(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1812416 B
(45)授权公告日 2012.03.28

(21)申请号 200610006245.0
(22)申请日 2006.01.24
(30)优先权数据
0550254 2005.01.28 FR
(73)专利权人 汤姆森许可贸易公司
地址 法国布洛里
(72)发明人 让－皮埃尔·安德里克斯
阿兰·迪朗 西尔万·勒列夫尔
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 罗松梅
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
EP 1271279 A,2003.01.02, 全文.
CN 1166144 C,2004.09.08, 全文.
CN 1414552 A,2003.04.30, 全文.
审查员 孙志玲

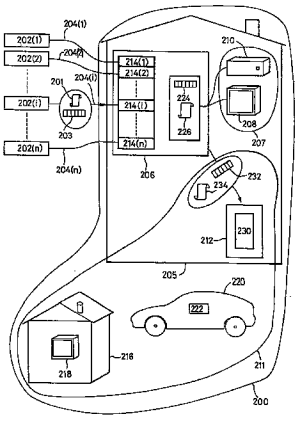
权利要求书 1 页 说明书 8 页 附图 4 页

(54)发明名称

在客户域内管理数字内容的消费的方法及设备

(57)摘要

本发明涉及一种在包括便携式设备(212)的客户域(200)内管理供应商(202(i))的数字内容(201)的消费的方法。根据本发明,这种保护方法的特征在于:a.便携式设备(212)接收隔离内容(232)、对音频和/或视频供应商内容(201)进行数字处理的结果、以及与内容相关联并包含使用隔离内容(232)的权利和授权信息的隔离许可(234),b.便携式设备(212)根据其已经接收到的关联权利,管理内容(232)在客户域(200)的设备中的消费,与供应商(202(i))无关。



CN 1812416 B

1. 一种用于管理数字内容的消费的方法，包括以下步骤：

- 在属于给定域 (200) 的接入设备 (206、302) 中，从供应商 (202(i)) 接收数字内容 (203) 和包含与该内容相关联的消费权利在内的第一许可 (201)；

- 将所述内容与第二许可 (234) 一起传输给便携式设备 (212)，所述第二许可 (234) 包含消费来自便携式设备的内容的次级权利，所述次级权利是在第一许可中接收到的消费权利的至少一部分，在所述域内消费内容需要授权数据的情况下，所述第二许可还包含这些授权数据；

其中，所述便携式设备 (212) 根据在第二许可中接收到的次级权利，授权或不授权所述内容在所述域的呈现设备 (218、222) 内的消费。

2. 根据权利要求 1 所述的方法，还包括以下步骤：

在所述呈现设备中消费内容需要授权数据的情况下，从便携式设备 (212) 向所述域的呈现设备 (218、222) 传输授权数据 (316)。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，接入设备 (206、302) 创建控制数据分组 (322)，称为 TECM，所述控制数据分组 (322) 被引入发送给便携式设备 (212) 的内容中并被发送给便携式设备 (212)，所述控制数据分组包含：

- 以下数据的加密集合 (320)：

○用于对形成了所述内容的数据分组进行加扰的密钥，和

○授权数据，以及

- 与加密有关的信息 (324)，该信息允许便携式设备 (212) 以安全的方式解密所述集合 (320)。

4. 根据权利要求 3 所述的方法，其特征在于，包含在控制数据分组中的加扰密钥还通过授权数据加以保护。

在客户域内管理数字内容的消费的方法及设备

技术领域

[0001] 本发明涉及一种用于在包含用于处理数字内容的设备的客户域内管理数字内容的消费的方法。本发明还涉及实现此方法的设备。

背景技术

[0002] 为了监控其产品通过如因特网等数字网络的消费和避免盗版，数字内容的生产商（例如但不限于：电影、记录片、音乐、剪辑、视频游戏、视听内容、服务等）实施了用于管理授予其客户的、与内容相关联的消费权利的方法。此后，将这些方法称为 DRM 方法（表示“数字权利管理”）。

[0003] 例如，与内容相关联的权利可以授权对内容再现特定的小时数和 / 或特定的次数和 / 或制作特定数量的副本。因此，需要在用户消费内容时对权利进行跟踪。

[0004] 实现 DRM 方法的手段在于：在供应商侧，被称为供应商 DRM 的软件模块形式，以及在客户侧，被称为客户 DRM 的软件模块形式。

[0005] 通常，在与传递内容的网络（被称为供应商网络）相连的电子设备（被称为访问设备）级实现内容的消费，如计算机等，并且此设备包含一个或多个客户 DRM 模块。

[0006] 可能会发生在并未与供应商网络直接相连的客户的另一设备上存储或消费内容的情况。

[0007] 为了避免内容的不受控制的传播，可以将这些内容的传输限制于一组内容处理设备，通常属于同一个客户（例如，电视、游戏机、无线电、用于再现音乐的设备、解码器等）。

[0008] 将与客户相关联的这组设备称为客户域，图 1 示出了客户域的示例。

[0009] 视频和 / 或音频内容供应商 102(i)，1 ＜＝ i ＜＝ n，提供被称为供应商内容 103 的数字化内容 103（具体地，已加扰或明文）和被称为供应商权利的权利，与供应商内容 103 相关联，并包含在供应商许可 101 中。这种提供通过与客户域 100 的接入设备 106 相连的供应商网络 104(i)，1 ＜＝ i ＜＝ n，来完成。

