

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 12/14

G06F 17/60

G11B 20/10

G11B 27/00



[12] 发 明 专 利 说 明 书

专利号 ZL 02802454.0

[45] 授权公告日 2005 年 12 月 14 日

[11] 授权公告号 CN 1231848C

[22] 申请日 2002. 6. 18 [21] 申请号 02802454.0

[30] 优先权

[32] 2001. 6. 18 [33] JP [31] 183217/01

[86] 国际申请 PCT/JP2002/006062 2002. 6. 18

[87] 国际公布 WO2002/103530 日 2002. 12. 27

[85] 进入国家阶段日期 2003. 3. 20

[71] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 阿部三树 细井隆史 松田宽美

田中理生

审查员 徐 薇

[74] 专利代理机构 北京市柳沈律师事务所

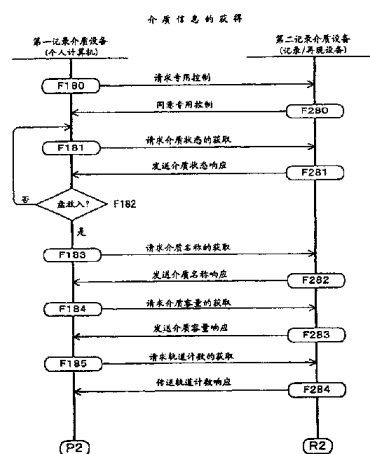
代理人 邸万奎 黄小临

权利要求书 2 页 说明书 61 页 附图 45 页

[54] 发明名称 数据传送方法

[57] 摘要

一种通过获取关于作为内容传送目的地的第二记录介质的信息实现适当系统操作的数据传送设备。例如，当诸如袖珍盘的使用其原始管理方法的介质被用做检出目的地的第二记录介质时，数据传送设备侧(第一记录介质侧)请求数据记录设备侧(第二记录介质侧)发送关于第二记录介质的信息并获得必要的信息。关于第二记录介质的信息包括第二记录介质是否安装在数据记录设备上的信息、第二记录介质的名称信息、记录在第二记录介质上的内容数据的名称信息、第二记录介质的容量信息、记录在第二记录介质上的内容数据的数量信息、和记录在第二记录介质上的内容数据的属性信息。



1、一种由形成传送系统的数据传送设备采用的数据传送方法，其中：
所述数据传送设备具有用于存储加密内容数据的第一记录介质：

5 采用了数据记录设备；

所述数据记录设备能够以不加密状态把所述内容数据记录到第二记录介质上，和从第二记录介质再现所述内容数据；和

所述数据传送设备连接于所述数据记录设备，使所述数据传送设备和所述数据记录设备能够彼此通信，所述数据传送方法包括：

10 确认处理过程，用于确认所述第二记录介质已经被安装在所述数据记录设备上；

信息获取处理过程，用于从所述数据记录设备获取安装在所述数据记录设备上的所述第二记录介质的信息；

15 验证处理过程，用于通过采用不对称加密验证数据记录设备确实是充当所述第一记录介质中存储的所述内容数据的有效传送目的地的一个设备，其中

所述数据记录设备将公共密钥发送给所述数据传送设备，然后，所述数据传送设备产生随机数并将该随机数发送给所述数据记录设备，所述数据记录设备利用其保存的密钥将该随机数加密，并将所产生的加密数据发送给所述数据传送设备，随后，所述数据传送设备利用所述公共密钥将所产生的加密数据解密，并将解密结果与所述随机数相比较；

判断处理过程，用于根据所述验证处理过程产生的验证结果，判断所述第一记录介质中存储的所述内容数据是否应当传送给所述数据记录设备；

25 传送处理过程，根据判断处理过程形成的判断结果，传送内容数据到所述数据记录设备。

2、根据权利要求1所述的数据传送方法，其中执行所述信息获取处理过程，从所述数据记录设备中获取安装在所述数据记录设备上的所述第二记录介质的名称，或者记录在所述第二记录介质上的每个内容数据的名称，以作为所述第二记录介质的所述信息。

30 3、根据权利要求1所述的数据传送方法，其中执行所述信息获取处理过程，从所述数据记录设备中获取安装在所述数据记录设备上的所述第二记录

介质的容量，以作为所述第二记录介质的所述信息。

4、根据权利要求1所述的数据传送方法，其中执行所述信息获取处理过程，从所述数据记录设备中获取安装在所述数据记录设备上的所述第二记录介质所存储的内容数目，以作为所述第二记录介质的所述信息。

- 5 5、根据权利要求1所述的数据传送方法，其中执行所述信息获取处理过程，从所述数据记录设备中获取所述第二记录介质所记录的每个内容数据的属性，以作为所述第二记录介质的所述信息。

数据传送方法

5 技术领域

本发明涉及适合于传送和/或记录诸如音乐的内容数据的数据传送系统、数据传送设备、数据记录设备和数据传送方法。

背景技术

10 在如音乐的内容数据的典型应用中,存储在诸如个人计算机的HDD(硬盘驱动器)的第一记录介质中的数据被传送到用作第二记录介质的另一个记录介质,以便允许欣赏从第二记录介质再现的数据。需要注意的是,内容数据包括音乐数据、视频数据、游戏数据和计算机软件,提供这些数据和软件主要是用于分布、传送和利用的目的地。

15 在该情况下,个人计算机中使用的HDD被用来存储内容数据,比如存储从诸如CD-DA(致密盘数字音频)和DVD(数字通用盘)的数据包记录介质中再现的音乐,或者被用来存储通过通信网络从外部音乐服务器下载到连接该网络的个人计算机。然后,用户把个人计算机连接到一个记录设备上,用于记录数据到第二记录介质上,将内容数据从HDD复制或移到第二记录介质上。

20 为了欣赏内容数据,再现设备用来从第二记录介质再现数据。

可以想到的第二记录介质的实例是一个利用半导体存储器的存储卡,比如快闪存储器、用作磁光盘的袖珍盘、CD-R(可记录CD)、CD-RW(可改写CD)、DVD-RAM、DVD-R、DVD-RW。

25 作为分别用于第二记录介质的记录设备和再现设备,用于这些记录介质(包括半导体存储器、袖珍盘、CD-R、CD CD-RW、DVD-RAM、DVD-R、DVD-RW)的记录器和播放器已经变得非常普及。记录器和播放机被设计成各种实施,比如固定记录/再现设备和便携记录/再现设备。因此,通过使用用户喜爱的或者与用户已经拥有的设备相称的记录器和播放机的实施,用户可以记录和再现内容数据。

30 需要注意的是,当考虑内容数据的这种应用时,例如必须考虑内容数据

的版权保护。例如假如用户通过使用分布内容数据的服务或者通过购买包含内容数据的封装式介质获得内容数据，在把内容数据存储到 HDD 之后，允许用户没有任何限制地把内容数据复制到第二记录介质上。在此情况下，内容数据的这种应用造成版权所有者不能得到适当保护的情况。为了解决此问题，人们已经提出了各种在处理诸如数字数据的内容数据时保证版权得到保护的协定和技术。该协定之一是称之为 SDMI（安全数字音乐创制权）的标准。

ISMI 标准中规定的数据路径将在下面描述。至少，在考虑了版权保护和普通用户的利益之后，可以把存储在作为第一记录介质的个人计算机中使用的一个 HDD 中的内容适当地传送或者记录到第二记录介质上。所述的利益包括内容的个人复制的权利。HDD 中存储的内容的例子包括网络内容和盘内容。网络内容是将要在 HDD 中存储的由一个外部服务器典型地通过一个网络分布到个人计算机上的内容数据。另一方面，从数据包记录介质中读出将要存储在 HDD 中的盘内容。如上所述，数据包记录介质的例子是 CD-DA 和 DVD。数据包记录介质被安装在用于再现盘内容的盘驱动器上。通常，盘驱动器被安装在个人计算机内或者与个人计算机连接。盘驱动器包括一个 CD-ROM 驱动器。

顺便说明，当内容数据在一个复制操作中从诸如 HDD 的第一记录介质传送到诸如袖珍盘或者存储卡的第二记录介质时，进行满足版权和个人复制权的保护的测量。

为了满足这种保护，从符合下述的 SDMI 标准的第二记录介质传递数据。

符合 SDMI 标准的第二记录介质被假定为这样一个记录介质，它包括利用符合 SDMI 标准的一个诸如快闪存储器的半导体存储器的存储卡。这种第二记录介质在类似例如 HDD 的第一记录介质中，符合 SDMI 标准的内容以一种加密状态存储，这样实际上，内容还将以加密装置复制到第二记录介质上。

当然，为这样一种第二记录介质准备的再现设备具有加密功能，以允许在加密状态下复制到第二记录介质上的内容数据被再现。

在符合 SDMI 标准的第二记录介质中，记录格式包括一个用于记录内容 ID 的一个区域，该内容 ID 被用作识别每条内容数据的一个标识符。

内容 ID 是为存储在所述第一记录介质中的每条内容数据而生成的，并且与该条内容数据一起存储，其中所述的第一记录介质可以是在用于第一记录介

质的设备中使用的 HDD。当内容数据被复制到第二记录介质上时，识别内容数据的内容 ID 也被存储在第二记录介质中。

内容数据 ID 被用来管理第一和第二记录介质中的内容权。第一记录介质中的内容的内容权是一种在复制内容到第二记录介质的操作中，把内容从
5 第一记录介质传送到第二记录介质的权利。另一方面，第二记录介质中的内容的内容权是从第二记录介质中再现内容的权利。

需要注意的是，在以下说明中，从第一记录介质到第二记录介质的内容数据的传送（一种权利传送）被称之为检出（check-out）。另一方面，从第二记录介质到第一记录介质的内容数据的传送（事实上，仅仅一种权利的传
10 送）被称之为检入（check-in）。

根据 SDMI 标准，为检出和检入建立了一些传送应用规则。

例如，对于一条内容数据，仅允许从第一记录介质到第二记录介质的多达三次检出。这样，传送权允许该条内容数据被传送三次。

在检出中，还从第一记录介质向第二记录介质传送权利。因此，第一记录介质中的传送权现在只允许该条内容数据被传送两次。另一方面，把再现权给予第二记录介质。
15

另一方面，在检入中，从第二记录介质向第一记录介质返回权利。因而，第二记录介质损失一个再现权，同时恢复第一记录媒一个已传送的权利。

通过使用识别一条内容数据的内容 ID 管理用于每条内容数据的这种检出和这种检入。
20

此外，在检出中，一条内容数据和识别该条内容数据的内容 ID 被记录到第二记录介质上。给予第二记录介质一个再现该条内容数据的再现权。另一方面，第一记录介质被认为传送了一个内容 ID，根据应用规则该第一记录介质则损失一个传送权。

另一方面，在检入中，实际上不返回内容数据。相反，内容数据只是从第二记录介质擦除，并且将内容 ID 返回到第一记录介质，以把应用规则规定的传送权的数量递增 1。第二记录介质损失再现内容数据的再现权。
25

如上所述，内容数据还以加密状态复制到符合 SDMI 标准（该 SDMI 标准规定数据以加密状态存储到记录介质中）的第二记录介质上，并且在检出或者检入情况下管理内容权，以避免内容数据被复制无限制的次数，同时保护
30 版权以及确保用户的个人复制权。

需要注意的是，通常从外部服务器下载到用作第一记录介质的 HDD 的内容数据是以使用内容密钥 CK 进行加密的状态存储到 HDD 中的。

在本说明中，假定 HDD 中存储的内容数据是作为压缩和加密该压缩的结果得到的，即采用 ATRAC3 技术或者其它压缩技术压缩原始内容数据并且通过
5 通过使用内容密钥 CK 对压缩的数据 A3D 加密而得到的。

另一方面，符号 $D\{x, E, (x, y)\}$ 是指作为使用密钥 x 对加密数据 $E(x, y)$ 解密的结果而得到的解密数据。

因而，作为压缩原始内容数据和使用内容密钥 CK 加密该压缩数据 A3D 的结果得到的内容数据可以由这样一个符号表示：

10 $E(CK, A3D)$

另一方面，作为使用密钥 CK 对加密数据 $E(CK, A3D)$ 解密的结果获得的解密数据由这样一个符号表示：

$D\{CK, E(CK, A3D)\}$

除了加密的内容数据 $E(CK, A3D)$ 以外，用作第一记录介质的 HDD 还被用
15 来存储 $E(KR, CK)$ ，它是处于使用根密钥进行加密状态下的内容密钥 CK。因此，例如在从外部服务器下载已加密内容数据 $E(CK, A3D)$ 的情况下，还从服务器下载加密内容密钥 $E(KR, CK)$ 。

在这种情况下，在加密内容数据 $E(CK, A3D)$ 到第二记录介质的检出
20 中，加密内容数据 $E(CK, A3D)$ 和加密内容密钥 $E(KR, CK)$ 需要从用作第一记录介质的 HDD 传送到第二记录介质。

用于第二记录介质的设备保持对加密的内容密钥 $E(KR, CK)$ 解密的根密钥 KR，以产生原始内容密钥 CK。该内容 CK 随后被用来对加密的内容数据 $E(CK, A3D)$ 解密，以产生原始内容数据 A3D。

然而，根据版权所有者的愿望或者各种原因，可以改变该根密钥 KR。
25 也就是说，可以为每条内容数据设置根密钥 KR。此外，这里提供了一种通过处理根密钥 KR 强化对内容分配的限制的功能。下面将具体说明这种功能。

因此，在某些情况下，分配称之为 EKB（启动密钥字块）的数据。此外，在某些情况下，接收被传送的内容数据的一个固定终端采用一种使用 EKB 确认根密钥的技术。也就是说，从服务器分布一个将要与加密内容数据和加密
30 内容密钥一同存储在 HDD 中的 EKB。

考虑这样一种情况，将已经变得非常流行的袖珍盘（或者磁光盘）用作

符合 SDMI 标准的袖珍盘记录设备中的第二记录介质。在此情况下，将检出中传送到袖珍盘的加密内容数据 $E(CK, A3D)$ 实际上以加密状态存储到袖珍盘中。

5 然后，在再现操作中，符合 SDMI 标准的记录设备对加密的内容数据 $E(CK, A3D)$ 解密，以产生内容数据 $D\{CK, E(CK, A3D)\} = A3D$ ，该内容数据是采用 ATRAC3 压缩技术压缩的内容数据。然后，袖珍盘记录设备对压缩的内容数据 A3D 执行预定的解码处理，以输出诸如音乐的再现数据。

10 另一方面，在普通袖珍系统中使用的一个袖珍盘（已经变得非常流行）中，不以加密状态存储数据。因而，作为一个袖珍盘再现设备，袖珍盘系统实际上没有解密功能。

所以，通过符合 SDMI 标准的袖珍盘记录设备记录在袖珍盘中的内容数据不能被大多数不符合 SDMI 标准的袖珍盘播放器再现。也就是说，通过符合 SDMI 标准的袖珍盘记录设备记录在袖珍盘中的内容数据与袖珍盘播放器的再现不兼容。

15 这意味着，普通用户购买的 SDMI 内容的正确使用受到限制，从而极大地降低了向普通用户提供 SDMI 内容的服务价值以及用户满意这种服务的程度。

为了解决上述问题，在把 SDMI 内容复制到第二记录介质，比如安装在不符合 SDMI 标准的袖珍盘记录设备上的袖珍盘的记录操作中，对 SDMI 内容解密，以便可以以实际上未加密的状态将内容存储在袖珍盘中。

然而，如果可以执行这样一种复制操作，则能够容易地复制内容数据。这样一种复制操作也留下了能够非法复制的空间，导致不能实施作为 SDMI 标准的原本目标的版权保护的担心。

25 为了解决上述问题，作为传送内容数据的一种方法，本发明的专利申请人已经提出了如下所述的一种传送技术。

在传送内容数据的操作中，用作第一记录介质设备的数据传送设备验证充当传送目的地的用作第二记录介质设备的数据记录设备。如果验证的结果是 OK，则在内容提供者（比如版权所有）许可该传送的条件下允许该内容数据的传送。然后，经由传输线路以加密状态传送内容数据，并且在存储在第二记录介质之前，对加密的内容数据解密。此外，管理用于检出和检入的权利。

这样，由于允许复制和记录未加密状态的内容数据的操作，因此向用户提供了更多的便利，而且不损失保护版权的功能。

通过在包括一个用作数据传送设备的个人计算机和一个用作数据记录设备的袖珍盘记录器的系统中采用这种技术，从个人计算机中使用的 HDD 实施的第一记录介质到安装在袖珍盘记录器上的袖珍盘实施的第二记录介质的内容传送实际上确实适合于内容供应者和用户双方。

通过把诸如袖珍盘（已经变得很普及）的介质用作上述的检出的目的地，使袖珍盘实际使用中的有用性得到增加。然而，存在这样一种情况，诸如个人计算机的数据传送设备不可能识别采用其自己唯一数据管理方法的一种介质的条件或者属性。采用自己唯一数据管理方法的介质的一个例子是袖珍盘。

例如，通过使用 FAT 管理作为符合 SDMI 标准的一个介质实例给出的一个存储卡中记录的内容数据，以便使该存储卡确实与个人计算机兼容。也就是说，充当数据传送设备的个人计算机仅通过从作为可移动介质连接的存储卡读出 FAT，就能够获得该存储卡的状态的信息，其中，该可移动介质用作一个检出中的目的地。存储卡的状态通常包括存储卡的存储容量和存储卡记录的内容数量。

因此，当希望在检出中传送某些内容数据到存储卡时，能够根据存储卡的存储容量和其它信息形成一个判断：是否可以向存储卡传送内容数据。

然而，在通常用于音频数据应用的作为采用自己唯一数据管理方法的介质而开发的介质实际上具有袖珍盘情形的情况下，个人计算机不能够直接获得该介质的状态信息，所以不能在检出或者其它操作中形成所述判断。

因此，当假定作为检出的目的地的第二记录介质使用袖珍盘或者其它介质时，充当数据传送设备的个人计算机需要具有一种允许袖珍盘或者其它介质的状态被识别的方法。

25

发明内容

因此，本发明的目的是解决上的问题，提供一种当数据传送系统中的数据传送设备连接到能够以不加密状态把内容数据记录到第二记录介质以及从第二记录介质再现数据的数据记录设备时实施的数据传送方法。

30 为了实现上述目的，本发明提供了一种由形成传送系统的数据传送设备采用的数据传送方法，其中所述数据传送设备具有用于存储加密内容数据的

第一记录介质：采用了数据记录设备；所述数据记录设备能够以不加密状态把所述内容数据记录到第二记录介质上，以及从第二记录介质再现所述内容数据；并且，所述数据传送设备连接于所述数据记录设备，使所述数据传送设备和所述数据记录设备能够彼此通信，该数据传送方法包括：确认第二记录介质已经被安装在数据记录设备上的确认处理过程；获取安装在数据记录设备上的第二记录介质的信息的信息获取处理过程；验证处理过程，用于通过采用不对称加密验证数据记录设备作为充当第一记录介质中存储的内容数据的传送目的地的一个设备的有效性，其中，所述数据记录设备将公共密钥发送给所述数据传送设备，然后，所述数据传送设备产生随机数并将该随机数发送给所述数据记录设备，所述数据记录设备利用其保存的密钥将该随机数加密，并将所产生的加密数据发送给所述数据传送设备，随后，所述数据传送设备利用所述公共密钥将所产生的加密数据解密，并将解密结果与所述随机数相比较；判断处理过程，用于根据信息获取设备获取的信息判断是否执行把第一记录介质中存储的内容数据传送到数据记录设备的处理；传送处理过程，根据判断处理过程形成的判断结果传送内容数据。

在该数据传送方法中，第二记录介质的信息包括：指示第二记录介质是否已经安装到数据记录设备上的信息；关于安装在数据记录设备上的第二记录介质的名称的信息；关于安装在数据记录设备上的第二记录介质中所存储的诸多条内容数据的名称的信息；关于安装在数据记录设备上的第二记录介质的存储容量的信息；关于安装在数据记录设备上的第二记录介质中存储的诸多条数据内容的数量的信息；关于安装在数据记录设备上的第二记录介质中存储的诸多条数据内容的属性的信息。

附图说明

图 1 是显示本发明一个实施例所采用的加密技术的树结构的示范性视图；

图 2A 和图 2B 分别是显示该实施例所采用的加密技术的 EKB 的示范性示意图；

图 3 是显示该实施例所采用的加密技术的 EKB 结构的示范性示意图；

图 4 是显示由该实施例实施的数据传送系统的结构的方框图；

图 5 是显示该实施例的 SDMI 内容的典型数据路径的示范性视图；

-
- 图 6 是显示由该实施例提供的第一记录介质设备的方框图；
- 图 7 是显示由该实施例提供的第二记录介质设备的方框图；
- 图 8 是显示袖珍盘系统的簇格式的示范性视图；
- 图 9 是显示袖珍盘的区域结构的示范性视图；
- 5 图 10 是袖珍盘系统的 U-TOC（用户内容表）扇区 0 的示范性视图；
- 图 11 是显示袖珍盘系统的 U-TOC 扇区中的链接的示范性视图；
- 图 12 是显示袖珍盘系统的 U-TOC 扇区 1 的示范性视图；

图 13 显示了一个表示该实施例的验证处理的流程图;

图 14 是显示待传送的分布内容数据和加密数据的处理的示范性视图;

图 15A 和图 15B 是显示本实施例采用的典型加密技术和该技术中使用的 DNK (装置节点密钥) 的示范性视图;

5 图 16 是显示由解密内容数据的实施例采用的处理过程的示范性视图;

图 17 显示了代表该实施例执行的检出操作的流程图;

图 18 显示了代表该实施例执行的检出操作的延续流程图;

图 19 是显示在该实施例中使用的记录对象控制命令的示范性视图;

图 20 是显示在该实施例中使用的记录对象响应命令的示范性视图;

10 图 21 是显示在该实施例中使用的检出控制命令的示范性视图;

图 22 是显示在该实施例中使用的检出响应命令的示范性视图;

图 23 显示了代表该实施例执行的检入操作的流程图;

图 24 是显示在该实施例中使用的检入控制命令的示范性视图;

15 图 25 是显示在该实施例中使用的检入控制命令的子函数 (sub-function) 的示范性视图;

图 26 是显示在该实施例中使用的检入响应命令的示范性视图;

图 27 是显示该实施例中生成内容 ID 的示范性视图;

图 28 显示了该实施例中的关联内容 ID 的表;

图 29 显示了代表由该实施例执行获取介质信息的操作的流程图;

20 图 30 显示了由该实施例执行获取介质信息的操作的延续流程图;

图 31 是显示该实施例中使用的相容登记 (log-in) 控制命令的示范性视图;

图 32 是显示该实施例中使用的相容注销 (log-out) 控制命令的示范性视图;

25 图 33 是显示该实施例中使用的得到盘状态控制命令的示范性视图;

图 34 是显示该实施例中使用的得到盘状态响应命令的示范性视图;

图 35 是显示该实施例中使用的得到盘名称控制命令的示范性视图;

图 36 是显示该实施例中使用的得到盘名称响应命令的示范性视图;

30 图 37 是显示该实施例中使用的得到盘容量信息控制命令的示范性视图;

图 38 是显示该实施例中使用的得到盘容量信息响应命令的示范性视图;

图;

图 39 是显示该实施例中使用的得到盘容量信息响应命令的示范性视图;

图 40 是该实施例中使用的得到音频轨道计数控制命令的示范性视图;

5 图 41 是显示该实施例中使用的得到音频轨道计数响应命令的示范性视图;

图 42 是显示该实施例中使用的得到音频轨道名称控制命令的示范性视图;

图 43 是显示该实施例中使用的得到音频名称响应命令的示范性视图;

10 图 44 是显示轨道属性的读出信息块控制命令的示范性视图;

图 45 是显示轨道属性的读出信息块响应命令的示范性视图;

图 46 是显示轨道模式的读出信息块控制命令的示范性视图;

图 47 是显示轨道模式的读出信息块响应命令的示范性视图;

图 48 是显示轨道大小的读出信息块控制命令的示范性视图;

15 图 49 是显示轨道大小的读出信息块响应命令的示范性视图;

具体实施方式

本发明的优选实施例按照以下顺序安排的段落进行解释。

- 1、 加密密钥和 EKB 的树结构
- 20 2、 系统配置
- 3、 SDMI 内容的数据路径
- 4、 数据传送设备（第一记录介质设备或者 PC）的典型配置
- 5、 数据记录设备（第二记录介质设备或者记录/再现设备）的典型配置
- 25 6、 袖珍盘的管理技术
- 7、 验证处理
- 8、 内容加密技术
- 9、 内容检出/检入
- 10、 内容 ID 的生成和管理技术
- 30 11、 介质信息的获取
- 12、 加密密钥和 EKB 的树结构

首先，在具体解释由本发明的实施例实施的传送系统之前，先说明内容分布中使用的加密密钥的结构。

首先，下面的说明通过参考图 1、图 2A、图 2B 和图 3 解释装置的加密密钥所有权方案和数据分布方案，这些方案是从内容分配器向充当内容收件人的装置分配加密数据时采用的方案。

图 1 是显示加密密钥的树结构的示范性视图。图 1 中所示的分层树结构的底层上的参考标记 DV0 至 DV15 是指内容收件人方的装置。因此，分层树结构的每个树叶相当于这样的装置。

在制造时、运送时或者以后给予装置 DV0 至 DV15 之每个装置一组密钥。在每个装置使用的存储器中存储的给予装置的该组密钥包括：一个树叶密钥，被分配给代表图 1 所示分层树结构中的装置的一个树叶；多个节点密钥，其每个分配给分层树结构的树叶与树根之间的一个节点。包含在该密钥组中的诸多密钥被称作 DNK（装置节点密钥），下面说明用于解释的例子。

图 1 所示的分层树结构的底层上的 K0000 至 K1111 是分别给予装置 DV0 至 DV15 的树叶密钥。KR 是分配给分层树结构顶层上树根的树根密钥。K000 至 K111 是分配给从底层到第二分层层上的节点的节点密钥。在下面的说明中，节点密钥是指包括分配给树根的树根密钥 KR 的节点密钥。

在图 1 所示的分层树结构中，给予装置 DV0 的 DNK 包括：一个树叶密钥 K0000，节点密钥 K000、K00 和 K0，以及一个树根密钥 KR。包含在 DNK 中的节点密钥 K000、K00 和 K0 以及树根密钥 KR 由装置 DV0 以使用树叶密钥 K0000 进行加密的状态保持。

出于同样原因，给予装置 DV5 的 DNK 包括：一个树叶密钥 K0101，节点密钥 K010、K01 和 K0，以及一个树根密钥 KR。同样，给予装置 DV15 的 DNK 包括：一个树叶密钥 K1111，节点密钥 K111、K11 和 K1，以及一个树根密钥 KR。

需要说明的是，尽管在图 1 所示的树结构中只显示了 16 个装置 DV0 至 DV15，以及把树结构设计成具有 4 个分层层的一个平衡的左右对称结构，但是树结构可以包括更多的装置，并且具有从一部分到一部分变化的层计数的配置。

此外，包含在图 1 所示的树结构中的各种信息处理设备具有各种记录介质。这些信息处理设备是各种类型的装置。装置具有诸如 DVD、CD、MD 和快

闪存储器的记录介质，它们或者被置入装置中，或者可以高度自由地装在装置上和从该装置中拆卸。此外，可以为信息处理设备提供各种应用服务。图 1 所示的树结构用来向执行各种应用的装置分配内容和密钥。

在存在这些不同信息处理设备（或装置）和应用的一个系统中，允许一组被设置成包含使用相同记录介质的装置 DV0、DV1、DV2 和 DV3。在图 1 所示的树结构中，装置组由虚线包围。例如，假定对于所有装置，内容提供者对将要发送给诸多装置的内容加密，这些装置属于被虚线包围的装置组，所加密的内容被用作这些装置公用的内容。在该情况下，内容提供者还向这些装置发送内容密钥，它作为这些装置公用的密钥由这些装置使用。该系统的其它处理包括从装置到内容提供者、财务结算机构或者其它企业的内容费用的加密支付数据的传送。诸如内容供应者或者财务结算机构的企业执行发送处理，把数据共同地发送给由虚线包围的装置，即 DV0、DV1、DV2、DV3。该企业与形成上述组的装置交换数据。图 1 所示的树结构中存在多个这样的组。与装置交换数据的诸如内容提供者或者财务结算机构的企业充当消息数据分配装置。

需要说明的是，节点密钥和树叶密钥还可以由单一密钥管理中心统一管理。作为选择，密钥还可以由与上述的组交换各种数据的消息数据分配装置以组为单元进行管理。如上所述，消息数据分配装置是诸如内容提供者或者财务结算机构的企业。当密钥之一已经被泄漏时，更新节点密钥和/树叶密钥。更新密钥的处理由密钥管理中心、提供者、财务结算机构或者其它企业完成。

从图 1 中可以明白，在这种数结构中，包含在该组中的 4 个装置，即 DV0、DV1、DV2、DV3 具有公共密钥：节点密钥 K00 和 K0 以及树根密钥 KR。通过向该组中的装置 DV0、DV1、DV2、DV3 分配作为这些装置共有的密钥的这些节点密钥和树根密钥，可以仅向这些装置提供公共内容。

