[19]中华人民共和国专利局

[51]Int.Cl[6]
G11C 7/00
G05F 1/00

[12]发明专利申请公开说明书

[21] 申请号 96195969.X

[43]公开日 1998年9月2日

[11] 公开号 CN 1192286A

[22]申请日 96.7.31

[30]优先权

[32]95.8.2 [33]GB[31]9515879.6

[86]国际申请 PCT/GB96/01874 96.7.31

[87]国际公布 WO97/05618 英 97.2.13

[85]进入国家阶段日期 98.1.26

[71]申请人 记忆体公共有限公司

地址 英国爱丁堡

[72]发明人 A·R·德斯

C·麦科尔

[74]专利代理机构 中国专利代理(香港)有限公司

代理人 王 勇 王 岳

权利要求书 1 页 说明书 3 页 附图页数 1 页

[54]发明名称 模块安全装置

[57]摘要

一种存储器模块，包含多个存储电路、存储预定代码的非易失性存储器、在模块加电时向上计数到预定值或从预定值向下计数的计数装置、如果在到达该预定计数之前该模块未接收到该预定代码时便禁止该模块的控制装置。

权　利　要　求　书

1.一种包括多个存储电路及用于存储预定代码的非易失性存储器的存储器模块，其特征在于它包含在该模块加电时计数到一个预定值的计数装置以及如果在到达该预定计数之前该模块未接收到该预定代码便禁止该模块的控制装置。

2.按照权利要求 1 的存储器模块，其特征在于该计数器装置计数读或写周期数。

3.按照权利要求 1 的存储器模块，其特征在于该计数器装置计数时钟周期数。

4.按照任何一项前面的权利要求的存储器模块，其特征在于该预定代码为一代码序列。

5.按照任何一项前面的权利要求的存储器模块，其特征在于该预定代码是手动输入的。

6.按照任何一项前面的权利要求的存储器模块，其特征在于该控制装置通过设定该输出禁止不活跃来禁止该模块。

7.按照任何一项前面的权利要求的存储器模块，其特征在于该存储器模块为一单列直插式存储器模块。

8.一种包含按照前面的权利要求中任何一项的存储器模块的计算机系统。

说　明　书

模块安全装置

本发明涉及存储器模块，更具体地涉及在许多普通个人计算机中用来扩展计算机的动态存储器的单列直插式存储器模块（ SIMM ）。

从计算机中盗窃单列直插式存储器模块（ SIMM)的事件已在明显增加。由于下述原因 SIMM 成为有吸引力的盗窃物品:

它们小而轻，这意味着运输毫无困难;

容易将它们从计算机系统上取下;

它们是可互换并对用户高度透明的，因此不存在大的兼容性问题;

它们是贵重的，每块 SIMM 售价 75 美元;

在全世界范围内存在着对 SIMM 的巨大需求;

它们在操作中难予发现，因而难于追踪被盗的 SIMM ;

现代软件需要大量存储器来运行，因此越来越需要它们;

SIMM 非常难于防盗（物理上）;

许多现代办公室具有大量计算机，各包含一些 SIMM，这意味着具有 SIMM 的高集中区。

由于这些器件的尺寸小及立即可互换性而难于防止被盗。每晚可从各计算机卸下 SIMM 并保存在保险箱中，但由于每天拆卸与重插这些器件很麻烦而在大型办公室中做不到这一点。

传统的 SIMM 在一块小的印刷电路板（ pcb ）上包含若干存储电路，通常为 DRAM （动态随机存取存储器）电路。在启动计算机时，该计算机内的处理器检验各 SIMM 是否都在计算机的适当插接槽中。通常 SIMM 并不包含任何存储器管理逻辑或控制器，因为它们是多余的。因此，除了在各 SIMM 上放上某种物理（可见或不可见的）标记或标签之外似乎无法识别它。为了安全目的而采用标签具有若干缺点。由于必须看见标记或标签才能识别与检测出 SIMM 是盗窃的，所以不能阻止被盗的 SIMM 的使用。不可能通知 SIMM 的粗心使用者其 SIMM 是偷来的。最好有某种方法使任何计算机能检测出其所连接的特定 SIMM 实际上是偷来的，然后禁止该 SIMM 的操作。

本发明提供了一种存储器模块，它包括若干存储电路、存储有一个

代码的非易失性存储器、在计算机启动时拦截对模块的存取的控制装置，使得在起动该存储器模块的初始化时必须输入正确的代码。

本发明最适用于利用部分存储电路的存储器模块，因为它们已在模块上具有对故障的单元的存取进行重定向的控制器。如果绕过这一控制器，模块便不能工作。如果将本发明用在标准存储器模块上则可以绕过附加的控制装置，因为对于模块的正常操作不需要附加的控制装置。从而在正常的存储器模块上可以容易地避开完全措施。

