(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 103444195 A
(43)申请公布日 2013.12.11

(21)申请号 201280015182.9
(22)申请日 2012.02.24
(30)优先权数据
1105156.2 2011.03.28 GB
(85)PCT申请进入国家阶段日
2013.09.25
(86)PCT申请的申请数据
PCT/GB2012/050429 2012.02.24
(87)PCT申请的公布数据
WO2012/131316 EN 2012.10.04
(71)申请人 索尼公司
地址 日本东京
申请人 索尼欧洲有限公司
(72)发明人 戴维·理查德·希尔-乔伊特
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 吴孟秋
(51)Int.Cl.
H04N 21/266(2006.01)
H04N 21/418(2006.01)
H04N 21/436(2006.01)
H04N 21/4623(2006.01)
H04N 21/6377(2006.01)

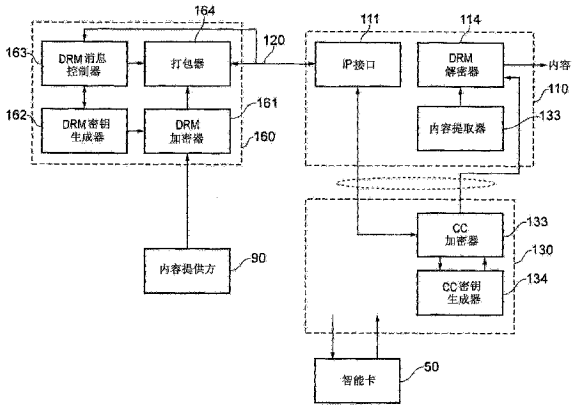
权利要求书2页 说明书9页 附图5页

(54)发明名称

内容加密

(57)摘要

一种音频/视频内容传送系统包括由互联网数据连接链接至内容接收器的内容源，该内容接收器被配置为经由互联网数据连接从内容源接收内容并且通过单独的广播数据路径从该内容源或另一个内容源接收访问受控的编码广播内容，其中，所述内容源包括加密器，该加密器用于根据内容加密密钥将加密的内容经由互联网数据连接发送给内容接收器；所述内容接收器包括：主机模块，具有解密器，该解密器用于将通过互联网数据连接从内容源接收的加密内容解密；以及可移除的条件访问模块(CAM)，所述CAM具有访问控制单元，该访问控制单元用于对访问受控的编码广播内容进行解码，主机模块和可移除的CAM被设置为在条件访问模块和主机模块之间为解码的访问受控的编码广播内容提供加密的通信链接；其中：内容源和CAM被配置为通过互联网数据连接进行通信，从而建立主机模块内的解密器对从内容源接收的加密内容进行解密所需要的密钥。



CN 103444195 A

1. 一种音频 / 视频内容传送系统，包括通过互联网数据连接链接至内容接收器的内容源，所述内容接收器被配置为经由所述互联网数据连接从所述内容源接收内容并且通过单独的广播数据路径从所述内容源或另一个内容源接收访问受控的编码广播内容，其中：

所述内容源包括：加密器，用于根据内容加密密钥将加密内容经由所述互联网数据连接发送给所述内容接收器；

所述内容接收器包括：

主机模块，具有解密器，该解密器用于将经由所述互联网数据连接从所述内容源接收的加密内容解密；以及

可移除的条件访问模块（CAM），所述 CAM 具有访问控制单元，该访问控制单元用于对所述访问受控的编码广播内容进行解码，所述主机模块和所述可移除的 CAM 被设置为在所述条件访问模块与所述主机模块之间为解码后的访问受控的编码广播内容提供加密通信链接；

其中：

所述内容源和所述 CAM 被配置为经由所述互联网数据连接进行通信，从而建立所述主机模块内的所述解密器解密从所述内容源接收的所述加密内容所需要的密钥。

2. 根据权利要求 1 所述的系统，其中：

所述 CAM 与所述主机模块共享加密密钥信息，以允许在所述 CAM 与所述主机模块之间进行加密通信；

所述 CAM 被配置为将该共享密钥信息的至少一部分传输给所述内容源；以及

所述内容源被配置为使用从所述 CAM 接收的所述密钥信息来加密内容，以传输给所述主机模块。

3. 根据权利要求 1 所述的系统，其中：

所述内容源被配置为将用于对所述加密内容进行解密的密钥信息传送给所述 CAM；以及

所述 CAM 被配置为经由在所述 CAM 与所述主机模块之间的所述加密通信链接将从所述内容源接收的所述密钥信息传输给所述主机模块。

4. 根据任一前述权利要求所述的系统，其中，所述 CAM 和所述内容源被配置为经由所述互联网数据连接建立安全的低速通信链接。

5. 根据任一前述权利要求所述的系统，其中，在内容源处的所述加密器被配置为使用对称加密算法为内容加密，用于传输给内容接收器。

6. 根据权利要求 5 所述的系统，其中，在所述 CAM 与所述主机模块之间的所述加密通信链接根据对称加密算法运行。

7. 根据权利要求 6 所述的系统，其中，在所述 CAM 与所述主机模块之间的所述加密通信链接、在所述内容源处的所述加密器以及在所述内容接收器处的所述解密器根据相同的加密算法运行。

8. 根据权利要求 7 所述的系统，其中，所述加密算法为 AES 算法。

9. 根据任一前述权利要求所述的系统，其中，在所述 CAM 与所述主机模块之间的所述加密通信链接根据专用于该特定的 CAM 与主机模块对的密钥信息运行。

10. 根据任一前述权利要求所述的系统，其中，所述内容源被配置为将数据发送给所述

主机模块作为 IP 电视数据。

11. 根据任一前述权利要求所述的系统，其中，所述 CAM 为根据通用接口增强标准的 CAM。

12. 根据任一前述权利要求所述的系统，其中，所述内容源和所述 CAM 被配置为经由所述互联网数据连接进行通信，从而不时地改变所述主机模块内的所述解密器解密从所述内容源接收的所述加密内容所需要的密钥。

13. 一种音频 / 视频内容接收器，被配置为经由互联网数据连接从内容源接收加密内容，并且通过单独的广播数据路径从该内容源或另一个内容源接收访问受控的编码广播内容，所述内容接收器包括 ：

主机模块，具有解密器，该解密器用于将经由所述互联网数据连接从所述内容源接收的加密内容解密 ；以及

可移除的条件访问模块（CAM），所述 CAM 具有访问控制单元，该访问控制单元用于对所述访问受控的编码广播内容进行解码，所述主机模块和所述可移除的 CAM 被设置为在所述条件访问模块与所述主机模块之间为解码后的访问受控的编码广播内容提供加密通信链接 ；

其中 ：

所述 CAM 被配置为经由所述互联网数据连接与所述内容源进行通信，从而建立所述主机模块内的所述解密器解密从所述内容源接收的所述加密内容所需要的密钥。

14. 一种音频 / 视频内容传送方法，其中，内容源通过互联网数据连接被链接至内容接收器，所述内容接收器被配置为经由所述互联网数据连接从所述内容源接收内容并且通过单独的广播数据路径从该内容源或另一个内容源接收访问受控的编码广播内容，并且所述内容接收器具有 ：主机模块，具有解密器，该解密器用于将经由所述互联网数据连接从所述内容源接收的加密内容解密 ；以及可移除的条件访问模块（CAM），所述 CAM 具有访问控制单元，该访问控制单元用于对所述访问受控的编码广播内容进行解码，所述主机模块和所述可移除的 CAM 被设置为在所述条件访问模块与所述主机模块之间为解码后的访问受控的编码广播内容提供加密的通信链接 ；