[0010] 具体地，网络 104(i) 可以属于供应商或者是公众的，如因特网等。

[0011] DRM 方法存在于每个供应商 102(i) 与接入设备 106 之间。

[0012] 已经开发出用于保护权利的方法来保护域 100 内的供应商权利，并检查是否合法地进行了内容消费：

[0013] - 在接入设备 106，或者

[0014] - 在电子设备的一部分，称为网络部分 107，例如包括电视 108 或用于再现音乐的设备 110，通过同轴电缆、光纤或无线通信系统，在网络中与接入设备 106 相连。这些设备被称为已链接设备。

[0015] 具体地，检查内容消费通常需要连接客户 DRM 模块 114(i)，以验证消费的授权，该操作可以在消费内容期间进行多次。

[0016] 在题为“Digital Home Network and method for creating andupdating such a network”的文献 WO 00/62505 A1 中描述了仅包括接入设备 106 和网络部分 107 的域 100

的创建和管理。

[0017] 更准确地,题为“Process for managing a symmetric key in acommunication network and devices for the implementation of thisprocess”的文献 EP 1 253 762 A1 定义了一种管理方法,其中借助于设备 106 和网络部分 107 的消费设备所公知的对称密钥,对内容进行加密和解密。

[0018] 在题为“Method of secure transmission of digital data froma source to a receiver”的文献 WO 02/47356 A2 中处理了权利的特殊情况(只有消费权利,而没有复制权利,被称为“只观看”权利)。

发明内容

[0019] 本发明源自于以下发现:现有技术的 DRM 方法和内容保护方法目前不能安全地管理内容和与此内容相关联的权利,通过接入设备 106、针对域 100 获得,在内容消费设备(被称为隔离设备(isolateddevice))中,包括在被称为域 100 的隔离部分的部分 111 中,并未将不同的完整 DRM 模块(每一个依赖于潜在的可用提供商(i))引入该隔离设备。例如,所述隔离设备是:

[0020] -便携式设备 112,例如,个人音频和/或视频播放器,能够在客户希望的地方消费内容;如设备 112 等、被称为便携式隔离设备的这类隔离设备可以按照临时的方式与接入设备 106 相连,以加载内容和权利,

[0021] -位于地点 116 的设备 118(例如另一房子中的电视),地点 116 不同于接入设备 106 所处的地点 115,或运输车辆 120 的车载设备 122;如设备 122 和 118 等、被称为远程隔离设备的这类隔离设备可以不与接入设备 106 相连。

[0022] 具体地,这些隔离设备不能建立与客户 DRM 模块 114(i) 的网络连接,以便在消费内容期间获得所需的授权。

[0023] 现在,将依赖于供应商 (i) 的、不同的完整 DRM 模块引入隔离设备遇到很多困难,例如:

[0024] -大量的隔离设备并不具有足以包含几个不同 DRM 模块 (i) 的信息处理装置;

[0025] -需要将被引入的全部 DRM 装置的完整和明确的列表,这用于防止竞争;

[0026] -这些技术中的每一个都是不可改变的,因为不能对其进行更新;

[0027] -如果将这些 DRM 模块的全部秘密收集在单一的隔离设备中,仍将存在安全性问题。

[0028] 因此,本发明致力于提供一种确保客户在整个客户域上、尤其是在隔离部分 111 处、汇集与由客户从内容供应商接收到的给定内容相关联的权利。

[0029] 本发明涉及一种在包括便携式隔离设备的客户域内管理供应商的数字内容的消费的方法,其特征在于:

[0030] a. 便携式隔离设备接收隔离内容、对音频和/或视频供应商内容进行数字处理的结果、以及与内容相关联并包含使用隔离内容的权利 和授权信息的隔离许可,

[0031] b. 便携式隔离设备根据其已经接收到的关联权利,管理内容在客户域的设备中的消费,与供应商无关。

[0032] 通过本发明,隔离部分中的权利管理并不预示着将每一个依赖于不同的潜在可用

供应商的不同 DRM 模块引入隔离设备，以便消费各个供应商的内容。

[0033] 同样，来自供应商且与内容相关联的单一许可是必需的，与用于消费内容的客户域的设备无关。此许可由客户 DRM 模块处理。

[0034] 另一优点在于本发明的方法与实现了在包括接入设备和网络部分的域内保护内容的现有方法（文献 WO 00/62505 A1、EP 1 253 762A1 和 WO 02/47356 A2 中所描述的方法）的兼容性。因此，可以单独使用本发明的方法，或以（从便携式隔离设备）补充这些现有方法的方式使用本发明的方法。

[0035] 本发明的另一优点在于以下事实：如果针对已经被处理从而从便携式隔离设备进行消费的内容，获得了新权利，不必重新处理相同的内容，从而再次从便携式隔离设备进行消费。

[0036] 最后，对于能够暂时与便携式隔离设备相连的所有客户域设备，此保护方案是有效的。这意味着：在可以位于域内的消费设备的整个集合上，可以利用单一的整体保护方法来消费内容，而不必具有专用于客户域的特定设备的特定保护方法。

[0037] 在实施例中，便携式隔离设备暂时与接入设备相连，以便获得隔离内容和包含使用隔离内容的权利和授权信息在内的隔离许可。

[0038] 在实施例中，接入设备创建用于管理使用内容的权利的数据分组，称为 TEMM，尤其包括以下内容的加密结果，可由便携式隔离设备解密：

[0039] ○验证数据，

[0040] ○内容标识符，

[0041] ○使用内容的权利，

[0042] 并将此分组 TEMM 发送给便携式隔离设备。

[0043] 根据实施例，接入设备创建控制数据分组，称为 TECM，将其引入 隔离内容，并发送给便携式隔离设备，所述控制数据分组包含：

[0044] - 以下数据的加密集合：

[0045] ○用于加扰形成了内容的数据分组的密钥，和

[0046] ○授权数据，以及

[0047] - 与加密有关的信息，允许便携式隔离设备以安全的方式解密所述集合。

[0048] 优选地，包含在控制数据分组中的加扰密钥还通过授权数据加以保护。

[0049] 在实施例中，通过减去发送给便携式隔离设备的权利，更新接入设备中、与供应商内容相关联的权利。

[0050] 根据实施例，在便携式隔离设备处，消费内容。

[0051] 在实施例中，便携式隔离设备的权利管理装置将对消费的授权发送给专用于便携式隔离设备的消费装置，并在便携式隔离设备中消费内容时，更新包含在隔离许可中的权利。

