[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/30 (2006.01)
G06F 12/16 (2006.01)

[12] 发明专利说明书

专利号 ZL 94119411.6

[45] 授权公告日 2007 年 6 月 20 日

[11] 授权公告号 CN 1322424C

[22] 申请日 1994.12.20 [21] 申请号 94119411.6
[73] 专利权人 肖 勇
地址 272116 山东省济宁市建设北路 47 号
[72] 发明人 肖 勇
[56] 参考文献
CN 2081110U 1991.7.17
US5144660 1992.9.1
CN 1080750A 1994.1.12
US 5144660 1992.9.1
审查员 熊 婷

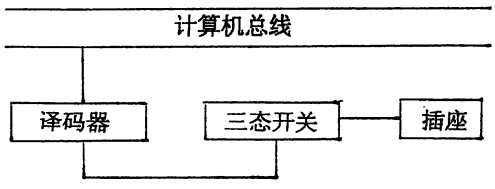
权利要求书 1 页 说明书 3 页 附图 2 页

[54] 发明名称

计算机防病毒卡

[57] 摘要

本发明属计算机防病毒技术的计算机技术领域。它包括一块防病毒卡和与之相适应的钥匙软盘。防病毒卡中又包括译码器和三态开关，其工作过程为由逻辑电路对计算机访问病毒侵害硬盘的指令进行译码，所说的钥匙盘其作用是引导用户安全操作，本发明与现有技术相比在原理上解决了安全区内不被病毒入侵且不非法限制操作系统的正常权利，还有防病毒卡体积小，使用元器件少和操作简单易行。



1、一种计算机防病毒卡，其特征在于防病毒卡中包括硬盘指令译码器和三态开关，其中译码器的输出端连接三态开关的通断控制端，由逻辑电路对包括侵害硬盘的病毒指令在内的计算机访问硬盘的指令进行译码，修改硬盘的某些物理空间组成的安全区时，译码器可以控制三态开关断开，不修改硬盘的某些物理空间组成的安全区时，译码器可以控制三态开关闭合。

2、根据权利要求 1 所述的计算机防病毒卡，其特征在于，修改硬盘的某些物理空间组成的安全区时，译码器可以输出高电平控制信号，此信号控制三态门断开，使主系统和硬盘无法通讯，不修改硬盘的某些物理空间组成的安全区时，三态开关闭合，主 CPU 对硬盘通讯无阻。

3、根据权利要求 1 所述的计算机防病毒卡，其特征在于，通过读取钥匙盘上的程序，可以实现逻辑盘分区链的修改，引导用户安全操作。

计算机防病毒卡

本发明涉及的计算机防病毒技术属计算机技术领域。

对于计算机病毒的防治，基于“治”的，主要是各种消毒软件，其意义在于它是对于已遭到病毒侵害的对象的一种补救。其致命缺点是被动。基于“防”的，主要是一些免疫软件和一些抗毒卡。其意义在于它们不同程度地增加了病毒入侵的难度，其缺陷在于，它们主要仍然依靠系统主CPU控制，病毒完全可以通过主CPU攻破其防线。虽然也已有人提出“独立于系统主CPU的预防方法”，但离实用产品乃至一种切实可行的技术方案恐怕还有一段距离。其缺陷在于“非法访问（病毒入侵）”与“合法访问（非病毒操作）”的划分仍然延用人为限制标准，即对病毒入侵采取“堵截”之法，这必然导致系统正常合法权利受到非法限制，使某些应用软件运行受碍。这是因为对于操作系统管辖的资源，系统随时都有权访问。这是其一，也是上述方法在防毒机理上的原理性不足。而且“访问权利表”的生成亦不易实现。其二，按上述方法“在原系统硬件环境中附加的保护机构硬件”，在技术上不易实现，尤其是对于那些缺乏技术资料的机型（如：原装AST、COMPAQ计算机），在技术上更难实现。