所述方法包括 ：

所述内容源和所述 CAM 经由所述互联网数据连接进行通信，从而建立所述主机模块内的所述解密器解密从所述内容源接收的所述加密内容所需要的解密密钥 ；以及

所述内容源根据适合于所述主机模块内的所述解密器处建立的所述解密密钥的内容加密密钥，加密并经由所述互联网数据连接发送加密内容至所述内容接收器。

15. 一种计算机软件，用于实现根据权利要求 14 所述的方法。

16. 一种计算机程序产品，包括储存根据权利要求 15 所述的计算机软件的储存介质。

内容加密

技术领域

[0001] 本发明涉及在传送加密视频和 / 或音频内容(例如,电视内容)的系统内的对音频和 / 或视频内容的加密。

背景技术

[0002] 作为背景技术,DVB 通用接口(“CI”)规范允许电视接收器或机顶盒(“主机”)与安全硬件模块(条件访问模块或“CAM”)交互,以使得主机可以对访问受控的内容解密。CI 规范规定在主机和 CAM 之间的接口,从而如果主机和 CAM 符合 CI 规范,那么这两者协作。由于在原则上,这种互操作性允许用户选择不同制造商的兼容产品,所以这种互操作性提供了 CI 系统的显著优势。

[0003] 在 CI 规范内,CAM 与智能卡和 / 或用户的个人识别号码(“PIN”)相互作用,以提供用户认证。

[0004] 然而,原始 CI 规范的缺点在于,提供了复制经解密的数字内容的可能性。这个问题由主机和 CAM 相互作用的方式引起。在使用时,主机将加密数据发送给 CAM。CAM 检查用户认证,并且假设已认证用户,那么将访问受控的内容解密。然后,CAM 通过 CAM 主机接口将解密的内容送回主机,虽然该接口不限于 PCMCIA (个人计算机存储卡国际协会)接口,但是通常为这种接口,例如,可使用 USB 接口。从 CAM 到主机的这种连接存在着安全漏洞,这是因为在原则上可拦截并且非法复制解密的数字内容。该安全漏洞意味着某些内容提供方优选将主机和 CAM 用作单个单元的集成装置,这是因为这允许在将未加密数据从 CAM 传输到主机时具有更好的安全性。然而,这当然违反 CI 关于不同 CAM 和主机可能具有的互操作性的优点。

[0005] CI 增强规范被设计为通过两个主要路线解决这些问题。CI 增强规范在 CAM 和主机之间提供安全接口,从而在这两个装置之间并不是以透明的形式发送解密后的内容数据。而且,CI 增强规范提供主机和 CAM 两者的认证,而非 CI 技术中的仅仅认证 CAM。

[0006] 认证系统使用证书层次结构,从而主机和 CAM 必须均已经由当局签发证书(例如,CI 增强 LLP)。

[0007] 在从 CAM 发送到主机之前,将解密的内容数据加密,然后,在主机处解密,从而保护在主机和 CAM 之间的 PCMCIA 接口。该加密与由内容提供方建立的访问控制加密 - 解密分开,并且专用于每个特定的 CAM- 主机对。通过 Diffie-Hellman 密钥交换技术,在 CAM 和主机之间交换密钥。这些密钥也时常循环,从而即使一个密钥损坏,无论如何也会在几秒钟以后更换该密钥。

[0008] CI 增强规范提供进一步的特征,例如,所谓的使用权限信息(URI),该信息允许内容提供方规定由主机应用于内容的内容保护等级。

[0009] 总之,使用由认证机构签发的证书,在 CAM 和主机之间形成可信信道。

发明内容

[0010] 本发明提供了一种音频 / 视频内容传送系统，包括通过互联网数据连接链接至内容接收器的内容源，该内容接收器被配置为经由互联网数据连接从内容源接收内容并且通过单独的广播数据路径从该内容源或另一个内容源接收访问受控的编码广播内容，其中：

[0011] 内容源包括加密器，该加密器用于根据内容加密密钥将加密的内容经由互联网数据连接发送给内容接收器；

[0012] 内容接收器包括：

[0013] 主机模块，其具有解密器，该解密器用于将经由互联网数据连接从内容源接收的加密内容解密；以及

[0014] 可移除的条件访问模块（CAM），CAM 具有访问控制单元，该访问控制单元用于为访问受控的编码广播内容解码，所述主机模块和所述可移除的 CAM 被设置为在条件访问模块与主机模块之间为解码后的访问受控的编码广播内容提供加密的通信链接；

[0015] 其中：

[0016] 内容源和 CAM 被配置为通过互联网数据连接进行通信，从而建立主机模块内的解密器解密从内容源接收的加密内容所需要的密钥。这种内容可基于节点到节点发送（即，传输）给专用接收器，或者这种内容可为广播互联网内容。

[0017] 本发明认识到，在使用 CAM（虽然并非完全地）（例如，CI 增强 CAM）的系统内，在主机和 CAM 之间已经具有安全加密通信路径。通常，这会使用对称加密算法，例如，AES 算法。

[0018] 因此，本发明认识到，该安全加密通信路径可有助于建立一个或多个密钥，用于将内容从内容源中安全地传输到内容接收器中。

[0019] 在一个实例中，可由 CAM 将用于在 CAM 和主机之间建立安全加密通信路径的共享的密钥信息的至少一部分发送给内容源。通过这种方式，内容源可利用通过该安全加密通信路径的建立而被该主机已知的密钥对用于传输到该主机以供解密的内容进行加密。

[0020] 在另一个实例中，CAM 可与内容源协商密钥，供主机使用，以将加密的内容解密。然后，CAM 可利用安全加密的通信路径，通过安全的方式将该密钥发送给主机。

附图说明

[0021] 现在，参照附图，仅仅通过实例，描述本发明的实施方式，其中：

[0022] 图 1 为具有 CAM 和智能卡的主机装置的示意图；

[0023] 图 2 为包括图 1 的主机装置的条件接收（CA）系统的示意图；

[0024] 图 3 为示出图 2 的系统操作的示意图；

[0025] 图 4 示意性示出一种 IPTV 音频 / 视频内容传送系统；

[0026] 图 5 示意性示出在图 4 的 IPTV 内容传送系统内进行的内容信号处理；

[0027] 图 6 示意性示出在图 4 的 IPTV 内容传送系统内进行的密钥数据处理；

[0028] 图 7 为示出图 4 的系统的一个操作模式的示意性流程图；以及

[0029] 图 8 为示出图 4 的系统的另一个操作模式的示意性流程图。

具体实施方式

[0030] 现在参照图 1，主机装置 10 在此处显示为电视机，但是可为例如机顶盒（要注意，对于技术人员，措辞“机顶盒”并非表示在使用时对该装置的特定物理位置的任何要求）。主

机装置 10 通过广播数据路径接收访问受控的电视信号 15。虽然在下面讨论其他类型的电视信号，但是这可为例如由圆盘式卫星接收天线（未显示）接收的卫星电视信号、地面电视信号、电缆电视信号等。主机装置 10 具有 PCMCIA 插槽 20，该插槽包括电气连接以及用于插入式模块的物理空间，电气连接与物理空间均根据 PCMCIA 标准。

[0031] CI 增强条件访问模块称为 CICAM30，是可插入 PCMCIA 插槽 20 内的 PCMCIA 模块。在 CICAM30 完全插入插槽 20 内时，在 CICAM30 上的连接器和在插槽 20 内的配合连接器之间形成电气连接。要注意的是，虽然描述了 CI 增强 CAM 的实施方式，但是其他类型的可移除的 CAM 适用于本技术。