例如，通过设置作为内容密钥的共享节点密钥 K00，可以仅为这些装置设置对装置 DV0、DV1、DV2、DV3 公用的内容密钥，而不发送新密钥。作为选择，可以按以下方式加密新内容密钥 CK：使用节点密钥 K00 产生一个加密密钥 E (E00, CK)，然后经由网络分配给装置 DV0、DV1、DV2、DV3，或者使用记录该加密密钥的记录介质并把该介质供应给这些装置。这样，只有装置 DV0、DV1、DV2、DV3 能够通过使用作为一个公共密钥共享的节点密钥 K00

对加密密钥 $E(K00, CK)$ 解密, 从而产生内容密钥 CK 。

假定在时间 t 发现装置 $DV3$ 拥有的密钥 $K0011$ 、 $K001$ 、 $K00$ 、 $K0$ 、 KR 已经被黑客分析并暴露给黑客。在此情况下, 必须将装置 $DV3$ 与系统分离, 特别是将 $DV3$ 与包括 $DV0$ 、 $DV1$ 、 $DV2$ 、 $DV3$ 的组分离, 以便此后保护与系统交换的数据。

此外, 还必须把密钥 $K001$ 、 $K00$ 、 $K0$ 、 KR 分别更新为密钥 $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$, 并且把密钥 $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ 发送给 $DV0$ 、 $DV1$ 、 $DV2$ 。需要注意的是, 符号 $K(t)aaa$ 是指密钥 $Kaaa$ 的 t 时生成的更新密钥。

显然, 在内容分配中, 在某些情况下, 由于包括版权所有者的愿望和传输到系统的状态等原因, 也可以更新节点密钥和树根密钥 KR 。

因此, 当更新一个密钥时, 必须向拥有更新前密钥的正式装置发送已更新密钥。

下面解释分配已更新密钥的处理。通过使用类似于图 2A 所示的表, 组织和发送已更新的密钥。通过网络将表发送给装置, 或者将表存储在记录介质中然后把该介质供应给装置。该表包括称作 EKB (启动密钥块) 的块数据。例如, 如果装置 $DV3$ 与上述系统分离, 则把 EKB 供应给装置 $DV0$ 、 $DV1$ 、 $DV2$ 。

需要注意的是, EKB 包含作为对类似于图 1 所示的树结构的树叶上某些装置分配的新密钥加密结果而获得的加密密钥。 EKB 还被称作 KRB (密钥更新块)。

图 2A 所示的 EKB 的块数据包括加密的更新节点密钥, 该密钥可以由需要更新节点密钥的装置解密。图 2A 和图 2B 所示的典型 EKB 的每一个是为分配更新节点密钥的目的地建立的, 即为了把 t 时刻生成的更新节点密钥分配给图 1 所示的树结构中装置 $DV0$ 、 $DV1$ 、 $DV2$ 之目的地而建立的。

假定密钥 $K0011$ 、 $K001$ 、 $K00$ 、 $K0$ 、 KR 已经被非法披露给未授权的个人。在此情况下, 装置 $DV0$ 、 $DV1$ 需要更新的密钥 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$, 而装置 $DV2$ 需要更新的密钥 $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ 。

如图 2A 所示, EKB 包括多个多个加密的更新密钥。 EKB 底部的加密的更新密钥是 $E(k0010, k(t)001)$, 它是使用由装置 $DV2$ 拥有的树叶密钥 $K0010$ 加密一个更新密钥 $K(t)001$ 的结果。因此, 装置 $DV2$ 能够通过使用装置本身拥有的树叶密钥解密加密的更新密钥 $E(K0010, K(t)001)$, 从而得到更新

的节点密钥 $K(t)001$ 。

此外,自图 2A 所示的 EKB 底部算起第二行上的加密的更新密钥 $E(K(t)001, K(t)00)$ 可以使用更新节点密钥 $K(t)001$ 解密,以得到更新节点密钥 $K(t)00$ 。接着,自 EKB 顶部算起第二行上的加密的更新密钥 $E(K(t)00, K(t)0)$ 可以使用更新节点密钥 $K(t)00$ 解密,以得到更新节点密钥 $K(t)0$ 。最后, EKB 顶行上的加密的更新密钥 $E(K(t)0, K(t)R)$ 可以使用更新节点密钥 $K(t)0$ 解密,以得到更新树根密钥 $K(t)R$ 。

至于装置 DV0 和 DV1,不更新树叶密钥 $K0000$ 和 $K0001$ 以及节点密钥 $K000$ 。这样,仅需要更新密钥 $(K(t)00, K(t)0$ 和 $K(t)R$ 。

因此,对于装置 DV0 和 DV1 来说,自图 2A 所示的 EKB 顶部算起第三行上的加密的更新密钥 $E(K(t)000, K(t)00)$ 可以使用更新节点密钥 $K(t)000$ 解密,以得到更新节点密钥 $K(t)00$ 。接着,自 EKB 顶部算起第二行上的加密的更新密钥 $E(K(t)00, K(t)0)$ 可以使用更新节点密钥 $K(t)00$ 解密,以得到更新节点密钥 $K(t)0$ 。最后, EKB 顶行上的加密的更新密钥 $E(K(t)0, K(t)R)$ 可以使用更新节点密钥 $K(t)0$ 解密,以得到更新树根密钥 $K(t)R$ 。

如上所述,装置 DV0、DV1、DV2 能够获得更新树根密钥 $K(t)R$ 。需要注意的是,包含在图 2A 所示的 EKB 中的索引的每一个是树叶或者节点密钥的绝对地址,该树叶或者节点密钥被用作解密与索引相同行上的加密密钥的解密密钥。

作为另一个实例,假定图 1 所示的树结构的高分层层上的更新树根密钥 $K(t)R$ 和更新节点密钥 $K(t)0$ 是不需要的,而仅仅需要更新节点密钥 $K00$ 。在此情况下,图 2 所示的 EKB 可以用来吧更新节点密钥 $K(t)00$ 分配给装置 DV0、DV1、DV2。

图 2B 所示的 EKB 通常可以用来向属于一个特定组的装置分配一个共用的新内容密钥。

具体说,属于由图 1 虚线包围的组的装置 DV0、DV1、DV2、DV3 共用一个记录介质并需要一个新共用内容密钥 $CK(t)$ 。在此情况下,图 2B 所示的加密数据 $E(K(t)00, CK(t))$ 和 EKB 被发送给装置 DV0、DV1、DV2、DV3。加密数据 $E(K(t)00, CK(t))$ 是使用更新节点密钥 $K(t)00$ 加密新的共用内容密钥 $CK(t)$ 的一个结果,而更新节点密钥 $K(t)00$ 是更新装置 DV0、DV1、DV2、DV3 共用的节点密钥 $K00$ 的结果。

通过仅仅分配加密的数据 $E(K(t)00, CK(t))$ 和 EKB, 数据将不可能由属于其它组的诸如装置 DV4 的其它装置解密。

装置 DV0、DV1、DV2 以处理图 2A 所述的 EKB 相同的方式处理图 2B 所示的 EKB, 以得到更新节点密钥 $K(t)00$, 该更新节点密钥 $K(t)00$ 用来解密所述加密的数据 $E(K(t)00, CK(t))$, 以便获得 t 时刻生成的新的共用内容密钥 $CK(t)$ 。

如上所述, 组织形成一个树结构的密钥, 并且使用类似于上述的 EKB 更新分配给所述装置的这些密钥。

通过使用这样的密钥组织, 可以因各种原因容易地更新树根密钥 KR 和节点密钥, 并且可以灵活地分配处于正常状态的内容。

图 3 是显示一个 EKB 的典型格式的示意图。节点密钥的数字具有 4 个字节的长度。节点密钥深度也具有 4 个字节的大小。节点密钥深度是充当分配 EKB 的目的地的装置的分层树中分层层数。

EKB 版本还具有 4 个字节的长度。需要注意的是, EKB 版本具有识别最近的 EKB 的功能, 以及具有指示与内容的关系的功能。保留的字段是一个有效区域。

从 16 个字节的区距(offset)开始的字段是存储具有 16 兆字节(Mbyte)长度的 EKB 的实际数据的字段。实际数据是一个加密的节点密钥或者是多个加密的节点密钥。这些加密的节点密钥是先前参考图 2A 和图 2B 解释的加密密钥。

此外, 格式包括加密的 EKB 版本和电子签名。电子签名由发放 EKB 的 EBK 发行机构(办公室)发放。EBK 发行机构的例子是密钥管理中心、内容提供者和财务结算机构。接收 EKB 的装置通过签名的验证核实该发放 EKB 的 EBK 发行机构是有效的。

2、系统配置

下面的说明解释了采用上述的密钥组织的本发明的一个实施例。

图 4 是显示典型系统配置的示意图。第一记录介质设备 1 相当于本发明提供的数据传送设备。另一方面, 第二记录介质设备 20A 相当于本发明提供的数据记录设备。第一记录介质设备 1 和第二记录介质设备 20A 构成数据传送系统。

第一记录介质设备 1 通常由个人计算机实现。为了叙述便利，在下面的解释中，第一记录介质设备是指个人计算机。然而，第一记录介质设备不一定是个人计算机。

5 为了执行本发明提供的数据传送设备的操作，充当第一介质记录设备 1 的个人计算机运行软件，以实行在个人计算机 1 中启动的 SDMI 内容数据的累积和传送。

装入或者从外部加到个人计算机 1 上的 HDD 5 充当第一记录介质（和第一记录介质驱动装置）。需要说明的是，尽管 HDD 5 在该实施例的解释中被用作第一记录介质，但是充当第一记录介质的记录介质不一定是 HDD。第一记录介质可以是各种可以想到的记录介质，比如光盘、磁光盘、装入第一记录介质设备 1 中的半导体存储器以及诸如存储卡的便携式半导体存储器。

15 第一记录介质设备 1 能够经由通信网络 110 与内容服务器 91 通信。诸如音乐的内容数据可以从内容服务器 91 下载到第一记录介质设备 1。当然，可以将多个内容服务器 91 连接到通信网络 110 上。第一记录介质设备 1 的用户可以从任意一个内容服务器 91 接受下载各种数据的服务。

从内容服务器 91 下载到个人计算机 1 的内容数据可以是符合 SDMI 标准的内容数据或者是不符合 SDMI 标准的内容数据。

20 构成通信网络 110 的传输线路是有线或者无线公共通信线路。作为一种选择，构成通信网络 110 的传输线路可以是把个人计算机连接到内容服务器 91 的专用线路。具体说，通信网络 110 可以是互联网、卫星通信网络、光纤网络或者任何其它通信线路。

个人计算机 1 的 HDD 5 可以是装入式或者外部连接式盘驱动器，用于驱动诸如 CD-DA 或者 DVD 的封装式介质，从中再现诸如音乐的内容数据。在下面的说明中，封装式介质 90 还被称作盘 90 或者可移动记录介质 90。

25 个人计算机 1 连接第二记录介质设备 20A 或者 20B，以向它们传送存储在 HDD 5 中的内容数据。第二记录介质设备 20A 或者 20B 是记录设备或者是记录/再现设备，用于把数据记录到第二记录介质上。因而，在复制操作中，可以把从个人计算机 1 接收的内容数据记录到第二记录介质上。

30 存在各种可以想到的第二记录介质设备 20A 或者 20B 的例子。然而在下面的说明中，第二记录介质设备 20B 是符合 SDMI 标准的记录设备。

在符合 SDMI 标准的第二记录介质设备 20B 中，第二记录介质被假定为

符合 SDMI 标准的存储卡。这样的存储卡利用诸如快闪存储器的半导体存储器。因而，第二记录介质设备 20B 是记录/再现设备，用于把数据记录到符合 SDMI 标准的存储卡上或者从该存储卡再现数据。在此情况下，SDMI 内容加密状态存储到第二记录介质上。

- 5 这里建立了一个信息管理格式，包括存储在符合 SDMI 标准的第二记录介质中的内容 ID。该内容 ID 被用作识别 SDMI 内容的标识符。当内容数据被存储在个人计算机 1 的 HDD 5 中时，通过应用存储在 HDD 5 中的内容数据与该内容数据一同生成内容 ID。此外，检出和检入通过使用内容 ID 来管理。假定，当内容数据被记录到符合 SDMI 标准的第二记录介质上时，内容数据的内容 ID 还可以与内容数据一同记录到第二记录介质上。

- 10 另一方面，第二记录介质设备 20A 是不符合 SDMI 标准的数据记录设备。稍后将说明第二记录介质设备 20A。第二记录介质设备 20A 的第二记录介质用来存储处于未加密状态并需要版权保护的 SDMI 内容。这种第二记录介质设备的例子是袖珍盘。该第二记录介质设备 20A 的一个例子是袖珍盘记录/再现设备。在下面的说明中，第二记录介质设备 20A 在某些情况下还被简单地称作记录/再现设备 20A。

在此情况下，为了即使在以未加密状态下存储 SDMI 内容，也不损失版权保护功能，将采用下面将要说明的成功验证，以作为复制 SDMI 内容操作的条件。

- 20 第二记录介质设备 20A 的第二记录介质是已经流行的传统介质。第二记录介质的一个例子是袖珍盘。然而，第二记录介质设备 20A 的第二记录介质不包括存储内容 ID 的区域。为此，采用下面将要说明的用于内容 ID 的特定管理技术。

- 25 需要说明的是，第二记录介质设备 20A 记录数据和再现数据的介质不限于袖珍盘。第二记录介质设备 20A 的其它第二记录介质可能包括：存储卡，利用了诸如快闪存储器的半导体存储器；充当磁光盘的袖珍盘；SD-R（可记录 CD）；CD-RW（可重写 CD）；DVD-RAM；DVD-R；DVD-RW。因而，第二记录介质设备 20A 可以是任何记录设备，只要该记录设备能够把数据记录到这些记录介质的任何一个上。个人计算机 1 通过符合传输标准（比如 USB（通用串行总线）或者 IEEE-1394 标准）的线路连接第二记录介质设备 20A 或者 20B。当然，也可以使用其它类型的传输线路，只要其它传输线路能够传输内容数
- 30

据等。其他传输线路的例子是有线传输线路和无线传输线路。

3、SDMI 内容的数据路径

例如，假定一个系统类似于图 4 所示的系统。在此情况下，SDMI 标准
5 规范的数据路径被显示在图 5 中。

需要注意的是，在个人计算机 1（装备有作为第一记录介质的 HDD）执行的
处理中，音乐内容通过数据路径，以便把音乐内容存储在 HDD5 上，或者
传送内容到诸如第二记录介质设备 20A 或者 20B 的外部设备。换句话说，
通过由个人计算机 1 运行的软件实现数据路径，以执行存储音乐内容到 HDD 5
10 的处理，或者传送内容到外部设备的处理。

图 5 所示的经由数据路径将音乐数据内容存储到 HDD 5 或者传送到外部
设备的过程和处理由参考标记 DP1 至 DP9 表示。在下面的说明中，参考标记
DP1 至 DP9 被用来指示它们各自的处理过程。

在处理过程 DP1 中，依据 SDMI 标准检查图 4 所示的由外部内容服务器
15 91 经由通信网络 110 分配给个人计算机 1 的内容数据，以形成一个该数据
是否为一个需要对其版权保护的内容的判断。外部内容服务器 91 经由通信
网络 110 分配给个人计算机 1 的内容数据被称作网络内容。

外部内容服务器 91 分配给第二记录介质设备 20A 或者 20B 的网络内容
可以是符合 SDMI 标准的内容也可以使不符合 SDMI 标准的内容。符合 SDMI
20 标准的内容和不符合 SDMI 标准的内容分别被称作 SDMI 符合内容和非 SDMI
内容。

在诸如 DES 处理的密钥加密处理中，通过使用内容密钥 CK 加密 SDMI 符
合内容。通常，SDMI 符合内容的加密前数据是使用诸如 ATRAC3 的压缩技术
压缩的编码数据 A3D。在这种情况下，加密的 SDMI 符合内容由参考标记 E(CK,
25 A3D) 表示。

如果分配的网络内容是一个 SDMI 符合内容，则数据路径从处理过程 DP1
连续到处理过程 DP2，在此，网络内容作为 SDMI 内容被存储在充当第一记
录装置的 HDD 5 中。

在此情况下，内容数据实际上以分配的状态 E(CK, A3D) 写入 HDD 5
30 中。作为选择，在使用另一个内容密钥 CK' 再次进行加密以生成将要存储在
HDD5 的加密数据 E(CK', A3D) 之前，内容数据曾经被解密。也就是说，内

容密钥从 CK 变成 CK'。

另一方面，如果分配的网络内容是非 SDMI 内容，则数据路径从处理过程 DP1 连续到处理过程 DP3，其中执行水印检验处理。水印检验处理是基于水印的筛选 (screening) 处理。

5 此外，在处理过程 DP3 中，对盘内容进行水印检验处理，但不执行处理过程 DP1。盘内容是从封装式介质读取的内容，该封装式介质被安装在装入个人计算机 1 内的驱动器上，或者安装在连接个人计算机 1 的盘驱动器上。装入式驱动器的一个例子是 ROM 驱动器。封装式介质的例子包括 CD-DA 和 DVD。

10 也就是说，对于盘内容（它是不符合 SDMI 标准的内容数据）执行水印检验处理。

如果盘内容没有通过水印检验处理，则数据路径从处理过程 DP3 前进到处理过程 DP5，在此确定盘内容是一个在该数据路径中不能进行复制的内容。通过软件的设计，可以实施各种可以想象的具体处理。例如，这样的盘内容
15 被存储到 HDD 5 中，但是不能把它当作为复制或者移动数据到另一个介质的目的而传送的内容数据。作为一个可替换的想象的处理，在符合 SDMI 标准的内容处理中，不把这盘内容存储到 HDD 5 中。

另一方面，如果内容通过水印检验处理，也就是，如果电子水印存在以及指示允许复制操作的复制控制比特被确认，则确定该内容是可以合法复制
20 的内容数据。在此情况下，数据路径连续（前进）到处理过程 DP4，形成该内容是否要根据 SDMI 标准被处理的判断。内容是否按照符合 SDMI 标准的数据来处理取决于软件设计、用户设置等。

如果不依据 SDMI 标准处理内容，则数据路径连续到处理过程 DP6，在此把内容当作一个非 SDMI 内容，并且排斥在符合 SDMI 标准的内容数据路径
25 之外。例如，启动一个把内容送入不遵从 SDMI 标准的记录设备上的传送。

另一方面，如果将内容依据 SDMI 标准来处理，则数据路径从处理过程 DP4 连续到处理过程 DP2，在此将内容数据作为 SDMI 内容加密并存储到 HDD 5 中。具体说，通常以 $E(CK, A3D)$ 或者 $E(CK', A3D)$ 状态将内容数据存储到 HDD 5 中。

30 根据上述的数据路径，SDMI 网络内容或者 SDMI 盘内容被存储到用作第一记录介质的 HDD 5 中。SDMI 网络内容是从通信网络 110 接收的并且将按

照 SDMI 标准处理的内容。另一方面, SDMI 盘内容是从诸如 CD-DA 或者其它介质读出的并且将按照 SDMI 标准处理的内容。

此外, 对于 SDMI 内容, 生成该 SDMI 内容专有的内容 ID, 并且把该内容 ID 与 SDMI 内容一同存储到 HDD 5 中。内容 ID 被用于应用规则的管理方面, 该应用规则为每个 SDMI 内容而运行, 下面将进行说明。

根据预定规则, 存储在 HDD 5 中 SDMI 内容被传送到符合 SDMI 标准的记录/再现设备 20B, 以便可以把内容数据复制到也符合 SDMI 标准的第二记录介质上。如上所述, SDMI 内容可以是 SDMI 网络内容或者是 SDMI 盘内容。此外, 就该实施例而言, 除了符合 SDMI 标准的记录/再现设备 20B 之外, 存储在 HDD 5 中的 SDMI 内容还可以在预定的条件下传送给不符合 SDMI 标准的记录/再现设备 20A。

首先假定, 利用了 HDD 5 的个人计算机被连接到符合 SDMI 标准的记录/再现设备 20B。在此情况下, 存储在 HDD 5 中的 SDMI 内容按下述方式传送给记录/再现设备 20B。

就 SDMI 盘内容而言, 事先确定传送内容的应用规则。在处理过程 DP8 中, 识别用于复制内容到记录/再现设备 20B 的目的、根据应用规则将 SDMI 盘内容送至符合 SDMI 标准的记录/再现设备 20B 的传送。

需要说明的是, 这些数据路径是检出或者操作的路径, 用于把内容从充当第一记录介质的 HDD 5 传送到诸如存储卡的第二记录介质, 以复制由记录/再现设备 20B 或者 20A 再现的内容, 所述的第二记录介质被安装到符合 SDMI 标准的记录/再现设备 20B 或者不符合 SDMI 标准的记录/再现设备 20A 上。与检出相反的操作是检入, 它是把内容从第二记录介质反向传送或者移动到第二记录介质上的操作。值得注意的是, 在内容从第二记录介质反向传送到第一记录介质的移动操作中, 内容数据从第二记录介质中擦除。

作为 SDMI 盘内容的传送的应用规则, 对可容许的检出数强加了一个上限。例如, 容许一条内容检出达到三次。因此, 在检出操作时可以复制内容到多达三个符合 SDMI 标准的第二记录介质上。在检入中, 当内容从第二记录介质反向移动到第一记录介质上时, 将目前为止的内容数据所执行的检出的次数递减 1。因此, 假如内容数据已经在检入中从三个第二记录介质中的一个反向移动到第一记录介质, 即使当内容数据已经被复制到三个符合 SDMI 标准的第二记录介质上, 也可以再次把内容复制到一个符合 SDMI 标准的第

二记录介质上。也就是说，允许内容数据存在于多达三个符合 SDMI 标准的第二记录介质之中。

此外，就 SDMI 网络内容而言，事先确定传送内容的应用规则。在处理过程 DP7 中，识别用于复制内容到记录/再现设备 20B 的目的、根据应用规则将 SDMI 盘内容送至符合 SDMI 标准的记录/再现设备 20B 的传送。

作为 SDMI 网络内容的传送的应用规则，对可容许的检出数强加了一个上限，如同 SDMI 盘内容的情况。该上限可以与为 SDMI 盘内容设置的上限相同或者不同。强加给容许检出的数量的上限为 1 是可能的。在此情况下，每条内容数据仅仅能够复制到一个符合 SDMI 标准的第二记录介质上。如果在检入中，内容从第二记录介质反向移动到第一记录介质上，则内容数据可以被再次复制到符合 SDMI 标准的第二记录介质上。

在检出中，根据这些应用规则从第一记录介质到符合 SDMI 标准的第二记录介质复制的 SDMI 内容，是经由传输线路以加密状态传送的。具体地说，SDMI 内容经由传输线路以 E(CK, A3D) 或者 F(CK', A3D) 状态传送。

然后，由符合 SDMI 标准的记录/再现设备 20B 接收按加密状态传送的 SDMI 内容，以便实际上以加密状态把 SDMI 内容复制到第二记录介质上。

在由符合 SDMI 标准的记录/再现设备 20B 执行对复制和记录到第二记录介质上的 SDMI 内容再现的操作中，从第二记录介质中取出并解密该内容，以便再现所述内容。具体说，通过使用内容密钥 CK 或者 CK' 解密以 E(CK, A3D) 或者 E(CK', A3D) 状态记录到第二记录介质上的内容数据，以分别生成内容 $D\{CK, E(CK, A3D)\} = A3D$ 或者 $D\{CK', E(CK', A3D)\} = A3D$ ，所生成的内容是使用 ATRAC3 压缩技术压缩的原始未加密的内容数据。对原始未加密压缩内容 A3D 进行诸如以下处理：与 ATRAC3 压缩处理相反的解压缩处理，以执行产生诸如音乐的输出声音的解调处理。

如上所述，符合 SDMI 标准的内容数据的版权可以通过以下状态得到恰当保护以及通过复制管理（该复制管理是通过检验为内容传送设置的应用规则执行的）得到恰当保护，这些状态是：沿着到达符合 SDMI 标准的记录/再现设备 20B 的内容数据检出的数据路径的内容数据的加密状态，第二记录介质的中的内容数据的加密状态。

另一方面，如果记录/再现设备 20A 被连接到个人计算机 1，则执行以下处理。

需要注意的是,如上所述,与符合 SDMI 标准的记录/再现设备 20B 不同,记录/再现设备 20A 以未加密状态把内容记录到诸如袖珍盘的第二记录介质上。由于内容以未加密状态记录到袖珍盘上,因此复制到和记录到袖珍盘上的内容数据可以由普通的袖珍盘再现设备来再现,该普通袖珍盘再现设备已经变得很流行,所以可以向用户提供更大的方便。

然而,由于内容以未加密状态被记录到袖珍盘上,因此出现了内容的版权保护方面的问题。为了解决此问题,必须满足把内容数据传送到记录/再现设备 20A 的预定条件。

为了把 SDMI 网络内容传送到记录/再现设备 20A 上,以及为了在复制操作中以未加密状态把内容数据记录到第二记录介质上,复制操作必须满足以下三个传送条件:

(1) 记录/复制设备 20A 应当通过给出 OK 验证结果的验证处理。

(2) 版权所有者应当识别复制操作,即识别把内容数据传送到记录/复制设备 20A 和把数据记录到第二记录介质上的操作。

(3) 内容数据的传送应当遵守为检出和检入所设置的应用规则。

即使上述传送条件(1)、(2)和(3)得到满足,也不能执行无限制地传送内容数据到与符合 SDMI 标准的记录/再现设备 20B 不同的设备上的复制操作。这样,保护版权的功能得到保留。此外,保护版权的功能是由于内容数据以加密状态经由传输线路传送的事实发挥作用的,在内容数据被记录/再现设备 20A 接收并对数据解密之前保护版权功能不起作用。

在处理过程 DP9 中,在 SDMI 网络内容被传送到记录/再现设备 20A 之前,检验上述传送条件(1)、(2)和(3)。

具体地说,记录/再现设备 20A 经历了预定的验证处理。此外,检查包含在内容数据中的标志信息或者类似信息,以确认版权所有者的关于是否允许复制操作的意图。此外,实施检出和检入应用规则。

在上述条件下复制到记录/再现设备 20A 的 SDMI 网络内容经由传输线路实际上以加密状态传送。具体地说,SDMI 网络内容经由通信线路以 E(CK, A3D)或者 E(CK', A3D)状态传送。

加密的 SDMI 网络内容被具有图 7 所示配置的记录/再现设备 20A 接收,然后被解密处理单元 28 解密,以生成通过使用 ATRAC3 压缩技术压缩的原始

数据 A3D。接着，由包含在图 7 所示配置的 EFM/ACIRC 编码器/解码器 24 执行对加密内容数据 A3D 的编码处理，之后把编码数据供应给记录/再现单元 25，用于把数据记录到袖珍盘 100 上。

因此，在再现复制到或者记录到袖珍盘 100 的 SDMI 内容的操作中，记录/再现设备 20A 对于从袖珍盘 100 上读出的数据需要执行与普通袖珍盘系统相同的解码处理。解码处理包括：EFM 解调处理，ACIRC 纠错处理，和采用与 ATRAC 压缩技术对应的解压缩技术的解压缩处理。

这意味着，当袖珍盘 100 被安装到普通的袖珍盘再现设备上时，该设备可以正常地再现被记录到袖珍盘 100 上的被复制内容数据。也就是说，借助于不符合 SDIM 标准的普通袖珍盘再现设备通过内容再现，用户可以欣赏复制到和记录到袖珍盘 100 上的 SDMI 网络内容。

需要注意的是，如果根据图 5 所示数据路径内的处理过程 DP7、DP8、DP9 的检验应用规则的结果，不允许内容传送时，内容必定不能传送到记录/再现设备 20A 或者 20B。

15

4、数据传送设备的典型配置（第一记录介质设备或者 PC）

图 6 是显示充当数据传送设备的第一记录介质设备 1 的配置的方框图。以下说明解释用作第一记录介质设备 1 的个人计算机。然而，通过建立专用软件与执行和第一记录介质设备 1 相同的功能的配置，还能够建立一个专用于数据传送的设备。

20

在该实施例中，为执行数据传送设备的功能而运行的软件程序被安装到个人计算机 1 上，以把第一记录介质设备实施为数据传送设备。需要注意的是，在该说明中，个人计算机或者计算机具有所谓的通用计算机的广义。

软件程序可以被事先存储到装入计算机中的记录介质中。装入式记录介质的例子是硬盘驱动器（HDD）5 和 ROM3。

25

作为选择，软件程序可以被临时或者永久存储在可移动记录介质 90 中，比如存入软盘、CD-ROM（致密盘只读存储器）、MO（磁光）盘、DVD（数字通用盘）、磁盘和半导体存储器。存储在可移动记录介质 90 中的程序被以作为所谓的封装式软件包呈递给用户。

需要注意的是，除了把程序从可移动式记录介质 90 安装到计算机之外，还可以通过利用无线通信进行数字卫星广播的人造卫星或者通过利用有线通

30

信的诸如 LAN（局域网）或者互联网的网络将程序从下载站点下载到计算机中。在该计算机中，由安装在装入式 HDD 5 内的通信单元 8 接收下载的程序。

图 6 所示的计算机 1 包括装入式 CPU（中央处理单元）2。CPU 2 通过总线 2 连接到输入/输出接口 10。根据用户操作诸如键盘、鼠标或者麦克风的输入单元 7 经由输入/输出接口 10 键入 CPU 2 的命令，CPU 2 运行事先存储在 ROM（只读存储器）3 中的程序。作为选择，CPU 2 把程序从 HDD 5 装载到用于运行的 RAM（随机存取存储器）4 中。首先，把程序存储到 HDD 5 中，该程序由通信单元 8 从卫星或者网络接收并安装到 HDD 5 中，或者从移动式记录介质 90（比如，装在驱动器 9 上的光盘）中读出并安装到 HDD 5 中。