[0052] 根据实施例，具有消费内容的装置的呈现设备暂时与便携式隔离设备相连。

[0053] 在实施例中，当呈现设备向便携式隔离设备请求获得内容从而对其进行消费的授权时，便携式隔离设备的权利管理装置验证隔离许可中是否存在呈现设备所请求的权利，如果授权请求被证实，更新所述隔离许可，并将授权和内容发送给呈现设备，从而在其中进行消费。

[0054] 本发明还涉及一种用于管理数字内容的消费的方法，包括以下步骤：

[0055] -在属于给定域的接入设备中，从供应商接收数字内容和包含与该内容相关联的消费权利在内的第一许可；

[0056] -将所述内容与第二许可一起传输给便携式设备，所述第二许可包含消费来自便携式设备的内容的权利，以及在所述域内消费内容需要授权数据的情况下，包含这些授权数据；

[0057] 其中所述便携式设备根据在第二许可中接收到的权利，授权或不授权所述内容在所述域的呈现设备内的消费。

[0058] 在一个实施例中，本方法还包括以下步骤：在呈现设备中消费内 容需要授权数据的情况下，从便携式设备向所述呈现设备传输授权数据。

[0059] 本发明还涉及一种便携式隔离设备，包含：接收装置，从属于给定域的接入设备接收数字内容和许可，所述许可包含消费来自便携式设备的内容的权利，以及在所述域内消费内容需要授权数据的情况下，包含这些授权数据；授权装置，根据在许可中接收到的权利，授权或不授权所述内容在所述域的呈现设备内的消费。

[0060] 本发明还涉及一种接入设备，包括：接收装置，从供应商接收数字内容和包含与该内容相关联的消费权利在内的第一许可；以及传输装置，用于将所述内容与第二许可一起传输给便携式设备，所述第二许可包含消费来自便携式设备的内容的次级权利，所述次级权利是在第一许可中接收到的消费权利的至少一部分，在消费内容需要授权数据的情况下，所述第二许可还包含这些授权数据。

附图说明

[0061] 通过以下参考附图，作为非限制性示例给出的详细描述，本发明的其他特征和优点将变得显而易见，其中：

[0062] 图 1，已经描述过，示出了设备的现有技术域 100 的示例；

[0063] 图 2 示意性地示出了本发明在客户域内的实施例；

[0064] 图 3 是在客户 DRM 模块和便携式隔离设备之间传送内容的方法的示意性描述；

[0065] 图 4 是根据特定标准、在客户 DRM 模块和便携式设备之间进行传送期间、特定数据的结构的示意图。

具体实施方式

[0066] 本发明能够管理在整个客户域上消费由客户获得的内容的权利，所述域可能包括便携式隔离设备和远程隔离设备。

[0067] 图 2 示意性地示出了本发明的典型实施例。

[0068] 客户具有一组用于处理音频和 / 或视频数字内容的电子设备，称为域 200。

[0069] 域 200 的客户借助于集成在接入设备 206 中的管理权利的装置 214(i)，1 <= i <= n，(被称为客户 DRM 模块 214(i))，向内容供应商 202(i)，1 <= i <= n，发出对内容的预定，具有相关联的权利。

[0070] 然后，接入设备 206 通过网络 204(i)(如因特网或电缆网络)接收音频和 / 或视频供应商内容 203 和消费供应商许可 201。内容 203 通常以由供应商 DRM 保护的音频 / 视

频数据（或其他数据）分组的形式提供，例如，借助于供应商的密钥进行加密或加扰。

[0071] 供应商许可 201 实际上包含与内容 203 相关联的消费权利、使其能够访问内容的数据（例如，用于加密内容的数据分组的供应商密钥）、以及内容的标识符。对全部内容进行保护，例如，通过加密，从而不能由与内容供应商 202(i) 相关联的客户 DRM 模块 214(i) 以外的其他装置访问。许可 201 由客户 DRM 模块 214(i) 接收和管理。

[0072] 然后，在接入设备 206 中，将内容 203 和许可 201 转换为专用于域 200 的内容（称为私人化内容 224）和专用于域 200 的许可（称为私人化许可 226）。这尤其需要数据结构对域 200 的适配。然后，客户可以选择直接在接入设备 206 中或在网络部分 207（设备 210 或 208）中消费私人化内容 224，与现有技术中类似。

[0073] 具体地，在实施例中，可以根据文献 WO 00/62505 A1、EP 1 253762 A1 和 WO 02/47356 A2 中所描述的方法之一具体实现内容的这种私人化、及其在接入设备 206 中或网络部分 207 中的管理和消费。

[0074] 更准确地，根据这些典型实施例，在接入设备 206 中，将接收到的内容 203 转换为适当的形式（如果其并非所需的形式），从而以表示为 CW 的控制字对音频 / 视频或其他数据分组进行加扰，在信号的每个加密周期期间进行更新（通常为每隔 10s），以形成私人化内容 224。将包括在许可 201 中的、与内容 203 相关联的消费权利转换为专用于域 200 的格式。在上述文献中所描述的典型实施例中，权利的域专用格式包含三种可能的状态：