本发明的目的在于克服上述缺点：根据新的防病毒机理，提出一种新的防病毒卡的产品及切实可行的技术方案。

本发明采取的措施为：

1.在防毒机理上，以对病毒入侵采取“疏导”之法代替原有的

“堵截”之法。在非挥发性介质上（主要是硬盘）上开辟安全区，使病毒无法入侵，同时引导系统避开此安全区或将系统引导向别的地方，从而使系统的正常合法权力不会受到非法限制。

2.上述安全区被插在扩展槽上的硬卡绝对地保护着。硬卡在技术上易于实现，即使对于技术很不透明的原装AST、COMPAQ机型，实验证明均切实可行。

3.上述安全区的合法访问通过干净（无病毒）钥匙软盘启动机器，并根据屏幕提示辅以人为硬开关设置进行安全访问。

结合一种实施例说明原理及实现方法：

图1是防病毒卡在计算机总线上的框图。

图2是防病毒卡的原理图。

本发明的特征在于，它包括防病毒卡和与之相适应的钥匙软盘，在防病毒卡中包括译码器和三态开关，其工作过程为由逻辑电路对计算机访问病毒侵害硬盘的指令进行译码，从而达到保护硬盘安全区的目的，所说的钥匙盘，它是一张干净的启动盘，在盘上记录有关操作硬盘安全区，使该安全区成为操作系统的不访问的隐含区域的应用程序以及引导用户安全操作的应用程序。

我们可以通过DOS系统的INT13得到某一具体机型是怎样访问硬盘的。在实施例中，我们知道，对于COMPAQ、AST机型，系统主CPU写硬盘0100—01FF磁道时，是通过向I/O端口1F5写01（硬盘磁道高2位），向1F7写30（写命令码）来完成的。

U1、U6、U8与U2组成主系统的一个I/O端口（地址为1F5），U1、

U6、U8 与 U4 组成系统的另一个 I / O 端口（地址为 1F7），两个端口与U7、U9、U10、U11、U12、U3、U5共同作用，使主CPU修改(写或格式化）硬盘 0100 — 11FF 磁道时，由 U12 第三脚输出高电平控制信号，此信号控制三态门 U13 断开， 从而将连在 U13 上的电缆线（连接主系统与硬盘的控制电缆线）断开，使主系统和硬盘无法通讯，而达到保护硬盘的目的。主 CPU 对硬盘的其他操作，则此卡保证主 CPU 对硬盘通迅无阻。

在硬盘开工时，我们可以用 DOS 的 FDISK 将待开辟的安全区（例如：硬盘 0100 — 11FF 磁道）设为一个逻辑盘（例如 D 盘）。然后将此逻辑盘的分区链改掉（例如改为全 0）。这样，此逻辑盘就成为操作系统的一个隐含盘，正常情况下，系统不会访问此安全区。

需合法访问安全区时，用一张干净的钥匙软盘启动机器，用户只需根据提示操作即可。在用户的人为干预下（拨动开关 U18，使硬卡接通或关闭）由钥匙盘上的软件自动完成隐含逻辑盘分区链的恢复、修改访问（安全区一般不要设为工作区，只有确认无病毒的软件才可直接在隐含盘上运行）操作。

