

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 12/14 (2006.01)

G11B 20/10 (2006.01)

H04N 5/913 (2006.01)



[12] 发明专利说明书

专利号 ZL 200310118678.1

[45] 授权公告日 2007 年 2 月 14 日

[11] 授权公告号 CN 1300710C

[22] 申请日 2003.11.28

[21] 申请号 200310118678.1

[30] 优先权

[32] 2002.11.29 [33] JP [31] 348925/2002

[73] 专利权人 株式会社东芝

地址 日本东京都

[72] 发明人 小岛正 山田尚志 加藤拓 石原淳
平良和彦

[56] 参考文献

CN1154551A 1997.7.16

WO2002/047081A 2002.6.13

审查员 赵 妍

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 李 强

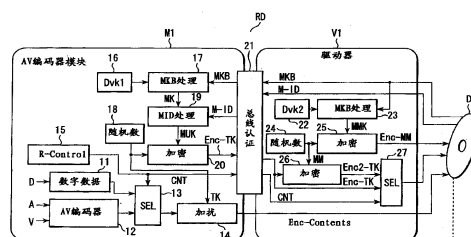
权利要求书 5 页 说明书 20 页 附图 14 页

[54] 发明名称

内容管理方法和记录装置

[57] 摘要

在一种内容管理方法中，通过第一密钥(TK)对内容数据进行加密，通过多种第二密钥(MUK)对第一密钥进行加密，通过一个第三密钥(MM)对加密后的第一密钥(Enc-TK)进行多重加密，并且通过一个第四密钥(MMK)对第三密钥进行加密。这些加密后的内容数据(Enc-Contents)、一个媒体密钥(为通过第二密钥加密后的第一密钥(Enc-TK))和一个移动密钥(为第二和第三密钥多重加密后的第一密钥(Enc2-MM))被存储在一个记录媒体中，由第四密钥加密后的第三密钥(Enc-MM)被记录在一个安全区域内。此管理方法通过所述移动密钥和所述媒体密钥而管理。



1. 一种内容管理方法，其特征在于包括：
通过第一密钥（TK）对内容数据进行加密；
通过预定的多种第二密钥（MUK）对第一密钥进行加密；
通过第三密钥（MM）对所述加密后的第一密钥（Enc-TK）进行多重加密；
通过预定的第四密钥（MMK）对第三密钥进行加密；以及
在记录媒体中记录通过第一密钥加密后的内容数据（Enc-Contents），通过预定的多种第二密钥加密后的第一密钥（Enc-TK），以及通过第二和第三密钥（MM）对所述加密后的第一密钥（Enc-TK）进行多重加密而获得的第一密钥（Enc2-TK），并在该记录媒体的安全区域中记录通过第四密钥加密的第三密钥（Enc-MM）。
2. 如权利要求 1 所述的内容管理方法，其特征在于所述的第一密钥（TK）有多个，所述的内容数据有多个，并且其中的每一个被单独加密，所产生的加密后的第一密钥（Enc-TK）也有多个。
3. 如权利要求 1 所述的内容管理方法，其特征在于所述的第三密钥（MM）根据多个第一密钥的数量也有多个，而所述的多个第一密钥是根据多个内容数据的数量而提供的，所述的多个加密的第一密钥（Enc-TK）被记录以通过多个第三密钥（MM）而被分别进行多重加密。
4. 如权利要求 1 所述的内容管理方法，其特征在于，其中记录有所述加密的内容数据（Enc-Contents）、通过第二密钥加密的第一密钥（Enc-TK）、通过第二和第三密钥多重加密的第一密钥（Enc2-TK）的记录媒体与其中存在一个安全区域并在该安全区域中记录有通过第四密钥加密后的第三密钥（Enc-MM）的记录媒体是相同的。
5. 如权利要求 1 所述的内容管理方法，其特征在于所述第二密钥（MUK）之一是记录媒体的特定信息。

6. 如权利要求 1 所述的内容管理方法, 其特征在于所述的内容管理方法是在一个具有一个编码器模块和一个通过一个认证处理与其通信的驱动模块的记录装置中实施的, 而且所述的第三密钥 (MM) 只在该驱动模块中产生。

7. 如权利要求 1 所述的内容管理方法, 其特征在于通过所述的第二密钥加密后的第一密钥 (Enc-TK) 和通过所述的第二和第三密钥多重加密后的第一密钥 (Enc2-TK) 记录在所述记录媒体的不同记录区中。

8. 如权利要求 1 所述的内容管理方法, 其特征在于当内容数据从第一记录媒体 (D1) 移动到第二记录媒体 (D2) 中时, 所述的内容数据在解密后被再次加密, 该加密的内容数据仅和用于控制内容移动的加密密钥被记录在第二记录媒体中, 记录在第一记录媒体中的用于控制内容移动的加密密钥被删除。

9. 如权利要求 8 所述的内容管理方法, 其特征在于当内容数据从其中仅记录有用于控制内容移动的加密密钥的第二记录媒体 (D2) 移动到第三记录媒体 (D3) 时, 内容数据在解密后被再次加密, 该加密后的内容数据和用于控制内容的移动的加密密钥被记录在所述的第三记录媒体中, 用于控制第二记录媒体中的内容的移动的加密密钥被删除, 从而在记录媒体间执行内容移动处理。

10. 如权利要求 1 所述的内容管理方法, 其特征在于该方法还包括:

通过一个特定的随机数发生器 (24) 产生密钥源数据;

基于指定多个内容数据的信息乘以一个特定的函数, 以产生多个第三密钥 (MM1 至 MMn);

记录作为多个加密后的第一密钥的多重加密后的密钥的多个第三密钥、多个加密后的内容数据以及多重加密后的第一密钥在一个记录媒体中; 以及

通过一个预定的加密密钥, 对由所述随机数发生器产生的密钥源数据进行加密, 然后将加密后的数据记录在该记录媒体中的一个安

全区域内。

11. 如权利要求 1 所述的内容管理方法，其特征在于该方法还包括：

在由第二密钥加密后的第一密钥以及由第二密钥和第三密钥多重加密后的第一密钥各作为独立的文件数据而记录在一个独立的记录区域内的情况下，提供一个加密后的加密密钥文件，该文件具有处于存储区域的密钥文件的开始或预定位置的指示文件密钥数据是由第二密钥加密后的第一密钥还是由第二和第三密钥多重加密后的第一密钥的标识信息，以及指示各个对应密钥文件是否存在的标识信息。

12. 如权利要求 11 所述的内容管理方法，其特征在于所述加密后的加密密钥文件被重复写多次。

13. 如权利要求 1 所述的内容管理方法，其特征在于该方法还包括：

在第一记录媒体（D1）和第二记录媒体的再现处理中，在其上的一个安全区域内记录加密后的内容数据、由第二和第三密钥多重加密后的第一密钥（Enc2-TK）、和由第四密钥加密后的第三密钥，

在第一记录媒体中，读出由第二密钥加密后的第一密钥（Enc-TK），对通过预定的多种第二密钥（MKB，M-ID）加密过的第一密钥进行解密，读出加密后的内容数据（Enc-Contents），并通过解密后的第一密钥对内容数据进行解密，从而执行再现，以及

在第二记录媒体中，从安全区域内读出加密过的第三密钥（Enc-MM），对由预定的多种第四密钥（MMK）加密过的第三密钥进行解密，读出由第二和第三密钥多重加密后的第一密钥（Enc2-TK），以检测出由第三密钥（MM）解密后的及由第二密钥加密后的第一密钥（Enc-TK），对由预定的多种第二密钥（MUK）加密后的第一密钥进行解密，并通过解密后的第一密钥（TK）对加密后的内容数据（Enc-Contents）进行解密，从而执行再现。

14. 一种记录装置，其特征在于该装置包括：

一个加密部分（158），通过第一密钥（TK）对指定的内容数

据进行加密，通过预定的多种第二密钥（MUK）对第一密钥进行加密，通过第三密钥（MM）对所述加密后的第一密钥（Enc-TK）进行多重加密，并通过预定的第四密钥（MMK）对第三密钥进行加密；

记录部分（154、156），在第一记录媒体中记录在加密部分加密过的内容数据（Enc-Contents）、由第二密钥加密后的第一密钥（Enc-TK）、以及由第二和第三密钥多重加密后的第一密钥（Enc2-TK），并将由第四密钥加密后的第三密钥（Enc-MM）记录在一个安全区域内。

15. 如权利要求 14 所述的记录装置，其特征在于该装置还包括：

处理部分（154、156），在内容数据从第一记录媒体（D1）中移动到一个第二记录媒体（D2）中的情况下，在内容数据被解密后对其进行加密，只在第二记录媒体中记录加密后的内容数据和一个用于控制内容移动的加密密钥，并删除记录在第一记录媒体中的用于控制内容移动的加密密钥；以及

在内容数据从其上只记录了如第二记录媒体（D2）中的用于控制内容移动的加密密钥的记录媒体移动到第三记录媒体（D3）的情况下，在内容数据被解密后对其进行再次加密，将加密后的内容数据和用于控制内容移动的加密密钥记录在第三记录媒体中，并删除用于控制作为源媒体的第二记录媒体的内容移动的加密密钥，从而执行记录媒体间内容数据的移动处理。

16. 如权利要求 14 所述的记录装置，其特征在于该装置还包括：

处理部分（154，156），通过多个第一密钥分别对多个内容数据进行加密，通过预定的多种第二密钥对多个第一密钥进行加密，以及

在处理部分通过多个第三加密密钥对加密后的第一密钥进行加密的情况下，通过一个特定的随机数发生器（24）生成密钥源数据，

并且基于指定多个内容数据的信息乘以一个特定函数以生成多个第三密钥（MM1 到 MMn），

所述处理部分将多个第三密钥记录为多个加密后的第一密钥，在一个记录媒体中记录多个加密后的内容数据和多重加密后的第一密钥，以及

所述处理部分通过一个预定的加密密钥对由所述随机数发生器生成的密钥源数据进行加密，并将加密后的数据记录在记录媒体的一个安全区域中。

17. 如权利要求 14 所述的记录装置，其特征在于该装置还包括：

处理部分（154，156），在由第二密钥加密后的第一密钥以及由第二密钥和第三密钥多重加密后的第一密钥被分别记录为第一记录媒体的一个独立记录区域中的独立文件数据的情况下，

记录一个加密后的加密密钥文件，该文件具有处于该密钥文件的开始或预定位置的指示文件密钥数据是由第二密钥加密后的第一密钥还是由第二和第三密钥多重加密后的第一密钥的标识信息，以及指示各个对应密钥文件是否存在的标识信息。

内容管理方法和记录装置

技术领域

本发明涉及一种管理内容数据的内容管理方法，一种使用该管理方法的记录和/或再现装置，以及一种其上由该装置记录有内容数据等的记录媒体。更具体地说，本发明涉及一种内容管理方法，一种记录和/或再现装置，能够在允许内容数据进行预定移动的同时防止无限制的非法拷贝，以及一种用于该方法和装置的记录媒体。

背景技术

通常情况下，作为记录数字化信息（如一个文档、一段语音、一幅图像或一个程序）的媒体，光盘（CD）或激光唱盘（LD）用作记录一段语音或一幅图像的媒体。另外，软盘或硬盘用在计算机等中作为记录程序或数据的媒体。除了这些记录媒体外，还开发出了一种大容量记录媒体 DVD（数字多功能光盘）。

在各种这样的数字记录媒体中，在记录过程中数字数据（包括可以解码的压缩或编码数据）是无损记录的。这样，所记录的数据可以很容易地从一个媒体中拷贝到另一个媒体中，而不会例如产生声音损失或降低图像质量。因此，在这些数字记录媒体中，存在一个问题，就是可以进行大量的拷贝，而产生版权侵犯。

同时，作为传统技术的一种内容加密和/或解密方法（参见日本专利申请公开第 09 - 136709 号），一种叫做 CSS（Content Scramble System，内容加扰系统）的版权保护系统被引入专用于再现的 DVD 视频光盘中，以防止内容的非法拷贝。

但是，在上述传统装置中，在防止非法拷贝和保护版权的同时内容也发生了移动，并且内容的再现不能由传统的通用再现装置来执

行。也就是说，存在一个问题，在正确执行了内容数据的移动时，不能保证用户通过传统的装置进行再现的便利。

发明内容

本发明的一个实施例提供了一种内容管理方法，一个记录和/或再现装置，和一个记录媒体，能够在防止内容传播的同时允许内容的移动，并且保证在传统的通用设备中的最低再现兼容性。

根据本发明，为了解决上述问题，提供了一种内容管理方法，包括：用第一密钥（TK）对内容数据进行加密；用预定的多种第二密钥（MUK）对第一密钥进行加密；用第三密钥（MM）对加密后的第一密钥（Enc-TK）进行多重加密；用预定的第四密钥（MMK）对第三密钥进行加密；在记录媒体中记录由第一密钥加密的内容数据（Enc-Content），由预定的多种第二密钥加密的第一密钥（Enc-TK），及通过对加密后的第一密钥（Enc-TK）用第三密钥（MM）进行多重加密而得到第一密钥（Enc2-TK），并且在记录媒体的安全区域内记录由第四密钥加密后的第三密钥（Enc-MM）。

