(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 101258552 B
(45)授权公告日 2012.05.30

(21)申请号 200680032529.5

(22)申请日 2006.06.20

(30)优先权数据
0507766 2005.07.21 FR
11/256,124 2005.10.21 US

(85)PCT申请进入国家阶段日
2008.03.05

(86)PCT申请的申请数据
PCT/US2006/024161 2006.06.20

(87)PCT申请的公布数据
WO2007/018761 EN 2007.02.15

(73)专利权人 爱特梅尔卢梭公司
地址 法国鲁塞

(72)发明人 阿兰·佩塔维
亚历山大·克罗盖内克

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 孟锐

(51)Int.Cl.
G11C 5/00(2006.01)

(56)对比文件
US 5639696 ,1997.06.17, 全文.
CN 1093465 A,1994.10.12, 全文.
US 4691350 ,1987.09.01, 全文.

审查员 刘芳

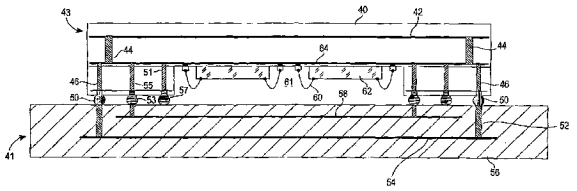
权利要求书 1 页 说明书 4 页 附图 5 页

(54)发明名称

用于数据保护的安全方法及装置

(57)摘要

一种用于数据安全的方法及装置，其包含各自具有由电屏蔽层(12、32)屏蔽的导电迹线层的印刷电路板(30)及集成电路(20)。在所述装置任一侧的篡改均可导致对流经用作电屏蔽的导电迹线层(13)的电流的干扰。这会触发安全电路擦除存储在集成电路(20)中的数据，且停止所述印刷电路板(30)与所述集成电路(20)之间的数据流。



CN 101258552 B

1. 一种用于数据保护的方法，其包括：

a) 提供印刷电路板，其包含第一电屏蔽及表面触点垫，所述第一电屏蔽嵌入在所述印刷电路板中；

b) 在包含第二电屏蔽的经封装集成电路中提供无引脚引线栅格阵列，所述第二电屏蔽位于所述集成电路的与所述引线栅格阵列中空腔区朝下方向上的触点相对的一侧上，所述集成电路与所述印刷电路板的所述表面触点垫接触；

