(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 101061714 B
(45)授权公告日 2014.10.15

(21)申请号 200580039182.2
(22)申请日 2005.11.17
(30)优先权数据
60/628,786 2004.11.17 US
(85)PCT国际申请进入国家阶段日
2007.05.16
(86)PCT国际申请的申请数据
PCT/US2005/042018 2005.11.17
(87)PCT国际申请的公布数据
WO2006/055853 EN 2006.05.26
(73)专利权人 摩托罗拉移动有限责任公司
地址 美国伊利诺伊州
(72)发明人 亚历山大·麦德温斯盖
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 刘光明 穆德骏
(51)Int.Cl.
H04N 7/167(2011.01)
H04N 21/2343(2011.01)
H04N 21/835(2011.01)
H04N 21/266(2011.01)
H04N 21/472(2011.01)
H04N 21/2347(2011.01)
H04N 21/4623(2011.01)
H04N 21/6334(2011.01)
H04H 60/23(2008.01)

(56)对比文件
US 20040101138 A1,2004.05.27, 说明书第110段.
US 20010029581 A1,2001.10.11, 全文.
CN 1111335 C,2003.06.11, 全文.
WO 2003079689 A1,2003.09.25, 全文.
US 20020044658 A1,2002.04.18, 说明书第44－48、59－62、73－75、102－104、133－135段及附图1－6.
CN 1134161 C, 权利要求5,说明书第3、4页及附图2.

审查员 谢佳妮

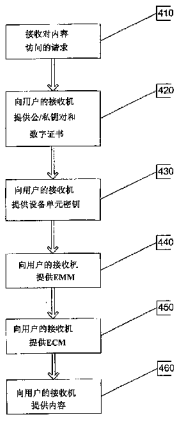
权利要求书2页 说明书12页 附图7页

(54)发明名称

用于提供对数字内容的授权访问的系统和方法

(57)摘要

本文所描述的实施例提供了一种对数字产权管理(DRM)体系结构进行密钥管理的方法,该DRM体系结构包括多级密钥管理,用于为该DRM体系结构最小化带宽使用同时最大化保密性。在一个实施例中,提供了一种用于密钥管理的数据结构,其包括公/私钥对以及三个附加的对称密钥层用于授权访问多种内容。



CN 101061714 B

1. 一种用于提供对内容的授权访问的方法，包括步骤：

接收来自多个 PPV 用户对内容的 PPV 访问请求；

响应于所述 PPV 访问请求，向所述多个 PPV 用户中的每一个提供具有公用加密密钥和私用加密密钥的非对称密钥对；

为所述多个 PPV 用户中的每一个提供唯一的设备单元密钥，其中用与所述每一个 PPV 用户关联的公用加密密钥对所述设备单元密钥中的每一个进行加密；

为所述 PPV 访问请求提供第一权限控制消息 ECM，所述提供所述第一 ECM 的步骤包括：

a) 在所述第一 ECM 中为所述 PPV 访问请求提供 PPV 访问规则；

b) 在所述第一 ECM 中为至少所述 PPV 访问规则提供第一消息验证代码 MAC；以及

c) 将所述第一 ECM 作为分组寻址的多播 ECM 提供给所述多个 PPV 用户；以及此外

为所述 PPV 访问请求提供第二 ECM，其中所述提供所述第二 ECM 的步骤包括：

a) 用所述设备单元密钥对节目密钥的第一副本进行加密，所述节目密钥可操作用于对所述 PPV 访问请求的内容进行解密和得出所述第一 MAC；以及

b) 在所述第二 ECM 中提供所述节目密钥的第一副本。

2. 根据权利要求 1 的所述方法，进一步包括步骤：

将所述第二 ECM 作为单元寻址的 ECM 提供给所述多个 PPV 用户中的每一个，其中所述单元寻址的 ECM 包括用所述设备单元密钥加密的节目密钥，所述设备单元密钥对每个所述 PPV 用户是唯一的。