[0075] - “私人复制”（也就是说，授权内容的复制，但只能在域 200 中消费）；

[0076] - “无限制复制”（无条件授权的复制）；或

[0077] - “只观看”（也就是说，只授权消费内容，而不能对其进行复制）。

[0078] 将转换后的权利包括在表示为 LECM 的消息中，消息 LECM 还包含以对称密钥 K_{LECM} 加密的控制字 CW，并以域专用密钥 K_N 对此密钥 K_{LECM} 进行加密。属于域 200 的、用于向用户呈现内容的设备 208、210 包含密钥 K_N（存储在安全存储器中），因此，能够获得 K_{LECM}，然后，获得控制字 CW，从而对私人化内容 224 的数据分组进行解扰。

[0079] 将本示例中与私人化许可 226 对应的消息 LECM 与内容 224 的数据分组一起进行传输，并在每个加密周期期间重复。

[0080] 应当注意，通过本发明，客户也可以在客户域 200 的隔离部分 211 处，消费私人化内容 224（在可能的适配之后，其变为隔离内容 232），例如，所述隔离部分 211 包括便携式设备 212 和 / 或车辆 220 中的设备 222 和 / 或另一房子 216 中的设备 218，后者被称为远程隔离设备。

[0081] 便携式设备 212 可以包含消费装置（例如，显示屏幕和扬声器或手机的拾取器），具体地，如果此设备 212 是个人音频和 / 或视频播放器，或者不包含这些（在这种情况下，该设备可以是密码处理和存储设备）。

[0082] 因此，便携式设备 212 包含用于管理权利的模块 230，实现保护方法，尤其是针对客户域 200 的隔离部分 211，称为隔离保护方法。

[0083] 模块 230 是通用（即，不依赖于内容 203 的供应商）且安全的（即，防伪），并存储有加密数据和消费授权。

[0084] 便携式设备 212 在其与接入设备 206 相连时进行接收，以获取内容：

[0085] - 隔离内容 232，适合于在设备 212 中进行消费，或者按照受控的方式从便携式设

备 212 向外传输；

[0086] - 以及附加许可 234，称为隔离许可，包含用户想要在域 200 中使用来自便携式设备 212 的内容的权利，尤其是在隔离部分 211 中，以及授权这种使用的数据。

[0087] 通过从供应商许可 201 中推出在许可 234 中传输给便携式设备 212 的权利，来执行接入设备 206 中对剩余权利的更新。

[0088] 例如，如果客户已经获得观看电影两次的权利，并且如果他希望在另一房子 216 中观看一次，则将观看一次的权利传输给便携式便携式设备 212，以便在需要时，传输给电视 218。

[0089] 同时，从接入设备 206 中的权利中推出已传输的权利，从而在接入设备 206 中只留下观看该电影一次的权利。

[0090] 通过已存储在模块 230 中的加密数据，对与内容相关联的特定数据进行加扰 / 加密，确保内容 232 和许可 234 的传输安全。

[0091] 因此，将权利管理模块 230 包括在智能卡或安全处理器中，用于实现隔离保护方法，并包含以安全方式存储的加密密钥。

[0092] 因此，将私人内容 224 和私人许可 226 适配为隔离内容 232 和隔离许可 234 是必须确保由便携式设备 212 管理的权利的安全性的重要步骤。

[0093] 现在，将结合图 3 和图 4（提供了数据结构的细节），对将私人内容 224 和私人许可 226 适配为隔离内容 232 和隔离许可 234 的这种适配的典型实施例进行描述。

[0094] 根据本发明的优选实施例，以两个“对象”的形式，向便携式设备 212 传输隔离许可 234：

[0095] - 一方面，被称为 TECM 的消息，对应于私人化许可 226 的 LECM 消息，但其中不再以用户域专用的密钥 K_N 而是以便携式设备 212 专用的密钥 K_{DP} 对对称加密密钥 K_{LECM} 进行加密；

[0096] - 另一方面，在与内容相关联的权利是“只观看”类型的情况下，表示为 TEMM 的消息，包含使其能够随后在用户域的远程隔离设备 218、222 上消费内容的授权信息。

[0097] 图 3 示出了在与要传输的内容相关联的权利是“只观看”类型时，用于在以下设备之间传送隔离许可的传送协议：

[0098] - 接入设备 302，等价于图 2 的接入设备 206，

[0099] - 和专用于便携式设备 212 的管理模块 304（等价于图 2 的模块 230）。

[0100] 模块 304 具有可用的已证实非对称加密系统，包括公用密钥 306(KpubTr) 和私用密钥 312(KprivTr)，以便向接入设备 302 标识其 自身。

[0101] 模块 304 还包括专用于便携式设备的对称加密密钥 $314K_{DP}$。

[0102] 当请求在设备 302 和模块 304 之间传送内容时，执行以下步骤：

[0103] - 步骤 350：模块 304 将包括密钥 306KpubTr 的证书 307 发送给接入设备 302；

[0104] - 步骤 352：设备 302 通过表示为 KpubDRM 的公用密钥 308 验证密钥 306KpubTr（并由此验证便携式设备 212 的身份），公用密钥 308 用于验证便携式设备 212 的证书 307（如果设备 212 的身份未被识别为有效，则对内容的适配及其传送并不发生）；

[0105] - 步骤 354：如果步骤 352 的验证是肯定的，则设备 302 创建用于管理使用内容的权利的数据分组 340，对应于消息 TEMM，包含通过密钥 306KpubTr 对以下内容进行加密的结

