[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G11B 20/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 03800684.7

[45] 授权公告日 2006 年 7 月 26 日

[11] 授权公告号 CN 1266639C

[22] 申请日 2003.4.10 [21] 申请号 03800684.7
[30] 优先权
[32] 2002.4.15 [33] JP [31] 111555/2002
[86] 国际申请 PCT/JP2003/004548 2003.4.10
[87] 国际公布 WO2003/088058 日 2003.10.23
[85] 进入国家阶段日期 2004.1.16
[71] 专利权人 索尼株式会社
地址 日本东京都
[72] 发明人 川本洋志 石黑隆二 江面裕一
长野元彦
审查员 张 妍

[74] 专利代理机构 北京市柳沈律师事务所
代理人 蒲迈文 黄小临

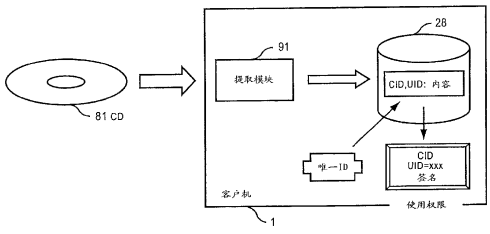
权利要求书 1 页 说明书 15 页 附图 18 页

[54] 发明名称

信息管理装置和方法

[57] 摘要

一种信息管理装置、方法、记录介质及程序，能够防止内容的非授权使用。客户机(1)的提取模块(91)从 CD(81)获取内容。在客户机(1)中，生成标识内容的内容 ID 和内在于客户机(1)的唯一 ID，并且将这些 ID 加到由提取模块(91)获取的内容。而且，生成并保存包含内容使用条件等的使用权限。使用权限包括表示仅允许在具有与加到内容的唯一 ID 相同的 ID 的装置(客户机)上回放内容的信息。本发明适用于如个人计算机的信息处理装置。



1. 一种用于管理内容的信息管理装置，包括:

内容获取部件，用于获取内容;

标识信息获得部件，用于获得唯一标识信息和内容标识信息，其中所述唯一标识信息用于标识所述信息管理装置并且唯一于所述信息管理装置;

内容存储部件，用于存储由所述内容获取部件所获取的内容，其中该内容被加有由所述标识信息获得部件所获得的所述唯一标识信息和所述内容标识信息；以及

使用权限存储部件，用于存储使用权限作为内容使用信息，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

2. 如权利要求 1 所述的信息管理装置，还包括回放部件，用于当加到内容的标识信息与由标识信息获得部件获得的标识信息相同时回放内容。

3. 如权利要求 1 所述的信息管理装置，其中，内容获取部件通过连至信息管理装置的记录介质获取内容。

4. 如权利要求 1 所述的信息管理装置，其中，标识信息获得部件使用所生成的随机数作为标识信息。

5. 一种用于管理内容的信息管理装置的信息管理方法，所述信息管理方法包括:

内容获取步骤，获取内容;

标识信息获得步骤，获得唯一标识信息和内容标识信息，其中所述唯一标识信息用于标识所述信息管理装置并且唯一于所述信息管理装置;

内容存储步骤，存储在所述内容获取步骤中所获取的内容，其中该内容被加有在所述标识信息获得步骤中所获得的所述唯一标识信息和所述内容标识信息；以及

使用权限存储步骤，存储使用权限作为内容使用信息，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

信息管理装置和方法

技术领域

本发明涉及一种信息管理装置和方法，特别涉及一种可以容易地防止内容非授权回放的信息管理装置和方法。

背景技术

近来，各种宽带环境的普及得到迅猛发展，并且各种内容发行服务包括音乐数据、运动图像数据等已变得可商业获得。

存在基于订阅的音乐发行服务，例如“PressPlay(商标)”。在该音乐发行服务中，按月支付固定费用的用户可以在预定条件下(例如，在可以以流回放的方式回放最大可达 1,000 首歌曲、可以下载并保存最大可达 100 首歌曲到个人计算机的硬盘中、可以复制最大可达 20 首歌曲以写入(复制)到 CD(Compact Disk, 致密盘)-R 等上的条件下)享用音乐内容。

一种用于管理使用该发行服务接收内容的用户的权限信息的系统公开于例如日本未审专利申请公开 No. 2001-352321，其中，该系统具有形成树型的对应于多个服务的节点，其中，使用激活密钥块(enabling key block, EKB)，它包括分配给以对应于给定服务的一个节点开始且以属于该服务的叶子节点(设备)结束的路径上的各节点的密钥信息(DNK(Device Node Key, 设备节点密钥))。

在该系统中，将 EKB 加到由特定服务发行的内容，并且使用分配给各设备的 DNK 来获得包含在 EKB 中的更新密钥信息，从而可以管理允许使用该服务的设备。不能使用 DNK 从 EKB 获得更新密钥信息的设备此后不能接收该服务。

因此，可以管理各设备上的内容使用，而无需在提供内容的服务器与各设备之间进行认证。

在该内容权限信息管理系统中，从例如 CD(致密盘)引入内容的设备使用 ICV(Integrity Check Value, 完整性校验值)来管理内容。

图 1 是用于根据 ICV 管理引入内容的机制的示意图。

如图 1 所示，例如，一个设备如个人计算机将从 CD 引入的内容(音乐数据)登记在硬盘的管理表中，并且通过将根据登记内容生成的 MAC(Message Authentication Code, 消息认证码)(C1, C2, ..., Cn)应用于 ICV=hash(Kicv, C1, C2, ..., Cn)来生成 ICV。Kicv 是用于生成 ICV 的密钥信息。

将在创建内容时生成且安全保存的 ICV 与在预定时候如回放时候新生成的 ICV 进行比较。当 ICV 匹配时，判定该内容未被篡改。当所生成的 ICV 与在创建内容时所生成的 ICV 时不匹配，判定该内容遭到篡改。当判定该内容未被篡改时，随后对内容进行回放。当判定该内容遭到篡改时，不执行回放操作。因此，可以防止回放被篡改内容。

然而，上述基于 ICV 的内容管理机制存在一个问题是每次引入或回放内容时都必须生成 ICV，并且操作繁琐。

因此，便携式设备如音乐回放设备必须包括具有哈希（hash）计算功能以生成 ICV 的高性能计算单元，但是由于该计算单元而使设备成本提高。

发明内容

本发明是鉴于上述问题而提出的，并且其意图是容易地防止内容的未授权回放。

本发明的一种信息管理装置，包括：内容获取部件，用于获取内容；标识信息获得部件，用于获得唯一标识信息和内容标识信息，其中所述唯一标识信息用于标识所述信息管理装置并且唯一于所述信息管理装置；内容存储部件，用于存储由内容获取部件获取的内容，其中该内容被加有由所述标识信息获得部件所获得的所述唯一标识信息和所述内容标识信息；以及使用权限存储部件，用于存储使用权限作为内容使用信息，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

信息管理装置还可以包括用于回放内容的回放部件，并且只有当加到内容的标识信息与由标识信息获得部件获得的标识信息相同时，回放部件才可以回放内容。

内容获取部件通过连至信息管理装置的记录介质获取内容。

标识信息获得部件可以将自身生成的随机数加到内容等作为标识信息。标识信息可以从外部设备等提供。

本发明的一种用于信息管理装置的信息管理方法，包括：内容获取步骤，获取内容；标识信息获得步骤，获得唯一标识信息和内容标识信息，其中所述唯一标识信息用于标识所述信息管理装置并且唯一于所述信息管理装置；内容存储步骤，存储在内容获取步骤获取的内容，其中该内容被加有在标识信息获得步骤中所获得的所述唯一标识信息和所述内容标识信息；以及使用权限存储步骤，存储使用权限作为内容使用信息，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

本发明的一种程序使控制用于管理内容的信息管理装置的计算机执行如下步骤：内容获取控制步骤，控制获取内容；标识信息获得控制步骤，控制获得用于标识信息管理装置的标识信息；内容存储控制步骤，控制存储在内容获取控制步骤获取的内容，其中加有在标识信息获得控制步骤获得的标识信息；以及使用权限存储控制步骤，控制存储使用权限作为内容使用信息，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

在本发明的信息管理装置和方法及程序中，获取内容，并且获得用于标识信息管理装置的标识信息。存储加有所获得标识信息的所获取内容，并且存储使用权限作为内容使用信息，其中，使用权限包括标识信息以及用于允许在具有与加到内容的标识信息相同的标识信息的装置上使用内容的信息。

附图说明

图 1 是相关技术的内容管理系统的示意图；

图 2 是本发明的内容提供系统的图；

图 3 是图 2 所示的客户机的方框图；

图 4 示出了密钥结构的图；

图 5 是类别节点图；

图 6 示出了节点与设备之间的对应关系的图；

图 7 示出了激活密钥块的图；

图 8 示出了另一激活密钥块的图；

图 9 示出了激活密钥块使用的示意图；

图 10 是激活密钥块格式的示例图；

图 11 示出了激活密钥块的标记(tag)结构的图；

图 12 是本发明的内容管理系统的示意图；

图 13 示出了图 1 所示的客户机的内容检索过程的流程图；

图 14 是内容格式的示例图；

图 15 示出了图 1 所示的客户机的使用权限生成过程的流程图；

图 16 是使用权限格式的示例图；

图 17 示出了图 1 所示的客户机的内容回放过程的流程图；

图 18 示出了图 17 所示步骤 S46 的解码过程细节的流程图；

图 19 是图 18 所示的解码过程的示意图；

图 20 是包括在图 19 所示的 EKB 中的信息的示例图。

最佳实施方式

图 2 示出了本发明的内容提供系统。客户机 1-1 和 1-2(除非需要相互区分它们，否则下面简称作客户机 1)连接到因特网 2。虽然在本例中仅示出两个客户机，但是可以有任意数目的客户机连接到因特网 2。

连接到因特网 2 的还有：内容服务器 3，用于向客户机 1 提供内容；许可证服务器 4，用于向客户机 1 提供使用由内容服务器 3 提供的内容所需的使用权限；以及收费服务器 5，向接收使用权限的客户机 1 收费。

可以有任意数目的内容服务器 3、许可证服务器 4 和收费服务器 5 连接到因特网 2。

图 3 示出客户机 1 的结构。

在图 3 中，CPU(Central Processing Unit，中央处理单元)21 根据存储在 ROM(Read Only Memory，只读存储器)22 中的程序或者从存储单元 28 装载到 RAM(Random Access Memory，随机存取存储器)23 中的程序执行各种处理。计时器 20 测量时间，并且将时间信息提供给 CPU 21。RAM 23 根据需要还存储 CPU 21 执行各种处理所需的数据等。

加密/解密单元 24 对内容进行加密，并且对加密内容进行解码。编解码器 25 根据例如 ATRAC(Adaptive Transform Acoustic Coding，自适应变换声学

编码)3 等对内容进行编码，并且将编码内容提供给通过输入/输出接口 32 与驱动器 30 连接的半导体存储器 44 以进行记录。否则，编解码器 25 对通过驱动器 30 从半导体存储器 44 读取的编码数据进行解码。半导体存储器 44 可以由例如存储棒(商标)等形成。

CPU 21、ROM 22、RAM 23、加密/解密单元 24 以及编解码器 25 通过总线 31 相互连接。输入/输出接口 32 也与总线 31 连接。

包括键盘、鼠标等的输入单元 26、包括由 CRT(Cathode Ray Tube, 阴极射线管)、LCD(Liquid Crystal Display, 液晶显示器)等形成的显示器、扬声器等的输出单元 27、包括硬盘等的存储单元 28 以及包括调制解调器、终端适配器等的通信单元 29 与输入/输出接口 32 连接。通信单元 29 通过因特网 2 执行通信。通信单元 29 还与另一客户机执行模拟或数字信号通信。

