[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06F 12/16 (2006.01)

[12] 发 明 专 利 说 明 书

专利号 ZL 02113032.9

[45] 授权公告日 2009 年 4 月 8 日

[11] 授权公告号 CN 100476761C

[22] 申请日 2002.5.20 [21] 申请号 02113032.9

[73] 专利权人 邵 通

地址 211100 南京市江宁科学园科宁路 766 号综合楼三楼

[72] 发明人 邵 通

[56] 参考文献

CN1170160A 1998.1.14

US5657445A 1997.8.12

CN1210307A 1999.3.10

审查员 赵 强

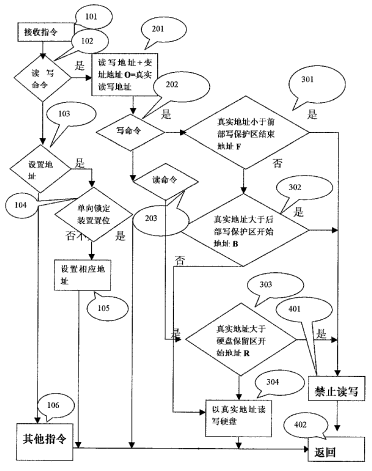
权利要求书 2 页 说明书 14 页 附图 8 页

[54] 发明名称

一种实现硬盘安全隔离的装置及方法

[57] 摘要

本发明提出了一种实现安全并兼容地隔离硬盘中操作系统的装置及方法。它采用单向锁定装置和硬盘设定地址禁止改变装置构成一个完整且安全的隔离硬盘操作系统的装置。进一步使用硬盘保留区、硬盘前部写保护区、硬盘后部写保护区及硬盘变址技术，可以安全实现一个硬盘在实现隔离操作系统的同时进行数据交换或进行单向数据交换。



1、 一种实现硬盘安全隔离的装置，它包括

单向锁定装置；

硬盘设定地址禁止改变装置；

硬盘变址装置；

硬盘保留区装置；

其中，单向锁定装置是一有当计算机加电或复位时，才能复位的寄存器装置，或为一有机械开关才能改变状态的装置，当单向锁定装置置位时，锁定当前硬盘设定地址；硬盘设定地址禁止改变装置根据单向锁定装置的置位状态，禁止硬盘执行任何能够改变硬盘设定地址的命令；硬盘变址装置用于读写保护硬盘前部区域数据安全及提供软件兼容性，其中硬盘变址基址属于所述硬盘设定地址；硬盘保留区装置，用于读写保护硬盘后部区域数据安全，其中硬盘保留区开始地址属于所述硬盘设定地址。

2、 根据权利要求 1 的装置，其特征在于还包括硬盘后部写保护区装置及硬盘前部写保护区装置。硬盘后部写保护区装置用于写保护硬盘后部区域数据安全，其中硬盘后部区域开始地址属于所述硬盘设定地址；硬盘前部写保护区装置，用于写保护硬盘前部区域数据安全，其中硬盘前部写保护区域结束地址是属于所述硬盘设定地址。

3、 根据权利要求 1 的装置，还包括一个改变硬盘变址装置基址地址的装置及一个改变硬盘保留区开始地址的装置。

4、 根据权利要求 1 的装置，其特征在于它连接于计算机主板与硬盘之间。

5、 根据权利要求 2 的装置，其特征在于还包括改变硬盘后部写保护区开始地址的装置及改变硬盘前部写保护区域结束地址的装置。

6、 根据权利要求 4 的装置，其特征在于它处于计算机主板上控制与处理硬盘接口的芯片组中。

7、 根据权利要求 4 的装置，其特征在于它处于硬盘驱动器中。

8、 根据权利要求 4 的装置，其特征在于它还包括身份认证装置。

9、 一种实现硬盘安全隔离的方法，它包括：

重新启动计算机，同时复位单向锁定装置；

设定用户可存取区域硬盘设定地址；

置位单向锁定装置；

启动计算机操作系统；

其中设定用户可存取区域硬盘设定地址步骤包括设定变址基址及保留区开始地址。

10、根据权利要求 9 的方法，其中设定用户可存取区域硬盘设定地址步骤还包括一个根据用户身份认证步骤。

11、根据权利要求 9 的方法，其中所述变址基址、保留区开始地址、后部写保护区开始地址、前部写保护区结束地址存放于 CMOS 或硬盘中。

一种实现硬盘安全隔离的装置及方法

发明领域

本发明涉及的是一种实现硬盘安全隔离的装置及方法，具体地说，涉及一种如何安全并兼容地隔离硬盘中多个操作系统的装置及方法。

背景技术

目前在计算机安全中，出于安全考虑实行内部网（办公或机密网）与外部网（例如，因特网）进行物理隔离；或者在家用电脑中，需要内部网（私密数据，不一定连网）与外部网（例如，因特网）进行物理隔离。解决的方法有所谓的单硬盘方案及双硬盘方案。双硬盘方案是指在一台计算机中安装两个硬盘，当需要使用内部网时，用对应于内部网的硬盘启动，并接通对应于内部网的网络联接（或不与网络连接）；当需要使用外部网时，用对应于外部网的硬盘启动，并接通对应于外部网的网络联接。显然，为了安全当外部网（或内部网）启动后，使得内部网（或外部网）用硬盘及网络联接，从物理上被隔离（即绝对不可用，或不能有效地读写）。这样实现了一台计算机可以使用内部网及外部网，同时保证内外网隔离及内部数据安全。

显然双硬盘方案，安全地实现了内外网的物理隔离。但是这个方案需要两个硬盘，使得该方案的实现成本也比较高，这样就有所谓的单硬盘方案。它指的是，在一个硬盘上分两个分区，每个分区均有自己的操作系统（分别对应于内部网和外部网）；然后选择计算机启动内部网或外部网；或使用实时切换计算机，请见本人申请号为 01115545.0 及 01117401.3 的待批中国发明专利申请。在单硬盘方案中，当系统处于外部网时，至少必须保证内部网中的数据不能被读写。有关该技术详细内容请见本人的已授权发明专利 ZL94111461；当系统处于内部网时，必须保证外部网的硬盘区域不能被写(最好不能被读写)，这样才能保证内部网中的数据不被泄漏到外部网中；同时又需要启动多个操作系统（内部网及外部网）。启动多个操作系统，比较好的方法是二次启动，有关该技术详细内容请见本人申请号为 97116855.5 的待批中国发明专利申请，上述的所有在在

先申请作为参考结合在本发明中。同时它还可以方便地恢复系统，解决了操作系统崩溃后的安全管理问题。另外在单硬盘方案中，如果从硬盘上实现一个交换区，在外网启动时该区能读写，而在内网启动后，该区只读不写。这样可以保证信息只能从外网向内网单向传递，保证内网信息绝对不可能自动泄露。当然也可以让交换区任何时候均可读写，但是，这将使安全性有所下降。总之在保证安全隔离的同时，可以以灵活而安全的方式实现内外网数据的安全交换。

总之，使用单硬盘解决方案的实质是把硬盘分为多个操作系统区域(两个或更多)，当一个操作系统启动后，根据具体安全需求使其不能读写（或不能写）其他操作系统所占用的硬盘区域。

但是，分区安全保证及多操作系统的安装，对于广大的计算机使用人员是比较困难的，对它的理解也比较困难。同时，一般情况下，多操作系统的启动均需要改变分区表中的程序或数据。这样对于有些操作系统的安装与启动，会产生一定的兼容性问题。另外，当硬盘增大而操作系统升级跟不上时，也会产生安装的困难。例如，一个 40G 的硬盘，为了分区安装内外网，需要对硬盘进行相应的规化，最好是前 20G 为内部网，后 20G 为外部网。但是，由于产品设计上的缺陷，WIN95 不能安装到 8G 以后，所以这样分割硬盘，实际上无法安装。为了解决这个问题，只能采取内部网（或外部网）使用 6G，其它给外部网（内部网）；或者使用多个分区，使内部网使用的分区与外部网使用的分区交错，所以实际上无法按照上述要求进行硬盘分区和安装多操作系统。前一种解决方案使用不方便灵活，后一种方案保护的方法相对复杂成本较高、用户理解困难且安装困难。

