[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/28 (2006.01)
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 00104046.4

[45] 授权公告日 2006 年 8 月 16 日

[11] 授权公告号 CN 1270470C

[22] 申请日 2000.3.14 [21] 申请号 00104046.4

[30] 优先权

[32] 1999. 3.15 [33] JP [31] 069151/99

[32] 1999. 6.24 [33] JP [31] 178188/99

[71] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 大石丈於 浅野智之 木原信之 横田哲平

审查员 刘剑波

[74] 专利代理机构 北京市柳沈律师事务所

代理人 黄小临

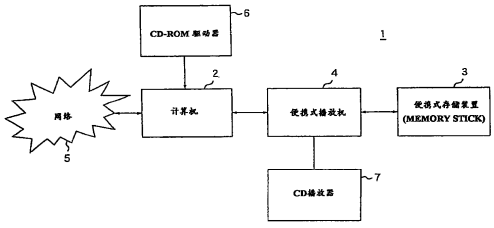
权利要求书 4 页 说明书 39 页 附图 27 页

[54] 发明名称

用于装置之间相互识别的数据处理系统和方法

[57] 摘要

第一相互识别单元中的存储单元存储主密钥数据，第二相互识别单元中的第二存储单元存储识别密钥数据。 随机数产生单元产生用来在各相互识别单元选择主密钥和相应的识别密钥的数值。 第一相互识别单元采用所选主密钥来产生所选识别密钥的估计值，并采用该估计值作为共用密钥执行与第二相互识别单元的相互识别。



1. 一种用于执行第一数据处理装置和第二数据处理装置之间的相互识别的数据处理系统，其中：

所述第一数据处理装置包括：

第一存储装置，用于存储多个不同的第一密钥数据；和

第一相互识别处理装置，用于从所述多个第一密钥数据中选出一个第一密钥，并使用所选第一密钥与所述第二数据处理装置进行相互识别，及

所述第二数据处理装置包括：

第二存储装置，用于存储多个不同的第二密钥数据；和

第二相互识别处理装置，用于从所述多个第二密钥数据中选出一个与由所述第一相互识别处理装置选出的第一密钥对应的第二密钥，并使用所述第二密钥与所述第一数据处理装置进行相互识别，

其中，所述第一数据处理装置还包括：第一随机数产生装置，用于产生第一随机数、并向所述第二相互识别处理装置输出所述第一随机数；

所述第二数据处理装置还包括：第二随机数产生装置，用于产生第二随机数、并向所述第一相互识别处理装置输出所述第二随机数；

所述第一数据处理装置还包括：第一密钥数据计算装置，用于使用所选第一密钥来计算由所述第二相互识别处理装置选出的所述第二密钥的估计值；并且

所述第二数据处理装置还包括：第二密钥数据计算装置，用于使用所选第二密钥来计算由所述第一相互识别处理装置选出的所述第一密钥的估计值。

2. 如权利要求 1 所述数据处理系统，其中：

所述第一和第二数据处理装置中的至少一个产生一随机数、并输出所述随机数；

所述第一相互识别处理装置根据所述随机数来选择所述第一密钥；及

所述第二相互识别处理装置根据所述随机数来选择所述第二密钥。

3. 如权利要求 1 所述数据处理系统，其中：

所述第一相互识别处理装置采用所述第二密钥的估计值作为一共用密钥，来执行与所述第二相互识别处理装置的相互识别。

4. 如权利要求 3 所述数据处理系统，其中：

所述第二数据处理装置还包括用于存储识别数据、并将所述识别数据输出到所述第一数据处理装置的装置；及

所述计算装置使用从所述第二数据处理装置输入的所述识别数据，来计算所述第二密钥的估计值。

5. 如权利要求 3 所述数据处理系统，其中：

所述第二数据处理装置的所述第二相互识别处理装置采用从所述第一数据处理装置输入的所述第一随机数及所选第二密钥作为变元，来执行单向散列函数运算，以计算第一处理结果，并将所述第一处理结果输出到所述第一数据处理装置；及

所述第一相互识别处理装置采用由所述第一随机数产生装置产生的所述随机数及所述第二密钥的估计值作为变元，来执行单向散列函数运算，以产生第二处理结果，并当从所述第二数据处理装置输入的所述第一处理结果与所述第二处理结果相匹配时，将所述第二数据处理装置识别为合法方。

6. 如权利要求 5 所述数据处理系统，其中：

所述第一数据处理装置的所述第一相互识别处理装置采用从所述第二数据处理装置输入的所述第二随机数及所述第二密钥的估计值作为变元，来执行第二单向散列函数运算，以计算第三处理结果，并将所述第三处理结果输出到所述第二数据处理装置；及

所述第二相互识别处理装置采用由所述第二数据处理装置的所述第二随机数产生装置产生的所述第二随机数及所选第二密钥作为变元，来执行第二单向散列函数运算，以产生第四处理结果，并当从所述第一数据处理装置输入的所述第三处理结果与所述第四处理结果相匹配时，将所述第一数据处理装置识别为合法方。

7. 如权利要求 1 所述数据处理系统，其中：

所述第一数据处理装置和所述第二数据处理装置接收密钥选择数据作为输入；

所述第一相互识别处理装置根据所述密钥选择数据从所述多个第一密钥数据中选择一个第一密钥；及

所述第二相互识别处理装置根据所述密钥选择数据从所述多个第二密钥数据中选择一个第二密钥。

8. 如权利要求 1 所述的数据处理系统，其中：

当所述第一相互识别处理装置和所述第二相互识别处理装置彼此将对方认作是合法方时，所述第一数据处理装置和所述第二数据处理装置输出用于对在所述第一和第二数据处理装置之间传送的数据进行解密的密钥数据。

9. 如权利要求 8 所述的数据处理系统，其中，所述第二数据处理装置还包括用于存储从所述第一数据处理装置输入的编码数据的装置。

10. 一种用于执行在第一数据处理装置和第二数据处理装置之间的相互识别的数据处理方法，该方法包括下列步骤：

在所述第一数据处理装置上，从多个第一密钥数据中选出一个第一密钥，并使用所选第一密钥与所述第二数据处理装置进行相互识别；及

在所述第二数据处理装置上，从多个第二密钥数据中选出一个与所选第一密钥对应的第二密钥，并使用所选第二密钥与所述第一数据处理装置进行相互识别，

其中，所述第一数据处理装置采用所选第一密钥，来计算由所述第二数据处理装置选出的所述第二密钥的估计值，

所述第一数据处理装置产生第一随机数，并将所述第一随机数输出到所述第二数据处理装置；

所述第二数据处理装置采用从所述第一数据处理装置输入的所述第一随机数及所选第二密钥作为变元，来执行单向散列函数运算，以计算第一处理结果，并将所述第一处理结果输出到所述第一数据处理装置；

所述第一数据处理装置采用所述第一随机数及所述第二密钥的估计值作为变元，来执行单向散列函数运算，以产生第二处理结果，并当从所述第二数据处理装置输入的所述第一处理结果与所述第二处理结果相匹配时，将所述第二数据处理装置识别为合法方；以及

所述第二数据处理装置产生第二随机数，并将所述第二随机数输出到所述第一数据处理装置；

所述第一数据处理装置采用从所述第二数据处理装置输入的所述第二随机数及所述第二密钥的估计值作为变元，来执行第二单向散列函数运算，以计算第三处理结果，并将所述第三处理结果输出到所述第二数据处理装置；以及

所述第二数据处理装置采用所述第二随机数及所选第二密钥作为变元，

来执行第二单向散列函数运算，以产生第四处理结果，并当从所述第一数据处理装置输入的所述第三处理结果与所述第四处理结果相匹配时，将所述第一数据处理装置识别为合法方。

11. 如权利要求 10 所述的数据处理方法，还包括下列步骤：

所述第一和第二数据处理装置中的至少一个产生一随机数，并输出所述随机数；

所述第一数据处理装置根据所述随机数来选择所述第一密钥；及

所述第二数据处理装置根据所述随机数来选择所述第二密钥。

12. 如权利要求 10 所述的数据处理方法，还包括下列步骤：

采用所述第二密钥的估计值作为一共用密钥，来执行所述第一数据处理装置与所述第二数据处理装置之间的相互识别。

13. 如权利要求 12 所述的数据处理方法，还包括将存储在所述第二数据处理装置中的识别数据输出到所述第一数据处理装置的步骤；并且所述计算步骤包括使用所述识别数据以计算所述第二密钥的估计值的步骤。

14. 如权利要求 10 所述的数据处理方法，还包括下列步骤：

所述第一数据处理装置和所述第二数据处理装置接收密钥选择数据作为输入；

所述第一相互识别处理装置根据所述密钥选择数据从所述多个第一密钥数据中选择一个第一密钥；及

所述第二相互识别处理装置根据所述密钥选择数据从所述多个第二密钥数据中选择一个第二密钥。

15. 如权利要求 10 所述的数据处理方法，还包括如下步骤：当所述第一数据处理装置和所述第二数据处理装置彼此将对方认作是合法方时，输出用于对在所述第一和第二数据处理装置之间传送的数据进行解密的密钥数据。

16. 如权利要求 15 所述的数据处理方法，还包括如下步骤：将从所述第一数据处理装置输入的编码数据存储到所述第二数据处理装置。

用于装置之间相互识别的数据处理系统和方法

技术领域

本发明涉及一种用于执行数据处理装置之间相互识别的数据处理系统和方法。

背景技术

为了防止非法使用音频和其他数据，即为了保护这些数据的版权，可限制第一数据处理装置向第二数据处理装置输出任何这种数据，除非执行各装置之间的相互识别并且每个装置被认作是合法方。

有众多用于执行这种相互识别处理的系统。一个示例为共用密钥系统。

在该共用密钥系统中，第一和第二数据处理装置共享单个共用密钥。例如，一个装置向另一装置通告它所产生的随机数，两个装置采用该随机数和共用密钥来执行操作，并且每个装置将处理结果输出给另一方。这些数据处理装置各将其本身的处理结果与从对方输入的结果相比较，从而当其结果匹配时将对方认作是合法方。

在这种共用密钥系统中，必须对合法方以外的人保守该共用密钥的秘密。如果该共用密钥被一非法方获取，则该非法方将被该系统错误地认作是合法方，从而能够非法使用数据。

发明内容

本发明是鉴于上述问题而提出的，本发明的目的是提供一种采用使用共用密钥的改进的相互识别技术的数据处理系统和方法。

通过阅读本说明书和附图，本发明的其他目的和优点将变得清楚。

为了解决上述问题并且实现上述目的，根据本发明，在第一数据处理装置和第二数据处理装置之间执行相互识别，其中所述第一数据处理装置包括：第一存储装置，用于存储多个不同的第一密钥数据；和第一相互识别处理装置，用于从所述多个第一密钥数据中选出一个第一密钥数据，并使用所选第一密钥数据与所述第二数据处理装置进行相互识别。所述第二数据处理

装置包括：第二存储装置，用于存储多个不同的第二密钥数据；和第二相互识别处理装置，用于从所述多个第二密钥数据中选出一个与由所述第一相互识别处理装置选出的第一密钥数据对应的第二密钥数据，并使用该第二密钥数据与所述第一数据处理装置进行相互识别，其中，所述第一数据处理装置还包括：第一随机数产生装置，用于产生第一随机数、并向所述第二相互识别处理装置输出所述第一随机数；所述第二数据处理装置还包括：第二随机数产生装置，用于产生第二随机数、并向所述第一相互识别处理装置输出所述第二随机数；所述第一数据处理装置还包括：密钥数据计算装置，用于使用所选第一密钥来计算由所述第二相互识别处理装置选出的所述第二密钥的估计值。

另外，根据本发明的一优选实施例，第一和第二数据处理装置中的至少一个产生一随机数，并将所产生的随机数通告给对方。相应地，第一相互识别处理装置根据该随机数来选择第一密钥数据，第二相互识别处理装置根据该随机数来选择第二密钥数据。

根据本发明的该优选实施例，所述第一相互识别处理装置采用所计算出的第二密钥数据作为一共用密钥，来执行与所述第二相互识别处理装置的相互识别。

另外，根据该优选实施例，所述第二数据处理装置的所述第二相互识别处理装置采用从所述第一数据处理装置输入的第一随机数及所选第二密钥数据作为变元，来执行单向 Hash(散列)函数运算，以计算第一处理结果，并将该第一处理结果输出到所述第一数据处理装置；并且，所述第一相互识别处理装置采用由所述第一随机数产生装置产生的随机数及所计算出的第二密钥数据作为变元来执行所述单向 Hash 函数运算，以产生第二处理结果，并当从第二数据处理装置输入的第一数据处理结果与第二处理结果相匹配时，将该第二数据处理装置识别为合法方。

另外，根据该优选实施例，所述第一数据处理装置的所述第一相互识别处理装置采用从所述第二数据处理装置输入的随机数及所计算出的第二密钥数据作为变元，来执行单向 Hash 函数运算，以计算第三处理结果，并将该第三处理结果输出到所述第二数据处理装置；并且，所述第二相互识别处理装置采用由所述第二数据处理装置的所述随机数产生装置产生的随机数及所选第二密钥数据作为变元，来执行单向 Hash 函数运算，以产生第四处

理结果，并当从第一数据处理装置输入的第三数据处理结果与第四处理结果相匹配时，将该第一数据处理装置识别为合法方。

此外，根据本发明的该优选实施例，所述第一数据处理装置和所述第二数据处理装置接收密钥选择数据作为输入，其中所述第一相互识别处理装置根据该密钥选择数据从多个第一密钥数据中选择一个第一密钥数据，并且所述第二相互识别处理装置根据该密钥选择数据从多个第二密钥数据中选择一个第二密钥数据。

最后，本发明的数据处理方法是一种用于执行在第一数据处理装置和第二数据处理装置之间的相互识别的方法，该方法包括：在所述第一数据处理装置上，从多个第一密钥数据中选出一个第一密钥数据，并使用所选第一密钥数据与所述第二数据处理装置进行相互识别；在所述第二数据处理装置上，从多个第二密钥数据中选出一个与所选第一密钥数据对应的第二密钥数据，并使用该第二密钥数据与所述第一数据处理装置进行相互识别，其中，所述第一数据处理装置采用所选第一密钥，来计算由所述第二数据处理装置选出的所述第二密钥的估计值，所述第一数据处理装置产生第一随机数，并将所述第一随机数输出到所述第二数据处理装置；所述第二数据处理装置采用从所述第一数据处理装置输入的所述第一随机数及所选第二密钥作为变元，来执行单向散列函数运算，以计算第一处理结果，并将所述第一处理结果输出到所述第一数据处理装置；所述第一数据处理装置采用所述第一随机数及所述第二密钥的估计值作为变元，来执行单向散列函数运算，以产生第二处理结果，并当从所述第二数据处理装置输入的所述第一处理结果与所述第二处理结果相匹配时，将所述第二数据处理装置识别为合法方；以及所述第二数据处理装置产生第二随机数，并将所述第二随机数输出到所述第一数据处理装置；所述第一数据处理装置采用从所述第二数据处理装置输入的所述第二随机数及所述第二密钥的估计值作为变元，来执行第二单向散列函数运算，以计算第三处理结果，并将所述第三处理结果输出到所述第二数据处理装置；以及所述第二数据处理装置采用所述第二随机数及所选第二密钥作为变元，来执行第二单向散列函数运算，以产生第四处理结果，并当从所述第一数据处理装置输入的所述第三处理结果与所述第四处理结果相匹配时，将所述第一数据处理装置识别为合法方。

因此，本发明包括几个步骤，以及这些步骤中的一个或多个与其他各步

骤的相互关系，将示出体现结构、部件组合及适于实现这些步骤的各部分排列的特征(均将在下面的详细公开中举例说明)的装置。

附图说明

通过参照下面的描述和附图，将更完整地理解本发明，附图中：

图 1 表示根据本发明构成的音频系统的总体系统结构；

图 2 表示图 1 所示便携式存储装置和便携式播放器的内部结构；

图 3 表示图 2 所示便携式存储装置的存储单元中存储的数据；

图 4 表示图 2 所示便携式装置的闪速存储器中存储的数据；

图 5 表示图 2 所示便携式存储装置中存储的作为子目录的再现管理文件 PBLIST.MSF 的数据结构；

图 6 表示 ATRAC3 数据文件的数据结构，该数据文件被分成预定单位长度的多个块，并且包含属性首标；

图 7 表示再现管理文件 PBLIST 的总体数据结构；

图 8 表示包含首标部、主数据部、附加信息数据部的再现管理文件 PBLIST 的详细数据结构；

图 9 表示图 2 所示便携式播放器的存储单元中存储的数据的结构；

图 10 表示 ATRAC3 数据文件的详细数据结构；

图 11 表示 ATRAC3 数据文件属性首标的上部的数据结构；

图 12 表示 ATRAC3 数据文件属性首标中部的数据结构；

图 13 表示用于对记录模式、记录时间和其他信息进行相关的相关表；

图 14 是表示复制控制状态的表；

图 15 表示 ATRAC3 数据文件属性首标的下部的数据结构；

图 16 表示 ATRAC3 数据文件的数据块首标的数据结构；

图 17 表示图 2 所示便携式播放器的存储单元中存储的数据；

图 18 解释的是图 2 所示便携式播放器的加密/解密单元中的 CBC 加密模式；

图 19 解释的是图 2 所示便携式播放器的加密/解密单元中的 CBC 解密模式；

图 20 是解释图 2 所示从便携式播放器到便携式存储装置的写入操作的流程图；

图 21 表示由图 2 所示相互识别单元进行的对识别密钥数据 IK_j 的选择;

图 22 解释的是在图 2 所示便携式存储装置和便携式播放器之间的相互识别处理;

图 23 解释的是会话密钥数据 Sek 的创建;

图 24 解释的是图 2 所示从便携式播放器到便携式存储装置的音频数据写入操作;

图 25 是解释图 2 所示从便携式存储装置到便携式播放器的读取操作的流程图;

图 26 解释的是图 2 所示从便携式存储装置到便携式播放器的音频数据读取操作;

图 27 解释的是由便携式播放器的编辑模块执行的轨道数据文件的分离编辑;

图 28 表示在图 27 的分离编辑之后轨道(1)的簇(cluster)CL(2)中的数据;

图 29 表示在图 27 的分离编辑之后轨道(2)的簇 CL(0)中的数据;

图 30 是表示在由图 2 所示便携式播放器的编辑模块执行的分离编辑步骤上创建轨道密钥数据和新轨道数据文件的部分(part)密钥数据的流程图;

图 31 解释的是由图 2 的便携式播放器的编辑模块执行的轨道数据文件的耦合编辑; 和

图 32 是表示用于创建由图 2 所示便携式播放器的编辑模块中新创建的轨道数据文件(3)的部分(1)和(2)的部分密钥数据的流程图。

具体实施方式

图 1 是根据本发明构成的音频系统 1 的系统结构的示意图。该音频系统 1 例如具有计算机 2、便携式存储装置 3、便携式播放器 4、CD-ROM 驱动器 6 及 CD 播放器 7。音频系统 1 对应于本发明的数据处理系统，便携式存储装置对应于本发明的存储装置，而便携式播放器 4 对应于本发明的数据处理装置。

在该实施例中，本发明的第一密钥数据对应于内容密钥数据 CK，第二密钥数据对应于部分密钥数据 PK，第三密钥数据对应于暂时密钥数据 TMK，第四密钥数据对应于块种子(block seed)数据 BS，而第五密钥数据对应于块密钥数据。

图 2 是图 1 所示便携式存储装置 3 及便携式播放器 4 的内部结构的示意图。在该实施例中，本发明的模块使用密钥数据计算装置对应于图 2 中所示的密钥创建/密钥处理单元 62，加密装置对应于加密/解密单元 64，而密钥数据处理装置对应于编辑模块 44。

计算机 2

计算机连接到网络 5，它经网络 5 从提供 EMD(电子音乐分布)或其他服务的服务提供商的主计算机(未示出)接收音频数据(轨道(track)数据)，根据需要对所接收音频数据进行解密，并将该数据输出到便携式播放器 4。当接收内容数据时，计算机 2 与服务提供商的主计算机交换有关识别、记费及其他的必要信息。计算机 2 还将从 CD-ROM 驱动器 6 输入的音频数据传送到便携式播放器 4。

便携式存储装置 3

如图 2 进一步所示，便携式存储装置 3 中设有内置可重写半导体存储器，如市面上可见的商标为 Memory Stick 的 Sony(索尼)公司的闪速存储器 34。便携式存储装置 3 还具有主控模块 31、通信接口 32、控制模块 33 及闪速存储器管理模块 35。

控制模块 33

控制模块 33 是专用于加密的具有多层结构的单片集成电路。各内部存储单元由诸如铝层的伪层夹住。另外，控制模块 33 具有范围较窄的工作电压或工作频率，并且是不能篡改的，从而不能由外部非法地读取任何存储数据。

如图 2 所示，控制模块 33 包含有随机数产生单元 50、存储单元 51、密钥创建/处理单元 52、相互识别单元 53、加密/解密单元 54、及控制单元 55。随机数产生单元 50 在接收到随机数产生指令时产生 64 比特(8 字节(byte))随机数。存储单元 51 可包含 EEPROM(电可擦除只读存储器)或其他非易失性

存储器，它存储密钥数据和为识别所需的其他各种数据。

图3表示存储在存储单元51中的数据。该存储数据包括识别密钥数据IK_0至IK_{31}、装置识别数据ID_m、及存储使用密钥数据Skm。

识别密钥数据IK_0至IK_{31}是当便携式存储装置3执行与便携式播放器4的相互识别处理时使用的密钥数据。每当执行相互识别处理时，随机地从识别密钥数据IK_0至IK_{31}中选出一个识别密钥。要注意的是，不能从便携式存储装置3的外部读取识别密钥数据IK_0至IK_{31}和存储使用密钥数据Skm。装置识别数据ID_m是唯一地附着在每个便携式存储装置3中的识别数据，并且当便携式存储装置3执行与便携式播放器4的相互识别处理时被读出。当对内容密钥数据CK进行加密并将其存储在闪速存储器34中时(如后所述)，使用存储使用密钥数据Skm。