10 通过运行这种程序，CPU 2 执行用于 SDMI 内容的数据传送设备的处理。

例如，CPU 2 经由输入/输出接口 10 向输出单元 6 或者通信单元 8 输出处理结果，或者按照需要把该结果记录到 HDD 5 中。

在此情况下，通信单元 8 能够通过图 4 所示的通信网络 110 与各种服务器通信。具体说，计算机 1 能够从外部内容服务器 91 下载诸如音乐内容的网络内容。下载的网络内容沿着上述的数据路径经历符合 SDMI 标准的内容处理或者经历不符合 SDMI 标准的处理。完成符合 SDMI 标准的内容处理的下载网络内容至少作为 SDMI 内容被存储到 HDD 5 中。存储在 HDD 5 中的 SDMI 内容是将要传送到符合 SDMI 标准的记录/再现设备 20B 或者传送到通过了验证检验的记录/再现设备 20A 的内容。

15

20 连接单元 11 是在记录/再现设备 20A 与记录/再现设备 20B 之间连接的部件，所以可以在第一记录设备 1 与记录/再现设备 20A 或者记录/再现设备 20B 之间通信数据。连接单元 11 的可能的例子是 USB 接口和 IEEE-1394 接口。当然，符合其它标准的有线接口和使用红外线或者（电）波的无线接口也可以用作通信单元 11。

25 需要注意的是，实施上述结合图 5 所述数据路径的各种处理不一定是沿着时间轴的顺序处理，而是实施数据路径的处理可以包括同时或者分别执行诸多段处理（同时或者分别执行的处理的例子是同时处理和面向对象的处理）。

程序可以由单个计算机或者分布处理中的多个计算机执行。此外，程序
30 可以被传送到运行的远程计算机。

5、数据记录设备的典型配置（第二记录介质设备或者记录/再现设备）

图 7 是显示记录/再现设备 20A 的典型配置的方框图。

在此情况下，记录/再现设备 20A 例如由一个袖珍盘记录器配置。第二记录介质 100 是袖珍盘（或者是磁光盘）。第二记录介质 100 还被称之为袖珍盘 100。

需要注意的是，图 7 显示了记录/再现设备 20A 的配置，它仅仅包括一个处理将要记录到用作第二记录介质 100 的袖珍盘的数据或者从该袖珍盘再现的数据的系统，以及一个处理从第一记录介质设备 1 传送的数据的系统。由于诸如驱动系统、伺服系统和再现系统的其他系统类似于普通袖珍盘记录/再现设备中使用的它们的各自对应物，因此省略了它们的图示。

在记录/再现设备 20A 中，MD 控制单元（CPU）21 用作控制记录数据到袖珍盘 100 和从该袖珍盘 100 再现数据的操作的控制器。具体地说，MD 控制单元 21 分别控制旋转驱动机构、芯轴伺服、聚焦伺服、跟踪伺服、线程伺服、把激光束和磁场分别施加到光头和磁头的操作，并且控制对待记录的数据编码和对再现的数据解码的处理。

记录/再现单元 25 包括光学头、磁头、盘旋转系统和伺服系统。在实际情况下，记录/再现单元 25 充当记录到袖珍盘 100 和从袖珍盘 100 再现数据的部件。

EFM/ACIRC 编码器/解码器 24 对将要记录到袖珍盘 100 上的数据编码以及对从袖珍盘 100 再现的数据解码。正如通常知道的那样，对于袖珍盘系统，将要记录的数据经历 ACIRC 纠错码的编码处理和 EFM 调制处理。在把数据施加到记录/再现单元 25 之前，EFM/ACIRC 编码器/解码器 24 对将要记录的数据执行 ACIRC 编码处理和 EFM 编码处理。

在再现操作中，EFM/ACIRC 编码器/解码器 24 对于由记录/再现单元 25 从袖珍盘 100 读出并供应到 EFM/ACIRC 编码器/加码器 24 上的数据执行解码处理。解码处理包括二进制转换处理、EFM 解调处理和采用 ACIRC 技术的纠错处理。

缓冲存储器 30 缓存将要记录到袖珍盘 100 的数据和从袖珍盘 100 再现的数据。也就是说，缓冲存储器 30 具有通称为抗冲击功能的缓冲功能。

在记录数据的操作中，使用 ATRAC/ATRAC3 技术压缩和编码的数据被暂时存储在缓存器 30 中。然后，从缓存器 30 中以预定数据单元断续地读出数

据并供应给 EFM/ACIRC 编码器/解码器 24, 以便记录到袖珍盘 100 上。

在重放数据的操作中, 从袖珍盘 100 中读出数据, 并由 EFM/ACIRC 编码器/解码器 24 解码该数据。解码的数据被暂时存储到缓存器 30 中。然后, 从缓存器 30 中连续读出所存储的数据并供应给编解码器 23, 用于执行解压缩/解码处理。

编解码器 23 是分别基于采用 ATRAC/ATRAC3 技术的编码和解码处理执行压缩处理和解压缩处理的部件。

将要记录到修袖珍盘 100 上的数据在经历编码处理之前使用 ATRAC/ATRAC3 技术进行压缩。因此, 当记录/再现设备 20A 接收例如未完成压缩和编码的数据、PCM 音频数据时, 编解码器 23 采用 ATRAC/ATRAC3 技术对将要记录的数据执行压缩和编码处理, 并且把压缩的数据供应给 EFM/ACIRC 编码器/解码器 24。

在再现操作中由记录/再现单元 25 从袖珍盘 100 读出并由 EFM/ACIRC 编码器/解码器 24 解码的数据是处于采用 ATRAC/ATRAC3 技术进行压缩和解码状态下的数据。数据通过缓存器 30 供应给编解码器 23。编解码器 23 使用对应于 ATRAC/ATRAC3 技术的解压缩技术对数据解压缩, 以生成具有 44.1KHz 频率的 16 比特量化数字音频数据。数字音频数据在图中未示出的输出电路中经历包括 A/D 转换处理、模拟信号处理和放大处理的处理, 以生成代表再现的音乐或者类似物的扬声器输出信号。

作为选择, 再现信号作为数字音频数据被输出给另一个设备。

上述的配置包括普通袖珍盘系统的记录/再现设备的诸多部件。然而, 该实施例所实施的记录/再现设备 20A 具有在个人计算机中使用的充当第一节录介质设备 1 的附加部件。具体地说, 用于执行诸如接收传送的内容数据以及解码该数据地处理的部件包括: 通信单元 26、DMA 27、解密处理单元 28、高速缓冲存储器 29、流控制单元 31 和系统控制单元 32。

系统控制单元 32 (CPU) 是控制整个记录/再现设备 20A 的部件。

通常, 系统控制单元 32 控制诸如以下处理: 发出数据生成的请求和在个人计算机 1 与记录/再现设备 20A 之间进行验证通信的处理; 与个人计算机 1 进行各种命令交换的处理; 对从个人计算机 1 接收的内容数据进行的处理。此外, 根据各种控制, 把命令给予 MD 控制单元 21, 并且控制记录内容数据到袖珍盘 100 和从袖珍盘再现内容数据的操作以及读出和更新管理信息

的操作。

操作单元和显示单元（图中未示出）被提供为用户接口。系统控制单元 32 控制监视由用户在操作单元所执行的操作的处理、根据该操作所执行的处理和显示单元的显示处理。

5 与图 6 所示的个人计算机 1 的连接单元 11 相连，通信单元 26 是与个人计算机 1 交换数据的部件。通信单元 26 按照如 USB 或者 IEEE-1394 技术的通信技术处理信号。

通信单元 26 从个人计算机 1 接收的数据包括各种命令和 SDMI 内容。

10 通信单元 26 接收的 SDMI 内容通过 DMA（直接存储器存取）27 执行的控制，被存储到高速缓冲存储器中。需要注意的是，当然可以在由替代 DMA27 的 CPU 执行的控制下，将这样的内容存储在高速缓冲存储器 29 中。

解密处理单元 28 是执行与加密 SDMI 内容的处理相反的处理的部件。也就是说，解密处理单元 28 对存储在高速缓冲存储器 29 中的内容数据解密。然后把未加密的内容数据存储在高速缓冲存储器 29 的另一个区域。

15 由于 SDMI 已经通过使用内容密钥 CK 或者 CK'加密，因此存储可用来至少识别内容密钥 CK 或者 CK'的信息。如下面将要具体说明的那样，存储结合图 1 所解释的 DNK（装置节点密钥）。记录/再现单元 25 相当于图 1 所示的装置（DVx）。存储在 DVx 中的 DNK 包括一个树叶密钥以及多个节点密钥和一个树根密钥（通过使用树叶密钥已经被加密）。内容密钥可以通过使用这种
20 DNK 或者在某些情况下使用上述的被接收的 EKB 来识别。

因此，DNK 是可以用来识别用于 SDMI 内容的内容密钥 CK 的信息。通过使用内容密钥 CK，解密处理单元 28 能够对加密状态下接收的加密的 SDMI 内容进行解密。例如，加密的 SDMI 内容是 $E(CK, A3D)$ 。解密的结果是 $D\{CK, E(CK, A3D)\} = A3D$ ，它是被解密的使用 ATRAC3 技术压缩的数据。使用 ATRAC3
25 技术压缩的被解密的数据由 EFM/ACIRC 编码器/解码器 24 编码，然后由记录/再现单元 25 存储到袖珍盘 100 中。

需要注意的是，SDMI 内容不总是使用 ATRAC3 技术压缩的数据。例如，由内容密钥加密的线性 PCM 数据是可能的。因此，还存在一种以 $E(CK, PCM)$ 输入所传送的内容的方法。在此情况下，解密处理单元以 $E(CK, PCM)$ 解密
30 所加密的内容，以生成 $D\{CK, E(CK, PCM)\} = PCM$ ，它是一种解密的线性 PCM 数据。在此情况下，PCM 数据由编解码器 23 使用 ATRAC3 技术来压缩，然后

由 EFM/ACTRC 编码器/解码器 24 进行编码, 并通过记录/再现单元 25 记录到袖珍盘 100 上。

5 密钥可以被存储在加密处理单元 28 中, 以在某些情况下用于验证处理。在下面将要说明的典型验证处理中, 记录/再现设备 20A 使用被存储的公共密钥 P 和被存储的保密密钥 S。在此情况下, 公共密钥 P 和保密密钥 S 都被存储在解密处理单元 28 中。保密密钥 S 还用于加密处理。

此外, 解密处理单元 28 包括装入式散列引擎, 用于执行所谓的散列函数处理, 以便生成内容 ID。

需要注意的是, 内容 ID 的生成将稍后说明。

10 被解密的加密 SDMI 内容, 比如通过 ATRAC3 技术压缩的数据, 或者 PCM 数据从高速缓冲存储器 29 传送到流控制单元 31。

流控制单元 31 是把被解密的加密 SDMI 内容传送到 MD 控制单元 21 的部件, 该 MD 控制单元充当将数据记录到袖珍盘 100 上的记录处理系统 (该记录处理系统包括编解码器 23、EFM/ACIRC 编码器/解码器 24、记录/再现单元 25 和缓存器 30)。

流控制单元 31 根据 MD 控制单元 21 做出的请求 (XARQ), 传送被解密地加密 SDMI 内容。该流控制单元 31 判断内容数据的接收、解密处理和记录数据到袖珍盘 100 上的处理的定时。

20 总线 22 是允许各种数据在 MD 控制单元 (CPU) 21、编解码器 23、缓冲存储器 30、EFM/ACIRC 编码器/解码器 24、流控制单元 31、DMA 27、高速缓冲存储器 29、通信单元 26、解密处理单元 28 和系统控制单元 32 之中交换数据的通信线路。

25 在上述配置中, 作为由个人计算机 1 传送的 SDMI 内容数据, EFM/ACIRC 编码器/解码器 24 利用 ATRAC3 压缩技术解密和编码 E(CK, A3D) 状态的数据或者 E(CK, PCM) 状态的数据, 然后由记录/再现单元 25 把解密的数据记录到袖珍盘 100 中。

顺便指出, 在个人计算机 1 与记录/再现设备 20A 之间和其它通信会话中的内容数据的检入和检出中, 还传送各种命令。

30 这些命令由通信单元 26 接收并且被转送到系统控制单元 32。系统控制单元 32 根据这些命令执行各种处理, 并且把对这些命令的响应从通信单元 26 发送到个人计算机 1 上。

6、袖珍盘的管理技术

下面的说明解释将要记录到袖珍盘 100 的数据和管理信息。

- 5 在诸如袖珍盘系统的数字记录/再现系统中，TOC（内容表）被记录到记录介质上，以作为管理信息，用于控制记录数据到诸如一个盘的介质和从该介质再现数据的操作。记录/再现设备从记录介质读出 TOC 信息并且预先将该信息保存在存储器中。在记录和再现操作中，查阅该 TOC 信息以获得写或者读位置，以便允许用于要执行的记录或者再现操作的存取操作。

- 10 对于袖珍盘，TOC 信息包括 P-TOC（预先原版录制（pre-mastered）的 TOC）和 U-TOC（用户 POC）。P-TOC 是按凹点记录的不可改变的信息。U-TOC 是采用磁光技术记录的信息。U-TOC 伴随着诸如记录和删除音乐内容处理的操作而改变。具体地说，当音乐数据被记录或者被删除时，首先更新存储在存储器中的 U-TOC，然后在一个预定定时将其存储在光盘的 U-TOP 区域中。

- 15 需要注意的是，通过使用 U-TOC，以每个被称作一条轨道的诸多单元来管理内容数据，比如记录到光盘上的音频数据。通常 1 条轨道相当于一段音乐。

首先，把被称作簇的数据单元解释为存储在袖珍盘 100 中数据。在袖珍盘系统中，作为被记录的数据，创建用于称作簇的每个单元的数据流。用作记录操作的单元的簇的格式在图 8 中示出。

- 20 袖珍盘系统中的被记录的轨道是图 8 所示的簇 CL 的连续序列。簇是记录操作中使用的最小单元。

一簇包括三个扇区链接的扇区 SCFC 至 SCFE、副数据扇区 SCFF 和 32 个主扇区 SC00 至 SC1F。因此，一簇包括总共 36 个扇区。

一个扇区是具有 2352 字节长度的数据单元。

- 25 扇区链接扇区 SCFC 至 SCFE 被用作缓冲区域、两个连续记录操作之间的停顿区域，和用于各种操作的调整区域。副数据扇区 SCFF 被用来记录被设置为副数据的信息。

32 个主扇区 SC00 至 SC1F 被用来记录各类数据，比如 TOC 数据和音频数据。

- 30 一个扇区还被细分为称作声音组的单元。具体说，两个扇区被分成 11 各声音组。

也就是说, 如图所示, 两个连续扇区, 即一个偶数扇区 (比如扇区 SC00) 和一个奇数扇区 (比如扇区 SC01) 包括声音组 SG00 至 SG0A。每个声音组具有 424 字节的大小, 用于存储具有相当于 11.61msec 的量的音频数据。

数据以一个声音组 SG 记录, 被分成 L 和 R 声道, 例如, 被记录在声音组 SG00 中的数据包括数据 L0 和数据 R0。另一方面, 记录在声音组 SG01 中的数据包括用于 L 声道的数据 L1 以及 R 声道的 R1。

需要注意的是, 用做 L 或者 R 声道的数据区的 212 字节被称之为一个声音帧。

图 9 是显示袖珍盘 100 的区域结构示意图。

具体说, 图 9 (a) 是一个显示从盘最内圆周侧延伸到盘最外圆周侧的区域的示意图。用做磁光盘的袖珍盘 100 的最内圆周侧上具有凹点区域。该凹点区域是只再现区域, 用来建立如凸点 (emboss) 的数据。在该凹点区域中, 记录 P-TOP。

凹点区域的外侧的圆周是磁光记录/再现区域。在该区域中, 建立如记录轨道的引导槽的凹槽。

磁光区域的最内圆周侧上从簇 0 到簇 49 的区段被用作管理区域。簇 50 到簇 2251 是程序区域, 用来按照轨道存储每段音乐数据。程序区域外侧上的区域被用作读出区域。

另一方面, 图 9 (b) 是显示管理区域细节的示意图。在管理区域中, 水平线条代表扇区, 垂直排列的诸多线条的每一个代表一簇。

在管理区域中, 簇 0 和 1 用作具有凹点区域的缓冲区域。簇 2 被用作调整激光束输出功率的功率定标区域 (PCA)。

簇 3、4、5 用来记录 U-TOC, 其内容将在下面进行详细说明。一簇中的 32 个主扇区 (SC00 至 SC1F) 的每一个中规定了数据格式, 管理信息被包含在每个扇区中。也就是说, 规定 U-TOP 的扇区, 使记录在程序区域中的每个轨道的地址和自由区域的地址以及诸如每个轨道的名称和记录时间可以被记录到 U-TOC 中。三个相同的簇 3、4 和 5 (每一个包含用作 U-TOC 扇区的诸多扇区) 被连续记录。

簇 47、48、49 是具有程序区域的缓冲区域。

需要注意的是, 阴影部分 PD 是设置稍后将要说明的预付信息的区域。

在簇 50 开始的程序区域 (或者, 如果以十六进制格式表示, 则为簇 32h)

中，每个簇中的 32 个主扇区（SC00 至 SC1F）用来以称为 ATRAC 格式的压缩格式存储诸如音乐的音频数据。通过使用 U-TOC 管理每个记录轨道（或者内容数据）以及自由区域。需要注意，程序区域中每簇的扇区 SCFF 可以用来记录用作副数据的信息（如前面所说明）。

5 下面结合图 10 解释 U-TOC 的扇区。

需要注意的是，如上文结合图 9 所解释的那样，P-TOC 是在盘 90 的最内圆周侧上的凹点区域中建立的只读信息。P-TOC 被用来管理区域的位置，这些区域比如是：盘的可记录区域（可记录用户区域），导出区域和 U-TOC 区域。值得注意的是，在以凹点形式记录所有数据的只再现光盘中，P-TOC
10 还可以用来管理以类似 ROM 的方式记录的诸多首音乐。在此方式中，不建立 U-TOC。这里不对 P-TOC 进行详细说明。

图 10 是显示 U-TOC 扇区 0 的格式的示范性视图。

扇区 0 至 32 可以用作 U-TOC 扇区。在上述的簇中，U-TOC 扇区是主扇区 SC00 至 SC1F。

15 U-TOC 扇区 0 是记录管理信息的数据区域，该管理信息管理自由区域，在该自由区域中记录内容数据（或者轨道）如所记录的多段音乐和新内容数据。

例如，在把一段音乐记录到袖珍盘 100 的操作中，MD 控制单元 21 搜索 U-TOC 扇区 0 寻找盘上的自由区域，并且把多段音乐写入该区域。另一方面，
20 在再现操作中，MD 控制单元 21 搜索 U-TOC 扇区 0 以寻找记录要被再现的一段音乐的区域，并且访问该区域以读出该段音乐。

在图 10 所示的 U-TOC 扇区 0 的数据区域（2352 字节 = 4 字节 × 588）的起始位置上，把多条 1 字节数据的字符串记录为一个同步码（synchronization pattern）。每条 1 字节数据包括所有 0 或者所有 1 的字符串。
25

同步码的后面是具有 3 字节长度的地址。第一个 2 字节（即簇 H 和簇 L）是簇地址，以及第三字节是扇区地址（扇区）。该 3 个字节的后面是一个存取用于模式的字节（MODE）。同步码和 4 个字节构成报头（header）。3 字节地址是扇区本身的地址。

30 需要注意的是，包括同步码和地址的报头配置不仅适用于 U-TOC 扇区 0，而且还适用于 P-TOC 扇区和程序区域中的诸多扇区。扇区本身的地址和同步

码被记录在每个扇区的报头中。

预定的下列字节位置被用来记录数据，比如厂商识别码、模型码、第一轨道号（第一 TNO）、最后轨道号（最后 TNO）、所使用的扇区的情况（所使用的扇区）、盘序列号和盘 ID。

- 5 跟随盘 ID 的区域是指针部分，用于存储各种指针（即，P-DFA、P-EMPTY、P-FRA 以及 P-TN01 至 P-TN0255）。这些指针的每个指向后面将要说明的表中的部分描述符。部分描述符是存储由用户记录的轨道（音乐和类似物）的区域的部分描述符，或者是自由区域的部分描述符。

- 10 关联指针（P-DFA 至 P-TN0255）的表是包括 255 个部分描述符（01h 至 FFh）的 255 部分描述符表。部分描述符包括部分的起始地址、该部分的结尾地址和该部分的模式（轨道模式）。如果一个特定部分被延续到另一个部分，则特定部分的部分描述符还包括指示其它部分的部分描述符的链接。同样的原因，其它部分的部分描述符包括其它部分的起始地址、其它部分的结尾地址和其它部分的模式。

- 15 需要注意的是，轨道是记录数据的轨道中的部分，它以物理上连续的状态沿着时间轴连续。

起始和结尾地址是组成一段音乐（或者轨道）的一部分或者多个部分中的每个部分的起始和结尾地址。

这些地址的每个以缩短形式记录，指示簇、扇区或者声音组的位置。

- 20 即使一段音乐（轨道）的数据以物理上连续方式来记录，即被记录在多个部分上，该类型的记录/再现设备也能够通过顺序地（一部分接一部分地）访问这些部分再现一段音乐，而不会产生再现问题。因此，数据如一段被用户记录的音乐通过分离多个部分来存储，以用于高效率使用可记录区域的目的。

- 25 由于上述原因，一个部分描述符包括一个链接。如上所述，如果一个特定部分被连续到另一个部分，则特定部分的部分描述符还包括指示另一个部分的部分描述符。指示部分描述符的链接是分配给其它部分的部分描述符的数字（范围是 01h 到 FFh）。

也就是说，在 U-TOC 扇区 0 的表部分中，每个部分描述符描述一个部分。

- 30 例如，如果一段音乐被记录在三个部分上，则第一部分的部分描述符包括一个到第二部分的部分描述符的链接，第二部分的部分描述符包括一个到第三

部分的部分描述符的链接。这样就管理了各部分的位置。

需要说明的是,通过一个链接指向的一个部分描述符的实际字节位置(在 U-TOC 扇区 0 中)由下列等式用数字表示:

实际位置 = 304 + 链接 × 8 (= 按字节表示的部分描述符的长度)。

- 5 在 U-TOC 扇区 0 (具有范围 01h 到 FFh 中的号码) 中由表部分的部分描述符所描述的一个部分的内容通过以下方式确定: 诸多指针 (P-DFA、P-EMPTY、P-FRA 和 P-TN01 到 P-TN0255) 中的哪一个指针与该部分描述符相关联 (下面将说明)。

- 10 指针 P-DFA 查阅磁光盘 90 上的缺陷区域。也就是, 指针 P-DFA 指向描述因损坏或类似情况造成的缺陷区域 (或者缺陷轨道部分) 的一个部分描述符, 或者指向多个部分描述符的第一描述符, 该第一描述符描述这样一个缺陷区域或者这样一个缺陷轨道部分。具体说, 指针 P-DFA 具有范围 01h 至 FFh 的值。该值是分配给包括缺陷部分的起始和结尾地址的部分描述符的一个数字。如果另一个缺陷部分存在, 部分描述符包括对另一个描述其它缺陷部分
- 15 的部分描述符的链接。如果不存在更多的缺陷部分, 其它部分描述符中的链接被设置在指向没有部分描述符的 00h 上。

- 20 指针 P-EMPTY 指向未用的部分描述符或者多个未用的部分描述符的第一个。具体地说, 指针 P-EMPTY 具有在范围 01h 至 FFh 内的一个数值。该数值是分配给未用部分描述符或者多个未用部分描述符的第一描述符的一个数字。

如果多个未用部分描述符存在, 由指针 P-EMPTY 指向的第一个部分描述符包括一个指向第二部分描述符的链接, 该第二部分描述符包括一个指向第三部分描述符的链接, 等等。这样, 就把所有的未用部分描述符放入一个链接列表上。

- 25 指针 P-FRA 查阅磁光盘 90 上的自由区域。自由区域是一个可以记录数据的区域 (包括删除数据的区域)。也就是说, 指针 P-FRA 指针指向一个描述一个自由区域 (或者一个自由轨道部分) 部分描述符, 或者指向描述这样一个自由区域或者这样一个自由轨道部分的多个部分描述符的第一部分描述符。具体说, 指针 P-FRA 具有一个范围 01h 到 FFh 内的数值。该数值是一个
- 30 分配给包括自由区域的起始和结尾地址的一个部分描述符的数字。如果存在另一个自由区域, 则部分描述符包括一个对另一个部分描述符 (描述其它自

由区域) 的链接。如果不存在更多的自由区域, 则其它部分描述符中的链接被设置在指向没有部分描述符的 00h 上。

图 11 是显示多个部分的管理的模型的示范性示意图, 所述的多个部分的每个可作为自由区域利用。假定具有编号 03h、18h、1Fh、2Bh 和 E3h 的部分描述符的每一个被指定为描述自由区域的部分描述符。在此情况下, 在指向第一部分描述符的 03h 上设置指针 P-FRA。在指向第二描述符的 18h 上设置第一部分描述符中的链接, 而在指向第三描述符的 1Fh 上设置第二部分描述符中的链接, 等等。最后, 第五部分描述符中的链接被设置在指向没有部分描述符的 00h 上。需要注意的是, 可以以相同的方式管理缺陷区域和未用部分描述符。

指针 P-TN01 至 P-TN255 的每一个查阅磁光盘 90 上的轨道, 比如用户记录的一段音乐。例如, 指针 P-TN01 指向描述第一轨道的部分描述符, 或者指向多个部分描述符之一, 所述多个部分描述符描述时间轴上的第一轨道的引导部分。

例如, 假定第一轨道是一段未在盘上划分成多个部分的音乐, 也就是该轨道是按照单一部分记录的。在此情况下, 指针 P-TN01 被设置在指向一个部分描述符的编号位置上, 所述的部分描述符描述记录第一轨道的一个区域的起始和结尾地址。

作为另一个实施例, 假定第二轨道是一段在盘上划分成多个部分的音乐, 也就是该轨道被记录为多个分离部分。在此情况下, 指针 P-TN02 被设置在指向多个部分描述符的第一部分描述符的编号位置上, 其中每个描述符描述记录第二轨道的诸多部分之一的区域的起始和结尾地址。部分描述符以各部分的时间顺序被置入上述的链接列表上。具体地说, 指针 P-TN02 被设置在指向第一部分描述符的编号位置上, 该描述符描述时间轴上的第一部分。第一部分描述符中的链接被设置在指向描述时间轴上第二部分的第二描述符的编号位置上, 而第二部分描述符中的链接被设置在描述时间轴上第三部分的第三描述符的编号位置上, 等等。最后, 最后部分描述符中的链接被设置在指向没有部分描述符的 00h 位置上。结果部分描述符被置入到一个链接列表上 (与图 11 所示的相类似)。

如上所述, 第二段音乐的数据被记录在按诸多部分的时间顺序排列的部分描述符所描述的诸多部分上。在使用 U-TOC 扇区 0 的数据再现第二段音乐

的一个操作中，设置在指针 P-TN02 中的编号被用来访问包括第一部分的起始地址的第一部分描述符。然后把记录/再现头引到起始地址。在完成读取第一部分数据的操作之后，第一部分描述符中的链接用来访问包括第二部分的起始地址的第二部分描述符。然后把记录/再现头引到起始地址，等等。

- 5 这样，可以从离散部分读出连续的音乐数据。此外，通过高效率地使用记录区域，能够执行记录操作。

顺便指出，具有 1 字节大小的轨道模式也可以被记录到每个部分描述符中。该轨道模式描述了由部分描述符描述的轨道的属性。

- 10 假设 d1 (MSB) 至 d8 (LSB) 为组成轨道模式字节的 8 个比特。在此情况下，轨道模式被定义如下：

- d1...0: 写允许; 1: 写保护 (禁止改写和编辑)。
- d2...0: 版权存在; 1: 版权不存在。
- d3...0: 原始; 1: 第一或者较新的一代 (generation)。
- d4...0: 音频数据; 1: 未定义。
- 15 d5 和 d6...01: 标准音频; 其它: 未定义。
- d7...0: 单声道; 1: 立体声。
- d8...0: 加重关; 1: 加重开。

- 20 图 12 是显示 U-TOC 扇区 1 的格式的示范性视图。U-TOC 扇区 1 是存储字符的数据区域，该字符描述了由 U-TOC 扇区 0 管理的每个轨道的名称和盘本身的名称。

- 25 U-TOC 扇区 1 的指针部分包括与记录的轨道关联的指针 P-TNA1 至 P-TNA255。指针 P-TNA1 至 P-TNA255 的每一个指向槽隙 (slot) 部分中的 8 字节槽隙。因而，槽隙部分包括 255 个槽隙 01h 至 FFh。此外，该槽隙部分还包括也具有 8 字节长度的槽隙 99h。U-TOC 扇区 1 用来以和上述 U-TOC 扇区 0 的相同方式管理字符数据。

