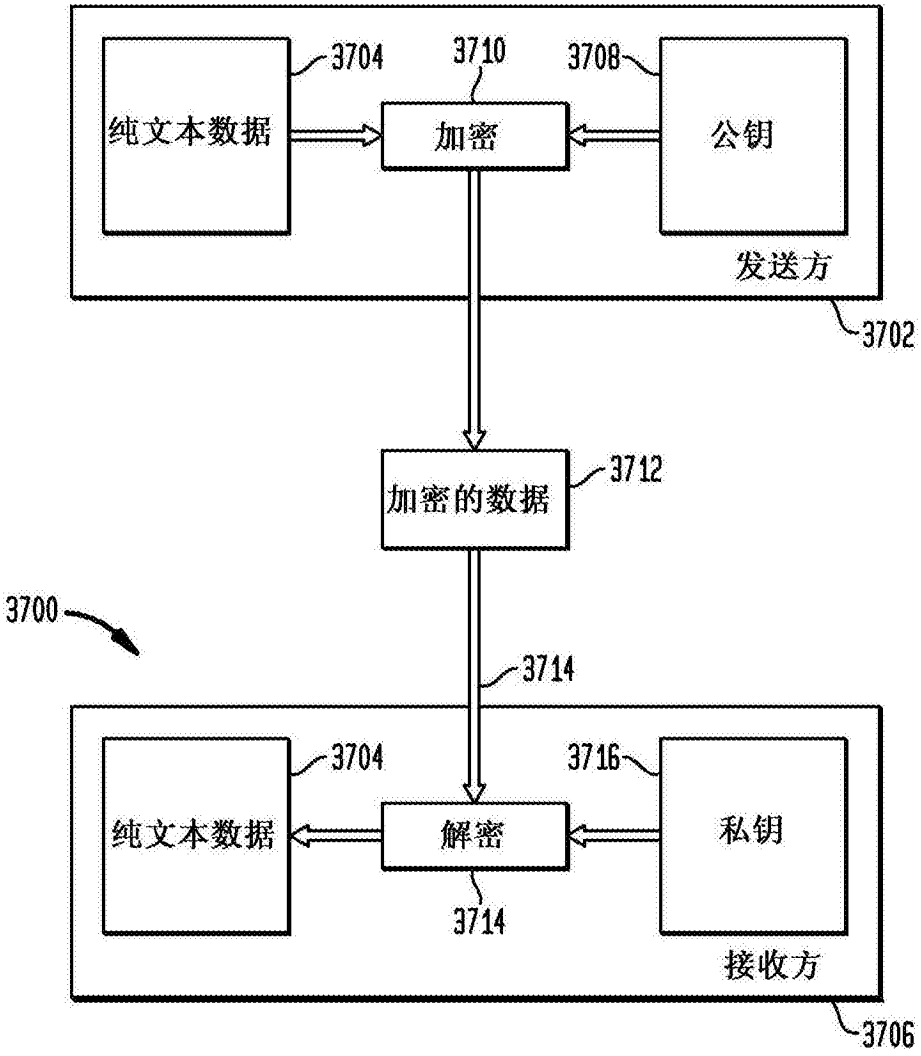

3704
3710
3708
纯文本数据
加密
公钥
发送方
3702
加密的数据
3712
3700
3714
3704
3716
纯文本数据
解密
私钥
3714
接收方
3706