[0032] CICAM 本身可为无卡式模块或者可具有插槽 40，所谓的智能卡 50 可插入该插槽内。智能卡可移除并且以防干扰、安全以及非易失性形式携带限定内容接收器的当前用户的信息。在智能卡完全插入插槽 40 内时，通过使用在智能卡 50 上以及在插槽 40 内的配合电气连接器，或者通过使用在非常短的距离（例如，1 到 2cm）内无线传输数据的已知非接触式连接技术，在智能卡 50 和 CICAM30 之间形成数据连接。

[0033] 图 2 示意性示出了在条件接收系统的背景下的主机装置 10。所谓的前端（head end）60 表示访问受控的电视信号 15 的源。前端可表示例如卫星广播设备的上行链接站或地面或电缆广播设备的信号分配中心。CA 系统使用 CA 系统加密对在前端的内容加扰。前端也可将其他与 CA 相关的信息引入加密数据流内，这使得 CICAM 能够将内容解扰并且管理用户的（使用者的）访问和授权。

[0034] 前端 60 将电视信号 15 发送给主机 10，该主机转而将信号传送给 CICAM30，用于对访问控制加密进行解密。然后，CICAM30 使用本地加密为该信号再次加密，并且通过 PCMCIA 连接将再次加密的信号发送回主机 10。主机对从 CICAM30 接收的信号进行解密，以用于在显示屏上显示或者用于提供给另一个装置 70，例如，基于硬盘的录像机。

[0035] 图 3 为示出图 2 的系统操作的示意图。在 CI 增强规范 1.3（2010-01）中，描述了图 3 的系统的详细操作，在 http://www.ci-plus.eom/data/ci-plus_specification_v1.3.pdf 处（在申请时）可获得该规范。该文档并入本说明书内，以作参考。图 3 的描述简单地概述了该详细操作，其目的在于，将随后的说明置于适当的技术背景内。

[0036] 如上所述，图 3 示出了前端 60（其从内容提供方 90 接收内容信号）、主机装置 10、CICAM30 以及智能卡 50。信号 15 被示出为被从前端 60 传送到主机装置 10。在主机装置 10 和 CICAM30 之间的安全接口 80 称为通用接口。

[0037] 条件接收

[0038] 已知的 CA 系统提供可拒绝或允许用户访问数字电视流的技术。仅仅为具有有效支付账号的那些用户或使用者提供访问。在实践中，为用户提供智能卡 50，该智能卡通过（理想地）无干扰的方式标识该用户，并且建立该系统，从而只有具有有效智能卡的用户能够获得对访问受控的内容的访问。

[0039] 通过使用加扰和加密，提供访问控制。使用 8 字节控制字为内容信号加扰，该控制字频繁地改变（每分钟高达几次），以避免 CA 系统受到控制字外泄的损害。通过加密的形式将控制字作为授权控制消息（ECM）发送给接收器的 CICAM，用于为加扰的内容解扰。只有在 CICAM 通过接收授权管理消息（EMM）被授权解密控制字以允许将访问受控的内容解扰时，CICAM 才会这么做。EMM 专用于每个用户或用户组；通过比较在 EMM 内提供的用户标识和在

智能卡 50 内提供的用户信息，CICAM 确认 EMM 提供的权利。与 ECM 相比，可不太频繁地发送 EMM，在当前商业系统内的连续 EMM 之间的间隔在 12 分钟与 6 周之间变化。

[0040] ECM 和 EMM 本身是在 MPEG 电视分配系统内众所周知的消息类型。在使用时，其有效载荷的格式可专用于 CA 系统中，在格式之间的差异通常是语义性的，而没有技术意义。

[0041] 前端

[0042] 前端 60 包括 CA 加密器 61、密钥生成器 62、授权控制单元 63 以及多路复用器和调制器 64。

[0043] 内容提供方 90 将内容(例如，电视信号)提供给前端 60。前端 60 将条件访问(CA)加扰和加密施加于该内容中。

[0044] 更具体而言，CA 加密器 61 将 CA 密钥用作控制字，对内容加密或加扰。CA 密钥由 CA 密钥生成器 62 生成。将由 CA 加密器生成的加扰的内容提供给多路复用器和调制器 64。

[0045] 还将 CA 密钥提供给授权控制单元 63，该单元根据 CA 密钥生成 ECM 并且根据规定了哪些用户被授权解扰哪些内容流的用户数据生成 EMM。将 ECM 和 EMM 提供给多路复用器和调制器 64。来自 CA 加密器 61 的一个或多个加扰的内容流、一个或多个未加扰(开放访问或“免费接收”)的内容源和授权控制消息共同多路复用，以形成传输流，例如，MPEG2 传输流。已知的格式用于携带内容数据、ECM 和 EMM。ECM、EMM 以及限定在每个基本流(与单独的加扰内容流对应)上使用的加扰类型的数据以已知的格式提供在条件访问表(CAT)内，该条件访问表具有预定的程序标识符(PID)0x001，从而可在 CICAM 处识别 CAT。

[0046] 然后，由多路复用器和调制器 64 调制多路复用的传输流，用于作为电缆、卫星或地面广播信号 15 进行传输。

[0047] 主机装置

[0048] 主机装置 10 包括调谐器 11、解调器和解复用器 12、解复用器(“多路分用器”)13 和 CC(内容控制)解密器 14。要注意的是，主机装置可具有其他额外的功能，例如，网络(IPTV)电视接收。

[0049] 根据广播信号 15 的类型，调谐器用于将所接收的信号变换回基带，从而解调器和解复用器 12 可从所接收的信号中选择和解复用单个基本内容流和相关的 CAT 数据。通过通用接口 80 将内容流和 ECM/EMM 数据传递给 CICAM30。

[0050] 在访问受控的内容数据的情况下，由于通过通用接口 80 将内容数据传递给 CICAM30，所以在该阶段，依然将内容数据加扰。由于 CA 加密，所以通过通用接口 80 进行传输的这部分因此安全。

[0051] 假设 ECM 和 EMM 允许这样做，那么 CICAM30 对内容数据解扰并且使用内容控制(CC)加密对该内容数据再次加密。下面将描述这样做的方式。CC 加密的数据返回主机装置 10，其中，该数据由解复用器 13 解复用并且由 CC 解密器 14 解密，从而该内容可作为清晰的内容显示或传递给另一个装置 70。

[0052] CICAM

[0053] CICAM30 包括 CA 解密器 31、CA 密钥生成器 32、CC 加密器 33 以及 CC 密钥生成器 34。

[0054] CA 解密器 31 和 CA 密钥生成器 32 可视为访问控制单元，用于为访问受控的广播内容或其他数据解码。CICAM30 的 CC 密钥生成器 34 和 CC 加密器 33 以及主机装置 10 的解复

用器 13 和 CC 解密器 14 配合，用于在 CICAM 和主机装置之间为解码后的访问受控的编码广播内容提供加密的通信链接（通用接口 80）。

[0055] CA 解密器 31 使用由 CA 密钥生成器 32 利用智能卡 50 的用户身份的校验而根据所接收的 ECM 和 EMM 生成的密钥，将所接收的访问控制内容解扰。CICAM 的这部分操作使用已知的 CA 技术来获取和应用 CA 密钥。

[0056] 将清晰的内容数据从 CA 解密器 31 中传递到 CC 加密器 33 中。然而，在该数据传输完全位于 CICAM 内部时，通过已知的技术，例如，通过在单个集成电路装置内提供 CA 解密器 31、CC 加密器 33 以及清晰的内容接口，可使该数据传输安全并且防干扰。