根据本发明，如上所述，通过在记录媒体中记录一个多重加密的第一密钥（Enc2-TK）能进行内容的移动具有预定限制，该第一密钥（Enc2-TK）是作为用于控制内容移动的加密密钥的移动密钥（Move-Key），并且是一个通过用第二和第三密钥对一个用于内容的加密密钥进行多重加密而获得的标题密钥。另一方面，为了使得内容能够由传统的通用设备来再现，不采用一种对应于移动密钥（Move-Key）的专用设备，而是在不同的区域还记录一个媒体密钥（Enc-TK），该媒体密钥是一个具有一个仅由第二密钥（MKB，M-ID）加密一次的标题密钥（TK）的媒体绑定的标题密钥。以这种方式，利用通用设备的再现可由媒体密钥（Enc-TK）来使能，内容的移动在防止内容数据的传播的同时由移动密钥（Move-Key）来使能。

根据本发明，提供一种内容管理方法，其中，当记录媒体间的

移动已经被允许时，在内容数据从一个已经存储有内容数据的内容数据源（S）记录在第一记录媒体（D1）的情况下，在第一记录媒体（D1）中记录有（流程1）：由第一密钥（TK）加密的内容数据（Enc-Contents）；由第二密钥加密的第一密钥（Enc-TK），该第二密钥是一个绑定于记录媒体的内容加密密钥（MB-KEY）；以及由第二和第三密钥多重加密的内容移动控制加密密钥（Enc2-TK）；在内容数据从第一记录媒体（D1）移动到第二记录媒体（D2）的情况下，内容数据在解密后被再次加密，记录在第一记录媒体中的内容移动控制加密密钥被删除（流程2）。

根据本发明的内容管理方法的特征在于，移动内容的方案是特定的，并且当内容数据从一个内容数据源（S）涉及上述两种密钥即用于通用设备再现的媒体密钥（Enc-Tk）和用于移动内容的移动密钥（Move-Key）记录到第一盘（D1）时，所述两种密钥都被记录，从而能够允许内容的进一步移动，同时允许通过通用设备而不是专用设备的再现。当内容数据从第一盘（D1）移动到第二盘（D2）时，移动密钥（Move-Key）从第一盘中删除，只留下用于通用设备再现的媒体密钥（Enc-TK）。这样，不能进行进一步的移动，而且通用设备再现能够随后执行。当内容数据移动到第二盘，只记录移动密钥（Move-Key），因此只允许通过专用设备执行再现。而且，可以随后继续移动到第三及后续的盘。

根据本发明的内容管理方法提供了一种内容管理方法，一种记录和/或再现装置，及一种记录媒体，允许通过上述的第一盘记录方案和随后的移动方案来再现或移动内容数据，能够在允许移动内容数据的同时防止内容数据的传播，而且允许在传统的通用设备和专用设备中再现。

附图说明

图1是表示根据本发明的一个实施例的内容管理方法进行加密的实例的框图。

图 2 是表示通过一般的方法对根据本发明的一个实施例的内容管理方法加密后的内容进行解密的实例的框图。

图 3 是表示通过根据本发明的一个实施例的方法对根据本发明的一个实施例的内容管理方法加密后的内容进行解密的实例的框图。

图 4 是表示一个其中记录了根据本发明实施例的内容管理方法加密后的内容的记录媒体的实例的视图。

图 5 是表示根据本发明的一个内容管理方法实施例移动移动密钥 (Move-Key: Enc2-TK) 和媒体密钥 (MB-Key: Enc-TK) 的实例的示意性视图。

图 6 是表示应用了本发明实施例的内容管理方法的一个记录和/或再现装置的结构实例的框图。

图 7 是表示当记录和/或再现装置应用了本发明实施例的内容管理方法时的加密方法的细化实例的框图。

图 8 是表示当记录和/或再现装置应用了本发明实施例的内容管理方法时的解密方法的细化实例的框图。

图 9 是表示在记录媒体 D1 中记录根据本发明实施例的内容管理方法加密后的内容和密钥信息的操作流程图中。

图 10 是表示当内容从记录有根据本发明实施例的内容管理方法加密的内容的记录媒体 D1 移动到另一记录媒体 D2 时的操作流程图中。

图 11 是表示当内容从记录有根据本发明实施例的内容管理方法加密后的内容的记录媒体 D2 移动到另一记录媒体 D3 时的操作流程图中。

图 12 是表示在减少通道的情况下从记录有根据本发明实施例的内容管理方法加密后的内容的记录媒体 D2 到这样的另一记录媒体 D3 移动内容时的操作流程图中。

图 13 是表示在根据本发明实施例的内容管理方法中产生一个保密密钥 (MM) 的方法的视图。

图 14 是表示在根据本发明实施例的内容管理方法中, 在记录媒

体中用于一个移动密钥 (Move-Key: Enc2-TK) 和一个媒体密钥 (MB-Key: Enc-TK) 的存储区的实例视图。

图 15 是表示在根据本发明实施例的内容管理方法中, 在记录媒体中用于一个移动密钥 (Move-Key: Enc2-TK) 和一个媒体密钥 (MB-Key: Enc-TK) 的表格实例的视图。

具体实施方式

下文中, 根据本发明的一个内容管理方法, 一个记录和/或再现装置, 和一个记录媒体将结合附图进行详细的描述。图 1 是表示根据本发明的内容管理方法进行加密的实例的框图。图 2 和图 3 是表示对加密后的内容进行解密的实例的框图。图 4 示出了一个记录有加密后的内容的记录媒体的实例。图 5 是表示根据本发明的内容管理方法移动移动密钥 (Move-Key: Enc2-TK) 和媒体密钥 (MB-Key: Enc-TK) 的实例的示意性视图。

<根据本发明的内容管理方法的概括性描述>

现在, 将结合附图对根据本发明实施例的内容管理方法进行概括性描述。首先, 下面将描述一种加密和/或解密方法。根据本发明的内容管理方法的特征在于在记录媒体中连同加密后的内容数据记录有: 一个能够确保内容数据移动的移动密钥 (Move-Key: Enc2-TK); 一个确保由再现装置再现的媒体密钥 (MB-Key: Enc-TK)。

(加密)

通过结合一个 AV 编码器模块 M1 的工作和一个驱动器 V1 的工作, 可对根据本发明的内容管理方法中的加密和/或记录内容数据的方法进行描述。在图 1 的 AV 编码器模块 M1 中, 利用一个编码器 12 以 DVD 格式对视频 (V) 或音频 (A) 信号进行编码, 利用一个选择器 (SEL) 13 对编码后的信号和数字数据 11 进行选择。然后, 利用一个标题密钥 (TK) 在一个加扰电路 14 中对被选择的信号进行加扰 (加密) 处理, 处理过的信号作为 Enc-Contents 记录在一个盘 D

中。

此时, 通过一个随机数发生器 18 生成标题密钥 (TK)。利用一个加密密钥 (MUK) 在一个加密电路 20 中对所生成的密钥 TK 进行加密, 生成加密后的标题密钥 (Enc-TK)。这里, 用于加密标题密钥 (TK) 的加密密钥 (MUK) 以如下方式获得。利用一个 MKB 处理器 17, 通过使用从记录媒体中读取的 (MKB) 数据来对一个设备密钥 K1 (DvK1 16) 进行 MKB 处理, 以生成一个媒体密钥 (MK), 然后, 在通过一个 MID 处理器 19 进行 MID 处理之后生成结果密钥。

另外, 利用一个保密密钥 (MM) 对加密标题密钥 (Enc-TK) 进行多重加密, 从而生成一个多重加密标题密钥 (Enc2-TK), 然后, 和一个加密标题密钥 (Enc-TK) 一起提供给选择器 27。

这里, 保密密钥 (MM) 由一个随机数发生器 24 提供。根据记录媒体中给出的 MKB, 通过 MKB 处理器 23 对驱动器 V1 特定的设备密钥 (DvK2) 进行 MKB 处理。利用所获得的加密密钥 (MMK) 对此保密密钥 (MM) 进行加密, 从而获得一个加密后的加密密钥 (Enc-MM)。

这样获得的加密后的内容数据 (Enc-Contents)、一个被加密密钥 (MUK) 加密后的标题密钥 (Enc-TK) (= 媒体密钥 (MB-key))、和一个被第二和第三密钥多重加密后的标题密钥 (Enc2-TK) (= 移动密钥 (Move-key)) 都被记录在光盘 D 的记录区域内。另外, 先前加密过的第三密钥 (Enc-MM) 被记录在光盘 D 的一个安全区域内。将这些信号记录在光盘 D 中的例子示于图 4。

也就是说, 根据作为记录处理控制部分的 R-Control 15 发出的控制信号, 通过选择器 27 将移动密钥 (Move-Key; Enc2-TK) 和媒体密钥 (MB-Key; Enc-TK) (内容移动之后的其中之一) 记录在光盘 D 中。

这里, 为了实现由另一个再现装置来再现和交换记录在光盘记录媒体中的信息, 生成相同的密钥信息 (MK) 和多个设备密钥

(DvK)。另外，通过媒体特定的信息(M-ID)执行媒体绑定，从而防止全部拷贝到其它媒体中。

如后面详细所述，当内容被拷贝或移动时，两个加密密钥，即移动密钥(Move-Key; Enc2-TK)和媒体密钥(MB-Key; Enc-TK)被选择性的记录在光盘D中，因此，使得可由通用设备在预定条件下进行再现，或进行限制内容数据的移动处理。

(两种再现方法)

对于其上记录有如图4所示加密的内容数据和加密后的密钥信息的光盘D，如下所示，其上至少记录有一个媒体密钥(MB-Key; Enc-TK)的光盘D可以被传统的通用光盘再现装置再现。另外，其上只记录有移动密钥(Move-Key; Enc2-TK)的光盘D只能通过执行根据本发明的内容管理方法的光盘再现装置来再现。

也就是，图2是一个显示了通过只使用根据本发明的媒体密钥(MB-Key; Enc-TK)在一个再现装置中执行解密过程的视图，所述再现装置是一个通用设备。在此图中，在其上至少记录有一个媒体密钥(MB-Key; Enc-TK)的光盘D上，提前记录在一个媒体中的媒体密钥块信息(MKB)和媒体特定信息(M-ID)，以及一个媒体密钥(MB-Key; Enc-TK)通过一个总线认证21提供给一个AV解码器模块M2。另外，加密后的内容数据(Enc-Contents)也提供给AV解码器模块M2。

加密后的内容数据(Enc-Contents)在解扰器29中通过一个标题密钥(TK)被解扰(解密)，生成的数据提供给AV解码器30后被再现。这里，标题密钥(TK)是通过从盘D读出，发送至解密部分28并通过一个加密密钥(MUK)解密的一个加密标题密钥(Enc-TK)而获得的。另外，在记录侧，加密密钥(MUK)是基于媒体密钥块信息(MKB)和媒体特定信息(M-ID)通过MKB处理器17和MID处理器19而获得的。

以此方式，即使在传统的光盘再现装置或类似的不执行根据本发明的内容管理方法的处理的装置中，在其中记录有媒体密钥(MB-

Key)的光盘D中所包含的内容数据能够被再现。

另一方面,如图3所示,在光盘D中,只分配了移动密钥(Move-Key,Enc2-TK),根据本发明的内容数据管理方法执行处理,从而允许再现。

也就是说,驱动器V1从光盘单元中被分配了媒体密钥块信息(MKB),加密标题密钥(Enc-MM),多重加密标题密钥(Enc2-TK),和加密后的内容(Enc-Contents)。驱动器V1通过由一个解密单元31利用一个密钥(MMK)解密来获得一个保密密钥(MM),该密钥(MMK)是利用驱动器V1专用的一个设备密钥(DvK2)经过MKB处理器23的处理而获得的。以此方式,多重加密标题密钥(Enc2-TK)被解密成一个加密标题密钥(Enc-TK),并通过总线认证21提供给模块M2。

在模块M2中,专用于模块M2的设备密钥(DvK)根据媒体密钥块信息(MKB)经过MKB处理器17的处理,加密后的标题密钥(Enc-TK)在解密部分28由加密密钥(MUK)来解密,从而获得一个标题密钥(TK),其中该加密密钥(MUK)是基于媒体特定信息(M-ID)经过MID处理器19的处理而获得的。

利用这种标题密钥(TK),加密后的内容数据(Enc-Contents)在解扰单元29中被解密,由此内容数据可以被提供给AV解码器30。

这样,在盘D中仅分配了移动密钥(Move-Key;Enc2-TK)的情况下,后面将介绍的再现或移动只能通过一个执行本发明的内容管理方法的处理的光盘记录和/或再现装置来实现。

(根据本发明的内容管理方法移动内容)

