[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G11B 20/10 (2006.01)
H04L 9/08 (2006.01)

[12] 发明专利说明书

专利号 ZL 03801866.7

[45] 授权公告日 2008 年 8 月 6 日

[11] 授权公告号 CN 100409204C

[22] 申请日 2003.9.11 [21] 申请号 03801866.7

[30] 优先权

[32] 2002. 9.11 [33] JP [31] 265417/2002

[86] 国际申请 PCT/JP2003/011616 2003.9.11

[87] 国际公布 WO2004/025482 日 2004.3.25

[85] 进入国家阶段日期 2004.6.28

[73] 专利权人 索尼株式会社

地址 日本东京都

[72] 发明人 永井规浩 栗原章 北谷义道
大泽义知 浦野直美 盛田昌夫
福井俊治

[56] 参考文献

JP2001176192A 2001.6.29

JP2001250322A 2001.9.14

JP2000293439A 2000.10.20

JP2001358707A 2001.12.26

JP200250122A 2002.2.15

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 黄小临 王志森

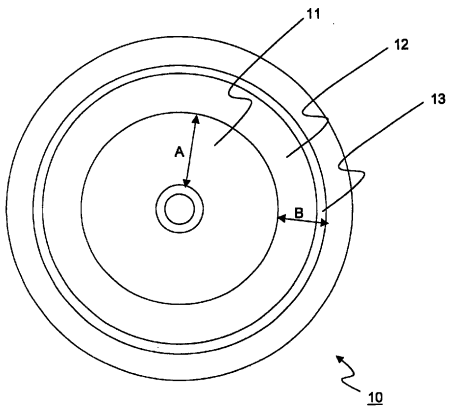
权利要求书 3 页 说明书 30 页 附图 28 页

[54] 发明名称

信息记录媒体、信息处理装置、信息处理方法

[57] 摘要

提供一种信息记录媒体、一种信息处理设备和一种信息处理方法，其能够使用内容，同时在 CD 播放器和信息处理设备如 PC 中都保护版权。 该信息记录媒体包含：第一数据存储区域，它已经经过复制防止处理；第二数据存储区域，包含加密内容文件，该加密内容文件包括通过加密用于解码的密钥数据已经得到的、并仅能通过具有许可的设备解密的、加密的密钥数据和加密的内容。 在重现设备如 CD 播放器中，可以执行记录于第一数据记录域的内容的重现；并且如果能够获得许可，在信息处理设备如 PC 中，可以执行记录于第二数据记录域的加密的内容的解密/重现。



1. 一种信息记录媒体，其上存储内容数据，所述信息记录媒体包含:

第一数据存储区域，它设置为其上执行复制防止过程的内容存储区域;和

第二数据存储区域，它是这样的内容存储区域：其上不执行复制防止过程，并且其中存储包含加密的内容和加密的内容文件的加密的密钥数据，使得在解密加密的内容的过程中使用的密钥数据被加密，并且它仅能在具有许可的设备中解密。

2. 根据权利要求 1 所述的信息记录媒体，其中存储于所述第二数据存储区域的加密的内容文件中的加密的内容是

利用作为加密处理密钥的内容密钥 Kc 加密的内容，并且所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据，解密使能密钥块(EKB)的过程。

3. 根据权利要求 1 所述的信息记录媒体，其中存储于所述第二数据存储区域的数据包含

执行从信息记录媒体读取获得许可必需的识别信息的程序。

4. 根据权利要求 1 所述的信息记录媒体，其中所述第二数据存储区域以这样的方式构造:

存储标识符数据(PID)，它包含：媒体 ID，用作对信息记录媒体唯一的标识符；和 MAC，作为变化验证数据。

5. 根据权利要求 4 所述的信息记录媒体，其中所述第二数据存储区域以这样的方式构造:

存储用作标识符的产品 ID，它为对应于多个信息记录媒体的集合的每个产品设置，并且所述媒体 ID 和产品 ID 的结合数据构造为全局唯一标识符。

6. 根据权利要求 1 所述的信息记录媒体，其中存储于所述第二数据存储区域的内容文件包含

用内容密钥[Kc]加密的内容数据(Enc (Kc, 内容))，用根密钥[Kroot]加密的内容密钥数据(Enc (Kroot, Kc))和使能密钥块(EKB)，其中，通过使用作为许可数据存储于服务数据中的设备节点密钥(DNK)的解密过程，从该使能密钥块(EKB) 能得到根密钥[Kroot]。

7. 根据权利要求 1 所述的信息记录媒体，其中所述第一数据存储区域和所述第二数据存储区域各自具有设置为独立的会话区域的多会话结构，该会话区域由指示数据开始区域的引入区域、内容存储区域和指示数据结束区域的引出区域构成。

8. 一种作为播放信息记录媒体的存储内容的过程的条件而执行许可获得过程的信息处理装置，所述信息处理装置包含:

用于执行这样的过程的配置，该过程用于：从其上存储有加密的内容数据的信息记录媒体获得标识符数据(PID)，该标识符数据包含媒体 ID 作为对信息记录媒体唯一的标识符和作为变化验证数据的 MAC；并获得产品 ID 作为为对应于多个信息记录媒体的集合的每个产品而设置的标识符；并且作为许可获得数据传送得到的 PID 和产品 ID 到各许可提供系统部件实体。

9. 根据权利要求 8 所述的信息处理装置，其中所述加密的内容是利用作为加密处理密钥的内容密钥 Kc 加密的内容，并且所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程，并且，

所述信息处理装置从所述许可提供系统部件实体接收服务数据和使用权信息作为许可数据，根据许可数据的存储数据执行用于所述使能密钥块(EKB)的过程，并且执行用于解密存储于所述信息记录媒体的加密的内容数据的过程。

10. 一种作为播放信息记录媒体的存储内容的过程的条件而执行许可获得过程的信息处理方法，所述信息处理方法包含:

ID 读取步骤，从其上存储有加密的内容数据的信息记录媒体读取标识符数据(PID)，该标识符数据包含媒体 ID 作为对信息记录媒体唯一的标识符和作为变化验证数据的 MAC；并读取产品 ID 作为为对应于多个信息记录媒体的集合的每个产品而设置的标识符；和

ID 传送步骤，将在所述 ID 读取步骤获得的 PID 和产品 ID 作为许可获得数据传送到各许可提供系统部件实体。

11. 根据权利要求 10 所述的信息处理方法，其中所述加密的内容是利用作为加密处理密钥的内容密钥 Kc 加密的内容，所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程，所述信息处理方法还包含:

接收步骤，从所述许可提供系统部件实体接收服务数据和使用权信息作为许可数据；和

执行步骤，根据所述许可数据的存储数据，执行用于所述使能密钥块(EKB)的过程并执行解密存储于所述信息记录媒体的加密的内容数据的过程。

信息记录媒体、信息处理装置、信息处理方法

技术领域

本发明涉及信息记录媒体、信息处理装置、信息处理方法和计算机程序。特别是，本发明涉及信息记录媒体、信息处理装置、信息处理方法和计算机程序，其中在内容记录媒体如 CD 中设置第一数据记录域作为具有可保护版权的防止复制或剥离（ripping）功能的内容记录域，以及其中记录有加密的内容的第二数据记录域，从而使第一数据记录域的记录内容能够在 CD 播放器上播放；并且其中，在能够执行复制和剥离处理的信息处理设备如 PC 中，可能在得到许可的条件下，解密和播放第二数据记录域的加密的内容。

背景技术

近年，各种软件数据（以下称为“内容”），如音频数据如音乐、图象数据如电影、游戏程序和各种应用程序，已经通过网络如因特网或通过记录媒体如 DVD 和 CD 分配。通过在用户拥有的 PC（个人计算机）、CD 播放器、DVD 播放器等中播放，使用这些分配的内容。

对于大多数内容，例如音乐数据、图象数据等，一般而言，分配权由其创建者或其销售者拥有。因此，除了例外的免费分配的内容，为播放或使用常规内容，得到授权的内容使用权是必要的。例如，在 CD 的情况，通过支付与 CD 相当的价钱购买 CD 是在播放器中播放的条件。

进而，要用 PC、通信终端等通过网络如因特网接收内容时，在通过输入用户信息，如用户的信用号码，向内容提供者支付与内容使用相当的价钱的条件下，内容从提供者提供。

但是，即使在提供内容时执行这样的价钱支付过程，如果得到内容的用户从例如 CD 录制如另一记录媒体（所谓的复制），或者如果允许所谓的剥离过程，非法复制的数据也将传播，在该剥离过程中，在 PC 等中，内容从 CD 等读取作为数字数据并作为文件存储到计算机中。

在 PC 等中剥离是数字地复制数据的过程，并且保持原始数据的质量。当剥离的数据写入另一个 CD-R 时，创造出与原始 CD 具有完全相同质量的

内容 CD。进而，记录剥离的数据为压缩的 MP3 数据等，或通过网络传送剥离的数据也变为可能。

如上所述，从版权保护的观点，下面的情形是不希望的：其中，在内容暂时交给用户之后，有版权的内容被非法复制或改变，然后被分配。

作为防止这样的情形的版权保护技术，已经开发出配备复制控制功能的信息记录媒体（例如，具有复制防止功能 CD）。复制防止功能的例子包括由 Midbar Technologies Ltd.开发的复制控制技术和由 US Macrovision Corporation 开发的复制控制技术。

上面具有这样的配置：其中，例如作为在 CD 的第一轨道内记录伪信号（peudo-signal）的结果，当 CD 放入 PC 的 CD-ROM 驱动器时，PC 不将它识别为音乐 CD，使其不可能利用 PC 的 CD 播放器程序执行播放过程。不能执行剥离过程的一般的 CD 播放器，可以通过忽略伪信号执行只有内容数据的播放。

以上述方式，如果企图播放记录了复制控制内容的信息记录媒体如 CD，如上所述，在只播放的 CD 播放器，播放是可能的，但在 PC 等中，播放是不可能的。虽然这提供了消除非法过程如复制或剥离的好处，但对没有执行非法复制或剥离意图的、授权的内容使用用户是不便的。

发明内容

鉴于上述问题，已经做出本发明。本发明的目标是提供一种信息记录媒体、信息处理装置、信息处理方法和计算机程序，其中，在其上记录了具有复制防止功能的内容的内容记录媒体如 CD 中，提供加密的内容记录域，使得即使在信息处理设备如 PC 中，作为得到预定的许可的结果，通过解密记录于加密的内容记录域的加密的内容，也使内容的播放和使用成为可能。

特别地，本发明提供一种信息记录媒体、信息处理装置、信息处理方法和计算机程序，其中，在内容记录媒体如 CD 中设置：第一数据记录域，用作其上执行可保护版权的复制防止过程的内容存储区域；和第二数据记录域，用作其上不执行复制防止过程并且其中记录有加密的内容的内容存储区域，因此，使第一数据记录域的记录的内容能够在播放设备如 CD 播放器中播放，并且即使在能够执行复制和剥离处理的信息处理设备如 PC 中，在得到许可的条件下，解密和播放第二数据记录域的加密的内容也是可能的。

本发明的第一方面是关于一种其上存储内容数据的信息记录媒体，该信息记录媒体包括:

第一数据存储区域，它设置为其上执行复制防止过程的内容存储区域;和

第二数据存储区域，它是这样的内容存储区域：其上不执行复制防止过程，并且其中存储包含加密的内容和加密的内容文件的加密的密钥数据，使得在解密加密的内容的过程中使用的密钥数据被加密，并且它仅能在具有许可的设备中解密。

在本发明的信息记录媒体的一种形式中，存储于所述第二数据存储区域的加密的内容文件中的加密的内容是利用作为加密处理密钥的内容密钥 Kc 加密的内容，并且所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据，解密使能密钥块(EKB)的过程。

在本发明的信息记录媒体的一种形式中，存储于所述第二数据存储区域的数据包含用于执行读取识别信息的过程的程序，该识别信息是从信息记录媒体获得许必需的。

在本发明的信息记录媒体的一种形式中，所述第二数据存储区域以这样的方式构造：存储标识符数据(PID)，它包含：媒体 ID，用作对信息记录媒体唯一的标识符；和 MAC，作为变化验证数据。

在本发明的信息记录媒体的一种形式中，所述第二数据存储区域以这样的方式构造：存储用作标识符的产品 ID，它为对应于多个信息记录媒体的集合的每个产品设置，并且所述媒体 ID 和产品 ID 的结合数据构造为全局唯一标识符。

在本发明的信息记录媒体的一种形式中，存储于所述第二数据存储区域的内容文件包含：用内容密钥[Kc]加密的内容数据(Enc (Kc, 内容))，用根密钥[Kroot]加密的内容密钥数据(Enc (Kroot, Kc))和使能密钥块(EKB)，其中，通过使用作为许可数据存储于服务数据中的设备节点密钥(DNK)的解密过程，从该使能密钥块(EKB) 能得到根密钥[Kroot]。

在本发明的信息记录媒体的一种形式中，所述第一数据存储区域和所述第二数据存储区域各自具有设置为独立的会话区域的多会话结构，该会话区域由指示数据开始区域的引入区域、内容存储区域和指示数据结束区域的引

出区域构成。

本发明的第二方面是关于一种作为播放信息记录媒体的存储内容的过程的条件而执行许可获得过程的信息处理装置，所述信息处理装置包含:

用于执行这样的过程的配置，该过程用于：从其上存储有加密的内容数据的信息记录媒体获得标识符数据(PID)，该标识符数据包含媒体 ID 作为对信息记录媒体唯一的标识符和作为变化验证数据的 MAC；并获得产品 ID 作为为对应于多个信息记录媒体的集合的每个产品而设置的标识符；并且作为许可获得数据传送得到的 PID 和产品 ID 到各许可提供系统部件实体。

在本发明的信息处理装置的一种形式中，所述加密的内容是利用作为加密处理密钥的内容密钥 Kc 加密的内容，并且所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程，并且，所述信息处理装置从所述许可提供系统部件实体接收服务数据和使用权信息作为许可数据，根据许可数据的存储数据执行用于所述使能密钥块(EKB)的过程，并且执行用于解密存储于所述信息记录媒体的加密的内容数据的过程。

本发明的第三方面是关于一种作为播放信息记录媒体的存储内容的过程的条件而执行许可获得过程的信息处理方法，所述信息处理方法包含:

ID 读取步骤，从其上存储有加密的内容数据的信息记录媒体读取标识符数据(PID)，该标识符数据包含媒体 ID 作为对信息记录媒体唯一的标识符和作为变化验证数据的 MAC；并读取产品 ID 作为为对应于多个信息记录媒体的集合的每个产品而设置的标识符；和

ID 传送步骤，将在所述 ID 读取步骤获得的 PID 和产品 ID 作为许可获得数据传送到各许可提供系统部件实体。

在本发明的信息处理方法的一种形式中，所述加密的内容是利用作为加密处理密钥的内容密钥 Kc 加密的内容，并且所述内容密钥 Kc 设置为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程。所述信息处理方法还包含：接收步骤，从所述许可提供系统部件实体接收服务数据和使用权信息作为许可数据；和执行步骤，根据所述许可数据的存储数据，执行用于所述使能密钥块(EKB)的过程并执行解密存储于所述信息记录媒体的加密的内容数据的过程。

根据本发明的配置，在信息记录媒体如 CD 中，设置第一数据存储区域

和第二数据存储区域作为不同的会话区域，第一数据存储区域设置为执行复制防止过程的内容存储区域；第二数据存储区域是这样的内容存储区域：其上不执行复制防止过程，并且其中存储包含加密的内容和加密的密钥数据的加密的内容文件，使得对在解密加密的内容的过程中使用的密钥数据加密，并且它仅能在具有许可的设备中解密。因此，在播放设备如 CD 播放器中，播放第一数据记录域的记录的内容是可能的；并且甚至在能够进行复制和剥离处理的信息处理设备如 PC 中，在得到许可的条件下，解密或播放第二数据记录域的加密的内容也是可能的。

根据本发明的配置，存储于第二数据存储区域的加密的内容文件中的加密的内容是这样的内容：它使用用作加密处理密钥的内容密钥 Kc 加密，并且设置内容密钥 Kc 为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程。因此，在严格的许可管理下，内容使用的管理变为可能。

根据本发明的配置，标识符数据(PID)存储于第二数据存储区域，该标识符数据包含：媒体 ID，用作对信息记录媒体唯一的标识符；和 MAC，用作变化验证数据，所以，当发行许可时，执行使用 MAC 验证的变化验证。因此，可能消除得到非法的许可的可能性。

根据本发明的配置，用作标识符的产品 ID 存储于第二数据存储区域，该产品 ID 为对应于多个信息记录媒体的集合的每个产品设置；并且媒体 ID 和产品 ID 的结合数据设置为全局唯一标识符。因此，可能可靠和有效地执行许可发行管理。

本发明的计算机程序是这样的计算机程序：它被提供给，例如能够执行

各种程序代码的通用计算机系统，这样的计算机程序通过以计算机可读形式提供的存储媒体和通信媒体提供，例如，存储媒体如 CD、FD 和 MO，通信媒体如网络。通过以计算机可读的形式提供这样的程序，在计算机系统上实现对应于程序的过程。

从参考附图的本发明的实施例（随后要描述），本发明更进一步的目的、特征和好处将变得明显。在本说明书中，系统指多个设备的逻辑的集合，并且在同一框架内布置设备不是必需的。

附图说明

图 1 显示信息记录媒体的结构，该信息记录媒体具有执行复制防止过程的第一数据存储区域和不执行复制防止过程第二数据存储区域。

图 2 显示 PID 数据的数据格式的例子。

图 3 显示 MAC 值产生过程的例子。

图 4 显示第二数据存储区域的目录结构的例子。

图 5 显示在内容使用和播放过程中执行许可获得过程的系统的例子。

图 6 显示信息处理装置和服务器的配置的例子。

图 7 是说明加密和分配各种密钥和数据的过程的树结构的视图。

图 8 显示用于分配各种密钥和数据的使能密钥块(EKB)的例子。

图 9 显示使用内容密钥的使能密钥块(EKB)的分配的例子和解密过程的例子。

图 10 显示使能密钥块(EKB)的格式的例子。

图 11 说明使能密钥块(EKB)的标记的结构。

图 12 说明在一个树结构中的种类划分。

图 13 说明在该树结构中的种类划分。

图 14 说明在该树结构中的种类划分的具体例子。

图 15 显示在许可获得过程中实体之间的处理顺序(No.1)。

图 16 显示专辑主表的结构的例子。

图 17 显示交易表(transaction table)的结构的例子。

图 18 显示盘表和专辑价格主表的例子。

图 19 显示在许可获得过程中实体之间的处理顺序(No.2)。

图 20 显示轨道表(track table)的结构的例子。

图 21 是说明在许可获得过程中、在许可提供侧的处理的流程图。

图 22 显示在许可获得过程中实体之间的处理顺序(No.3)。

图 23 显示在许可获得过程中呈现给客户的购买页面的例子。

图 24 显示在许可获得过程中提供给客户的启动文件的例子。

图 25 显示服务数据和使用权信息的数据结构的例子。

图 26 显示在许可获得过程中实体之间的处理顺序(No.4)。

图 27 说明内容播放过程的总览。

图 28 说明使用使能密钥块(EKB)的内容解密和使用过程的例子。

具体实施方式

现在下面将详细描述本发明的配置。根据下述的每一项给出描述。

1.信息记录媒体的内容记录结构

2.系统配置

3.作为密钥分配结构的树结构

4.使用 EKB 的密钥的分配

5. EKB 的格式

6.树的目录分类

7.许可购买和内容播放过程

[1.信息记录媒体的内容记录结构]

首先，将参考图 1 给出根据本发明的信息记录媒体的内容记录结构的描述。图 1 显示信息记录媒体 10 如 CD、DVD 等的平面图。信息记录媒体的数据记录域分为两个区域。

在盘形的信息记录媒体 10 的内部区域(A)中，设置可保护版权的内容数据记录域、即第一数据记录域（recording field）（第一会话（session））11 为具有复制和剥离防止功能的内容记录域。进而，在信息记录媒体 10 的外部区域(B)中，设置其中记录加密的内容的第二数据记录域（第二会话）12。

即，信息记录媒体 10 是这样的信息记录媒体：其中设置第一数据记录域（第一会话）11，用作其上执行复制防止过程的内容存储区域；和第二数据记录域（第二会话）12，它是其上不执行复制防止过程并且其中存储加密的内容文件的内容存储区域，该加密的内容文件包含加密的内容和加密的密钥数据，使得加密用于加密内容的解密过程的密钥数据，并且对于其仅在具有

许可的设备中解密过程是可能的。

一个会话（session）是一个单元区域，该单元区域包含：引入（lead-in）区域，它由指示数据开始区域的数据区域（例如静数据（silence data））构成；内容存储区域；和引出（lead-out）区域，它指示数据结束区域。图 1 中所示的信息记录媒体 10 是具有多会话结构的记录媒体，其上记录了两个会话。