[0057] CC 加密器 33 使用由 CC 密钥生成器 34 提供的 CC 密钥为解扰后的内容加密。该密钥通过在 CI CAM30 与主机装置 10 之间的安全互换建立，并且专用于该 CICAM- 主机装置对。通过通用接口 80 将 CC 加密的内容传送给主机装置 10。因此，在内容数据传递给主机装置时，该内容数据被 CC 加密，此时，通用接口的这部分也安全。

[0058] 密钥交换

[0059] CICAM30 和主机装置 10 均包含逻辑、固件或软件，该逻辑、固件或软件提供 :用于 Diffie-Hellman （DH）安全密钥交换的算法、使用已知算法 SHA-256、DES 以及 AES 的散列法和加密、由发证机构（例如，新 CI LLP）发布的各个证书、以及具有相应的公开密钥的私有密钥。

[0060] 在 CICAM30 首先与主机装置 10 相关时，CICAM30 启动与主机装置 10 的认证过程。在这个过程中，每个装置验证对方的证书，并且发生 DH 密钥交换处理，从而在这两个装置之间安全地共享密钥。具体地，CICAM 首先请求主机装置提供其证书数据。CICAM 验证在主机装置证书上的签名。然后，由主机执行相同的处理，请求和验证 CICAM 证书。然后，通过签署 DH 公共密钥并且将该密钥发送给对方装置以供验证，从而 CICAM 和主机均表明拥有与在证书内公共密钥对应的私有密钥。然后，CICAM 从主机中获得并且验证认证密钥 AKH。CICAM 和主机开始计算和交换用于为通过通用接口 80 发送的数据进行加密和认证的密钥数据。通过这种方式，密钥、密钥对或由 CICAM 和主机建立的用于通过通用接口 80 进行通信的其他密钥信息对于该 CICAM- 主机对来说是专用的。

[0061] 在认证之后，CICAM 也开始计算 CC 密钥。CICAM 也可指导主机装置计算 CC 密钥。然后，如上所述，CC 密钥用于根据算法 AES 对从 CICAM30 中传送到主机装置 10 的内容数据进行加密。因此，要理解的是，用于安全的通用接口 80 的密钥专用于一个特定的 CICAM- 主机对。

[0062] 现在描述在通过互联网传送的电视内容（所谓的 IPTV 或互联网协议电视）的情况下使用部分或所有上述设置以提供访问控制的技术。

[0063] 概括地说，并且参照图 4，IPTV 提供方的前端 160 用作内容源，通过互联网数据连接 120 将访问受控的电视内容传送给运行主机应用 110 的主机装置（作为内容接收器的主机装置）。主机应用与前端 160 以及与相关的 CICAM130 进行通信，以确认用户访问该内容的权利。如果这些权利有效，那么前端 160 开始通过 IP 将作为视频的该内容发送给主机应用，该内容可使用加密技术（例如，AES 算法）加扰。主机应用 110 将所接收的内容解扰并且使该内容在显示屏 140 上进行显示。要注意的是，在 IPTV 接收的方面，通常不需要 CICAM ;在图 4 中所示的内容接收器实际上被配置为通过互联网数据连接 120 接收内容，并且在另一

种操作模式中，被配置为通过单独的广播数据路径接收访问受控的编码广播内容信号 15。广播内容源和互联网内容源可为相同的内容源（在不同的模式中进行操作）或者可为不同的内容源。该内容源和内容接收器共同形成内容传送系统。

[0064] 在下面要描述的技术中，CC 密钥本身用于将加扰的 IPTV 内容解扰，或者 CC 加密用于将 CAM 从主机中获得的密钥从 CAM 中安全地发送到主机中。在任一种情况下，内容源和 CAM 被设置为通过互联网数据连接进行通信，从而建立主机装置内的解密器解密从 IPTV 内容源接收的加密的内容所需要的密钥。

[0065] 图 5 示意性示出在图 4 的 IPTV 内容传送系统内进行的内容信号处理。

[0066] 在图 5 中所示的特征与在图 3 中所示的特征具有相似性，但是在 IPTV 传送的背景下，内容接收器通过互联网连接与内容源连接并且被配置为通过互联网连接从内容源接收内容并且通过单独的广播数据路径（例如，卫星、地面或电缆链接）从该或另一个内容源接收访问受控的编码广播内容。

[0067] 前端 160 包括 DRM（数字版权管理）加密器 161，该加密器从内容提供方 90 接收内容数据并且从 DRM 密钥生成器 162 接收密钥。由 DRM 消息控制器 163 处理向或从内容接收器通信的 DRM 密钥的通信。内容和消息数据由打包器（packetiser）164 打包，用于通过互联网数据连接 120 进行传输。DRM 加密器 161 用作为根据内容加密密钥经由互联网数据连接 120 将加密的内容发送给内容接收器的加密器。

[0068] 主机应用包括 IP（互联网协议）接口 111，其将所接收的数据传送给拆包器（depacketiser）112。内容提取器 113 从拆包的数据中检索内容，并且将该内容传送给 DRM 解密器 114，该解密器将经由互联网数据连接 120 从内容源接收的加密内容解密，以传送给例如显示器 140。

[0069] 该系统包括可移除的 CI 增强 CAM（CICAM）130，但是在 IPTV 传输系统内未使用 CICAM130 的多个特征。与本公开相关的是 CC 密钥生成器 134 和 CC 加密器 133（虽然不一定与在图 5 中所示的内容信号处理相关）。智能卡 50 依然可连接至 CICAM130 并且可用于或不用于该系统内以进行用户认证。

[0070] 在图 5 中的内容分配路径因此如下。主机应用 110 与前端 160 交互，以确定要将内容数据从作为内容源的前端 160 中发送到作为内容接收器的主机应用 110。这个交互的阶段可为传统阶段。例如，主机应用的用户可将主机应用指向与前端相关的互联网地址，前端工作于互联网广播的模式或者点对点的传输模式。或者，主机应用的用户可选择查看内容（例如，视频点播（VOD）电影），并且主机应用查阅查找表，以确定可从其中接收该内容的前端，然后，主机应用对该前端发布请求。前端已经开始分配所需内容（在多接收器或广播操作模式的情况下）或者响应于主机应用的请求开始进行分配。

[0071] 前端 160 的 DRM 加密器 161 通过内容密钥为所需内容加密。主机应用的 DRM 解密器也掌握该密钥（在对称加密算法的情况下）或互补型私有密钥（在非对称或公共 - 私有密钥加密算法的情况下）。下面参照图 6 到 8 描述分配密钥的方法。

[0072] 加密内容被打包，并且由前端 160 通过互联网数据连接 120 将该内容发送给主机应用 110，其中，该加密内容被拆包并且 DRM 所保护的内容由 DRM 解密器 114 解密以供显示。

[0073] 在本发明的实施方式中，CICAM130 不需要直接参与 IPTV 内容分配数据路径；其仅仅用于提供或分配密钥信息。

[0074] 图 6 示意性示出在图 4 的 IPTV 内容传送系统内进行的密钥数据处理。

[0075] 在图 6 的示图中再现图 5 的个体特征，除了密钥分配路径不需要的拆包器 112 以外。

[0076] 在图 6 中显示了该设备的两个主要可选的操作模式。参照图 7 的示意性流程图描述第一模式，并且参照图 8 的示意性流程图描述第二模式。要注意的是，图 8 仅仅示出了与图 7 的流程图不同的那些步骤。即，在图 7 中的步骤 230（下面要进行描述）可通向图 7 中的步骤 240，或者在另一个实施方式中，沿着一个不同的路线通向图 8 中的步骤 270。