3. 根据权利要求 1 的所述方法，进一步包括步骤：

接收对所述内容的预定服务访问请求；以及

响应于所述预定服务访问请求，提供权限管理消息 EMM，所述提供所述 EMM 的步骤包括：

a) 用对于所述预定服务访问请求的源而言唯一的设备单元密钥对服务密钥进行加密，所述服务密钥可操作以提供对所述节目密钥的加密和解密；以及

b) 在所述 EMM 中提供所述服务密钥。

4. 根据权利要求 3 的所述方法，其中响应于所述预定服务访问请求，所述提供所述第一 ECM 的步骤进一步包括：

c) 在所述第一 ECM 中为所述预定服务访问提供预定服务访问规则；

d) 用所述服务密钥对所述节目密钥的第二副本进行加密；

e) 在所述第一 ECM 中提供所述节目密钥的所述第二副本；以及

f) 为至少所述预定服务访问规则和所述节目密钥的所述第二副本提供第二 MAC，所述节目密钥的所述第二副本可操作用于对所述预定服务访问的内容进行解密和得出所述第二 MAC。

5. 根据权利要求 1 的所述方法，其中所述在所述第一 ECM 中为所述 PPV 访问请求提供 PPV 访问规则的步骤包括步骤：

以第一速率在所述第一 ECM 中为所述 PPV 访问请求提供所述 PPV 访问规则的预定子集；以及

以比提供所述 PPV 访问规则的所述预定子集的速率更低的速率在所述第一 ECM 中提供所述 PPV 访问规则的剩余部分。

6. 根据权利要求 1 的所述方法，进一步包括步骤：

接收对所述内容的漫游请求，其中所述漫游请求是漫游 PPV 访问请求或漫游预定服务访问请求；以及

响应于所述漫游请求，提供对于所述漫游请求的源而言唯一的漫游设备单元密钥。

7. 根据权利要求 6 的所述方法，进一步包括步骤：

响应于所述漫游请求是所述漫游 PPV 访问请求，提供漫游 ECM，所述提供所述漫游 ECM 的步骤包括：

a) 用所述漫游设备单元密钥对漫游节目密钥进行加密，所述漫游节目密钥可操作用于对通过漫游的所述 PPV 访问请求的内容进行解密；以及

b) 在所述漫游 ECM 中提供所述漫游节目密钥。

8. 根据权利要求 6 的所述方法，进一步包括步骤：

响应于所述漫游请求是所述预定服务访问请求，提供漫游 EMM，其中所述提供所述漫游 EMM 的步骤包括：

c) 用至少所述漫游设备单元密钥对漫游服务密钥进行加密；以及

d) 在所述漫游 EMM 中提供所述漫游服务密钥。

9. 根据权利要求 8 的所述方法，进一步包括步骤：

响应于所述漫游请求是所述预定服务访问请求，提供漫游 ECM，所述提供所述漫游 ECM 的步骤包括：

a) 用所述漫游服务密钥对漫游节目密钥进行加密，所述漫游节目密钥可操作用于对通过漫游的所述预定服务访问的内容进行解密；以及

b) 在所述漫游 ECM 中提供所述漫游节目密钥。

10. 根据权利要求 1 的所述方法，进一步包括步骤：

提供包括免费预览节目密钥的权限管理消息 EMM，其中所述免费预览节目密钥可操作以使得能够免费预览所述 PPV 访问请求的内容。

用于提供对数字内容的授权访问的系统和方法

[0001] 优先权

[0002] 本申请要求11/17/2004提交的题为“DVB TM-CBMS-CALL FORTECHNOLOGIES”(Docket No.P5000)的美国临时专利申请No.60/628,786的优先权,通过引用将其全部内容并入本文,本申请还是申请于2005年9月16日、题为“SYSTEM AND METHOD FORPROVIDING AUTHORIZED ACCESS TO DIGITAL CONTENT”的美国实用专利申请No.11/228180的部分延续,通过引用将其全部内容并入本文。

背景技术

[0003] 传送到有线和卫星机顶盒(STB)的数字收费电视节目长期以来都装备有附条件访问和数字产权管理(DRM)。如照惯例所理解的,附条件访问指的是对访问特别的传输或广播的控制,而不考虑在这类传输或广播中的特定内容。Scientific Atlanta的PowerKEY以及Motorola的MediaCipher是附条件访问技术的常见例子。此外,如照惯例所理解的,DRM指的是对访问特殊内容的控制,而不考虑这类内容的传输或广播模式。

