[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 12/14
G09C 1/00 H04L 9/08
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 03800794.0

[43] 公开日 2004 年 11 月 10 日

[11] 公开号 CN 1545659A

[22] 申请日 2003.4.10 [21] 申请号 03800794.0
[30] 优先权
[32] 2002. 4.15 [33] JP [31] 112109/2002
[86] 国际申请 PCT/JP2003/004546 2003.4.10
[87] 国际公布 WO2003/088056 日 2003.10.23
[85] 进入国家阶段日期 2004.2.5
[71] 申请人 索尼株式会社
地址 日本东京都
[72] 发明人 石黑隆二 多田惠子 二神基诚

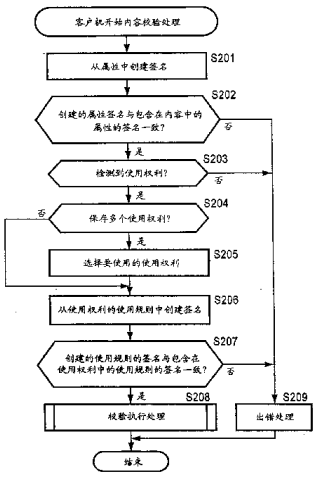
[74] 专利代理机构 北京市柳沈律师事务所
代理人 邵亚丽 马 莹

权利要求书 3 页 说明书 25 页 附图 24 页

[54] 发明名称 信息处理设备、方法和程序

[57] 摘要

公开了信息处理设备、方法和程序，甚至使低容量的内容存储设备也能防止未授权使用内容。CPU 选择要保存在内容存储设备中的内容。 在步骤(S202)中，CPU 认证分配给内容的第一数字签名。 存储单元保存使用权利。 在步骤(S203)中，CPU 在存储单元中搜索使用权利。 在步骤(S207)中，CPU 认证分配给使用权利的第二数字签名。CPU 依据包含在使用权利中的信息产生错误变更检测数据。 在步骤(S208)中，如果内容和使用权利没有被改变，那么 CPU 向内容存储设备输出使用权利、错误变更检测数据以及内容。 本发明可以应用到 DRM 系统的客户机中。



ISSN1008-4274

1．一种信息处理设备，根据与内容相关的使用权利来允许使用该内容，所述设备包括：

第一选择装置，用于选择将被保存在内容存储器设备中的内容；

第一验证装置，用于验证附加到由第一选择装置选择的内容上的第一数字签名；

存储装置，用于保存允许使用由第一选择装置所选择内容的使用权利；

检索装置，用于从存储装置中检索与第一选择装置所选内容相关的使用权利；

第二验证装置，用于验证附加到由检索装置检索的使用权利上的第二数字签名；

第一数据产生装置，根据包含在检索装置检索的使用权利中的信息来产生第一变更检测数据；以及

第一输出装置，当根据第一验证装置的验证结果和第二验证装置的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、由第一数据产生装置产生的第一变更检测数据以及内容。

2．依据权利要求1的信息处理设备，进一步包括第二选择装置，当由检索装置检索多个使用权利时，从多个被检索的使用权利中选择一个使用权利。

其中第二验证装置用于验证附加到由第二选择装置所选使用权利上的数字签名；

第一数据产生装置，根据包含在由第二选择装置选择的使用权利中的信息来产生第一变更检测数据；

3．依据权利要求1的信息处理设备，进一步包括转换装置，将第一选择装置选择的内容转换为与内容存储设备相关的格式，

其中，第一输出装置向内容存储设备输出由转换装置转换的内容。

4．依据权利要求1的信息处理设备，进一步包括转换装置，将与内容相关的使用权利转换为与内容存储设备相关的格式，

其中，由第一数据产生装置产生的第一变更检测数据是基于由转换装置

转换的使用权利的变更检测数据。

5．依据权利要求1的信息处理设备，其中由第一数据产生装置产生的第一变更检测数据是根据包含在使用权利中的使用规则而产生的。

6．依据权利要求1的信息处理设备，进一步包括：

获得装置，用于根据与保存在内容存储设备中的内容相关的使用权利，从内容存储设备中获得由第一数据产生装置产生的全部第一变更检测数据；

第二数据产生装置，用于根据由获得装置获得的全部第一变更检测数据来产生第二变更检测数据；以及

第二输出装置，用于向内容存储设备输出由第二数据产生装置产生的第二变更检测数据。

7．一种信息处理方法，根据与内容相关的使用权利来允许使用该内容，所述方法包括：

选择步骤，用于选择将被保存在内容存储设备中的内容；

第一验证步骤，验证附加到选择步骤中所选内容上的第一数字签名；

存储控制步骤，用于控制允许使用在选择步骤中所选内容的使用权利在存储装置中的存储；

检索步骤，用于从存储装置中检索与选择步骤中所选内容相关的使用权利；

第二验证步骤，用于验证附加到检索步骤中检索的使用权利上的第二数字签名；

数据产生步骤，根据包含在检索步骤所检索的使用权利中的信息来产生变更检测数据；以及

输出步骤，当根据第一验证步骤的验证结果和第二验证步骤的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、在数据产生步骤中产生的变更检测数据以及内容。

8．一种用于使计算机执行处理的程序，所述计算机根据与内容相关的使用权利来控制允许使用内容的信息处理，所述处理包括步骤：

选择步骤，选择将被保存在内容存储设备中内容；

第一验证步骤，验证附加到选择步骤中所选内容上的第一数字签名；

存储控制步骤，控制允许使用在选择步骤中所选内容的使用权利在存储装置中的存储；

检索步骤，从存储装置中检索与选择步骤中选择的内容相关的使用权利；

第二验证步骤，验证附加到检索步骤中检索的使用权利上的第二数字签名；

数据产生步骤，根据包含在检索步骤中所检索的使用权利中的信息来产生变更检测数据；以及

输出步骤，当根据第一验证步骤的验证结果和第二验证步骤的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、在数据产生步骤中产生的变更检测数据和内容。

信息处理设备、方法和程序

技术领域

本发明涉及信息处理设备、方法和程序。更具体地说，本发明涉及将内容传递到另一个设备的信息处理设备、方法和程序，同时在内容和使用权利是分开分配的版权管理系统中保护内容的版权。

背景技术

最近，已经实现了通过因特网向用户分配内容诸如音乐数据或图像数据的系统。

在这些已知的保护著作版权的 DRM(数字权利管理)系统中，使用了相同的保护方法，而不管终端的吞吐量。特别是低吞吐量终端或内容存储器设备在防止未授权内容的使用方面是很困难的。

在使用权利和内容被分开分配的系统中，终端或内容存储器设备具有很大的负担和困难来调查使用权利和内容的真实性以及对使用权利和内容进行匹配。例如，对于低吞吐量终端，很难判定设备是否具有与内容相关的使用权利，很难调查使用权利和内容的真实性，以及允许设备对内容的使用。

发明说明

考虑到上述情况，本发明的一个目的是使甚至低吞吐量内容存储器设备也能使用内容，并可靠地防止对内容的未授权使用。

本发明的信息处理设备包括第一选择装置，用于选择将被保存在内容存储器设备中的内容；第一验证装置，用于验证附加到由第一选择装置所选内容上的第一数字签名；存储装置，用于保存允许使用由第一选择装置所选择内容的使用权利；检索装置，用于从存储装置中检索与第一选择装置所选内容相关的使用权利；第二验证装置，用于验证附加到由检索装置检索的使用权利上的第二数字签名；第一数据产生装置，根据包含在检索装置检索的使用权利中的信息来产生第一变更检测数据；以及第一输出装置，当根据第一

验证装置的验证结果和第二验证装置的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、由第一数据产生装置产生的第一变更检测数据以及内容。

信息处理设备还可以包括第二选择装置，当检索装置检索出多个使用权利时，从多个被检索出的使用权利中选择一个使用权利。第二验证装置可以验证附加到第二选择装置选择的使用权利上的数字签名。第一数据产生装置可以根据包含在由第二选择装置选择的使用权利中的信息，产生第一变更检测数据。

信息处理设备还可以包括转换装置，将第一选择装置选择的内容转换成与内容存储设备相关的格式。第一输出装置可以向内容存储设备输出由转换装置转换的内容。

信息处理设备还可以包括转换装置，用于将与内容相关的使用权利转换成与内容存储设备相关的格式。根据转换装置转换的使用权利，由第一数据产生装置产生的第一变更检测数据可以是变更检测数据。

由第一数据产生装置产生的第一变更检测数据可以根据包含在使用权利中的使用规则来产生。

信息处理设备还可以包括获得装置，用于根据与保存在内容存储设备中内容相关的使用权利，从内容存储设备中获得由第一数据产生装置产生的全部第一变更检测数据；第二数据产生装置，用于根据由获得装置获得的全部第一变更检测数据来产生第二变更检测数据；以及第二输出装置，用于向内容存储设备输出由第二数据产生装置产生的第二变更检测数据。

本发明的信息处理方法包括选择步骤，用于选择将被保存在内容存储设备中的内容；第一验证步骤，验证附加到选择步骤中所选内容上的第一数字签名；存储控制步骤，用于控制允许使用在选择步骤中所选内容的使用权利在存储装置中的存储；检索步骤，用于从存储装置中检索与选择步骤中所选内容相关的使用权利；第二验证步骤，用于验证附加到检索步骤中检索的使用权利上的第二数字签名；数据产生步骤，根据包含在检索步骤所检索的使用权利中的信息来产生变更检测数据；以及输出步骤，当根据第一验证步骤的验证结果和第二验证步骤的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、在数据产生步骤中产生的变更检测数据以及内容。

本发明的程序使计算机执行处理，所述处理包括选择步骤，选择将被保存在内容存储设备中的内容；第一验证步骤，验证附加到选择步骤中所选内容上的第一数字签名；存储控制步骤，控制允许使用在选择步骤中所选内容的使用权利在存储装置中的存储；检索步骤，从存储装置中检索与选择步骤中所选内容相关的使用权利；第二验证步骤，验证附加到检索步骤中检索的使用权利上的第二数字签名；数据产生步骤，根据包含在检索步骤所检索的使用权利中的信息来产生变更检测数据；以及输出步骤，当根据第一验证步骤的验证结果和第二验证步骤的验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、在数据产生步骤中产生的变更检测数据和内容。

依据本发明的信息处理设备、方法和程序，选择将被保存在内容存储设备中的内容；验证附加到所选内容上的第一数字签名；保存允许使用所选内容的使用权利；从存储装置中检索与所选内容相关的使用权利；验证附加到被检索的使用权利上的第二数字签名；根据包含在被检索使用权利中的信息来产生变更检测数据；以及，当根据第一验证结果和第二验证结果判断出内容和使用权利未被改变时，向内容存储设备输出使用权利、变更检测数据和内容。

内容可以包括任何格式的信息，如音频、图像或文本，只要它用作有用的信息。

数字签名可以由任何方法产生，只要它用作证明真实性的信息。

附图说明

图 1 是表示依据本发明的内容提供系统的结构示意图。

图 2 是表示图 1 中所示每个客户机结构的方框图。

图 3 是描述图 1 中所示客户机的内容下载处理的流程图。

图 4 是描述图 1 中所示内容服务器的内容提供处理的流程图。

图 5 是表示图 4 的步骤 S26 中格式的示例。

图 6 是描述图 1 中所示客户机的内容播放处理的流程图。

图 7 是描述在图 6 的步骤 S43 中的使用权利获得处理的细节的流程图。

图 8 是表示使用权利结构的说明。

图 9 是描述图 1 中所示的许可证服务器的使用权利提供处理的流程图。

图 10 是描述密钥安排的示意图。

图 11 是描述类目节点的示意图。

图 12 是表示节点与设备之间相关的具体示例的示意图。

图 13 是描述使能密钥块结构的说明。

图 14 是描述使能密钥块结构的说明。

图 15 是描述使能密钥块使用的示意图。

图 16 是表示使能密钥块格式示例的说明。

图 17 是描述在使能密钥块中每个标记结构的示意图。

图 18 是描述使用 DNK 进行内容解密过程的示意图。

图 19 是表示使能密钥块示例的说明。

图 20 是描述多段内容在设备中分配的示意图。

图 21 是表示记忆棒结构的示意图。

图 22 是描述内容校验处理的流程图。

图 23 是描述客户机的校验执行处理的流程图。

图 24 是表示使用 DES 加密算法产生 MAC 值的示例的示意图。

图 25 是描述保存在记忆棒中索引和内容的示意图。

图 26 是描述记忆棒的校验执行处理的流程图。

具体实施方式

图 1 表示依据本发明的内容提供系统的结构。客户机 1-1 和客户机 1-2(在此之后当不需要区分单个客户机时，简称为客户机 1)连接到因特网 2。虽然在该示例中只表示了两个客户机，但是任意数量的客户机都可以连接到因特网 2。

另外，向客户机 1 提供内容的内容服务器 3，向客户机 1 授予使用内容服务器 3 上提供内容所必需的使用权利的许可证服务器 4，以及当收到客户机 1 的使用权利时向客户机 1 记帐的记帐服务器 5 都连接到了因特网 2。

在需要的情况下，内容服务器 3、许可证服务器 4 和记帐服务器 5 中每一个都可以是以任意数量连接到因特网 2 上。

图 2 表示每个客户机 1 的结构。

参考图 2，CPU(中央处理单元)21 依据保存在 ROM(只读存储器)22 中的程序或从存储器单元 28 调入到 RAM(随机存取存储器)23 中的程序来执行各

种处理。定时器 20 保持时间，并向 CPU 21 提供时间信息。RAM 23 适当地保存 CPU 21 执行各种处理所需要的数据。

加密/解密单元 24 加密内容数据和解密被加密的内容数据。编解码器 25 按例如 ATRAC(自适应转换声音编码) 3 对内容数据编码，并通过输入/输出接口 32 将编码后的内容数据提供并记录在与驱动器 30 连接的半导体存储器 44 中。编解码器 25 还解码通过驱动器 30 从半导体存储器 44 中读出的编码数据。

半导体存储器 44 包括，例如，记忆棒(商标)。

CPU 21、ROM 22、RAM23、加密/解密单元 24 以及编解码器 25 都通过总线 31 相互连接。输入/输出接口 32 还连接到总线 31 上。

输入单元 26、输出单元 27、存储单元 28、以及通信单元 29 均连接到输入/输出接口 32 上，其中输入单元 26 包括键盘、鼠标等，输出单元 27 包括显示器，如 CRT 或 LCD，扬声器等，存储单元 28 包括硬盘等，并且通信单元 29 包括调制解调器、终端适配器等。通信单元 29 通过因特网 2 执行通信。通信单元 29 与另一个客户机进行模拟信号或数字信号通信。

在必要的情况下，驱动器 30 连接到输入/输出接口 32。在驱动器 30 中，可适当地放置磁盘 41、光盘 42、磁光盘 43 或半导体存储器 44。在必要的情况下，从放置的媒介中读出的计算机程序被安装在存储单元 28 中。

虽然在图中未表示出，但是内容服务器 3、许可证服务器 4 和记帐服务器 5 中的每个基本上都具有与图 2 中所示的客户机 1 相似结构的计算机。在以下的说明中，图 2 中表示的结构还可以引申为内容服务器 3、许可证服务器 4、记帐服务器 5 等的结构。

虽然在图中未表示出，但是 PD(便携式设备)还包括与图 2 中所示的客户机 1 基本相似结构的计算机。

下面参考图 3 的流程图，说明客户机 1 接收内容服务器 3 提供的内容的处理。

在步骤 S1 中，当用户通过操作输入单元 26 来命令客户机 1 访问内容服务器 3 时，CPU 21 控制通信单元 29 通过因特网 2 来访问内容服务器 3。在步骤 S2 中，当用户操作输入单元 26 来具体说明将被提供的内容时，CPU 21 接收这个具体说明的信息，并利用通信单元 29 通过因特网 2 来通知内容服务器 3 具体内容的内容 ID。如以下将参考图 4 的流程图所说明的，已经被

通知了内容 ID 的内容服务器 3 发送包含加密内容数据的内容。在步骤 S3 中，CPU 21 通过通信单元 29 接收内容数据。在步骤 S4 中，CPU 21 在包含于存储单元 28 的硬盘中提供并保存加密后的内容数据。

下面参考图 4 的流程图，说明与客户机 1 执行的上述处理相关的内容服务器 3 的内容提供处理。在以下的说明中，图 2 中所示的客户机 1 的结构也被引述为内容服务器 3 的结构。

在步骤 S21 中，内容服务器 3 的 CPU 21 被排队等候，直到内容服务器 3 被客户机 1 利用通信单元 29 通过因特网 2 访问。在步骤 S22 中，当判断出内容服务器 3 已被客户机 1 访问时，内容服务器 3 的 CPU 21 装载客户机 1 发送的内容 ID。该内容 ID 是在图 3 的步骤 S2 中由客户机 1 通知的信息。

在步骤 S23 中，内容服务器 3 的 CPU 21 从保存在存储单元 28 的内容中，读出由步骤 S22 中的处理装载的内容 ID 所具体说明的内容数据。在步骤 S24 中，CPU 21 向加密/解密单元 24 提供从存储单元 28 读出的内容数据，而加密/解密单元 24 利用内容密钥 Kc 依次加密内容数据。

