

(12) 发明专利

(10) 授权公告号 CN 1771551 B

(45) 授权公告日 2010.10.13

(21) 申请号 200480009470.9

G06F 7/00 (2006. 01)

(22) 申请日 2004.03.25

G06F 12/00 (2006. 01)

(30) 优先权数据

03007801.8 2003.04.04 EP

G06F 3/06 (2006. 01)

(85) PCT申请进入国家阶段日

2005.10.08

(56) 对比文件

US 6523102 B1, 2003.02.18, 全文.

(86) PCT申请的申请数据

PCT/EP2004/003177 2004.03.25

US 2002/0174102 A1, 2002.11.21, 说明书第
29栏—第44栏, 附图1-3.

(87) PCT申请的公布数据

W02004/088658 EN 2004.10.14

US 2002/0004884 A1, 2002.01.10, 说明书第
47栏—第72栏, 附图1-6.

审查员 金曦

(73) 专利权人 索尼达德克奥地利股份公司

地址 奥地利安尼弗

(72) 发明人 M·库尔茨 A·温特

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

代理人 杨凯 陈景峻

(51) Int. Cl.

G11B 20/00 (2006. 01)

G06F 17/30 (2006. 01)

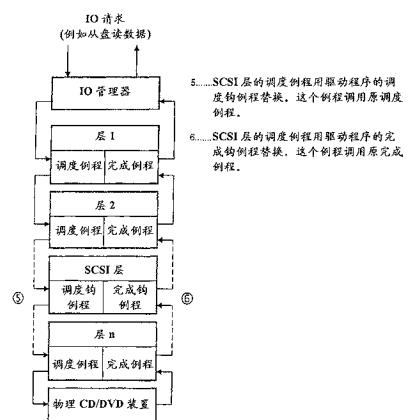
权利要求书 2 页 说明书 7 页 附图 2 页

(54) 发明名称

光介质保护驱动器

(57) 摘要

一种保护目标光学记录载体上的被保护数据区内的内容免于计算机非法读出和 / 或拷贝的方法, 包括如下步骤: 确定目标光学记录载体还是非目标光学记录载体插入到计算机的驱动器中, 并且在目标光学记录载体插入在计算机的驱动器中的情况下, 修改对被保护数据区的读出请求, 以便没有数据被读出或者读出的数据是无用的, 和 / 或修改将被保护数据区内的数据写入可记录的记录载体或其它存储器的写入命令, 使得写入的数据是无用的。



1. 保护目标光学数据载体上的被保护数据区内的内容免于被计算机非法读出和 / 或拷贝的方法, 其特征在于如下步骤 :

- 确定是目标光学数据载体还是非目标光学数据载体插入到计算机的驱动器中, 并且
- 在目标光学数据载体插入在所述计算机的驱动器中的情况下,
- 修改对所述被保护数据区的读出请求, 以便没有数据被读出或者读出的数据是无用的, 和 / 或
- 修改将被保护数据区内的数据写入可记录的数据载体或其它存储器的写入命令, 使得写入的数据是无用的。

2. 如权利要求 1 所述的方法, 其特征在于, 修改读出请求和 / 或写入命令仅仅在没有认证的情况下进行。

3. 如权利要求 1 或 2 所述的方法, 其特征在于, 所述确定和修改步骤通过实施在计算机内的驱动器控制层中的例程来执行。

4. 如权利要求 3 所述的方法, 其特征在于, 例程

- 替换调度例程和完成例程, 以及
- 具有这样的功能 : 执行所述确定和修改步骤以及调用替换下来的调度和完成例程, 以便根据原始的或修改的读出请求和 / 或写入命令执行所述替换下来的调度和完成例程。

5. 如权利要求 3 所述的方法, 其特征在于, 所述例程通过由可执行程序安装的驱动程序执行, 该可执行程序在目标光学数据载体被插入驱动器中时自动地启动。

6. 如权利要求 5 所述的方法, 其特征在于, 所述驱动程序

- 在每次启动计算机之后自动加载、和 / 或
- 不包括卸载例程、和 / 或
- 随机改变所述驱动程序的名称、和 / 或
- 包括随机设置的文件时间、和 / 或
- 包括随机改变的代码、和 / 或
- 安装多次, 但只有一次有效、和 / 或
- 能通过安装程序遍布计算机系统安装。

7. 如权利要求 5 所述的方法, 其特征在于, 所述驱动程序包括通信接口, 以允许控制数据和 / 或验证数据的交换。

8. 如权利要求 1 或 2 所述的方法, 其特征在于, 通过评价如下内容使目标光学数据载体区别于非目标光学数据载体 :