[0004] 当前DRM系统的密钥管理的一种常规方法涉及将正常静态的内容解密密钥传送到诸如有线或卫星机顶盒的各接收机,借以利用接收机的公钥和服务提供商(例如有线电视(CATV)或卫星电视服务提供商)的数字签名对内容解密密钥进行加密。接收机然后使用内容解密密钥来解密和访问服务提供商所提供的内容。该常规方法对高级内容提供了并不充分的保密等级,因为相同的静态内容解密密钥用于单片内容。因而,无论服务提供商何时广播该内容,拥有与该内容关联的内容解密密钥的任何人都可以查看该内容,而密钥可能已经通过因特网等被泄漏和被非法分发。这样的保密缺口的范围有可能是极大的,并且仅在其被发现并用新的内容解密密钥对内容重新加密之后才终止。

[0005] 与常规密钥管理方法关联的另一问题在于其并不足以适用于支持广播系统。这是因为用于向各用户传送内容解密密钥的公钥密码太慢并且将需要经营者投入大量昂贵的硬件。这对于按次计费(PPV)广播来说尤其是个问题,在PPV广播的情况下,上百万的潜在用户会在相对短的期间内请求访问。

发明内容

[0006] 因此,本文所描述的实施例提供了一种对数字产权管理(DRM)体系结构进行密钥管理的方法,该DRM体系结构包括多级密钥管理,用于为该DRM体系结构最小化带宽使用同时最大化保密性。在一个实施例中,提供了一种用于密钥管理的数据结构,其包括公/私钥对以及三个附加的对称密钥层用于授权访问多种内容。

附图说明

[0007] 借助于例子且不限于以下附图对实施例进行说明,其中相同的标号表示相同的元件,其中:

[0008] 图1根据一个实施例,说明了内容分发系统100的高层级视图;

[0009] 图 2 根据一个实施例，说明了用于 DRM 体系结构的密钥管理层次；

[0010] 图 3 根据一个实施例，说明了用于接收机的高层级配置；

[0011] 图 4 根据一个实施例，说明了用于实现图 1 所示的密钥管理层次的流程；

[0012] 图 5 根据一个实施例，说明了用于图 2 所示的密钥管理层次的详细流程；

[0013] 图 6 根据一个实施例，说明了用于 DRM 体系结构的可选的密钥管理层次；

[0014] 图 7 说明了用于图 6 所示的可选的密钥管理层次的详细流程。

具体实施方式

[0015] 出于简化和说明性目的，通过主要参照实施例的例子来描述其原理。在以下描述中，阐述了许多具体的细节，以便提供对实施例的全面理解。然而，对于本领域的普通工作人员来说这会是显而易见的，即可以不限于这些具体的细节而实践实施例。在其它实例中，并没有详细描述公知的方法和结构，以免对实施例造成不必要的混淆。

[0016] 图 1 根据一个实施例，说明了内容分发系统 100 的高层级视图。系统 100 包括服务提供商 110、无线传输网络 120（例如卫星传输网络）、陆线传输网络 130（例如陆地区域网或电缆网）、经由卫星传输网络 120 为用户接收来自服务提供商 110 的内容的多个接收机 140a-140n 和 150a-150n。如文中所指，提供给用户的内容包括任何音频或视频数据或信息，例如流式音频服务、流式视频服务、流式数据服务或使用诸如 FLUTE 的协议广播的 DRM 保护文件。同样如文中所指，用户是个人、一群人、公司、协会，或者购买、预定或者用别的方式被授权接收对一个或多个特定内容的访问的任何其它实体。用户的例子有但不限于 CATV 订户、卫星 TV 订户、卫星无线电订户以及按次计费 (PPV) 事件的 PPV 购买者。同样如文中所指，PPV 事件是这样的特定内容，即每次访问这样的内容时对用户收费。

[0017] 如文中进一步所指，服务提供商是个人、一群人、公司、协会，或者向一个或多个用户分发内容的任何其它实体。服务提供商的例子有 CATV、卫星 TV、卫星无线电以及在线音乐提供商或公司。反过来，服务提供商又从诸如电影制片厂、唱片公司、电视广播网等一个或多个内容提供商（未示出）接收内容。应当指出内容提供商还可操作为服务提供商，以便用与图 1 中对服务提供商 110 所示的相同方式将其内容直接提供给用户。同样如文中所指，接收机是用户用于访问由服务提供商（或内容提供商）所提供的内容的设备，用户有权访问该内容。接收机的例子有 CATV 和卫星 TV STB 以及卫星无线电接收机。应当指出接收机可操作为独立单元，或者内容查看设备（例如具有内置卫星或 CATV 接收机的电视）的组成部分。