密钥创建/处理单元52通过执行MAC(消息验证代码)运算和/或由ISO/IEC9797标准定义的其他各种运算来创建密钥数据。目前，该MAC运算使用作为DES(数据加密标准)的由FIPSPUB46-2定义的“块加密算法”。MAC运算是一种单向Hash(散列)函数，其中将具有任意长度的数据压缩成固定长度，并且由一保密密钥来确定函数值。

相互识别单元53在从便携式播放器4接收到音频数据并将其写入闪速存储器34之前执行与便携式播放器4的相互识别处理。相互识别单元53在从闪速存储器34读取音频数据并将其输出到便携式播放器4之前执行与便携式播放器4的相互识别处理。相互识别单元53还执行MAC运算作为相互识别处理的一部分。存储在存储单元51中的数据用来执行相互识别处理。

加密/解密单元54采用DES、IDEA、MISTY或其他块加密算法之一来执行加密和解密。所使用的模式为ECB(电子码本)模式和CBC(加密块链接)模式，它们在FIPS PUB81“DES运算模式(DES MODES OF OPERATION)”中规定。在基于ECB和CBC模式的块加密/解密中，通过采用指定的密钥数据来对指定数据进行加密/解密。控制单元55集中控制随机数产生单元50、存储单元51、密钥创建/处理单元52、相互识别单元53及加密/解密单元54的处理。

闪速存储器34

一旦便携式播放器4被相互识别单元53认作是合法方，则将从播放器4

输入的音频数据写入闪速存储器 34。反过来，一旦便携式播放器 4 被相互识别单元 53 认作是合法方，则可将音频数据从闪速存储器 34 输出到便携式播放器 4。闪速存储器 34 的存储容量为 32Mbytes(兆字节)。

如图 4 所示，闪速存储器 34 存储再现管理文件 100，其后为一系列轨道数据文件 101_0、101_1、101_2 及 101_3。再现管理文件 100 包含用于管理轨道数据文件 101_0 至 101_3 的再现的数据。轨道数据文件 101_0 至 101_3 包含实际的轨道数据(音频数据)。在本实施例中，轨道数据用于表示一首歌的音频数据。

图 5 和 6 表示再现管理文件如何被用来实现样本文件格式。ATRAC3 是在 Mini-Discs(迷你盘)™(“MD”)中使用的自适应变换声音编码(“ATRAC”)格式的一种修改形式，它是用于音频数据的高效编码格式。图 5 表示再现管理文件的结构。图 6 表示 ATRAC3 数据文件的文件结构。ATRAC3 数据文件由属性首标和每个音乐节目的加密音乐数据区构成。再现管理文件和 ATRAC3 属性首标的长度均为固定的 16KB(一个块)。

图 5 所示的再现管理文件由首标、存储器卡名 NM-1S(对于一个字节码)、存储器卡名 NM2-2S(对于两个字节码)、节目再现序列表 TRKTBL、及附加信息区 INF-S 组成。位于数据文件开头的属性首标(图 6 中所示)由首标、节目名 NM1(对于一个字节码)、节目名 NM2(对于两个字节码)、轨道消息 TRKINF(如轨道密钥信息)、部分信息 PRTINF、及附加轨道信息区 INF 组成。首标包括有关各部分总数、轨道名、附加信息区尺寸等的信息。

属性首标后面是 ATRAC3 音乐数据。该音乐数据以 16KB 块分段，每个块以一首标开始。该首标包含用于对加密数据进行解密的初始值。仅对 ATRAC3 数据文件的音乐数据进行加密。因此，不对再现管理文件、首标等进行加密。

图 7 是表示再现管理文件的详细数据结构的示意图；图 8 表示图 7 中再现管理文件的首标部和剩余部。该再现管理文件包含32字节的首标、名NM1-S区(256 字节)(用于存储器卡)、名 NM2-S 区(512 字节)、内容密钥区、MAC 区、S-YMDhms 区、再现序列管理表 TRKTBL 区(800 字节)、存储器卡附加信息 INF-S 区(14720 字节)、及冗余首标信息区。该再现管理文件中这些区的每个的开始位置是预定的。

如图 8 所示，开始的 32 字节(0x0000)至(0x0010)用于首标。在该文件中，将 16 字节区称作槽(slot)。该首标放置在由 0x000 和 0x0010 表示的第一和第

二槽中。由“保留”表示的区为未定义区。通常，将空字节(0x00)写入该保留区中。但是，即使将数据写入保留区中，仍忽略该数据。保留区将被用于文件格式的将来更新。未被使用的任选区被看成保留区。另外，再现管理文件首标包含下列定义的区。

=BLKID-TK0(4 字节)

含义：块 ID(标识符) 文件 ID

功能：识别再现管理文件的顶部

值：固定值=“TL=0”(例如，0x544C2D30)

=MCode(2 字节)

含义：制作者码

功能：识别记录器/播放器的标记和模式

值：高阶 10 比特(制作者码)；低阶 6 比特(模式码)

=REVISION(4 字节)

含义：PBLIST 的重写次数

功能：每当重写再现管理文件时增加。

值：以 0 开始，并递增 1。

=SY1C+l(2 字节)

含义：写入 NM1-S 区的存储器卡名(一字节码)的属性

功能：将字符码和语言码表示为一字节码

值：字符码(C)：高阶 1 字节

00：非字符码，二进制数

01：ASCII(美国信息交换标准码)

02：ASCII + KANA(假名)

03：修改的 8859-1

81：MS-JIS

82：KS C 5601-1989

83：GB(大不列颠)2312-80

90：S-JIS(日本工业标准)(用于话音)

语言码(L)：低阶一字节根据 EBU 技术 3258 标准来识别语言

00：未设定

08：德语

09：英语

0A：西班牙语

0F：法语

15：意大利语

1D：荷兰语

65：韩语

69：日语

75：汉语

当未记录数据时，该区全部为 0。

=SN2C+L(2 字节)

含义：NM2-S 区中存储器卡名的属性

功能：将字符码和语言码表示为一字节码

值：与 SN1C+L 同

=SINFSIZE(2 字节)

含义：INF-S 区中存储器卡的附加信息的总尺寸

功能：将数据尺寸表示为 16 字节的增量。当不记录数据时，该区全部为 0。

值：尺寸：0x0001 至 0x39C(924)

=T-TRK(2 字节)

含义：总轨道数

功能：表示总轨道的数

值：1 至 0x190(最多 400 个轨道)

当不记录数据时，该区全部为 0。

=VerNo(2 字节)

含义：格式版本号

功能：表示主版本号(高阶一字节)和次版本号(低阶一字节)

值：0x0100(版本 1.0)

0x0203(版本 2.3)

接下来，将描述该首标前的区。

=NM1-S

含义：存储器卡名(为 1 字节码)

功能：将存储器卡名表示为一字节码(最大 256)。在该区结尾处，写入结束码(0x00)。该尺寸由该结束码计算。当不记录数据时，从该区的开头(0x0020)开始记录至少一个字节的空字节(0x00)。

值：各种字符码

NM2-S

含义：存储器卡名(为 2 字节码)

功能：将存储器卡名表示为 2 字节码(最大 512)。在该区结尾处，写入结束码(0x00)。该尺寸由该结束码计算。当不记录数据时，从该区的开头(0x0120)开始记录至少一个字节的空字节(0x00)。

值：各种字符码

=CONTENTS KEY

含义：音乐节目的值。用 MG(M)保护并被存储。与 CONTENTS KEY(内容密钥)相同。

功能：用作计算 S-YMDhms 的 MAC 所必须的密钥

值：0 至 0xFFFFFFFFFFFFFFFF

=MAC

含义：假造的版权信息校验值

功能：表示以 S-YMDhms 和 CONTENTS KEY 产生的值

值：0 至 0xFFFFFFFFFFFFFFFF

=S-YMDhms(4 字节)(任选)

含义：由记录器/播放器以可靠时钟记录的年、月、日、小时、分钟、秒。

功能：识别最后记录的数据和时间。在 EMD 情况下，该区为强制的。

值：比特 25 至 31：年 0 至 99(1980 至 2079)

比特 21 至 24：月 0 至 12

比特 16 至 20：日 0 至 31

比特 11 至 15：小时 0 至 23

比特 05 至 10：分钟 0 至 59

比特 00 至 04：秒 0 至 29(两秒间隔)

= TRK-nnn

含义：再现的 ATRAC3 数据文件的 SQN(序列)号

功能：表示 TRKINF 的 FN0

值：1 至 400(0x190)

当无轨道时，该区全部为 0。

=INF-S

含义：存储器卡的附加信息(例如，对应于相片、歌曲、向导等的信息)

功能：用一首标表示可变长度附加信息。可使用多种类型的附加信息。每种类型的附加信息具有 ID 和一数据尺寸。包含一首标的每个附加信息区由至少 16 个字节和 4 字节的倍数组成。有关细节请参见后面的部分。

值：参照“附加信息的数据结构”部分。

在该再现管理文件的最后的槽中，冗余地从该首标写入 BLKID-TL0、MCode 和 REVISION 区的副本。

如果一存储器卡意外地脱落，或在将数据记录到该卡中时记录器/播放器的电源关断，则应检测终止错误。如上所述，REVISION 区被放置在每个块的开头和结尾。每当写入数据时，便增大 REVISION 区的值。如果在写一块时的中间出现终止错误，则位于块开头的 REVISION 区的值将不与位于块尾部的 REVISION 区的值相匹配。两个 REVISION 区的这种偏差使得能够以高概率确定终止错误。当检测到这种异常终止时，产生告警，如差错消息。

另外，由于将固定值 BLKID-TL0 写入一个块(16KB)的开头处，因此，该

固定值可被用作恢复数据的基准。换言之，该固定值能够确定文件类型。由于将固定值 BLKID-TL0 冗余地写入每个块的首标中和结尾处，因此，保证了可靠性。此外，还可冗余地记录整个再现管理文件。

由于 ATRAC3 数据文件中的数据量远大于轨道信息管理文件中的数据量，因此，ATRAC3 数据文件没有冗余地记录。代之以，使用 CONNUM0 和 BLOCK SERIAL 值来帮助恢复丢失的 ATRAC3 数据(如将在后面叙述的)。另外，一个 ATRAC3 数据文件可由多个分散的块组成。为了识别相同文件的各块，使用 CONNUM0，而为了合并各块的顺序，则使用 BLOCK SERIAL。同样，如上所述，在每个块的开头和结尾冗余地记录制造者码(MCode)。从而识别已经被不正确地记录的文件的制造者。

图 8 表示附加信息区的结构。该附加信息区由首标及附加可变长度数据组成，该首标包括如下数据：

=INF

含义：字段 ID

功能：表示附加信息的开始(固定值)

值：0x69

=ID

含义：附加信息密钥码

功能：表示附加信息的分类

值：0 至 0xFF

=SIZE

含义：单个附加信息的尺寸

功能：表示每种类型附加信息的尺寸。尽管未限制数据尺寸，但它应至少为 16 字节和 4 字节的倍数。数据其余部分应采用空值填充(0x00)。

值：16 至 14784(0x39C0)

Mcode

含义：制造者码

功能：识别记录器/播放器的制造者和模式

值：高阶 10 比特(制造者码)，低阶 10 比特(机器码)

=C+L

含义：从字节 12 开始的数据区中的字符的属性

功能：将字符码和语言码表示为一字节码

值：与 SNC+L 相同

=DATA

含义：单个附加信息

功能：以可变长度数据表示每种附加信息。实数据始终从字节 12 开始。实数据的长度(尺寸)应至少为 4 字节和 4 字节的倍数。数据区的其余部分应采用空值填充(0x00)。

值：对应于每种类型的附加信息的内容来单独定义。

接下来，将描述轨道数据文件 101_1 至 101_3，如图 9 所示。轨道数据文件 101_0 包括一个部分，该部分包括 5 个簇 CL(0)、CL(1)、CL(2)、CL(3)和 CL(4)。构成轨道数据文件 101_0 的部分以簇 CL(0)的开头开始，并且在簇 CL(4)的声音单元 SU(4)结束。

要注意的是，每个轨道数据文件 101_0 至 101_3 具有如图 9 所示基本上相同的结构，但簇中的各部分的号、簇号、及声音单元 SU 的号独立地确定，并且可随轨道数据文件而发生变化。

接下来，将描述音乐节目和 ATRAC3 数据文件之间的关系。一个轨道等效于一个音乐节目。另外，一个音乐节目由一个 ATRAC3 数据组成(见图 6)。该 ATRAC3 数据文件一次将一个簇记录到存储器卡 40 中。每个簇的容量为 16KB。每个簇中仅包含一个文件。闪速存储器 42 的最小可擦除数据单元是一个块。块与簇或扇区是同一个意思。

一个音乐节目(或轨道)通常记录在轨道数据文件的一个部分中。但是，当对节目进行编辑时，该音乐节目被分离成多个部分。包含单个音乐节目的一个或多个部分之间的关系由存储在每个音乐节目属性首标中的部分信息 PRTINF(参见图 6)管理。部分尺寸由部分信息 PRTINF 的部分尺寸 PRTSIZE(4 字节)表示。尺寸 PRTSIZE 的头两个字节表示当前部分中全部簇的数目。接下

来的两个字节分别表示第一和最后簇的开始声音单元(SU)和结束声音单元(SU)。通过对各部分的这种标记，可跟踪在编辑期间出现的音乐数据的移动。

SU 是根据 ATRAC3 格式压缩的部分的最小单元。一个 SU 由 44.1kHz 的 1024 个样本(1024×16 比特×2 个信道)，并可以 10 为系数进行压缩。这对应于约 23msec 的音频。通常，单个部分包含几千个 SU。因此，由 42 个 SU 构成的簇存储约 1 秒的音频。

理论上讲，构成一个轨道的部分的最大数为 645。但是，任意给定轨道中可用部分的实际数目受首标、节目名、附加数据、即附加信息尺寸的限制。

图 10 是表示在 1 SU 为 N 字节(例如 N=384 字节)时 ATRAC3 数据文件 A3Dnnnn 的数据排列的示意图。图 10 还表示了数据文件的属性首标(1 个块)和音乐数据文件(1 个块)以及两个块(16×2=32k 字节)的每个槽的第一字节(0x0000 至 0x7FFF)。如图 11 所示，属性首标的头 32 个字节被用作首标；256 个字节被用作音乐节目区 NM1(256 个字节)；512 个字节被用作音乐节目标题区 NM2(512 字节)。ATRAC3 数据文件的首标包含如下区：

=BLKID-HD0(4 字节)

含义：块 ID 字段 ID

功能：识别 ATRAC3 数据文件的顶部

值：固定值= “HD=0” (例如，0x48442D30)

=MCode(2 字节)

含义：制作者码

功能：识别记录器/播放器的制作者和模式

值：高阶 10 比特(制作者码)；低阶 6 比特(机器码)

=BLOCK SERIAL(4 字节)

含义：轨道序列号

功能：从 0 开始并递增 1。即使对音乐节目进行编辑，该值仍不改变。

值：0 至 0xFFFFFFFF

=N1C+L(2 字节)

含义：表示轨道(音乐节目文件)的数据(NM1)的属性。

功能：将 NM1 的字符码和语言码表示为一字节码。

值：与 SN1C+L 相同

=N2C+L(2 字节)

含义：表示轨道(音乐节目文件)的数据(NM2)的属性。

功能：将 NM1 的字符码和语言码表示为一字节码。

值：与 SN1C+L 相同

=INFSIZE(2 字节)

含义：当前轨道的附加信息的总尺寸

功能：将数据尺寸表示为 16 字节的倍数。当不记录数据时，该区应全部为 0。

值：0x0000 至 0x3C6(966)

=T-PRT(2 字节)

含义：字节总数

功能：表示构成当前轨道的各部分数。通常，T-PTR 的值为 1。

值：1 至 285(645，十进制)

=T-SU(4 字节)

含义：SU 总数

功能：表示对应于节目执行期间的一个轨道内的 SU 总数。

值：0x01 至 0x001FFFFF

=INX(2 字节)(任选)

含义：INDEX(索引)的相对位置

功能：用作表示音乐节目表示部的顶部的指针。INX 的值由其 SU 的数目被 4 除的值指定，作为节目的当前位置。INX 的值是 SU 的数的 4 倍(大约 93msec(毫秒))。

值：0 至 0xFFFF(最大值，约 6048 秒)

=XT(2 字节)(任选)

含义：INDEX 的再现时段

功能：采用其SU数目被4除的值指定由INX-nnn指定的再现时段。INDEX 的值为通常 SU 的 4 倍(约 93msec(毫秒))。

值：0x0000(未设定)；0x01 至 0xFFFF(至 6084sec(秒))；0xFFFF(至音乐节目的结尾)。

接下来，将描述音乐节目标题区 NM1 和 NM2。

=NM1：

含义：音乐节目标题的字符串

功能：将音乐节目标题表示为一字节码(最多 256 个字符)(可变长度)。该标题区应以结尾码结束(0x00)。应根据该结尾码计算尺寸。当不记录数据时，应从该区的开头(0x0020)开始记录至少一个字节的记录空值(0x00)。

值：各种字符码

=NM2

含义：音乐节目标题的字符串

功能：将音乐节目标题表示为二字节码(最多 512 个字符)(可变长度)。该标题区应以结尾码结束(0x00)。应根据该结尾码计算尺寸。当不记录数据时，应从该区的开头(0x0120)开始记录至少两个字节的记录空值(0x100)。

值：各种字符码

从属性首标的固定位置(0x320)开始的 80 字节数据被称作轨道信息区 TRKINF。该区主要用于总体管理特定轨道的保密信息和复制控制信息。图 12 表示 TRKINF 的一部分。该 TRKINF 区包含下列区。

=CONTENTS KEY(8 字节)

含义：每个音乐节目的值。CONTENTS KEY(内容密钥)的值在存储器卡的保密块中保护，然后被存储。

功能：用作用于再现音乐节目的密钥。它被用来计算 MAC 的值。

值：0 至 0xFFFFFFFFFFFFFFFF

=MAC(8 字节)

含义：假造的版权信息校验值

功能：以多个包括内容累积号及保密序列号的 TRKINF 的值表示所产生的值。保密序列号是记录在存储器卡保密区内的序列号。非版权保护类型记录器不能从存储器卡的保密区读取数据。另一方面，版权保护类型记录器和以能够从存储器卡读取数据的程序运行的计算机能够访问该保密区。

=A(1 字节)

含义：部分的属性

功能：表示诸如一部分的压缩模式的信息。

值：参见后面的讨论(参见图 12 和 13)。

接下来，将描述区 A 的值。在下面的描述中，将单声道模式(N=0 或 1)定义为一特定联合模式，其比特 7=1，子信号=0，并且主信号=(L+R)。无版权保护能力的播放器可忽略信息比特 2 和 1。

区 A 的比特 0 表示是否关断加重(emphasis)。比特 2 指定数据类型，如音频数据、FAX(传真)数据等。比特 3 未定义。ATRAC3 的模式信息由比特 4、5 和 6 的组合表示，如图 13 表示。换言之，N 表示模式，并且由 3 个比特表示。图 13 中，对于列出的 5 种类型的模式(单声道(N=0 或 1)、LP(N=2)、SP(N=4)、EX(N=4)和 HQ(N=7))，提供记录时段(仅 64MB 存储器卡)、数据发送率和每个块的 SU 数。每个 SU 中的字节数取决于所定义的模式。在单声道模式中，1 SU 为 136 个字节。在 LP 模式中，1 SU 为 192 个字节。在 SP 模式中，1 SU 为 304 个字节。在 EX 模式中，1 SU 为 384 个字节。在 HQ 模式中，1 SU 为 512 个字节。区 A 的比特 7 表示 ATRAC3 类型模式(0：双；1：联合)。

下面举例描述 SP 模式中使用的 64MB 存储器卡。64MB 存储器卡具有 3968 个块。在 SP 模式中，由于 1 SU 为 304 个字节，因此，一个块由 53 个 SU 组成。因此，1 SU 等效于(1024/44100)秒。因此 64MB 存储器卡存储(1024/44100)×53×(3968-10)=4863 秒=81min(分钟)。发送速率为(44100/1024)×304×8=104737bps。

回过来参照图 12，将描述 TRKINF 的区的其余部分。

=LT(一字节)

含义：再现限制标志(比特 7 和 6)及保密分区(比特 5 至 0)。

功能：表示当前轨道的限制。

值：比特 7：0=无限制，1=限制

比特 6：0=未期满，1=期满

比特 5 至 0：保密分区(除 0 以外的再现禁止)

=FNo(2 字节)

含义：文件号

功能：表示最初记录的轨道号，该轨道号指定记录在存储器卡保密区中的 MAC 计算值的位置。

值：1 至 1x190(400)

=MG(D) SERIAL-nnn(16 字节)

含义：表示记录器/播放器的保密块(保密 IC 20)的序列号。

功能：每个记录器/播放器的唯一值。

值：0 至 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

=CONNUM(4 字节)

含义：内容累积号

功能：表示对每个音乐节目累积的唯一值。该值由记录器/播放器的保密块来管理。该值的上限为 232，即 4,200,000,000，用于识别记录的节目。

值：0 至 0xFFFFFFFF

=YMDhms-S(4 字节)(任选)

含义：具有再现限制的轨道的再现开始日期和时间。

功能：以 EMD 表示允许数据再现的日期和时间。

值：与其他区的日期和时间的表示相同。

=YMDhms-E(4 字节)(任选)