- 涉及专门修改的所述光学数据载体的预定会话, 和 / 或
- 涉及专门项目的所述光学数据载体的内容的至少一个表格, 和 / 或
- 涉及专门子码修改的所述光学数据载体的预定会话, 和 / 或
- 涉及水印的光学数据载体上存储的预定数据。

9. 如权利要求 1 或 2 所述的方法, 其特征在于, 被保护数据区在如下基础上识别 :

- 扇区类型, 和 / 或
- 多个扇区, 和 / 或
- 具有特定读出序列的扇区。

10. 如权利要求 1 或 2 所述的方法, 其特征在于, 被保护数据区定义为 :

- 至少一个预定区,和 / 或
- 存储在光学数据载体本身上的数据。

11. 如权利要求 1 或 2 所述的方法,其特征在于,所述修改读出请求以致读出数据无用、和 / 或修改写入命令以致写入数据无用的步骤包括 :

- 用一个错误放弃对应的输入输出请求和 / 或输入输出命令,和 / 或
- 完成对应的输入输出请求和 / 或输入输出命令,但不处理实际的请求和 / 或命令,和 / 或
- 修改相应的数据使其无用。

12. 保护目标光学数据载体上的被保护数据区内的内容免于被计算机非法读出和 / 或拷贝的装置,其特征在于所述装置包括 :

用于确定目标光学数据载体是否插入到计算机的驱动器中的组件 ;

第一修改组件 ; 和 / 或

第二修改组件,

其中在目标光学数据载体插入在所述计算机的驱动器中的情况下,

所述第一修改组件用来修改对所述被保护数据区的读出请求,以便没有数据被读出或者读出的数据是无用的,和 / 或

所述第二修改组件用来修改将被保护数据区内的数据写入可记录的数据载体或其它存储器的写入命令,使得写入的数据是无用的。

13. 如权利要求 12 所述的装置,其特征在于所述目标光学数据载体为可执行的光学数据载体,所述可执行的光学数据载体在所述光学数据载体被插入驱动器中时自动启动,并且所述可执行的光学数据载体用来安装确定目标光学数据载体是否插入所述计算机的驱动器的驱动程序,以及

用来修改对所述被保护数据区的读出请求,以便没有数据被读出或者读出的数据是无用的,和 / 或

用来修改将被保护数据区内的数据写入可记录的数据载体或其它存储器的写入命令,使得写入的数据是无用的。

光介质保护驱动器

[0001] 技术领域

[0002] 本发明涉及保护目标光学记录载体上的被保护数据区内的内容免于计算机的非法读出和 / 或拷贝的方法、以及光学记录载体。

[0003] 背景技术

[0004] 信息存储在其一侧或两侧上的光存储载体已经开始用于各种目的，最显著地是在音乐、游戏、视频以及计算机产业中。数字信息以沿盘的一侧或两侧上环形的同心轨迹布置的坑的形式存储在光存储介质上。轨迹一般从里向外读出，但也可以从外向里读出，就与已经用于一些光存储介质的一样。

[0005] 轨迹上的数据本身再分成帧，每一帧长度相等，并包含等量的信息。取决于光存储介质的类型 (CD、DVD)，每一帧都有一个专用的布局。这种帧总包含用户数据符号本身，但也可以包含用于同步的数据、数据符号和纠错之间的合并数据。

[0006] 光存储介质本身上的信号是异步的，这表明在解码过程中，必须从信号中去除同步、定时信息、奇偶校验数据或其它数据，并且信号必须符合某些要求以便它能够由读出装置访问。

[0007] 由于这种存储介质的特性，因此容易形成拷贝。为了应对这个情况，现有各种拷贝保护方案，根据这些方案，与信息本身有关的数据和 / 或存储介质上提供访问信息或涉及同步的其它数据被修改，以在可由重放装置完成访问的同时，禁止数字拷贝。

[0008] 一般地，这些拷贝保护方案通过使计算机驱动器至少在对信息内容的访问方面混淆，从而禁止在这些驱动器上重放信息内容。为了确保对内容的安全访问，“防拷贝”地存储在光学记录载体的第一会话中的内容的质量降低版本可以用计算机可访问的方式提供在光学记录载体的第二会话中。或者，第二会话可包括到内容服务器的链接，以提供计算机存取。这种内容服务器也可包括附加值，例如音乐剪辑或与光学记录载体上的信息内容有关的赠与材料。对保存在第二会话中的内容和 / 或内容服务器的访问可以通过一个可执行文件提供，该可执行文件在拷贝保护的光学记录载体被插入计算机驱动器中之后自动开始。

