(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104735049 A
(43)申请公布日 2015.06.24

(21)申请号 201410789499.9
(22)申请日 2014.12.18
(30)优先权数据
13199063.2 2013.12.20 EP
(71)申请人 远升科技股份有限公司
地址 瑞士查伯斯蒂特内大道 7
(72)发明人 米歇拉札克·马切伊
(74)专利代理机构 北京律和信知识产权代理事务所(普通合伙) 11446
代理人 王美石 武玉琴
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/28(2006.01)

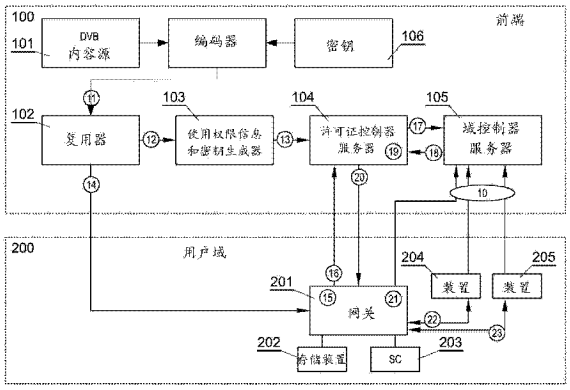
权利要求书2页 说明书4页 附图1页

(54)发明名称

用于在家庭网络中分配多媒体内容的系统和方法

(57)摘要

用于在家庭网络中分配多媒体内容的方法包括下述步骤:将多媒体内容从前端系统播送到多个家庭网络,每个家庭网络包括网关和多个家庭装置,网关用来从前端系统接收使用广播内容密钥来加密的多媒体内容,而多个家庭装置用来从网关接收多媒体内容;通过提供将要针对特定家庭网络进行注册的家庭装置的识别符,而在域控制器服务器上注册特定家庭网络的多个家庭装置;基于针对特定家庭网络来注册的装置的识别符,为家庭网络生成域内容许可证,域内容密钥允许加密多媒体内容,从而使得其可以由具有特定识别符的装置加以解密;将域内容许可证传输到特定家庭网络的网关;在网关中,解密所接收的多媒体内容,使用从域许可证中提取的密钥来加密多媒体内容,并将通过域内容密钥而加密的内容提供给家庭装置。



CN 104735049 A

1. 一种用于在家庭网络中分配多媒体内容的方法，所述方法包括下述步骤：

将多媒体内容从前端系统 (100) 播送 (14) 到多个家庭网络 (200)，每个家庭网络 (200) 包括网关 (201) 和多个家庭装置 (204、205)，所述网关 (201) 被配置来从所述前端系统 (100) 接收使用广播内容密钥来加密的多媒体内容，而所述多个家庭装置 (204、205) 被配置来从所述网关 (201) 接收多媒体内容；

通过提供将要针对特定家庭网络 (200) 进行注册的所述家庭装置 (204、205) 的识别符，而在域控制器服务器 (105) 上注册 (10) 所述特定家庭网络 (200) 的所述多个家庭装置 (204、205)；

基于针对所述特定家庭网络 (200) 来注册的所述装置 (204、205) 的识别符，为家庭网络 (200) 生成 (19) 域内容许可证，所述域内容密钥允许加密多媒体内容，从而使得其可以由具有所述特定识别符的所述装置 (204、205) 加以解密；

将所述域内容许可证传输 (20) 到所述特定家庭网络 (200) 的所述网关 (201)；

在所述网关 (201) 中，解密 (15) 所述接收的 (14) 多媒体内容，使用从所述域许可证中提取的所述密钥来加密 (21) 所述多媒体内容，并且，将通过所述域内容密钥而加密的所述内容提供给所述家庭装置 (204、205)。