[0018] 图 2 说明了用于 DRM 体系结构的密钥管理层次 200，该 DRM 体系结构能够向多个用户提供对内容的附条件访问以及 DRM。DRM 结构可操作为编码于计算机可读介质上的计算机可读数据结构，并且可扩缩以适应用户，同时最小化带宽使用且不需要添加昂贵的硬件加速器。密钥管理层次 200 可在单向 IP 多播环境中操作，在单向 IP 多播环境中没有可从各接收机获得的返回路径。然而，设想了可选的实施例，在其中还将密钥管理层次 200 优化用于在双向 IP 多播环境中操作，在双向 IP 多播环境中，至少一个或多个接收机拥有基于 IP 向服务提供商发送上行消息的能力。

[0019] 参照图 2，各接收机拥有唯一的公 / 私钥对，其中示出了密钥对的设备私钥 210，以及相应的数字证书 115，例如 X.509 证书，其已由认证机构 (CA) 发布来检验来自该公 / 私钥

对的公钥属于特定的接收机。在双向 IP 多播环境中，接收机在用户向服务提供商注册期间向上发送其数字证书 115 到服务提供商。在单向 IP 多播环境中，各 CA 在在线目录中或在可由服务提供商访问的任何位置发行其用于接收机的 X.509 证书，而不是在注册期间使接收机向上发送其数字证书。因为数字证书仅含公开信息，所以对访问该目录不需要专门保密。

[0020] 根据任意公钥算法来创建用于各接收机的唯一的公 / 私钥对。可用的公钥算法的例子包括但不限于 Rivest-Shamir-Adlerman(RSA)、E1-Gamal 和数字签名算法 (DSA) 的结合，以及椭圆曲线。在一个实施例中，采用椭圆曲线是因为其密码性能随密钥尺寸线性增加。因而，椭圆曲线能够在相对较小的密钥尺寸和较少复杂性的情况下提供足够的保密等级。

[0021] 如图 2 所示，密钥管理层次 200 中最高层级的密钥是前述公 / 私钥对，由设备私钥 210 表示。优先于对称密钥而选择该非对称密钥操作是出于保密性原因。举例来说，当持有对称密钥的在线全局数据库引起极大的保密性问题并且需要极端的保密预防措施时，只有较少的保密性会涉及创建数字证书的在线数据库（常常将数字证书视为公开信息，尽管用户数据库中诸如权限的其它信息必须保持没有未授权访问的危险）。此外，公钥系统提供了用于终止或取消其关联的数字证书的标准化方法。

[0022] 密钥管理层次 200 中的下一层级是设备单元密钥 220。如同设备私钥 210 的情况一样，设备单元密钥 220 对各接收机是唯一的。然而，与设备私钥 210 的非对称相反，设备单元密钥 220 是对称的。在一个实施例中，设备单元密钥 220 包括用于各接收机的多个不同的单元密钥，且至少一个密钥用于加密以及一个密钥用于消息验证。因而，设备单元密钥 220 包括多个对称密码算法，其可应用于密钥管理层次 200 中所有的对称密钥层级。举例来说，设备单元密钥 220 包括用于加密的 128 比特高级加密标准 (AES) 密钥，以及 160 比特密钥散列的消息验证代码，其具有用于消息验证的特定散列函数 SHA-1(HMACSHA-1) 密钥。在用户为了内容服务而向服务提供商注册期间，服务提供商传送设备单元密钥 220，以及设备权限和用于该用户的接收机的其它配置数据。在传送前利用来自公 / 私钥对的公钥对设备单元密钥 220 进行加密，并且在接收机收到时由来自公 / 私钥对的设备私钥 210 对其进行解密。