c) 通过所述第一电屏蔽及所述第二电屏蔽引入电流；

d) 监控流经所述第一电屏蔽及所述第二电屏蔽的所述电流；及

e) 当检测出所述电流中的干扰时，停止在所述经封装的集成电路与所述印刷电路板之间传输的数据的传输。

2. 如权利要求 1 所述的方法，其进一步包含：

f) 当检测出所述电流中的所述干扰时，擦除存储在所述经封装的集成电路中的敏感数据。

3. 一种集成电路安全装置，其包括：

印刷电路板；

第一电屏蔽，其嵌入在所述印刷电路板中；

无引脚触点阵列集成电路，其安装在所述印刷电路板上；

第二电屏蔽，其位于所述印刷电路板上的所述触点阵列集成电路上；

所述第一电屏蔽与所述第二电屏蔽经导电元件连接以形成安全包封；及

安全电路，其经配置以监控流经所述安全包封的电流且在检测出篡改的情况下采取行动来保护数据。

4. 如权利要求 3 所述的装置，其中所述集成电路是球栅阵列。

5. 如权利要求 3 所述的装置，其中所述集成电路是列栅格阵列。

6. 如权利要求 4 所述的装置，其中所述集成电路是空腔区朝下的球栅阵列。

7. 如权利要求 5 所述的装置，其中所述集成电路是空腔区朝下的列栅格阵列。

8. 如权利要求 3 所述的装置，其中所述第二电屏蔽是蛇形迹线。

9. 如权利要求 8 所述的装置，其中所述蛇形迹线纳含于所述集成电路的一个层中。

10. 如权利要求 8 所述的装置，其中所述蛇形迹线包含所述集成电路的一单一层上的一单一网。

11. 如权利要求 8 所述的装置，其中所述蛇形迹线包含所述集成电路的一单一层上的两个网。

12. 如权利要求 8 所述的装置，其中所述蛇形迹线包含所述集成电路的两个层上的一单一网。

13. 如权利要求 8 所述的装置，其中所述蛇形迹线包含所述集成电路的两个层上的两个网。

14. 如权利要求 3 所述的装置，进一步包含延伸于所述第一电屏蔽与所述第二电屏蔽之间的通孔。

用于数据保护的安全方法及装置

技术领域

[0001] 本发明涉及数据安全装置及方法。

[0002] 背景技术

[0003] 目前需要为数据和软件提供安全。例如，在银行终端中，使用触摸板来输入数据或由读卡器（例如，磁性读卡器）来导出数据。这些数据用来进行安全交易。对这种交易来说，安全很必要且对这些数据的存取必须受到保护。

[0004] 为了确保数据不被篡改、窃取或以其他方式未经授权地存取，在传输前通常对所述数据进行加密。然而，通过存取未加密数据首先发送到的集成电路的引线，数据或软件仍可在加密前被存取。

[0005] 在现有装置中，已使用三维网格来围住一组集成电路并防止篡改。例如，美国第6,646,565号专利揭示一种用于电子电路安全的装置，其中将电子装置封闭在第一与第二电路板之间，每一电路板均具有蛇形导电层。将篡改检测电路连接到所述导电层来检测电路篡改。整个电路被包裹在网格中。在所述电路板或所述网格处的任何篡改都会通过检测到对流经所述电路板及网格中的安全层中的电流的干扰而感测到。这个电流干扰向安全系统发信号来擦除敏感数据，以使其不会被截取。其他类似的装置包含美国第4,593,384号、第4,691,350号及第4,807,284号专利。

[0006] 美国第5,406,630号专利揭示一种防篡改集成电路（IC）装置。封装和盖包含重金属，以防止对芯片机能的x光辐射和红外线检测。这将有效地提供对所述IC运作的电屏蔽。

[0007] 美国第6,396,400号专利揭示一种用于保护数据存储装置的安全系统。所述数据存储装置封闭在第一外壳中，所述第一外壳安装在第二外壳内且通过若干支撑结构与其分离。在所述第一外壳与所述第二外壳之间的间隙中形成真空。第二外壳的破裂会导致压力变化。传感器检测所述压力变化，并向数据存储装置发信号以采取行动来保护数据不被篡改。

[0008] 所揭示的这些装置是复杂且昂贵的。已寻找到替代的更简单的解决办法。

[0009] 发明内容

[0010] 本文揭示一种使用印刷电路板上的空腔区朝下的无引脚触点栅格阵列来保护数据的装置及方法。所述栅格阵列封装必须具有覆蔽附加电路的集成电路。这种集成电路的封装包含介电层及所述介电层下方的导电层。以类似方式，所述电路板还包含用作电屏蔽层的导电层。所述印刷电路板与所述空腔区朝下的栅格阵列集成电路二者均具有通过每一各自装置上的导电层引入的电流。如果通过电流干扰检测出篡改，则指引芯片搅乱或擦除所述芯片上的数据以防止被存取。

附图说明

[0011] 图1是定位在印刷电路板上的集成电路的剖面图。

[0012] 图2是所述安全过程的实施例的流程图。

[0013] 图 3 是显示集成电路及印刷电路板的另一实施例的剖面图。

[0014] 图 4a 是具有两个球形触点的蛇形迹线的顶视图。

[0015] 图 4b 是具有两个球形触点的替代蛇形迹线的顶视图。

[0016] 图 5a 是双网蛇形迹线的第一实施例的顶视图，其中每一网均具有两个球形触点。

[0017] 图 5b 是双网蛇形迹线的第二实施例的顶视图，其中每一网均具有两个球形触点。

[0018] 图 5c 是双网蛇形迹线的第三实施例的顶视图，其中每一网均具有两个球形触点。

[0019] 图 6 是具有两个球形触点的蛇形迹线的顶视图，其中所述迹线延伸到两个层中。

[0020] 图 7a 是双网蛇形迹线的第一实施例的顶视图，其中每一网均具有两个球形触点，且所述网占据两个层。

[0021] 图 7b 是双网蛇形迹线的第二实施例的顶视图，其中每一网均具有两个球形触点，且所述网占据两个层。

具体实施方式

[0022] 在图 1 所图解说明的实例性实施例中，安全的集成电路具有安全保护，以使其可用于安全交易。在这个实施例中，空腔区朝下的球栅阵列集成电路 20 定位于印刷电路板 30 上。集成电路 20 包含球栅阵列上的球 14。空腔 18 向下朝向印刷电路板 30。因此，在不钻透集成电路封装或电路板的情况下，不能接入空腔 18 中的线引脚 16 以进行篡改。