2. 根据权利要求 1 所述的方法，其包括允许针对所述特定家庭网络 (200) 来注册有限数量的家庭装置 (204、205)。

3. 根据前述权利要求中任一项所述的方法，其特征在于所述装置 (204、205) 的所述识别符为公共密钥。

4. 根据前述权利要求中任一项所述的方法，其特征在于所述域内容许可证包括多媒体内容的使用权限信息。

5. 根据前述权利要求中任一项所述的方法，其特征在于在从所述网关 (201) 接收 (16) 请求时，生成 (19) 所述域内容密钥。

6. 根据前述权利要求中任一项所述的方法，其特征在于针对特定多媒体内容事件而生成 (19) 所述域内容许可证。

7. 根据前述权利要求中任一项所述的方法，还包括下述步骤：将所述接收的 (14) 多媒体内容存储在所述网关 (201) 的海量存储器 (202) 上，且使用所述接收的域内容许可证，在时间延迟的情况下加密 (21) 来自所述海量存储器 (202) 的所述多媒体内容，并且，将通过所述域内容密钥而加密的所述内容提供给所述装置 (204、205)。

8. 一种用于在家庭网络中分配多媒体内容的系统，所述系统包括：

前端系统 (200)，其用于将多媒体内容播送 (14) 到多个家庭网络 (200)，每个家庭网络 (200) 包括网关 (201) 和多个家庭装置 (204、205)，所述网关 (201) 被配置来从所述前端系统 (100) 接收使用广播内容密钥来加密的多媒体内容，而所述多个家庭装置 (204、205) 被配置来从所述网关 (201) 接收多媒体内容；

域控制器服务器 (105)，其被配置来通过接收将要针对特定家庭网络 (200) 进行注册的所述家庭装置 (204、205) 的识别符，注册 (10) 所述特定家庭网络 (200) 的所述多个家庭装置 (204、205)；

许可证控制器服务器 (104)，其被配置来基于针对所述特定家庭网络 (200) 来注册的所述装置 (204、205) 的识别符，而在所述域控制器服务器 (105) 上，为家庭网络 (200) 生成

(19) 域内容许可证，所述域内容密钥允许加密多媒体内容，从而使得其可以由具有所述特定识别符的所述装置 (204、205) 加以解密，并且允许将所述域内容许可证传输 (20) 到所述特定家庭网络 (200) 的所述网关 (201)；

其特征在于，所述家庭网络 (200) 的所述网关 (201) 被配置来解密 (15) 所述接收的 (14) 多媒体内容，使用所述接收的域内容许可证来加密 (21) 所述多媒体内容，并且，将通过从所述域内容许可证中提取的所述域内容密钥而加密的所述内容，提供给所述家庭装置 (204、205)。

9. 根据权利要求 8 所述的系统，其特征在于所述域控制器服务器 (105) 被配置来限制可以针对所述特定家庭网络 (200) 而注册的家庭装置 (204、205) 的数量。

10. 根据权利要求 8 和 9 中任一项所述的系统，其特征在于所述装置 (204、205) 的所述识别符为公共加密密钥。

11. 根据权利要求 8 和 9 中任一项所述的系统，其特征在于所述域内容许可证包括多媒体内容的域内容密钥和使用权限信息。

12. 根据权利要求 8 和 9 中任一项所述的系统，其特征在于所述许可证控制器服务器 (104) 被配置来在从所述网关 (201) 接收 (16) 请求时，生成所述域内容许可证。

13. 根据权利要求 8 和 9 中任一项所述的系统，其特征在于所述许可证控制器服务器 (104) 被配置来针对特定多媒体内容事件而生成所述域内容许可证。

14. 根据权利要求 8 和 9 中任一项所述的系统，其特征在于所述网关 (201) 连接到海量存储器 (202)，而且被配置来使用所述接收的域内容许可证，在时间延迟的情况下加密 (21) 来自所述存储器 (202) 的所述多媒体内容，并将通过所述域内容密钥而加密的所述内容提供给所述装置 (204、205)。

用于在家庭网络中分配多媒体内容的系统和方法

技术领域

[0001] 本发明涉及一种用于在家庭网络中分配多媒体内容的系统和方法。

背景技术

[0002] 家庭网络，也称为家庭区域网络 (HAN)，是从促进存在于家庭附近区域内部或附近区域中的数字装置之间的通信和互操作性的需要中发展起来的局域网络。此类装置可以包括数字电视机顶盒、电视机、移动装置、游戏机等。