与输入/输出接口 32 相连的还有驱动器 30，如果必要，磁盘 41、光盘 42、磁光盘 43、半导体存储器 44 等根据需要与之相连，并且如果必要，将从中读取的计算机程序安装在存储单元 28 中。

虽未示出，但内容服务器 3、许可证服务器 4 和收费服务器 5 基本上也由与图 3 所示的客户机 1 具有类似结构的计算机形成。在下面描述中，图 3 所示的结构也可以用作内容服务器 3、许可证服务器 4 或收费服务器 5 的结构。

在本发明中，如图 4 所示，设备和密钥根据广播加密方案原理来管理。密钥形成分层树，其中，底层叶子表示唯一于各设备的密钥。在本发明的系统中采用的基于分层树的密钥管理机制在日本未审专利申请公开 No. 2001-352321 中有描述。在图 4 所示的例子中，生成与编号为 0 到 15 的 16 个设备相对应的密钥。

在图 4 中，密钥分配给以圆圈表示的树节点。在本例中，根密钥 KR(适当时也称作 Kroot)分配给顶层根节点，并且密钥 K0 和 K1 分配给第二层节点。密钥 K00 到 K11 分配给第三层节点，并且密钥 K000 到 K111 分配给第四层节点。密钥 K0000 到 K1111 分配给底层叶子节点(设备节点)。

由于分层结构，例如，高于密钥 K0010 和 K0011 的密钥为密钥 K001，并且高于密钥 K000 和 K001 的密钥为密钥 K00。同样，高于密钥 K00 和 K01 的密钥为密钥 K0，并且高于密钥 K0 和 K1 的密钥为密钥 KR。

使用内容的密钥根据以底层设备节点(叶子)开始且以顶层根节点结束的

一条路径上的各节点所对应的密钥来管理。例如，在与编号为 3 的叶子相对应的设备上使用内容的密钥根据包括密钥 K0011、K001、K00、K0 和 KR 的路径上的密钥来管理。

在本发明的系统中，如图 5 所示，设备密钥和内容密钥由根据图 4 所示的原理形成的密钥系统来管理。在图 5 所示的例子中，8+24+32 层节点形成一树，并且在低于并包括根节点层的八层中的节点与类别相关联。在此所用的术语“类别”是指诸如使用半导体存储器例如存储棒的设备类别或者数字广播接收设备类别这样的类别。这些类别节点之一与用作使用权限管理系统的本系统(适当时，以下称作 T 系统)相关联。

与低于 T 系统节点层的第 24 层节点相对应的密钥与服务提供商或由服务提供商提供的服务相关联。因此，在图 5 所示的例子中，可以分配 2^{24}(约 16 兆)服务提供商或服务。在 32 层的底部，可以分配 2^{32}(约 4 吉)用户(客户机 1)。与以底部第 32 层节点开始且以 T 系统节点结束的路径上的各节点相对应的密钥组成 DNK(Device Node Key, 设备节点密钥)，并且与底层叶子相对应的 ID 称作叶子 ID。

用来对内容进行加密的内容密钥使用更新根密钥 KR’来加密，并且高层的更新节点密钥使用直接下一层的更新节点密钥来加密。这些加密密钥安排在 EKB(激活密钥块)中(如下面参照图 7 所述)。

在比 EKB 高一层的层中更新节点密钥使用 EKB 底部的节点密钥或叶子密钥来加密，然后安排在 EKB 中。客户机 1 使用在服务数据中描述的任一 DNK 密钥来对在与内容一起发行的 EKB 中描述的最接近的上一层的更新节点密钥进行解码，并且使用结果节点密钥来对在 EKB 中描述的该层高一层的层中的更新节点密钥进行解码。依次执行类似处理，从而客户机 1 可以获得更新根密钥 KR’。服务数据是当登记客户机 1 的信息时从许可证服务器 4 发送的数据。作为允许使用特定内容的信息的下述服务数据和使用权限的组合称作许可证。

图 6 示出了分层树结构中类别的特定例子。

在图 6 中，在分层树的顶部设置根密钥 KR 2301，并且在较低中间层设置节点密钥 2302，并且在底部设置叶子密钥 2303。各设备均具有由独有叶子密钥、以叶子密钥开始且以根密钥结束的一系列节点密钥以及根密钥形成的设备节点密钥(DNK)。

从顶层向下直到第 M 层(在图 5 所示的例子中，M=8)的预定节点设为类别节点 2304。换句话说，第 M 层的各节点是向其分配设备的特定类别的节点。第 M 层中的节点之一作为根来分配，并且在第 M+1 和以下层的节点以及叶子是与属于该类别的设备相关联的节点和叶子。

例如，图 6 所示的第 M 层节点 2305 分配为类别[存储棒(商标)]，并且该节点和节点之下叶子设为包括使用存储棒的各种设备的类别特定节点或叶子。因此，低于节点 2305 的节点限定为与限定在存储棒类别内的设备相关联的一组节点和叶子。

第 M 层之下若干层的层中的节点可以设为子类别节点 2306。在图 6 所示的例子中，类别[存储棒]节点 2305 的层之下两层的层中的节点分配为属于使用存储棒的设备类别的子类别节点，称作[回放单功能设备]节点 2306。在作为子类别节点的回放单功能设备节点 2306 之下配置属于回放单功能设备类别的配备有音乐回放功能的电话节点 2307，并且在其下配置属于配备有音乐回放功能的电话类别的[PHS]节点 2308 和[蜂窝电话]节点 2309。

类别和子类别可以根据设备类型以及任意单元如制造商、内容提供商、结帐机构等的唯一管理节点即处理单元、管理单元或提供服务单元(以下统称作实体)来设置。

作为例子，假定一个类别节点分配为特定于由一家游戏设备制造商出品的游戏设备 XYZ 的顶节点，低于顶节点层的层中的节点密钥和叶子密钥可以存储在由该制造商出品的游戏设备 XYZ 中，并且可以出售游戏设备 XYZ。此后，生成并发行由顶节点密钥之下的节点密钥和叶子密钥形成的 EKB，因此只有在顶节点之下的设备(游戏设备 XYZ)上才允许发行加密内容、发行各种密钥、更新密钥等。

因此，可以在不影响不属于顶节点而属于另一类别节点的设备的情况下更新密钥等。

如果在时间 t 发现由设备 3 拥有的密钥 K0011、K001、K00、K0 和 KR 被攻击者(黑客)泄露，则为了保护以后要在系统(设备 0、1、2 和 3 的组)中交换的数据，设备 3 必须与系统隔开。因此，需要将节点密钥 K001、K00、K0 和 KR 分别更新成新密钥 K(t)001、K(t)00、K(t)0 和 K(t)R，并且将更新密钥报告给设备 0、1 和 2。在此所用的 K(t)aaa 表示密钥 Kaaa 的 t 代更新密钥。

现在将描述用于发行更新密钥的过程。密钥更新操作通过在网络上或者

通过预定记录介质将一个由例如图 7 所示的 EKB 形成的表发送到设备 0、1 和 2 来执行，其中，预定记录介质中存储有该表。EKB 由用于将新更新的密钥发行到与图 4 所示的树的叶子(底部节点)相对应的设备的加密密钥形成。

图 7 所示的 EKB 形成为具有如下数据结构的数据块，其中，可以只更新其节点密钥必须被更新的设备。图 7 示出用于将 t 代更新节点密钥发行给图 4 所示的树中的节点 0、1 和 2 的数据块。

从图 4 可以看出，更新节点密钥 K(t)00、K(t)0 和 K(t)R 必须发送到设备 0 和 1，并且更新节点密钥 K(t)001、K(t)00、K(t)0 和 K(t)R 必须发送到设备 2。

如图 7 所示，EKB 包含多个加密密钥。例如，图 7 所示的底部加密密钥为 Enc(K0010, K(t)001)。这意味着更新节点密钥 K(t)001 使用设备 2 的叶子密钥 K0010 来加密，因此设备 2 可以使用其叶子密钥 K0010 来对加密密钥进行解码以获得更新节点密钥 K(t)001。

设备 2 还可以使用通过解码获得的更新节点密钥 K(t)001 来对图 7 所示的下起第二行的加密密钥 Enc(K(t)001, K(t)00)进行解码以获得更新节点密钥 K(t)00。

同样，设备 2 可以对图 7 所示的上起第二行的加密密钥 Enc(K(t)00, K(t)0)进行解码以获得更新节点密钥 K(t)0，并且可以使用结果密钥来对图 7 所示的上起第一行的加密密钥 Enc(K(t)0, K(t)R)进行解码以获得更新根密钥 K(t)R。

节点密钥 K000 不被更新，并且节点 0 和 1 所需的更新节点密钥为 K(t)00、K(t)0 和 K(t)R。

节点 0 和 1 使用设备密钥 K0000 和 K0001 来对图 7 所示的上起第三行的加密密钥 Enc(K000, K(t)00)进行解码以获得更新节点密钥 K(t)00。同样，节点 0 和 1 依次对图 7 所示的上起第二行的加密密钥 Enc(K(t)00, K(t)0)进行解码以获得更新节点密钥 K(t)0，并且进一步对图 7 所示的上起第一行的加密密钥 Enc(K(t)0, K(t)R)进行解码以获得更新根密钥 K(t)R。从而，设备 0、1 和 2 可以获得更新密钥 K(t)R。

图 7 所示的索引表示用作解码密钥来对图 7 的右列所示的加密密钥进行解码的节点密钥和叶子密钥的绝对地址。

在无需更新图 4 所示的树中的较高层节点密钥 K(t)0 和 K(t)R 而只需更新节点密钥 K00 的情况下，可以使用图 8 所示的 EKB 来将更新节点密钥 K(t)00 发行到设备 0、1 和 2。

图 8 所示的 EKB 对于例如发行在特定组内共享的新内容密钥是有用的。

例如，假定图 4 所示的以虚线圈起的组内设备 0、1、2 和 3 使用记录介质并且必须分配一个新公共内容密钥 K(t)con 给这些设备。因而，与图 8 所示的 EKB 一起发行通过使用公共于设备 0、1、2 和 3 的节点密钥 K00 的更新 K(t)00 对新的公共更新内容密钥 K(t)con 进行加密而形成的数据 Enc(K(t)00, K(t)con)。该发行允许发行不能被其他组内设备如设备 4 解码的数据。

具体地说，设备 0、1 和 2 使用通过处理 EKB 而获得的密钥 K(t)00 对加密数据进行解码以获得时间 t 的内容密钥 K(t)con。

图 9 是作为用于获得时间 t 的内容密钥 K(t)con 的过程示出设备 0 的处理的示意图，其中，通过预定记录介质向设备 0 提供通过使用 K(t)00 对新公共内容密钥 K(t)con 进行加密而形成的数据 Enc(K(t)00, K(t)con)以及图 8 所示的 EKB。在图 9 所示的例子中，通过 EKB 形成的加密消息数据是内容密钥 K(t)con。

