



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 00811708.X

[45] 授权公告日 2005 年 5 月 4 日

[11] 授权公告号 CN 1200393C

[22] 申请日 2000.8.17 [21] 申请号 00811708.X

[30] 优先权

[32] 1999.8.17 [33] DE [31] 19938890.3

[86] 国际申请 PCT/DE2000/002792 2000.8.17

[87] 国际公布 WO2001/013330 德 2001.2.22

[85] 进入国家阶段日期 2002.2.10

[71] 专利权人 因芬尼昂技术股份公司

地址 德国慕尼黑

[72] 发明人 A·韦德尔

审查员 田 竞

[74] 专利代理机构 中国专利代理(香港)有限公司

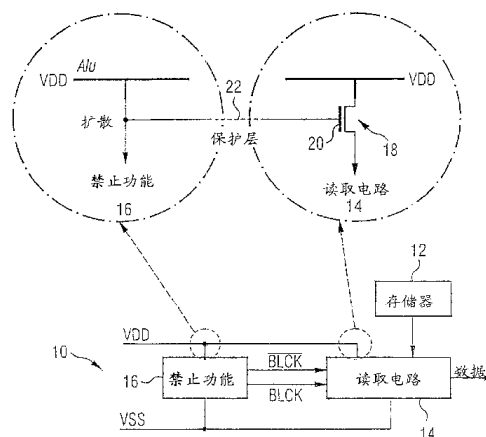
代理人 程天正 张志醒

权利要求书 1 页 说明书 6 页 附图 1 页

[54] 发明名称 集成电路和用于给集成电路供电的电路装置

[57] 摘要

具有数据输出电路和访问控制电路(14, 16)的、用于处理安全性较重要的数据的集成电路, 其中, 安全性较重要的部分(14)的供电通过一个或多个开关(18)进行控制, 当所述访问控制电路(16)的供电被干扰时, 所述的开关被断开。



1. 用于给集成电路的安全性较重要的部分(14)提供供电的电路装置, 所述安全性较重要的部分由相应的访问控制电路(16)进行保护, 其特征在于:

5 所述安全性较重要的部分(14)的供电通过一个或多个开关(18)进行控制, 当所述访问控制电路(16)的供电被干扰时, 所述的开关被断开。

2. 如权利要求 1 所述的电路装置, 其特征在于:

10 在所述的供电 V_{DD} 和所述安全性较重要的部分(14)的供电之间布置了 NMOS 开关(18), 该开关的门极(20)通过在扩散层或在保护层中输送的线路(22)而被连接到所述访问控制电路(16)的 V_{DD} 供电上。

3. 具有数据输出电路(14)和访问控制电路(16)的、用于处理安全性较重要的数据的集成电路, 其特征在于:

15 所述访问控制电路(16)的供电干扰将导致禁止所述的数据输出电路(14)。

4. 如权利要求 3 所述的集成电路, 其特征在于:

 由所述的访问控制电路(16)产生总是成对地倒相的禁止信号($BLCK, \overline{BLCK}$), 只有当两个倒相的禁止信号($BLCK, \overline{BLCK}$)指示取消禁止时, 所述的数据输出电路(14)才工作。

20 5. 如权利要求 4 所述的集成电路, 其特征在于:

 所述相互倒相的禁止信号($BLCK, \overline{BLCK}$)并行地、且优选为相叠地在所述的集成电路内输送。

6. 如权利要求 4 或 5 所述的集成电路, 其特征在于:

 所述的禁止信号($BLCK, \overline{BLCK}$)在扩散层或保护层内输送。

25 7. 如权利要求 4 所述的集成电路, 其特征在于:

 所述数据输出电路(14)的供电被连接到所述访问控制电路(16)的供电上。

8. 如权利要求 3 所述的集成电路, 其特征在于:

30 在所述的供电 V_{DD} 和所述数据输出电路(14)的供电之间布置了 NMOS 开关(18), 该开关的门极(20)通过在扩散层或在保护层中输送的线路(22)而被连接到所述访问控制电路(16)的 V_{DD} 供电上。