[0003] 多媒体内容常常由有条件存取 (CA) 安全机制加以保护，所述有条件存取 (CA) 安全机制会保证内容提供商和最终用户之间传递的防护性和安全性。CA 系统允许将所加密的内容播送给多个用户，但是只允许拥有适当解密权限的用户进行解密。CA 安全机制常常是专有的且可与有限数量的装置兼容。举例而言，通常家庭网络中只有有限数量的装置能够正确接收和解密 CA 保护内容。举例而言，CA 安全机制只可以由机顶盒和电视机进行处理，而其他装置（如其他电视机、移动装置、游戏机等）则可能无法处理 CA 安全机制。在典型场景中，CA 保护内容不可用于这些其他装置。

[0004] 有利的是，提供一种用于在家庭网络中分配多媒体内容的方法和系统，其会使得所述内容可以用于家庭网络中的多个装置，而同时又确保所述内容是安全的。

发明内容

[0005] 本发明的目标是一种用于在家庭网络中分配多媒体内容的方法，所述方法包括下述步骤：将多媒体内容从前端系统播送到多个家庭网络，每个家庭网络包括网关和多个家庭装置，所述网关被配置来从所述前端系统接收使用广播内容密钥来加密的多媒体内容，而所述多个家庭装置被配置来从所述网关接收多媒体内容；通过提供将要针对特定家庭网络进行注册的所述家庭装置的识别符，而在域控制器服务器上注册所述特定家庭网络的所述多个家庭装置；基于针对所述特定家庭网络来注册的所述装置的识别符，为家庭网络生成域内容许可证，所述域内容密钥允许加密多媒体内容，从而使得其可以由具有所述特定识别符的所述装置加以解密；将所述域内容许可证传输到所述特定家庭网络的所述网关；在所述网关中，解密所述接收的多媒体内容，使用从所述域许可证中提取的所述密钥来加密所述多媒体内容，并且，将通过所述域内容密钥而加密的所述内容提供给所述家庭装置。

[0006] 优选地，所述方法包括允许针对所述特定家庭网络来注册有限数量的家庭装置。

[0007] 优选地，所述装置的所述识别符为公共密钥。

[0008] 优选地，所述域内容许可证包括多媒体内容的使用权限信息。

[0009] 优选地，在从所述网关接收请求时，生成所述域内容密钥。

[0010] 优选地，针对特定多媒体内容事件而生成所述域内容许可证。

[0011] 优选地，所述方法还包括下述步骤：将所述接收的多媒体内容存储在所述网关的海量存储器上，且使用所述接收的域内容许可证，在时间延迟的情况下加密来自所述海量存储器的所述多媒体内容，并且，将通过所述域内容密钥而加密的所述内容提供给所述装

置。

[0012] 本发明的另一目标是一种用于在家庭网络中分配多媒体内容的系统，所述系统包括：前端系统，其用于将多媒体内容播送到多个家庭网络，每个家庭网络包括网关和多个家庭装置，所述网关被配置来从所述前端系统接收使用广播内容密钥来加密的多媒体内容，而所述多个家庭装置被配置来从所述网关接收多媒体内容；域控制器服务器，其被配置来通过接收将要针对特定家庭网络进行注册的所述家庭装置的识别符，而注册所述特定家庭网络的所述多个家庭装置；许可证控制器服务器，其被配置来基于针对所述特定家庭网络来注册的所述装置的识别符，而在所述域控制器服务器上，为家庭网络生成域内容许可证，所述域内容密钥允许加密多媒体内容，从而使得其可以由具有所述特定识别符的所述装置加以解密，并且允许将所述域内容许可证传输到所述特定家庭网络的所述网关；其中，所述家庭网络的所述网关被配置来解密所述接收的多媒体内容，使用所述接收的域内容许可证来加密所述多媒体内容，并且，将通过从所述域内容许可证中提取的所述域内容密钥而加密的所述内容，提供给所述家庭装置。