为此，比较好的方法是使用硬盘变址，有关该技术内容请见本人申请号为 00132989.8 的待批发明专利申请，该在先申请作为参考结合在本发明中。现在硬盘厂家已经意识到硬盘变址技术在解决硬盘多系统启动中的用途，并以一种特殊（不方便）的方式实现了硬盘变址技术。现在硬盘标准中实现变址技术的

方法如图 1（参见 US 6,415,383）。 首先，计算机用硬盘的特殊命令（F 8 及 F 9）（参见 US 5,966,732），例如以 R 值执行非易失 Set Max_Address (F9)命令后，如图 1A 所示将硬盘分出两个区域：用户可存取硬盘区域 **LBA（0）－LBA（R）** 及用户不可存取硬盘区域 **LBA（R）－LBA（M）**，在该图中 R 表示一个中间地址值，而 M 为硬盘的真实最大地址值。显然如果我们把用户可存取硬盘区域看成外网硬盘区域，用户不可存取硬盘区域为内网硬盘，则当计算机处于外网时，计算机不能存取内网区域。然后用户可以通过命令（Feature 寄存器中置 0 9 H，Command 寄存器中置 F E H），进入变址模式，其状态如图 1B 所示。显然如果我们把用户可存取硬盘区域看成内网硬盘区域，用户不可存取硬盘区域为外网硬盘，则当计算机处于内网时，计算机不能存取外网区域。但是，现行硬盘标准对于计算机安全的考虑有欠缺。用户可以通过命令（Feature 寄存器中置 8 9 H， Command 寄存器中置 F E H），退出变址模式，也可以通过软件复位（Device Control 寄存器 SRST 位置位）使硬盘退出变址模式。造成硬盘安全考虑不周的主要原因是硬盘的变址标准不是根据计算机使用者信息安全的要求来制定的。

显然从信息安全的角度，必需绝对禁止（包括禁止使用口令方式，因为口令方式相对不安全）用户能够改变用户可存取硬盘区域及用户不可存取硬盘区域大小（绝对禁止使用 F 9 命令），必需绝对禁止用户能够不受控制地进入或退出变址模式（禁止通过 Command 寄存器中置 F E H，进入或退出变址模式，禁止通过软件复位使硬盘退出变址模式），来破坏硬盘的安全策略。这里我们可以认为退出变址模式是，改变了变址地址（从变址地址值 R 改变到 0 —即不进行变址）。

显然从上述现行硬盘标准中可以看出，如果使用变址技术就没有硬盘后部的

保留区。这样就不可能在使用变址技术解决多操作系统兼容性同时，使用保留区原来的功能（BIOS 功能扩展，并保证用户的不可存取）。图 1 可以理解为，以 R 值设置变址（SetOffset）。

另外，在现在的硬盘标准中，有一些设置硬盘使用状态的命令及命令序列，也有一些保护用户设置的手段。但是这些保护手段一般为口令保护（即只要有口令就可以改变硬盘使用状态，如 F9 设置状态保护），或可以用软件复位（Device Control 寄存器 SRST 位置位）复位到初始状态（如，硬盘退出变址模式），或直接改变硬盘设置状态（如，硬盘退出变址模式，通过命令ＦＥＨ及子命令 89H）。而从隔离及安全的角度看，计算机必须具有单向锁定功能。它保证只有计算机加电或计算重新启动才能改变硬盘设定的状态。这样才能保证，当单向锁定装置置位后，任何硬盘设定状态的改变必须先通过计算机重新启动，进入肯定安全的程序（如 BIOS），在受控情况下进行硬盘状态的设置。绝对防止黑客改变硬盘的安全设置状态。

发明内容

为了在现有硬盘标准下实现单硬盘物理隔离的安全要求，本发明利用一个单向锁定装置来保证硬盘区域的物理隔离。当单向锁锁定（置位）后，可以禁止任何可能违反单硬盘隔离安全策略的硬盘命令。而单向锁定装置及禁止可能违反单硬盘隔离安全策略命令的装置（硬盘隔离装置）可能处于主板ＩＤＥ接口与硬盘ＩＤＥ接口之间，也可以处于主板控制ＩＤＥ的芯片组中，还可以处于硬盘控制器中。

本发明的目的是提出一种具体的实现硬盘安全隔离的装置及方法，其利用硬盘存取变址装置及硬盘变址存取方法与硬盘读写保护区有机结合，结合二次启动方法及单向锁锁定装置，可简单且安全地解决在单硬盘中安装多个操作系统时，操作系统之间隔离和软件兼容性、BIOS 扩展及兼容性问题。

显然，利用在前的专利可以解决这些问题，但是解决的方法不具体，综合以上三个专利及现有硬盘标准，可以用计算机用户容易理解的方式实现以上三个

专利，简单解决多操作系统隔离，软件兼容性，BIOS 扩展等安全问题。

本发明的目的是利用所述三个专利及硬盘标准，解决多操作系统隔离，软件兼容性，BIOS 扩展等安全问题。并提供一种具体的利用硬盘存取变址装置及硬盘变址存取方法与硬盘读写保护区的有机结合，加上二次启动方法及单向锁锁定装置，可以简单且安全地解决在单硬盘中安装多个操作系统时安全操作系统隔离及的软件兼容性问题。

根据本发明的一个方面，提供了一种具体实现硬盘安全隔离的装置，它包括：

单向锁定装置；

硬盘设定地址禁止改变装置；

其中，单向锁定装置是一只有当计算机（或硬盘）加电或复位时，才能复位的寄存器，当单向锁定装置为置位时，锁定当前硬盘设定地址，硬盘设定地址禁止改变装置根据单向锁定装置的置位状态，禁止硬盘执行任何能够改变硬盘设定地址的命令。

一般地，现行硬盘标准 ATA-7 中，在现在硬盘标准下被禁止计算机向硬盘发出的能够改变硬盘设定地址的命令：**SetMax Address** 命令、**Set features** 命令的子命令（89H）、及 **SRST**（软复位）命令。进一步可能禁止的命令是：**Set behind**(硬盘设置后部写保护区),**Set front**（设置硬盘前部写保护区）,**Set Offset**（设置硬盘变址地址）。

较佳地，实现硬盘隔离的装置处于硬盘控制器中，也就是说改变硬盘 **SetMax Address** 命令及 **Set features** 命令的安全使用方式。利用单向锁定装置，当其置位后，锁定当前硬盘设定地址。硬盘设定地址禁止改变装置根据单向锁定装置置位状态，禁止硬盘执行任何能够改变硬盘设定地址的命令。最好取消现行硬盘标准 ATA-7 中的 Address Offset 命令，禁止通过 Command 寄存器中置ＦＥＨ进入或退出硬盘变址模式（features 寄存器中置 09H 或 89H），而用新的

命令 Set Offset（设置硬盘变址基址）代替。

可选地，实现硬盘隔离的装置处于硬盘控制器与计算机主板 IDE 口之间。当单向锁定装置置位后，如果计算机向硬盘发出需要禁止任何能够改变硬盘设定地址的命令，则硬盘隔离的装置，不进行相应的转发，以达到硬盘接收不到能够改变硬盘设定地址的命令，从而禁止执行任何能够改变硬盘设定地址的命令。

可选地，实现硬盘隔离的装置处于硬盘控制器与计算机主板 IDE 口之间，但是处于监控位置。当单向锁定装置置位后，如果计算机向硬盘发出需要禁止任何能够改变硬盘设定地址的命令。则硬盘隔离的装置，向计算机发出复位信号重新启动计算机，从而实际上禁止执行任何能够改变硬盘设定地址的命令；或向硬盘发出复位信号，这里最好只能由计算机复位信号才能清除该复位信号以保证安全。

方便地，实现硬盘隔离的装置处于主板管理 IDE 口的芯片中（例如南桥）中，在单向锁定装置置位后，如果 CPU 向硬盘发出需要禁止的命令，则主板管理 IDE 口芯片使该命令不能通过 IDE 口到达硬盘，以保证硬盘状态不被改变。