含义：具有再现限制的轨道的再现开始日期和时间。

功能：以 EMD 表示数据再现期满的日期和时间。

值：与其他区的日期和时间的表示相同。

=MT(1 字节)(任选)

含义：允许的再现次数的最大值

功能：表示由 EMD 指定的最大再现次数。

值：1 至 0xFF。当不使用时，区 MT 的值为 00。

=CT(1 字节)(任选)

含义：再现次数

功能：表示所允许再现次数中的再现次数。每当再现数据时，区 CT 的值减小。

值：0x00 至 0xFF。但不使用时，区 CT 的值为 0x00。当区 LT 的比特 7 为 1、区 CT 的值为 00 时，禁止再现数据。

=CC(1 字节)

含义：复制控制

功能：控制复制操作。

值：(参见图 14)比特 6 和 7 表示复制控制信息。比特 4 和 5 表示高速数字复制操作的复制控制信息。比特 2 和 3 表示保密块验证级。比特 0 和 1 未定义。

CC 的示例：

(比特 7 和 6)

11：允许不受限制的复制操作

01：禁止复制

00：允许一次复制操作

(比特 3 和 2)

00：模拟/数字输入记录

MG 验证级为 0。当采用来自 CD 的数据执行数字记录操作时，(比特 7 和 6)为 00，(比特 3 和 2)为 00。

=CN(1 字节)(任选)

含义：高速串行复制管理系统中所允许的复制次数

功能：扩展复制允许的复制次数，不限于一次复制允许及不允许复制。仅在第一次复制产生时无效。每当执行复制操作时，区 CN 的值的减小。

值：00：禁止复制

01 至 0xFF：次数

0xFF：不受限的复制次数

再次参见图 10，轨道信息区 TRKINF 后面是从 0x0370 开始的 24 字节的部分管理信息区(PRTINF)。当一轨道由多个部分组成时，各单个部分的地址依次排列在 PRTINF 中。图 15 表示 PRTINF 区的各个部分。接下来，将按排列顺序描述 PRTINF 区。

=PRTSIZE(4 字节)

含义：部分尺寸

功能：表示一个部分的尺寸。簇：2 字节(最高位置)，开始 SU：1 字节(上)，结尾 SU：1 字节(最低位置)。

值：簇：1 至 0x1F40(8000)

开始 SU：0 至 0xA0(160)

结尾 SU：0 至 0xA0(16)(注意，SU 从 0 开始。)

=PRTKEY(8 字节)

含义：部分加密值

功能：对一个部分进行加密。起始值=0。要注意的是，应采用编辑规则。

值：0 至 0xFFFFFFFFFFFFFFFF

=CONNUM0(4 字节)

含义：起始产生的内容累积号密钥

功能：唯一地指定内容的 ID

值：与内容累积号起始值密钥的值相同的值

接下来如图 10 所示，ATRAC3 数据文件的属性首标包含附加信息 INF

区。除开始位置不固定外，该附加信息与再现管理文件的附加信息 INF-S 区(参见图 7 和 8)相同。一个或多个部分的尾部的最后的字节位置(4 字节的倍数)后面是附加信息 INF 区。

=INF

含义：对应于轨道的附加信息

功能：以首标表示可变长度附加信息。可排列多个不同类型的附加信息。每个附加信息区具有 ID 和数据尺寸。几个附加信息区由至少 16 个字节及 4 字节的倍数组成。

值：与再现管理文件的附加信息 INF-S 相同

上述属性首标后面跟着多个数据块。给每个数据块加上一个首标。接下来，将描述如图 16 所示加上了首标的每个块。

=BLKID-A3D(4 字节)

含义：块 ID 文件 ID

功能：识别 ATRAC3 数据的顶部。

值：固定值=“A3D”(例如，0x41334420)

=MCode(2 字节)

含义：制作者码

功能：识别记录器/播放器的制作者和模式

值：高阶 10 比特(制作者码)；低阶 6 比特(模式码)

=CONNUMO(4 字节)

含义：起初创建的内容的累积号

功能：为内容指定唯一的 ID。即使对内容进行编辑时，区 CONNUMO 的值也不改变。

值：与内容累积号起始密钥相同

=BLOCK SERIAL(4 字节)

含义：指定给每个轨道的序列号

功能：从 0 开始并递增 1。即使对内容进行编辑，区 BLOCK SERIAL 的

值也不改变。

值：0 至 0xFFFFFFFF

=BLOCK-SEED(8 字节)

含义：用于对一个块进行加密的密钥

功能：块的开始是由记录器/播放器的保密块产生的随机数。该随机数之后为增 1 的值。当区 BLOCK-SEED 的值丢失时，由于未在等效于一个块的约 1 秒内产生声音，因此，将相同的数据写入该块的首标和结尾。即使对内容进行编辑，区 BLOCK-SEED 的值也不改变。

值：起初的 8 比特随机数

=INITIALIZATION VECTOR(8 字节)

含义：对 ATRAC3 数据进行加密/解密所必须的值

功能：表示用于对于每个块对 ATRAC3 数据进行加密和解密的起始值。块从 0 开始。下一个块从最后的 SU 处最后加密的 8 比特值开始。当分离一个块时，使用恰好在开始的 SU 之前的最后的 8 个字节。即使对内容进行编辑，区 INITIALIZATION VECTOR 的值也不改变。

值：0 至 0xFFFFFFFFFFFFFFFF

=SU-nnn

含义：声音单元的数据

功能：表示从 1024 个样本压缩的数据。输出数据的字节数取决于压缩模式。即使对内容进行编辑，区 SU-nnn 的值也不改变。例如，在 SP 模式中，N=384 个字节。

值：ATRAC3 的数据值。

在图 10 中，由于 N = 384，因此，将 42 个 SU 写入一个块中。将该块的头两个槽(4 字节)用作首标。在最后的槽(2 字节)中，冗余地写入 BLKID-A3D、MCode、CONNUM0、和 BLOCK SERIAL。因此，一个块的 M 字节的剩余区为(16,384-384×42-16×3=208)个字节。如上所述，还冗余地记录 8 字节区 BLOCK SEED。

另外，声音单元 SU(0)～(101)每个均由 8 字节密报(cryptogram)C_i 组成，该密报是在图 2 所示加密/解密单元 64 中在 CBC(加密块链接)模式中以 64 比特(8 字节)密码块为单位进行加密而创建的。在本实施例中，声音单元 SU 的字节数(例如 160 字节)被构成为密码块(即加密单元)的字节数(例如 8 字节)的整数倍。亦即，一个声音单元 SU 例如由 20 个密报 C_i 组成。每个密报 C_i 位于一声音单元 SU 内，并且密报从不横跨多个声音单元 SU。

存储在闪速存储器 34 中的音频数据如后所述地压缩。压缩单元是声音单元 SU。因此，当将音频数据从便携式存储装置 3 读到便携式播放器 4 时，最小可读单元是声音单元 SU。基于此，各加密块之间无中断，从而当访问存储在闪速存储器 34 中的加密的音频数据时降低了访问数据的处理负荷。要注意的是，包含在每个簇中的声音单元 SU 的数目可以是从 1 到 102 范围内的任意数。另外，音频数据的压缩方法可以是 ATRAC3 或另外的 CODEC 方法。

块种子数据 BS 是通过对每个簇产生随机数而创建的，并且如后所述，当在便携式播放器 4 中创建每个块的块密钥数据 BK 时使用。块种子数据 BS 被存储在每个块中作为对抗差错的措施。另外，每个簇中的声音单元按加密顺序存储在闪速存储器 34 的连续的地址上。因此，按加密顺序将加密块连续地存储在闪速存储器 34 中。

闪速存储器管理模块 35

闪速存储器管理模块 35 执行向闪速存储器 34 写入数据、从闪速存储器 34 读取数据等处理的控制。

便携式播放器 4

再参见图 2，便携式播放器 4 由主控模块 41、通信接口 42、控制模块 43、编辑模块 44、压缩/扩展模块 45、扬声器 46、D/A 转换器 47、和 A/D 转换器 48 组成。

主控模块 41

主控模块 41 集中控制便携式播放器 4 的处理。

控制模块 43

控制模块43包括随机数产生单元60、存储单元61、密钥创建/密钥处理单元62、相互识别单元63、加密/解密单元64、及控制单元65。

控制模块43是专用于加密的多层结构的单片集成电路，它类似于控制模块33。各内部存储单元由诸如铝层的伪层夹住。另外，控制模块43具有范围较窄的工作电压或工作频率，并且是不能篡改的，从而不能由外部非法读取数据。

随机数产生单元60在接收到随机数产生指令时产生64比特(8字节)的随机数。

存储单元61存储为识别所需的各种数据。如图17所示，存储单元61存储主密钥数据MK_0至MK_{31}、及装置识别数据ID_m。

下面的方程(1)表示主密钥数据MK_0至MK_{31}、识别密钥IK_0至IK_{31}、及装置识别数据ID_m之间的关系。在下面的方程中，f(a b)是用于根据变元a和b提取一个值的函数。

$$IK_j=f(MK_j, ID_m) \quad (1)$$

其中，j是满足$0\leq j\leq 31$的整数。

存储单元61中识别密钥数据IK_0至IK_{31}的存储地址由5个比特表示。对它们指定了与存储单元51中的主密钥数据MK_0至MK_{31}的存储地址相对应的存储地址。

密钥创建/处理单元62通过执行各种运算(例如由ISO/IEC9797标准定义的MAC运算)来创建密钥数据。此时，将在FIPS PUB 46-2中规定的DES用作“块加密算法”。

相互识别单元63在将音频数据从计算机2传送到便携式存储装置3之前执行与便携式存储装置3的相互识别处理。相互识别单元63还在从便携式存储装置3接收音频数据之前执行与便携式存储装置3的相互识别处理。另外，在相互识别处理期间，相互识别单元63还执行MAC运算，并使用存储在存储单元61中的数据。相互识别单元63在音频数据被输入或输出到这些装置之前，执行与计算机2或网络5上的计算机的相互识别处理。

加密/解密单元64通过有选择地使用在FIPS PUB81中规定的ECB模式或CBC模式来执行块加密。加密/解密单元64在CBC模式中使用56比特密钥k，以根据下面的方程(2)以由64个比特构成的密码块为单位对从计算机2或CD播放器7输出的音频数据(明文)进行加密，从而创建加密的音频数据(密

报)。

在 CBC 模式中，使用前者对后面的数据组进行加密。因此，即使在输入相同的数据时，也输出不同的密报。这就使得解密较困难。

$$C_i=E_k(P_i \text{ XOR } C_{i-1}) \quad (2)$$

其中，

i：1 或更大的整数

P_i：明文(64 个比特)

C_i：密报(64 个比特)

XOR：异或，及

E_k：DES 系统采用 56 比特的密钥数据 k 进行的加密

下面将参照图 18 来解释方程(2)的运算。“IV”是块加密起始值(64 比特)，并且恰好存储在便携式存储装置 3 的闪速存储器 34 中簇 CL 中的声音单元 SU(0)之前。

ATRAC 是在 MiniDisks®中使用的编码和压缩方法，其中，采用频带分割和 MDCT(改进的离散余弦变换)来对 288kbit/s 44.1kHz 样本立体声信号进行编码。首先，由频带分割滤波器将数据分成 1/4、1/4 和 1/2 的 3 个频带，采用 MDCT 将各频带的信号下采样并转换到频域，并通过自适应比特分布对 MDCT 的系数进行阶梯量化。

加密/解密单元 64 采用 FIPS81 模式中的 ECB 模式 15 和 CBC 模式有选择地执行解密。通过根据下述方程(3)采用 56 比特的密钥 k 以密码块为单位对密报进行解密，加密/解密单元 64 创建明文。

$$P_i=C_{i-1} \text{ XOR } D_k(C_i) \quad (3)$$

其中，

I：1 或更大的整数

P_i：明文(64 个比特)

C_i：密报(64 个比特)

XOR：异或，及

D_k：DES 系统采用 56 比特的密钥数据进行的解密

下面将参照图 19 来描述方程(3)的运算。要注意的是，图 19 中，“IV”是块加密起始值(64 比特)，并且恰好存储在便携式存储装置 3 的闪速存储器 34 中簇 CL 中的声音单元 SU(0)之前。

控制单元65集中控制随机数产生单元60、存储单元61、密钥创建/密钥处理单元62、相互识别单元63、及加密/解密单元64的处理。

编辑模块44

编辑模块44根据来自用户的指令对存储在便携式存储装置3的闪速存储器34中的轨道数据文件101_0至101_3(参见图4)进行编辑，以创建新的轨道数据文件。这种编辑可包括用于将一个轨道数据文件分成两个轨道数据文件的分离编辑和用于将两个轨道数据文件合并成一个轨道数据文件的耦合(coupled)编辑。这种编辑的结果是，按需要重写再现管理文件100和轨道数据文件101_0至101_3。

压缩/扩展模块45

作为选择解密的音频数据的处理的一部分，压缩/扩展模块45扩展压缩的ATRAC3音频数据，并将其输出到D/A转换器47。另外，在便携式存储装置3中，当从CD播放器7或计算机2输入存储的音频数据时，模块45采用ATRAC3格式对音频数据进行压缩。

D/A转换器47

D/A转换器47将从压缩/扩展模块45输入的数字音频数据转换成模拟音频数据，该模拟音频数据被输出到扬声器46。

扬声器46

扬声器46根据从D/A转换器47输入的音频数据而输出声音。

A/D转换器48

A/D转换器48将从CD播放器7输入的模拟音频数据转换成数字数据，将其输出到压缩/扩展模块45。

便携式存储装置3的写入操作

图20是表示用于将数据从便携式播放器4写入到便携式存储装置3的操作的流程图。

步骤 S1：从便携式播放器 4 向便携式存储装置 3 发送写入请求信号。

步骤 S2：选择用于在便携式存储装置 3 与便携式播放器 4 之间的相互识别的识别密钥数据 IK_j。该步骤中的处理将在后面详细描述。

步骤 S3：在便携式存储装置 3 与便携式播放器 4 之间执行相互识别处理。该步骤中的处理将在后面详细描述。

步骤 S4：当便携式存储装置 3 和便携式播放器 4 中的每一个根据步骤 S3 的相互识别处理彼此将对方认作合法方时，控制过程进到步骤 S5。否则，终止该处理。

步骤 S5：在便携式存储装置 3 和便携式播放器 4 两者中创建会话密钥数据 Sek。该步骤中的处理将在后面详细描述。

步骤 S6：将加密的音频数据通过通信接口 32 和 42 从便携式播放器 4 输出并写入便携式存储装置 3。该步骤中的处理将在后面详细描述。

以这种方式，在便携式存储装置 3 与便携式播放器 4 之间执行相互识别处理，并且仅当便携式存储装置 3 和便携式播放器 4 均将对方认作是合法方时，才将加密的音频数据从便携式播放器 4 写入便携式存储装置 3。采用这种方法，较容易地避免了音频数据的非法复制。

选择识别密钥数据 IK_j(图 20 的步骤 S2)

图 21 解释的是在图 20 的步骤 S2 中起初表示的识别密钥数据 IK_j 的选择。通过图 2 所示便携式播放器 4 的随机数产生单元 60 来产生 64 比特的随机数 R_j。该随机数 R_j 从便携式播放器 4 输出到便携式存储装置 3。便携式存储装置 3 的相互识别单元 53 采用 64 比特随机数 R_j 中的 5 个低有效位，以从存储在存储单元 51 中的预先存储的识别密钥数据 IK_0 至 IK_{31} 中规定识别密钥数据 IK_j(其中 j 是满足 $0 \le j \le 31$ 的整数)。将装置识别数据 ID_m 类似地从便携式存储装置 3 的存储单元 51 读出，并将其输出到便携式播放器 4。便携式播放器 4 的相互识别单元 63 采用随机数 R_j 中的 5 个低有效位，以从预先存储的主密钥数据 MK_0 至 MK_{31} 中规定主密钥数据 MK_j。

密钥创建/密钥处理单元 62 采用所规定的主密钥数据 MK_j 和装置识别数据 ID_m，以根据下述方程(4)创建识别密钥数据 IK_j。要注意的是，f(a, b)例如是根据变元 a 和 b 提取一个值的任何函数。

$$IK_j = f(MK_j, ID_m) \qquad (4)$$

一旦便携式存储装置3和便携式播放器4具有的识别密钥数据IK_0至IK_{31}和主密钥数据MK_0至MK_{31}具有方程(4)所示的关系，便通过图21所示的处理来选择相同的识别密钥数据IK_j。

所选识别密钥数据IK_j被用作相互识别处理中的保密密钥，如后所述。每当执行图21所示的处理时，便根据随机数R_j从32个识别密钥数据IK_j中随机选择该识别密钥数据。这就将伪装非法识别的成功概率降低到仅使用一个识别密钥数据的情况的1/32，从而非常可靠地避免了非法识别。

在上述实施例中，采用随机数来选择识别密钥数据。然而，还可根据从便携式存储装置3及便携式播放器4的外部输入的密钥指定信号来确定识别密钥数据。

便携式存储装置3及便携式播放器4之间的相互识别

(图20的步骤S3)

图22是用于解释在便携式存储装置3与便携式播放器4之间执行的相互识别处理的示意图。在开始相互识别处理之前，已结束对图21中所示的识别密钥数据IK_j的选择，并且便携式播放器4的相互识别单元53具有所选出的识别密钥数据IK_j和装置识别数据ID_m。另外，便携式存储装置3的相互识别单元63具有所选出的便携式存储装置3的识别密钥数据IK_j和装置识别数据ID_m。该相互识别处理如下地进行。

步骤S10:便携式存储装置3的随机数产生单元50创建64比特的随机数R_{ms}，并将其输出到便携式播放器4。

步骤S11：便携式播放器4的随机数产生单元60创建64比特随机数R_d和S_d。

步骤S12：便携式播放器4的相互识别单元63采用在图20所示步骤S2获得的识别密钥数据IK_j以及“$R_d||R_{ms}||ID_m$”，以根据下述方程(5)执行MAC运算，从而求出MAC_A。这里，A||B表示耦合A和B(将m比特B耦合到n比特A，以构成(n+m)比特)。

$$MAC_A=MAC(IK_j, R_d||R_{ms}||ID_m) \quad (5)$$

步骤S13：便携式播放器4将“$R_d||S_d||MAC_A||j$”输出到便携式存储装置3。

步骤S14：便携式存储装置3的相互识别单元53采用在图20所示步骤

S2 获得的识别密钥数据 IK_j 以及“$R_d||R_{ms}||ID_m$”，以根据下述方程(6)执行 MAC 运算，从而求出 MAC_B。

$$MAC_B=MAC(IK_j, R_d||R_{ms}||ID_m) \quad (6)$$

步骤 S15：便携式存储装置 3 的相互识别单元 53 将在步骤 S14 求出的 MAC_B 与在步骤 S13 输入的 MAC_A 进行比较。如果两者相符，则便携式播放器 4 具有适当的识别密钥数据 IK_j，从而便携式存储装置 3 将便携式播放器 4 识别为合法方。

步骤 S16：便携式存储装置 3 的相互识别单元 53 采用在步骤 20 所示步骤 S2 获得的识别密钥数据 IK_j 以及“$R_{ms}||R_d$”，以根据下述方程(7)执行 MAC 运算，从而求出 MAC_C。

$$MAC_C=MAC(IK_j, R_{ms}||R_d) \quad (7)$$

步骤 S17：便携式存储装置 3 的随机数产生单元 50 创建 64 比特随机数 S_{ms}。

步骤 S18：将“$S_{ms}||MAC_C$”从便携式存储装置 3 输出到便携式播放器 4。

步骤 S19：便携式播放器 4 的相互识别单元 63 根据方程(8)执行 MAC 运算，从而求出 MAC_d。

$$MAC_d=MAC(IK_j, R_{ms}||R_d) \quad (8)$$

步骤 S20：便携式播放器 4 的相互识别单元 63 将在步骤 S19 求出的 MAC_d 与在步骤 S18 输入的 MAC_C 进行比较。如果两者相符，则便携式存储装置 3 具有适当的识别密钥数据 IK_j，从而便携式播放器 4 将便携式存储装置 3 识别为合法方。

如上所述，可实现便携式存储装置 3 与便携式播放器 4 之间的相互识别。

创建会话密钥数据 Sek(图 20 的步骤 S5)

图 23 解释的是会话密钥数据 Sek 的创建。在开始创建会话密钥数据 Sek 之前，结束对图 21 所示识别密钥数据 IK_j 的选择和图 22 所示的相互识别处理。便携式存储装置 3 和便携式播放器 4 两者均具有所选识别密钥数据 IK_j 及随机数 S_d 和 S_{ms}。会话密钥数据 Sek 的创建如下。

步骤 S30：便携式播放器 4 的相互识别单元 63 使用所选识别密钥数据 IK_j 和“$S_d||S_{ms}$”以根据方程(9)执行 MAC 运算，从而创建会话密钥数据 Sek。

$$Sek=MAC(IK_j, S_d||S_{ms}) \quad (9)$$

步骤 S31：便携式存储装置 3 的相互识别单元 53 使用所选识别密钥数据 IK_j 及“$S_d \| S_{ms}$”，以根据方程(10)执行 MAC 运算，从而创建会话密钥数据 Sek。

$$Sek=MAC(IK_j, S_d \| S_{ms}) \quad (10)$$

如果便携式存储装置 3 和便携式播放器 4 两者均为合法，则在便携式存储装置 3 上创建的会话密钥数据 Sek 与在便携式播放器 4 上创建的相同。

将音频数据写入便携式存储装置 3(见图 20 的步骤 S6)