[0009] 发明内容

[0010] 鉴于以上所述，本发明的目的是提供一种改进系统，以保护目标光学记录载体上的被保护数据区内的内容免于计算机的非法读出和 / 或拷贝。

[0011] 根据本发明，此目的通过保护目标光学记录载体上的被保护数据区内的内容免于计算机的非法读出和 / 或拷贝的方法解决。

[0012] 根据本发明的保护目标光学记录载体上的被保护数据区内的内容免于计算机非法读出和 / 或拷贝的方法包括如下步骤：

[0013] - 确定是目标光学记录载体还是非目标光学记录载体插入到计算机的驱动器中，并且

[0014] - 在目标光学记录载体插入在计算机的驱动器中的情况下，

[0015] - 修改对被保护数据区的读出请求，以便没有数据被读出或者读出的数据是无用的，和 / 或

[0016] - 修改将被保护数据区内的数据写入可记录的记录载体或其它存储器的写入命令,使得写入的数据是无用的。

[0017] 同时,根据本发明,提供拷贝保护,它在已知的拷贝保护方案的不同层次上工作,因为根据本发明,没有要保护的内容或者与之相关的信息或者确保到信息的安全访问的内容被改变。所以,此方案允许对除了计算机驱动器的现有回放设备的完全可访问性。另一方面,提供根据本发明的方法的计算机无法访问和 / 或拷贝目标光学记录载体,即根据本发明这种光学记录载体受到拷贝保护,因为读出请求和 / 或写入命令被修改以便保护区中的数据、即特别标示的区域,例如 CD 的音频会话,被读出和 / 或写入的是无用数据。

[0018] 根据本发明显而易见的是,目标光学记录载体以某种方式与非目标光学记录载体相区别,并且根据本发明的方法以某种方式在所用的计算机中实施。

[0019] 在根据本发明的方法中,修改读出请求和 / 或写入命令最好仅仅在没有认证的情况下进行。

[0020] 此方案加宽了不许任何计算机读出和 / 或写入的概念,以便具有认证的用户能完全地用计算机访问受保护的内容。还可以这样规定:这样访问的内容可能不能由计算机从其副本访问,由于拷贝可表示为不可由计算机访问。同时,可以产生不同认证可提供访问的副本。这样,还可以限定原件的“子级”数量,即允许副本的级数,例如只有一个原件和它的一个直接拷贝允许复制各自的认证。

[0021] 在本发明的优选实施例中,确定和修改步骤通过实施在计算机内的驱动器控制层中的例行程序执行。

[0022] 这允许创造性方法实现在一个计算机中,并且并非一定要重新启动计算机,重新启动计算机会干扰用户,因为重新启动通常需要时间。驱动器控制层一般是控制计算机驱动器的层,例如 CSI 层。

[0023] 在优选实施例中,例行程序最好

[0024] - 替换调度例程和完成例程,以及

[0025] - 具有这样的功能:执行确定和修改步骤以及调用替换下来的调度和完成例程,以便根据原始的或修改的读出请求和 / 或写入命令执行它们。

[0026] 这些特性允许例如作为缺省,计算机的操作系统的行为没有因为实现本发明而改变。此外,此操作系统在“替换”例程方面的基本功能还可以通过用修改的参数调用它们来使用,以避免对它们的置换,由此防止不必要的系统故障的出现。

[0027] 或者或另外地,在此实施例中,例程最好通过用可执行程序安装的驱动程序实现,该可执行程序在目标光学记录载体被插入驱动器中时自动地启动。

[0028] 此过程允许在安装驱动程序之后至少利用一次计算机驱动技术。同时,安装的驱动程序可以在每次重新启动计算机之后自动地加载,以便不包括可执行程序的其它目标光学记录载体根据按照本发明的方法得到拷贝保护。当然,有可能以任何其它方式将驱动程序安装在计算机上,例如在用户在计算机上执行不同的应用时,同时用户正访问因特网服务器时,通过这个不同的应用,或者利用安装的计算机的操作系统。