本发明还提出，为了解决硬盘的安全隔离及兼容性，可以利用设置最大地址（**SetMax Address** 命令）使硬盘分为两个区：用户可存取硬盘区域及用户不可存取硬盘区域，利用硬盘提供的变址技术使计算机可以在这两个区域中转换，再利用单向锁定装置及特殊硬盘命令操作禁止装置保证安全，实现操作系统之间的硬盘隔离。

更好的，可以设置硬盘为多个区：用户可存取硬盘区域、用户不可存取硬盘区域及用户只读不写区域，利用新的手段使计算机可以方便设置这些区域。再利用单向锁定装置及特殊硬盘命令操作禁止装置保证安全，实现操作系统之间的硬盘隔离。

根据本发明的一个具体方面，提供了一种硬盘存取变址装置与硬盘保护区相结合的装置，它包括：

硬盘保留区装置，用于保护硬盘后部数据的安全性（读写均保护），使用 **SetMax Address** 命令，参见图 4A；

硬盘变址装置，用于保护硬盘前部数据安全（读写均保护）及提供软件兼

容性，使用 **Set Offset**（设置硬盘变址地址），参见图 4B；

硬盘后部写保护装置，用于写保护硬盘后部数据的安全性，使用 **SetBehind** 命令，参见图 4C；

硬盘前部写保护装置，用于写保护硬盘前部数据的安全性，使用 **SetFront** 命令，参见图 4D；

单向锁定装置；

硬盘设定地址禁止改变装置；

其中，单向锁定装置是一只有当计算机加电或复位时，才能复位的寄存器，当单向锁定装置置位时，锁定当前硬盘设定地址。硬盘设定地址禁止改变装置根据单向锁定装置置位状态，禁止硬盘执行任何能够改变硬盘设定地址的命令，即改变硬盘保留区装置、硬盘变址装置、硬盘后部写保护区装置、硬盘前部写保护区装置所设定的地址。

实用地，当计算机重新启动后，先使硬盘全部只读或只有硬盘前部区域可读，其他地方不可读写；或设置一个开机时计算机可读区域，类似硬盘前部写保护区，其他区域不可读写。通过口令（或不需要口令），才能打开该锁。这样可以把设置硬盘设定地址的工作放入硬盘。这样可以兼容老计算机。

根据本发明的另一方面，一种实现硬盘隔离的方法，它包括：

重新启动计算机，同时复位单向锁定装置；

根据需要设定用户可存取硬盘区域地址；

置位单向锁定装置；

正常启动计算机操作系统。

进一步，根据需要设定用户可存取硬盘区域地址包括，设定硬盘保留区装置地址、硬盘变址装置、硬盘后部写保护区装置地址、硬盘前部写保护区装置地址之任意组合。

附图说明

下面参照附图，根据最常用的硬盘标准（IDE）及 IBM 兼容机描绘本发明，

其中

图 1 是表示现有技术中硬盘隔离状态的示意图；

图 2 表示结合有按照本发明第一实施例的硬盘安全隔离装置的计算机系统示意图；

图 3 表示结合有按照本发明第二实施例的硬盘安全隔离装置的计算机系统示意图；

图 4A－4D 表示设置硬盘不同保护区的状态示意图；

图 5 表示结合有按照本发明第三实施例的硬盘安全隔离装置的硬盘驱动器示意图；

图 6 表示根据本发明的实现硬盘安全隔离方法的流程图；

图 7 表示实现图 6 所示安全隔离方法的进一步的流程图；

图 8 表示实现图 5 所示硬盘安全隔离装置的方法的流程图；

具体实施方式

下面参照附图，根据最常用的硬盘标准（IDE）及 IBM 兼容机描绘本发明。

[实施例 1]

根据本发明第一种实施方式，实现硬盘隔离装置如图 2 所示（其上不是所有装置均为必须）。其中：1 为计算机主板；11 为 BIOS；12 为 PCI 总线；13 为主板复位装置；14 为主板 IDE 接口；2 为硬盘隔离装置；21 为硬盘设定地址禁止改变装置；22 为存放用户选择程序的 ROM；23 为单向锁定装置；3 是硬盘驱动器（IDE 接口）；**43** 连接主板 PCI 总线 12 与硬盘隔离装置 2 中选择程序 ROM22；复位线 42 连接硬盘隔离装置中硬盘设定地址禁止改变装置 21 与主板复位装置 13 ；导线 **41** 连接主板复位装置 13 与单向锁定装置。IDE 总线 5 连接硬盘驱动器 3 及硬盘隔离装置 2。当计算机加电或重新启动后，计算机发出复位信号并执行 BIOS11 程序，同时通过复位信号线 41 复位单向锁定装置 23。通过 BIOS11 程序使计算机进入设置硬盘状态的选择程序（或通 PCI 总线 12 并连接线 43，执行 ROM22 中选择程序），根据用户选择（或身份认证后根据权利选择）设置硬盘相

应地址，如使用 **SetMax Address**（F9）命令，设置硬盘保留区；或使用硬盘标准提供的功能进入变址模式（Set Feature 子命令 09H），用于保护硬盘前部数据安全（读写均保护）及提供软件兼容性。完成后置位单向锁定装置 23。

计算机正常进入操作系统后，当计算机主板 1 向硬盘驱动器 3 发出改变改变硬盘设定地址的命令，如退出变址模式（Set Feature 子命令 89H），重新设置硬盘保留区及软件复位（Device Control 寄存器 SRST 位置位）使硬盘退出变址模式。这些可能破坏安全原则的命令，均通过 IDE 总线 5 到达硬盘隔离装置 2 中硬盘设定地址禁止改变装置 21，硬盘设定地址禁止改变装置 21 根据单向锁定装置 23 已置位的状态，向主板复位装置 13 发出复位信号重新启动计算机，以保证硬盘设定地址不能被非法改变。这个实施例是在不改变现行硬盘标准 ATA-7 的基础上，利用附加装置实现硬盘安全隔离。

显然在实施例 1 中，PCI 总线 12 及选择程序 ROM22 不是必须，可以通过把选择程序放入 BOIS11 中即可。另外当计算机发出改变硬盘设定地址命令后，硬盘设定地址禁止改变装置 21 也可以通过保持复位硬盘驱动器 3 来禁止设定地址的改变，然后重新启动计算机。总之实际上都需要重新启动计算机，这虽然保证了安全，但是这对一些用户可能不方便。这就有下一个实施例。

[实施例 2]

根据本发明第二种实施方式，实现硬盘隔离装置如图 3 所示（其上不是所有装置均为必须）。其中：1 为计算机主板；11 为 BIOS；12 为 PCI 总线；13 为主板复位装置；14 为主板 IDE 接口；2 为硬盘隔离装置；21 为硬盘设定地址禁止改变装置；22 为存放用户选择程序的 ROM；23 为单向锁定装置；3 是硬盘驱动器（IDE 接口）；41 连接主板 PCI 总线 12 与硬盘隔离装置 2 中选择程序 ROM22；42 连接主板复位装置 13 与硬盘隔离装置 2 中单向锁定装置 23；IDE 总线 51 连接主板与硬盘隔离装置；IDE 总线 52 连接硬盘隔离装置与硬盘驱动器。当计算机加电或重新启动后，计算机发出复位信号并执行 BIOS11 程序，同时通过复位信号线 42 复位单向锁定装置 23。通过 BIOS11 程序使计算机进入设置硬盘状态的选择程序（或通 PCI 总线 12 并连接线 43，执行 ROM22 中选择程序），根据用户选择（或身份认证后根据权利选择）设置硬盘相应地址，如使用 **SetMax Address（F9）**命令，设置硬盘保留区；或使用硬盘标准提供的功能进入变址模式（Set