图 24 表示从便携式播放器 4 向便携式存储装置 3 的音频数据写入操作。在开始写入处理之前，图 23 所示会话密钥数据 Sek 的创建处理已结束，并且便携式存储装置 3 和便携式播放器 4 具有相同的会话密钥数据 Sek。将音频数据写入便携式存储装置 3 的处理是如下进行的。

步骤 S40：便携式播放器 4 请求随机数产生单元 60 为每个轨道产生一随机数，并根据每个随机数来创建相应的内容密钥数据 CK。

步骤 S41：便携式播放器 4 在加密/解密单元 64 采用会话密钥数据 Sek 对在步骤 S40 创建的内容密钥数据 CK 进行加密。

步骤 S42：便携式播放器 4 将在步骤 S41 加密的内容密钥数据 CK 输出到便携式存储装置 3。

步骤 S43：便携式存储装置 3 在加密/解密单元 54 对在步骤 S42 输入的加密的内容密钥数据 CK 进行解密。

步骤 S44：便携式存储装置 3 在加密/解密单元 54 采用从存储单元 51 读出的存储使用密钥数据 Skm 对在步骤 S43 解密的内容密钥数据进行加密。

步骤 S45：便携式存储装置 3 将加密的 CK 输出到便携式播放器 4。

步骤 S46：便携式播放器 4 在轨道数据文件 101_n 中的 TRKINF 中设定相关的加密的内容密钥数据 CK。

步骤 S47：随机数产生单元 60 产生轨道数据文件的每个部分的随机数，并根据随机数来创建部分密钥数据 PK。在轨道数据文件 101_n 中的 PRTINF 中设定所创建的部分密钥数据 PK。

步骤 S48：在密钥创建/处理单元 62 中对轨道数据文件的每个部分获得在步骤 45 创建的部分密钥数据 PK 与内容密钥数据 CK 的异或，如方程(11)所示。处理结果是产生了暂时密钥数据 TMK。暂时密钥数据 TMK 的产生不局限于使用 XOR 函数。可以使用其他函数算子，如简单的 AND(“与”)算子。

TMK=PK XOR CK (11)

步骤 S49：随机数产生单元 60 为每个块产生一随机数，并根据随机数产生块种子数据 BS。另外，便携式播放器 4 将所创建的块种子数据 BS 设定在每个相应块的其适当位置中。

步骤 S50：密钥创建/处理单元 62 使用在步骤 S46 创建的暂时密钥数据 TMK 和在步骤 S47 创建的块种子数据 BS 以方程(12)执行 MAC 运算，并对每个块创建块密钥数据 BK。

BK=MAC (TMK, BS) (12)

可根据 SHA-1(保密 Hash 算法)、RIPEMD-160 或其他单向 Hash 函数的输入采用保密密钥来执行除 MAC 运算以外的处理，以创建块密钥数据 BK。这里，该单向函数 f 定义了这样一种函数，即由 x 计算 y=f(x)较容易，而反过来由 y 求 x 则较难。在"应用密码学手册(Handbook of Applied Cryptography), CRC 出版社"一书中详细公开了一种单向 Hash 函数。

步骤 S51：便携式播放器 4 在压缩/扩展模块 45 中根据 ATRAC3 格式对从计算机 2 或便携式播放器 4 输入的音频数据进行压缩。然后，加密/解密单元 64 在 CBC 模式中采用在步骤 S50 创建的块密钥数据 BK 对压缩的音频数据进行加密。

步骤 S52：便携式播放器 4 将首标加到在步骤 S51 加密的音频数据上，然后经通信接口 32 和 42 将它们输出到便携式存储装置 3。

步骤 S53：便携式存储装置 3 将加密的音频数据和首标写入闪速存储器 34 中。

因此，将音频数据从便携式播放器 4 写入便携式存储装置 3 的处理结束。尽管上面仅讨论了轨道数据文件 101_0 至 101_3 的写入，但便携式播放器 4 也以这种方式写再现管理文件 100。

从便携式存储装置 3 读取

图 25 是解释从便携式存储装置 3 向便携式播放器 4 读取数据的读取操作的流程图。

步骤 S61：规定所需轨道数据(曲调(tune))的读取请求信号从便携式播放器 4 发送到便携式存储装置 3。

步骤 S2：以上述方式选择当在便携式存储装置 3 与便携式播放器 4 之间

执行相互识别时所使用的识别密钥数据 IK_j。

步骤 S3：以上述方式在便携式存储装置 3 与便携式播放器 4 之间执行相互识别处理。

步骤 S4：当便携式存储装置 3 和便携式播放器 4 彼此将对方识别为合法方时，处理过程继续。否则，终止处理。

步骤 S5：以上述方式在便携式存储装置 3 和便携式播放器 4 上创建会话密钥数据 Sek。

步骤 S63：经通信接口 32 和 42 将加密的音频数据从便携式存储装置 3 读到便携式播放器 4。后面将详细描述该处理过程。

在便携式存储装置 3 与便携式播放器 4 之间执行相互识别。仅当双方各将对方识别为合法方时，才可使用适当的会话密钥数据 Sek 来对加密的内容密钥数据进行解密。

从便携式存储装置 3 读取音频数据(图 25 的步骤 63)

图 26 解释的是将音频数据从便携式存储装置 3 读到便携式播放器 4 的处理。该读取步骤需要采用上述方法写入数据。轨道数据文件 101_0 至 101_3 的写入对设定 TRKINF 中的内容密钥数据 CK、PRTINF 中的部分密钥数据、及每个簇 CL 中的块种子数据 BS 是非常关键的。由于步骤 S5 的处理结束，因此，便携式存储装置 3 和便携式播放器 4 具有相同的会话密钥数据。从便携式存储装置 3 读取音频数据的处理如下进行。

步骤 S71：便携式存储装置 3 规定对应于读取请求信号的轨道数据文件，并从包含所规定的轨道数据的簇中以声音单元 SU 为单位输出音频数据。便携式存储装置 3 还读出音频数据的相应的属性首标，并将其输出到便携式播放器 4。

步骤 S72：便携式播放器 4 从输入的属性首标中的 TRKINF 中拾取 CK，并将其输出到便携式存储装置 3。

步骤 S73：便携式存储装置 3 的加密/解密单元 54 采用存储在存储单元 51 中的存储密钥数据 Skm 对在步骤 S72 输入的内容密钥数据 CK 进行解密。

步骤 S74：便携式存储装置 3 的加密/解密单元 54 采用在图 25 所示步骤 S5 获得的会话密钥数据 Sek，对在步骤 S73 解密的内容密钥数据 CK 进行加密。

步骤 S75：便携式存储装置 3 将在步骤 S74 加密的内容密钥数据 CK 输出到便携式播放器 4。

步骤 S76：便携式播放器 4 的加密/解密单元 64 采用会话密钥数据 Sek 对从在步骤 S73 从便携式存储装置 3 输入的内容密钥数据 CK 进行解密。

步骤 S77：便携式播放器 4 的密钥创建/处理单元 62 获得在步骤 S76 解密的内容密钥数据 CK 与在步骤 S71 输入的属性首标中的 PRTINF 中的部分密钥数据 PK 的异或，并根据方程(13)将处理结果定义为暂时密钥数据 TMK。

$$TMK=PK\ XOR\ CK \tag{13}$$

步骤 S78：便携式播放器 4 的密钥创建/处理单元 62 采用在步骤 S77 创建的暂时密钥数据 TMK 和在步骤 S71 输入的轨道数据文件中的块种子数据 BS，来执行下述方程(14)的 MAC 运算，以将处理结果定义为块密钥数据 BK。对每个簇(块)如下地求出块密钥数据 BK。

$$BK=MAC\ (TMK,\ BS) \tag{14}$$

步骤 S79：便携式播放器 4 采用在步骤 S78 创建的块密钥数据 BK 在加密/解密单元 64 中对在步骤 S71 输入的音频数据进行解密。

因此，采用分别求出的块密钥数据 BK，对于每个簇(块)对音频数据进行解密。另外，以用于加密的相同的 8 字节块为单位执行解密。

步骤 S80：便携式播放器 4 在压缩/扩展模块 45 中采用 ATRAC3 系统对在步骤 S79 解密的音频数据进行扩展，并在 D/A 转换器 47 上将扩展的音频数据转换成模拟格式，并将其输出到扬声器。

在步骤 S78 解密的音频数据以声音单元 SU 为单位进行扩展。

轨道数据文件的分离编辑

如前面所提到的，便携式播放器 4 的编辑模块 44 适于执行用于将一个轨道数据文件分离成两个轨道数据文件的分离编辑、以及将两个轨道数据文件耦合以创建一个轨道数据文件的耦合编辑。

首先，将解释分离编辑。图 27 解释的是由便携式播放器 4 的编辑模块 44 对轨道数据文件执行分离编辑。作为一示例，编辑模块 44 将图 27(A)所示的轨道数据文件(1)分离为图 27(B)所示的轨道数据文件(1)和图 27(C)所示的轨道数据文件(2)。最小分离单元是声音单元 SU。在该示例中，簇 CL(2)的声音单元 SU(3)和 SU(4)如图 27(B)所示地分离。

分离后，轨道数据文件(1)的簇 CL(2)如图 28 所示，而新创建的轨道数据文件(2)的簇 CL(0)如图 29 所示。分离前的轨道数据文件(1)的簇(2)的声音单元 SU(4)变为轨道数据文件(2)中簇 CL(0)的声音单元 SU(0)。类似地，分离前的轨道数据文件(1)的簇(2)的声音单元 SU(5)变为轨道数据文件(2)中簇 CL(0)的声音单元 SU(1)。

另外，将轨道数据文件(2)的簇 CL(0)的块加密初始值 IV 设定为等于轨道数据文件(1)的簇 CL(2)中声音单元 SU(3)的最后的 8 个字节，如图 27(A)和 27(B)所示。如上所述，在每个簇中，块加密初始值 IV 被排列为正好在第一声音单元 SU(0)之前的 8 个字节。因此，每个分离的簇包含其自身的加密信息，从而不管后续的分离如何，仍可容易地再现数据。

分离前的轨道数据文件(1)的内容密钥数据、部分密钥数据、及块密钥数据为 CK-1、PK-1、及 BK-1。分离后的轨道数据文件(1)的内容密钥数据、部分密钥数据、及块密钥数据为 CK-1′、PK-1′、及 BK-1。另外，轨道数据文件(2)的内容密钥数据、部分密钥数据、及块密钥数据为 CK-2、PK-2、及 BK-1。

图 30 是解释在便携式播放器 4 的编辑模块 44 中创建新轨道数据文件(2)的内容密钥数据及部分密钥数据的流程图。通过分离而创建的新轨道数据文件(2)具有从轨道数据文件(1)分离出的新内容密钥数据 CK-2。通过下述地计算部分密钥数据 PK-2，块密钥数据 BK-1 与分离前的相同。该处理过程如下地进行。

步骤 S90：编辑模块 44 等待，直至其接收到分离指令，在此情况下，控制处理进到步骤 S91。

步骤 S91：随机数产生单元 60 产生一随机数，并根据所产生的随机数来创建新内容密钥数据 CK-2。

步骤 S92：便携式存储装置 3 的加密/解密单元 54 采用存储在存储单元 51 中的存储使用密钥数据，对在步骤 S91 创建的内容密钥数据 CK-2 进行加密。

步骤 S93：编辑模块 44 将加密的内容密钥数据 CK-2 写入相应轨道数据文件中的 TRKINF 中。

步骤 S94：编辑模块 44 根据方程(15)创建轨道数据文件(2)的部分密钥数据 PK-2。

$$PK\text{-}2=CK\text{-}1 \text{ XOR } PK\text{-}1 \text{ XOR } CK\text{-}2 \qquad (15)$$

该处理过程使得轨道数据文件(2)的暂时密钥数据(由方程(11)得到)与轨

道数据文件(1)的暂时密钥数据相同，并且使得所创建的簇密钥数据(由方程(12)得到)与分离前的块密钥 BK-1 相同。为此，不必再次采用新块密钥数据对轨道数据文件(2)中的声音单元 SU 进行加密。

步骤 S95：编辑模块 44 将在步骤 S94 创建的部分密钥数据 PK-2 写入相应轨道数据文件中的 PRTINF 中。

因此，即使当新内容密钥数据 CK-2 与新创建的轨道数据文件(2)的内容密钥数据相同时，基于方程(15)创建的部分密钥数据 PK-2 也能够使得暂时密钥数据与分离前的暂时密钥数据相同。其结果是，块密钥数据也与分离前的相同。因此，不必再次采用新的簇密钥数据对轨道数据文件(2)中的声音单元 SU 进行加密。类似地，根据内容密钥数据 CK-1 来确定分离后的轨道数据文件(1)的部分密钥数据 PK-1′，从而不改变块密钥数据 BK-1。其结果是，不必再次采用新的块密钥数据对分离后的轨道数据文件(1)中的声音单元 SU 进行加密。这就使得能够在不明显增大处理量的同时对轨道数据文件进行分离编辑。尽管上述描述仅涉及到轨道数据文件 101_0 至 101_3，编辑模块 44 也可以相应方式写再现管理文件。

图 31 解释的是由便携式播放器 4 的编辑模块 44 对两个轨道数据文件进行的耦合(合并)。例如，编辑模块 44 将图 31(A)所示的轨道数据文件(1)与图 31(B)所示的轨道数据文件(2)进行耦合，以创建图 31(C)所示的轨道数据文件(3)。通过耦合，创建的新轨道数据文件(3)包括由耦合前的轨道数据文件(1)组成的部分(1)及由耦合前的轨道数据文件(2)组成的部分(2)。

另外，新创建轨道数据文件(3)的内容密钥数据 CK-3、部分(1)的部分密钥数据 PK-3-1、及部分(2)的部分密钥数据 PK-3-2，如后所述。该新创建的密钥数据被设定在轨道数据文件(3)中的 TRKINF 和 PRTINF 中。

耦合之前的轨道数据文件(1)的簇 CL(0)和 CL(4)变成耦合之后的轨道(3)的部分(1)的开始簇和结束簇。另外，耦合之前的轨道数据文件(2)的簇 CL(0)和 CL(5)变成耦合之后的轨道(3)的部分(2)的开始簇和结束簇。

图 32 是解释创建用于新创建的轨道数据文件(3)的部分(1)和(2)的部分密钥数据的流程图。在下面的解释中，轨道数据文件(1)使用内容密钥数据 CK-1、部分密钥数据 PK-1、及块密钥数据 BK-1，而轨道数据文件(2)使用内容密钥数据 CK-2、部分密钥数据 PK-2、及块密钥数据 BK-2。通过以下述方式计算部分(1)和(2)的部分密钥数据，轨道数据文件(3)获得新的内容密钥数据

CK-3。块密钥数据 BK-1 和 BK-2 保持与耦合前相同。该耦合处理如下地进行。

步骤 S100：编辑模块 44 等待，直至它接收到耦合指令，在此情况下，控制过程进到步骤 101。

步骤 S101：随机数产生单元 60 产生随机数，并因此创建内容密钥数据 CK-3。

步骤 S102：便携式存储装置 3 的加密/解密单元 54 采用存储在存储单元 51 中的存储使用密钥数据 Skm，对在步骤 S101 创建的内容密钥数据 CK-3 进行加密。

步骤 S103：编辑模块 44 将加密的内容密钥数据 CK-3 写入轨道数据文件(3)中的 TRKINF 中。

步骤 S104：编辑模块 44 根据方程(16)创建轨道数据文件(3)的部分(1)的部分密钥数据 PK-3-1。

PK-3-1=CK-1 XOR PK-1 XOR CK-3 (16)

因此，部分(1)的暂时密钥数据(由方程(11)得到)与耦合之前轨道数据文件(1)的暂时密钥数据相同。其结果是，部分(1)的块密钥数据(由方程(12)得到)也与耦合前的轨道数据文件(1)的块密钥数据 BK-1 相同。为此，不必再次采用新块密钥数据对轨道数据文件(1)中的声音单元 SU 进行加密。

步骤 S105：编辑模块 44 根据方程(17)创建轨道数据文件(3)的部分(2)的部分密钥数据 PK-3-2。

PK-3-2=CK-2 XOR PK-2 XOR CK-3 (17)

因此，部分(2)的暂时密钥数据与轨道数据文件(2)的暂时密钥数据相同。其结果是，部分(2)的块密钥数据也与轨道数据文件(2)的块密钥数据 BK-2 相同。为此，不必再次采用新块密钥数据对部分(2)的声音单元 SU 进行加密。

步骤 S106：编辑模块 44 将在步骤 S104 创建的部分密钥数据 PK-3-1 写入轨道数据文件(3)的部分(1)的 PRTINF 中。

步骤 S107：编辑模块 44 将在步骤 S105 创建的部分密钥数据 PK-3-2 写入轨道数据文件(3)的部分(2)的 PRTINF 中。

因此，即使当新内容密钥数据 CK-3 与新创建的轨道数据文件(3)的内容密钥数据相同时，基于方程(16)和(17)创建的部分密钥数据 PK-3-1 及 PK-3-2 也能够使得每个部分的暂时密钥数据与耦合前的相应数据相同。其结果是，相应部分的块密钥数据也与分离前的 BK-1 及 BK-2 相同。因此，不必再次采

用新的块密钥数据对部分(1)和(2)中的声音单元 SU 进行加密。因此，就避免了通常伴随耦合编辑出现的处理量的显著增大。尽管上述描述仅涉及到轨道数据文件 101_0 至 101_3，但编辑模块 44 也可以相应方式重写再现管理文件。

本发明不局限于上述实施例，例如，上述实施例的声音单元 SU 的字节数(160 字节)为密码块(CBC 模式中的加密单元)字节数(8 字节)的整数倍。但是，在非整数倍时，也可通过插入填充值来调节声音单元 SU 的数据长度，来调整本发明。

另外，所示的情况为，当如图 22 所示地执行相互识别处理时，首先将在便携式存储装置 3 创建的随机数 R_{ms} 输出到便携式播放器 4。也可首先将在便携式播放器 4 创建的随机数输出到便携式存储装置 3。

另外，所示的情况为将 32 组识别密钥数据和主密钥数据存储在存储单元 51 和 61 中，但也可以是任意数目的组，只要其为 2 或更大。

此外，所给出的情况是在便携式播放器 4 中根据主密钥数据 MK_0 至 MK_{31} 产生识别密钥数据 IK_0 至 IK_{31}。但也可以与便携式存储装置 3 相同的方式将识别密钥数据 IK_0 至 IK_{31} 存储在便携式播放器 4 中，并根据随机数 R_j 选择识别密钥数据。

另外，如图 21 所示，以示例方式示出了通过采用在便携式播放器 4 创建的随机数 R_j 在便携式存储装置 3 及便携式播放器 4 选择识别密钥数据 IK_j 和主密钥数据 MK_j 的情况。但也可使用在便携式存储装置 3 创建的随机数或使用在便携式存储装置 3 和便携式播放器 4 两者中产生的随机数。

此外，上述实施例表示的根据随机数 R_j 在便携式存储装置 3 和便携式播放器 4 中选择识别密钥数据 IK_j 和主密钥数据 MK_j 的情况。但是，根据本发明，还可将 5 比特的密钥选择指令数据从外部输入到便携式存储装置 3 和便携式播放器 4，并且在便携式存储装置 3 和便携式播放器 4 上相应于由相关的密钥选择指令数据指示的每个其他数据来选择识别密钥数据 IK_j 和主密钥数据 MK_j。

另外，前面给出了包含有音频数据作为轨道数据的数据的示例，但本发明也可应用于将包含有运动图像数据、静止图像数据、文件数据、节目数据和其他类型数据的轨道数据存储在闪速存储器 34 中的情况。

如上所述，根据本发明的数据处理装置和数据处理系统及其方法，即使在通过使用第三密钥数据对轨道数据进行加密并将其存储到存储装置中之后

第一密钥数据改变的情况下，第三密钥数据也不改变，因此，不必对轨道数据进行解密和再加密。因此，显著降低了当第一密钥数据改变时所需的处理量。

因此，可以看出，有效地实现了在前述描述中清楚解释了的所述目的，并且，由于可在实现上述方法及前述结构时进行一些变化而不背离本发明宗旨和范围，因此，包含在上述描述中并且在附图中示出的所有内容均为解释性的，而不作为限定。