第一数据记录域 11 的记录内容被记录为经过复制防止过程的内容。例如，该配置是这样使得：当其第一轨道记录伪信号的 CD 放入 PC 的 CD-ROM 驱动器时，PC 不将它识别为音乐 CD，所以不执行使用 PC 的音乐 CD 播放处理程序的播放过程。作为复制防止功能，例如，可以使用各种复制防止功能，如由 Midbar Technology Ltd.开发的复制控制技术和由 US Mcrovision Corporation 开发的复制控制技术。

设置第一数据记录域 11 的记录内容为这样的内容记录域：其中防止剥离过程和复制过程，通过这些过程，从装入例如 PC 的 CD 驱动器的 CD，作为数字数据读取记录的内容，并在另一个记录媒体中存储，或者使得记录的内容转换为压缩的 MP3 数据。

第一数据记录域 11 的记录内容可以在具有播放功能作为专用功能的如一般的 CD 播放器的播放处理设备（播放器）播放。也就是，即使伪信号记录在第一轨道内，没有复制处理和剥离处理程序并且仅能执行 CD 播放的 CD 播放器，也能够通过忽略伪信号播放内容数据。

另一方面，第二数据记录域 12 的记录内容是加密内容。可以通过执行解密过程播放该加密内容。执行解密过程的密钥数据可以通过获得内容使用权（许可）得到。虽然随后将更详细地描述这一点，通过执行这样的过程，内容解密变为可能，该过程包括使用密钥分配树结构分配的密钥数据解密使能数据块（EKB）的过程。

因此，仅当拥有合法(valid)的许可时才可以使用第二数据记录域 12 的记录内容。甚至在不能播放第一数据记录域 11 的记录内容的 PC 中，通过接收合法的许可，播放和使用第二数据记录域 12 的记录内容也变得可能。

在第二数据记录域 12 的部分提供 PID (Postscribed-ID)记录区域（recording area）13。PID 是包含媒体 ID 和版本信息的数据，其中媒体 ID 在预定的如标题单元、专辑(album)单元和制造签(manufacturing lot)单元的盘簇单元中，作为对每个盘的唯一标识符(ID)给出，并且向媒体 ID 添加 MAC

作为数据变化验证码。

图 2 显示 PID 的数据结构的例子。PID 具有的配置包含：指示 PID 的格式版本的格式版本 21，PID 保留域 22 和作为每个盘的唯一识别数据的媒体 ID 23，其中作为变化验证码的 MAC 24 添加到该数据。

作为验证数据的变化的数据，产生消息鉴别码(MAC)。对 MAC 产生过程和验证过程，各种模式是可能的，但作为一个例子，图 3 中显示使用 DES 加密处理结构的 MAC 值产生例子。

给出使用图 3 的 DES 加密处理结构的 MAC 值产生例子的描述。要处理的消息分割为 8 字节单元（以下分割的消息称为 “M1, M2, ..., MN”）。首先，计算初始值（以下缩写为 “IV”）和 M1 的异或 OR（结果表示为 I1）。其次，I1 输入到 DES 加密部分，在那里使用密钥（以下称为 “K1”）对 I1 加密（以下输出称为 “E1”）。然后，计算 E1 和 M2 的异或 OR，其输出 I2 输入到 DES 加密部分，在那里使用密钥 K1 对 I2 加密（输出 E2）。此后，这被重复，使得对所有消息进行加密过程。最后的输出的 EN 变为消息鉴别码（MAC）。

当改变生成源数据时，MAC 值变为不同的值。由此，当根据要验证的数据（消息）产生的 MAC 与记录的 MAC 比较时，如果发生匹配，就证明要验证的数据（消息）没有被改变或变更。

图 4 中显示存储于第二数据记录域 12 的数据文件的目录结构例子。目录具有 CD 应用文件[MQDISK.EXE]，在装入 PC 的 CD 驱动器时它被自动执行；具有在更低级别（order）上的定义文件[MQDISK.INI]；并包含一个或多个加密的内容文件[MQT 文件]。

在定义文件[MQDISK.INI]中，存储了：产品 ID，它设置为预定的盘簇单元，如标题单元、专辑单元、目录单元和制造签单元中的标识符；设置为验证服务器的 PID 验证服务器的 URL 信息，在许可获得过程中，该验证服务器验证来自用户侧的传送数据作为播放和使用存储于第二数据记录域 12 的加密内容的权限；等等。

上述定义在 PID 中的媒体 ID 是这样的 ID，它对于一个产品 ID 设置为每个盘的不同的 ID，并且产品 ID 和媒体 ID 的结合基本上是全局唯一识别数据。

加密的内容文件[MQT 文件]拥有数据[Enc (Kc, Content)]，使得用内容密钥 Kc 加密内容。Enc (A, B)指示使得用 A 加密 B 的数据。

进而，加密的内容文件[MQT 文件] 拥有包含使能密钥块(EKB)的头信

息。使能密钥块(EKB)是可以用设备节点密钥(DNK)解密的加密数据，其被分配给合法的设备。通过得到许可作为授权的内容使用权，对用户解密使能密钥块(EKB)变为可能，使得加密的内容数据[Enc (Kc, Content)]可以使用内容密钥 Kc 解密，Kc 在 EKB 解密过程的基础上得到，并且内容因此可以播放和使用。随后将描述这些过程的细节。

当要播放记录于第二数据记录域的加密内容时，获得许可是必要的。为得到许可，想要执行播放过程的如 PC 的信息处理装置读取记录于第二数据记录域的产品 ID 和 PID（见图 2），并传送它们到由定义文件[MQDISK.INI]中描述的 URL 指定的 PID 验证服务器。在 PID 验证服务器，进行所述 PID 的 MAC 验证过程以进行关于是否用户的传送数据是合法的数据的确定过程。当数据是合法的时，通过预定的过程给予用户许可。随后将详细描述许可给予过程。

[2.系统配置]

参考图 5，现在将给出系统配置的例子的描述，该系统配置包含：参考图 1 描述的执行信息记录媒体制造和提供过程的实体；许可提供实体，它用来执行许可提供过程作为播放和使用第二数据记录域的加密内容的权限；和使用内容的客户。

使用内容的客户 50 从盘制造和提供实体购买信息记录媒体 80，如 CD。参考图 1，如上所述的信息记录媒体 80 是这样的信息记录媒体，其中设置第一数据记录域(第一会话)，它设置为执行复制防止过程的内容存储区域；和第二数据记录域(第二会话)，它是不执行复制防止过程并且其中存储加密的内容文件的内容存储区域，并且对其解密过程仅在具有许可的设备中才是可能的，所述加密的内容文件包含加密的内容和加密的密钥数据，使得用于加密内容的解密过程的密钥数据被加密。

客户是打算使用图 1 的信息记录媒体 10 的第二数据记录域 12 的加密内容的客户。图 1 的信息记录媒体 10 的第一数据记录域 11 的内容使得：在购买盘（CD 等）的同时分配使用权。在普通的 PC 等中，因为复制防止功能而使内容不能自由地播放，但是在普通的 CD 播放器等中可以自由地播放。

因此，在下面将给出这样情况的处理的重点描述：打算播放和使用信息记录媒体中的第二数据记录域的加密内容的客户得到使用内容的许可。

图 5 的客户 50 是作为能够使用，也就是播放内容的信息处理装置。其例

子包括各种信息处理设备，如 PC、PDA 等。客户 50 具有浏览器 51 和客户应用 52 作为软件，并且浏览器 51、客户应用 52 和其它程序通过控制装置如 CPU 执行。

客户应用 52 是这样的应用：进行记录于信息记录媒体如 CD 的执行文件（见图 4）的过程；执行获得包含服务数据和内容使用权信息的许可信息的过程，该过程作为许可获得过程的一系列的过程执行。客户应用 52 存储于客户的信息处理装置。

客户 50 通过例如通信网络如因特网连接到商店服务器 72、PID 验证服务器 73 和许可服务器 74。当客户 50 打算播放和使用信息记录媒体 80 中的第二数据记录域的加密内容时，商店服务器 72 用作通过其购买内容使用权（许可）的窗口并通过浏览器 51 显示内容信息如许可获得费用，使得来自客户 50 的购买请求被接受。进而，必要时商店服务器 72 为购买许可执行结账（billing）过程。

PID 验证服务器 73 执行 PID 验证过程，该过程作为来自客户 50 的许可获得过程的预过程执行。在 PID 验证服务器 73 验证成功的条件下，许可服务器 74 向客户 50 提供客户使用的内容的使用权信息。

进而，管理系统 75 连接到盘制造和提供实体 71、商店服务器 72、PID 验证服务器 73 和许可服务器 74。管理系统 75 和盘制造和提供实体 71 一起共享要记录在由盘制造和提供实体 71 制造的内容存储盘中的 PID 信息。在许可发布过程，该 PID 信息从客户传送到 PID 验证服务器 73，并且在验证服务器 73 执行验证过程。

管理系统 75 进而执行发布交易 ID（TID）的过程，交易 ID 用作来自客户 50 的许可获得请求的允许信息。进而，管理系统 75 允许发布使用权数据（使用权）作为内容的使用权信息。随后将描述这些过程的细节。

在数据库 77 中，存储在访问权范围内允许访问的数据，该访问权在盘制造和提供实体 71、商店服务器 72、PID 验证服务器 73、许可服务器 74 和管理系统 75 的每一个中设置。如随后将详细描述的，在数据库 77 中，例如，存储专辑主表（album master）、交易表、盘表、专辑价格主表和轨道表等。随后将详细描述这些表的结构和使用这些表的过程。

在图 5 中，商店服务器 72、PID 验证服务器 73、许可服务器 74 和管理系统 75 显示为单独的实体。但是，如图中所示，它们可以通过分离地安排构

成为网络连接的配置，并且，它们也可以构成为执行所有服务器的过程的一个装置。或者，它们的每个可以构成为执行一个或多个服务器的过程的多个装置。在本说明书中，执行在商店服务器 72、PID 验证服务器 73、许可服务器 74 和管理系统 75 的部分或全部处理的系统称为“许可管理系统”。

在客户应用 52 的控制下，客户 50 执行一系列涉及 PID 验证的处理，包括：PID 和产品 ID 到 PID 验证服务器 73 的传送，和通过与许可服务器 74 的连接的许可获得过程。商店服务器 72 提供的信息的浏览和结账（settlement）过程通过在客户应用 52 的控制下启动浏览器 51 进行。

在图 5 中，虽然显示一个客户和一个服务器，但是大量的客户和服务器在如例如因特网的通信网络上连接。适当时，客户选择对应于要进行的服务或过程的服务器，并与所选择的服务器进行连接以便继续进行处理。

从许可服务器 74 提供对应于内容的内容使用权信息到客户 50。客户 50 的客户应用 52 验证使用权信息，并当确定有使用权时，解密和使用加密的内容。

作为允许基于内容使用权的内容使用的密钥信息，客户 50 保存密钥数据，如使能密钥块（EKB）和设备节点密钥（DNK）。使能密钥块（EKB）和设备节点密钥（DNK）是用来获得使用内容必需的加密密钥的密钥数据，获得加密密钥的目的是：仅在具有授权的内容使用权的用户设备使其可能解密和使用加密内容。随后将描述 EKB 和 DNK。

许可服务器 74 在预定的内容使用权条件的基础上产生使用权信息（使用权），并把它提供给客户 50。进而，许可服务器 74 在设备节点密钥（DHK）和从管理系统 75 提供的使能密钥块（EKB）的基础上产生服务数据，并将它们提供给客户 50。服务数据包含具有服务设备节点密钥（SDNK）的使能密钥块（EKB），服务设备节点密钥在解密加密内容的过程中是必要的。

对于内容使用条件，可以设置如使用时段的限制、拷贝的数目的限制和通过其可以同时使用内容的便携媒体（PM）的数目（相应于所谓的检出（check-out）的数目）的限制。便携媒体（PM）的例子包括：闪存和可以用于便携设备的记录媒体，如小的 HD 、光盘、磁光盘或 MD（迷你盘）。

参考图 6，现在将给出能够用作客户 50、商店服务器 72、PID 验证服务器 73、许可服务器 74 和管理系统 75 的信息处理装置的硬件配置的例子。通过实现对应于如具有 CPU 的 PC、服务器等中的每个过程的处理程序而实现

这些系统的每一个。下面将给出图 6 的配置。

CPU（中央处理单元）101 根据存储于 ROM（只读存储器）102 的各种程序或存储于存储部分 108 并装入 RAM（随机访问存储器）103 的程序进行各种处理。定时器 100 执行时间测量过程并给 CPU 101 提供时钟信息。

ROM（只读存储器）102 其中已经存储 CPU 101 使用的程序、计算的参数和固定的数据等。RAM（随机访问存储器）103 存储执行期间使用的程序、计算的参数，适当时这些参数在通过 CPU 101 执行期间变化。这些元件通过 CPU 总线等构成的总线 111 互相连接。

加密和解密部分 104 执行通信数据或内容加密过程，使用如 DES（数据加密标准）加密算法的加密过程、MAC 产生和验证过程等，作为使用设备节点密钥（DNK）和使能密钥块（EKB）的过程。进而，加密和解密部分 104 执行各种加密过程，如在传送和接收通信数据如许可信息期间的鉴别过程，和对于另一个连接的设备执行的会话密钥共享过程。

编解码部分 105 进行各种方法的数据编码过程和数据解码过程，如例如 ATRAC（自适应转换声音编码）3 方法和 MPEG 方法、JPEG 方法等。要处理的数据从可移除记录媒体 121 通过总线 111、输入/输出接口 112 和驱动 110 输入，或通过通信部分 109 输入。进而，处理的数据必要时存储于可移除记录媒体 121 或通过通信部分 109 输出。

包括键盘、鼠标等的输入部分 106，包括如 CRT 或 LCD 的显示器、扬声器等的输出部分 107，如硬盘的存储部分 108，和包括调制解调器、终端适配器等的通信部分 109 连接到输入/输出接口 112，使得通过如例如因特网的通信网络进行数据发送和接收。

[3.作为密钥分配结构的树结构]

接着，将给出由树结构构成的设备和密钥管理配置的描述，它是广播加密方法的一种形式，该方法用于使只有拥有授权的内容使用权的客户使用内容成为可能。

在图 7 的最低级显示的数字 0 到 15 表示作为使用内容的客户的用户设备。即，图 7 中显示的层次化的树结构的每个叶子对应于每个设备。

在制造期间，交货之前，或其后，设备 0 到 15 在存储器存储由密钥（节点密钥）和叶子的叶子密钥构成的密钥集（设备节点密钥（DNK）），它们分配给图 7 中显示的、层次化的树结构中的、从它自己的叶子到根的各节点。

在图 7 的最低级显示的 K0000 到 K1111 是叶子密钥，它们分别分配给设备 0 到 15，并且假定从最高级直到从最低级数的第二个节点指示的密钥 KR 到 K111 为节点密钥。

在图 7 中显示的树结构中，例如，设备 0 拥有叶子密钥 K0000 和节点密钥 K000、K00、K0 和 KR。设备 5 拥有 K0101、K010、K01、K0 和 KR。设备 15 拥有 K1111、K111、K11、K1 和 KR。在图 7 的树中，仅指示 16 个设备 0 到 15，并且树结构显示为对于右和左侧对称地平衡的四级结构。同样，拥有这样的结构是可能的，其中更大数目的设备在树中形成，并且在树的每一部分提供不同的级数。

包含于图 7 的树结构中的设备包括各种类型的设备，它们使用各种类型的记录媒体，例如，设备嵌入类型或 DVD、CD、MD 和闪存等，它们以这样的方式配置，以便装入设备或可从设备移走。进而，各种应用服务可以共存。作为图 7 中显示的内容或密钥分配结构的、层次化的树结构，应用到这样的结构，其中这样的不同的设备和不同的应用共存。

在这些各种设备和应用共存的系统中，例如，由图 7 的虚线包围起来的部分，即设置设备 0、1、2 和 3 设置为一组，其中使用同样的记录媒体。例如，对于包含于由虚线包围的该组中的设备，由一个操作执行这样的过程：从提供者发送加密的共同的内容；发送在这些设备中共用的内容密钥；或从每个设备输出加密的内容价钱的支付数据到提供者或结账机构等。对用于执行到每个设备的数据传送和从每个设备的数据接收的实体，如内容服务器、许可服务器或商店服务器，通过假定用图 7 的虚线包围起来的部分，即设备 0、1、2 和 3 为一组，执行集中发送数据的过程变为可能。

利用具有一个特殊的密钥管理中心功能的管理系统，可以以集中的方式管理节点密钥和叶子密钥，或者通过执行各种到每个组的数据传送和从每个组的数据接收的消息数据分配装置，如提供者和结账机构，可以管理每个组的节点密钥和叶子密钥。例如，在密钥泄漏的情况下，对这些节点密钥和叶子密钥执行更新过程，并且由具有密钥管理中心功能的管理系统、提供者和结账机构执行该更新过程。

在该树结构中，如从图 7 可见，作为设备节点密钥(DNK)，包含于一个组中的设备 0、1、2 和 3 拥有包含公共的密钥 K00、K0 和 KR 的设备节点密钥(DNK)。通过使用该节点密钥共享的结构，仅提供如公共的密钥给设备 0、

1、2和3变为可能。例如，共同拥有的节点密钥K00是设备0、1、2和3中共同拥有的密钥。进而，如果使得用节点密钥K00加密新的密钥Knew的值Enc (K00, Knew)通过网络或通过该值存储于其中的记录媒体分配给设备0、1、2和3，只有设备0、1、2和3，可能通过使用每个设备中拥有的共享节点密钥K00解密Enc (K00, Knew)，获得新的密钥Knew。Enc (Ka, Kb)指示使得用Ka加密Kb的数据。

在特定时间t，当发现这样的情况：设备3拥有的密钥K0011、K001、K00、K0和KR被攻击者（黑客）分析并暴露的时候，其后，为保护由系统（设备0、1、2和3的组）传送和接收的数据，从系统断开设备3是必要的。为了该目的，分别更新节点密钥K001、K00、K0和KR为K(t)001、K(t)00、K(t)0和K(t)R，并发送更新的密钥到设备0、1和2是必要的。这里，K(t)aaa指示密钥Kaaa的t代的更新密钥。

下面描述分配更新密钥的过程。通过网络或通过其中存储表的记录媒体，提供图 8(A)中显示的称为使能密钥块(EKB)的数据块构成的表，进行密钥的更新。使能密钥块(EKB)由加密密钥构成，该加密密钥用于分配新更新的密钥给对应于构成图7中显示的树结构的每个叶子的设备。使能密钥块(EKB)也称为“密钥更新块(KRB，key renewal block)”。

在图 8(A)中显示的使能密钥块(EKB)中，只有节点密钥需要更新的设备构成为具有可以更新的数据结构的数据块。图8的例子显示为以下目的构成的块数据：分配图7中所示的树结构中的、设备0、1和2中的、t代的更新节点密钥。从图7可见，设备0和设备1要求K(t)00、K(t)0和K(t)R作为更新节点密钥，并且设备2要求K(t)001、K(t)00、K(t)0和K(t)R作为更新节点密钥。

如图8 (A)的EKB中所示，EKB包含多个加密密钥。在最低级的加密密钥是Enc (K0010, K(t)001)。这是更新节点密钥K(t)001，它由设备2拥有的叶子密钥K0010加密，并且设备2通过用设备自身拥有的叶子密钥，解密该加密密钥可以得到 K(t)001。进而，通过使用由解密得到的 K(t)001，可以解密从图8 (A)中底端数第二级的加密密钥Enc (K(t)001, K(t)00)，使得到更新节点密钥K(t)001成为可能。以下，以顺序的方式，通过解密从图8 (A)中顶端数第二级的加密密钥Enc (K(t)00, K(t)0)，得到更新节点密钥K(t)0，并且通过解密来自图8 (A) 中顶端的加密密钥Enc (K(t)0, K(t)R)，得到K(t)R。另一方面，

在设备 K0000.K0001 中，节点密钥 K000 不包含在要更新的目标中，并且必要的更新节点密钥是 K(t)00、K(t)0 和 K(t)R。通过解密从图 8 (A)中顶端数第三级的加密密钥 Enc (K000, K(t)00)，设备 K0000.K0001 得到 K(t)00。此后，通过解密从图 8 (A)中顶端数第二级的加密密钥 Enc (K(t)00, K(t)0)，得到更新节点密钥 K(t)0。通过解密从图 8 (A) 顶端数第一级的加密密钥 Enc (K(t)0, K(t)R)，得到 K(t)R。以这种方式，设备 0、1 和 2 得到更新的密钥 K(t)R 是可能的。图 8 (A)中的索引指示节点密钥和叶子密钥的绝对地址，它们用作解密密钥。

在这样的情况下: 图 7 中所示的树结构的、较高阶的级的、节点密钥 K(t)0 和 K(t)R 的更新是不必要的，而只更新节点密钥 K00 的过程是必要的，图 8(B)的使能密钥块(EKB)的使用使其可能分配更新节点密钥 K(t)00 给设备 0、1 和 2。