[0029] 最好,驱动程序

[0030] - 在每次启动计算机之后自动加载、和 / 或

[0031] - 不包括卸载例程、和 / 或

- [0032] - 随机改变它的名称、和 / 或
 - [0033] - 包括随机设置的文件时间、和 / 或
 - [0034] - 包括随机改变的代码、和 / 或
 - [0035] - 安装多次，但只有一次有效、和 / 或
 - [0036] - 能通过遍布计算机的系统的安装程序安装。
- [0037] 根据本发明驱动程序的特性旨在使驱动程序常驻在操作系统计算机内而非易于从其移去，以便在首次安装之后，最好不需要第二次安装，但根据本发明的拷贝保护方案永久地在特定计算机上可用。同时，也对没有实现根据本发明的拷贝保护的目标光学记录载体、即，老的目标光学记录载体实现拷贝保护。这些目标光学记录载体仅仅需要具有识别目标光学记录载体适于根据本发明的拷贝保护的身份特性。
- [0038] 或者或另外，驱动程序最好包括通信接口，以允许控制数据和 / 或验证数据的交换。
- [0039] 此通信接口可用于表示目标光学记录载体上的保护区，传递验证数据给驱动程序，和 / 或根据本发明在不同的已安装的驱动程序当中建立通信，以实现只有它们中的一个是有效的。经通信接口的通信最好加密。
- [0040] 根据本发明，目标光学记录载体可以通过判断如下内容而区别于非目标光学记录载体：
- [0041] - 涉及专门修改的所述光学记录载体的预定会话，和 / 或
 - [0042] - 涉及专门项目的所述光学记录载体的内容的至少一个表格，和 / 或
 - [0043] - 涉及专门子码修改的所述光学记录载体的预定会话，和 / 或
 - [0044] - 涉及水印的光学记录载体上存储的预定数据。
- [0045] 同时，根据本发明，目标光学记录载体可简单地承载将其分类为目标光学记录载体的特殊符号。但是，也可以使用更复杂的特性，例如包括某种拷贝保护的每个记录载体可分类为目标光学记录载体，或者包括特定专用的拷贝保护或包括识别特定盘标志的指示等的记录载体。同时，根据本发明，预定的“破解”拷贝保护方案可以重新激活，或者可由其内容识别的预定光学记录载体即使在交货和销售之后也可以“配备”拷贝保护。
- [0046] 根据本发明，被保护数据区最好在如下基础上识别：
- [0047] - 扇区类型，和 / 或
 - [0048] - 多个扇区，和 / 或
 - [0049] - 具有特定读出序列的扇区。
- [0050] 同时，根据本发明，被保护数据区对于一个特定的目标光学记录载体不必一定是静态的，而且还可以是动态的，例如根据某些访问特征，如在检测到对盘克隆程序或者分裂(ripping)程序的访问的情况下。
- [0051] 根据本发明，被保护数据区最好定义为：
- [0052] - 至少一个预定区，和 / 或
 - [0053] - 存储在光学记录载体本身上的数据。
- [0054] 预定数据区可以是固定的，例如总是音频会话，或者预定多个扇区，或者是可变的。可变的预定数据区可以通过其通信接口指示给驱动程序。驱动程序还可以从目标光学记录载体导出可变的预定数据区，例如，根据其目录或者根据存储在目标光学记录载体上

的列表。

[0055] 根据本发明，修改读出请求以致读出数据无用、和 / 或修改写入命令以致写数据无用的步骤最好包括：

[0056] - 以一个错误放弃对应的 I/O 请求和 / 或 I/O 命令，和 / 或

[0057] - 完成对应的 I/O 请求和 / 或 I/O 命令，但不处理实际的请求和 / 或命令，和 / 或

[0058] - 修改相应的数据使其无用。

[0059] 修改数据使其无用可包括用任意或者预定值置换数据，以致例如，干扰复制的音频 CD 的播放，或者给出没有再现的原件的注解。

[0060] 根据本发明的计算机程序产品包括计算机程序部件，用于在计算机、数字信号处理器等上执行时，执行上述方法步骤。

[0061] 根据本发明的计算机可读存储部件包括根据本发明的计算机程序产品。

[0062] 根据本发明的光学记录载体包括可执行程序，它在光学记录载体被插入驱动器中时自动启动，并且

[0063] - 在计算机、数字信号处理器等上执行时，执行上述方法步骤，和 / 或

[0064] - 安装在计算机、数字信号处理器等上执行时执行上述方法步骤的驱动程序。

[0065] 换句话说，光学记录载体包括一个可执行程序，它可直接和 / 或间接地实施根据本发明的方法。

[0066] 如上所示，根据本发明，光学记录载体最好是多会话 CD，它包括音频会话和数据会话，其中可执行程序最好具有自动启动功能。然而，自动启动功能并非强制的。

[0067] 附图说明

[0068] 本发明如上所述以及如下所述的所有不同方面可以用任何方式组合。结合到此说明书中并构成此说明书一部分的附图，图示了本发明的示例性实施例，并且附图和以上对本发明的一般说明、以及以下对实施例的详细说明一起，用于解释发明原理，其中：

