[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 19/00 (2006.01)
H04L 9/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 01140774.3

[45] 授权公告日 2006 年 3 月 29 日

[11] 授权公告号 CN 1248142C

[22] 申请日 2001.7.24 [21] 申请号 01140774.3

[30] 优先权

[32] 2000.7.24 [33] JP [31] 222122/00

[32] 2000.8.17 [33] JP [31] 247460/00

[71] 专利权人 索尼公司

地址 日本东京都

[72] 发明人 冈上拓己 石黑隆二

审查员 赵 芳

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 梁 永

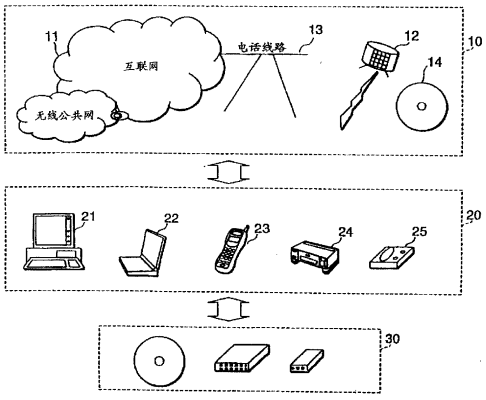
权利要求书 2 页 说明书 66 页 附图 45 页

[54] 发明名称

数据处理方法

[57] 摘要

这一数据处理系统通过在储存经过加密的内容密钥在存储器中作为相应的内容数据的标题数据之前执行一个通过施加相互不同的加密密钥来加密用来解码经过加密的内容数据的内容密钥的步骤而实现。其中一个经过加密的内容密钥包含被一个加密密钥加密的已加密数据，该加密密钥由使能密钥块提供，通过安排相关的密钥到一个处在用来发布密钥的密钥树结构的从根到枝叶的路径上的相应的节点，使能密钥块包含唯一能被特定的装置解码的数据组份。另外一个经过加密的内容密钥包含被一个对相应的存储装置正当的特定的密钥所加密的数据，存储装置使得用来再生内容数据的装置能够正当和选择性地利用经过加密的密钥的数据，从而数据处理系统正当地再生经过解码的内容数据。



1. 一个数据处理方法，包括一个初始的储存多个对加密内容数据有用的内容数据加密密钥到一个存储装置作为相应所述的内容数据的标题数据的步骤，和一个通过应用在所述的标题数据提供的一个所述的内容数据加密密钥而加密相应的内容数据的确保步骤；其中：

所述的标题数据被储存在所述的存储装置中；其中所述的标题数据包含多个经由通过施加相互不同的密钥加密密钥加密所述的内容加密密钥的过程生成经过加密的内容加密密钥。

2. 根据权利要求 1 所要求的数据处理方法，其中：

所述的相互不同的密钥加密密钥包括：

多个处在用来构建一个密钥树的路径上的更新密钥，该密钥树包含多个按照相应的多个处在从所述密钥树的根到所述的包含多个装置作为自己枝叶的密钥树的枝叶的路径上的多个根、节点和枝叶分布的密钥；

多个使能密钥块，它们分别包含一个密钥加密密钥，这一密钥加密密钥被包含通过施加下一层密钥加密上一层的密钥的数据的使能密钥块所加密；和

一个对一个用来储存内容数据在其中的存储装置正当的储存密钥。

3. 根据权利要求 2 所要求的数据处理方法，其中在构成所述的密钥树结构的枝叶的多个装置中，

每个包含所述使能密钥块分布密钥加密密钥的所述使能密钥块使得只有有正当的授权的装置能够解码所述的使能密钥块发布密钥加密密钥，而每个所述的使能密钥块阻止所述的没有正当的授权的装置解码所述的发布密钥加密密钥。

4. 根据权利要求 2 所要求的数据处理方法，其中：

所述的标题数据包含一个用以辨认所述使能密钥块发布的密钥加密密钥是实际储存还是没有储存的辨识数据。

5. 根据权利要求 1 或 2 所要求的数据处理方法，其中，在从所述的标题数据的存储装置中再生一个内容数据和一个分布在相应的标题数据的内容数据的处理过程中，

所述的数据处理方法在最终通过施加所述的获取的内容加密密钥解码所述的内容数据之前选择所述的多个内容加密密钥中的一个，以获取一个适当的内容加密密钥。

6. 根据权利要求 2 所要求的数据处理方法，其中，在从所述的标题数据的存储装置中再生一个内容数据和一个分布在相应的标题数据的内容数据的处理过程中，

所述的数据处理方法执行以下的序列的步骤：首先，基于一个相应自己的枝叶安排的枝叶密钥，该枝叶处在包含多个再生装置作为自己的枝叶和包含多个处在从所述的根到述所的密钥树的所述的枝叶的路径上的相应的多个根、节点和枝叶上的密钥的密钥树结构中，所述的数据处理方法执行：

一个经由一个解码装置密钥块的处理过程获取一个特定的节点密钥的装置密钥块处理步骤，装置密钥块包含一个经过加密的密钥的集合，这一集合包含多个分布在从自己的枝叶到上一层的密钥的路径上的节点密钥的步骤；和

一个基于获取的节点密钥处理所述的使能密钥块的最终步骤。

数据处理方法

技术领域

本发明涉及一种数据处理系统、一种数据处理方法、一种数据处理装置、以及一种计算机程序提供介质。更具体地讲，本发明涉及这样一种数据处理系统、一种数据处理方法、一种数据处理装置、以及一种程序提供介质，在其中引入一个树状结构类型的分层密钥发布系统，使得它可能通过减少信息的体积减少发布内容密钥和发布其它加密密钥的负载，从而能够通过分层的密钥发布树管理装置保持数据的安全性和相应获得处理数据的更高的效率。

背景技术

最近，经包括音乐数据、游戏程序、图片数据等各种软件数据发布的所谓“内容”数据进一步增长，这些数据是分别通过诸如互联网服务线路、或包括记录卡、DVD（数字多功能盘）、CD（密致盘）等便于分发的记录介质分别发布的。

以上的发布的内容数据由个人计算机、再生装置或得到许可的游戏机再生，或者通过包括存储卡、CD、DVD 等装载到以上所提到的装置的记录介质再生。另外，以上的内容数据还被可再生地存储在安装在个人计算机的一个再生装置和一个记录介质中，比如存储卡或硬盘等记录介质中。

任何以上提到的再生装置、游戏机、以及诸如个人计算机等信息装置包含有一个接口装置以接收发布的内容数据或者访问 DVD 和 CD，而且还包含一个用来再生内容数据所需的控制装置，还包含 RAM（随机存储器）和 ROM（只读存储器），用来存放程序和各种数据。

基于由用户通过再生装置、游戏机、诸如个人计算机等信息装置发出的指令，或者基于使用者通过联接的输入装置发出的指令，各种内容数据，例如音乐数据、图片数据、程序数据，分别由内建的或可载入的记录介质输出，接着通过数据再生装置再生或通过相连的显示装置和扬声器单元重现。

传统上，发布游戏程序、音乐数据、图片数据或类似的数据的权利由

相应的生产者或市场代理商所保留。因此，当发布内容数据时，只限定正当用户被授权使用该内容数据，而不允许未授权的用户进行内容数据的再生。换句话说，建立一个保护以确保数据的安全性是一个惯例。

一个加密发布的内容数据的处理过程构成了一个可行的限制使用者应用内容数据的手段。具体的说，加密方法通过例如互联网服务线路发布各种内容数据，包括诸如经过加密的音频数据、图片数据、游戏程序或类似的数据，另外，它也使得只有那些得到授权而成为正当用户的人才能解码所发布的经过加密的内容数据。换句话说，只有那些经过验证的用户才被授权接收到解码密钥。

经过加密的数据只有通过完成与先前的处理过程相应的解码处理过程时才能正确地恢复成为实际可用的解码数据，比如纯文本数据。这些用于加密数据的处理过程和用于解码数据的解码方法和处理过程是众所周知的。

在那些通过应用一个加密密钥和一个解码密钥以加密和解码数据的方法中，其中有一种称作公共密钥加密系统。这一公共密钥加密系统通过应用一个公钥实现数据加密和数据解码。这一系统提供给经过验证的正当使用者以公钥，以加密和解码接收的数据，借此阻止未经验证没有公钥的使用者不正当地访问数据。一个典型的被引用的公钥加密系统是 DES（数据加密标准）。

以上用于所述的加密和解码的处理过程的加密密钥和解码密钥可以通过一个单向的函数来进行保护，例如通过象基于某个口令的 Hash 函数来保护。这种单向函数使得反向地从输出值计算出输入值变得异常困难。例如，基于使用者输入的预定的口令，通过应用单向函数，产生的输出值、一个加密密钥、一个解码密钥被分别生成。另一方面，实际上不可能从通过以上的处理过程产生的加密密钥和解码密钥来识别上述的作为原始数据的口令。

有一种称作公开密钥加密的处理方法，它采用一种运算法则，基于一个利用加密密钥的加密处理过程和一个利用解密密钥的解码过程，这些密钥针对不同的运算法则而各不相同。公开密钥加密处理过程采用一个公开密钥公共地给非特定的用户使用。这一加密方法通过施加一个特定的用户发布的公开密钥来加密发布给这一特定用户的文档。这一被公开密钥加密的文档只能被通过施加一个与用来加密这一文档的公开密钥相应的唯一的

私钥而解密。由于私钥为发布公钥的特定的用户所保留，被公开密钥所加密的文档也只能唯一地被保留有私钥的特定的用户所解码。RSA（Rivest Shamir Adleman）是上述的公开密钥加密方法的一个典型的体系。通过利用公开密钥加密方法，就可能建立一个使得加密的内容数据唯一被验证的正当用户解码的体系。

上面提到的多个内容数据发布系统通过互联网线路或诸如 DVD、CD 等存储介质向指定的用户提供加密的内容数据，同时发布一个对经过验证的正当的用户唯一的特定的内容密钥来解码经过加密的内容数据。而且，也提出了这样一个体系，它加密内容数据密钥以防止犯罪者非法地再生内容数据，然后将加密的内容数据密钥发布给经过验证的正当用户，使得它们可用通过应用为经过验证的正当用户所唯一持有的解码密钥而解码内容数据密钥，从而使得其可以使用付送的内容数据密钥。

通常，在发送数据内容的内容数据提供者和个人用户的特定的装置之间，这个认定相应的使用者是否是正当用户的判定先于内容数据或内容数据密钥执行。执行这样一个通常的授权过程是，首先，确认对方的身份，然后生成一个只对相关的传送过程起作用的阶段性的区间密钥。只有完成授权过程之后，利用相应产生的阶段性的密钥进行加密的内容相关的数据或内容数据密钥才实施相应的传送。有两类授权的方法，一是通过利用以上所述的公共密钥加密办法进行公共的授权；另一是利用以上所述的公开密钥加密方法。但在利用公共密钥进行授权的情形中，需要另一个公共密钥以应付系统结构的扩展，因而产生了更新相关的密钥的不便。另一方面，在采用公开密钥的加密方法的情形中，计算的负担和需要的存储的空间相应很大，因此，不希望进一步为各个装置提供额外的处理装置。

发明内容

本发明的目的是提供一种数据处理系统、一种数据处理方法、数据处理装置、以及程序提供介质，它们分别有一个被施加了加密密钥块的系统，这一加密密钥块能够使用一个能够安全发布数据到正当的用户而不依靠在以上所述的数据传送放和接收方之间的相互授权认证处理过程的分层密钥发布树而实现一个安全发布密钥到一个有正当授权的装置的管理结构。在本发明中，用来解码经过加密的数据的加密处理过程密钥被以许多形式提供，更具体的说，其中一个被通过以上所述的分层密钥发布树中的加密密钥以加密模式提供，相应地，在用来执行内容再生的装置中，本发明可以

提供一个数据处理系统、数据处理方法、数据处理装置、以及一种程序提供介质，它们可以通过提供一个能够选择性选择加密密钥数据的结构而实现在装置中高效处理数据。

根据被发明的第一方面，提供了这样一个系统，它初始储存有一个能够应用于加密内容数据处理过程的加密内容数据的一个特定的密钥作为相应的内容数据标题，随后通过施加在标题数据中的内容数据加密密钥而执行一个加密的处理过程，其中标题数据包括多个分别通过以相互不同的密钥加密密钥的方式加密以上所述的内容数据加密密钥而生成的经过加密的内容数据的加密密钥。

根据基于本发明的新颖的数据处理系统的进一步的一个实用方面，以上所述的相互不同的密钥加密密钥包含以下方面：一个在从有多个装置作为枝叶构成的树的根到每一枝叶的路径上的根；一个节点；一个在构成密钥树的路径上的更新密钥，其中分别的密钥和枝叶相链接；一个（EKB）发布密钥加密密钥（KEK），包括由使能密钥块（EKB）加密的密钥加密密钥构成，该使能密钥块包含一个通过施加下层的密钥加密上层密钥的数据；和对用来储存内容数据的存储装置正当的储存密钥（Kstm）。

根据基于本发明的新颖的数据处理系统的进一步的一个实用方面，上述的包含以上所述的使能密钥块（EKB）发布密钥加密密钥（KEK）的完成的密钥块（EKB）由这样一个使能密钥块（EKB）组成，它能在处于构成以上的密钥树的枝叶的装置中的保有经过认证的正当的许可的装置所解码。从而以上的（EKB）密钥被阻止了在没有经过认证的正当许可的不当装置中被解码。

根据基于本发明的数据处理系统的进一步的一个实用方面，以上的标题数据包含一个指示实际储存的数据或指示缺少（EKB）发布密钥加密密钥（KEK）的数据。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理系统包含一个用来储存以上所述的标题数据和想应所述的标题数据的内容数据的存储装置和一个再生储存在所述的存储装置中的内容数据的再生装置，其中再生装置初始选择经过加密的内容数据加密密钥的任何一个从而执行一个加密内容数据的处理过程。

根据基于本发明的数据处理系统的进一步的一个实用方面，被以上所述的使能密钥块（EKB）加密和提供的使能密钥块（EKB）发布密钥加密

密钥（KEK）在每一代被执行一个版本管理和升级处理过程。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理装置包含一个用来储存以上所述的标题数据和与所述的标题数据相联的内容数据的存储装置和一个再生储存在所述的存储装置中的内容数据的再生装置。在以上所述的再生装置包含这样一个构造，在密钥树的结构单元中，在通过施加对每一再生装置正当的储存密钥（Kstd）加密枝叶密钥之后，相应自己的枝叶的枝叶密钥被储存在多个再生装置的每个的储存装置中,该密钥树具有个自根据在有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列的密钥。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理装置包含一个用来储存以上所述的标题数据和相应每一标题数据的内容数据的存储装置和多个再生储存在所述的存储装置中的内容数据的再生装置。在密钥树的结构单元中，一个相应自己的枝叶被提供的枝叶标识成分被储存在安置在以上所述的再生装置中的每个中的存储装置中，该密钥树具有个自根据在有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列的密钥。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理装置包含一个用来储存以上所述的标题数据和相应每一标题数据的内容数据的存储装置和多个再生储存在所述的存储装置中的内容数据的再生装置。在密钥树的结构单元中，在通过施加对每一再生装置正当的储存密钥（Kstd）加密枝叶密钥之后，每个的再生装置储存一个相应在安装在每个再生装置中的存储装置中的自己的枝叶的枝叶密钥，该密钥树具有个自根据在有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列的密钥。对每一再生装置正当的储存密钥（Kstd）基于相应在以上所述的密钥树结构中的一个再生装置的枝叶部分的以上所述的枝叶标识成分而生成。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理装置包含一个用来储存以上所述的标题数据和相应每一标题数据的内容数据的存储装置和多个再生储存在所述的存储装置中的内容数据的再生装置。在密钥树的结构单元中，基于一个相应自己的枝叶提供的特定的枝叶密钥，每一再生装置使自己的存储装置可以存储装置密钥块（DKB），这一装置密钥块（DKB）包含一个由各个承受从密钥树中自己

的枝叶到上一层的枝叶的多个路径上的多个步骤的经过加密的节点密钥的集合，该密钥树具有个自根据在有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列的密钥。

根据基于本发明的数据处理系统的进一步的一个实用方面，本发明的数据处理装置包含一个用来储存以上所述的标题数据和相应每一标题数据的内容数据的存储装置和多个再生储存在所述的存储装置中的内容数据的再生装置。进一步，每个再生装置包含一个储存装置，这一储存装置用来储存这样一个初始的使能密钥块（EKB），它使得低一层的密钥去加密构成一个密钥树结构的多个路径上的多个密钥，这一密钥树结构包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列单个的密钥。

根据基于本发明的数据处理系统的进一步的一个实用方面，以上所述的初始的使能密钥块（EKB）被和在以上所述的密钥树的一个特定的阶段形成的多个目录节点的低一层的装置一起储存。

本发明的第二个使用方面涉及一个独创的数据处理方法。它包含一个初始的储存一个标题数据到一个存储装置的步骤，其中标题数据包含一个特定的用来加密和相关的内容数据相应排列的内容数据的内容数据加密密钥；和另外一个通过施加一个包含在标题数据中的特定的内容数据加密密钥而执行一个加密相应的内容数据的处理过程的步骤。

储存在以上所述的储存装置的标题数据包含多个经过加密的内容数据加密密钥，它通过施加相互不同的密钥加密密钥而加密内容数据加密密钥而生成。

根据基于本发明的数据处理方法的进一步的一个实用方面，以上所述的相互不同的密钥加密密钥包含一下方面：分布在密钥树的从根到枝叶的路径上的更新密钥，这一密钥树包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列单个的密钥；一个 EKB 密钥发布密钥，由被一个使能密钥块（EKB）加密的包含一个用来通过下一层的密钥加密上一层的密钥的加密数据的密钥加密密钥构成；和一个对以上所述的用来储存内容树的存储装置正当的储存密钥（Kstm）。

根据基于本发明的数据处理方法的进一步的一个实用方面，以上所述的包含以上所述的使能密钥块（EKB）发布密钥加密密钥（KEK）的使能密钥块（EKB）这样一个 EKB 所组成，它只能被在分别构成以上所述的

密钥树结构的枝叶的部分的装置中的有正当的授权的装置所解码，而不能被不当的没有经过认证的正当的授权的装置所解码。

根据基于本发明的数据处理方法的进一步的一个实用方面，以上的标题数据包含一个指示实际储存的数据或指示缺少（EKB）发布密钥加密密钥（KEK）的标识数据。

根据基于本发明的数据处理方法的进一步的一个实用方面，在再生从用来储存以上的标题数据的存储装置中读出的内容数据和相应标题数据的内容数据的处理过程中，数据处理方法首先在选定一个以上所述的多个经过加密的内容数据加密密钥之后获得一个正当的内容数据加密密钥，然后执行一个通过施加获得用来解码经过加密的内容数据的密钥解码经过加密的内容数据。

根据基于本发明的数据处理方法的进一步的一个实用方面，在再生从用来储存以上的标题数据的存储装置中读出的内容数据和相应标题数据的内容数据时，数据处理方法执行以下的系列的步骤：首先，包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应的多个密钥的密钥树的结构单元中，基于一个特定的相应自己的枝叶的枝叶密钥，数据处理方法执行一个 DKB 处理步骤通过一个被 DKB 执行的解码处理过程而获取一个特定的节点密钥，作为一个包含分别加密的节点密钥的加密密钥的集合，随后，数据处理方法基于获取的节点密钥执行一个处理以上所述的使能密钥块（EKB）的 EKB 处理步骤。该节点密钥负担从自身的枝叶到上一层的密钥的路径的不同的步骤。

本发明的第三个实用方面涉及一个独创的用来再生和记录内容数据的数据处理装置。数据处理装置首先执行一个储存这样一个内容数据密钥（Kcon）的处理过程，它用来加密被储存在存储装置中作为相应的所述的内容数据的标题数据的内容数据；接着通过施加包含在标题数据中的内容密钥（Kcon）加密相应的内容数据。数据处理装置通过施加在以上所述的存储装置中的不同的密钥加密密钥而促成一个包含多个经过加密的内容密钥（Kcon）的标题数据。

根据基于本发明的数据处理装置的进一步的一个实用方面，以上所述的相互不同的密钥加密密钥包含以下方面：分布在密钥树的从根到枝叶的路径上的更新密钥，这一密钥树包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应排列单个的密钥；一个 EKB 密钥

发布密钥，由被一个使能密钥块（EKB）加密的包含一个用来通过下一层的密钥加密上一层的密钥的加密数据的密钥加密密钥构成；和一个对以上所述的用来储存内容树的存储装置正当的储存密钥（Kstm）。

根据基于本发明的数据处理装置的进一步的一个实用方面，以上所述的包含以上所述的使能密钥块（EKB）发布密钥加密密钥（KEK）的使能密钥块（EKB）这样一个 EKB 所组成，它只能被在分别构成以上所述的密钥树结构的枝叶的部分的数据处理装置中的有正当的授权的数据处理装置所解码而不能被不当的没有经过认证的正当的授权的数据处理装置所解码。

根据基于本发明的数据处理装置的进一步的一个实用方面，以上的标题数据包含一个指示实际储存的数据或指示缺少（EKB）发布密钥加密密钥（KEK）的标识数据。

根据基于本发明的数据处理装置的进一步的一个实用方面，数据处理装置执行以下的系列的步骤：再生从用来储存以上的标题数据的存储装置中读出的内容数据和相应标题数据的内容数据；通过选定一个包含在标题数据中的多个经过加密的内容数据加密密钥而获得一个特定的内容数据密钥（Kcon）；和执行一个通过施加获得的内容密钥（Kcon）解码内容数据的处理过程。

根据基于本发明的数据处理装置的进一步的一个实用方面，数据处理装置执行一个再生储存在用来储存标题数据的存储装置中的内容数据和相应标题数据的内容数据的处理过程。进一步，数据处理装置在最终储存经过加密的储存密钥（Kstd）在设置在数据处理装置中的储存装置中之前，加密一个这样的枝叶密钥，它通过通过施加一个对在密钥树中的结构单元中的数据处理装置正当的储存密钥（Kstd）相应自己的枝叶而生成，该密钥树包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应的多个密钥。

根据基于本发明的数据处理装置的进一步的一个实用方面，数据处理装置执行再生储存在用来储存标题数据的存储装置中的内容数据和相应标题数据的内容数据。进一步，在包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应的单个的密钥的密钥树的结构单元中，数据处理装置通过利用一个对数据处理装置正当的储存密钥（Kstd）加密枝叶密钥的方式储存一个相应自己的枝叶的枝叶密钥到数据处理装置

中的储存装置中，其中的对数据处理装置正当的储存密钥（Kstd）基于这样的枝叶的一个枝叶标识成分而生成，它分别响应那些联合构成密钥树的数据处理装置。

根据基于本发明的数据处理装置的进一步的一个实用方面，数据处理装置执行再生储存在用来储存标题数据的存储装置中的内容数据和相应标题数据的内容数据。进一步，在密钥树的结构单元中，基于一个相应自己的枝叶提供的枝叶密钥，数据处理装置使得一个装置密钥块（DKB）作为这样一个加密密钥的集合被储存在设置在数据处理装置中的储存装置中，该密钥树包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上根、节点和枝叶相应的单个的密钥，这样一个加密密钥包含有有着多个从密钥树中自己的枝叶到上一层的密钥的路径上的不同的步骤的经过加密的节点密钥。

根据基于本发明的数据处理装置的进一步的一个实用方面，数据处理装置执行再生储存在用来储存标题数据的存储装置中的内容数据和相应标题数据的内容数据。进一步，数据处理装置使得一个初始完成的密钥块能够被储存在设置在数据处理装置的中储存装置中，该密钥块包含有多个通过下一层的密钥加密的在构成密钥树的路径上的密钥，密钥树有与在包含有多个装置作为枝叶构成的树的根到每一枝叶的路径上的根、节点和枝叶相应的单个的密钥。

本发明的第四个实用方面涉及一个程序提供介质。首先，使用这一独到的程序提供介质，作为相应的内容数据的标题数据用来加密内容数据的内容数据加密密钥被储存在存储装置中。随后，通过施加包含在标题数据中的内容数据加密密钥，程序提供介质提供一个用来通过计算机系统执行加密相应的内容数据的处理过程的计算机程序。这一独到的程序提供介质提供的计算机程序执行一个通过施加相互不同的密钥加密密钥加密内容数据加密密钥的初始的步骤和一个使得包含有多个经由先前的密钥加密步骤生成经过加密的内容数据的标题数据能够被储存在以上所述的存储装置的最终的步骤。

本发明的第四个实用方面的程序提供介质包含各种介质，它们能够经由这样一个计算机可读程序所提供，它包含各种用于能够执行所提供的程序代码的通用计算机的程序代码。实际上，这一独到的程序提供介质包括多个记录介质（如 CD、FD（软盘）、MO(磁光盘)），或者一个传送介质

（包括网络服务线路或其他的形式，没有限定）。

以上所述的独到的程序提供介质定义了计算机程序和程序提供介质之间的结构的或者功能的合作关系，以实现一个计算机系统的预定的程序的操作功能。换句话说，通过经由这一独到的程序提供介质在计算机系统安装计算机程序，合作动作在计算机系统中实现，从而使得能够和先前的本发明的实践形态一样保护一个有用的操作效果。

本发明进一步方面、特征和优势会在以下基于实践形态和附带图纸的描述中得到更全面的了解。

附图说明

图 1 示出一个涉及本发明的数据处理系统的概念的总体的示意性的设计；

图 2 示出一个涉及本发明的数据处理系统所使用的系统和数据的总体的概念的示意性的设计；

图 3 示出一个分层树状密钥结构的原理框架图，它说明涉及本发明的数据处理系统中的数据和密钥的加密处理过程；

图 4 示出用来发布涉及本发明的数据处理系统中的各种各样的密钥和数据的使能密钥块（EKB）的例子；

图 5 示出使用涉及本发明的数据处理系统中的内容密钥的使能密钥块（EKB）发布数据（或密钥）和解码的示例；

图 6 示出涉及本发明的数据处理系统中的使能密钥块（EKB）一种典型的格式；

图 7 示出涉及本发明的数据处理系统中的使能密钥块（EKB）的原理框架图；

图 8 示出涉及本发明的数据处理系统中的使能密钥块（EKB）、相联内容密钥发布的数据和内容数据的一个结构；

图 9 示出另一个涉及本发明的数据处理系统中的使能密钥块（EKB）、相联内容密钥发布的数据和内容数据的结构；

图 10 示出在向涉及本发明的数据处理系统中的存储装置存储使能密钥块（EKB）和内容数据的处理过程；

图 11 示出一个在涉及本发明的数据处理系统中的归类再每一个目录的分层树状密钥结构的例子；

图 12 示出一个在涉及本发明的数据处理系统中生成简化的使能密钥

块（EKB）的处理过程；

图 13 示出一个在涉及本发明的数据处理系统中生成使能密钥块（EKB）的处理过程；

图 14 示出在涉及本发明的数据处理系统中的简化的使能密钥块（EKB）；

图 15 示出一个在涉及本发明的数据处理系统中用到的再生装置和存储装置的原理框架图；

图 16 示出一个存储在涉及本发明的数据处理系统中的存储装置的数据；

图 17 示出一个存储在涉及本发明的数据处理系统中的存储装置的储存单元中的数据；

图 18 示出一个存储在涉及本发明的数据处理系统中的再生控制数据文件中的数据的原理示意结构；

图 19 示出一个存储在涉及本发明的数据处理系统中的数据文件中的数据的原理示意结构；

图 20 示出一个存储在涉及本发明的数据处理系统中的数据再生控制文件中的数据的进一步原理示意结构；

图 21 示出一个存储在涉及本发明的数据处理系统中的数据文件中的数据的进一步原理示意结构；

图 22 示出部分存储在涉及本发明的数据处理系统中的数据文件中的属性标题数据；

图 23 示出部分存储在涉及本发明的数据处理系统中的数据文件中的属性标题数据；

图 24 示出涉及本发明的数据处理系统中的数据文件操作模式的种类以及各个模式的记录时间；

图 25 示出在涉及本发明的数据处理系统中再生控制数据；

图 26 示出部分存储在涉及本发明的数据处理系统中的数据文件中的属性标题数据；

图 27 示出一个相应的在涉及本发明的数据处理系统中的数据文件的数据块的标题数据的原理示意布置；

图 28 示出在涉及本发明的数据处理系统中记录相关数据的过程的流程图；

图 29 示出一个可施加于涉及本发明的数据处理系统的相互授权认证处理过程；

图 30 示出在涉及本发明的数据处理系统中再生相关数据的过程的流程图；

图 31 示出一个用以认可涉及本发明的数据处理系统中的密钥的发布的数据文件的格式；

图 32 示出涉及本发明的数据处理系统中存储的数据的一个方案；

图 33 示出通过利用涉及本发明的数据处理系统中的使能密钥块（EKB）解码相关数据的过程的流程图；

图 34 示出用于联合发布使能密钥块（EKB）、授权认证密钥的数据结构，以及通过涉及本发明的数据处理系统中的相关装置处理数据的一个示例；

图 35 示出另一个用于联合发布使能密钥块（EKB）、授权认证密钥的数据结构，以及通过涉及本发明的数据处理系统中的相关装置处理数据的一个示例；

图 36 示出伴随向涉及本发明的数据处理系统施加一个虚拟存储装置的一个授权认证处理序列；

图 37 示出一个用来生成完整性检测值（ICV）的信息授权认证代码（MAC）的示例，检测值（ICV）被涉及本发明的数据处理系统使用；

图 38 示出涉及本发明的数据处理系统中的完整性检测值（ICV）的储存的一方案；

图 39 示出涉及本发明的数据处理系统中的信息授权认证代码（MAC）的存储的序列页的格式；

图 40 示出涉及本发明的数据处理系统中的完整性检测值（ICV）的存储的组页面的格式；

图 41 示出涉及本发明的数据处理系统中的完整性检测值（ICV）的检测的流程图；

图 42 示出生成可扩充的 MAC 的值的过程和存储启用密钥块扩充的 MAC 的值在涉及本发明的数据处理系统中的过程；

图 43 示出通过利用涉及本发明的数据处理系统中的使能密钥块（EKB）获得一个内容密钥的过程的一方案；

图 44 示出被用涉及本发明的数据处理系统用到的装置密钥块（DKB）

的结构；

图 45 示出示例一个涉及本发明的数据处理系统中储存使能密钥块（EKB）和装置密钥块（DKB）的结构安排；

图 46 示出通过利用涉及本发明的数据处理系统中的使能密钥块（EKB）和装置密钥块（DKB）获得一个内容密钥的处理过程的一个方案。

具体实施方式

数据处理系统概要

图 1 图示了一个可应用本发明的数据处理系统的内容数据发布系统的一个示例。一个内容数据发布装置 10 传送各种加密的数据（包括内容数据或内容密钥、实施授权认证的特定的密钥等类似的数据）到数据处理装置 20。然后，数据处理装置 20 在加密的条件下开始解码接收到的内容数据或内容密钥；然后在最终重新生成图片数据或音频数据或执行各种程序之前获得这些内容数据或内容密钥。在内容数据发布装置 10 和数据处理装置 20 之间交换数据通过网络服务线路（如互联网服务线路）或可发布的记录介质（如 DVD、CD 或其他方式）来执行。

数据处理装置 20 在数据储存装置（30）(如带有闪存等类似的存储装置的储存卡等)储存多个数据。数据储存装置 30 包含带有加密功能的存储装置，一个具体的例子时，存储装置包含一个“存储棒 Memory Stick”（Memory Stick 是 sony 公司的注册商标）。无论何时当从数据处理装置 20 向数据储存装置 30 转移数据或反向转移使，一个相互授权认证过程和一个数据加密过程被执行，以阻止未经授权的内容数据和密钥的再生被允许。

也可能在数据处理装置 20 中的各个装置之间转移内容数据，通过在部件装置之间执行一个相互授权认证过程和一个数据加密过程。

内容数据发布装置 10 包含一条互联网服务线路 11、一个卫星广播站 12、一条电话线路 13、诸如 DVD,CD 等类似的记录介质。另一方面，数据处理装置（20）也可能是个人计算机（21）、PD（便携式装置）22、便携式电子装置 23（象便携式电话、PDA 个人数字助理等类似的）、数字数据再生装置 25（利用记录和再生装置如 DVD、CD 等）、游戏终端单元 24、存储卡（如“存储棒” （Memory Stick）（Memory Stick 是 sony 公司的注册商标）等）。数据处理装置 20 的单个的装置分别可以经由通讯装置（如网络服务线路）获取从内容数据发布发布装置 10 的内容数据，

或者可以从其他的数据处理装置获取，或者从以上提到的数据储存装置 30 获取。

图 2 示意性地图示了转移内容数据的过程的典型示例。图 2 所示的系统例示了一个在个人计算机 100、再生装置 200 和存储装置 300 之间转移内容数据的典型示例。个人计算机 100 包含一个硬盘（HD）和一个内在地载入外部存储媒体（例如 CD、DVD）的机制。

个人计算机 100 被接入如互联网和公共电话线路等网络服务线路。例如，个人计算机 100 可以通过网络服务线路从被服务提供商（图中未示）所有的主机接收各种数据（包括音频数据、图片数据和程序等），服务提供商通过 EMD（电子音乐发布）提供数据服务；随后，按需求解码接收的数据并递送松据到再生装置 25。当接收内容数据时，个人计算机 100 按服务提供商拥有的主机的要求执行一个授权认证过程和一个付费处理过程。而且，个人计算机 100 输出从 CD 或 DVD 接收到的各种数据到数据再生装置 200。

存储装置 300 可以被装载到数据再生装置 200 和卸载。以上提到的“存储棒”（sony 公司的产品和注册商标）自己作为一个存储装置 300，包含一个如闪存的可重写的半导体存储器。

如图 2 所示，无论何时在上述的个人计算机 100、数据再生装置 200 和存储装置 300 中转移数据、再生如音频数据，图片数据等数据、记录数据和再生数据时，一个相互授权认证过程被在数据转移装置之间执行，以阻止内容数据被未经授权的装置转移，这一过程会在稍后描述。而且，无论何时在个人计算机 100 和再生装置之间或在数据处理装置和诸如存储卡等存储装置之间转移数据或通过网络服务线路发布内容数据或通过各种存储介质发布数据时，内容数据的安全可以通过加密内容数据的到保证。

[构建一个密钥发布系统的树状结构]

现在参照图 3，以下阐述一个分层密钥树状结构，它使得本系统能够向正当的授权装置发布加密密钥以加密以上提到的内容数据，例如，这些各种各样的加密密钥包括用来加密内容数据的内容数据密钥和用来正确地加密内容数据的内容数据密钥加密密钥。

参照图 3 的底部所示，标号 0 到 15 分别表示用以够成以上所述的用以再生或执行相关内容数据的数据处理装置 20 的各个装置，例如，这些装置独自地构成一个内容数据（音乐数据）再生装置。用另一句话说，分

层树状结构的每一个枝叶与相应内容数据再生装置相对应。

或者在生产阶段、或者在从生产工厂交货的时候、或者在生产过程或从工厂交货后的某个时候，从 0 到 15 的每个装置存储一个从自身的枝叶到相应的根的为这一节点分配的节点密钥和包含有分层树状结构中各个枝叶的枝叶密钥的一个密钥集合（如图 3 所示）在一个预定的存储器中。在图 3 的底部所示的标数 K0000 到 K1111 分别表示为装置 0 到 15 分配的枝叶密钥。也已做出这样的安排，底部的第二个节点的从 KR（根密钥）到 K111 的密钥相应的构成节点密钥。

例如，在图 3 所示的树状结构中，提供给装置 0 以枝叶密钥 K0000 和节点密钥 K000，K00，K0，以及 KR；提供给装置 5 以密钥 K0101，K010，K01，K0，以及 KR；提供给装置 15 以密钥 K1111，K111，K11，K1，以及 KR。图 3 所示的装置包含有从 0 到 15 的 16 个装置，因而，树状结构包含有在双向对称平衡的 4 个级别的单元。然而，树状结构也可以有更多的装置，也可以在各个不同的部分有不同的级别数量。

图 3 所示的为树状结构提供的每个装置包含有一个能够利用各种存储装置（包含各种记录介质，如利用内建的或者可卸载的闪存的存储卡、DVD、CD 或 MD 等）的装置。另外，许多服务应用程序也可内建提供。基于联合存在的各种装置和服务应用程序，采用了用以发布内容数据和加密密钥的分层树状结构以应用本发明。