如图 9 所示，设备 0 使用存储在记录介质中的 t 代 EKB 以及预先向其分配的节点密钥 K000 执行上述 EKB 处理(顺序对密钥进行解码的处理)，以生成节点密钥 K(t)00。设备 0 还使用解码更新节点密钥 K(t)00 对更新内容密钥 K(t)con 进行解码，并且为以后使用起见，使用仅由设备 0 拥有的叶子密钥 K0000 对更新内容密钥 K(t)con 进行加密以作存储。

图 10 是 EKB 格式的示例图，并且包括各种信息的 EKB 包含在内容数据首标中。

版本 61 是表示 EKB 版本的标识符。版本 61 具有标识最近 EKB 并表示与内容的对应关系的功能。深度 62 表示 EKB 所发行的设备在分层树中的层数。数据指针 63 是表示数据部分 66 在 EKB 中的位置的指针，并且标记指针 64 和签名指针 65 分别是表示标记部分 67 和签名 68 的位置的指针。

数据部分 66 包含例如通过对更新节点密钥进行加密而获得的数据。数据部分 66 例如包含图 9 所示的更新节点密钥的加密密钥等。

标记部分 67 包括表示存储在数据部分 66 中的加密节点密钥与叶子密钥之间的位置关系的标记。标记的分配规则将参照图 11 进行描述。

在图 11 所示的例子中，如图 11B 所示，所要传递的数据是图 7 所示的加密密钥。包含在加密密钥中的顶节点的地址称作顶节点地址。

在本例中，包含根密钥的更新密钥 K(t)R，并且顶节点地址为 KR。例如，

顶层数据 Enc(K(t)0, K(t)R)位于图 11A 所示的分层树中的位置 P0。下一层数据为 Enc(K(t)00, K(t)0)，并且位于树中前一数据 Enc(K(t)0, K(t)R)的左下位置 P00。

因此，当数据位于树中预定位置之下时，各标记设为 0，否则设为 1。标记定义为{左(L)标记，右(R)标记}。

图 11B 所示的顶层数据 Enc(K(t)0, K(t)R)分配为 L 标记=0，因为数据位于对应位置 P0 的左下位置 P00，并且分配为 R 标记=1，因为数据不位于位置 P0 的右下位置。其余数据也是分配标记，并且配置图 11C 所示的数据串和标记串。

分配这些标记是为了表示对应数据 Enc(Kxxx, Kyyy)在树中的位置。存储在数据部分 66 中的密钥数据 Enc(Kxxx, Kyyy)...仅是加密密钥的数据序列；然而，作为数据存储的加密密钥在树中的位置可以根据这些标记来确定。例如，可以配置下面使用与图 7 或 8 所示的加密数据相对应的节点索引而不使用标记的数据结构:

0: Enc(K(t)0, K(t)R)

00: Enc(K(t)00, K(t)0)

000: Enc(K(t)000, K(t)00)

...

然而，该使用索引的数据结构具有大数据量，并且不适于网络发行等。相反，使用上述标记作为表示密钥位置的索引数据来以较小数据量确定密钥位置。

回到图 10，签名 68 包括由例如签发 EKB 的密钥管理中心(许可证服务器 4)、内容提供商(内容服务器 3)、结帐机构(收费服务器 5)等处理的电子签名。接收 EKB 的设备检查包含在 EKB 中的签名以判定所获得的 EKB 是否为由授权签发者签发的 EKB。

图 12 示出了由客户机 1 检索记录在 CD 81 中的内容的上述密钥管理系统的过程的示意图。

客户机 1 的 CPU 21 执行预定程序来控制提取(ripping)模块 91，从而检索存储在与客户机 1 相连的 CD 81 中的内容。

// CPU 21 将内容 ID(CID)和唯一于客户机 1 的 ID(唯一 ID(Uniq ID))加到由提取模块 91 检索的内容，并且使结果数据存储在存储单元 28 中。唯一 ID 例如是具有预定位数的随机数，并且作为加到该内容的唯一 ID 的相同的唯一 ID

由客户机 1 保存。

CPU 21 还生成使用由提取（ripping）模块 91 检索的内容的使用权限，作为上述密钥管理系统中的服务。例如，假定提取模块 91 是可以三次转出(check out)所检索内容的模块，则生成具有表示允许转出三次的使用条件的描述的使用权限。使用权限还规定加到内容的内容 ID 和唯一 ID，并且内容和使用权限相互对应。

当回放如此检索的内容时，判定使用权限是否允许在要回放内容的客户机上进行回放，而且判定加到内容的唯一 ID 和要回放内容的客户机的唯一 ID 是否相同。只有当使用权限允许回放内容并且加到内容的唯一 ID 和要生成内容的客户机的唯一 ID 相同时，才回放内容。因此，例如通过复制内容和使用权限而仅获得它们的客户机，即使使用权限允许回放，也不能回放内容。

现在将参照一个流程图描述用于检索和使用内容的客户机 1 的一系列操作。

首先，参照图 13 所示的流程图描述客户机 1 检索内容的过程。

例如，当其中记录有内容的预定记录介质如 CD 81(光盘 42)连至客户机 1 的驱动器 30 并且指示检索内容时，客户机 1 的 CPU 21 在步骤 S1 控制通过执行预定程序而形成的提取模块 91 来检索内容。

在步骤 S2，CPU 21 生成用于标识内容的内容 ID。在步骤 S3，CPU 21 判定是否有唯一于客户机 1(提取模块 91)的唯一 ID 存储在例如存储单元 28 中。如果判定尚未存储唯一 ID，则在步骤 S4，生成具有预定位数的唯一 ID。所生成的唯一 ID 保存在存储单元 28 中。

代替由客户机 1 生成的唯一 ID，例如，可以使用当客户机 1 的用户在许可证服务器 4 中登记预定信息时由许可证服务器 4 分配给客户机 1 从而允许在提取模块 91 上使用的唯一 ID。如果以这种方式分配了唯一 ID 或者如果在先前提取操作期间已经生成了唯一 ID，则在图 13 所示的步骤 S3 判定存在唯一 ID，并且跳过在步骤 S4 执行的操作。

在步骤 S5，CPU 21 在描述预定内容属性信息的“属性”区域中描述内容 ID 和唯一 ID。内容格式将在下面进行详述。

在步骤 S6，CPU 21 使用其自己的秘密密钥根据作为属性信息描述的信息生成数字签名。秘密密钥例如是当登记客户机 1 的信息时从许可证服务器 4 递送的。

在步骤 S7，CPU 21 生成要与内容相关联记录的首标数据。首标数据包括内容 ID、使用权限 ID、表示获得使用权限的访问目的地的 URL 以及水印。

在步骤 S8，CPU 21 使用其自己的秘密密钥来根据在步骤 S7 生成的首标数据生成数字签名。在步骤 S9，CPU 21 控制加密/解密单元 24 以使用所生成的内容密钥对内容进行加密。在步骤 S10，将所生成的内容和信息如附属于它的首标保存在存储单元 28 中。

图 14 示出内容的示例格式。

如图 14 所示，内容包括首标、EKB、通过使用根密钥 Kroot 对内容密钥 Kc 进行加密而获得的数据(Enc(Kroot, Kc))、其中描述内容 ID 和唯一 ID 的属性信息(属性)、证书(Cert)、根据首标生成的数字签名(签名(首标))、通过使用内容密钥 Kc 对内容进行加密而获得的数据(Enc(Kc, Content))、元数据(Meta Data)以及标记(Mark)。

在首标中，描述有内容 ID(CID)、用于标识内容使用权限的用户权限 ID(用户权限 ID)、从其获得使用权限的一方(客户机 1)的 URL 以及水印(WM)。

内容属性包括内容 ID、作为用于标识内容提供商的标识信息的记录公司 ID、作为用于标识艺术家的标识信息的艺术家 ID、唯一 ID 等。在本实施例中，属性用来指定由使用权限限定的内容。

元数据包括与内容相关的各种信息；例如，对于音乐内容，将包括封皮、照片和歌词的数据加到内容作为元数据。在标记中，描述用户 ID(叶子 ID)、所有权标志、首次使用时间、复制计数以及根据该信息生成的数字签名。例如，当直接购买允许仅在预定期限内使用内容的使用权限时(当改变有效期从而永久使用内容时)，增加标记的所有权标志。在标记的复制计数中，描述包括内容复制时间等的记录(日志)。

虽然所描述的是从 CD 81 中获取(提取)内容，但是客户机 1 还保存在因特网 2 等上从预定服务器获取的内容，其中也加有客户机 1 的内容 ID 和唯一 ID。

下面，参照图 15 所示的流程图描述客户机 1 生成所检索内容的使用权限的过程。

在步骤 S21，从存储单元 28 读取要加到由提取模块 91 检索的内容的预设使用权限作为在图 13 所示的过程中检索的内容的使用权限。存储在存储单元 28 中的使用权限包括如使用权限 ID、版本号、创建日期和有效期的信息。

在步骤S22，CPU 21将唯一ID和表示只有具有与作为内容属性信息描述的唯一ID相同的ID的客户机1才允许回放内容的信息加到所选使用权限。在步骤S23，CPU 21选择使用条件并且添加它。在提取模块91限定为所检索内容可以同时转出到提取模块91三次的例子中，选择表示允许三次转出的使用条件。在提取模块91允许自由复制所检索内容的另一个例子中，选择表示该允许的使用条件。

在步骤S24，CPU 21生成在如此选择的使用权限中描述的数据的数字签名，并且添加它。在步骤S25，将加有数字签名的使用权限保存在存储单元28中。

图16是使用权限格式的示例图。

“版本”是通过使用点号分隔主版本和次版本来描述的使用权限版本信息。“档次(Profile)”是以十进制整数值描述的用于指定使用权限描述方法限制的信息。“使用权限 ID”是以十六进制常数值描述的用于标识使用权限的标识信息。“创建日期”表示创建使用权限的日期。“有效期”表示使用权限的有效期。“9999 23:59:59”的有效期表示无限制有效期。“使用条件”包含如下信息，例如，根据使用权限可以使用内容的截止日期、根据使用权限可以回放内容的回放限制、内容的最大回放次数、根据使用权限可以复制内容的次数(复制允许次数)、最大转出次数、表示根据使用权限是否可以将内容记录到CD-R上的信息、可以将内容复制到PD(Portal Device, 便携式设备)的次数、表示是否可以转让使用权限的信息、表示是否必须维护使用日志的信息等等。使用条件的电子签名是对应于使用条件的电子签名。

“常数值”是在使用条件或使用状态中引用的常数值。“唯一 ID”是当检索内容时生成的。“电子签名”是整个使用权限的电子签名。“证书”是包含许可证服务器4的公开密钥的证书。

客户机1的存储单元28存储使用权限的使用条件以及作为表示内容或使用权限状态的信息的使用状态(内容条件)。使用状态包括如下信息，例如，内容根据使用权限已被回放的次数、内容已被复制的次数、内容已被转出的次数、内容的首次回放时间和日期、内容被记录到 CD-R 上的次数以及其他表示内容或使用权限记录的信息。根据包括在使用权限中的使用条件和与使用权限一起存储在存储单元28中的使用状态来检查内容回放要求。例如，当存储在使用状态中的内容已被回放的次数小于包括在使用条件中的内容回放最

大次数时，判定满足回放要求。

现在参照图 17 所示的流程图描述客户机 1 使用提取模块 91 检索内容以回放内容的过程。

在步骤 S41，客户机 1 的 CPU 21 根据内容 ID 从存储单元 28 读取由操作输入单元 26 的用户指示的内容，并且读取作为读取内容的属性信息描述的唯一 ID。在步骤 S42，CPU 21 根据使用权限 ID 读取指示回放的内容的使用权限，并且读取在所读取使用权限中描述的唯一 ID。