[0013] 优选地，所述域控制器服务器被配置来限制可以针对所述特定家庭网络而注册的家庭装置的数量。

[0014] 优选地，所述装置的所述识别符为公共加密密钥。

[0015] 优选地，所述域内容许可证包括多媒体内容的域内容密钥和使用权限信息。

[0016] 优选地，所述许可证控制器服务器被配置来在从所述网关接收请求时，生成所述域内容许可证。

[0017] 优选地，所述许可证控制器服务器被配置来针对特定多媒体内容事件而生成所述域内容许可证。

[0018] 优选地，所述网关连接到海量存储器，而且被配置来使用所述接收的域内容许可证，在时间延迟的情况下加密来自所述存储器的所述多媒体内容，并将通过所述域内容密钥而加密的所述内容提供给所述装置。

附图说明

[0019] 用于在家庭网络中分配多媒体内容的系统和方法，在附图中通过示范性实施方案加以展示，其中图 1 示出所述系统的结构和所述方法的步骤。

具体实施方式

[0020] 图 1 展示用于在家庭网络中分配多媒体内容的系统。所陈述的实施方案涉及根据 DVB（数字视频播送）标准的内容传输。

[0021] 系统包括前端系统 100，其在步骤 11 中将多媒体内容播送给多个用户家庭网络 200，也就是用户域。

[0022] 系统包括提供多媒体内容的 DVB 内容源 101。使用播送内容密钥 106（如有条件存取安全密钥）来加密所述内容。内容可以通过参数加以识别，所述参数如 ONID（原始网络 ID）、TSID（传送流 ID）、SVID（服务 ID）和任选地 EVID（事件 ID）。

[0023] 内容在步骤 11 中由复用器 102 加以接收，复用器 102 组合来自各种源的内容，而且生成传送流，以便播送到用户域 200。复用器 102 还在步骤 12 中将加密播送事件列表提

供给使用权限信息生成器 103。使用权限包括传输事件的识别符（如 ONID、TSID、SVID 和 EVID），连同特定事件的 CA 限制条件有关的信息。生成器 103 针对特定事件生成内容密钥（如果特定 CA 保护系统需要，那么包括使用权限信息 (URI)），而且在步骤 13 中将内容密钥传输到许可证控制器服务器 104。许可证控制器服务器生成域内容密钥，从而允许加密所述内容，以便家庭网络 200 的用户域中的家庭装置进行接收。

[0024] 在家庭网络上，网关 201 在步骤 14 中接收所播送的多媒体内容。网关 201 可以是机顶盒，用于接收特定类型的 DVB 播送信号，诸如 DVB-C、DVB-S、DVB-T 或 DVB-H。网关 201 能够在步骤 15 中通过使用（例如）具有智能卡 (SC) 203 的 CA 安全系统，来解密所加密的内容。多个家庭装置 204、205（如个人计算机、膝上型计算机、掌上型计算机、智能电话、机顶盒、电视机等）与网关 201 相连。为了使所述内容（其可以由于 URI CA 而进行共享）可用于装置 204、205，STB 网关在步骤 16 中向许可证控制器服务器 104 索要特定事件的域内容许可证，所述特定事件通过（例如）ONID、TSID、SVID 和任选地 EVID 加以识别。

[0025] 在所述系统初始化时，网关 201 和装置 204、205 在步骤 10 中针对用户域进行注册。注册由用户发起。举例而言，家庭网络的用户可以在域控制器服务器上设置账户，其中所述账户可以确定家庭网络中可以共享所述内容的装置的数量、特定装置的用户权限（包括父代控制权限）、内容权限（存取附加或正常内容）等。在账户设置时确定的参数会界定特定装置 204、205 对网关 201 所共享内容的可存取性。每个装置，通过提供所述装置的至少识别符（如 X.509 证书），而在域控制器服务器 105 上注册，所述识别符对于所述装置而言是独特的且可以用来生成域内容密钥。