当例如分配在一个具体组中共享的新的内容密钥时，可以使用图 8(B)中所示的 EKB。在一个具体例子中，假定由图 7 中的虚线指示的组中的设备 0、1、2 和 3 使用特定的记录媒体，并且新的公共内容密钥 K(t)con 是必要的。这时，与图 8(B)中所示的 EKB 一起分配数据 Enc (K(t), K(t)con)，使得用 K(t)00 加密新的公共更新密钥 K(t)con，以便加密设备 0、1、2 和 3 的公共节点密钥 K00。作为该分配的结果，在另一个组中的设备如设备 4 中未加密的数据的分配变为可能。

即，如果设备 0、1 和 2 通过使用通过处理 EKB 得到的 K(t)00 解密上面的加密的文字，得到在时间 t 的密钥，如用于加密和解密内容的内容密钥 K(t)con，变为可能。

[4.使用 EKB 的密钥的分配]

作为处理的例子，在该例子中，获得在时间点 t 时的密钥，例如用于加密和解密内容的内容密钥 K(t)con，图 9 显示设备 0 的处理的例子，该设备 0 通过记录媒体接收数据 Enc (K(t)00, K(t)con)，以便用 K(t)00 和图 8(B)中所示的 EKB 加密新的公共的内容密钥 K(t)con。即，这是使利用 EKB 的加密的消息数据成为内容密钥 K(t)con 的例子。

如图 9 中所示，通过与所述使用 t 代时的 EKB 的过程相似的 EKB 过程，设备 0 产生存储于记录媒体中的节点密钥 K(t)00，以及预存于设备自身中的节点密钥 K000。进而，设备 0 通过使用解密的更新内容密钥 K(t)00 解密更新

内容 K(t)con，用只有设备自身拥有的叶子密钥 K0000 加密它，并为将来使用存储它。

[5.EKB 的格式]

图 10 显示使能密钥块(EKB)的格式的例子。版本 201 是指示使能密钥块(EKB)的版本的标识符。版本具有识别最近的 EKB 的功能和指示与内容的对应关系的功能。深度指示关于使能密钥块(EKB)的分配目的地的设备的、层次化树的层次的数目。数据指针 203 是指示使能密钥块(EKB)中的数据部分的位置的指针。标记指针 204 是指示标记部分的位置的指针。签名指针 205 是指示签名位置的指针。

数据部分 206 存储如数据，使得加密要更新的节点密钥。例如，存储图 8 中所示的属于更新的节点密钥的加密密钥。

标记部分 207 是指示存储于数据部分的加密节点密钥和叶子密钥之间的位置关系的标记。参考图 11 描述分配该标记的规则。在图 11 中，显示图 8(A)中描述的使能密钥块作为数据发送的例子。这时的数据如图 11 的表(b)中所示。这时包含于加密密钥的顶端节点的地址假定为顶端节点地址。在这种情况下，因为包含根密钥的更新密钥 K(t)R，顶端节点的地址是 KR。此时，例如，最高级的数据 Enc (K(t)0, K(t)R)处于图 11(a)中所示的层次化的树中的指示的位置。这里，下一个数据是 Enc (K(t)00, K(t)0)，并且处于树中的前一个数据的左下的位置。当有数据时，标记设为 0，并且当没有数据时，标记设为 1。标记设为{左(L)标记，右(R)标记}。因为最高级的数据 Enc (K(t)0, K(t)R)的左侧有数据，L 标记=0，并且因为右侧没有数据，R 标记=1。此后，设置所有数据的标记，并且形成图 11(c)中所示的数据序列和标记序列。

设置标记指示数据 Enc (Kxxx, Kyyy)位于树结构的哪个位置。因为存储于数据部分的密钥数据 Enc (Kxxx, Kyyy)...仅仅是简单地加密的密钥的序列的数据，通过所述标记，在树中确定作为数据存储的加密密钥的位置是可能的。通过使用对应于加密数据的节点索引而不使用所述标记，可以构成下面的数据结构，如在参考图 8 的所述结构中那样，例如，

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

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

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

...但是，在使用这样的索引的结构的情况下，数据变为冗余的，并且数

据量增大，这在通过网络的分配中是不希望的。当与此比较时，通过使用所述标记作为指示密钥的位置的索引数据，用较小量数据确定密钥的位置变为可能。

返回来参考图 10，将进一步描述 EKB 格式。签名 208 是电子签名，该签名由已经发出使能密钥块(EKB)的、如具有密钥管理中心功能的管理系统、内容服务器、许可服务器或商店服务器放置。接收 EKB 的设备通过签名验证确认使能密钥块(EKB)由合法的使能密钥块(EKB)发行者发行。

[6.树的目录分类]

下面将给出这样的结构的描述，在该结构中，通过对定义节点密钥等的层次化的树结构的分类，对每个设备的每个目录执行高效的密钥更新过程、加密密钥分配和数据分配。

图 12 显示在层次化的树结构中目录的分类的例子。在图 12 中，在层次化的树结构的最高级设置根密钥 Kroot 301，在低于最高级的中间级设置节点密钥 302，并且在最低级设置叶子密钥 303。每个设备保存单独的叶子密钥、从叶子密钥直到根密钥的一系列的节点密钥和根密钥。

这里，作为例子，设置从最高级数第 M 级的一个具体节点为目录节点 304。也就是，设置第 M 级的每个节点为具体目录的设备设置节点。通过设置第 M 级一个节点为顶点，以下，假定第(M+1) 级或更低级的节点和叶子为属于包含于那个目录的设备的节点和叶子。

例如，在图 12 的第 M 级的一个节点 305 设置目录[记忆棒（商标）]，并且设置连接到该节点或更低的节点的节点和叶子为包含各种使用记忆棒的设备的目录专用的节点和叶子。也就是，定义节点 305 和更低的节点为与在记忆棒的目录中定义的设备相关联的节点和一组叶子。

进而，可设置比第 M 级低几级的级为子目录节点 306。例如，如图中所示，在比目录[记忆棒]节点 305 低两级的节点，设置节点[只播放设备]为包含于使用记忆棒的设备的目录中的子目录节点。进而，在作为子目录节点的只播放设备的节点 306 和更低的节点，设置包含于只播放设备的目录中的有音乐播放功能的电话的节点 307，并且在比节点 307 更低的节点，可以设置包含于有音乐播放功能的电话的目录中的[PHS]节点 308 和[蜂窝电话]节点 309。

进而，不仅可以通过设备的类型，而且可以通过节点设置目录和子目录，这些节点由如制造者、内容提供者、结账机构等，即如处理单元、管理单元

或提供的服务单元的任何单元（以下将统称为“实体”）单独管理。例如，如果一个目录节点设置为专门用于由游戏设备制造者出售的游戏设备 XYZ 的顶点节点，出售游戏设备 XYZ 变得可能，在该设备中存储顶点和更低的节点的级的节点密钥和叶子密钥。其后，对分配加密内容的过程或分配和更新各种密钥的过程，产生并分配由顶点和更低的节点的节点密钥和叶子密钥构成的使能密钥块(EKB)，使得可以分配仅可以用于顶点和更低的节点的设备的数据。

以这种方式，作为构成这样的结构的结果，在该结构中，假定一个节点为顶点并且设置更低的节点为与在顶点节点定义的目录或子目录相关联的节点，下面的结构变为可能，在该结构中，管理该目录级或该子目录级的一个顶点节点的制造者、内容提供者等，单独产生其中那个节点是顶点的使能密钥块(EKB)，并且使能密钥块(EKB)分配给属于该顶点和更低的节点的设备，并且可以执行密钥更新而一点也不影响属于其它的不属于该顶点节点的目录的节点的设备。

例如，如图 13 中所示，在树结构的系统中执行密钥管理。在图 13 的例子中，8+24+32 级的节点形成为树结构，并且对应从根节点到低 8 阶的级的每个节点定义目录。这里目录意味着，例如使用半导体存储器如记忆棒的设备的目录，或接收数字广播的设备的目录。然后，该系统（称为“T 系统”）作为管理许可的系统对应于目录节点中的一个节点。

也就是，对应于比 T 系统的节点低的层次的 24 级的节点的密钥，作为如商店服务器或许可服务器的管理实体用于服务提供者，或用于由服务提供者提供的服务。在该例子的情况，这使其可能指定 2^{24}（大约 16 兆字节）个服务提供者或服务。进而，最低端的 32 级的级次使其可能指定 2^{32}（大约 4 千兆字节）个用户（或用户设备）。对应于从最低端的 32 级的节点到 T 系统的节点的路径上的每个节点的密钥构成设备节点密钥(DNK)，并且假定对应于最低级的叶子的 ID 为叶子 ID。

例如，用更新的根密钥 KR’加密使得内容加密的内容密钥，并且使用最近的较低阶级次的更新节点密钥加密较高阶级次的更新节点密钥并放置在 EKB 中。用 EKB 的最低端的节点密钥或叶子密钥加密比 EKB 的最低端高一级的级的更新节点密钥，并放置在 EKB 中。

通过使用服务数据中描述的 DNK 的密钥之一，用户设备解密最近的较

高阶级次的更新节点密钥，该密钥在与内容数据一起分配的 EKB 中描述；并通过使用由解密得到的密钥，解密在 EKB 中描述的高于它的级次的更新节点密钥。通过顺序地执行上面的过程，用户设备可能得到更新根密钥 KR'。

以所述方式，树目录分类使这样的结构成为可能，其中，设置一个节点为顶点，设置较低的节点为与在顶点节点定义的目录或子目录相关联的节点。因此，实现这样的结构，其中，管理目录级或子目录级的一个顶点节点的制造者、服务提供者等，单独产生其中那个节点是顶点的使能密钥块(EKB)，并且分配使能密钥块(EKB)给属于该顶点和更低的节点的设备。

给出内容分配和使用形式的进一步描述，其中，通过使用利用所述树结构的设备管理的 EKB 分配系统，采用 EKB 分配结构。

参考图 14，下面描述两个目录。如图 14 中所示，在低于根节点 350 的级上设置 T 系统节点 351，并在低于那个节点的级上设置 T 服务节点 352 和 T 硬件节点 353。其中 T 硬件节点 353 为顶点的树是这样的目录树，其中，用户设备自身设置为叶子 355，并且分配对应于硬件的 EKB [EKB (H)]，对设备的对象发行它。另一方面，其中 T 服务节点 352 为顶点的树是这样的目录树，其中，分配对应于服务的 EKB [EKB (S)]，发行它以便对应提供给用户设备的服务。

对应于硬件的 EKB [EKB (H)]和对应于服务的 EKB [EKB (S)]都有给予具有授权的权限的设备的 DNK（设备节点密钥），也就是，对应于从 T 系统的叶子到节点的路径上的每个节点的密钥，因此使其可能解密每个 EKB。

[7.许可购买和内容播放过程]

现在将给出许可获得过程和在获得的许可的基础上进行的内容使用（播放）过程的描述，当客户打算使用，也就是播放图 1 中所示的、信息记录媒体 10（盘）的、第二数据记录域 12 的、记录内容，也就是加密的内容时，许可获得过程变为必需的。

图 15 显示内容购买过程中的通信顺序的初始步骤，它在客户如具有客户应用和浏览器的 PC 与商店服务器、PID 验证服务器、许可服务器和管理系统之间执行。用户、客户应用和浏览器的整体统称为“客户”，并且商店服务器、PID 验证服务器、许可服务器和管理系统的整体统称为“许可管理装置”。现在将描述顺序图中所示的过程。对于实体间的数据通信，除了当确保通信路径为安全的通信路径时，通过执行加密过程，例如基于 SSL 的加密过程，执

行数据的发送和接收。

最初，在客户端，打算播放图 1 中所示的、信息记录媒体（盘）10 的第二数据记录域 12 的、记录内容，也就是加密的内容的用户，指定播放内容（步骤（1））。但是，如参考图 4 所描述的，因为作为放置 CD 于 PC 中的过程的结果，自动执行应用，用户对内容的指定对应于由用户放置信息记录媒体如 CD 于驱动器（例如，CD-RW 驱动器）中的过程。

如 PC 的信息处理装置中的客户应用从信息记录媒体如放置的 CD 读取 PID 的信息（见图 2）、PID 验证服务器 URL 的信息和产品 ID 的信息（步骤（2））。如上所述，PID 是图 1 中所示的信息记录媒体 10 的 PID (后刻 ID, Postscribed-ID)记录区域 13 中记录的数据，包含媒体 ID 和版本信息并且添加 MAC 作为数据变化验证码，其中媒体 ID 作为预定的盘簇(disk set)单元，例如标题单元、专辑单元、目录单元和制造签单元中每个盘唯一的标识符(ID)给出。如参考图 4 描述的，PID 验证服务器 URL 的信息和产品 ID 的信息是存储于数据文件中的定义文件中的信息，该数据文件存储于第二数据记录域 12。

其次，客户应用在得到的 PID 验证服务器 URL 的基础上，发送得到的 PID 和产品 ID 到 PID 验证服务器（步骤（3））。

当从客户接收到 PID 和产品 ID 时，PID 验证服务器执行 MAC 验证过程作为验证收到的 PID 是否已经被改变的过程（步骤（4））。作为这样的过程执行 MAC 验证过程，在该过程中，例如，基于收到的消息(PID)执行参考图 3 描述的 MAC 产生过程，并且确定是否产生的 MAC 值匹配添加到收到的 PID 的 MAC 值。

PID 验证服务器从专辑主表得到产生 MAC 需要的密钥。专辑主表的结构的例子在图 16 中显示。专辑主表作为这样的表构成，其中，使产品 ID、作为用于 PID 的 MAC 验证的密钥信息的 PID 密钥、标题信息和对应于存储于盘的内容的艺术家信息互相对应。

基于从客户接收到的产品 ID，PID 验证服务器从图 16 中所示的专辑主表得到作为 MAC 验证密钥的 PID 密钥，产生 MAC，并执行验证从客户接收到的 PID 的变化的过程。当产生的 MAC 值与添加到接收到的 PID 的 MAC 值不同时，确定 PID 数据已经改变，传送错误消息到客户，并且不执行随后的许可获得过程。

当产生的 MAC 值与添加到接收到的 PID 的 MAC 值匹配时，确定 PID 数据还未改变，并且 PID 验证服务器发送 PID 和产品 ID 到管理系统（步骤（5））。当从 PID 验证服务器接收到 PID 和产品 ID 时，基于例如随机数，管理系统产生交易 ID (TID)作为用于一系列的处理序列（交易）的识别数据（步骤（6））。

进而，管理系统产生交易表条目，其中，使产品 ID、PID 和许可的价格，也就是，内容使用价格信息，对应于产生的交易 ID，并且在表中存储条目（步骤（7））。交易表的结构的例子如图 17 中所示。如图 17 中所示，交易表是这样的表，其中，存储产品 ID、PID 中的媒体 ID 和作为许可价格的内容使用价格，以便对应作为用于一系列的处理序列（交易）的识别数据的交易 ID。

作为许可价格的内容使用价格可以以这样的方式固定以便对应于内容。或者，它可以设置为根据内容的使用数、即许可的购买数而变化的价格。

如上所述，产品 ID 和 PID（媒体 ID）的结合是全局唯一识别数据。设置例如图 18(a)中所示的盘表这样的表，其中，使产品 ID 和 PID（媒体 ID）的结合对应于购买数，也就是，基于来自客户的内容使用请求而发放的许可数。进而，产生图 18(b)中所示的专辑价格主表，其中，使产品 ID、购买数和价格互相对应，并且该表在数据库中存储和管理。

在设置图 18 中所示的盘表和专辑价格主表并且产生来自新的的客户的内容使用请求的情况下，通过参考盘表，基于产品 ID 和 PID（媒体 ID）检查过去购买数，并且通过参考专辑价格主表，基于产品 ID 和购买数，确定要呈现的价格。

例如，当从客户提出的产品 ID 和 PID（媒体 ID）匹配图 18(a)中所示的第一个条目的[P-1, PID1-001]时，确定过去购买数是 1，并且这时的购买请求是第二次。因此，使图 18(a)中所示的专辑价格主表的产品 ID (= P-1)和购买数(=2)的设置价格，也就是¥300 为呈现的价格。进而，执行更新过程，盘表的第一个条目的[P-1, PID1-001]的购买数增加一个。

在许可管理装置一侧的管理系统中，可以执行盘表更新过程和价格设置过程。或者，可以在商店服务器、PID 验证服务器和许可服务器的任何一个中执行这些过程。也就是，在这些服务器之一中，基于与从客户接收到的许可获得请求有关的识别数据，从盘表得到客户的内容使用信息；基于内容使用信息，从专辑价格主表得到许可提供条件信息；并且基于得到的许可提供

条件信息，确定客户的许可提供条件。在一个服务器或管理系统中，执行许可提供条件确定过程的处理程序存储于存储部分，而控制部分，如 CPU，用作许可提供条件确定处理装置。

价格设置可以采取各种形式。这样的结构是可能的，使得来自客户的同一内容的购买数增加得越多，价格降低得越多，并且设置固定的次数或更多次，如三次或更多次的购买过程为免费。

除了根据购买数改变价格的形式，还以各种不同的方式改变服务，例如，当设置有时间限制的许可时，根据购买数，设置设置时间段为长的时间段。或者，根据购买数，可以提供各种服务，如根据购买数免费提供的内容。

管理系统中的交易表（图 17）的条目中的价格信息是通过参考图 18 中所示的盘表和专辑价格主表设置的价格。该价格设置过程可以由如 PID 服务器执行，并且价格设置信息可以传送到管理系统。或者，必要的信息可以从管理系统传送到商店服务器或许可服务器，可以在商店服务器或许可服务中进行价格设置，并且设置的价格信息可以传送到管理系统。另外，通过参考图 18 中所示的盘表和专辑价格主表，管理系统自身可以确定价格。

现在将参考图 19 描述图 15 的顺序图后面的处理。在管理系统中，当完成交易（图 17）的条目的产生时，管理系统传送播放内容必需的许可购买页信息(URL) 和交易 ID (TID)到 PID 验证服务器（步骤（8）），并且 PID 验证服务器传送许可购买页信息(URL) 和交易 ID (TID)到客户应用（步骤（9））。

客户应用在接收到的 URL（步骤（10））基础上启动浏览器，以便显示商店服务器呈现的许可购买页，并且传送交易 ID (TID)到商店服务器（步骤（11））。

基于接收到的交易 ID (TID)，商店服务器从交易表（见图 17）得到对应于 TID 的价格信息和产品 ID、PID（媒体 ID）（步骤（21））。商店服务器进而从图 20 中所示的轨道表得到内容标题信息，其中使内容号、产品 ID 和内容标题互相对应。进而，基于产品 ID，商店服务器从专辑主表（见图 18(b)）得到内容信息，如相应的专辑标题和艺术家名字（步骤(13)）。基于得到的信息，商店服务器生成要呈现给客户的购买页。商店服务器包括 Web 页产生和呈现装置，并且购买页作为 Web 页产生并呈现给客户。随后将参考附图详细描述购买页结构的例子。

现在将参考图 21 中的流程图给出，从客户接收到 PID 和产品 ID 时直到

购买页传送到客户，在许可管理装置侧的一系列过程的描述。

起初，在步骤 S101，基于从客户接收到的产品 ID，从专辑主表（见图 16）得到相应的 PID 密钥。然后，在步骤 S102，使用 PID 密钥，计算接收到的 PID 的 MAC 值。

在步骤 S103，执行比较计算的 MAC 值和存储于接收到的 PID 中的 MAC 值的过程。如果它们不匹配，确定接收到的 PID 已经改变，并且过程前进到步骤 S108，在那里传送错误消息到客户，并完成处理。

如果计算的 MAC 值等于存储于 PID 中的 MAC，确定接收到的 PID 未改变。接着，在步骤 104，基于从客户接收到的[产品 ID，PID（媒体 ID）]，从盘表（见图 18(a)）得到关于购买数的数据。然后，在步骤 105，基于产品 ID，从专辑价格主表（见图 18(b)）得到对应于购买数的设置的价格。

接着，在步骤 106，执行产生 TID 的过程，然后设置交易表（见图 17）的条目，其中使产品 ID、PID（媒体 ID）和价格与 TID 对应。

接着，在步骤 107，从专辑主表和轨道表得到内容信息，从交易表得到价格信息，产生包括价格和内容信息的购买页，并且该页和 TID 一起传送到客户。作为在许可管理装置侧的 PID 验证服务器、管理系统和其它实体中的协调的过程，进行图 21 中所示的每个步骤的过程。

现在将参考图 22 的处理顺序图描述图 19 的处理序列后面的许可提供过程。商店服务器在所述处理的基础上产生购买页，并且将它呈现给客户的浏览器（步骤(14)）。

呈现给客户的浏览器的购买页的结构的例子在图 23 中显示。购买页包含内容信息 501、价格信息 502 和指示用于用户的输入请求项信息的用户输入域 503。内容信息 501 是记录于如 CD 的信息记录媒体（见图 1）的第二数据记录域的加密内容的信息，它在客户设置。对于价格信息 502，当根据购买数以所述方式改变设置时，显示根据购买数设置的价格。