在步骤 S43，CPU 21 从存储单元 28 读取所保存的唯一 ID，也就是，客户机 1 的唯一 ID。然后，在步骤 S44，判定这些唯一 ID 即在内容中描述的唯一 ID、在使用权限中描述的唯一 ID 与保存在客户机 1 中的唯一 ID 是否相同。可以仅判定在内容中描述的唯一 ID 与保存在客户机 1 中的唯一 ID 是否相同。

如果 CPU 21 在步骤 S44 判定所有唯一 ID 相同，则在步骤 S45，它根据其中描述的使用条件，判定使用权限是否准许使用内容。例如，CPU 21 比较在使用权限中描述的有效期(参见图 16)与由计时器 20 测量的当前时间，以判定使用权限是否有效或者，换句话说，是否准许使用内容。

如果在步骤 S45 判定使用权限准许使用内容，则在步骤 S46，CPU 21 对在 RAM 23 中存储(读取)的内容进行解码。下面将参照图 18 的流程图描述在步骤 S46 执行的内容解码过程。

在步骤 S47，CPU 21 将由加密/解密单元 24 解码的内容提供给编解码器 25 以进行解码。然后，CPU 21 通过输入/输出接口 32 将由编解码器 25 解码的数据提供给输出单元 27，以进行数模转换，从而从扬声器输出结果数据。

如果在步骤 S44 判定在内容中描述的唯一 ID 与保存在客户机 1 中的唯一 ID(以及在使用权限中描述的唯一 ID)不同，以及如果在步骤 S45 判定使用权限不准许回放内容，则在步骤 S48，执行错误处理。然后，过程结束。

在图 17 所示的步骤 S46 执行的客户解码过程的细节参照图 18 所示的流程图来描述。

在步骤 S61，客户机 1 的 CPU 21 根据包含在服务数据中且从许可证服务器 4 发送的 DNK 对包含在 EKB 中的密钥信息进行顺序解码，以获得根密钥 Kroot(KR)。当 CPU 21 获得根密钥 Kroot 时，则在步骤 S62，使用根密钥 Kroot 对内容密钥 Kc 进行解码。如图 14 所示，内容包括通过使用根密钥 Kroot 对内容密钥 Kc 进行加密而形成的数据 Enc(Kroot, Kc)。

在步骤 S63，CPU 21 使用在步骤 S62 获得的内容密钥 Kc 对内容进行解码。

图 19 是上述解码过程的示意图。在图 19 中，内容由客户机 1 保存，并且仅示出图 14 所示的信息中的主要信息。

具体地说，根据从许可证服务器 4 发送到客户机 1 的 DNK 从 EKB 获得根密钥 Kroot(图 18 的步骤 S61)，并且使用所获得的根密钥 Kroot 对数据 Enc(Kroot, Kc)进行解码，从而获得内容密钥 Kc(图 18 的步骤 S62)。然后，使用内容密钥 Kc 对数据 Enc(Kc, Content)进行解码，以获得内容(Content)(图 18 的步骤 S63)。如图 20 所示，图 14 和 19 所示的 EKB 包括通过使用 DNK 对根密钥 Kroot 进行加密而形成的数据 Enc(DNK, Kroot)。

通过以上述方式控制内容回放，即使客户机(其唯一 ID 未被管理的客户机)以非授权方式获得内容和使用权限，也不能回放内容。

在前述过程中，当允许转出由客户机 1 检索的内容时(当在使用条件中规定所允许转出时)，可以将使用预定方法加密的内容、使用权限和客户机 1 的唯一 ID 发送到要将内容从客户机 1 向其转出的另一客户机。在这种情况下，接收到该信息的客户机执行类似于图 17 和 18 所示的处理来回放内容。因此，在首先检索内容的客户机 1 的控制下执行内容的转出/转入(checkout/checkin)等。

在前述实施例中，内容属性和使用权限的内容条件用来指定使用内容所需的使用权限；然而，本发明不限于此。例如，内容可以包含使用内容所需的使用权限的使用权限 ID，在这种情况下，一旦内容被指定，则可以唯一确定使用它所需的使用权限，而无需确定匹配的过程。