图 37

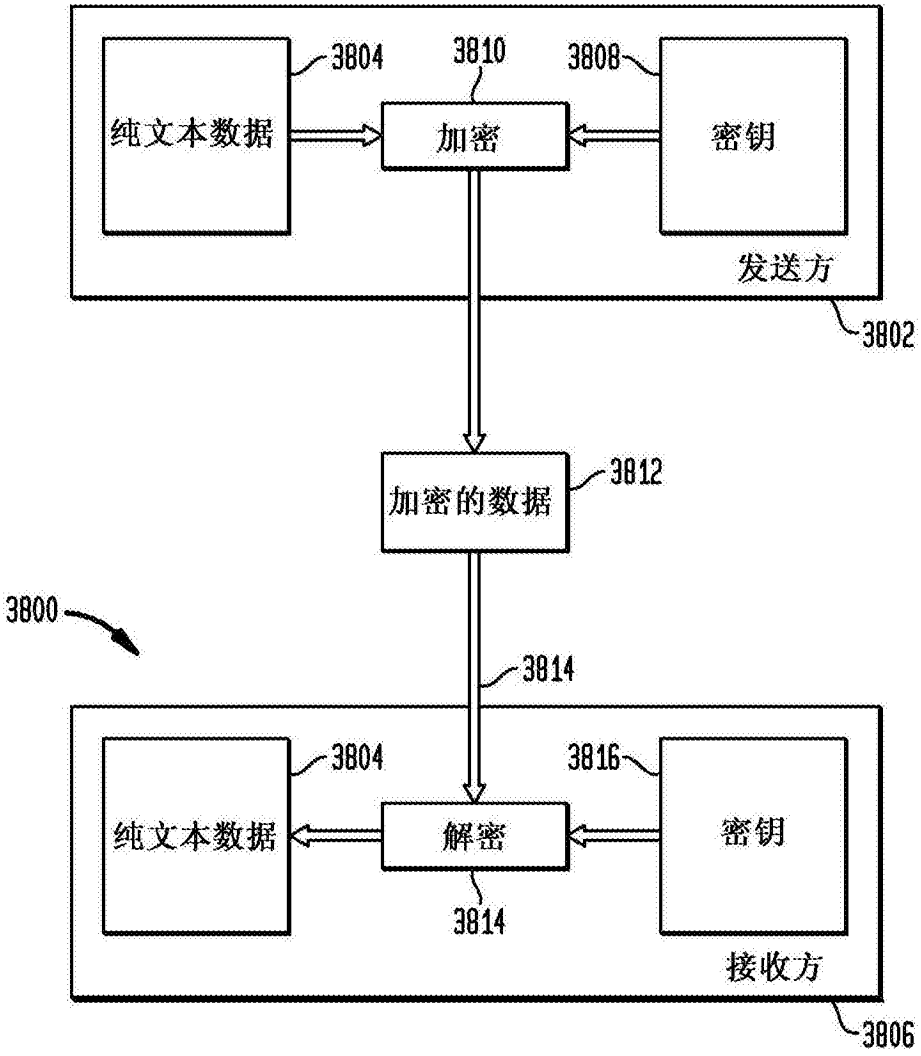

3804
3810
3808
纯文本数据
加密
密钥
发送方
3802
加密的数据
3812
3800
3814
3804
3816
纯文本数据
解密
密钥
3814
接收方
3806