还应理解的是，所附权利要求书将覆盖这里所公开的本发明的所有一般和特定特征以及本发明范围的表述。

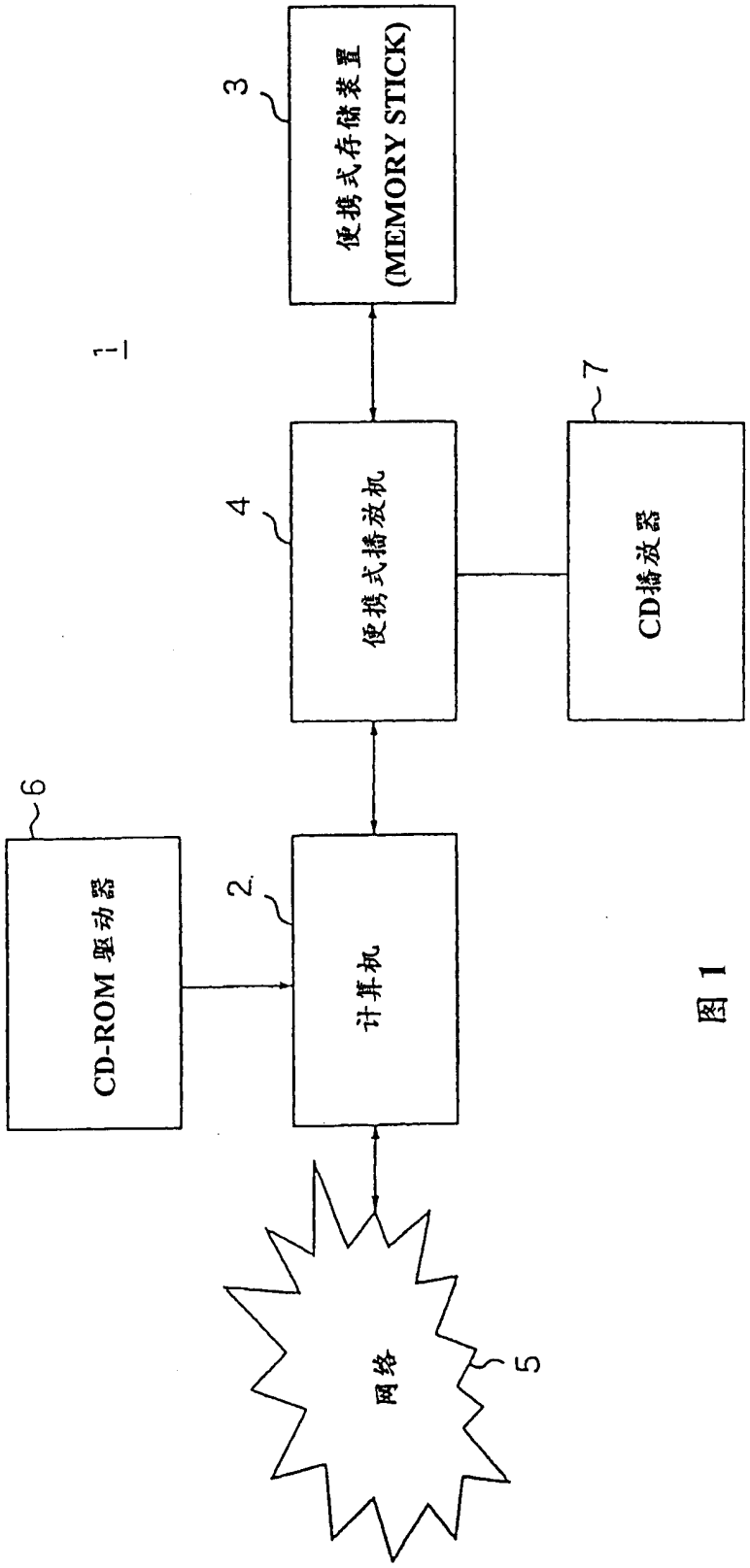


图 1

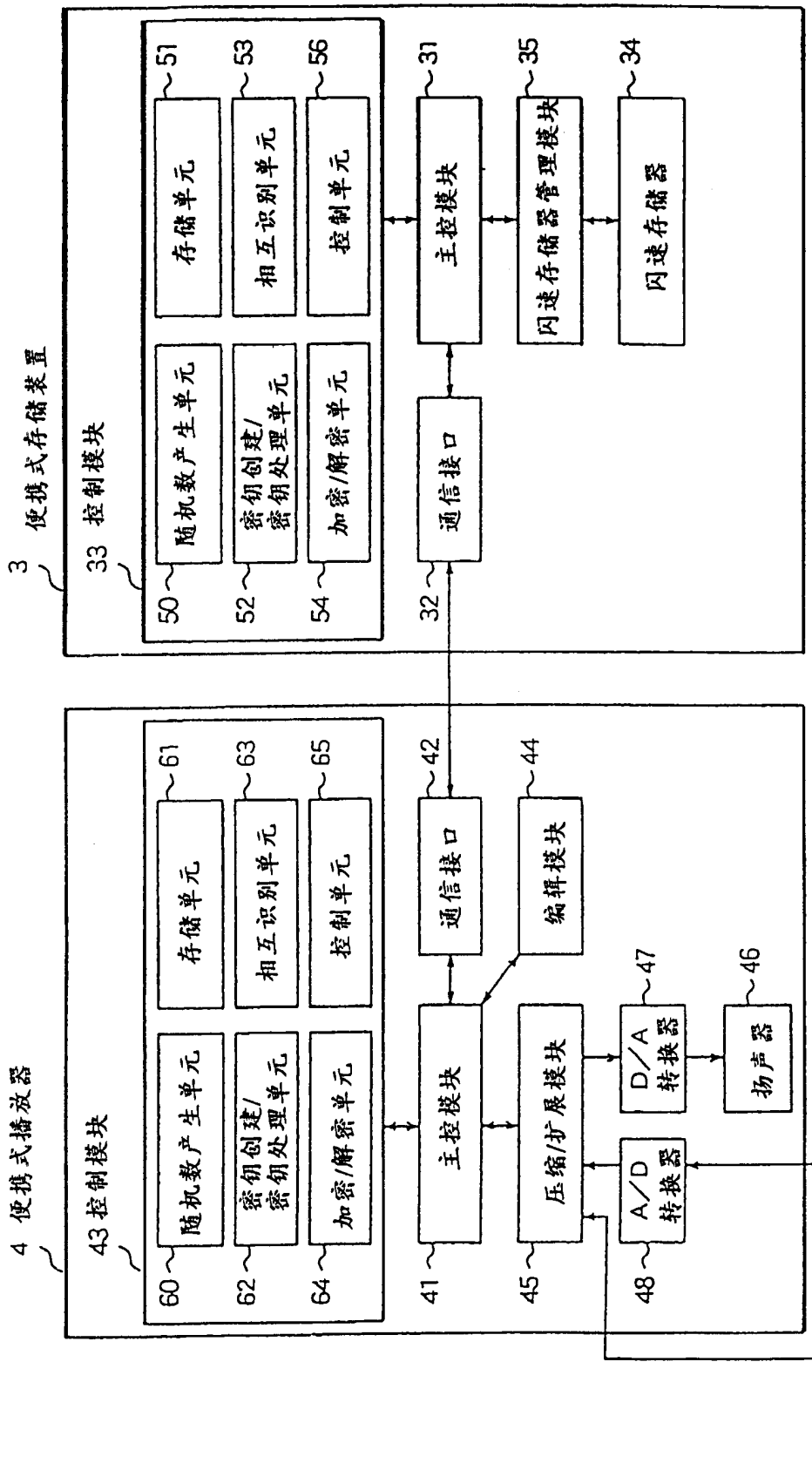
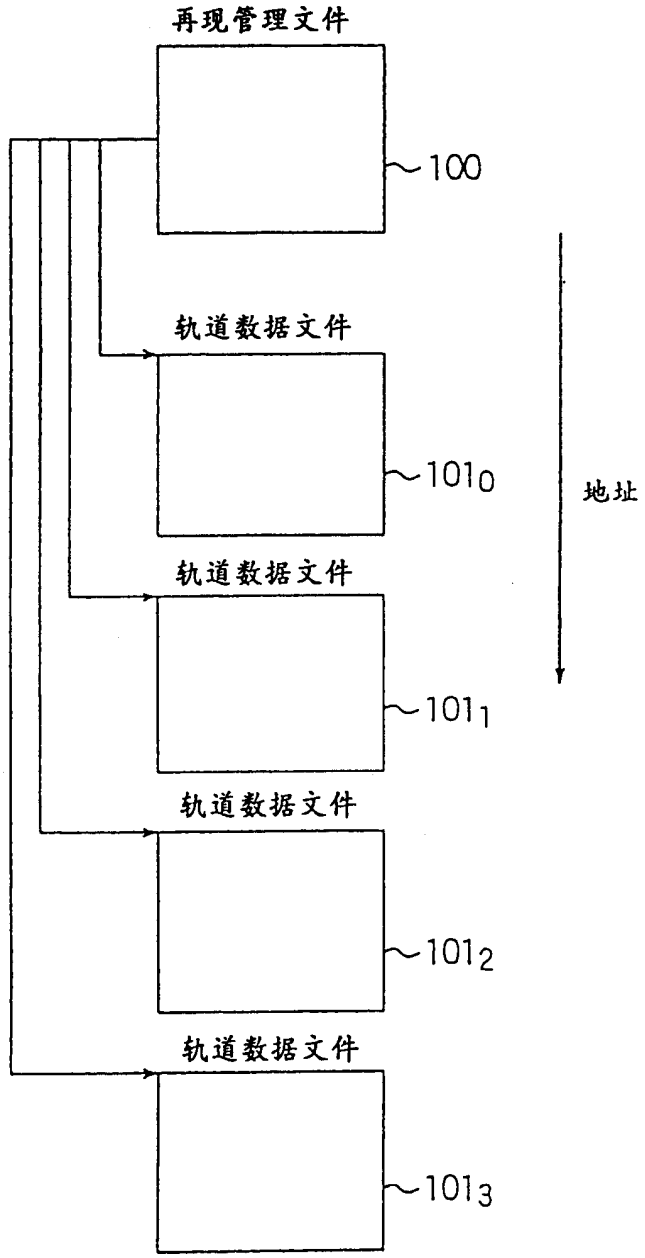

3 便携式存储装置
33 控制模块
50 随机数产生单元
52 密钥创建/密钥处理单元
54 加密/解密单元
51 存储单元
53 相互识别单元
56 控制单元
32 通信接口
31 主控模块
35 闪速存储器管理模块
34 闪速存储器
4 便携式播放器
43 控制模块
60 随机数产生单元
62 密钥创建/密钥处理单元
64 加密/解密单元
61 存储单元
63 相互识别单元
65 控制单元
42 通信接口
44 编辑模块
41 主控模块
45 压缩/扩展模块
48 A/D转换器
47 D/A转换器
46 扬声器
音频数据(来自计算机2)
音频数据(来自CD播放器7)

图 2

便携式存储装置3的存储单元51中存储的数据

	IK_0
识别密钥数据	IK_1
	IK_2
	IK_3
	⋮
	IK_{30}
	IK_{31}
装置识别数据	ID_m
存储使用密钥数据	SK_m

图 3



便携式存储装置3的闪速存储器34中的存储数据

图 4

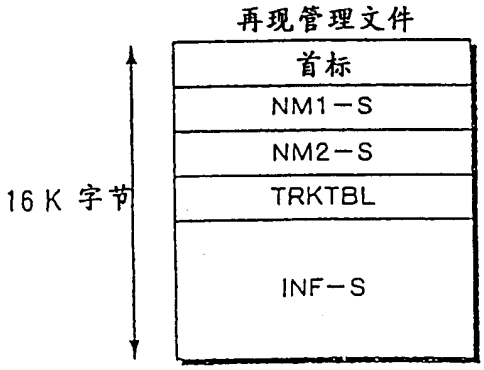


图 5

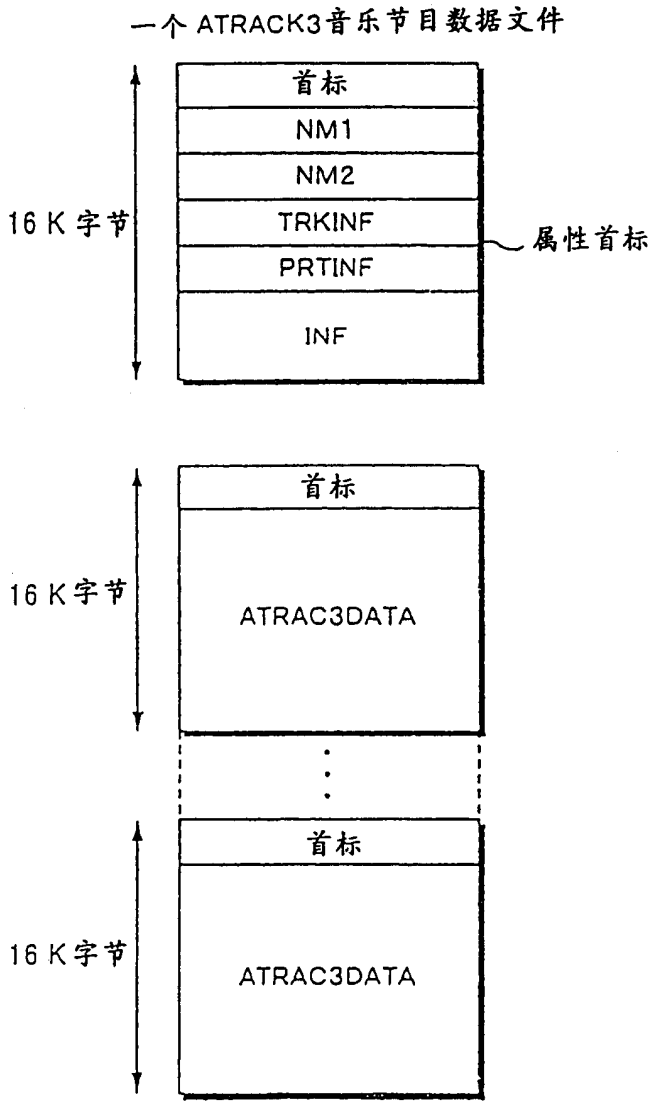

一个 ATRACK3音乐节目数据文件
首标
NM1
NM2
TRKINF
PRTINF
INF
16 K 字节
属性首标
首标
ATRAC3DATA
16 K字节
首标
ATRAC3DATA
16 K字节

图 6

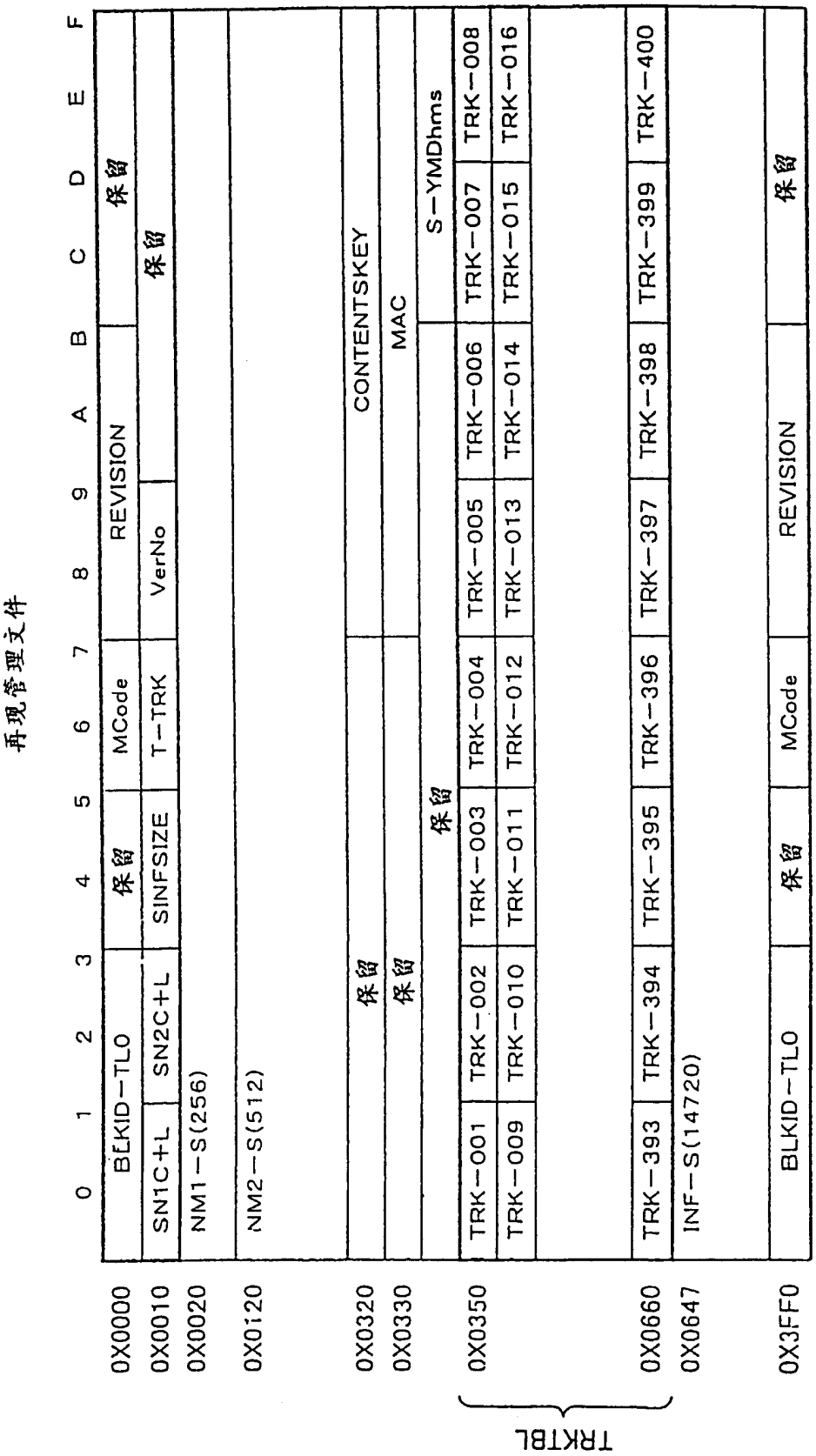

再现管理文件
0 1 2 3 4 5 6 7 8 9 A B C D E F
0X0000 BEKID-TL0 保留 MCode REVISION 保留
0X0010 SN1C+L SN2C+L SINFSIZE T-TRK VerNo 保留
0X0020 NM1-S(256)
0X0120 NM2-S(512)
0X0320 保留 CONTENTSKEY
0X0330 保留 MAC
0X0350 保留 S-YMDhms
TRK-001 TRK-002 TRK-003 TRK-004 TRK-005 TRK-006 TRK-007 TRK-008
TRK-009 TRK-010 TRK-011 TRK-012 TRK-013 TRK-014 TRK-015 TRK-016
TRKTBL
0X0660 TRK-393 TRK-394 TRK-395 TRK-396 TRK-397 TRK-398 TRK-399 TRK-400
0X0647 INF-S(14720)
0X3FF0 BLKID-TL0 保留 MCode REVISION 保留

图 7

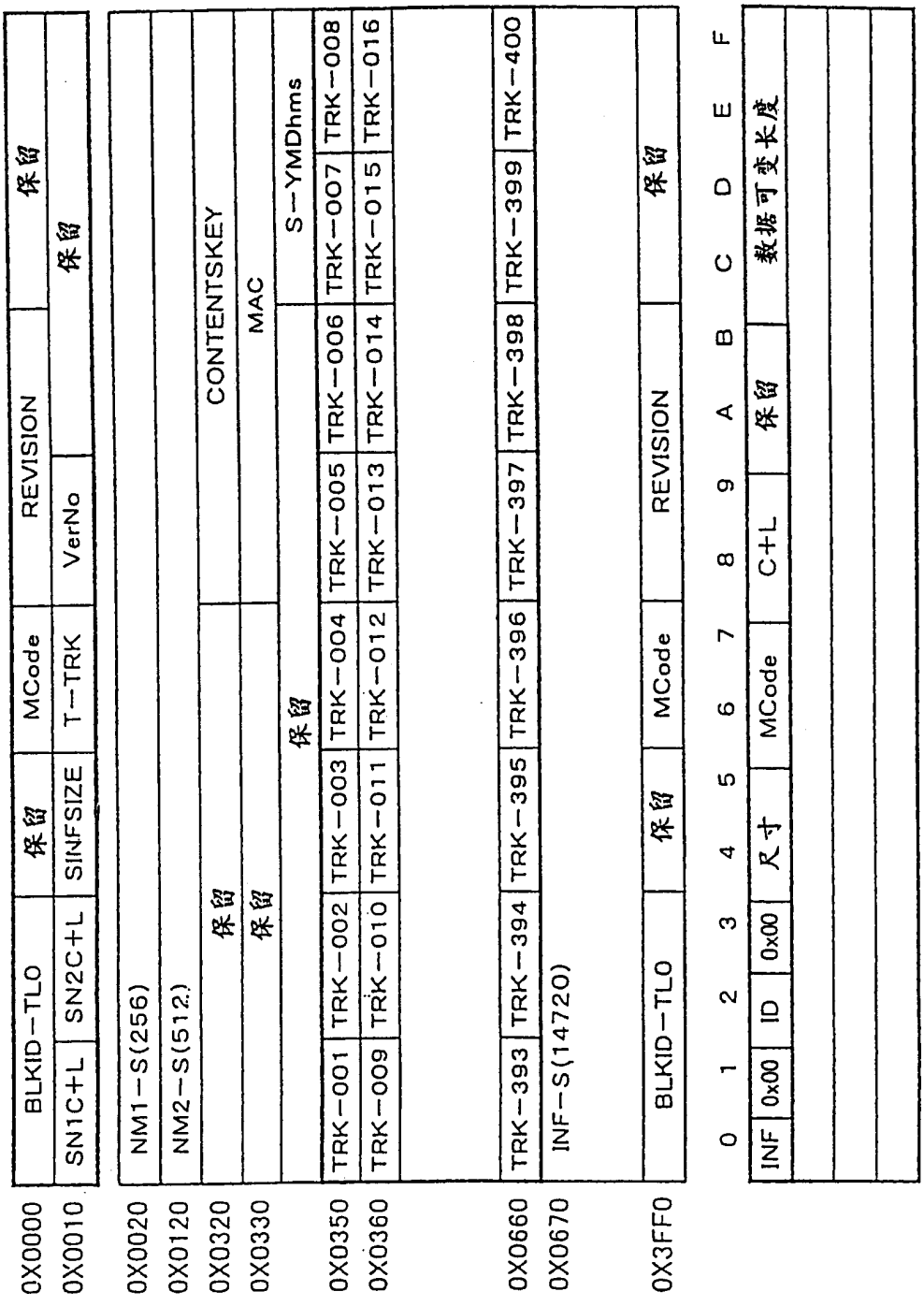

0 1 2 3 4 5 6 7 8 9 A B C D E F
0X0000 BLKID—TL0 保留 MCode REVISION 保留
0X0010 SN1C+L SN2C+L SINFSIZE T—TRK VerNo 保留
0X0020 NM1—S(256)
0X0120 NM2—S(512.)
0X0320 保留 CONTENTSKEY
0X0330 保留 MAC
S—YMDhms
0X0350 TRK—001 TRK—002 TRK—003 TRK—004 TRK—005 TRK—006 TRK—007 TRK—008
0X0360 TRK—009 TRK—010 TRK—011 TRK—012 TRK—013 TRK—014 TRK—015 TRK—016
0X0660 TRK—393 TRK—394 TRK—395 TRK—396 TRK—397 TRK—398 TRK—399 TRK—400
0X0670 INF—S(14720)
0X3FF0 BLKID—TL0 保留 MCode REVISION 保留
0 1 2 3 4 5 6 7 8 9 A B C D E F
INF 0x00 ID 0x00 尺寸 MCode C+L 保留 数据可变长度