[0026] 当许可证控制器服务器 104 接收域许可证的请求时，其在步骤 17 中，在域控制器服务器上验证网关 201 成员资格。验证可以涉及到检查特定网关 201 是否在域控制器服务器 105 上注册、其使用权限是什么、与所述网关 201 相关联的家庭装置 204、205 是什么，等等。在步骤 18 中接收到成功验证结果之后，许可证控制器服务器 104 在步骤 19 中至少基于针对与特定网关 201 相关联的家庭网络而注册的家庭装置的识别符，来生成域内容许可证。然后，在步骤 20 中将域内容许可证发送给网关 201。域内容许可证可以优选地含有使用权限信息。

[0027] 举例而言，如果家庭装置 204、205 的识别符是以 X.509 证书的形式提供，那么域内容许可证可以包括针对特定家庭装置 204、205 的公共密钥。

[0028] 在接收域许可证时，网关 201 在步骤 21 中从域许可证中提取域内容密钥，而且使用域内容密钥来加密多媒体内容。因此，加密内容可以由网关 201 以及针对特定家庭网络（用户域）而注册的装置 204、205 加以存取（也就是，可以由它们进行解密）。优选地，所述加密内容只可以由针对网关 201 的特定家庭网络而注册的装置 204、205（以及网关自身）进行解密。举例而言，加密可以利用 AES-CTR 机制或其他机制，这取决于所述系统中所使用的数字权限管理系统的类型。网关 201 可以生成 PIFF 格式（保护互操作文件格式）或其他格式的内容，这取决于用户域和所选传送内所使用的加密技术，包括嵌入式域许可证。然后，在步骤 22 中将所述内容提供给家庭网络的装置 204、205。网关 201 可以利用 DRM PlayReady(R) 内容保护机制。所述内容可以在步骤 23 中，从这些装置 204、205 播送到其他装置 204、205 或者按需提供。加密内容可以存储在海量存储装置 202（如网关 201 的硬盘）上或云存储器中。这允许在接收内容之后，在时间延迟的情况下将多媒体内容提供给

家庭装置 204（前提是时间延迟并未超出使用权限限制条件）。

[0029] 内容经由通常用于 DVB-C、DVB-S、DVB-T 或 DVB-H 网络的传输信道，而从前端系统传输到用户域。举例而言，网关 201 经由互联网（使用以太网、WiFi、DVB-C 系统（例如，DOCSIS）中的回传信道，优选地经由加密信道）来与许可证控制器服务器进行通信。

[0030] 本领域技术人员可以轻易地认识到，上述用于分配多媒体内容的方法可以由一个或多个专用电子电路或计算机程序加以执行和 / 或控制。此类计算机程序通常利用装置的计算资源加以运行。所述计算机程序可以存储在非易失性存储器（或者非临时性计算机存储介质），例如闪存中，或者存储在易失性存储器，例如 RAM 中，并且由处理单元加以运行。这些存储器是示范性记录介质，用于存储计算机程序，包括相应的计算机可运行指令，其执行根据本文所陈述的技术概念的方法的所有步骤。

[0031] 虽然已参考特定的优选实施方案来描绘、描述并已定义文中陈述的本发明，但是前述说明书中的实施方式的这些参考和示例并不意味对本发明的任何限制。然而，较为明显的是，可在不脱离技术概念的较宽范围的情况下对本发明作出各种修改和变化。本发明的优选实施方案仅仅是示例性的，而且并不是本文所陈述的技术概念的范围的详尽内容。因此，保护范围不限于本说明书中描述的优选实施方案，而仅由随附权利要求书加以限制。