由于保存在存储单元 28 中的内容数据已经被编解码器 25 按 ATRAC 编码，所以，加密被编码的内容数据。

可选择地，被加密的内容数据也可以保存在存储单元 28 中。在这种情况下可以省略步骤 S24 中的处理。

在步骤 S25 中，内容服务器 3 的 CPU 21 将密钥信息附加到用于发送被加密内容数据的格式的引导头上。该密钥信息被要求用来解密被加密内容(以下参考图 5 说明 EKB 和 K_{EKBC}(KC))。在步骤 S26 中，内容服务器 3 的 CPU 21 利用通信单元 29 通过因特网 2，向已访问内容服务器 3 的客户机 1 发送在步骤 S24 处理中所加密的内容和在步骤 S25 处理中将密钥信息附加到引导头中的格式数据。

图 5 是内容服务器 3 向客户机 1 提供的内容格式的结构说明。如附图中所示的那样，该格式基本上包括引导头和数据。

引导头包括内容信息、URL(统一资源定位符)、使能密钥块(EKB)、利用从 EKB 产生的密钥 K_{EKBC} 加密的并用作内容密钥 Kc 的数据 K_{EKBC}(KC)、内容属性和签名。以下将参考图 3 和图 4 来说明 EKB。

内容信息包括作为识别信息的内容 ID(CID)，用于识别被格式化为数据的内容数据，以及指示内容编解码格式的数据。

URL 是通过访问以得到使用内容的必要使用权利所要求的地址信息。在图 1 所示系统的情况下，具体而言，URL 是需要接收使用权利的许可证服务器 4 的地址。

内容属性是关于内容的信息。内容属性包括内容 ID、作为识别信息来识别内容提供者的记录公司 ID，以及作为识别信息用于识别艺术家的艺术家 ID。在该实施例中，属性被用来具体说明将由使用权利使用的内容。

签名是与内容属性相关的数字签名。

数据包括任意数量的加密块。每个加密块包括初始向量(IV)、种子和通过利用密钥 K'c 加密该内容数据所产生的数据 $K_{K'C}$(数据)。

如以下的方程所示，密钥 K'c 是通过将内容密钥 Kc 和随机数种子作用到 hash 函数所计算出的值：

K'c＝hash(Kc，Seed)

在每个加密块中，初始向量 IV 和种子被设置成不同的值。

内容数据被以 8 个字节为单位加密。内容数据被加密成 CBC(密码块链接)模式，在其中相继的 8 个字节是利用前 8 个字节的加密结果加密的。

在 CBC 模式中，当内容数据的第一 8 个字节要被加密时，没有在这些第一 8 个字节之前的 8 个字节的加密结果。于是，第一 8 个字节是利用用作初始值的初始向量 IV 来加密的。

利用 CBC 模式中的加密，甚至当一个加密块被解密时，它的影响也不会扩展到其它的加密块。

可选择地，该内容也可以以另外的加密模式来加密。

在上述方式中，客户机 1 免费地从内容服务器 3 自由地获得内容。因此，可以分配很多段的内容。

为了使每个客户机 1 使用获得的内容，客户机 1 需要具有使用权利，以证明该内容的使用是被允许的。现在将参考图 6 说明客户机 1 的内容播放处理。

在步骤 S41 中，客户机 1 的 CPU 21 获得由用户通过操作输入单元 26 所具体指定的内容识别信息(CID)。该识别信息包括，例如，内容的题目、附加到所保存内容每段上的序号等。

当该内容被具体指定时，CPU 21 读出该内容的属性。如图 5 中所示的，属性是在内容的引导头中说明的。

在步骤S42中，CPU 21判断客户机1是否已经获得使用权利，其中包含在该使用权利中的内容规则是满足在步骤S41中读出的属性的，并判断是否已将该使用权利保存在了存储单元28中。在步骤S43中，当还没有获得这样的使用权利时，CPU 21执行使用权利获得处理。下面会参考图7的流程来说明使用权利获得处理的细节。

在步骤S44中，当在步骤S42中判断出已获得使用权利，或者当在步骤S43中执行了使用权利获得处理并获得了使用权利时，CPU 21判定所获得的使用权利是否在它的截止期内。通过比较在使用权利(参看以下说明的图8)中定义的日期和由定时器20保持的当前的日期和时间来判断使用权利是否在截止期内。在步骤S45中，当判断出使用权利的截止期已经过了时，CPU 21执行使用权利更新处理。

在步骤S46中，当判断出在步骤S44使用权利在截止期内，或者当使用权利在步骤S45中被更新了时，CPU 21读出保存在存储单元28中的包含在使用权利中的使用规则和使用状态(以下说明)，并判断使用规则和使用状态是否满足回放规则。

在步骤S47中，根据包含在使用权利中的使用规则和使用状态，当在步骤S46中判断出允许播放该内容时，CPU 21从存储单元28中读出加密的内容数据，并将加密的内容数据保存在RAM 23中。在步骤S48中，CPU 21以图5所示数据中排列的加密块为单位，向加密/解密单元24提供保存在RAM 23中的加密内容数据，加密/解密单元24利用内容密钥Kc依次解密所加密的内容数据。

以下会参考图13和14来说明获得内容密钥Kc的方法的具体示例。利用设备节点密钥(DNK)，获得包含在EKB(图5)中的密钥K_{EKBC}。利用密钥K_{EKBC}，可从数据K_{EKBC}(Kc)(图5)获得内容密钥Kc。

在步骤S49中，CPU 21向编解码器25提供由加密/解码单元24解密的内容数据以便被解码。CPU 21将编解码器25解码的数据从输入/输出接口32提供给输出单元27，对这些数据作D/A转换，并通过扬声器输出转换后的数据。

当在步骤S46中根据包含在使用权利的使用规则和使用状态判断出该内容被禁止播放时，将不输出该内容。并且结束处理。

以下将参考图7的流程图来详细说明在图6的步骤S43中执行的使用权

利获得处理。

通过将其自身登记在许可证服务器中，客户机 1 可获得包括叶 ID、DNK(设备节点密钥)、客户机 1 的一对私钥和公钥、许可证服务器的公钥以及每个公钥的证书的服务数据。

叶ID指示分配给每个客户机的识别信息。DNK是必要的设备节点密钥，用于解密由包含在内容(以下参考图 10 说明)中 EKB(使能密钥块)所加密的内容密钥Kc。

在步骤S61中，CPU 21获得在内容引导头中说明的URL。如上所述，URL 是获得通过访问以获得使用内容所需的使用权利的地址。在步骤 S62 中，CPU 21 访问在步骤S61中获得的URL。具体地说，通信单元29通过因特网2访问许可证服务器4。为了响应该访问，许可证服务器4向客户机1发送使用权利列表。并且，许可证服务器4还请求客户机1输入使用权利具体说明信息，以具体说明要被购买的使用权利(使用内容所需的使用权利)，还有用户ID和口令(以下图9的步骤S102说明)。CPU 21在输出单元27的显示单元上显示该请求。根据所显示的请求，用户操作输入单元26来输入使用权利具体说明信息、用户ID和口令。用户ID和口令是客户机1的用户通过因特网2访问许可证服务器4预先获得的。

在步骤S63和64中，CPU 21调出由单元26输入的使用权利具体说明信息、用户ID和输入口令。在步骤S65中，CPU 21控制通信单元29通过因特网2向许可证服务器4发送输入用户ID、口令、使用权利具体说明信息以及包含叶ID的使用权利请求，其中叶ID包含在服务数据(以下将说明)中。

如参考图9所说明的那样，许可证服务器4根据用户ID、口令和使用权利具体说明信息来发送使用权利(步骤S109)。可选择地，如果不满足规则，那么许可证服务器4就不发送使用权利(步骤S112)。

在步骤S66中，CPU 21判断使用权利是否已经从许可证服务器4发送出来。在步骤S67中，当已经发送了使用权利时，CPU 21提供使用权利并将使用权利保存在存储单元28中。

在步骤S68中，当在步骤S66中判断出没有发送使用权利时，CPU 21执行出错处理。具体地说，由于没有获得使用内容的使用权利，CPU 21禁止内容播放处理。

如上所述，每个客户机 1 只有当获得使用内容所需的使用权利之后才能使用内容。

可选择地，每个用户可在获得内容之前执行图 7 中所示的使用权利获得处理。

如图 8 中所示，提供给客户机 1 的使用权利包括使用规则、叶 ID、数字签名等。

版本是通过用点分开主版本和次版本来说明使用权利版本的信息。

使用十进制整数表示的简档定义了描述使用权利方法的限制的信息。

使用十六进制常数表示的使用权利 ID 是识别使用权利的识别信息。

创建日期指示使用权利被创建的日期。

截止日期指示使用权利的截止日期。截止日期 9999 年 23：59：59 表示对截止日期没有限制。

使用规则包括以下信息：根据使用权利，表示使用内容的截止日期；根据使用权利，播放内容的截止日期；内容可被播放的最大次数；根据使用权利，内容可以被复制的次数(允许复制的次数)；内容被校验的最大次数；根据使用权利，内容是否可以被记录在 CD-R 上；内容被复制到 PD(便携式设备)的次数；使用权利是否可以被传递；以及是否被强制保持使用日志。

使用规则的数字签名与使用规则相关。

这些常值被使用规则或使用状态参考。

叶 ID 是用于识别客户机的识别信息。

数字签名与全部使用权利相关。

证书包括许可证服务器的公钥。

客户机 1 的存储单元 28 除了保存使用权利的使用规则外，还保存用作表示内容和使用权利状态的信息的使用状态。使用状态包括以下信息：根据相关使用权利，内容被播放的次数；内容被复制的次数；内容被校验的次数；内容第一次被播放的日期；内容被记录在 CD-R 上的次数；以及与内容或使用权利相关的记录信息。

根据包含在使用权利中的使用规则以及同使用权利一起保存在存储单元 28 中的使用状态，在图 6 的步骤 S46 中判断是否满足播放内容的规则。例如，当保存在使用状态中的内容被播放的次数小于包含在使用规则中的内容可被播放的最大次数时，就判定出满足了回放规则。

以下将参考图 9 的流程图，说明许可证服务器 4 的使用权利提供处理，该处理与在图 7 中表示的客户机 1 的使用权利获得处理结合执行。图 2 中的客户机 1 的结构被引用为许可证服务器 4 的结构。

在步骤 S101 中，许可证服务器 4 的 CPU 21 被排队等候直到许可证服务器 4 被客户机 1 访问为止。在步骤 S102 中，当许可证服务器 4 被客户机 1 访问时，CPU 21 向已访问许可证服务器 4 的客户机 1 发送包括与每个使用权利相关信息的使用权利列表。还有，许可证服务器 4 的 CPU 21 请求客户机 1 发送用户 ID、口令和使用权利具体说明信息。如上所述，当客户机 1 通过图 7 中步骤 S65 的处理发送了用户 ID、口令、叶 ID 和使用权利具体说明信息(可以是使用权利 ID)时，许可证服务器 4 的 CPU 21 通过通信单元 29 接收这些信息段，并装载所接收的信息。

在步骤 S103 中，许可证服务器 4 的 CPU 21 通过通信单元 29 访问记帐服务器 5，并请求记帐服务器 5 执行与用户 ID 和口令相关的用户的信用处理。为响应通过因特网 2 从许可证服务器 4 来的信用处理请求，记帐服务器 5 调查与用户 ID 和口令相关的用户过去的支付记录，并判断用户在过去是否没有为使用权利而付费。如果没有存在这样的记录，那么，CPU 21 发送允许授予使用权利的信用。如果存在没有支付的记录，那么，CPU 21 发送禁止授予使用权利的信用结果。

在步骤 S104 中，许可证服务器 4 的 CPU 21 判断从记帐服务器 5 来的信用结果是否允许授予使用权利。在步骤 S105 中，当允许授予使用权利时，CPU 21 从保存在存储单元 28 中的使用权利中，获得与步骤 S102 处理中装载的使用权利具体说明信息相关的使用权利。保存在存储单元 28 中的每个使用权利包括事先的信息，如使用权利 ID、版本、创建日期和截止日期。在步骤 S106 中，CPU 21 将所接收的叶 ID 加到使用权利上。在步骤 S107 中，CPU 21 选择与步骤 S105 中选择的使用权利相关的使用规则。可选择地，当用户通过步骤 S102 的处理已具体说明了使用规则时，如果需要，被具体说明的使用规则也加到准备好的使用规则中。CPU 21 将选择的使用规则加到使用权利中。可选择地，使用规则也可以预先加到使用权利中。

在步骤 S108 中，CPU 21 利用许可证服务器的私钥对使用权利签名，并将包含许可证服务器公钥的证书加到使用权利中，于是，产生图 8 中所示排列的使用权利。

在步骤S109中，许可证服务器4的CPU 21使通信单元29通过因特网2向客户机1发送使用权利(如图8中所示排列)。

在步骤S110中，许可证服务器4的CPU 21将已由步骤S109处理所发送的使用权利(包括使用规则和叶ID)，结合步骤S102的处理所装载的用户ID和口令，保存在存储单元28中。在步骤S111中，CPU 21执行处理。具体地说，CPU 21利用通信单元29请求记帐服务器5对与用户ID和口令相关的用户计账。为响应计账请求，记帐服务器5对用户计账。如上所述，当已为费用而被计账的用户没有支付费用时，从这一点向前，该用户将不被允许接收使用权利，甚至当该用户请求授予使用权利时。

具体地说，在此情况下，记帐服务器5发送禁止授予使用权利的信用结果。处理从步骤S104前进到步骤S112。CPU 21执行出错处理。具体地说，许可证服务器4的CPU 21控制通信单元29向已访问许可证服务器4的客户机1发送指示使用权利的授予被禁止的消息。处理结束。

在此情况下，如上所述，由于客户机1没能接收到使用权利，所以，客户机1就被禁止使用内容(解密被加密的内容和播放该内容)。

在本发明中，如图10中所示，根据广播加密的原则来管理设备和密钥。密钥被排列成分层树型结构，使得底层的叶与各个设备唯一密钥相关。对于在本发明系统中使用的分层树型结构的密钥管理，可以参考专利申请号为2001-352321的日本未审查专利。在图10所示的示例中，产生与16个设备0到15相关的密钥。

每个密钥的定义与说明中圆圈表示的树型结构节点相关联。在该示例中，根密钥KR的定义与顶层的根节点相关联。密钥K0和K1的定义与第二层的节点关联、密钥K00到K11的定义与第三层节点相关联。密钥K000到K111的定义与第四层节点相关联。密钥K0000到K1111的定义与作为底层节点的叶(设备节点)相关联。

由于密钥被安排成分层结构，例如，密钥K0010和密钥K0011的上层密钥是K001，而密钥K000和密钥K001的上层密钥是K00。相似地，密钥K00和密钥K01的上层密钥是K0，密钥K0和密钥K1的上层密钥是KR。

使用内容的密钥，是通过从底层每个设备节点(叶)到顶层根节点路径上相关节点的密钥来管理的。例如，与叶3相关的设备，通过在相应路径上的密钥K0011、K001、K00、K0和KR来管理使用内容的密钥。

如图 11 所示的，在本发明的系统中，设备密钥和内容密钥是根据图 10 中所示原则由密钥系统来管理的。在图 11 所示的示例中，在 8+24+32 层上的节点被安排成树型结构，并且，从根节点到根节点下第八层节点的节点是与类目相关的。术语类目指的是，例如，使用半导体存储器设备如记忆棒的类目，或者接收数字广播节目设备的类目。这些类目节点之一是与作为管理许可证系统(称为 T 系统)的本系统相关的。

具体地说，在与 T 系统相关节点之下，在与 24 层上节点相关的密钥，是与服务提供商或由服务提供商提供的服务相关联的。在该示例中，可以定义 2^{24}(大约 16M)个服务提供商或服务。使用底层 32 层，可以定义 2^{32}(大约 4G)个用户(或客户机 1)。从底层或第 32 层的每个节点到与 T 系统相关的节点路径上的节点，与这些节点相关的密钥构成了 DNK(设备节点密钥)。与底层每个叶相关的 ID 是叶 ID。

已加密内容的内容密钥被更新的根密钥 KR'加密。在较高层上更新的节点密钥是利用较低层上更新的节点密钥加密的，所述较低层上更新的节点密钥是与较高层上更新的节点密钥最邻近的节点密钥。这种被加密的节点密钥被安排在一个 EKB(后面将参考图 13 和 14 说明)中。在 EKB 中，在 EKB 结尾之上的层上，更新的节点密钥是由在 EKB 结尾的节点密钥或叶密钥来加密的，并且，所加密的节点密钥被安排在 EKB 中。利用在服务数据中所描述的、包含在 DNK 中的任何密钥，客户机 1 解密比所使用密钥更高层上的更新节点密钥，所述更新的节点密钥是与所使用的密钥最邻近的，并被描述在随内容数据一起分配的 EKB 中(图 13 和 14)。利用解密的密钥，客户机 1 解密比 EKB 中说明的密钥更高层上更新的节点密钥。客户机 1 逐个地执行相似处理，以获得更新的根密钥 KR'。

图 12 表示在分层树型结构中类目分类的具体示例。参考图 12，根密钥 KR2301 被设置在分层树型结构的顶层上；节点密钥 2302 被设置在低于顶层的中间层上；而叶密钥 2303 被设置在底层上。每个设备持有一个设备节点密钥(DNK)，设备节点密钥(DNK)由相应叶密钥、从叶密钥到根密钥的一系列节点密钥和根密钥构成。

在从顶层起的第 M 层(在图 11 所示示例中 M=8)上预先确定的节点被设置为类目节点 2304。具体地说，在 M 层上的节点被设置为属于具体类目的设备设置节点。让第 M 层上的一个节点是顶点。在第 M+1 层上及以下的

