

[12] 发明专利说明书

[21] ZL 专利号 96122285.9

[45] 授权公告日 2002 年 5 月 22 日

[11] 授权公告号 CN 1085359C

[22] 申请日 1996. 12. 11

[21] 申请号 96122285.9

[73] 专利权人 中国科学院长春光学精密机械研究所

地址 130022 吉林省长春市人民大街 140 号

[72] 发明人 乔燕燕

[56] 参考文献

CN 1063372A 1992. 8. 5 G06F12/14

CN 1070058A 1993. 3. 17 G06F12/14

US 5081675A 1992. 1. 14 H04L9/00

审查员 朱世茵

[74] 专利代理机构 长春科宇专利代理有限责任公司

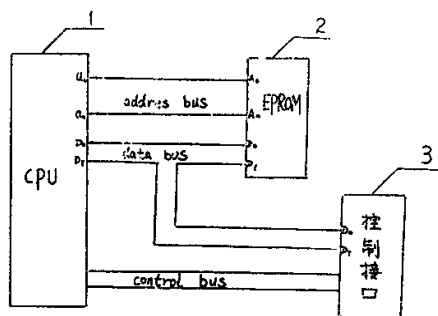
代理人 梁爱荣

权利要求书 1 页 说明书 3 页 附图页数 2 页

[54] 发明名称 一种应用程序的加密方法及装置

[57] 摘要

本发明属于计算机应用技术领域,涉及用装有应用程序的可编程只读存储器 和利用计算机寻址,对应用程序进行加密的方法及装置。本发明在可编程只读存储器的地址总线输入端产生与中央处理器地址总线输出端的地址信号不同址的寻址信号,由中央处理器执行可编程存储器的指令去控制接口完成控制工作。它包括中央处理器、可编程只读存储器、控制接口,采用地址总线交叉对应联接方式 克服了已有技术中的缺点,使得加密装置简单且工作可靠,造价降低,使用方便。



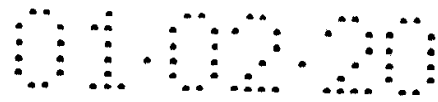
ISSN 1008-4274



权 利 要 求 书

1、一种应用程序的加密方法，其特征在于：首先在电可编程只读存储器的地址总线输入端(A_j)产生与中央处理器地址总线输出端(a_i)输出的地址信号不同址的寻址信号，然后用计算机系统和万能编程器把地址总线(a_i)的寻址内容转换成与地址总线(A_j)相同地址的寻址内容，再将其转换的地址内容固化在电可编程只读存储器中，中央处理器通过读出电可编程只读存储器的内容，由中央处理器执行电可编程只读存储器的指令去控制接口完成控制工作。

2、一种应用程序的加密装置，它包括中央处理器(1)、电可编程只读存储器(2)、控制接口(3)，其特征在于：中央处理器(1)的地址总线的输出端(a_i)与电可编程只读存储器(2)地址总线的输入端(A_j)根据应用程序加密程度可任意互换，使地址总线(a_i)和(A_j)任意交叉对应联接，电可编程只读存储器(2)的数据输出端与中央处理器(1)的数据端联接，中央处理器(1)的数据端与控制接口(3)的数据端联接。



说明书

一种应用程序的加密方法及装置

本发明属于计算机应用技术领域，涉及用装有应用程序的电可编程只读存储器和利用计算机寻址，对应用程序进行加密的方法及其装置。

已有技术如《电子技术应用》1993年第9期P39-40 公开的对应用程序加密的方法及装置。其加密方法是：把应用程序比作密码锁，利用单片机内部的RAM区，预先写入可计算出应用程序入口地址的有关密码数据。其装置是由中央处理器、随机存取存储器，电可编程只读存储器、掉电保护电路、键盘或开关组成。它是通过掉电保护电路保护随机存取存储器中存放计算应用程序入口地址首址程序的数据，通过计算入口地址首址程序产生电可编程只读存储器程序的入口地址。其缺点是更换掉电保护电路的电池或对电池碰撞都会使上述工作失效，使应用程序陷于瘫痪。在恢复工作时，需要借助附加的随机存取存储器程序输入手段和键盘或开关则使加密装置造价高，且给使用者带来许多不方便。