现在,将通过实例对根据本发明的内容管理方法移动内容数据的方法进行概括性描述。图5中,在根据本发明的内容管理方法中,使用了两种类型的密钥,即一个移动密钥(Move-Key;Enc2-TK)和一个媒体密钥(MB-Key;Enc-TK),这些密钥根据需要记录在记录媒体中,由此可以对再现、拷贝或移动实施限制。也就是说,根据本

发明的内容数据管理方法，存在三种类型的如光盘的记录媒体，“一个媒体密钥（MB-Key）和一个移动密钥（Move-Key）”，“只有一个媒体密钥（MB-Key）”，“只有一个移动密钥（Move-Key）”。这里，不再描述内容数据等，只对两种密钥，即媒体密钥和移动密钥进行概括性描述。

在图 5 中，对于拷贝受限的源内容 S，一个媒体密钥（MB-Key）和一个移动密钥（Move-Key）被分配给一个第一盘 D1（记录媒体）。这样，可以允许根据本发明的再现装置和通用的再现装置实施再现。

然后，当盘 D1 中的内容数据通过根据本发明的再现装置被移动到一个新的盘 D2 时，移动密钥（Move-Key）从盘 D1 中删除，获得一个仅具有媒体密钥（MB-Key）的盘 D1'。新的盘 D2 中只记录有移动密钥（Move-Key）。这样，盘 D1' 仅可以由通用的再现装置实施再现。而且，盘 D2 不能由通用的再现装置实施再现。该盘仅可以通过根据本发明的记录和/或再现装置实施再现或移动处理。

另外，当包含这样的移动密钥（Move-Key）的盘 D2 中的内容数据被移动到一个新的光盘 D3 中时，光盘 D2 的移动密钥（Move-Key）通过本发明的再现装置删除，并且不能再次被再现。只有移动密钥（Move-Key）记录在光盘 D3 中，该盘仅能够通过根据本发明的记录和/或再现装置实施再现或移动处理。

而且，在从光盘 D 通过根据本发明的记录和/或再现装置移动内容数据的过程中，目标并不仅限于光盘。通用的数字记录媒体如 SD（安全数字）卡也可以作为移动的目标。这里，移动密钥（Move-Key）可从光盘 D3 移动到 SD（安全数字）卡 D4。当从前一光盘 D2 移动到光盘 D3 时，移动密钥（Move-Key）从光盘 D2 中删除，并且不能被再现。只有移动密钥（Move-Key）记录在 SD（安全数字）卡 D4 中，该盘仅能够通过根据本发明的记录和/或再现装置实施再现或移动处理。

<根据本发明的内容管理方法的应用实例>

现在将参考附图，对将根据本发明的内容管理方法应用到特定光盘记录和/或再现装置中的一个实施例进行详细描述。图 6 是一个描述了将根据本发明的内容管理方法应用到其中的记录和/或再现装置的示例性结构框图。图 7 是一个描述了将一种加密方法应用到记录和/或再现装置中的详细示例性框图。图 8 是一个描述了一个解密方法的详细示例性框图。

(记录和/或再现装置)

图 6 示出了一个其中应用了根据本发明的内容管理方法的光盘记录和/或再现装置 A。该光盘记录和/或再现装置 A 具有一个控制部分，包括：一个控制整体操作的系统控制部分 162；一个作为工作区域的 RAM 161；一个 ROM 160；和一个伺服控制部分 152。另外，此装置具有一个将激光束照射到光盘 D 上的光学拾取器 154；和一个接收用于再现的检测信号并提供记录用信号，从而执行 ECC 处理等的信号处理部分 156。装置 A 具有一个先前在图 1 等中所描述的总线认证部分 21。并且，该装置具有一个类似通过电缆提供的总线认证部分 21，以及具有一个执行编码或解码等的数据处理部分 158。另外，一个媒体读取器和/或写入器 166 连接于信号处理部分 156，该媒体读取器和/或写入器 166 是一个用于记录媒体如 SD 卡的接口。一个执行信号输入或输出的接口 165 和一个 RAM 159 或一个外部设备一起连接于数据处理部分 158。并且，装置 A 具有：连接于上述伺服控制部分 152 的伺服控制系统处理器电路 155；一个连接在其上的致动器驱动器 153；和一个盘电机 (M) 151。

在具有这样的配置的光盘装置 A 中，系统控制部分 162 将 RAM 161 用作一个工作区域，并且根据包含本发明的一个程序来执行预定操作，该程序被记录在 ROM 160 中。从光学拾取器 154 输出的激光束被照射到光盘 D 上。通过一个光头放大器，来自光盘 D 的反射光被转化成电信号。此电信号被输入给信号处理部分 156。信号处理部分 156 中包括一个 RF 放大器或类似的器件。

在记录过程中，参考图 1 详细描述的加密过程被应用于内容数

据, 并且为光盘 D 执行一个记录过程。更具体地, 数据处理部分 158 使用由写通道电路(未示出)产生的一个写时钟向通过接口 165 发送来的内容数据分配一个检错码(EDC)或 ID, 并且使用上述编码而进行数据加扰处理。另外, 此数据处理部分分配一个纠错码(ECC), 指定一个同步信号, 对除同步信号以外的信号进行调制, 并且通过使用正确策略(对兼容媒体来说是最佳的)控制下的激光束在光盘 D 中记录信号。

在再现过程中, 参考图 2 和图 3 详细描述和解码过程被应用于内容数据, 并且对存储在光盘 D 中的数据进行再现处理。更具体地, 从光学拾取器 154 的光头放大器中读出的 RF 信号被通过一个最优均衡器而发送给信号处理部分 156 中一个 PLL 电路(未示出)。通道数据根据由 PLL 电路产生的一个读时钟来读取。使用上述解密方法的解密过程被应用于读出的数据。另外, 由数据处理部分 158 对解密后的数据进行同步, 读出符号数据。然后, 执行一个利用纠错或上述解密处理的解扰处理, 解扰后的数据通过接口 165 发送给外部。

如此, 通过上述光盘记录和/或再现装置 A 实现了所述的记录过程和再现过程。

另外, 信号处理部分 156 和数据处理部分 158 各具有一个总线认证部分 21, 并且提供对通过断开两部分上的电缆提取信号而试图进行非法拷贝的第三人的防护。也就是说, 每一总线认证部分 21 具有一个随机数发生器(未示出)。以这种方式, 该发生器产生同样的加密密钥, 对发送信息进行加密, 并将其发送到远端方。远端设备接收到发送的信息后对加密后的发送信息通过本地产生的同样的加密密钥进行解密。该加密密钥随预定的时间变化及产生, 因此第三人很难再生。只要此时的加密密钥不能被再生, 那么即使信号通过断开电缆而被提取, 内容数据的非法拷贝等行为也不能进行。

(通过调制和/或解调处理的加密密钥的安全性)

下面将描述对由信号处理电路 156 执行的调制器和/或解调器电

路操作应用的加密密钥信息的保密处理过程。在图 7 所示的对记录过程的内容管理方法的主要部分中，一个 AV 编码器模块 M1 与图 1 所示的相同。在图 8 所示的对再现过程的内容管理方法的主要部分中，一个 AV 解码器模块 M2 与图 3 所示的相同。在此不再重复描述。

在图 7 所示的驱动部分 V3 中，除了图 1 的驱动器 V1 的构成外，还示出了一个 ECC 电路或类似的结构。也就是说，来自内容加扰器 14 的信号作为主要数据在由 ECC 电路 43 分配了一个纠错信号时被调制器电路 44 调制。而且，加密后的保密密钥 (Enc-MM) 也通过 ECC 电路 47 进行了纠错编码，该加密后的密钥由第二调制电路 48 调制。然后，调制后的密钥通过选择器 45 由主要数据的一部分来代替，然后由一个写通道电路 46 记录在光盘 D 的一个存储区域中。

一方面，在图 8 的驱动部分 V4 中，被分配了纠错码的数据从光盘 D 中读出，读出的数据然后由第二解调器电路 45 解调。然后，可通过 ECC 电路 46 提取加密后的保密密钥 (Enc-MM)。另一方面，在图 7 中，加密后的保密密钥 (Enc-MM) 由第二调制器 48 调制并记录，该调制器 48 不同于调制主要数据的调制器 44。因此，加密后的保密密钥 (Enc-MM) 不能在读出部分的用于主要数据的解调器 42 中解调，密钥作为误差数据处理。这样，第三人就不能提取加密后的保密密钥 (Enc-MM) 来进行非法拷贝。通过这样应用调制和/或解调过程，不能通过通用的主要数据调制过程进行检测的安全信息就能够产生。而且，可以以同样的方式进行处理，使得加密的密钥信息 (Enc-MM) 实质上记录并再现于安全区域中。以此方式，即使通过如光盘等无源记录媒体，也可能构筑高水平的保护系统。

(移动流程图 1)

之前简要描述的记录媒体间移动内容数据的过程在此将通过流程图进行详细描述。图 9 的流程图示出了将根据本发明的内容管理方法加密的内容和密钥信息记录至记录媒体 D1 中的操作。图 10 是表示当内容从记录媒体 D1 移动到另一记录媒体 D2 时的操作流程图。图 11 是表示当内容从记录媒体 D2 移动到另一记录媒体 D3 时的操作

流程图。图 12 是表示在减少信道的情况下进行这种移动时的操作流程图。

根据本发明的内容管理方法如上所述，是通过在光盘记录和/或再现装置中配置信号处理部分 156 和数据处理部分 158 来实现的。这些处理即使通过描述应用该内容管理方法来检测信息的过程的程序等也能执行。以下，根据本发明的内容管理方法将通过流程图进行详细描述。

如图 9 所示的流程图中，将给出一个关于内容数据从拷贝受限的内容数据源 S 拷贝至一个记录媒体 D1 如光盘 D 中的情况的描述。

首先，用于产生密钥信息 (MK) 的媒体密钥块信息 (MKB) 和媒体特定信息 (M-ID) 从记录媒体 D1 中读出，这些信息被传送到一个 AV 编码器部分 M1 (S11)。然后，在 AV 编码器部分 M1，密钥信息 (MK) 通过利用一个设备专用解密密钥 (DvK1) 16 被从媒体密钥块信息 (MKB) 中提取出。然后，用于加密标题密钥的加密密钥 (MUK) 从密钥信息 (MK) 和媒体特定信息 (M-ID) 产生 (S12)。

接下来，通过一个随机数发生过程产生一个标题密钥 (TK)。然后，已经被指定了版权保护的内容数据通过标题密钥 (TK) 被加扰加密。然后，该标题密钥 (TK) 通过一个用来加密标题密钥的一个密钥 (MUK) 加密，产生加密标题密钥 (Enc-TK) (S13)。然后，加密后的内容 (Enc-Contents) 和加密标题密钥 (Enc-TK) 被通过总线认证部分传送到驱动器 V1 (S14)。

然后，确定记录内容是否被允许移动 (S15)。如果所确定的结果是肯定的，则通过一个随机数发生过程产生一个保密密钥 (MM)。然后，该加密标题密钥 (Enc-TK) 通过该保密密钥 (MM) 被多重加密，产生一个多重加密标题密钥 (Enc2-TK)。然后，用于该加密后的内容 (Enc-Contents) 和一组加密标题密钥 (Enc-TK) 的一个媒体密钥 (MB-Key) 及一个用于一组多重加密标题密钥 (Enc2-TK) 的移动密钥 (Move-Key) 被记录在记录媒体 D1

中 (S16)。

而且, 通过驱动器 V1 中的一个设备密钥 (DvK2), 一个加密密钥 (MMK) 被根据媒体密钥块信息 (MKB) 检测。一个保密密钥 (MM) 被通过该加密密钥 (MMK) 加密, 产生一个加密后的加密密钥 (Enc-MM) (S17)。然后, 加密后的加密密钥 (Enc-MM) 信号被记录在一个安全区域中 (S18)。

如果步骤 S15 的确定结果是否定的, 用于加密后的内容 (Enc-Contents) 和一组加密标题密钥 (Enc-TK) 的媒体密钥 (MB-Key) 被记录在记录媒体 D1 中 (S19)。

通过这些过程, 内容数据被加密, 作为本发明的内容管理方法的特征的移动密钥 (Move-Key; Enc2-TK) 和媒体密钥 (MB-Key; Enc-TK) 或者只有媒体密钥被记录在光盘 D1 中。

(移动流程图 2)

在图 10 所示的流程图中, 将给出一个关于内容从一个记录媒体 D1 移动到另一记录媒体 D2 的情况下的操作的描述。

首先, 媒体密钥块信息 (MKB) 和媒体特定信息 (M-ID) 从移动目标记录媒体 D2 中读出, 并从中产生一个加密密钥 (MUK2) (S21)。然后设置记录媒体 D1, 内容管理信息被检测 (S22)。然后, 确定是否存在对应的内容媒体密钥 (MB-Key) 和移动密钥 (Move-Key) (S23)。