客户显示图 23 中所示的购买页、结算过程必需的输入数据，如姓名、邮件地址、信用卡号、信用卡的过期数据等（步骤(15)），并通过浏览器传送输入信息到商店服务器（步骤(16)）。

接收结算信息的商店服务器在接收到的信息的基础上执行结账过程（步骤(17)）。更具体地，与结账机构，如提供在线结账过程作为服务的财务机构建立连接，并执行确定是否客户呈现的信用卡号是有效的和合法的及确定是

否存在可以结账的账户结余（account balance）的过程。之后，在结账机构，从指定的账户中提取相应于购买金额的一定数量的款项或执行传送过程，并且商店服务器从结账机构接收结账完成消息。

当完成结账过程时，对于客户，商店服务器在客户应用中产生用于启动内容使用程序（播放过程等）的启动文件，并通过客户浏览器将它发送到客户应用。

参考图 24 将描述启动文件的例子。启动文件 551 包含：先前由管理系统产生的交易 ID (TID)，要由客户使用和播放的内容 ID (CID)，由管理系统产生的使用权信息(UID)、服务 ID、许可服务器 URL 和商店服务器 URL。

客户应用启动应用以响应从商店服务器接收到的启动文件（步骤(19)）。

在由客户应用执行的应用启动过程中，首先，确定在启动文件（见图 24）中设置的、对应服务 ID 的服务数据是否存储于用作客户系统的信息处理装置。

当客户想要接收各种服务例如内容使用服务时，从许可服务器接收服务数据，并且服务数据是用于认可的数据，例如由特定的服务提供者提供的服务的集体服务使用权。图 25(a)显示服务数据的数据结构的例子。

如图 25(a)中所示，服务数据 570 包含：对客户唯一的叶子 ID，它在 EKB 分配树中设置；用作服务标识符的服务 ID；和数据 E (Kroot, DNK)，使得用根密钥（Kroot）加密设备节点密钥(DNK)。为接收服务数据，客户要求执行许可服务器的注册过程。

注册过程对应于图 26 中所示的处理步骤(20)和(21)的过程。当确定客户未拥有对应于服务 ID 的服务数据时，执行处理步骤(20)和(21)的注册过程，使得从许可服务器接收服务数据。当客户已经拥有对应于服务 ID 的服务数据时，不需要执行该注册过程。

然后为其执行注册过程的客户得到使用权信息作为来自许可服务器的、对应于使用（播放）内容的许可。

图 25(b)显示使用权信息的数据结构的例子。如图 25(b)中所示，在使用权信息 571 中存储：用作使用权信息标识符的使用权信息 ID；用作发布日期和时间信息的时间标记；和对客户唯一的叶子 ID。进而，当使用权信息对应于内容时，存储用于使用条件的目标的内容 ID 和内容类型信息。对于内容 ID，可以列出存储于图 1 中所示的信息记录媒体的第二数据存储区域中的加密的

内容的各内容 ID，或者可以设置产品 ID。

内容 572，即图 1 中所示的信息记录媒体 10 的第二数据记录域 12 的记录内容，以这样的方式记录于盘中，以便包含：内容数据 Enc (Kc, 内容)，它用内容密钥[Kc]加密；内容密钥数据 Enc (Kroot, Kc)，它用根密钥[Kroot]加密；EKB，它仅由具有合法的使用权的用户解密，并且从它可以得到根密钥[Kroot]；和服务 ID。

现在将参考图 26 中的顺序图给出获得使用权信息的处理顺序的描述，它作为许可获得过程执行。

客户传送获得对应于要播放或使用的内容的、使用权信息（使用权）的请求到许可服务器（步骤(22)）。该请求包含：使用权信息(UID)，它包含于先前来自商店服务器的启动文件（见图 24）中；用作客户识别数据的叶子 ID；和交易 ID(TID)，它包含于先前来自商店服务器的启动文件（见图 24）中。

当接收获得使用权信息（使用权）的请求时，许可服务器对管理系统执行定单查询过程（步骤(23)）。该请求包含使用权信息 ID(UID)和交易 ID(TID)。接收定单查询的管理系统将作为定单查询响应的响应信息传送到许可服务器，定单查询响应中设置对应于使用权信息 ID(UID)的使用条件（步骤(24)）。

接收响应信息的许可服务器产生使用权信息（使用权），其中设置内容使用条件，并且发布使用权信息到客户（步骤(25)）。内容使用条件形成为内容的播放数、过期数据、各种过程如用于外部设备的复制和结账(check out)过程的允许信息。

对于先前从内容服务器接收的内容，在记录于使用权信息（使用权）中的使用条件下，接收使用权信息（使用权）的客户使用内容变为可能。当其中指定内容 ID (CID)和使用权信息（使用权）的内容播放请求从用户发生（步骤(26)）时，客户应用根据使用条件执行内容播放（步骤(27)）。

现在将参考图 27 给出基本的内容播放过程的步骤的描述。从图 1 中所示的信息记录媒体的第二数据存储区域（第二会话）582 读取包含加密的内容的内容文件 584。从许可服务器 581 提供服务数据和用作许可的使用权信息（使用权）到客户 583。通过使用服务数据和使用权信息（使用权），执行解密内容文件 584 中的加密内容的过程。

用内容密钥 Kc 加密包含于内容文件 584 中的内容（ Enc (Kc, 内容)，并且内容密钥 Kc 是从根密钥 Kroot 得到的密钥，根密钥 Kroot 可以从 EKB 得

到。

客户 583 从服务数据得到设备节点密钥 (DNK)，该服务数据从许可服务器接收，并在得到的 DNK 的基础上，通过解密内容文件的 EKB，得到根密钥 Kroot。进而，通过使用得到的根密钥 Kroot 解密 Enc (Kroot, Kc)，客户 583 得到内容密钥 Kc；通过执行由得到的内容密钥 Kc 解密加密的内容 Enc (Kc, 内容)的过程，得到内容；并播放该内容。

现在将参考图 28 给出内容播放过程的细节的描述，其中使内容播放过程对应于服务数据和使用权信息（使用权）。

图 28 是使用对应于硬件的 EKB [EKB (H)]和对应于软件的 EKB [EKB (S)]、基于内容解密过程的内容使用处理顺序的图解。

图 28 中所示的服务数据 601 和使用权信息 603 是从许可服务器接收到的数据，并且加密的内容文件 602 是从图 1 中所示的信息记录媒体的第二数据存储区域（第二会话）读取的数据。服务数据 601 其中已经存储用作叶子标识符的叶子 ID、要使用的 EKB 的版本和数据 E (Kroot', SDNK)，使得对应于服务的设备节点密钥(SDNK)由根密钥 Kroot'加密，其中，该设备节点密钥(SDNK)对解密对应于服务的 EKB [EKB (S)]是必需的，并且以这样的方式设置该根密钥 Kroot'，以便与对应于硬件的目录树相对应。

加密的内容文件 602 是这样的文件，它包含：对应于服务的 EKB [EKB (S)]，其中存储以这样的方式设置的根密钥 Kroot，以便与对应于服务的目录树相对应；数据 E (Kroot, CID+Kc)，使得加密用于内容加密和解密过程的内容 ID(CID)和内容密钥(Kc)；和数据 E (Kc, 内容)，使得用内容密钥 Kc 加密内容（内容）。

进而，使用权信息 603 是使叶子 ID 和内容使用条件信息存储于其中的数据。内容使用条件信息包括各种使用条件，如使用时间段、使用的次数、复制限制等，它们以这样的方式设置以便对应于内容。接收使用权信息 603 的用户设备存储使用权信息作为对应于内容的安全信息，或存储使用权信息作为在播放设备（PC 等）中设置的 AV 索引文件中的内容的索引数据。

例如，在用户设备如 PC 中，使用权信息可以作为对应于内容的安全信息存储，该用户设备没有大容量的存储装置并且处理器的处理性能高。优选地，存储所有的使用权信息，使得当使用内容时执行引用所有的使用权信息的过程。另一方面，在用户设备如便携设备（PD）中，该设备没有大容量的

存储装置并且处理器的处理性能低，这样的处理是可能的，其中，由选择的信息构成的使用权信息 403 存储于用作内容的索引数据的 AV 索引文件，并且执行过程使得 AV 索引文件中的使用权信息被引用。

在图 28 中所示的步骤 S701，用户设备执行这样的过程：通过使用对应于硬件的设备节点密钥(HDNK) 602，解密对应于硬件的 EKB (H) 611，因此从 EKB (H) 611 得到根密钥 Kroot'，根密钥 Kroot'以这样的方式设置以便与对应于硬件的目录树对应。使用 DNK 的 EKB 的过程是根据参考图 9 的所述方法的过程。

接着，在步骤 S702，通过使用从 EKB (H)提取的根密钥 Kroot'，执行解密服务数据 601 中的加密的数据 E (Kroot', SDNK)的过程，从而得到用于对应于服务的 EKB [EKB (S)]的过程（解密）的设备节点密钥(SDNK)。

接着，在步骤 S703，通过使用从服务数据提取的设备节点密钥(SDNK)，执行存储于加密的内容文件 602 中的、对应于服务的 EKB [EKB (S)]的过程（解密），从而得到以这样方式设置的根密钥 Kroot，以便与存储于对应于服务的 EKB [EKB (S)]的对应于服务的目录树相对应。

接着，在步骤 S704，通过使用从对应于服务的 EKB [EKB (S)]提取的根密钥 Kroot，执行解密存储于加密的内容文件 602 中的加密的数据 E (Kroot, CID+Kc)的过程，从而得到内容 ID (CID)和内容密钥(Kc)。

接着，在步骤 S705，执行匹配（比较）从加密的内容文件 602 提取的内容 ID (CID)和存储于使用权信息中的内容 ID (CID)的过程。当在匹配过程中确认内容可以使用时，在步骤 S706，通过使用从加密的内容文件 602 提取的内容密钥(Kc)，解密存储于加密的内容文件 602 中的加密的内容 E (Kc, Content)以播放内容。

如上所述，用作对应于目录树的 EKB 的、对应于硬件的 EKB [EKB (H)]以及用作对应于目录树的 EKB 的、对应于软件的 EKB [EKB (S)]分别提供给用户，其中，EKB [EKB (H)]以这样的方式设置以便对应于作为内容使用设备的硬件，而 EKB [EKB (S)]以这样的方式设置以便对应于使用服务的内容。因此，只有对于每个 EKB 具有合法的 DNK 的用户可以使用服务。

可以提供用于解密对应于服务的 EKB [EKB (S)]的 DNK，即 SDNK，作为对应于内容的服务数据 601，并且使用根密钥 Kroot'加密 SDNK，其中，该根密钥 Kroot'以这样的方式设置以便与对应于硬件的目录树相对应，只有具

有对应于硬件的合法的 DNK，即 HDNK 的设备可以得到该 SDNK。因此，只有具有合法的 HDNK 的用户设备可以得到 SDNK 并且可以使用服务。

在使用内容中，执行匹配从加密的内容文件 602 获得的内容识别符(CID)和从使用权信息得到的 CID 的过程。因此，使下面的事实变为可能：得到使用权信息 603，并且存储 CID 信息作为内容播放过程的不可缺少的条件，并且实现根据使用条件的内容使用。

在前述中，当涉及具体实施例时，已经详细地描述了本发明。但是，无需说明，本领域技术人员可以修改或替代这些实施例而不脱离本发明的精神和范围。也就是，本发明已经以例举形式公开，并且不应该视为限制于这些例子。为确定本发明的实质，应该考虑所附的权利要求。

可以用硬件、软件或它们的结合的配置执行本说明书中描述的系列过程。当过程要由软件执行时，记录处理顺序的程序可以安装到集成为专用硬件的计算机的存储器中，由此执行程序，或者程序可以安装到能够执行各种处理的通用计算机中，由此执行程序。

例如，可以预先在作为记录媒体的硬盘和 ROM（只读存储器）中记录程序。或者，可以在可移除记录媒体中暂时或永久地存储（记录）程序，可移除记录媒体例如软盘、CD-ROM（紧凑盘只读存储器）、MO（磁光）盘、DVD（数字多用途盘）、磁盘或半导体存储器。可以提供这样的可移除记录媒体作为所谓的包式软件。

除了从如所述那些可移除记录媒体安装到计算机，程序还可以以无线的方式从下载站点传送，或者可以通过如 LAN（局域网）或因特网的网络有线传送到计算机，并且计算机可能接收以这样的方式传送的程序并安装程序到包含于其中的硬盘。

本说明书中描述的各种过程不仅可以根据描述按时间顺序执行，而且可以根据执行过程的装置的处理性能或必要时，并发或单独地执行。

产业上的可利用性

如已经这样描述的，根据本发明的配置，在信息记录媒体如 CD 中，设置第一数据存储区域和第二数据存储区域作为不同的会话区域，第一数据存储区域设置为执行复制防止过程的内容存储区域；第二数据存储区域是这样的内容存储区域：其上不执行复制防止过程，并且其中存储包含加密的内容

和加密的密钥数据的加密的内容文件，使得对在加密的内容的解密过程中使用的密钥数据加密，并且它仅能在具有许可的设备中解密。因此，在播放设备如 CD 播放器中，播放第一数据记录域的记录的内容是可能的；并且甚至在能够进行复制和剥离处理的信息处理设备如 PC 中，在得到许可的条件下，解密或播放第二数据记录域的加密的内容也是可能的。

根据本发明的配置，存储于第二数据存储区域的加密的内容文件中的加密的内容是这样的内容：它使用用作加密处理密钥的内容密钥 Kc 加密，并且设置内容密钥 Kc 为可以通过执行这样的过程得到的密钥，该过程包括基于利用密钥分配树结构提供的密钥数据、解密使能密钥块(EKB)的过程。因此，在严格的许可管理下，内容使用的管理变为可能。

根据本发明的配置，标识符数据(PID)存储于第二数据存储区域，该标识符数据包含：媒体 ID，用作对信息记录媒体唯一的标识符；和 MAC，用作变化验证数据，所以，当发行许可时，执行使用 MAC 验证的变化验证。因此，可能消除得到非法的许可的可能性。

根据本发明的配置，用作标识符的产品 ID 存储于第二数据存储区域，该产品 ID 为对应于多个信息记录媒体的集合的每个产品设置；并且媒体 ID 和产品 ID 的结合数据设置为全局唯一标识符。因此，可能可靠和有效地执行许可发行管理。

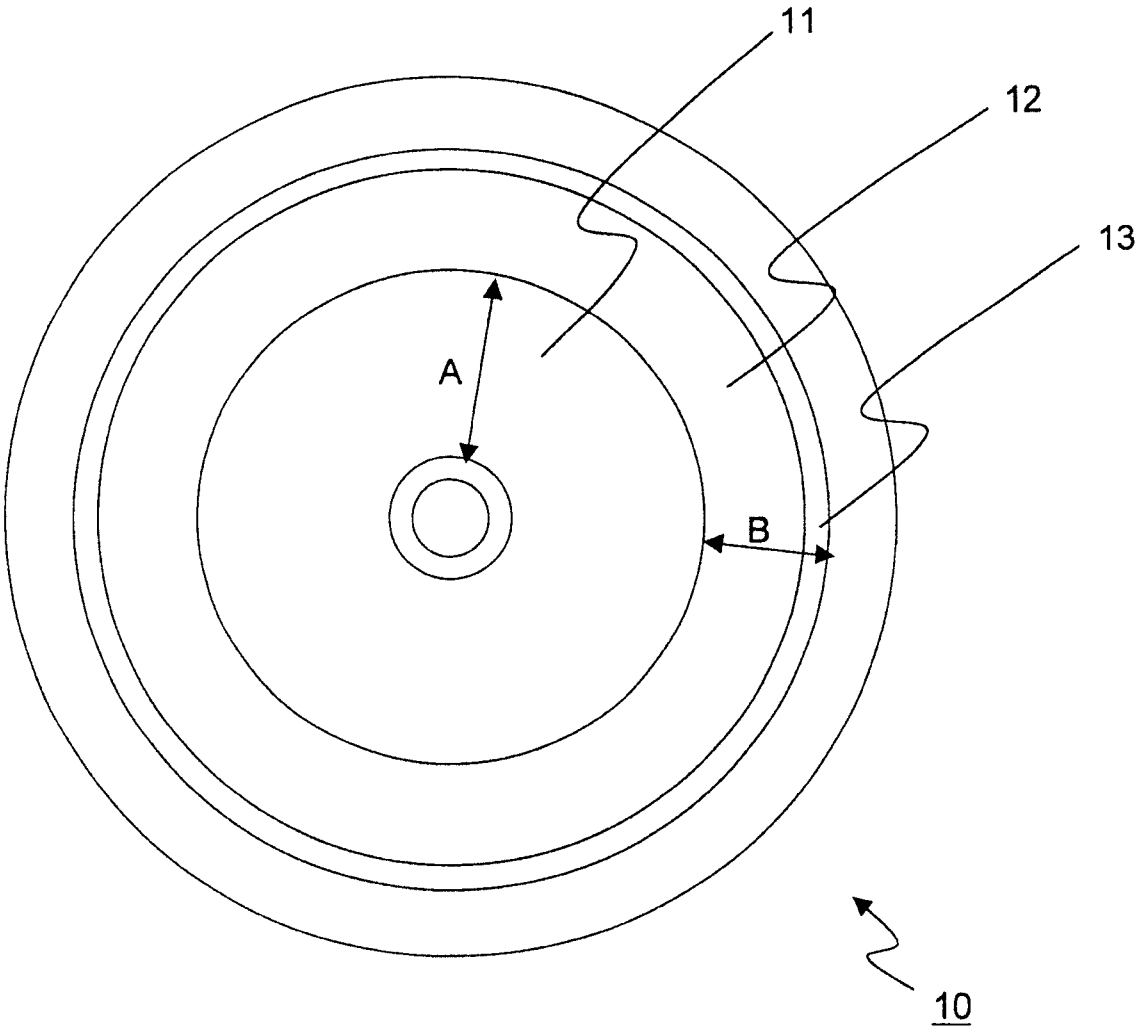


图 1

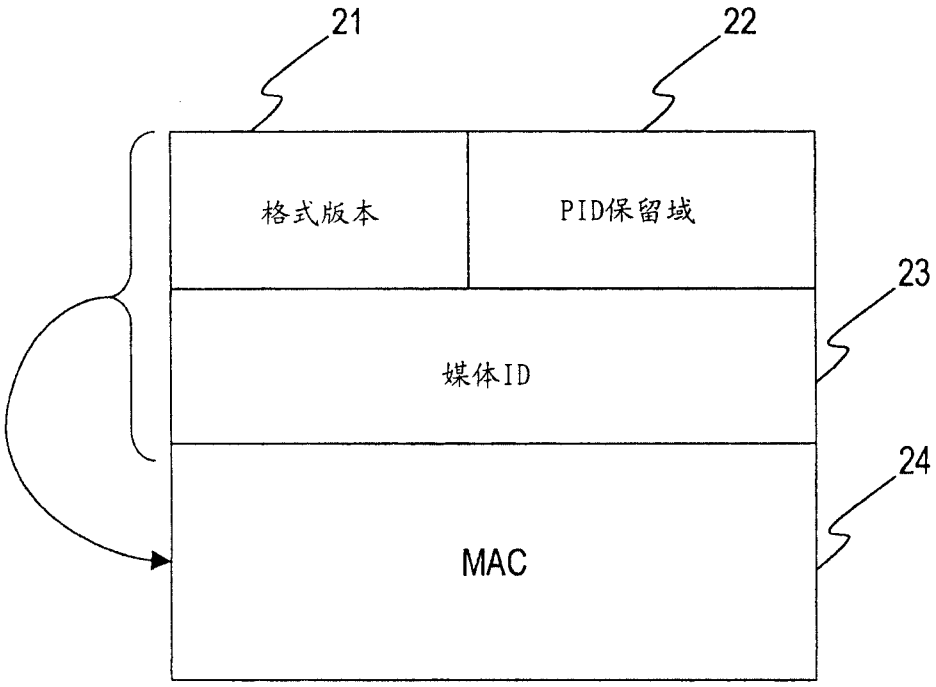


图 2

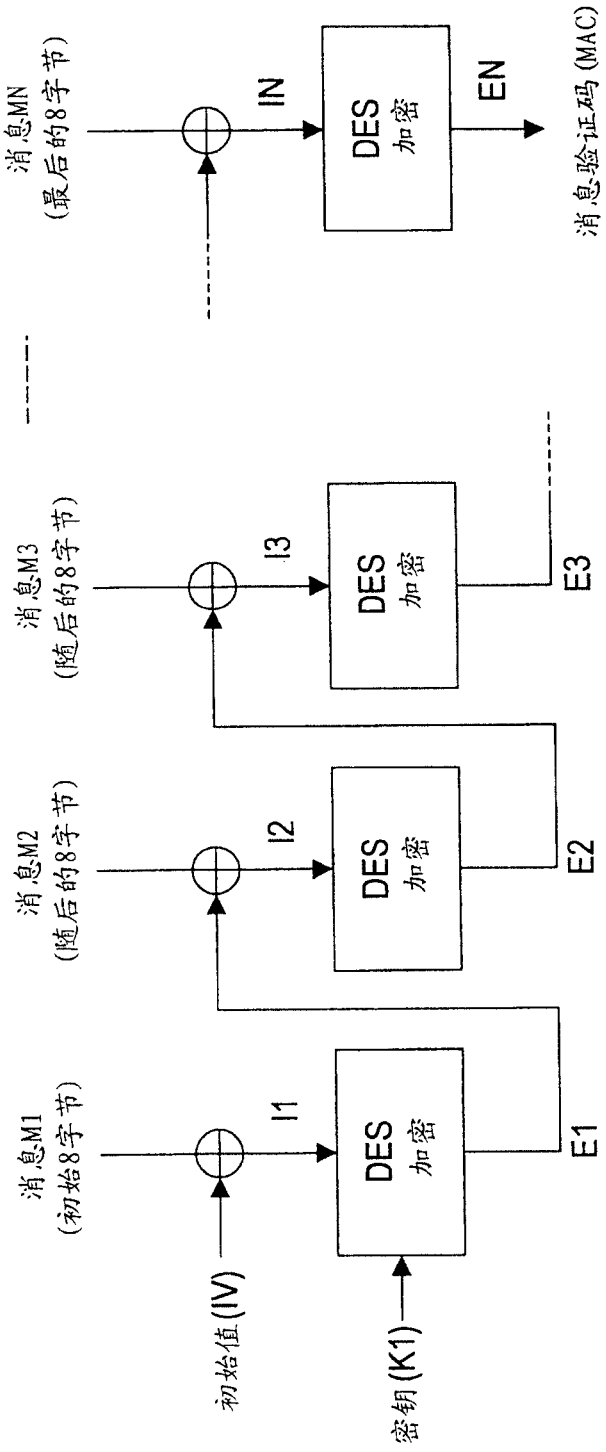

消息M1
(初始8字节)
消息M2
(随后的8字节)
消息M3
(随后的8字节)
消息MN
(最后的8字节)
初始值(IV)
密钥(K1)
I1
I2
I3
IN
DES
加密
E1
E2
E3
EN
消息验证码(MAC)
⊕：异或过程(以8字节为单位)