Feature 子命令 09H），用于保护硬盘前部数据安全（读写均保护）及提供软件兼容性。完成后置位单向锁定装置 23。

计算机正常进入操作系统后，当计算机主板 1 向硬盘驱动器 3 发出改变改变硬盘设定地址的命令，如退出变址模式（Set Feature 子命令 89H），重新设置硬盘保留区及软件复位（Device Control 寄存器 SRST 位置位）使硬盘退出变址模式。这些可能破坏安全原则的命令，均首先通过 IDE 总线 51 到达硬盘隔离装置 2 中硬盘设定地址禁止改变装置 21，硬盘设定地址禁止改变装置 21 根据单向锁定装置 23 已置位的状态，不通过 IDE 总线 52 向硬盘驱动器 3 转发该命令，使硬盘驱动器收不到这个命令，硬盘设定地址不能被非法改变。对于非硬盘设定地址改变命令，硬盘设定地址禁止改变装置 21 通过 IDE 总线 52 转发该命令到硬盘驱动器 3。这个实施例是在不改变现行硬盘标准 ATA-7 的基础上，利用附加装置实现硬盘安全隔离。

显然在实施例 2 中，PCI 总线 12 及选择程序 ROM22 不是必须，可以通过把选择程序放入 BOIS11 中即可。禁止或转发硬盘命令可以通过多种方法实现，参见前述专利。

另外容易看见，可以把该实施例所用装置集成于主板 IDE 控制 14 中，或集成于硬盘驱动器 3 中。

实施例 3

根据本人已授权发明专利 9 4 1 1 1 4 6 1，其中磁道组可以理解为硬盘两个地址所包含的硬盘区域。在其权利要求 6 中，说明了一种只需要一个地址就可以实现的磁道组。这里用三个特殊的磁道组组成保护区装置：硬盘保留区装置，硬盘后部写保护区装置及硬盘前部写保护区装置，关于这些保护区的安全保护装置可参见所述专利。如图 4 所示，假设 M 为硬盘真实最大地址、0、K、R、B、F、M 均为硬盘 LBA 地址值。其中图形上方各值为计算机使用的地址，图形下方各值为硬盘真实地址。显然设置硬盘保留区只需要设置硬盘最大用户可存取地址即可，这与现行硬盘标准一致。它使硬盘形成一个读写保护的硬盘保留区装置，如图 4A，以 **R** 值执行 **SetMax** 命令，它使计算机能够读写硬盘从 0 到 R 的区域，不能读写 R 到 M 的硬盘区域。

为解决软件兼容性，比较好的方法是使用硬盘变址技术（本人待批发明专

利００１３２９８９．８），以 **O** 值执行 **SetOffset** 命令后，所有读写硬盘的命令中，均把读写硬盘的地址加上 O 值作为硬盘真实读写地址，如图 4B 所示。用真实读写地址比较 R 值，作为保留区判别地址。所以，该命令它使计算机能够读写硬盘从 O 到 R 真实地址的区域（表现为 0 到 R-O 硬盘区域），不能读写其它区域。这样可以用比较自然的方式实现硬盘变址技术，而不用硬盘标准 ATA—7 中的硬盘变址技术。

同理容易理解硬盘后部写保护区装置，它与硬盘保留区装置标准基本一致，差别在于只进行写保护不进行读保护，如图 4C，以 B 值执行 **Set behind** 命令后，不能写硬盘 B 到 M 真实地址区域。

同理容易理解硬盘前部写保护区装置，它与硬盘保留区装置标准基本一致，差别在于只进行写保护不进行读保护，如图 4D，以 F 值执行 **Set Front** 命令后，不能写硬盘 0 到 F 实地址区域。

结合上述保护区装置、硬盘变址装置及硬盘隔离装置（单向锁定装置；硬盘设定地址禁止改变装置），并取消现行硬盘标准 ATA-7 中的变址命令，形成根据本发明第三种实施方式，如图 5 所示。

根据本发明第三种实施方式，实现硬盘隔离装置如图 5 所示，它表示所述装置与硬盘驱动器结合在一起。其中：1 为加有硬盘隔离装置、硬盘变址装置及硬盘保护装置的硬盘驱动器；11 为硬盘读写装置；12 为硬盘 IDE 总线接口；13 为硬盘变址装置；14 为硬盘读写保护装置；15 为硬盘隔离装置；141 为存储硬盘读写地址装置；142 为合法性判定装置；143 为非法操作禁止装置；144 为硬盘保留区装置；145 为硬盘后部写保护区装置；146 为硬盘前部写保护区装置；147 为设置硬盘设定地址装置；151 为硬盘设定地址禁止改变装置；152 为单向锁定装置。

其中，硬盘 IDE 总线接口 12 与硬盘变址装置 13 及硬盘隔离装置 15 相连接；硬盘变址装置 13 与存储读写地址装置 141 及设置硬盘设置地址装置 147 相连接；硬盘保留区装置 144、硬盘后部写保护区装置 145 及硬盘前部写保护区装置 146 与设置硬盘设置地址装置 147 及合法性判断装置相连接；非法操作禁止装置 143 与合法性判定装置 142 及硬盘读写装置 11 相连接；单向锁定装置 152 与硬盘设定地址禁止改变装置 151 相连接；硬盘设定地址禁止改变装置 151 与设置硬盘

设定地址装置 147 及 IDE 总线接口 12 相连接；存储读写地址装置 141 与硬盘变址装置 13 及硬盘读写装置 11 相连接。

当硬盘驱动器加电或硬盘驱动器硬复位后，硬盘驱动器 1 利用硬盘收到的复位信号复位单向锁定装置 152。硬盘驱动器通过 IDE 总线接口 12 接收设置硬盘设定地址。当单向锁定装置 152 处于复位状态时，硬盘设定地址禁止改变装置 151 通过设置硬盘设定地址装置 147 设置：硬盘变址装置变址地址（O）、硬盘保留区装置地址（R）、硬盘后部写保护区地址（B）及硬盘前保护区装置地址（F）。然后硬盘驱动器通过 IDE 总线接口 12 接收置位单向锁定装置。

当硬盘驱动器通过 IDE 总线接口 12 接收硬盘读写命令后，通过硬盘变址装置 13 形成硬盘真实读写地址，并放入存储读写地址装置 141。合法性判断装置 142 通过存储读写地址装置 141 中地址及硬盘变址装置变址地址（O）、硬盘保留区装置地址（R）、硬盘后部写保护区地址（B）、硬盘前保护区装置地址（F）判断读写操作是否合法，如果合法则非法操作禁止装置 143 允许硬盘读写装置 11 根据存储读写地址装置 141 的地址读写硬盘，并通过 IDE 总线接口 12 接收数据（写）或返回数据（读）。如果非法则非法操作禁止装置 143 禁止硬盘读写装置 11 读写硬盘。

当硬盘驱动器通过 IDE 总线接口 12 接收改变硬盘设定地址（如，如退出变址模式，重新设置硬盘保留区及软件复位使硬盘退出变址模式等），硬盘设定地址禁止改变装置 151 根据单向锁定装置 152 置位状态禁止设置硬盘设定地址装置 147 执行改变：硬盘变址装置变址地址（O）、硬盘保留区装置地址（R）、硬盘后部写保护区地址（B）及硬盘前保护区装置地址（F）。

需要说明的是，单向锁定装置 152 可以是硬盘驱动器输入的一条线。当该线处于某种状态（高电平，相当于 151 置位）时，硬盘设定地址禁止改变装置 151 禁止设置硬盘设定地址装置 147 执行改变：硬盘变址装置变址地址（O）、硬盘保留区装置地址（R）、硬盘后部写保护区地址（B）及硬盘前保护区装置地址（F）。而当该线处于处于另外状态（底电平）时，可以进行硬盘设定地址改变。显然，单向锁定装置的锁定部分处于硬盘驱动器之外，与处于硬盘驱动器中的部分合起来构成一个完整的硬盘隔离装置。当然这个线选单向锁定装置的置位可以使用机械装置。

[实施例 4]

图 6，7 中示出了根据本发明的一实施例的一种实现硬盘隔离的方法的流程图。如图 6 所示，该方法包括步骤：该方法包括有步骤：（1）首先重新启动计算机，同时复位单向锁定装置；（2）根据需要设定用户可存取硬盘区域地址；（3）置位单向锁定装置；（4）正常启动操作系统。