在各种装置和服务应用程序联合存在的系统中，也已做出这样的安排，图 3 所示的以点划线园圈起来的部分的装置 0、1、2 和 3 被安装为一个使用同一记录介质的群组。例如，经过加密处理过程之后，提供商交付加密的公用内容数据或者为以点划线园圈起来的装置所公用的内容数据密钥。在另一个例子中，每一装置输出与内容数据使用付费相关的加密数据到提供商或金融机构。另一方面，诸如提供商或指定的结算账户的金融机构（通常从单个装置接收数据或向它们发送数据）执行一个进程以发送整块的相关数据给装置 0、1、2 和 3（如图 3 所示的以点划线园圈起来的作为一个单个群组的部分）。实际上，在图 3 所示的树状结构中有多个类似群组，此类通常向诸如数据提供商或机融机构等单个装置发送或接收数据的相关的部分自己作为一个发布信息数据的装置。

以上提到的节点密钥和枝叶密钥可能整个地被一个单个的密钥控制中心所控制。相应地，它也允许在提供商或指定的结算账户的金融机构方的，

通常和单个的群组交换大量数据的信息数据发布装置能够控制节点密钥和枝叶密钥。在节点密钥或枝叶密钥泄漏或失窃的情形下，一个升级的进程就被密钥控制中心、相关的供应商者相关的金融机构所执行。

就像图 3 所清楚表现的，在这一独到的树状结构中，以上提到的包含在一个群组中的三个装置 0、1 和 2 分别被赋予公共节点密钥 K000，K00 和 KR。例如，通过利用节点密钥沟通结构，就可能为装置 0、1 和 2 唯一地提供公共内容密钥。例如，通过将公共持有的节点密钥 K00 自己安装为一个内容密钥，就可能安装这样一个对装置 0、1 和 2 唯一的内容密钥，而不用交付新的密钥。而且，通过经由网络服务线路或经由储存在记录介质中发布一个包含有被节点密钥 K00 加密的新的内容密钥（Kcon）的数值编码（K00，Kcon）给装置 0、1 和 2（利用为单个装置所持有的公共密钥 K00），就唯一使得装置 0、1、2 和 3 在请求内容数据密钥（Kcon）之前可以解码加密的加密的码值编码（K00，Kcon）。编码(Ka，Kb)表示了数据的 K 数（为 Ka 所加密）。

而且，在装置 3 持有的密钥 K0011，K001，K00，K0 和 KR 最终被骇客的非法分析所泻漏的情况下，为了保护包含有装置 0、1、2 和 3 的群组所接收和发送的数据，因此就非常必要使装置 3 从群组系统中被拆卸。为实现这点，就非常必要使节点密钥 K0011，K001，K00，K0 和 KR 相应为新的密钥 K(t)0011，K(t)001，K(t)00，K(t)0 和 K(t)R 所替换，而且也必要知会装置 0、1 和 2 更新的密钥。字符 K(t)aaa 表示新的密钥更新于先前密钥 Kaaa 的第（t）代。

其次，发布更新密钥的进程描述如下：对密钥的更新只通过经由网络服务线路交付一个如图 4 中 A 所示的包含有一个称之为使能密钥块(EKB)的数据块的表格或经由储存在记录介质中给装置 0、1 和 2 而执行。EKB 包含了发布升级密钥给和如图 3 所示的构成树状结构的各个枝叶相应的装置。以上的 EKB 也可称之为密钥更新块（KRB）。

如图 4 中 A 所示，以上提到的 EKB 包含有这样一个数据块，它有一个数据结构，其中只有装置请求的更新节点密钥被更新。图 4 中 A 所示的 EKB 表示了这样一个数据块，它共享图 3 所示的密钥树状结构的一部分，发布升级装置 0、1 和 2 中的第“t”代节点密钥。如图 3 清楚表明的，装置 0 和 1 分别请求更新节点密钥的 K(t)00、K(t)0 和 K(t)R，而装置 2 请求更新节点密钥的 K(t)001、K(t)00、K(t)0 和 K(t)R。

如图 4 中 A 所示，以上提到的 EKB 包含多个加密密钥。底层的加密密钥对应着 Enc（K0010，K(t)001），对应着为装置 2 所拥有的以上提到的枝叶密钥 K0010 所加密的升级节点密钥 K(t)001。通过应用自身的枝叶密钥，装置 2 也可以解码加密的密钥从而获得经过升级节点密钥 K(t)001。进一步，通过使用升级的节点密钥 K(t)001，装置 2 也可以解码图 4 中 A 所示的第二底层的加密的密钥 Enc（K(t)001 和 K(t)00），从而获得经过升级的节点密钥 K(t)00。通过这种方式，装置 2 顺次解码了图 4 中 A 所示的第二最上层的加密的密钥 Enc（K(t)00 和 K(t)0）。从而也解码了图 4 中 A 所示的最上层的经过升级的节点密钥 K(t)0 和加密的密钥 Enc（K(t)0 和 K(t)），因而获得经过升级的节点密钥 K(t)R。另一方面，在装置 K0000 和装置 K0001 方面，节点密钥 K000 不包括在更新的对象中，因而只有 K(t)00、K(t)0 和 K(t)R 被请求为更新的节点密钥。在另一方面，装置 K0000 和装置 K0001 分别解码图 4 中 A 所示的第三最上层的加密的密钥 Enc（K000 和 K(t)00），从而获得节点密钥 K(t)00。

装置 K0000 和装置 K0001 更进一步地解码图 4 中 A 所示的第二层的加密的密钥 Enc（K(t)0 和 K(t)0），从而分别获取经过升级的节点密钥 K(t)0。装置 K0000 和装置 K0001 更进一步地解码图 4 中 A 所示的作上层的加密的密钥 Enc（K(t)0 和 K(t)R），从而分别获取经过升级的节点密钥 K(t)R。通过这种方式，就可能使得装置 0、1 和 2 分别获取经过升级的节点密钥（包括 K(t)001、K(t)00、K(t)0 和 K(t)R）。图 4 中 A 所示的索引分别表示了用作解码密钥的节点密钥和枝叶密钥的绝对地址。

并不要求更新图 3 所示的密钥树状结构的顶层相应的节点密钥 K(t)0 和 K(t)R），加入只要更新节点密钥 K00，通过施加图 4 中 B 所示的 EKB，就可以发布经过升级的节点密钥 K(t)00 到装置 0、1 和 2。

图 4 中 B 所示的 EKB 可以应用到新的被特定的群组所公共拥有的内容数据被发布的情形，举一个具体的例子，假定图 3 所示的以点划线园圈起来的群组的装置 0、1、2 和 3 分别使用某种记录介质，并且分别不同的新的内容数据密钥 K(t)。在这种情形下，利用从对装置 0、1、2 和 3 同样的节点密钥 K00 升级来的节点密钥 K(t)00，通过加密一个和如图 4 中 B 所示的 EKB 相连的经过升级的公共内容数据密钥 K(t)con，一个数据 Enc（K(t)00 和 K(t)con）就被产生。作为这一发布过程的结果，这样一个内容数据密钥就可以作为数据发布，这一数据不能为包含装置 4 的群组中的

其他装置所解码。

也就是说，通过使得装置 0、1 和 2 能够通过应用经由利用 EKB 产生的 K(t)00 解码以上提到的加密字符，就可能获得在相应的“t”瞬间获得内容密钥 K(t)con。

[发布对 EKB 有用的内容密钥]

图 5 给出了装置 0（已经接收到通过应用 K(t)00 从一个升级的公共内容密钥 K(t)con 加密的数据 Enc（K(t)00 和 K(t)con））执行的一个进程作为产生在相应的“t”时刻生成内容密钥 K(t)con 和分别经由记录介质接收到的图 4 中 B 所示的 EKB 的进程的例子。具体的说，它举例说明了通过应用 EKB 加密的信息数据已经被转换为内用数据密钥 K(t)con 的情形。

如图 5 所示，利用储存在记录介质的相应的“t”代的 EKB 和一个先前储存在装置 0 自己上的节点密钥 K000，通过执行一个于以上描述同样的 EKB 进程，装置 0 生成一个节点密钥 K(t)00。而且，通过施加解码的经过升级的节点密钥 K(t)00，装置 0 通过施加该装置 0 自己唯一拥有的枝叶密钥 K0000 加密经过升级的内容密钥 K(t)con，然后，为了以后利用经过升级的内容密钥 K(t)con，装置 0 储存经过加密的升级过的内容密钥 K(t)con 在自身上。

[EKB 的格式]

图 6 例示了 EKB 的格式。相应的识别成分的版本（601）表示了 EKB 的版本。版本包含了这样一个功能——指明相应的标识最新的 EKB 的功能和内容数据之间的关系。深度标示相应的作为 EKB 发布的目标的装置的分层密钥树的层树。数据指针（603）代表一个表示 EKB 中数据块的位置的指针。标签指针标示标签部分的位置。签名指针标示签名位置。

数据部分（606）储存有包含等待升级的加密节点密钥的数据。例如，数据部分（606）储存和图 5 所示的经过升级的节点密钥相关的加密密钥。

标签指针（607）标示储存在数据部分（606）的经过加密的节点密钥和枝叶密钥之间的位置关系。接下来，参照图 7，提供标签的规则描述如下：图 7 例示了在先前参照图 4 中 A 描述为数据的 EKB 的交付。这一数据通过表格对应图 7 中 b 所示。加密密钥包含的顶节点地址被假定为顶节点地址。在本例中，由于一个经过升级的根密钥的密钥 K(t)R 包含在加密密钥中，顶节点地址就变成 KR。在本例中，在顶层的数据 Enc（K(t)00 和 K(t)con）在图 7 中 a 所示的分层密钥树的位置中。相应 Enc（K(t)00 和

K(t)con）的下一个数据，处在一个相对低些的位置，在分层密钥树中表示为在先前数据的左面。当上面的数据有时，标签的值是 0，当上面的数据没有时，标签的值是 1。标签被假定为左标签和右标签。由于左面的数据是做上面的数据 Enc（K(t)001 和 K(t)00），左标签就变成 0。而且，由于在最上层的数据的左面没有数据，有标签就变成 1。通过这种方式，所有的数据都被提供一个标签，从而形成一个如图 7 中 c 所示的数据阵列和标签阵列。

以上提到的标签被提供以指定分层密钥树状结构的数据 Enc（Kxxx，Kyyy）的实际位置。储存在数据部分的密钥数据 Enc（Kxxx，Kyyy）表示对应多个加密的密钥数据。因而，也做出安排使得加密密钥的实际位置可以通过应用标签所表明。另外，在利用以上所述的标签的情形下，通过以上参照图 4 所述的应用节点索引兼容加密的数据，也可能构建以下所示的数据结构。

0： Enc（K(t)0，K(t)root）

00： Enc（K(t)00，K(t)0）

000：Enc（K(t)000，K(t)00）

尽管如此，当通过涉及以上的节点索引应用以上的数据结构时，冗长的数据的体积就会增加，因而，利用这样一个冗长的数据通过网络服务线路发布并不理想。另一方面，通过利用以上提到的标签作为标示密钥的实际位置的方式，就可能通过应用少量的数据标示相关密钥的实际位置。

参照图 6，EKB 的格式在下面作进一步的描述。签名包含有被发行 EKB 的控制中心、内容数据提供商或指定的金融机构等所执行的电子签名。接收 EKB 的装置通过签名验证接收到的 EKB 确实对应的有权发布的经过验证的正当的 EKB 的发行商。

[通过应用 EKB 发布内容密钥和内容数据]

在以上所述的本发明的实践形态中，一个与 EKB 一道发布内容数据的例子已被详尽描述。以下的描述进一步参照这些：一个经由用加密密钥加密的发布内容数据的结构安排；一个施加内容密钥加密密钥加密的内容密钥；一个以 EKB 加密的内容密钥加密密钥。

图 8 标明了单个数据的结构。在图 8 所示的结构中，Enc（Kcon，内容）801 对应一个包含被内容密钥（Kcon）加密的内容数据的数据。Enc（KEK，Kcon）802 对应一个包含有施加内容密钥加密密钥（Key Encryption

Key，KEK）的内容密钥（Kcon）的数据。Enc（KEB，KEK）803 对应一个包含以 EKB 加密的内容密钥加密密钥（KEK）的数据。

在本例中，内容密钥加密密钥（KEK）可能包含如图 3 所示的节点密钥（K000，K00）、或者根密钥（KR）自身，它也可能包含一个被根密钥（KR）加密的密钥。

图 8 在（b）中标明了这样一个示例，多个数据被记录在记录介质中，在其中这些内容数据分别利用一个相同的 Enc（EKB，KEK）（805）。在这种结构中，也可以添加数据一个指向 Enc（KEB，KEK）的表示联接，而不用为每个数据添加同样的 Enc（KEB，KEK）。

图 9 示例了这样一个结构安排，内容密钥加密密钥（KEK）通过更新图 3 所示的节点密钥 K00 转换为一个升级的节点密钥 K(t)00。在这种情形下，假定在图 3 所示的点划线圆圈起来的一组中的装置 3 由于泄漏密钥被废除，剩下的装置 0、1 和 2 可以如图 9（a）所示通过使得它们可以接收 EKB，经由发布而分别获取内容数据；获取一个包含一个通过施加如 9（b）所示的内容密钥加密密钥（KEK=K(t)00）加密的内容密钥的数据；获取一个包含有通过施加图 9（c）所示的内容密钥所加密的内容数据的数据。

装置 0 的序列的解码进程如图 9 右面所示。首先，装置 0 通过利用自己的枝叶密钥 K000 从接收到的 EKB 中获取一个内容密钥加密密钥（KEK=K(t)00）。随后，装置 0 通过利用获取的加密密钥 K(t)O0 的解码进程获取一个内容密钥（Kcon）。随后，装置 0 通过施加内容密钥（Kcon）进一步解码内容数据。在完成这些进程之后，装置 0 就可以利用解码的数据。装置 1 和装置 2 也可以由相互的不同的进程通过处理 EKB 而获取内容密钥加密密钥（KEK=K(t)00），从而使它们能够利用解码的内容数据。

在另一方面，即使接收到和 EKB 相关的数据，图 3 中属于另一组的装置 4、5、6…不能通过施加自身的枝叶密钥和节点密钥来获取内容密钥加密密钥（KEK=K(t)00）。相似的，以上提到的废除的装置 3 不能施加自身的枝叶密钥和节点密钥来获取内容密钥加密密钥（KEK=K(t)00）。更具体地说，只有那些得到正当授权认证的装置才能解码和利用内容数据。

在通过利用 EKB 来执行发布以上的内容密钥时，只有得到授权的人才唯一可能安全正当地通过减少数据体积的方式解码和发布加密的内容数据。

以上提到的 EKB、内容密钥和加密的内容数据可以经由网络服务线路安全发布。在本例中，也可以通过储存在 DVD、CD 等记录介质中来向各个用户提供以上的 EKB、内容密钥和加密的内容数据。在本例中，通过利用在解码储存在记录介质中的加密内容数据之前经由解码储存在同一储存介质中 EKB 生成的内容密钥，就可能实现发布只能唯一为施加经过认证的正当的用户拥有的枝叶密钥和节点密钥才能利用的经过加密的内容数据的发布。换句话说，可能在一个简单的系统结构上实现一个以限制用户方的有效装置的内容数据发布系统。

图 10 例示了一个储存以上提到的 EBK 和加密的内容数据联合出储存的记录介质的结构。在图 10 所示的例中，多个从 C1 到 C4 的数据以及包含有和相应的各个内容数据对应的 EKB 的数据联合储存在某个记录介质。另外，另一个和版本 M 相应的 EKB 也被储存在这一记录介质中。例如，EKB-1 用以生成一个内容数据 1 中加密的内容密钥 Kcon-1。类似的，EKB-2 用以生成一个内容数据 2 中加密的内容密钥 Kcon-2。在本例中，一个和版本 M 相应的 EKB-2 也被储存在某一记录介质中。其余的内容数据 C3 和 C4 分别对应一个 EKB-M，因而通过解码 EKB-M，就可能获取和内容数据 C3 和 C4 对应的内容密钥。另一方面，由于以上提到的 EKB-1 和 EKB-2 不储存在记录碟中，因而就有必要通过利用如网络服务线路或记录介质之类的新的发布方式获取用以解码的各个内容密钥。

[分层树状密钥结构的编目分类]

以上的描述已经参照了多种为图 3 所示的分层树状密钥结构的提供密钥（包括根密钥、节点密钥、枝叶密钥、内容密钥、认证密钥、ICV 生成密钥等）的系统，也已参考了通过加密联合 EKB 一起加密程序代码和数据以发布程序代码和数据的系统。

随后，通过划分归类定义节点密钥和归入目录的装置的分层树状密钥结构，用以有效更新以上提到的密钥和有效地发布加密的密钥和数据的结构安排描述如下：

图 11 例示了一个编目分类的分层树状密钥结构。在图 11 中，一个根密钥 Kroot 1101 被安装在分层树状密钥结构的最顶层。一个节点密钥 1102 被安装在中间层，而一个枝叶密钥 1103 被安装在底层。每一单元装置包含有从枝叶密钥到根密钥的自己的枝叶密钥以及一系列的节点密钥和根密钥。

例如，对应从最顶层第 M 层的节点被安装上为目录节点 1104，明确地说，对应第 M 层的每个节点被确定为特定目录的装置设置节点。那些在 M+1 层以下的节点和枝叶距顶节点较 M 层的节点低一层，分别构成节点和包含在相应的目录的装置的相关的枝叶。

例如，一个“存储棒”（“memory stick”是 sony 公司的注册商标）的被设定在图 11 所示的对应第 M 层的一个节点 1105。相应地，在 M 层以下的节点和枝叶被确定为只为包含含有“存储棒”的各种装置的目录所使用的节点和枝叶。用另外一句话说，在 1105 节点以下的节点和枝叶被定义为定义和在“存储棒”目录之中的装置相关的节点和枝叶的集合。

而且，也可以设置在第 M 层以下的相应的几个层中的一个为子目录节点 1106。例如，如图 11 所示，一个称之为只再生的装置的节点被设置在一个低于与以上提到的目录“存储棒” 相应的节点 1105 两级的节点，作为一个包含在利用“存储棒”的装置的目录的一个子目录节点。进一步，一个和包含在只再生装置目录下的有音乐再生功能的电话相应的节点 1107 被设置在节点 1106（对应只再生装置，其本身是一个子目录节点）之下。更进一步地，也可以在节点 1107 下包含有音乐再生功能的目录中设置一个 PHS（个人手持系统）节点 1108 和一个手持电话节点 1109。

进一步，不只是装置的类型，也可以基于为特定的生产商、内容数据提供商和特定的金融机构所单独控制的节点的目录和子目录，用另一句话说，就是基于一个处理单元、一个控制单元，或者基于提供的服务，或者某一可选的单元（这些单元因而对应某一“实体”）。例如，当某一目录节点被设置为顶为某一游戏机生产商销售的游戏机 XYZ 所唯一所有的节点时，就可能通过储存节点密钥和顶层以下的相应的层的枝叶节点来销售这一游戏机 XYZ。从而，发布加密的内容数据或者发布更新各种加密密钥就可以通过生成包含这些节点密钥和枝叶密钥的 EKB 来执行。更具体的说，只有可以应用到定点节点以下的装置的数据可以被发布。

如上所需的，通过建立这样一个系统，其中与某一特定的目录或子目录相关的节点包含在被定义为顶节点的顶点节点以下的节点，就可能使得生产商和内容数据提供商可以控制某一顶节点，以独立地生成包含顶节点的目录或子目录的 EKB，以发布给属于顶节点以下的节点的装置，因而使得可能不更新顶节点而更新相关的密钥，而且不用影响整个的属于本节点以下其他目录的装置。

[应用简化（EKB）的密钥发布系统]

以以上描述的图 3 所示的树状密钥结构为例，例如，当付送一个内容密钥到预定的装置（枝叶）时，以装置拥有的枝叶密钥和节点密钥作为密钥发布的目标，一个可解码的 EKB 被生成以付送到目标。例如，如图 12 所示的树状密钥结构中，当传送一个内容密钥给装置 a，g 和 j 以合成枝叶时，一个可以为个别的装置 a，g 和 j 的节点所解码的 EKB 被生成以用于发布。

例如，这样一个情形假定，内容密钥 K(t)con 通过施加升级过的根密钥 K(t)root 加密，然后与 EKB 联合在一起发布。在这种情形下，使用图 12(b) 所示的枝叶密钥和节点密钥，执行一个 EKB 进程以请求内容密钥 K(t)root，然后通过执行一个施加获取的经过升级过的根密钥 K(t)root 解码内容密钥 K(t)con 的进程，获取内容密钥。

图 13 标示了以上例子的 EKB 的结构。图 13 所示的 EKB 和前面参照图 6 描述的 EKB 的格式一样。图 13 所示的 EKB 包括加密密钥数据和相应的标签。就像前面参照图 7 所叙的，加入在左方或右方有任何数据，标签指示为 0，否则加入两个方向都没有数据的话，标签指示为 0。

在接收到 EKB 之后，基于加密 EKB 的密钥和相应的标签，装置在请求更新上一层的节点的密钥之前顺次执行一个进程以解码加密密钥。如图 13 所示，从根到枝叶的深度的数越大，包含在 EKB 的数据的体积就越大。具体地说，由于深度相关装置（枝叶）的数量而增长，因而，当更多的装置成为密钥发布的目标时，EKB 中数据的体积也随之增加。

一个可以减少 EKB 的数据的体积的系统结构被描述如下，图 14 示例了这样一个与密钥发布装置相应的简化了的 EKB 的结构。

在图 13 的情形中，假定了这样一种情况，内容密钥被传送到装置 a，g 和 j 以组成枝叶。如图 14 中(a)所示，这样一个只有密钥发布装置所组成的树状密钥结构就被构建成了。新的树状密钥结构可能是从 Kroot 到 Kj 只含有单个的分支而没有其他的分支。通过提供一个唯一地指向从 Kroot 到 Ka 和 Kj 之间的 K0 的分支指针，就形成了一个如图 14 中(a)包含有两个分枝的树状密钥结构。

如图 14 中(a)所示，一个只有一个节点 K0 的简化的树状密钥结构就被生成。基于这个简化的树状密钥结构，一个简化的 EKB 就被生成以用于发布升级的密钥。图 14 中(a)表示了这样一个通过删除不必要的节点（通

过选择包含双分支类型的树状结构构成 EKB 的路径作为一个可解码的底层的终端节点或枝叶）而重新构建的分层树状密钥结构。这样一个用来发布经过升级的密钥的 EKB 仅仅基于这样一个相应于重构的分层树状密钥结构的节点和枝叶的密钥而构建。

先前的参照图 13 描述的 EKB 储存所有的从各个枝叶 a，g 和 j 到 Kroot 的经过加密的密钥的数据。而以上提到的简化的 EKB 储存经过解码的用来构成简化树状密钥结构的节点的数据。如图 14 中(b)所示，以上提到的标签包含 3 个数位，其中第一和第二数位分别和图 13 所示的例子表示相同的含义，当左或右右有任何数据时，指定为 0；当左右都为数据时，指定为 1。第三个数位指示是否有一个加密密钥储存在 EKB 中，当任何数据储存其中时，第三数位指示为 1，而当没任何数据时，它指示为 0。

对照图 13 所示的结构，这个图 14 中(b)所示的经由数据通讯网络服务线路或储存有这一数据的记录介质发布给装置的 EKB 的体积较先前的 EKB 急剧减少。如图 14 所示，在接收到 EKB 的情况下，通过唯一地解码相应后续的标签的第三数位储存为二近制 1 的部分的数据，个体的装置被允许解码预定的加密密钥。例如，装置 a 通过一个密钥 Ka 解码一个加密数据 Enc(Ka，K(t)0)，然后请求节点密钥 K(t)0。随后，装置 a 通过应用节点密钥 K(t)0 解码加密数据 Enc(K(t)0，K(t)root)，从而请求一个解码的数据 K(t)root。另一个装置 j 通过一个枝叶密钥 Kj 解码一个加密数据 Enc(Kj，K(t)root)，从而请求一个解码数据 K(t)root。

如上面所述，通过最初形成一个简化的新的树状密钥结构，它通过唯一利用构建密钥树状结构的枝叶密钥和节点密钥，只包含相应的作为根据 EKB 的世代的发布对象的装置，从而可能生成一个包含较小数据体积的 EKB，从而使得可能有效地发布 EKB 的数据。

以上提到的简化分层树状密钥结构在控制 EKB 结构的系统中可以非常有效地被操作，以下描述它的每一个实体（“entity”）。术语“entity”代表一个包含多个选自于用来构建用来发布相关的密钥的树状密钥结构的节点和枝叶的集合。这一实体可能是和相关的种类的装置一起提供的集合。另外，这一实体作为多个形态的集合而建立，这些形态包括如相关装置的装置的制造商、内容提供商和指定的结算账户的金融机构等控制单元，各个再生的处理单元、控制单元、或者服务提供单元等相互公共存在的单元。每一实体包含有一个可以划分到同一目录的装置的集合。例如，

有可能在属于特定的选定的实体中的装置中生成和发布简化的、可解码的EKB，通过重建经过多个实体的顶节点（子路径）简化的以上提到的树状密钥结构而生成一个 EKB 的方式。控制实体的系统的每一单元将在以后叙述。

也可能储存 EKB 在如光盘、DVD 或 CD 等类似的数据记录介质中。例如，有可能构建这样一个系统，为每一装置提供这样一个数据记录介质，它储存有 EKB（包含有一个由以上提到的加密数据密钥的数据部分和用作标示以上包含有加密的密钥数据的分层树状密钥结构的位置的标签部分），而且还储存有如被以上描述的升级过的节点密钥加密的内容数据信息数据。有可能使每一个装置顺次分离出包含在 EKB 中的经过加密的密钥数据；而且，也可能使得每一装置在请求内容数据之前请求特定的用以解码内容数据的密钥。也允许通过如互联网服务等网络服务线路发布EKB。

[在有加密功能的储存介质和数据处理装置之间交换数据的处理过程]

随后，参照在有加密功能的储存介质（如存储卡，典型的如“存储棒”——一种产品及 sony 公司的注册商标）和数据处理装置之间交换数据的处理过程，以下描述一个利用一个经由 EKB 发布的特定的加密密钥应用以上描述的分层密钥树状结构的一个处理系统。

图 15 给出了一个说明数据再生装置和储存如存储卡等有数据加密功能的存储装置（它们分别能够相互交换数据）的详细结构的原理框架图。

如图 15 所示，存储装置 300 包含以下各个方面：一个主模块 31、一个通讯接口单元 32、一个控制模块 33、一个闪存 34、一个闪存控制模块 35。详细的各模块的描述如下：

[控制模块 33]

如图 15 所示，控制模块 33 包含以下各个方面：一个随机数生成单元 50、一个储存单元 51、一个密钥生成/算法单元 52、一个相互授权认证单元 53、一个加密/解码单元 54 以及一个控制单元 55。控制模块 33 包含有一个整合的唯一用作某一单个芯片或类似的电路。而且，控制模块 33 包含一个多层结构，它包含一个借助由铝层制作成的样本层之间的内在的储存单元。而且，控制模块 33 还含一个窄幅的操作电压和一个窄带的操作频率，因而进而有了防窜改的能力以防止由外部原因的非法阅读数据。在接到生成随机数的命令的情况下，随机数生成单元 50 生成一个 64 位（也

就是 8 字节）的随机数。

储存单元 51 包含一个非易变的存储器（例如，由 EEPROM（可电擦写可编程只读存储器））构成）。例如，其中储存有各种数据，包括为授权认证所需要的数据。图 16 是特地用于说明储存在储存单元 51 中的数据的。如图 16 所示，储存单元 51 储存了授权认证数据 IK0 到 IK31、装置标示数据 Idm 以及存储器储存密钥数据 Kstm。

授权认证数据 IK0 到 IK31 各个用于使存储装置 300 能与相应的再生装置 200 共同认证相关数据。如以后要讲到的，无论何时它们之间执行认证操作时，IK0 到 IK31 中的一个被随机选定。也已做出这样的安排，无论以上的认证密钥数据 K0 到 IK31 还是存储器储存的密钥数据 Kstm 都不能被除开存储装置 300 以外的装置读出。如以后要讲到的，当执行相互授权认证操作时，装置标示数据 Idm 被读出以付送到相应的再生装置 200。如以后要讲到的，当储存一个用来加密闪存 34 中的内容数据的经过加密的密钥数据 CK 时，存储器储存的密钥数据 Kstm 被利用到。

通过执行各种算法操作（如 MAC（信息认证码）），以上的密钥生成/算法单元 52 生成密钥数据。为了实施 MAC 处理操作，例如，FIPSPUB 46-2 描述的 DES（数据加密标准）用作“块加密算法”。以上的 MAC 处理操作与单向 Hash 函数一样，压缩一个长度任意的数据到一个有固定长度的数据，其中函数的值依赖于私钥。

在从再生装置 200 向闪存 34 写音频数据之前，以上提到的相互授权认证单元 53 和相应的再生装置 200 执行一个授权认证处理。类似的，在从闪存 34 读出数据付送到再生装置 200 之前，相互授权认证单元 53 和再生装置 200 执行一个授权认证处理。而且，相互授权认证单元 53 在通过施加储存在储存单元 51 中的数据执行相互授权认时，执行以上提到的 MAC 处理操作。

基于以上提到的如 DES、IDEA 或 MISTY 等“块加密算法”，加密/解码单元 54 执行一个加密操作。加密/解码单元 54 采用以下方式：FIPSPUB 81 （DES 操作模式）所规定的 ECB（电子码书本）模式和 CBC （加密块链）模式。而且，加密/解码单元 54 通过施加以上描述的 ECB 模式和 CBC 模式而基于如 DES、IDEA 和 MISTY 等块解码算法执行一个解码操作。在通过施加 ECB 和 CBC 模式进行块加密和解码的处理过程中，加密/解码单元 54 通过施加一个特定的密钥数据而加密和解码特定的数据。以上提

到的控制单元 55 整体地控制以上的随机数生成单元 50、储存单元 51、密钥生成/算法单元 52、相互授权认证单元 53 和加密/解码单元 54。

[闪存 34]

闪存 34 包含一个有能力记录 32 兆字节的存储器。只有当以上提到的相互授权认证单元 53 验证再生装置 200 和存储装置 300 已经通过在它们之间执行的相互授权认证时，从再生装置 200 发送的诸如音频数据和图片数据等各种数据才被写入闪存 34。同样的，有当以上提到的相互授权认证单元 53 验证再生装置 200 和存储装置 300 已经通过在它们之间执行的相互授权认证时，音频数据和图片数据才被正当地从存储装置 300 读出以付送到相应的再生装置 200。

随后，可储存在闪存 34 中的数据和相关的格式描述如下。如图 17 所示，闪存 34 储存再生控制文件和多个磁道数据（可再生数据）文件。再生控制文件包含控制磁道数据文件再生的数据。每一个磁道数据文件包含相应的磁道数据（音频数据）。在应用本发明的实例的情形下，每个磁道数据蕴涵相对一个音乐曲目的音频数据。以下的描述参照储存音频数据在闪存 34 中的情形。

图 18 标示了再生控制文件的组成。图 19 标示了一个音乐曲目的 ATRAC-3 数据文件的组成。再生控制文件包含 16K 字节的固定长度。ATRAC-3 数据文件包含一个引导属性标题和跟着的真正加密的音乐数据。引导属性标题也包含 16K 字节的固定长度，有和再生控制文件类似的组成。

再生控制文件包含以下各个组份：一个标题，一个叫做 NM2-S 的 2 个子节的编码储存器，以音乐曲目顺序的回放表格，以及一个整体的加进储存卡的附加的数据 INF-S。数据文件的导属性标题包含一个标题，叫作 NM1 的 1 字节的编码音乐曲目，叫作 NM2 的 2 字节的编码音乐曲目，磁道数据 TRKINF（例如，包含磁道密钥数据），分段数据数据 PRINF，以及加到磁道的附加数据 INF。标题包含如分段的总数，属性的名称，附加数据的大小等数据。

接着属性标题的是相应于 ATRAC-3 数据的音乐数据。音乐数据划为 16K 字节一个部分。标题被加入到每块数据的开头。标题包含用于解码加密数据的初始值。只有包括 ATRAC-3 数据文件中的音乐数据等数据被进行加密操作，而再生控制文件和标题的数据不进行加密操作。

图 20 标示了以上提到的有一个簇（一块=16K 字节）的再生控制文件 PBLIST 的详细的数据组成。图 20 中 A 所示的标题包含 32 字节。除了如图 20 的 B 中所示的标题部分之外，图 20 的 B 中的其余部分再与以下的部分一起记录：为整个储存卡提供的名称 NM1-S（256 字节），另一个名称 NM2-S（512 字节），经过加密的内容密钥（CONTENTS KEY），MAC，S-YMDhms，控制再生顺序的表格 TBKTTBL（800 字节），加入到整个储存卡的附加数据 INF-S（14720 字节），以及一部分包含在标题的数据。也已做出这样的规定，各类单个数据组的标题部分相应安置到再生控制文件的一个预定的位置。

参照再生控制文件，从最开始部分到图 20A 所示的由（0×0000）和（0×0010）所表示的 32 字节部分组成标题。从最前面的单元的包括每 16 字节的单元被称之为一个“槽”。为再生控制文件的第一和第二个槽提供的标题被从最前面的位置加入顺次有特定的含义、功能和值的数据（如下面所述）。指示为“保留”的数据表示一个还未定义的数据。通常，标示为 0（0×00），但是无论写入的内容是什么，“保留”的数据被忽略。在将来的版本中任何修改都有可能。在这一部分写入数据被禁止。除非被使用，标示为“可选”的部分完全和以上提到的“保留”数据得到相同的对待。

*BLKID-TLO（4 字节）

含义：BLOCKID FILEID

功能：一个标示再生控制文件的最前部的值

值：固定值=“TL=0”（例如，0×544C2D30）

*MCODE（2 字节）

含义：MAKER CODE

功能：标示生产商和记录装置的产品型号

值：上面的 10 字节（生产商代码）

下面的 6 字节（产品型号代码）

*REVISION（4 字节）

含义：PBLIST 的重写轮数

功能：每重写再生控制文件一次增加

值：初始为 0，按加 1 增加

*SN1C+L（2 字节）

含义：指示写在 NM1-S 域中的储存卡的名称（1 字节）的属性

功能：指示每一字节的可用的字符代码和语言代码

值：字符码通过如下所示的上面的一个字节辨别字符

00：没有设定字符代码：00 只被处理为二进制数

01：ASCII（美国信息交换标准码）

02：ASCII+KANA

03：修正的 8859-1

81：MS-JIS 82：KS V 5601-1989 83：GB（英国）2312-80

90：S-JIS（日本声音工业标准）

和 EBU Tech3258 规则一致，使用下面的一个字节，语言代码（L）辨别语言。

00：没有设定语言代码：

08：德语 09：英语 0A：西班牙语

0F：法语 15：意大利语 1D：荷兰语

65：朝鲜语 69：日语 75：中文

假如没有提供数值的话，语言代码整个被重设为 0。

*SN2C+L（2 字节）

含义：指示写在 NM2-S 域中的储存卡的名称（1 字节）的属性

功能：指示每一字节的可用的字符代码和语言代码

值：和以上参照 SN1C+L 描述的相同

*SINFSIZE（2 字节）

含义：指示写在 INF-S 域中的整个储存卡的附加数据的整体大小

功能：假如在一个 16 字节的单元中没有数据大小的描述，以上 SINFSIZE 的值被重设为 0

值：大小从 0×0001 到 0×39C

*T-TRK（2 字节）

含义：磁道的总数目

功能：指示磁道的总数目

值：从 1 到 0×3190（最大 400 个磁道）

假如没有提供数值，以上的 T-TRK 的值被重设为 0

*VerNo（2 字节）

含义：格式的版本号

功能：上面的字节指示主的版本号

下面的字节指示从版本号

VerNo 也被用作指示是否一个发布的数据是否有相应版权，也就是说，是否发布的数据需要利用基于以上在分层树状密钥结构中的 EKB 数据发布密钥。

值：例如，0×0100（1.0 版） 0×0203（2.3 版）

以下的叙述参照一个卸载跟着以上描述的标题的后面的域的数据（如图 20 中 B 所示）

*NM1-S：

含义：相关整个储存卡的一个字节的名称

功能：无论何时终止一个被一个字节的字符代码指示的有可变长度的数据（最大 256），终止码（0×00）必须写。

计算大小必须从终止码开始。假如没有给出数据，至少一个从最开始（0×0020）到空值的数据必须被一最少 1 个字节储存。

值：各种字符代码类型

*NM2-S：

含义：相关整个储存卡的 2 个字节的名称

功能：无论何时终止一个被 2 个字节的字符代码指示的有可变长度的数据（最大 512），终止码（0×00）必须写。

计算大小必须从终止码开始。假如没有给出数据，至少一个从最开始（0×0020）到空值的数据必须被一最少 2 个字节储存。

值：各种字符代码类型

*EKB_Version（4 个字节）

含义：指示以上所述的在分层树状密钥结构中的 EKB 所提供的内容密钥的代数，或者指示 EKB 文件的名称

功能：指示一个 EKB 以获得一个正当的在以上所述的分层树状密钥结构中的 EKB 所提供的内容密钥。

值：从 0 到 0×FF

*E（Kstm，Kcon）（8 个字节）

含义：包含有用来加密各个内容数据的内容密钥的数据，其中数据在通过施加一个储存卡的储存密钥（Kstm）加密内容数据而生成。

功能：用来加密数据

值：从 0 到 0×FFFFFFFFFFFFFFFF

*E（KEKn，Kcon）（8 个字节）

含义：包含有用来加密各个内容数据的内容密钥的数据，其中数据在通过施加一个以上所述的分层树状密钥结构中的 EKB 提供的密钥加密密钥（KEKn）加密内容数据而生成。

功能：用来加密内容数据

值：从 0 到 0×FFFFFFFFFFFFFFFF

*C_MAC[0]（8 个字节）

含义：用来检查版权数据的窜改的值

功能：用来检查窜改行为的值，其中这个值基于储存在以上的再生控制文件中的数据、指示诸如记录最终数据的内容数据处理过程的时间和日起、以及其他数据而生成。假如时间/日期数据 S-YMD 已经被窜改，它就表明在检查 C_MAC[0]时已经进行了窜改数据的动作，从而阻止了复制数据的操作。

值：从 0 到 0×FFFFFFFFFFFFFFFF

*MGR：

含义：内容密钥的类型

功能：当是 0×00 时，就有两种内容密钥，包括密钥 Kcon 和 E（KEKn，Kcon）。当指示为 0c01 时，只提供内容数据 E（KEKn，Kcon）.