如果在步骤 S23 中确定只存在密钥 (Move-Key) 时, 利用媒体密钥块信息 (MKB) 和一个设备密钥 (DvK2) 检测加密密钥 (MMK)。然后, 加密的加密密钥 (Enc-MM) 被解密, 保密密钥 (MM) 被检测。然后, 通过一个保密密钥 (MM), 多重加密标题密钥 (Enc2-TK2) 被解密, 产生一个加密标题密钥 (Enc-TK) (S31)。

当在步骤 S23 中确定媒体密钥 (MB-Key) 和移动密钥 (Move-Key) 都存在时, 记录媒体 D1 中的媒体密钥块信息 (MKB) 和媒体特定信息 (M-ID) 通过总线认证进行传送, 一个加密密钥 (MUK)

通过一个设备专有加密密钥 (DvK1) 进行检测 (S24)。而且, 一个加密标题密钥 (Enc-TK) 通过一个加密密钥 (MUK) 被解密, 产生一个标题密钥 (TK)。而且, 加密的内容从记录媒体 D1 中读出, 读出的内容通过一个标题密钥 (TK) 进行解密。然后, 解密的内容通过一个由一个新的随机数发生器产生的标题密钥 (TK2) 被重新加扰 (加密), 加密的内容临时被记录 (S25)。然后, 作为记录媒体 D1 中对应的内容的移动密钥 (Move-Key) 的多重加密标题密钥 (Enc2-TK) 被删除 (S26)。

然后, 当前的记录媒体变为记录媒体 D2; 一个标题密钥 (TK2) 被一个加密密钥 (MUK2) 加密; 产生一个加密标题密钥 (Enc-TK2) (S27)。然后, 在记录驱动器中产生一个新的保密密钥 (MM2); 加密标题密钥 (Enc-TK2) 被多重加密; 产生一个多重加密标题密钥 (Enc2-TK2)。

然后, 利用记录媒体 D2 中的媒体密钥块信息 (MKB) 以及一个设备密钥 (DvK2) 产生一个加密密钥 (MMK); 保密密钥 (MM2) 被加密; 产生一个加密的加密密钥 (Enc-MM2) (S28)。然后, 由标题密钥 (TK2) 加密的内容 (Enc-Contents) 以及多重加密标题密钥 (Enc2-TK2) 记录在记录媒体 D2 中。而且, 加密后的加密密钥 (Enc-MM2) 记录在安全区域中 (S29)。

另外, 当在步骤 23 中确定不存在移动密钥 (Move-Key) 时, 移动被禁止 (S30)。

在该方式中, 移动密钥 (Move-Key) 被从移动源记录媒体 D1 中删除, 只得到媒体密钥 (MB-Key)。并且内容的移动是禁止的。结果, 通过传统的通用再现装置可以执行再现, 但不能移动数据。另一方面, 只有移动密钥 (Move-Key) 存在于移动目标记录媒体 D2 中。只有能够执行本发明的内容管理方法的专用设备才能进行再现及进一步的移动。

(移动流程图 3)

在图 11 所示的流程图中, 将给出内容被从记录媒体 D2 中移到

另一个记录媒体 D3 中的情况下的操作的描述。

首先，媒体密钥块信息（MKB）和媒体特定信息（M-ID）被从移动目标记录媒体 D3 中读出，并生成一个加密密钥（MUK3）（S21）。

然后，设置记录媒体 D2，并检测内容管理信息（S22）。然后，确定是否存在对应的内容媒体密钥（MB-Key）和移动密钥（Move-Key）（S23）。

当移动密钥（Move-Key）不存在时，禁止移动内容数据（S30）。

当确定出只存在移动密钥（Move-Key）时，通过使用媒体密钥块信息（MKB）和设备密钥（DvK2）来提取加密密钥（MMK）。然后，解密加密后的加密密钥（Enc-MM）以检测一个保密密钥（MM）。然后，通过一个保密密钥（MM）来对多重加密标题密钥（Enc2-TK2）进行解密，从而生成一个加密标题密钥（Enc-TK2）（S31）。

当在步骤 S23 中确定出媒体密钥（MB-Key）和移动密钥（Move-Key）都存在时，记录媒体 D2 中媒体密钥块信息（MKB）和媒体特定信息（M-ID）被通过总线认证而传送。然后，通过一个设备特定解密密钥（DvK1）检测出一个用于标题密钥的加密密钥（MUK2）（S42）。然后，通过用于标题密钥的解密密钥（MUK2）对加密标题密钥（Enc-TK）进行解密，从而检测出一个标题密钥（TK2）。然后，从记录媒体 D2 中读出加密后的内容（EC-Contents），并临时存储读出的内容（S43）。然后，删除一个多重加密标题密钥（Enc2-TK2），它是一个用于记录媒体 D2 中对应内容的移动密钥（Move-Key）（S26）。

然后，当前记录媒体变成记录媒体 D3；通过一个加密密钥（MUK3）对一个标题密钥（TK3）进行加密；从而生成一个加密标题密钥（Enc-TK3）（S27）。然后，生成记录驱动器中一个新的保密密钥（MM3）；一个加密标题密钥（Enc-TK3）被多重加密；从

而生成一个多重加密标题密钥 (Enc2-TK3)。然后, 通过使用记录媒体 D3 中媒体密钥块信息 (MKB) 和设备密钥 (DvK2) 生成一个加密密钥 (MMK); 一个保密密钥 (MM3) 被加密; 从而生成一个加密后的加密密钥 (Enc-MM3) (S28)。然后, 通过标题密钥 (TK2) 加密后的内容 (Enc-Contents) 和多重加密标题密钥 (Enc2-TK3) 被记录在记录媒体 D3 中, 并且加密后的加密密钥 (Enc-MM3) 被记录在安全区域中 (S29)。图 11 的流程图 3 中的加密标题密钥 (Enc-TK3) 中包括多个与图 10 的流程图 2 相同的步骤, 但有所不同, 在步骤 S42 和 S43 中, 标题密钥 (TK2) 通过加密密钥 (MUK2) 被加密, 从而生成加密标题密钥 (Enc-TK3)。

这样, 在移动源记录媒体 D2 中, 移动密钥 (Move-Key) 被删除, 因此就不可能移动或再现内容数据。另一方面, 在移动目标记录媒体 D3 中, 只获得了移动密钥 (Move-Key), 因此, 使得只有通过能够执行根据本发明的内容管理方法的专用设备可以实现再现和进一步移动。

另外, 根据本发明的内容管理方法的目标记录媒体, 并不仅限于光盘, 还可以包括一个通用数字记录媒体, 例如如图 5 所示的一个 SD (安全数字) 卡 D4 等。

(移动流程图 4)

另外, 在图 12 的流程图中示出的内容数据的移动过程中, 将给出多通道音频源数据 (5.1 通道) 被减少到 2 通道而处理的情况下的描述。这些处理基本上与图 11 的流程图中所示的相同。图 11 的流程图中的步骤 S42 和步骤 S43 被图 12 中步骤 S41 代替。

也就是说, 在图 12 的流程图的步骤 S41 中, 通过一个加密密钥 (MUK2) 来对一个加密标题密钥 (Enc-TK) 进行解密, 从而生成一个标题密钥 (TK2)。然后, 加密后的内容 (Enc-Contents) 被从记录媒体 D2 中读出, 通过一个标题密钥 (TK2) 对读取的内容进行解密。另外, 多通道音频源数据被减少为 2 通道; 通过由随机数发生器产生的一个标题密钥 (TK3) 对数据进行再次加扰 (加密), 加密

后的数据被临时记录下来 (S41)。

在此过程中, 当音频源数据 (5.1 通道) 被减少为 2 通道时, 内容数据可以被从记录媒体 D2 中移动到一个新的记录媒体 D3 中。它的有益效果与图 11 的流程图中的移动过程相同。

(用于增加密钥信息的方法和用于每一个音乐项文件的密钥)

另外, 根据本发明的内容管理方法的目标内容数据可以是大量声音文件的形式, 如大量音乐项目的音乐信息。大量信息可以被存储在例如一个虚拟图像文件或图像文件中。这里, 将通过声音文件为例进行描述。在此形式中, 由图 1 中的随机数发生器 18 所提供的不同标题密钥 (TK) 以逐个文件为基础提供, 并且这些密钥中的每一个都是加密过的, 从而使得音乐信息中的每一个音乐项目都可以移动到另一个记录媒体中。如此, 用户利用内容的自由度可以被大大地提高。

但是, 如果移动密钥 (Move-Key = Enc2-TK) 的生成与一个接一个的多个标题密钥 (TK) 相关, 则需要在驱动部分 V1 中按大量音乐文件的数目提供保密密钥 (MM)。但是, 如果按大量音乐项目的数目提供保密密钥 (MM), 然后将所有这些密钥存储在光盘 D 中的安全区域, 这是不可取的, 因为安全区域需要很大的存储容量, 引起了存储容量的增加。更具体地, 在一个使用上述的调制和/或解调过程的安全信息记录系统中, 当部分主数据被破坏时, 而安全信息就记录在其中。在主数据的再现处理中此情况是不可取的, 因此, 需要将安全信息减少到最小。

由此, 根据预定的过程基于一个保密密钥 (MM) 增加了多个密钥; 增加的密钥用于加密; 并且只将作为增加源的保密密钥 (MM) 存储在安全区域内, 从而在降低安全区域的存储容量的情况下, 可能管理大量文件。

图 13 是一个表示用于在根据本发明的内容管理方法中产生一个保密密钥 (MM) 的方法的视图。在此图中, 在图 1 的随机数发生器 24 或类似的器件中, 基于从一个随机数 G 61 生成的密钥源数据

(MM) 来生成一个保密密钥 (MM1), 然后, 用一个内容数据标识码或由序号确定的号码等乘以一个特定的函数 K, 以此生成新的保密密钥 (MM2 到 MMn)。通过使用多个这些保密密钥 (MM2 到 MMn), 多个加密标题密钥 (Enc-TK1 到 Enc-TKn) 63-1 到 n 被用于加密 64。

但是, 只有具有在其中加密过的密钥源数据 (MM) 的加密后的加密密钥 (Enc-MM) 可以被存储在安全区域中, 这样, 安全区域所需的存储容量并没有增加。因此, 就可能在保持高度安全的同时管理大量文件的内容。

(管理信息)

在根据本发明的内容管理方法中, 内容数据的再现或移动是通过一个移动密钥 (Move-Key) 和一个媒体密钥 (MB-Key) 来管理的。这样, 这些加密密钥文件是如加密后的内容一样非常重要的数据。也就是说, 如果一个加密后的加密密钥不能被解密, 加密后的内容也就不能被解密或再现。由此, 如图 14 所示, 在记录媒体 (例如一个光盘) 的一个数据区域内, 一个移动密钥 (Move-Key) 文件和一个媒体密钥 (MB-Key) 文件设置在不同的文件区域内。然后, 每一个 ECC 块中被分配了一个表, 并且每一个表在四个 ECC 块中写四次, 从而提高数据的可靠性。