集成电路和用于给集成电路供电的电路装置

技术领域

- 5 本发明涉及一种具有数据输出电路和访问控制电路的、用于处理安全性较重要的数据的集成电路，以及涉及一种用于给集成电路的安全性较重要的部分提供供电的电路装置。

背景技术

- 10 对于包含有安全性较重要的数据的芯片卡，其内部所安装的集成电路可能会成为各种入侵的目标，以企图访问该集成电路所包含的安全性较重要的数据。

对芯片卡的物理入侵可能有各种目的：

- 读取（探测）保密信号
- 强行施加（强加）控制信号。

- 15 因此在安全技术中，保密信号和控制信号是在很难访问的掩模层中进行输送的，并另外通过屏蔽层来进行保护（所谓的保护层）。

然而，除了上述探测和强加的方法之外，还可能将电路块与供电隔开，以便有目的地使控制信号产生“固定(stuck-at)”故障，并由此譬如取消禁止功能。

- 20 根据现有技术，为了防止这种有目的地使 IC 上的访问控制电路处于无电压状态的入侵，现在是给这种访问控制电路进行双路供电（既在铝层又在扩散层进行供电）。于是人们按照现有技术以如下方式来防止上述的入侵，即在不可分离的层（IC 的层）中（譬如在扩散层内）给所述的访问控制电路进行供电。

- 25 双路供电有个缺点，就是在 IC 上消耗了很大的地方，因为否则的话可以在扩散层中输送信号。只在扩散层中输电有个缺点，就是扩散层通常具有较高的电阻。因此要么会造成电压降，要么必须在扩散层中设置相应宽的导轨，这又会导致较大的位置损失。

发明内容

- 30 因此本发明的任务在于，创造一种用于处理安全性较重要的数据的集成电路和一种用于给集成电路的安全性较重要的部分提供供电的电路装置，其中，在安全性相同或甚至改善的情况下，不需要那么多

的地方来给该 IC 的安全性较重要的部分提供附加的供电或只在扩散层中输电。

根据本发明的用于给集成电路的安全性较重要的部分提供供电的电路装置，所述安全性较重要的部分由相应的访问控制电路进行保护，其中所述安全性较重要的部分的供电通过一个或多个开关进行控制，当所述访问控制电路的供电被干扰时，所述的开关被断开。

该解决方案的一种优选的改进在于，由所述的访问控制电路产生总是成对地倒相的禁止信号，只有当两个倒相的禁止信号指示取消禁止时，所述的数据输出电路才工作。如果此时所述访问控制电路的一个供电被中断，则必定有一个禁止信号为“错误”值，从而禁止数据的输出。

此处有利的是，所述相互倒相的禁止信号并行地、且优选为相叠地在所述的集成电路内输送。这便加难了入侵单个的禁止信号。

另外有利的是，所述的禁止信号在扩散层或保护层内输送。否则的话，可能费些力气就能通过访问该禁止信号来解禁所述的数据输出电路。

本发明的另一种优选改进方案在于，如此地控制所述数据输出电路的供电，使得当所述访问控制电路的供电被干扰时，便中断所述的供电。

为此，可以优选地把所述数据输出电路的供电连接到所述访问控制电路的供电上。这是一种非常简单的防止集成电路受到所述干扰操作的方法。

如下的优选解决方案提供了更高的安全性，即所述数据输出电路的供电通过一个或多个开关进行控制，当所述访问控制电路的供电被干扰时，所述的开关被断开。通过这种方法也可以避免如下情况，即：尽管所述访问控制电路的供电被干扰，但可以通过把导电针放到 IC 的相应磁畴区上来重新建立所述数据输出电路的供电。

对此，如下解决方案是非常有利的，即在所述的公共供电 V_{DD} 和所述数据输出电路的供电之间布置了 NMOS 开关，该开关的门极通过在扩散层或在保护层中输送的线路而被连接到所述访问控制电路的 V_{DD} 供电上。

同样，本发明的上述任务可以由如下的用于给集成电路的安全性

较重要的部分提供供电的电路装置来解决，所述安全性较重要的部分由相应的访问控制电路进行保护，其方法在于，所述安全性较重要的部分的供电是如此地被输送的，使得当所述访问控制电路的供电被干扰时，便中断所述的供电。

5 在此，如下解决方案是非常简单的，即所述安全性较重要的部分的供电被连接到所述访问控制电路的供电上。

一种能提供更高安全性的解决方案在于，所述安全性较重要的部分的供电通过一个或多个开关进行控制，当所述访问控制电路的供电被干扰时，所述的开关被断开。在访问控制电路的供电被中断期间，

10 利用该方法可以防止强行地再建立所述安全性较重要的部分的供电。

对此，尤其有利的是，在所述的公共供电 V_{DD} 和所述安全性较重要的部分的供电之间布置了 NMOS 开关，该开关的门极通过在扩散层或在保护层中输送的线路而被连接到所述访问控制电路的 V_{DD} 供电上。