值：从 0 到 0×01

*S-YMDhms（4 个字节）（可选）：

含义：被一个含有可靠的时钟的装置所记录的年、月、日、时、分和秒

功能：用来鉴别最后处理内容数据的日期的值，如记录数据的作后的时间和日期等。

值： 第 25 到 31 数位：年 0 到 99（1980 到 2079）

第 21 到 24 数位：月 0 到 12

第 16 到 20 数位：日 0 到 31

第 11 到 15 数位：小时 0 到 23

第 05 到 10 数位：分 0 到 59

第 00 到 04 数位：秒 0 到 29（每单元 2 秒）

这一 S-YMDhms 数据依据内容数据的处理而更新，例如，在记录内

容数据时。更进一步地，给予更新的数据，以上提到的 C_MAC[0]也被更新，然后被储存在存储器中。

*TRK-nnn：

含义：用来复制的 ATRAC-3 数据的文件的序号

功能：描述在 TRKINF 中的 Fno

值：从 0 到 400（0×190）

*INF-S：

含义：相关整个储存卡的附加数据，其中附加数据包括照片、单词、备注等

功能：伴随标题的长度可变的附加数据

多个相互各异的附加数据可以通过为每个附加数据提供一个 ID 码和一个预定的数据大小而排列。每一个附加数据分别被提供一个最小包含 16 个数位的标题和一个整数两倍长的 4 个字节的单元。详细的描述见后面。

值：参照附加数据的组成

为了构建再生控制文件的最后一个槽，和储存在标题相同的 BLKID-TLO、Mcode、和 Revision 被写入。

当操作一个用户的音频装置时，可能有这样一种情况，以上提到的储存卡被故意抽出或电源被切断，因此，就需要在恢复正常操作时检测这一意外发生的情形。如上所述，已经作出这样的安排，，以上所述的“修正 Revision”被写入到每一块的最前部和最后部，然后任何时候重写时，Revision 的值增加 1。假如在处理块的过程中有任何意外的中止发生，Revision 在最前和最后的相互不一致，从而使得可以检测意外的中断操作。由于提供了两个“修正 Revision”代码，就有很高的几率检测意外的中断操作。假如意外的中断操作被检测到的话，就生成一个警告（如通过显示错误信息）。

而且，由于固定值 BLKID-TLO 被插入到每一块（16KB）的最前部，这个固定的值可以在出现意外时用作标注 FAT 的修复程度。明确地说，就是通过检测在每一个块的最前部的固定值，就可以辨认文件的类型。而且，由于固定值是被双双写进标题和各个块的中断部分，也就有可能检测固定值的可信度。也允许双倍记录和再生控制文件 PBLIST 相同的数据。

和磁道数据控制文件相比，ATRAC-3 数据文件包含一个相当大的数

据体积。ATRAC-3 数据文件被提供以块数目 BLOCK SERIAL。在 ATRAC-3 数据文件中，通常在储存卡中有许多文件，因而，除非在通过 CONNUM0 辨认内容数据之后加入块数目 BLOCK SERIAL，否则使得当 FAT 乱了时，难以恢复文件。换句话说，由于一个 ATRAC-3 数据文件包含有很多块，每一块可能和其他分离而处理，因此，为了识别构成统一的 ATRAC-3 数据文件的块，就采用了 CONNUM0，而且在 ATRAC-3 数据文件中的序修改和降低通过块数目 BLOCK SERIAL 而决定。

同样的，在有逻辑错误在文件中产生任何偏差而没有导致 FAT 的破坏的情况下，为了写在文件中的装置制造商的产品型号可以被指明，制造商的编码 Mcode 被记录在每一块的最前面和最后面。

图 20 中 A C 标示了包含附加数据的数据的结构。显示在下面的标题被写在附加数据的最前部。长度可变的数据被卸载接着标题部分的部分。

*INF：

含义：域 ID

功能：固定值指示包含附加数据的数据的最前部分

值：从 0 到 0×FF

*SIZE：

含义：单个附加数据的数量

功能：数据的大小是自由的。但是，数据的大小必须是 4 字节整数的倍数。数据大小必须最小为 16 字节。假如在数据的结束点之外生成任何多余的部分，超过的部分必须被填为空码（0×00）。

值：从 16 到 14784（0×39C0）

*MCODE：

含义：生产商代码

功能：这一代码分辨性地表明生产商的名称和用来记录数据的装置的产品型号。

值：上面的 10 字节指示生产商代码

下面的 6 字节指示产品型号代码

*C+L：

含义： 指示写入到数据文件最前面部分开始的第 112 个字节相关的域中的字符的属性

功能：通过应用每个字节指示可用的字符代码和语言代码

值：和以上所述的 SNC+L 的值相同

*DATA：

含义：包含附加数据的单个数据

功能：单个数据被指定为长度可变的数据。实际数据的最前面部分总是从第 12 字节开始，其中数据的长度最少为 4 个字节，而且必须始终是 4 个字节的整数的倍数。假如在数据的结束点之外生成任何多余的部分，超过的部分必须被填为空码（0×00）。

值：依据内容，值被个别地定义。

图 21 例示了一个相应于 ATRAC-3 数据文件 A3Dnnnn 的数据的排列。图 21 标示了数据文件的一个属性标题（一个块）和一个音乐数据文件（一个块）。图 21 标示了相应以上两个块（16 字节×2=32 字节）的个体的槽的最前面的字节（0×000 到 0×7FF0）。就像图 22 明确表明的，标题包含有一个从最前面到属性标题的 32 字节的部分，其中 256 字节构成音乐名称域 NM1，而且 512 字节构成另一个音乐名称 NM2。属性标题的前面部分包含以下所示的数据的描述。

*BLKID-HD0（4 个字节）：

含义： BLOCK FILE ID

功能：识别以上的 ATRAC-3 数据文件的最前面的字节的值

值：固定值=“HD=0”（例如，0×48442D30）

*MCODE（2 个字节）：

含义：生产商代码

功能：这一代码分辨性地表明生产商的名称和用来记录数据的装置的产品型号。

值：上面的 10 字节指示生产商代码

下面的 6 字节指示产品型号代码

*BLOCK SERIAL（4 个字节）：

含义：加入到每一磁道的序列码

功能：初始的块的最前面的字节以 0 开始，然后接着的块增加 1。即使块数据被编辑，值不变。

值：从 0 到 0×FFFFFFFFFFFFFFFF

*N1C+L（2 个字节）：

含义： 指示磁道数据（NM1）的属性（音乐名称）

功能：为数据 NM1 所用的字符码和语言码分别由一个字节指示。

值：和前面的 SN1C+L 的值相同

*N2C+L（2 个字节）：

含义： 指示磁道数据（NM2）的属性（音乐名称）

功能：为数据 NM2 所用的字符码和语言码分别由一个字节指示。

值：和前面的 SN1C+L 的值相同

*SINFSIZE（2 字节）

含义：指示与磁道相关的附加数据的总的大小。

功能：基于 16 字节单元描述数据的大小，假如没有数据的话，数据到小被强制设定为 0

值：数据大小从 0×0000 到 0×3C6（966）

*T-PRT（2 字节）

含义：部分的总数

功能：指示构成磁道的部分的数目，通常，部分的数目为 1。

值：从 1 到 0×285（十进制为 645）

*T-SU（4 字节）

含义：相应部分的最小单元的声音单元 SU 的总数，同时它也在应用 ATRAC-3 压缩音频数据时构成最小的数据单元。声音单元的总数相应有几百字节，包含与通过将音频数据压缩到大约原始数据大小的 1/10、经由 44.1KHz 的取样频率取样而生成的 1024 样本应（1024×16 位×2 声道）相对应的音频数据。每一个 SU 大约相应通过时间转换的 23 毫秒。通常，一个部分由几千个 SU 组成。在单个簇包含 42 个 SU 单元的情形下，就可以用单个簇表达大约 1 秒的声音。构成单个磁道的部分的数来内附加数据的大小所影响。由于本分的数量在去掉标题、音乐名称和包含附加数据的数据之后由单个块的数目所决定，这样一个情形整个地避免了相应于启动多个部分（645 个单元）的条件的附加数据被利用。

功能：指示在磁道中的 US 的总数。这相应于完成一个音乐曲目的时间。

值：从 0×01 到 0×001FFFFF

*INX（2 字节）(可选)

含义：INDEX 的相对位置

功能：表示一个音乐曲目的典型的部分的顶端的指针。通过除 SU 的单元数为 1/4 而指示一个音乐曲目的顶端的位置。这一位置相应于一个四倍于 SU 通常长度的时间（大约 93 毫秒）。

值：从 0 到 0×FFFF（最多大约 6084 秒）

*XT（2 字节）(可选)

含义：复制 INDEX 的时间

功能：表示从以 INX-nnn 指定的最前面代码复制的 SU 的时间单元数目，通过除这一数为 1/4。这相应于一个四倍于 SU 通常长度的时间（大约 93 毫秒）。

值：0×0000=除去时间设定影响

从 0×01 到音乐曲目的结束 0×FFF（最大 6084 秒）

随后，音乐名称域 NM1 和 NM2 描述如下。

*NM1：

含义：表达音乐名称的字符阵列

功能：通过一个字节字符代码表达长度可变的音乐名称（最多 256）：无论何时终止音乐名称数据，有必要必须写终止码（0×00）。大小应该有终止码计算出。假如没有提供数据，必须至少有一个从最前面（0×0020）到空码（0×00）的字节被记录。

值：各种字符代码

*NM2：

含义：表达音乐名称的字符阵列

功能：通过两个字节字符代码表达长度可变的音乐名称（最多 512）：无论何时终止音乐名称数据，有必要必须写终止码（0×00）。大小应该有终止码计算出。假如没有提供数据，必须至少有 2 个从最前面（0×0020）到空码（0×00）的字节被记录。

值：各种字符代码

TRKINF 在属性标题的一个固定的位置（0×320）开始。TRKINF（磁道数据域）包含 80 字节数据，主要整体地控制相干安全和再生控制数据的控制数据。图 23 标示了 TRKINF 部分。以下按照排列的顺序描述 TRKINF 域中的数据。

*EKI（1 字节）：

含义：以上所述的分层树状密钥结构中的 EKB 提供的内容加密密钥。

EKI 标示是否提供了 E(KEKn，Kcon)。

功能：数位 7=1 标示提供了密钥 E

数位 7=0 标示未提供密钥 E

当是条件“数位 7=0”时，应该不参照 R(KEKn，Kcon)进入 EKB_version。

值：从 0 到 0×FF

*EKB_version（4 字节）：

含义：表示以上所述的在分层树状密钥结构中的 EKB 所提供的内容密钥的代数，或者/和表示 EKB 文件的名称

功能：表示一个 EKB 以获得一个正当的在以上所述的分层树状密钥结构中的 EKB 所提供的内容密钥。

值：从 0 到 0×FF

*E(Kstm，Kcon)（8 个字节）：

含义：包含有用来加密内容数据的内容密钥的数据，这一数据被储存卡中的储存密钥（Kstm）加密。

功能：用来加密内容数据。

值：从 0 到 0×FFFFFFFFFFFFFFFF

*E（KEKn，Kcon）（8 个字节）

含义：包含有用来加密各个内容数据的内容密钥的数据，其中数据被通过施加一个以上所述的分层树状密钥结构中的 EKB 提供的密钥加密密钥（KEKn）而加密。

功能：用来加密内容数据

值：从 0 到 0×FFFFFFFFFFFFFFFF

*C_MAC[n]（8 个字节）

含义：用来检测版权数被窜改的值。

功能：一个从包含内容数据的累积数的以上的多个 TRKINF 数据的内容和从隐藏的序列数中生成的值。隐藏的序列数值的是记录在一个储存卡中的隐藏域的中的序列数。一个没有安全版权装置的记录装置不能阅读隐藏域。另一方面，一个有版权装置的激励装置和一个装载有能够阅读储存卡的应用程序的个人计算机可以获得访问隐藏的域的权限。

*A（1 个字节）

含义：部分的属性

功能：表示在部分中的如压缩模式等数据

值：参照图 24，详细描述如下。

一个特别的结合方式被称之为诞生到信号的“单声道”模式 1（其中 N=0），但声道闹包含为二进制码 1 的数位 7 和为 0 的子信号，其中主信号只包含（L+R）信号部分。对应于数位 2、1 的数据可能被传统的再生装置所忽略。

以上属性 A 的数位 0 构成降噪开/关的数据，而数位 1 构成一个表示跳过再生模式或者正常再生模式的数据。数位 2 构成一个差异数据，换句话说，数位 2 构成一个比较音频数据和其他的诸如电传数据或类似的数据等的数据。数位 3 还未定义。如图 24 所示，通过组合数位 4、5、6，ATRAC-3 的模式的数据就被规定。特别的，N 标示一个由数位 4、5、6 表述的模式值。模式值标示了记录时间（当利用 64M 储存卡时），数据传输速率，相应于 5 类模式（包括单声道（N=0，1），LP（N=2），SP（N=4），EX（N=5）和，HQ（N=2））的每一块的 SU 的数。SU 单元在单声道模式包含 136 字节，在 LP 模式包含 192 字节，在 SP 模式包含 304 字节，在 EX 模式包含 384 字节，在 HQ 模式包含 512 字节。进一步的，以上提到的 ATRAC-3 的“双声道”模式（N=0）和“联合”模式（N=1）在数位 7 指出。

例如，假定在利用 64M 储存卡时进入 SP 模式。64M 储存卡包含 3968 块。由于每隔 SU 单元包含 304 字节，当进入 SP 模式时，每一块有 53 个 SU 单元。一个 SU 单元相应 1024/44100 秒。相应地，每一块相应（1024/44100）×53×(3968-16)=4863 秒=81 分。另一方面，数据传输率计算如下。

（44100/1024）×304×8=104737bps

*LT（1 个字节）

含义：复制限制的标记（包括数位 6 和 7）和安全版本（数位 5 到 0）。

功能：标示加到磁道的限制条款

值：数位 7：0=没有限制　1=限制

数位 6：0=有效期内　1=过期

数位 5 到 0：安全版本=0

*FNo（2 个字节）

含义：初始记录的磁道数。这一值指定用来计算记录在储存卡的隐藏

的域的 MAV 得值的位置。

功能：每一记录装置完全不同的是当的值

值：从 0 到 0×FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

*CONNUM（4 个字节）

含义：一个以每一音乐曲目累积的值。这一值被每个记录装置提供的安全块控制。总共准备了 42 亿音乐曲目（2^{32}）用来表示记录的音乐曲目。

功能：每一记录装置完全不同的是当的值

值：从 0 到 0×FFFFFFFF

* YMDhms-S（4 个字节）（可选）：

含义：开始复制限制被复制的磁道的日期和时间

功能：核准由 EMD 指定的复制开始的日期和时间

值： 和以上提到的日期和时间相同

* YMDhms-E（4 个字节）（可选）：

含义：终止复制限制被复制的磁道的日期和时间

功能：核准由 EMD 指定的核准复制的日期和时间的终止

值： 和以上提到的日期和时间相同

* XCC（1 个字节）：

含义：以下所描述的 CC(复制控制)的扩展部分

功能：控制复制

* CT（1 个字节）（可选）：

含义：复制的回合

功能：和总的可复制的回合数相对的实际的复制回合数。回合数载每次复制之后减少。

值： 从 0×00 到 0×FF，当允许的复制的回合数还完全未被使用时，值是空值（0×00）。当 LT 的第 7 数位指向 1 而 CT 的指向 00 时，复制被禁止。

* CC（1 个字节）：

含义：控制复制

功能：控制复制操作

值： 如图 25 所示，数位 6 和 7 一起表示一个再生控制数据，数位 4 和 5 一起联合表示一个相关高速数码复制操作的再生控制数据，数位 2 和 3 一起联合表示一个安全块授权认证等级。数位 0 和 1 尚未定义。

再生控制操作包含以下方面：当使用数位 6 和 7 时，数据代码 11 允许不确定的操作；数据代码 01 禁止复制操作；数据代码 00 允许复制操作一次。当使用数位 2 和 3 时，数据代码 00 允许从一个模拟输入或数码输入记录；数据代码 0 表示 MG 授权认证等级。在通过 CD 数码记录的情形下，数位 6 和 7 相应前面的功能 00，而数位 2 和 3 相应后面的功能 00。

* CN（1 个字节）（可选）：

含义：在 HSCMS（高速串联复制管理系统）复制允许的回合数

功能：在一次复制和不确定复制回合数之间的区分本扩展未表示允许复制的回合数。允许复制的回合数只在第一次复制时有效，然后再每次复制操作时减少。

值： 00=禁止复制。从 01 到 0×FE 表示可复制的回合数，0×FF 标示不确定回合数。

接着以上所述的磁道数据域 TRKINF，这样一个从 0×0370 开始的 24 字节的数据被称作控制部分的部分数据域 PRTINF。当用河多部分合成一个单一的磁道时，PRTINF 按时间轴顺序排列。图 26 标示了和 PTTINF 相关的部分。以下按照排列的顺序详细描述 PRTINF 域中的数据。

* PRTSIZE (4 个字节)：

含义：部分的大小

功能：表示部分的大小，包括以下：簇被提供 2 个字节（最上面）；开始 SU 一个字节（上些的部分）和终止 SU 一个字节（最下面的部分）。

值： 簇：从 1 到 0×1F40(8000)

开始 SU：从 0 到 0×A0(160)

终止 SU：从 0 到 0×A0(160)

注意 SU 码是从 0，1，2……向上计数。

* PRTKEY(8 个字节)：

含义：用来加密部分的值

功能：初始值= 0

当进入一个编辑进程时，编辑规则比如遵守。

值：从 0 到 0×FFFFFFFFFFFFFFFF

* CONNUM0（4 个字节）：

含义：一个初始产生的用来表示内容数据的累积数的密钥

功能：作为定性内容数据的 ID 的角色

值：和累积内容数据数的初始值的值相同。

再次参照图 21，如图 21 所示，ATRAC-3 数据文件的属性标题包含一个附加数据 INF。附加数据 INF 和磁道相关，磁道有着可变的长度，和标题相伴。根据情形，多个和相互不同的附加数据可能被排列。每一附加数据被加入一个 ID 号和一个数据大小。这样一个附加数据包含最少有 16 字节的标题，而且含有倍数于 4 个字节的整数的倍数的单元。

以上所述的 ATRAC-3 数据文件的各个块跟在以上所述的属性标题的后面。如图 27 所示，在每个块中加入标题。用在 ATRAC-3 数据文件的每一块的数据描述如下。

* BLKID-A3D（4 个字节）：

含义：块化的文件的 ID

功能：表示 ATRAC-3 数据文件的最前部的值

值：固定值=“A3D”（例如，0×41334420）

值：固定值=“HD=0”（例如，0×48442D30）

*MCODE（2 个字节）：

含义：生产商代码

功能：这一代码分辨性地表明生产商的名称和用来记录数据的装置的产品型号。

值：上面的 10 字节表示生产商代码，而下面的 6 字节表示产品型号代码

* CONNUM0（4 个字节）：

含义：初始产生的用来表示累积内容数据数

功能：作为定性内容数据的 ID 的角色。即使被编辑时，值不变。

值：和累积内容数据数的初始值密钥的值相同。

*BLOCK SERIAL（4 个字节）：

含义：加入到每一磁道的序列码

功能：初始的块的最前面的字节以 0 开始，然后接着的块增加 1。即使块数据被编辑，值不变。

值：从 0 到 0×FFFFFFFFFFFFFFFF

*BLOCK SEED（8 个字节）：

含义：用来加密一个块的密钥

功能： 初始的块使得相应记录装置的安全块能够产生随机数。接着

的块记数加 1。假如本值丢失的话，相应的块的任何一秒声音都不能生成，而且，一个相同的值被双倍写入到块的标题和作后部分。即被编辑，值保持不变。

值：在初始阶段是 8 个字节的随机数

*INITIALIZATION VECTOR（8 个字节）：

含义：一个必须的用来加密的解密以上所述的每一磁道的 ATRAC-3 数据文件的初始值

功能：初始的块以 0 开始，而结下的块利用最后的 SU 的最终的加密的 8 字节值。在加密和解码一个块的中间的部分的数据的情形下，最后的在初始 SU 之前的 8 个字节被利用。即被编辑，值保持不变。

值：从 0 到 0×FFFFFFFFFFFFFFFF

*SU-nnn：

含义：声音单元的数据

功能：从 1024 样本压缩的数据。依据压缩的模式，输出的字节数不同。即被编辑，值保持不变。比如，当进入 SP 模式时，N 对应 384 字节。

值：ATRAC-3 数据文件的数据的值

参照图 21 所示的结构，由于 N=384，总共 42 个 SU 被写入一个块中。每块一对最前面的槽（4 个字节）构成标题。并且，BLKID-A3D、Mcode、CONNUM0 和 BLOCK SERIAL 双倍写入最后一块（2 个字节）。相应地，富余的域占了每块的 M 字节（16384-384×42-16×3=208 字节）就像以前提到的，一个 8 字节的 BLOCK SEED 被双倍记录在 M 字节的剩余的域。

块寻址数据通过每块生成随机数的方式生成。

[闪存控制模块 35]

闪存控制模块 35 控制写进数据到闪存 34 和从闪存读出数据的操作。

图 15 所示的再生装置的构造描述如下。图 15 所示的再生装置包含以下部分：一个主控制模块，一个通讯接口装置 42，一个控制模块 43，一个编辑模块 44，一个压缩/扩展模块 45，一个扬声器模块 46，一个数/模转换器 47，以及一个模/数转换器 48。

[主控制模块 41]

主控制模块 41 整合地控制操作再生装置 200 的操作的进程。

[控制模块 43]

如图 15 所示的控制模块 43 包含以下部分：一个随机数生成单元 60，

一个储存单元 61，一个密钥生成和密钥算法操作单元 62，一个相互授权认证单元 63，一个加密和解码单元 64，一个控制单元 65。类似另外一个控制模块 33，控制模块 43 自己由一个单芯片的多层集成电路组成，这一电路值对秘密处理过程可操作，控制模块 43 的储存单元夹在由铝制造的伪层之间。进一步地，控制模块 43 还含一个窄幅的操作电压和一个窄带的操作频率，因而进而有了防窜改的能力以防止由外部原因的非法阅读数据。在接到生成随机数的命令的情况下，随机数生成单元 60 生成一个 64 位（也就是 8 字节）的随机数。储存单元 61 储存各种执行授权认证处理所要的各种数据。

通过执行许多算法操作（如采用 ISO/IEC9797 MAC 算法操作格式），密钥生成和密钥算法操作单元 62 生成各种密钥数据。在生成密钥数据时，密钥生成单元 62 采用 FIPS PUB46-2 所规定的 DES 作为“块”加密算法 2。

在把从个人计算机输入的音频数据付送到存储装置 300 之前，相互授权认证单元 63 和存储装置 300 执行一个授权认证处理。进一步，在从存储装置 300 接收音频数据之前，相互授权认证单元 63 也和存储装置 300 执行一个授权认证处理。而且，在执行相互授权认证时，共授权认证单元 63 也执行 MAC 算法操作。为了实现相互授权认证，储存在存储装置 300 中的数据也被利用到。进一步，在和个人计算机 100 或另外一个在网络服务线路上的个人计算机 100 之间减缓输入或输出的音频数据时，共授权认证单元 63 也和个人计算机 100 或另外一个在网络服务线路上的个人计算机 100 之间交换共授权认证。

如以上提到的，通过选择性地利用 FIPS PUB81 规定的 ECB 或 CBC 模式，加密/解码单元 64 执行一个加密处理操作。

在 FIPS PUB81 规定的模式中，加密/解码单元 64 选择性地解码 ECB 和 CBC 模式。当解码 CBC 模式时，如通过施加一个 56 位的密钥数据“K”，加密/解码单元 64 通过在最终生成纯文本之前将包含有 64 数位的加密的块作为一个处理单元的方式而解码一个加密的字母。

以上提到的控制单元 65 整体地控制随机数生成单元 60、储存单元 61、密钥生成/算法单元 62、相互授权认证单元 63 和加密/解码单元 64 执行的功能性操作。

[编辑模块 44]

例如，如图 15 所示，基于从用户来的操作指令，编辑模块 44 编辑储

存在存储装置 300 的闪存 34 中的磁道数据文件，从而生成新的磁道数据文件。

[压缩/扩展模块 45]

例如，当复制一个解码于从比如存储装置 300 输入的加密音频数据时，压缩/扩展模块 45 首先扩展相应的被 ATRAC-3 数据文件格式压缩的音频数据，然后付送扩展的音频数据到数/模转换器 47。进一步，当储存从 CD，DVD 或个人计算机输入的音频数据到以上的存储装置 300 时，压缩/扩展模块 45 基于 ATRAC-3 数据文件格式压缩相应的音频数据。

[数/模转换器 47]

通过转换从压缩/扩展模块 45 接收到的数字格式的应聘数据成模拟格式的音频数据，数/模转换器 47 输出经过数/模转换的音频数据到扬声器单元 46。

[扬声器单元 46]

扬声器单元 46 相应从数/模转换器 47 输入的模拟音频数据输出声音。

[模/数转换器 48]

例如，通过转换从 CD 播放器输入的模拟格式的音频数据成数字格式，模/数转换器 48 经过模/数转换的音频数据到压缩/扩展模块 45。

[储存器 49]

储存器 49 本身由 E2PROM 构成（例如，闪存），其中内在储存有包括以上所述的 EKB 或通过 EKB 生成的装置密钥块、和一个作为装置识别成分的装置 ID。

[储存内容数据到一个存储装置的处理过程和再生内容数据的处理过程]

在再生装置和存储装置 300 之间交换的内容数据如图 15 所示。具体地说，一个通过再生装置 200 再生内容数据的处理过程和一个同时的储存内容数据到存储装置 300 的闪存的操作被执行。另外，一个通过从存储装置 300 的闪存 34 来的数据到再生装置 200 的处理过程被执行。

记录和再生内容数据的处理过程描述如下。首先，通过参照图 28 所示的流程图，记录再生装置 200 的数据到存储装置 300 的闪存的处理过程描述如下。

在交换数据之前，起初，再生装置和存储装置 300 分别执行一个相互授权认证处理过程，如处理步骤 S2701 和 S2702 所示。图 29 标示了一个

如 ISO/IEC9798-2 所规定的通过施加一个公钥加密的方式的公共公授权认证方法。虽然在图 29 中采用 DES 作为公钥加密方式，任何其他的除开的 DES 的方式用作公钥加密方式也是实际可行的。参照图 29，开始，B 单元生成 64 位的随机数 Rb 然后传送随机数 Rb 和自己标示的代码 ID 给 A 单元。在接收到发送的代码的情况下，A 单元最新生成 64 位的随机数，然后基于 DES 的 CBC 模式，A 单元通过施加加密密钥(Kab)而顺次加密接收到的数据 Ra，Rb 和 ID（b），最终返还加密的数据给 B 单元。加密密钥（Kab）分别存在 A 单元和 B 单元的相应的记录部分中。在采用如 DES 格式的 CBC 模式用加密密钥的加密处理过程中，初始值和加密密钥（Kab）被进行异或操作。随后两个值都被通过施加加密密钥（Kab）由 DES 加密单元加密，从而生成一个经过加密的字符 E1。接着经过加密的字符 E1 和上面的随机数 Rb 进行一个异或操作。随后，经过加密的字符 E1 和随机数 Rb 通过施加加密密钥（Kab）而被 DES 加密单元加密，从而生成另一个经过加密的字符 E2。

进一步的，加密的字符 E2 和 ID(b)被进行一个异或操作。最终，DES 加密单元通过利用经过加密的字符 E3（经由一个使用加密密钥（Kab）的加密处理过程而生成的）而生成一个可传送的数据（Token-AB）。

在接收到数据的条件下，B 单元施加储存在相应的记录单元的作为公钥的授权认证密钥（Kab）而解码接收到的数据。接收到的数据通过以下所述的序列步骤所解码。开始，经过加密的字符 E1 通过施加授权认证密钥（Kab）而解码以生成随机数 Ra。随后，经过加密的字符 E2 通过施加公钥的授权认证密钥（Kab）而解码。随后。解码的结果和经过加密的字符 E1 被进行一个异或操作以生成随机数 Rb。最后，经过加密的字符 E3 通过施加授权认证密钥（Kab）而解码。随后，解码的数据和经过加密的字符 E2 被进行一个异或操作以生成 ID(b)。随后，对于那些结果数据 Ra，Rb 和 ID(b)，一个验证操作被执行以验证是否结果数据 Rb 和 ID(b)精确地和从 B 单元传来的数据一致。只有当两者之间的一致被验证时，B 单元才认证 A 单元为正当。

随后，通过施加随机数，B 单元生成一个之后实现授权认证操作有用的区间密钥。随后，通过经由 DES 格式的 CBC 模式施加授权认证密钥（Kab），本单元在将数据返还给 A 单元之前顺次加密随机数 Ra、Rb 和区间密钥（Kses）。

在接收到以上的经过加密的随机数和区间密钥的情况下，A 单元基于和已经施加到为 B 单元所执行的解码处理过程的解码方法相同的解码方法解码接收到的数据。对于那些结果数据 Ra，Rb 和区间密钥（Kses），A 单元执行一个验证操作是否结果数据 Ra 和 Rb 和从 A 单元传送的数据完全一致。只有当两者之间的一致被验证时，A 单元才认证 B 单元为正当。在相互都被认证为正当之后，区间密钥（Kses）被用作接着相互授权认证之后的执行机密的通讯的公钥。

即使在验证接收的数据的过程中有差异和不正当行为的情况下，被认定为相互授权认证被忽略，从而终止相关的过程。在流程度所示的处理步骤 S2703 中，以上的失败被表示为“否”。

当相互授权认证已经被实行时（处理步骤 S2703 中的“是”），进入步骤 S2794，在这一步骤终，再生装置 200 执行一个生成内容密钥（Kcon）的操作。这一操作被以上所述的密钥生成/密钥算法操作单元 62 执行，通过施加图 15 所示的以上所述的随机数生成单元 60 所生成的随机数来执行。

随后，进入步骤 S2705，在这一步骤中，那些序列的处理操作被执行。第一步，密钥数据 E（KEK，Kcon）通过施加从 EKB 获得的加密密钥（KEK）加密内容密钥（kcon）而生成。第二步，内容密钥（kcon）通过施加以上认证过程产生的区间密钥（Kses）而加密。从而生成密钥数据 E（Kses，Kcon），这一数据接着被传送到储存卡，以构建以上的存储装置 300。

随后，进入步骤 S2706，在这一步骤中，存储装置 300 通过解码以上的密钥数据 E（KEK，Kcon）的方式获得内容密钥（kcon），以上的密钥数据 E（KEK，Kcon）通过施加区间密钥（Kses）而从再生装置 200 接收到。随后，内容密钥（kcon）被一个前面储存在存储装置 300 的储存密钥（Kstm）加密，从而生成一个密钥数据 E（Kstm，Kcon），这一数据接着被传送到再生装置 200。

随后，进入步骤 S2707，在这一步骤中，使用由步骤 S2705 生成的密钥数据 E（Kses，Kcon）和另一个在前面的步骤 S2706 中从储存装置 300 接收到的密钥数据 E（Kstm，Kcon），再生装置 200 生成一个构成如图 21 所示的数据文件的磁道数据域 TRKINF。在格式化数据文件之后，经过格式化的数据文件被传送到存储装置（储存卡）300。

随后，进入步骤 S2708，在这一步骤中，存储装置（储存卡）300 储

存从再生装置接收的数据文件到它自己的闪存中。

依据以上的安排，如图 21 和 23 所示，已经做出这样的安排，以上所述的格式化的数据文件的磁道数据域 TRKINF 储存以下内容：通过施加从 EKB 中获取的加密密钥（KEK）加密内容密钥（kcon）而得到的经过加密的密钥数据 E（KEK，Kcon）；另一个通过施加先前储存在存储装置 300 中的储存密钥（Kstm）加密内容密钥（kcon）而得到的经过加密的密钥数据 E（Kstm，Kcon）。

也可能通过直接利用内容密钥（kcon）作为加密内容数据的密钥而执行一个加密音乐数据和图片数据的处理过程。进一步，也可能通过基于内容密钥的代数相关的数据将它们划分到部分单元和块单元而初始生成那些加密密钥和基于时的密钥加密处理过程能被每一部分和块单元执行而生成其它的密钥。

在利用以上所述的数据问件的再生处理过程中，可能通过选择性地施加加密密钥数据 E（KEK，Kcon）和其它的加密密钥数据 E（Kstm，Kcon）而获取内容密钥（Kcon）。

接着参照图 30 所示的流程图，从存储装置 300 的闪存 34 中读出储存的数据的处理过程被再生装置 200 执行，换言之，执行再生处理过程的情形，被描述如下。

在交换数据之前，再生装置 200 和存储装置 300 分别按照先前的依图 29 所示的流程图的方式执行一个相应步骤 S2901 和 S2902 的相互授权认证处理过程。当相互授权认证处理被忽略时（在步骤 S2902 中标示为“否”），整个的处理过程被终止。

当相互授权认证已经被执行时（步骤 S2903 所指示的“是”），进入步骤 S2704，在这一步骤中，存储装置 300 传送特定的数据文件到再生装置 200。在接收到数据问件的条件下，再生装置 200 检查数据文件中的磁道数据域 TRKINF 以辨认储存的内容密钥（Kcon）的实际状态。本处理过程使得再生装置 200 辨认是否内容密钥（比如，由 EKB 获取的加密密钥（KEK）加密的加密密钥数据 E（KEK，Kcon））真正储存在磁道数据域 TRKINF 中。有或没有密钥数据 E（KEK，Kcon）可以通过先前参照图 21 和 23 描述的磁道数据域 TRKINF 中的数据[EKI]而辨认。

当加密密钥数据 E（KEK，Kcon）储存在磁道数据域 TRKINF 时（步骤 S2906 标示的“是”），进入步骤 S2907 以通过操作 EKB 获取加密密

钥（KEK），随后，基于获取的加密密钥（KEK），加密密钥数据 E（KEK，Kcon）被解码。从而获取内容密钥（Kcon）。

相反的，当加密密钥数据 E(KEK，Kcon)未储存在磁道数据域 TRKINF 时（步骤 S2906 标示的“否”），进入步骤 S2908，在这一步骤中，通过施加储存密钥（Kstm），存储装置 300 的控制模块 33 解码由预先储存在存储装置 300 的储存密钥（Kstm）加密的加密密钥数据 E（Kstm，Kcon）。进一步，控制模块 33 利用以上的相互授权认证处理过程中为再生装置 200 和存储装置 200 之间所共有化的区间密钥(Kses)而生成一个数据 E(Kses，Kcon），接着传送数据 E 到再生装置 200。

随后，进入步骤 S2909，在这一步骤中，再生装置 200 通过在获取内容密钥（Kcon）之前施加区间密钥（Kses）而解码从存储装置 300 接收到的数据 Kses，Kcon）。