[0077] 首先描述在图 7 中所示的配置。在该配置中，CAM 和主机模块共享加密密钥信息，以允许在 CAM 和主机模块之间进行加密通信（通过安全接口 80）；CAM 被配置为将该共享的密钥信息（CC 密钥信息）的至少一部分发送给内容源；并且内容源被配置为将从 CAM 接收的密钥信息用于加密内容，从而传输到该主机模块。

[0078] 该处理在步骤 200 处开始，CICAM130 和主机应用 110 交互。在步骤 210 处，CICAM130 检查是否已经存在用于在 CICAM 的 CC 加密器 133 和主机应用之间进行安全数据交换的密钥对。如果已经存在这种密钥对，那么将控制前进至步骤 230。否则，将控制前进至步骤 220，在该步骤中，CICAM 和主机应用执行安全密钥交换，以在其间建立密钥对，用于进行安全通信。

[0079] 要注意的是，如在上述说明书文件中所定义的，步骤 210 和 220 涉及 CI 增强 CAM 的标准操作。还要注意的是，在本发明的实施方式中（并且在 CI 增强标准中），CC 加密器 133 可使用对称加密算法（例如，AES 算法），在这种情况下，在 CICAM 和主机应用之间建立的“密钥对”表示相同的密钥，以用于这两个节点的每个节点处。在另一实施方式中，CICAM 和主机应用可使用非对称算法，其中，发生初始的密钥交换，使得 CICAM 掌握与由主机应用掌握的私有密钥对应的公共密钥。

[0080] 在步骤 230 处，CICAM130 与前端 160 建立安全通信链接。如在 CI 增强规范中所定义的，这可为例如通过互联网连接 120 的所谓的低速通信（LSC）链接 / 资源。如在新 CI 规范中所定义的，LSC 是允许 CAM 使用主机装置的互联网连接（IP 端口）作为到前端的返回路径的资源。CAM 和前端可使用散列（hashing）在其间的认证和 / 或加密和 / 或消息来确保使用 LSC 资源发送的消息的完整性和安全性。

[0081] 在步骤 240 处，CICAM 的 CC 加密器 133 将密钥信息发送给前端。尤其地，该密钥信息与已经在 CICAM 和主机应用之间交换的密钥对相关，从而主机应用可使用其对从与该主机应用相关的 CICAM 中的 CC 加密器直接发送至其的数据进行解密所使用的密钥相同的密钥将来自前端的内容解密。

[0082] 因此，在 CC 加密器使用对称加密算法通过安全接口 80 将数据发送给 CC 解密器的情况下，CICAM 的 CC 加密器 133 通过安全 LSC 链接将由 CC 加密器使用的共享密钥发送给前端 160，从而前端也可根据共享的密钥使用（或者通常相同）对称算法将内容传送给主机 110。该算法可为 AES 算法。在 CC 加密器将非对称算法用于与主机应用进行通信的情况下，CC 加密器将公共 - 私有密钥对的公共密钥发送给前端。要注意的是，在仅仅发送公共密钥的情况下，虽然实际上依然可使用安全链接，但是从 CC 加密器 133 到前端的链接并非严格地需要是安全链接。

[0083] 发送给前端 160 的密钥信息由 DRM 消息控制器 163 接收并且传递给 DRM 密钥生成

器 162，该生成器被配置为将适当的密钥数据提供给 DRM 加密器 161，以对内容数据加密，从而传输给该主机应用。在步骤 250 中，前端将加密内容数据发送给主机，并且在步骤 260 中，主机接收该数据并且利用该通过 CC 加密器 133 建立的密钥将该数据解密。

[0084] 要注意的是，在该实施方式中，DRM 加密器使用专用于特定的主机应用的加密密钥，因此，加密的数据包只适合于由该主机应用接收。

[0085] 图 8 示意性示出了系统操作，其中，内容源被配置为将用于对加密内容进行解密的密钥信息传送给 CAM，并且 CAM 被配置为在 CAM 和主机模块之间通过加密的通信链接（安全接口 80）将从内容源接收的密钥信息发送给主机模块。

[0086] 现在参照图 8，在一个可选的设置中，控制从步骤 230 前进到步骤 270 中，其中，前端通过由 CAM 与前端建立的 LSC 链接将解密密钥发送给 CICAM。该密钥由 CC 加密器 133 接收并且通过在 CICAM 和主机应用之间建立的安全 CC 链接传递（在步骤 280 中）给主机应用，在主机应用中，DRM 解密器 114 使用该密钥，将从前端接收的内容解密。

[0087] 通过 CICAM 发送给主机应用的解密密钥可为对称密钥或者可为公共 - 私有密钥对的私有密钥。DRM 加密器 161 使用合适的互补型密钥。

[0088] 步骤 290 和 300 与上述步骤 250 和 260 对应，除了一种情况以外：在步骤 300 中，主机应用使用由 CC 加密器 133 通过在 CICAM 和主机应用之间的安全链接传递给主机应用的密钥将该内容解密。要注意的是，在该实施方式中，DRM 加密器使用并非必须专用于一个特定的主机应用的加密密钥，因此，加密的数据包适合于由该主机应用并且可能由已经从前端接收相同密钥的其他主机应用接收。

[0089] 在任一个实施方式中，用于进行内容加密和解密的密钥可不时地变化。在图 7 的实施方式中，这可以通过 CICAM 与主机应用时常重复其初始的密钥交换处理（步骤 220），并将最新建立的密钥发送给前端而实现。由 CICAM 本身、由主机或者由前端的消息辅助实现步骤 220 的这种重复。在图 8 的实施方式中，在其自激励情况下，或者响应于 CICAM 要这样做的请求，前端可定期（或者更广泛地说不时地）将一个新密钥发送给 CICAM。在本发明的实施方式中，在停止使用旧密钥之前，建立该新密钥，以使接收的内容不中断。

[0090] 本发明的实施方式也可提供一种发送信号的灵活技术，其中，接收器应定位电子节目指南（EPG）资源。

[0091] 其背景在于，CI 增强标准定义了操作者配置（operator_profile）资源，该资源告知主机要储存的服务及其 LCN（逻辑频道编号）。该资源也可用于并不一定被主机理解的网络上，例如，未使用标准的 DVB 表的网络。

[0092] 目前，该资源仅仅通知主机正在广播的 EIT（事件信息表）是否可信，其是否存在，其是否被交叉承载（crossed carried）或是巴克频道（barker channel）或者其是否是应用。查看有关应用的信息，并不能指明引用的来源（其可为 CAM 或广播）。

[0093] 本技术的实施方式将操作者配置资源扩展为包括来自 CAM 的消息，从而通知主机获得 EPG 的地点，不仅仅通知主机是否可信任 EIT 或者是否具有基于 EPG 的应用。其思想在于，CAM 通知主机可获得 EPG 信息的确切地点。

[0094] 其实例为：

[0095] 广播 EPG

[0096] EIT（已经覆盖在 CI 增强规范中）

[0097] 应用(传送带(carousel)ID)-MHEG、HTML-CE(HbbTV)、MHP 等

[0098] 以太网(IP 地址)

[0099] EIT (DVB 表)

[0100] 应用 -MHEG、HTML-CE(HbbTV)、MHP 等

[0101] CAM

[0102] 应用

[0103] EIT (CI APDU 中的 DVB 表)

[0104] 私有 EPG

[0105] 操作者和制造商私有 EPG 机制

[0106] 通过该信息,主机可在远程将 EPG 密钥重新映射到合适的 EPG 机制中。

[0107] 要理解的是,可由特定的硬件、运行合适的软件的通用硬件、半可编程硬件(例如,现场可编程门阵列或专用集成电路)或这些硬件的组合执行上述技术。要理解的是,在使用软件执行这些技术或这些技术的一部分时,这种软件以及携带这种软件的储存介质(例如,非暂时性机器可读储存介质,例如,磁盘或光盘或闪速存储器)被视为表示本发明的实施方式。