图 38

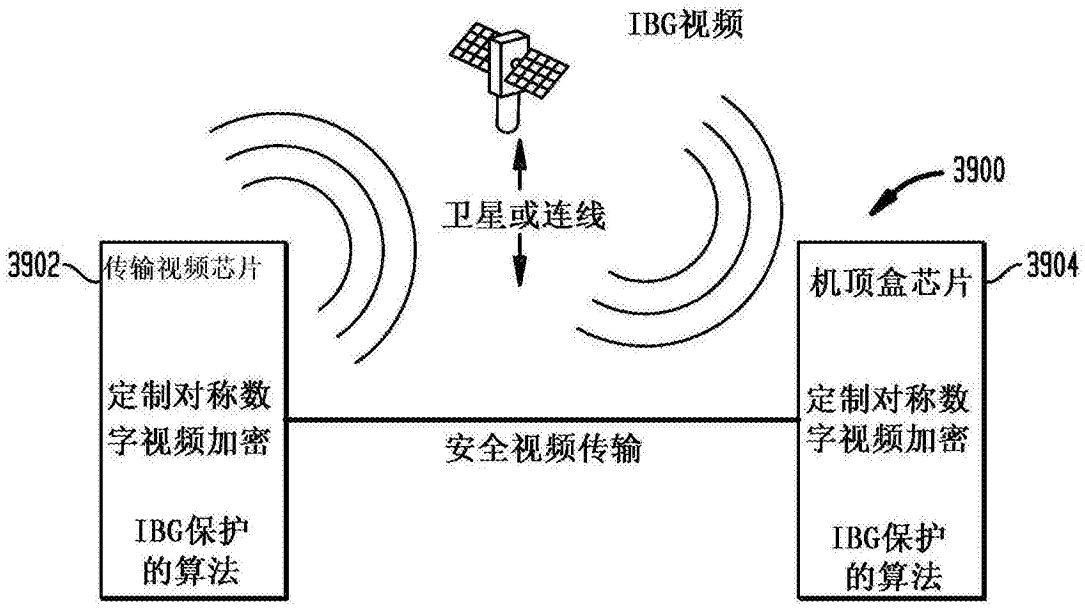

IBG视频
卫星或连线
3900
3902
传输视频芯片
定制对称数字视频加密
IBG保护的算法
安全视频传输
机顶盒芯片
3904
定制对称数字视频加密
IBG保护的算法