[0023] 用于各接收机的唯一的设备单元密钥 220 起到减少带宽使用并增加对内容保密性的扩缩能力的作用。举例来说，在购买了按次计费 (PPV) 事件的情况下，唯一的节目密钥和访问规则被传送给请求该 PPV 事件的各接收机，并且因而被各请求接收机的唯一的设备单元密钥 220 加密。否则，必须对各节目密钥进行加密以及用公钥加密对其进行数字签名，并且对每个这样的接收机和在其内请求的各 PPV 内容重复该过程。对公钥加密这样的大量使用需要服务提供商与请求接收机之间的高带宽使用，并且引起扩缩能力的问题，因为其有可能并且严重地限制可以对相同的 PPV 事件授权的接收机的数目。根据一个实施例，基于预定的周期对所有预定接收机的设备单元密钥进行更新，例如，一年一次以最小化其可能的损害。

[0024] 密钥管理层次 200 中低于设备单元密钥 220 的下一层级是用于各接收机的一个或多个服务密钥 230。在一个实施例中，服务密钥用于预定服务而不是 PPV 事件。各服务密钥 230 保护单个的预定服务，通过对这种预定服务的内容进行加密而将该预定服务作为单

元来购买。如文中所指，预定服务是除了 PPV 事件之外的对内容的任何预定。单个预定服务的例子包括但不限于单个物理节目频道、节目频道的一部分或者作为单元被全部购买的节目频道的集合。如稍后进一步描述的，各接收机周期性地接收包括了一组一个或多个服务密钥的权限管理消息 (EMM)，其中用接收机唯一的设备单元密钥 220 对 EMM 进行加密和验证。设想了各种实施例，其中每个 EMM 包括单个服务密钥或多个服务密钥。

[0025] 如同密钥管理层次 200 中所有对称密钥的情况那样，每个服务密钥 230 包括多个密钥，且至少一个密钥用于加密（例如，AES）以及一个密钥用于消息验证（例如，HMAC SHA-1）。根据一个实施例，基于预定的周期对各接收机的服务密钥进行更新（例如，每一计费周期一次），从而使得当用户舍弃预定服务时，一旦更新了服务密钥，就在密码上终止用户对已舍弃的服务的访问。

[0026] 密钥管理层次 200 中低于服务密钥 230 的下一层级是节目密钥 240，其是为服务提供商所提供的各 PPV 事件创建的，即使这样的事件还通过预定服务来提供。根据一个实施例，用唯一的设备单元密钥 220 对各节目密钥 240 进行加密，并将其连同一个或多个访问规则传送给与设备单元密钥 220 关联的预定接收机。访问规则的例子包括地理限制（例如，中断）、内容等级（由接收机将其与输入亲本上限进行比较），以及复制控制信息（在一般情况下，这包括一整组 DRM 规则，该规则允许将内容持久存储于个人录像机 (PVR)、也称为数字录像机 (DVR)，并且与用户所拥有的其它设备共享，但却有一列限制，例如截止时间；对于非持久内容，有可能希望该信息转发复制控制比特用于数字和模拟输出，例如复制保护管理系统 - 数字或 CGMS-D，以及复制保护管理系统 - 模拟或 CGMS-A）。对于仅通过预定服务提供的事件，还希望在按节目的基础上随唯一的节目密钥 240 发出访问规则，以便记录设备可以连同访问规则和节目密钥 240（而不是服务密钥 230，其可能用于访问来自相同预定服务的、并未授权记录的其它加密内容）保存单独的节目事件。此外，使用节目密钥验证访问规则提供了重放保护工具 - 不可能重放来自旧的节目事件的访问规则并且使其作为当前事件的访问规则而通过。因为密钥管理层次 200 支持对预定服务的灵活及重叠定义，所以有可能在多于一个服务密钥 230 的情况下分发相同的节目密钥 240。

[0027] 密钥管理层次 200 中低于节目密钥 240 的下一层级是内容解密密钥 150。根据一个实施例，节目密钥 240 并不实际用于直接解密所预定的内容。相反，每个内容 IP 分组标题包括预定长度（例如，4 字节）的随机值。这样的值在下文中称为“内容密钥 ID”或“CKID”，其中 ID 代表识别或标识符。将节目密钥 240 和 CKID 的组合输入单向散列函数，例如 HMAC SHA-1，以便产生内容解密密钥 150。因而，内容解密密钥用于对节目事件的实际内容 IP 分组进行解密，并且其基于 CKID 中的改变相对频繁地改变，例如每几秒一次。内容解密密钥起到权限控制消息 (ECM) 中控制字的作用，如稍后进一步描述的。