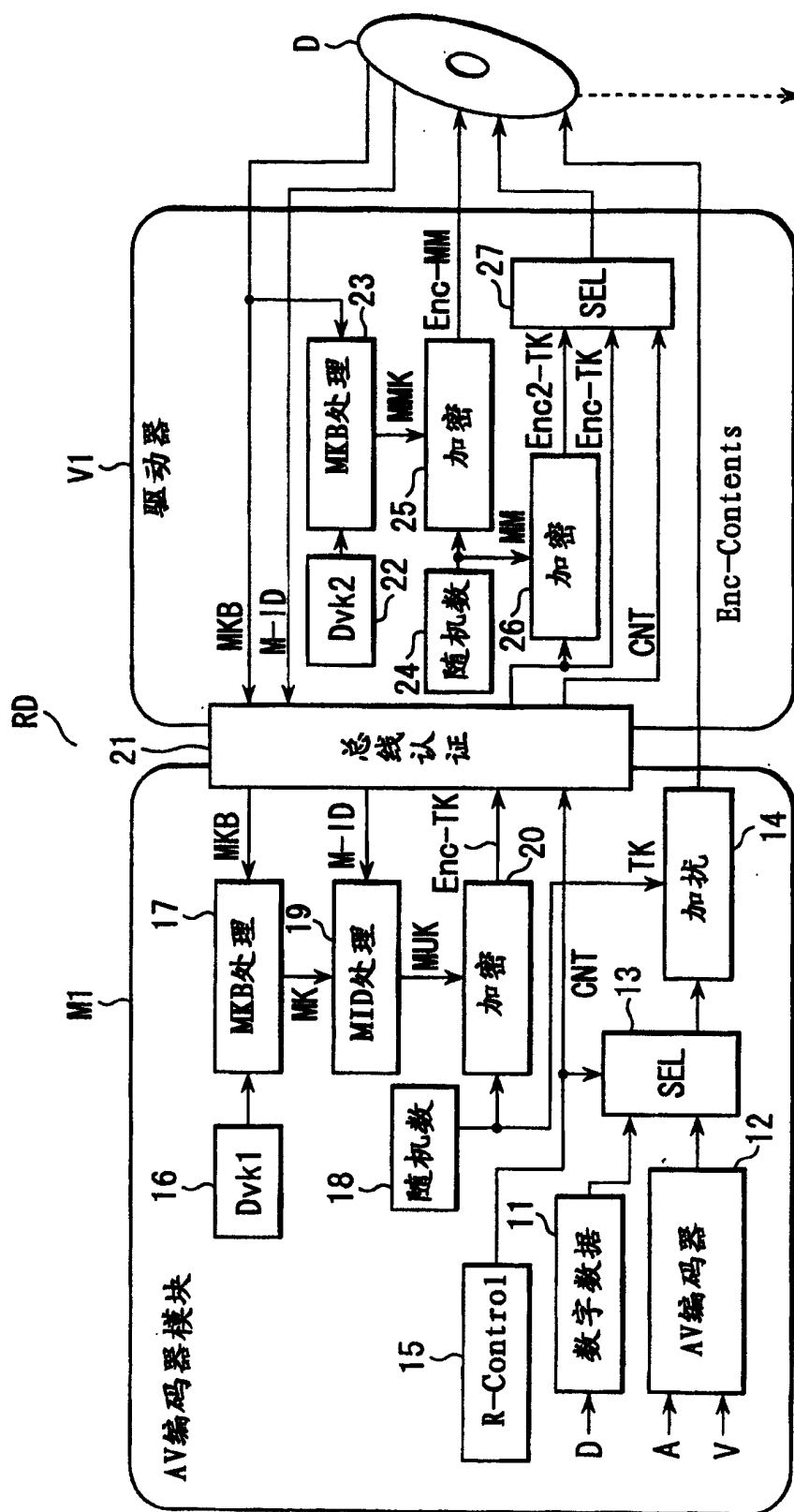
这些文件的一个表如图 15 所示。即, 在一个记录媒体中存在三种密钥形式, “一个媒体密钥 (MB-Key) 和一个移动密钥 (Move-Key)”, “只有一个媒体密钥 (MB-Key)”, “只有一个移动密钥 (Move-Key)”。另外, 在存在大量内容 (Cont) 文件的情况下, 需要很容易地读出与单个管理的内容加密密钥中的各个相关的媒体密钥 (MB-Key) 和移动密钥 (Mobile-Key) 之间的关系。由此, 在图 15 所示的移动密钥 (Move-Key) 表和媒体密钥 (MB-Key) 表中, 这些表中配置了一对信息, 即指示加密密钥 (与加密后的加密密钥中的各个相关的) 存在与否的信息, 以及在使用图 13 所示的生成保密密钥 (MM) 的方法的情况下使用的信息。通过列出这些表, 可

以很容易地确定与各个内容数据相关的内容移动是否允许。

通过上述的各种实施例，本领域的技术人员可以实现本发明。另外，本领域的技术人员也可以很容易的想出并且在不需要花费创造性劳动的情况下对这些实施例进行各种修改。因此，本发明覆盖了一个较宽的与所披露的原理和创新的特征不矛盾的保护范围，并且并不仅限于上述实施例。

例如，对于在其中存储保密密钥的一个安全区域，当使用上述调制和/或解调过程时，一个用于记录和/或再现安全信息的区域可以与除主数据外的记录和/或再现区域相关。通过使用这样一种方法，主数据将不包括误差部分，这样内容数据的可靠性不会损失。

如上的详细描述，根据本发明，用于保证内容数据移动的移动密钥（Move-Key: Enc2-TK）和用于保证由传统通用再现装置（如光盘装置）进行再现的媒体密钥（MB-Key: Enc-TK）与加密后的内容数据一起记录在一个记录媒体中。在根据本发明的能够对存储在安全区域内的保密密钥进行解密的记录和/或再现装置中，通过移动密钥（Move-Key）的再现或移动是允许的。在作为传统的通用设备的再现装置中，确保了通过媒体密钥（MB-Key）的再现。这样，能够在防止内容数据的传播的同时，允许专用设备的移动处理。另外，由传统设备对内容数据的再现也是允许的。