槽隙 01h 至 FFh 的每一个用来记录盘标题和轨道名称，作为以 ASCII 码写入的字符信息。

- 30 例如，由指针 P-TNA1 指向的槽隙被用来记录用于第一轨道的由用户键入的字符串。此外，槽隙可以包括指向另一个槽隙的链接。因此，如果用于一个轨道的由用户键入的字符串超过 7 个字节 (或者七个字符)，则通过这样的链接把字符串存储到多个彼此链接槽隙上。

需要注意的是,槽隙 00h 的 8 个字节被用作记录盘名称的一个特定区域。在指针 P-TNA(x) 一个也没有的情况下,指向该槽隙。

U-TOC 扇区 1 的指针 P-EMPTY 还被用来管理未用的槽隙。

值得注意的是,非常类似于 U-TOC 扇区 1, U-TOC 扇区 4 也被用作存储由用户键入的字符信息的数据区域。字符信息可以是分配给一段由用户记录的音乐的名称或者是盘标题。由于 U-TOC 扇区 4 具有类似于 U-TOC 扇区 1 的格式,因此 U-TOC 扇区 4 未在图中示出。

然而, U-TOC 扇区 4 被用来存储日本汉字字符或者欧洲字符的代码数据。因此, U-TOC 扇区 4 包括字符代码的属性以及图 12 所示的 U-TOC 扇区 1 中存储的数据。该属性被记录在预定字节位置上。

记录在 U-TOC 扇区 4 中的字符信息通过使用字符槽隙指示数据部分以与 U-TOC 扇区 1 的相同方式来进行管理。该字符槽隙指示数据部分包括槽隙指针 P-TNA1 至 P-TNA255 以及由该槽隙指针 P-TNA1 至 P-TNA255 指向的 255 个槽隙 01h 至 FFh。

U-TOC 扇区 2 被用作数据区域,主要存储由用户记录的每段音乐的记录日期。图中省略了 U-TOC 扇区 2 的示意或者细节。

如上所述,对于可重写的磁光盘 90,使用 P-TOC 管理盘的各个区域。另一方面,使用 9-TOC 扇区 0 管理其它区域,比如存储各段音乐的可记录用户区域和自由区域。

通过提供具有这种配置的 U-TOC 扇区 0 可以清楚的看到,对于袖珍盘 100 上记录的诸多轨道,可以仅仅通过更新 U-TOC 扇区 0 执行以下处理:把一个轨道分成多个部分,把一个部分链接到另一个部分,包括删除的轨道编辑。

此外,通过提供 U-TOC 扇区 1 和 4,能够执行对代表盘标题的字符串和编辑代表每个轨道名称的字符串编目录的编辑操作。

在记录/再现设备 20A 中,当袖珍盘 100 被装在记录/再现单元 25 上时,首先,MD 控制单元 21 从袖珍盘 100 中读出 TOC 信息,然后把该信息存储到缓存器 30 的指定区域中。此后,在袖珍盘 100 上执行记录、再现和编辑操作过程中查阅缓存器 30 中 TOC 信息。

需要注意的是,在把内容数据(或者轨道)记录到袖珍盘 100 和编辑袖珍盘 100 上已经记录的轨道的操作中,通过更新已经存储在缓存器 30 中的 U-TOC 信息,来更新 U-TOC 扇区。

然后，在一个预定时刻，把缓存器 30 中存储的（更新）U-TOC 信息重写到袖珍盘 100 上，以更新袖珍盘 100 上的 U-TOC。

7、验证处理

5 作为（如解释 SDMI 数据路径过程所描述的）把内容数据传送/记录（检出）到记录/再现设备 20A 和以未加密状态记录到袖珍盘 100 中的条件，用于记录/再现设备 20A 的由个人计算机 1 所执行的验证处理的结果必须是 OK。验证处理是检验记录/再现设备 20A 是一个允许在未加密状态下执行记录内容数据操作的有效设备的处理。

10 除了符合 SDMI 标准的记录/再现设备 20B 外，对于连接到个人计算机 1 的连接单元 11 的记录/再现设备执行验证处理。需要注意的是，假设符合 SDMI 标准的被连接的记录/再现设备 20B 也经历一个确认处理，以确认被连接的记录/再现设备 20B 是一个真正符合 SDMI 标准的记录/再现设备 20B。如果假定符合 SDMI 标准的被连接的记录/再现设备 20B 没有被确认为一个真正符合 SDMI 标准的记录/再现设备 20B，则执行下述的验证处理，以检验所连接的记录/再现设备 20B 是一个有效记录/再现设备 20A。

 该实施例提供的验证处理是采用基于不对称加密（或者公共密钥加密）的验证技术执行的。在不对称加密处理中，加密密钥不同于解密密钥。假定参考标记 Db 是指加密处理之前的数据，参考标记 Ke 是指加密密钥，参考标记 Kd 是指解密密钥，参考标记 C 是指作为加密处理的结果获得的加密数据。在此情况下，加密处理由参考标记 $C=E(Ke, Db)$ 表示，对加密的数据 C 解密以获得加密前数据 Db 的解密处理由参考标记 $DB=D(Kd, C)$ 表示。

 这里，将加密密钥 Ke 和解密密钥 Kd 称之为“一对密钥”。其中一个密钥作为公共密钥公开，而另一个密钥作为保密密钥被隐藏在一个预定编号中。

25 在下述的验证处理中，公共密钥（是加密密钥 Ke 和解密密钥 Kd 之一）由参考标记 P 表示，而其它的用作保密密钥的解密密钥由参考标记 S 表示。对于上述情况，在记录/再现设备 20A 中，解密处理单元 28（或者系统控制单元 32）保存作为公共密钥 P 和保密密钥 S 的加密密钥 Ke 和解密密钥 Kd。

 验证处理通常通过一个命令启动，该命令由第一记录介质设备（个人计算机）1 的 CPU 2 发送到记录/再现设备 20A 的系统控制单元 32 以请求一个验证处理。然后根据该命令，在 CPU2（第一记录介质设备（个人计算机））

与系统控制单元 32 (记录/再现设备 20A) 之间执行类似图 13 所示的处理。

验证处理从处理 S1 开始, 在该处理 1 中, 记录/再现设备 20A 的系统控制单元 32 经由通信单元 26 把解密处理单元 28 保存的公共密钥 P 发送给个人计算机 1。需要注意的是, 公共密钥 P 是第一记录介质设备 1 已知的一个
5 密钥。因此, 如果记录/再现设备 20A 和第一记录介质设备 1 识别与公共密钥 P 相同的密钥, 则处理 1 不必执行。

当第一记录介质设备 1 的 CPU 2 收到公共密钥, 则验证处理被继续到处理 S2, 以生成一个随机数 r 。然后, 在下一个处理 S3 中, 把随机数 r 发送到记录/再现设备 20A。

10 然后, 在处理 S4 中, 记录/再现设备 20A 的系统控制单元 32 使用由解密处理单元 28 保存的保密密钥 S 加密随机数 r , 以生成加密的数据 $E(S, r)$ 。接着, 在处理 S5 中, 将加密的数据 $E(S, r)$ 发送到第一记录介质设备 1。

然后, 在处理 S6 中, 第一记录介质设备 1 的 CPU 2 使用公共密钥 P 解密从记录/再现设备 20A 接收的加密数据 $E(S, r)$ 。因此, 处理 S6 是一个由
15 $D\{P, E(S, r)\}$ 表示的解密处理。

接着, 在处理 S7 中, 将处理 S2 中生成的随机数 r 与处理 S6 中获得的解密结果 $D\{P, E(S, r)\}$ 进行比较。

如果公共密钥 P 和保密密钥 S 是一对正确的密钥, 那么比较结果应当显示解密结果 $D\{P, E(S, r)\}$ 等于随机数 r 。

20 因此, 指示解密结果 $D\{P, E(S, r)\}$ 匹配随机数 r 的比较结果确认记录/再现设备 20A 保存了用于公共密钥 P 的正确保密密钥 S。在此情况下, 验证处理从处理 S8 前进到处理 S9。在该处理 S9 中, 记录/再现设备 20A 被验证为一个有效连接伙伴。

另一方面, 如果比较结果指示解密结果 $D\{P, E(S, r)\}$ 与随机数不匹配,
25 则验证处理从处理 S8 前进到处理 S10。在处理 S10 中, 把第二记录介质设备确定为一个非有效连接的伙伴 (不是允许接收 SDMI 内容的设备), 生成一个 NG (否定) 验证结果。

另一方面, 如果上述验证处理的结果指示所连接的设备是一个有效的记录/再现设备 20A, 则第一记录介质设备 1 认可允许 SDMI 内容传送到所连接的
30 的设备的条件之一被满足。

8、内容加密技术

该实施例提供的数据传送系统的记录/再现设备 20A 和记录/再现设备 20B 的每一个对应于图 1 所示树结构底部的装置。下面的说明解释了数据传送系统中的类似图 1 所示结构的加密结构的一个典型实施。

5 图 14 是显示内容数据和密钥流的一个示范性视图。

当内容数据 CT1 从外部内容服务器 91 分配到个人计算机 1 时，内容数据 CT1 的传输单元实际上包括 $E(CK, A3D)$ 、 $E(KR, CK)$ 和 EKB。传输单元被分配给个人计算机 1，以存储到 HDD 5 中。

10 $E(CK, A3D)$ 是使用内容密钥 CK 加密内容数据 A3D 的结果。内容数据 A3D 是通过 ATRAC3 压缩的数据。因此， $E(CK, A3D)$ 是将要实际分配的音乐段。

$E(KR, CK)$ 是一个内容密钥 CK 加密的结果，用于使用结合图 1 解释的树根密钥 KR 解密已加密的内容数据。

EKB 是结合图 1 至图 3 解释的启动密钥块。正如从该实施例的描述中可以看到，EKB 是用于更新树根密钥 KR 的信息。

15 把多段内容数据 CT1、CT2 等等的每一个分配为包括 $E(CK, A3D)$ 、 $E(KR, CK)$ 和 EKB 的一个集合，HDD5 中存储的每个内容数据也被分配为如图 14 所示的一个集合。

根据预定的处理过程，还按照一个包括 $E(CK, A3D)$ 、 $E(KR, CK)$ 和 EKB 的集合，把内容数据从个人计算机 1 传送到记录/再现设备 20A 或者记录/再现设备 20B。

20 如上所述，记录/再现设备 20A 和记录/再现设备 20B 的每个相当于结合图 1 解释的一个装置（或者一个终端）。记录/再现设备 20A 专有的树叶 ID 被分配给记录/再现设备 20A，而记录/再现设备 20B 专有的树叶 ID 被分配给记录/再现设备 20B。在记录/再现设备 20A 和记录/再现设备 20B 的每一个中，存储 DNK（装置节点密钥）。

当记录/再现设备 20A 或者记录/再现设备 20B 从个人计算机 1 中接收一个内容数据集合时，对内容数据解密，然后存储到第二记录介质中（或者以未加密状态将内容数据存储到第二记录介质中）。对于符合 SDMI 标准的记录/再现设备 20B 而言，当再现内容数据时，解密已加密的内容数据。对于记录/再现设备 20A，当内容数据被记录到第二记录介质上时，解密已加密的内容数据。

如图所示，在解密已加密内容数据的处理中，首先使用所存储的 DNK 和所接收的 EKB 执行解密处理，以生成一个树根密钥 KR。

然后，把作为解密处理的一个结果得到的树根密钥 KR 用来解密 $E(KR, CK)$ ，以生成内容密钥 CK。

- 5 然后，把作为解密 $E(KR, CK)$ 的处理的一个结果得到的内容密钥 CK 用来解密 $E(CK, A3D)$ ，以生成内容密钥 A3D。

对于记录/再现设备 20A，将结合图 15A 和图 15B 以及图 16 具体解释 DNK 和解密已加密内容数据的处理过程。

- 10 假定一个图 15A 中所示的密钥树结构。SET0 的一个树叶 ID 和 K000 的树叶密钥被分配给记录/再现设备 20A。

在此情况下，存储在记录/再现设备 20A 中的 DNK 具有图 15B 中所示的多条信息。

首先，DNK 包括树叶 ID SET0。

DNK 还包括树叶密钥 K000。

- 15 包含在 DNK 中的其它条信息是如图 15A 所示的树叶密钥 K000 与树根密钥 KR 之间的路径上的节点密钥的信息。也就是说，其它条信息是节点密钥 K00 和 K0 以及树根密钥 KR 本身的信息。具体地说，节点密钥 K00 和 K0 以及树根密钥 KR 在被存储之前，已经通过使用树叶密钥 K000 予以加密。如图所示，加密节点密钥 K00 和 K0 以及加密的树根密钥 KR 按以下方式列出：

- 20 $E(K000, K00)$
 $E(K000, K0)$
 $E(K000, KR)$

- 25 通过使用包含在所存储的 DNK 中的信息，记录/再现设备 20A 解密从个人计算机 1 接收的已加密的内容密钥 $E(KR, CK)$ 和已加密的内容数据 $E(CK, A3D)$ 。

具体说，记录/再现设备 20A 首先通过使用树叶密钥 K000 解密 $E(K000, KR)$ ，以产生是树根密钥 KR 的 $D\{K000, E(K000, KR)\}$ 。

然后，将树根密钥 KR 用于解密已加密的内容密钥 $E(KR, CK)$ ，以产生是内容密钥 CK 的 $D\{KR, E(KR, CK)\}$ 。

- 30 最后，将内容密钥 CK 用于解密已加密的内容数据 $E(CK, A3D)$ ，以产生是内容数据 A3D 的 $D\{CK, E(CK, A3D)\}$ 。

然而，如前所述，树根密钥 KR 和内容密钥不是始终固定的。由于各种原因，它们被改变。对于在使用上述的树根密钥进行加密的状态下传送内容密钥 CK 的传送系统，可以为每个内容数据改变树根密钥。

例如，音乐分配企业在某些情况下逐条内容地改变树根密钥 KR，以强化版权保护。由于树根密钥 KR 是可变的，在上述的传送的同时，还传送一个 EKB，使授权的装置能够获得变化的树根密钥 KR。

假定对于加密的内容数据 $E(CK, A3D)$ ，由改变的树根密钥 KR' 加密的内容密钥 $E(KR', CK)$ 和一个 EKB 被接收，如图 16 所示。EKB 包括 $E(K0, KR')$ ，它是由节点密钥 K0 加密的被更新树根密钥 KR'。

需要注意的是，由节点密钥 K0 加密的被更新树根密钥 KR' 只能由拥有节点密钥 K0 的装置解密。如图 15A 和图 15B 所示，只有具有树叶 ID SET0 至 SET3 的装置才能够获得已更新的树根密钥 KR'。如果具有树叶 ID SET0 和 SET1 的装置只需要知道更新的树根密钥 KR'，则 EKN 需要包括 $E(K00, KR')$ ，它是使用节点密钥 K00 加密的已更新的树根密钥 KR'。

如结合图 15B 的上述解释，存储在记录/再现设备 20A 中 DNK 包括 $E(K000, K00)$ 和 $E(K000, K0)$ ，它们分别是使用树叶密钥 K000 加密的节点密钥 K00 和 K0。DNK 还包括 $E(K000, KR)$ ，它是使用树叶密钥 K000 加密的树根密钥 KR。

在上述状况中，解密内容数据 A3D 的处理过程在图 16 所示的步骤 (1) 至步骤 (4) 中描述。

步骤 (1): 由于接收的 EKB 是加密的更新树根密钥 $E(K0, KR')$ ，因此从 DNK 首先获得节点密钥 K0。也就是说，使用树叶密钥 K000 解密加密的节点密钥 $E(K000, K0)$ ，以产生作为节点密钥 K0 的 $D\{E(K000, K0)\}$ 。

步骤 (2): 然后，使用节点密钥 K0 解密包含在 EKB 中的加密的更新树根密钥 $E(K0, KR')$ ，以产生作为更新树根密钥 KR' 的 $D\{E(K0, KR')\}$ 。

步骤 (3): 使用作为步骤 (2) 解密处理结果而获得更新树根密钥 KR' 来解密加密的内容密钥 $E(KR', CK)$ ，以产生作为内容密钥 CK 的 $D\{E(KR', CK)\}$ 。

步骤 (4): 使用作为步骤 (3) 解密处理结果而获得的内容密钥 CK 来解密加密的内容数据 $E(CK, A3D)$ ，以产生作为内容数据 A3D 的 $D\{E(CK, A3D)\}$ 。

根据上述处理过程，记录/再现设备 20A 能够解密加密的内容数据，并能够把内容数据存储到袖珍盘 100 上。

另一方面，对于记录/再现设备 20B，在再现以加密状态记录在第二记录介质上的内容数据的操作中，执行上述处理过程，对加密内容数据进行解密，以生成再现的音乐或者类似物。

5 9. 内容检出/检入

下面的说明解释了由个人计算机 1 和记录/再现设备 20A 执行的处理，所述处理是：在检出中，把来自个人计算机 1 的 HDD 5 的内容数据传送到记录/再现设备 20A；在检入中，把检出到达记录/再现设备 20A 的内容数据返回到 HDD 5。

10 实际上，在一个通信对话中执行多个内容数据的检出和检入。然而，需要注意的是，为了解释方便起见，仅解释了内容数据的一个检出和内容数据的一个检入的流程。

图 17 和图 18 是显示检出处理的一个示意图。在图 17 和 18 所示的处理中，由个人计算机 1 利用的 CPU 2 执行的控制包括步骤 F101 至 F112。另一方面，由诸如系统控制单元 32 和解密处理单元 28 的部件（在记录/再现设备 20A 中使用）执行的控制包括步骤 F201 至 F215。

需要注意的是，通信对话是通过执行各种控制命令和发出对控制命令的响应来实施的。

HDD5 中存储的内容数据的检出开始于图 17 所示的步骤 F101。在步骤 F101 20 中，CPU 2 向记录/再现设备 20A 发出验证处理开始的一个请求。也就是说，向记录/再现设备 20A 发送一个验证开始控制命令。

响应验证开始控制命令，记录/再现设备 20A 在步骤 F201 通知个人计算机 1 同意验证处理开始。也就是说，向个人计算机 1 发送验证开始响应命令。

然后，在步骤 F102，个人计算机 1 作出一个树叶 ID 的请求。根据该请求，25 记录/再现设备 20A 在步骤 F202 发送一个存储的树叶 ID。

需要注意的是，个人计算机 1 检查连接个人计算机 1 的记录/再现设备 20A 的树叶 ID，由此确定记录/再现设备 20A 是否为一个具有有效树叶 ID 的设备。

然后，在步骤 F103，个人计算机 1 向记录/再现设备 20A 发送此后将被 30 传送的内容数据的 EKB。

当记录/再现设备 20A 收到 EKB 时，首先，在步骤 F203，记录/再现设

备 20A 存储 EKB 的版本号 (参见图 3)。然后, 在下一个步骤 F204, 记录/再现设备 20A 使用接收的 EKB 和存储的 DNK 执行图 16 所示的处理过程的步骤 (1) 和 (2), 以获得内容数据的树根密钥 KR 并存储该树根密钥 KR。

接着, 在下一个步骤 F205, 记录/再现设备 20A 通知个人计算机 1 已经
5 获得树根密钥 KR。

完成获得树根密钥 KR 的处理被通知之后, 在步骤 F104, 个人计算机 1 向记录/再现设备 20A 发出一个控制命令, 请求开始实际的检出对话开始。在步骤 F206, 根据该请求, 记录/再现设备 20A 发送一个响应命令, 该响应命令指示同意开始实际检出对话的开始请求。

10 需要注意的是, 该响应命令是响应控制命令通过执行结合图 13 说明的验证处理而发出的。

如上所述, 在图 13 所示的处理中, 验证不符合 SDMI 标准的记录/再现设备 20A, 以确定记录/再现设备 20A 是否是一个被允许解密已加密的内容数据并以不加密状态把内容数据存储在第一记录介质上的设备。如果验证处理的结果是 NG, 则检出对话一定是失败的, 尽管检出对话的失败未在图 17
15 中示出。

接着, 在步骤 F105, 个人计算机 1 向记录/再现设备 20A 发送加密的内容密钥 $E(KR, CK)$, 该加密的内容密钥与此后将要发送的内容数据有关。

接收加密的内容密钥 $E(KR, CK)$ 时, 记录/再现设备 20A 在步骤 F207 执行图 16 所示的处理过程的步骤 (3)。在步骤 (3), 使用存储的树根密钥 KR 解密加密的内容密钥 $E(KR, CK)$, 以产生内容密钥 CK。然后, 在下一个步骤 F208, 个人计算机 1 被通知已经完成了产生内容密钥 CK 的解密处理。
20

在步骤 F106, 个人计算机 1 向记录/再现设备 20A 发送一个记录对象控制命令, 以向记录/再现设备 20A 提供此后将检出的内容的信息。

25 记录对象控制命令的格式在图 19 中示出。记录对象控制命令的长度是 30 字节。记录对象控制命令是个人计算机 1 发出的命令, 通知记录/再现设备 20A (或者 20B) 实际内容数据将要在一个检出的通信对话中发送的信息。

如图 19 所示, 记录对象控制命令的格式包括作为操作码的 '记录对象'。此外, 该格式还包括: 诸如通信结果 (结果) 的信息比特, 通信对象设备的识别码 (目的地列表 ID), 第二记录介质的检出内容的轨道号 (新对象位置号), 内容数据类型 (内容类型), 第一记录介质中内容数据的格式 (下载的
30

格式轨道属性), 第二记录介质中内容的属性(轨道模式), 内容数据长度和内容数据的批数据长度(批数据长度)。

第一记录介质中内容数据的格式(下载的格式轨道属性)是从 HDD5 发送的内容数据的压缩技术及其比特速率以及内容数据的压缩技术(在内容数据被输出到传输线路上时采用)及其比特速率。

第二记录介质中内容的属性(轨道模式)是一个当内容被记录到袖珍盘 100 上时采用的压缩技术的规范, 并且是其它属性, 比如指定单声道或者立体声的属性。所指定的压缩技术通常是 132kbps 的 ATRAC、ATRAC3 或者是 66kbps 的 ATRAC3。

需要注意的是, 尽管在图 17 中未示出, 但是在步骤 F106 上, 记录/再现设备 20A 响应由个人计算机 1 发送的记录对象控制命令向个人计算机 1 发送一个响应命令。

依据在步骤 F208 发送的指示获得内容密钥 CK 的解密处理的完成的通知以及依据响应于记录对象控制命令发送的响应命令, 个人计算机 1 确认在记录/再现设备 20A 上已经完成了接收和解密内容数据的准备。因而, 检出的流程进行到代表图 18 所示的步骤 F107 的 P1。在此步骤中, 将内容数据传送到记录/再现设备 20A 上。具体说, 发送由内容密钥 CK 加密的内容数据 E(CK, A3D)。

另一方面, 记录/再现设备 20A 中的检出的流程进行到代表图 18 所示的步骤 F209 的 R1。在此步骤中, 接收从个人计算机 1 发送的内容数据 E(CK, A3D)。然后, 执行图 16 所示的处理过程的步骤(4), 以便使用内容密钥 CK 解密加密的内容数据 E(CK, A3D) 和把作为解密处理结果而获得的内容数据 A3D 存储到袖珍盘 100 上。

此外, 从不加密的内容数据中生成一个内容 ID。

当完成传送一条来自个人计算机 1 的内容数据(比如, 一段音乐)和把内容数据记录到袖珍盘 100 上的处理时, 有必要立即更新袖珍盘 100 上的 U-TOC。

如上所述, 记录在袖珍盘 100 的内圆周部分上的 U-TOC 被用来管理每个轨道(比如每段音乐和其它信息)的起始和结尾地址。在再现轨道的操作中, 从 U-TOC 中获得袖珍盘 100 上的轨道地址。

然而, 在该实施例, 在完成把内容数据记录到袖珍盘 100 的处理的时

刻，在步骤 F210 上仅仅更新缓存器 30 中存储的 U-TOC。也就是说，袖珍盘 100 上的 U-TOC 不是立刻更新。

当完成更新缓存器 30 中的 U-TOC 地处理时，在步骤 F211，向个人计算机 1 发送记录对象响应命令。

- 5 在此时刻，写该条内容数据的处理被完成，并向个人计算机 1 报告步骤 F209 上为内容数据生成的内容 ID。

图 20 中显示了记录对象响应命令的格式。

- 10 如图 20 所示，具有 62 字节长度的记录对象响应命令的格式包括作为一个操作码的“记录对象”。此外，该格式还包括：诸如一个通信结果（结果）的信息比特，通信对象设备的识别码（目的地列表 ID），第二记录介质的检出内容的轨道号（新对象位置号），内容数据类型（内容类型），第一记录介质中内容数据的格式（下载的格式轨道属性），第二记录介质中内容的属性（轨道模式），内容数据长度（内容大小）和内容数据的批数据长度（批数据长度）。

- 15 对于记录对象响应命令，该格式还包括具有 32 字节的对话数据字段。该字段被用作一个向个人计算机 1 报告由记录/再现设备 20A 生成的内容 ID 的区域。

因此，记录/再现设备 20A 使用这样一个记录对象响应命令，向个人计算机 1 报告内容数据和内容 ID 传送完成。

- 20 在步骤 F108，个人计算机 1 根据内容 ID 的通知执行内容 ID 表的处理。如下文所述，在步骤 F209，执行关联内容 ID 的处理，将个人计算机生成的并添加在 HDD 5 所存储的内容数据上的 ID 与记录/再现设备 20A 生成的内容 ID 相关联。

- 25 然后，在步骤 F109 上，个人计算机 1 向记录/再现设备 20A 发送检出控制命令。

在下一个步骤 F110 上，由于内容数据的检出，个人计算机 1 更新内容数据的应用规则。具体说，通过将内容数据的容许检出的数量递减 1 来改变内容权。

- 30 在步骤 F212，记录/再现设备 20A 执行由检出控制命令请求的实际检出的处理。具体而言，更新袖珍盘 100 上的 U-TOC，使所记录的内容数据处于可再现状态。这样，给予第二记录介质再现内容数据的权利。

需要注意的是，此时在 U-TOC 扇区 0 的内容数据的轨道模式中，把比特 d1 设置为 1，使内容数据处于写保护状态。

当完成更新用于检出的 U-TOC 的处理时，在步骤 F213，向个人计算机 1 发送一个检出响应命令，通知更新用于检出的 U-TOC 的处理已经完成。

5 此时，结束检出或者内容权的传送。

图 21 是一个显示检出控制命令的格式的示范性视图，图 22 是一个显示检出响应命令的格式的示范性视图。

检出控制命令具有 25 字节的长度，检出响应命令具有 17 字节的长度。

如图 21 所示，检出控制命令包括：作为操作码的诸如“检出”的信息
10 比特，通信结果（结果），通信对象设备的识别码（列表 ID），第二记录介质的用于检出内容的轨道号（对象位置号码）和加密的对话密钥（DES CBC (Ks, 00)）。

另一方面，如图 22 所示，检出响应命令包括：作为操作码的诸如“检出”的信息比特，通信结果（结果），通信对象设备的识别码（列表 ID），
15 第二记录介质的用于检出内容的轨道号（对象位置号码）。

如上所述，个人计算机 1 向记录/再现设备 20A 发送检入控制命令，并且，当检出响应命令从记录/再现设备 20A 发送到个人计算机以指示检出完成时，在步骤 F111，个人计算机 1 向记录/再现设备 20A 发送请求对话结束的控制命令。在步骤 F214 中，记录/再现设备 20A 向个人计算机 1 发送同意
20 对话结束的一个响应命令。

在步骤 F112，个人计算机 1 向记录/再现设备 20A 发送结束验证状态的控制命令。响应该控制命令，记录/再现设备 20A 在步骤 F215 向个人计算机 1 发送一个同意结束验证状态的响应命令。

此时，结束实施该检出的通信序列（sequence）。

25 需要注意的是，如果通过执行上述的通信检查具有公共树根密钥的多个内容，则仅需要对第二和后续内容之每个内容重复步骤 F105 至 F108 和步骤 F207 至 F211。

如果具有不同 EKB 版本的连续内容必须被连续传送，则 EKB 还需要与每个内容一起被传送。

30 下面，参考图 23 解释检入处理。

在图 23 所示的处理中，由个人计算机 1 使用的 CPU 2 执行的控制包括

步骤 F101 至 F156。另一方面，由诸如系统控制单元 32 和解密处理单元 28 的部件（这些部件被使用在记录/再现设备 20A 中）执行的控制包括步骤 F201 至 F257。

此外，在此情况下，通过使用各种控制命令和响应该控制命令的各种响应命令，实施一个通信对话。

此外，在一个检入情况下，按照以上述检出相同的方式执行包括验证处理的开始、EKB 的传送、树根密钥的搜索的处理。具体说，在步骤 F101 至 F103 和步骤 F201 至步骤 F205 上执行的各段处理与图 17 所示的它们的对应物相同，因此不需要重复对它们的解释。