图 8

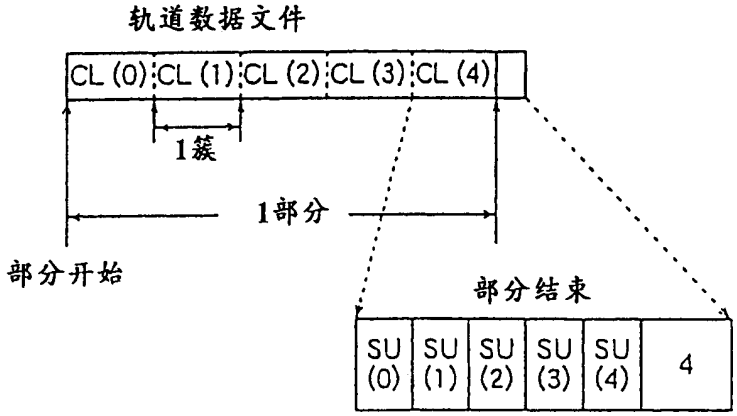

轨道数据文件
CL (0)
CL (1)
CL (2)
CL (3)
CL (4)
1簇
1部分
部分开始
部分结束
SU (0)
SU (1)
SU (2)
SU (3)
SU (4)
4

图 9

A3Dnnnnn.MSA(ATRAC3 数据文件)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-HD0				保留		MCode		保留				BLOCK SERIAL			
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU				INX		XT	
0x0020	NM1(256)															
0x0120	NM2(512)															
0x0310																
0x0320	保留(8)								CONTENTSKEY							
	保留(8)								MAC							
	保留(12)												A	LT	FNo	
	MG(D)SERIAL-nnn															
0x0360	CONNUM				YMDhms-S				YMDhms-E				MT	CT	CC	CN
0x0370	PRTSIZE				PRTKEY								保留(8)			
0x0380					CONNUM0				PRTSIZE(0x0388)				PRTKEY			
0x0390					保留(8)								CONNUM0			
	INF(0x0400)															
0x3FFF	BLKID-HD0				保留		MCode		保留				BLOCK SERIAL			
0x4000	BLKID-A3D				保留		MCode		CONNUM0				BLOCK SERIAL			
0x4010	BLOCK SEED								INITILIZATION VECTOR							
0x4020	SU-000(N字节=384字节)															
0x41A0	SU-001(N字节)															
0x4320	SU-002(N字节)															
0x04A0	SU-041(N字节)															
0x7DA0																
0x7F20	保留(N字节=208字节)															
	BLOCK SEED															
0x7FF0	BLKID-A3D				保留		MCode		CONNUM0				BLOCK SERIAL			

图 10

图 11

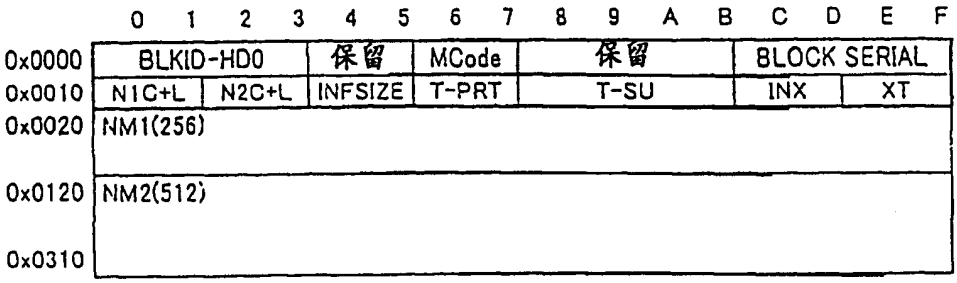


图 12

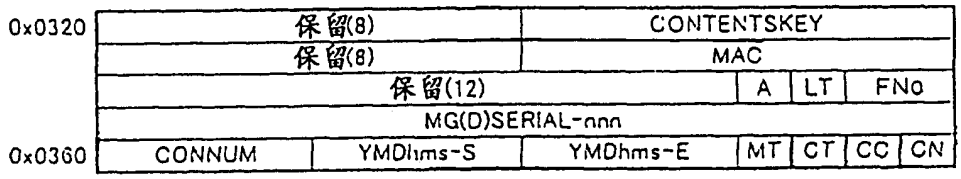


图 13

比特 7: ATRAC3 的模式

比特 6,5,4 3 比特的N:模式值

N	模式	时间	发送速率	SU	BYTES
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	单	181min	47kbps	119SU	136
0	单	258min	33kbps	169SU	96

比特 3: 保留

比特 2: 数据类型 0: 音频 1: 其他

比特 1: 再现跳跃 0: 正常接收 1: 跳跃

比特 0: 加重 0: 断 1: 开(50/15μS)

图 14

HCMS

比特7：允许复制 0：禁止复制 1：允许复制

比特6： 产生 0：原始的 1：首先或后来的副本生成

比特5-4：高速数字复制的复制控制

00:允许复制 01:复制首先生成 10：允许复制

禁止首先副本生成的复制

比特3-2: MagicGate验证级

00:级10(非MG) 01:级1

10:级2 11:保留

在级10以外中，禁止分离和组合

比特1.0: 保留

图 15

0x0370	PRTSIZE	PRTKEY		保留(8)
0x0380		CONNUM0	PRTSIZE(0x0388)	PRTKEY
0x0390		保留(8)		CONNUM0

图 16

0x4000	BLKID-A3D	保留	MCode	CONNUM0	BLOCK SERIAL
0x4010	BLOCK SEED			INITILIZATION VECTOR	
0x4020	SU-000(N字节=384字节)				

要被存储在便携式播放器 4 的存储单元61中的数据

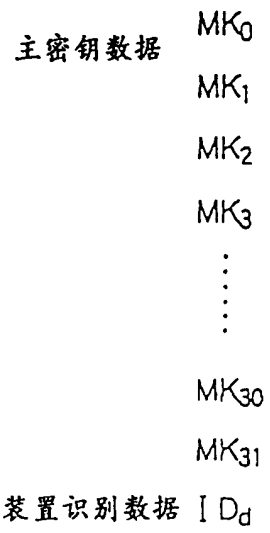


图 17

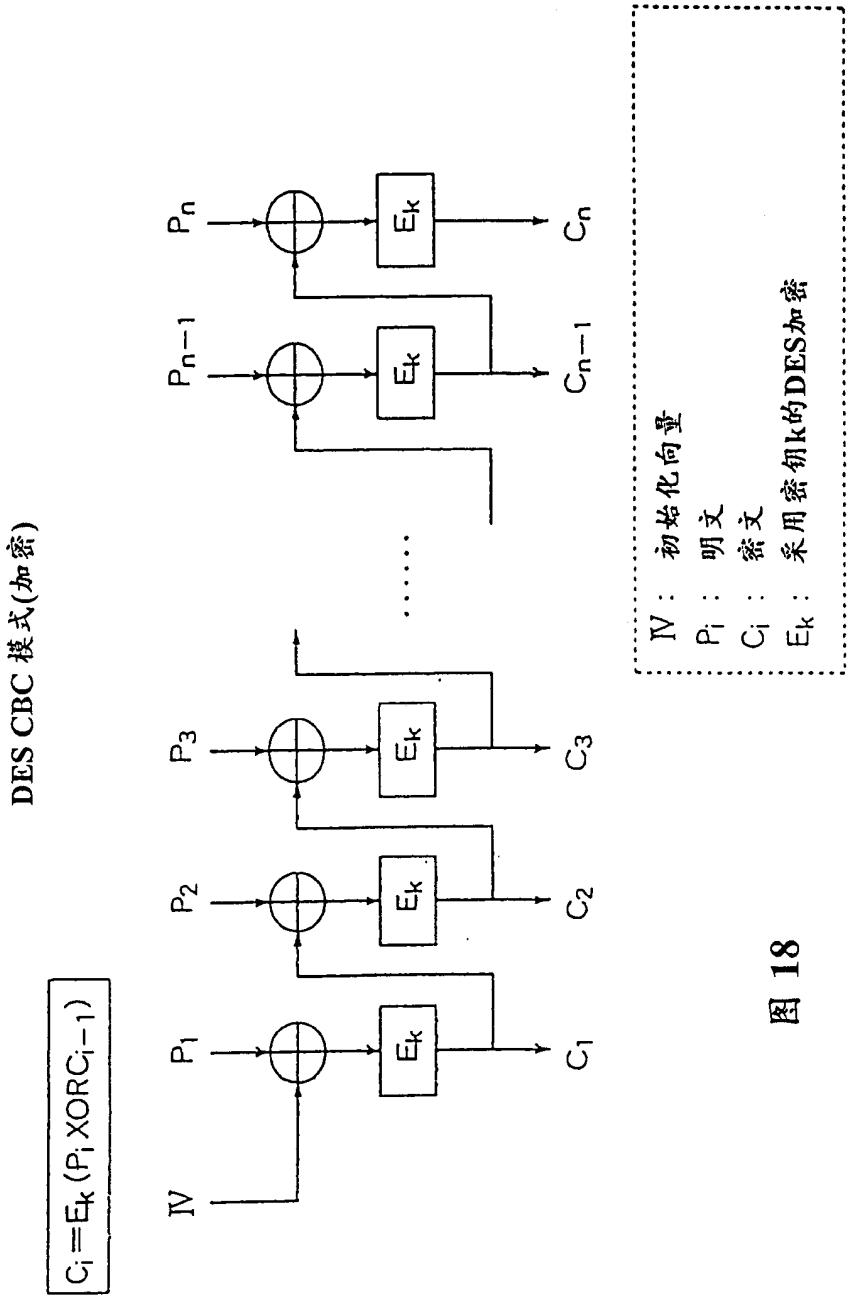

DES CBC 模式(加密)
$C_i = E_k(P_i \text{ XOR } C_{i-1})$
IV
P_1
P_2
P_3
P_{n-1}
P_n
E_k
C_1
C_2
C_3
C_{n-1}
C_n
IV：初始化向量
P_i：明文
C_i：密文
E_k：采用密钥k的DES加密

图 18

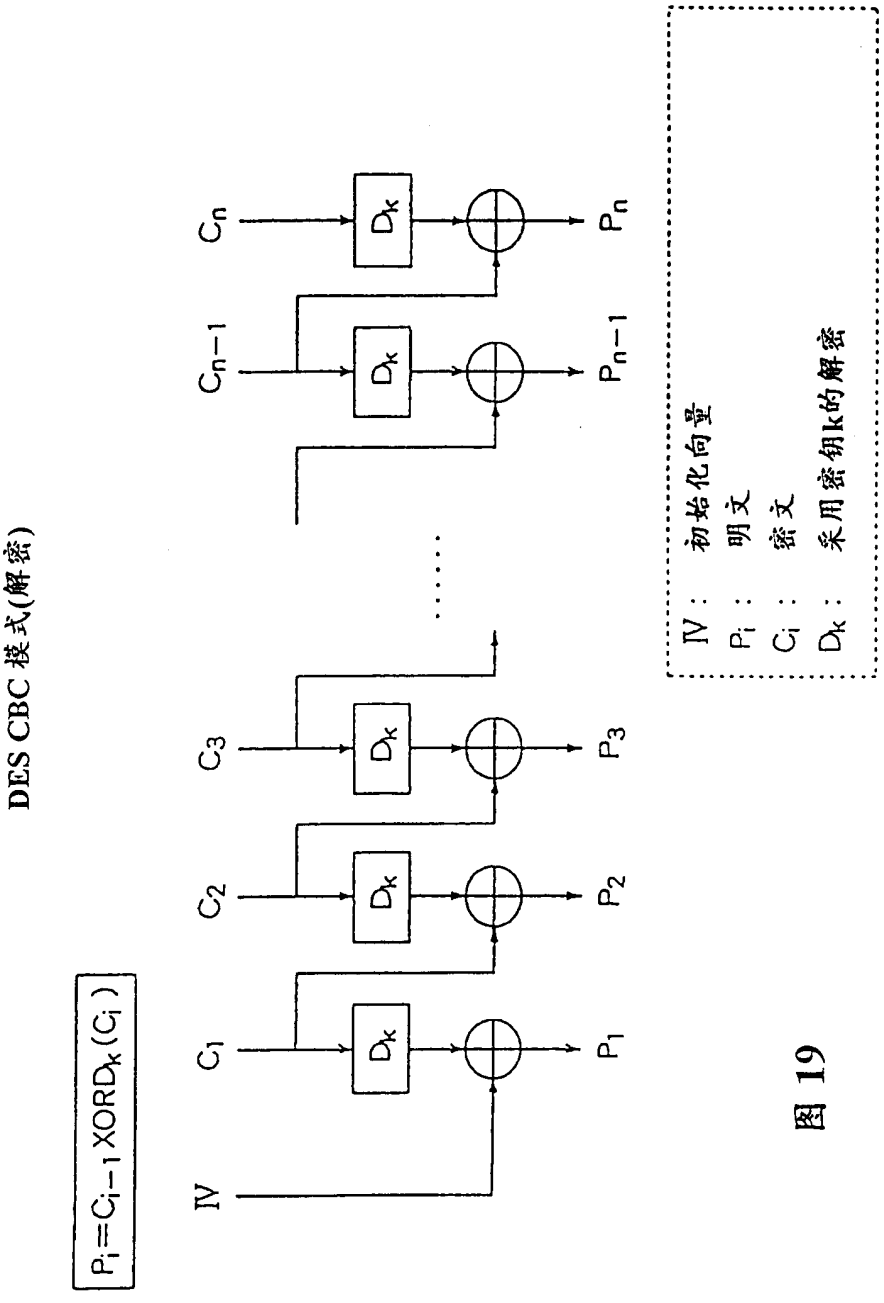
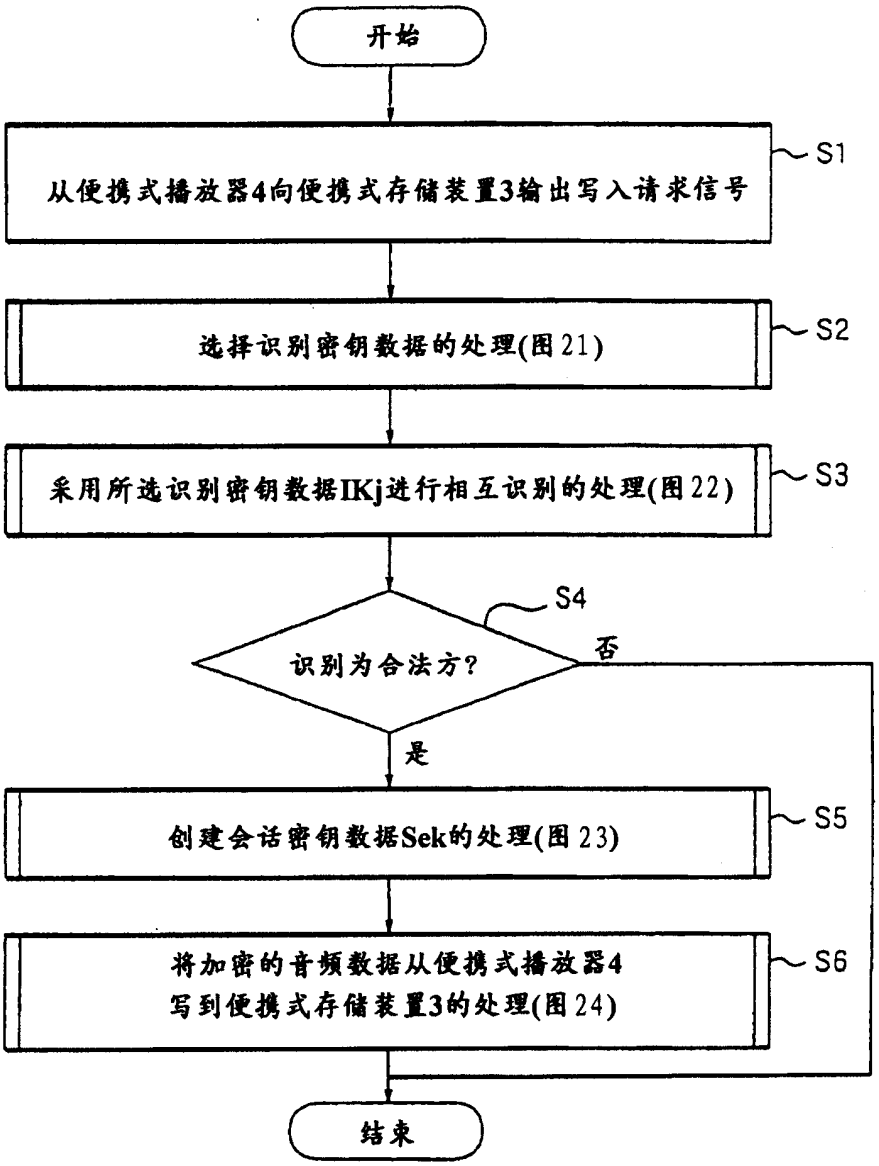

DES CBC 模式(解密)
$P_i = C_{i-1} XOR D_k(C_i)$
IV
C_1
C_2
C_3
C_{n-1}
C_n
D_k
P_1
P_2
P_3
P_{n-1}
P_n
IV : 初始化向量
P_i : 明文
C_i : 密文
D_k : 采用密钥k的解密

图 19



向便携式存储装置的写入处理

图 20

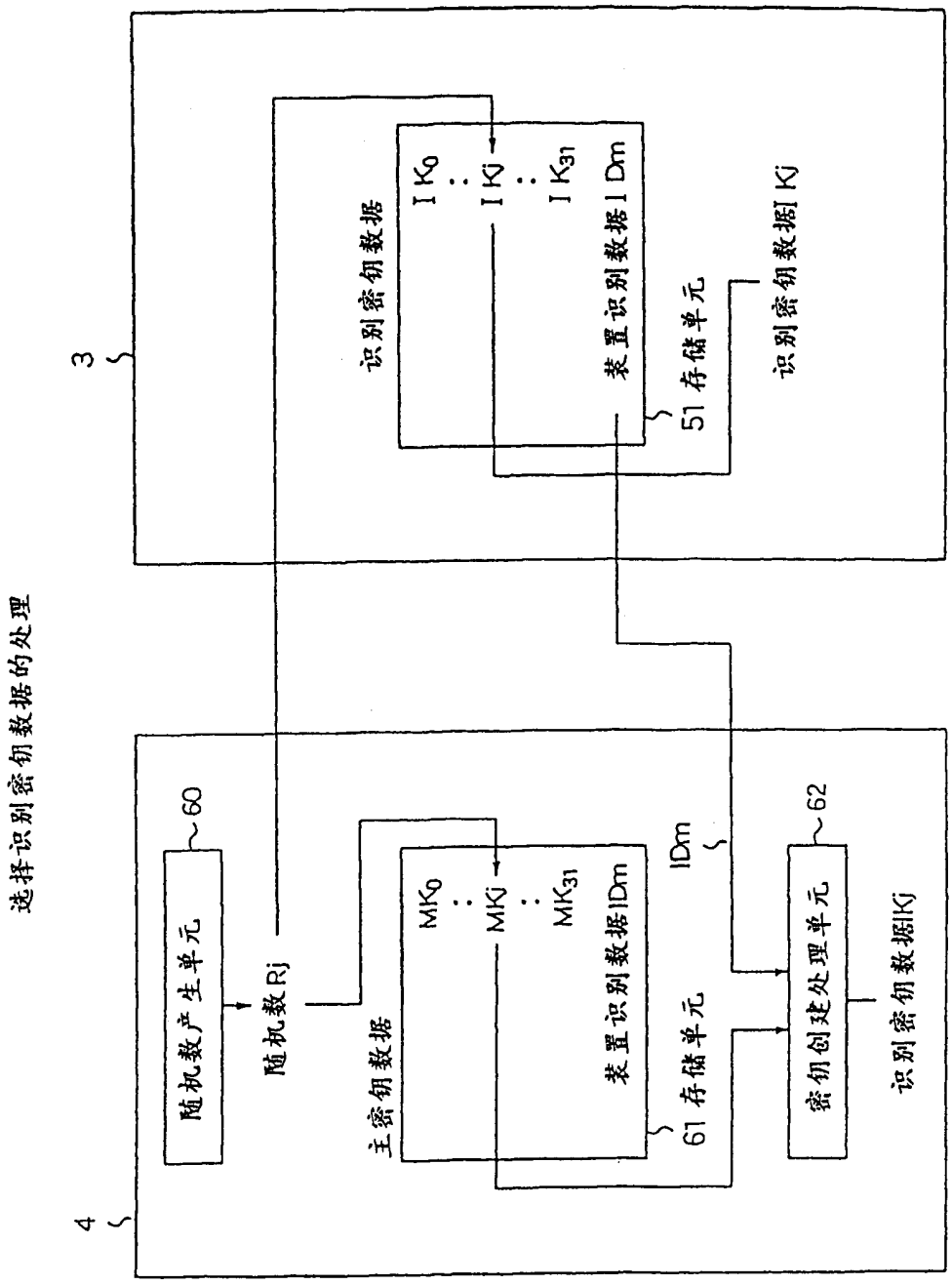

选择识别密钥数据的处理
3
识别密钥数据
I K0
I Kj
I K31
装置识别数据I Dm
51 存储单元
识别密钥数据I Kj
4
随机数产生单元
60
随机数Rj
主密钥数据
MK0
MKj
MK31
装置识别数据IDm
IDm
61 存储单元
密钥创建处理单元
62
识别密钥数据IKj