果：

[0106] ○授权数据 316，

[0107] ○内容标识符 318，

[0108] ○源自于许可 210 的、使用内容的权利 319。

[0109] 接下来，设备 302 将此分组 340TEMM 发送给模块 304。授权数据 316 可以包含瞬时认证密钥 K 和瞬时加密密钥 R，由接入设备 302 以随机的方式产生，如上述专利申请 WO 02/47356 中定义的那样。使用内容的权利 319 定义了在便携式设备中使用内容的条件，例如“观看电影两次的权利”。

[0110] -步骤 356：接入设备 302 随机地产生对称密钥 $310K_{LECM}$。接下来，以密钥 306KpubTr 对此密钥 $310K_{LECM}$ 进行加密，并将结果 $311E\{KpubTr\}(K_{LECM})$ 发送给模块 304；

[0111] -步骤 358：模块 304 以私用密钥 312KprivTr 对 $E\{KpubTr\}(K_{LECM})$ 进行解密，以便携式设备的对称密钥 $314K_{DP}$，对 K_{LECM} 重新进行加密，并将此加密的结果 $324E\{K_{DP}\}(K_{LECM})$ 返回给接入设备 302；

[0112] -步骤 360：接入设备 302 创建与 TECM 消息对应的数据分组 322；将这些分组 322TECM 引入内容 232，如图 3b 所示，示出了 DVB-MPEG2（表示“数字视频广播运动图像专家组”）标准示例中的内容 232（图 2）的数据结构 330。分组 322TECM 包含：

[0113] ○包括结果 $324E\{K_{DP}\}(K_{LECM})$ 在内的数据 326；

[0114] ○包括以对称密钥 310KLECM 对尤其包括以下内容在内的数据集合进行加密的结果 320 在内的数据 328：

[0115] ■用于加扰形成了内容的数据分组的密钥（例如控制字 CW），

[0116] ■授权数据，和

[0117] ■内容标识符 318。

[0118] 应当注意，可以在 TECM 分组中作为明文传送内容标识符 318，TECM 分组在其明文部分中还包含根据专用于域 200 的格式转换后的使用内容的权利。

[0119] 应当注意，在包含在分组 340TEMM 中的授权数据 316 包含由接入设备 302 以随机方式产生的瞬时（emphemeral）认证密钥 K 和瞬时加密密钥 R 的情况下，在分组 322TECM 中，如下使用这些密钥：瞬时加密密钥 R 用于对用于加扰形成内容的分组的密钥进行“过加密”，以及瞬时验证密钥 K 对应于授权数据。因此，根据此特定示例，每个分组 322TECM 包含：

[0120] $E\{K_{DP}\}(K_{LECM})|E\{K_{LECM}\}(E\{R\}(CW),K,标识符)|$ 权利

[0121] 每个分组 322TECM 与传送部分内容 232 的分组集合 332 一起位于加密周期 331 中（在条件访问世界中，加密周期 331 对应于其间将同一加扰密钥 CW 用于加密内容的周期，其通常具有大约 10 秒的持续时间），然后，设备 302 将插入到内容 330 中的分组 322TECM 发送给模块 304。

[0122] 当内容 232 已经被传送到设备 212（利用分组 322TECM）时，如果获得了新权利，则内容 232 可重新使用（例如，获取与将来消费相对应的权利），从而可以在便携式设备 212 或在能够消费由便携式设备 212 管理的内容的任何其他设备中进行消费。

[0123] 在与关联隔离许可 234（图 2）一起、从接入设备 206 向便携式设备 212 传送隔离内容 232 的步骤之后，可以发生对内容 232 的消费：

[0124] -如果此设备 212 包含实现此消费所需的装置（如显示屏幕、扬声器或手机的拾取

器等），在便携式设备 212 中。则实施以下步骤：

[0125] ○模块 230 检查可以在许可 234 中获得的权利的框架内实现消费（如果不是这种情况，则拒绝消费）；

[0126] ○模块 230 更新许可 234 中使用内容的权利；然后

[0127] ○模块 230 向专用于便携式设备 212 的消费装置发送消费授权。

[0128] －或者在域 200 的、能够暂时与设备 212 相连的另一设备处，尤其是域 200 的隔离部分 211 的设备，称为内容呈现设备。于是，执行以下步骤：

[0129] ○便携式设备 212 连接域 200 的一个或多个设备；

[0130] ○便携式设备 212 向与之相连的域 200 的那些设备传输内容 232；

[0131] ○呈现设备（例如，另一住所 216 的电视 218）向设备 212 请求消费内容 232 的授权（也就是说，在电视 218 的情况下，在屏幕上进行显示的权利）；

[0132] ○然后，便携式设备 212 的管理模块 230 验证许可 234 中的权利，如果能够接受该请求，其更新许可 234，并向呈现设备发送授权和内容。

[0133] 在其中授权数据是用在上述专利申请 WO 02/47356 中的、描述其中只授权对内容的直接消费而没有复制权利（“只观看”）的协议的那些授权数据的优选实施例中，如下运行在呈现设备 218、222（图 2）处消费内容的方法。

[0134] 首先，在呈现设备（起到图 3 的管理模块 304 的作用，并且包含专用于域 200 的密钥 K_N）和便携式设备 212（起到图 3 的接入设备 302 的作用）之间运行与结合图 3 所描述的相类似的处理，在完成时，设备 212 可以用包含以域的密钥 K_N（而不是如 TECM 中那样，以设备 212 的密钥 K_{DP}）进行了加密的对称密钥 K_{LECM} 在内的 LECM 分组代替内容的 TECM 分组。然后，将 LECM 分组与内容一起发送给呈现设备。