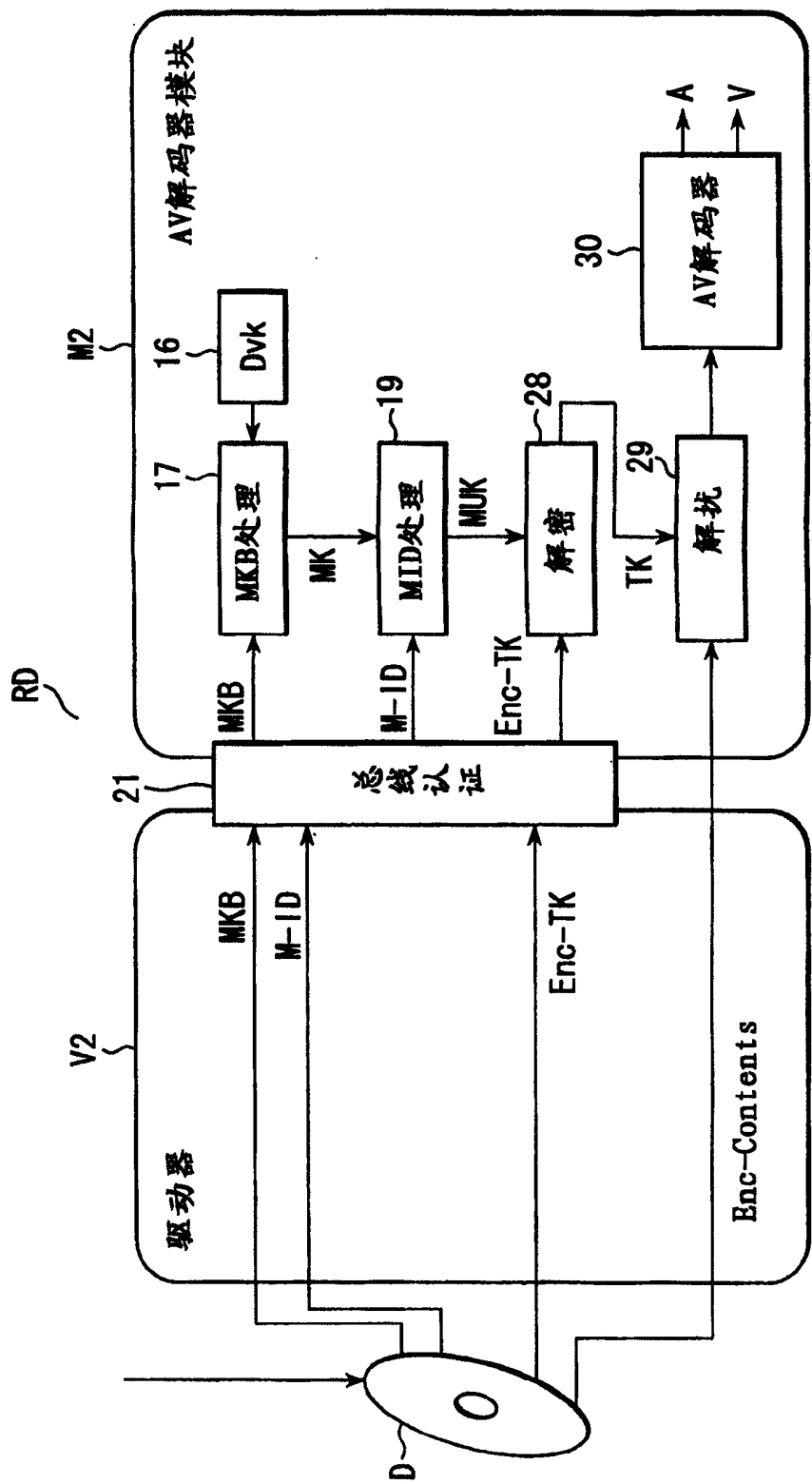


图2

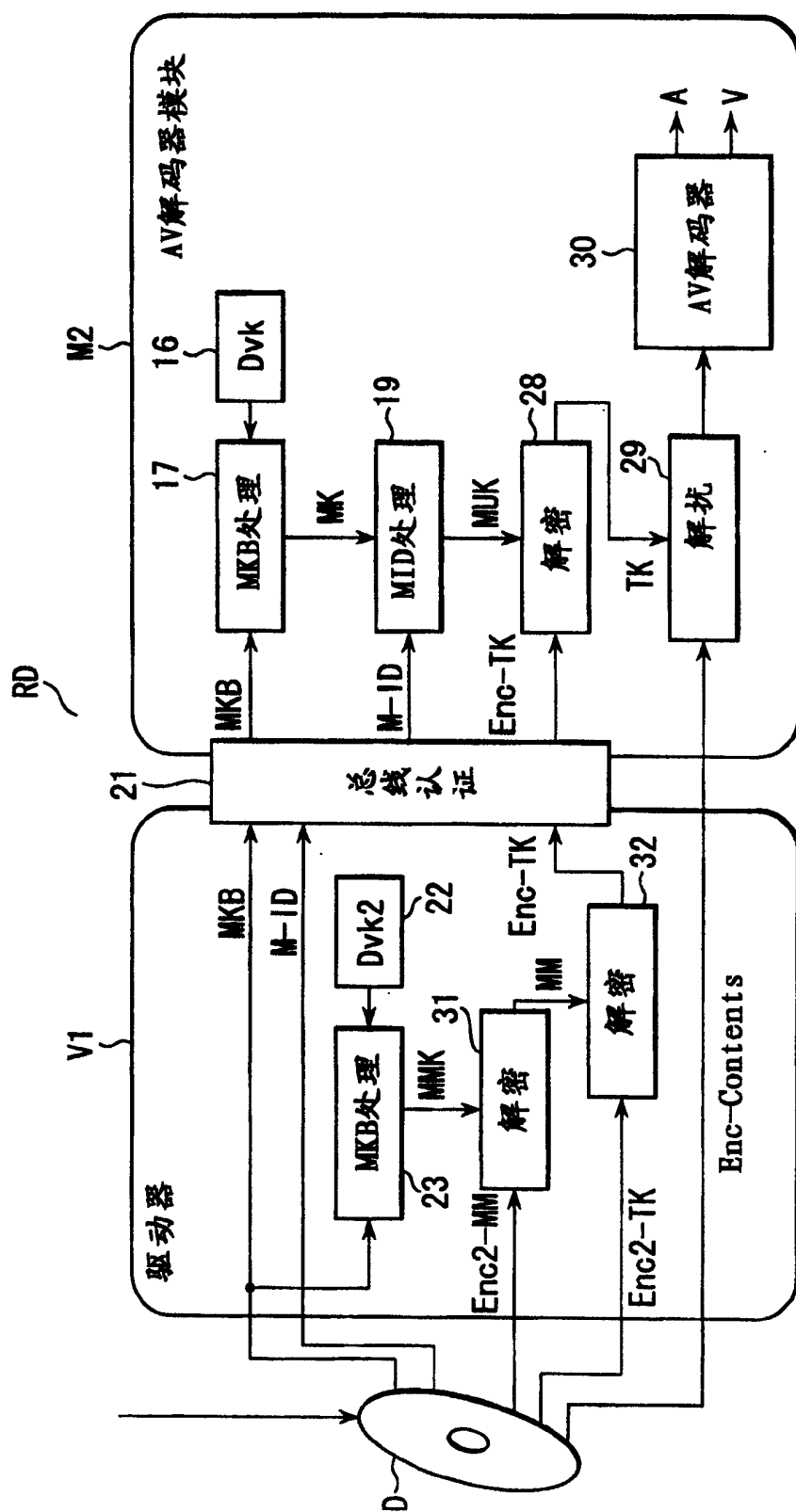


图 3

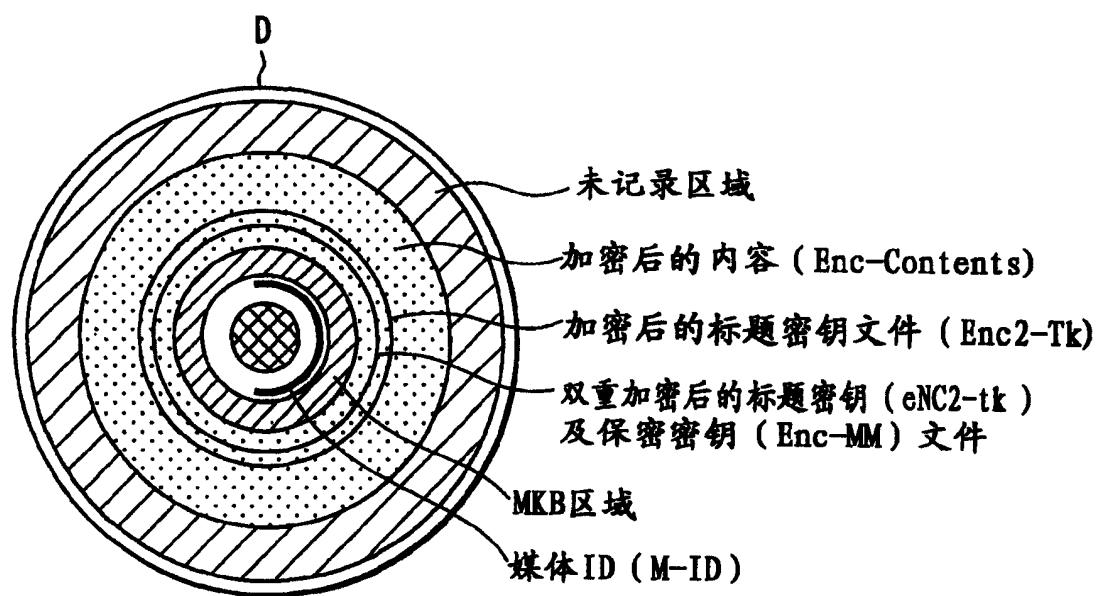


图 4

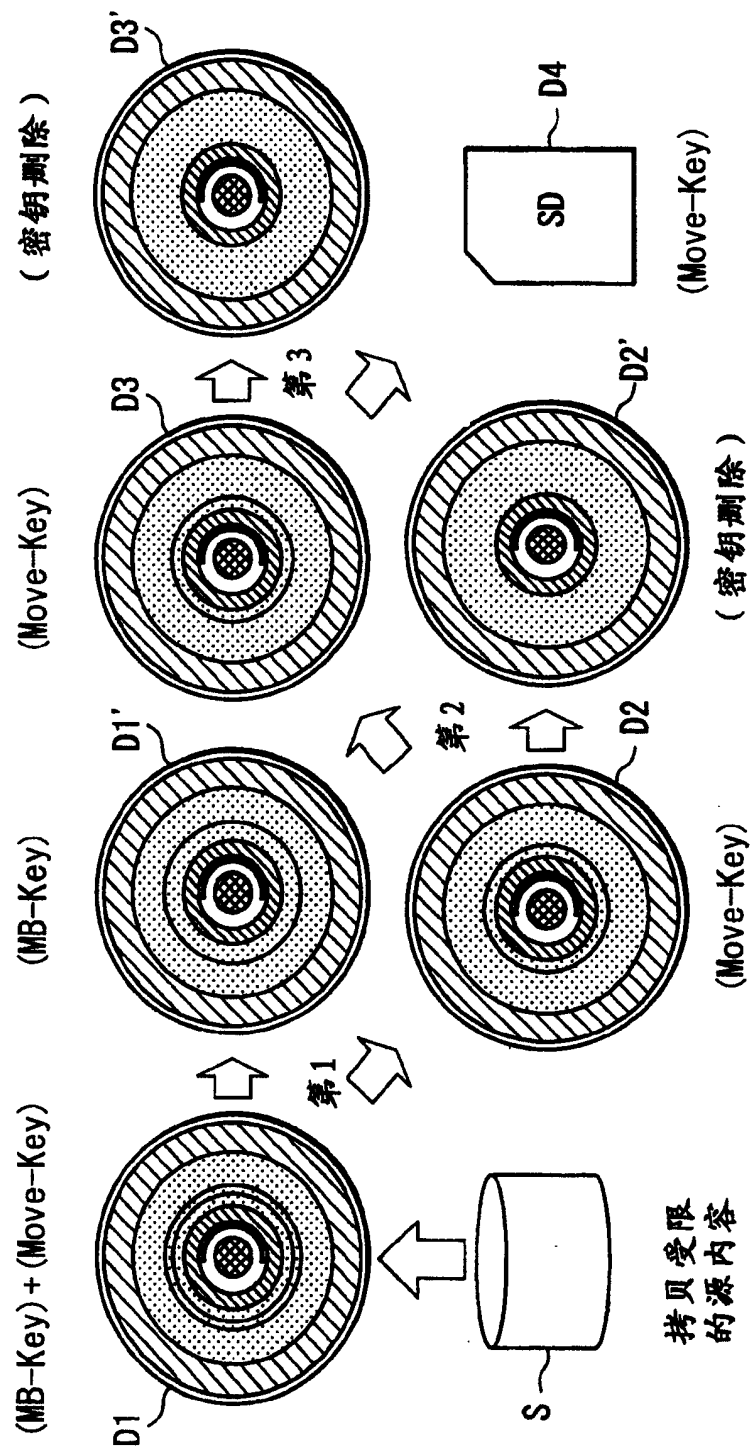


图 5

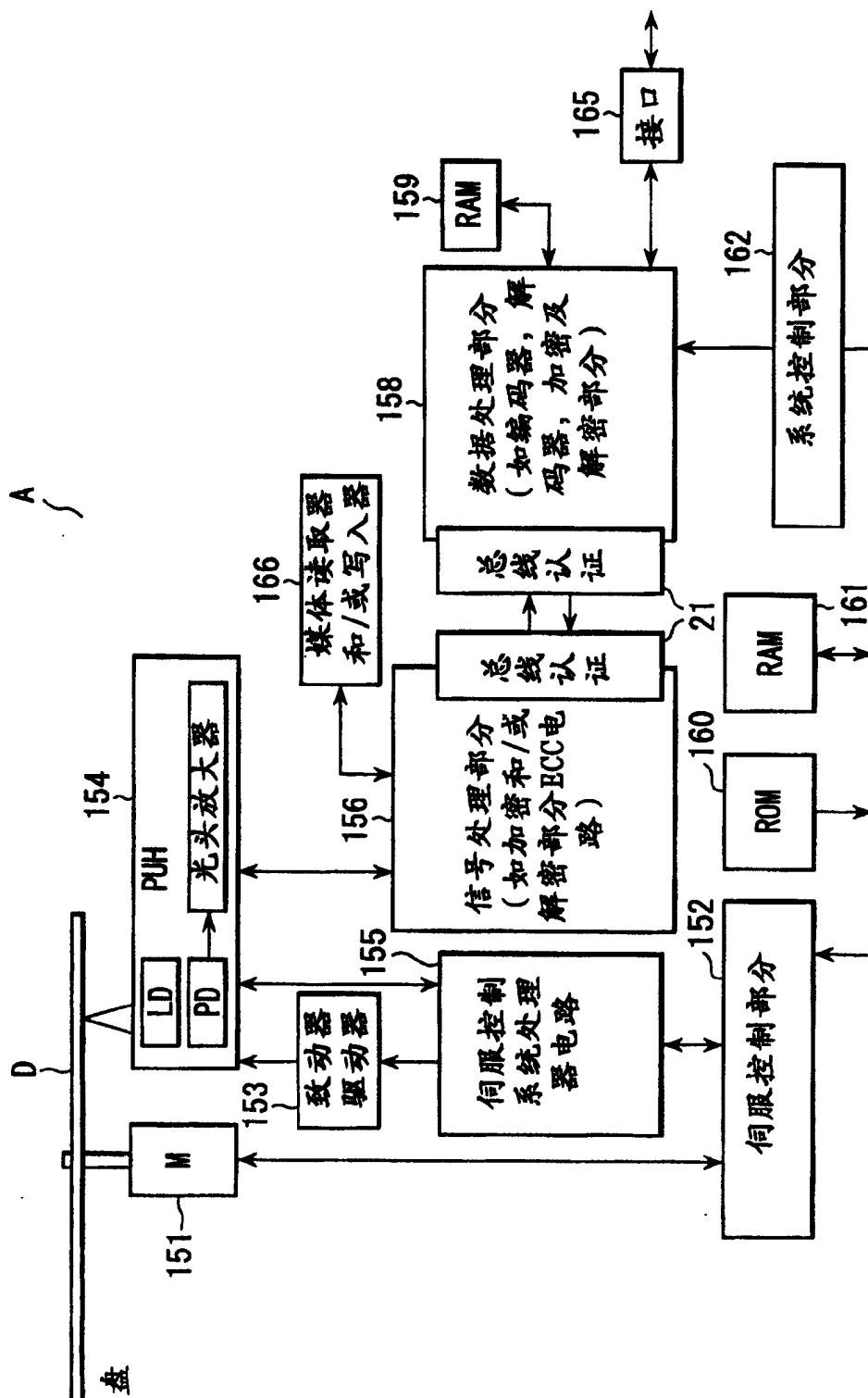
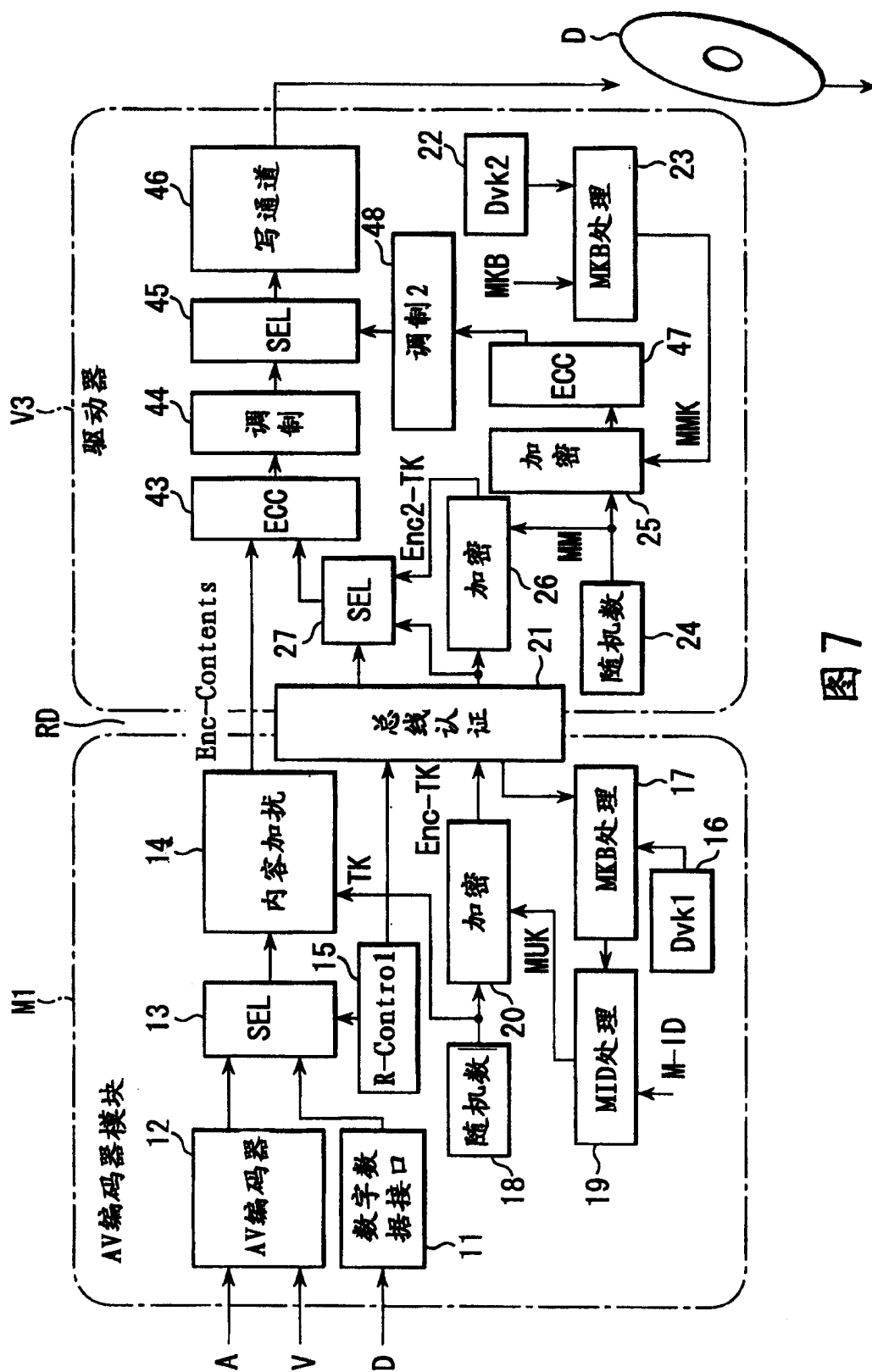


