[19]中华人民共和国专利局

[51]Int.Cl[6]
G06K 19/10
G11C 11/00

[12]发明专利说明书

[11] ZL 专利号 94103312.0

[45]授权公告日 1998 年 5 月 13 日

[11] 授权公告号 CN 1038367C

[22]申请日 94.3.18 [24]颁证日 98.2.28

[21]申请号 94103312.0

[30]优先权

[32]93.3.20 [33]GB[31]9305827.9

[73]专利权人 摩托罗拉公司

地址 美国伊利诺斯

[72]发明人 阿尼尔·格尔克西

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

代理人 范本国

[56]参考文献

GB2205667A	1988.12.14	G06F12/14
US5,081,675	1992. 1.14	H04L9/00

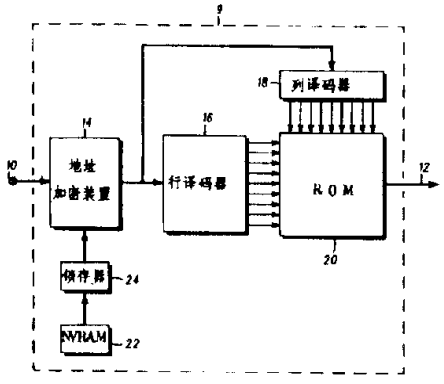
审查员 王晓光

权利要求书 2 页 说明书 5 页 附图页数 0 页

[54]发明名称 数据存储装置

[57]摘要

数据存储设备（9）包括用来存储数据的一个电子存储单元阵列（20）。地址输入端（10）提供对地址信号源的接口，提供来自地址信号源的第一存储单元地址信号以便为存储器阵列（20）中的存储单元寻址。数据输出端（12）为数据接收装置提供接口并与存储器阵列（20）相连接，用于接收响应地址信号而产生的数据信号。地址加密装置（14）连接在地址输入端（10）和存储器阵列（20）之间，用于对第一存储单元地址信号进行加密。



权 利 要 求 书

1. 一个数据存储装置包括：

一个用于存储数据的电子存储器单元阵列；

一个地址输入端，用于为地址信号源提供接口，并且提供来自地址信号源的第一单元的地址信号，以便对存储器阵列中的存储单元进行寻址。

一个数据输出端，用于为数据接收装置提供接口并被连接到存储器阵列，且用来接收为响应地址信号而由此产生的数据信号，该数据信号用以表示存储在由地址信号寻址的存储单元中的数据；

其特征在于还包括：

地址加密装置，被连接在地址输入端和存储器阵列之间，用于对第一存储单元地址信号进行加密；

地址加密装置中含有加密用数据，该数据能避免被直接光学探测，加密用数据用于对第一存储单元地址信号进行加密。

2. 权利要求 1 中所述的设备，其中的数据存储器阵列是含有以加密方式存储的数据的只读存储器，此中的数据加密方法与加密数据装置相配套。

3. 权利要求 1 中所述的设备，其中加密用的数据存储在非易失性存储器中。

4. 权利要求 1 中所述的设备，其中的地址加密装置包括用来接收从非易失性存储器来的加密用的数据的锁存器，以致于在正常工作期间非易失性存储器可以独立于地址加密装置而工作。

5. 权利要求 1 中所述的设备，其中的设备用半导体集成电路做成。

6. 一种智能卡，包括根据上述任一权利要求构造的数据存储设备。

说　明　书

数据存储装置

本发明一般涉及数据存储装置。

数据存储装置，例如，含有以数值形式存储在集成电路(*IC*)存储单元中的银行帐户细节的智能卡，存在着被欺诈性光学检测的风险。这种检测是这样进行的，通过去除 *IC* 的塑料封装，蚀刻掉覆盖层，然后再使用能选择吸收的着色剂，就能看到存储器上的数据。

众所周知，可以使用地址加密(*encrypting*)装置，这能使 *IC* 存储器中的数据变得无序。这样，这些数据在被光学分析时就无法理解，但可以通过地址加密装置而合法地存取。但使用这种地址加密装置的一个问题是：通过使用上述的光学检测技术，人们可以得知加密装置的细节，从而可以破译出 *IC* 存储器中的数据。

本发明试图提供一种数据存储装置，在这种装置中上述问题将得到解决。

该数据存储装置含有一个用于存储数据的电子存储单元阵列。地址输入端提供对地址信号源的接口，从而为存储器阵列上的存储单元寻址提供来自地址信号源的第一存储单元的地址信号。数据输

出端为数据接收装置提供接口并连接到存储器阵列，用来接收响应地址信号而产生的数据信号。该数据信号用来表示存储在由地址信号寻址的存储单元中的数据。地址加密装置连接在地址输入端和存储器阵列之间，用于加密第一存储单元的地址信号。地址加密装置含有能防止直接光学检测的加密用的数据，这些数据用于加密第一存储单元的地址信号。