如图 7 所示，当硬盘隔离装置接收到硬盘命令后，判断单向锁是否置位，当单向锁复位时正常执行硬盘命令，单向锁置位时判断该硬盘命令是否是影响硬盘设定地址的命令：如是则禁止该命令执行，如不是则正常执行该命令。

[实施例 5]

图 5，6，8 中示出了根据本发明的一实施例的一种实现硬盘隔离的方法的流程图。如图 6 所示，该方法包括步骤：该方法包括有步骤：（1）首先重新启动计算机，同时复位单向锁定装置；（2）根据需要设定用户可存取硬盘区域地址；（3）置位单向锁定装置；（4）正常启动操作系统。进一步，根据需要设定用户可存取硬盘区域地址包括，设定硬盘保留区装置地址、硬盘变址装置地址、硬盘后部写保护区装置地址、硬盘前部写保护区装置地址之任意组合。

当设置完成后，图 8 中硬盘隔离装置接收到操作指令（101）后，判断是否为读写指令（102），如果不是读写指令则进一步判断是否为设置地址指令（103），如果还不是则为其他指令，硬盘隔离装置让硬盘执行该指令（106）后返回（402）；如为设置地址指令则判断单向锁定装置是否置位（104）；如果单向锁定装置置位，则不执行设置操作并返回（402）；如果单向锁定装置没有置位，则执行设置操作（105）并返回（402）。

当硬盘隔离装置接收到操作指令（101）为读写指令后，把命令所含的地址与硬盘变址装置 13（图 5）中所保存的硬盘变址地址 O 相加形成硬盘读写的真实地址（201）；判断当前操作是否为写操作，如是则判断真实地址是否小于前部写保护区结束地址 F（301）及真实地址是否大于后部写保护区开始地址 B（302），如是则禁止读写（401）并返回（402），否则以真实地址写硬盘（304）

并返回。

如当前操作不是写操作则为读操作，判断真实地址大于是否硬盘保留区开始地址 R（303），如不大于硬盘保留区开始地址 R，则以真实地址读硬盘（304）并返回（402），如大于硬盘保留区开始地址 R，禁止读硬盘（401）并返回（402）。

需要注意的是，对于写操作为了保证绝对安全，应该是真实地址加需要读的扇区数是否大于后部写保护区开始地址 B（302）及真实地址加需要读的扇区数是否大于硬盘保留开始地址 R（303）；对于读操作为了保证绝对安全，判断真实地址加需要读的扇区数是否大于硬盘保留区开始地址 R（303）。

显然，当计算机加电或重新启动后，计算机会发出复位信号并进入 BIOS 程序。利用复位信号可以复位单向锁定装置，通过 BIOS 程序使计算机进入设置硬盘状态的选择程序，根据用户选择或进行身份认证后选择，设置硬盘相应状态，并置位单向锁定装置，这样就可以把身份认证技术与硬盘隔离技术相结合，以达到更高的安全性。

虽然本发明通过实施例进行了描述，但本领域技术人员可在本发明的精神的范围内，作出各种变形和改进，所附的权利要求应包括这些变形和改进。

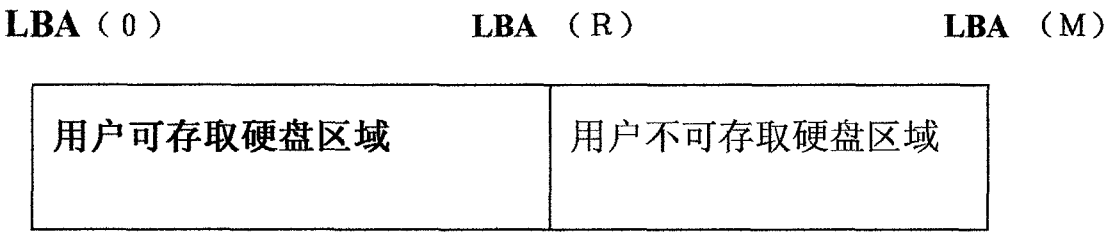


图 1A（现有技术）

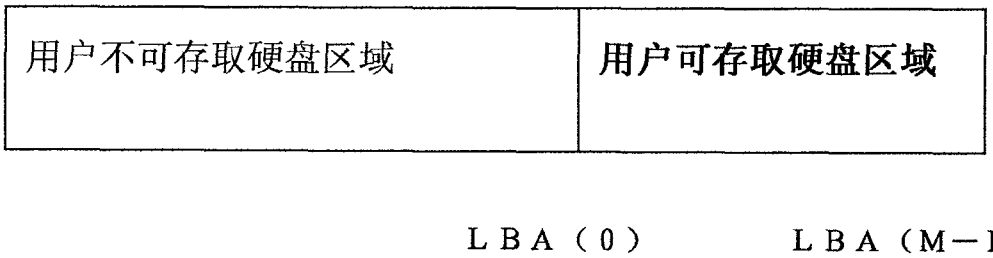


图 1B（现有技术）

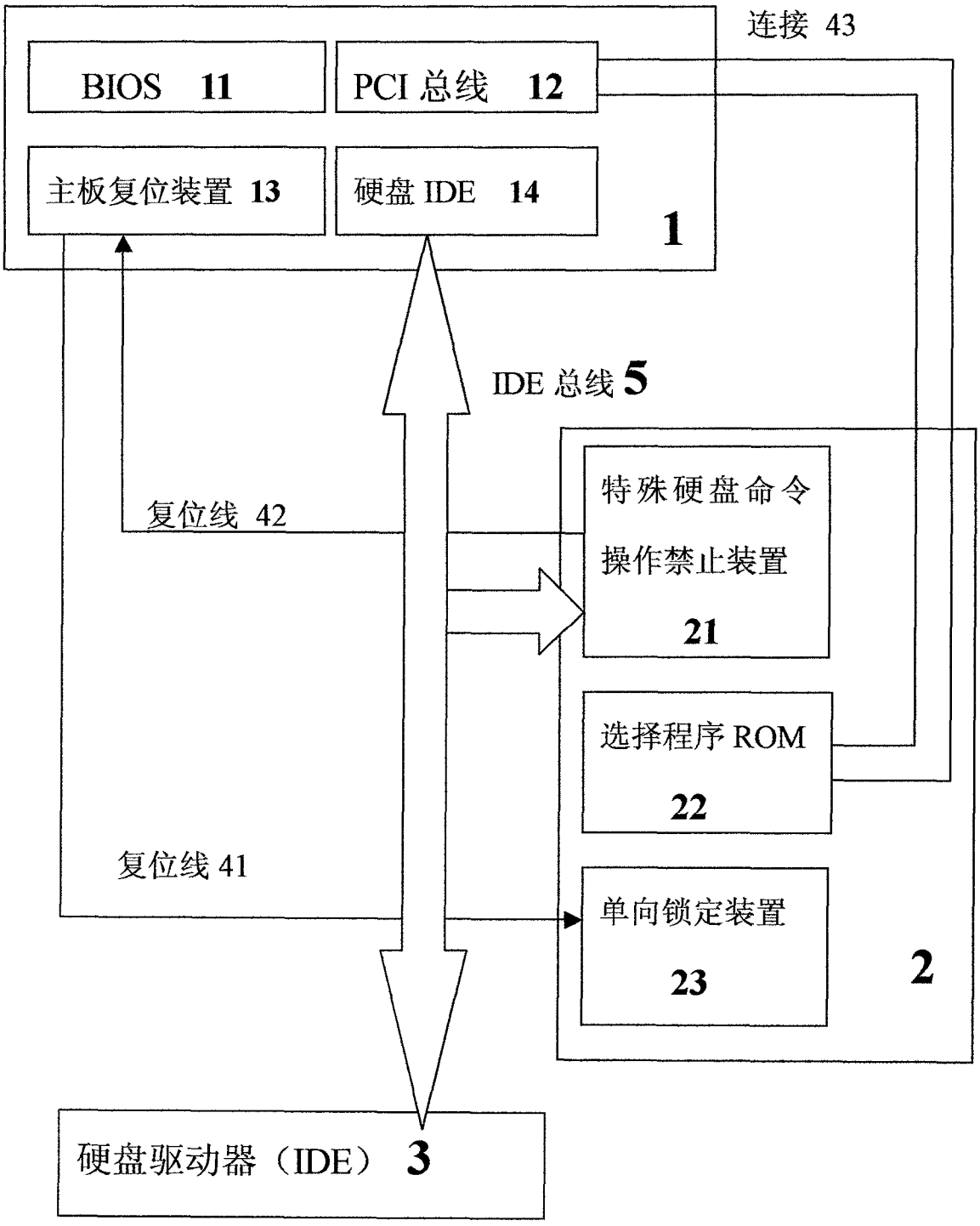

连接 43
BIOS 11
PCI 总线 12
主板复位装置 13
硬盘 IDE 14
1
IDE 总线 5
复位线 42
特殊硬盘命令
操作禁止装置
21
选择程序 ROM
22
复位线 41
单向锁定装置
23
2
硬盘驱动器（IDE） 3