图 6



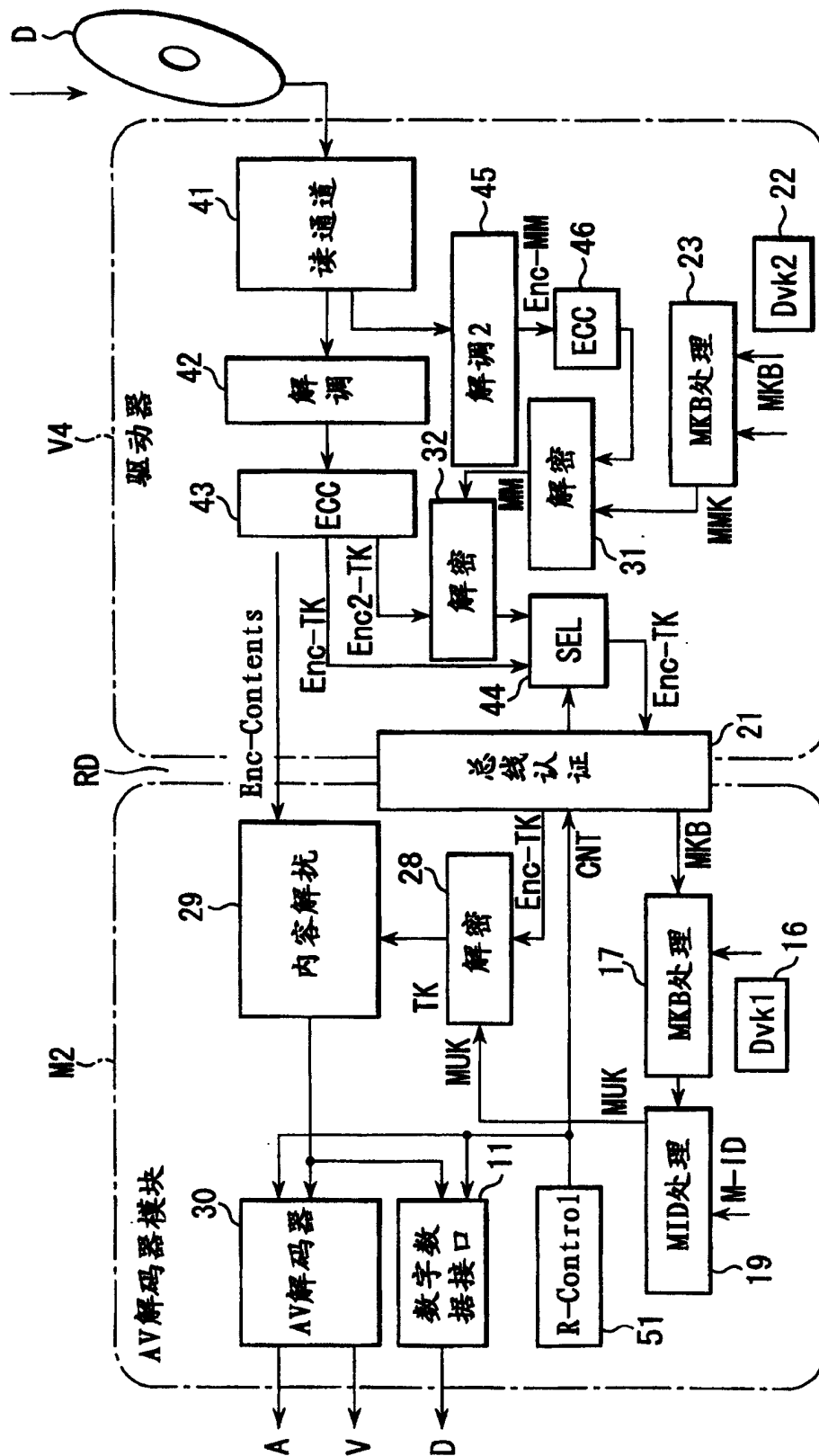
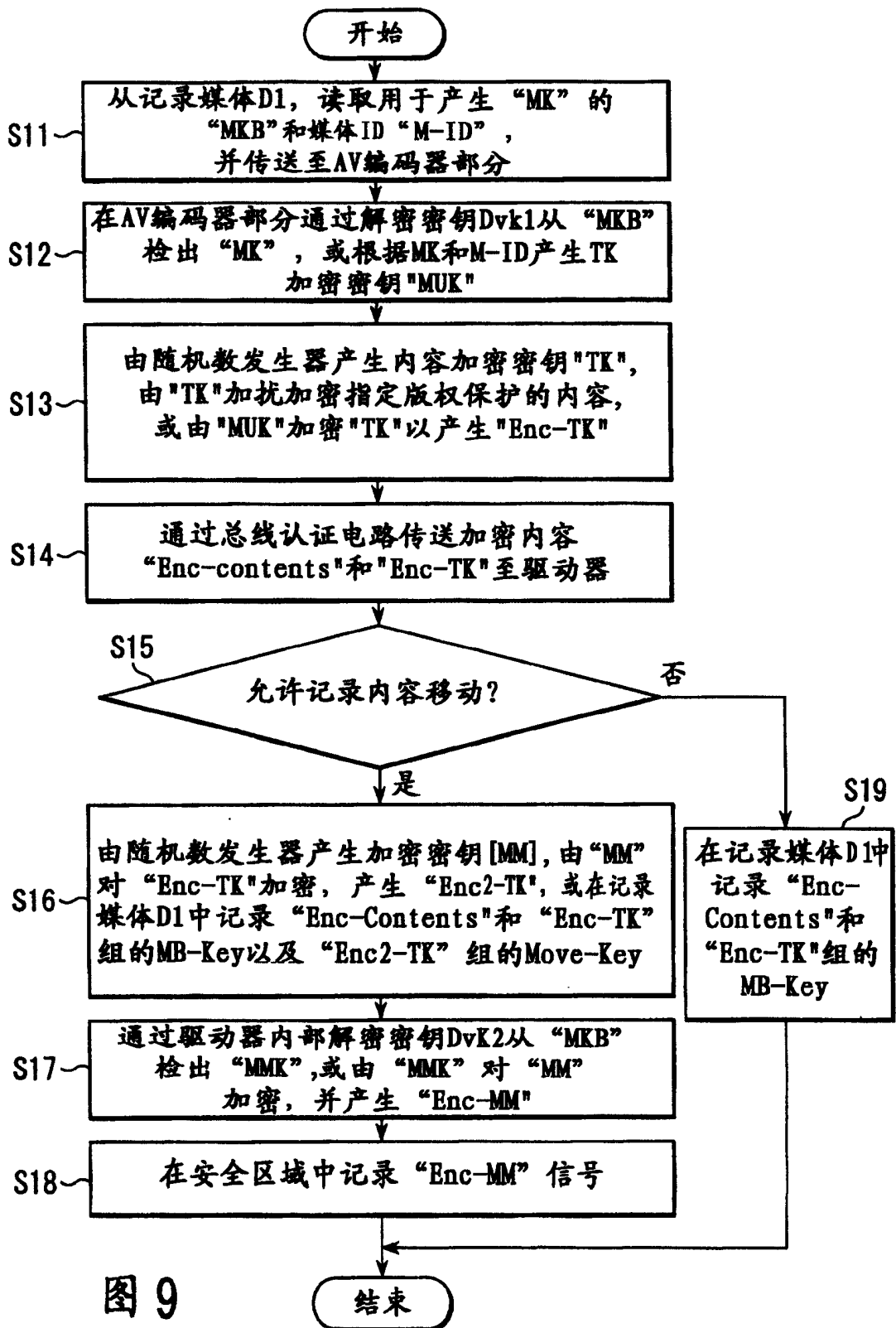


图 8



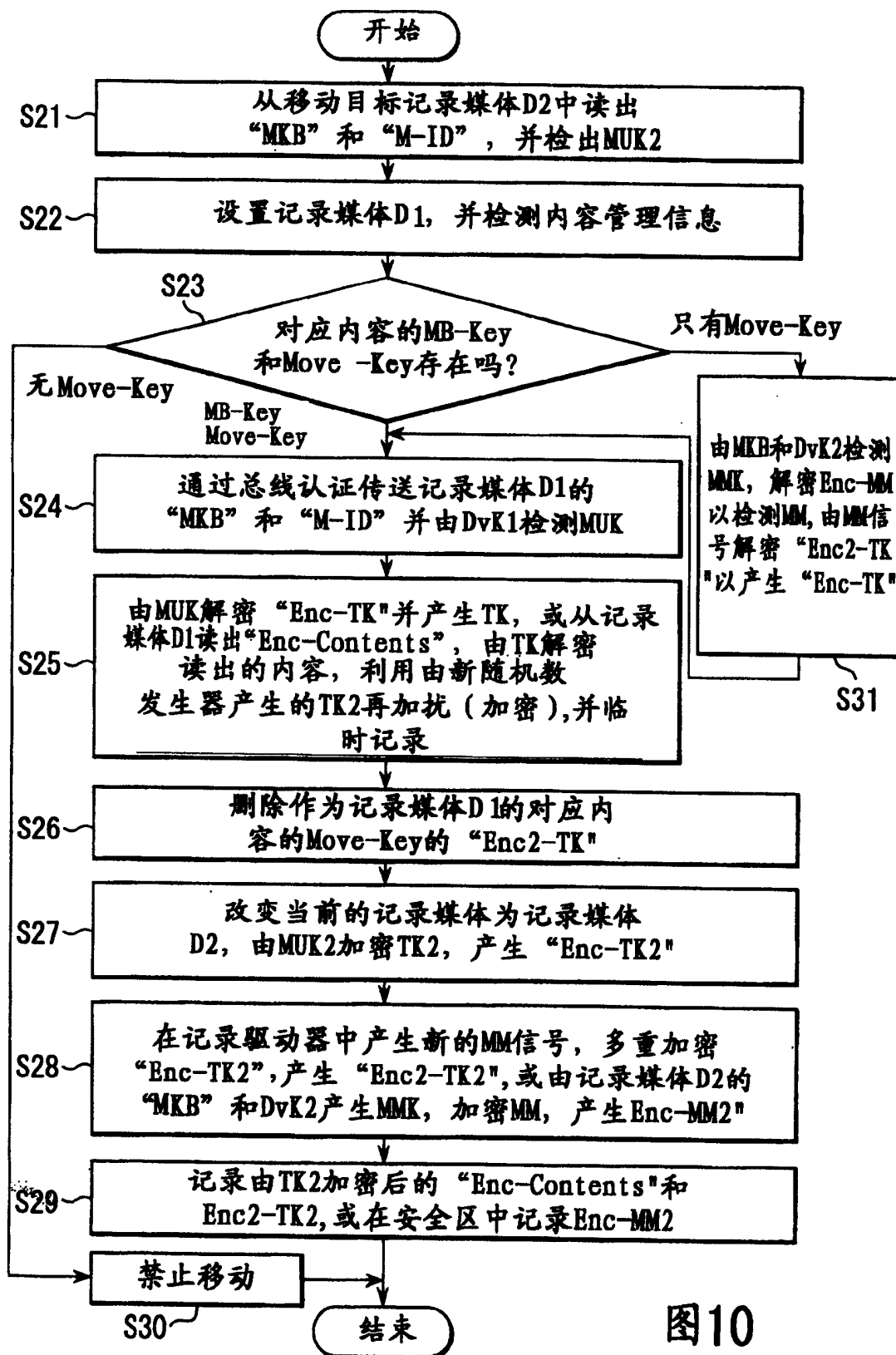
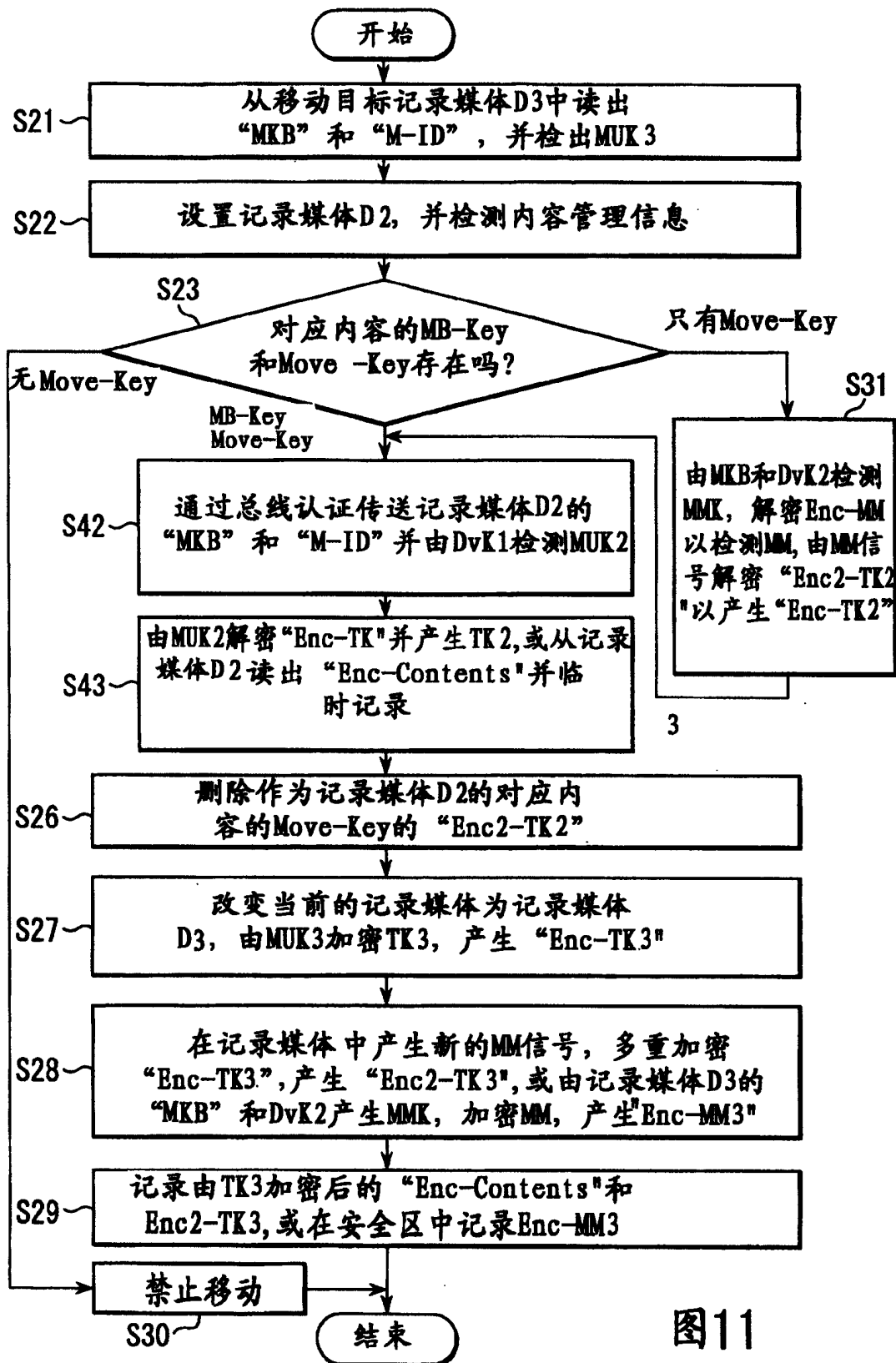