本发明的目的在于：解决掉电保护电路带来的加密装置工作不可靠，易使应用程序陷于瘫痪的问题。恢复数据时要附加随机存取存储器、键盘或开关等带来加密装置造价高，使用不方便的问题。

本发明的加密方法：首先在电可编程只读存储器的地址总线输入端 A_j 产生与中央处理器地址总线输出端 a_i 输出的地址信号不同址的寻址信号。

第二，用计算机系统和万能编程器把地址总线 a_i 的寻址内容转换成与地址总线 A_j 相同地址的寻址内容，然后将其转换的地址内容固化在电可编程只读存储器中，中央处理器通过读出电可编程只读存储器的内容，由中央处理器执行电可编程只读存储器的指令去控制接口完成控制工作。

本发明的加密装置：它包括中央处理器 1、电可编程只读存储器 2、控制接口 3，其特点是：中央处理器 1 的地址总线的输出端 a_i 与电可编程只读存储器 2 地址总线的输入端 A_j 根据应用程序加密程度可任意互换，使地址总线 a_i 和 A_j 任意交叉对应联接，电可编程只读存储器 2 的数据输出端与中央处理器 1 的数据端联接，中央处理器 1 的数据端与控制接口 3 的数据端联接。 $i=1, 2, 3 \dots n, j=$



1、2、3……n。其中i为中央处理器1地址总线序号, j为电可编程只读存储器2的地址总线序号, n为电可编程只读存储器允许地址线根数。

本发明的积极效果: 已有技术由于采用随机存储器则需要用掉电保护电路使其工作正常, 更换电池或有电池故障时则会使应用程序瘫痪, 本发明采用地址总线交叉对应联接, 则不需要随机存储器也就不使用掉电保护电路和恢复工作中所需的随机存储器、键盘或开关等, 使得加密装置工作可靠、造价低、使用方便, 若拷贝本发明电可编程只读存储器2的内容, 只能得到与加密前完全不同的程序, 该程序指令排列无序, 则不能完成任何控制功能, 从而达到对应用程序加密目的。本发明不会给系统扩展带来任何不良影响, 没有系统的兼容性问题。

图1是本发明的结构示意图。

图2是本发明中的一种实施例示意图。

本发明的实施例: 中央处理器1可选择Z-80, 8031或8098单片CPU芯片, 可编程只读存储器2可选择2716、2732、2764等电可编程只读存储器, 控制接口3可选择串行口SIO、8251或并行PIO、8255等。用图2叙述本发明中的一种实施例, 当中央处理器1选Z-80, 电可编程只读存储器2选择2716电可编程只读存储器, 控制接口3选择PIO并行输入输出芯片, 随机存储器4选择6116静态RAM芯片, 输入输出I/O译码器5选择74LS138译码器, 显示器及键盘电路6选择8段共阴极显示器及相应的按键电路时, 其工作程序为:

用Z-80指令系统编写应用程序, 用能编译Z-80指令系统的计算机编写对应用程序进行变换的程序; 然后由万能编程器将变换的应用程序写入电可编程只读存储器中。

变换应用程序的变换程序为:

- 1、将应用程序的首址存入变址寄存器。
- 2、将应用程序交换循环次数存入计数器。
- 3、交换的步长16送步长寄存器。
- 4、通过变址寄存器取来要交换的应用程序地址所对应的一对内容进行交换之后, 再取下一对内容交换。例如当选择i和j不同的数值时, 中央处理器1地址总线 a_i 端联接到2716存储器2的地址总线 A_j 端, 及地址总线 a_j 端联接到 A_i 端, 所