工业应用

根据本发明，可以提供内容。

此外，根据本发明，可以防止内容的非授权使用。

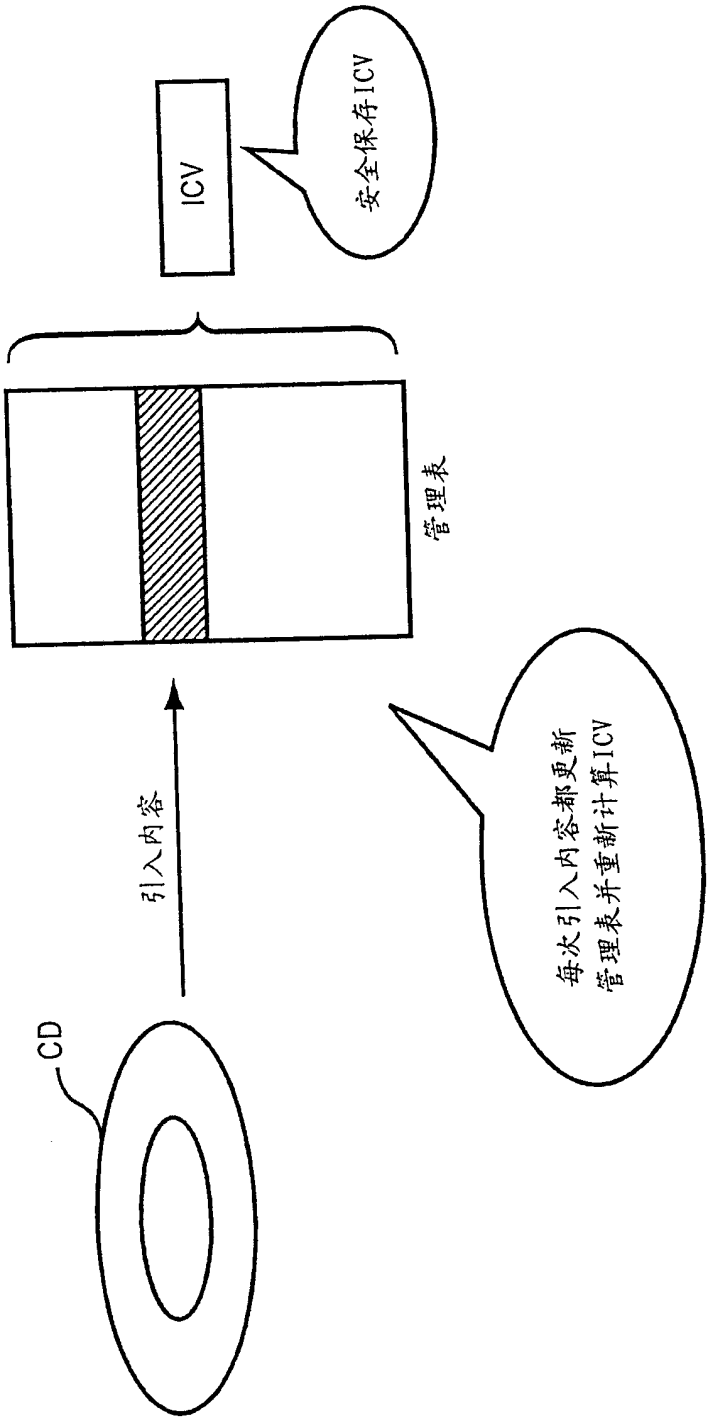


图 1

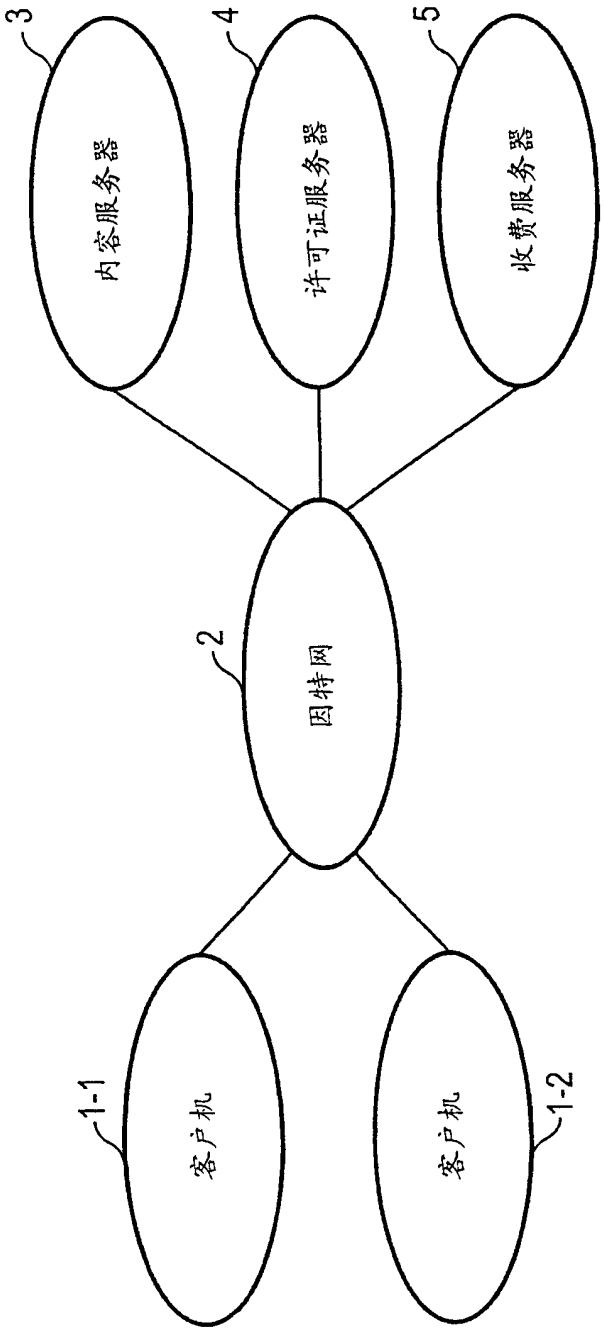


图 2

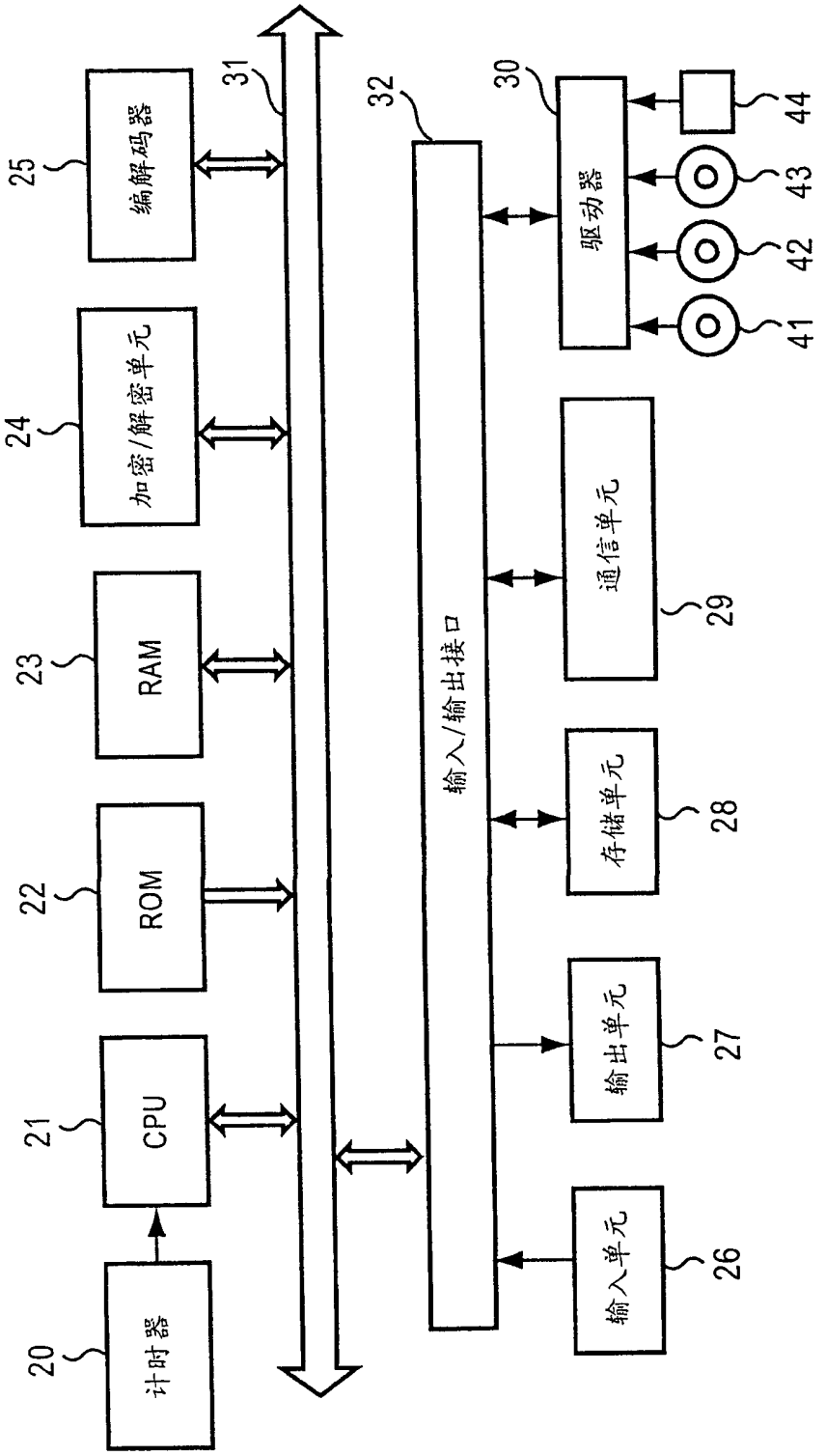

计时器
CPU
ROM
RAM
加密/解密单元
编解码器
输入单元
输出单元
存储单元
通信单元
输入/输出接口
驱动器
20
21
22
23
24
25
26
27
28
29
30
31
32
41
42
43
44