节点和叶被认为是与包含在那个类目中设备相关的节点和叶。

例如，在图 12 中第 M 层上的节点 2305 被设置成类目[记忆棒(商标)]。在节点 2305 以下的一系列节点和叶被设置为专门用于该类目即包含使用记忆棒的各种设备的类目的节点和叶。具体地说，在节点 2305 以下的节点和叶被定义为一组节点和叶，并且与所定义的属于类目“记忆棒”的设备相关。

在比第 M 层低几层的层上的节点被设置为子类目节点 2306。在图 12 的示例中，[只回放单元]节点 2306 被设置在比类目[记忆棒]节点 2305 低两层的层上。[只回放单元]节点 2306 是包含在使用记忆棒设备类目中的子类目节点。在作为子类目节点的只回放单元节点 2306 以下，节点 2307 被设置与具有音乐回放功能的电话相关，所述音乐回放功能的电话包含在只回放单元的类目中。在节点 2307 以下，设置[PHS]节点 2308 和[蜂窝电话]节点 2309，它们包含在具有音乐回放功能的电话类目中。

类目和子类目可以被设置为不仅与设备类型相关，而且还可以与例如由特定的制造商、内容提供商、付款机构等独立管理的节点相关，也就是在例如处理、权限部分或所提供的服务(在此之后这些统称为实体)的任意单元中。例如，让一个类目节点是专用于游戏机制造商出售的游戏机 XYZ 的顶点节点。由制造商出售的每个游戏机 XYZ，可以在顶点节点以下的层中保存节点密钥和叶密钥。随后，包含顶点节点密钥下这些节点密钥和叶密钥的使能密钥块(EKB)的产生和分配，使得能只向该顶点节点下那些设备分配加密内容以及分配和更新各种密钥。

当顶点节点下的节点被设置为与这些类目或子类目相关，即与该顶点节点相关定义的类目或子类目相关时，管理这些类目层或子类目层的顶点节点的制造商或内容提供者会独立产生使能密钥块(EKB)，使该顶点节点作为 EKB 的顶点，并且将该 EKB 分配给该顶点节点下的设备。因此，可以在不影响不属于该顶点节点和属于另一个类目的节点的设备下来更新密钥。

当在特定的时间 t，由设备 3 拥有的密钥 K0011、K001、K00、K0 和 KR 被黑客分析而泄漏出去时，需要将设备 3 从系统(设备 0、1、2 和 3 的组)分离出去，以便随后保护在系统内部传输的数据。为此，节点密钥 K001、K00、K0 和 KR 需要分别更新为新密钥 K(t)001、K(t)00、K(t)0 和 K(t)R，并需要将这些更新的密钥发送给设备 0、1 和 2。在该示例中，K(t)aaa 表示在产生时间 t 密钥 Kaaa 的更新密钥。

以下将说明更新密钥的分配方法。利用因特网或其中保存表格的记录媒介，通过向设备 0、1 和 2 提供例如包含称为使能密钥块(EKB)的表，如图 13 所示，来更新密钥。使能密钥块(EKB)包括用于向树型结构中所包含的叶(底层节点)相关的设备，分配新的更新密钥的加密密钥，其中树型结构如图 10 所示。使能密钥块(EKB)还可以被称为密钥恢复块(KRB)。

图 13 中所示的使能密钥块(EKB)包括具有一个数据结构的块数据，该数据结构只可以由节点密钥需要更新的那些设备来更新。在图 13 的示例中，创建该块数据，以便在产生时间 t 向图 10 所示树型结构中的设备 0、1 和 2 分配这些更新的节点密钥。从图 10 可以清楚地看到，设备 0 和 1 需要更新的节点密钥 K(t)00、K(t)0 和 K(t)R，而设备 2 需要更新的节点密钥 K(t)001、K(t)00、K(t)0 和 K(t)R。

如图 13 中的 EKB 所示，EKB 包括多个加密密钥。例如，在图 13 底层的加密密钥是 Enc(K0010，K(t)001)，它是由设备 2 拥有的叶密钥 K0010 所加密的更新节点密钥 K(t)001。设备 2 利用它自己拥有的叶密钥 K0010 解密该加密的密钥以获得更新的节点密钥 K(t)001。利用解密获得的更新的节点密钥 K(t)001，设备 2 解密从图 13 底层起的第二层加密密钥 Enc(K(t)001，K(t)00)，以获得更新的节点密钥 K(t)00。

相似地，按这个顺序，设备 2 解密从图 13 顶层起的第二层加密密钥 Enc(K(t)00，K(t)0)以获得更新的节点密钥 K(t)0。利用更新的节点密钥 K(t)0，设备 2 解密从图 13 顶层第一层加密密钥 Enc(K(t)0，K(t)R)，以获得更新的根密钥 K(t)R。

相反地，节点密钥 K000 没有包含在要被更新的密钥中。节点 0 和 1 使下面的节点密钥更新：K(t)00、K(t)0 和 K(t)R。每个节点 0 和 1 都利用从图 13 顶层起的第三层的设备密钥 K0000 和 K0001 解密加密密钥 Enc(K000，K(t)00)，以获得更新的节点密钥 K(t)00。按照相似的顺序，每个节点 0 和 1 解密从图 13 的顶层起的第二层的加密密钥 Enc(K(t)00，K(t)0)以获得更新的节点密钥 K(t)0。每个节点 0 和 1 解密从图 13 顶层起的第一层加密密钥 Enc(K(t)0，K(t)R)以获得更新的密钥 K(t)R。以这种方式，设备 0、1 和 2 中的每个都获得了更新的密钥 K(t)R。

图 13 中的索引表示用作解密图 13 右边所示加密密钥的解密密钥的节点密钥和叶密钥的绝对地址。

当在图 10 中所示的树型结构的上层节点密钥 K(t)0 和 K(t)R 不需要更新，并且只有节点密钥 K00 需要更新时，图 14 中的使能密钥块(EKB)才被用于向设备 0、1 和 2 分配更新的节点密钥 K(t)00。

图 14 中所示的 EKB 可以被用于分配例如将由具体组共享的新内容密钥。在这个具体的示例中，假定包含在由图 10 点线表示的组中的设备 0，1，2 和 3 每个都使用特定的记录媒介，并需要一个新的公共内容密钥 K(t)con。在这种情况下，加密的数据 Enc(K(t)00，K(t)con)随着图 14 所示的 EKB 一起分配。加密的数据 Enc(K(t)00，K(t)con)是通过使用 K(t)00 加密新的公共更新内容密钥 K(t)con 而产生的，而 K(t)00 已更新了由设备 0，1，2 和 3 共享的节点密钥 K00。通过这种分配，就分配了不能被属于另一个组的设备例如设备 4 所解密的数据。

具体地说，设备 0，1 和 2 中的每个都使用处理 EKB 所获得的密钥 K(t)00 来解密密文，因此，获得在时间 t 的内容密钥 K(t)con。

图 15 表示获得时间 t 内容密钥 K(t)con 的处理，该处理是通过记录媒介由已收到加密数据 Enc(K(t)00，K(t)con)的设备 0 来执行的，其中加密数据是通过使用图 14 所示的 K(t)00 和 EKB 来加密新的公共内容密钥 K(t)con 而产生的。具体地说，在这个示例中，由 EKB 加密的消息数据就是内容密钥 K(t)con。

如图 15 所示，设备 0 使用保存在记录媒介中的在产生时间 t 的 EKB 以及预先保存在设备 0 中的节点密钥 K000，通过与上述相似的 EKB 处理来产生节点密钥 K(t)00。使用解密的更新节点密钥 K(t)00，设备 0 对更新的内容密钥 K(t)con 进行解密。为了以后使用解密的更新内容密钥 K(t)con，设备 0 使用仅由设备 0 持有的叶密钥 K0000 加密更新的内容密钥 K(t)con，并保存加密后的内容密钥。

图 16 表示使能密钥块(EKB)格式的示例。版本 601 是识别符，表示使能密钥块(EKB)的版本。版本的功能是识别最近的 EKB，以及表示 EKB 和内容之间的相关关系。深度表示与使能密钥块(EKB)分配给的设备所相关的分层树型的层数。数据指针 603 是表示使能密钥块(EKB)的数据部分 603 位置的指针。标记指针 604 是表示标记部分 607 的位置的指针，而签名指针 605 是表示签名 608 位置的指针。

数据部分 606 保存例如通过加密要更新的节点密钥所产生的数据。例

如，数据部分606保存与更新的节点密钥相关的加密密钥，如图15所示。

标记部分607包括一些标记，表示被加密的节点密钥和在数据部分606中保存的叶密钥之间的位置关系。下面将参考图18说明附加标记的规则。

在图17中，表示了这样的例子，在其中，发送数据，即发送图13中表示的使能密钥块。在这个案例中的数据被安排成如图17B来表示。包含在加密密钥中的顶层节点的地址被称为顶层节点地址。由于在这个示例中该数据包括更新的根密钥 K(t)R，所以顶层节点地址就是 KR。例如，在顶层的数据 Enc(K(t)0，K(t)R)是与图17A所示分层树型中的位置P0相关的。在下一层的数据是与树型中以前数据的左下方中位置 P00 相关的 Enc(K(t)00，K(t)0)。当在树型结构中预先确定的位置下有数据时，则该标记被设置为0。否则，该标记被设置为1。该标记被设置为{左(L)标记，右(R)标记}。在表B中，由于在与顶层 Enc(K(t)0，K(t)R)中数据相关的位置 P0 的左下方的位置 P00 上存在数据，所以L 标记＝0。由于在右方没有数据，所以R 标记＝1。采用这种方式标记所有段的数据，从而形成数据序列和标记序列，如图17C所示。

在树型结构中附加标记，来表示相应数据 Enc(Kxxx，Kyyy)的位置。保存在数据部分 66 之内的密钥数据段 Enc(Kxxx，Kyyy)...仅仅是一系列被加密的密钥的段。当如上所述标记了密钥数据时，在保存为数据的每个加密密钥的树型中的位置就变得可以检测了。如图 15 所示，代替对数据标记，数据结构可以通过例如下面的与加密数据相关的节点索引来定义:

0：Enc(K(t)0，K(t)R)

00：Enc(K(t)00，K(t)0)

000：Enc(K(t)000，K(t)00)

...

当该结构是使用这样的索引定义时，这些索引是冗余数据，并且数据量增加了，这是在通过网络等的分配中所不希望的。相反，当上述标记被用作表示密钥位置的索引数据时，密钥的位置变成了利用较少数据就可以检测了。

参考图16，对EKB格式作更详细地说明。签名608是数字签名，由例如密钥管理中心(许可证服务器4)，内容提供者(内容服务器3)，支付机构(记帐服务器5)等创建，并由例如密钥管理中心(许可证服务器4)，内容提供者(内容服务器3)，支付机构(记帐服务器5)等发行使能密钥块(EKB)。接收到EKB

的设备验证包含在 EKB 中的签名，以确定所得到的使能密钥块是否由真实的使能密钥块发行者发行。

根据许可证服务器 4 提供的使用权利，在图 18 中总结了上述使用内容服务器 3 提供的内容的处理。

具体地说，由内容服务器 3 向客户机 1 提供内容，并且由许可证服务器 4 向客户机 1 提供许可证。在客户机 1 登记的时间中，在许可证服务器和使用权利中提供的一组服务数据作为允许使用特定内容的信息，称为许可证。内容由内容密钥 Kc (Enc(K(t), Content))加密。内容密钥 Kc 由更新的根密钥 KR'(从 EKB 可得到的密钥；与图 5 中的 K_{EKBC} 相关) (Enc(KR′, Kc))加密。被加密的内容密钥 Kc(Enc(KR′, Kc))，与 EKB 一起被加到被加密的内容上，并被提供给客户机 1。

图 18 所示示例中的 EKB 包括例如图 19 中所示更新的根密钥 KR′, KR′可以由 DNK (Enc(DNK, KR′))解密。使用包含在服务数据中的 DNK，客户机 1 从 EKB 中获得更新的根密钥 KR′。使用更新的根密钥 KR′，客户机 1 解密 Enc(KR′, Kc)以获得内容密钥 Kc。使用内容密钥 Kc，客户机 1 解密 Enc(K(t), Content)以获得内容。

通过向每个设备分配 DNK，依据参考图 10 和图 15 所说明的原理，可以取消单个的客户机 1。

通过向每个客户机 1 添加和分配许可证叶 ID，每个客户机 1 检测服务数据和使用权利之间的相关性。这就防止未授权地复制使用权利。

通过分配每个客户机的证书和私钥作为服务数据的一部分，每个终端用户使用包括证书和私钥的服务数据以创建内容，并防止了内容的未授权复制。

依据本发明，如参考图 11 所说明的那样，使用各种类型的内容来管理许可证和设备类目的 T 系统是与类目节点相关的。这就使得一个设备能保持多个 DNK。结果，一个设备可以管理属于不同类的多个段的内容。

图 20 表示这种关系的示例。具体地说，根据 T 系统，DNK1 被分配设备 D1。结果，设备 D1 可以播放包含 EKB 的内容 1。相似地，例如 DNK2 被分配给设备 D1。结果，设备 D1 可以记录源自 CD 的内容到 2 记忆棒中。在这种情况下，设备 D1 可以处理由不同系统(T 系统和设备管理系统)分配的内容 1 和内容 2。另一方面，当只有一个 DNK 以这样的方式被分配给每

个设备时，即已经分配给该设备的旧的DNK被删除掉以分配新的DNK时，就不能实现这样的处理。

依据本发明，在每个类目下进行独立的密钥管理是可能的。

代替在每个设备或媒介中预先嵌入一个DNK，DNK是在登记时间中从许可证服务器4下载到每个设备或媒介中的。因此，实现了使用户能够购买密钥的系统。

在单独分配内容和内容使用权限的系统中，最好是创建之后的内容可用于所有目的，而与用法无关，也不管用法可能是什么。例如，最好是在不同的内容分配服务中，或对于不同的目的，可以使用相同的内容。如上所述，依据本发明，用作证明授权的许可证服务器4向单用户(客户机1)分配私钥以及与私钥相关的公钥证书。每个用户使用私钥来创建签名并将签名添加到内容中，以证明内容的完整性并防止未授权地改变内容。

下面将说明校验从客户机1到记忆棒(商标)的内容的处理，该记忆棒放在客户机1上，是一种安全媒介，并且是内容存储设备的示例。

图21表示记忆棒结构的说明。记忆棒651包括闪速存储器(非易失)651，存储器控制块662以及包含DES(数据加密标准)加密电路的安全块663，这些都封装在IC芯片内。

闪速存储器661在存储器控制块662的控制下，保存编码和加密的内容。

存储器控制块662执行串行/并行或并行/串行转换，分离出被提供的命令和数据，并执行分离出的命令。依据被提供的命令，存储器控制块662在闪速存储器上保存内容或读取保存在闪速存储器661中的内容。

记忆棒651的安全块663保存多个认证密钥和一个对每个存储卡唯一的存储密钥。安全块663具有一个随机数产生电路，在存储器控制块662的控制下执行与客户机1的相互认证，并与客户机1共享会话密钥。

安全块663保存包含使用规则和MAC值的索引，这将在下面说明。

安全块663在存储器控制块662的控制下对加密的内容进行解密。

图22是表示客户机1内容校验处理的流程图。

在步骤S201中，客户机1的CPU 21选择将被校验的内容，并从包含在所选择内容属性当中创建签名。

例如，客户机1的CPU 21通过利用许可证服务器的公钥对包含在内容中的属性进行加密，创建签名，其中，公钥包含在证书中。

在步骤S202中，客户机1的CPU 21将为属性创建的签名与包含在内容中属性的签名进行比较。当判断出为属性创建的签名与包含在内容中的属性的签名一致时，就确定属性未被更改。处理进行到步骤S203中。

当判断出在步骤S202中，为属性创建的签名与包含在内容中的属性的签名不一致时，就确定属性被更改。在步骤S209中，客户机1的CPU 21执行出错处理，如显示错误信息。CPU 21不执行校验，结束处理。

在步骤S203中，客户机1的CPU 21从存储单元28中搜索在其中的这样的存储权利，该存储权利的内容规则是满足目标内容属性的，因此，允许执行校验。在步骤S209中，当在存储单元28中没有检测到使用目标内容的这样的使用权利时，客户机1的CPU 21执行出错处理，如显示错误消息。CPU 21不执行校验并结束处理。

在步骤S204中，当检测到使用内容的使用权利时，客户机1的CPU 21判断是否有一个或多个使用内容的使用权利保存在存储单元28中。

在步骤205中，当判断出使用目标内容的多个使用权利保存在存储单元28中时，客户机1的CPU 21在输出单元27的显示器上显示信息，例如每个使用权利的使用规则，并命令用户判断哪个使用权利的使用规则用作将要校验内容的使用规则。根据由用户输入到输入单元26中的数据，判断出哪个使用规则将用于校验内容。

代替在步骤S205中由用户选择使用权利，使用权利也可以根据预先确定的规则优先处理。

当判断出使用目标内容的一个使用权利是保存在存储单元28中时，就意味着确定了将被用于校验内容的使用权利。因此，使用权利的选择不在步骤S205中执行。处理进行到步骤S206。

在步骤S206中选择了使用内容的使用权利之后，客户机1的CPU 21从使用权利的使用规则中创建签名。

例如，客户机1的CPU 21通过使用许可证服务器的公钥对包含在使用权利中的使用规则进行加密来创建签名，其中公钥包含在证书中。

在步骤S207中，客户机1的CPU 21比较所为使用规则创建的签名与包含在使用权利中的使用规则的签名。当判断出为使用规则创建的签名与包含在使用权利中的使用规则的签名一致时，就确定使用规则是没有改变的。处理进行到步骤S208中。在步骤S208中，客户机1的CPU 21执行校验。