[0028] 通过暗中从节目密钥 240 和 CKID 得到各内容解密密钥 150，密钥管理层次 200 允许内容解密密钥 150 较为频繁地改变并且独立于 ECM 更新速率。获得内容解密密钥 150 的动机，出于同样的目的而不依赖于节目密钥 240，在于获得在其中非常频繁地改变密钥的额外的密钥层级。该频繁改变允许了这样的 DRM 系统中附加的保密性，即该 DRM 系统对密钥管理使用便宜的保密芯片但却由于例如并不充足的处理能力以及没有跟得上传送内容分组的速率的能力而不支持内容解密。

[0029] 应当理解，密钥管理层次 200 中各种密钥的名称仅仅用于在描述本发明的各种实

施例时将那些密钥彼此区分开来。因此，有可能在不背离本公开的范围的情况下为密钥提供别的名称。例如，可能将设备私钥 110、设备单元密钥 120、服务密钥 130 等命名为第一密钥、第二密钥、第三密钥等。

[0030] 根据一个实施例，将密钥管理层次 200 实现为保密编码于用于插入接收机的智能卡上的计算机可读数据结构。由于接收机中可能的处理限制，该智能卡必须向不具有相同等级的物理保密性的接收机中的通用主处理器或视频处理器提供内容解密密钥 150。尽管如此，对内容解密密钥 150 的任何非法复制均被最小化，因为如以上所讨论的，内容解密密钥 150 被频繁地改变。该频繁改变迫使对内容解密密钥 150 的任何非法复制要包括以高速率对数千内容解密密钥实时地进行破坏和再分发 - 使得这样的攻击实用性较低且更容易被检测。随着内容解密密钥的改变速率的增加，对这样的内容解密密钥的非法复制变得愈发实用性较低。

[0031] 在另一实施例中，用于密钥管理层次 200 的这样的计算机可读数据结构编码于在接收机中受保护的或可由接收机安全访问的计算机可读介质 (CRM) 上。CRM 的实施例包括但不限于电子的、光学的、磁性的，或者能够向接收机中的处理器提供计算机可读指令的其它存储或传输设备。适合的 CRM 的其它例子包括但不限于 :软盘、CD-ROM、DVD、磁盘、存储芯片、ROM、RAM、ASIC、配置处理器、任何光学介质、任何磁带或任何其它的磁介质，或者处理器可能从其读取指令的任何其它的介质。

[0032] 图 3 根据一个实施例说明了接收机 300 的高层级配置，接收机 300 表示图 1 中所示出的接收机 140a-n 和 150a-n 中的任何一个。接收机 300 包括主处理器 310、诸如 CRM 的存储器 320、任选智能卡模块 330，以及保密硬件模块 350。主处理器 310 是负责接收机的大多数功能的组件，并且其访问存储器 320 获得实现这样的功能的可执行指令。然而，如早先所提及的，主处理器不是保密设备且易受篡改。因此，主处理器 310 通常仅处理短期密钥，例如内容解密密钥和 CKID（黑客主要对较长期的组件感兴趣，例如设备私钥、设备单元密钥和服务密钥）。任选智能卡模块 330 用于接收智能卡，智能卡上编码了用于密钥管理层次 200 的计算机可读数据结构，如早先根据一个实施例所提及的，用于由主处理器 310 执行。可选地，将智能卡中的一些或全部数据下载到存储器 320 用于由主处理器 310 执行。

[0033] 保密硬件模块 350 含有保密处理器 351、密代码 353 以及诸如 CRM 的存储器 360。在一个实施例中，保密硬件模块 350 是保密硅硬件设备，例如抵抗篡改硅微芯片。存储器 355 负责安全存储信道密钥数据 124。保密处理器 351 是受保护的处理器，其处理保密硬件模块 350 的处理功能，例如执行用于产生如早先所述的内容解密密钥的单向函数 (OWF)355（例如，HMAC SHA-1 散列函数）。密代码 353 是保密硬件模块 350 的一部分，保密硬件模块 350 包括由保密处理器执行的各种软件代码和应用。值得注意的是，一个密代码 353 包括 OWF 355。如早先所述，有可能将密钥管理层次 200 实现为在诸如保密硬件模块 350 中的存储器 360 这样的 CRM 上实现的计算机可读数据结构。这确保了保密硬件模块 350 内各种加密 / 解密密钥的保密性。在可选的实施例中，公 / 私钥对及关联的数字证书存储于智能卡上，并且在存储器 360 中得到并存储了诸如设备单元密钥、服务密钥、节目密钥和内容解密密钥这样的较低层级的密钥。