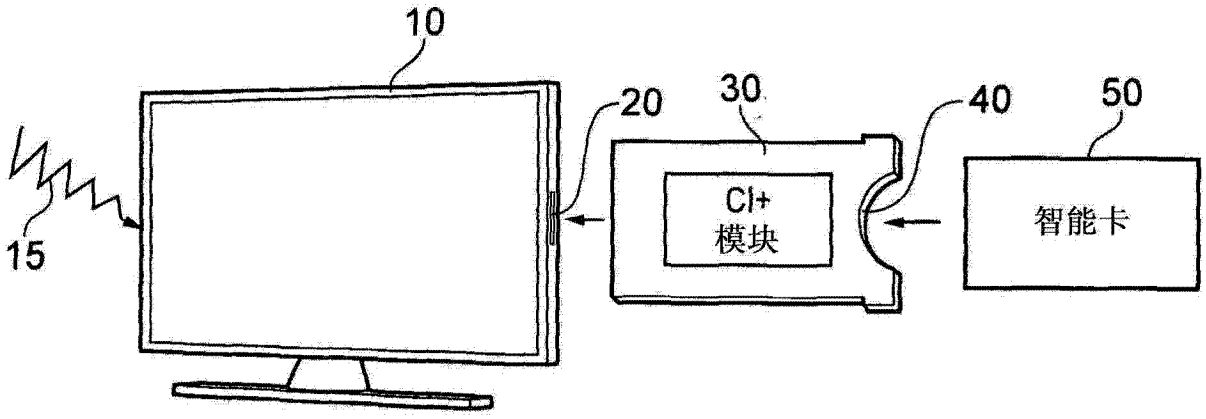


图 1

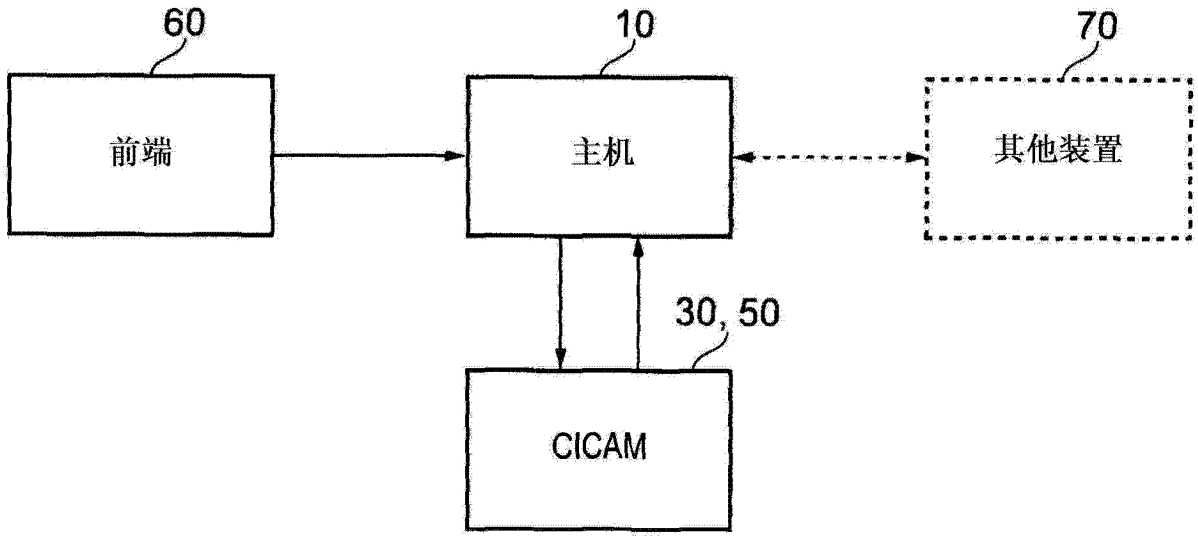


图 2

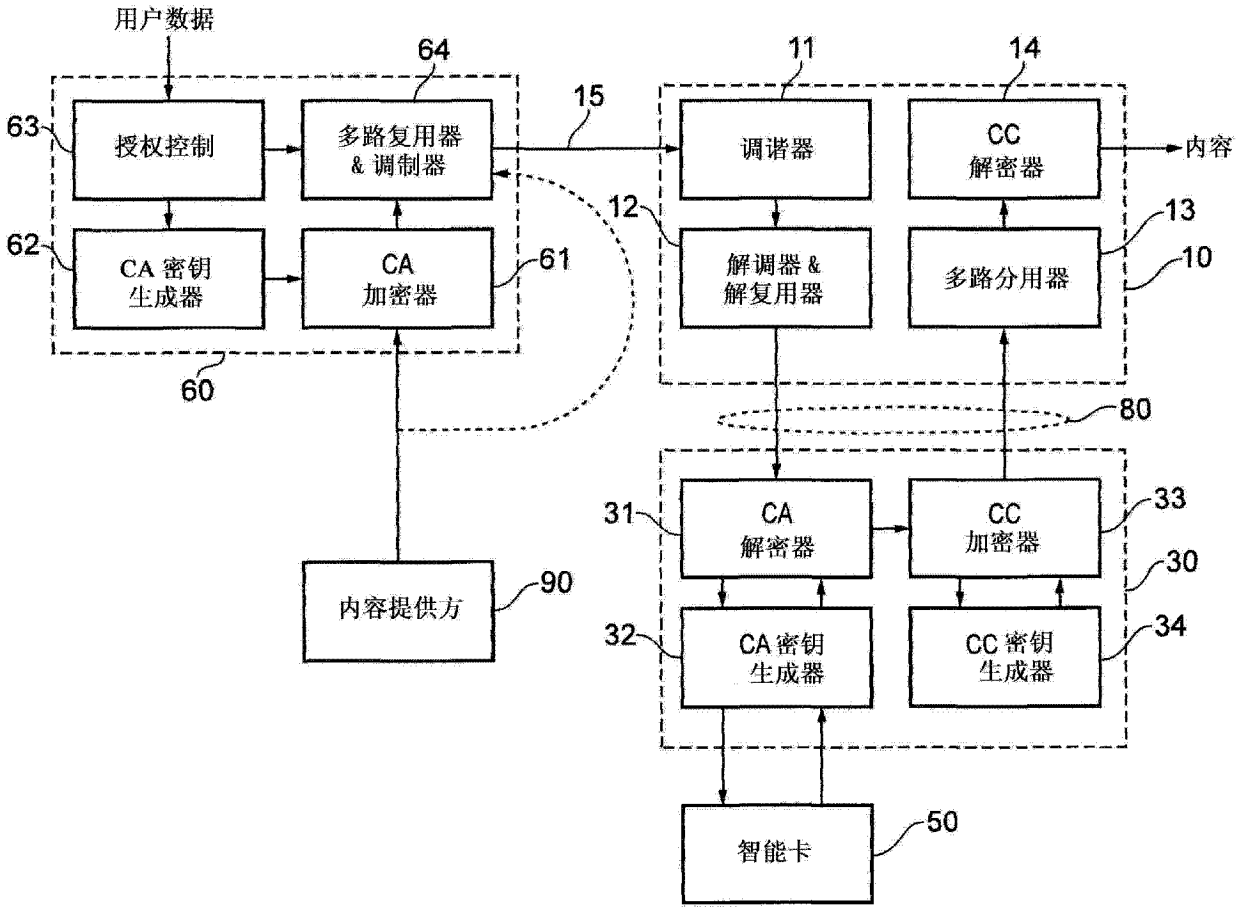

用户数据
64
11
14
15
63
授权控制
多路复用器
& 调制器
调谐器
CC
解密器
内容
62
CA 密钥
生成器
CA
加密器
61
12
13
解调器 &
解复用器
多路分用器
10
60
80
31
CA
解密器
CC
加密器
33
30
内容提供方
90
32
CA 密钥
生成器
CC 密钥
生成器
34
智能卡
50