图 39

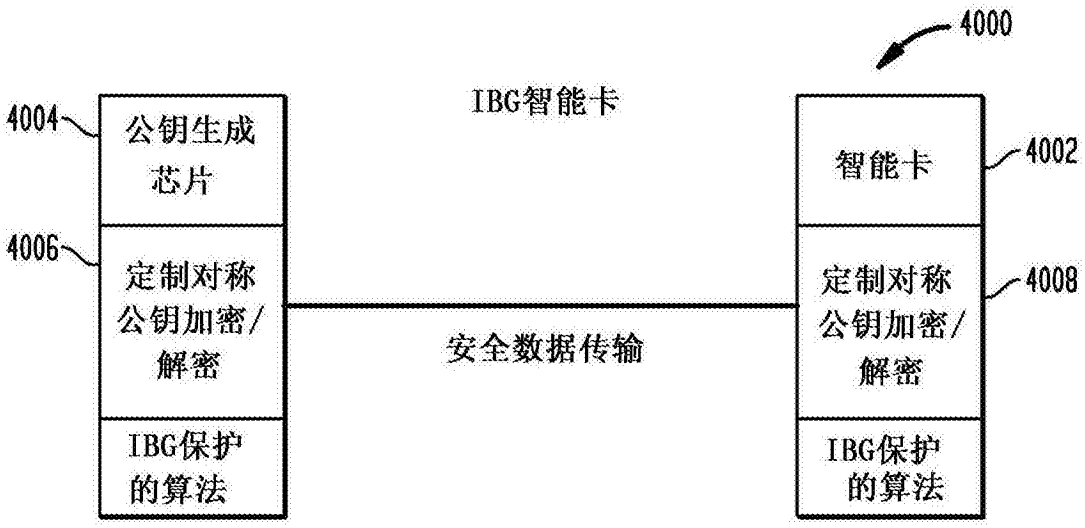

4000
IBG智能卡
4004
公钥生成芯片
4006
定制对称公钥加密/解密
IBG保护的算法
安全数据传输
智能卡
4002
定制对称公钥加密/解密
4008
IBG保护的算法

图 40

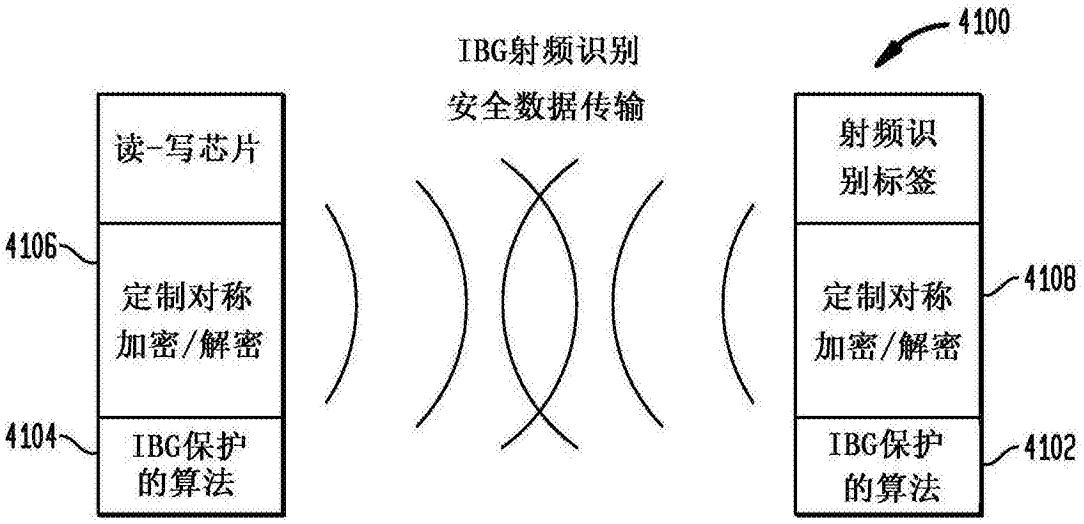

4100
IBG射频识别
安全数据传输
读-写芯片
4106
定制对称
加密/解密
4104
IBG保护
的算法
射频识
别标签
定制对称
加密/解密
4108
IBG保护
的算法
4102

图 41

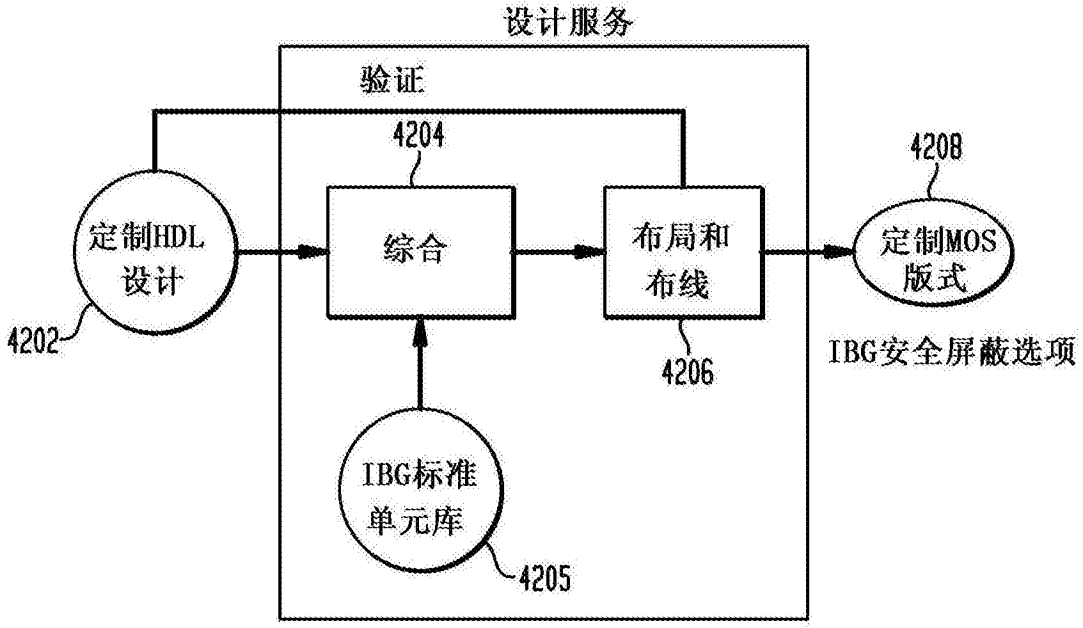

设计服务
验证
4204
定制HDL
设计
4202
综合
布局和
布线
4206
4208
定制MOS
版式
IBG安全屏蔽选项
IBG标准
单元库
4205

图 42

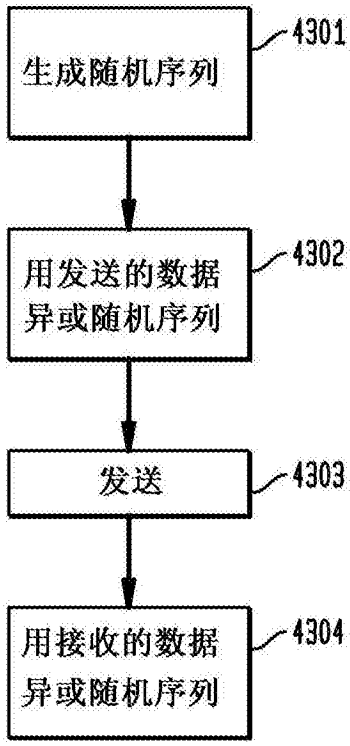


图 43