图 3

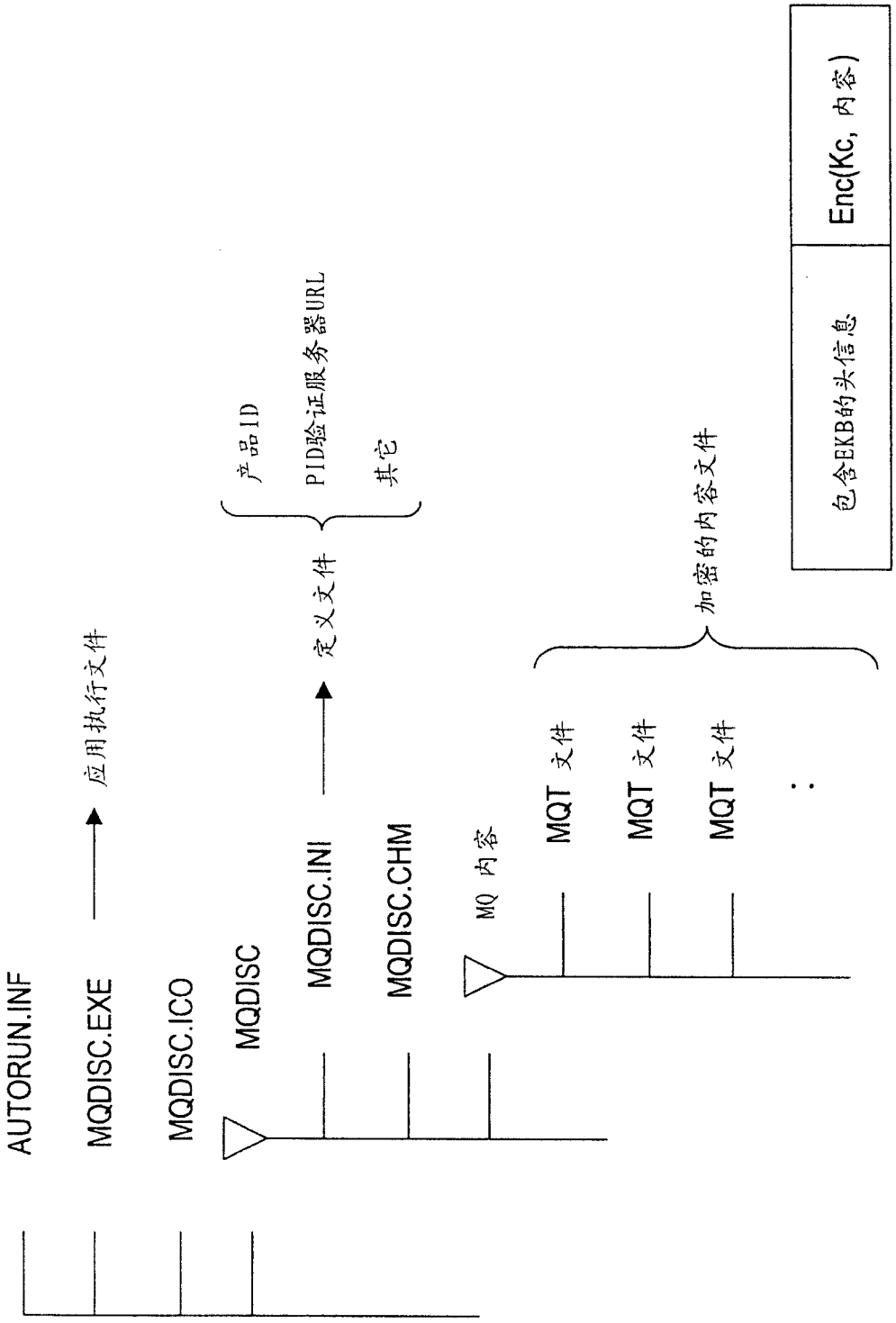

AUTORUN.INF
MQDISC.EXE
应用执行文件
MQDISC.ICO
MQDISC
MQDISC.INI
定义文件
产品ID
PID验证服务器URL
其它
MQDISC.CHM
MQ 内容
MQT 文件
MQT 文件
MQT 文件
加密的内容文件
包含EKB的头信息
Enc(Kc, 内容)

图 4

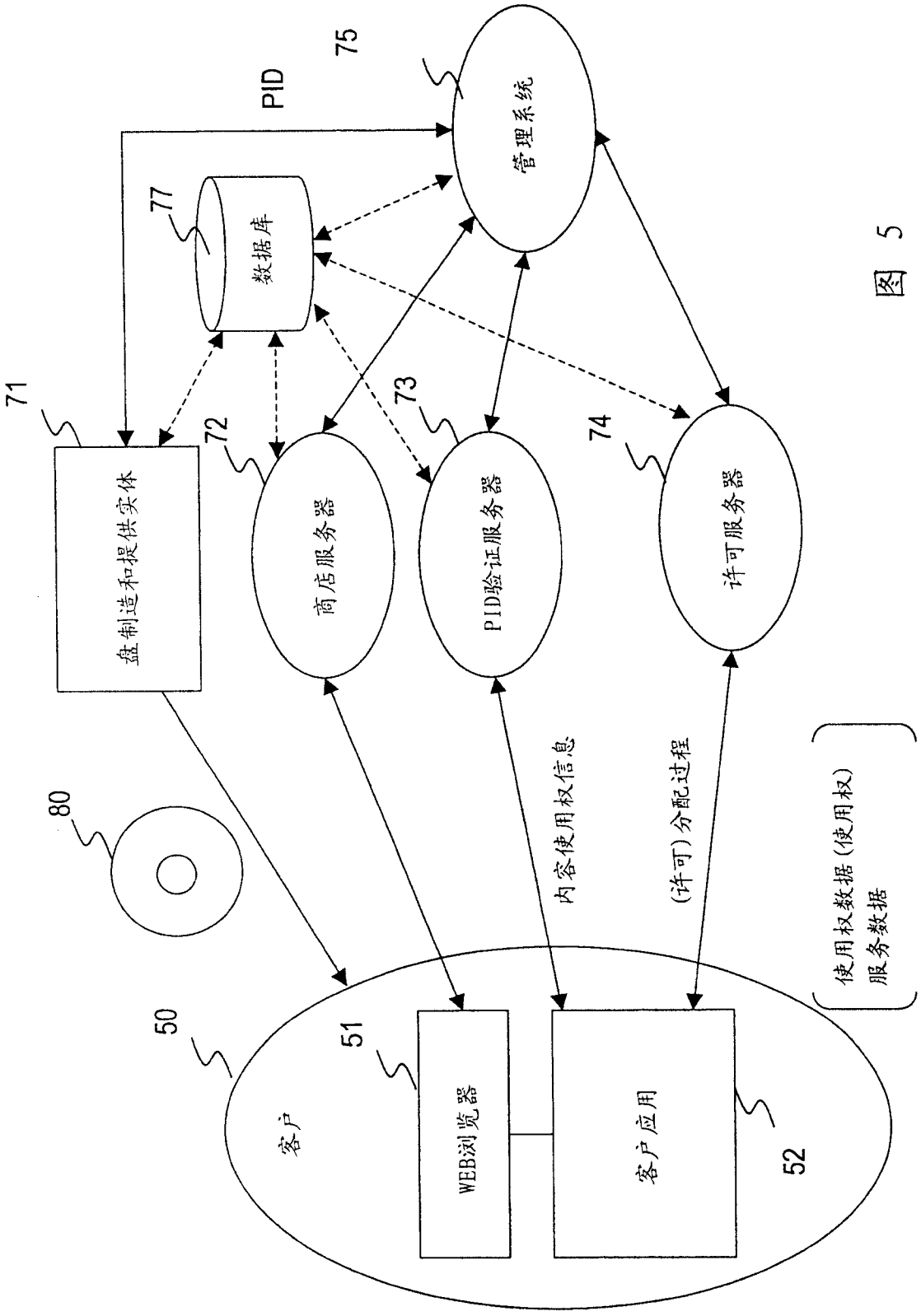

75
PID
管理系统
77
数据库
71
盘制造和提供实体
72
商店服务器
73
PID验证服务器
74
许可服务器
80
50
客户
51
WEB浏览器
客户应用
52
内容使用权信息
(许可)分配过程
使用权数据(使用权)
服务数据

图 5

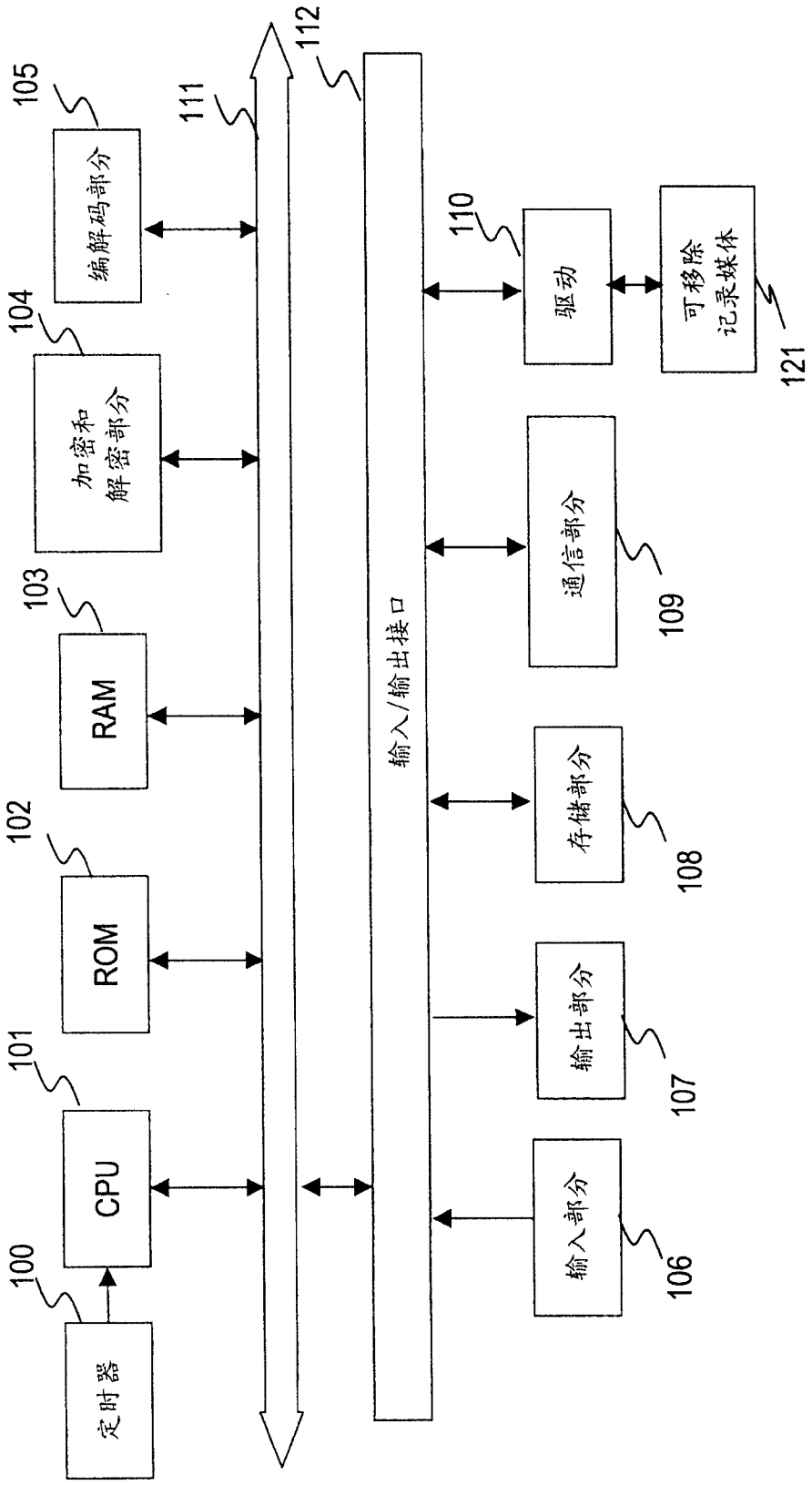

定时器
CPU
ROM
RAM
加密和解密部分
编解码部分
输入/输出接口
输入部分
输出部分
存储部分
通信部分
驱动
可移除记录媒体
100
101
102
103
104
105
106
107
108
109
110
111
112
121

图 6

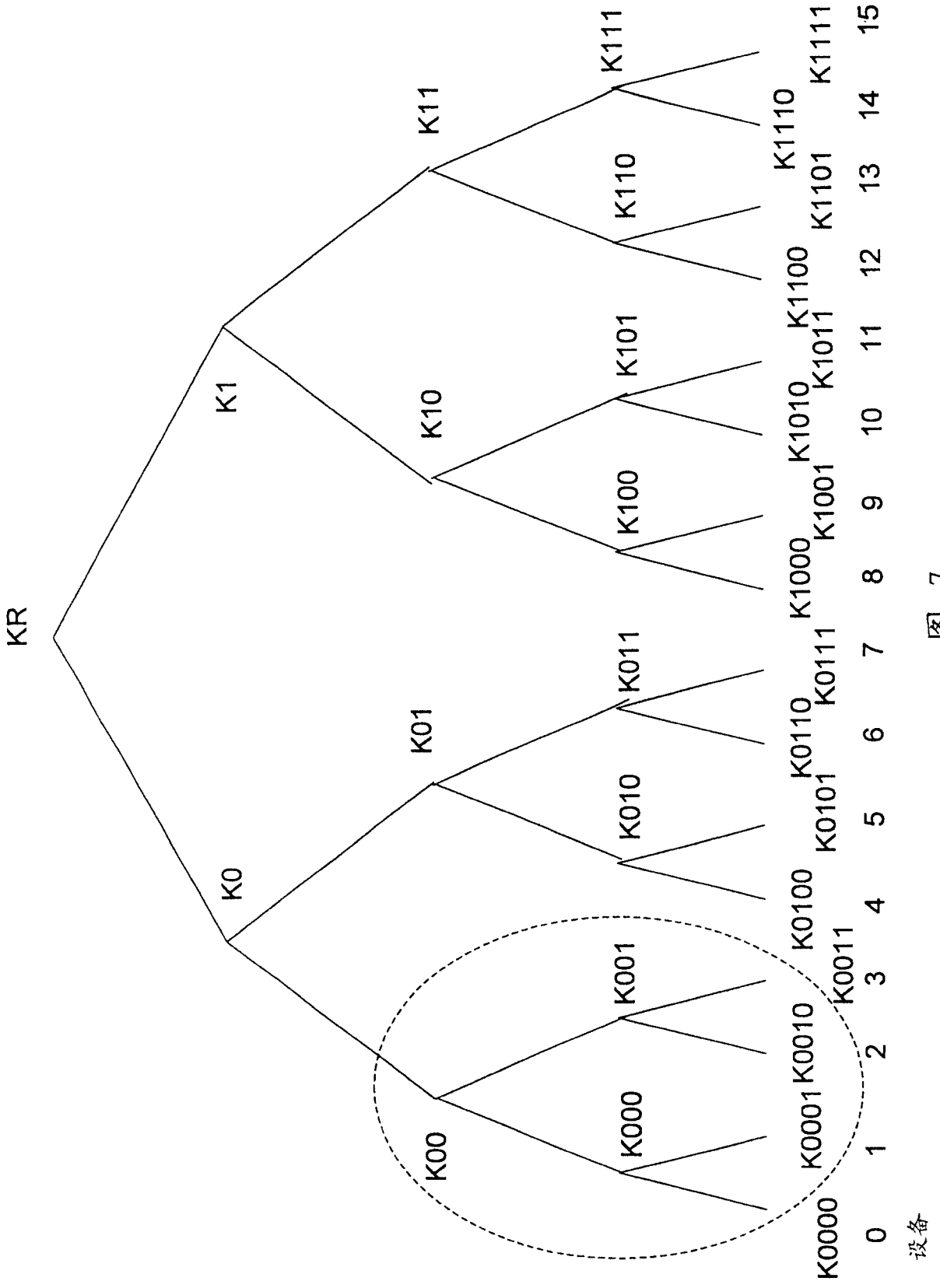

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
设备

图 7

(A) 使能密钥块(EKB) 例1

发送版本: t的节点密钥到设备0、1和2

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)

(A) 使能密钥块(EKB) 例2

发送版本: t的节点密钥到设备0、1和2

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

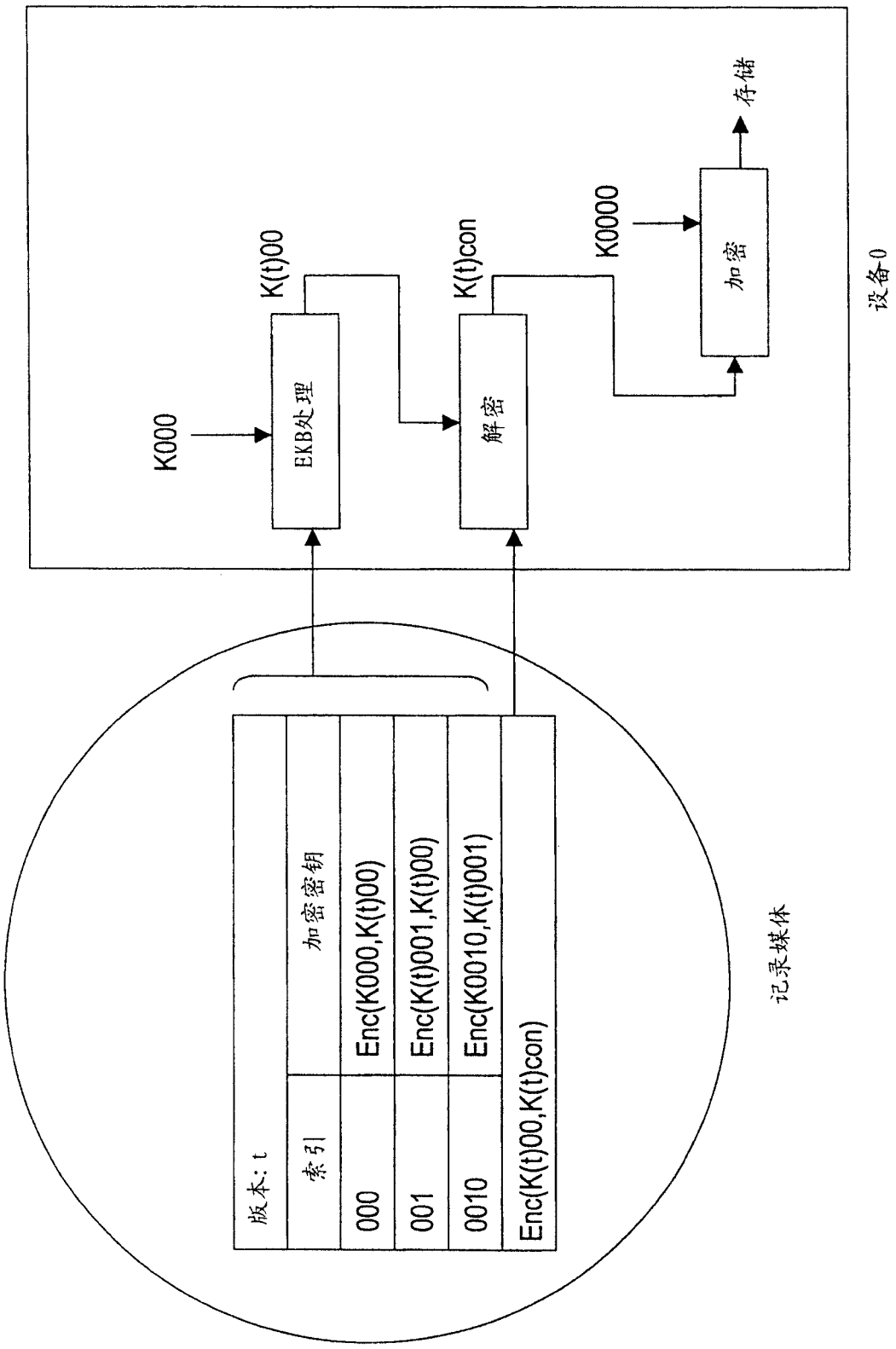

K000
EKB处理
K(t)00
解密
K(t)con
K0000
加密
存储
设备0
记录媒体
版本：t
索引
加密密钥
000
Enc(K000,K(t)00)
001
Enc(K(t)001,K(t)00)
0010
Enc(K0010,K(t)001)
Enc(K(t)00,K(t)con)

