微机 BIOS 的保护

房毅卓,雷亚川

(中国科学院青海盐湖研究所,青海 西宁 810008)

摘要:介绍了一种纯硬件方式的微机BIOS程序保护方法,从根本上解决了病毒对BIOS的侵害,具有一定实用价值。

关键词:计算机;BIOS;E^2PROM;CIH病毒

中图分类号:TP36 **文献标识码**:A **文章编号**:1008-858X(2001)03-0063-03

微机BIOS是操作系统和应用软件同硬件设备之间的桥梁,病毒对BIOS的破坏,将会使微机系统完全瘫痪,对实际工作造成的影响是不可估量的,对BIOS的保护具有十分重要的意义。

1 微机的启动

各类PC机在加电或系统启动[1](RESET)后,都要对基本组成的硬件系统进行自诊断测试及初始化。经诊断无误后,进行系统的初始化,开始引导磁盘上的操作系统,把系统的控制权交给DOS操作系统,进入正常运行,如果在自诊断中发现错误,将根据性质作出反应:包括停机、音响报警、显示出错讯息,供操作人员进行处理。

BIOS是基本输入输出系统。它既是操作系统和应用软件同硬设备之间的接口。也是所有系统软件和应用程序工作的基础。

2 系统板中的BIOS芯片介绍

从80286CPU到80486CPU的系统板中,用作BIOS的芯片大多数是采用紫外线可擦除的只读存储器。随着系统板的发展,先后有2764(8kB×8)、27128(16kB×8)、27256(32kB×8)、27512(64kB×8)、TC27010D-20(128kB×8)问世,除TC27010是32只引脚之外,其余的均为28脚芯片。它的工作原理是地址信号A0~A15输入到地址缓冲器,由译码器译出131072条控制线去选中每一个单元,产生8位数据。8位数据经门电路和缓冲器输出。$\overline{CE}$是片选信号,$\overline{CE}$为低电位时,芯片才能工作。$\overline{OE}$是输出使能,低电平时使数据输出。PGM是编程控制信号,写EPROM时,加入高压脉冲,才能把数据和程序固化。EPROM的一个特点是可用紫外线擦除。芯片正面有透明小窗口,紫外线透过可擦除原内容,随着系统时钟频率的提高,要求用作BIOS的芯片读出速度也要加快,应根据CPU速度选用相应的芯片。为提高CPU工作速度,586CPU以上的系统板中普遍采用电擦除E^2PROM(也称为FASH)芯片。

3 EPROM的工作模式[3]

EPROM的工作模式由片选信号$\overline{CE}$、输出允许$\overline{OE}$电平高低以及编程电压V_{pp}、编程脉冲PGM输入端所接电平决定。表1给出了EPROM的工作模式。可电擦除E^2PROM工作模式与EPROM基本相同,只是其编程电压与电源电压只用一组5V电源。

28Cxxx和29Cxxx系列[2]用Xicor有专利的高性能浮栅CMOS工艺制造。是只用5伏的E^2PROM

收稿日期:2000-03-18

作者简介:房毅卓(1963-),男,工程师。

表 1 EPROM 的工作模式

Table 1 Working made of EPROM

工作模式	输入					输出
	$\overline{CE}$	$\overline{OE}$	V_{pp}	V_{cc}	PGM	
读	L	L	H	V_{cc}	V_{cc}	数据输入
输出禁止	L	H	H	V_{cc}	V_{cc}	高阻态
使用(功率下降)	H	X	X	V_{cc}	V_{cc}	高阻态
禁止编程	H	X	X	V_{PP}	V_{cc}	数据输入
编程	L	H	L	V_{PP}	V_{cc}	数据输入
校验	L	L	H	V_{PP}	V_{cc}	数据输入

器件。具有高速存取和可编程不挥发的存储器，$28C_{xxx}$ 和 $29C_{xxx}$ 以被 JEDEC 批准的字节宽存储器引脚为特色，与工业标准 EPROM 兼容，586 以上微机中的 BIOS 芯片均支持 256 字节页而写入操作，有效的提供 19 μs/字节写入周期，并允许在 2.5 秒典型值时间内整个存储器写入完成。还以 DATA 轮询和反复位测试为特色，系统软件支持电路用以指示早先写入周期的完成。此外，还支持软件数据保护选件，其 BIOS 程序的升级可以在系统板上直接进行。