结束处理。

当在步骤 S207 中判断出为属性创建的签名与包含在内容中属性的签名不一致时，就确定属性改变了。在步骤 S209 中，客户机 1 的 CPU 21 执行出错处理，如显示错误信息。CPU 21 不执行校验。处理结束。

图 23 是说明与步骤 S208 的处理相关的客户机 1 校验执行处理的流程图。

在步骤 S221 中，客户机 1 的 CPU 21 执行与放置在客户机 1 上的记忆棒的相互认证。例如，客户机 1 的 CPU 21 和记忆棒 651 的安全块 663 执行挑战－响应相互认证。

当在步骤 S221 中处理所做的相互认证失败了，就意味着客户机 1 或记忆棒 651 没有得到认证。将跳过步骤 S222 到步骤 S228 的处理。内容不写到记忆棒 651 中。处理结束。

当在步骤 S221 中的处理所做的相互认证成功了，就意味着客户机 1 和记忆棒 651 得到相互认证。客户机 1 和记忆棒共享公共的临时密钥(会话密钥)。执行从步骤 S222 到步骤 S228 的处理。

在从这点向前的处理中，其中共享公共的临时密钥(会话密钥)，由客户机 发送给记忆棒 651 的信息由加密/解密单元 24 使用临时密钥来加密。由于客户机 1 从记忆棒 651 中接收到的这样的信息是使用临时密钥加密的，所以，由加密/解密单元 24 执行解密。

在步骤 S222 中，客户机 1 的 CPU 21 将内容写到记忆棒 651 中。例如，客户机 1 的 CPU 21 从记忆棒 651 中获得记忆棒 651 的内容密钥，并将记忆棒 651 的内容密钥重锁(relocked)的内容提供给记忆棒 651。

可选择地，记忆棒也可以重锁(relock)该内容。

在步骤 S223 中，客户机 1 的 CPU 21 将使用权利的使用规则的格式转换为与记忆棒相关的格式。

在步骤 S224 中，客户机 1 的 CPU 21 使加密/解密单元 24 计算使用权利的使用规则的消息认证码(MAC)(下面可以称为 MAC 值)。

图 24 表示使用 DES 加密算法的 MAC 值产生的示例。如图 24 所示的那样，目标消息(使用规则)被划分成 8 个字节的单位(消息的各个段由 M1，M2，...，MN)表示。首先，初始值(IV)和 M1 是通过算术运算单元 24-1A 计算的(结果由 I1 表示)。接下来，I1 被输入到 DES 加密单元 24-1B，并使用

密钥(下面称为 K1)进行加密(输出由 E1 表示)。E1 和 M2 的异或由算术运算单元 24-2A 计算。算术运算单元 24-2A 的输出 I2 被输入到 DES 加密单元 24-2B，并使用密钥 K1 进行加密(输出 E2)。重复该操作以加密整个消息。从 DES 加密单元 24-NB 的最后输出 EN 用作消息认证码(MAC)。

在步骤 S225 中，客户机 1 的 CPU 21 将使用规则，其格式已在步骤 S223 中处理中被转换，连同在步骤 S224 中所计算的 MAC 值写到记忆棒 651 的索引中。

图 25 是说明保存在记忆棒 651 中的索引和内容的示意图。

记忆棒 651 的索引 701，结合每段内容，保存了使用规则、MAC 和内容的指针。在索引 701 中的每个指针保存了内容的地址。

例如，保存在记忆棒 651 中表示内容 702-1 的指针，连同内容 702-1 的使用规则和与使用规则相关的 MAC 值被保存在索引 701 中。保存在记忆棒 651 中表示内容 702-2 的指针，连同内容 702-2 的使用规则和与使用规则相关的 MAC 值被保存在索引 701 中。保存在记忆棒 651 中表示内容 702-3 的指针，连同内容 702-3 的使用规则和与使用规则相关的 MAC 值被保存在索引 701 中。

在步骤 S226 中，客户机 1 的 CPU 21 从记忆棒 651 中获得包含新的使用规则和 MAC 值的索引 701，其中使用规则和 MAC 值是在步骤 S225 的处理中写的。

在步骤 S227 中，客户机 1 的 CPU 21 根据包含新的使用规则和 MAC 值的索引 701，计算全部记忆棒 651 的完整性检验值(ICV)。

索引 701 的完整性检验值是通过例如索引 701 的 hash 函数来计算：ICV=hash(Kicv, R1, R2, ...)，其中，Kicv 是 ICV 产生密钥，而 L1 和 L2 是由使用规则的 MAC 值组成的使用规则信息。

在步骤 S228 中，客户机 1 的 CPU 21 向计算后的完整性检验值上重写记忆棒 651 的完整性检验值。处理结束。

例如，客户机 1 的 CPU 21 根据与内容 702-1 到 702-3 相关的 MAC 值，计算完整性检验值，其中内容 702-1 到 702-3 是从记忆棒 651 中获得并包含在索引 701 当中的。

如图 25 所示，客户机 1 的 CPU 21 向记忆棒 651 中写入计算后的完整性检验值 703。

客户机 1 利用临时密钥加密完整性检验值，并将加密后的完整性检验值通过所谓的 SAC(安全认证信道)发送到记忆棒 651 中。

因此，记忆棒以安全的方式保存了与索引 701 相关的完整性检验值。

例如，在利用根据使用规则所产生的 ICV 703 来播放内容时，当根据索引 701 产生的 ICV 的比较结果显示出两个 ICV 是相同时，就能确保使用规则是没有改变的。当 ICV 是不一致时，就确定出使用规则是被改变了。

下面将参考图 26 的流程图说明记忆棒 651 的校验执行处理，这是与客户机 1 的校验执行处理相关的，如图 23 所示。

在步骤 S241 中，记忆棒 651 的安全块 663，结合客户机 1 的 S221 的处理，执行与客户机 1 的相互认证。

当相互认证成功时，客户机 1 和记忆棒 651 共享公共的临时密钥(会话密钥)。

在从这点向前的处理中，其中共享了公共的临时密钥(会话密钥)，由记忆棒 651 发送给客户机 1 的信息是使用临时密钥被安全块 663 加密的。由于记忆棒 651 从客户机 1 接收的信息是被临时密钥来加密的，所以记忆棒的安全块 663 解密被加密的信息。

在步骤 S242 中，由于客户机 1 执行步骤 S222 中的处理以发送内容，所以记忆棒 651 的存储器控制块 662 接收该内容并将该内容保存到闪速存储器 661 中。

在步骤 S243 中，由于客户机 1 执行步骤 S225 中的处理以发送其格式已被转换的使用规则，所以，记忆棒 651 的存储器控制块 662 接收使用规则，并将接收的使用规则写到安全块 663 的索引 701 中。结合使用规则，记忆棒 651 将表示通过步骤 S242 处理存储的内容的指针写到安全块 663 中。

通过步骤 S243 中的处理，如图 25 所示，安全块 663 的索引 701 保存与最新存储的内容相关的使用规则、MAC 值和表示内容的指针。

在步骤 S244 中，响应从客户机 1 来的请求，记忆棒 651 的存储控制块 662 从安全块 663 中读取索引 701，并将读到的索引 701 发送给客户机。当接收到由步骤 S224 中的处理发送的索引 701 时，客户机 1 通过步骤 S226 中的处理获得了索引 701。

在步骤 S245 中，由于客户机 1 执行步骤 S228 中的处理以发送一个新的 ICV，记忆棒 651 接收客户机 1 发送的 ICV，并根据接收到的 ICV 更新 ICV。

处理结束。

采用这种方式，通过使用公钥加密而产生的签名是一个完整性信息，被加到内容中。完整性信息，是根据公钥加密体制的 hash 值，由客户机 1 产生的并被添加到数据存储媒介上的使用规则中。关于内容的完整性信息以及关于使用规则的完整性信息结合起来，作为一段信息并且作为索引 701 的一部分来管理。

甚至当记忆棒的吞吐量较低时，客户机 1 也可以根据公钥体制利用签名校验给记忆棒的内容，而不降低内容的保护级别。

甚至低吞吐量的终端也可以使用相同的内容。因此，所有的设备都可以交换内容。

具体地说，当内容被写到记忆棒中时，内容就可以被保存在记忆棒中。

在带有数字签名的内容写入被控制的情况下，使用该内容的必要使用权利的使用规则被转换成与内容存储设备相关的格式，并产生用于检测格式转换后使用权利变更的使用规则变更检测数据，并且控制格式转换后使用规则和使用规则变更检测数据的写入，甚至低吞吐量的记忆棒也可以使用该内容，并且可靠地防止了未授权地使用该内容。

当提供了保存该内容的存储器时，就可以保存该内容。

在控制了带有数字签名的内容存储的情况下，该数字签名由信息处理设备提供的，并且控制了使用规则和用于检测使用规则变更的使用规则变更检测数据的存储的情况下，其中使用规则和用于检测使用规则变更的使用规则变更检测数据是由信息处理设备提供的，甚至低吞吐量的设备也可以使用该内容，并且可靠地防止未授权地使用内容。

在选择了内容的情况下，其中该内容将要保存在用作内容存储设备的记忆棒上，验证加到所选内容上的第一数字签名，保存允许使用所选内容的使用权利，从存储单元 28 中检索与所选择内容相关的使用权利，验证加到所检索使用权利上的第二数字签名，根据包含在所检索使用权利中的信息产生变更检测数据，并且，当根据第一验证结果和第二验证结果判断出内容和使用权利是未改变时，使用权利、变更检测数据和内容均被输出到内容存储设备中，甚至低吞吐量记忆棒也能使用该内容，并可靠地防止了内容的未授权使用。

虽然在示例中已说明了从客户机到记忆棒的内容校验，但是内容可以从

客户机复制到记忆棒中，或者内容从客户机传递到记忆棒中。

虽然在示例中已说明了从客户机到记忆棒的内容校验，但是内容可以从客户机到 PD 进行校验、传输或者复制，这是内容存储设备的另一个示例。

内容可以从客户机到放置在 PD 的记忆棒中进行校验，传输或复制。在这样的情况下，在客户机和 PD 之间，以及 PD 和记忆棒之间执行认证。

本发明应用到的客户机除了所谓的计算机外，还包括 PDA(个人数字助理)、蜂窝电话，游戏终端等等。

为了执行一系列的软件处理，包括软件的程序通过网络或记录媒介被安装到含有专用硬件的计算机中，如通过在个人计算机中安装各种程序能执行各种功能的通用个人计算机。

如图 2 所示，记录媒介不仅包括与设备分开的、向用户提供程序的分布型组件媒介，该分布型组件媒介包括如磁盘 41(包括软盘)、光盘 42(包括 CD－ROM(压缩盘－只读存储器)和 DVD(数字多用盘))、磁光盘 43(包括 MD(微型盘)(商标))、以及记录程序的半导体存储器 44，而且还可以包括记录程序的 ROM 22，或者通过预先包含在设备当中提供给用户并包含在存储器 28 中的硬盘。

在本发明的说明书中，记录在记录媒介上的程序的写入步骤不仅包括依据说明的顺序执行的时间序列处理，还包括并行或独立的处理，而这些处理可能不必按时间序列执行。

最好对执行与安全相关处理的程序进行加密以防止处理被分析。例如，执行加密处理的程序可以用反篡改模块实现。

在上述说明的实施例中，内容属性和使用权利的内容规则被用于具体说明使用该内容的必要使用权利。但是，具体说明该使用权利的必要信息不局限于这些段的信息。例如，内容可以包括使用该内容的必要使用权利的使用权利 ID。在这种情况下，当内容被具体说明时，使用该内容的必要使用权利是唯一确定的，因此，不必再执行判断内容和使用权利之间匹配的处理。

本发明的工业应用性说明如下:

如上所述，依据本发明，内容被保存在内容存储设备上。

依据本发明，甚至低吞吐量的内容存储设备也可以使用内容，从而可靠地防止了内容的未授权使用。

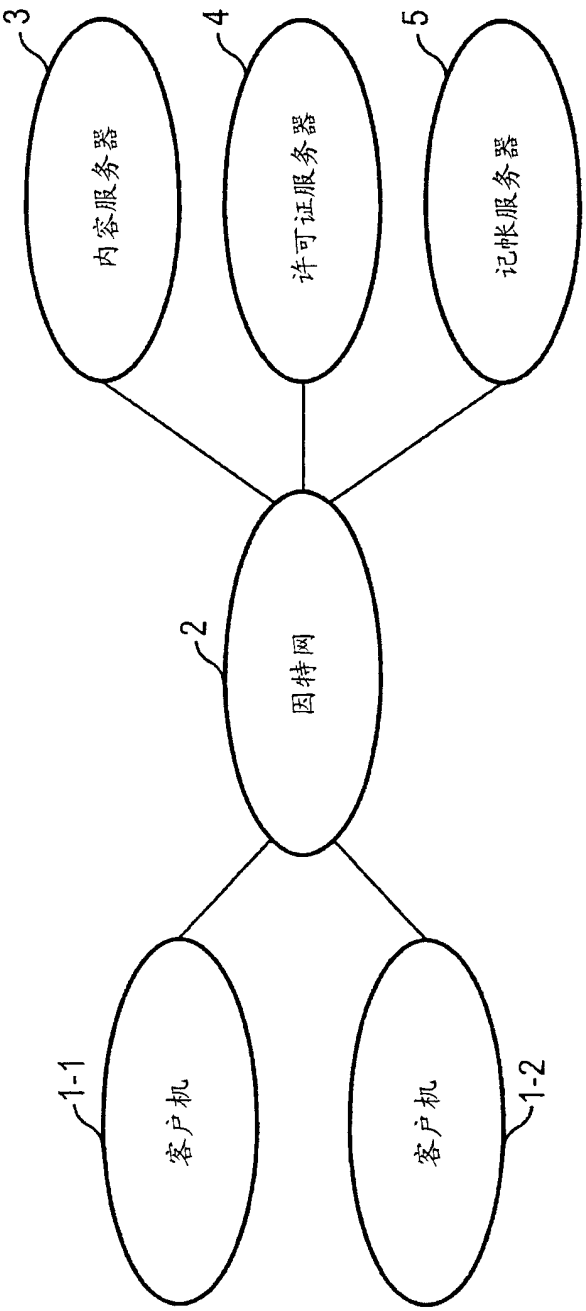


图 1

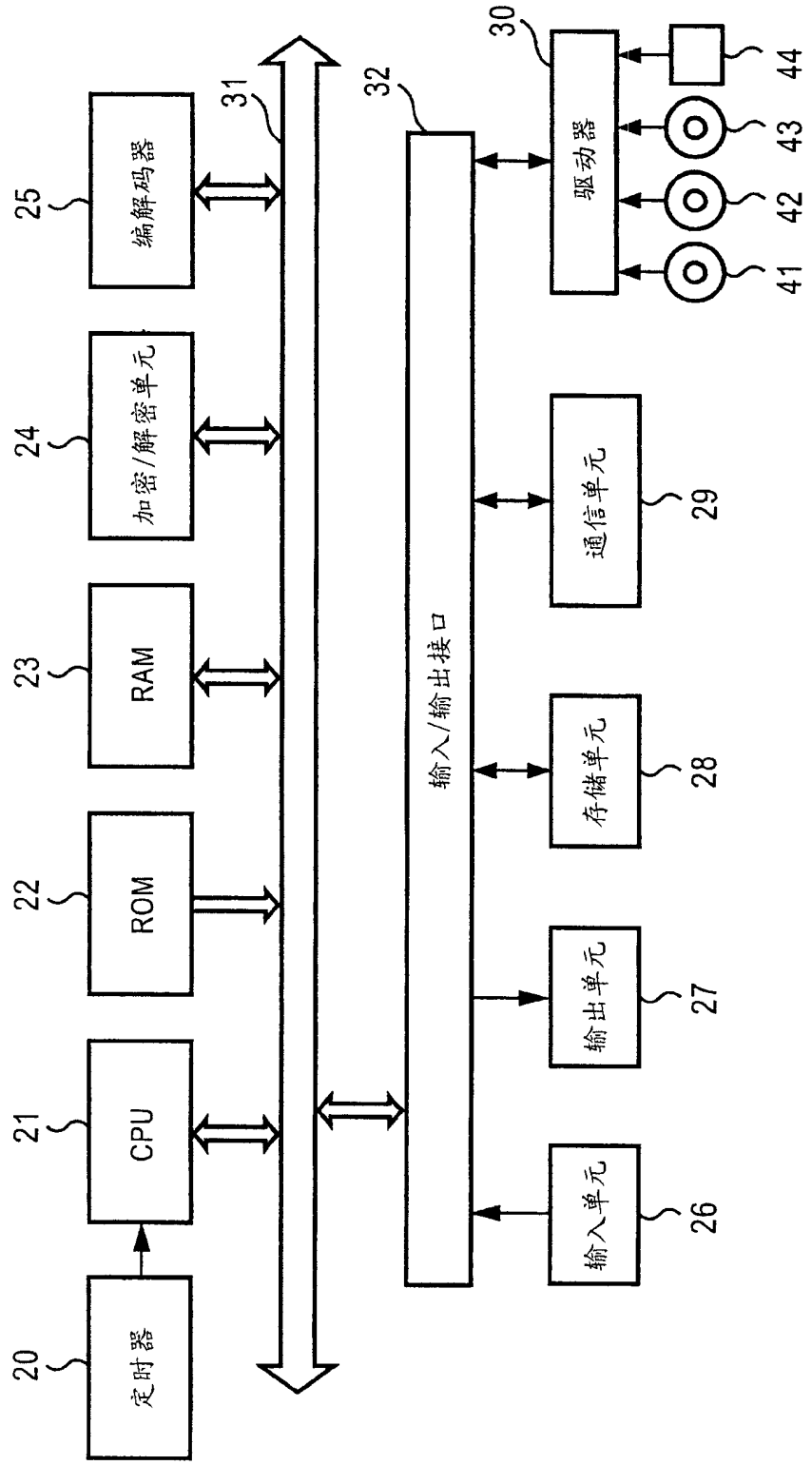

20
定时器
21
CPU
22
ROM
23
RAM
24
加密/解密单元
25
编解码器
31
32
输入/输出接口
26
输入单元
27
输出单元
28
存储单元
29
通信单元
30
驱动器
41
42
43
44