15 通过组合本发明的上述安全措施，可以有利地提高所述集成电路的安全性，显然同时也增加了一些费用。

附图说明

下面借助附图所示的实施例来详细讲述本发明。图中：

图 1 示出了集成电路的部分视图，其中同时设立了本发明所建议的所有安全特征。

20 具体实施方式

图 1 示出了 IC 的一种简略电路框图，在其存储器 12 内存放了安全性较重要的数据。因此，该集成电路 10 具有一个与读取电路 14 相连的存储器 12。由读取电路 14 把从该存储器 12 中读出的数据送到用“数据”表示的输出端上。

25 另外还装设了一个访问控制电路 16 的块，它包含有相应的禁止功能。通过该功能来确保譬如只有授权的用户在输入口令字后才能访问存放在存储器 12 内的数据。

30 如图 1 所示，所述访问控制电路 16 和读取电路 14 的供电是如此设置的，使得供电的两个支路 V_{DD} 和 V_{SS} 首先被输入到访问控制电路 16，然后再输入到读取电路 14。通过在访问控制电路 16 之前简单地断开 V_{DD} 或 V_{SS} 可以自动地使读取电路 14 没有电压，使得再也不能从存储器 12 读取数据。

在此，供电 V_{DD} 和 V_{SS} 通常是在铝层中输送的。

因此基本上存在如下的入侵可能性，即在禁止功能之前或之后中断 V_{DD} ，并通过直接在那儿把供电施加到铝上来单独地给读取电路供电。

- 5 为了避免这种情况，另外还在位于 V_{DD} 和读取电路 14 之间的、从铝层给读取电路 14 分支出供电电压 V_{DD} 的位置处连接了一个 NMOS 开关 18，该开关的门极 20 通过一个穿越保护层或扩散层的导线 22 而在所述的扩散层中与所述访问控制电路的供电相连。利用这种方式可以确保：每当通往访问控制电路 16 的供电被中断时，所述的 NMOS 开关 18
- 10 就会

断开，并导致读取电路 14 没有电流，从而使得不能读取存储器 12。

另外还规定，如图 1 所示，从访问控制电路 16 向读取电路 14 输送双路并且倒相的允许信号 $BLCK$ 。这意味着存在一个正 $BLCK$ 信号和一个负 $\overline{BLCK}$ 信号。只有当两个信号正确时，所述的读取电路才能读取数据。

5 此时，如果通往访问控制电路 16 的供电被中断，则所述的信号中将至少有一个“错误”，从而禁止所述的读取电路。这甚至与 V_{DD} 和 V_{SS} 是否中断无关。在任何情况下都能禁止该读取电路 14。在此，还可以通过如下方式来进一步提高安全性，即彼此倒相的禁止信号并行地在集成电路传送，优选地在所述的扩散层或在保护层内传送。

10 因此本发明还存在如下可能性，即如此地布置所述电路块的供电布线，使得产生控制信号的块位于那些生成保密信号的电路块之前。于是在供电被隔断时，利用禁止信号也可以消除所述的保密信号。

作为第二种措施，另外也可以同时生成所述的倒相禁止信号，并在产生保密信号时一起分析它。由此可以确保在生成控制信号的块上存在
15 两种供电。在此，位于该块内的供电必须在不可分离的层内输送。优选彼此相叠地将所述的倒相控制信号输入到待分析的块中，以加大“强加”的难度。

如果在产生控制信号的块之前断开供电，则因此可以同时截止保密信号。在此，不必要在所述的块之间实施双路的供电布线，而且可以获得
20 用于信号布线的布线面积。

作为上述措施的替代方案，可以通过一个开关来控制生成保密信号的块的供电，该开关根据所述控制块的供电来接通或关断。在此，需要由控制块内的不可分离的供电把保密信号输送到所述开关的门极。

为了加大物理干扰操作可能性的难度，本发明在供电布线方面建议
25 了一种块装置，它使设计针对干扰入侵具有更好的鲁棒性，而不会在供电布线方面产生高耗费（扩散层中的冗余供电）。通常，这种块布置看起来不同于那种没有考虑上述边界条件的特定平面布局。

所述的控制信号与其倒相的对称信号一起并行地从一块输送到另一个块，以便为可能被分析的块确保：在进行生成的块上出现两个供
30 电极性。

作为一种变型方案，建议通过一个开关使所述需截止的块的供电依赖于所述控制功能的供电，其中，如此来设计该装置，使得物理干扰操

作不会不利地导致在控制信号上产生“固定”故障。这是与附加的电路费用联系在一起的（加入了开关），如果不想防止这种干扰操作可能性，则这种费用是不合理的。

图 1 以实施例示出了在存储器模块中的布置，其中，从存储器 12 读出的数据通过禁止功能被禁止用于读访问。如此地布置禁止电路和读取电路，使得在禁止功能与供电隔开的同时使所述的读取电路也没有供电，由此来禁止该读取电路。