图10



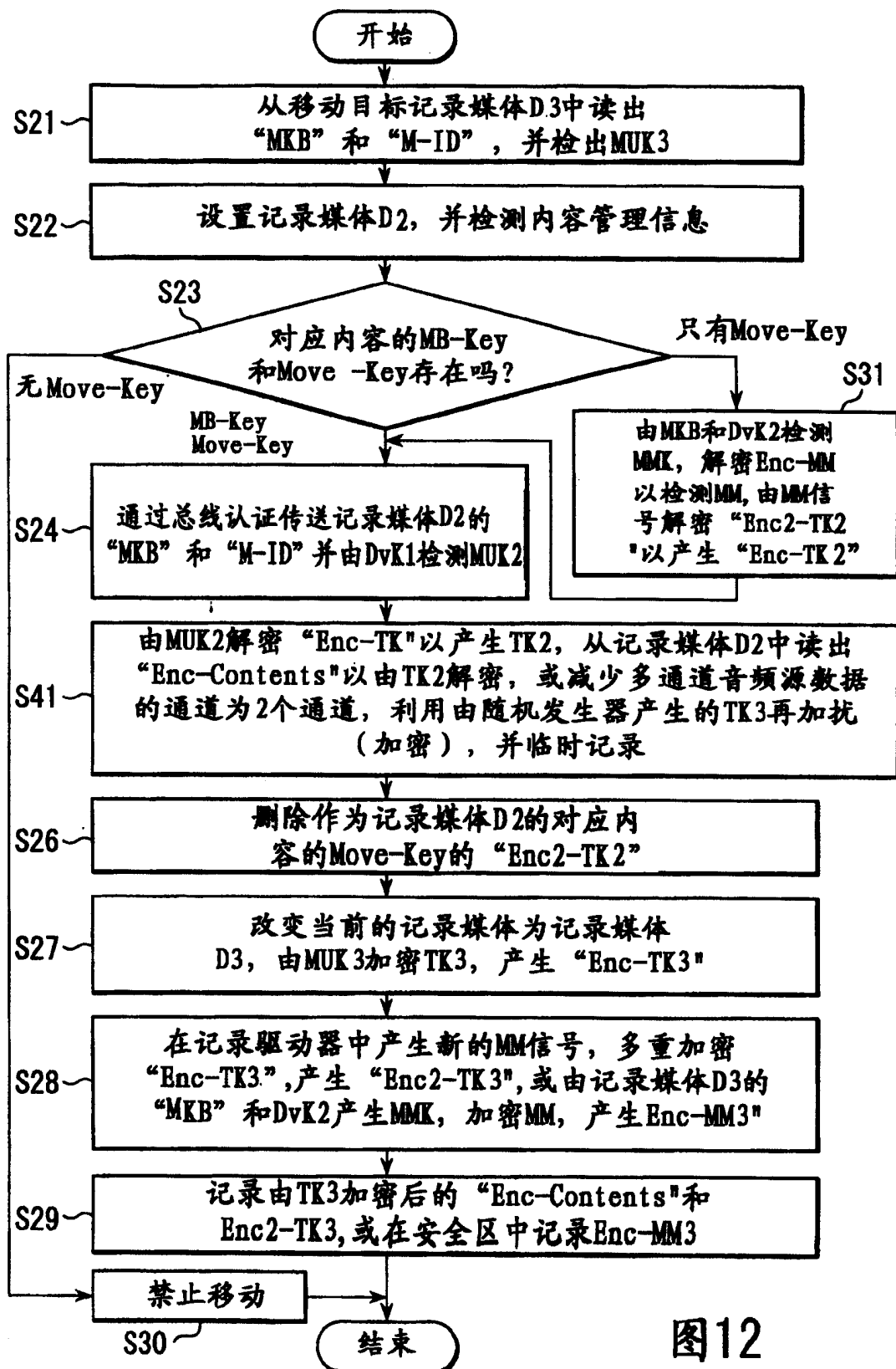
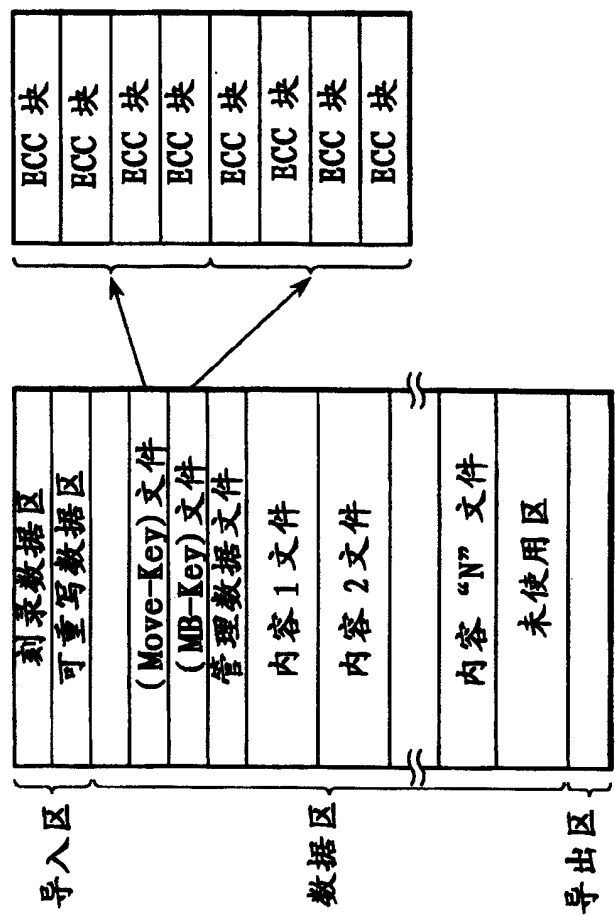
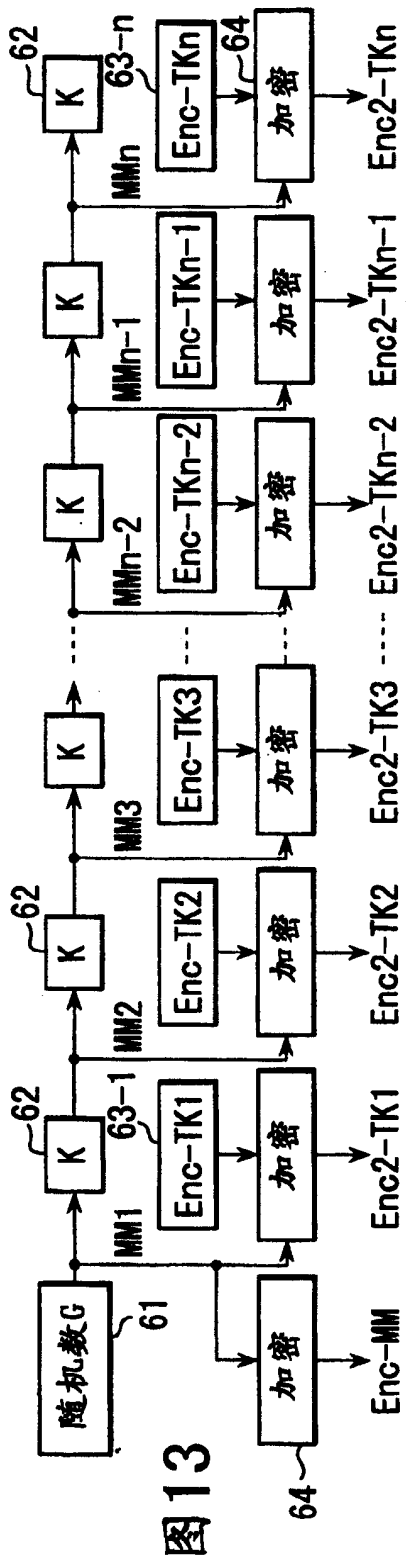


图12



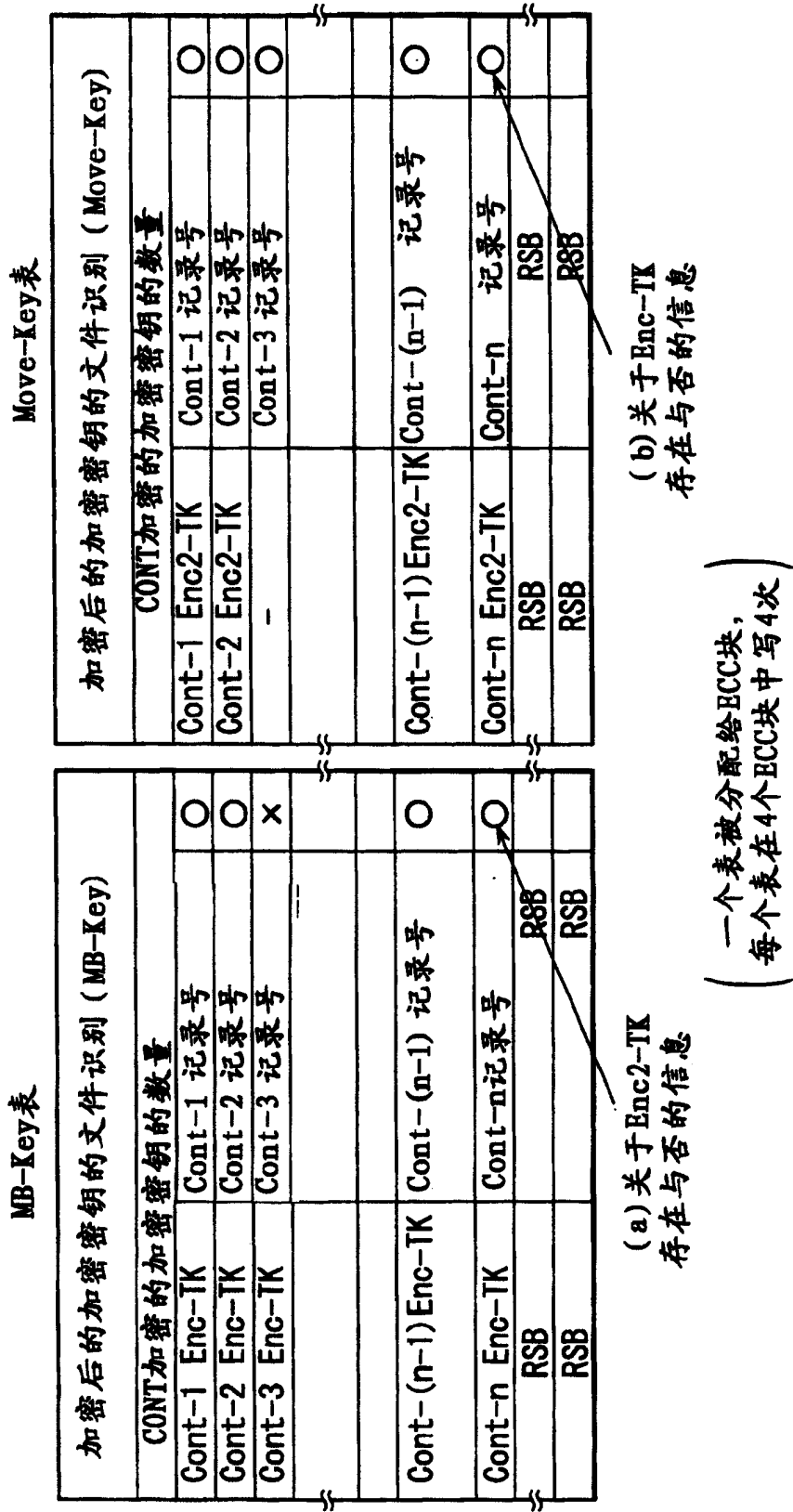


图15