[0034] 现在参照图 4 且进一步参照图 3 描述用于实现密钥管理层次 200 以向多个用户提供对内容的 DRM 和附条件访问的过程。开始于 410，内容（例如数字收费 TV 广播节目）的

服务提供商接收来自用户的内容请求。服务提供商然后以惯常的方式注册用户，例如，通过建立诸如由用户所提供的姓名和联系信息这样的用户身份。

[0035] 在420，在一个实施例中，作为注册的一部分，用户从服务提供商获得接收机，接收机借此装备有在用户与服务提供商之间发生任何注册之前已被预装（例如在生产设备中）的唯一的公／私钥对和数字证书。在该实施例中，公／私钥对和相应的数字证书115实现于接收机中，受保护于如早先所提及的可由接收机访问以便读取的（用于插入智能卡模块330的）智能卡或CRM（例如存储器360）中。在另一实施例中，服务提供商实现向智能卡或CRM的用户的物理传送，在该智能卡或CRM上存储了公／私钥对和数字证书，从而使得为该用户的接收机提供对所存储的信息的访问。而在另一实施例中，服务提供商经由陆线数据网（例如因特网）、无线数据网（例如蜂窝网），或者陆线和无线数据网的组合，通过远程安装到用户的接收机（例如，在存储器360中）而提供了公／私钥对和数字证书。

[0036] 因此，在图2所说明的供应过程之前，用户的接收机便装备了公／私钥对和数字证书，下面进一步对其进行描述。

[0037] 在430，同样作为注册的一部分，服务提供商向用户提供唯一的设备单元密钥220（图2）用于用户的接收机，并且可选地提供-设备配置数据和不是专用于特定的内容访问服务的一般权限（例如，用于存储在存储器320或360中）。传送设备单元密钥220，如早先所述，用公钥对其进行加密并在接收机内部用接收机唯一的公／私钥对中相应的私钥对其进行解密（用于存储在存储器360中）。

[0038] 在440，为了向用户提供任意内容访问服务，服务提供商首先向用户的接收机传输权限管理消息（EMM）以指定用户对内容访问服务的权限。通过陆线连接（例如，在CATV广播节目的情况下）或无线连接（例如，在卫星TV或无线电广播节目的情况下）将EMM传输至接收机。用对于接收机而言是唯一的设备单元密钥220对EMM进行加密以及验证，并且该EMM包括：接收机的服务权限（例如，用于存储在存储器320中），以及任何预定服务的一个或多个服务密钥230（例如，用于存储在存储器360中）。如早先所提及的，因为服务密钥230和设备单元密钥120随时间改变，所以各EMM还包括起标签作用的密钥标识符。根据一个实施例，将打算给特定接收机的所有EMM进一步映射到单个IP多播地址用于传输至这样的接收机。所映射的IP多播地址分离于用于发送内容和其它类型的密钥管理消息的其它IP多播。每个EMM具有这样的标题，即该标题包括：a）将其指示为EMM的消息类型；b）标识出打算给其EMM的接收机的设备ID（例如，5字节或更长）；c）用于对EMM进行加密的设备单元密钥220的标识符（例如，4字节），在设备单元密钥220的每次改变之后对其加一；以及d）检验消息完整性的消息验证代码（MAC），其中，MAC是诸如截取到12字节以保存带宽的HMAC SHA-1密钥这样的对称密钥。

[0039] 在450，服务提供商接下来向用户的接收机传输权限控制消息（ECM）以指定用于解密授权内容的密钥。因而，ECM是携带了节目密钥240和访问规则、在服务密钥230（用于预定服务）或设备单元密钥220（用于PPV事件）下加密的消息。对包括在预定服务中的每个节目事件广播用服务密钥230加密且携带了访问规则和唯一的节目密钥240的新ECM，而不管这样的节目事件是否还可作为PPV事件获得。