图 9

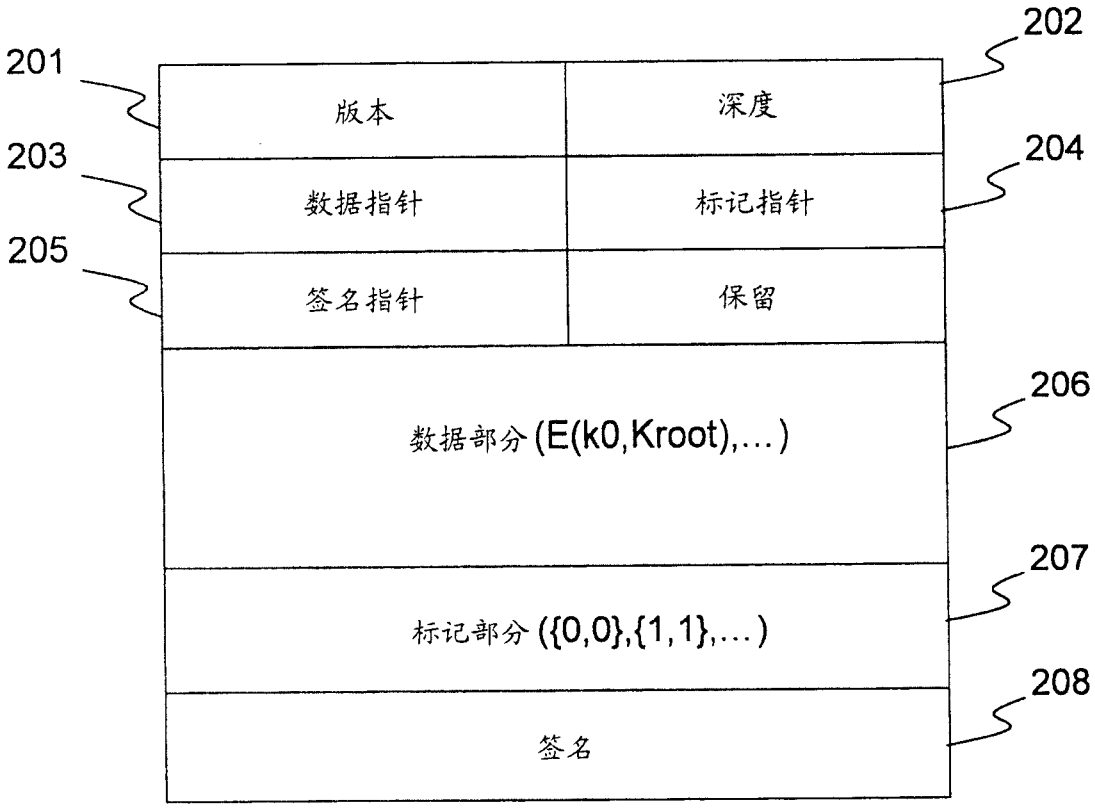

201
202
203
204
205
206
207
208
版本
深度
数据指针
标记指针
签名指针
保留
数据部分 (E(k0,Kroot),...)
标记部分 ({0,0},{1,1},...)
签名

图 10

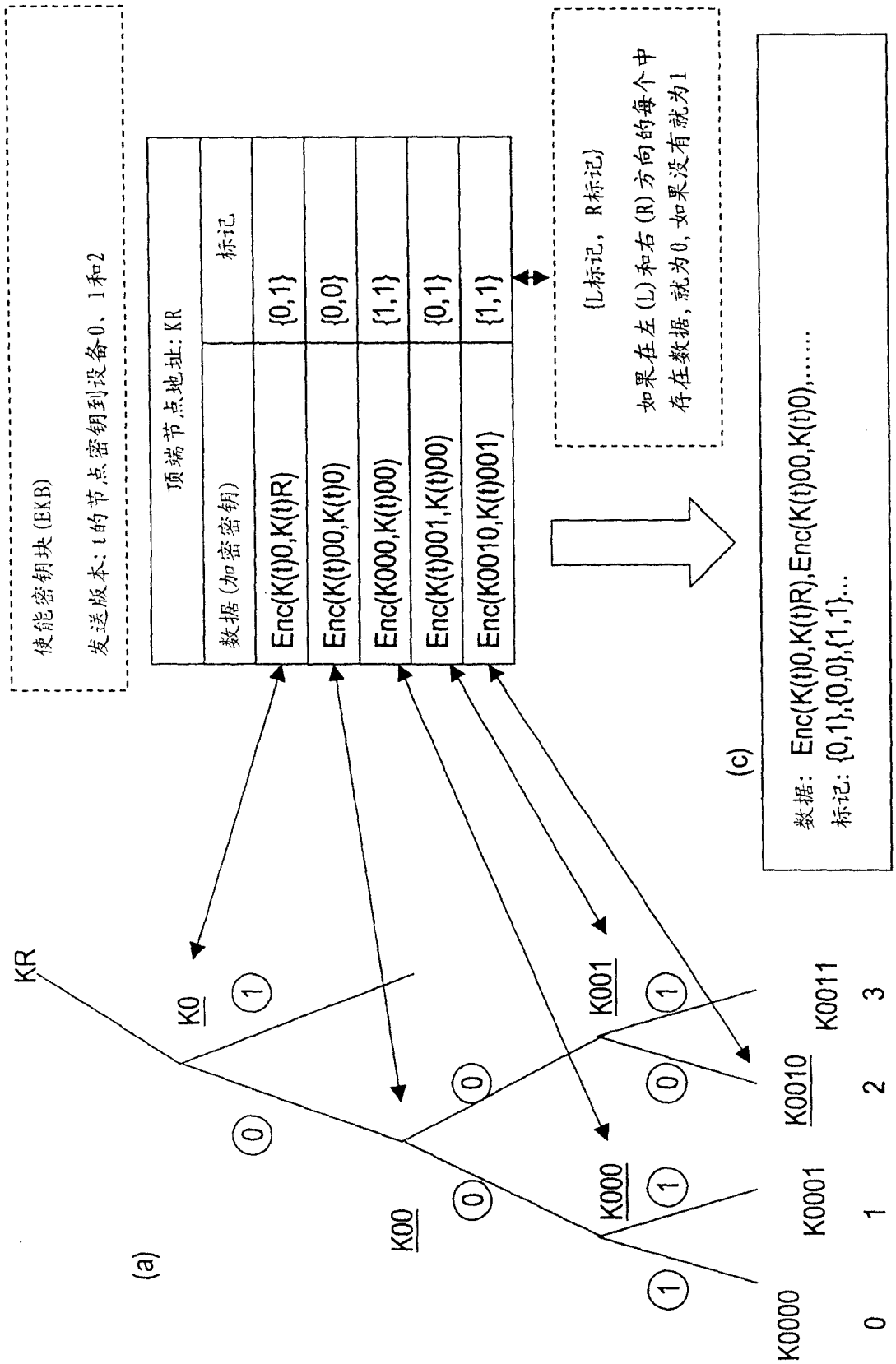

(a)
KR
K0
K00
K000
K0000
K0001
K001
K0010
K0011
0
1
2
3
(b)
使能密钥块(EKB)
发送版本：t的节点密钥到设备0、1和2
顶端节点地址：KR
数据(加密密钥)
标记
Enc(K(t)0,K(t)R)
{0,1}
Enc(K(t)00,K(t)0)
{0,0}
Enc(K000,K(t)00)
{1,1}
Enc(K(t)001,K(t)00)
{0,1}
Enc(K0010,K(t)001)
{1,1}
{L标记，R标记}
如果在左(L)和右(R)方向的每个中存在数据，就为0，如果没有就为1
(c)
数据：Enc(K(t)0,K(t)R),Enc(K(t)00,K(t)0),.....
标记：{0,1},{0,0},{1,1}...

图 11

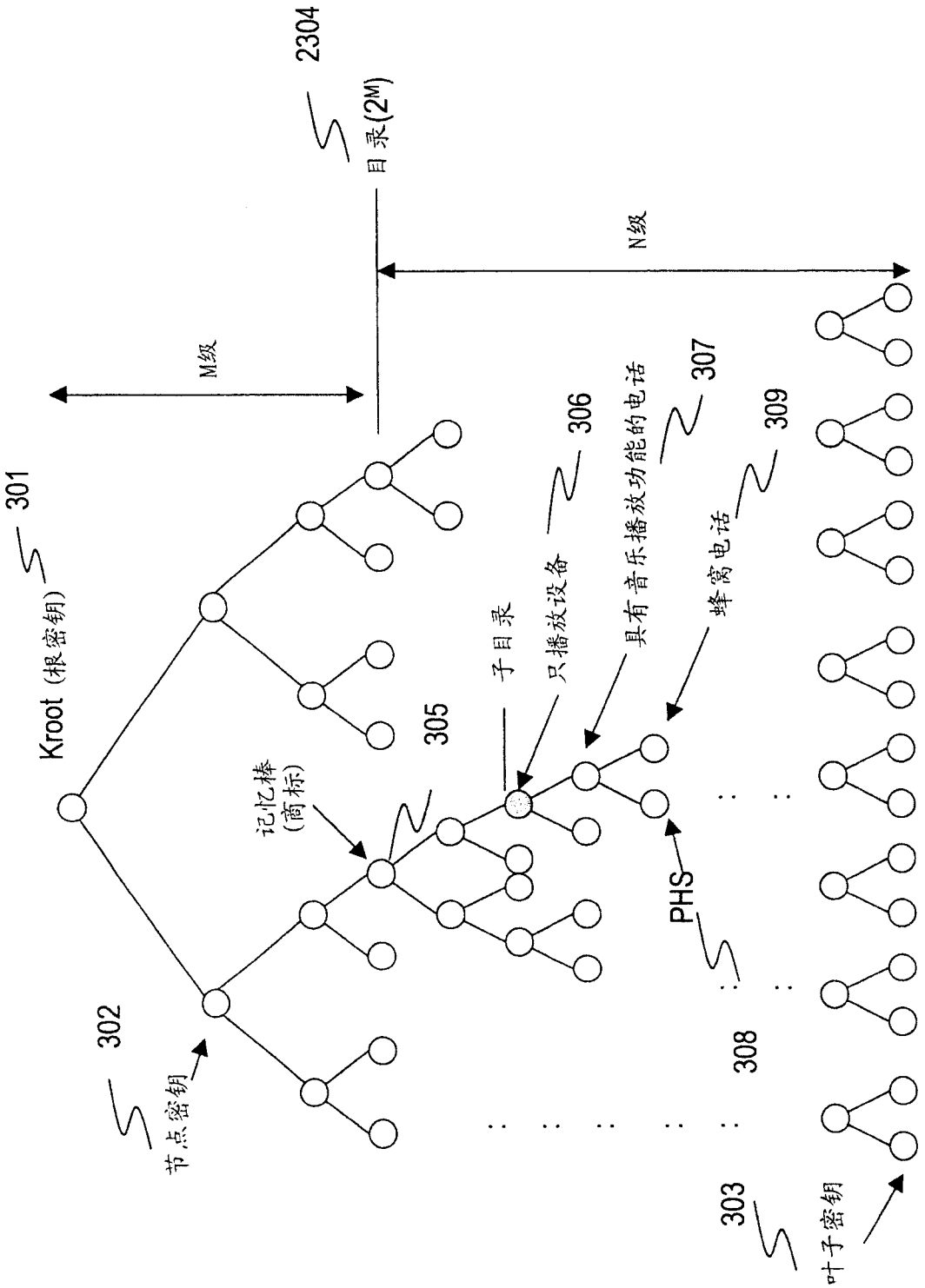

2304
目录(2M)
M级
N级
301
Kroot (根密钥)
302
节点密钥
记忆棒
(商标)
305
子目录
只播放设备
306
具有音乐播放功能的电话
307
蜂窝电话
309
PHS
308
303
叶子密钥

图 12

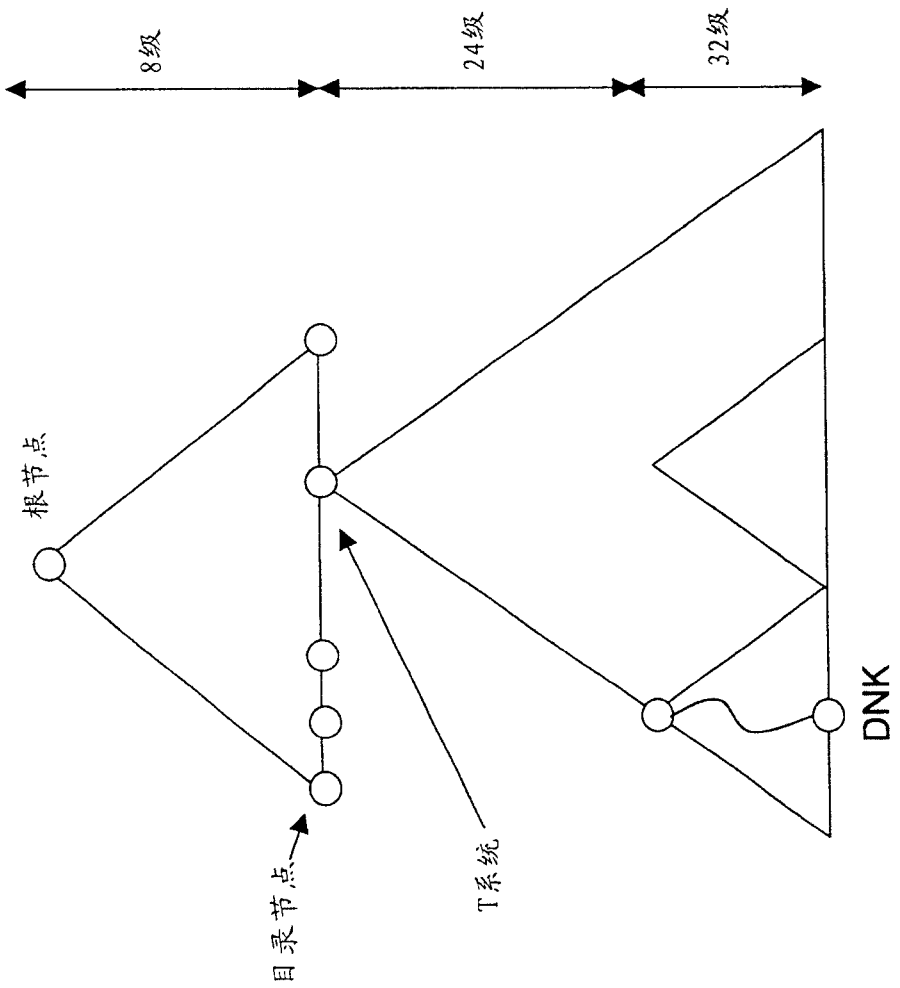


图 13

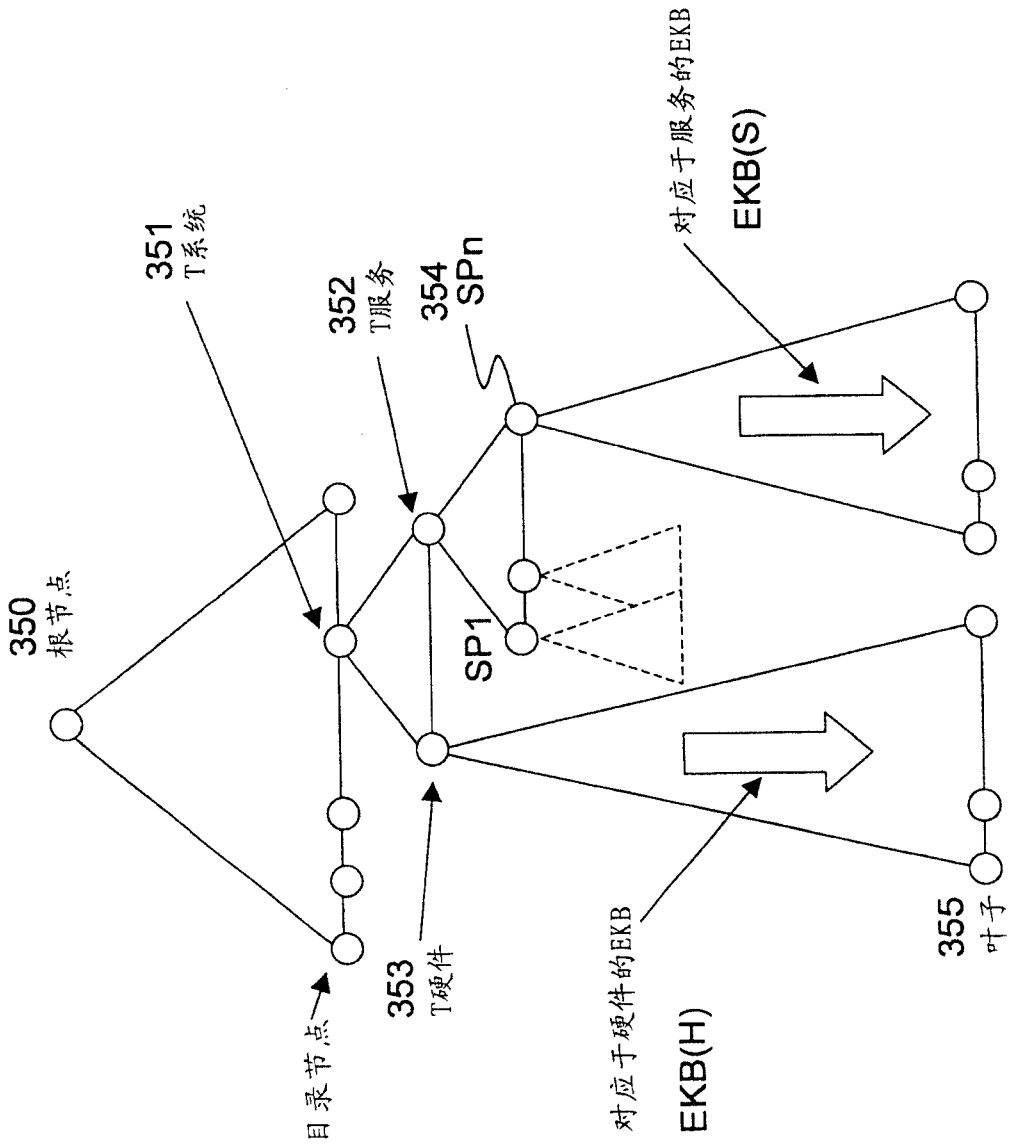

350
根节点
351
T系统
352
T服务
354
SPn
SP1
353
T硬件
目录节点
对应于硬件的EKB
EKB(H)
对应于服务的EKB
EKB(S)
355
叶子