[0069] 图 1 显示在根据本发明的多层驱动程序模型中处理 I/O 请求的一个简化方案，

[0070] 图 2 显示用于根据本发明的通信接口的修改的 SCSI 命令的概略结构，

[0071] 图 3 显示在根据先有技术的多层驱动程序模型中处理 I/O 请求的一个简化方案，以及

[0072] 图 4 显示根据先有技术的 SCSI 命令的大致结构。

[0073] 具体实施方式

[0074] 根据本发明的以下示例性实施例，特别标记的盘（目标盘）的光介质得到保护免于非法读出和 / 或复制。对于光介质上内容的这种保护（如 CD, DVD...）免于非法读出，使用可由操作系统读出（如 Windows）的包含标准文件格式（ISO、UDF...）数据的盘（称为数据会话）。除了数据会话，盘能具有任何数量的其它会话，不管什么类型。

[0075] 至少以下被归入数据会话：

[0076] • 特别修改的软件（在下面成为 EXE）。此 EXE 一般是启动菜单。

[0077] • 允许的自动播放，它在光介质被插入驱动器中之后启动 EXE。

[0078] 在介质插入（自动播放）驱动器中之后或者由用户手动开始 EXE 之后，在发起 EXE 时，它将提取和安装一个特别设计的过滤驱动程序（下面称为驱动程序），该过滤驱动程序执行以下任务：

[0079] • 区别需要被保护的目标盘和非目标盘。

[0080] • 以使读出数据无用的方式,修改目标盘的被保护数据区的特定 SCSI 读出请求。

[0081] 同时,指挥写入涉及目标盘的被保护数据这样的数据到可记录盘或者到另一个存储器的写入命令可以用使写入数据无用的方式进行修改。涉及目标盘的被保护数据的数据可以通过水印或者其它适当的机构识别。

[0082] 作为实施和应用过滤驱动程序强制重新启动操作系统的标准方式,采用一个特定而特别的过滤方法。

[0083] 图 3 显示在多层次驱动程序模型中如何处理 I/O 请求的一个简化方案,例如 Windows 操作系统中使用的。用①标注的是由 I/O 管理器对每层的调度例程的调用,从层 1 开始。最后一层访问物理设备,用②标注。在完成物理设备之后,I/O 管理器调用每层的完成例程,从的最后一层开始,标注为③。在第一层完成例程完成之后,I/O 请求结束,用④标注。

[0084] 根据本发明的示例性实施例,驱动程序搜索 SCSI 层并插入它自己的例程 DHR(调度钩例程)和 CHR(完成钩例程)代替原始的调度和完成例程,如图 1 所示。DHR 和 CHR 调用它们的原始对应体,即原始的调度例程和原始的完成例程,使得作为缺省,系统的行为没有通过引入钩例程而改变。

[0085] 具体地说,图 1 阐明驱动程序如何通过插入调度和完成钩例程到 SCSI 层中,而能够跟踪发送给 CD/DVD 装置的每个 SCSI 命令。用⑤标注的是 SCSI 层的调度例程用驱动程序的调度钩例程替换。这个例程调用原始的调度例程。用⑥标注的是 SCSI 层的完成例程用驱动程序的完成钩例程替换。这个例程调用原始的完成例程。

[0086] 因此,驱动程序能够通过利用 DHR 和 CHR 跟踪发送给 CD/DVD 驱动器的每个 SCSI 请求,下面的任务在 DHR 和 CHR 内部执行:

[0087] ● 辨别目标盘和非目标盘。

[0088] ● 如果正确地识别目标盘,则执行修改。

[0089] ● 处理 CCI 请求(秘密通信接口)。

[0090] 为了区别目标和非目标盘,将以下标准以任何组合用于:

[0091] ● 第二会话中的专用修改。

[0092] ● 专门的 TOC 项目。

[0093] ● 专门的子码修改(或者在第一会话中或者在第二会话中)。

[0094] ●(音频)数据中的水印。

[0095] 被保护数据是目标盘的一部分。下列标准可用于识别目标盘上的被保护数据区:

[0096] ● 扇区类型,它表示规定类型的所有扇区(CDDA、模式 1, ...) 是被保护数据区的一部分。

[0097] ● 多个扇区,其中被保护数据区能通过规定开始和结束扇区来限定。

[0098] ● 检测特定的读出序列,例如检测对于盘克隆和破裂程序为典型的顺序读出,并且拒绝所有其它的读出请求。

[0099] 被保护数据区可以按以下方式被保护:

[0100] ● 全部保护,这意味着不允许到保护区的任何读出请求。不管什么应用执行请求。

[0101] ● 可分离的保护,这意味着信赖的应用能通过经 CCI(秘密的通信接口)发送验证数据认证它们自己,由此仅仅允许认证后的过程读出被保护数据。

[0102] 因此,可以用上述标准以任何组合规定一个或者多个被保护数据区。

[0103] 被保护数据区可用以下定义:

[0104] ●驱动程序(驱动程序代码中硬编码)

[0105] ●盘上存储的数据

[0106] ●两者的组合。

[0107] 如果正确地识别了目标盘,则可以进行对尝试读出保护数据的 SCSI 读出请求的如下修改:

[0108] ●用一个出错放弃(完成)IO 请求。

[0109] ●用 STATUS_SUCCESS(状态成功) 完成 IO 请求,但不处理实际的读出。

[0110] ●修改读出数据,使其无用。

[0111] 为了保护驱动程序免于从系统移去,可以采取一个或多个下列措施:

[0112] ●驱动程序不能卸载,因为它不具有“卸载例程”。

[0113] ●驱动程序名称随机改变

[0114] ○安装处理选择一个随机的名称(由 EXE 完成)。

[0115] ○驱动程序在系统运行时间期间和 / 或在系统关机期间随机改变它的名称。

[0116] ●在安装序列(由 EXE 完成)期间和 / 或运行时间期间随机设置驱动程序文件时间(建立时间、最后的存取时间和最近写入时间)。

[0117] ●在安装序列期间随机改变驱动程序代码(不改变它的功能)。(由 EXE 完成)。

[0118] ●驱动程序多次安装它自己,并且除了一个之外,驱动程序的所有其它实例都无效。

[0119] ○在驱动程序之间存在一个秘密的受保护通信接口,用于检查是否已经存在一个有效的驱动程序实例在运行。

[0120] ○如果驱动程序检测到另一个驱动程序已经在运行,则它将自己设置为无效。

[0121] ●在整个系统中传播驱动程序安装程序(隐藏的)。

[0122] 在下面描述根据本发明的秘密通信接口(CCI),它用于允许软件与驱动程序通信,例如用于认证、和 / 或允许驱动程序彼此通信,例如在安装了驱动程序的多个实例的情况下。

[0123] SCSI 命令用来向驱动程序发送数据以及从其接收数据(背载)。图 4 显示 SCSI 命令大致的结构,它包括 CDB、即 CSI 命令描述符块、以及如果发送的命令请求,还包括一个数据缓冲器。取决于 CDB,数据缓冲器能被用于存储读出数据(读出命令),或者如果执行的是写入命令,则作为数据源。缓冲器长度可以是<= 0 的值,也取决于 CDB。

[0124] 根据本发明的示例性实施例,为了进行通信,SCSI 命令所需的数据块附着到 SCSI 命令,以产生一个修改的 SCSI 命令用于秘密的通信接口(CCI),如图 3 所示。SCSI 命令不再需要的数据缓冲区将在下面称为 DBE(数据缓冲延伸)。

[0125] DBE 用于 CCI 并包含驱动程序检测和计算的信息,并且驱动程序也将把可能的返回值放置在 DBE 中。

[0126] DBE 的内容由发送器加密并且由驱动程序解密。如果驱动程序将返回值放置在 DBE 中,它将在后面对 DBE 加密并且发送器将再对 DBE 解密。

[0127] 所有的 SCSI 命令都使用,即它们自己不需要数据缓冲器的命令特别适用于

CCI(例如测试单元就绪),因为它们易于操纵。也可以使用自己定义的SCSI命令。

[0128] 为了容易地安装驱动程序,根据本发明的例示性实施例,将驱动程序安装序列引入一个可执行程序中。这用来添加代码,该代码提取并且安装驱动程序到任何可执行程序(在下文中称为Target.exe)。所以,执行下列任务:

[0129] ●建立动态地可加载的库文件(例如用于Windows操作系统的DLL)。

[0130] ○包含驱动程序。

[0131] ○执行并且转发由使用的动态可加载库(称为目标库)的接口(例如Windows操作系统上的Kernel32.dll)