图 3

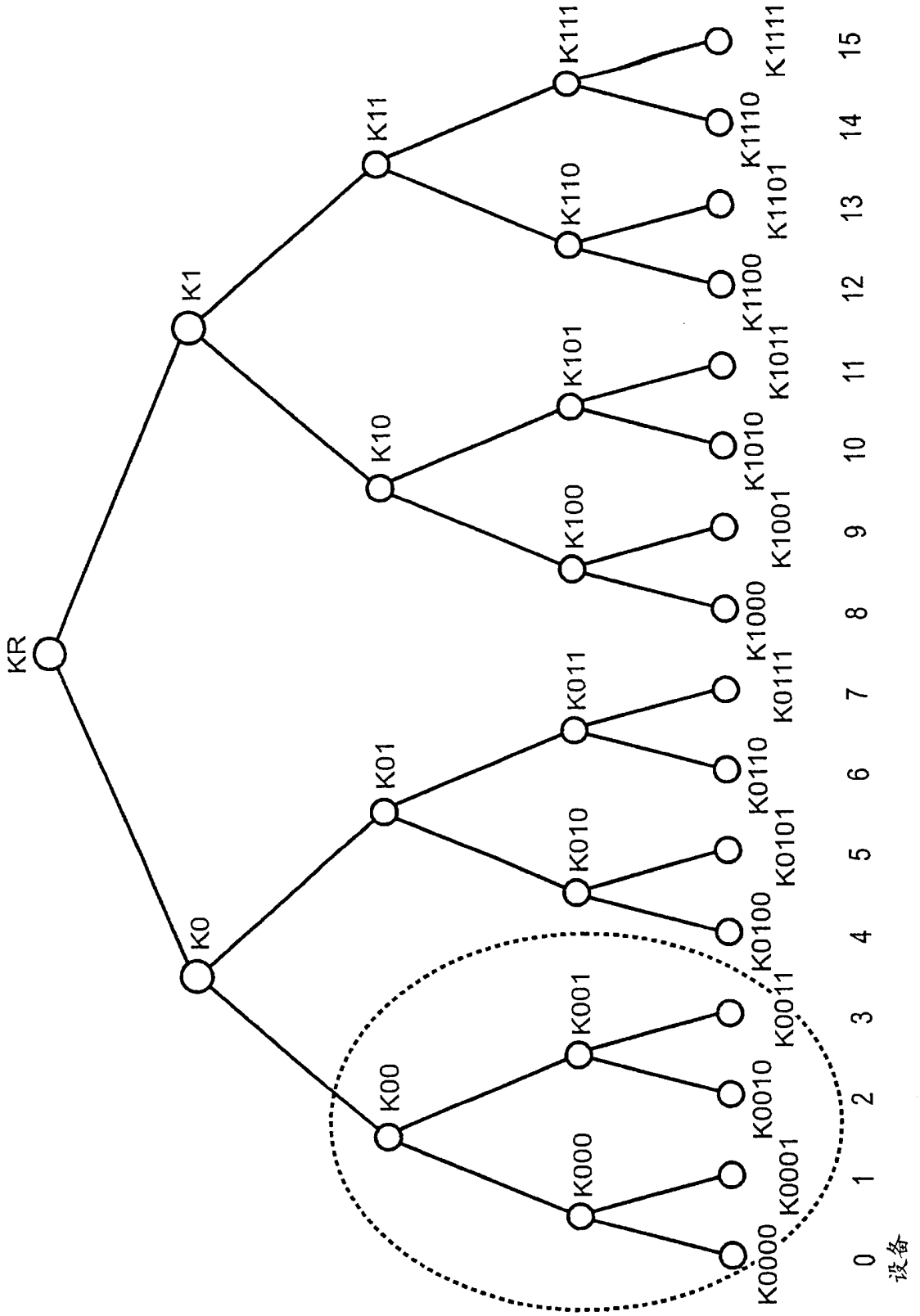

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
设备

图 4

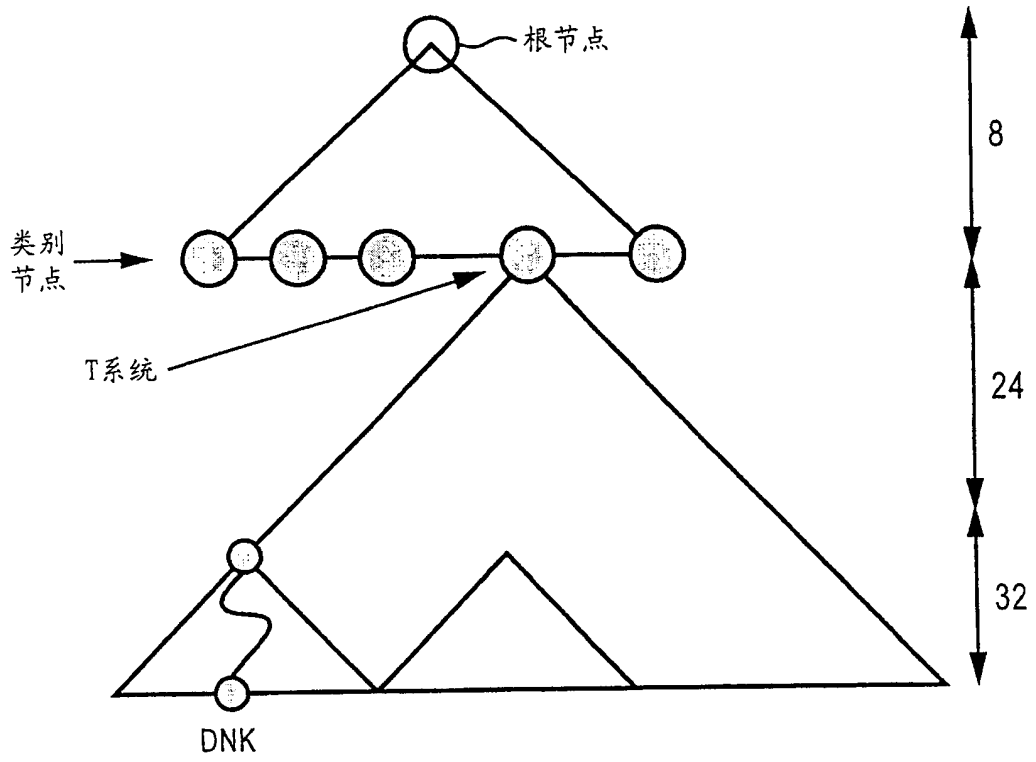


图 5

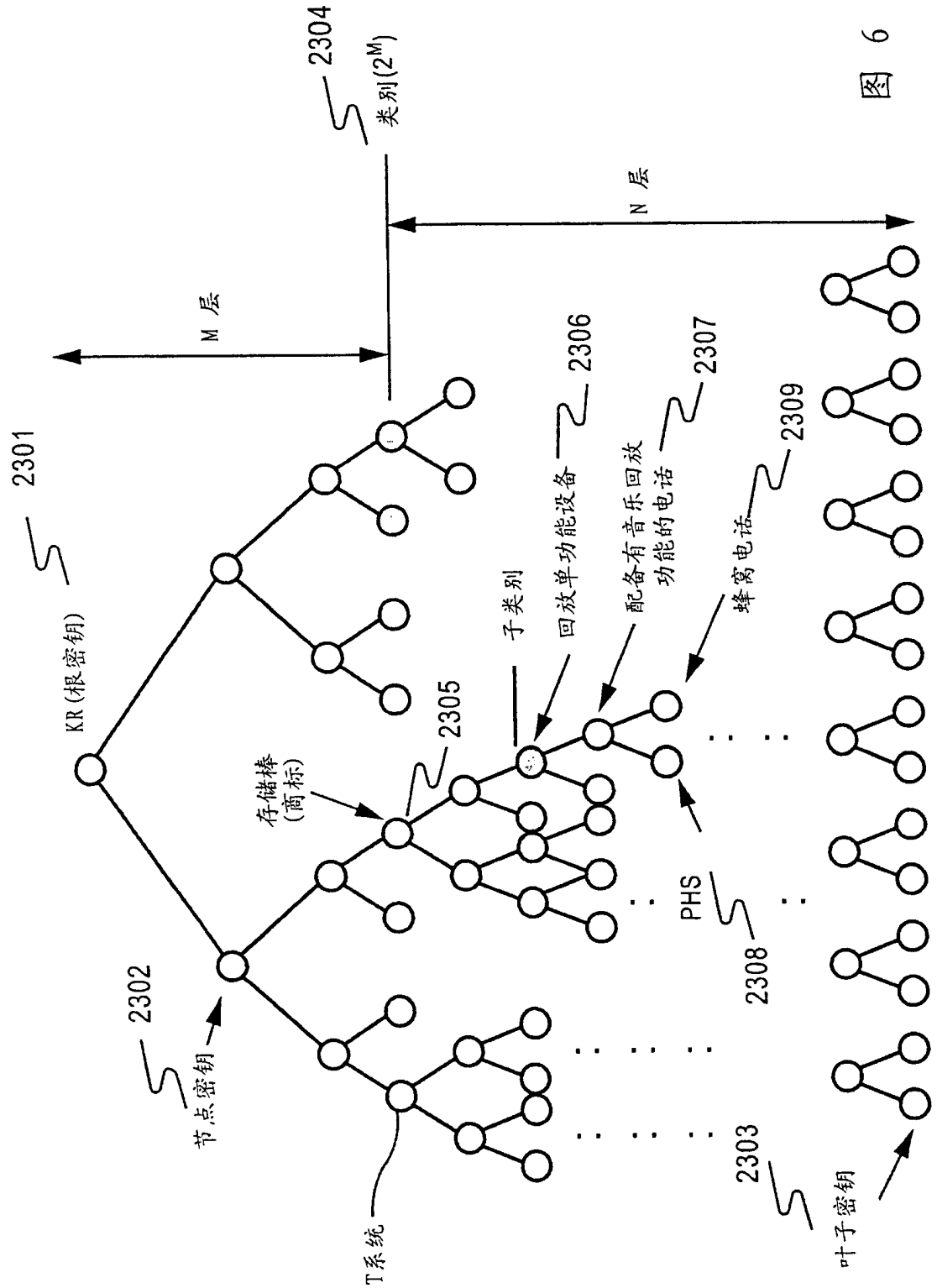

2301
KR(根密钥)
2304
类别(2^M)
M 层
N 层
2306
子类别
回放单功能设备
2307
配备有音乐回放
功能的电话
2309
蜂窝电话
2305
存储棒
(商标)
2302
节点密钥
PHS
2308
T系统
2303
叶子密钥

图 6

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)

图 7

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 8

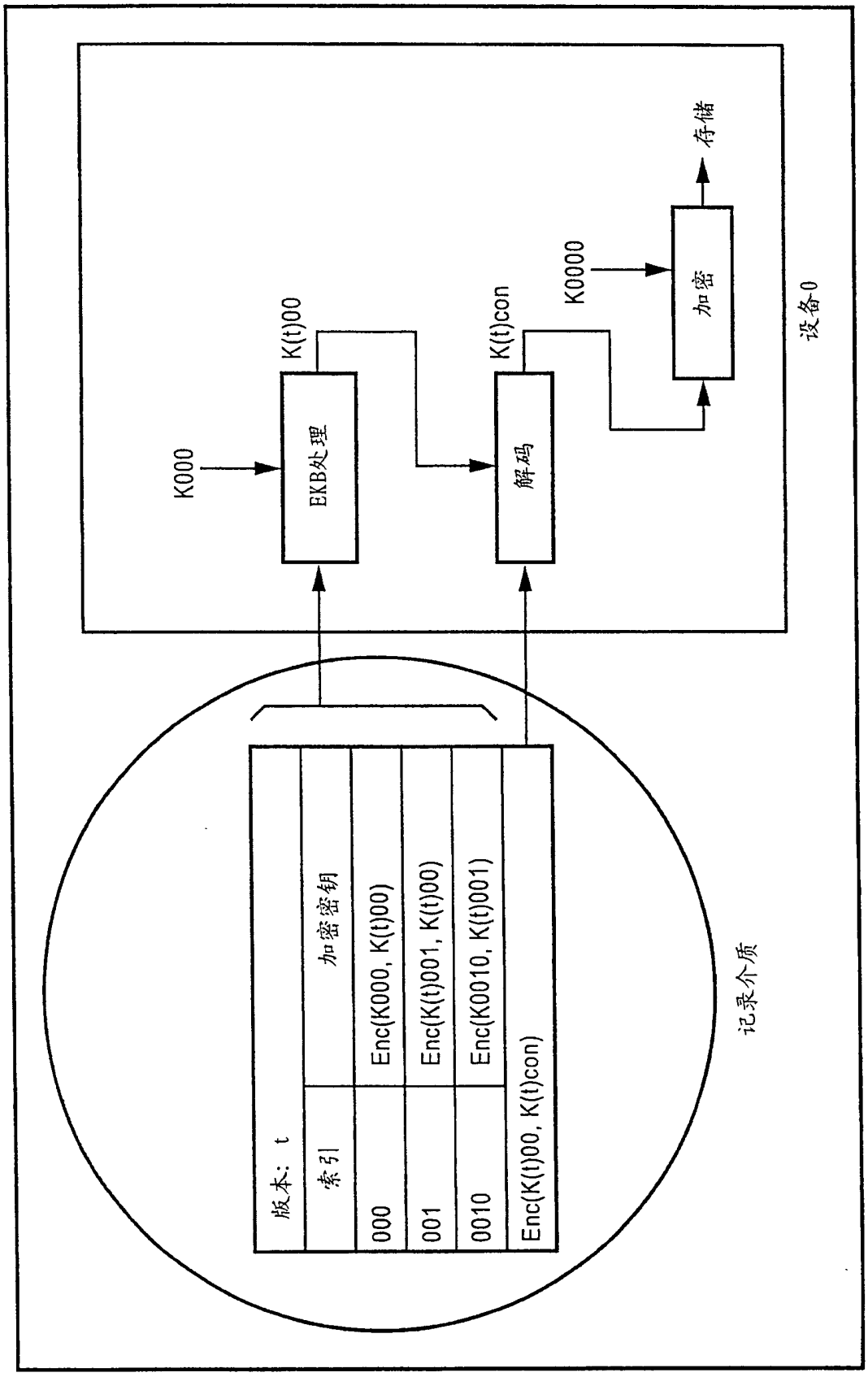

记录介质
版本: t
索引
加密密钥
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
设备0
K000
EKB处理
K(t)00
解码
K(t)con
K0000
加密
存储

图 9

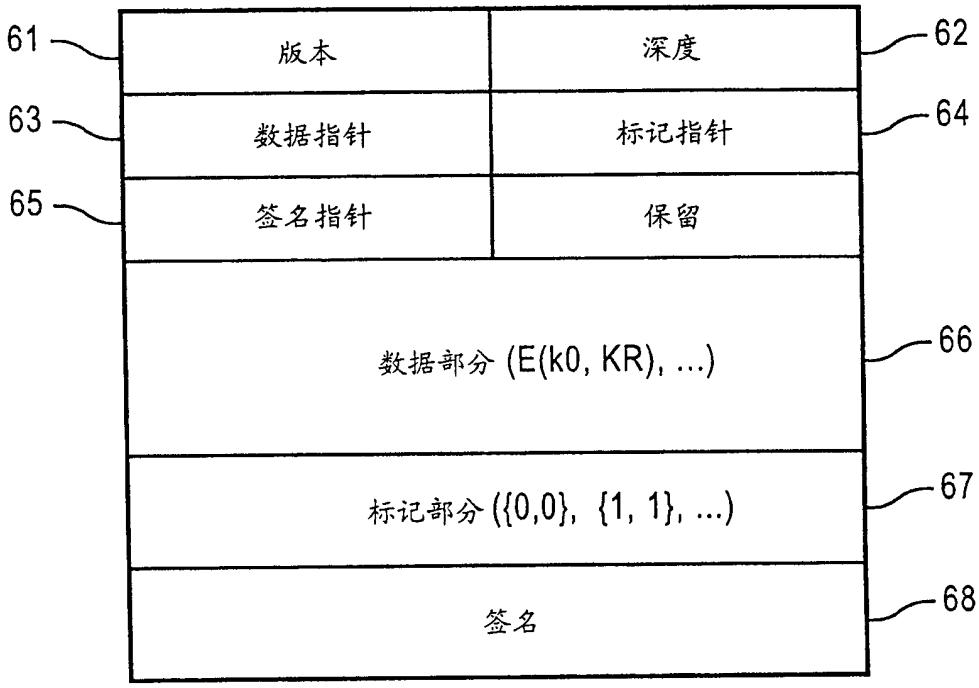

61
版本
深度
62
63
数据指针
标记指针
64
65
签名指针
保留
数据部分 (E(k0, KR), ...)
66
标记部分 ({0,0}, {1, 1}, ...)
67
签名
68

图 10

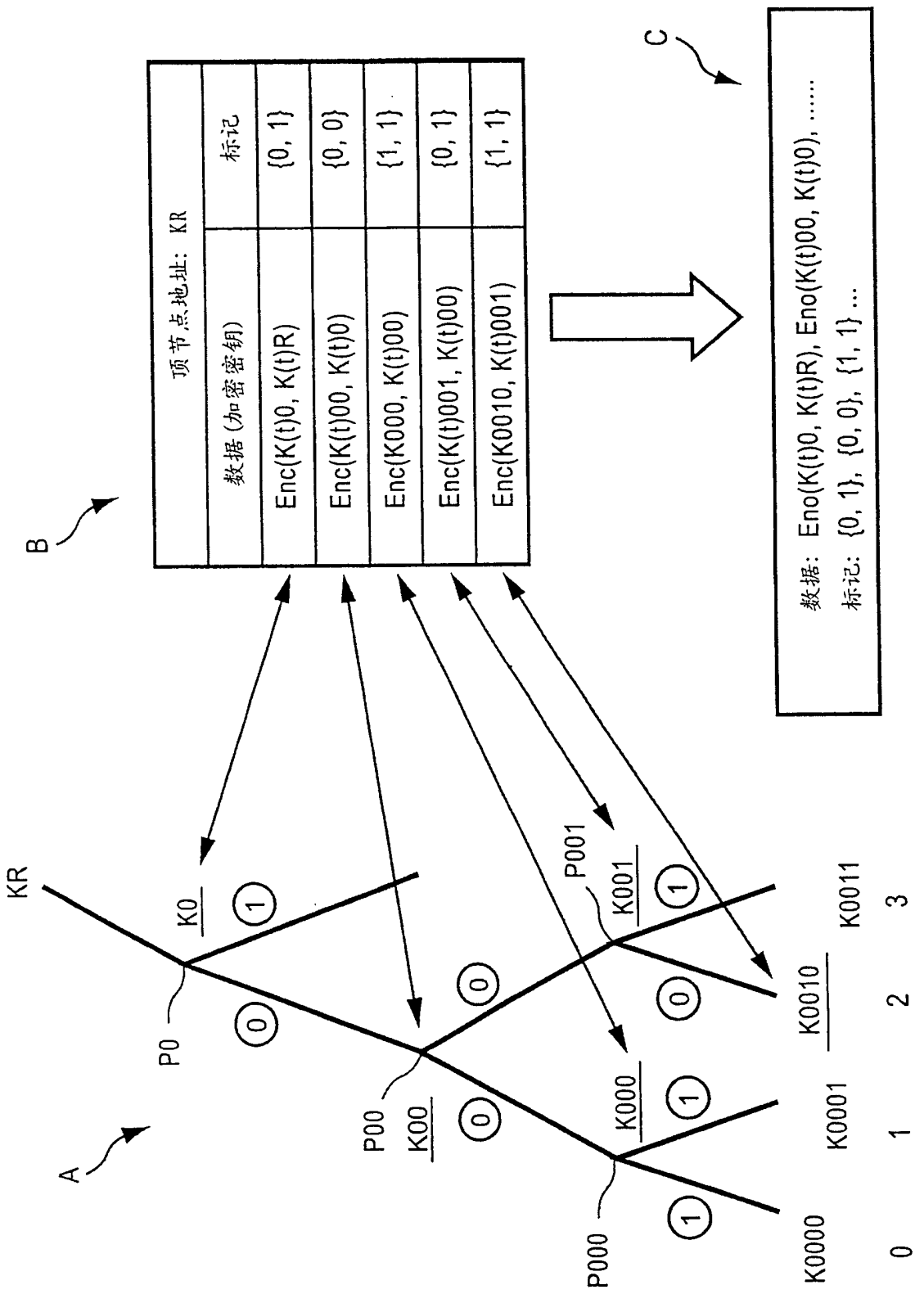

A
B
C
KR
K0
P0
K00
P00
K000
P000
K001
P001
K0010
K0011
K0001
K0000
0
1
2
3
顶节点地址: KR
数据 (加密密钥)
标记
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
数据: Eno(K(t)0, K(t)R), Eno(K(t)00, K(t)0), ...
标记: {0, 1}, {0, 0}, {1, 1} ...