图 3

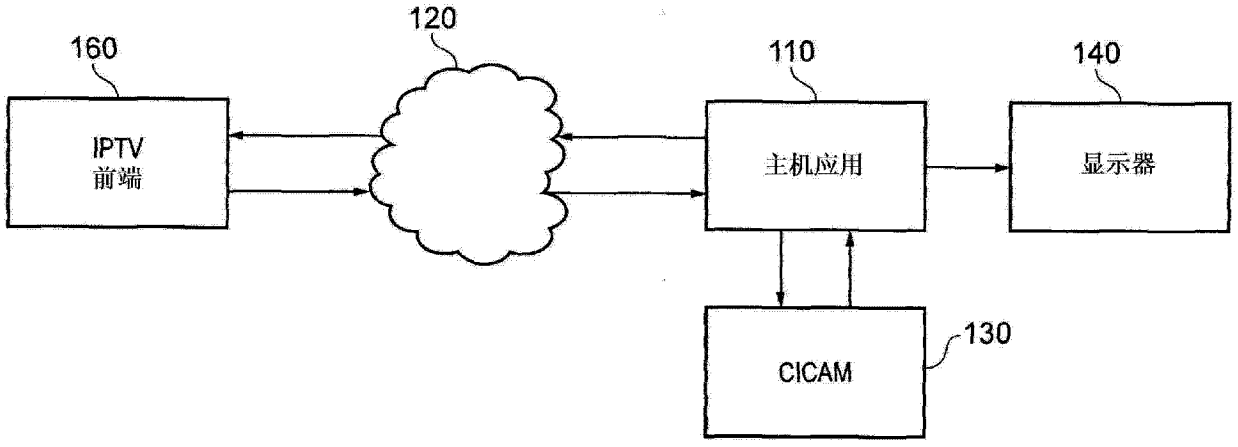

120
160
110
140
IPTV
前端
主机应用
显示器
CICAM
130

图 4

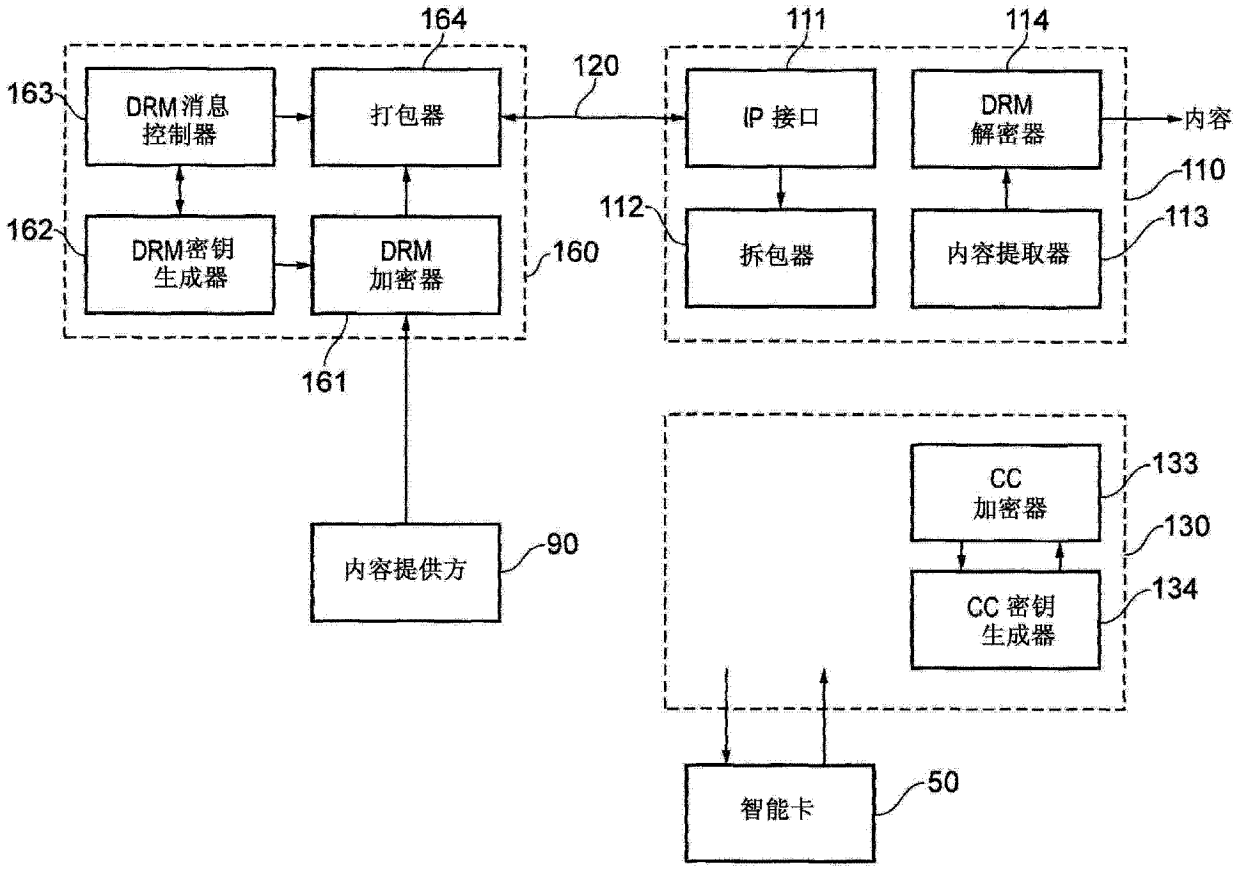

164
111
114
120
163
DRM消息
控制器
打包器
IP 接口
DRM
解密器
内容
110
112
162
DRM密钥
生成器
DRM
加密器
160
拆包器
内容提取器
113
161
133
CC
加密器
130
134
CC 密钥
生成器
内容提供方
90
智能卡
50