图 14

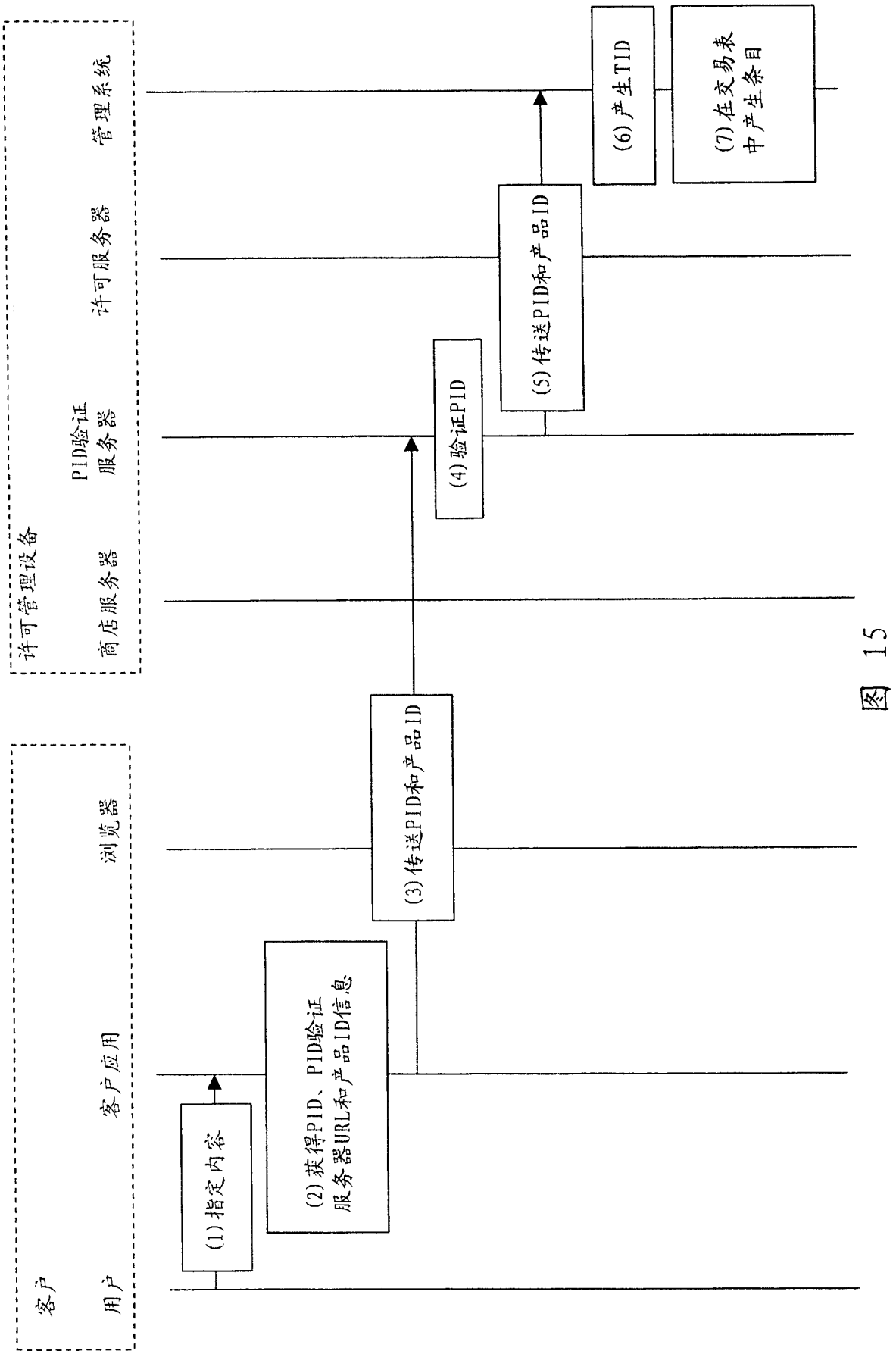

客户
用户
客户应用
浏览器
许可管理设备
商店服务器
PID验证
服务器
许可服务器
管理系统
(1)指定内容
(2)获得PID、PID验证
服务器URL和产品ID信息
(3)传送PID和产品ID
(4)验证PID
(5)传送PID和产品ID
(6)产生TID
(7)在交易表
中产生条目

图 15

专辑主表			
产品ID	PID密钥	标题	艺术家
P-1	0123456A	专辑A	艺术家A
P-2	B0123456	专辑B	艺术家B

图 16

交易表			
TID	产品ID	PID(媒体 ID)	价格
T-1	P-1	PID1-001	300
T-3	P-2	PID2-004	500

图 17

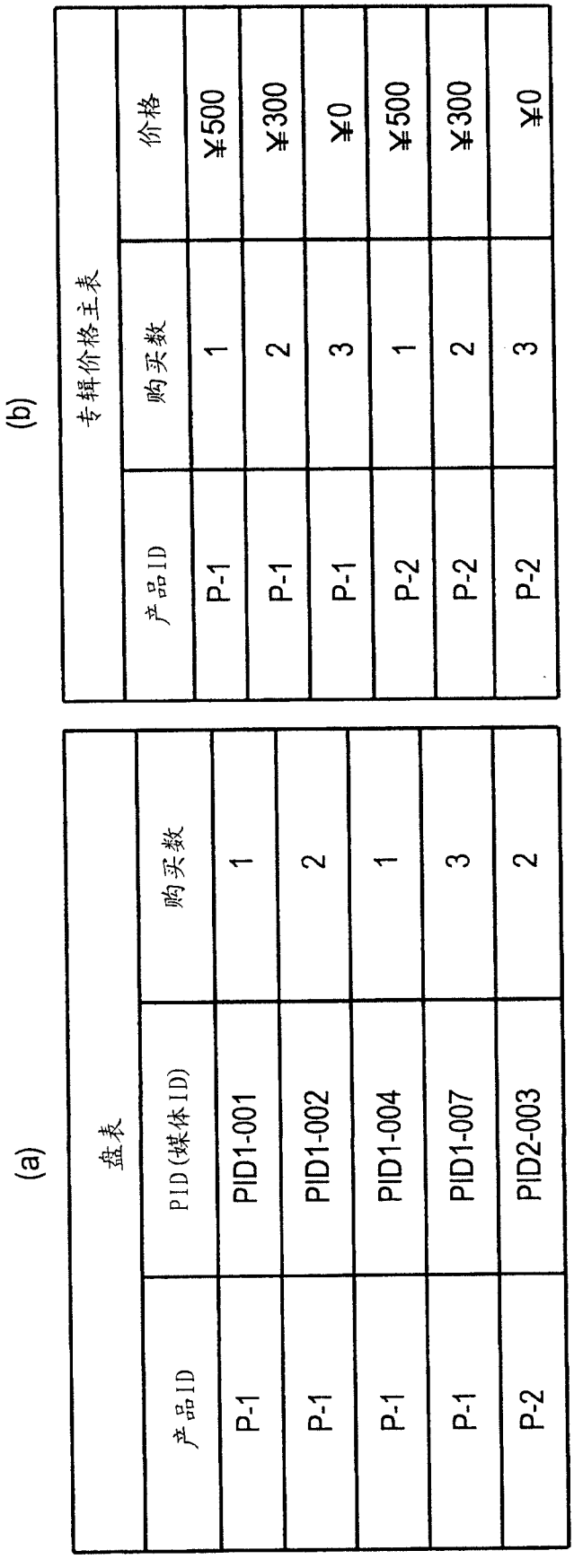

(a)
盘表
产品ID
P-1
P-1
P-1
P-1
P-2
PID(媒体ID)
PID1-001
PID1-002
PID1-004
PID1-007
PID2-003
购买数
1
2
1
3
2
(b)
专辑价格主表
产品ID
P-1
P-1
P-1
P-2
P-2
P-2
购买数
1
2
3
1
2
3
价格
¥500
¥300
¥0
¥500
¥300
¥0

图 18

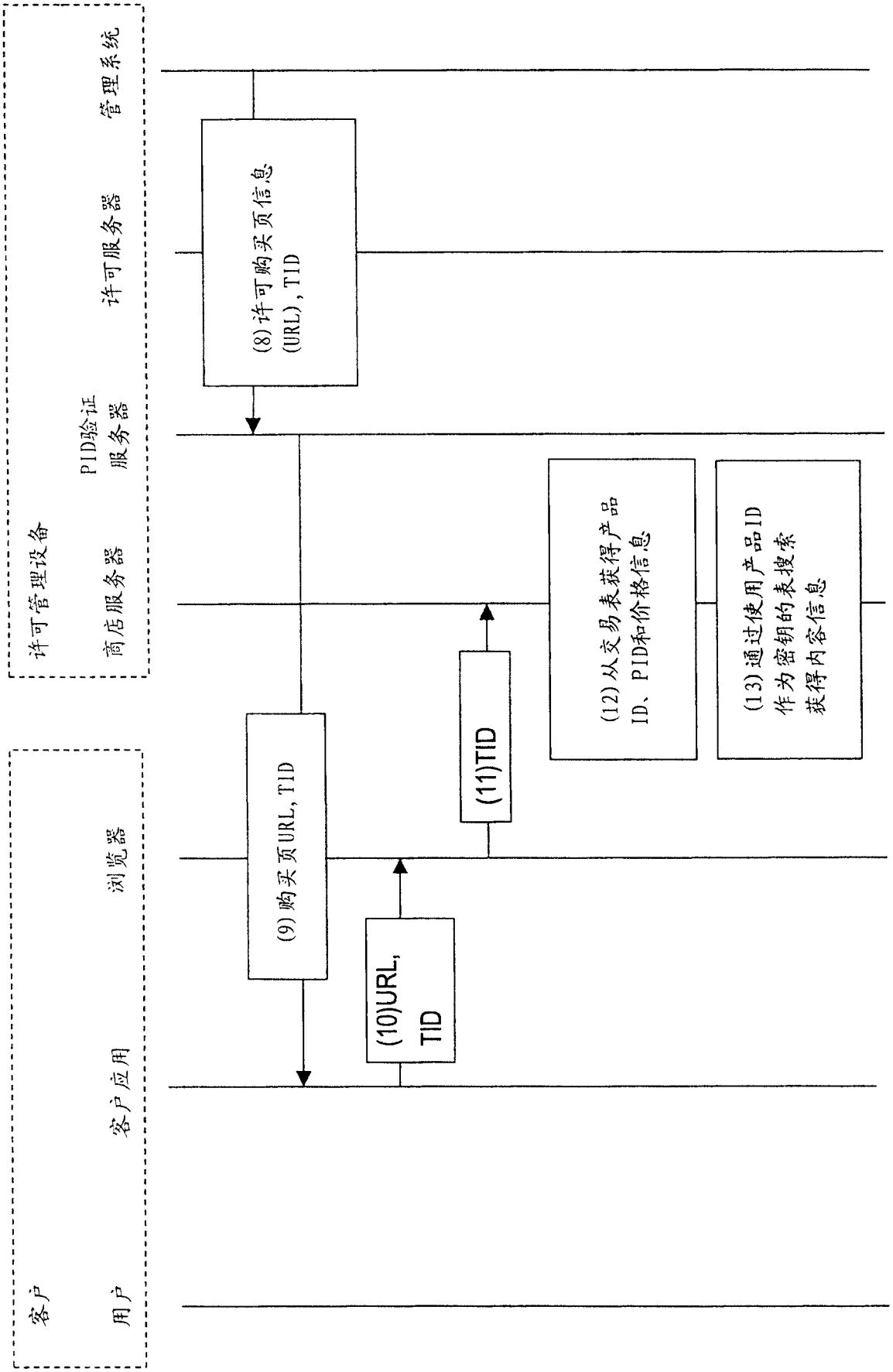

客户
用户
客户应用
浏览器
许可管理设备
商店服务器
PID验证
服务器
许可服务器
管理系统
(8)许可购买页信息
(URL)，TID
(9)购买页URL，TID
(10)URL，
TID
(11)TID
(12)从交易表获得产品
ID、PID和价格信息
(13)通过使用产品ID
作为密钥的表搜索
获得内容信息

图 19

轨道表		
内容号	产品ID	标题
P-1-1	P-1	内容 A
P-1-2	P-1	内容 B
P-1-3	P-1	内容 C
P-2-1	P-2	*Kana AIUEO*

图 20

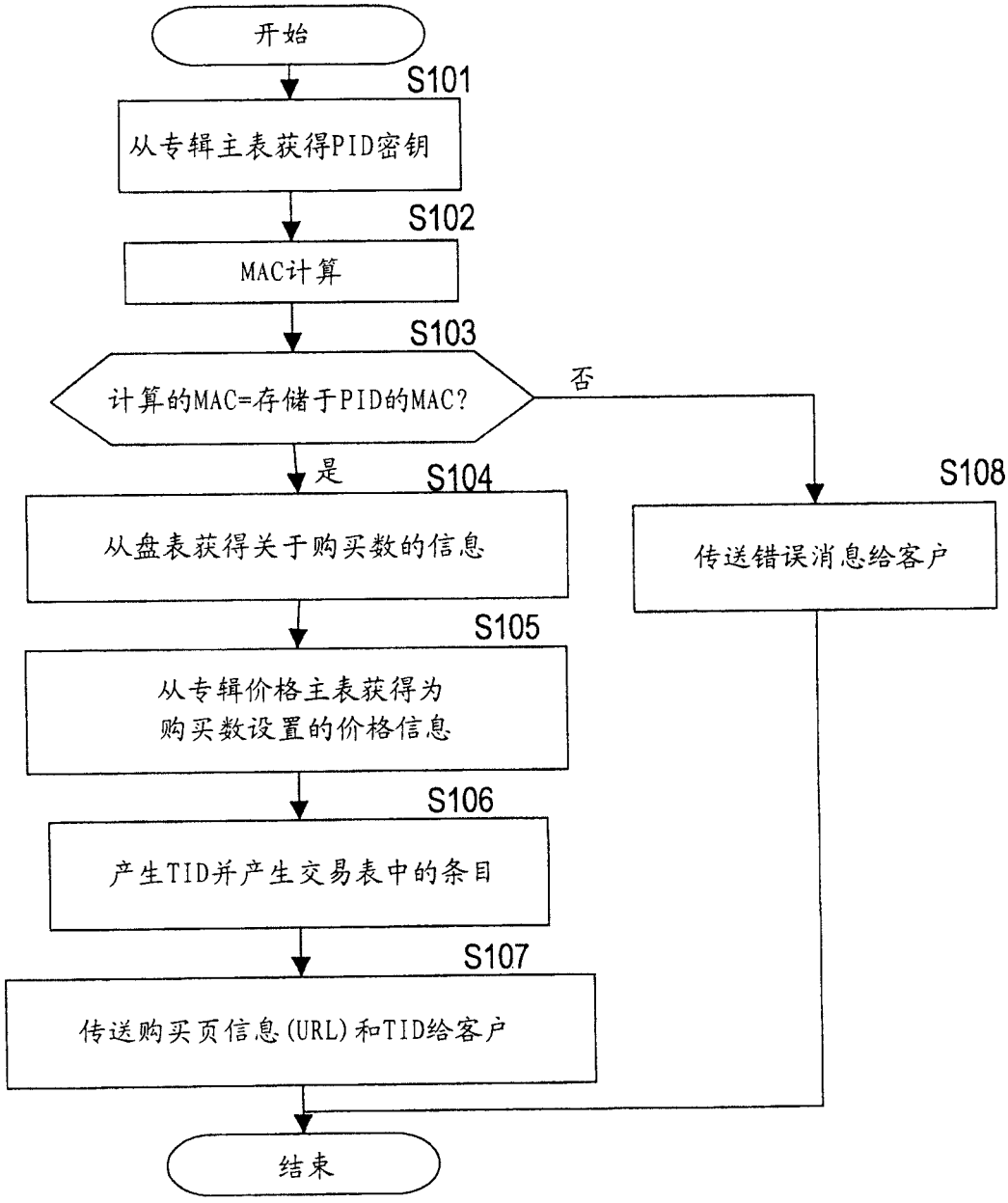

开始
S101
从专辑主表获得PID密钥
S102
MAC计算
S103
计算的MAC=存储于PID的MAC?
否
是
S104
从盘表获得关于购买数的信息
S105
从专辑价格主表获得为
购买数设置的价格信息
S106
产生TID并产生交易表中的条目
S107
传送购买页信息(URL)和TID给客户
S108
传送错误消息给客户
结束

图 21

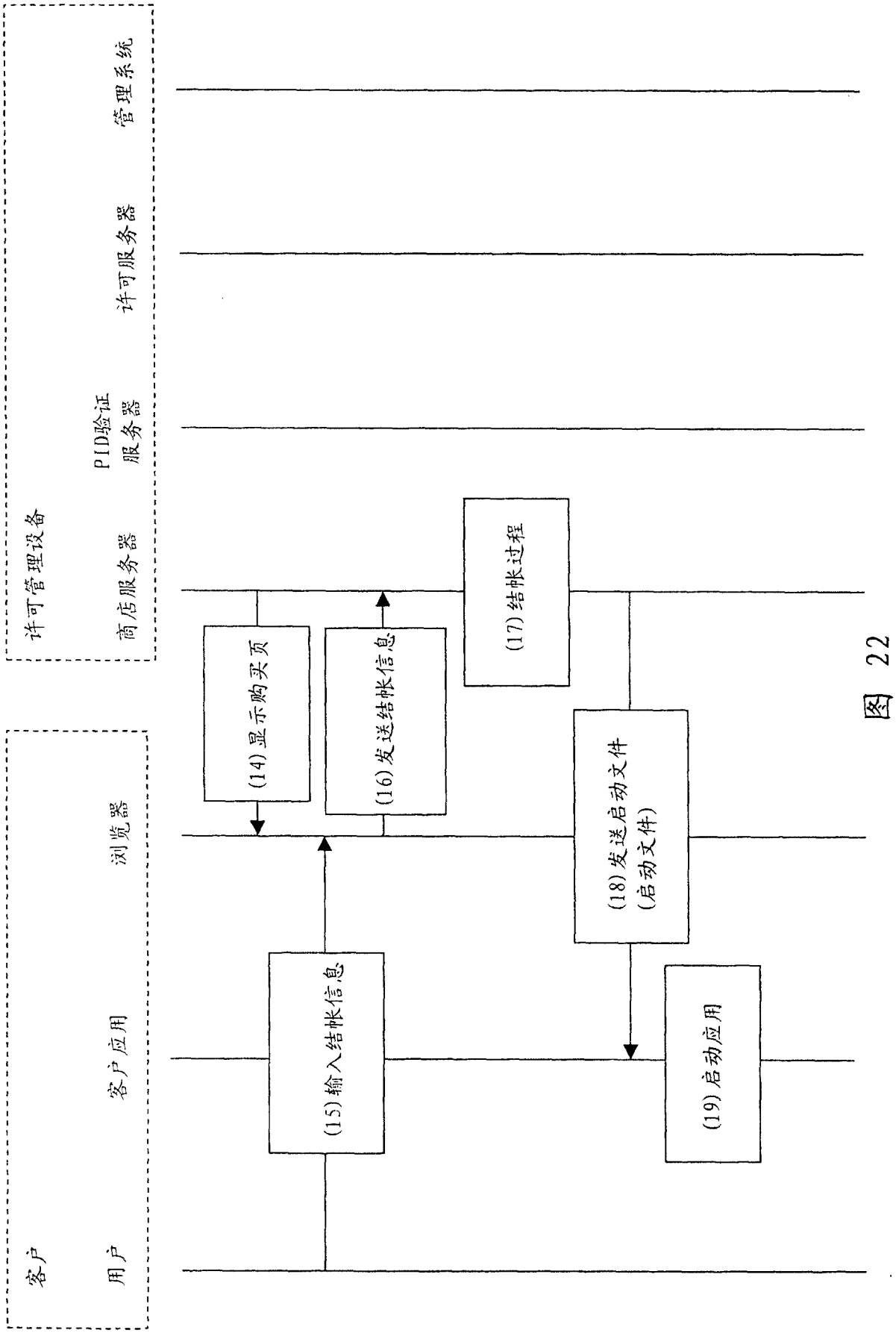

客户
用户
客户应用
浏览器
许可管理设备
商店服务器
PID验证服务器
许可服务器
管理系统
(14)显示购买页
(16)发送结帐信息
(17)结帐过程
(15)输入结帐信息
(18)发送启动文件(启动文件)
(19)启动应用