图 11

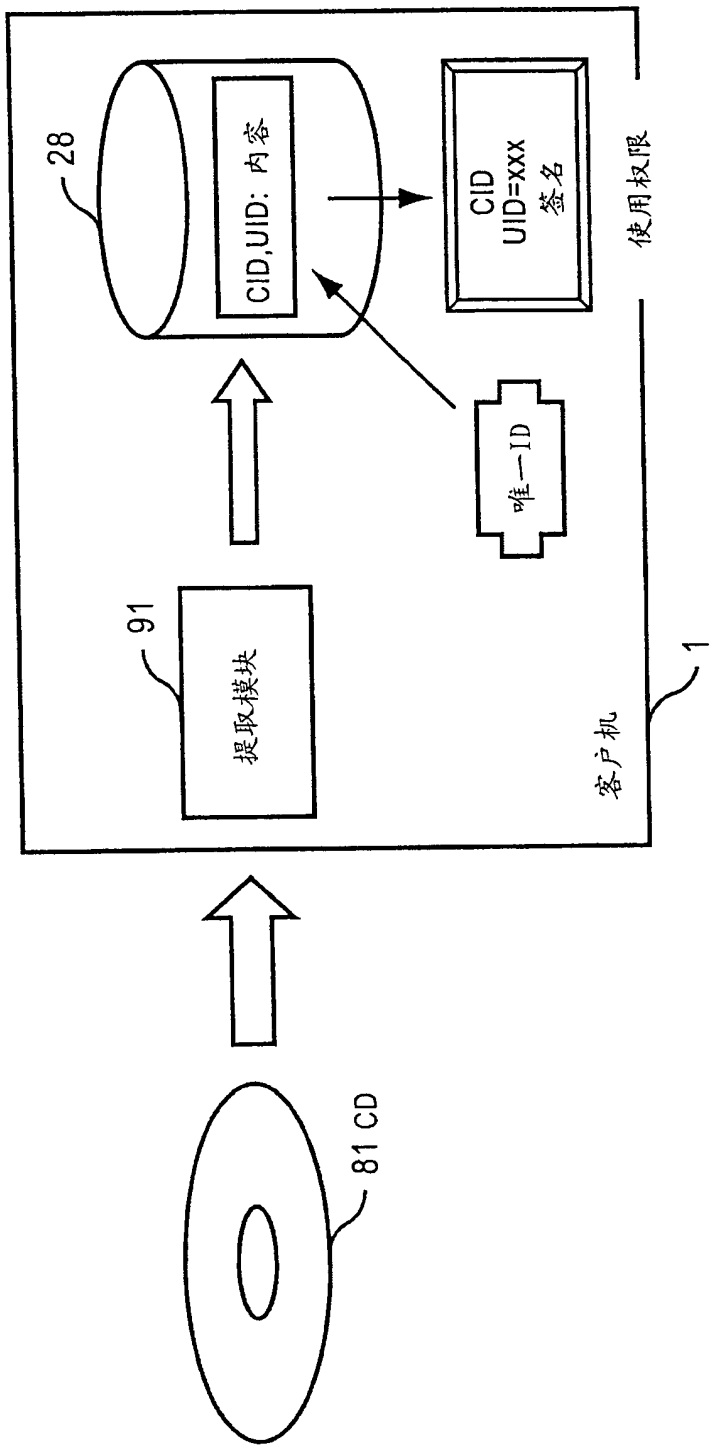


图 12

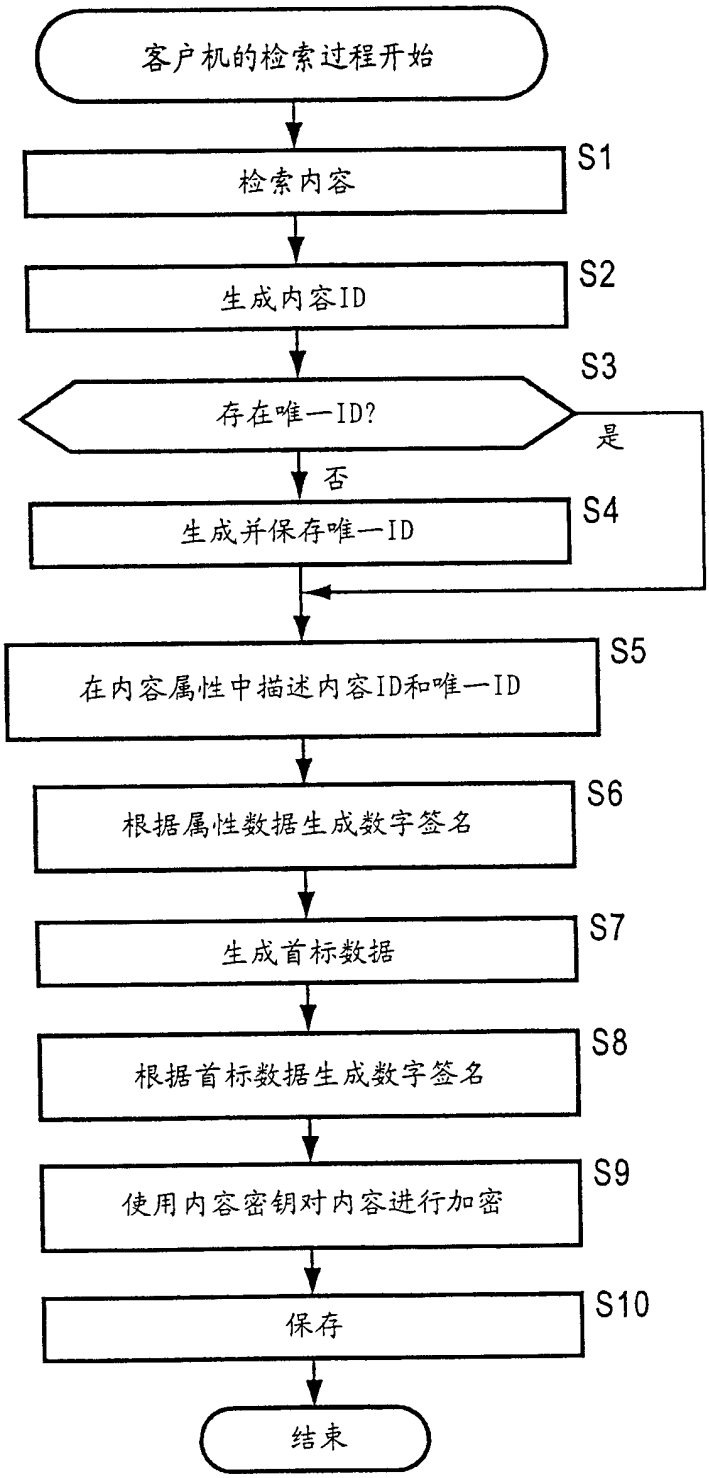

客户机的检索过程开始
检索内容
S1
生成内容ID
S2
存在唯一ID?
S3
是
否
生成并保存唯一ID
S4
在内容属性中描述内容ID和唯一ID
S5
根据属性数据生成数字签名
S6
生成首标数据
S7
根据首标数据生成数字签名
S8
使用内容密钥对内容进行加密
S9
保存
S10
结束