[0032] 另外，本申请中设想所附权利要求的任何组合。

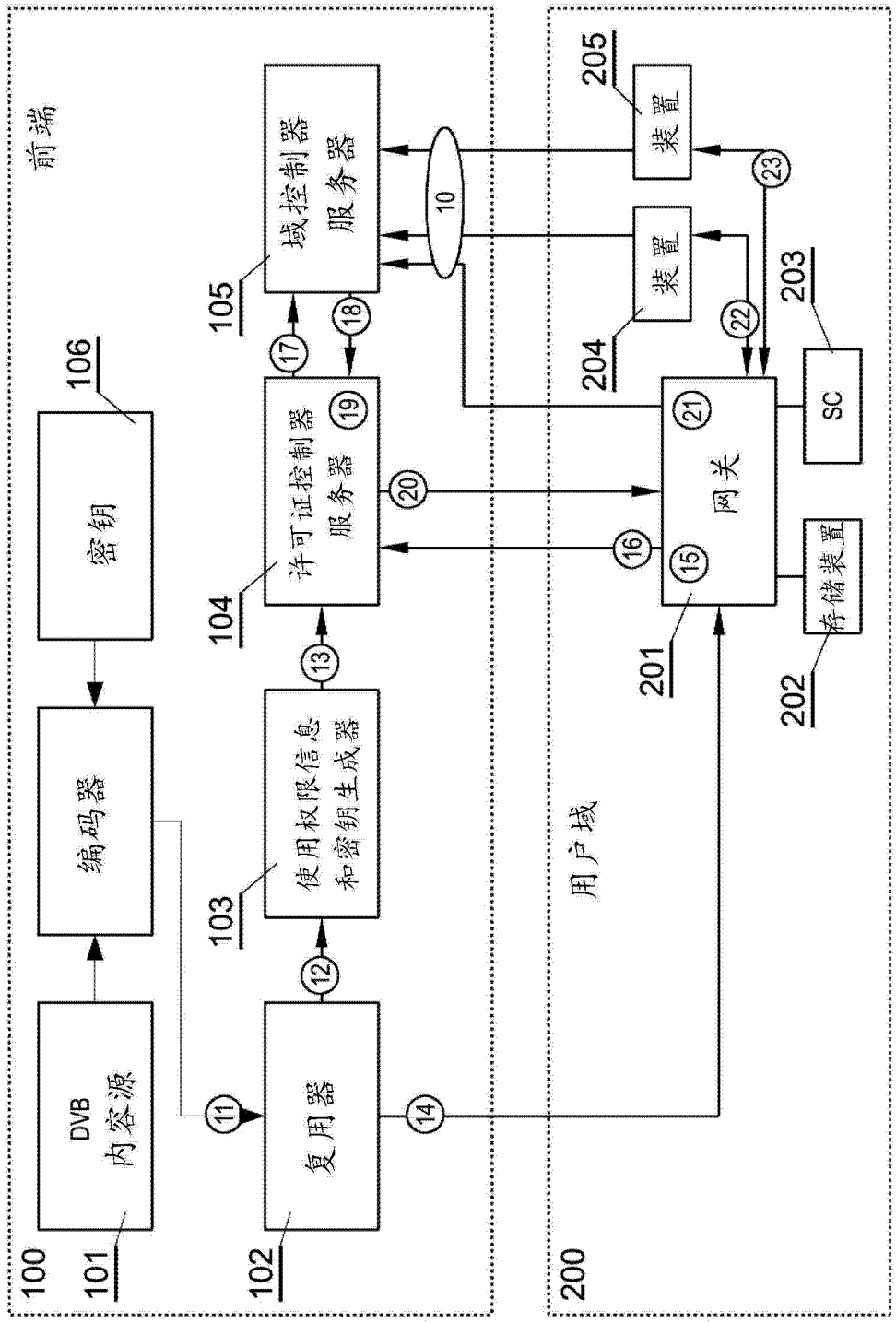

前端
100
DVB
内容源
101
编码器
密钥
106
复用器
102
使用权限信息
和密钥生成器
103
许可证控制器
服务器
104
域控制器
服务器
105
10
用户域
200
网关
201
存储装置
202
SC
203
装置
204
装置
205
11
12
13
14
15
16
17
18
19
20
21
22
23

图 1