[0132] ○包含启动例程,它在加载该库时被调用。(Windows操作系统上DLL中的D1lMain例程)。这个启动例程提取并且安装驱动程序。

[0133] ○所述库可具有任何名称,但是名称的长度不应比目标库的名称长。为了便于解释,将其称为Inject.dll。

[0134] ●可执行程序包含使用的所有动态可加载库的列表(称为importlist)。

[0135] ●当一个可执行程序开始执行时,importlist中列出的每个库都被加载,并且执行它的启动例程。

[0136] ●Target.exe的importlist中目标库的名称(例如Kernel32.dll)用Inject.dll的名称替换。

[0137] 因此,当Target.exe在执行时,Inject.dll也被加载,并且执行它的启动例程,由此提取并且安装驱动程序。

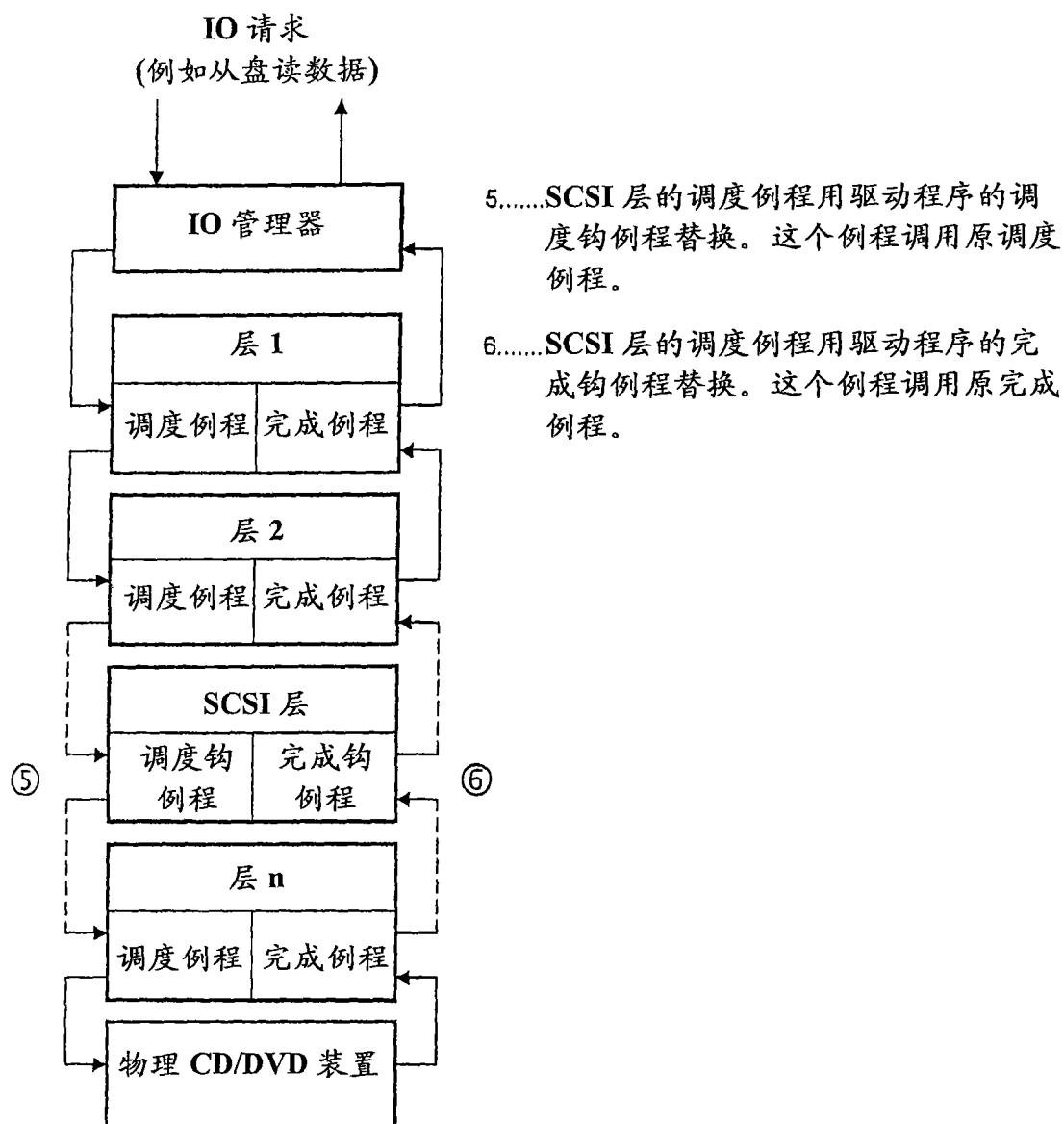


图 1

CDB	CDBSCSI 命令描述符块
数据缓冲	数据缓冲.....取决于 CDB, 缓冲长度可以是 ≥ 0 的值。 数据缓冲扩展.....用于 CCI 的数据缓冲的扩展
数据缓冲扩展	