本发明与现有技术相比在原理上解决了安全区内不被病毒入侵且不非法限制操作系统的正常权利，方案实践证明切实可行。还有就是防病毒卡体积小，使用元器件少和操作简单易行。

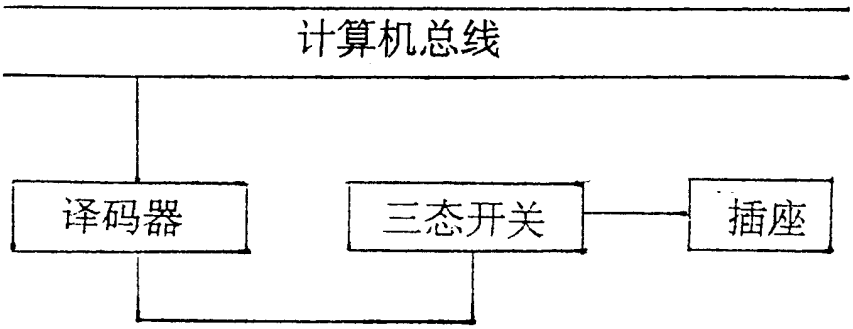


图1

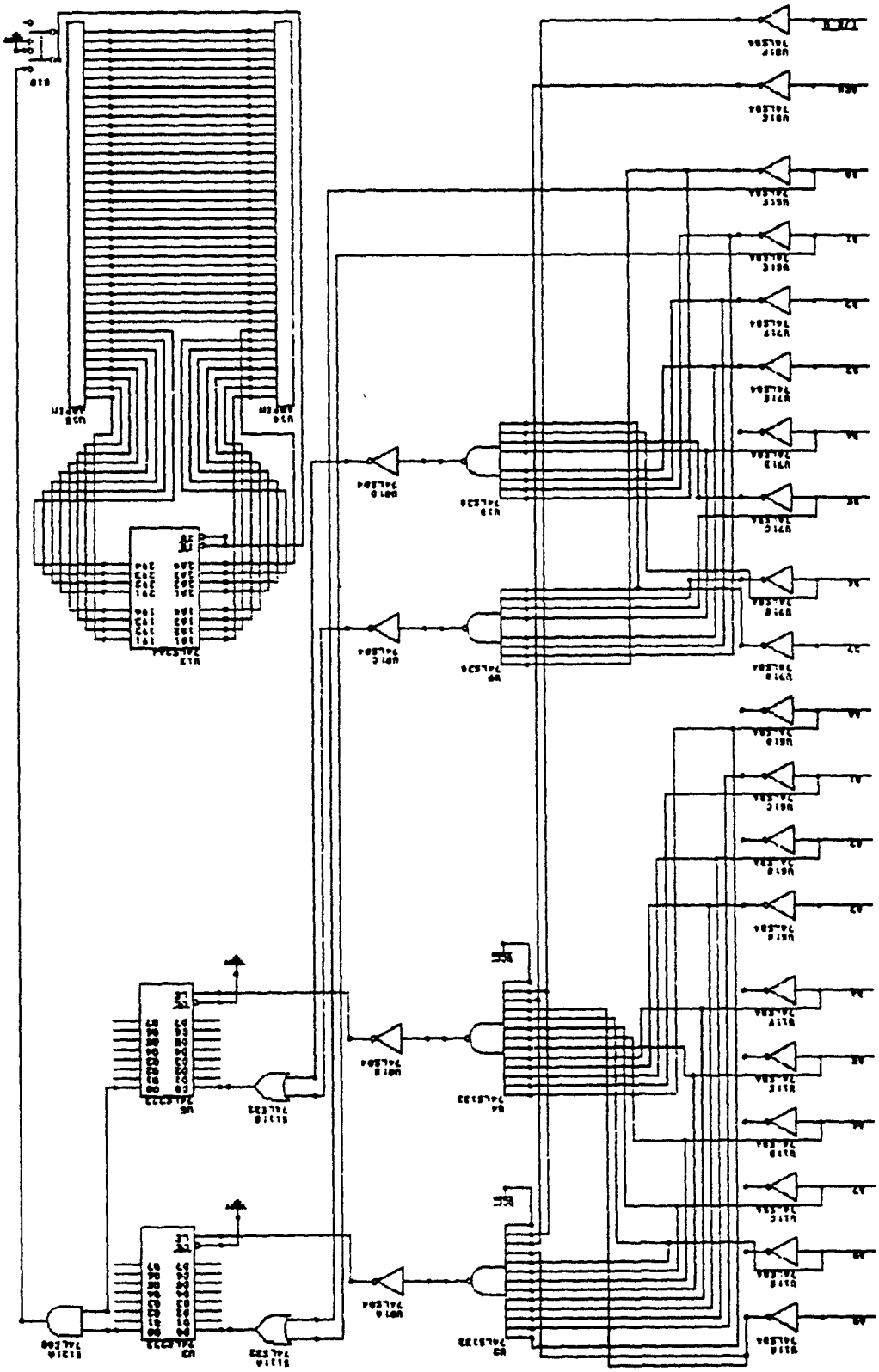


图2