随后，进入步骤 S2910，在这一步骤中，通过施加由以上的步骤 S2907 和 S2909 获取的内容密钥（Kcon），内容数据被解码。

如上所述的，作为经由操作 EKB 通过施加以上的加密密钥（KEK）使得再生装置 200 能够解码数据 E（KEK，Kcon）的结果和基于由预先储存在存储装置 300 中的储存密钥（Kstm）加密的数据 E 执行一个预定的处理步骤得结果，内容密钥（Kcon）最终被获取。

解码音乐数据和图片数据的操作过程通过施加内容密钥（Kcon）自己作为解码内容数据的密钥而执行。另外，解码音乐数据和图片数据的操作过程也可每部分单元或每块单元执行，通过基于相关其它密钥的代数的内容密钥和数据相应分别构成内容数据的部分和块而分别生成一个每部分单元或每块单元的解码密钥。

[储存 KEK 的 EKB 格式]

总体的 EKB 的格式先前参照图 6 描述。下面的描述参照一个具体的通过存储器保存密钥加密密钥（KEK）在 EKB 中的例子。

图 31 示例了一个可以发布密钥的数据文件的结构，其中相关 EKB 的数据文件包含储存在 EKB 中的密钥加密密钥（KEK）的数据。一个相关的装置(相应以再生装置)按请求从数据文件提取出密钥加密密钥(KEK)，接着通过密钥加密密钥（KEK）解码加密的密钥数据 E（KEK，Kcon），从而在最终解码内容数据之前获取内容密钥（Kcon）。可适用的数据的细节描述如下。

*BLKID-EKB（4 个字节）：

含义： BLOCKID FILE ID

功能：识别密钥的数据文件的最前面的值

值：固定值=“EKB”（例如，0×454B4220）

*MCODE（2 个字节）：

含义：生产商代码

功能：表明用来记录数据的装置的生产商的名称和产品型号。

值：上面的 10 字节（生产商代码）；下面的 6 字节（产品型号代码）

*LKF：

含义：连接文件信息

功能：标识一个包含有这样一个内容数据的连接文件，其中由 EKB 获取的内容数据可以被应用。

值：0 到 0×FF

数位 7：1=应用到再生控制文件（PBLIST）

0=没有应用

数位 6：1=应用到窜改检验值（ICV）

0=没有应用

数位 5 到 0：保留

*LINK COUNT：

含义：连接数

功能：连接的文件的数目（例如, ATTAC-3 数据文件）。

值：0 到 0×FFFFFFFF

*VERSION：

含义：版本

功能：标识密钥发布核准数据文件的版本

值：0 到 0×FFFFFFFF

*EA：

含义：加密算法

功能：标识密钥发布核准数据文件的跟踪算法

值：0 到 0×FF

00h：以三 DES 模式处理

01h：以单 DES 模式处理

三 DES 模式利用超过 2 种加密密钥处理，而单 DES 模式采用超过 1 个加密密钥。

*KEK1：

含义：密钥加密密钥

功能：一个被 EKB 中的根密钥（相应最上层）加密的内容密钥加密密钥

值：0 到 0×FFFFFFFFFFFFFFFF

*KEK2：

含义：密钥加密密钥

功能：一个被 EKB 中的根密钥（相应最上层）加密的内容密钥加密密钥

值：0 到 0×FFFFFFFFFFFFFFFF

*E（VERSION）：

含义：加密版本

功能：一个被 EKB 中的根密钥（相应最上层）加密的版本号。解码处理过程中底下的 4 个字节被保留。

值：0 到 0×FFFFFFFFFFFFFFFF

*SIZE OF TAG PART：

含义：标签部分的大小

功能：构成密钥发布核准数据文件的数据的标签部分的大小（字节）。

值：0 到 0×FFFFFFFF

*SIZE OF KEY PART：

含义：密钥部分的大小

功能：构成密钥发布核准数据文件的数据的密钥部分的大小（字节）。

值：0 到 0×FFFFFFFF

*SIZE OF SIGN PART：

含义：签字部分的大小

功能：构成密钥发布核准数据文件的数据的签字部分的大小（字节）。

值：0 到 0×FFFFFFFF

*TAG PART：

含义：标签部分

功能：相应的构成密钥发布核准数据文件的数据的标签部分的数据。

值：所有值

在少于 8 个字节的情形下，0 被使用以使之成为 8 个字节。

*KEY PART：

含义：密钥部分

功能：相应的构成密钥发布核准数据文件的数据的密钥部分的数据。

值：所有值

*SIGNATURE PART：

含义：签名部分

功能：相应的构成密钥发布核准数据文件的数据的签名部分的数据。

如图 31 所示，并且可以从上面的描述了解到，包含为相应的装置提供的密钥发布核准数据文件的数据文件储存数据 LKF 以识别一个特别的连接文件，连接文件包含有从以上所述的数据文件中获取的密钥加密密钥（KEK）可以施加的数据文件。另外，以上的数据文件也储存表示连接的文件数（例如，ATRAC-3 数据文件）的数据 Link Count。通过参照以上的数据 LKF 和 Link Count，就可能使再生装置辨识一个要求应用从以上的密钥发布核准数据文件获取的密钥加密密钥（KEK）的数据是否实际被提供，从而也可能辨识这一数据的编号。

[解码和再生使用连接数据的数据]

图 32 例示了存储装置 300 的一个数据储存域，明确地说，一个储存在存储装置 300 中的闪存 34 中的数据文件的示例。图 32 唯一地例示了一个高保真音乐数据的目录的结构。但是，也允许包括包含图片文件的目录。

图 32 所示的音乐数据目录包括一个再生控制文件（PBLIST）和多个 ATRAC-3 数据文件（A3D）。进一步，存储装置 300 也储存多个 EKB。储存在 ATRAC-3 数据文件（A3D）中的指针标示一个用来获取特定的可应用来解码 ATRAC-3 数据文件（A3D）的内容密钥的 EKBn。如图 32 所示，其中一个（表示为 3101）使能密钥块（EKB1）被利用来解码多个（3 个单元）的 ATRAC-3 数据文件（A3D）。

在这种情形中，可应用到三个内容数据的数据被储存在相应以上所述的使能密钥块（EKB1）3101 的密钥发布核准数据文件的 Link Count 数据中。

图 33 表示了一个描述从存储装置 300 解码和再生内容数据的序列的处理过程，存储装置如图 32 所示包含一个储存多个内容数据和多个 EKB

的储存卡。

在当储存卡被装载到再生装置 200 时或当装载有储存卡的再生装置 200 的电源被打开时，这些序列的处理过程被再生装置 200 执行。

首先，当进入 S3201 步骤时，再生装置 200 读出各个 EKB 文件的磁道数据，接着检查“Link Count”数据。随后，再生装置 200 按照有着较大的 Link Count 数据的 EKB 数据的顺序选择相应预定的编号[n]的 EKB 文件。单元编号[n]相应一个可储存在再生装置的预定的储存域（例如，单元编号可储存在保持 KEK 在储存中的域）中的单元编号。

随后，进入 S3202 步骤，在本步骤中，选定的 EKB 文件被处理，接着再生装置 200 采集多个（相应于[n]）密钥加密密钥（KEK），随后，它们被储存到安装到再生装置 200 中作为密钥储存域的 RAM 的一个预定的域中。

随后，进入 S3203 步骤，在本步骤中，再生装置 200 选择应被解码和再生的数据。当已经进入步骤 S3204 时，再生装置 200 辨识可应用来解码选定的内容数据的密钥加密密钥（KEK）是否真正储存在 RAM 中。假如密钥加密密钥（KEK）正真正地在 RAM 中（“是”），进入 S3205 步骤，在本步骤中，基于相应的密钥加密密钥（KEK），再生装置 200 解码加密数据 E（KEK，Kcon），接着获取一个内容密钥。当已经进入下一个步骤 S3209 时，再生装置 200 通过施加获取的内容密钥解码和再生内容数据。

当以上的步骤 S3206 在进行中时，在可用来解码选定的内容数据的密钥加密密钥（KEK）没有储存在 RAM 中的情况下，进入步骤 S3206，在本步骤中，再生装置 200 辨识被储存密钥（例如，加密数据 E（Kstm，Kcon））加密的内容密钥是否真正存在。假如存在的话，进入步骤 S3207，在本步骤中，加密数据 E（Kstm，Kcon）被解码以使再生装置 200 可以获取内容密钥，从而进入步骤 S3209，在本步骤中，再生装置 200 通过施加获取的内容密钥解码和再生数据。

假如辨识到在步骤 S3206 在进行中时加密数据 E（Kstm，Kcon）不存在，再生装置 200 获取一个应用到内容数据的从存储装置 300 解码的正当的 EKB，接着解码获取的 EKB 以保护密钥加密密钥（KEK）。再生装置 200 进一步解码加密数据 E（KEK，Kcon）从而获得内容密钥。当已经进入步骤 S3209 时，再生装置 200 通过施加获取的内容密钥解码和再生内容数据。

如上所述，再生装置 200 首先检查先前储存在存储装置 300 中的多个 EKB 的“Link Count”数据，接着执行解码这样一个包含多个“Link Count”数据的 EKB，从而储存密钥加密密钥（KEK）在再生装置自身。相应地，无论何时再生内容数据时，再生装置被能够以高概率使用储存在自身的 RAM 中的密钥加密密钥（KEK），因而使得它可能高效地再生内容数据。

[利用 EKB 发布授权认证密钥]

在利用以上所述的 EKB 发布加密密钥的情形中，也以作出这样的安排，一个对授权认证处理过程有用的授权认证密钥 Ikn 被发布给所有有关的方面。用经由付送一个为相关的装置共有的授权认证密钥作为一个安全的密钥来执行一个遵照公钥格式的授权认证处理过程的系统被描述如下。

一个经由利用根据 ISO/IEC 9798-2 标准的公钥加密格式的相互授权认证处理过程已经在先前参照图 29 描述。在执行数据传送和接收之前，为了确认和验证相关的装置和部分的正确性，一个相互的授权认证处理过程被执行。在实际的授权认证处理过程中，数据在相关的装置之间传送和接收。例如，再生装置和存储装置公有化一个授权认证密钥（Kab）。公钥(Kab)通过利用以上所述的 EKB 发布到相关的再生装置。

图 34 和图 35 分别例示了一个通过 EKB 发布一个相互授权认证密钥 Ikn 到多个装置的系统。图 34 例示了一个可解码的授权认证密钥 Ikn 被发布到装置 0，1，2 和 3 的情形，图 35 例示了一个可解码的授权认证密钥 Ikn 被发布到装置 0，1 和 2，而装置 3 唯一在 0，1，2 和 3 中被撤销的情形。

在图 34 所示的系统中，通过利用和包含一个被升级的节点密钥 K(t) 加密的授权认证密钥 Ikn 的数据相连的装置 0，1，2 和 3 所拥有的节点密钥，一个可以解码升级的节点密钥 K（t）00 的 EKB 被生成，接着生成的 EKB 被分别发布给装置 0，1，2 和 3。通过首先解码接收到的 EKB，这些装置分别获取升级的节点密钥 K（t）00，随后，解码被获取的节点密钥 K（t）00 加密的授权认证密钥 Enc(K(t)00，Ikn))，从而使得可能最终获取授权认证密钥 Ikn。

即使当接收到一个相同的 EKB 时，其余的装置 4，5，6，7……分别不能一个经由 EKB 升级的节点密钥 K（t）00，由于利用它们分别的节点密钥和枝叶密钥。由于这点，就可能安全地唯一传送授权认证密钥给经过验证的正当装置。

在另一方面，图 35 例示了另外一个情形，其中基于由于例如密钥泄

漏的结果而已经定义装置 3 为撤销的判定的情形，一个只能为装置 0，1 和 2 所解码的 EKB 就被生成，接着发布给这些装置 0，1 和 2。在这个情形中，一个使能密钥块 EKB（a）和一个包含有为图 35 所示的节点密钥 K（t）00 所加密的授权认证密钥 Ikn（b）被分别发布到装置 0，1 和 2。

解码顺序如图 35 右面所示。首先，利用从接收到的 EKB 提取出的枝叶密钥和节点密钥，装置 0，1 和 2 分别通过解码自己的枝叶密钥和节点密钥而获取升级的节点密钥 K（t）00。随后，通过解码经过升级的节点密钥 K（t）00，装置 0，1 和 2 分别获取一个授权认证密钥 Ikn。

即使当接收到一个相同的 EKB 数据时，其余的装置 4，5，6，…… 通过施加它们分别的节点密钥和枝叶密钥获取经过升级的节点密钥 K（t）00。类似的，撤销的装置 3 不能通过施加自己的枝叶密钥和节点密钥获取升级的节点密钥 K（t）00。相应地，只有那些有认证的正当的权力的装置能够解码授权认证密钥给分别使用。

如上所述，通过利用 EKB 发布授权认证密钥，就有可能减少数据的体积并安全地发布能唯一被那些认证为正当权限方面的（人）所解码。进一步，这样一个经由发布在被 EKB 数据加密之后付送的 EKB 数据的发布的授权认证密钥受版本的控制，从而使得它可能执行一个每版本的更新处理，因而它也有可能基于选择的时间撤销任意装置。

由于以上的用来经由应用 EKB 的处理过程付送授权认证密钥的处理过程，任何撤销的装置（如再生装置）不能和相应的储存设被实现相互的授权认证密，从而使得它实际上不可能发生非法的数据解码。

进一步，通过经由应用 EKB 的处理过程传送授权认证密钥，也可能正当地控制储存和再生数据，不能到任何除开储存卡（如装载到再生装置的硬盘）的记录介质中。

如早先参照图 28 和 30 所述的，为了通过应用一个存储装置执行记录和再生内容数据的处理过程，相互的授权认证处理过程被按时地执行。作为结果，基于相互的授权认证处理过程被按时地执行的条件，记录和再生相关数据被正当执行。相互的授权认证处理过程在如储存卡等能够执行相互的授权认证处理过程的装置之间有效地执行。另一方面，在储存和记录数据到没有基加密功能的存储装置（如装载到再生装置的不能执行相互的授权认证处理过程的硬盘和 CD-R(可记录 CD)）或从它们储存和记录时，执行相互的授权认证处理过程就没有意义。然而，这一独到的系统使得即

使在利用没有相互的授权认证处理过程能力的再生装置储存或再生数据数据的情形时，授权认证程序也被执行。由于硬盘和 CD-R 分别没有执行相互的授权认证处理过程能力，也做出这样的安排，一个虚拟的储存卡（“Memory Stick”Sony 公司的产品和注册商标）被装载到各个存储装置，以使得相互执行的授权认证处理过程在“Memory Stick”和再生装置之间执行以建立相互执行的授权认证相容的条件，从而使得可以储存数据到一个没有执行相互的授权认证处理过程能力的存储装置和从这一存储装置再生数据。

图 36 表示了一个描述通过应用虚拟储存卡记录和再生数据的序列处理过程的流程图。起始，相应的再生装置和装入的储存卡执行一个相互的授权认证处理过程。当进入步骤 S3502 时，再生装置辨认是否已经执行一个相互的授权认证处理过程。随后，基于应经执行相互的授权认证处理过程的条件，进入步骤 S3503，在这一步骤中，应用没有相互的授权认证功能的硬盘、CD-R、DVD 执行记录和再生数据。

当进行步骤 S3502 时，加入辨认到相互的授权认证处理过程已经失败，相应步骤 S3503 的应用没有相互的授权认证功能的硬盘、CD-R、DVD 无论记录还是再生数据都不被执行。

以上所述的预先装载入的有相互的授权认证功能的虚拟储存卡前面以经参照图 16 描述。进一步，也以作出这样的安排，对再生装置有用的授权认证密钥由以上所述的 EKB 提供。

如上所述，通过促成 EKB 付送对再生装置有用的授权认证密钥，就可能唯一地为有正当授权的再生装置提供一个能够和相应的虚拟储存卡交换相互的授权认证的授权认证密钥。一个没有使能授权认证密钥的再生装置不能实现相互的授权认证，结果，一个撤销的再生装置就不能正当地通过利用有授权认证功能的储存卡（如没有授权认证功能的硬盘、CD-R、DVD）记录和再生数据，从而可能阻止任何不当的装置非法记录和再生数据。

具体地说，在那些分别构成分层树状密钥结构的枝叶的数据处理装置中，提供的授权认证密钥的 EKB 只能唯一被有正当授权的数据处理装置所解码，从 EKB 不能为不当的没有正当授权的数据处理装置所解码。这一安排阻止了一个不当的数据处理装置和装载入不当的数据处理装置的虚拟储存卡交换授权认证。因而实现了一个能构阻止不当的数据处理装置非

法利用内容数据的授权系统。

[完整性检测值（ICV）的构成]

随后，一个辨识实际已经发生窜改内容数据或缺失这一条件的状态的系统描述如下，这一处理过程通过检查相应的内容数据的完整性检测值（ICV）而实现阻止内容数据非法被窜改。

例如，用来检测窜改内容数据行为的完整性检测值通过基于等式 ICV=Hash（Kicv，C1，C2……）对内容数据应用 Hash 函数计算而得。Kicv 表示一个生成完整性检测值的密钥。C1，C2 分别表示内容数据。为实现以上的等式，信息授权认证码 MAC 被利用以认证内容的重要数据。象先前描述的信息授权认证码 MAC 也被包含在参照图 21 所述的 ATRAC-3 数据文件中。通过利用以上的数据和 MAC，计算完整性检测值的操作被执行。

图 37 标示了一个利用 DES 加密处理过程生成以上所述的 MAC 值的示例。如图 37 所示，目标信息被分成包括 M1，M2……Mn 等 8 字节的单元。第一步，初始值 IV 和分成的信息 M1 被一起执行一个异或操作，从而生成结果值 I1。随后，结果值 I1 被加入 DES 加密单元，它在生成输出值 E1 之前通过时间密钥 K1 而加密。随后，输出值 E1 和分成的信息 M2 被一起执行一个异或操作，从而生成结果值 I2。随后，结果值 I2 被加入 DES 加密单元，它在生成输出值 E2 之前通过时间密钥 K1 而加密。这些序列的处理过程被重复直到所有的分成的信息全部被加密。最终的输出值 EN 包含“信息授权认证密钥”MAC。为了建构以上的信息，允许使用构成内容相关数据的部分数据，如内容数据和标题数据，作为以上授权认证处理的目标。

通过向以上所述的 MAC 值应用 Hash 函数以认证信息内容，和向以上所述的密钥 Kicv 应用 Hash 函数以生成完整性检测值（ICV），ICV 值就被生成以检测内容数据的整体性。在比较一个在生成内容数据的同时生成的不验证窜改行为的 ICV 值和另一个新近基于内容数据生成的 ICV 值之后，假如一个完全相同的 ICV 值被生成，就验证了没有对内容数据的窜改动作。相反的，假如 ICV 的结果值互不相同，就表明了内容数据实际已经被窜改。

通过应用多个经由和各个内容数据相应生成的信息授权认证代码 MAC，就有可能生成一个单一的完整性检测值（ICV）。例如，一个完整

性检测值（ICV）通过应用与下面所示的等式相应的多个 MAC 值等计算出。

ICV=HASH(Kicv，C_MAC[0]‖ C_MAC[1]‖ C_MAC[2]……)

首先，一个和生成内容数据同时生成的完整性检测值（ICV）被储存。这一 ICV 值和另一个在检测内容数据的完整性生成的 ICV 值比较。假如两个值相互一致，就表明没有内容数据的窜改动作。相反的，假如两个值互不相同，就表明实际有一个内容数据的窜改动作，因而有必要需要一个限制再生内容数据的装置。

不单是音乐数据，储存卡等存储装置也储存各种数据包括图片数据，游戏程序数据，或者其他的各种目录下的类似数据。为了阻止这些内容数据被非法窜改，就能有效地个别地为每个目录生成以上所述的完整性检测值（ICV），以被储存。

然而，相关储存在存储器中的内容数据的数目的增长，也带来一个困难，难以基于正当的内容数据生成授权认证所需的检测值并储存和控制检测值。实际上，在用包括版含闪存的储存卡等有更大的储存能力的记录介质升级记录介质时，那些诸如音乐数据，图片数据，程序数据和类似的处在各种目录下的内容数据被联合储存在存储器中。在这样一个情况的条件下，就难以正当地控制生成和储存 ICV 值，并辨识内容数据的窜改的处理过程。就有必要执行一个生成检测值以免整个的数据被检测的处理过程。例如，当通过应用如通过 DES-CBC 模式生成的信息授权认证代码 MAC 计算完整性检测值（ICV）时，就有必要执行一个将整个的数据以 DES-CBC 模式处理的处理过程。相应数据长度的扩展而来的计算体积的增长，结果导致产生处理效率的问题。

每一个储存卡作为一个储存有各种目录底下的各种数据的存储装置。通过经由生成一个完整性检测值（ICV）而执行一个检测各种目录底下的内容数据的窜改动作的处理过程，就可能在检测值 ICV 时或在检测 ICV 值和数据时新生成一个合检测值（ICV），通过以一个目录内的特定的数据为目标而不影响其它的目录。一个按每隔目录储存储存多个完整性检测值（ICV）的系统被描述如下。

图 38 表示了储存在存储装置中的数据的结构和一个储存与这些数据相关的完整性检测值（ICV）储存状态的示例。如这里所示的，储存在储存卡的闪存的音乐数据目录包括多个包含加密的内容数据的 ATRAC-3 数

据文件（A3D）。另外，多个属于许多目录的内容数据（#1 到#n）被储存在闪存中。多个目录包括音乐数据，图片数据，游戏程序和类似的数据。也可能控制类似的图片数据为一个独立的分类作为另一个和个别的数据提供商相关的目录。

也可能建立一个以上所述的 EKB 的控制单元（实体）作为一个单独的目录。换句话说，允许一个内容数据的集合作为一个单个的目录，一个被从某个 EKB 获取的密钥加密密钥（KEK）解码的内容密钥（Kcon）可以被应用到其中。

多个再生控制文件（PBLIST）和 ATRAC-3 数据文件（A3D）中的每一个包含有检查内容数据的窜改动作的信息授权认证码（MAC）。基于 MAC 码，完整性检测值（ICV）被生成。多个相应内容数据的 MAC 值被储存在闪存的序列的页中，并且，通过应用基于 MAC 列表而生成 ICV 密钥而获得的完整性检测值（ICV(con)）也被储存在再生控制文件（PBLIST）和 ATRAC-3 数据文件（A3D）中。

图 39 标示了用来储存检测内容数据的信息授权认证码 MAC 的序列页的格式。序列的页面域被提供来禁止写入常规的内容数据到其中。图 39 所示的序列页面的组成描述如下。

内容密钥 E（Kstr，Kcon）一个储存卡的储存密钥所加密。上面和下面的 Ids 分别储存储存卡的识别成分（ID）。相应 MAC 值的码 C_MAC[0]基于上面的再生控制文件（PBLIST）的组份数据而生成。例如，基于基于以上的 ATRAC-3 数据文件#1 而生成 MAC 值，每个内容数据的分别的 MAC 值储存在 C_MAC[1]值。基于这些 MAC 值，完整性检测值（ICV(con)）被生成，接着通过序列协议被写入存储器。为了处理各不相同的密钥系统，优先的是各个密钥系统生成的各个 ICV 值应该被储存到各不相同的特定区域。

为每一目录生成的用来检测每一个目录的内容数据的窜改动作的完整性检测值 ICV 被储存在储存卡的闪存的一组页面中。组页面包含有一个禁止写入常规的数据的域。

图 40 标示了储存每个目录的完整性检测值 ICV 的组页面的格式。码#0_revision 被提供一个目录#的更新日期。无论何时更新日期被升级时，一个增加过程被执行。码#0_version 相应一个目录#0 的版本。码#0_E(KEK，Kicv)相应一个被相应的目录#0 的密钥加密密钥（KEK）加密的 ICV 生成

密钥（Kicv）。码 ICV0 表示相应目录#的完整性检测值 ICV。也以作出这样的安排，类似的数据可以被储存到每个目录的组页面直到#15。

通过完整性检测值检测内容数据的实际情况的处理过程在电源被打开或如储存卡等储存装置被装载到相应的再生装置时被执行。图 41 标示用 Icv 值的检测处理过程的流程图。

首先，当再生装置检测到电源被打开或一个新的储存卡被装入时，进入步骤 S4001，在这一步骤中，识别是否相互的授权认证可以在再生装置和储存卡之间执行。假如识别到可以执行，进入步骤 S4002，在这一步骤中，一个相互认证再生装置和储存卡的处理过程被执行（参照图 29）。另一方面，当步骤 S4001 在进行中时，假如识别到在再生装置和储存卡之间的相互的授权认证不可执行，进入步骤 S4003，在这一步骤中，一个相互认证在再生装置和以上所述的虚拟储存卡的处理过程被执行。

当步骤 S4004 在进行中时，它识别是否相互的授权认证已经在再生装置和储存卡之间执行。假如它们之间的相互的授权认已经失败，所有的处理因此被终止不再执行。假如它们之间的相互的授权认已经实现，进入步骤 S4005，在这一步骤中，计算完整性检测值 ICV。如先前所述的，ICV 值基于用来检测内容数据完整性的信息授权认证码（MAC）而计算。

当以经进入下一步骤 S4006 时，经由计算生成的 ICV 值被和另一个先前储存的 ICV 值比较。当它们相互相同时，就表明没有内容数据的窜改操作，从而操作模式进行到步骤 S4007，在这一步骤中，各种操作被执行，包括再生内容数据。另一方面，假如以上的 ICV 值相互不同，就表明有窜改内容数据的动作，从而终止所有的处理，因而没有执行数据再生。通过顺次执行以上的处理，内容数据就可以被阻止被非法窜改，从而可能撤销被非法窜改的数据。

如上所述，控制性地生成多个对每个目录独立的完整性检测值 ICV，当检测各个 Icv 值时或当修改各个 Icv 值时或当相关内容数据的改变生成新的 Icv 值时，由可能只检测对某一个单个的目录的内容数据的 ICV 值，而不影响其它目录中的数据。

[扩展的 MAC 码的结构]

作为一个生成信息授权认证码（MAC）（用以检测先前通过参照以上所述的再生控制文件和储存在 ATRAC-3 数据文件中的内容数据描述的内容数的完整性）的处理过程的变化的例子，也作为一个储存以上的相应

数据文件的数据的处理过程的变化的例子，用来生成和储存一个扩展版本的 MAC 码的处理过程描述如下。

图 42 示例了生成和储存扩展版本的 MAC 码的处理过程。图 42 标示了图 21 和 23 所示的 ATRAC-3 数据文件的部分。信息授权认证码（MAC）相应于基于相应的多个如 ATRAC-3 数据文件中的数据目录的一些数据经过图 37 所示的处理过程而生成的值。通过比较预先储存在数据文件中的 MAC 值和在检测过程中生成的另一个 MAC 值，辨认了是否有一个窜改内容数据的动作的证据。

例如，那些储存在图 42 所示的 ATRAC-3 数据文件中的信息授权认证码（MAC）和那些通过 MAC 值检验完整性的内容数据相关，这些内容数据被划分为从“INF-seq#”开始的多个数据目录。那些 MAC 码预先基于被通过相应的储存在相应的数据文件中的 MAC 代码处理的数据目录而生成。具体地说，这一条件被表述为 MAC（INF-seq#||A||LT……）。在括号内的内容数据被通过 MAC 码执行检测处理过程，换句话说，这些内容数据被接收检测判定是否实际被窜改。

然而，有这样一种情形，有多个内容数据储存在每个 ATRAC-3 数据文件中，因而要检查完成性的内容数据可能增长很多。为了应付这一问题，假定有多个新近的 MAC 码和增加的数据相连生成，以接收检测，因而构成了扩展版本的 MAC 码。扩展的 MAC 码被储存在每个数据文件中。那些只生成来处理常规的接收完整性检测的原始的 MAC 码只处理不变的目标域，以检测相关数据的完整性。这以安排被描述如下。

如图 42 所示，一个用来检测以上所述的数据目录“INF-seq#”下的数据的完整性的原始 MAC 码 701 被生成，原始 MAC 码 701 被储存在 ATRAC-3 数据文件中。

进一步，在一个受检测连续性的内容数据置于多个记录在 ATRAC-3 数据文件的 INF 空间的情形下，基于所有的经受检测在 INF 空间的连续性的数据（包括相应于一个成为生成初始的 MAC 701 的 MAC 代码的目标的数据的以上所述的数据目录“INF-seq#”），这样一个 MAC 代码新近相应它们而生成。那些新生成的 MAC 代码被储存在相应的数据文件作为扩展版本的 MAC 代码。

图 42 所示的扩展 MAC 代码[MAC(INF)]720 被根据如下所示的规则生成：

MAC(INF-seq#||path|| MAC(profile)||others……)

如上面的规则清楚表明的，扩展版本的 MAC 代码包含部分的数据作为初始 MAC 码的代数的目标，然后，扩展版本的 MAC 码基于一个和别的数据复合以接收整体性检测的数据而生成。

进一步，在重写扩展的 MAC 码的过程中，换句话说，作为重新写这些数据在相应的扩展 MAC 数据的 INF 域中的“path”之下的结果，基于重写的数据，新的可扩展的 MAC 数据再次被生成和储存。那些在“path”之下的数据也被包括在扩展的 MAC 码中。进一步，作为初始 MAC 码的结果目标的“INF-seq#”也被重写，从而使得新的扩展 MAC 码被生成和储存。

在这种情形下，由于作为初始 MAC 码的结果目标的数据“INF-seq#”已经被重写，初始的 MAC 码新近被计算。换句话说，无论何时更新扩展 MAC 码时，重新生成和重新储存初始的 MAC 码也相连被执行。

也有可能通过生成新的随机数或通过由此而来的增加处理过程而重写以上的 INF-seq#数据。

以上的安排使得能够与那些包括初始 MAC 的部分的 MAC 目标数据一起出现 MAC 目标数据，这一 MAC 目标数据在相应的用来检测内容数据的完整性的增加的数据而生成的扩展 MAC 码的 MAC 目标数据中。作为结果，可能始终反映重写数据在 INF(作为新的基于初始的 MAC 码检测内容数据的整体性的数据，而不引致初始 MAC 码的 MAC 目标数据域被扩展)中的处理过程。

[应用 EKB 到存储装置和再生装置之间的解码处理过程]

随后，一个具体的获取一个内容密钥的处理过程被描述如下。这一内容密钥可用来通过施加以上所述的分层树状密钥结构的密钥发布系统而经由利用以上所述的 EKB 而解码经过加密的内容数据。

图 43 标示了一个如“存储棒”等存储装置 800，它内在储存有经过加密的内容数据（如 ATRAC-3 数据）和一双用来执行内容数据再生的再生装置 810 和 830。

存储装置 800 储存包含以上早先参照图 21 描述的经过加密的内容数据的 ATRAC-3 数据文件。为了使得再生装置 810 和 830 能够分别再生内容数据。就必须获取一个用来解码经过加密的内容数据所需的内容密钥（Kcon）。

首先，通过参照存储装置 800 和图 43 所示的再生装置 A810，一个使得再生装置 A810 能够直接从存储装置 800 获取内容密钥的处理过程描述如下。首先，存储装置 800 和再生装置 A810 相互在相互执行的授权认证处理过程的公共控制模块 801 和 811 之间执行一个授权认证处理过程。相互的授权认证处理过程被基于应用加密格式的公共钥或先前参照图 8 所述的应用加密格式的公开密钥而执行。在这种情形中，本质需要的是控制存储装置 800 的控制模块 801 和 811 和再生装置 A810 应该分别包含一个用来执行授权认证处理过程的算法和储存有一个授权认证处理过程所需的密钥。

在和以上的再生装置 A810 实现一个相互的授权认证之后，存储装置 800 提取出被储存密钥（Kstm）加密的内容密钥 E（Kstm，Kcon）和另一个被密钥加密密钥（KEK）加密的内容密钥 E（KEK，Kcon）（这一密钥可以通过一个利用储存在存储装置 800 中的闪存 802 的 ATRAC-3 数据文件中以上所述的 EKB 的处理过程而获取），随后，在最终获取内容密钥（Kcon）之前提取出内容密钥。

随后，利用一个在再生装置 A810 之间执行的相互的授权认证处理过程中生成的区间密钥（Kses），存储装置 800 再次加密内容密钥（Kcon），接着传送生成的加密数据 E（Kses，Kcon）到再生装置 A810。在再生装置 A810 的控制模块 811 在最终获取内容密钥（Kcon）之前解码接收到的内容密钥 E（Kses，Kcon）。

基于以上的序列处理过程，存储装置 800 最初解码和提取内容密钥（Kcon），随后，在再次用一个区间密钥（Kses）加密内容密钥（Kcon）之后，存储装置 800 付送内容密钥（Kcon）到再生装置 A810。

在存储装置 800 方面没有解码处理过程被执行，只有再生装置 A810 获取内容密钥（Kcon）。一个实际的执行这些处理过程的形式被描述如下。

参照图 43，在存储装置 800 和再生装置 B 830 之间执行的处理过程描述如下。首先，存储装置 800 指定一个用来从储存在 ATRAC-3 数据文件中的 EKB 的版本（或代数）中获取内容密钥（Kcon）的 EKB，随后，付送指定的 EKB 到储存密钥（Kstd）B 830。

在从存储装置 800 接收到指定的 EKB 的情况下，再生装置 B 830 在最终获取密钥加密密钥（KEK）之前，通过施加先前储存在再生装置 B 830 的闪存 E2PROM 中的装置密钥块（DKB）处理接收到的 EKB。

参照图 44，装置密钥块（DKB）的结构描述如下。如先前所描述的，那些为内容数据再生装置 B 830 提供的装置分别包含一个基于图 44 中(a)所示的分层树状密钥结构的密钥发布系统的终止成分，换句话说，内容数据再生装置的每个装置包含相应于连接到从枝叶到上一个层的根的单个节点的密钥。例如，一个相应于图 44 中（a）所示的终止节点的 SET 5 的装置包含从枝叶密钥 K101、节点密钥 K10 和 K1 到根密钥（Kroot）的密钥集，或包含一个到子目录节点密钥的密钥集，或包含一个到目录节点的密钥集。

以上所述的密钥分别被相应的装置所加密，并被储存在如闪存 E^2PROM 中。以上所述的装置密钥块（DKB）包含多个经过加密的密钥集，每个经过加密的密钥集分别对应于从储存在每个装置的枝叶到一个特定的包含如子目录字节等的节点的多个密钥、或从上述枝叶到根的多个密钥。

图 44 在（b）中例示了储存在装置密钥块（DKB）的数据的结构。如这里所示的，相应于一个加密密钥块的装置密钥块（DKB）包括一个包含分别枝叶密钥所加密的节点密钥和根密钥的数据和一个包含被一个装置（如再生装置）的储存密钥（Kstd）所加密的枝叶密钥的数据。通过使用储存密钥（Kstd），再生装置解码储存在装置密钥块（DKB）中的 Enc（Kstd，Kleaf），接着获取枝叶密钥（Kleaf），从而，就可能使再生装置直接解码通过应用得到的枝叶密钥（Kleaf）解码上一层的经过加密的节点密钥和经过加密的根密钥。从而，就可能通过序列解码在 EKB 中的低一层的密钥而获取高一层的密钥。装置密钥块（DKB）也包含一个枝叶标识成分“leaf ID”。

那些对每一装置正当的密钥各个装置之间互不相同。这些储存密钥也可以预先储存在一个安全的存储器中（如示为 SAM 的），或者被安排能基于枝叶 ID 而获取。具体地说，也允许通过基于和预定的集单元一起储存在主密钥（Kmas）而施加 Hash 函数到枝叶 ID 而建立一个以 Kstd=Hash（Kmas，leaf ID）表述的表格。

再次参照图 43，获取内容数据的处理过程进一步描述如下。在从存储装置 800 接收到 EKB 之后，通过施加经由解码储存在控制模块 831 中的存储器 832 中的装置密钥块（DKB）而生成的节点密钥和根密钥，再生装置 B 830 获取一个被 EKB 加密的密钥加密密钥（KEK）。

处理 EKB 的方法和先前参照图 5 或 9 描述的方法相同。

通过利用以上所述的通过处理 EKB 而生成的密钥加密密钥（KEK）和执行解码从存储装置 800 接收到的经过加密的内容密钥 E(KEK，Kcon)，再生装置 B 830 最终获取一个内容密钥。

储存在图 43 所示的再生装置 B 830 的存储器 832（E2PROM）中的初始的 EKB 和最初储存在再生装置 B 830 的简化 EKB 文件相应。实际上，初始的 EKB 版、包含一个公共储存在一些装置中的经过加密的密钥块，这些装置相应与一个与早先参照图 11 描述的目录节点的单个目录节点（比如包含“存储棒”）的低层的节点节点相连的枝叶。