图 21

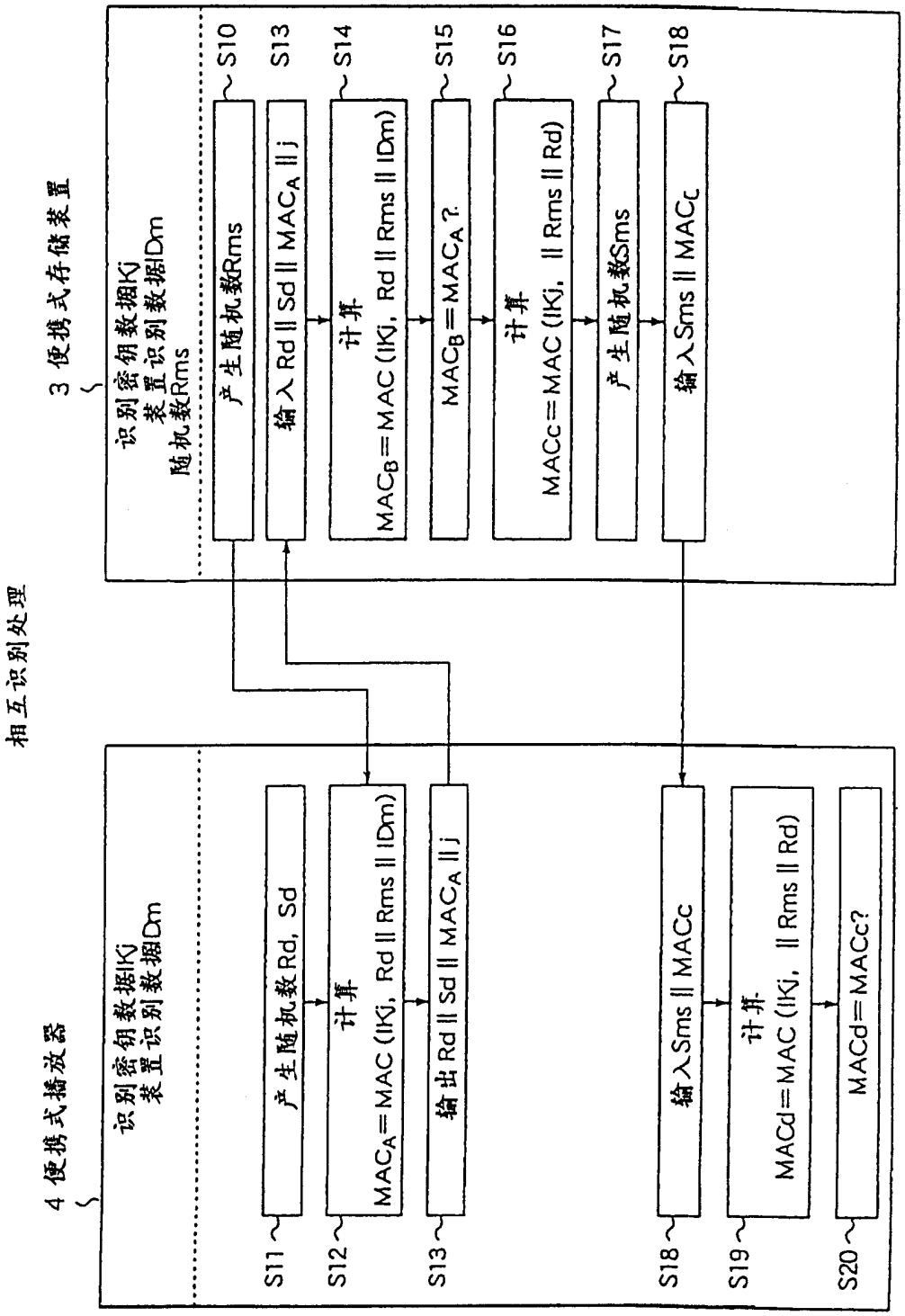

相互识别处理
4 便携式播放器
识别密钥数据IKj
装置识别数据IDm
S11 产生随机数 Rd, Sd
S12 计算
MACA = MAC (IKj, Rd || Rms || IDm)
S13 输出 Rd || Sd || MACA || j
S18 输入Sms || MACc
S19 计算
MACd = MAC (IKj, || Rms || Rd)
S20 MACd = MACc?
3 便携式存储装置
识别密钥数据IKj
装置识别数据IDm
随机数Rms
S10 产生随机数Rms
S13 输入 Rd || Sd || MACA || j
S14 计算
MACB = MAC (IKj, Rd || Rms || IDm)
S15 MACB = MACA ?
S16 计算
MACc = MAC (IKj, || Rms || Rd)
S17 产生随机数Sms
S18 输入Sms || MACc

图 22

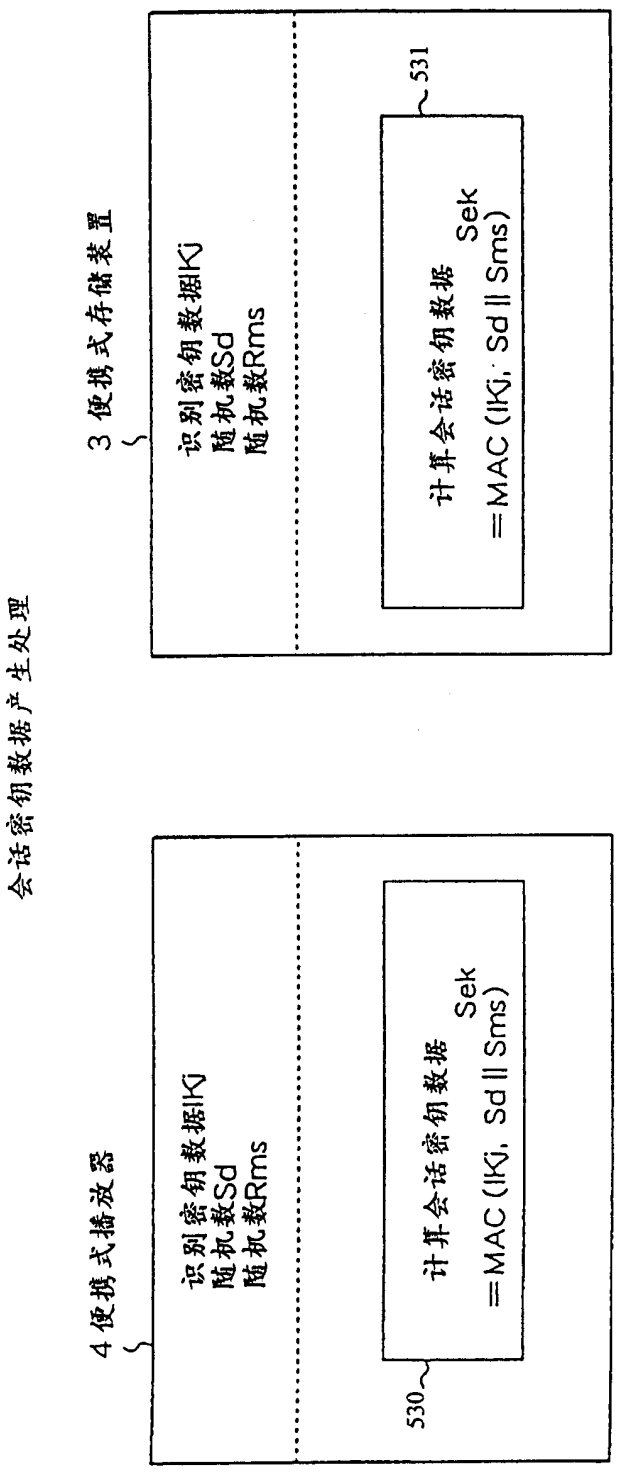

会话密钥数据产生处理
4 便携式播放器
识别密钥数据IKj
随机数Sd
随机数Rms
计算会话密钥数据 Sek
=MAC (IKj, Sd || Sms)
530
3 便携式存储装置
识别密钥数据IKj
随机数Sd
随机数Rms
计算会话密钥数据 Sek
=MAC (IKj, Sd || Sms)
531

图 23

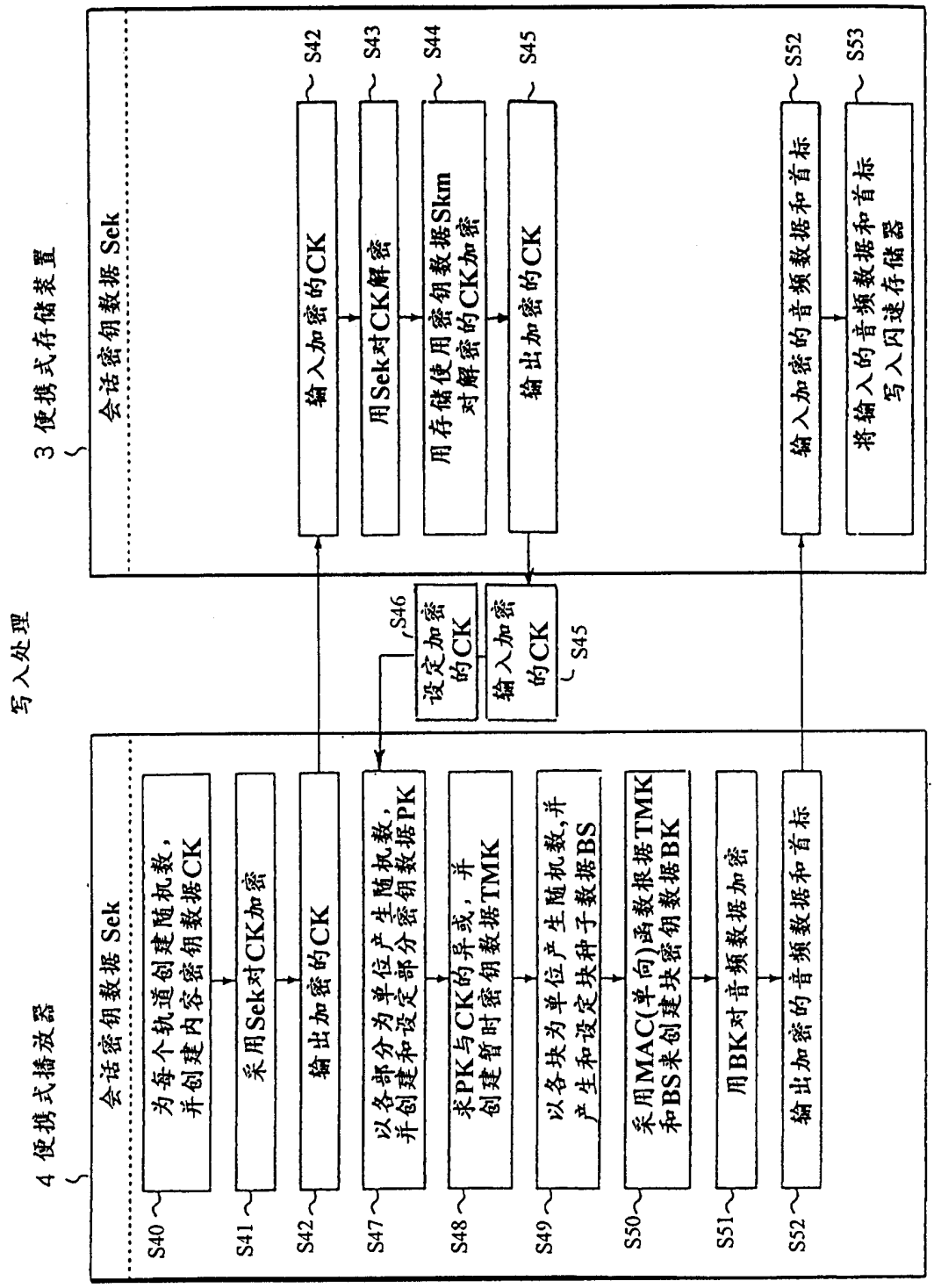
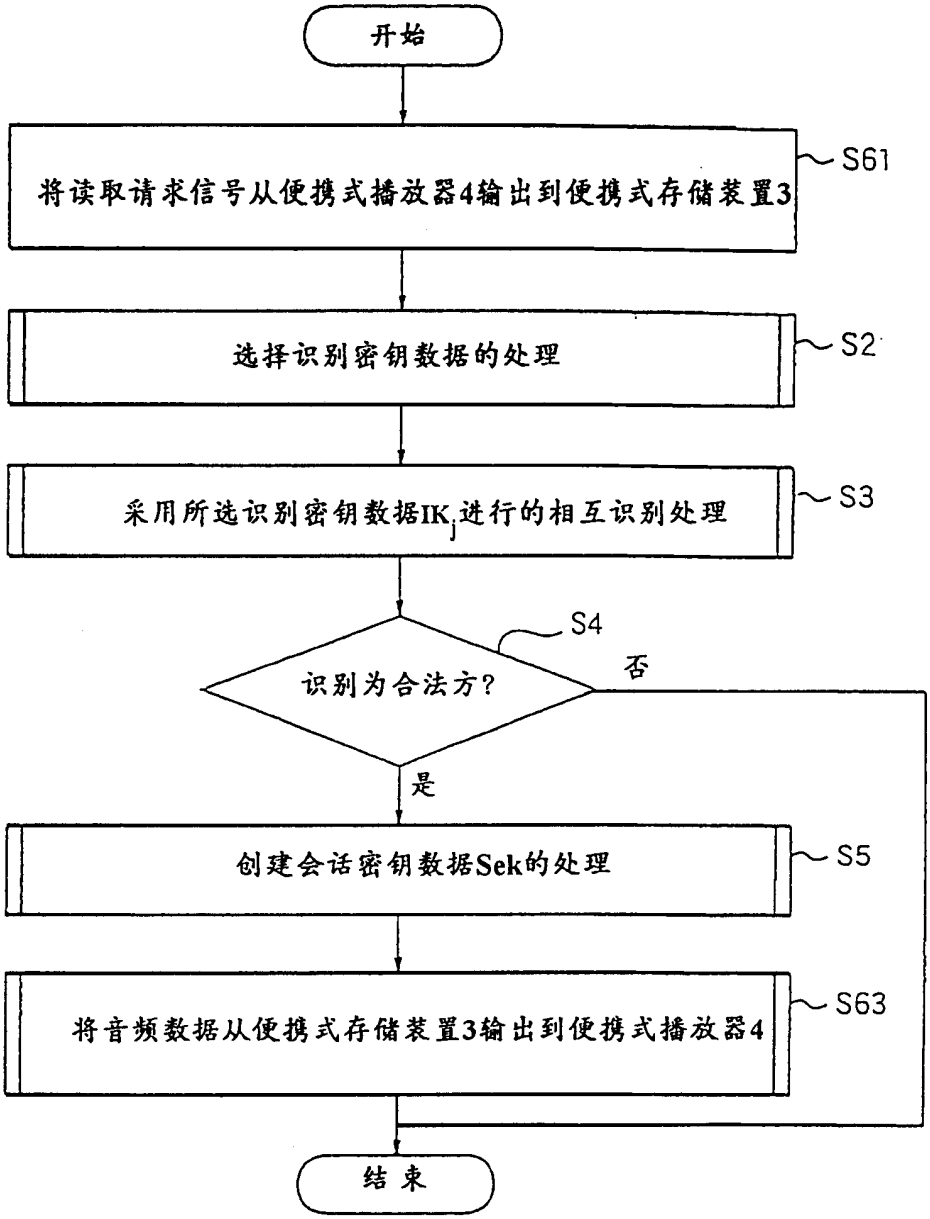

4 便携式播放器
3 便携式存储装置
写入处理
会话密钥数据 Sek
会话密钥数据 Sek
为每个轨道创建随机数，并创建内容密钥数据CK
采用Sek对CK加密
输出加密的CK
以各部分为单位产生随机数，并创建和设定部分密钥数据PK
求PK与CK的异或，并创建管时密钥数据TMK
以各块为单位产生随机数，并产生和设定块种子数据BS
采用MAC(单向)函数根据TMK和BS来创建块密钥数据BK
用BK对音频数据加密
输出加密的音频数据和首标
S40
S41
S42
S47
S48
S49
S50
S51
S52
输入加密的CK
用Sek对CK解密
用存储使用密钥数据Skm对解密的CK加密
输出加密的CK
输入加密的音频数据和首标
将输入的音频数据和首标写入闪速存储器
S42
S43
S44
S45
S52
S53
设定加密的CK
输入加密的CK
S46
S45

图 24



从便携式存储装置3 读取的处理

图 25

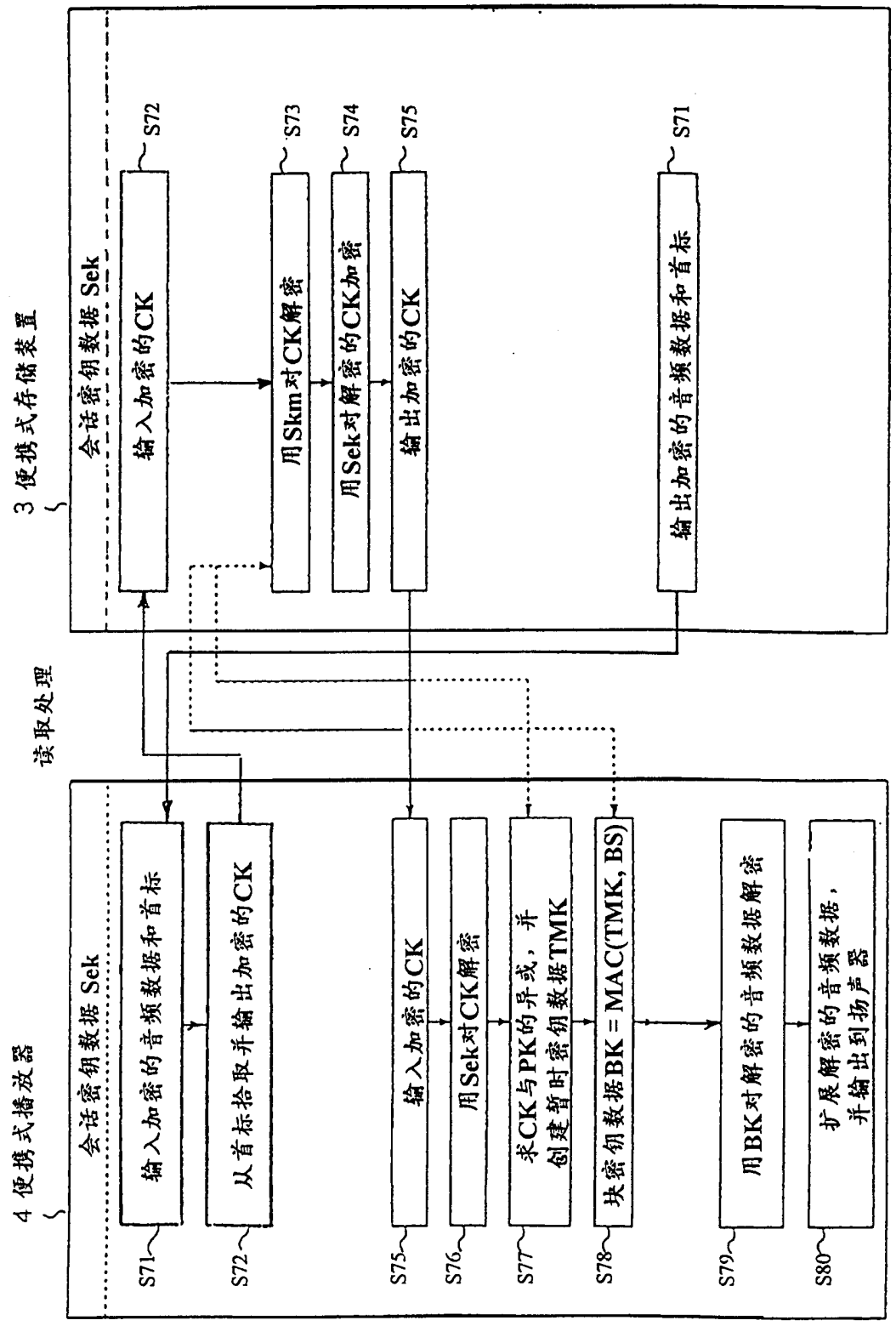

4 便携式播放器
读取处理
3 便携式存储装置
会话密钥数据 Sek
会话密钥数据 Sek
输入加密的音频数据和首标
从首标拾取并输出加密的CK
输入加密的CK
用Sek对CK解密
求CK与PK的异或，并
创建暂时密钥数据TMK
块密钥数据BK = MAC(TMK, BS)
用BK对解密的音频数据解密
扩展解密的音频数据，
并输出到扬声器
输入加密的CK
用Skm对CK解密
用Sek对解密的CK加密
输出加密的CK
输出加密的音频数据和首标
S71
S72
S75
S76
S77
S78
S79
S80
S72
S73
S74
S75
S71