图 5

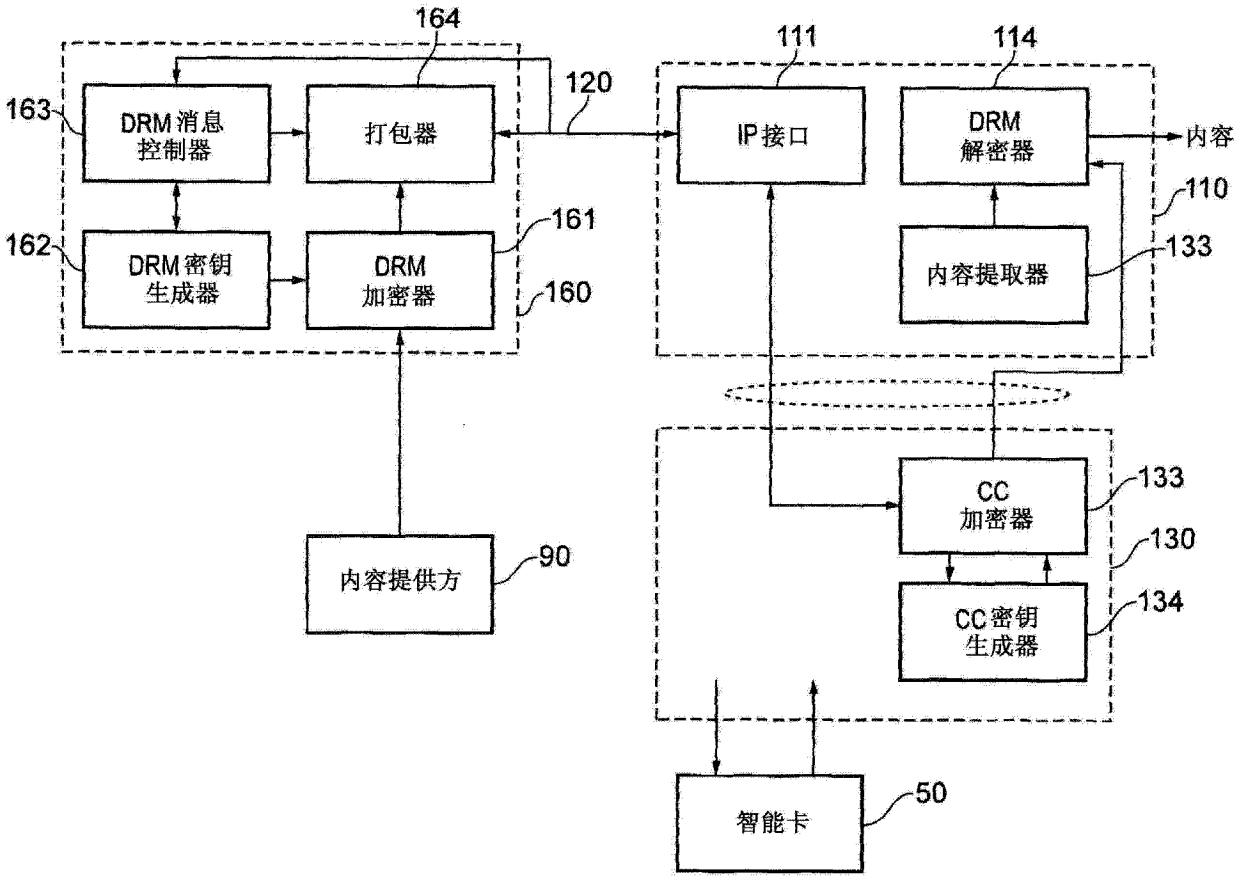

164
111
114
120
163
DRM消息控制器
打包器
IP接口
DRM解密器
内容
110
162
DRM密钥生成器
161
DRM加密器
160
内容提取器
133
133
CC加密器
130
CC密钥生成器
134
90
内容提供方
50
智能卡

图 6

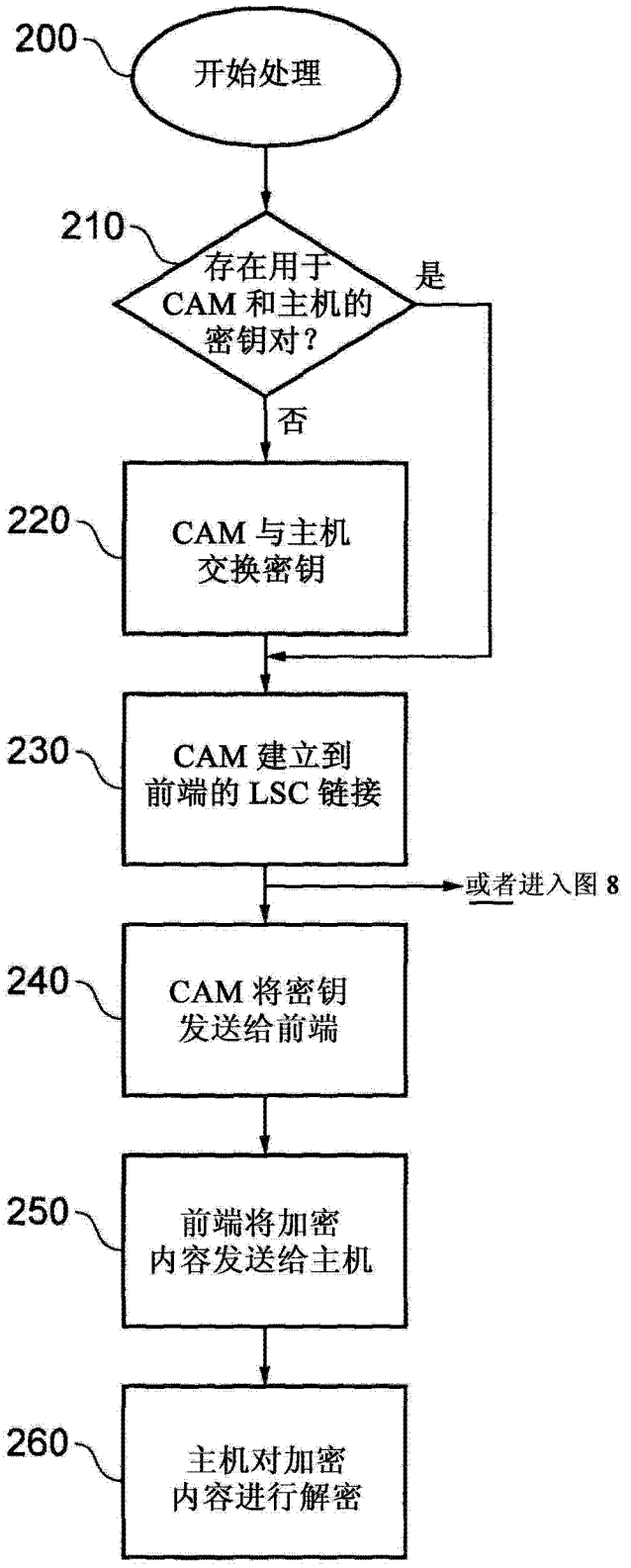

200
开始处理
210
存在用于 CAM 和主机的密钥对？
是
否
220
CAM 与主机交换密钥
230
CAM 建立到前端的 LSC 链接
或者进入图 8
240
CAM 将密钥发送给前端
250
前端将加密内容发送给主机
260
主机对加密内容进行解密

图 7

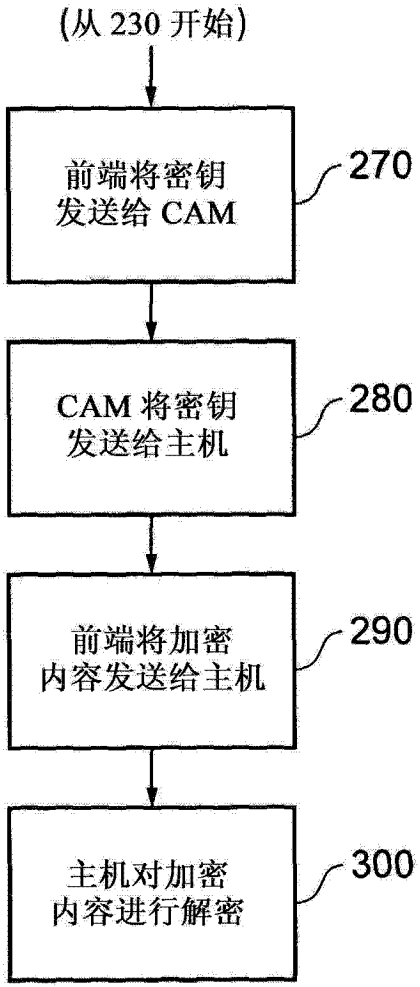

(从 230 开始)
前端将密钥发送给 CAM
270
CAM 将密钥发送给主机
280
前端将加密内容发送给主机
290
主机对加密内容进行解密
300

图 8