假如这样一个被目录节点所拥有的密钥相应于 K01（举例），也认为被 K01 加密的根密钥 Enc（K01，Kroot）被储存为初始的 EKB。作为处理初始的 EKB 的结果，就可能使得再生装置 B 830 获得根密钥。例如，在一个再生装置 B 830 接收到一个被根密钥加密的储存有密钥加密密钥（KEK）的 EKB 的情形下，就可能使得再生装置 B 830 通过应用经初始 EKB 生成的根密钥而获取密钥加密密钥（KEK）。

不只是一个付送初始的 EKB 到属于用一个目录节点相互一样的装置的系统，也允许提供初始的 EKB 给多个目录节点。例如，假设“存储棒”目录节点的节点密钥被定义为 K01，包含有再生内容数据的功能的个人计算机的目录节点的节点密钥被定义为 K10，能够使用网络服务线路的再生装置的目录节点的节点密钥被定义为 K11，通过在付送到市场之前预选安装储存有三种经过加密的根密钥（包括 Enc（K01，Kroot），Enc（K10，Kroot）和 Enc（K11，Kroot））的初始的 EKB，就可能发布可以被互不相同的装置所使用的经过加密的内容数据。

图 45 例示了一个再生装置，它包含一个整合储存有装置密钥块（DKB）的闪存（如 E2PROM）和一个影响内容数据的自我记录和再生的初始的 EKB。图 46 例示了一个通过利用以上的所述的密钥块获取内容密钥的处理过程。

图 45 所示的结构描述如下，图 45 所示的装置（例如包括一个记录/再生装置）和图 45 中（a）所示的枝叶相容。这一装置属于分层树状密钥结构的第八目录节点 Kn8 的目录。这一装置储存多个包含如图 45 中（b）所示的从 Enc（Kstd，Kleaf）到 Enc（Kleaf，Kn8）的装置密钥块（DKB）。这一结构和前面描述的 DKB 相同。那些储存在这一装置中的数据在被一个枝叶密钥所加密之后，分别构成从节点密钥 Kn47 到正处于枝叶密钥上

面的目录节点密钥 Kn8 的密钥。

这些装置进一步包括一个可用来自我记录和自我再生的 EKB。在记录和再生内容数据时，通过处理 EKB 和可用到自我记录和自我再生处理过程的装置密钥块（DKB），装置获取内容密钥（Kcon），从而执行解码的加密内容数据。

图 46 表示了一个流程图，它描述了在获取内容数据的过程中被一个包含有 EKB 和图 45 中（b）所示的 DKB 部分的装置所执行的序列步骤。当进入初始步骤 S4601 时，基于枝叶 ID 数据，装置提取出一个储存密钥（Kstd）。装置基于枝叶 ID 数据从包含其中的安全的存储器中提取储存密钥（Kstd），或者装置基于前面描述的主密钥（kmas）和枝叶 ID 数据计算储存密钥（Kstd）。

随后，进入步骤 S4602，在这一步骤中，基于储存密钥（Kstd），装置处理装置密钥块（DKB），用另外一句话说，解码 Enc（Kstd，Kleaf）从而获取一个枝叶密钥。随后，进入步骤 S4603，在这一步骤中，基于枝叶密钥，装置进一步处理装置密钥块（DKB），用另外一句话说，解码 Enc（Kleaf，Kn8）从而获取目录节点密钥。由于装置密钥块（DKB）储存有直接被枝叶密钥所加密的节点密钥，就可能直接从被枝叶密钥所执行的解码处理过程获取上一层的节点密钥。

随后，进入步骤 S4604，在这一步骤中，基于节点密钥 Kn8，装置处理 EKB 一序列地获得上一层的节点密钥，然后计算相应最上层的根密钥。随后，进入步骤 S4605，在这一步骤中，通过时间经过处理 EKB 获取的根密钥（Kroot），装置解码 Enc（Kroot，KEK）以获取密钥加密密钥（KEK）。最终，随后，进入步骤 S4606，在这一步骤中，使用获取的钥加密密钥（KEK），装置在最终获取内容密钥（Kcon）之前解码储存在附在内容数据的一个数据上的 Enc（KEK，Kcon）。

图 45 中（b）所示的 EKB 被唯一用来执行一个自我记录处理过程。然而，在一个下载多个内容数据到相应的装置的情形下，也实际可行联合下载指定的相应于预定的内容数据的 EKB，随后，和内容数据相应储存 EKB。进一步的，也可能对相应的在再生内容数据的时候下载的内容数据的 EKB 执行一个图 46 所示的操作。图 45 中（b）所示的装置密钥块（DKB）包含一个包含从上一层到第 8 节点 Kn8 的直接被枝叶密钥所加密的节点密钥。也允许同样地储存分布在更上层和更下层的节点密钥。

本发明已经通过参照特定的实现本发明的精髓的实践形式而清晰描述。然而，应该理解的是，本发明可以由本专业普通技术人员在一个不背离本发明的精神的范围内以对于本发明的修改和替代方式而进一步应用。换句话说，本发明被以示例的方式阐述，因而，本发明的范围没有被严格地解释。为了精确判断本发明的精髓点，应该参考本说明的后面说的权利要求的详细文本。

如上所述，根据用来处理本发明提出的各种数据的系统和方法，提供多个分别被多个 EKB 所加密的操作密钥，其中，EKB 包含各种加密升级密钥的数据，这些密钥处在构成分层的树状密钥结构的路径上，分层的树状密钥结构包含在相应的在从密钥述的根到枝叶的路径上的根、节点和枝叶而提供的密钥，密钥树包含多个装置作为枝叶。因而，以上提到的加密数据也包含有经由加密下层的密钥而加密上层密钥的数据。那些加密的密钥唯一使得选定的正当的装置可以解码经过加密的结果，从而实现一个用来正当地发布有高安全效果的内容数据的加密密钥或系统。

进一步，依据本发明，多个用于解码经过加密的内容数据的内容密钥被储存在内容数据的标题数据中。一个内容密钥被处理成被 EKB 所提供的加密密钥所加密的一个数据，而其它内容密钥被处理成被一个对存储装置正当的密钥所加密的一个数据。由于这样一个设计，无论何时操作这样一个装置再生内容数据时，内容数据被通过正当选择内容密钥的方式再生。

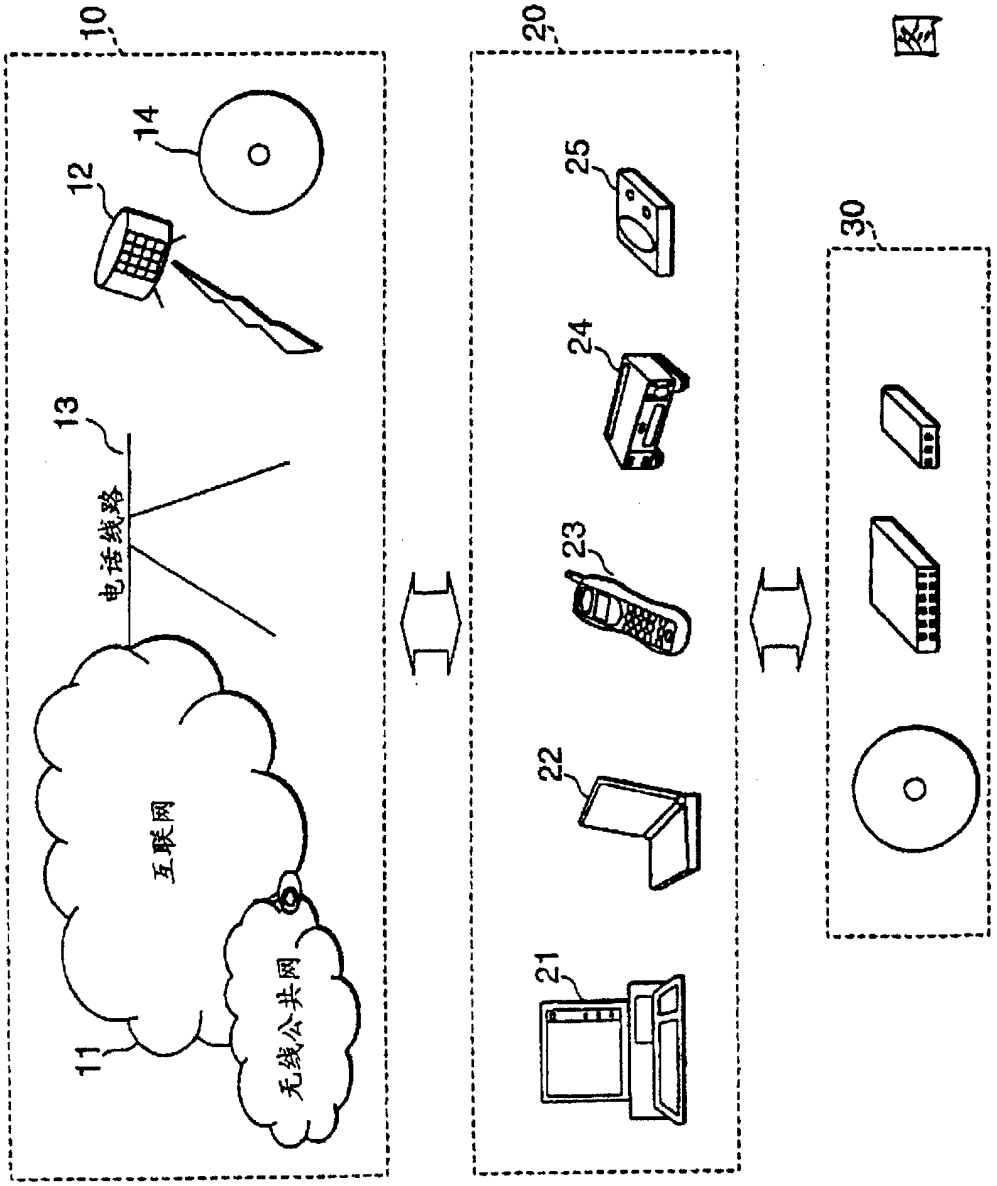


图 1

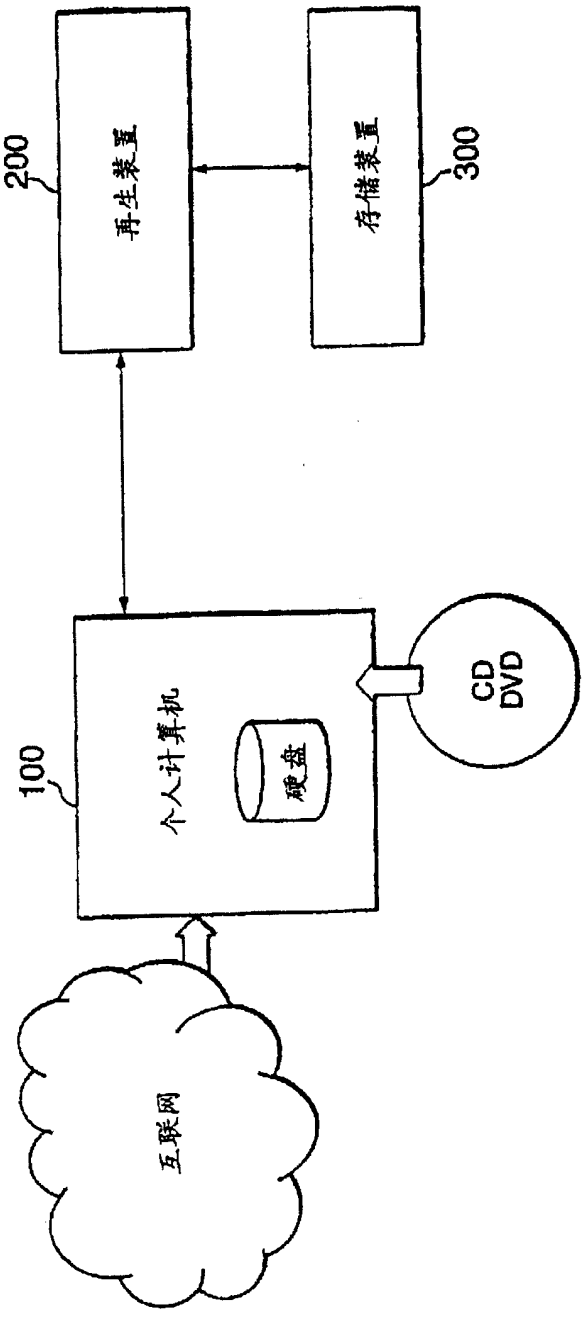


图 2

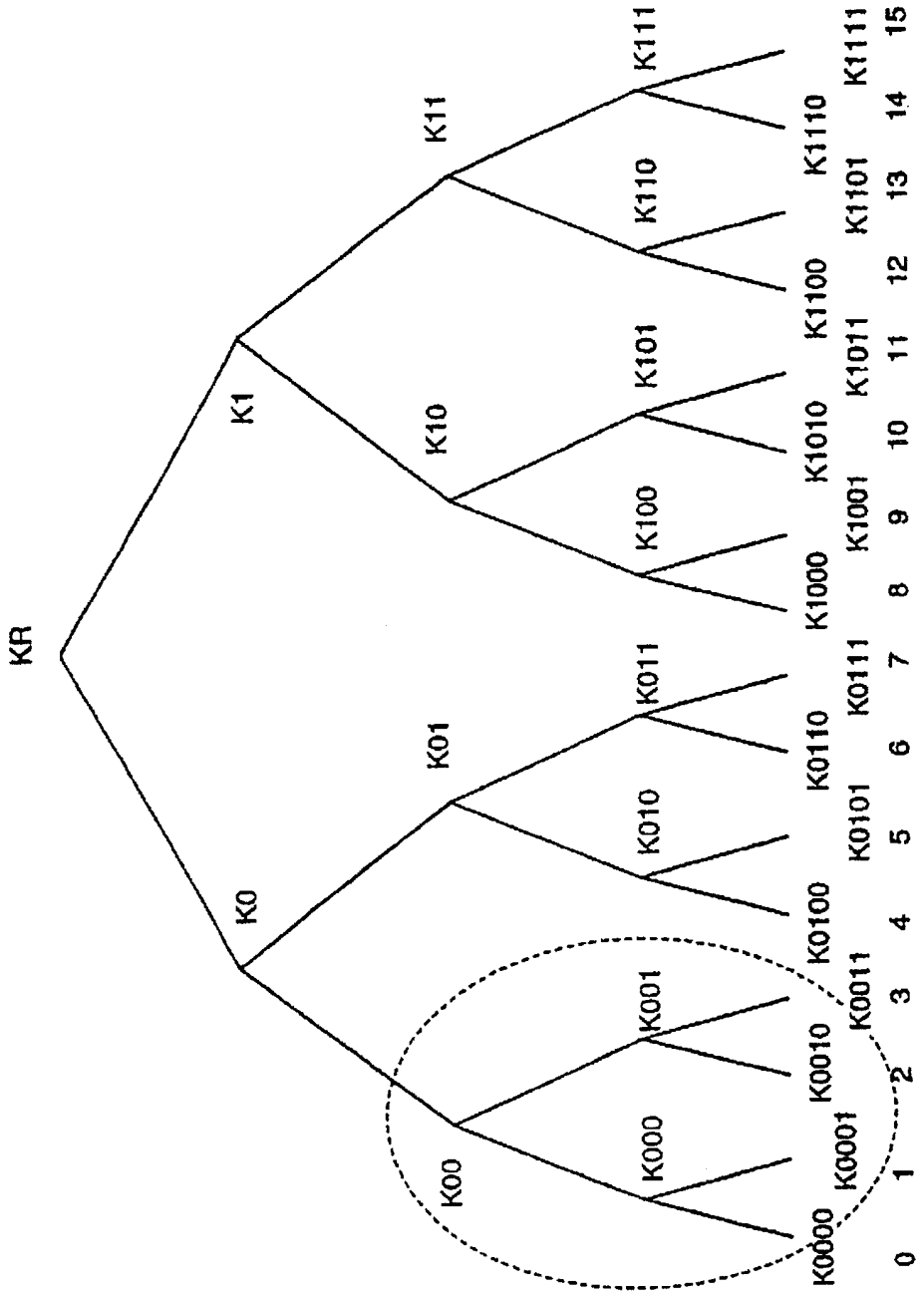

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
叶子

图 3

EKB (使能密钥块) 例1
对装置0、1和2付送(t)版节点密钥

(A)

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

EKB (使能密钥块) 例2
对装置0、1和2付送(t)版节点密钥

(B)

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

图 4

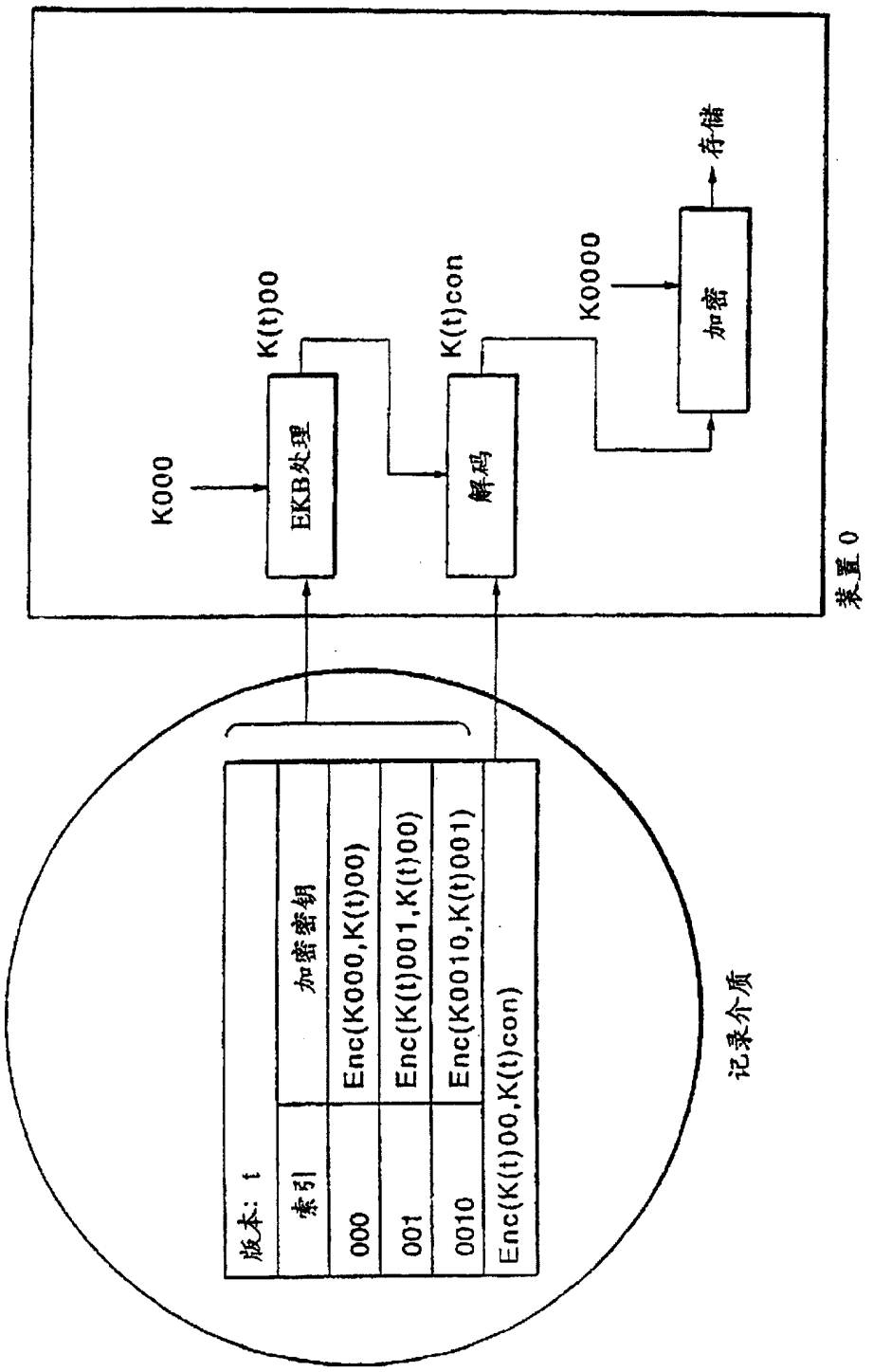

K000
EKB处理
K(t)00
解码
K(t)con
K0000
加密
存储
装置 0
记录介质
版本: t
索引
加密密钥
000
Enc(K000,K(t)00)
001
Enc(K(t)001,K(t)00)
0010
Enc(K0010,K(t)001)
Enc(K(t)00,K(t)con)

图 5

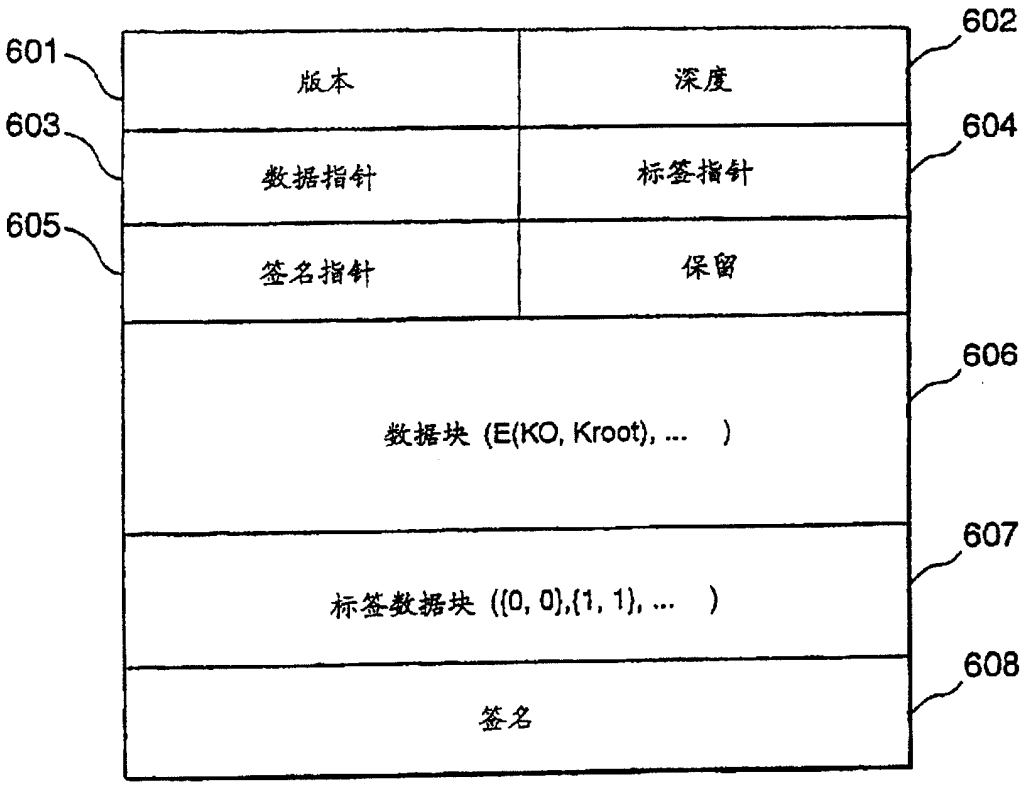

601
602
603
604
605
606
607
608
版本
深度
数据指针
标签指针
签名指针
保留
数据块 (E(KO, Kroot), ...)
标签数据块 ({0, 0},{1, 1}, ...)
签名

图 6

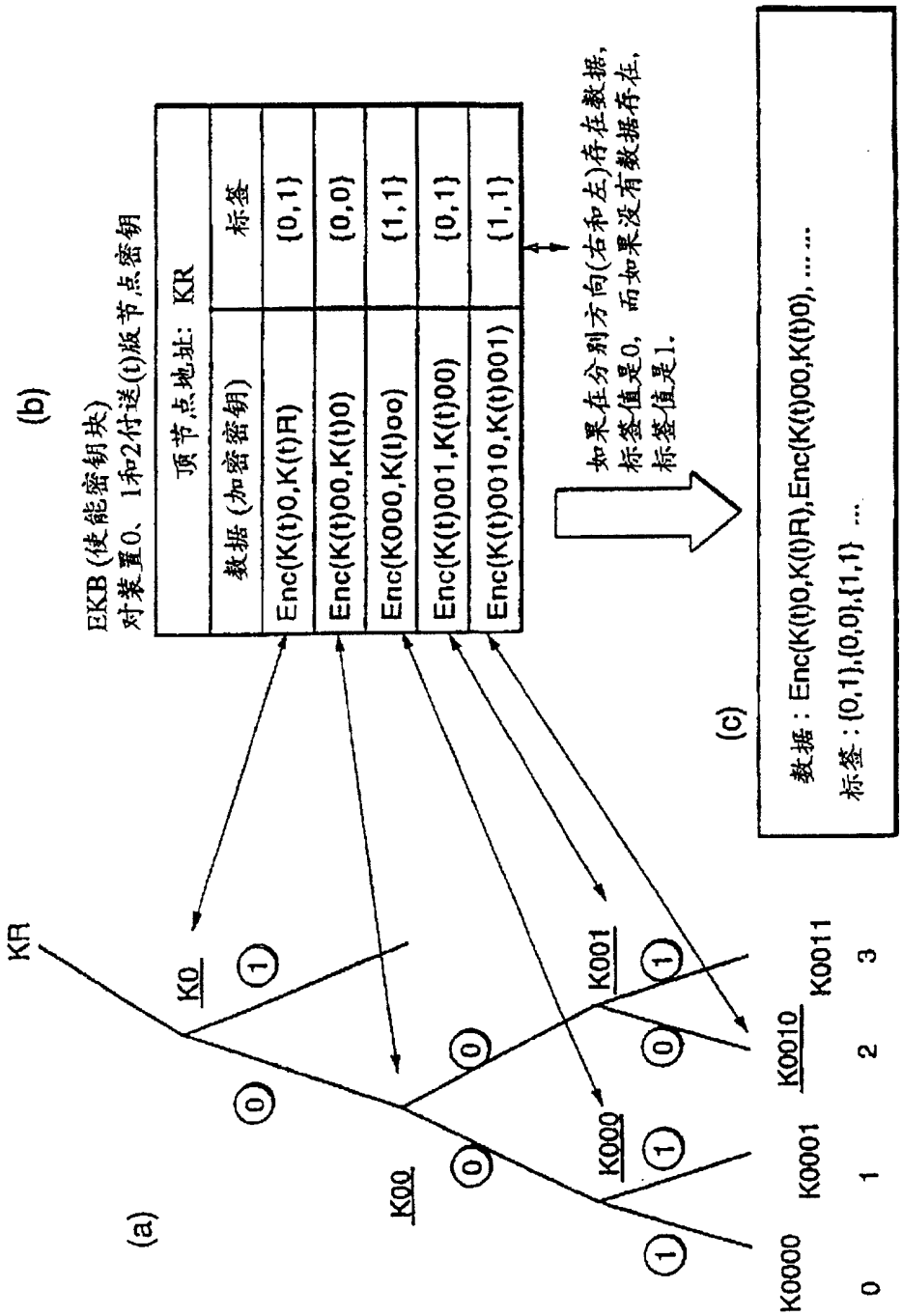

(a)
KR
K0
K00
K000
K001
K0010
K0011
K0000
K0001
0
1
2
3
(b)
EKB (使能密钥块)
对装置0、1和2付送(t)版节点密钥
顶节点地址: KR
数据 (加密密钥)
标签
Enc(K(t)0,K(t)R)
{0,1}
Enc(K(t)00,K(t)0)
{0,0}
Enc(K000,K(t)oo)
{1,1}
Enc(K(t)001,K(t)00)
{0,1}
Enc(K(t)0010,K(t)001)
{1,1}
如果在分别方向(右和左)存在数据,
标签值是0, 而如果没有数据存在,
标签值是1.
(c)
数据 : Enc(K(t)0,K(t)R),Enc(K(t)00,K(t)0), ……
标签 : {0,1},{0,0},{1,1} …

图 7

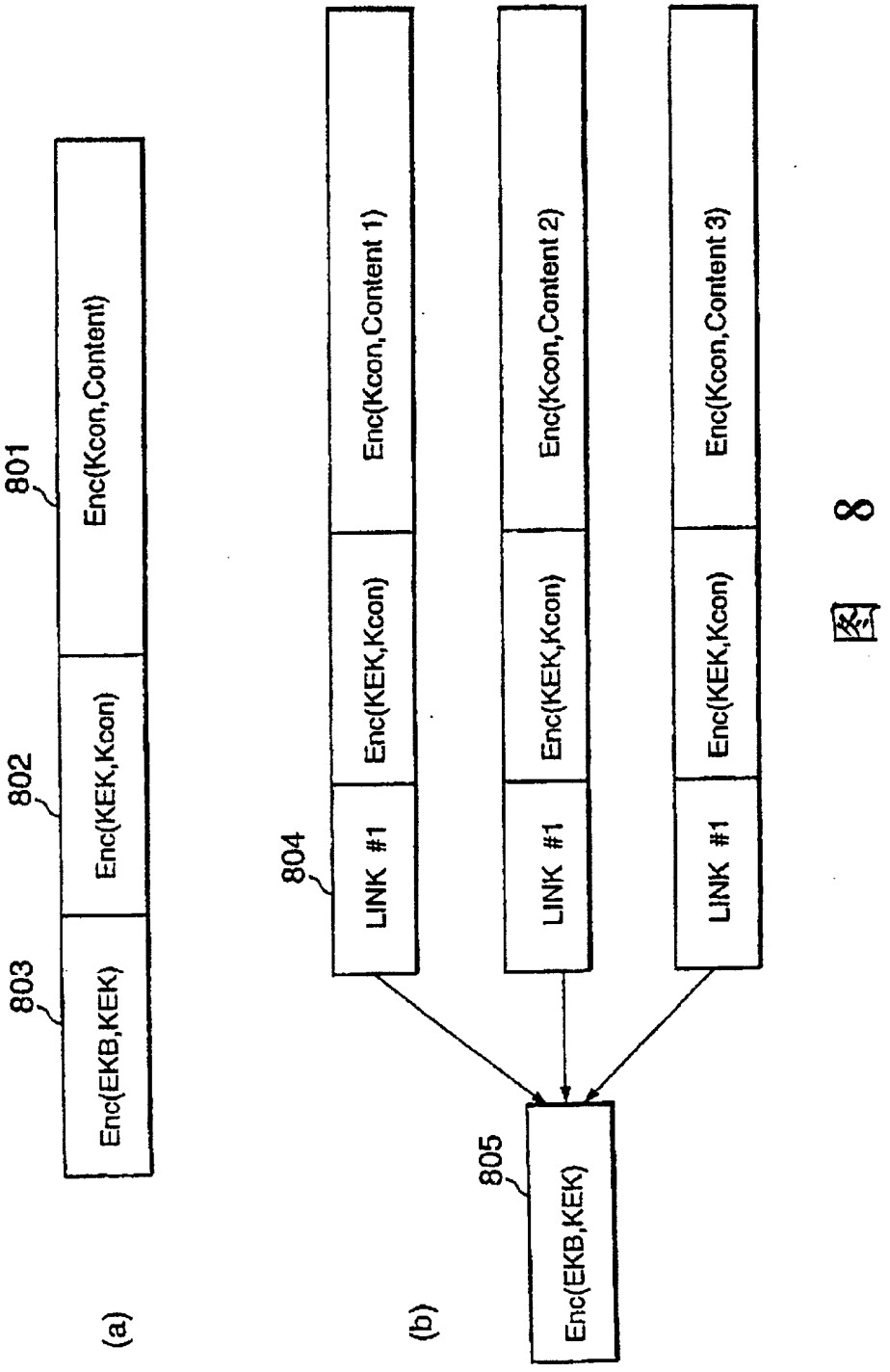

(a)
801
Enc(Kcon,Content)
802
Enc(KEK,Kcon)
803
Enc(EKB,KEK)
(b)
804
LINK #1
Enc(KEK,Kcon)
Enc(Kcon,Content 1)
LINK #1
Enc(KEK,Kcon)
Enc(Kcon,Content 2)
LINK #1
Enc(KEK,Kcon)
Enc(Kcon,Content 3)
805
Enc(EKB,KEK)

图 8

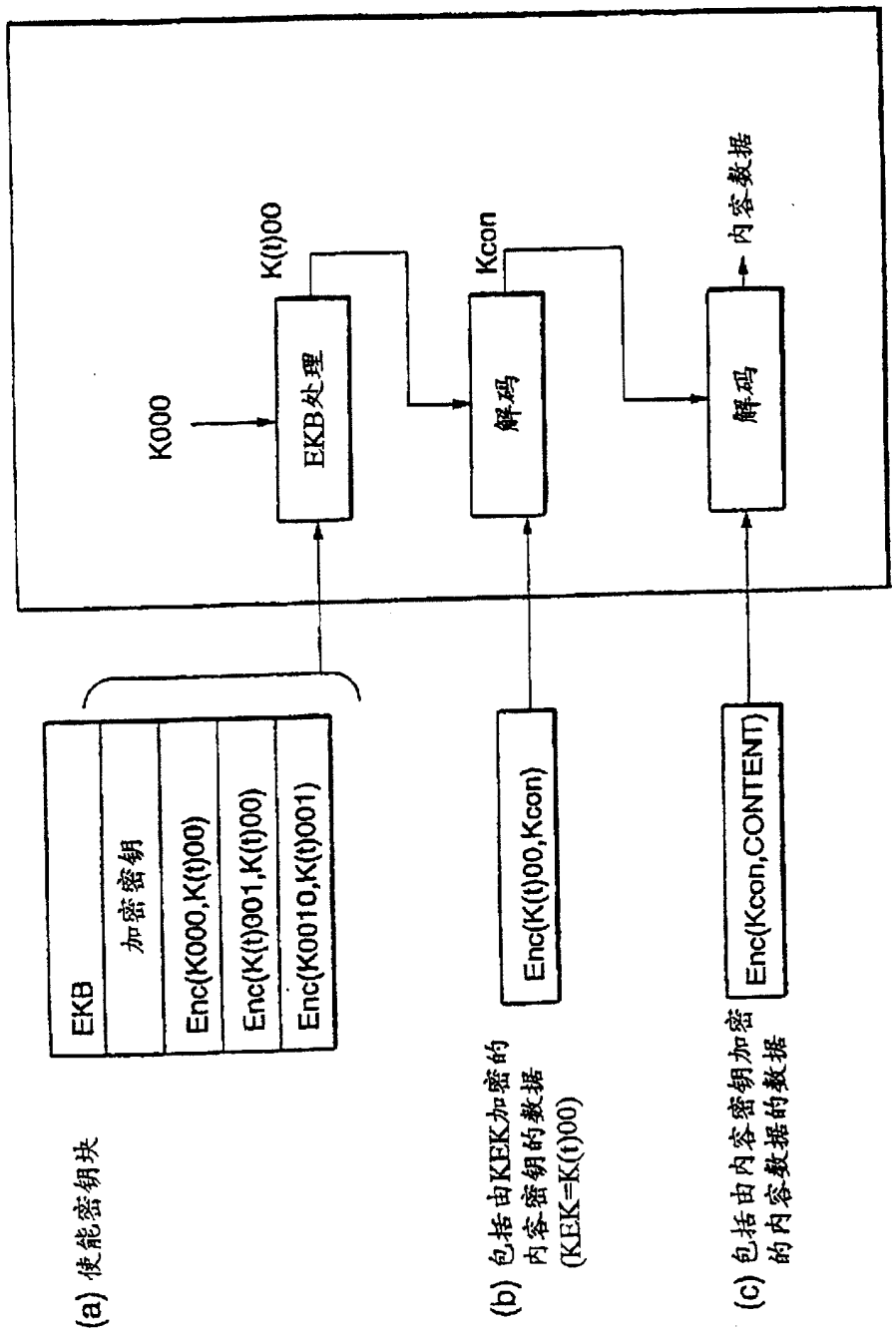

装置 0
K000
EKB处理
K(t)00
解码
Kcon
解码
内容数据
EKB
加密密钥
Enc(K000,K(t)00)
Enc(K(t)001,K(t)00)
Enc(K0010,K(t)001)
(a) 使能密钥块
Enc(K(t)00,Kcon)
(b) 包括由KEK加密的内容密钥的数据 (KEK=K(t)00)
Enc(Kcon,CONTENT)
(c) 包括由内容密钥加密的内容数据的数据