[0023] 集成电路的封装包含电屏蔽层 12。层 10 是介电层（例如，黑色环氧树脂或类似材料）。层 10 保护所述电屏蔽层在未事先去处理的情况下免遭物理篡改。在这个屏蔽层 12 下方是导电层 13，例如，镀铜层。层 13 是用于其他信号路由的导电层。层 12 由蛇形迹线制成。这个导电层 12 连接到监控电路、电流源及集成电路的存储器。如果集成电路（例如）通过钻孔或其他干扰而被篡改，则触发安全电路来擦除集成电路 20 上的数据。在类似方式中，印刷电路板 30 包含介电层 34。如果电流被中断或以其他方式篡改，则安全装置擦除数据以使其不能被存取。

[0024] 在所图解说明的实施例中，使用球栅阵列集成电路。或者可使用其他触点阵列，例如列栅格阵列。优选地，引线阵列不包含引脚（例如，为无引脚阵列）。延伸到印刷 电路板中及 / 或穿过印刷电路板的引脚将不再具有保护引线上的信号的能力。

[0025] 放入安全封装中的集成电路经设计以嵌有特定电路，所述特定电路将驱动集成电路安全层 12 及印刷电路板安全层 32 两者。这个电路检查确保所述电路的完整性没有被破坏或遭受篡改。

[0026] 在图 2 中，操作中的安全特征的流程图类似于现有装置的操作，在现有装置操作中使用多个印刷电路板和网格聚合体的组合，尽管本发明的装置与现有技术明显不同。在操作 70 的连续安全操作期间，监控流经安全系统的电流。可将任何既定时间检测到的电压与已知设定的电压电平进行比较，来确定所述电压是否为预期的且是否与过去的电压电平一致。在操作 72 中，逻辑询问所述电流是否已被扰乱。如果没有，则所述逻辑指引继续进行操作 70，其中监控安全电路。如果操作 72 确实检测出在电路处的篡改（由电流的扰乱表示），则起动操作 74，且起动安全措施来保护数据。一般来说，这种安全措施将是擦除数据。

[0027] 参照图 3，显示替代的集成电路及电路板的剖面。这个装置包含安装于电路板 41

上的集成电路 43。封装 40 防止对基础安全屏蔽的物理检验。

[0028] 这种材料可以是黑色环氧树脂或其他类似材料。

[0029] 集成电路安全屏蔽 42 嵌入到封装 40 中。这种安全屏蔽可以是任何可由安全电路监控以允许检测篡改的导电构件。蛇形迹线是一个安全屏蔽实施方案。导电连接 44 附装到安全屏蔽 42 的外部边缘，其连接到层 64，层 64 进而连接到导电元件 46，导电元件 46 终止于球 50 处。导电元件 44、46 及球栅阵列的球 50 提供连续导电侧屏蔽，以使对芯片的任何物理篡改均将由安全电路检测。导电元件 44 与 46 连接到层 64，以使其他信号可在层 64 上发送。这些信号可包含：经由连接 60 从装置 62 发送的信号、经由连接 57 从球 51 发送的信号，及经由连接 55 从球 53 发送的信号。

[0030] 球连接器 50 连接到印刷电路板 41 上的导电元件 52。这个导电元件连接到所述印刷电路板上的安全屏蔽层 54。导电元件 44、46 及球 50 的组合提供连续导电阻挡层，所述阻挡层可在导电元件 52（球 50 以导电方式耦合于其上）为电路板 41 提供同种阻挡层时保护集成电路不受到负面入侵。印刷电路板 41 上的安全屏蔽 54 及集成电路 43 上的电屏蔽 42 完成这个安全保护以形成安全包封，从而用导电屏蔽来保护所有侧。在这个屏蔽处的篡改将由安全电路检测出，然后所述安全电路可采取适当的行动（例如，擦除芯片上的敏感数据并防止从印刷电路板传输数据）。封装 40 防止对电屏蔽 42 与侧导电元件 44 及 46 二者的物理审查。