图 2

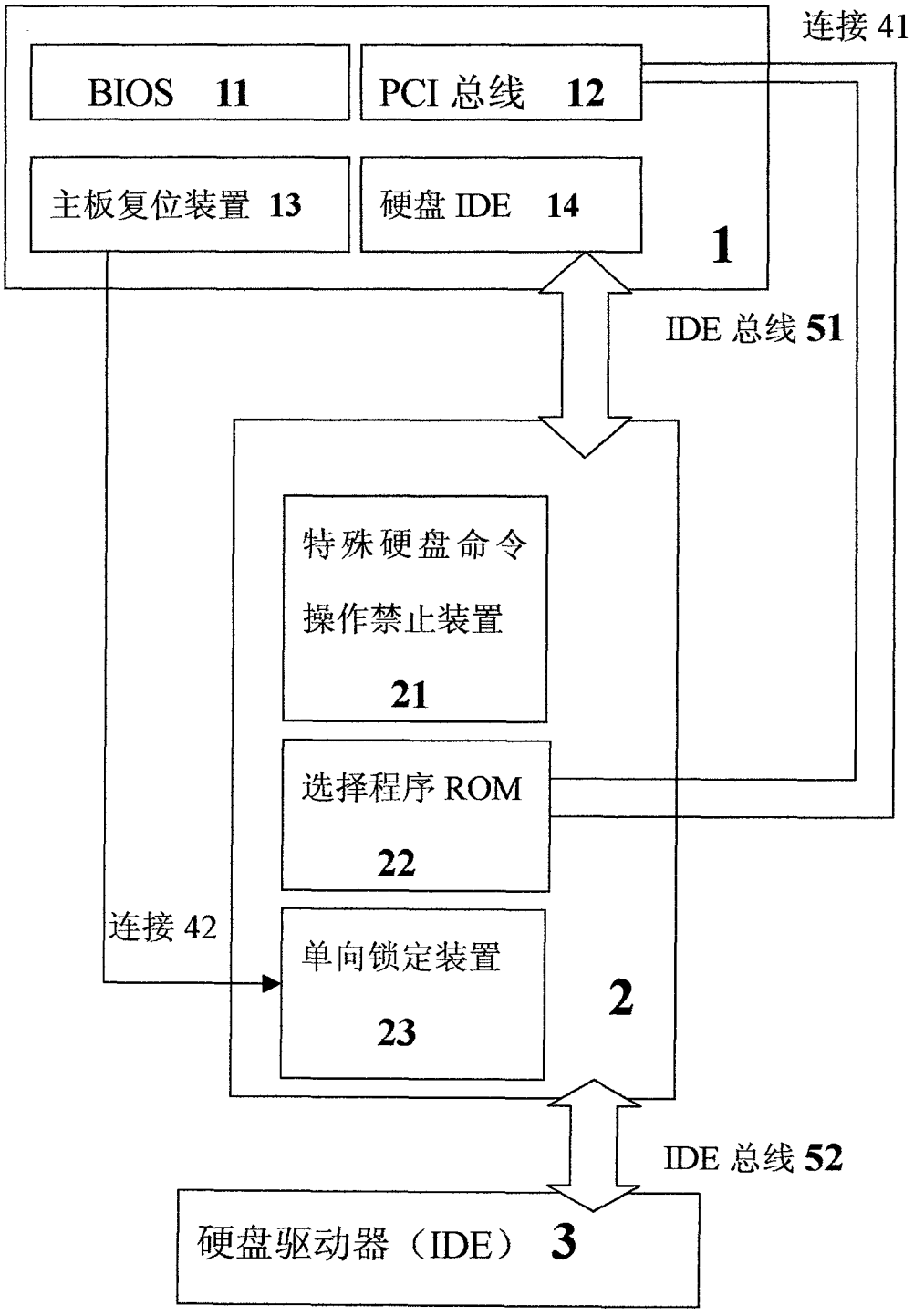

连接 41
BIOS 11
PCI 总线 12
主板复位装置 13
硬盘 IDE 14
1
IDE 总线 51
特殊硬盘命令
操作禁止装置
21
选择程序 ROM
22
连接 42
单向锁定装置
23
2
IDE 总线 52
硬盘驱动器（IDE） 3