图 9

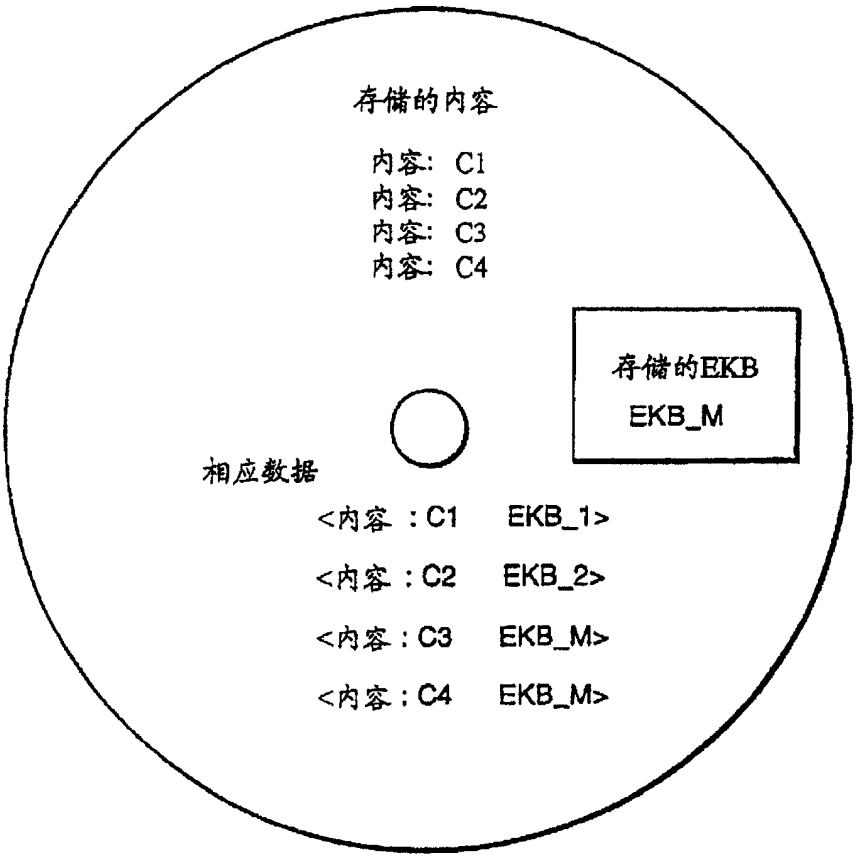

存储的内容
内容: C1
内容: C2
内容: C3
内容: C4
存储的EKB
EKB_M
相应数据
<内容 : C1 EKB_1>
<内容 : C2 EKB_2>
<内容 : C3 EKB_M>
<内容 : C4 EKB_M>
记录介质

图 10

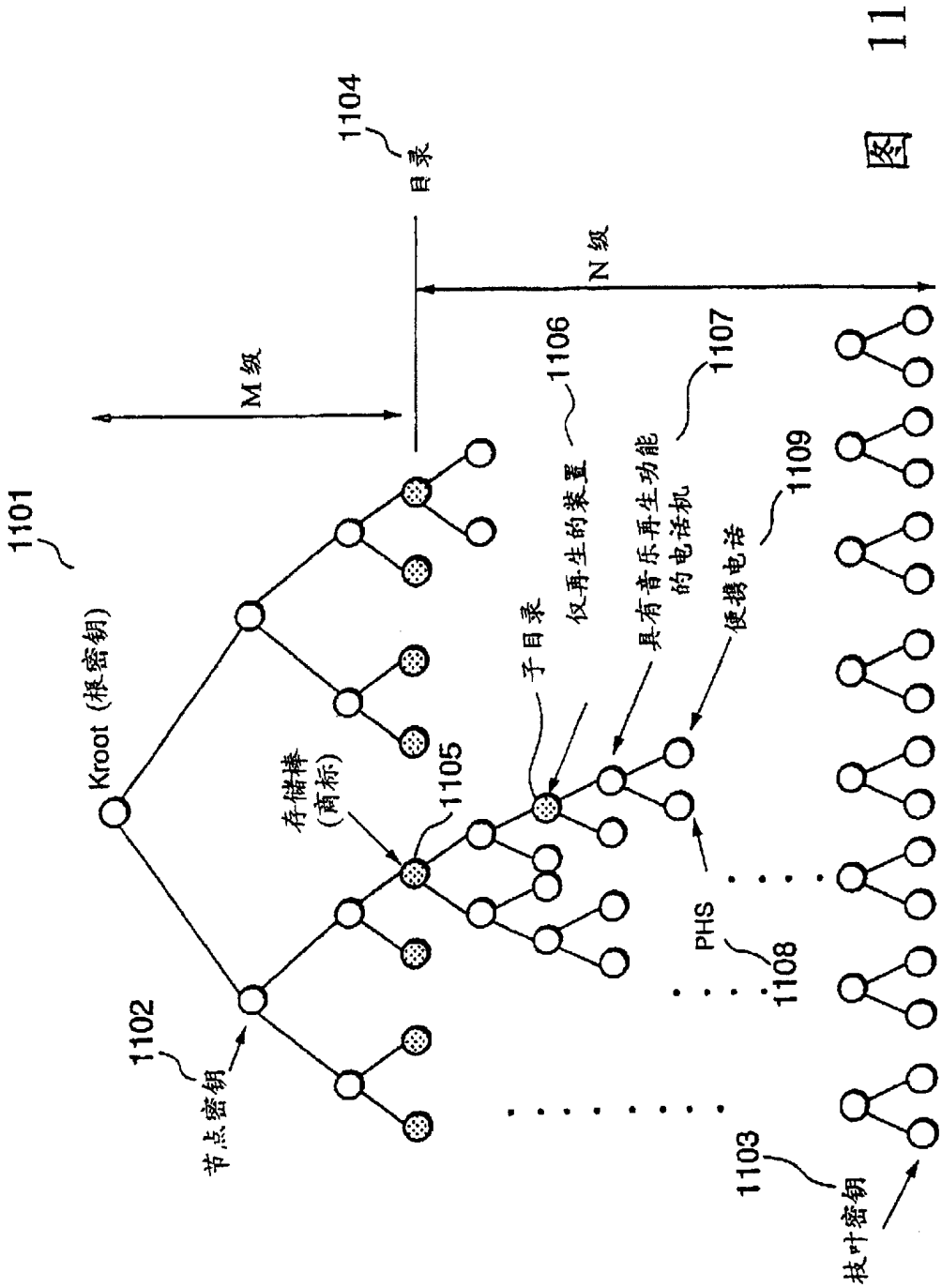

1101
Kroot (根密钥)
1102
节点密钥
1103
枝叶密钥
1104
目录
M 级
N 级
1105
存储棒
(商标)
1106
子目录
仅再生的装置
1107
具有音乐再生功能
的电话机
1108
PHS
1109
便携电话

图 11

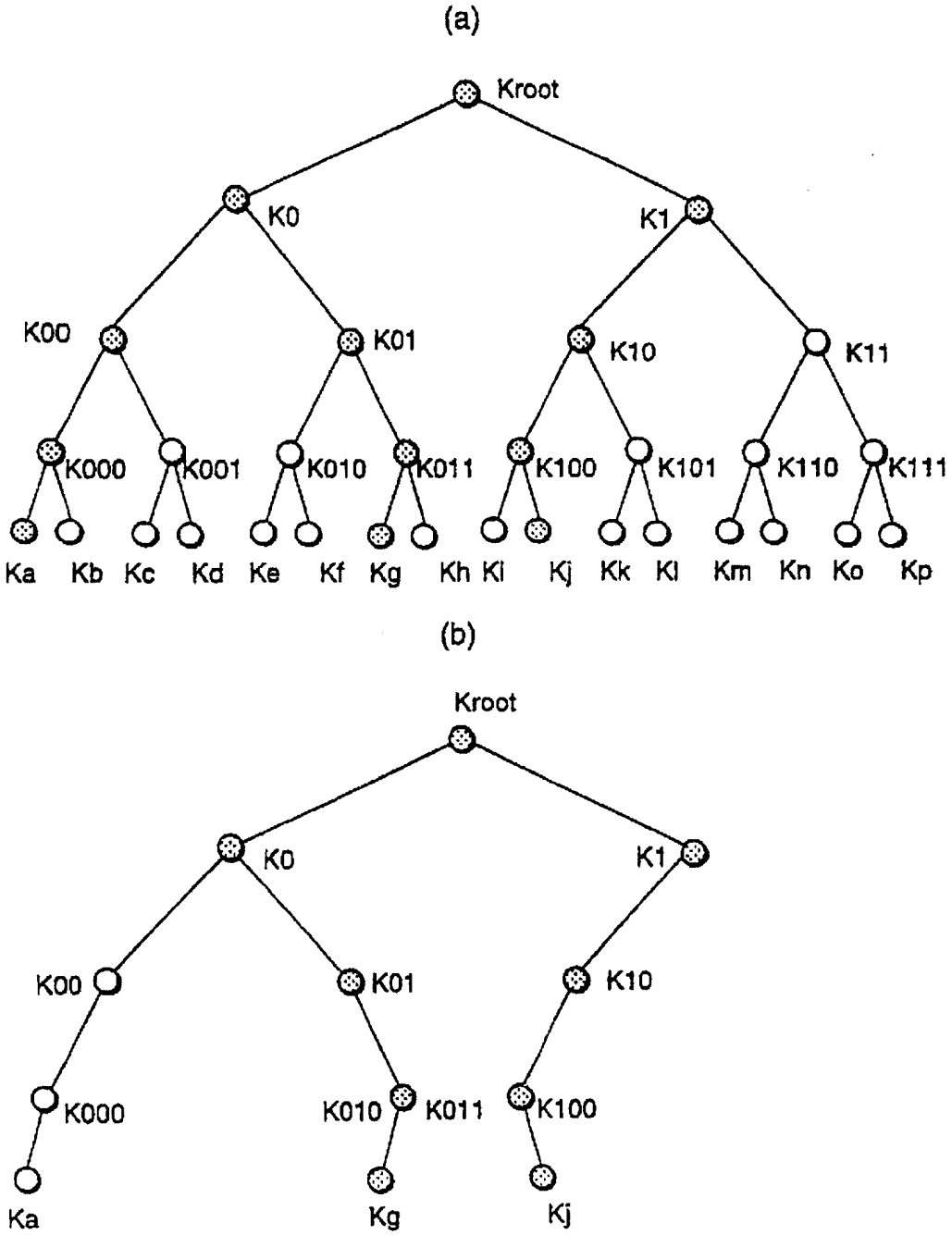

(a)
Kroot
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
Ka
Kb
Kc
Kd
Ke
Kf
Kg
Kh
Ki
Kj
Kk
Kl
Km
Kn
Ko
Kp
(b)
Kroot
K0
K1
K00
K01
K10
K000
K010
K011
K100
Ka
Kg
Kj

图 12

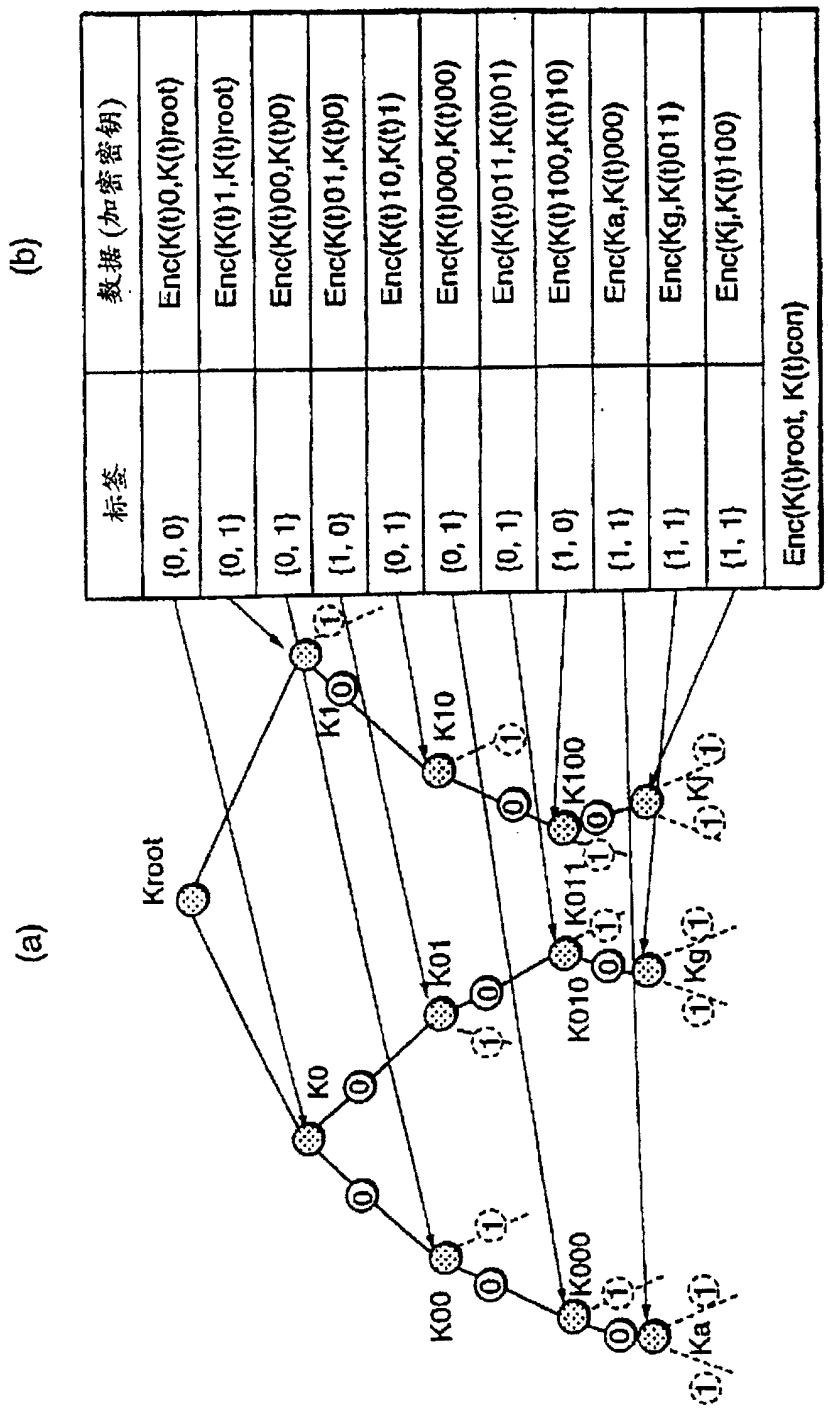

(a)
(b)
标签
数据 (加密密钥)
{0, 0}
Enc(K(t)0,K(t)root)
{0, 1}
Enc(K(t)1,K(t)root)
{0, 1}
Enc(K(t)00,K(t)0)
{1, 0}
Enc(K(t)01,K(t)0)
{0, 1}
Enc(K(t)10,K(t)1)
{0, 1}
Enc(K(t)000,K(t)00)
{0, 1}
Enc(K(t)011,K(t)01)
{1, 0}
Enc(K(t)100,K(t)10)
{1, 1}
Enc(Ka,K(t)000)
{1, 1}
Enc(Kg,K(t)011)
{1, 1}
Enc(Kj,K(t)100)
Enc(K(t)root, K(t)con)
Kroot
K0
K1
K00
K01
K10
K000
K010
K011
K100
Ka
Kg
Kj

图 13

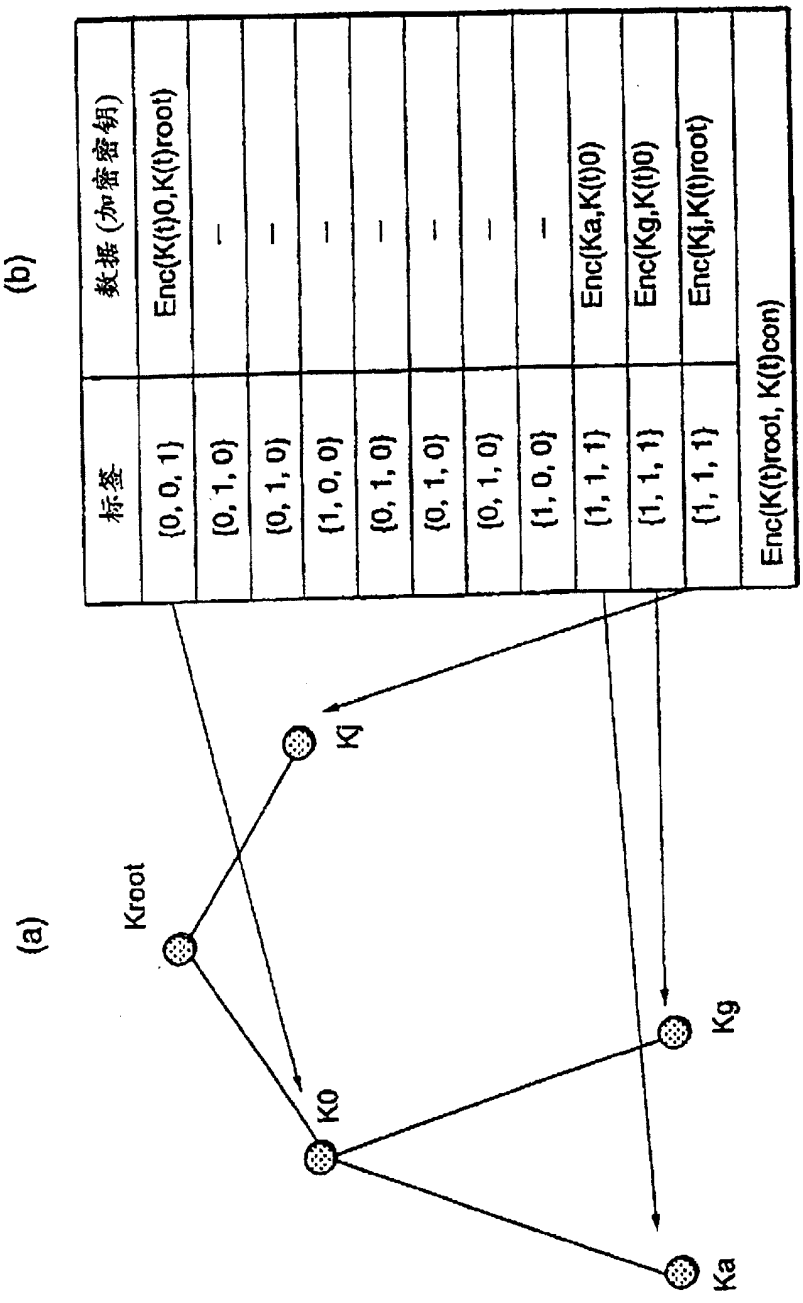

(a)
Kroot
Kj
K0
Kg
Ka
(b)
标签
数据 (加密密钥)
{0, 0, 1}
Enc(K(t)0,K(t)root)
{0, 1, 0}
—
{0, 1, 0}
—
{1, 0, 0}
—
{0, 1, 0}
—
{0, 1, 0}
—
{0, 1, 0}
—
{1, 0, 0}
—
{1, 1, 1}
Enc(Ka,K(t)0)
{1, 1, 1}
Enc(Kg,K(t)0)
{1, 1, 1}
Enc(Kj,K(t)root)
{1, 1, 1}
Enc(K(t)root, K(t)con)

图 14

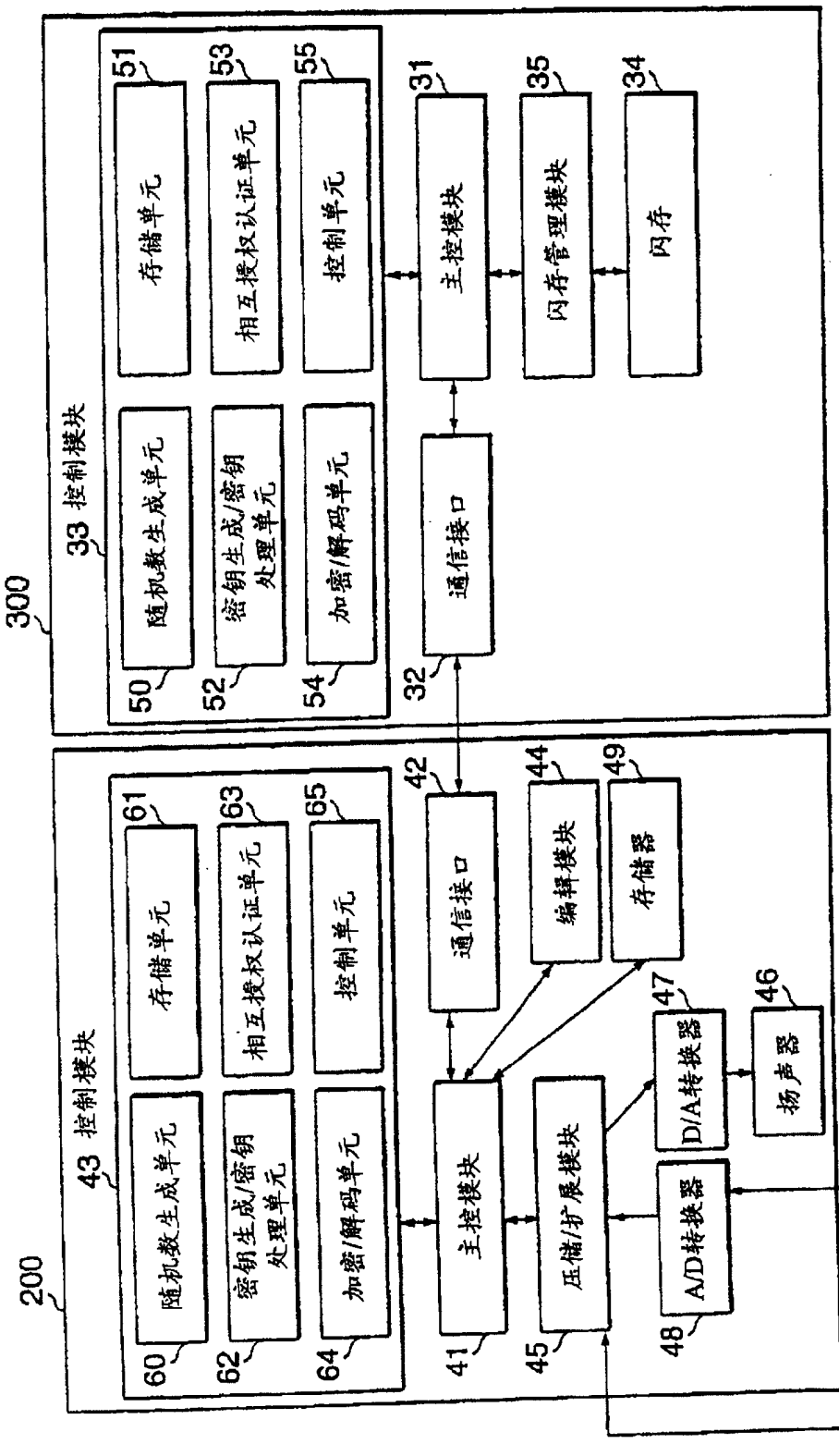

300
33 控制模块
随机数生成单元
密钥生成/密钥处理单元
加密/解码单元
存储单元
相互授权认证单元
控制单元
50
52
54
51
53
55
通信接口
主控模块
闪存管理模块
闪存
32
31
35
34
200
43 控制模块
随机数生成单元
密钥生成/密钥处理单元
加密/解码单元
存储单元
相互授权认证单元
控制单元
60
62
64
61
63
65
通信接口
主控模块
压缩/扩展模块
编辑模块
存储器
D/A转换器
A/D转换器
扬声器
42
41
45
44
49
47
48
46
数据 (EX.PC)
数据 (EX.CD,DVD)

图 15

存储在存储装置的存储单元中的数据

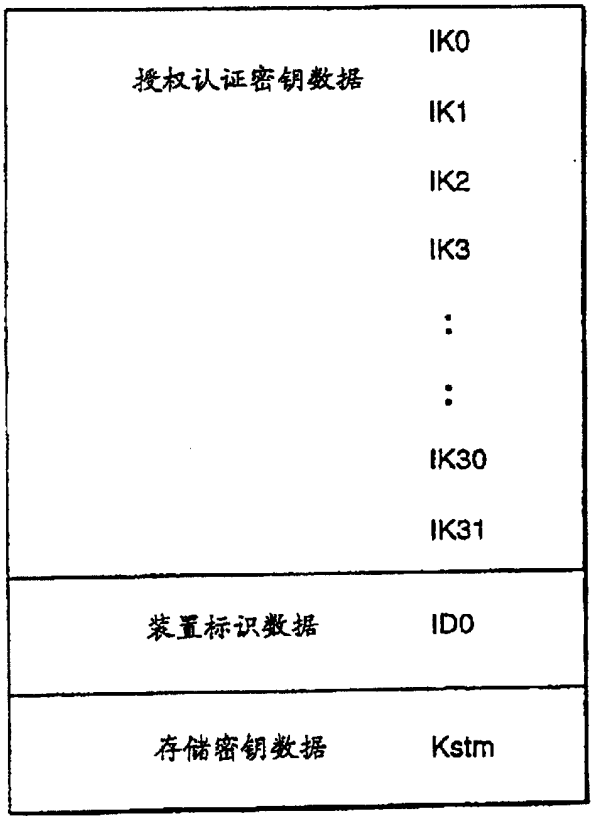


图 16

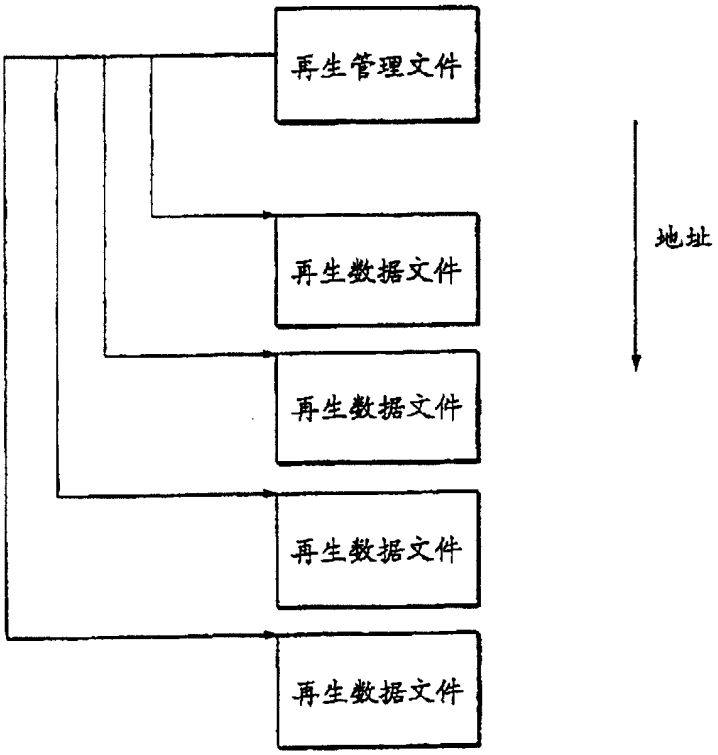


图 17

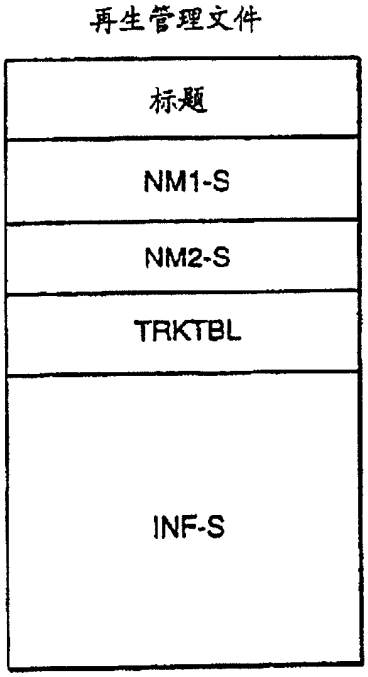


图 18

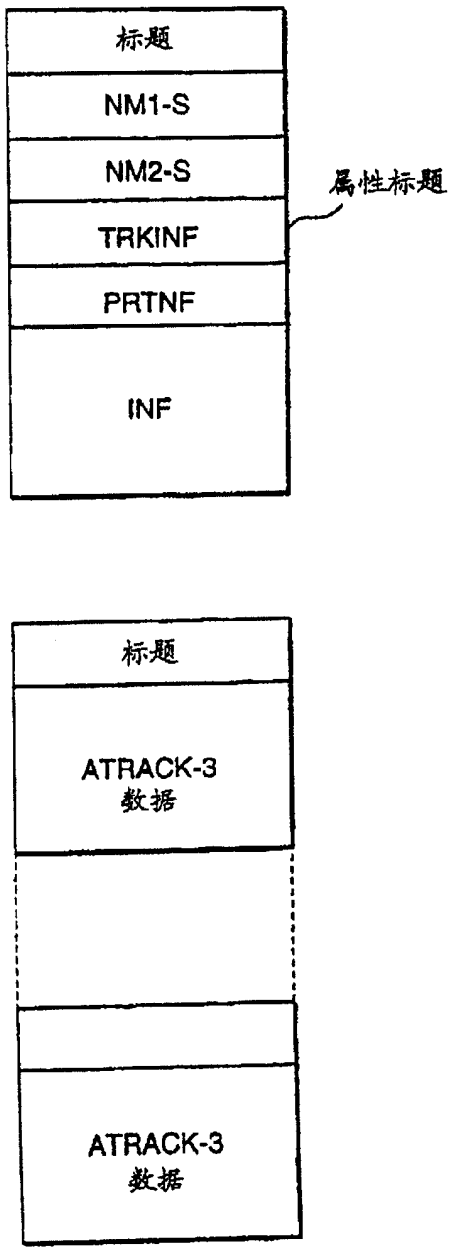


图 19

再生管理文件

A

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-TLO			保留			MCODE		REVISION				保留			
0x0010	SN1C+L		SN2C+L		SINFSIZE		T-TRK		VerNo.				保留			

B

0x0020	NM1-S(256)							
0x0120	NM2-S(512)							
0x0310								
0x0320	保留(4)		EKB VERSION		E(Kstm,Kcon)			
0x0330	E(KEKn,Kcon)				c_MAC[0]			
0x0340	保留(8)					MGR	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)							
0x3FFF	BLKID-TLO		保留		MCODE		REVISION	保留

C

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
INF	0X00	ID	0X00	SIZE		MCODE		C+L		保留		数据可变长度			

图 20

ATRACK-3 数据文件

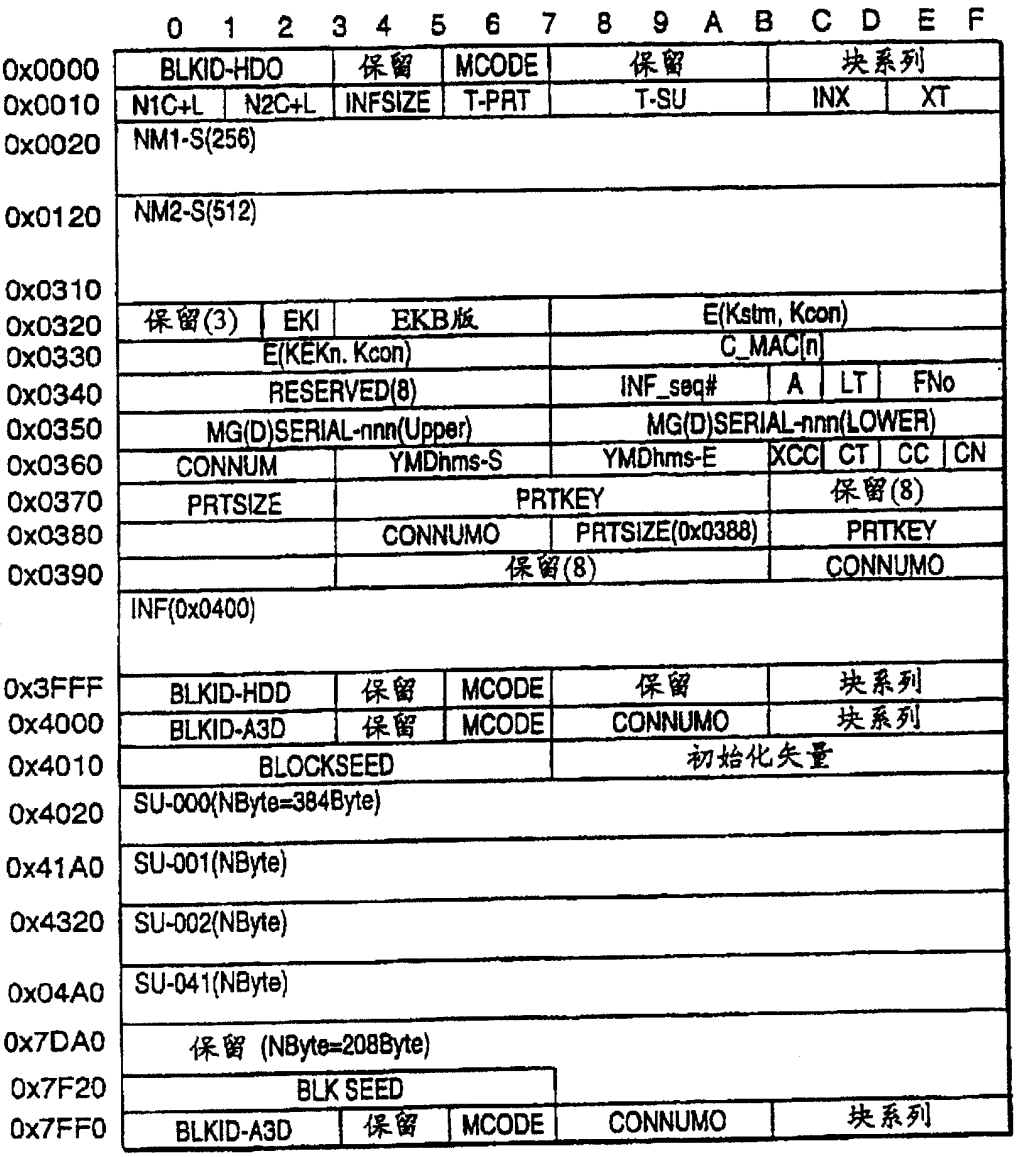


图 21

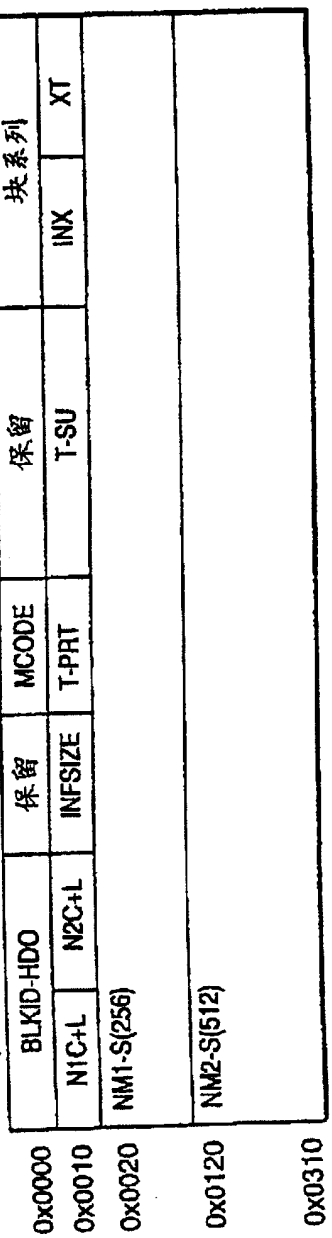

0 1 2 3 4 5 6 7 8 9 A B C D E F
BLKID-HDO
保留
MCODE
保留
块系列
N1C+L
N2C+L
INFSIZE
T-PRT
T-SU
INX
XT
NM1-S(256)
NM2-S(512)
0x0000
0x0010
0x0020
0x0120
0x0310

图 22

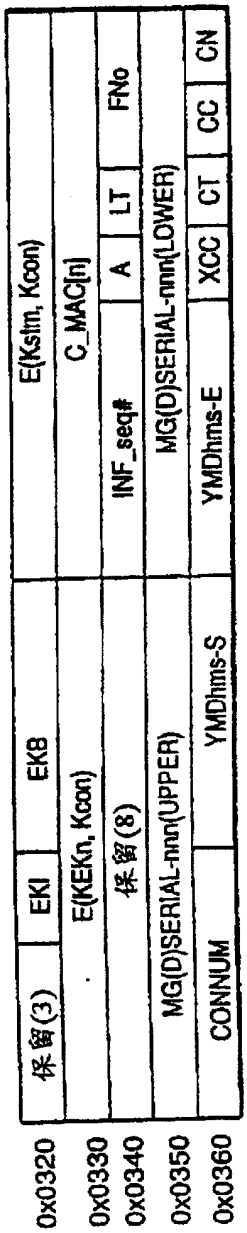

0x0320
0x0330
0x0340
0x0350
0x0360
保留(3)
EKI
EKB
E(Kstm, Kcon)
E(KEKn, Kcon)
C_MAC[n]
保留(8)
INF_seq#
A
LT
FNo
MG(D)SERIAL-nnn(UPPER)
MG(D)SERIAL-nnn(LOWER)
CONNUM
YMDhms-S
YMDhms-E
XCC
CT
CC
CN

图 23

比特7：ATRAC3模式　　0：Dual　　1：Joint

比特 6, 5, 4: N 对应模式值的3个比特数值

N	模式	时间	传送速率	SU (声音单元)	Byte
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	MONO	181min	47kbps	119SU	136
0	MONO	258min	33kbps	169SU	96