[0031] 这个安全包封中的若干元件可携载敏感数据。球 53 连接到印刷电路板 41 上的层 58。敏感数据可携载于层 58 的电路板上、通过球 53 传输、携载于集成电路层 64 上，且携载在装置 62 或导电连接 60 上。纳含于内部空腔 61 中的所有元件均将由安全包封保护，例如集成电路 43 中的内部元件及安全包封中的印刷电路板 41。相同的方法可用于不同的集成电路和同一印刷电路板上的其他元件（例如，显示器、键盘）。

[0032] 安全屏蔽可生产有若干不同设计。例如，图 4a、4b 中显示单层单网双球蛇形屏 蔽设计。在图 4a 中，通孔 81、83 位于迹线 80 末端处。在图 4b 中，通孔 84、85 位于迹线 82 末端处。在这两个图中，安全屏蔽形成直到通孔 81、83、84、85 的位置处的单层，其中导电元件延伸到通孔触点。所述球可在中央位置、在边缘位置，或在各位置的某一组合中。所述导电迹线可呈螺旋形状，或如刚才两个实例中所述有规律地来回摆动的形状。

[0033] 图 5a、5b 及 5c 中显示若干单层双网屏蔽设计。在图 5a 中，第一网迹线 90 包含两个通孔 90a、90b，且第二网迹线 92 终止于通孔 92a、92b 处。以类似的方式，在图 5b 中，第一网迹线 94 具有通孔 94a、94b，且第二迹线 96 终止于通孔 96a、96b 处。对图 5c 来说，第一迹线 100 终止于所述迹线末端处的通孔 100a、100b 处，且第二迹线 98 终止于通孔 98a、98b 处。在所述三个实例中，所述迹线的长度均在单个平面上，且所述通孔均通过沿集成电路各侧的导电路径而连接。

[0034] 图 6 图解说明双层单网蛇形安全装置。迹线 102 终止于通孔 102a、102b 处。通过封装厚度的连接允许所述蛇形迹线包含区段 102c 及 102d，区段 102c 及 102d 位于与所述蛇形迹线其余部分不同的层（也就是说，上方或下方）中。图 7a、7b 图解说明双层双网蛇形安全装置。在图 7a 中，第一层包含终止于通孔 104a、104b 处的第一迹线 104。在第二层中，第二迹线 106 终止于末端通孔 106a、106b 处。所述通孔可经由连接器延伸到如图 3 所示的集成电路上的表面位置。在图 7b 中，所述迹线的每一者均类似于图 6 的迹线。迹线 108 终

止于通孔 108a、108b 处。迹线 108 的区段 108c、108d 延伸到与含有迹线 108 其余部分的层不同的层中。迹线 110 终止于通孔 110a、110b 处。迹线 110 的区段 110c、110d 延伸到容纳迹线 108 的较长区段的层中。存在所述电屏蔽的许多其他可能配置。

[0035] 当将包含本发明安全屏蔽的集成电路安装于印刷电路板上时，向所述芯片提供外部电源。这允许将敏感数据存储在所述芯片上。所述电源还驱动安全电路，其中连续监控通过所述安全电路的电流。集成电路可接收敏感通信，并使敏感数据与电路板相关。印刷电路板上的供电电池可确保集成电路上的信息存储及芯片上的安全的运行。可使用主电源来将敏感信息从集成电路功率转移到电路板，且贯穿整个板。