图 3

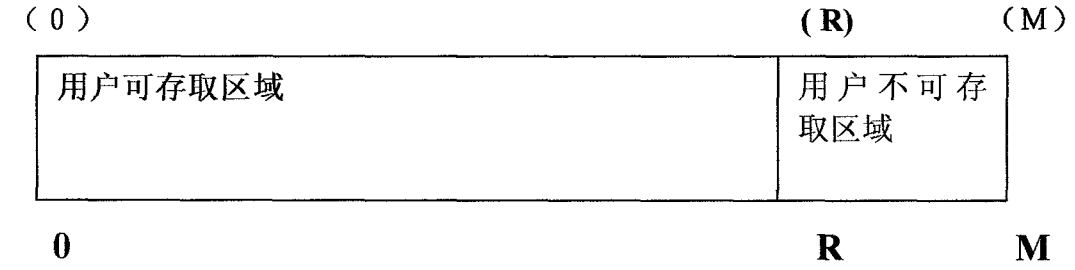


图 4A

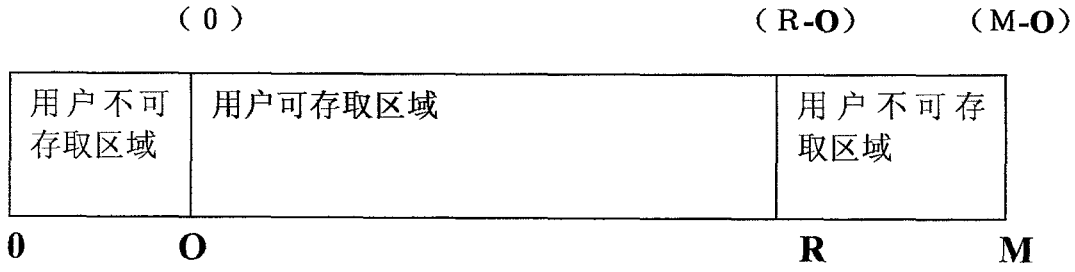


图 4B

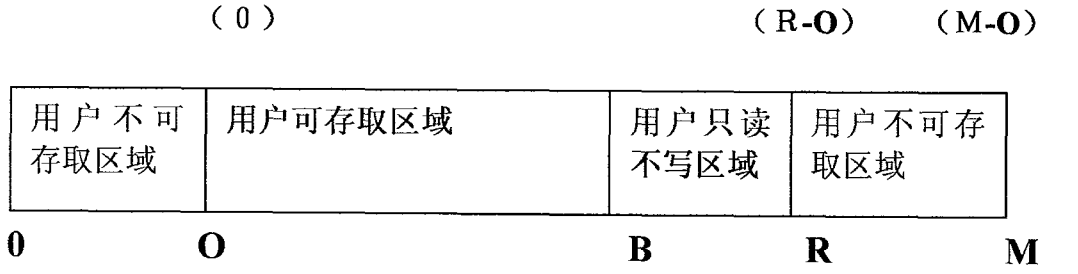


图 4C

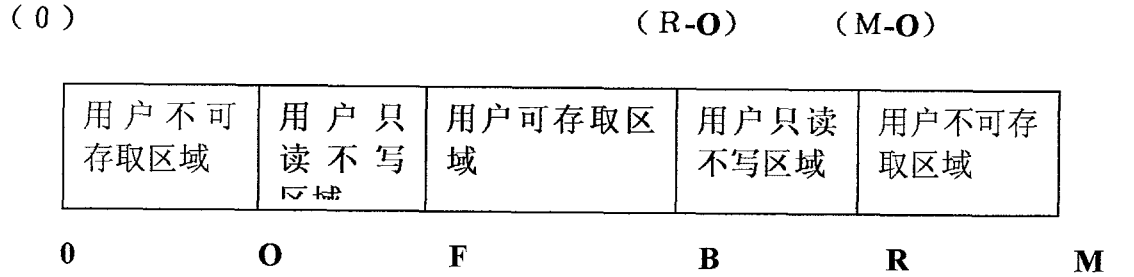


图 4D

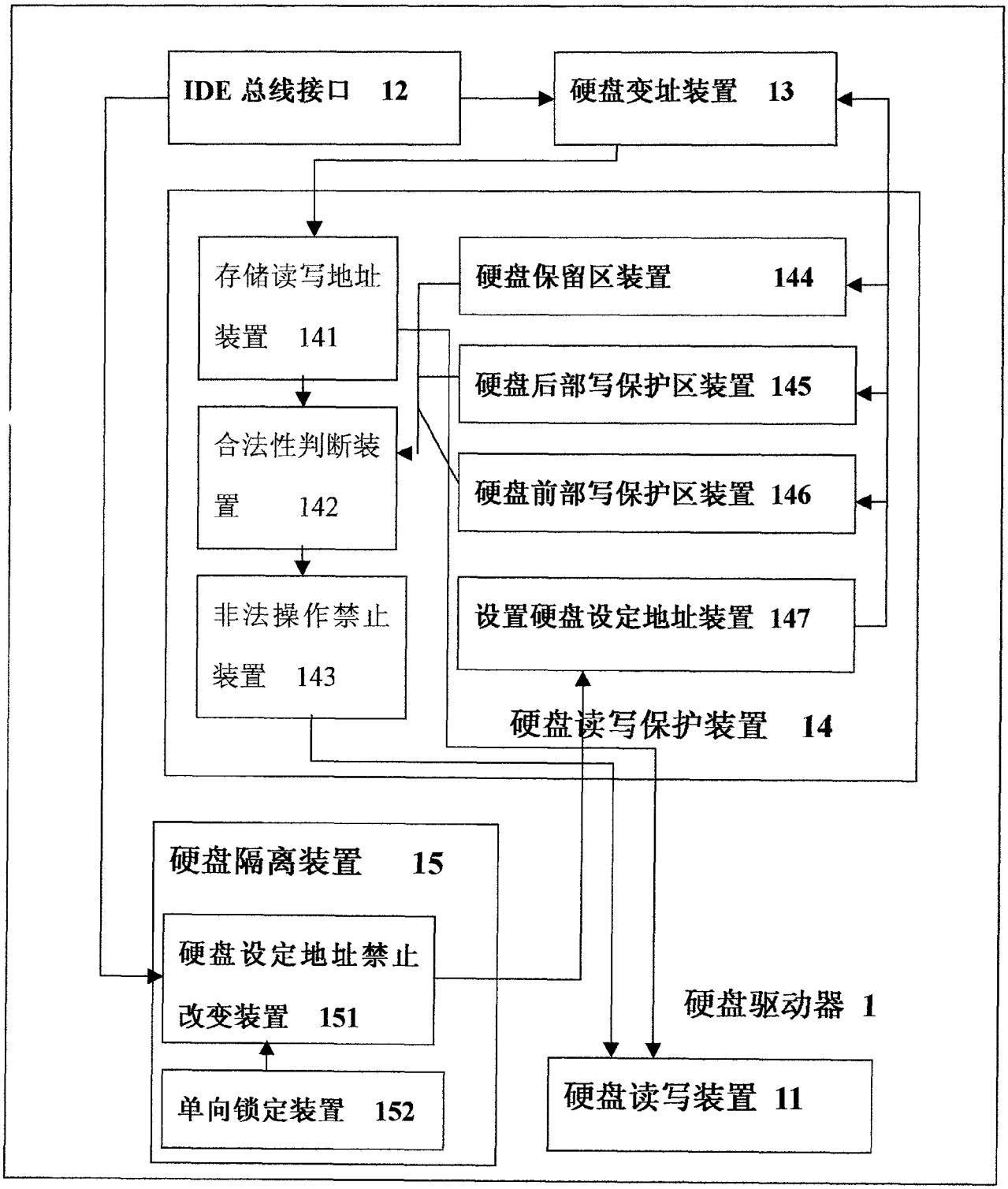

IDE 总线接口 12
硬盘变址装置 13
存储读写地址装置 141
硬盘保留区装置 144
硬盘后部写保护区装置 145
合法性判断装置 142
硬盘前部写保护区装置 146
非法操作禁止装置 143
设置硬盘设定地址装置 147
硬盘读写保护装置 14
硬盘隔离装置 15
硬盘设定地址禁止改变装置 151
单向锁定装置 152
硬盘驱动器 1
硬盘读写装置 11