图 13

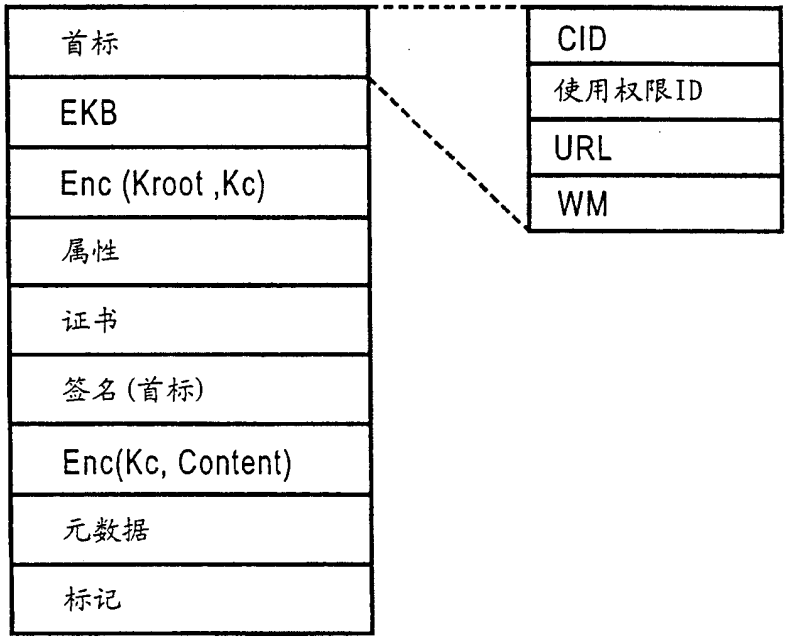

首标
EKB
Enc (Kroot ,Kc)
属性
证书
签名 (首标)
Enc(Kc, Content)
元数据
标记
CID
使用权限ID
URL
WM

图 14

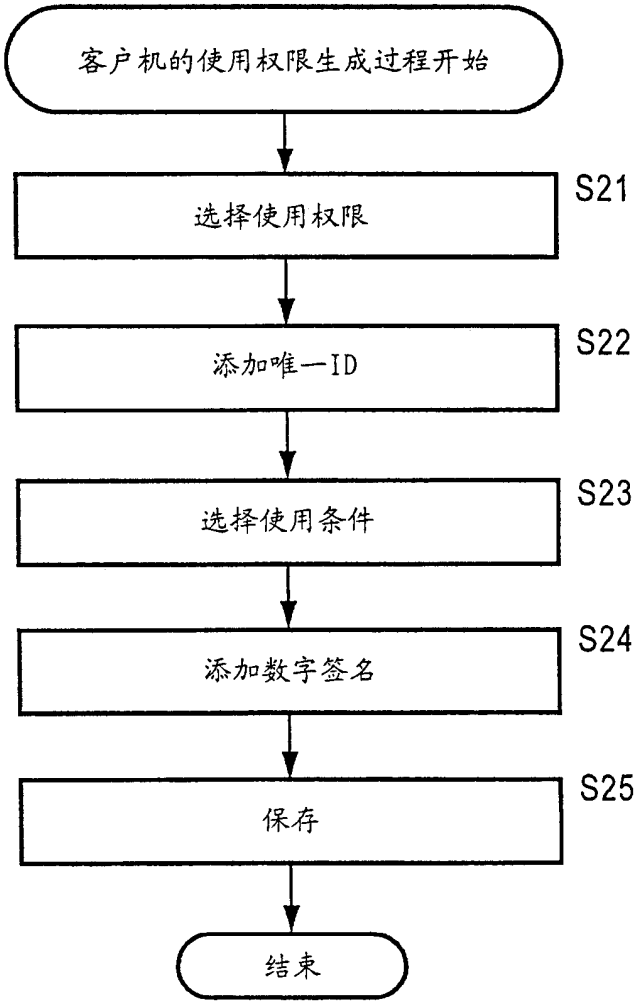

客户机的使用权限生成过程开始
选择使用权限
S21
添加唯一ID
S22
选择使用条件
S23
添加数字签名
S24
保存
S25
结束

图 15

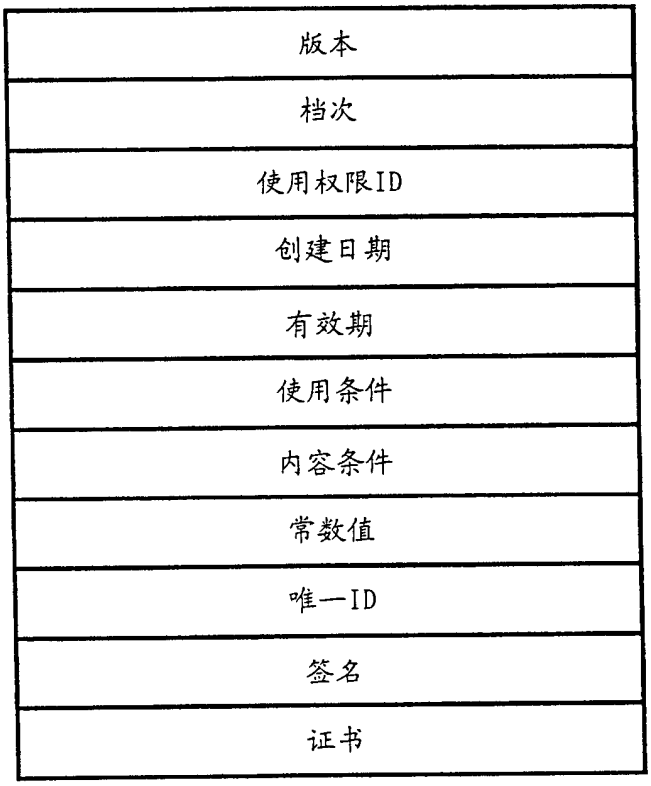


图 16

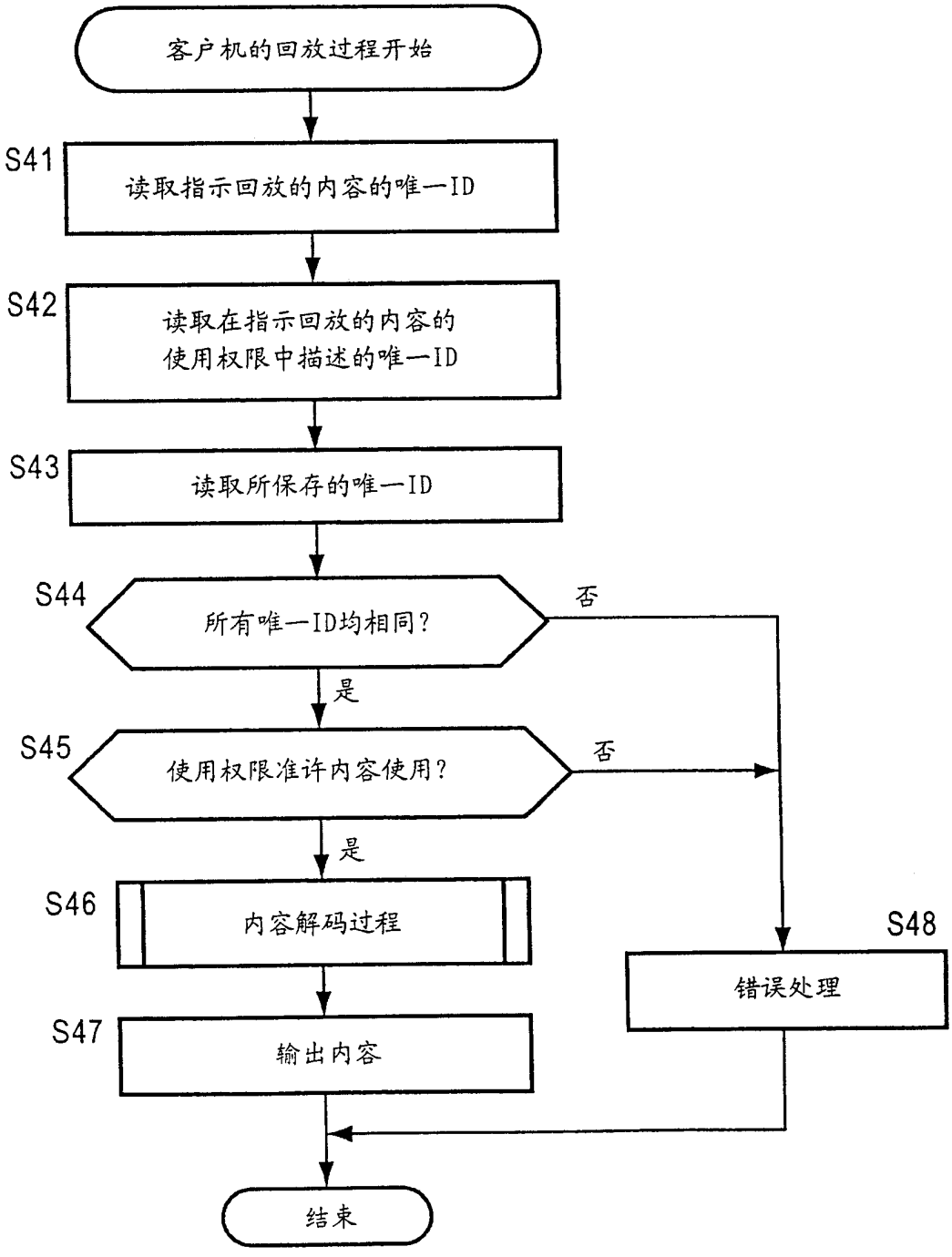

客户机的回放过程开始
S41
读取指示回放的内容的唯一ID
S42
读取在指示回放的内容的
使用权限中描述的唯一ID
S43
读取所保存的唯一ID
S44
所有唯一ID均相同?
否
是
S45
使用权限准许内容使用?
否
是
S46
内容解码过程
S47
输出内容
S48
错误处理
结束

图 17

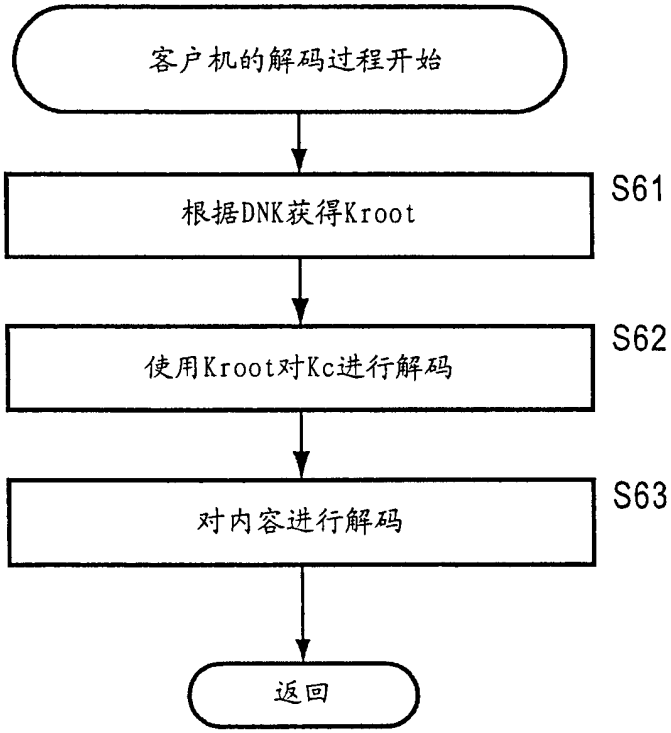

客户机的解码过程开始
根据DNK获得Kroot
S61
使用Kroot对Kc进行解码
S62
对内容进行解码
S63
返回

图 18

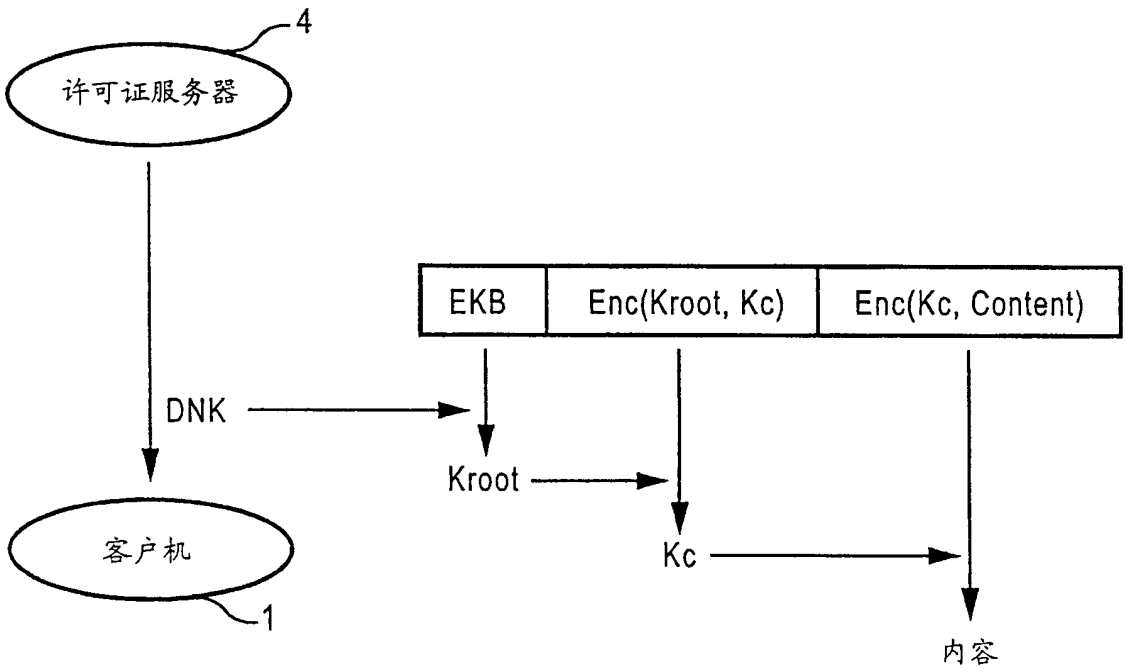

4
许可证服务器
EKB
Enc(Kroot, Kc)
Enc(Kc, Content)
DNK
Kroot
客户机
Kc
1
内容

图 19

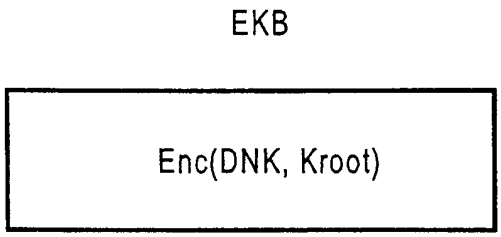

EKB
Enc(DNK, Kroot)

图 20