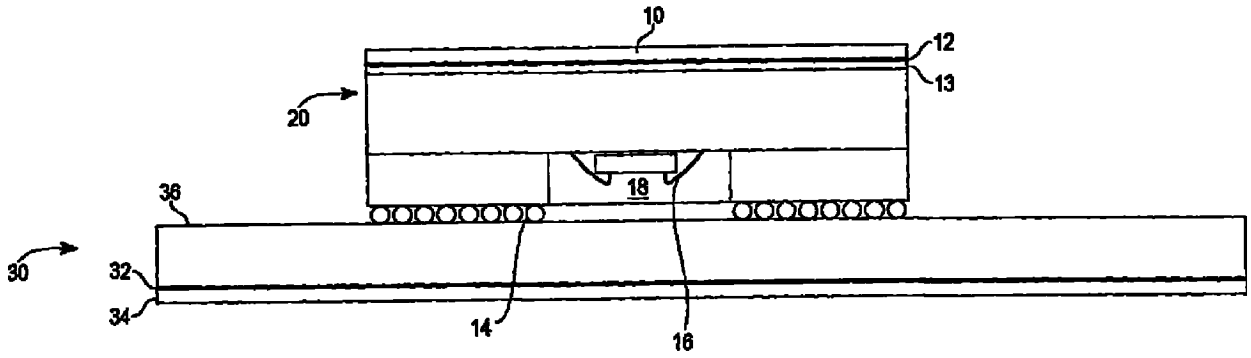


图 1

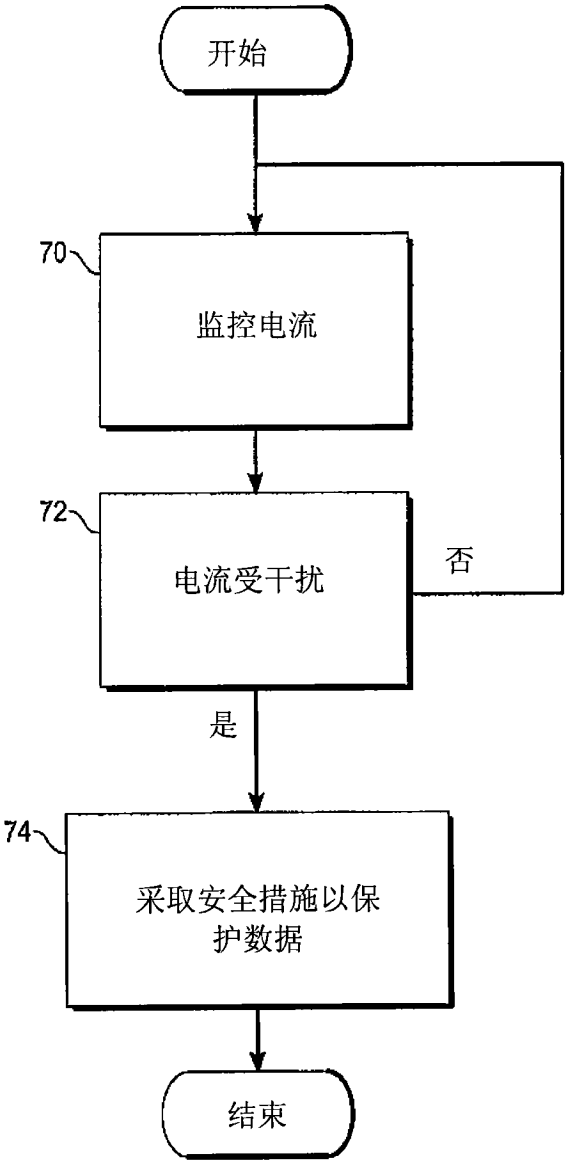


图 2

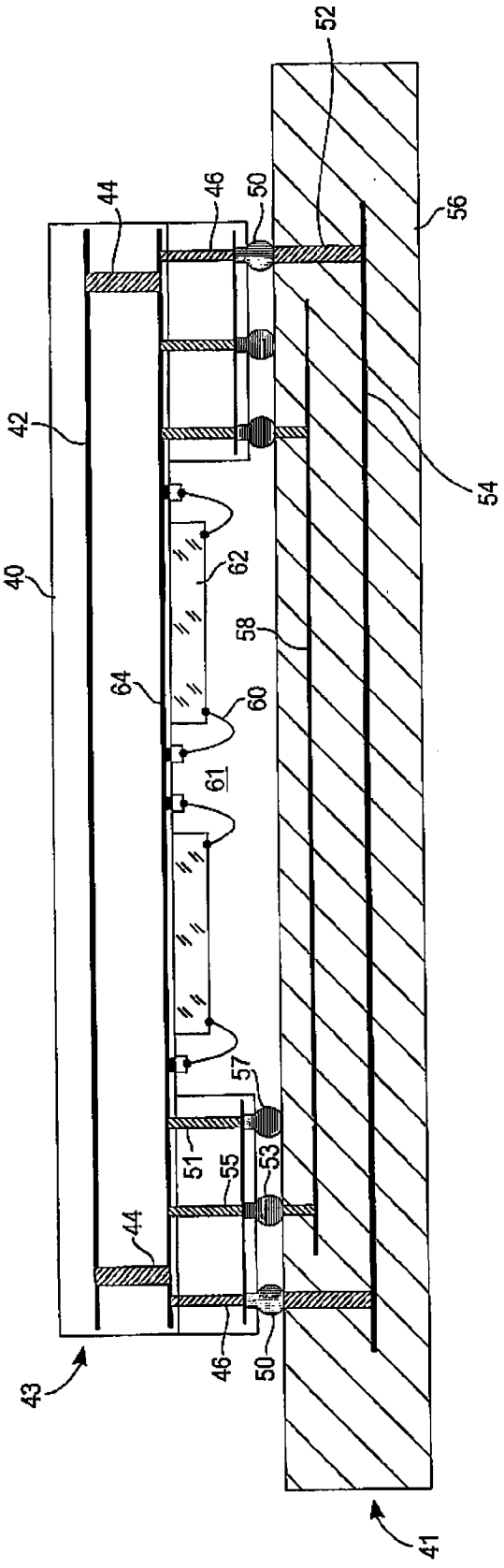


图 3

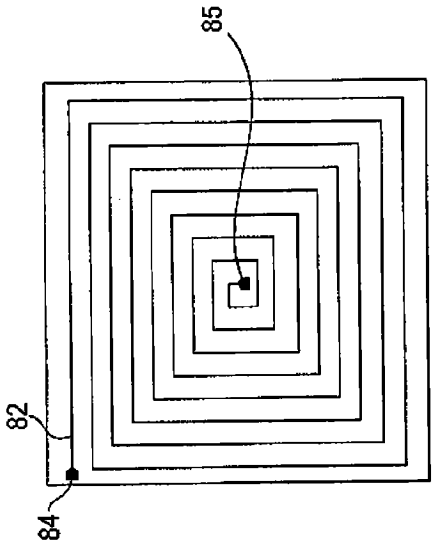


图 4b