本发明提供了一种存储器模块，包括多个存储电路、存储有预定的代码的非易失性存储器、在模块加电时向上计数到预定值或从一个预定值向下计数的计数装置、以及如果在到达预定的计数之前模块未收到预定的代码时便禁止该模块的控制装置。

下面参照附图以示例方式对本发明进行更好理解及展示其如何实现，附图中：

图 1 示出存储器模块（在本例中为 SIMM）的两面。

参见附图，图 1A 示出密集有 DRAM 电路 2 的模块 1 的正面，而图 1B 示出包含控制电路 3 及非易失性存储器 4 的模块背面。

控制电路及非易失性存储器不一定在 SIMM 上存储电路的反面，控制电路与非易失性存储器可在模块上存储电路同一面上，或者可以用任何其它方便方式布置系统。

采用代码来禁止 SIMM 的操作并非无足轻重的。这是因为存在着在初始化周期中中断控制 SIMM 的主计算机的问题。在加电时必须允许主计算机执行初始化功能。然而，一旦初始化了存储器便不容易禁止它。本发明采用在模块加电时递增（或递减）的计数器来克服这一问题。如果在计数器到达其预定值之前模块并未收到一定的代码或代码序列，模块上的控制机构便通过诸如禁止数据缓冲器而禁止该模块，从而导致计算机中的出错。

所采用的计数器可计数时钟周期、刷新周期数、读或写周期或某些其它操作数，例如列地址选通（CAS）进入活跃（或不活跃）的次数。

代码或代码序列是存储在模块上的非易失性存储器中的。在计算机的用户端上，由 BIOS（基本输入/输出系统）或从软件输入代码或代码序列，例如从计算机的初始化文件。甚至可令用户手动输入代码或代码序列。可以用类似于口令的方式输入代码或代码序列，甚至可将代码链

接在击键速度上，诸如用户口令的字符之间的“时间卷绕”间隔上。

在一些实施例中非易失性存储器与控制机构可在同一器件（应用特定的集成电路 ASIC ）中。

可以通过禁止这些存储电路或存储器件的输出使能而禁止该存储电路的输出。

本发明的优点在于控制机构在要求安全代码来启动或禁止该模块之前它等待初始化存储器模块。

虽然可以采用初始化文件之一（诸如个人计算机中的 autoexec.bat 文件）来输入代码，但这具有能复制文件及被检查以检索代码的缺点，而最好在每次引导计算机时手动输入代码。

作为避免这一问题的一种替代方案为将这一代码加入快速引导 EPROM 中或使用一个口令编码该文件，例如，在装入存储器模块时，配置或安装程序提示用户输入口令，安装软件将其与启动存储器安全器件所需的密钥一起编码。然后将一个程序加到 config.sys 、 autoexec.bat 或其它初始化批处理程序中以提示用户输入口令，然后用它来解密密钥文件并将其写入存储器模块的控制器上。不能提供正确的口令将导致计算机超时并使计算机的存储器不能操作。

可以理解在本发明的范围内可对上述实施例作出各种修正。

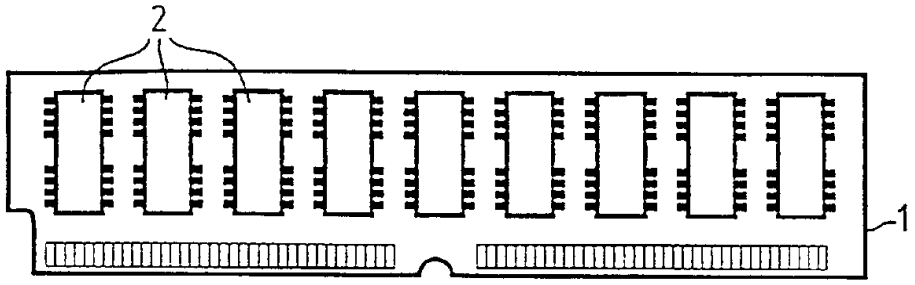

图 1A

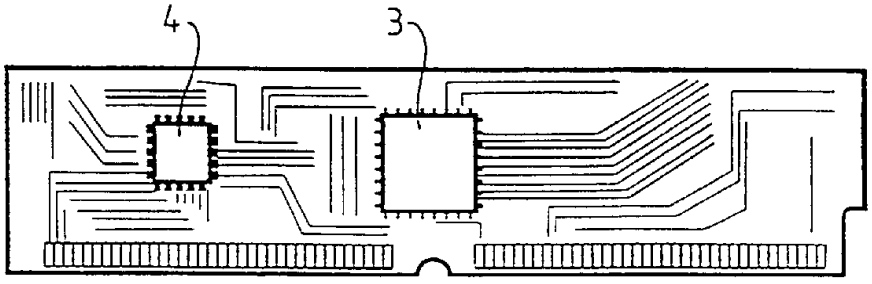

图 1B