图 2

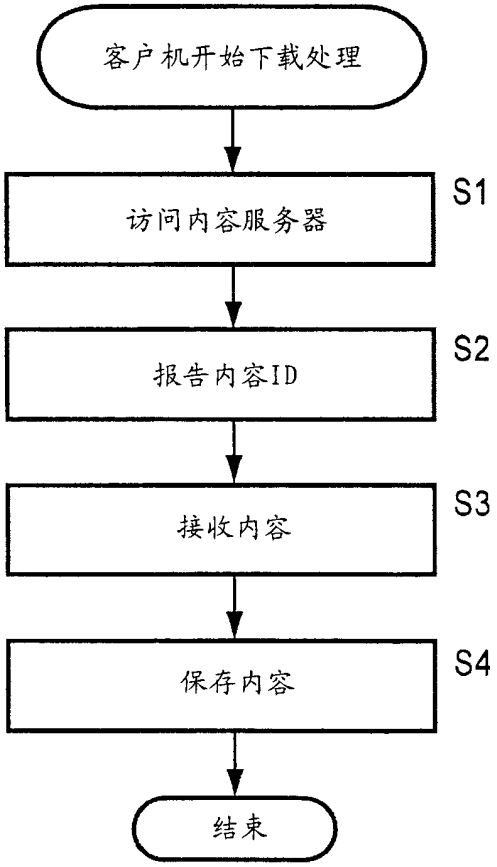


图 3

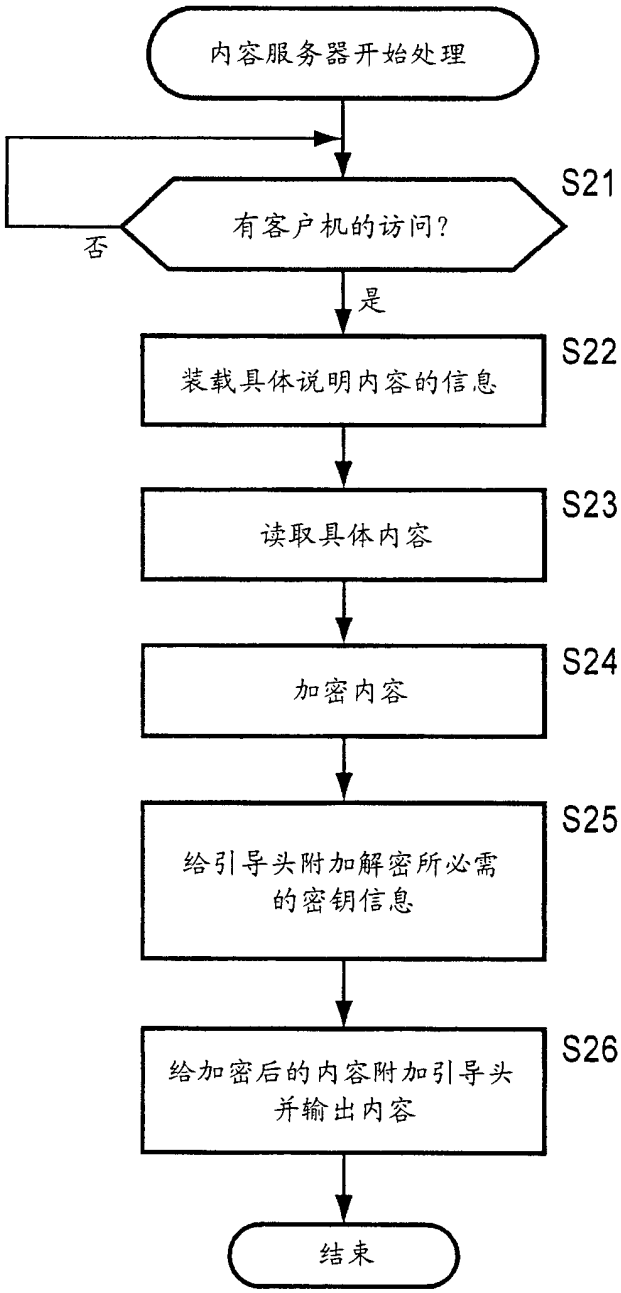

内容服务器开始处理
S21
有客户机的访问?
否
是
S22
装载具体说明内容的信息
S23
读取具体内容
S24
加密内容
S25
给引导头附加解密所必需的密钥信息
S26
给加密后的内容附加引导头并输出内容
结束

图 4

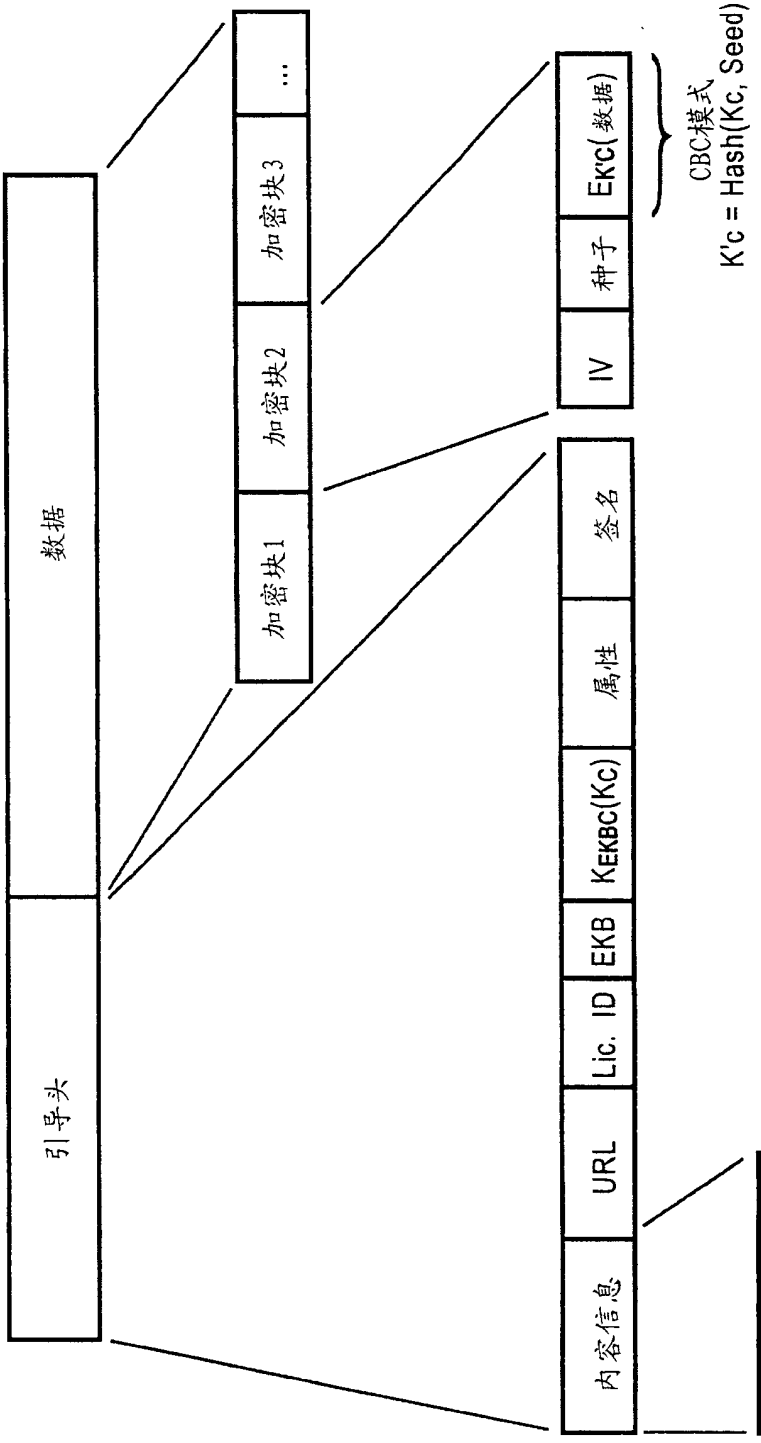

引导头
数据
加密块1
加密块2
加密块3
...
内容信息
URL
Lic. ID
EKB
KEKBC(Kc)
属性
签名
IV
种子
EKC(数据)
CBC模式
K'c = Hash(Kc, Seed)
内容ID
编解码等...

图 5

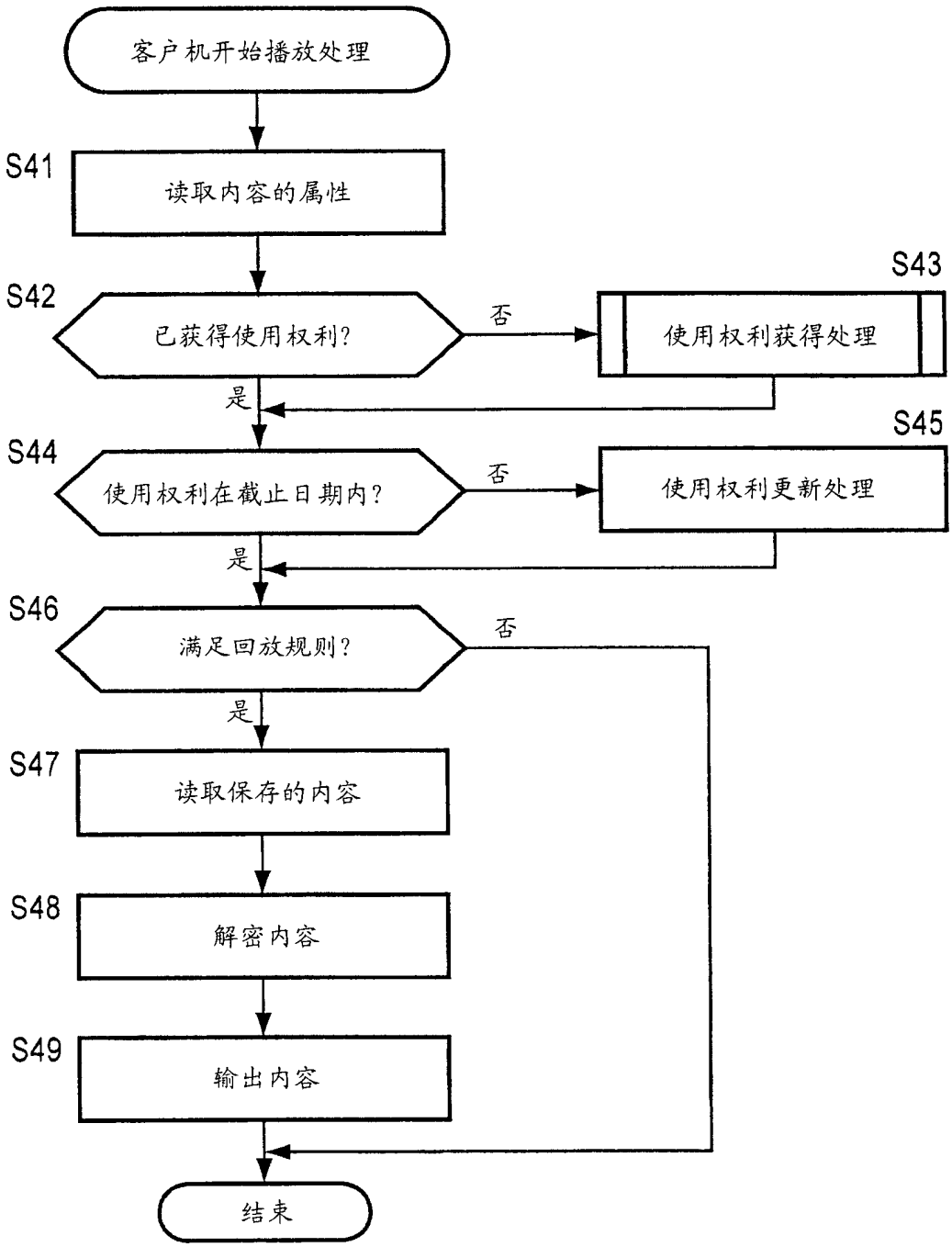

客户机开始播放处理
S41
读取内容的属性
S42
已获得使用权利?
否
S43
使用权利获得处理
是
S44
使用权利在截止日期内?
否
S45
使用权利更新处理
是
S46
满足回放规则?
否
是
S47
读取保存的内容
S48
解密内容
S49
输出内容
结束

图 6

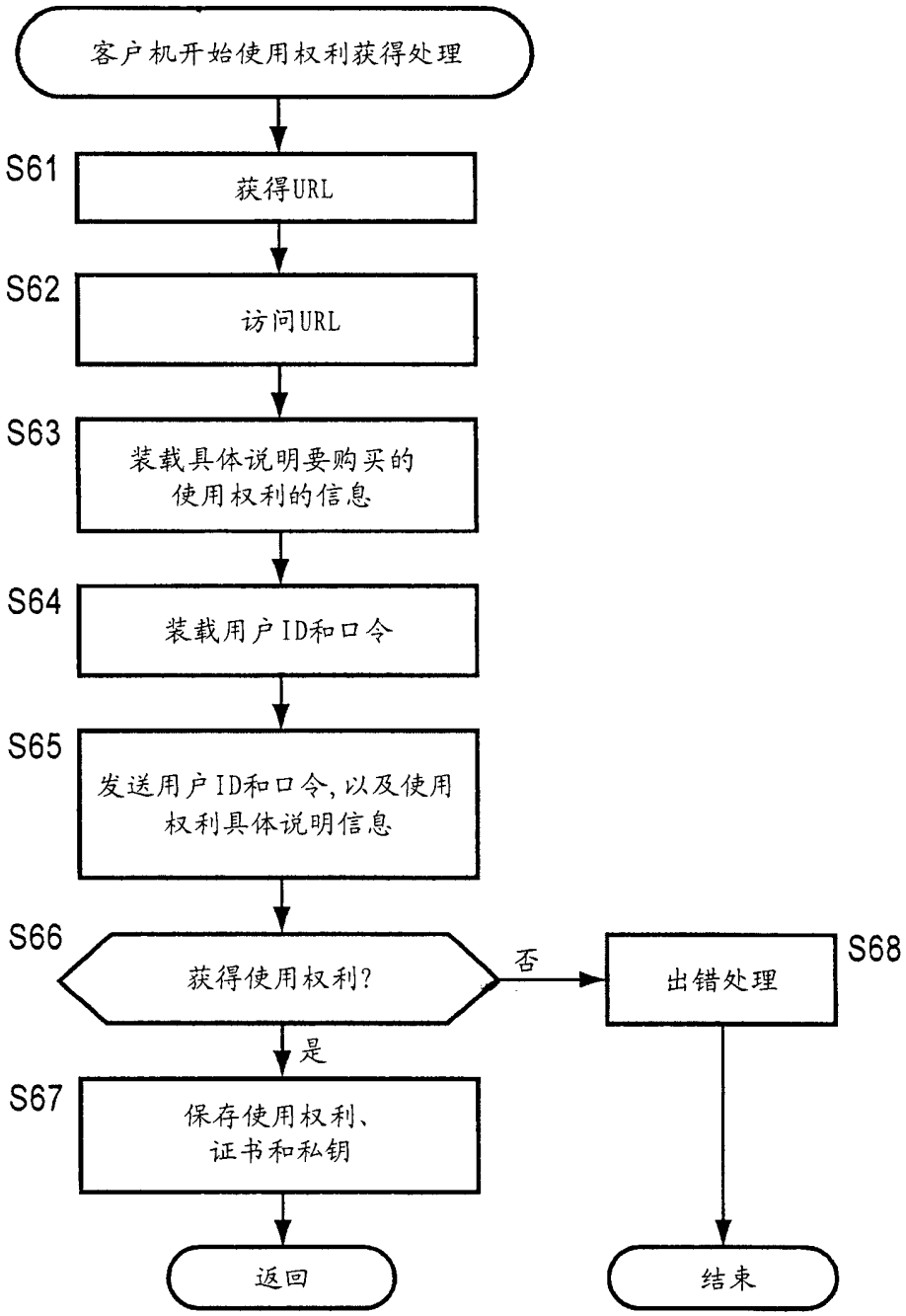

客户机开始使用权利获得处理
S61
获得URL
S62
访问URL
S63
装载具体说明要购买的
使用权利的信息
S64
装载用户ID和口令
S65
发送用户ID和口令,以及使用
权利具体说明信息
S66
获得使用权利?
否
S68
出错处理
是
S67
保存使用权利、
证书和私钥
返回
结束