禁止信号 BLCK 与其倒相的对称信号一起并行地被送到读取电路，在那儿对两个控制信号进行分析。

10 作为变型方案，在放大图中示出了一种布置，其中，所述禁止功能在扩散层中所输送的供电被输送到一个给读取电路供电的 NMOS 开关的门极上。如果禁止电路与 V_{DD} 隔开，那么读取地址也就同时失去供电。

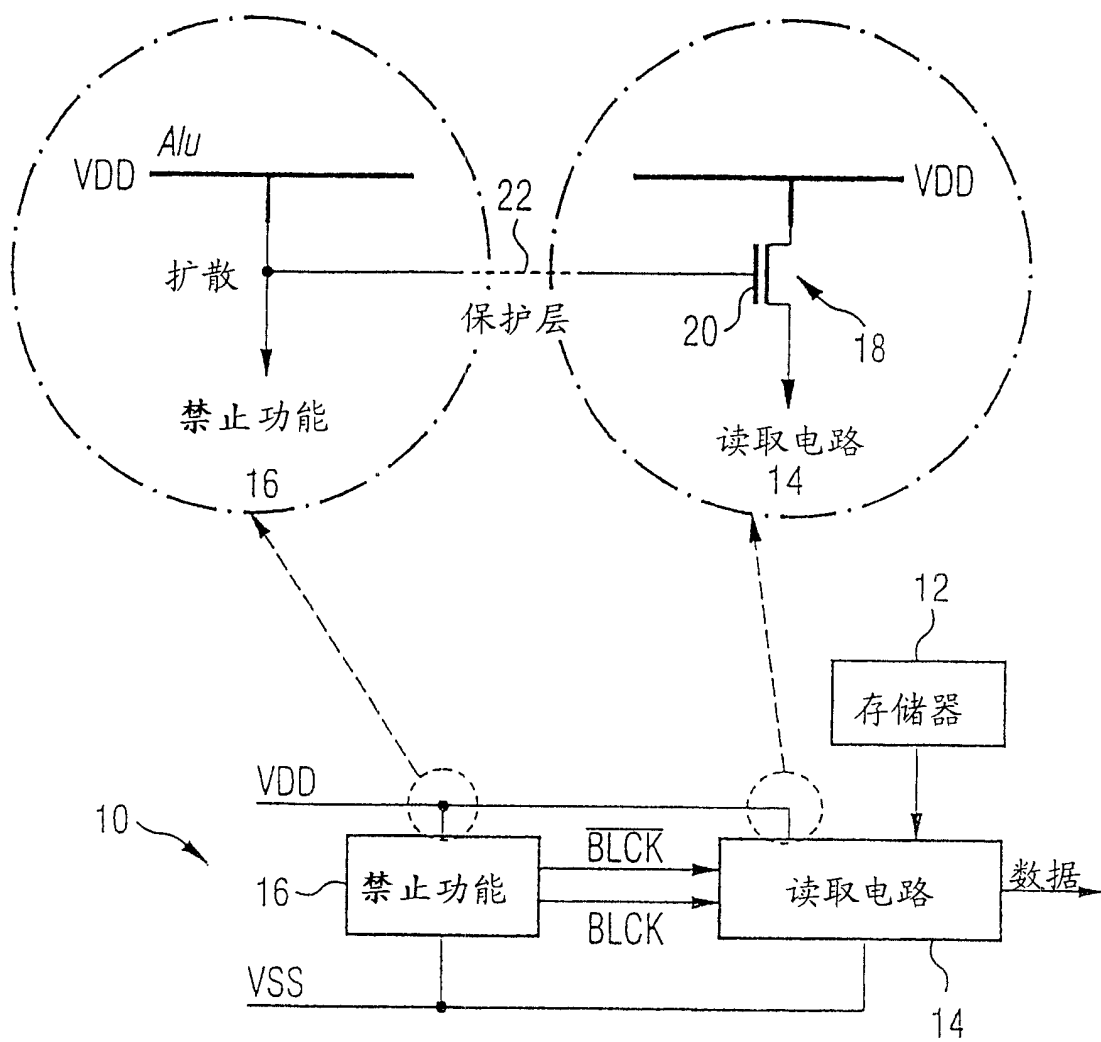


图 1