比特3：保留

比特2：数据识别　　0：声音　　1：其它

比特1：再生跳跃　　0：正常再生　　1：跳跃

比特0：强调　　0：断开　　1：接通 (50/15 μ 秒)

图　24

比特7：复制准许　　0：复制禁止　　1：复制准许

比特6：代次（版本）　　0：原始　　1：超过第一代

HCMS 比特5-4：高速数字复制操作的控制

00：复制禁止　　01：复制第一代　　10：复制准许

完成第一代复制的子被禁止进行进一步的复制操作

比特3-2：幅值门限认证授权级

00：等级10 (Non-MG)　　01：等级1

02：等级12　　11：保留

02：等级10

除10以外的等级不能被分割，也不能被组合

比特1，0：保留

图　25

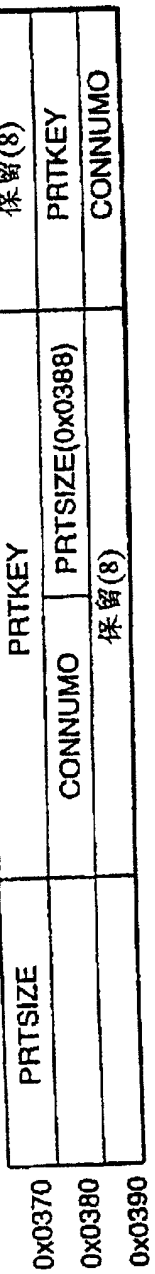

PRTSIZE
PRTKEY
保留(8)
CONNUMO
PRTSIZE(0x0388)
PRTKEY
保留(8)
CONNUMO
0x0370
0x0380
0x0390

图 26

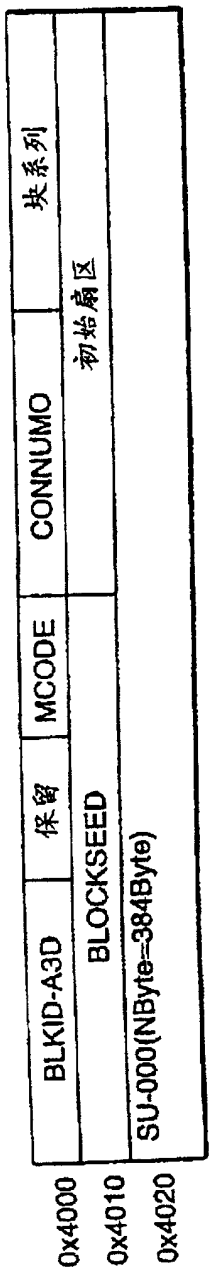

BLKID-A3D
保留
MCODE
CONNUMO
块系列
BLOCKSEED
初始扇区
SU-000(NByte=384Byte)
0x4000
0x4010
0x4020

图 27

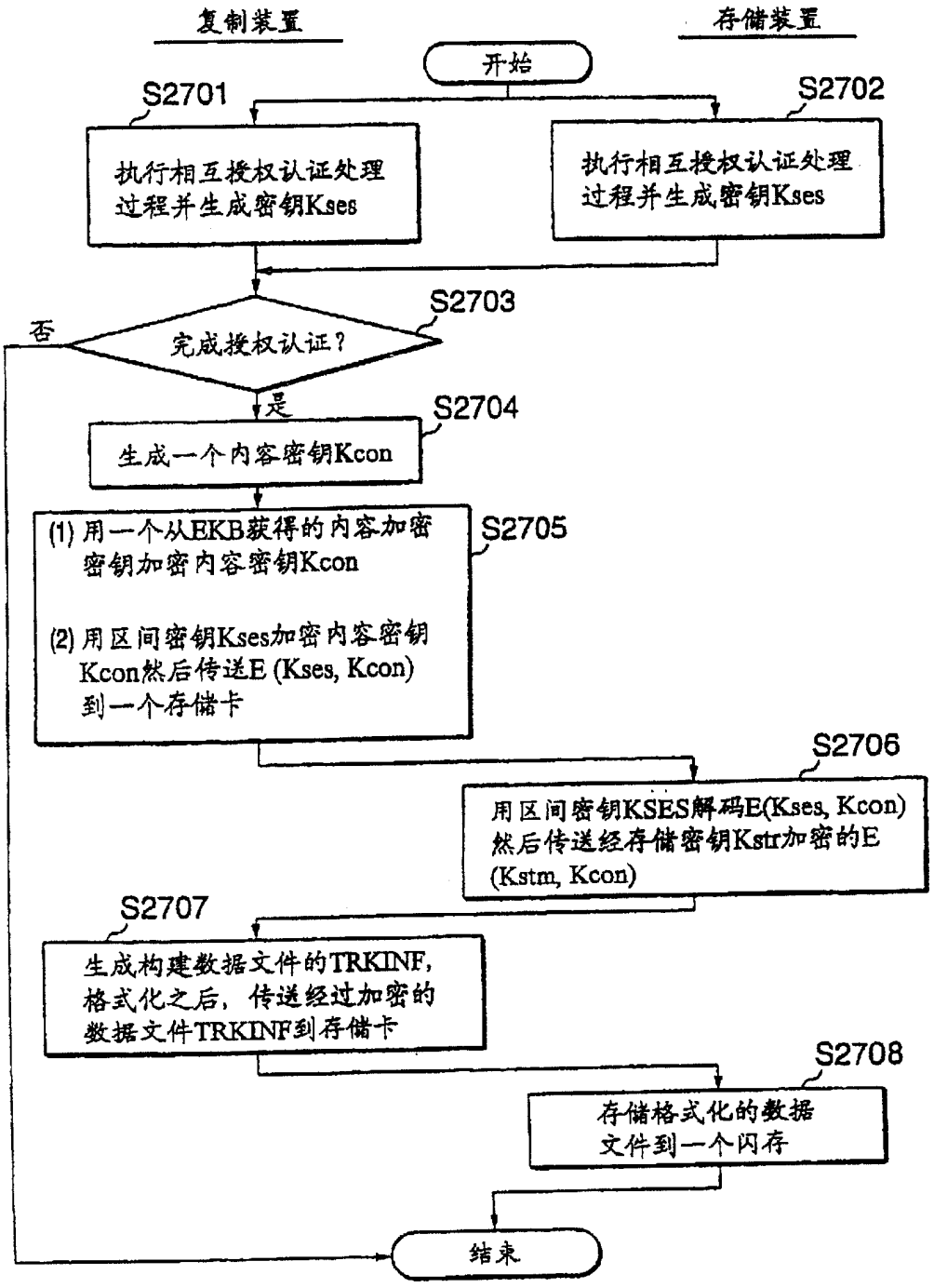

复制装置
存储装置
开始
S2701
S2702
执行相互授权认证处理过程并生成密钥Kses
执行相互授权认证处理过程并生成密钥Kses
S2703
否
完成授权认证？
是
S2704
生成一个内容密钥Kcon
(1) 用一个从EKB获得的内容加密密钥加密内容密钥Kcon
(2) 用区间密钥Kses加密内容密钥Kcon然后传送E (Kses, Kcon)到一个存储卡
S2705
S2706
用区间密钥KSES解码E(Kses, Kcon)然后传送经存储密钥Kstr加密的E (Kstm, Kcon)
S2707
生成构建数据文件的TRKINF，格式化之后，传送经过加密的数据文件TRKINF到存储卡
S2708
存储格式化的数据文件到一个闪存
结束

图 28

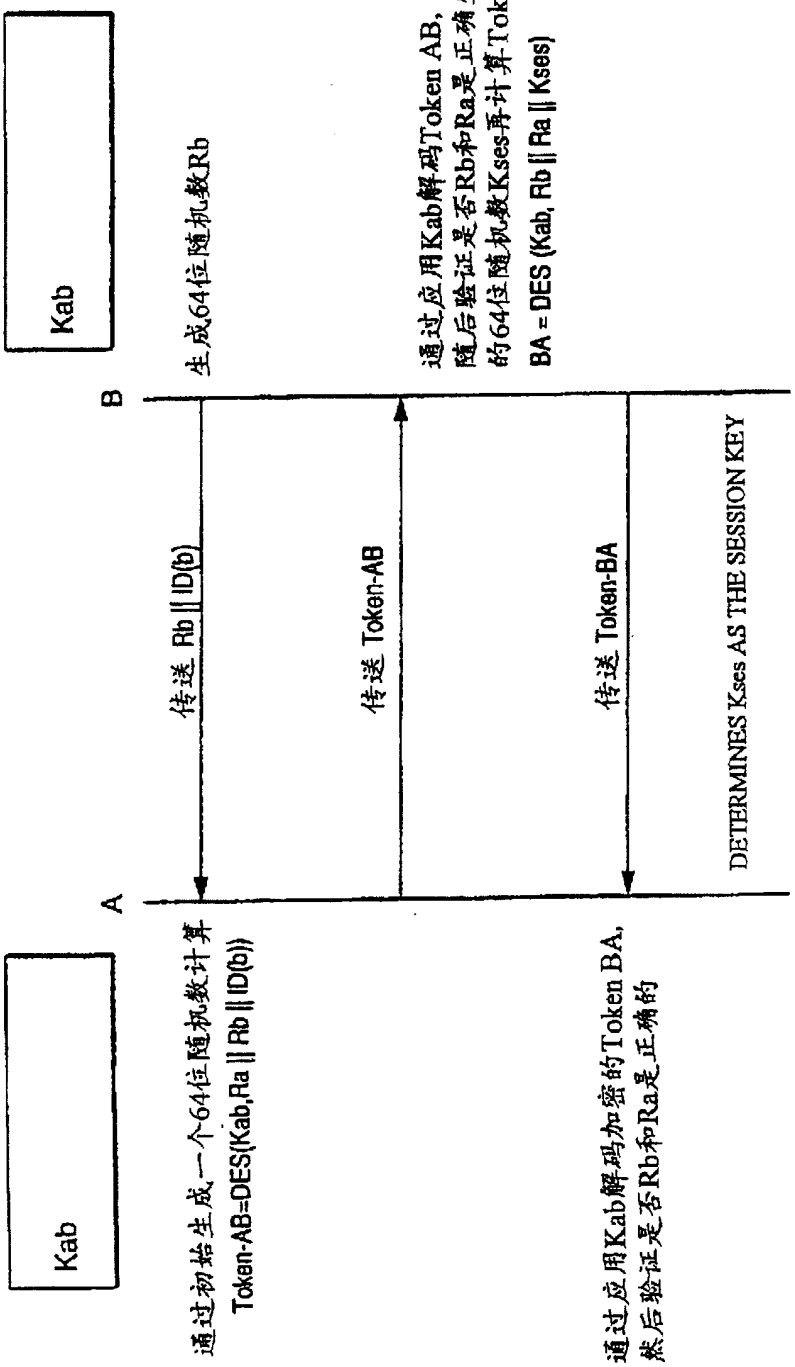

Kab
Kab
A
B
通过初始生成一个64位随机数计算
Token-AB=DES(Kab,Ra || Rb || ID(b))
传送 Rb || ID(b)
生成64位随机数Rb
传送 Token-AB
通过应用Kab解码Token AB,
随后验证是否Rb和Ra是正确生成
的64位随机数Kses再计算Token
BA = DES (Kab, Rb || Ra || Kses)
传送 Token-BA
通过应用Kab解码加密的Token BA,
然后验证是否Rb和Ra是正确的
DETERMINES Kses AS THE SESSION KEY
用ISO/IE9798-2标准对称密钥加密技术
的相互授权认证格式和密钥通信格式

图 29

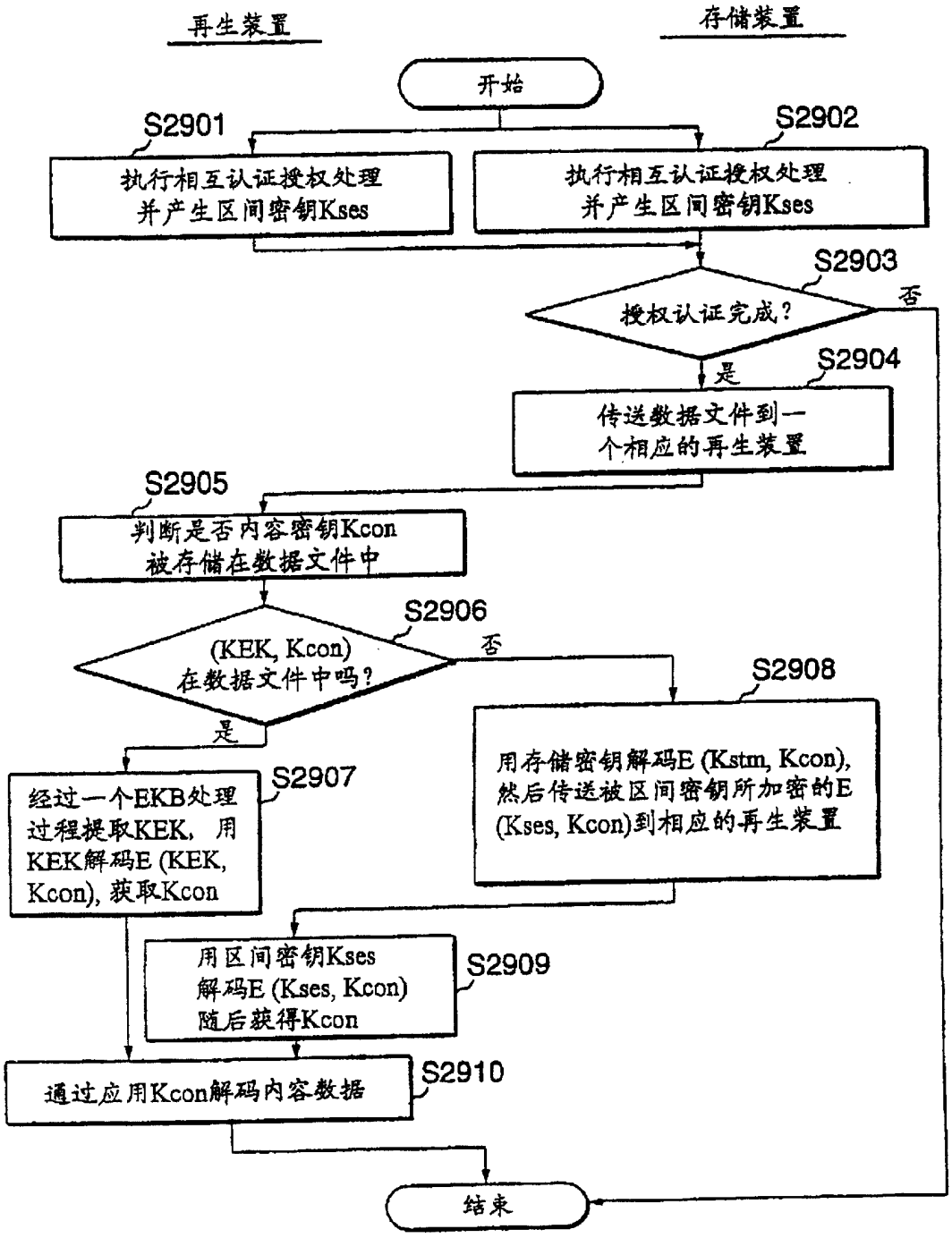

再生装置
存储装置
开始
S2901
执行相互认证授权处理
并产生区间密钥Kses
S2902
执行相互认证授权处理
并产生区间密钥Kses
S2903
授权认证完成?
否
是
S2904
传送数据文件到一
个相应的再生装置
S2905
判断是否内容密钥Kcon
被存储在数据文件中
S2906
(KEK, Kcon)
在数据文件中吗?
否
是
S2908
用存储密钥解码E (Kstm, Kcon),
然后传送被区间密钥所加密的E
(Kses, Kcon)到相应的再生装置
S2907
经过一个EKB处理
过程提取KEK, 用
KEK解码E (KEK,
Kcon), 获取Kcon
用区间密钥Kses
解码E (Kses, Kcon)
随后获得Kcon
S2909
通过应用Kcon解码内容数据
S2910
结束

图 30

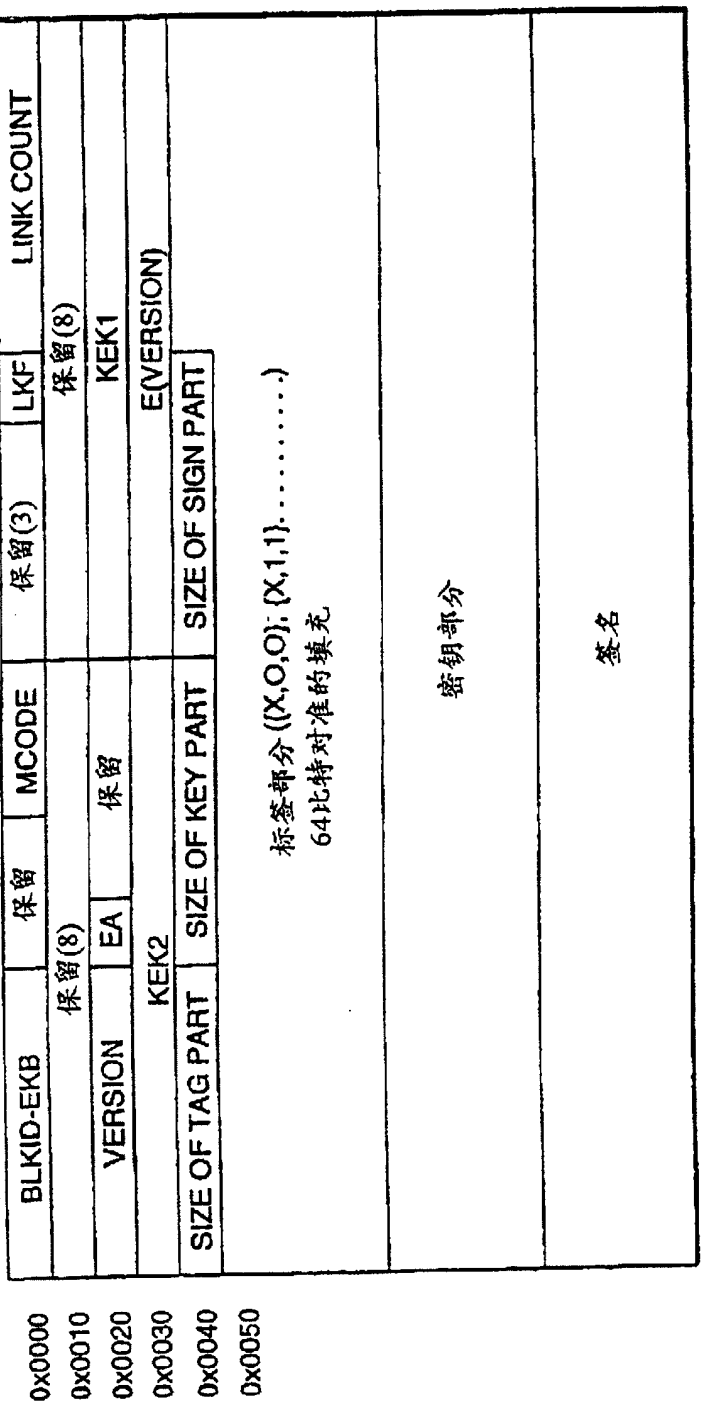

0 1 2 3 4 5 6 7 8 9 A B C D E F
BLKID-EKB
保留
MCODE
保留(3)
LKF
LINK COUNT
保留(8)
保留(8)
VERSION
EA
保留
KEK1
KEK2
E(VERSION)
SIZE OF TAG PART
SIZE OF KEY PART
SIZE OF SIGN PART
标签部分 ({X,O,O}; {X,1,1}.....)
64比特对准的填充
密钥部分
签名
0x0000
0x0010
0x0020
0x0030
0x0040
0x0050

图 31

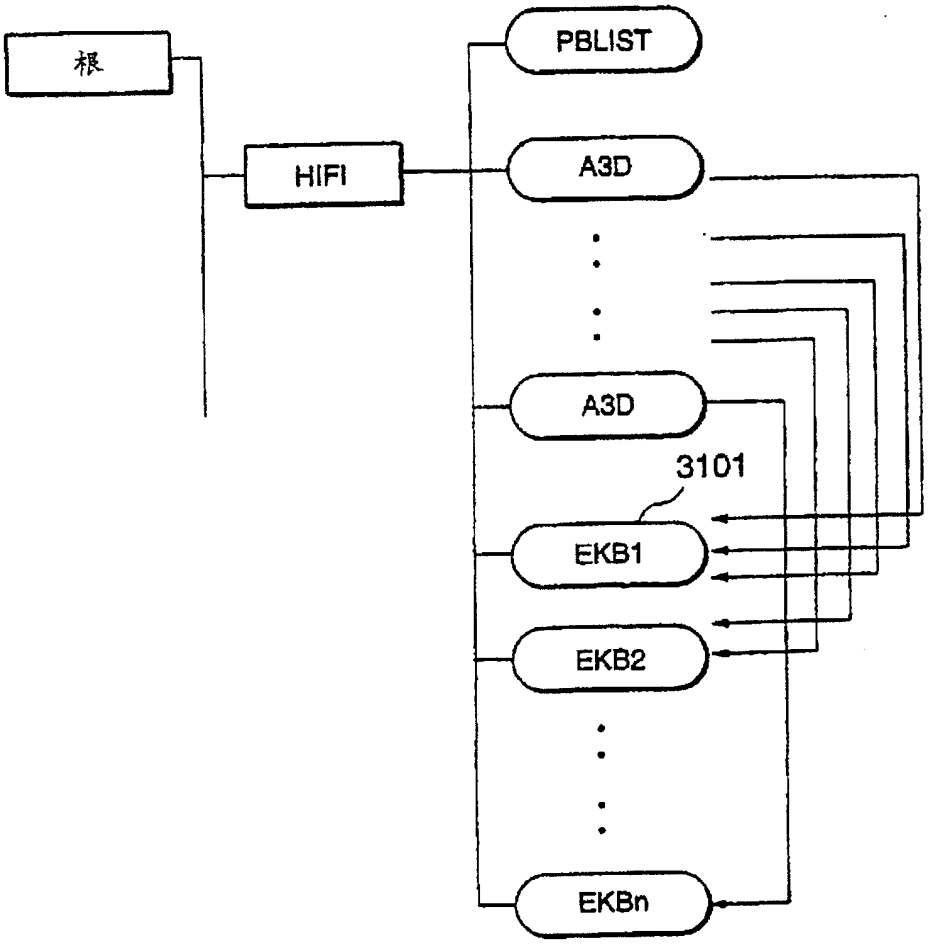


图 32

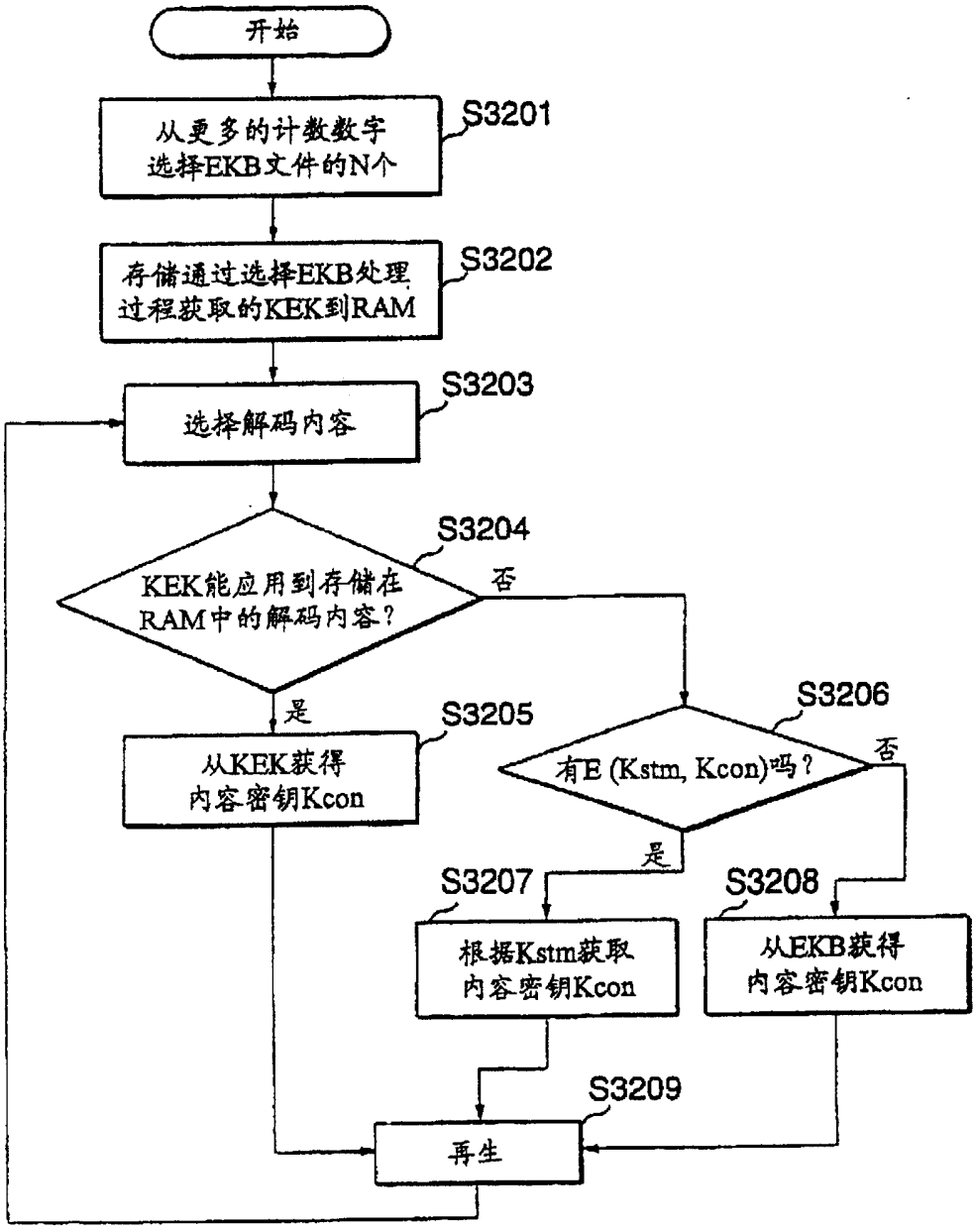

开始
从更多的计数数字选择EKB文件的N个
S3201
存储通过选择EKB处理过程获取的KEK到RAM
S3202
选择解码内容
S3203
KEK能应用到存储在RAM中的解码内容?
S3204
否
是
从KEK获得内容密钥Kcon
S3205
有E (Kstm, Kcon)吗?
S3206
否
是
根据Kstm获取内容密钥Kcon
S3207
从EKB获得内容密钥Kcon
S3208
再生
S3209

图 33

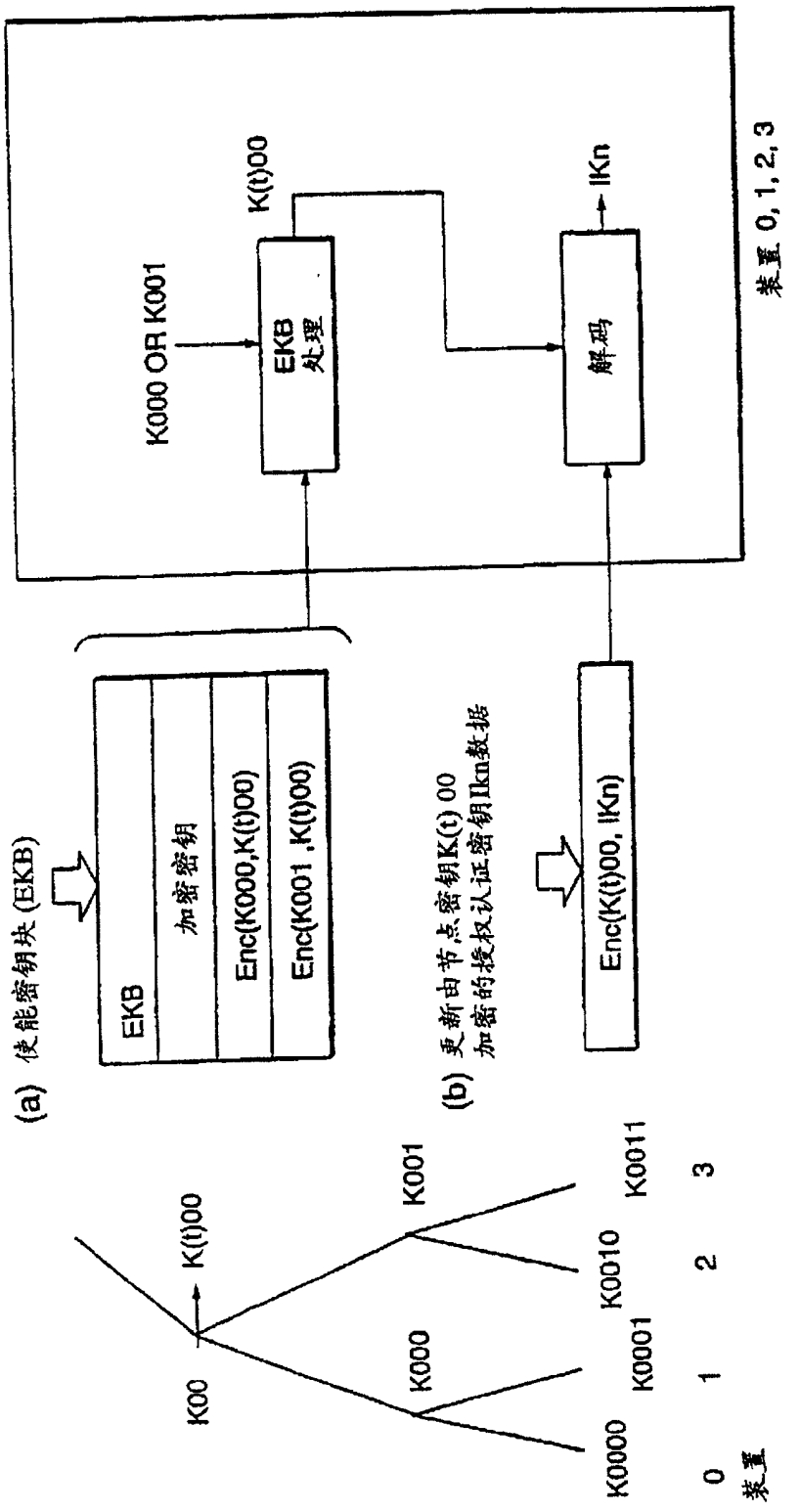

(a) 使能密钥块 (EKB)
EKB
加密密钥
Enc(K000,K(t)00)
Enc(K001 ,K(t)00)
(b) 更新由节点密钥K(t) 00
加密的授权认证密钥Ikn数据
Enc(K(t)00, IKn)
K000 OR K001
EKB 处理
K(t)00
解码
IKn
装置 0, 1, 2, 3
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
装置

图 34

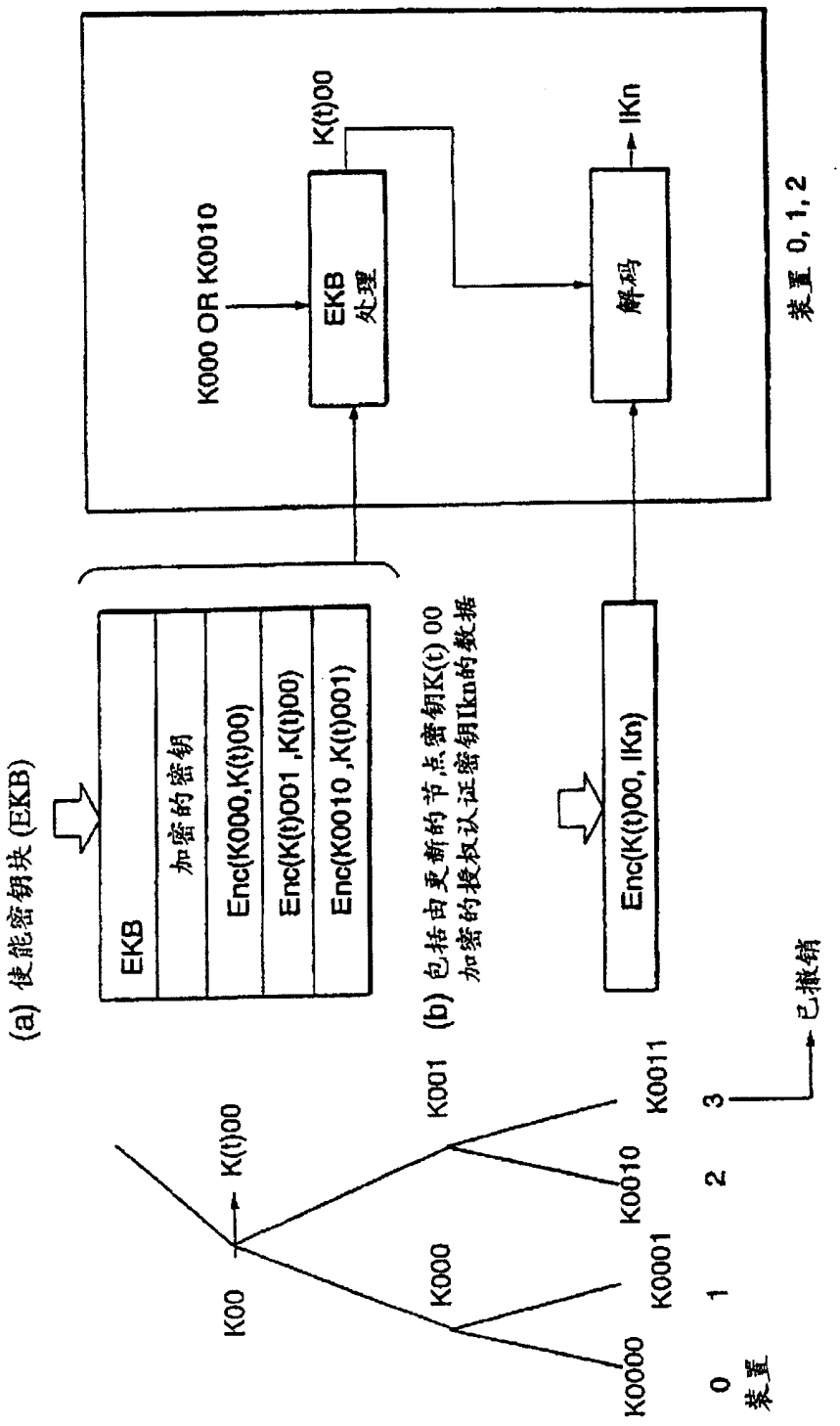

(a) 使能密钥块 (EKB)
EKB
加密的密钥
Enc(K000,K(t)00)
Enc(K(t)001 ,K(t)00)
Enc(K0010 ,K(t)001)
(b) 包括由更新的节点密钥K(t) 00
加密的授权认证密钥Ikn的数据
Enc(K(t)00, IKn)
K000 OR K0010
EKB
处理
K(t)00
解码
IKn
装置 0, 1, 2
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
装置
已撤销

图 35

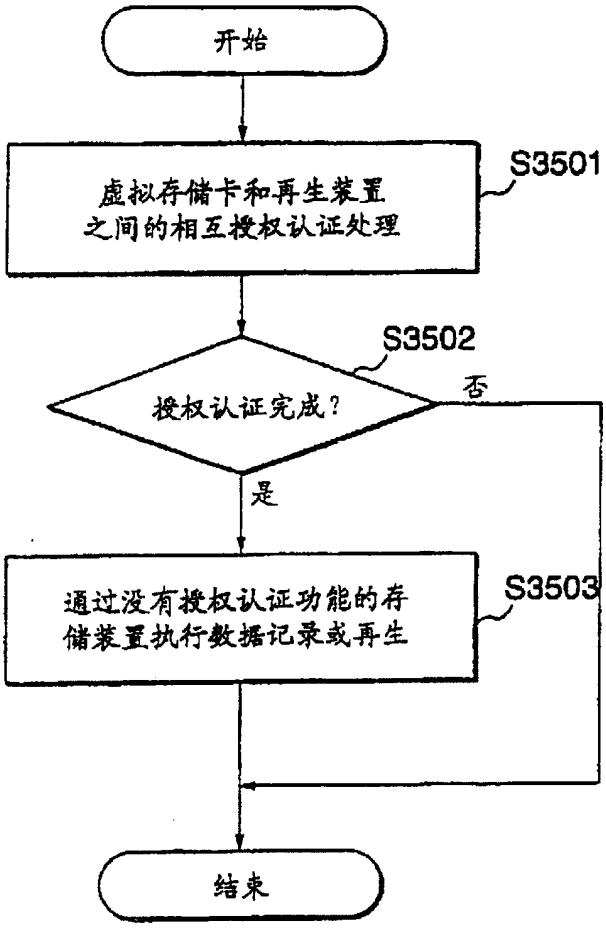

开始
虚拟存储卡和再生装置
之间的相互授权认证处理
S3501
S3502
授权认证完成？
否
是
通过没有授权认证功能的存
储装置执行数据记录或再生
S3503
结束