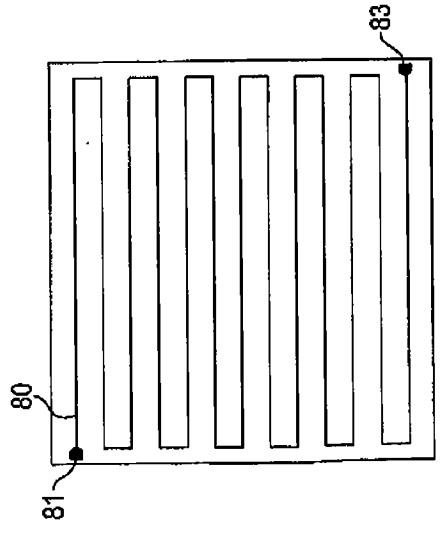


图 4a

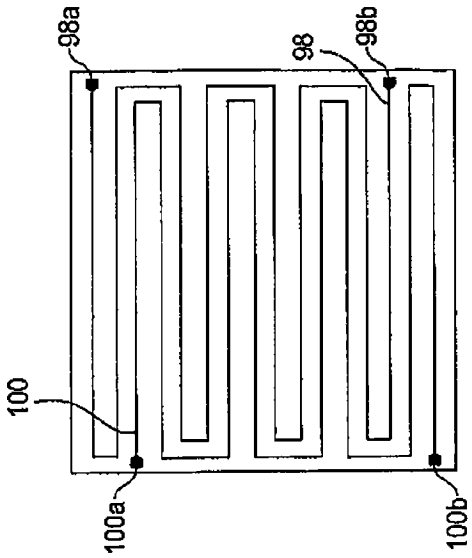


图 5c

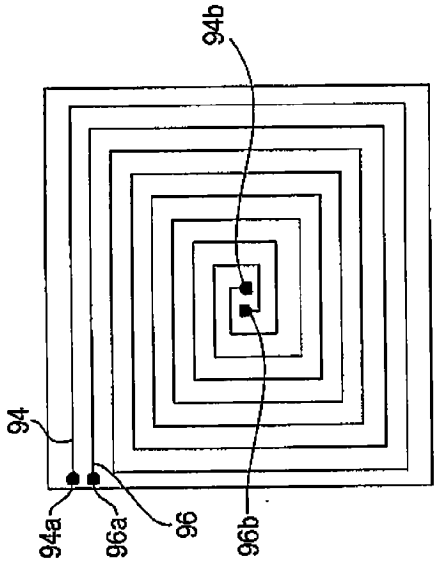


图 5b

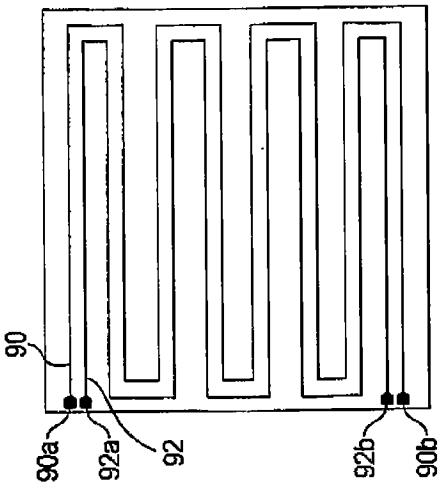


图 5a

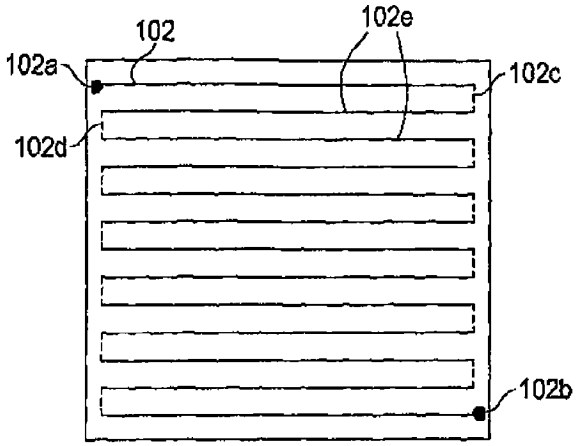