在步骤 F150，个人计算机 1 向记录/再现设备 20A 发送请求检入对话开始的控制命令。

响应该控制命令，记录/再现设备 20A 在步骤 F250 发送一个响应命令。

需要注意的是，在此情况下，还执行参考图 13 已经解释过的验证处理。

如果记录/再现设备 20A 上执行的验证处理的结果是 OK，则开始所请求的检入对话。在此情况下，个人计算机 1 在步骤 F151 作出将要检入的内容数据的 ID 的请求。例如，个人计算机 1 向记录/再现设备 20A 发送将要检入到袖珍盘 100 上的内容数据的轨道号，作出用户内容 ID 的请求。

根据该请求，首先在步骤 F251，记录/再现设备 20 形成一个被指定内容数据（或者被指定轨道）是否为可以检入的内容数据的判断。该判断可以通过检查记录在用于轨道的 U-TOC 中的写控制标志（或者轨道模式的 d1 比特）来形成。

如果作为检出的结果，内容数据已经被记录在袖珍盘 100 上，但未在袖珍盘 100 上编辑，则把内容数据确定为可以检入的内容数据。

当执行图 17 和图 18 所示的检出时，如上所述，作为检出结果，将用于记录在袖珍盘 100 上内容的 TOC 扇区 0 内的记录模式的 d1 比特设置为 1。

作为检出的结果，d1 比特用作记录在袖珍盘 100 上内容的写控制标志。

具体说，d1 比特是一个袖珍盘系统中的所谓写保护标志。具体而言，对于 d1 比特设置为 1 的轨道禁止如删除、划分、级联的编辑处理。也就是说，对于被设置为 1 的轨道不执行如删除、划分、级联的编辑处理，而与第二记录介质装置是否为当前流行的传统袖珍盘记录器还是用作记录/再现装置 20A 的袖珍记录器无关。

然而实际上，记录在袖珍盘 100 上（该袖珍盘 100 被装在袖珍盘系统上）的轨道的 d1 比特不是被自动设置为 1。

因此，d1 比特是一个指示信息，不仅清楚指示禁止对该轨道的编辑处理，而且还指示从个人计算机检出的内容。

- 5 如果 d1 比特指示要检入的内容数据是作为检出结果而获得的内容数据，或者是可以被检入的内容数据，则在步骤 F252 准备内容数据的 ID。具体说，此时计算内容 ID，或者读出已经计算并存储的 ID。下面将阐述产生内容 ID 的技术。

接着，在下一步骤 F253，将内容 ID 发送到个人计算机 1。

- 10 需要注意的是，另一方面，如果将要检入的内容数据不是能够检入的内容数据，则通知个人计算机 1 要检入的内容数据不是可以检入的内容数据，此后执行错误处理过程。

- 在步骤 F152，个人计算机 1 核对从记录/再现装置 20A 接收到内容 ID。具体说，从记录/再现装置 20A 接收的内容 ID 与保存的内容 ID 进行比较，
15 该保存的内容 ID 由记录/再现装置 20A 生成并在一个检出中发送给个人计算机 1。然后在个人计算机中存储保存的内容 ID，以作为与个人计算机 1 生成的内容 ID 相关联的表数据。多个内容数据彼此进行比较，以确保要检入的内容数据是正确的内容数据。如果核对结果是 OK，则在步骤 F153 中请求实际的检入。

- 20 另一方面，如果核对的结果是 NG，则执行错误处理。

在步骤 F153 中通过发出图 24 所示的检入控制命令来请求检入。

图 24 是显示检入控制命令格式的示范性视图，图 26 是显示检入响应命令格式的示范性视图。

检入控制命令的长度是 17 字节，检入响应命令到长度是 25 字节。

- 25 图 24 所示的检入控制命令具有信息比特，包括：作为操作码的“检入”，通信结果（结果），子函数，通信对象设备的识别码（列表 ID）和第二记录介质上检入内容的轨道号（对象位置号）。

子函数按图 25 所示定义。该定义描述了由检入控制命令请求的处理。

- 30 子函数值 00h 表示检入控制命令请求了内容 ID。检入控制命令是这样
一个命令，该命令请求了实际检入以便返回一个授予给第二记录介质的再现权。

子函数值 01h 保留。但是，在实际检入处理中该值可以用于一个命令。

具有其它子函数值的检入控制命令请求记录在第二介质上的如预付费信息的特有信息。因此，具有其它子函数值的检入控制命令仅仅请求被读出的预付费信息和类似信息，但不作出检入（和再现权的返回）的请求。

- 5 另一方面，图 26 所示的检入响应命令具有多个信息比特，包括作为操作码的“检入”，通信结果（结果），子函数，通信对象设备的识别码（列表 ID）和第二记录介质上检入内容的轨道号（对象位置号）。

此外，检入响应命令还包括 8 字节字段（散列 MAC），用于向个人计算机 1 报告通过执行散列（HASH）函数处理生成的内容 ID。

- 10 在图 23 所示的检入步骤 F153 中发送的检入控制命令中，子函数的值设置为 00h，以便表示实际的检入。列表 ID 设置为指定记录/再现装置 20A 的值。对象位置号被设置为指定袖珍盘 100 上检出内容的轨道号。

在下一个步骤 F154，根据检出控制命令更新内容数据的应用规则。具体说，将允许传送的数递增 1。

- 15 在步骤 F254，记录/再现装置 20A 更新 U-DOC 数据。详细地说，更新 U-DOC 扇区 0 的内容，以从袖珍盘 100 中删除用作检入对象的轨道。也就是说，轨道被设置成不可再现代状态和丧失再现权的状态。

接着，在下一步骤 F255，发送图 26 所示的检入响应命令。

在此时，结束检入和返回内容权的操作。

- 20 结束检入时，在步骤 F155，个人计算机 1 向记录/再现装置 20A 发送作出对话结束请求的控制命令。响应该控制命令，在步骤 E256，记录/再现装置 20A 向个人计算机 1 发送同意结束对话的响应命令。

- 25 在步骤 F156，个人计算机 1 向记录/再现装置 20A 发送结束验证状态请求的控制命令。响应该控制命令，在步骤 F257，记录/再现装置 20A 向个人计算机 1 发送同意结束验证状态响应命令。

此时，结束用于检入的通信序列。

需要指出的是，如果必须通过执行上述通信来检入多个内容，则需要为每个内容重复校验内容 ID 的操作和请求检入的操作，即重复步骤 F151 至 F154 和步骤 F251 至 F255。

30

10、内容 ID 的生成和管理技术

检入和检出中采用的应用规则是通过使用每个内容的内容 ID 来管理的。

如上所述，在符合 SDMI 标准的第二记录介质中，采用允许内容 ID 被记录的格式。因此，在检出或者检入中，个人计算机 1 和符合 SDMI 格式的记录/再现设备 20B，通过使用由个人计算机 1 生成的内容 ID，能够识别用作检出或者检入的对象的内容数据。

然而，用于如袖珍盘（在过去的几年已经变得很流行）的第二记录介质的记录/再现设备 20A 不能够通过使用由个人计算机 1 生成的内容 ID，来识别内容数据。这是因为，作为检出结果，内容数据被记录在不包括存储内容 ID 的区域的袖珍盘 100 上。即使近期在 U-TOC 中或者类似物中规定这样一个区域并且把内容 ID 记录在袖珍盘 100 上，也将在老式袖珍盘执行更新 U-TOC 的操作中无意地擦除。因此，在袖珍盘 100 中不可能管理内容 ID。

如果在第二记录介质中不能管理内容 ID，检入则是不可能的，因为即使检出是可能的，但不能在检入处理中核实内容数据。

为了解决该问题，记录/再现设备 20A 设有从内容数据本身中生成内容 ID 的功能。

此外，把表数据设置在个人计算机 1 中，以便可以将个人计算机 1 生成的第一内容 ID 与记录/再现设备 20A 生成的第二内容 ID 进行比较。

首先，解释记录/再现设备 20A 采用的生成内容 ID 的技术。

对于内容数据的内容 ID 的生成，这里提供了一种装置，它除了执行轨道信息和内容数据的内容长度（内容大小）的处理外，还通过采样内容数据流中的特定数据执行 CBC-MAC 处理。

图 27 是一个显示代表如音乐的完整内容数据的一个模型的示范性视图。该内容数据是一个处于通过采用 ATRAC 或者 ATRAC3 技术进行压缩的状态的数据流。内容数据在检出中已经由个人计算机 1 以加密状态发送，然后解密以产生数据流。

例如，假定把点 P1 和 P2 设置为内容数据的抽样点，并提取声音单元（每个单元表现为一个阴影线矩形）的数据。声音单元的数据具有 424 字节的典型长度。因此，声音单元的数据相当于在上文中结合图 8 解释的声音单元。

然而，声音单元的数据不必相当于上文解释过的声音单元。

然后，使用部分抽样的实际内容数据生成内容 ID。

应当避免将内容的起点和结尾作为设置抽样点的位置，因为它完全处于内容起点和内容结尾每个都是寂静数据的概率边界之内。此外，通过把抽样点设置在两个位置上，通常是上述的抽样点 P1 和 P2，可以增加提取独特数据的概率。依据该独特数据，能够生成内容 ID，它充分有效地充当一个内容描述符。当然，抽样点也可以被设置在三个或多个位置上。此外，不同于内容起点和结尾的一个位置上的一个抽样点是充分的。

此外，如果抽样点 P1 和 P2 被设置在根据数据长度（或者数据大小）确定的位置上，而不是设置在随机选择的位置上，则获得用于特定内容数据的同一内容 ID，而与重复内容 ID 计算的次数无关。尽管内容数据 ID 不保存在第二记录介质上，但是如果内容数据本身被记录在第二记录介质上，可以在不同时间点计算同一内容 ID。这一现象使得不需要在用作第二记录介质的袖珍盘 100 上记录这样的内容 ID。

具体而言，在从内容结尾起数据大小（或者数据长度）的 $1/3$ 和 $2/3$ 距离的位置上设置抽样点 P1 和 P2。当然，所述位置不局限于从内容结尾起数据长度的 $1/3$ 和 $2/3$ 距离的位置。例如，所述位置可以是数据长度的任何分数（部分），比如从内容结尾起数据长度的 $1/2$ 、 $1/4$ 、 $3/4$ 、 $1/5$ 、 $2/5$ 、 $3/5$ 、 $4/5$ 、 $1/6$ 、 $5/6$ 等距离的位置。

下面使用下式（1）表达通过使用散列函数从内容数据中发现内容 ID 的技术：

20 内容 ID = CBC_MAC（密钥散列，IV，流（P1）//流（P2））... (1)

在上式中，密钥散列是具有 8 字节长度的固有密钥数据。

流（P1）是抽样点 P1 上的一个声音群组的数据，流（P2）是抽样点 P2 上的一个声音群组的数据，符号//是指级联的一个算符。

25 因此，符号流（P1）//流（P2）表示抽样点 P1 上的声音群组的数据与抽样点 P2 上的声音群组的数据的级联。级联的数据具有 424×2 字节的长度。

符号 IV 是具有 8 字节长度的 CBC 模式的初始值。对于具有 4 字节长度和 1 字节轨道信息 TrackModeByte（轨道模式字节）的内容长度，初始值 IV 由下式（2）表示：

30 $IV = \{\text{长度} // \text{TrackModeByte} // \text{填充零的 32 比特}\} \dots (2)$

在此情况下，包含在图 19 所示的记录对象控制命令中的 4 字节内容长度 1 字节轨道模式可以被用作等式（2）中的具有 4 字节大小的内容长度和

1 字节轨道信息 (TrackModeByte)。

这样的内容 ID 由通常安装在记录/再现设备 20A 的解密处理单元 28 上的 HASH (散列) 引擎生成。使用等式 (2) 计算的初始值 IV 被代入等式 (1) 中的 IV 项。记录/再现设备 20A 能够从包含在记录对象控制命令 (在图 17 5 所示的检出对话的步骤 F106 上接收的) 中的信息中算出初始值 IV。

此外, 在传送内容数据之前, 可以从包含在记录对象控制命令中的内容大小中识别内容数据的长度。因此, 在传送内容数据之前, 还可以确定用于抽样点 P1 和 P2 的位置的内容长度的 1/3 和 2/3 的距离。

因此, 在随着内容数据的实际传送开始提取抽样点 P1 和 P2 上的声音群组的多片数据之后, 可以使用等式 (1) 计算内容 ID。 10

对于记录在袖珍盘 100 上的内容数据, 当然可以从 U-TOC 扇区 0 的数据中发现内容数据的长度。因此, 可以确定抽样点 P1 和 P2 的位置。

此外, 在检出中发送的记录对象控制命令中所包含的轨道模式被记录为 U-TOC 扇区 0 中的轨道模式, 以便可以通过使用等式 (2) 从 U-TOC 扇区 0 15 中发现初始值 IV。

因此, 对于记录在袖珍盘 100 上的内容数据, 可以在任何时间点发现内容 ID。

例如, 记录/再现设备 20A 能够生成用作上述检出的对象的内容数据的其自己的内容 ID。然而, 记录/再现设备 20A 生成的内容 ID 不能被适当利用, 除非记录/再现设备 20A 生成的内容 ID 与个人计算机 1 生成的并存储在 HDD5 中的内容 ID 相关联。 20

上述的 HDD5 中存储的内容 ID 是由个人计算机 1 上运行的应用程序, 为内容数据而生成的。通过该应用程序事先发现的内容 ID 包括: 对具有如 HDD 的第一记录介质的设备 (个人计算机 1) 特有的信息, 存储在 HDD5 内的时间信息, 随机数。该个人计算机 1 专有的信息的例子是安装在个人计算机 1 25 内的应用程序专有的 ID。

如图 28 所示的表数据, 个人计算机 1 将记录/再现设备 20A 生成的 (第二) 内容 ID 与上述由个人计算机 1 生成的 (第一) 内容 ID 相关联。

需要注意的是, 表数据代表使用如 HDD5 的第一记录介质的设备专有的 30 关联。

在图 18 所述的检出对话的步骤 F211 中, 记录/再现设备 20A 使用记录

对象响应命令将记录/再现设备 20A 生成的第二内容 ID 通知给个人计算机 1。然后，个人计算机 1 在步骤 F108 执行对于表数据的处理。在该处理中，为检出中传送的内容数据建立表数据（图 28 所示）的元素。该元素将个人计算机 1 生成的用于内容数据的第一内容 ID 与记录/再现设备 20A 生成的用于相同内容数据的第二内容 ID 相关联。

图 28 所示的典型表数据由三个元素组成，即由第一、第二和第三元素组成，每个元素将第一内容 ID 与第二内容 ID 相关联。

在个人计算机 1 的表数据（例如，HDD 5 中的记录/更新）的管理中，使用其内容 ID 管理检出到袖珍盘 100 的内容数据。因而，可以管理检出和检入。

如上所述，袖珍盘 100 不包括存储内容 ID 的区域。然而，记录/再现设备 20A 能够发现存储在袖珍盘 100 中的内容数据的内容 ID。

因此，当希望检入返回到个人计算机 1 的内容数据时，个人计算机 1 请求记录/再现设备 20A 发送内容数据的（第二）内容 ID。然后，个人计算机 1 确认从记录/再现设备 20A 接收的（第二）内容 ID 与作为图 28 所示的表数据的元素存储的（第二）内容 ID 是否匹配（在内容数据的检出中，从记录/再现设备 20A 接收作为表数据的元素存储的第二内容 ID）。如果从记录/再现设备 20A 接收的第二内容 ID 与作为表数据的元素存储的第二内容 ID 是匹配的，则个人计算机 1 对于由（第一）内容 ID 管理的内容数据执行检入处理。

上述说明解释了在图 23 中所述的步骤 F151、F152、F252、F253 执行的几部分处理。

通过采用这样的内容 ID 管理技术，甚至对于不符合 SDMI 标准的第二记录介质（袖珍盘 100 和类似物），也能够在数据传送系统中适当地执行检出和检入的管理，也就是，内容权的管理。

11、介质信息的获取

至此，已经解释了与用作第二记录介质的袖珍盘 100 有关的检出和检入（从袖珍盘检出和检入袖珍盘）。

当被执行从用作第二记录介质的袖珍盘 100 的检出时，个人计算机 1 需要获取袖珍盘 100 上的信息，该袖珍盘 100 被事先装在连接个人计算机 1 的

记录/再现设备 20A 上。

在该实施例中，在实际检出/检入执行之前的一个时间点上，例如在记录/再现设备 20A 通过典型的 USB 传输线连接个人计算机 1 的时间点，个人计算机 1 执行获取装在记录/再现设备 20A 上的袖珍盘 100 的信息的通信处理。该获取袖珍盘的信息的处理被称作介质信息获取处理。

下面结合图 29 和图 30 解释介质信息获取处理。在图 29 和图 30 中，个人计算机 1 通过运行驱动个人计算机 1（充当一个数据传送设备）的应用软件的运行，执行步骤 F180 至步骤 F188 的多条处理。另一方面，由记录/再现设备 20A 中使用的系统控制单元 32 执行步骤 F280 至步骤 F286 的多条处理。

当在记录/再现设备 20A 连接到个人计算机 1 的时间点上，例如在步骤 F180，执行介质信息获取处理时，个人计算机 1 向记录/再现设备 20A 发送专用控制的请求。在此情况下，向记录/再现设备 20A 发送图 31 所示的专用登录控制命令。

专用登录控制命令包括子单元类型和子单元 ID（指示控制对象设备）以及用于指示控制等级的优先权字段。专用登录控制命令避免或者限制记录/再现设备 20A 执行诸如以下处理的操作：从用作第二记录介质的袖珍盘 100 中删除数据，编辑袖珍盘 100 上的数据，拆卸（dismount）袖珍盘 100 和控制电源。

也就是说，专用登录控制命令使记录/再现设备 20A 处于这样一个状态：记录/再现设备 20A 仅仅在个人计算机 1 进行请求时执行上述的操作。

包含在专用登录控制命令中的优先权指示操作的禁止和限制的各种状态。

例如，记录/再现设备 20A 的操作按照以下等级来控制：

控制等级 4：完全禁止操作，除非存在一个来自个人计算机 1 的请求任何操作的命令。

控制等级 3：完全禁止控制电源操作、退出第二记录介质操作、划分轨道操作、链接轨道操作和删除轨道操作，除非存在一个来自个人计算机 1 的请求任何操作的命令。

控制等级 2：完全禁止划分轨道操作、链接轨道操作和删除轨道操作，除非存在一个来自个人计算机 1 的请求任何操作的命令。

控制等级 1: 允许编辑或者删除不同于检出内容的轨道的操作。

控制等级 0: 不对操作强加限制。

当然, 上述控制等级是典型的。实际上, 大量的各种控制等级都是可能的。

- 5 记录/再现设备 20A 根据专用等级控制命令设置控制模式, 并且在步骤 F208, 发送一个指示同意该专用控制请求的响应。

需要注意的是, 专用控制的状态一直持续到个人计算机 1 发送一个图 32 所示的专用登出控制命令。

- 10 该专用登出控制命令是一个给予记录/再现设备 20A 的终止专用登录控制状态的命令。专用登出控制命令的格式相同于专用登录控制命令的格式, 但不包括在指示自由状态的控制等级的 00h 上设置优先权。

- 在个人计算机 1 使记录/再现设备 20A 处于专用控制状态从而向个人计算机 1 上运行的应用程序转送控制权之后, 打开描述符, 并且在步骤 F181 上, 个人计算机 1 获得被装在记录/再现设备 20A 上的袖珍盘 100 的状态。
15 具体地说, 个人计算机 1 向记录/再现设备 20A 发送图 33 所示的获得盘状态控制命令。

 响应该获得盘状态控制命令, 记录/再现设备 20A 在步骤 F281 向个人计算机 1 发送一个图 34 所示的获得盘状态响应命令。然后, 个人计算机 1 根据获得盘状态响应命令关闭描述符。

- 20 如图 34 所示, 由记录/再现设备 20A 中使用的系统控制单元 32 发送到个人计算机 1 的获得盘状态响应命令包括: 一个在偏移 1Ah 的偏移字节上的“盘在驱动器中 (disc in drive)”字段。如果袖珍盘已经被装在记录/再现设备 20A 上, 则所发送的得到盘状态响应命令包括一个声称的“盘在驱动器中”字段。

- 25 因此, 通过检查包含在获得盘状态命令中的“驱动盘”字段, 个人计算机 1 能够确定袖珍盘 100 是否被安装到记录/再现设备 20A 上。

 如果袖珍盘 100 没有被安装到记录/再现设备 20A 上, 个人计算机 1 的处理从步骤 F182 返回到步骤 F181, 以再次发送获得盘状态控制命令, 以获得袖珍盘 100 的状态。

- 30 例如, 假定袖珍盘 100 没有被装在记录/再现设备 20A 上。在此情况下, 个人计算机 1 以通常为 1 秒钟的预定时间间隔向记录/再现设备 20A 发送获

取袖珍盘 100 的状态的获得盘状态控制信息。

当确认记录/再现设备 20A 上安装的袖珍盘 100 的状态时，个人计算机 1 打开描述符，并且在步骤 F183 发送图 35 所示的获得盘名称控制命令，以便获取袖珍盘 100 的名称。

- 5 接收获得盘名称命令时，记录/再现设备 20A 中使用的系统控制单元 32 获得袖珍盘 100 的 U-TOC 中记录的盘名称。然后，在步骤 F282，系统控制单元 32 建立图 36 所示的获得盘名称响应命令，并且响应于获得盘名称控制命令把获得盘名称响应命令发送给个人计算机 1。接收该响应时，个人计算机 1 关闭描述符。

- 10 如图 36 所示，所发送的获得盘名称响应命令包括：偏移字节 19h 至 (19 + N) h 上的一个“N 字节盘标题文本”字段。“N 字节盘标题文本”字段被用来存储一个描述取自 U-TOC 扇区 1 的盘名称的 N 字节文本。在偏移字节 17h 和 18h 的“第一字段长度”中描述符号 N，该符号 N 表示组成盘名称的字节数。

- 15 通过检查获取盘名称响应命令的“N 字节盘标题文本”字段，个人计算机 1 能够得知安装在记录/再现设备 20A 上的袖珍盘 100 的名称。

在步骤 F184，个人计算机 1 打开描述符，并且向记录/再现设备 20A 发送图 37 所示的获得盘容量信息控制命令，以便获得介质容量。

- 20 接收获得盘容量信息控制命令时，记录/再现设备 20A 中使用的系统控制单元 32 获得袖珍盘 100 的 U-TOC 扇区 0 中记录的信息。然后，在步骤 F283，系统控制单元 32 建立图 38 和图 39 所示的获得盘容量信息响应命令，并且响应于得到盘容量信息控制命令向个人计算机 1 发送获得盘容量信息响应命令。收到该响应时，个人计算机 1 关闭描述符。

- 25 如图 38 和图 39 所示，所发送的获得盘容量信息响应命令包括：偏移字节 1Bh 至 1Fh 上的命名为“时”、“分”、“秒”和“帧”的字段。这些字段显示了以时、分、秒、帧等表示的总执行时间。组成命名为“时”、“分”、“秒”和“帧”的字段的字节数被存储在偏移字节 19h 和 1Ah 的“总播放容量长度”字段。所述字节数是命名为“时”、“分”、“秒”和“帧”的字段的数据长度。需要注意的是，总执行时间是从袖珍盘 100 再现整个内容数据所用的时间长度。
- 30 度。

此外，在偏移字节 22h 至 26h 上也设置了命名为“时”、“分”、“秒”和

“帧”的字段。这些字段显示了以“时”、“分”、“秒”和“帧”为单元表示的最大记录时间。组成这些命名为“时”、“分”、“秒”和“帧”的字段的字节数被存储在偏移字节 20h 和 21h 的“最大记录容量长度”字段中。该字节数是命名为“时”、“分”、“秒”和“帧”的字段的数据长度。需要注意的是，
5 最大记录时间是再现以袖珍盘 100 的总容量容纳的数据所用的时间长度。

此外，在偏移字节 29h 至 2Dh 上也设置了命名为“时”、“分”、“秒”和“帧”的字段。这些字段显示了以“时”、“分”、“秒”和“帧”为单元表示的剩余时间。组成这些命名为“时”、“分”、“秒”和“帧”的字段的字节数被存储在偏移字节 27h 和 28h 的“剩余记录容量长度”字段中。该字节数是
10 命名为“时”、“分”、“秒”和“帧”的字段的数据长度。需要注意的是，剩余时间是数据可以记录到袖珍盘 100 上的剩余记录时间。即，剩余时间是从最大记录时间减去总执行时间之差。

通过检查获取盘容量信息响应命令的字段，个人计算机 1 能够得知作为安装在记录/再现设备 20A 上的袖珍盘 100 的存储容量的信息的，总执行时间、最大记录时间和剩余时间。
15

在步骤 F185，个人计算机 1 打开描述符，并且发送图 40 所示的获得声音轨道数控制命令，以便获得一个轨道编号。

收到获得声音轨道数控制命令时，记录/再现设备 20A 中使用的系统控制单元 32 获得袖珍盘 100 的 U-TOC 扇区 0 中记录的信息。然后，在步骤 F284，
20 系统控制单元 32 建立一个图 41 所示的获得声音轨道数响应命令，并且响应于获得声音轨道数控制命令，向个人计算机 1 发送获得声音轨道数响应命令。收到该响应时，个人计算机 1 关闭描述符。

如图 41 所示，所发送的获得声音轨道数响应命令包括位于偏移字节 17h 和 18h 上的一个“条目数”字段。该字段显示记录在袖珍盘 100 上的轨道或者内容数。
25

通过检查所发送的获得声音轨道数响应命令的“条目数”字段，个人计算机 1 能够得知袖珍盘 100（它安装在记录/再现设备 20A 上）上记录的轨道或者内容数。

然后，个人计算机 1 的处理前进到图 30 所示的步骤 F186，以获得轨道
30 上的信息。

首先，在步骤 F186 上，个人计算机 1 打开描述符，并且向记录/再现设

备 20A 发送图 42 所示的获得声音轨道名称控制命令，以便获得轨道#x 的名称。所发送的得到声音轨道名称控制命令包括偏移字节 07h 和 08h 上的“对象位置”字段。“对象位置”字段指定袖珍盘 100 上的轨道的编号 (#x)。

收到获得声音轨道名称控制命令时，记录/再现设备 20A 中使用的系统
5 控制单元 32 从 U-TOC 扇区 1 中获得轨道#x 的名称，并且在步骤 F285 响应于获得声音轨道名称控制命令，向个人计算机 1 发送图 43 所示的获得声音轨道名称响应命令。

如图 43 所示，获得声音轨道名称响应命令包括位于偏移字节 07h 和 08h 上的“对象位置”字段。该“对象位置”字段显示袖珍盘 100 上的轨道的编
10 号。获得声音轨道名称响应命令还包括位于偏移字节 19h 至 (19+M) h 上的一个“M 字节轨道标题文本”字段。该“M 字节轨道标题文本”字段用来存储一个描述取自 U-TOC 扇区 1 的轨道名称的 M 字节文本。符号 M 代表在偏移字节 17h 和 18h 的‘第一字段长度’字段中描述的组成轨道名称的字节数。

通过检查得到盘名称响应命令的“M 字节轨道标题文本”字段，个人计
15 算机 1 能够得知安装在记录/再现设备 20A 上的袖珍盘 100 所记录的轨道#x 的名称。

然后，不关闭描述符，个人计算机 1 执行获取“对象位置”字段中指定的一个轨道属性。具体地说，在步骤 F187，个人计算机 1 向记录/再现设备 20A 发送获得声音轨道信息控制命令，以便获得轨道#x 的属性。

20 获得声音轨道信息控制命令包括：图 44 所示的轨道属性阅读信息块控制命令，图 46 所示的轨道模式阅读信息块控制命令，和图 48 所示的轨道大小阅读信息块控制命令。

响应于轨道属性阅读信息块控制命令、轨道模式阅读信息块控制命令、轨道大小阅读信息块控制命令，记录/再现设备 20A 所使用的系统控制单元
25 32 分别向个人计算机 1 发送图 45 所示的轨道属性阅读信息块响应命令，图 46 所示的轨道模式阅读信息块响应命令，和图 49 所示的轨道大小阅读信息块响应命令。

图 44 所示的轨道属性阅读信息块控制命令是一个用于“对象位置”字段中指定的轨道的写保护信息的请求。

30 响应该轨道属性阅读信息块控制命令，系统控制单元 32 从 U-TOC 扇区 0 中获取轨道的模式，并且发出图 45 所示的轨道属性阅读信息块响应命令。

“对象位置”字段中指定的轨道的写保护信息从轨道模式中提取并且被包含在偏移字节 0Fh 上的“盘子单元对象属性”中。

个人计算机 1 确认轨道#x 处于如设置在 01h 上的字段所证明的锁定状态或者确认轨道#x 处于设置在 00h 上的字段证明的开锁装置。

5 图 46 所示的轨道模式阅读信息块控制命令是一个信息请求，该信息包括“对象位置”字段中指定的轨道的抽样率。

响应该轨道模式阅读信息块控制命令，系统控制单元 32 发出图 47 所示的轨道模式阅读信息块响应命令。

在字段轨道模式阅读信息块响应命令中，“对象位置”字段中指定的轨道的抽样频率被显示在设置在偏移字节 19h 上的“音频记录抽样率”字段中。

量化比特计数被显示在偏移字节 1Ah 上设置的“音频记录抽样大小”字段中。压缩模式被设置在位于偏移字节 1Bh 上的“音频记录压缩模式”字段中。压缩模式可以使 ATRAC 或者 ATRAC3 模式。