[0135] 然后，呈现设备借助于密钥 K_N 对 LECM 分组进行解密。因此，获得了瞬时认证密钥 K 以及内容加扰密钥 CW，借助于瞬时加密密钥 R 对其进行加密。然后，产生随机数 Ri，将其发送给便携式设备 212。

[0136] 设备 212 根据此随机数 Ri 和瞬时认证密钥 K，计算认证数据 $MAC_K(Ri)$（“MAC”表示“消息认证码”）。这里，应当注意，设备 212 通过以其私用密钥 KprivTr 解密 TEMM 分组（构成了许可 234 的一部分）的授权数据，恢复此密钥 K 以及此 TEMM 分组的密钥 R。然后，将瞬时加密密钥 R 和认证数据 $MAC_K(Ri)$ 发送给呈现设备。

[0137] 于是，呈现设备可以借助于密钥 K 验证接收到的认证数据，并从而验证内容是否真的来自于授权源。借助于密钥 R，可以对内容加扰密钥进行解密，并对内容进行解扰。

[0138] 本发明可修改为多种变体。

[0139] 便携式设备 212 也可以是接入设备 206。将内容 203 和许可 201 私人化为内容 224 和许可 226 并非本发明所必需的，也可以将内容 203 和许可 201 直接适配为内容 232 和许可 234。

[0140] 同样，包括在便携式设备 212 的模块 304 中的对称密钥 314 可以与来自接入设备 206 的、用于在网络的部分 207 中消费内容的对称密钥相同。

[0141] 模块 230 可以通过除了用于存储和处理加密信息的智能卡以外的其他装置来实现，如安全处理器或与防伪软件相关联的处理器。

[0142] 具体地，便携式设备 212 可以是个人音频或视频播放器、移动电话、用于管理个人数据的电子设备（PDA，表示“个人数字助理”）、或具有密码处理装置的数据存储设备。

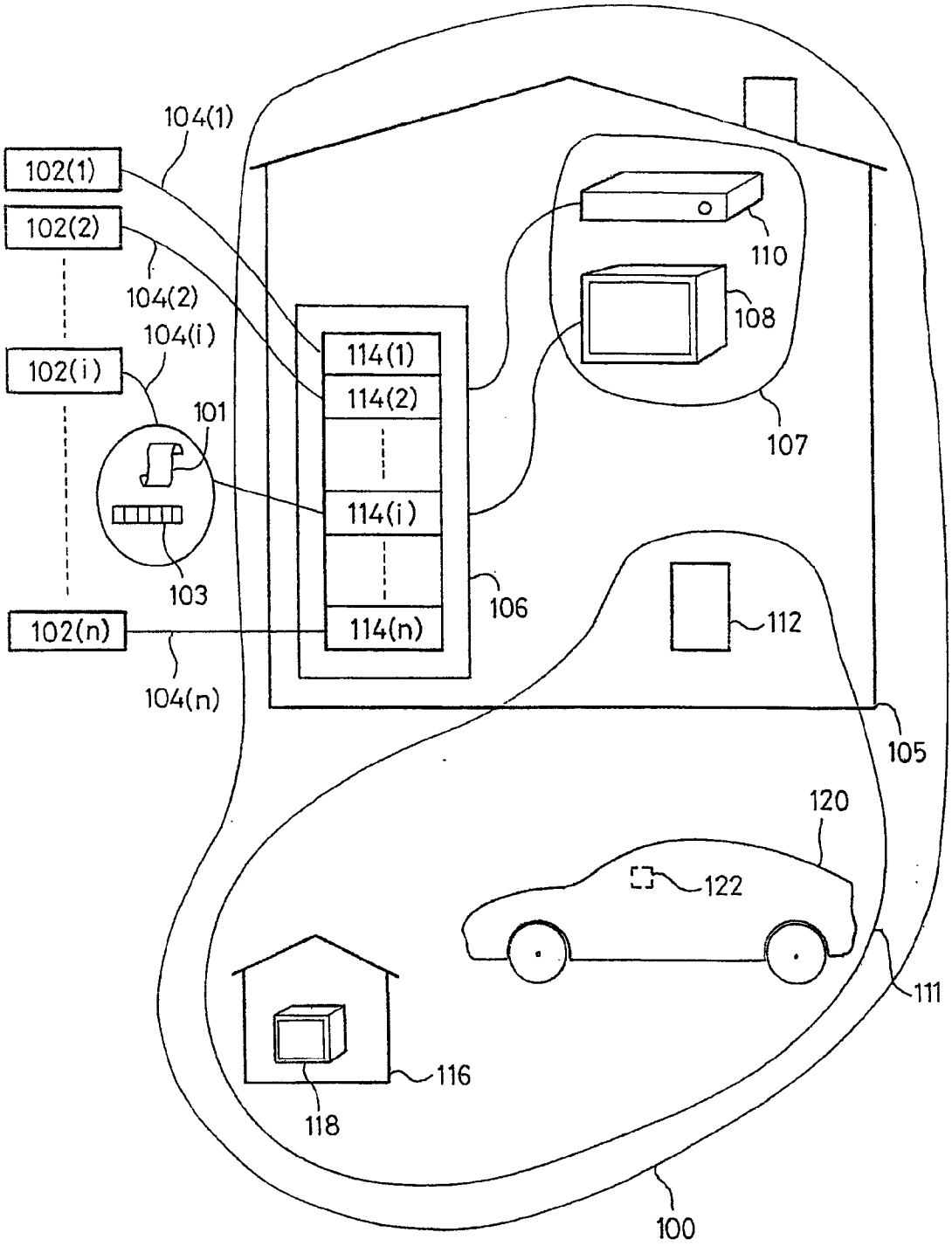

104(1)
102(1)
102(2)
104(2)
104(i)
102(i)
101
103
102(n)
104(n)
114(1)
114(2)
114(i)
114(n)
106
110
108
107
112
105
120
122
111
116
118
100