图 7

图 8

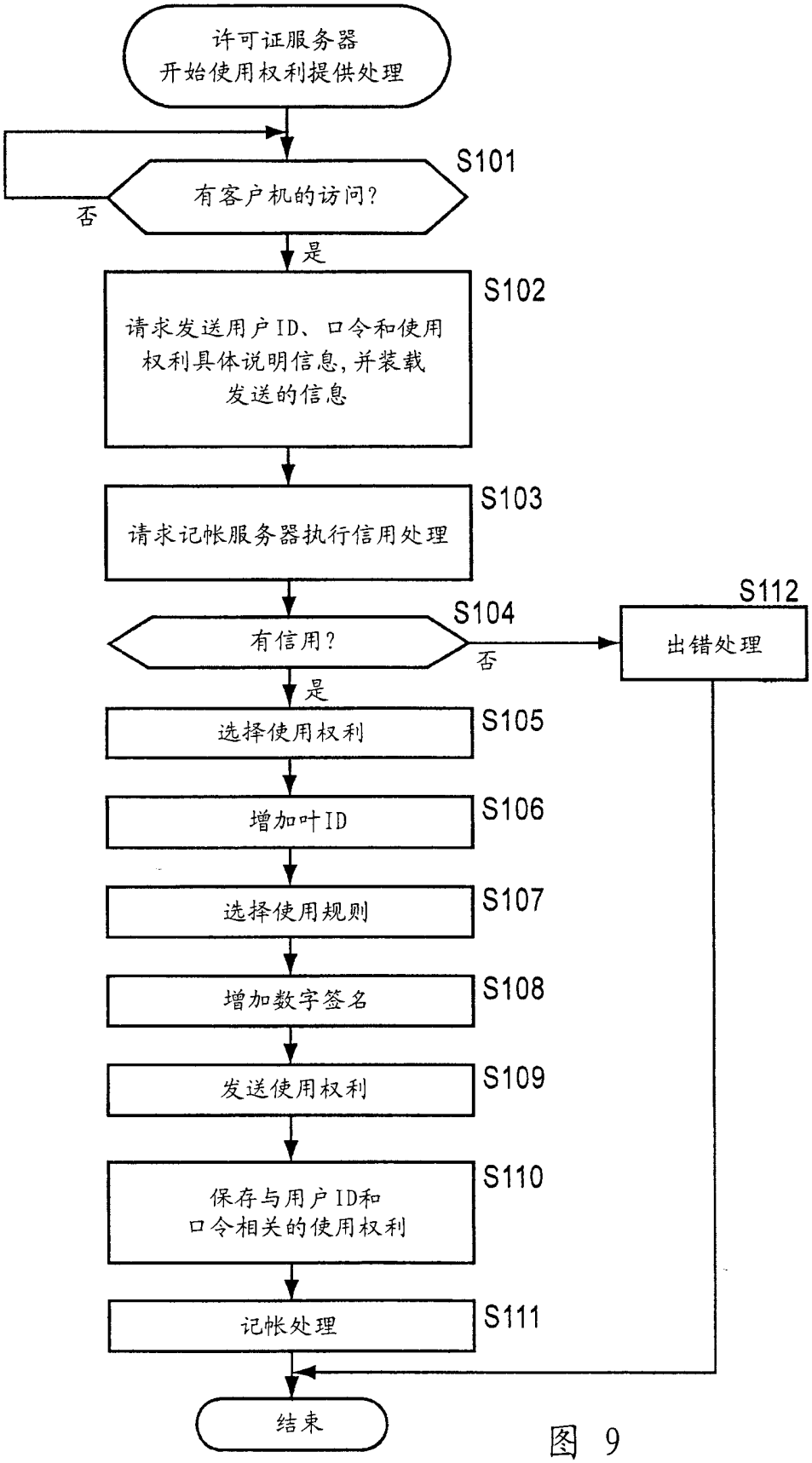

许可证服务器
开始使用权利提供处理
S101
有客户机的访问?
否
是
S102
请求发送用户ID、口令和使用权利具体说明信息,并装载发送的信息
S103
请求记帐服务器执行信用处理
S104
有信用?
否
S112
出错处理
是
S105
选择使用权利
S106
增加叶ID
S107
选择使用规则
S108
增加数字签名
S109
发送使用权利
S110
保存与用户ID和口令相关的使用权利
S111
记帐处理
结束

图 9

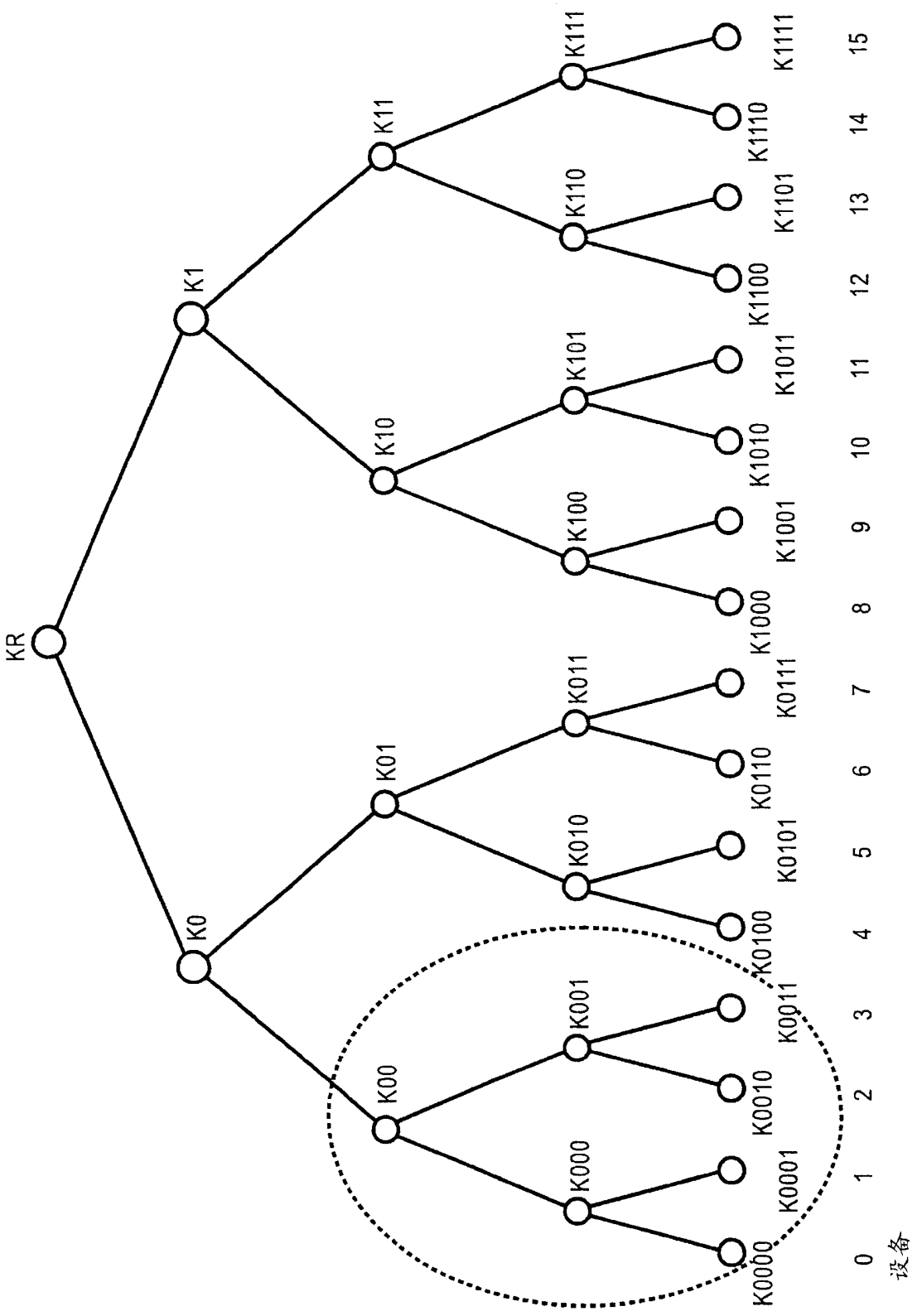

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
设备

图 10

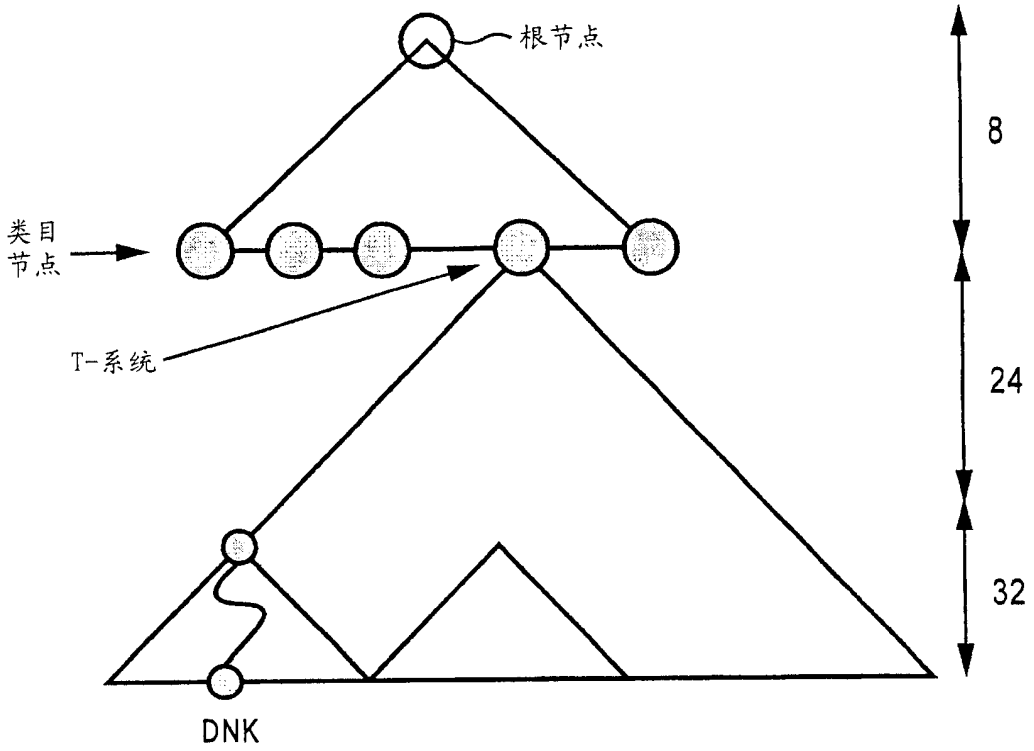


图 11

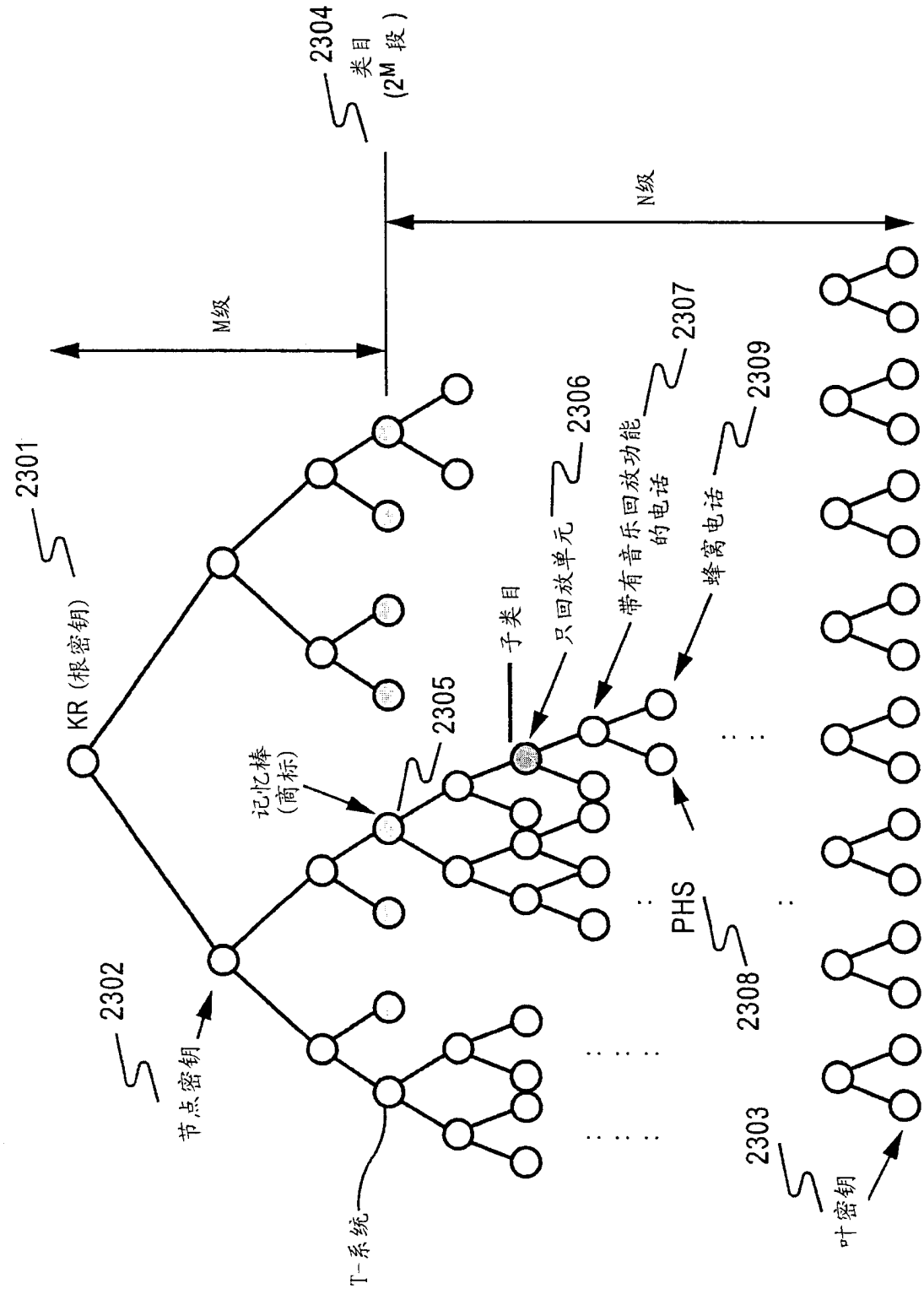

2304
类目
(2M 段)
M级
N级
2301
KR (根密钥)
2302
节点密钥
T-系统
记忆棒
(商标)
2305
子类目
只回放单元
2306
带有音乐回放功能
的电话
2307
蜂窝电话
2309
PHS
2308
2303
叶密钥

图 12

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 13

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 14

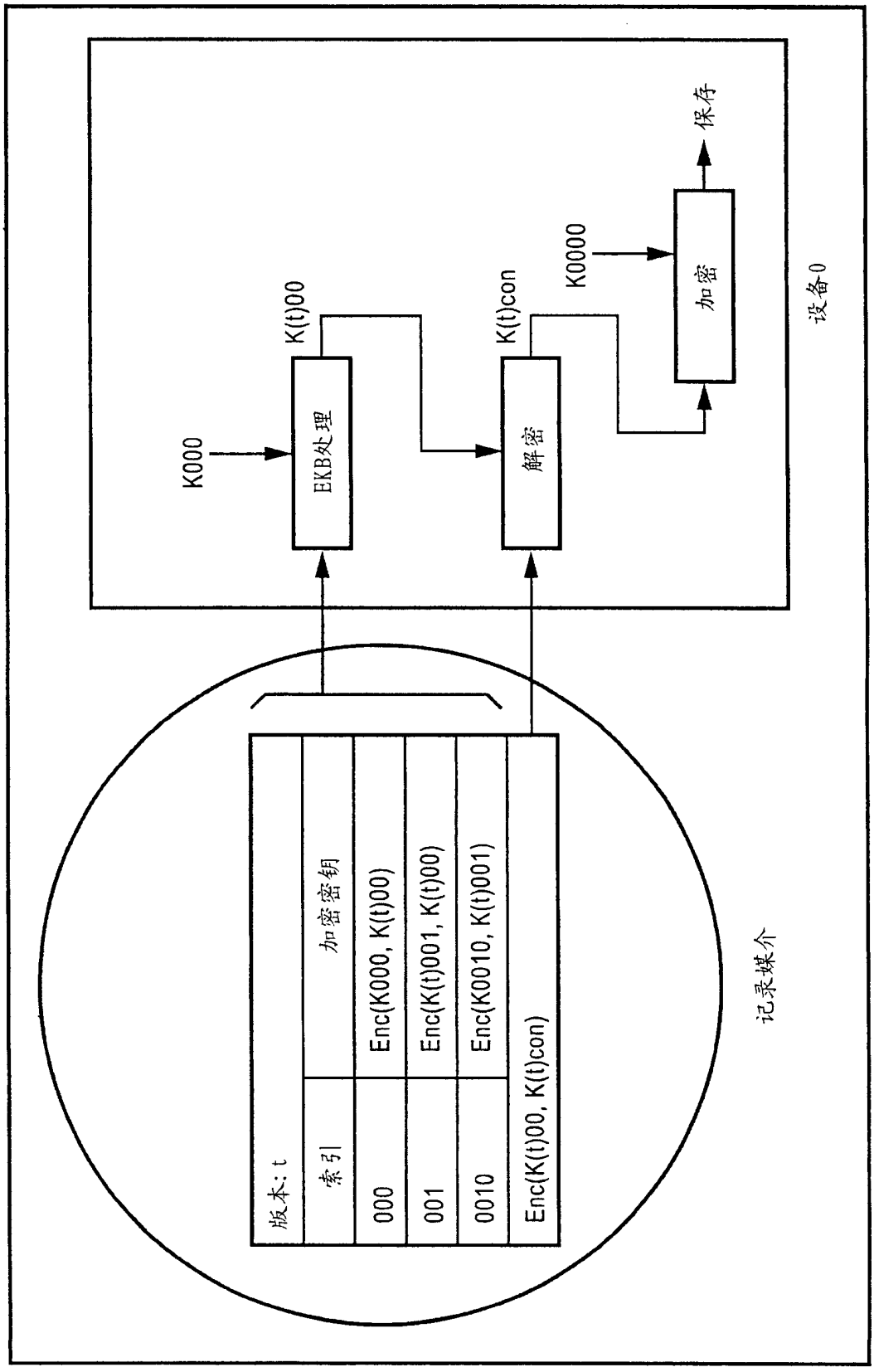

K000
EKB处理
K(t)00
解密
K(t)con
K0000
加密
保存
设备0
记录媒介
版本: t
索引
加密密钥
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)