102
102e
102a
102c
102d
102b

图 6

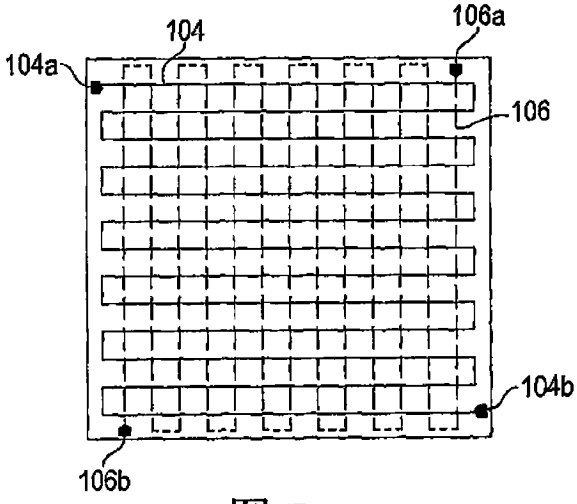

104
106a
104a
106
104b
106b

图 7a

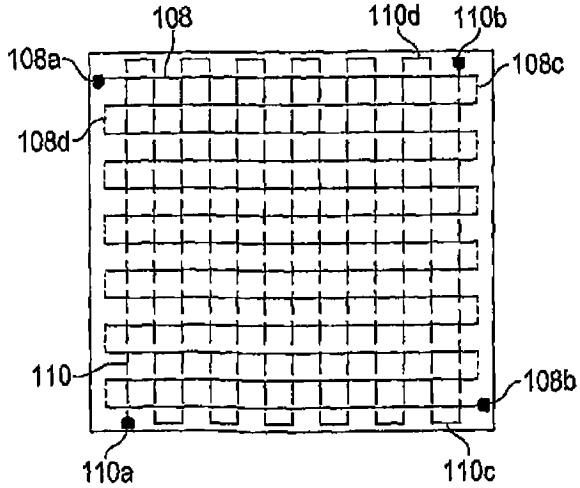

108
110d
110b
108a
108c
108d
110
108b
110a
110c

图 7b