图 1

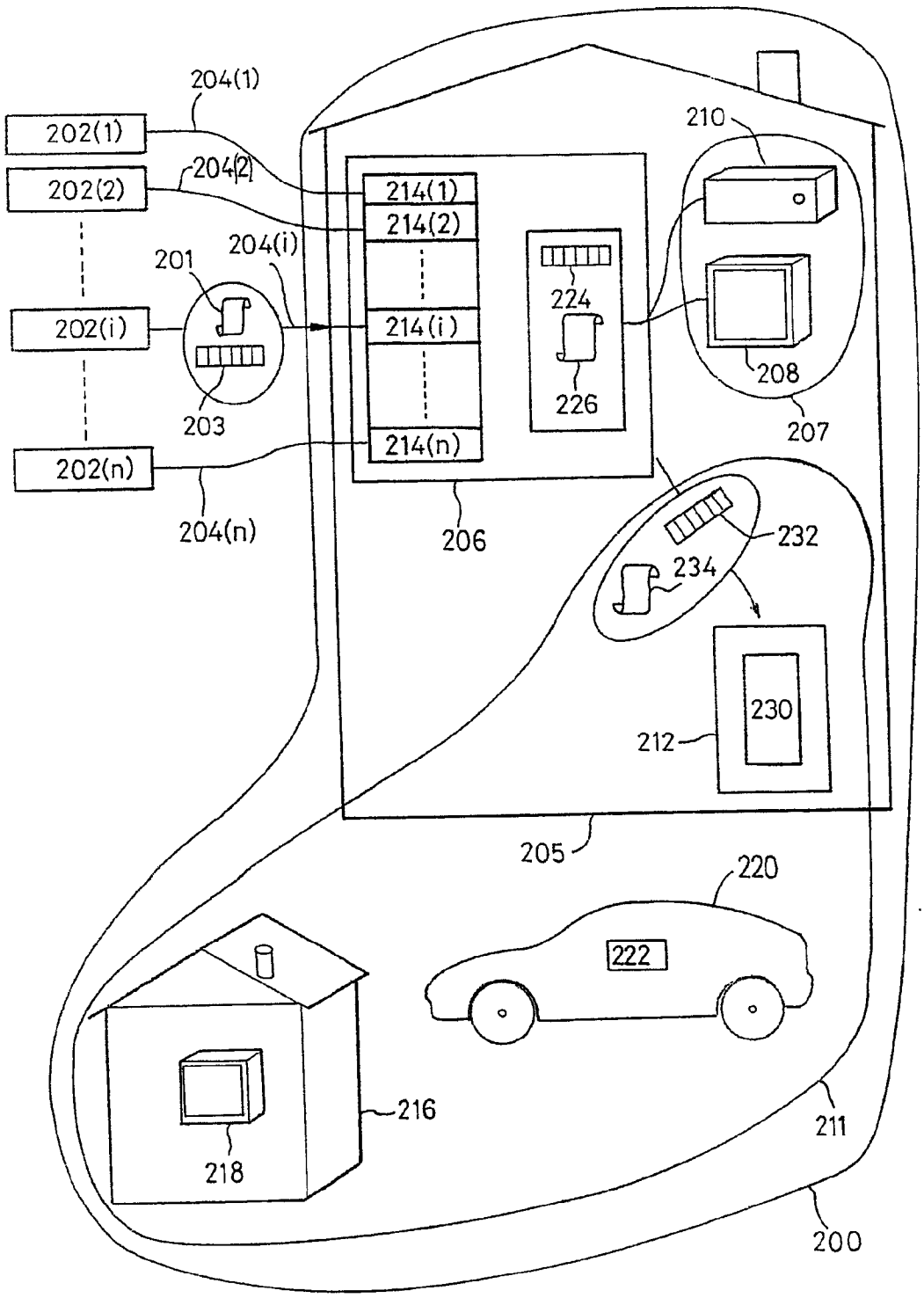

202(1)
202(2)
202(i)
202(n)
204(1)
204(2)
204(i)
204(n)
201
203
214(1)
214(2)
214(i)
214(n)
206
224
226
210
208
207
232
234
230
212
205
220
222
216
218
211
200