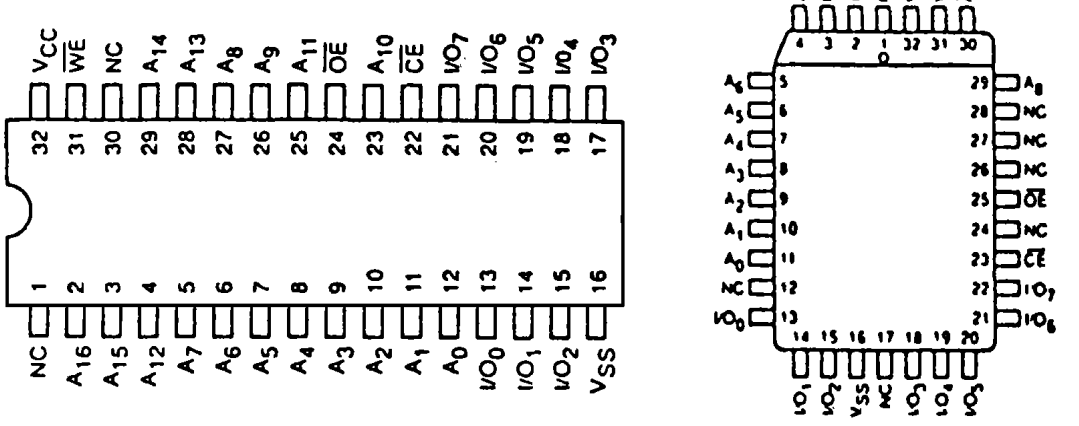
4 CIH 病毒简介

2000 年 4 月 26 日在全球爆发的 CIH 病毒，导致了数以万计的 PC 机瘫痪，整个亚太地区的损失尤为严重。据调查，CIH 病毒在我国造成的直接损失为 0.8 亿元，间接损失超过 10 亿元。

CIH 病毒是一种恶性病毒，也是迄今为止破坏力最为严重的病毒之一。CIH 病毒发作时，对主板的破坏是通过识别某些主板上 BIOS 的写入口，对 Flash BIOS 进行写操作，将一堆垃圾码写入 BIOS 中，造成 BIOS 程序紊乱，导致主板瘫痪；而对硬盘的破坏主要是通过覆盖和改写硬盘数据。CIH 病毒会调用 IOS Send Command 直接对硬盘进行存取，将垃圾码以 2048 个扇区为单位从主引导扇区开始依次写入硬盘，导致主分区表、逻辑盘引导记录、第一个逻辑盘的目录区和 FAT 表全被破坏。

5 系统板中的 BIOS 的程序的保护

从以上介绍可见，486 及以下系统板中，由于基本采用紫外线可擦除 EPROM，并需提供专用的 V_{pp} 编程电压，其编程需专用的设备在离板进行，因此，任何病毒程序均不能对其构成威协，586 以上系统板，因普遍采用 28 和 29 系列 E^2PROM，其 BIOS 程序可直接在板上升级，因此为病毒的入侵提供了可乘之机。由于，BIOS 程序在一般情况下，用户很少需要改动，并且从 EPROM 工作模式表可见，若$\overline{WE}$恒为高电平时，任何方式均不能对芯片写入数据，从根本上保证了 BIOS 程序在病毒入侵时不能被改写，彻底避免了病毒对 BIOS 的危害，其具体操作方法如下，从系统板上找到型号为 $28C_{xxx}$ 和 $29C_{xxx}$ 的芯片，此芯片一般装在一专用插座上，外型如图 2 所示，将 31 脚向外轻轻撬出，在 32 和 31 脚之间焊接－50kΩ1/16W 的电阻，再将其插入原来位置，注意，此时引脚不插入插座，对其写入时，应用导线将插座引脚和 E^2PROM 引脚接通。



(a) DIP 封装、扁平封装

(b) PLCC、LCC 封装

图 1 引脚配置图

Fig. 1 Confguration of interface

由于以上介绍的保护方法,是一种纯硬件保护方法,因此对任何侵害 BIOS 的病毒在改装后的系统板上均有防护作用,是一种行之有效的方法,若系统板厂家在生产时在板上装 BIOS 状态设置开关,相信对 BIOS 的保护大有裨益。

参考文献:

[1] 蒋连生.微机电路分析与维修全书[M].北京:电子科技大学出版社,1996.
[2] 侯光华.世界最新集成电路[M].大连:大连出版社,1993.
[3] 张友德.单片机原理、应用与实验[M].上海:复旦大学出版社,1993.

Protection of PC BIOS

FANG Yi-zhuo, LEI Ya-chuan

(*Qinghai Institute of Salt Lakes, Chinese Academy of Science, Xining* 810008, *China*)

Abstract: This article introduces a hardware methed to protect BIOS of PC from invention of virus, which may be actually useful.

Key words: Computer; BIOS; E^2PROM; Virus