图 26

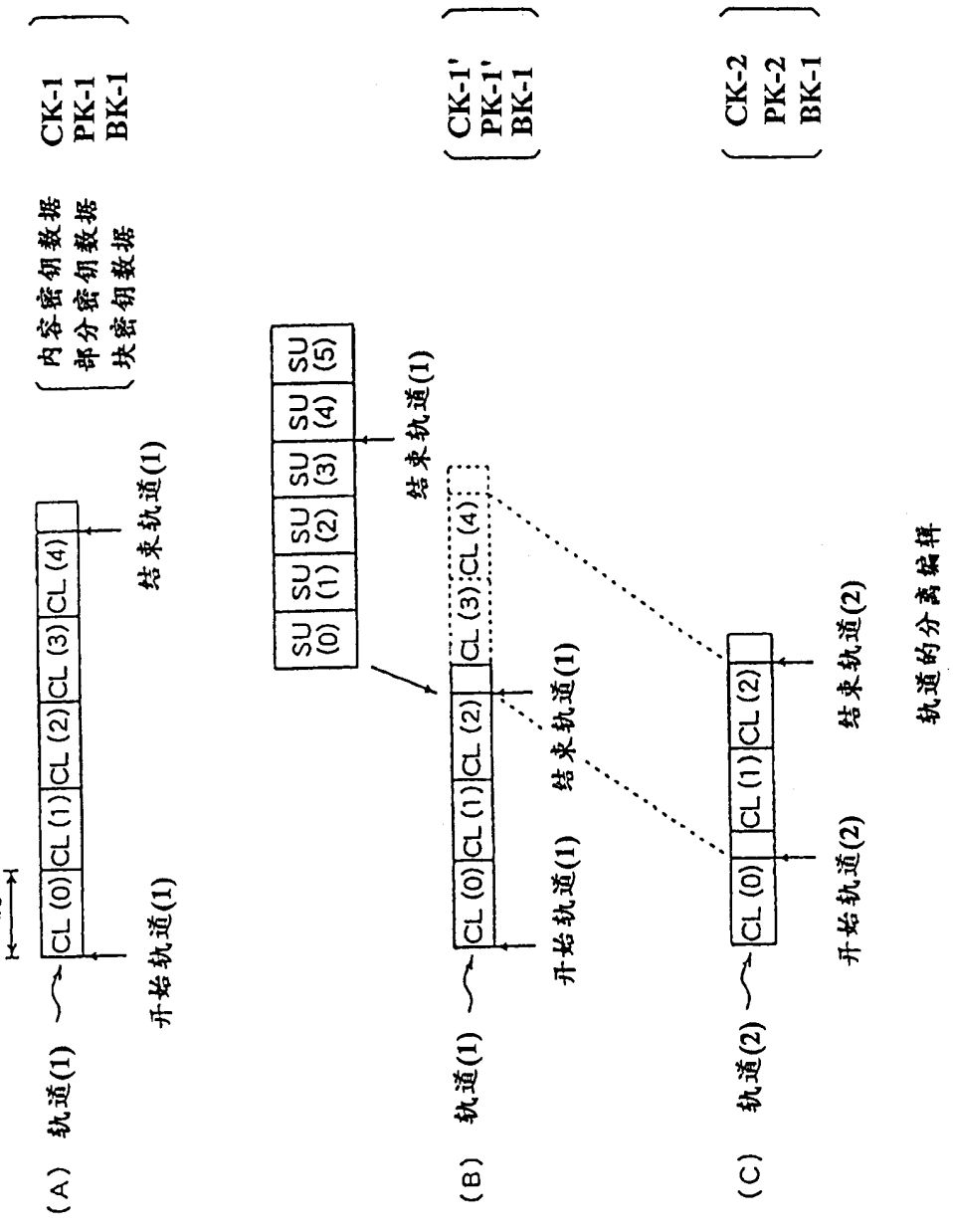

簇
(A) 轨道(1)
CL (0)
CL (1)
CL (2)
CL (3)
CL (4)
开始轨道(1)
结束轨道(1)
内容密钥数据
部分密钥数据
块密钥数据
CK-1
PK-1
BK-1
SU (0)
SU (1)
SU (2)
SU (3)
SU (4)
SU (5)
结束轨道(1)
(B) 轨道(1)
CL (0)
CL (1)
CL (2)
CL (3)
CL (4)
开始轨道(1)
结束轨道(1)
CK-1'
PK-1'
BK-1
(C) 轨道(2)
CL (0)
CL (1)
CL (2)
开始轨道(2)
结束轨道(2)
CK-2
PK-2
BK-1
轨道的分离编辑

图 27

分离后轨道(1)的簇CL(2)

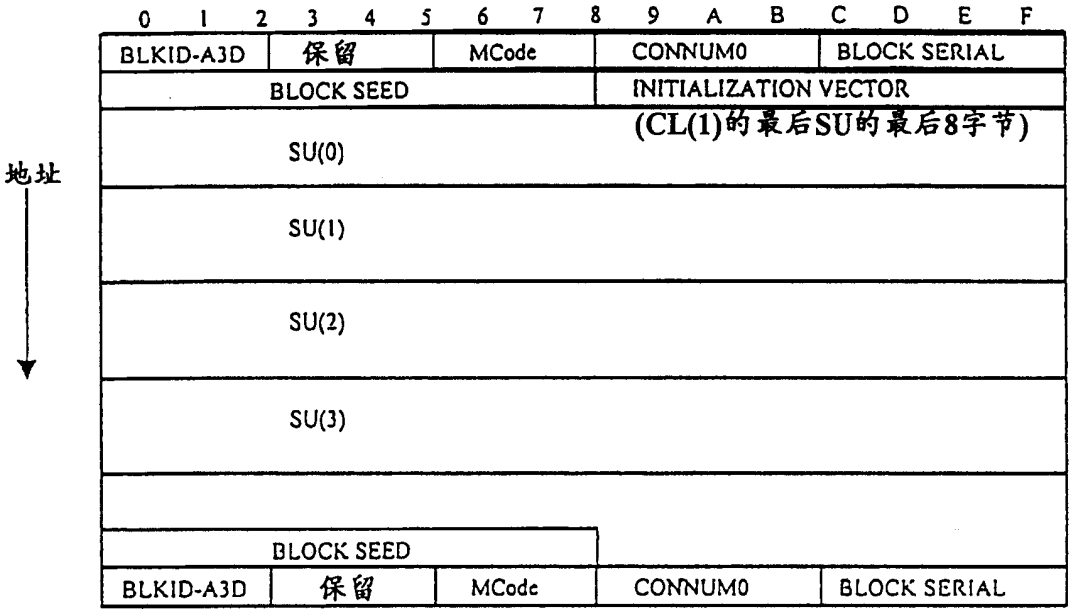


图 28

分离后轨道(2)的簇CL(0)

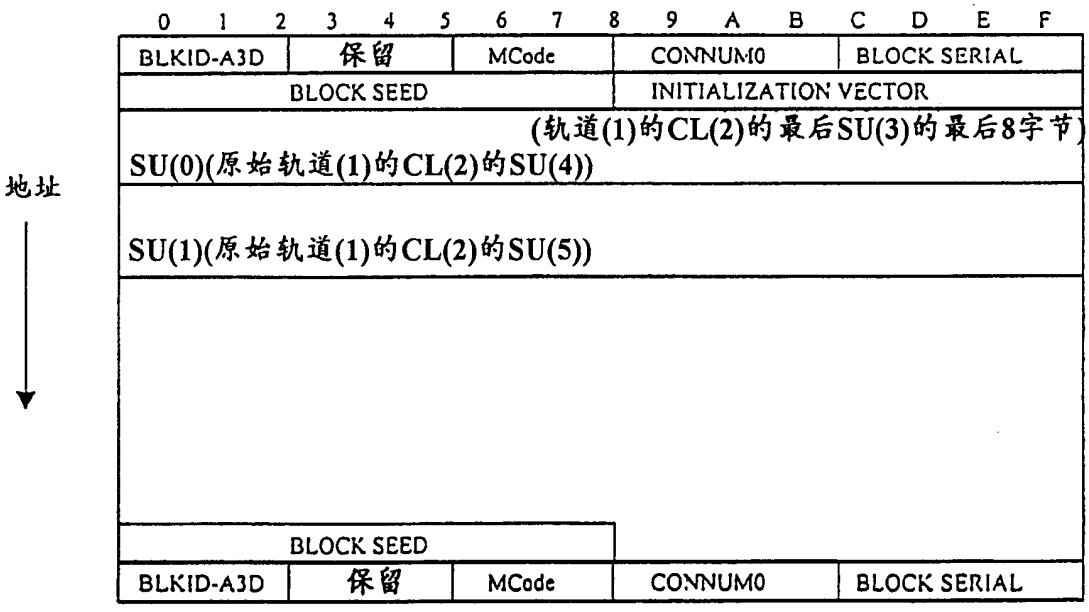


图 29

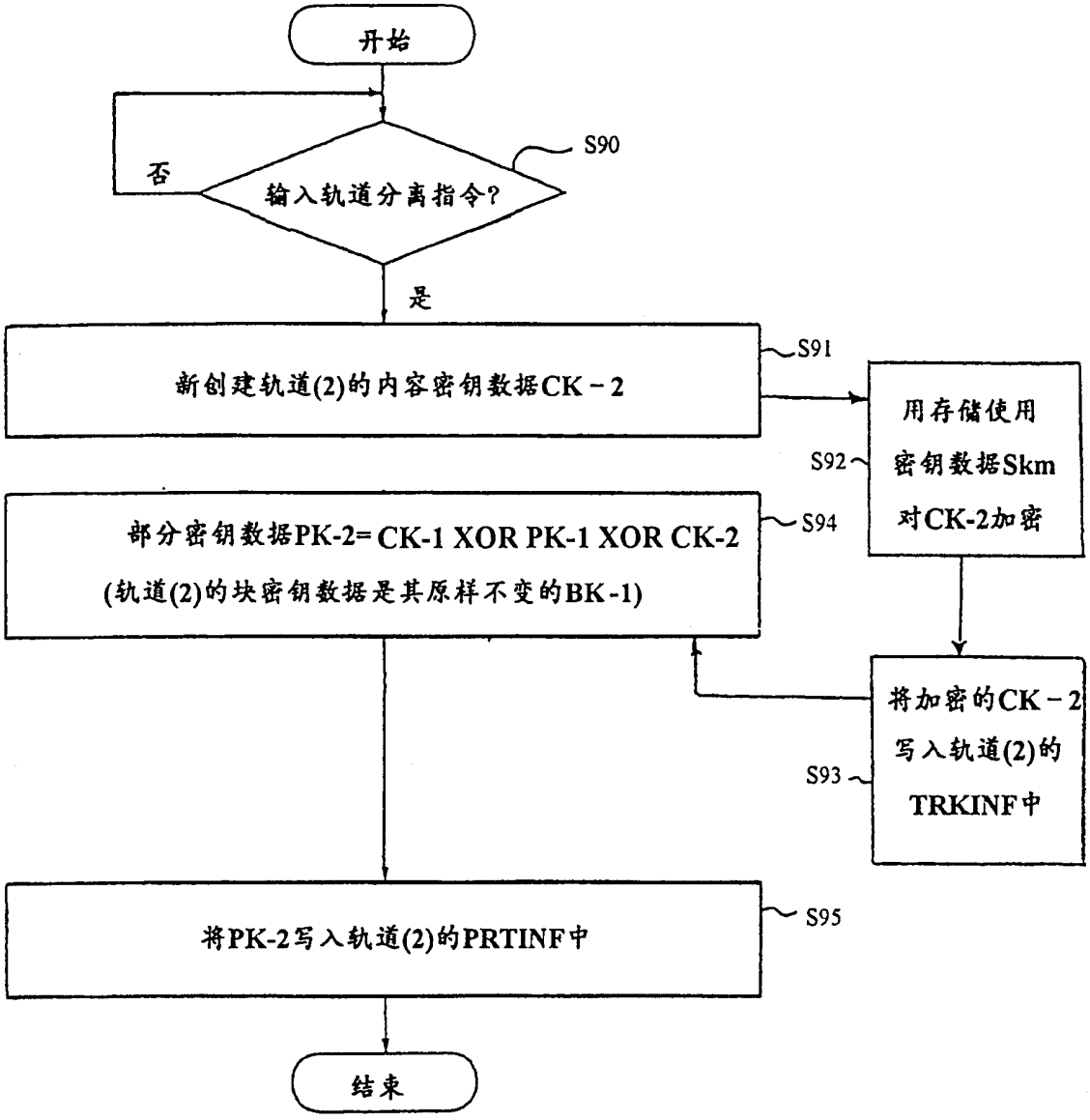

开始
S90
否
输入轨道分离指令?
是
S91
新创建轨道(2)的内容密钥数据CK－2
用存储使用
密钥数据Skm
对CK-2加密
S92
S94
部分密钥数据PK-2= CK-1 XOR PK-1 XOR CK-2
(轨道(2)的块密钥数据是其原样不变的BK-1)
将加密的CK－2
写入轨道(2)的
TRKINF中
S93
S95
将PK-2写入轨道(2)的PRTINF中
结束

图 30

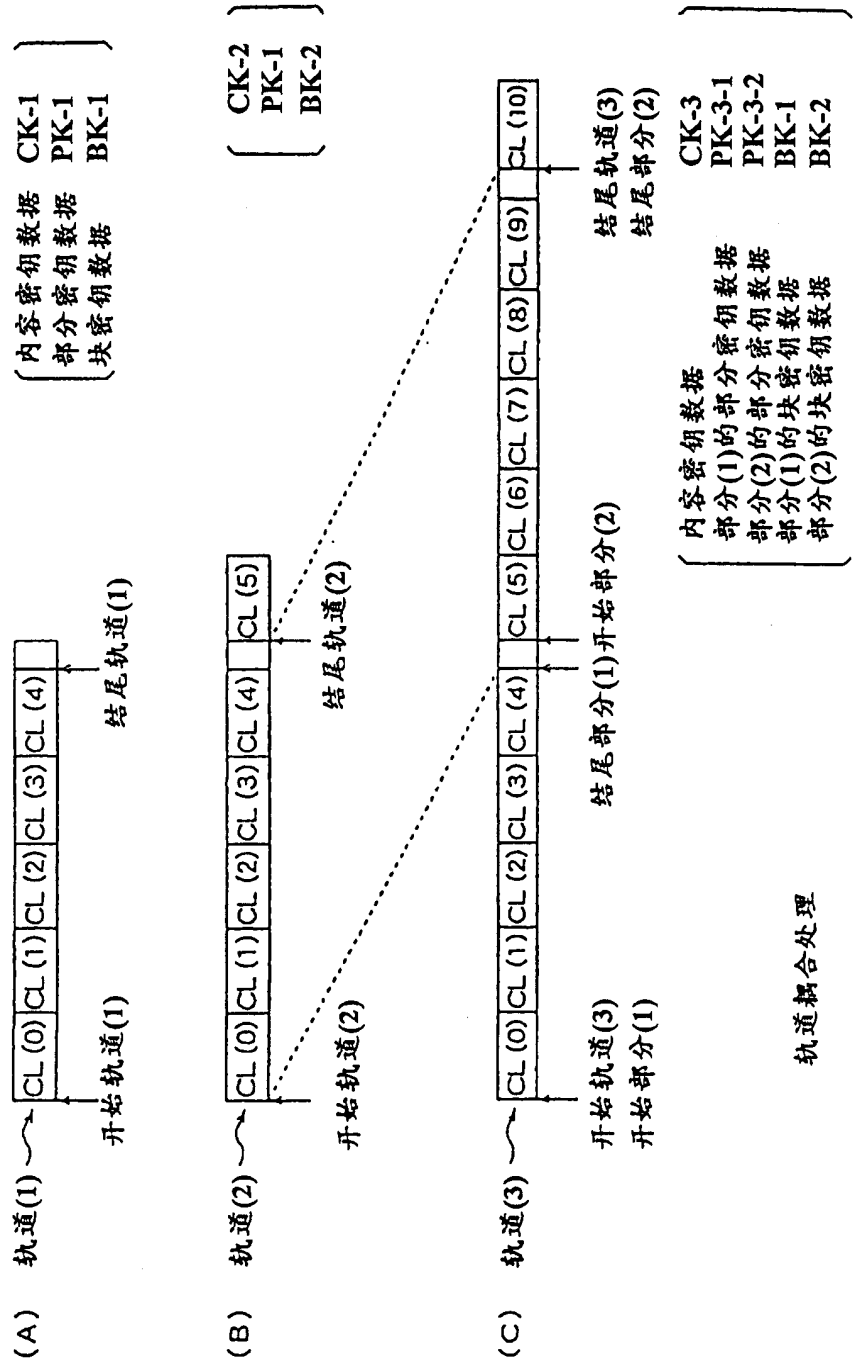

(A) 轨道(1)
CL (0) CL (1) CL (2) CL (3) CL (4)
开始轨道(1)
结尾轨道(1)
内容密钥数据 CK-1
部分密钥数据 PK-1
块密钥数据 BK-1
(B) 轨道(2)
CL (0) CL (1) CL (2) CL (3) CL (4) CL (5)
开始轨道(2)
结尾轨道(2)
CK-2
PK-1
BK-2
(C) 轨道(3)
CL (0) CL (1) CL (2) CL (3) CL (4) CL (5) CL (6) CL (7) CL (8) CL (9) CL (10)
开始轨道(3)
开始部分(1)
结尾部分(1)开始部分(2)
结尾轨道(3)
结尾部分(2)
轨道耦合处理
内容密钥数据 CK-3
部分(1)的部分密钥数据 PK-3-1
部分(2)的部分密钥数据 PK-3-2
部分(1)的块密钥数据 BK-1
部分(2)的块密钥数据 BK-2

图 31

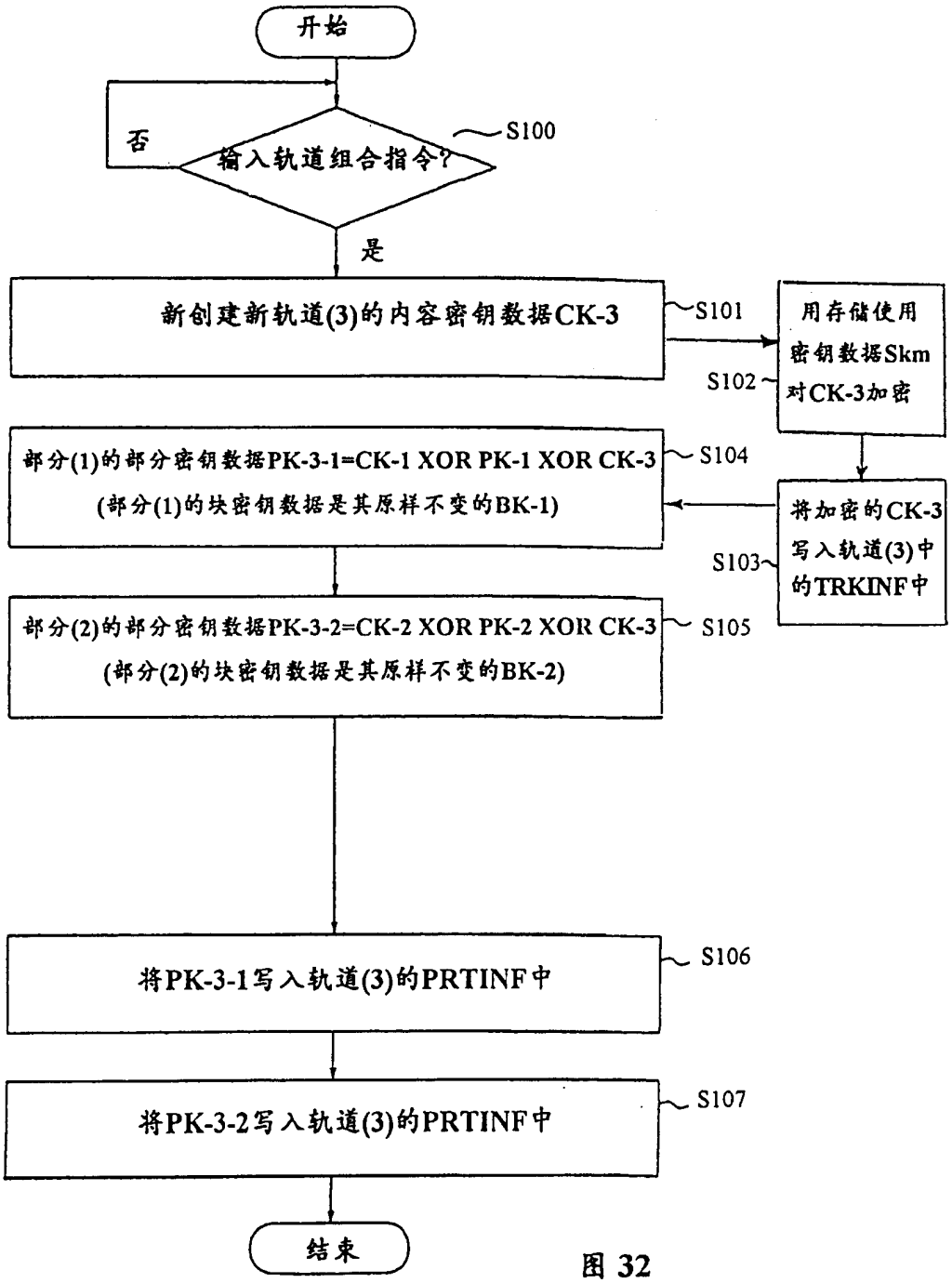

开始
否
输入轨道组合指令?
S100
是
新创建新轨道(3)的内容密钥数据CK-3
S101
用存储使用密钥数据Skm对CK-3加密
S102
部分(1)的部分密钥数据PK-3-1=CK-1 XOR PK-1 XOR CK-3
(部分(1)的块密钥数据是其原样不变的BK-1)
S104
将加密的CK-3写入轨道(3)中的TRKINF中
S103
部分(2)的部分密钥数据PK-3-2=CK-2 XOR PK-2 XOR CK-3
(部分(2)的块密钥数据是其原样不变的BK-2)
S105
将PK-3-1写入轨道(3)的PRTINF中
S106
将PK-3-2写入轨道(3)的PRTINF中
S107
结束

图 32