图 2

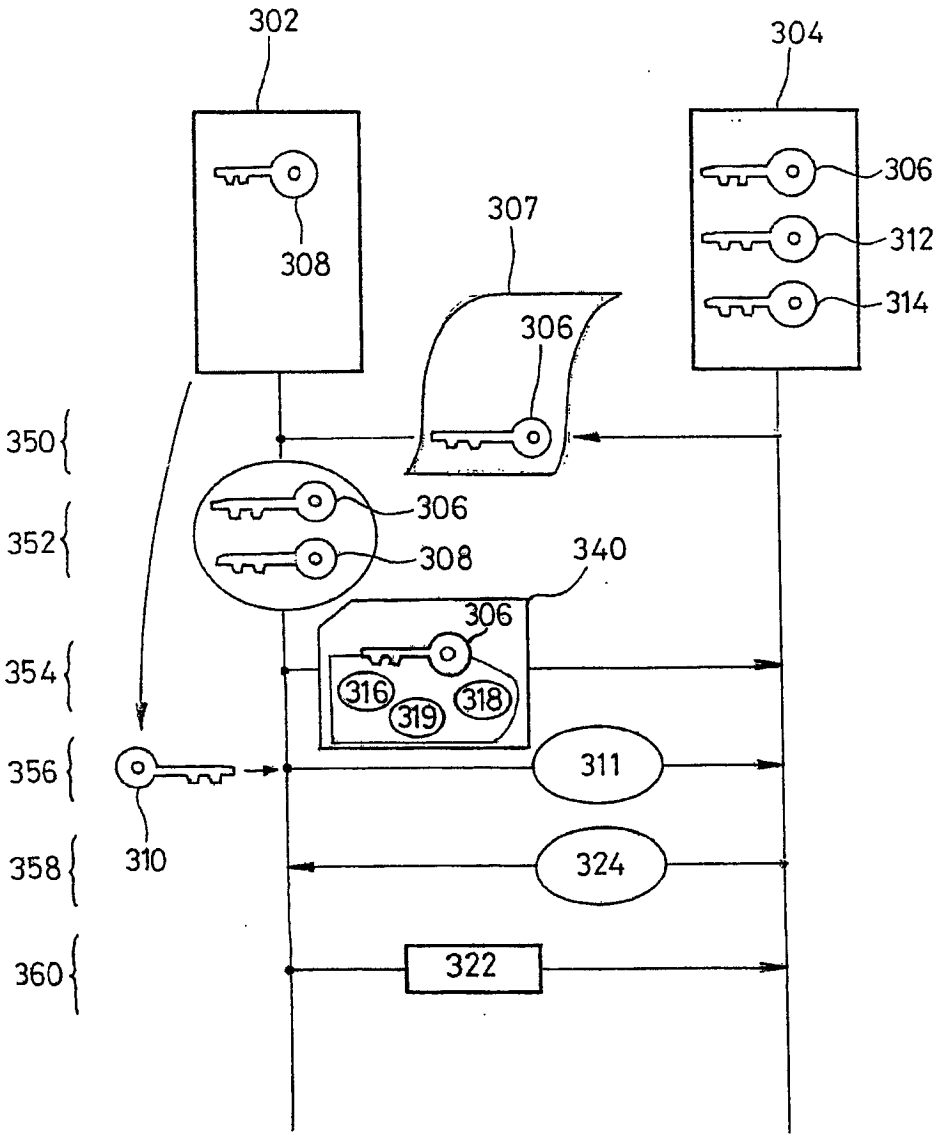

302
304
306
308
307
312
314
306
350
306
352
308
340
306
354
316
319
318
356
311
310
358
324
360
322

图 3

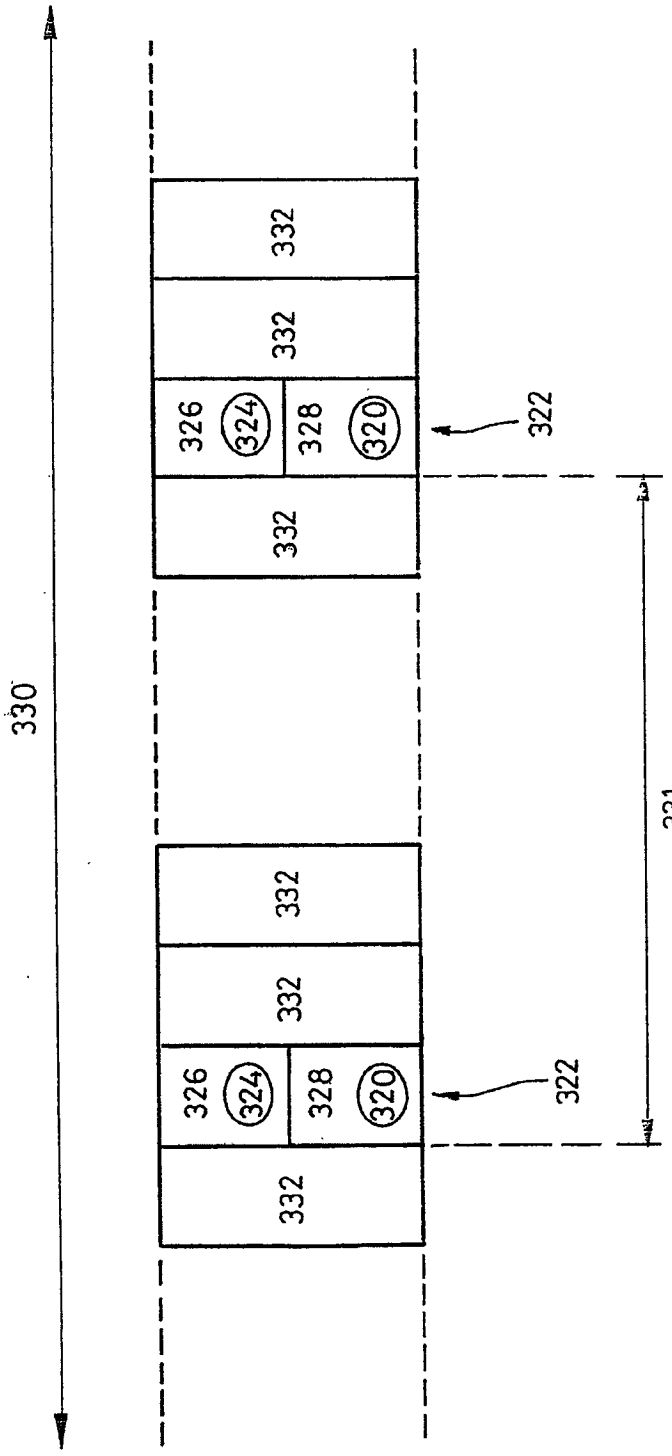

330
331
322
322
332
332
332
326
324
328
320
332
332
332
326
324
328
320
332

图 4