15 指示立体声或者单声道的通道信息被显示在偏移字节 1Ch 上的“音频记录通道模式”中。

因此，个人计算机 1 能够从上述字段中得知轨道#x 的信息。该信息包括抽样频率、量化比特计数、压缩模式和通道模式。

图 48 所示的轨道大小阅读信息块控制命令是一个用于“对象位置”字段中指定的轨道的数据长度的请求。

20 响应于轨道大小阅读信息块控制命令，系统控制单元 32 发出图 49 所示的轨道大小阅读信息块响应命令。

轨道大小阅读信息块响应命令包括偏移字节 1Ah 至 1Eh 上的名为“时”、“分”、“秒”和“帧”的字段。这些字段显示了在时、分、秒、帧方面表达的数据大小。个人计算机 1 能够从这些字段中得知轨道#x 的数据长度。

25 通过在步骤 F186、F187、F285 和 F286 上交换控制命令和响应命令，个人计算机 1 能够获得一个轨道的名称和属性。对于袖珍盘 100 上记录的每个轨道，重复交换控制命令和响应命令的操作。在步骤 F188，个人计算机 1 判断是否已经为袖珍盘 100 上记录的所有轨道获取了名称和属性。如果还没有为所有轨道获取名称和属性，则处理返回到步骤 F186，重复操作。在步骤 F186，“对象位置”字段中指定的轨道数被改变到指示下一次获取名称和属性的另一个轨道的另一个轨道数。

30

当获取用于所有轨道地名称和属性时，关闭描述符，以结束顺序处理。
在步骤 F185 上请求获取名称和属性的轨道数，并且在 F284 上得到轨道数。

需要注意的是，在交换控制命令和响应命令的操作中，不对“对象位置”
字段中指定的每个轨道打开和关闭描述符。因此，可以缩短获取轨道名称和
5 轨道属性所用的时间长度。

如上所述，在该实施例中，当记录/再现设备 20A 连接到个人计算机 1
时，个人计算机 1 能够获取安装在记录/再现设备 20A 上的袖珍盘 100 的信
息。该信息包括：介质名称，介质容量，轨道数（或者内容数据计数），每
个轨道的名称，写保护数据，每个轨道的模式数据，每个轨道的大小。容量
10 包括总执行时间、最大记录时间，剩余时间。模式数据包括抽样频率、量化
比特计数、压缩模式、通道模式。

如上所述，通过获取用作第二记录介质的袖珍盘 100（从现在起充当一
个检出/检入目标）上的信息，个人计算机 1 上运行的应用程序能够执行下
述的各种处理。

15 首先，用作第二记录介质的袖珍盘上的信息可以被显示为出现在个人计
算机 1 的监视器上的应用屏幕。因此，能够显示袖珍盘 100 的标题、总执行
时间、最大记录时间、剩余时间和轨道数。在显示屏幕上，诸多轨道按照其
轨道名称随同每个轨道的大小和每个轨道的其它信息来显示。结果，可以向
用户显示适当的信息。

20 第二，当 HDD 5 中存储的内容数据检出时，将内容数据的大小与袖珍盘
100 的剩余时间进行比较，以形成一个袖珍盘 100 自由区域是否可以用来容
纳该检出的判断。

如果判断结果指示袖珍盘 100 的自由区域可以容纳该检出，则执行图 17
和图 18 所示的检出处理。

25 第三，如果多个内容被指定为检出对象，并且袖珍盘 100 的自由区域不
能用来容纳检出对象，则可以执行仅对某些请求的内容的检出处理。

当然，显示在监视器上的信息还可以充当用户指定检入时的指导。此外，
检入增加了袖珍盘 100 中的自由区域的尺寸。最好是向被指定为检出对象的
内容数据分配具有增加了尺寸的自由区域。

30 也就是说，通过获取第二记录介质的信息，可以在数据传送系统中指定
适当操作。

至此已经说明了一个优选实施例。然而，本发明的范围不限于该实施例。

也就是说，通过改变数据传送系统的操作来提供处于本发明基本范围内的各种版本是可能的，所述改变的操作包括：加密、数据路径、检出/检入技术、确认技术、内容 ID 生成技术、内容 ID 管理技术、获取第二记录介质信息的技术。

此外，本发明不限于按照上文对一个 SDMI 内容所述的，从第一记录介质到第二记录介质处理数据传送的目的。而是，数据传送处理可以被广泛地应用于各类内容数据。此外，第一记录介质可以是不同于 HDD 的介质。

当然，第二记录介质不限于袖珍盘，记录/再现设备 20A 不限于袖珍盘记录设备。作为替换，第二记录介质可以是不同类型的介质。例如，对于袖珍盘 100，可能利用另一个介质，比如 CD-R、CD-RW、DVD-RAM、DVD-R、DVD-RW 或者各种存储卡之一。因此，对于记录/再现设备 20A，可以利用其它介质的记录设备。

从以上说明中可以明白，根据本发明，数据传送设备（或者第一记录介质设备）能够请求数据记录设备（或者第二记录介质设备）发送充当检目地的第二记录介质的信息，并且能够获取信息，即使，对于第二记录介质，利用了一个采用它自己唯一的管理技术的介质（如是一个袖珍盘）。

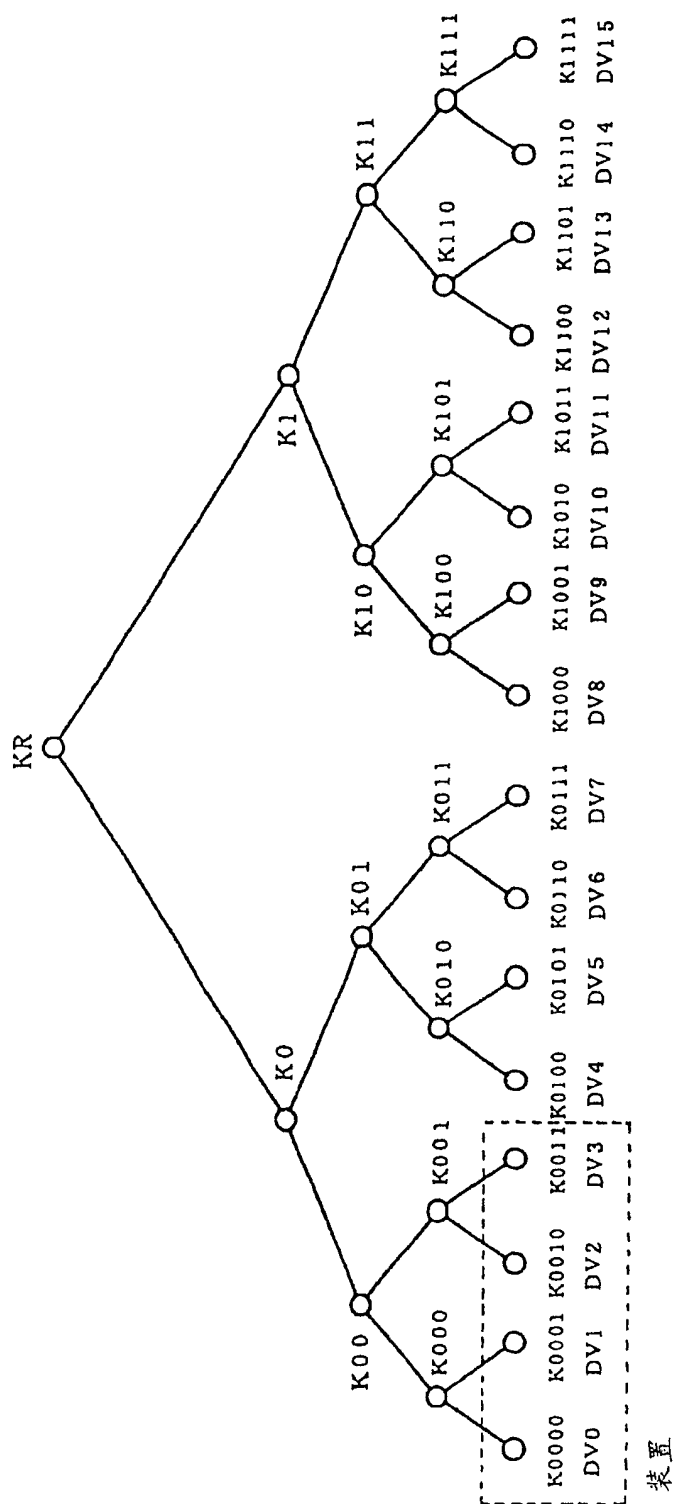
具体说，第二记录介质上的信息包括：指示第二记录介质是否安装在数据记录设备上的信息，第二记录介质的名称，第二记录介质上存储的每个内容数据的名称，第二记录介质的容量，第二记录介质上记录的每个内容数据的数量和第二记录介质上记录的每个内容数据的属性。

依据第二记录介质的信息，在检出或者从第一记录介质向第二记录介质传送内容数据之前，能够精确地形成关于能否实施检出、将要检出的内容是否适当、内容数据是否适合于该检出的判断。因此，展示了适当传送操作的实施效果。

此外，通过获取第二记录介质的信息，数据传送设备上运行的应用程序能够把第二记录介质的信息作为指南信息呈现给用户。

当然，由于内容数据是以未加密状态记录在第二记录介质上的，因此可以获得与传统设备的兼容，同时还可以保护版权。这是因为执行了确认处理，并且为一个检出检查应用规则。

上述效果对于用户是有益的，此外，能够向用户提供一个容易使用的数据传送系统。



一
圖

版本: t	
索引	加密密钥
0	$E(K(t)0, K(t)R)$
00	$E(K(t)00, K(t)0)$
000	$E(K000, K(t)00)$
001	$E(K(t)001, K(t)00)$
0010	$E(K0010, K(t)001)$

图 2A

版本: t	
索引	加密密钥
000	$E(K000, K(t)00)$
001	$E(K(t)001, K(t)00)$
0010	$E(K0010, K(t)001)$

图 2B

偏移地址	内容	大小 (字节)
0	节点密钥计数	4
4	节点密钥深度	4
8	EKB版本	4
12	保留	4
16	加密节点密钥	$16 \times M$
$16 + 16 \times M$	保留	16
$32 + 16 \times M$	加密EKB版本	8
$40 + 16 \times M$	电子签名	5

图 3

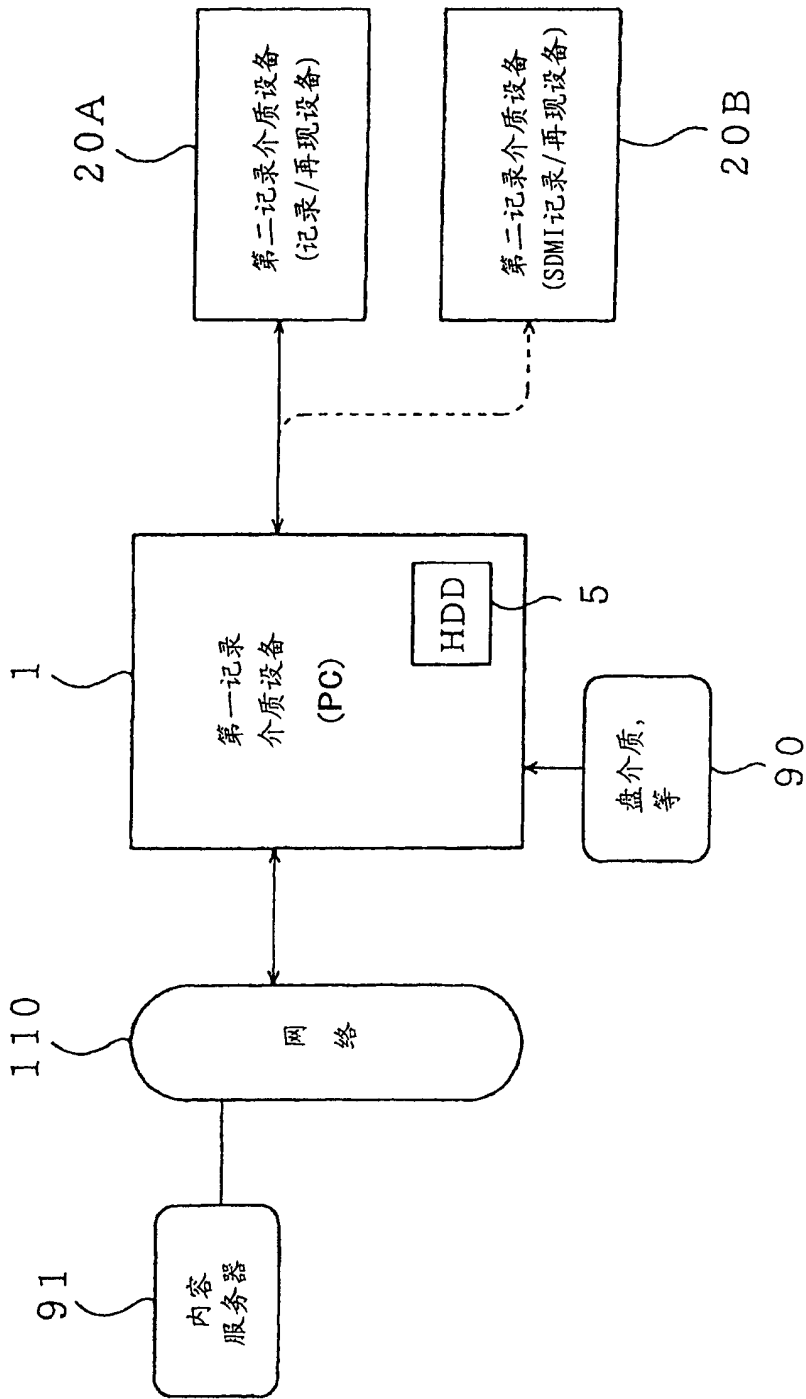
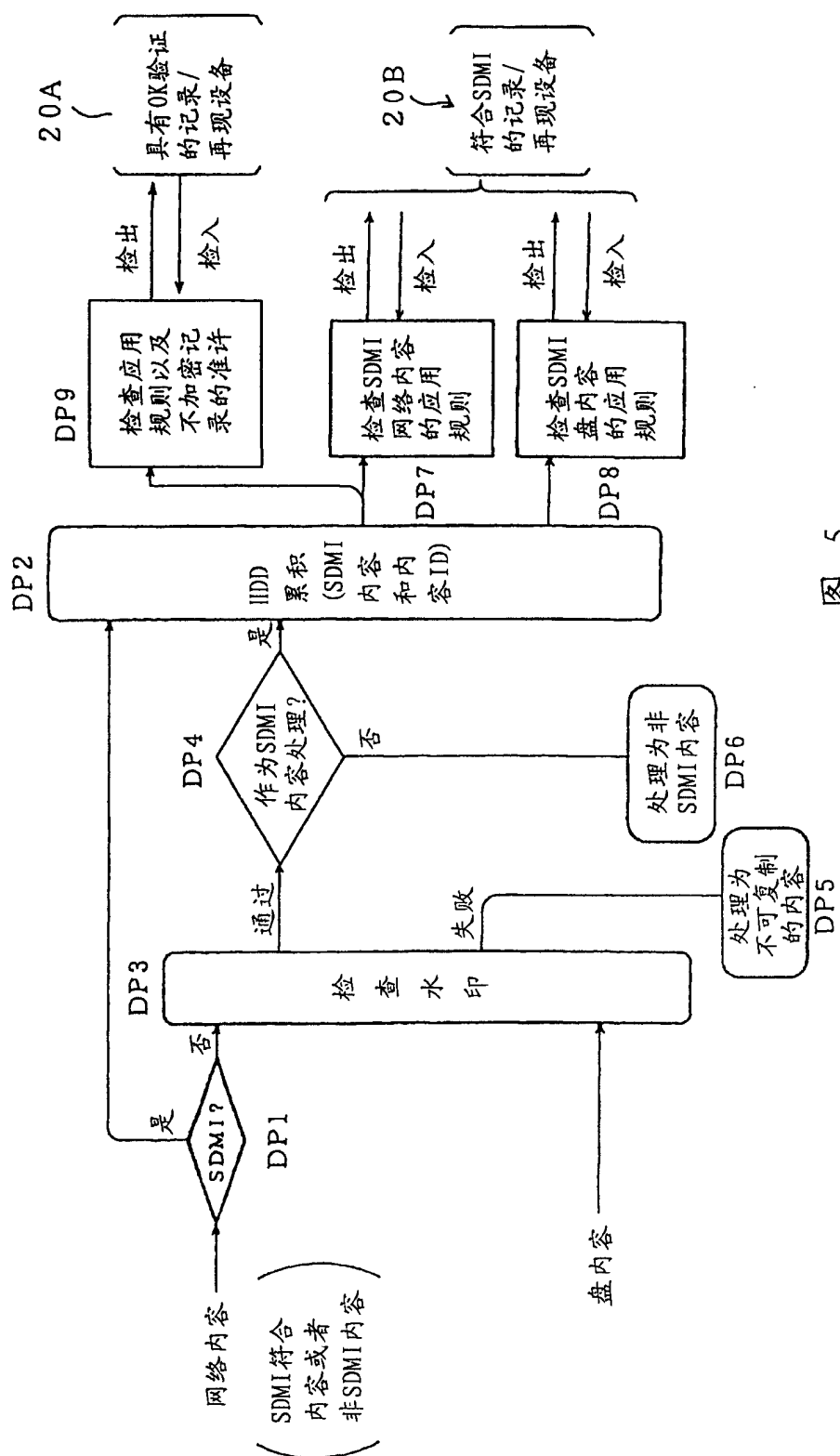