以要连续四次上述交换，即完成002H-008H, 003H-009H, 006-00CH, 007-00DH地址内容的交换。

5、步长寄存器与变址寄存器相加，得到下一组要变换的首址，同时交换循环次数减“1”，如果交换循环次数为“0”，则整个交换工作完成，否则继续进行上述的操作。

图2显示了本发明地址总线的交叉联接的一种结构，中央处理器1的 a_1 和 a_3 交叉联接到电可编程只读存储器 A_3 和 A_1 端即产生了新的寻址，当中央处理器要寻址电可编程只读存储器2的002单元时，其实际寻到是电可编程只读的存储器2的008单元，而中央处理器1要寻003单元时则寻到电可编程只读存储器2的009单元，如此继续下去就得到了因交叉互联方式，所产生的新的寻址内容的效应。在本发明中，中央处理器1可以准确无误地读到正确的指令序列，完成RAM4的读写数据，显示器6的输出，通过控制接口对键盘信号的读入及其它控制接口的控制工作。本发明交叉联接的地址结构使得一种新的寻址产生，能够正确引导中央处理器1完成应用程序所编制的工作，而又不能使应用程序被拷贝反汇编得到源目的代码，从而达到应用程序的加密目的。

根据图1和图2选择 a_i 与 A_j 的交叉联接关系有多种联接方式，即在电可编程只读存储器2的寻址范围内的地址总线与所对应中央处理器1的地址总线的任意二对，任意三对，任意 $n/2$ 对的地址线的交叉互换，其中 n 为电可编程只读存储器2的最高位地址序号。交叉联接的关系完全取决于加密者的需要和交换程序相对应的编写方法。