图 36

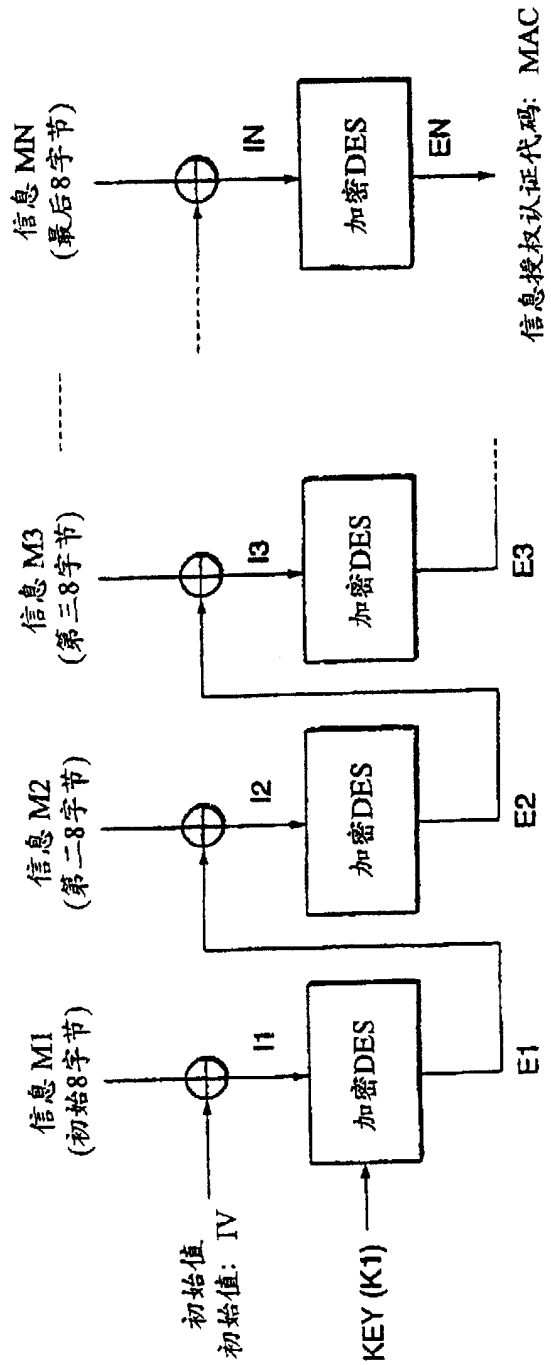

信息 M1
(初始8字节)
信息 M2
(第二8字节)
信息 M3
(第三8字节)
信息 MN
(最后8字节)
初始值
初始值: IV
KEY (K1)
I1
I2
I3
IN
加密DES
加密DES
加密DES
加密DES
E1
E2
E3
EN
信息授权认证代码: MAC
异或处理 (8字节单元)

图 37

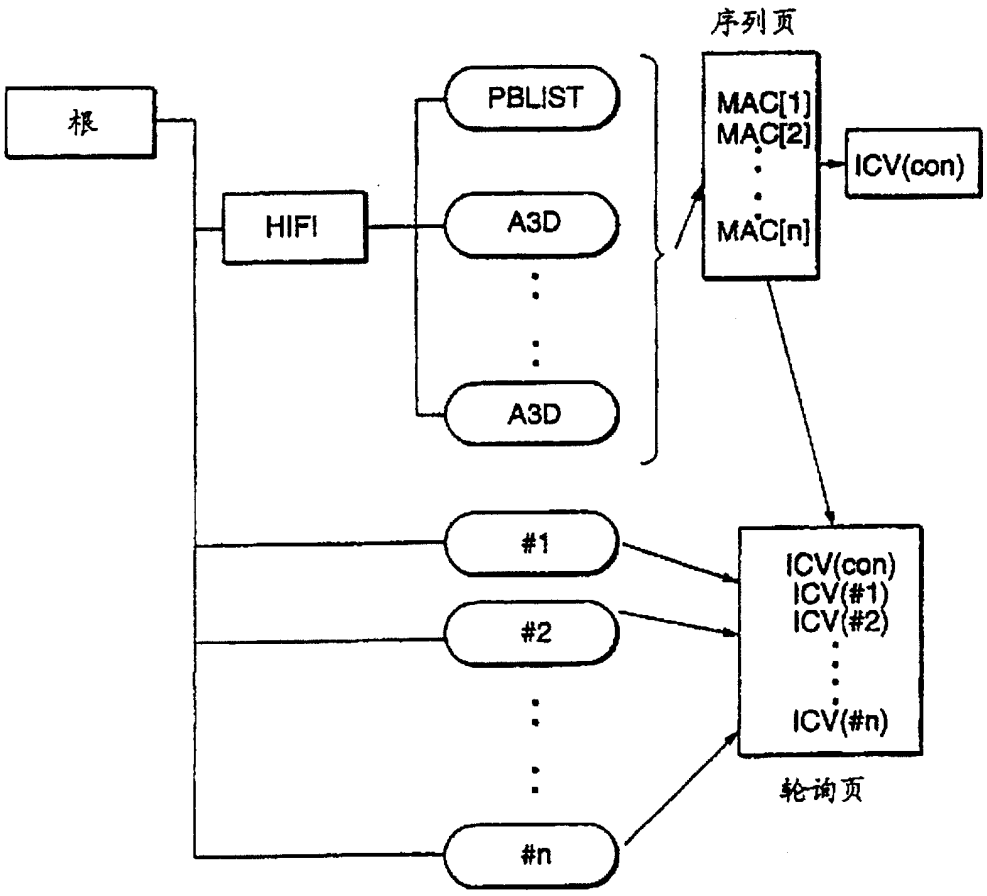

序列页
根
PBLIST
HIFI
A3D
A3D
MAC[1]
MAC[2]
MAC[n]
ICV(con)
#1
#2
#n
ICV(con)
ICV(#1)
ICV(#2)
ICV(#n)
轮询页

图 38

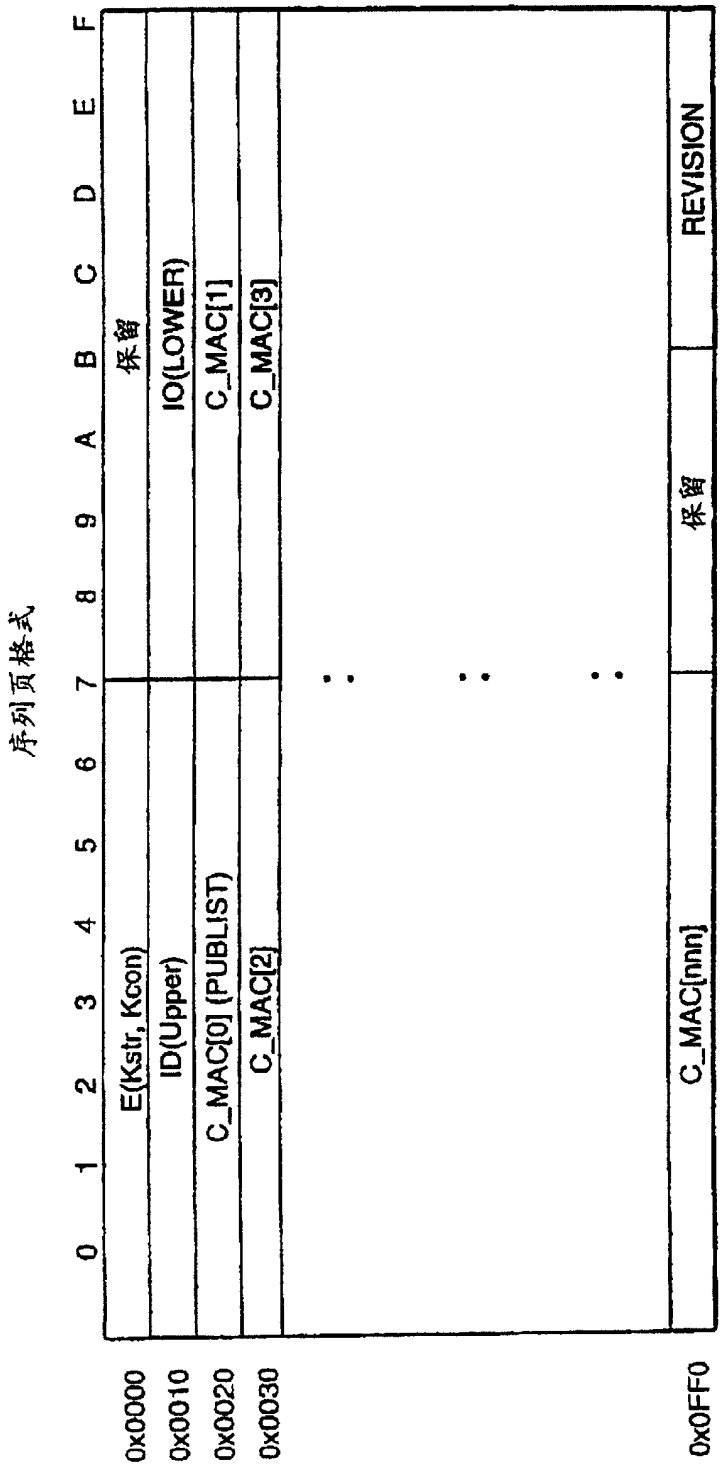

序列页格式
0 1 2 3 4 5 6 7 8 9 A B C D E F
0x0000
0x0010
0x0020
0x0030
0x0FF0
E(Kstr, Kcon)
保留
ID(Upper)
IO(LOWER)
C_MAC[0] (PUBLIST)
C_MAC[1]
C_MAC[2]
C_MAC[3]
C_MAC[nnn]
保留
REVISION

图 39

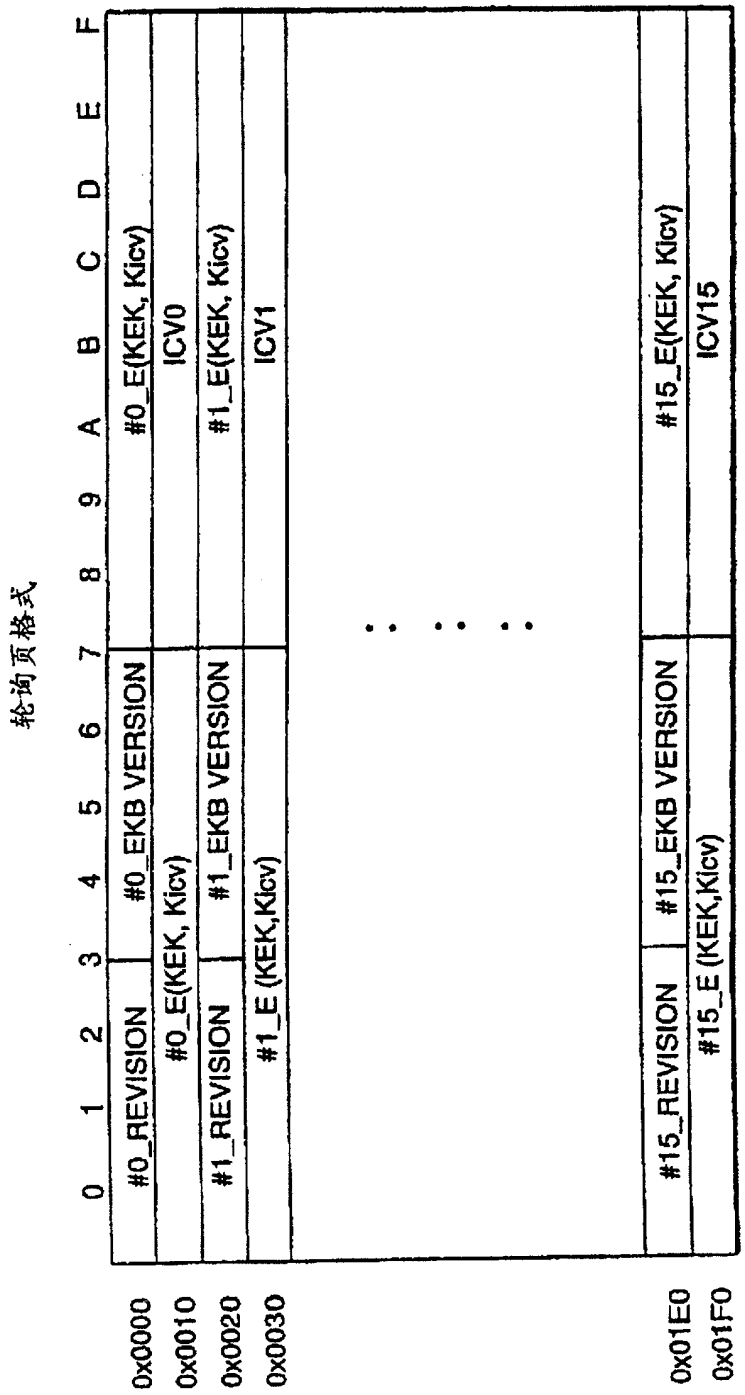

轮询页格式
0 1 2 3 4 5 6 7 8 9 A B C D E F
#0_REVISION
#0_EKB VERSION
#0_E(KEK, Kicv)
ICV0
#1_REVISION
#1_EKB VERSION
#1_E(KEK, Kicv)
ICV1
#1_E (KEK,Kicv)
#15_REVISION
#15_EKB VERSION
#15_E(KEK, Kicv)
ICV15
#15_E (KEK,Kicv)
0x0000
0x0010
0x0020
0x0030
0x01E0
0x01F0

图 40

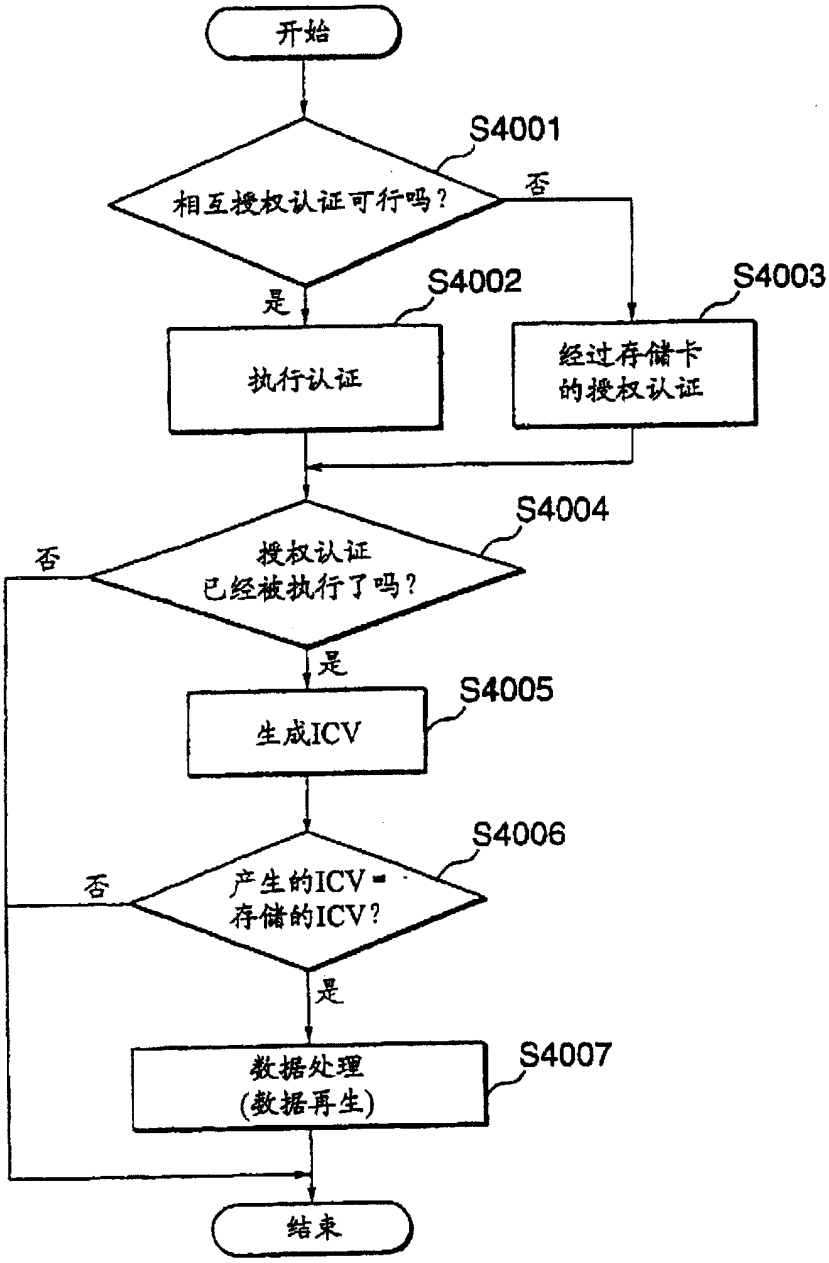

开始
S4001
相互授权认证可行吗?
否
是
S4002
执行认证
S4003
经过存储卡
的授权认证
S4004
授权认证
已经被执行了吗?
否
是
S4005
生成ICV
S4006
产生的ICV =
存储的ICV?
否
是
S4007
数据处理
(数据再生)
结束

图 41

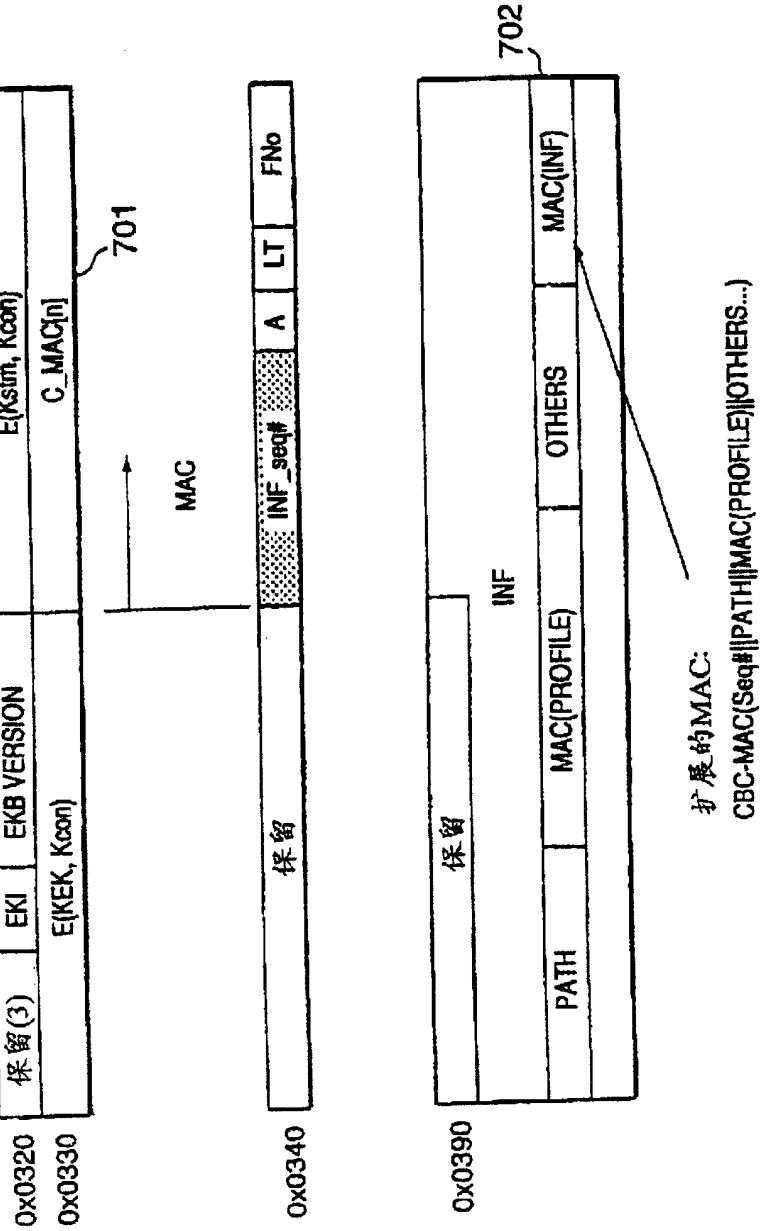

0x0320
0x0330
保留(3)
EKI
EKB VERSION
E(KEK, Kcon)
E(Kstm, Kcon)
C_MAC[n]
701
MAC
0x0340
保留
INF_seq#
A
LT
FNo
0x0390
保留
INF
PATH
MAC(PROFILE)
OTHERS
MAC(INF)
702
扩展的MAC:
CBC-MAC(Seq#||PATH||MAC(PROFILE)||OTHERS...)

图 42

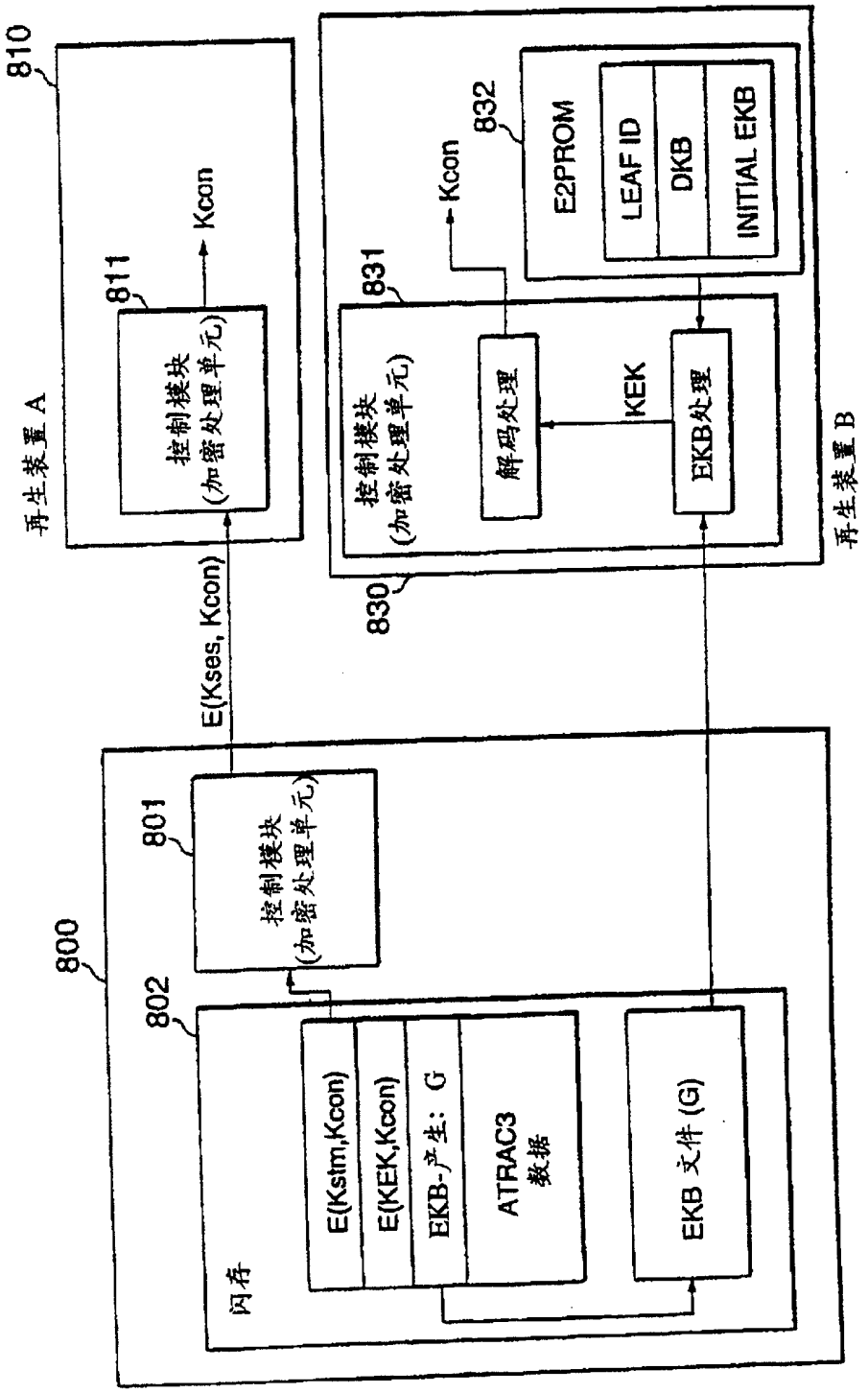

810
再生装置 A
811
控制模块
(加密处理单元)
Kcon
E(Kses, Kcon)
830
831
控制模块
(加密处理单元)
解码处理
KEK
EKB处理
Kcon
832
E2PROM
LEAF ID
DKB
INITIAL EKB
再生装置 B
800
801
控制模块
(加密处理单元)
802
闪存
E(Kstm,Kcon)
E(KEK,Kcon)
EKB-产生: G
ATRAC3
数据
EKB 文件 (G)

图 43

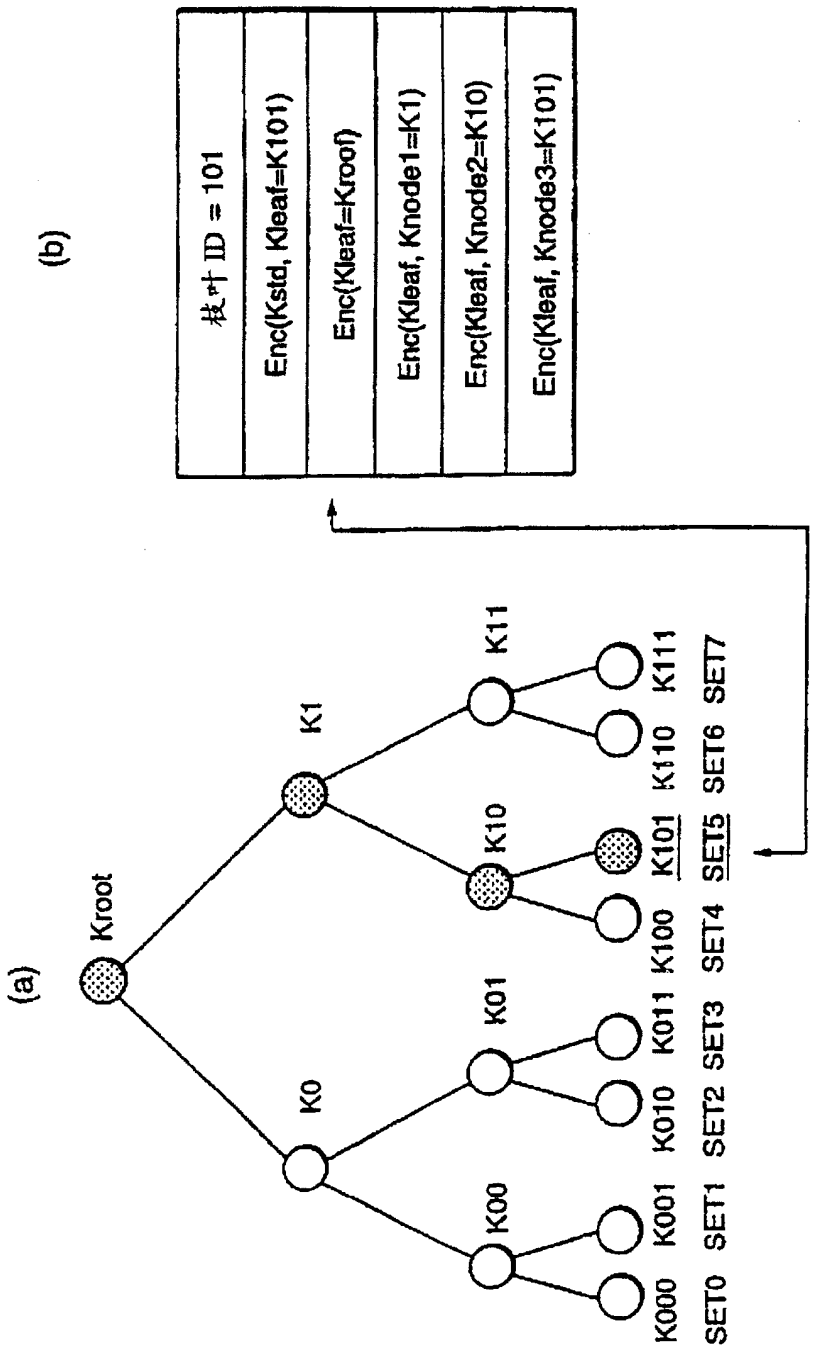

(a)
Kroot
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
SET0
SET1
SET2
SET3
SET4
SET5
SET6
SET7
(b)
枝叶 ID = 101
Enc(Kstd, Kleaf=K101)
Enc(Kleaf=Kroot)
Enc(Kleaf, Knode1=K1)
Enc(Kleaf, Knode2=K10)
Enc(Kleaf, Knode3=K101)

图 44

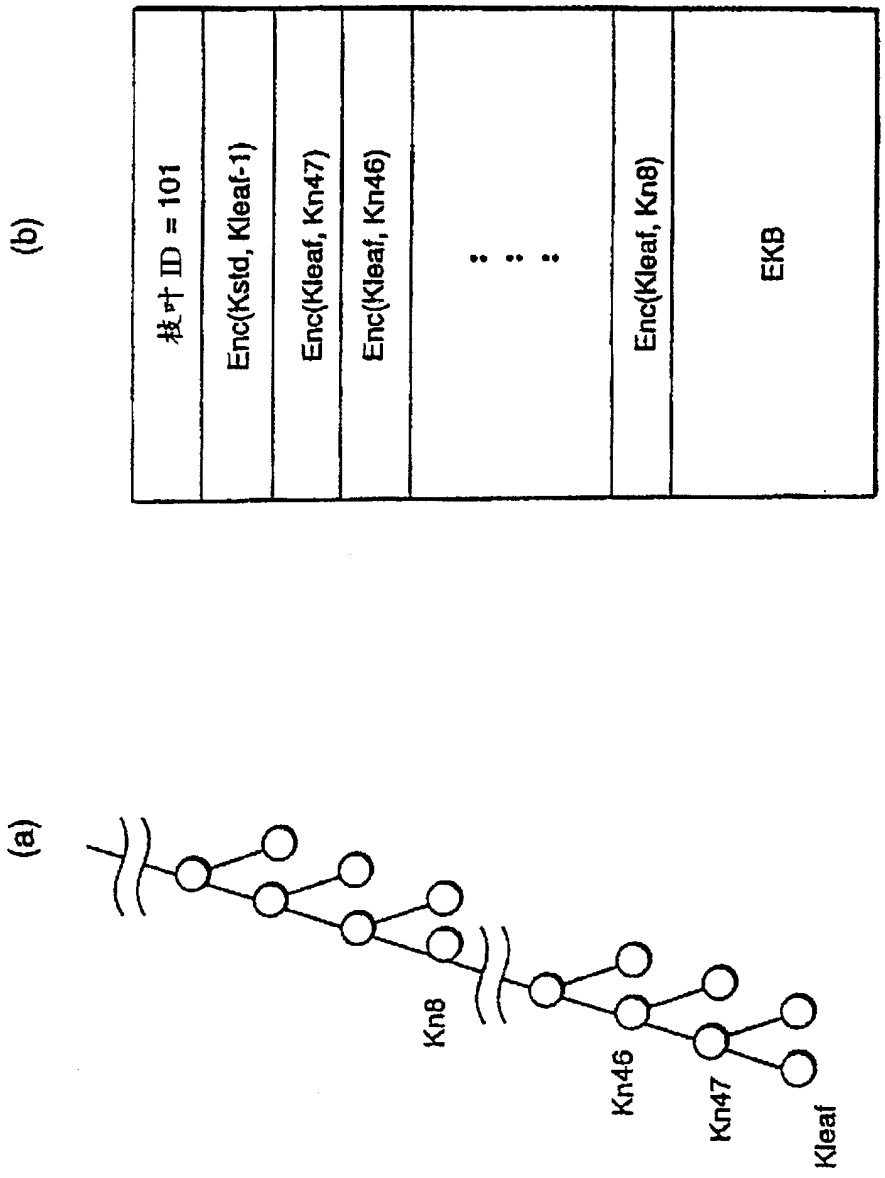

(a)
Kn8
Kn46
Kn47
Kleaf
(b)
枝叶 ID = 101
Enc(Kstd, Kleaf-1)
Enc(Kleaf, Kn47)
Enc(Kleaf, Kn46)
Enc(Kleaf, Kn8)
EKB

图 45

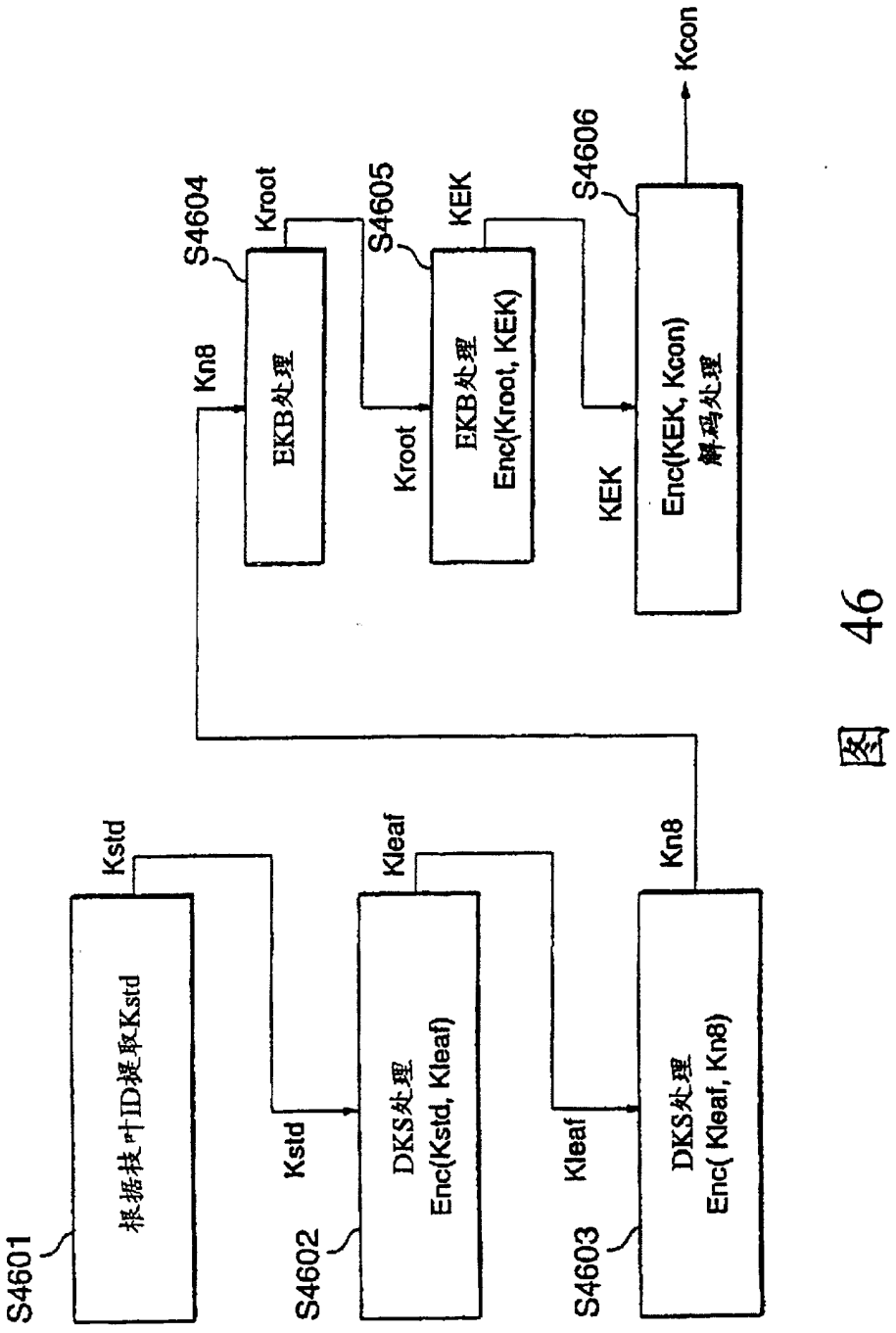

S4601
根据枝叶ID提取Kstd
Kstd
S4602
DKS处理
Enc(Kstd, Kleaf)
Kleaf
S4603
DKS处理
Enc(Kleaf, Kn8)
Kn8
S4604
EKB处理
Kn8
Kroot
S4605
EKB处理
Enc(Kroot, KEK)
Kroot
KEK
S4606
Enc(KEK, Kcon)
解码处理
KEK
Kcon

图 46