图 22

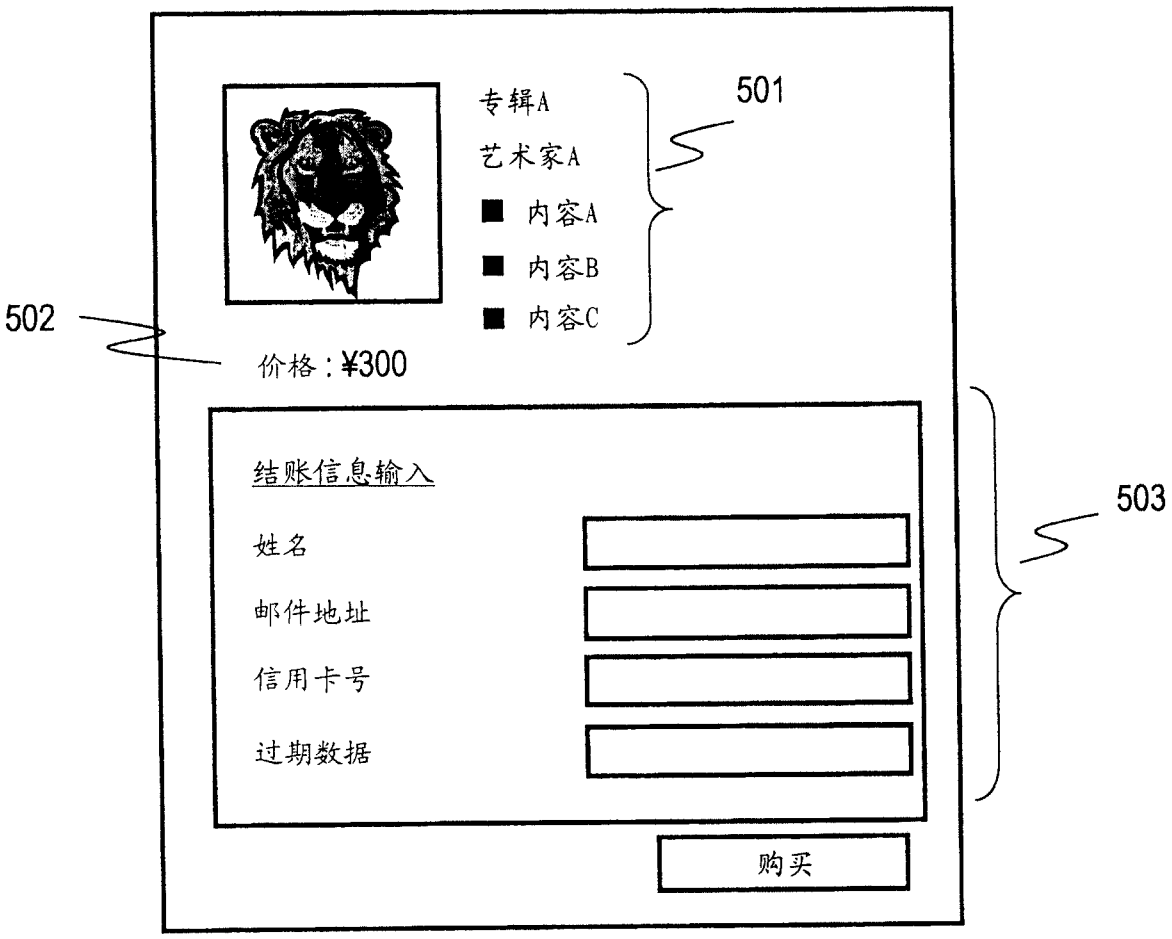

专辑A
艺术家A
内容A
内容B
内容C
501
502
价格：¥300
结账信息输入
姓名
邮件地址
信用卡号
过期数据
503
购买

图 23

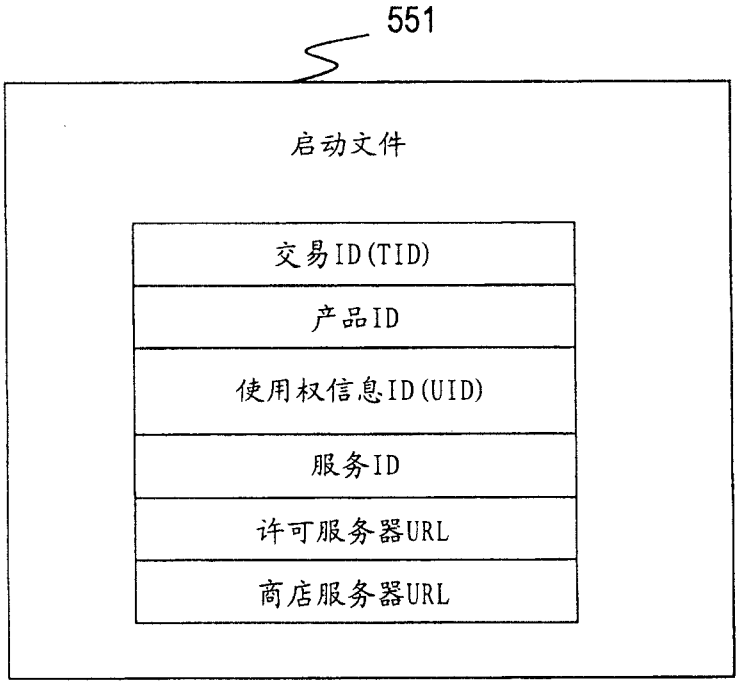


图 24

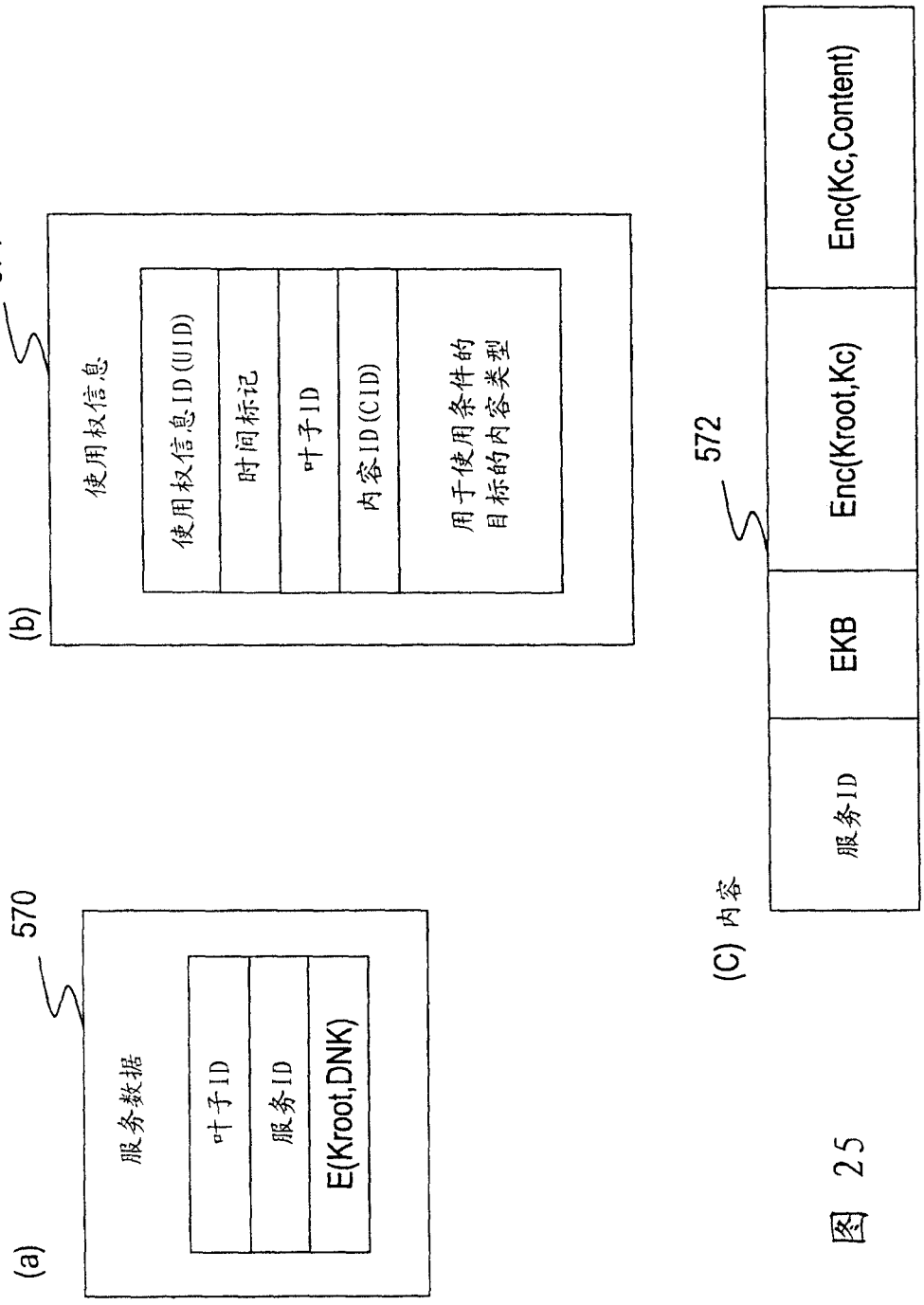

(a)
570
服务数据
叶子ID
服务ID
E(Kroot,DNK)
(b)
571
使用权信息
使用权信息ID(UID)
时间标记
叶子ID
内容ID(CID)
用于使用条件的
目标的内容类型
(C) 内容
572
服务ID
EKB
Enc(Kroot,Kc)
Enc(Kc,Content)

图 25

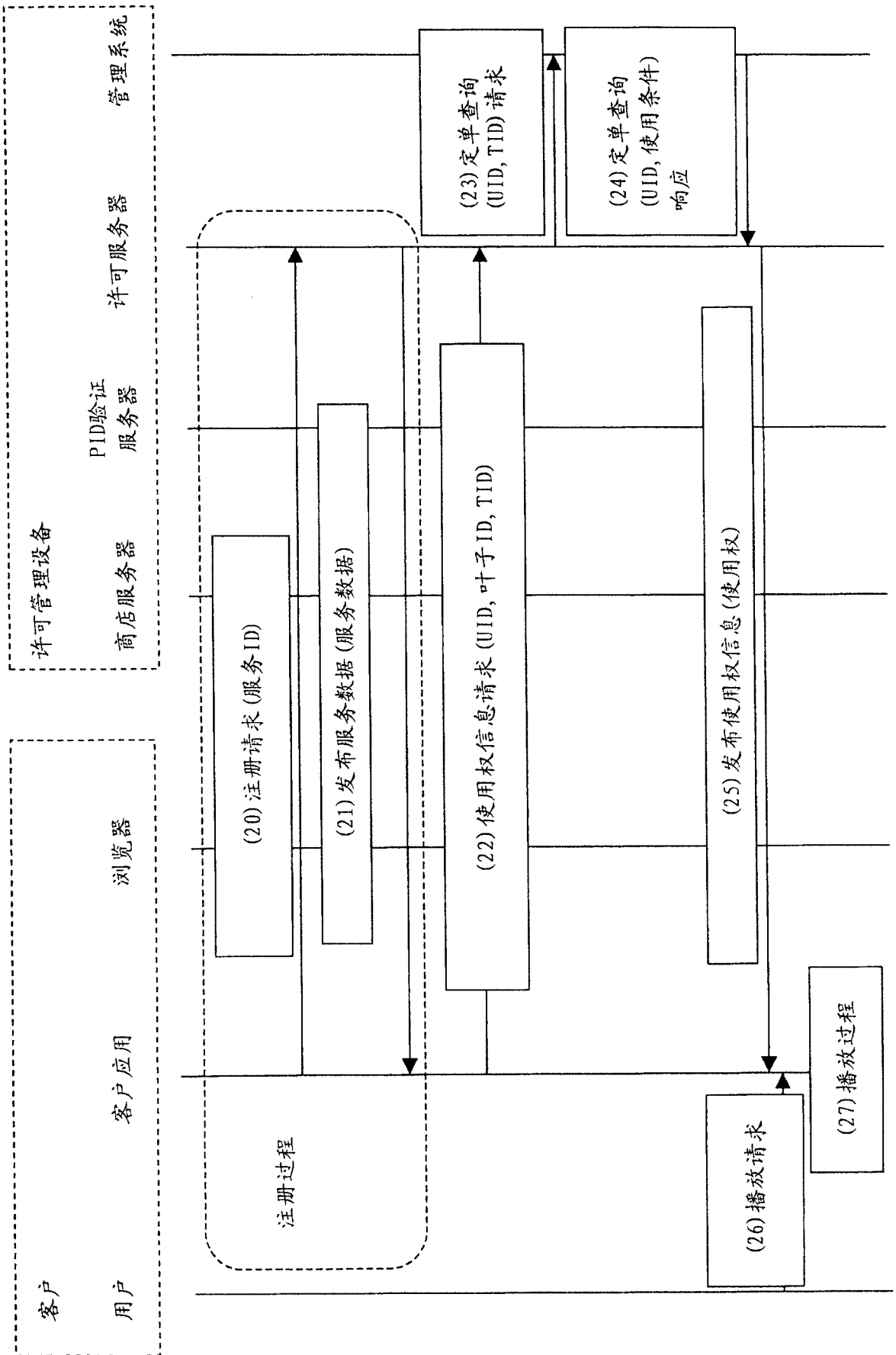

客户
用户
浏览器
客户应用
许可管理设备
商店服务器
PID验证
服务器
许可服务器
管理系统
注册过程
(20)注册请求(服务ID)
(21)发布服务数据(服务数据)
(22)使用权信息请求(UID,叶子ID,TID)
(23)定单查询
(UID,TID)请求
(24)定单查询
(UID,使用条件)
响应
(25)发布使用权信息(使用权)
(26)播放请求
(27)播放过程

图 26

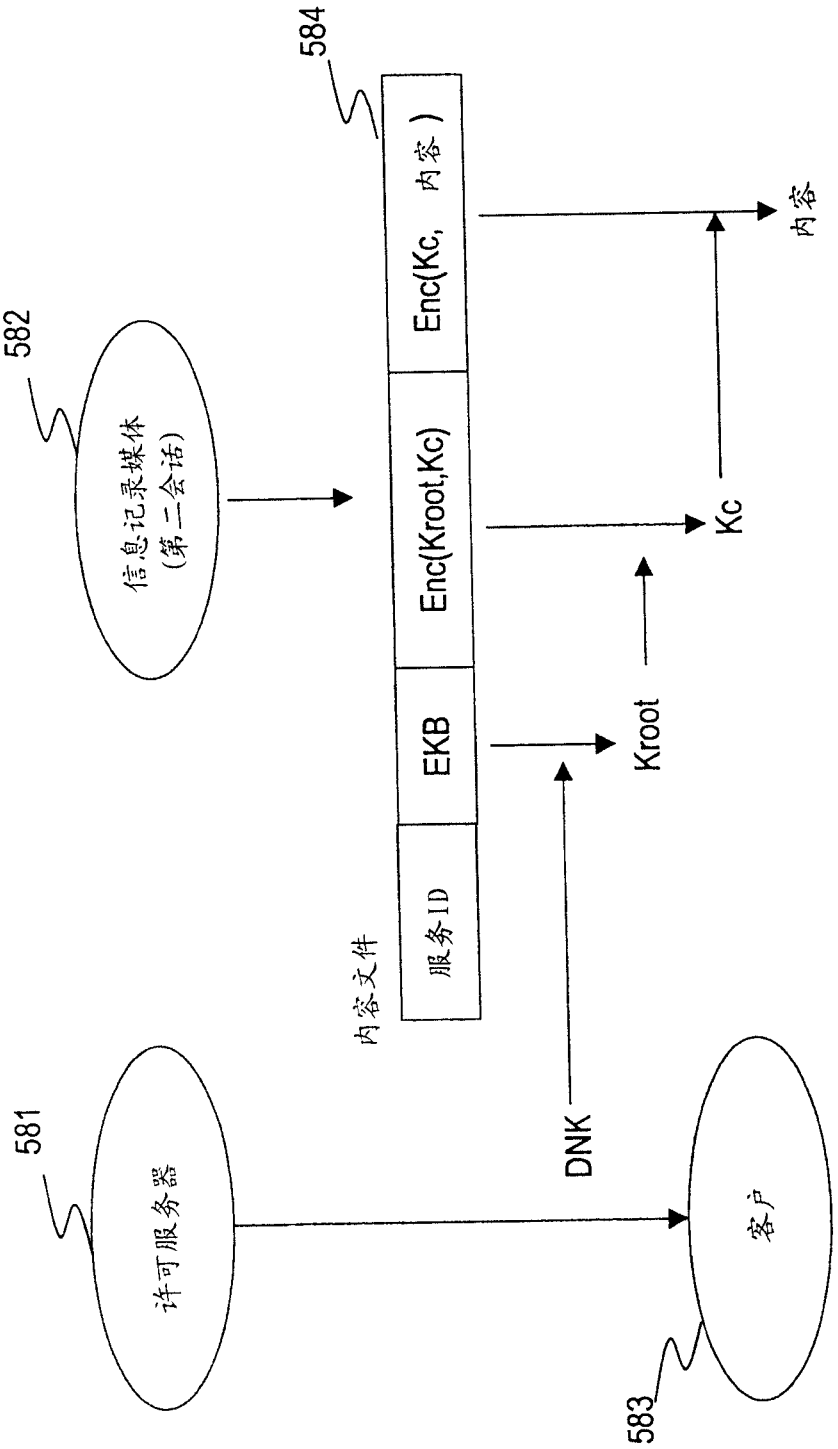

584
582
信息记录媒体
(第二会话)
Enc(Kc, 内容)
内容
Enc(Kroot,Kc)
Kc
EKB
Kroot
服务ID
内容文件
581
许可服务器
DNK
客户
583

图 27

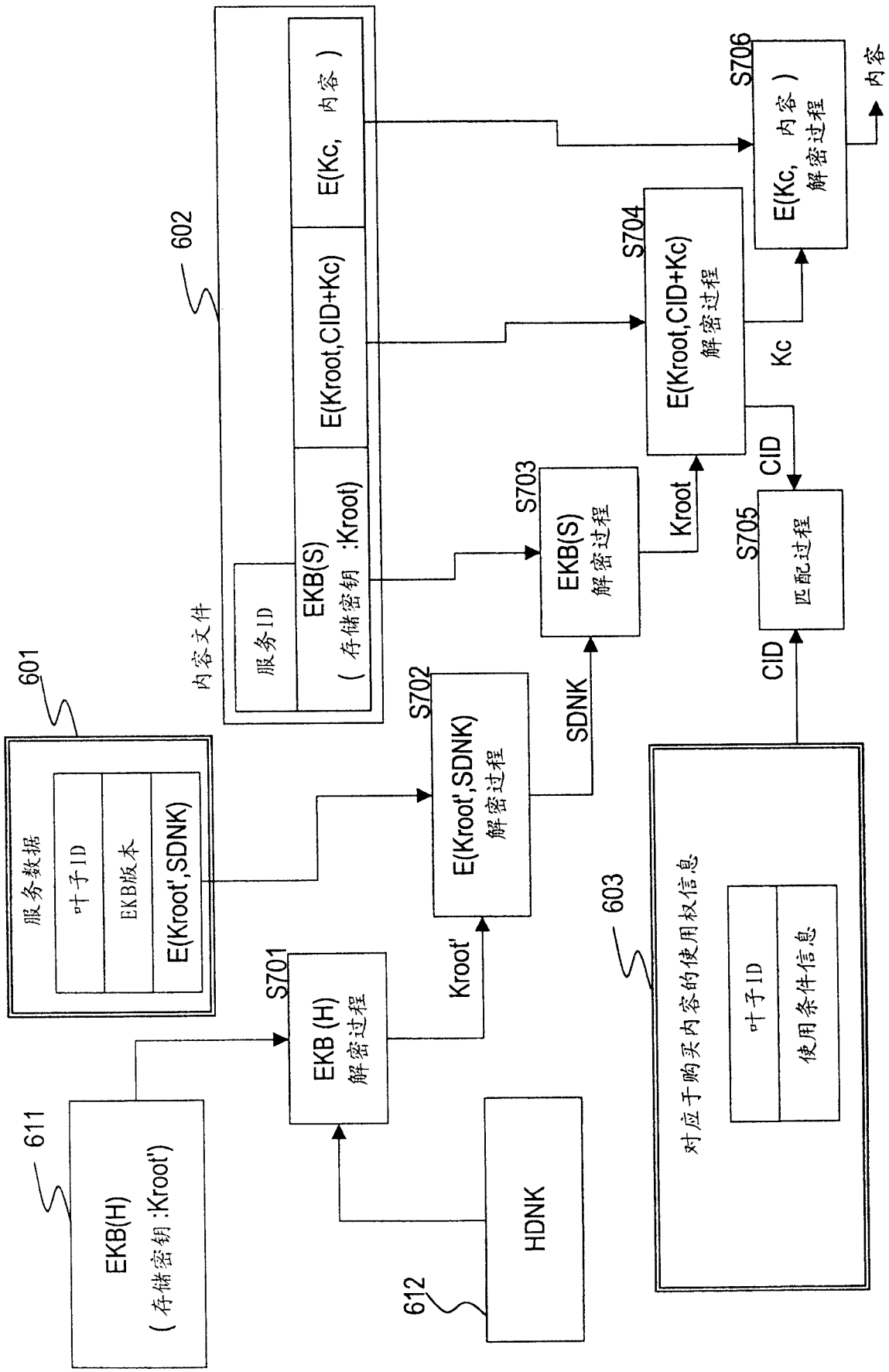

611
EKB(H)
（存储密钥:Kroot'）
612
HDNK
601
服务数据
叶子ID
EKB版本
E(Kroot',SDNK)
602
内容文件
服务ID
EKB(S)
（存储密钥:Kroot）
E(Kroot,CID+Kc)
E(Kc, 内容)
603
对应于购买内容的使用权信息
叶子ID
使用条件信息
S701
EKB (H)
解密过程
Kroot'
S702
E(Kroot',SDNK)
解密过程
SDNK
S703
EKB(S)
解密过程
Kroot
S704
E(Kroot,CID+Kc)
解密过程
Kc
CID
S705
匹配过程
CID
S706
E(Kc, 内容)
解密过程
内容

图 28