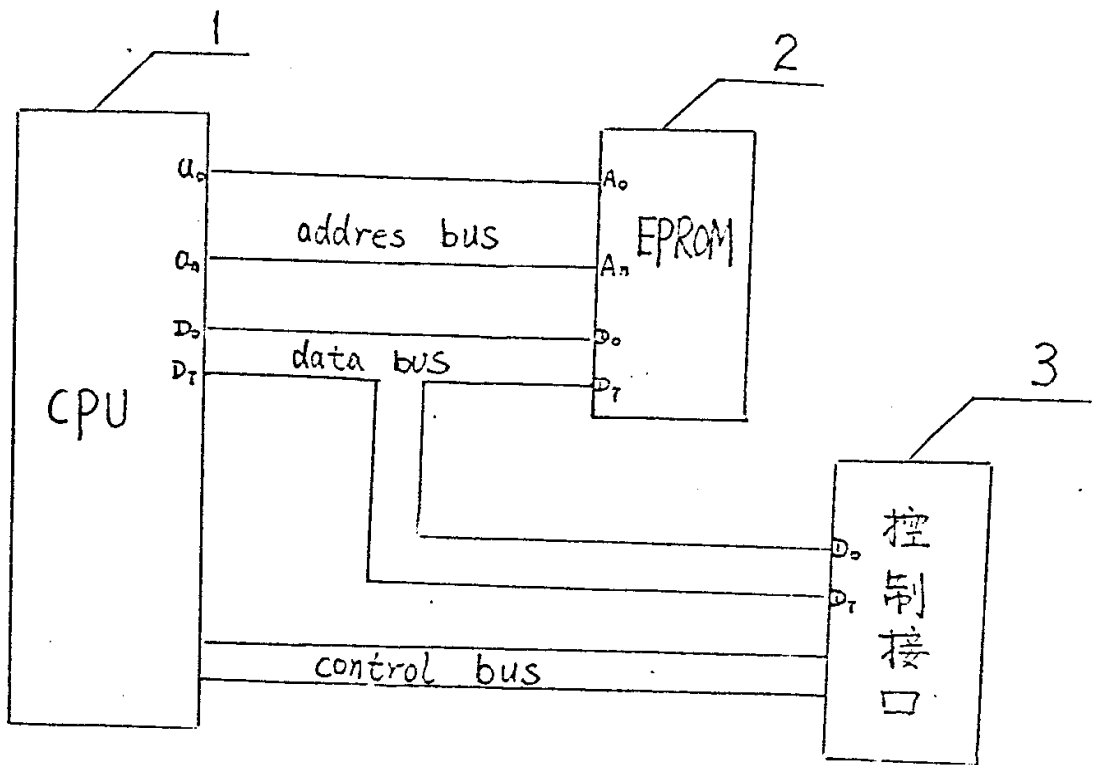


图 1

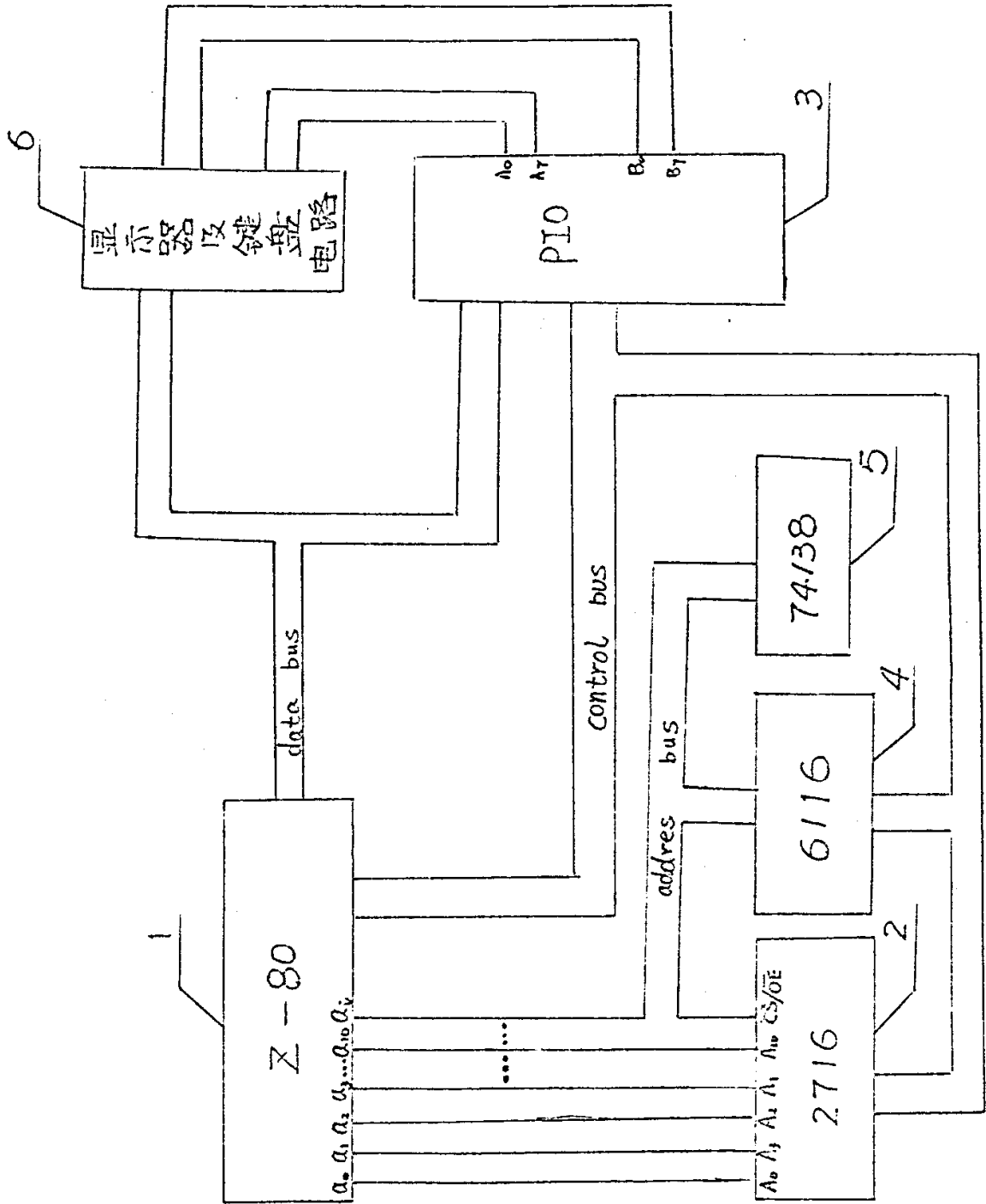


图 2