图 4



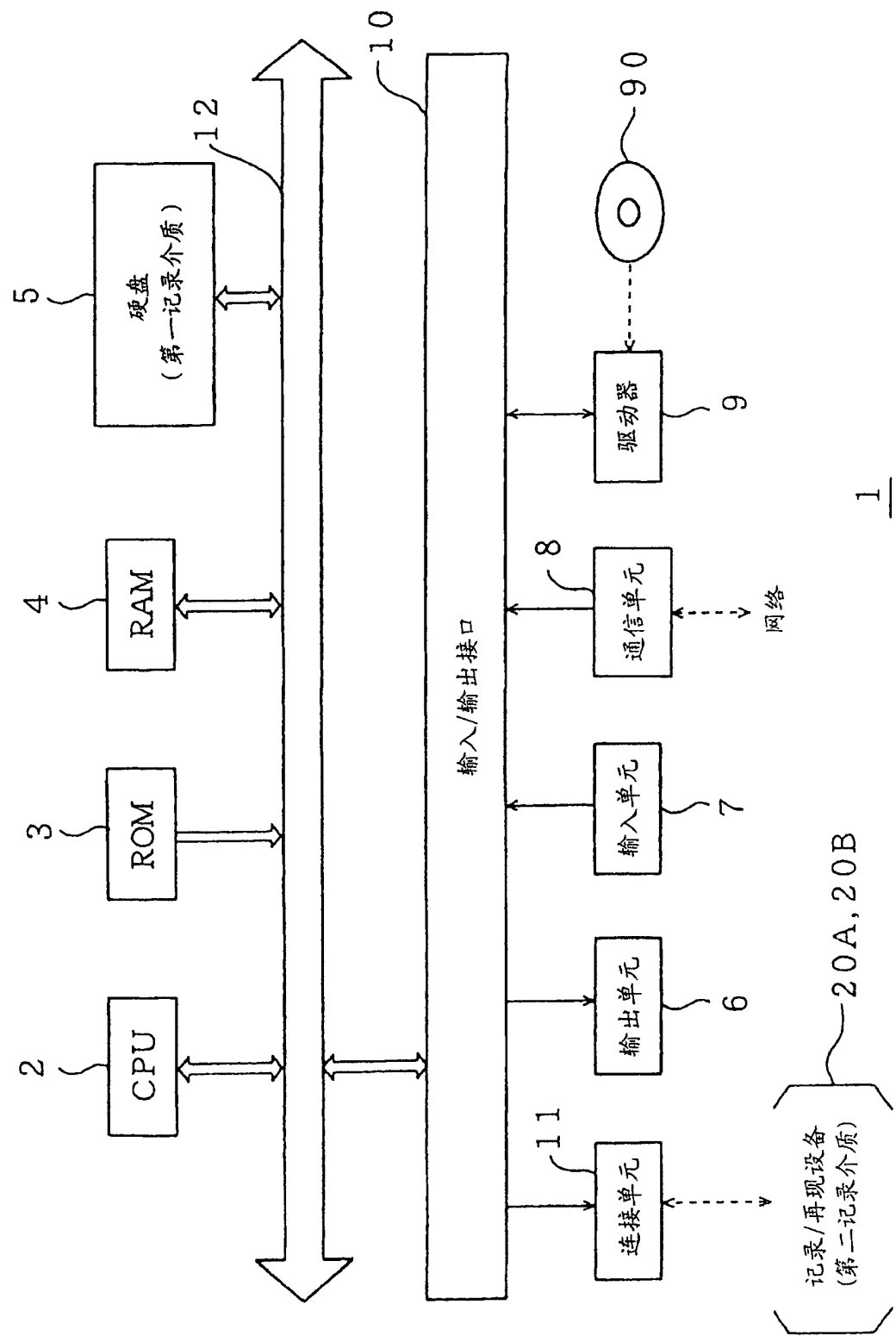


图 6

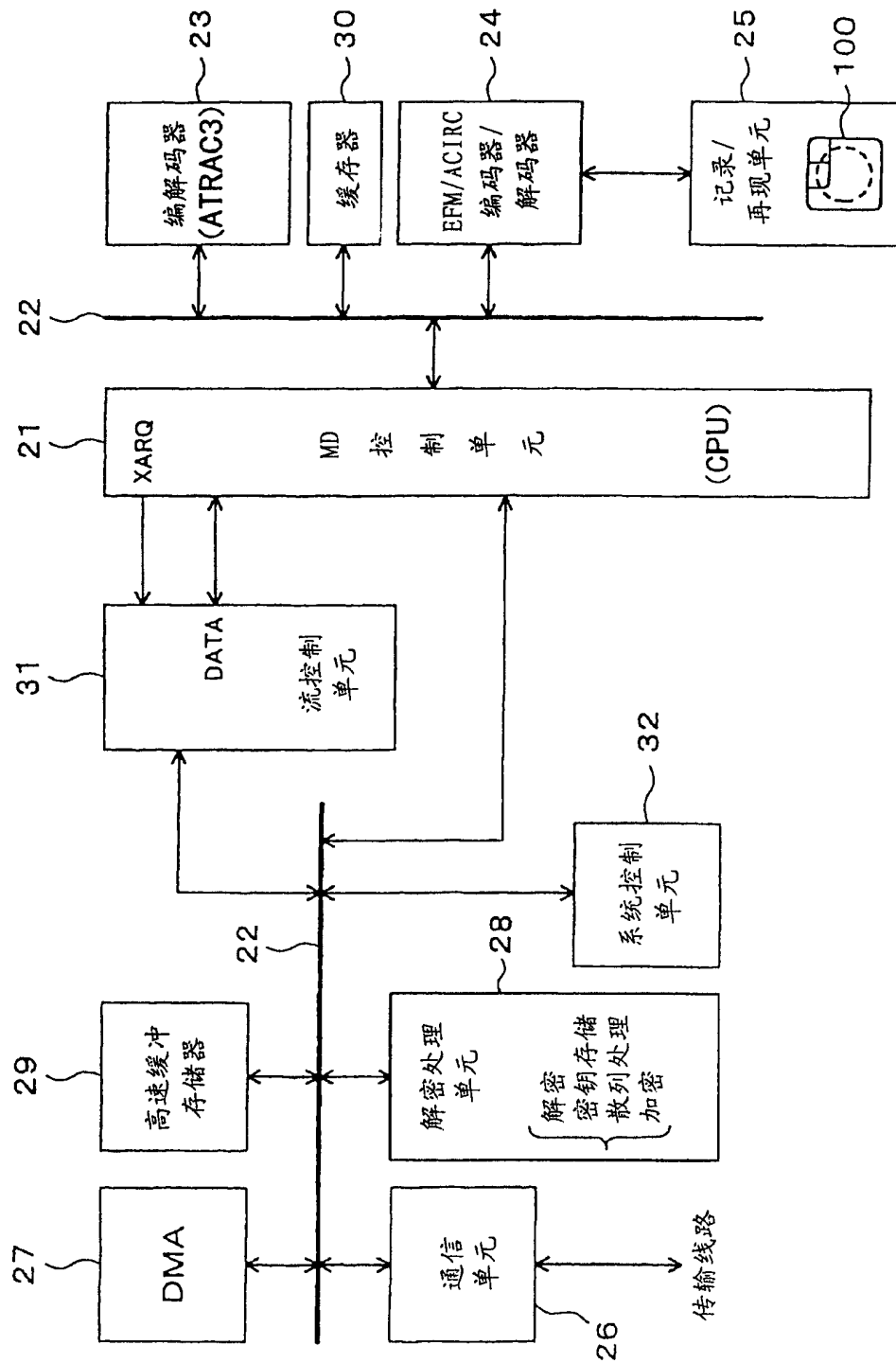
20A

图 7

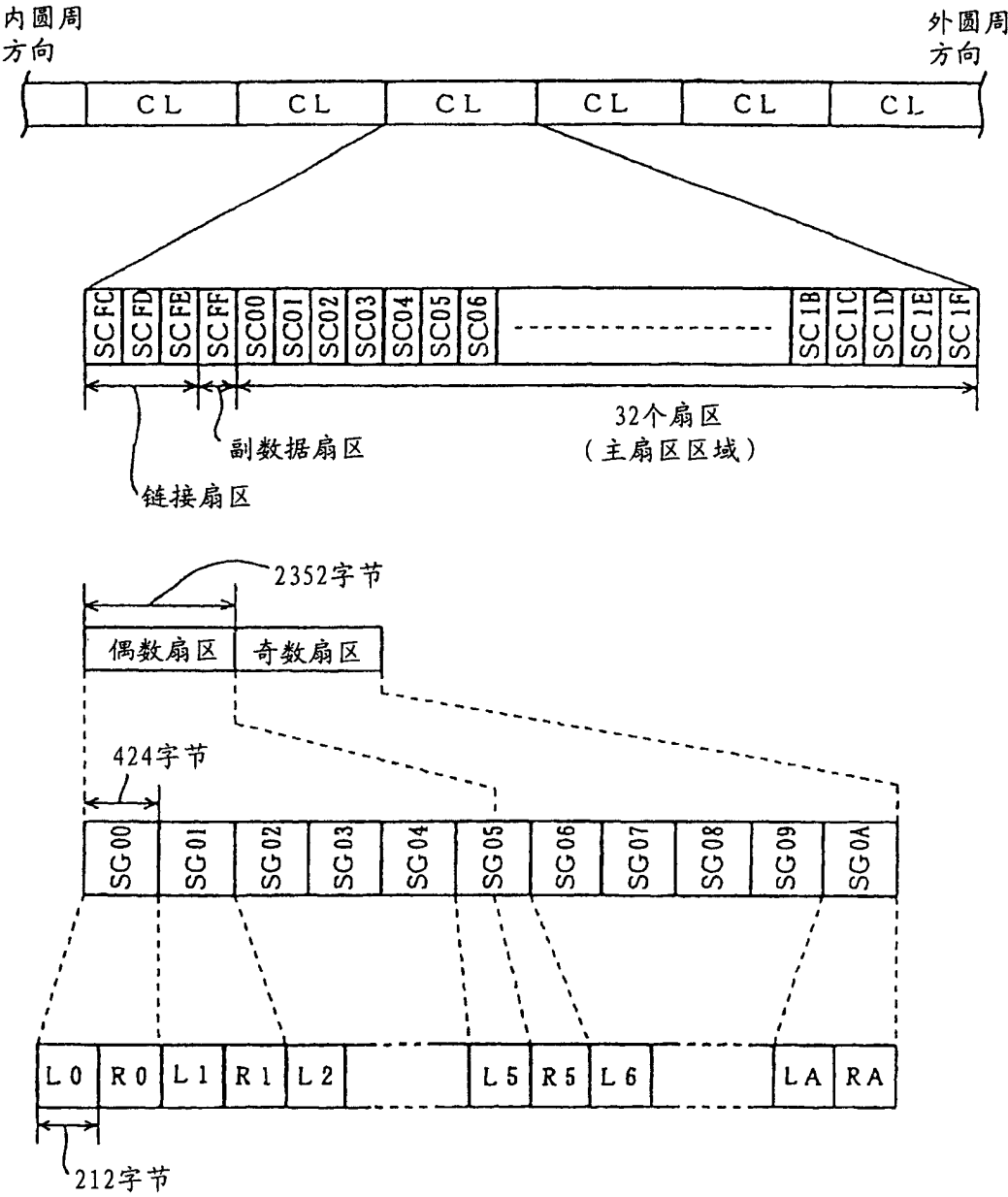


图 8

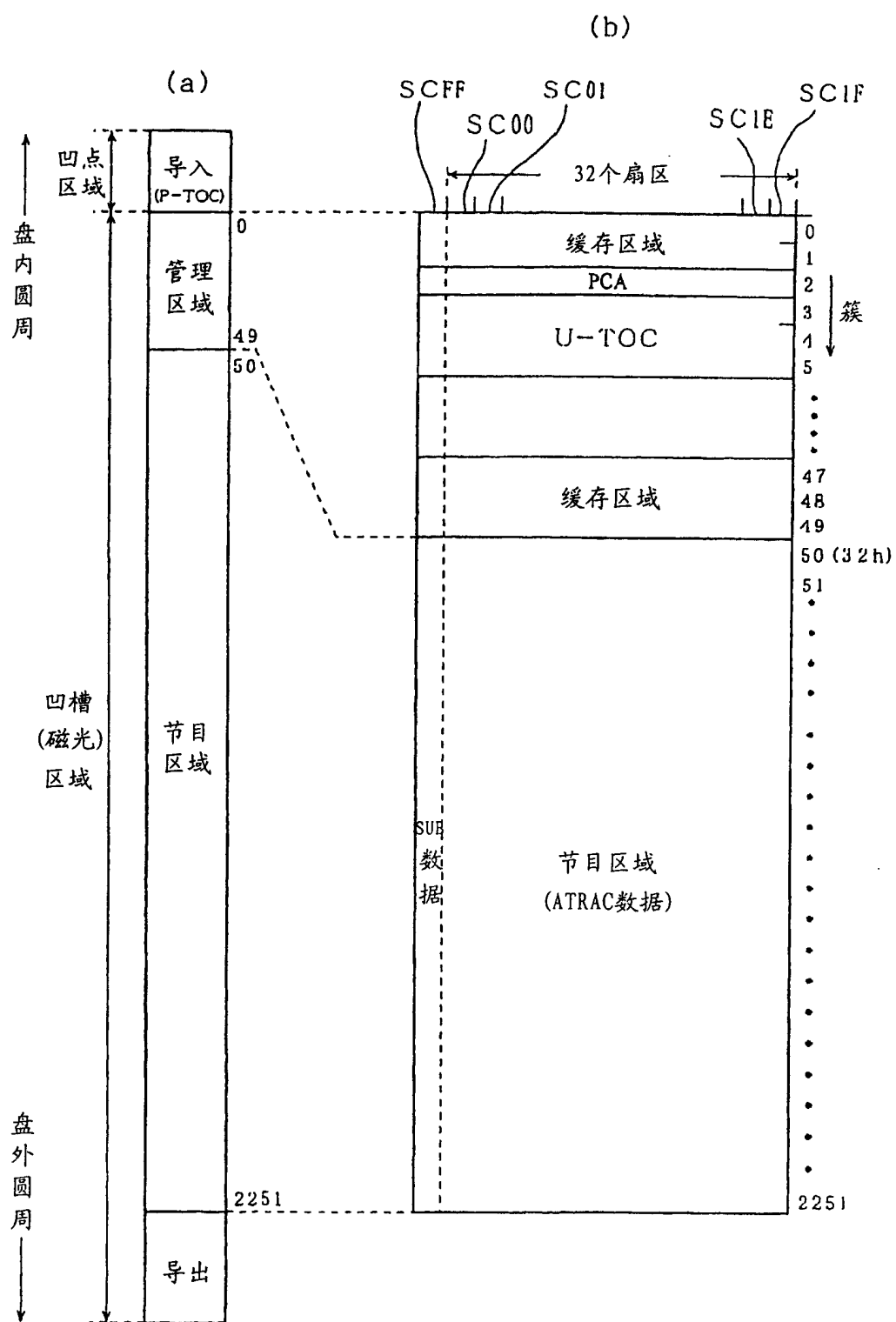


图 9

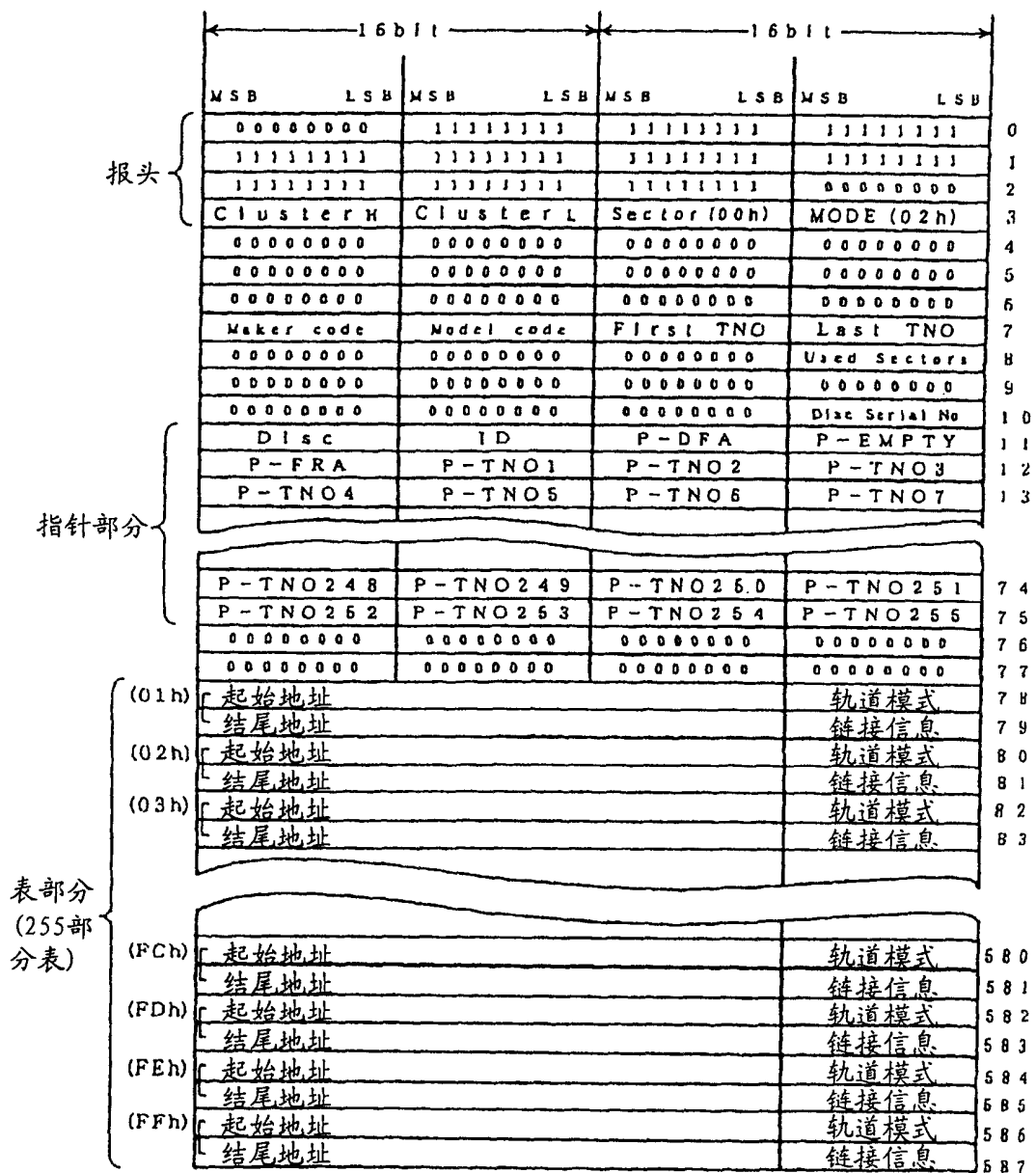


图 10

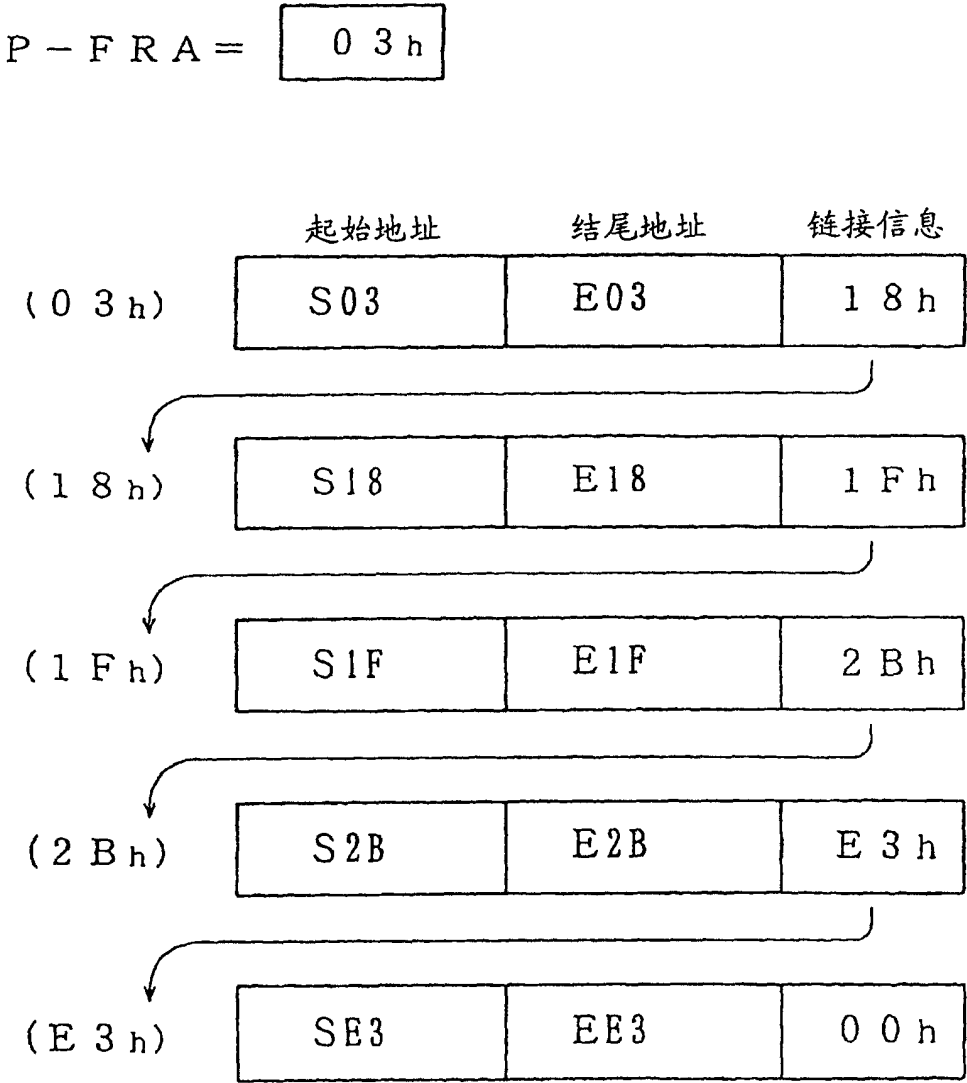


图 11

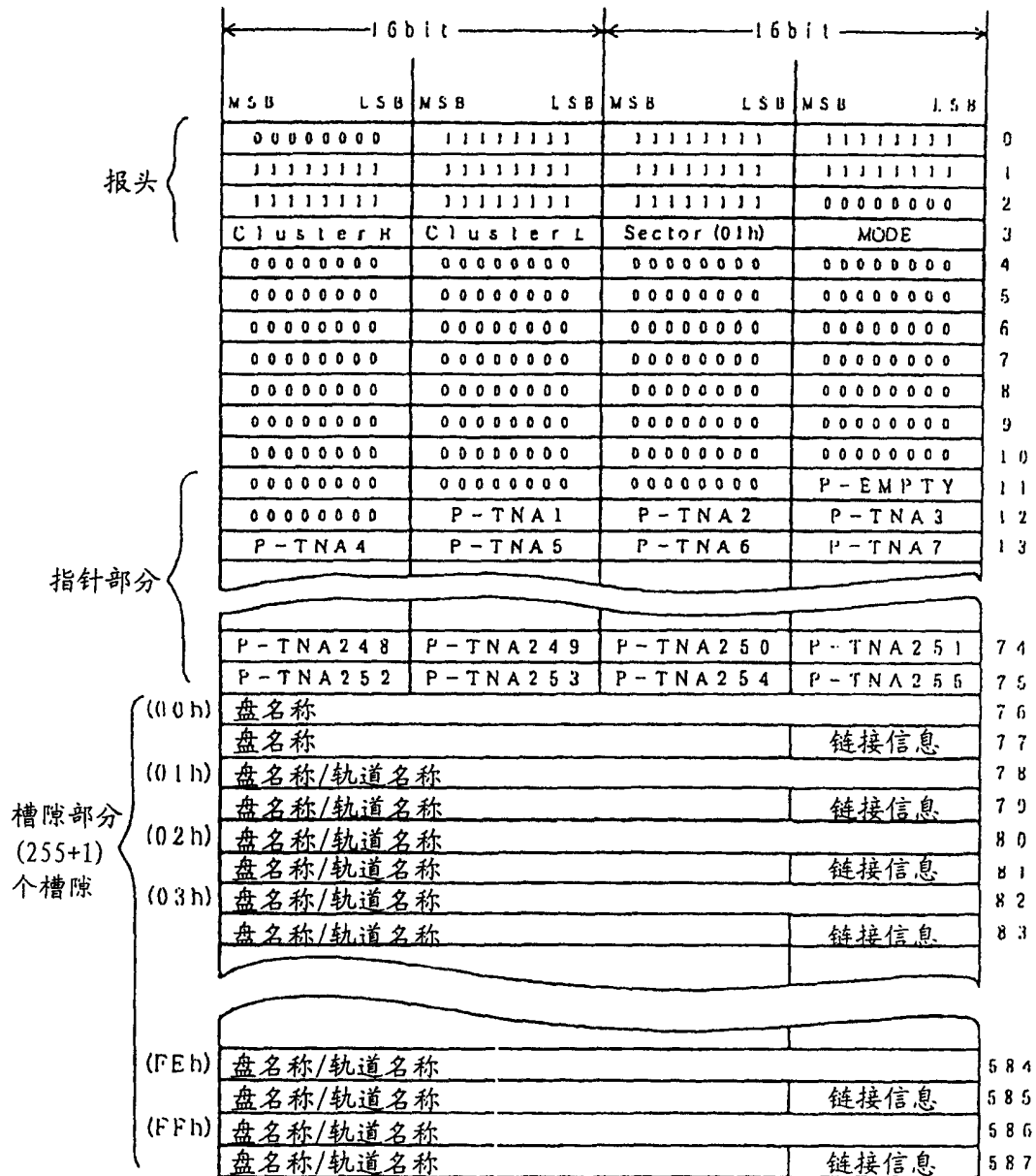


图 12

典型的验证处理过程

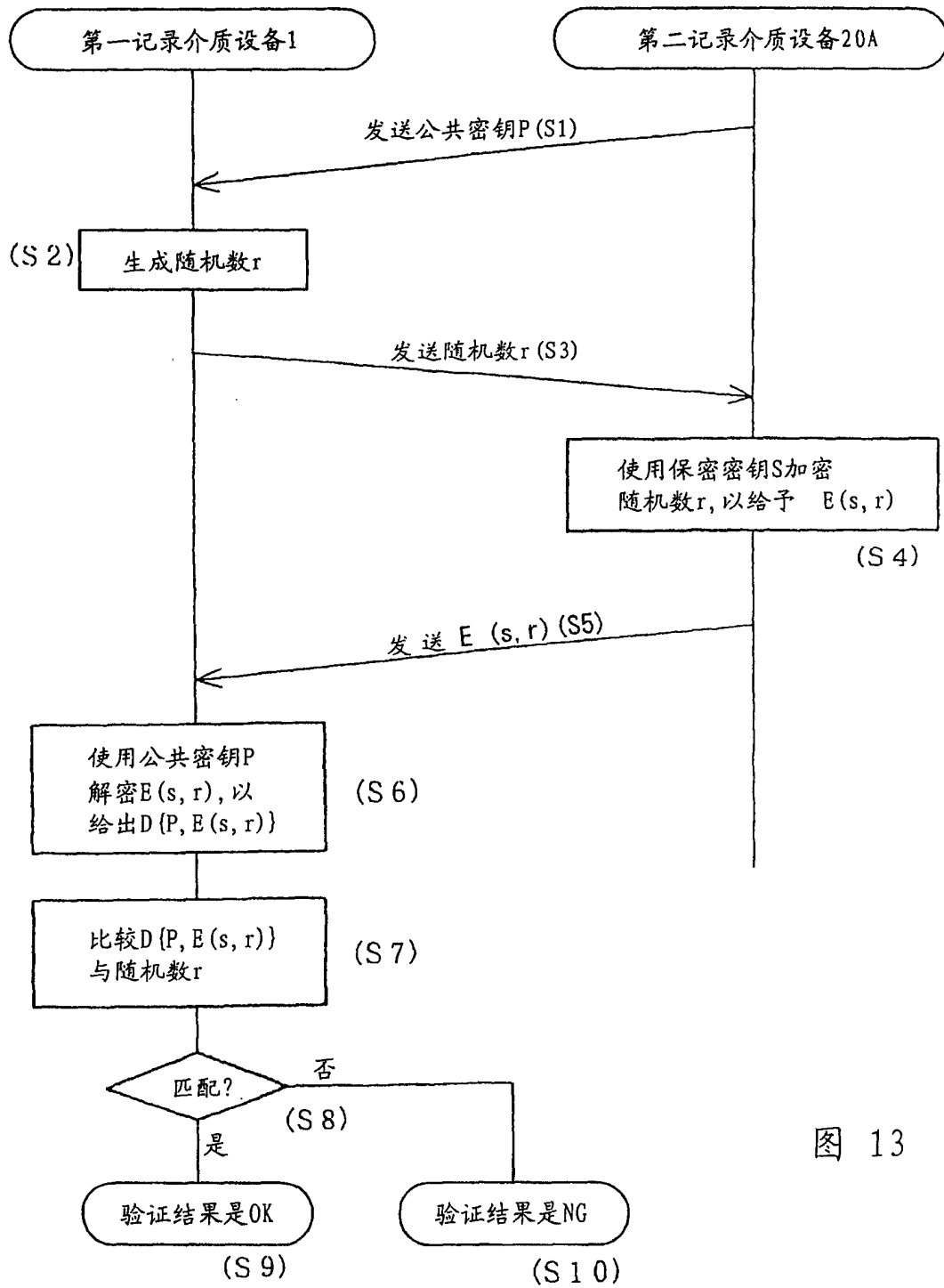


图 13

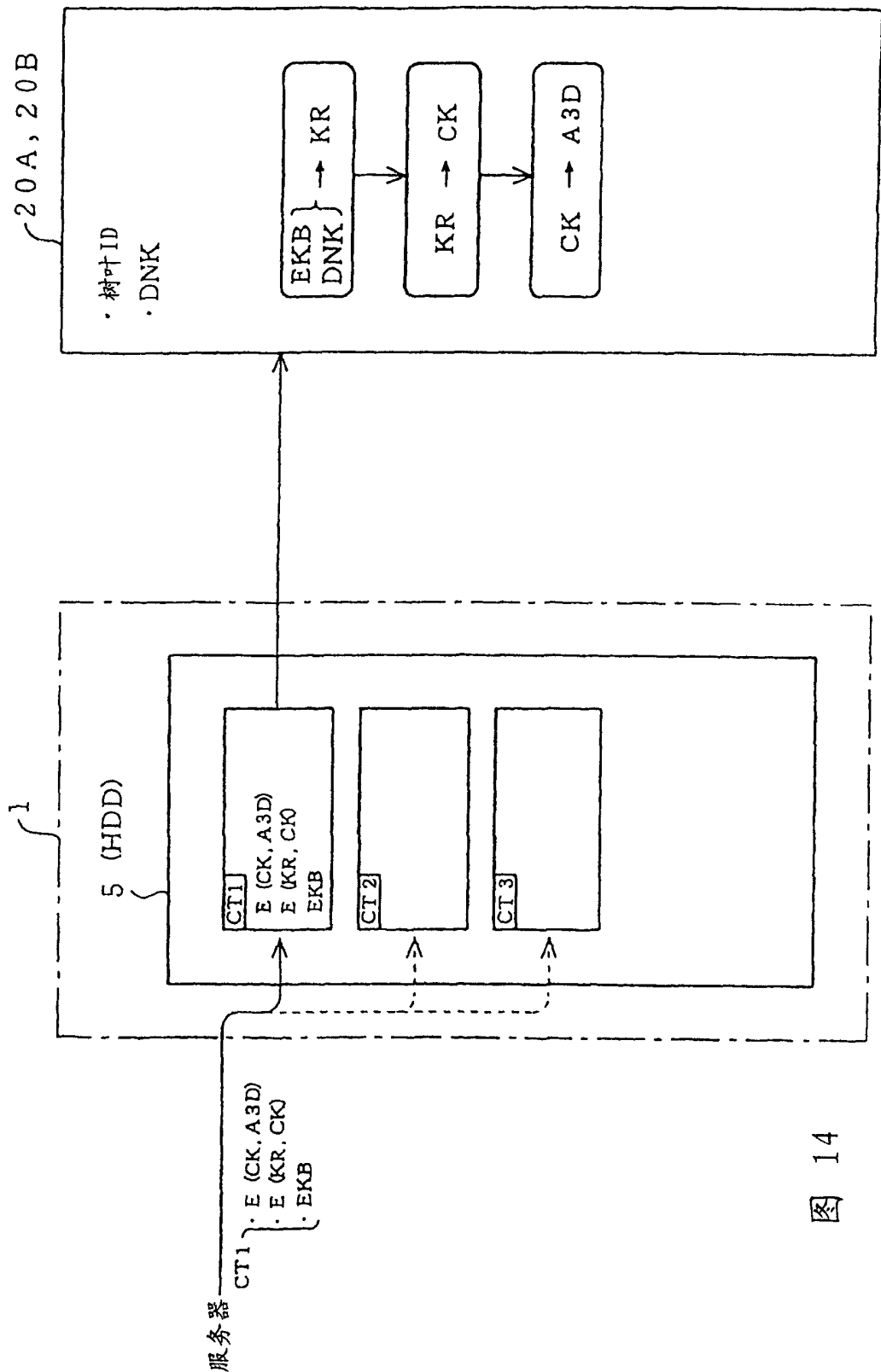


图 14

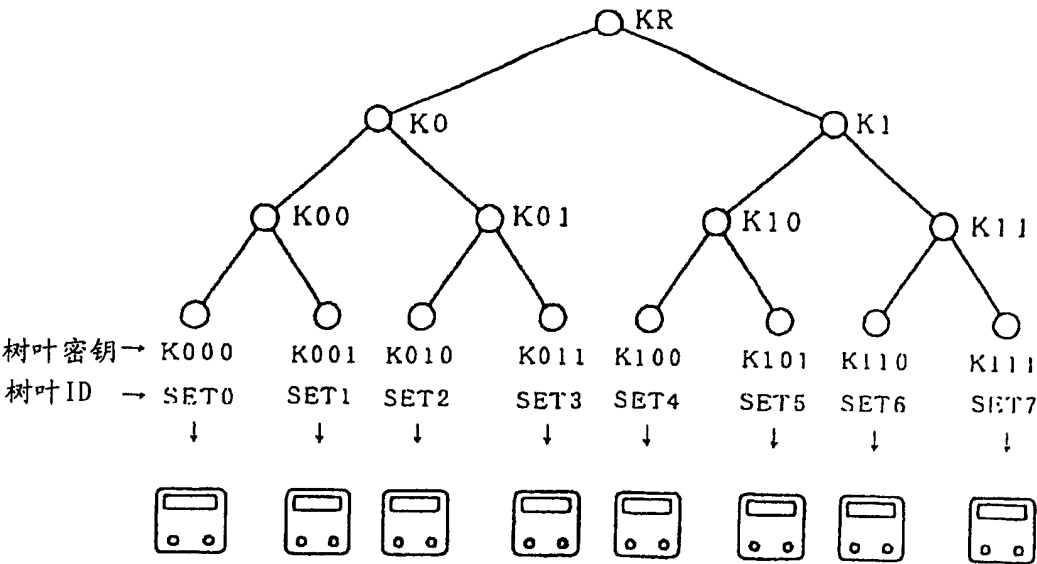
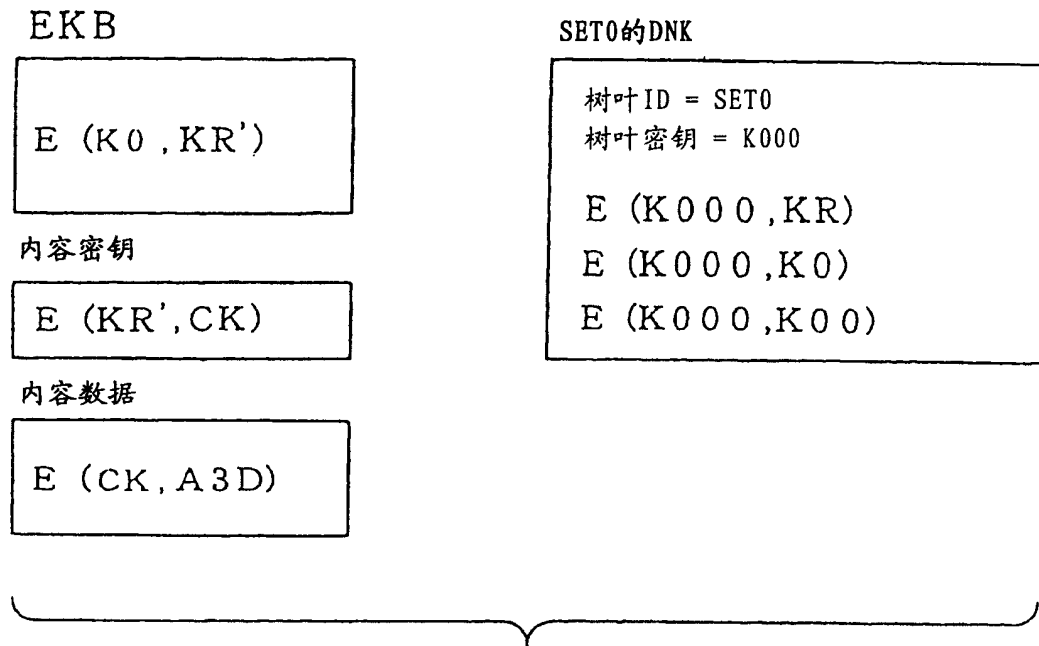


图 15A

树叶ID = SET0
使用树叶密钥加密的KR--E (K000, KR)
使用树叶密钥加密的K0--E (K000, K0)
使用树叶密钥加密的K00--E (K000, K00)
树叶密钥 = K000

图 15B



- (1) 在解密中使用树叶密钥K000, 产生节点K0, $D\{K000, E(K000, K0)\} = K0$
- (2) 在解密中使用节点密钥K0, 产生树根密钥KR', $D\{K0, E(K0, KR')\} = KR'$
- (3) 在解密中使用树根密钥KR', 产生内容密钥CK, $D\{KR', E(KR', CK)\} = CK$
- (4) 在解密中使用内容密钥CK, 产生内容数据A3D, $D\{CK, E(CK, A3D)\} = A3D$