图 2



图 4

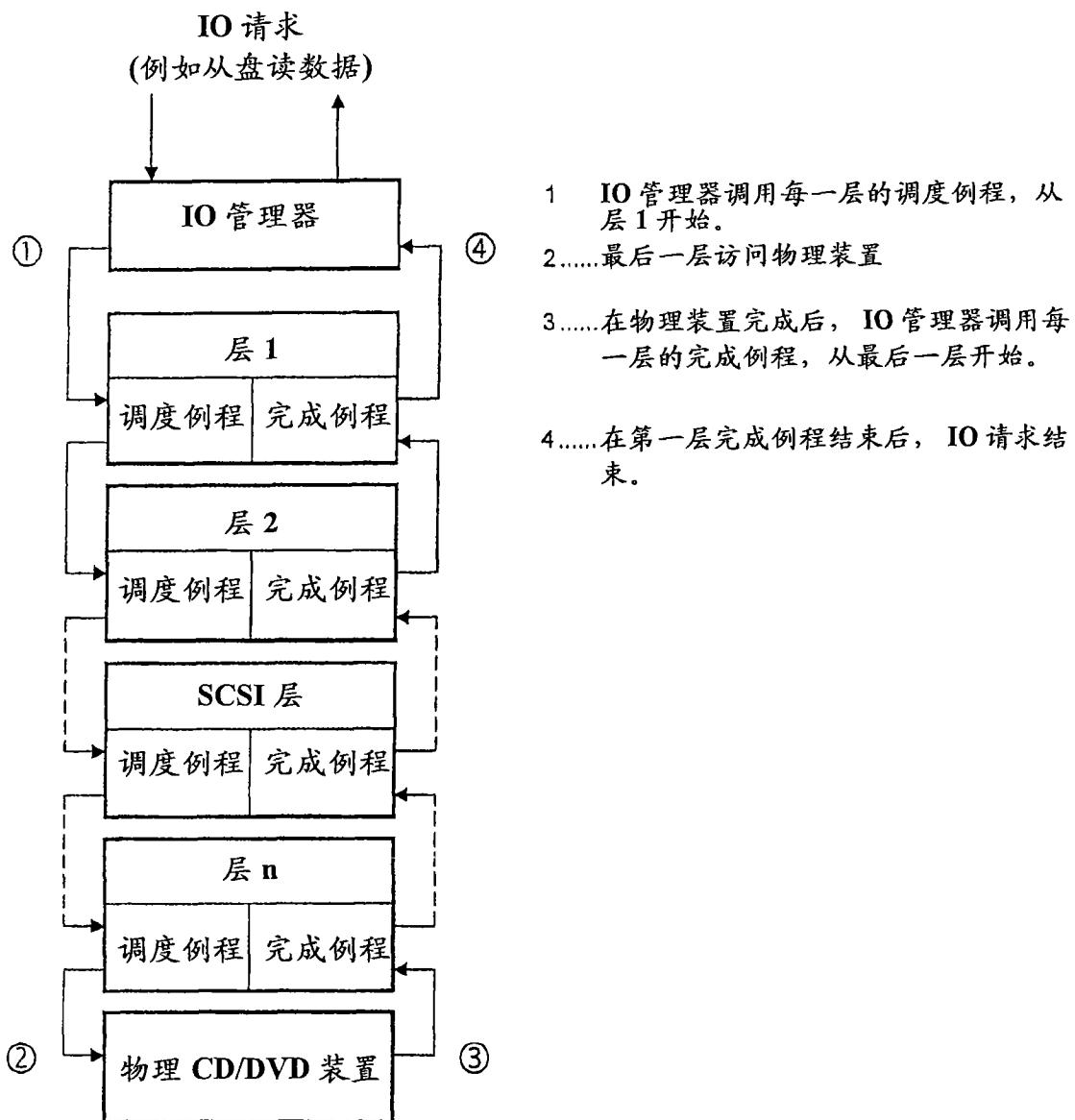


图 3