图 15

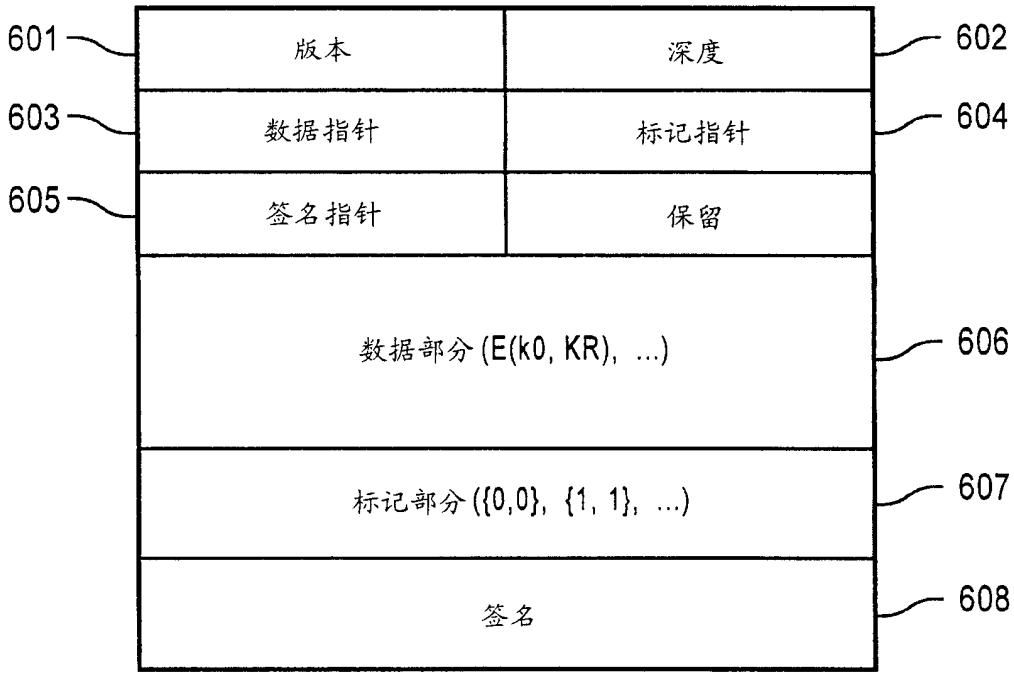

601
版本
深度
602
603
数据指针
标记指针
604
605
签名指针
保留
数据部分 (E(k0, KR), ...)
606
标记部分 ({0,0}, {1, 1}, ...)
607
签名
608

图 16

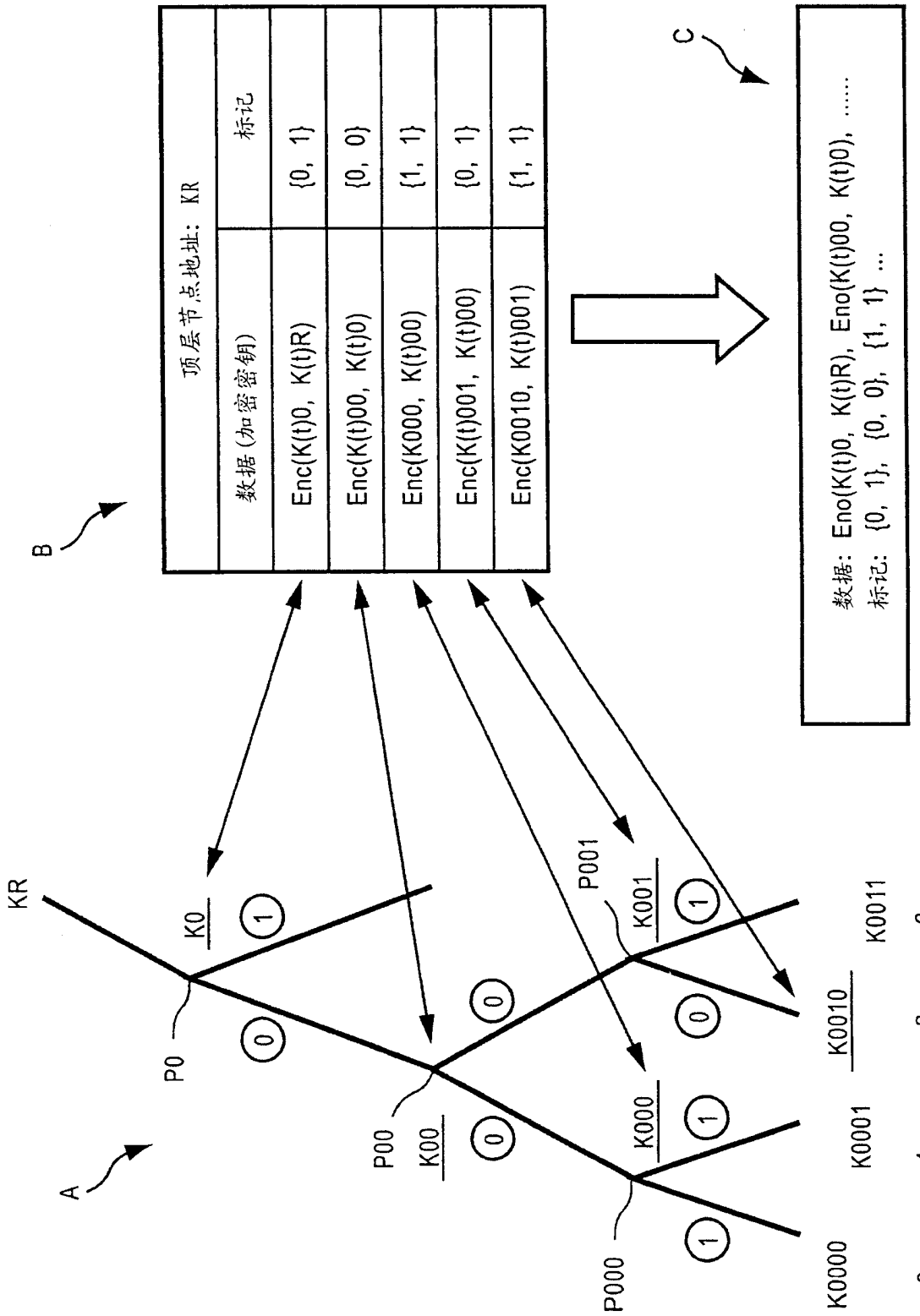

顶层节点地址: KR
数据(加密密钥)
标记
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
B
C
数据: Eno(K(t)0, K(t)R), Eno(K(t)00, K(t)0), ...
标记: {0, 1}, {0, 0}, {1, 1} ...
A
KR
K0
P0
K00
P00
K000
P000
P001
K001
K0010
K0011
K0001
K0000
0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

图 17

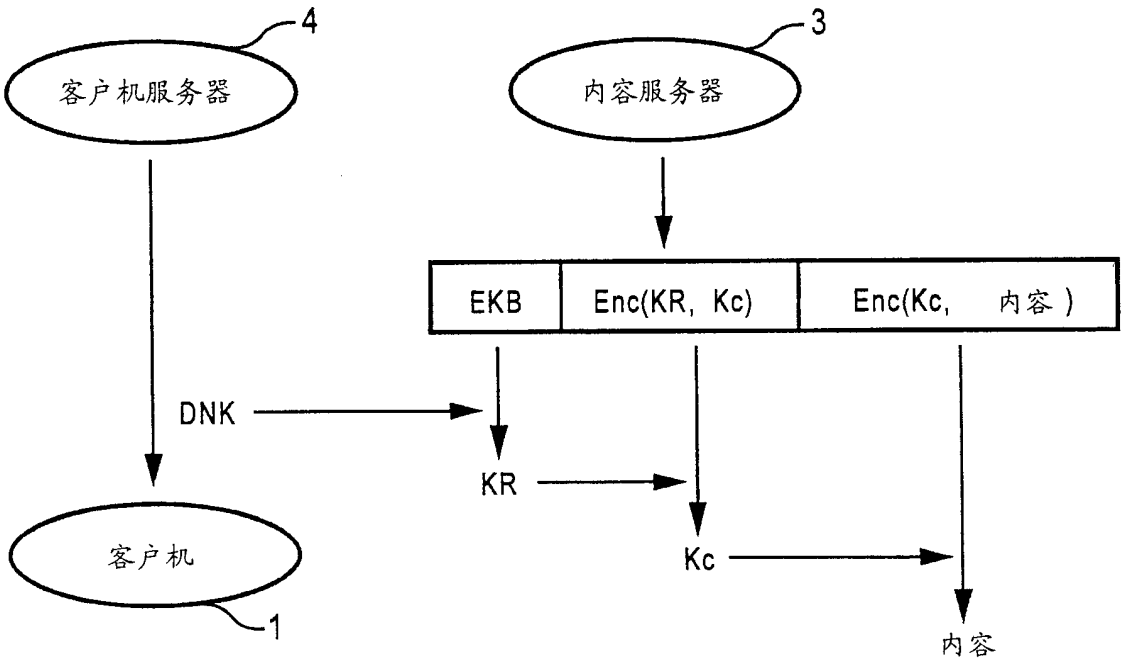

4
客户机服务器
3
内容服务器
EKB
Enc(KR, Kc)
Enc(Kc, 内容)
DNK
KR
Kc
客户机
1
内容

图 18

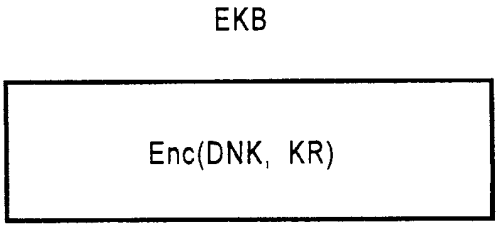

EKB
Enc(DNK, KR)