图 5

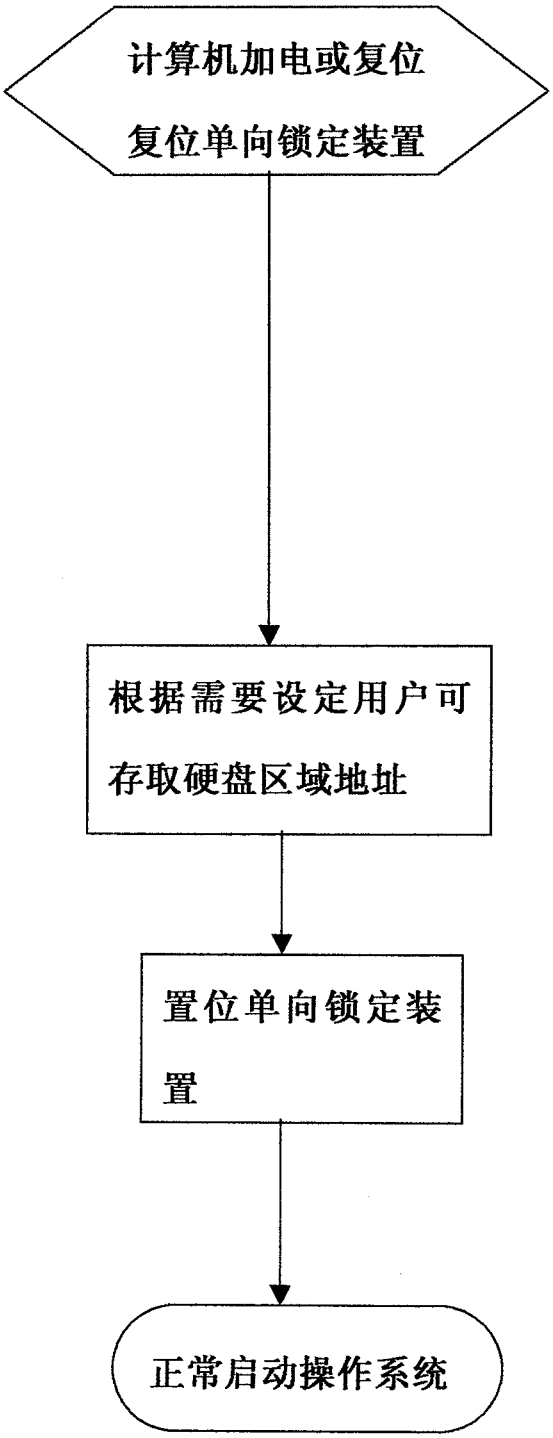


图 6

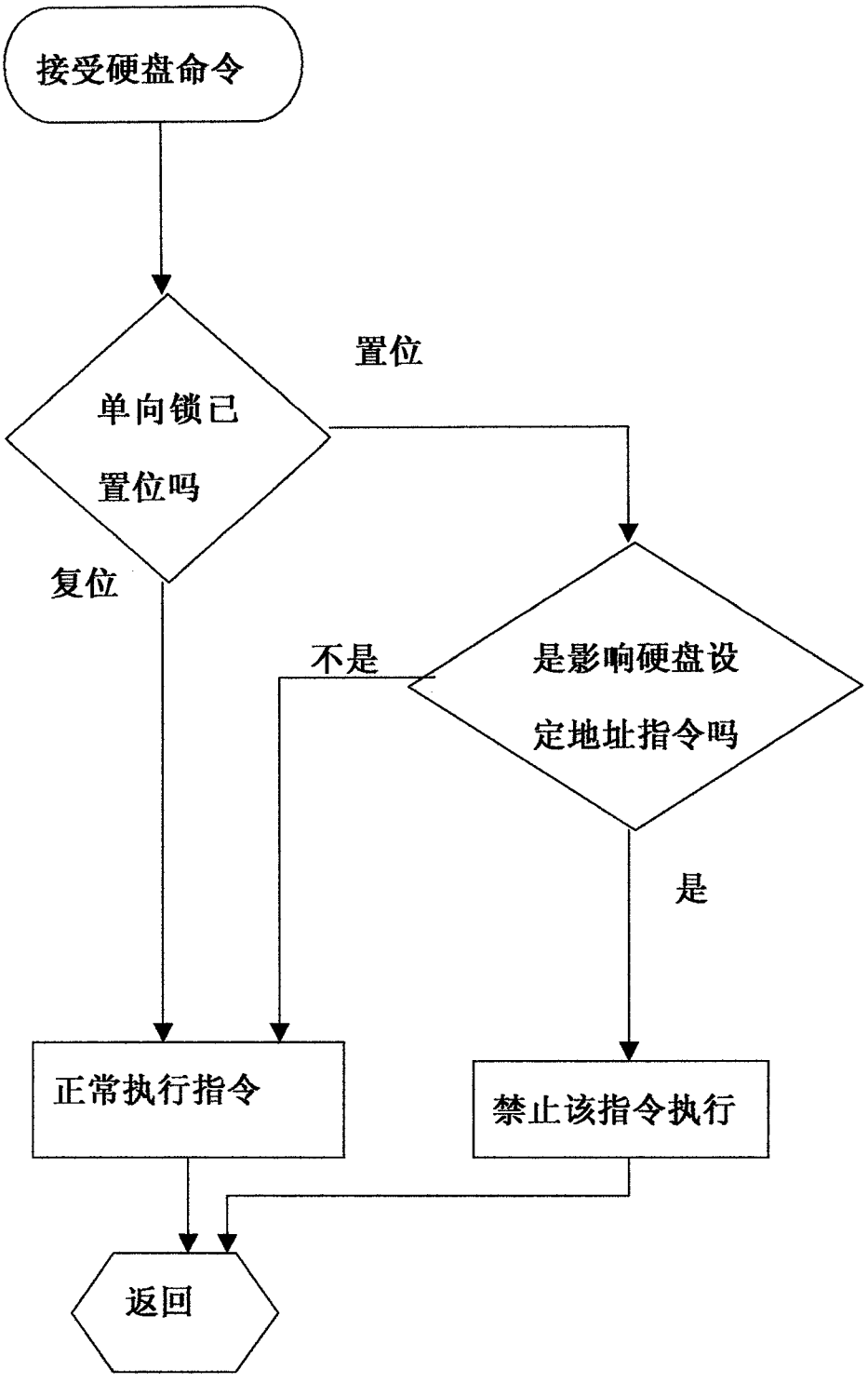


图 7

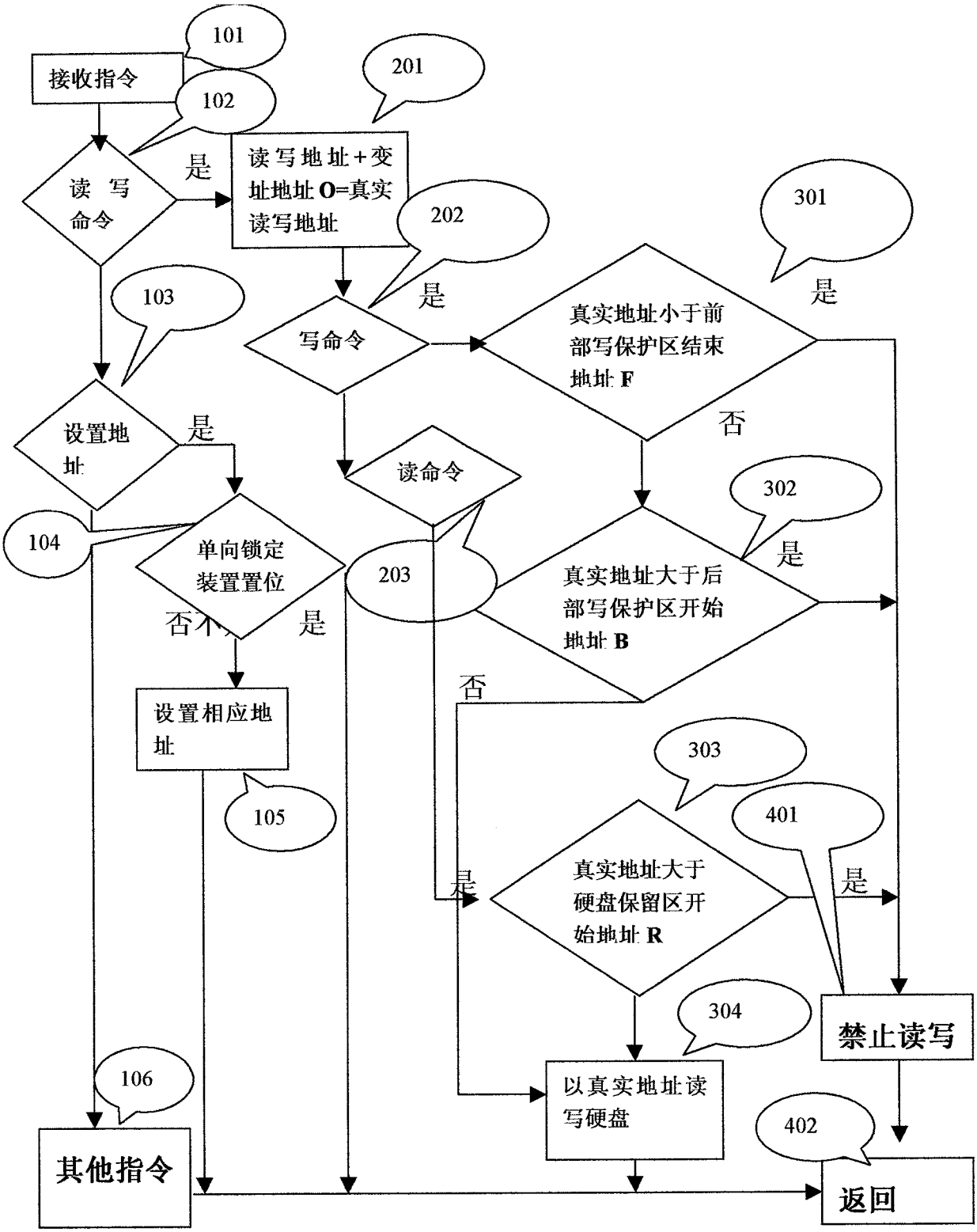

101
接收指令
102
读 写 命令
是
201
读写地址+变址地址O=真实读写地址
202
写命令
是
301
真实地址小于前部写保护区结束地址F
是
否
103
设置地址
是
读命令
302
真实地址大于后部写保护区开始地址B
是
104
单向锁定装置置位
否
是
203
否
设置相应地址
105
303
401
真实地址大于硬盘保留区开始地址R
是
是
304
禁止读写
106
以真实地址读写硬盘
402
其他指令
返回

图 8