数据存储器阵列可以是含有以加密的方式存储数据的只读存储器，这里的数据加密方法与数据加密装置相配套。

地址加密装置可以包括一个用于接收来自非易失性存储器的加密数据的锁存器。这样，在正常工作时该非易性存储器就可以独立于地址加密装置而工作。

值得注意的是，这样人们就不能得到该加密装置的加密细节，从而也就无法破译 IC 存储器中的数据。

现在通过参考附图来描述本发明的一个示范实施例。图 1 说明根据本发明设计的数据存储装置的一个最佳实施例。

现在参考图 1，图中给出了一个智能卡 9，该卡含有用于接收来自智能卡 9 的地址驱动线路（未示出）的地址信号的地址输入端 10。智能卡 9 是在单一的硅晶片上做成的集成电路。

地址加密器 14 连接到地址输入端 10，用于根据下文将要解释的密钥对接收到的地址信号进行加密。

行译码器 16 和列译码器 18 分别连接到地址加密器 14 上，用

于对只读存储器(*ROM*)20 提供存储器单元的寻址，该寻址是对来自地址加密器 14 的加密地址信号的响应。

ROM 20 含有存储在存储单元阵列中的电子数据。这些数据通过连接到 *ROM* 20 上的行译码器 16 和列译码器 18 来进行寻址，*ROM* 20 为响应寻址向数据输出端 12 提供数据信号。每个数据信号用于表示存储在被寻址存储单元中的数据值。

数据存储器 20 的存储单元的物理排列与自地址输入端 10 的地址信号并不明显地相对应，因为这些收到的地址信号要通过地址加密器 14 被加密。这样，上述的对存储单元内容所作的可能的光学检测从这些数据上将得不到任何有意义的东西，除非加密装置同样是可以被检查的。

数据输出端 12 用于接收来自数据存储器 20 的数据信号，为智能卡的数据处理单元(未示出)提供所述的数据信号。

包含在浮动栅极场效应晶体管装置中的非易失性随机存取存储器(*NVRAM*)22 通过锁存器 24 连接到地址加密器 14，以数值的形式提供密钥。

在正常工作期间，智能卡 9 为了引用数据存储器 20 的第一存储单元中存储的第一数据项，可能要检索这第一项数据的值。已知该数据驻留在第一存储单元中。

因此，第一存储单元的地址信号从地址驱动线路(未示出)送至地址输入端 10。第一存储单元的地址信号似乎用于表示第二个存储

单元的地址，且后者所在单元不含有所希望的值。地址加密器 14 根据从锁存器 24 收到的密钥对第一存储单元的地址信号进行加密。

译码器 16 和 18 收到经加密的第一存储单元的地址信号时，该信号清楚地表示出这是第一存储单元的地址。

这样，为了响应该加密的地址信号，*ROM* 20 的第一存储单元通过译码器 16 和 18 寻址，并为数据输出端 12 提供数据信号，该信号用于表示存储在第一存储单元的第一项数据值。

在智能卡 9 中，*NVRAM* 22 基本上用来作其他的用途。因此，当智能卡 9 开始正常工作时，锁存器 24 用以接收形成密钥的数据值，然后保持该密钥并在工作期间为地址加密器 14 提供密钥，以便 *NVRAM* 22 与加密器 14 相隔离。因此，地址加密器 14 的运行不会妨碍智能卡 9 的任何操作。

值得注意的是，试图使用上述对 *ROM* 20 进行检测的方法对 *NVRAM* 22 的内容进行光学检测将检测不出上述的密钥，因为这些方法对浮动栅极场效应晶体管装置的探测无效。

锁存器 24 可以用上述方法进行光学检测，但它仅在正常工作时保持密钥的值。这样，在被检测时，锁存器 24 将不再含有密钥值。因此，密钥是安全的。

地址加密器 14 用密钥来对收到的第一存储单元的地址信号进行变换。例如，密钥可能是一个四位的二进制数，而地址加密器可能对密钥和第一存储单元的地址信号进行加法运算。这样，地址加密

器 14 就为行译码器 16 和列译码器 18 提供了加密的地址信号。

对第一存储单元的地址信号进行加密意味着 *ROM* 20 中第一存储单元的物理地址并不显式地对应于所希望的物理地址。因此，在不知道密钥的情况下，根据第一存储单元的地址来计算和找出某一存储单元，并用前述的光学探测法来探测该存储的内容，这样做是不可能的。对 *ROM* 20 中的所有其余存储单元的地址也是如此。

此外，光学检测译码器 16 和 18 以及地址加密器 14 的构造均无助于码译存储单元的地址，因为密钥是安全的。

这样，就可以避免对 *ROM* 20 中所含数据进行非法和欺诈性的光学探测。

需要指出的是，技术熟练的人员均可按前述实施例完成其他的实施例。例如在一种不同于智能卡的设备中使用上述的装置，例如使用盒式存储器(*memory cartridge*) 或其他数据存储设备。

同样应懂得，*NVRAM* 22 可以用另外的技术连接到上述的浮动栅极晶体管，例如金属/氮化物氧化硅(*MNOS*) 半导体技术。

另外，*ROM* 20 也可以用其他的数据存储介质来代替，例如可擦除和可编程的 *ROM*(*EPROM*)。