图 16

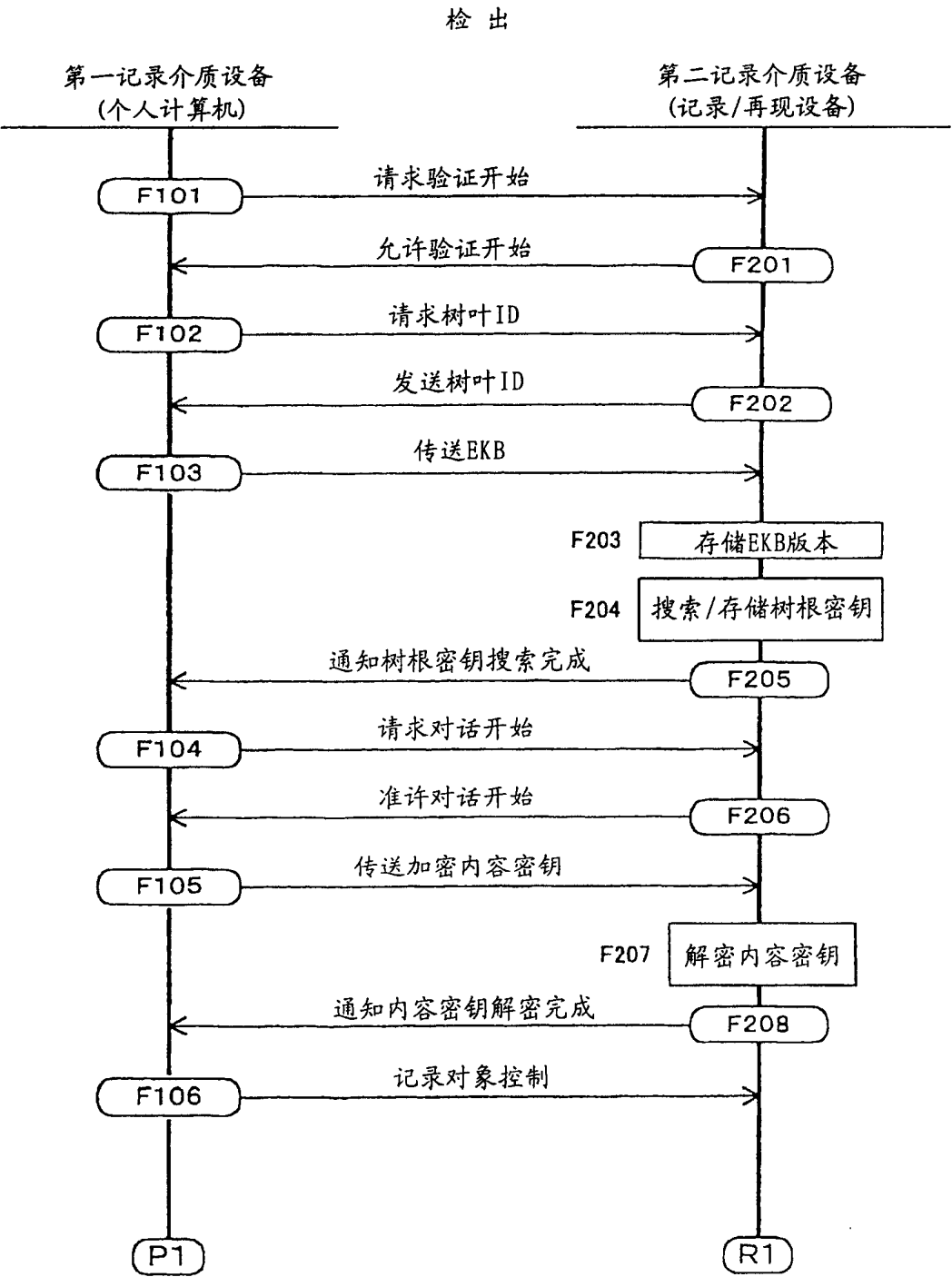
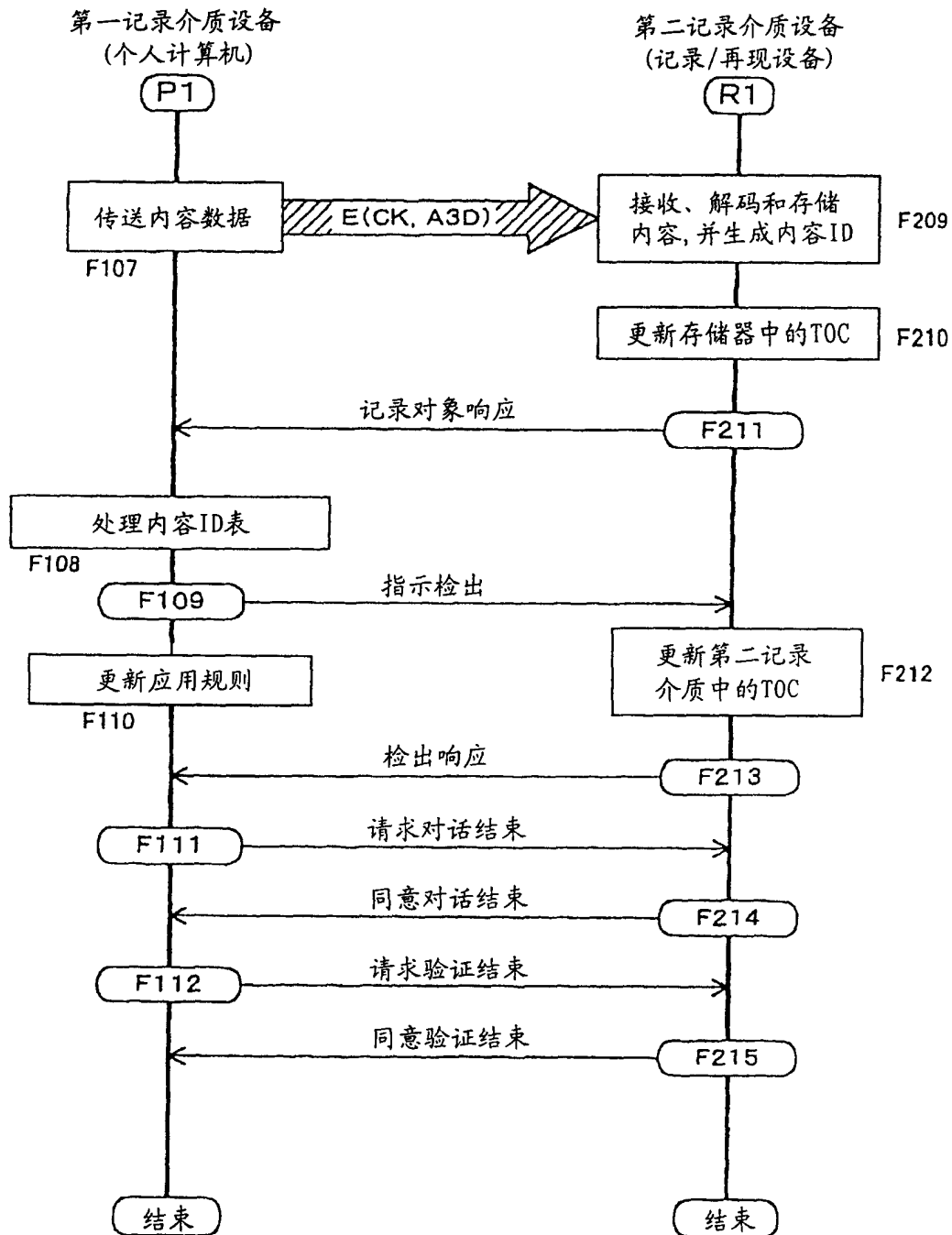


图 17



偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c类型: 控制							
:	:								:							
0Ah	操作码: 记录对象															
0Bh	通信结果															
0Ch	保留															
0Dh																
0Eh																
0Fh	通信对象设备的识别码															
10h																
11h	第二记录介质的检出内容的轨道数															
12h																
13h	内容数据类型															
14h	第一记录介质中的内容数据的格式															
15h	第二记录介质中的内容属性															
16h	内容数据长度															
17h																
18h																
19h																
1Ah	内容数据的批数据长度															
1Bh																
1Ch																
1Dh																

图 19

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				响应: 接受				
:					:				
0Ah	操作码: 记录对象								
0Bh	通信结果								
0Ch	保留								
0Dh									
0Eh									
0Fh									
10h	通信对象设备的识别码								
11h	第二记录介质的检出内容的轨道数								
12h									
13h	内容数据类型								
14h	第一记录介质中的内容数据的格式								
15h	第二记录介质中的内容属性								
16h	内容数据长度								
17h									
18h									
19h									
1Ah	内容数据的批数据长度								
1Bh									
1Ch									
1Dh									
1Eh	对话数据 (32字节) (内容ID)								
:									
3Dh									

图 20

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c类型: 控制							
⋮	⋮								⋮							
0Ah	操作码: 检出															
0Bh	通信结果															
0Ch	保留															
0Dh	通信对象设备的识别码															
0Eh																
0Fh	第二记录介质的检出内容的轨道数															
10h																
11h ⋮ 18h	DES CBC (ks,0)															

图 21

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
⋮	⋮								⋮							
0Ah	操作码: 检出															
0Bh	通信结果															
0Ch	保留															
0Dh	通信对象设备的识别码															
0Eh																
0Fh	第二记录介质上的检出内容的轨道数															
10h																

图 22

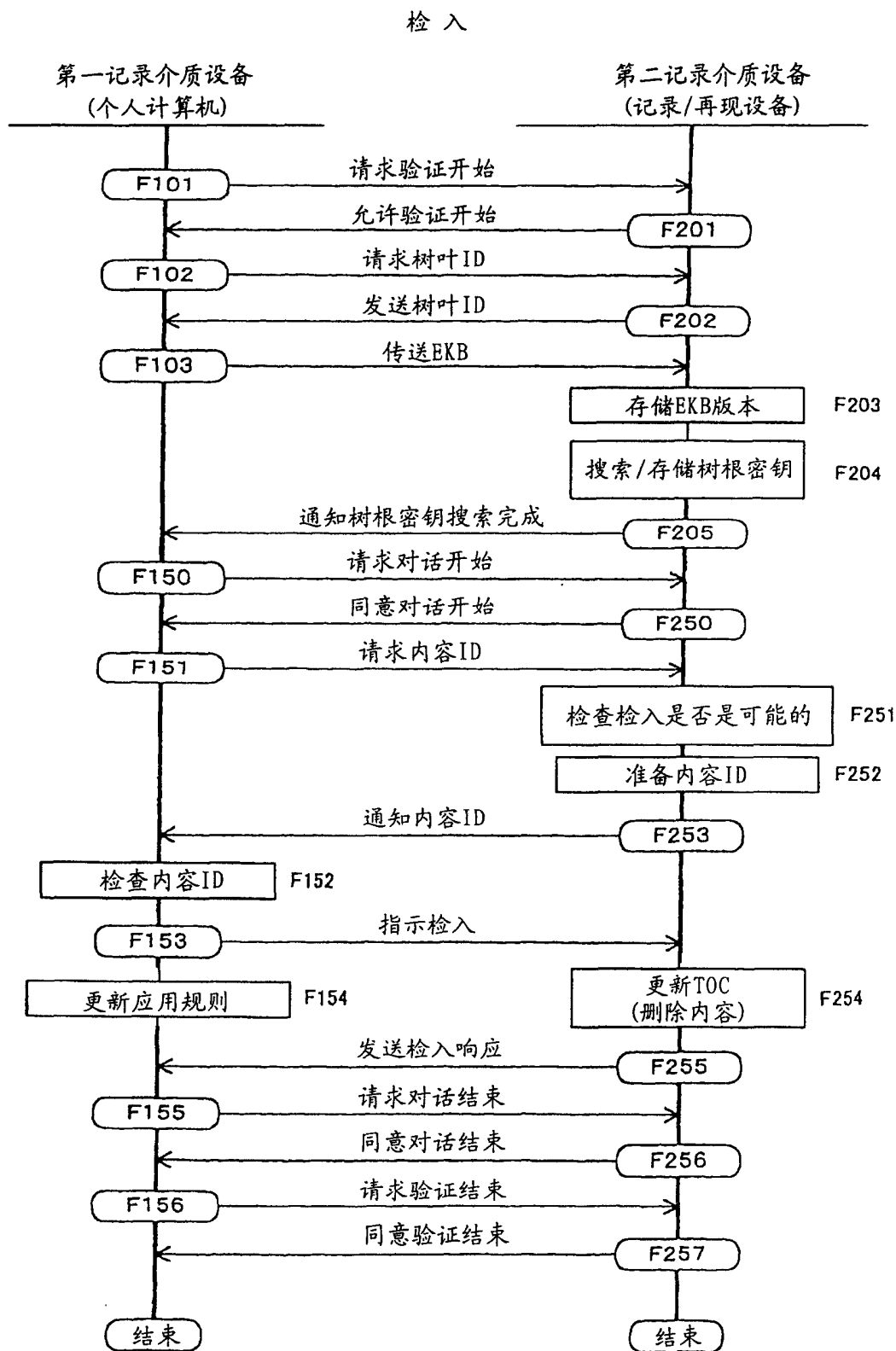


图 23

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
⋮	⋮								
0Ah	操作码: 检入								
0Bh	通信结果								
0Ch	子函数								
0Dh	通信对象设备的识别码								
0Eh									
0Fh	第二记录介质的检入内容的轨道数								
10h									

图 24

值	子函数
00h	内容ID
01h	保留
其它	预付信息

图 25

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				响应: 接受				
⋮	⋮				⋮				
0Ah	操作码: 检入								
0Bh	通信结果								
0Ch	子函数								
0Dh	通信对象设备的识别码								
0Eh									
0Fh	第二记录介质的检入内容的轨道数								
10h									
11h	散列MAC (内容ID)								
12h									
13h									
14h									
15h									
16h									
17h									
18h									

图 26

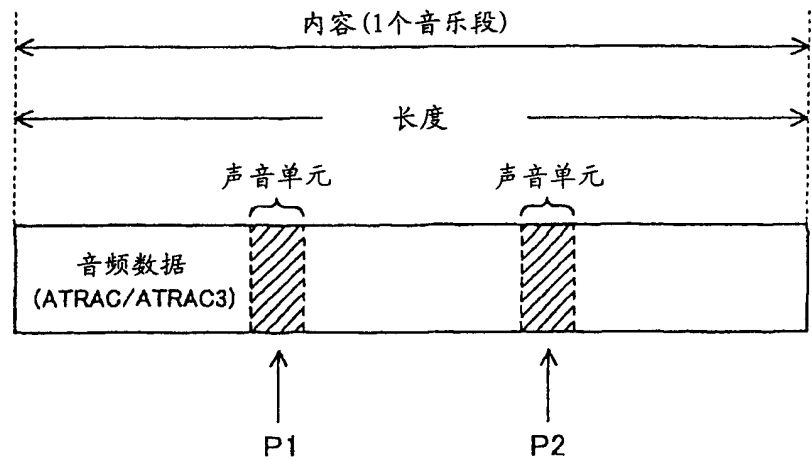


图 27

内容 ID 关联表

由PC应用程序设置的内容ID1	由第二记录介质 设备设置的内容ID1
由PC应用程序设置的内容ID2	由第二记录介质 设备设置的内容ID2
由PC应用程序设置的内容ID3	由第二记录介质 设备设置的内容ID3

图 28

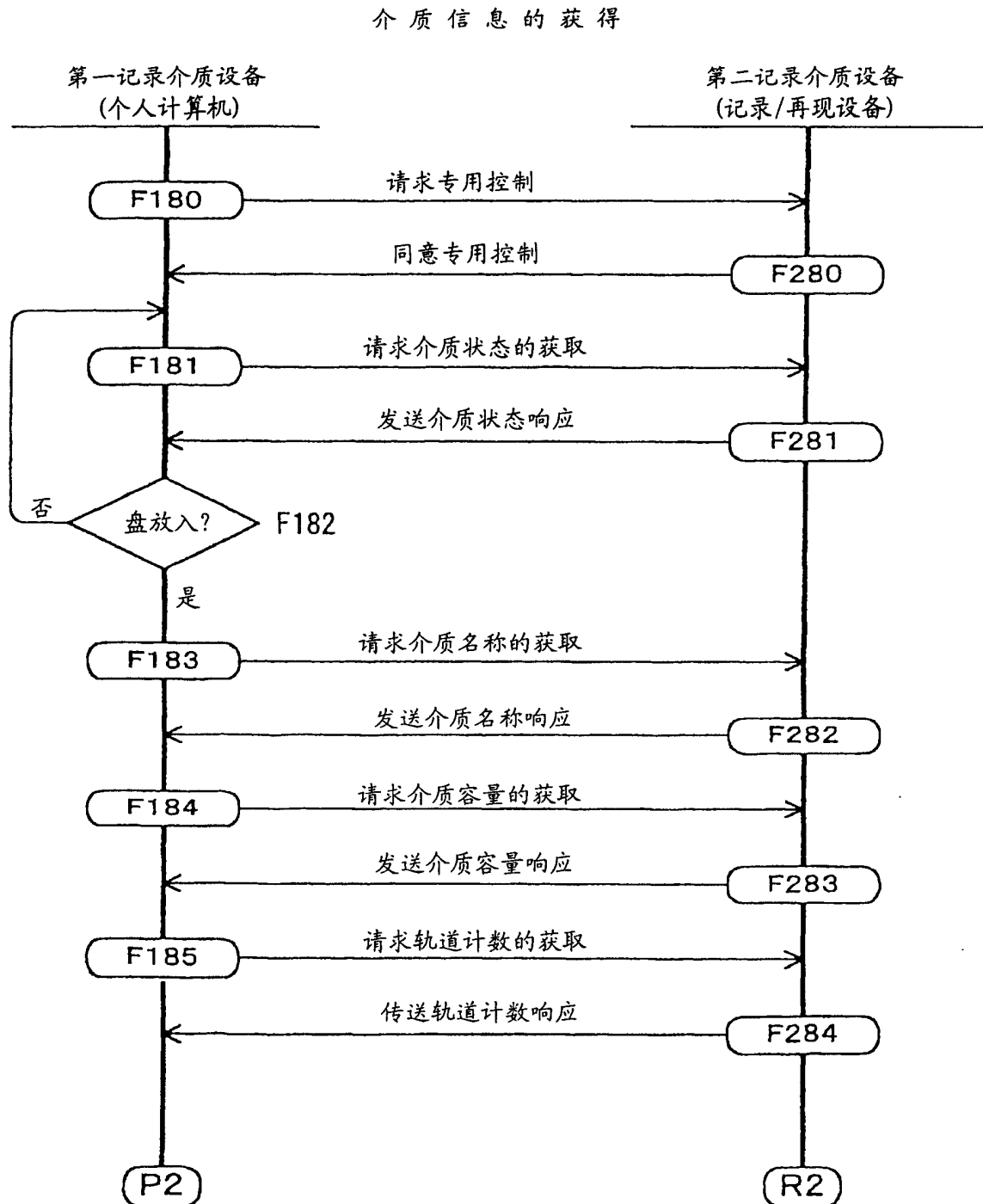


图 29

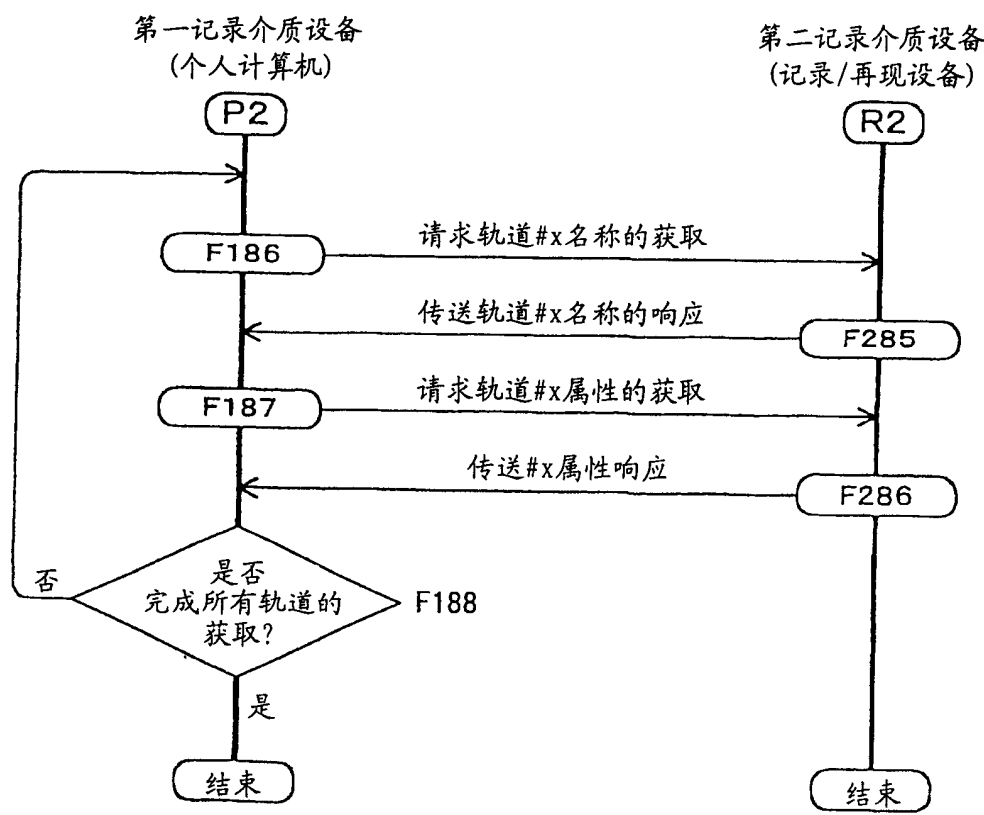


图 30

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型				子单元ID				
02h	保留								
03h	优先权								

图 31

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型				子单元ID				
02h	保留								
03h	优先权: 00h								

图 32

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型					子单元ID			
02h	<OpCode>读描述符								
03h	描述符类型: [盘子单元状态描述符]								
04h	参考方法: [信息块参考]								
05h	等级数								
06h	描述符类型: [信息块, 类型和计数]								
07h	信息块类型: [普通盘子单元状态区域信息块]								
08h									
09h	实例计数: [0]								
0Ah	描述符类型: [信息块, 类型和计数]								
0Bh	信息块类型: [介质和编辑状态信息块]								
0Ch									
0Dh	实例计数: [0]								
0Eh	读出结果状态								
0Fh	保留								
10h	数据长度: [全部]								
11h									
12h	地址: [忽略]								
13h									

图 33

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读描述符															
03h	描述符类型: [盘子单元状态描述符]															
04h	参考方法: [信息块参考]															
05h	等级数															
06h	描述符类型: [信息块, 类型和计数]															
07h	信息块类型: [普通盘子单元状态区域信息块]															
08h																
09h	实例计数: [0]															
0Ah	描述符类型: [信息块, 类型和计数]															
0Bh	信息块类型: [介质和编辑状态信息块]															
0Ch																
0Dh	实例计数: [0]															
0Eh	读出结果状态															
0Fh	保留															
10h	数据长度: [介质和编辑状态信息块的大小]															
11h																
12h	地址															
13h																
14h	组合的长度															
15h																
16h	信息块类型: [介质和编辑状态信息块]															
17h																
18h	第一字段长度:															
19h																
1Ah	驱动的盘				错误条件				保留							
1Bh	取消状态															
1Ch	差异		自动更新		保留											

图 34

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [对象位置]								
05h	列表ID: [文本数据库列出盘标题列表]								
06h									
07h	对象位置: [0=UTOC1]								
08h									
09h	描述符类型: [信息块, 类型和计数]								
0Ah	信息块类型: [未加工文本信息块]								
0Bh									
0Ch	实例计数								
0Dh	读出结果								
0Eh	保留								
0Fh	数据长度: [全部]								
10h									
11h	地址: [忽略]								
12h									

图 35

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				响应: 接受				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [对象位置]								
05h	列表ID: [文本数据库列出盘标题列表]								
06h									
07h	对象位置: [0=UTOC1]								
08h									
09h	描述符类型: [信息块, 类型和计数]								
0Ah	信息块类型: [未加工文本信息块]								
0Bh									
0Ch	实例计数								
0Dh	读出结果状态: [没问题]								
0Eh	保留								
0Fh	数据长度: [未加工文本信息块的大小]								
10h									
11h	地址: [偏移=0]								
12h									
13h	组合的长度: [N+4字节]								
14h									
15h	信息块类型: [未加工文本信息块]								
16h									
17h	第一字段长度: [N字节]								
18h									
19h	N字节盘标题文本								
⋮									
(18+N)h									

图 36

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [列表ID]								
05h	列表ID: [树根内容列表]								
06h									
07h	描述符类型: [信息块, 类型和计数]								
08h	信息块类型: [AV对象型特定容量信息块]								
09h									
0Ah	实例计数: [0=音频]								
0Bh	读出结果状态								
0Ch	保留								
0Dh	数据长度: [全部]								
0Eh									
0Fh	地址: [忽略]								
10h									

图 37

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [列表ID]															
05h	列表ID: [树根内容列表]															
06h																
07h	描述符类型: [信息块, 类型和计数]															
08h	信息块类型: [AV对象类型特定容量信息块]															
09h																
0Ah	实例计数: [0=音频]															
0Bh	读出结果状态: [没问题]															
0Ch	保留															
0Dh	数据长度: [AV对象类型特定容量信息块的大小]															
0Eh																
0Fh	地址															
10h																
11h	组合的长度: 27字节															
12h																
13h	信息块类型: [AV对象类型特定容量信息块]															
14h																
⋮	⋮															

(继续至图 39)

图 38

(接图 38)

⋮	⋮
15h	第一字段长度: 23字节
16h	
17h	对象类型: [音频轨道]
18h	容量格式指示符: [时间]
19h	总的回放容量长度
1Ah	
1Bh	小时
1Ch	
1Dh	分钟
1Eh	秒
1Fh	帧
20h	最大记录容量长度
21h	
22h	小时
23h	
24h	分钟
25h	秒
26h	帧
27h	剩余记录容量长度
28h	
29h	小时
2Ah	
2Bh	分钟
2Ch	秒
2Dh	帧

图 39

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [列表ID]								
05h	列表ID: [音频子内容列表]								
06h									
07h	描述符类型: [信息块, 类型和计数]								
08h	信息块类型: [条目信息块的数目]								
09h									
0Ah	实例计数: [0]								
0Bh	读出结果状态								
0Ch	保留								
0Dh	数据长度: [全部]								
0Eh									
0Fh	地址: [忽略]								
10h									

图 40

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [列表ID]															
05h	列表ID: [音频子内容列表]															
06h																
07h	描述符类型: [信息块, 类型和计数]															
08h	信息块类型: [条目信息块的数目]															
09h																
0Ah	实例计数: [0]															
0Bh	读出结果状态: [没问题]															
0Ch	保留															
0Dh	数据长度: [条目信息块数目的大小]															
0Eh																
0Fh	地址															
10h																
11h																
12h	组合的长度															
13h	信息块类型: [条目信息块的数目]															
14h																
15h	第一长度															
16h																
17h	条目数: [轨道数]															
18h																

图 41

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c类型: 控制							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [文本数据库列表音频标题UTOC1]															
06h																
07h																
08h	对象位置: [第N轨道]															
09h	描述符类型: [信息块, 类型和计数]															
0Ah	信息块类型: [未加工文本信息块]															
0Bh																
0Ch	实例计数															
0Dh	读出结果															
0Eh	保留															
0Fh	数据长度: [全部]															
10h																
11h	地址: [忽略]															
12h																

图 42

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [文本数据库列表音频标题UTOC1]															
06h																
07h	对象位置: [第N轨道]															
08h																
09h	描述符类型: [信息块, 类型和计数]															
0Ah	信息块类型: [未加工文本信息块]															
0Bh																
0Ch	实例计数															
0Dh	读出结果状态: [没问题]															
0Eh	保留															
0Fh	数据长度: [未加工文本信息块大小=N+6字节]															
10h																
11h	地址															
12h																
13h	组合的长度: [M+4字节]															
14h																
15h	信息块类型: [未加工文本信息块]															
16h																
17h	第一字节长度: [M字节]															
18h																
19h	M字节音频轨道标题文本															
⋮																
⋮																
(18+M)h																

图 43

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c类型: 控制							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [音频子内容列表]															
06h																
07h	对象位置: [第N轨道]															
08h																
09h	读出结果															
0Ah	保留															
0Bh	数据长度: [1字节]															
0Ch																
0Dh	地址: [盘子单元对象属性的指针]															
0Eh																

图 44

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				响应: 接受				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [对象位置]								
05h	列表ID: [音频子内容列表]								
06h									
07h	对象位置: [第N轨道]								
08h									
09h	读出结果状态: [没问题]								
0Ah	保留								
0Bh	数据长度: [1字节]								
0Ch									
0Dh	地址: [盘子单元对象属性的指针]								
0Eh									
0Fh	盘子单元对象属性: [内容锁定]								

图 45

偏移 (字节)	MSB								LSB
	7	6	5	4	3	2	1	0	
00h	CTS				c类型: 控制				
01h	子单元类型					子单元ID			
02h	<OpCode>读信息块								
03h	等级数								
04h	描述符类型: [对象位置]								
05h	列表ID: [音频子内容列表]								
06h									
07h									
08h	对象位置: [第N轨道]								
09h									
0Ah	信息块类型: [音频记录参数信息块]								
0Bh									
0Ch									
0Dh	实例计数								
0Eh	读出结果								
0Fh	保留								
10h	数据长度: [全部]								
11h									
12h									
	地址: [忽略]								

图 46

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [音频子内容列表]															
06h																
07h																
08h	对象位置: [第N轨道]															
09h	描述符类型: [信息块, 类型和计数]															
0Ah	信息块类型: [音频记录参数信息块]															
0Bh																
0Ch	实例计数															
0Dh	读出结果状态: [没问题]															
0Eh	保留															
0Fh	数据长度: [未加工文本信息块大小=10字节]															
10h																
11h	地址: [偏移=0]															
12h																
13h	组合的长度: [8字节]															
14h																
15h	信息块类型: [音频记录参数信息块]															
16h																
17h	第一字节长度: [4字节]															
18h																
19h	音频记录抽样率: [44.1KHz]															
1Ah	音频记录抽样大小: [16比特]															
1Bh	音频记录压缩模式: [ATRAC]															
1Ch	音频记录通道模式: [立体声]															

图 47

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								c类型: 控制							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [音频子内容列表]															
06h																
07h																
08h	对象位置: [第N轨道]															
09h	描述符类型: [信息块, 类型和计数]															
0Ah	信息块类型: [大小指示符信息块]															
0Bh																
0Ch	实例计数															
0Dh	读出结果															
0Eh	保留															
0Fh	数据长度: [全部]															
10h																
11h	地址: [忽略]															
12h																

图 48

偏移 (字节)	MSB								LSB							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
00h	CTS								响应: 接受							
01h	子单元类型								子单元ID							
02h	<OpCode>读信息块															
03h	等级数															
04h	描述符类型: [对象位置]															
05h	列表ID: [音频子内容列表]															
06h																
07h	对象位置: [第N轨道]															
08h																
09h	描述符类型: [信息块, 类型和计数]															
0Ah	信息块类型: [大小指示符信息块]															
0Bh																
0Ch	实例计数															
0Dh	读出结果状态: [没问题]															
0Eh	保留															
0Fh	数据长度: [大小指示符信息块的大小=12字节]															
10h																
11h	地址: [偏移=0]															
12h																
13h	组合的长度: [10字节]															
14h																
15h	信息块类型: [大小指示符信息块]															
16h																
17h	第一字节长度: [6字节]															
18h																
19h	大小指示符类型: [H M S F]															
1Ah	小时															
1Bh																
1Ch	分钟															
1Dh	秒															
1Eh	帧															

图 49