图 19

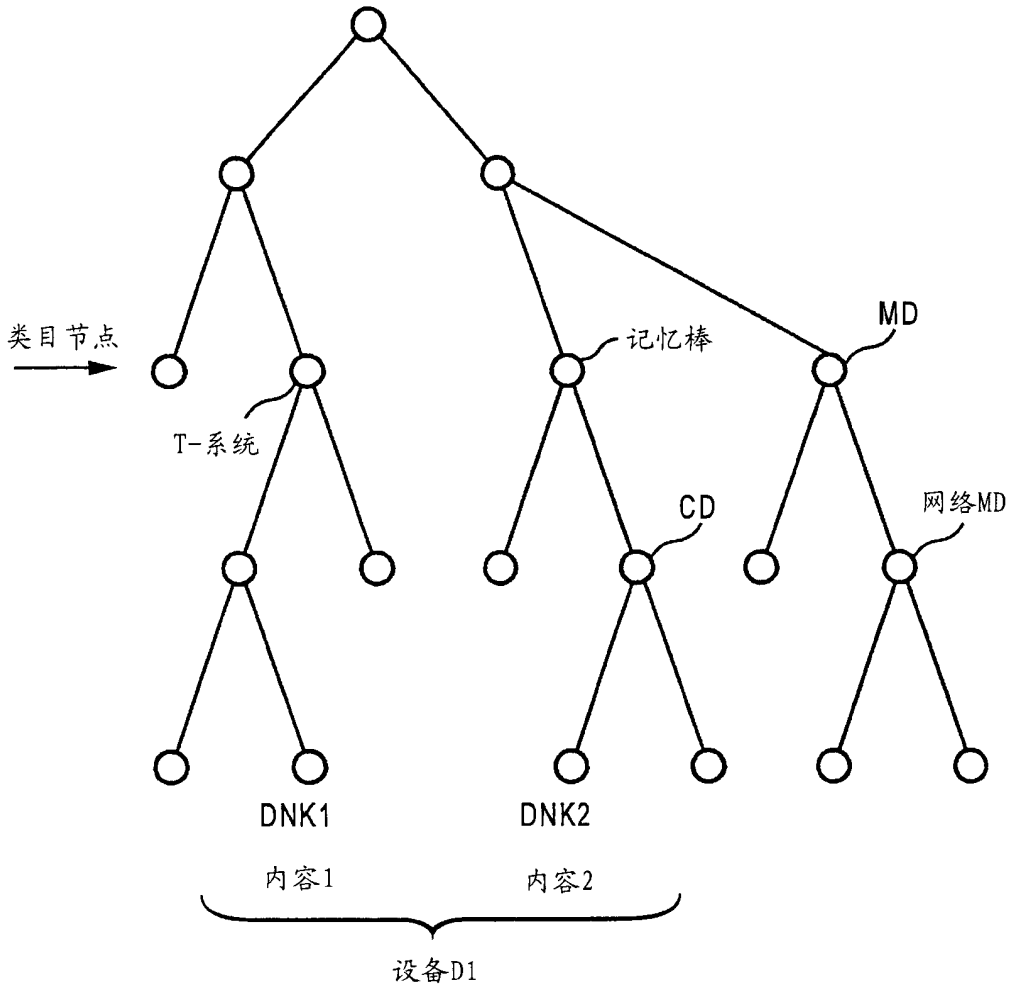


图 20

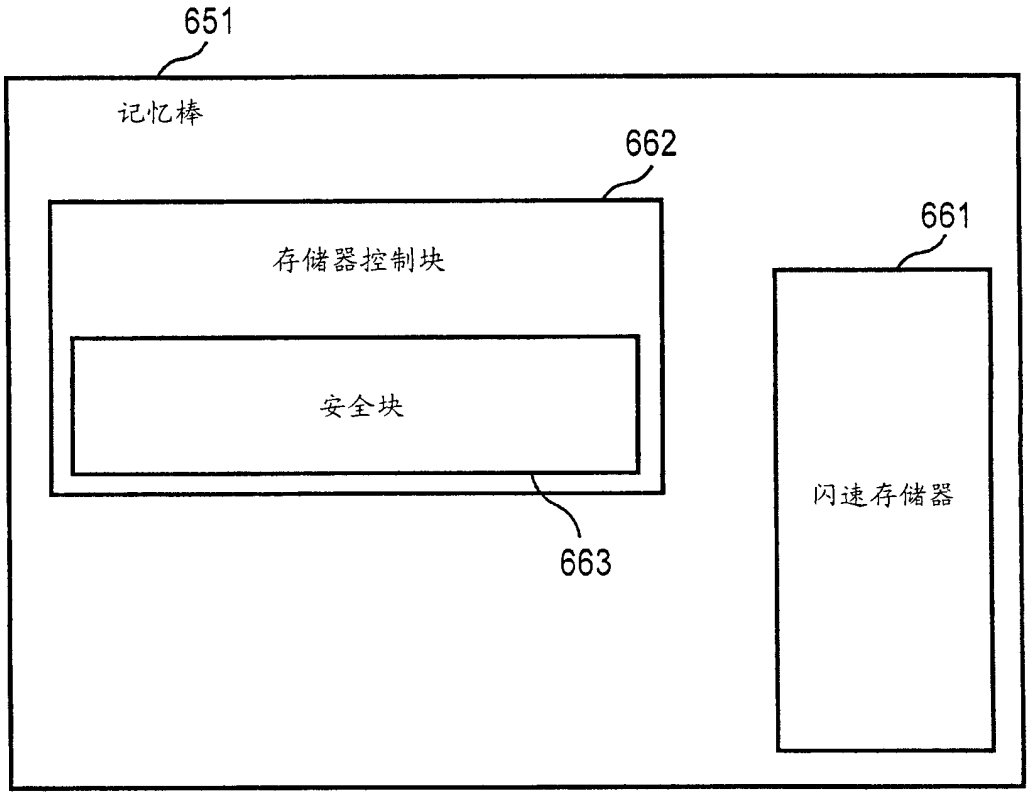


图 21

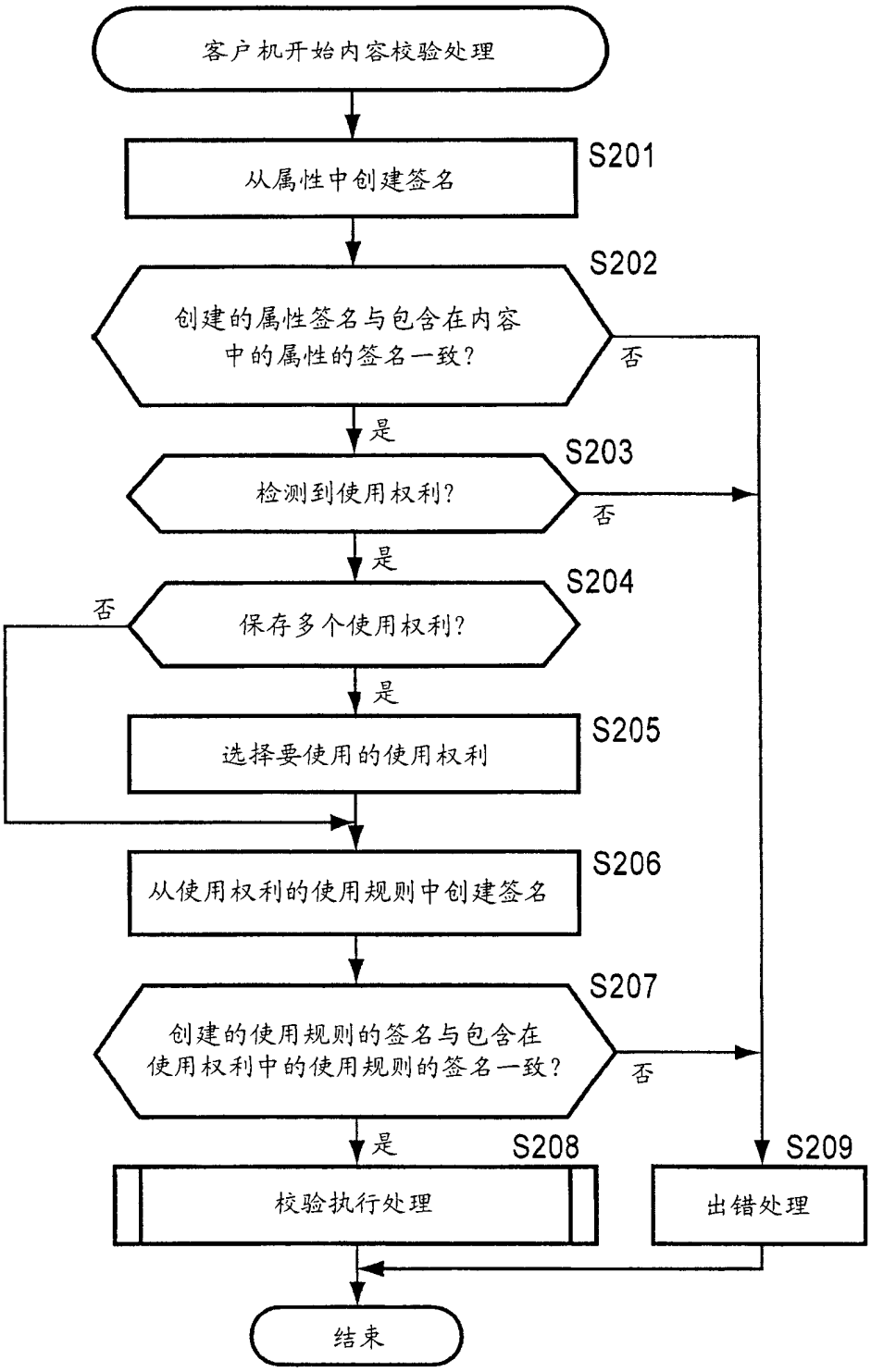

客户机开始内容校验处理
从属性中创建签名
S201
创建的属性签名与包含在内容中的属性的签名一致?
S202
否
是
检测到使用权利?
S203
否
是
保存多个使用权利?
S204
否
是
选择要使用的使用权利
S205
从使用权利的使用规则中创建签名
S206
创建的使用规则的签名与包含在使用权利中的使用规则的签名一致?
S207
否
是
校验执行处理
S208
出错处理
S209
结束

图 22

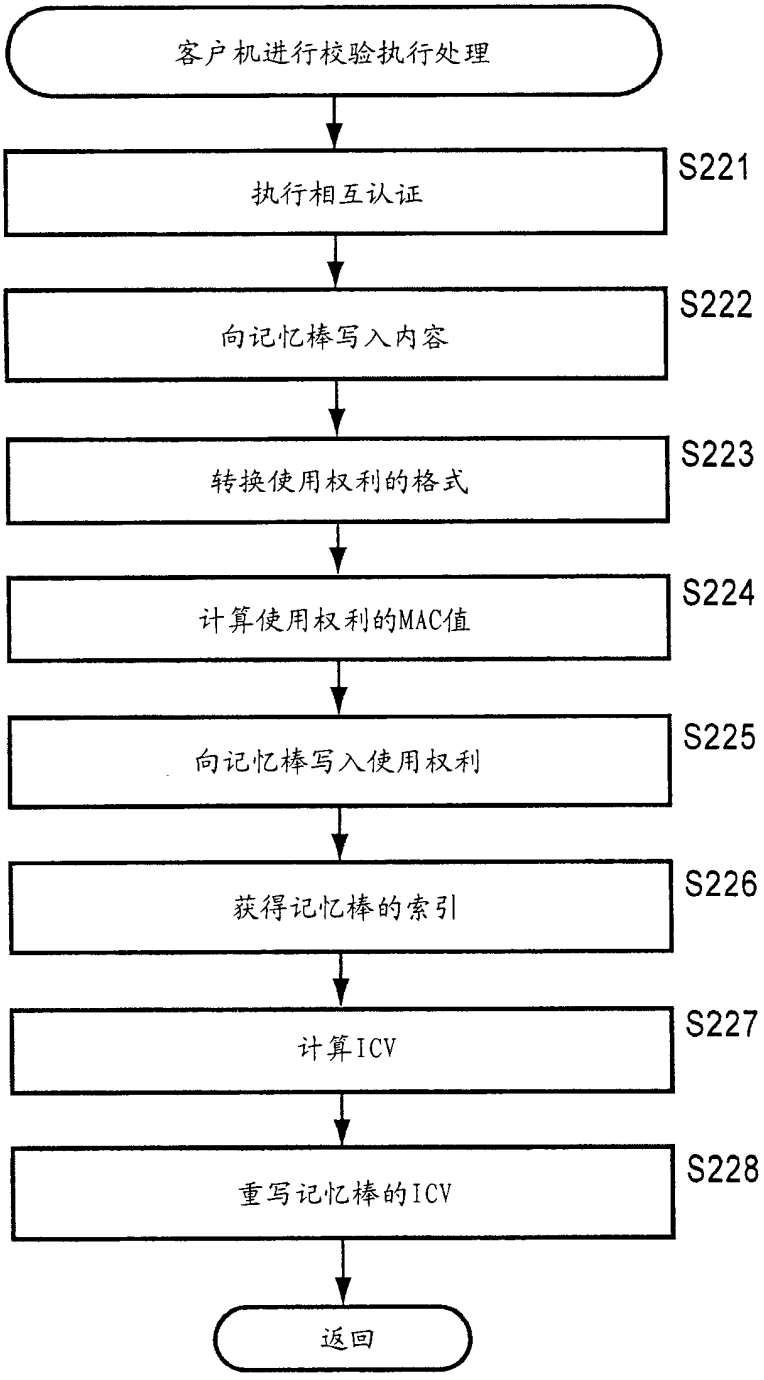

客户机进行校验执行处理
执行相互认证
S221
向记忆棒写入内容
S222
转换使用权利的格式
S223
计算使用权利的MAC值
S224
向记忆棒写入使用权利
S225
获得记忆棒的索引
S226
计算ICV
S227
重写记忆棒的ICV
S228
返回

图 23

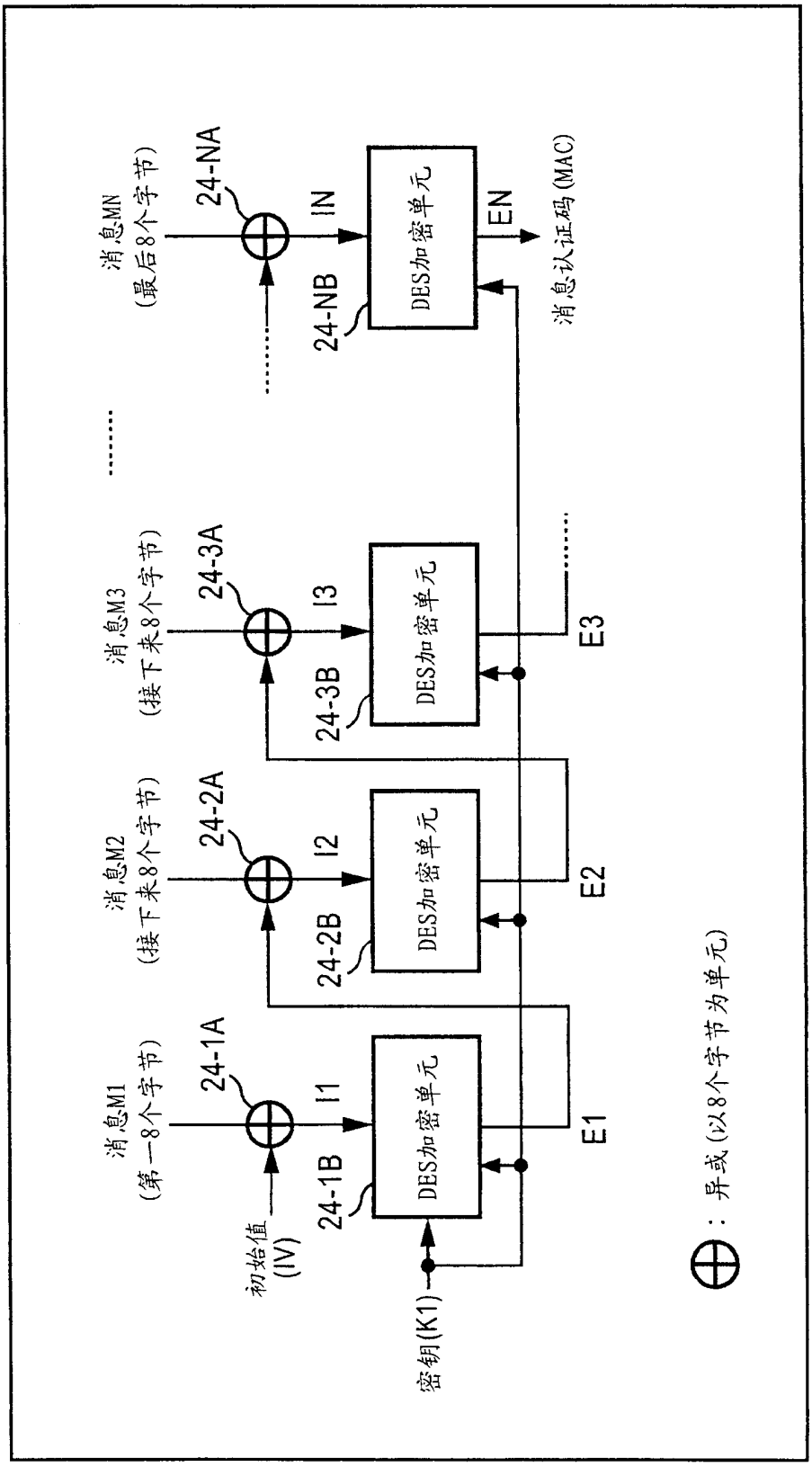

消息M1
(第一8个字节)
消息M2
(接下来8个字节)
消息M3
(接下来8个字节)
消息MN
(最后8个字节)
24-1A
24-2A
24-3A
24-NA
I1
I2
I3
IN
24-1B
24-2B
24-3B
24-NB
DES加密单元
DES加密单元
DES加密单元
DES加密单元
E1
E2
E3
EN
初始值
(IV)
密钥(K1)
消息认证码(MAC)
⊕：异或(以8个字节为单元)

图 24

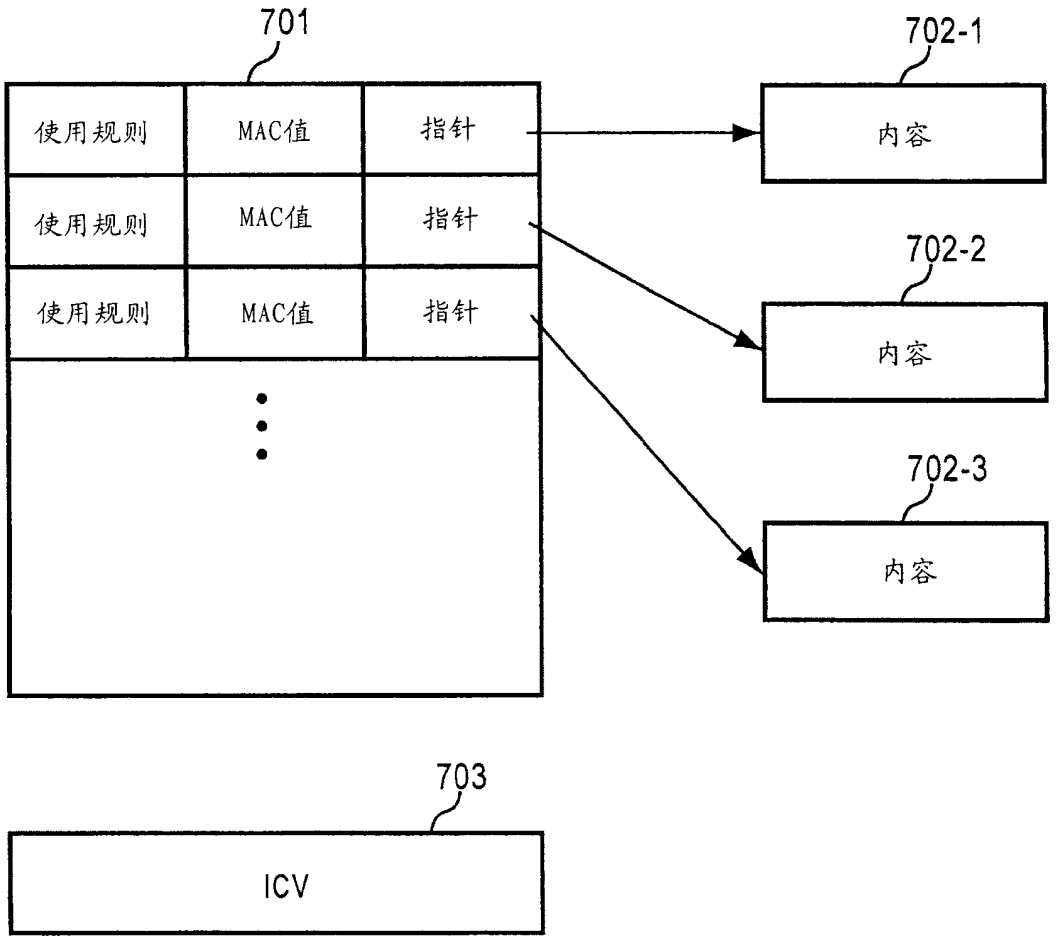

701
使用规则
MAC值
指针
使用规则
MAC值
指针
使用规则
MAC值
指针
702-1
内容
702-2
内容
702-3
内容
703
ICV

图 25

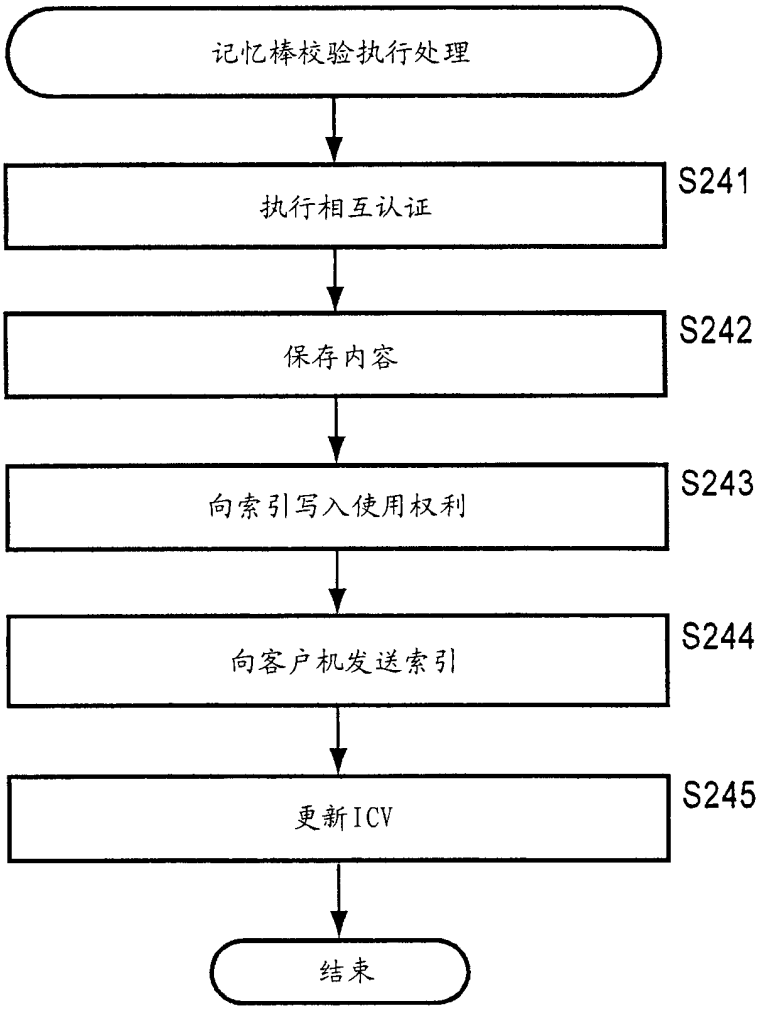

记忆棒校验执行处理
执行相互认证
S241
保存内容
S242
向索引写入使用权利
S243
向客户机发送索引
S244
更新ICV
S245
结束

图 26