[0040] 根据一个实施例，ECM具有若干不同的传送／加密模式。在第一模式下，当为预定服务传送ECM时，用服务密钥230加密及验证该ECM并且将其通过广播或IP多播发出。

因而，对这样的预定服务授权的所有用户能够接收并解密该 ECM。在第二模式下，当为 PPV 事件传送 ECM 时，用设备单元密钥 220 加密及验证该 ECM。当这样的 PPV 事件还可在预定服务中获得时，仍然用设备单元密钥 220 加密及验证该 ECM，因为并未授权打算给其 PPV 事件的接收机接收用于这种预定服务的相应的服务密钥 230。因而，密钥管理层次 200 还支持用户购买单个事件的附加权利的能力，例如以按需方式“通过中断购买 (buy-through blackouts)”。

[0041] 再次参照图 4，在 460，服务提供商接下来传输已用对称密钥加密过的单独数据分组中的内容。在一个实施例中，在 CBC 模式下用 128 比特的 AES 对内容进行加密。与对第 3 层加密使用网际协议安全性 (IPsec) 相反，优选地在服务提供商的系统中的应用层应用内容加密。这减少了否则由 IPsec 标题强加的带宽开销，并且还减少了内容保密系统对基本操作系统的依赖。每个已加密的单独的内容分组包括具有至少以下信息的应用层标题：如早先所述的 CKID、CBC 加密模式所需的初始化向量 (IV)，以及节目 ID（或者用于节目密钥 240 的一些其它类型的标识符）。用于 AES 的 IV 通常是 16 字节，但是为了保存带宽，有可能通过单向散列函数（例如 SHA-1）从较小的字节数（例如 4 字节）得出 IV。节目 ID 指向相应的节目密钥 240 和权限。如早先所提及的，节目密钥 240 与 CKID 结合得出内容解密密钥 150。

[0042] 如上所述，当多个用户请求相同的 PPV 事件时，每个请求用户接收单元寻址的 ECM（即专用于每个用户的接收机的 ECM），该 ECM 携带了用于这样的 PPV 事件的公共访问规则。因而，所有单元寻址的 ECM 所占据的带宽总量可能由于多个重复的公共访问规则而大量增加。因此，需要额外的时间来启动请求相同 PPV 事件的所有用户。相应地，在一个实施例中，为了最优化前述带宽和时间开销需求，以分组寻址的多播 ECM 来向所有的请求用户传送用于所请求的 PPV 事件的访问规则，其中分组寻址的多播 ECM 分离于单元寻址的 ECM。接下来参照图 5 描述该实施例，图 5 说明了用于图 4 中块 450 的流程。

[0043] 发送给请求用户的分组寻址的多播 ECM 的类型取决于用户所请求的节目事件的类型。因而，在 510，服务提供商确定所请求的节目事件是通过预定服务、PPV 服务还是二者来提供的。

[0044] 在 521，如果所请求的节目事件是仅通过预定服务提供的，则服务提供商向请求用户（下文中的“订户”）传输分组寻址的多播 ECM，其携带了用于所请求的节目事件的访问规则、用服务密钥 230 加密的节目密钥 240，以及在至少已加密的节目密钥 240 和访问规则之上的 MAC，该 MAC 由此是从服务密钥 230 得到的对称密钥。

[0045] 在 531，如果所请求的节目事件是仅通过 PPV 服务提供的，则服务提供商向请求用户（下文中的“PPV 用户”）传输分组寻址的多播 ECM，其携带了用于所请求的节目事件的公共访问规则、可经由 PPV 方法（甚至是已注册的订户）购买的任何附加的访问规则（增量访问规则）或选项，以及在至少访问规则和任何附加的访问规则之上的 MAC，该 MAC 由此是从节目密钥 240 得到的对称密钥。因为分组寻址的多播 ECM 并不含有用于 PPV 服务的任何节目密钥，所以在 533，服务提供商进一步向 PPV 用户中的每一个传输单独的、单元寻址的 ECM，该 ECM 含有用相应的设备单元密钥 220 加密的、必要的节目密钥 240，该单元寻址的 ECM 由此不再携带公共访问规则或任何附加的访问规则，以便为 PPV 用户最优化带宽使用和时间开销。

[0046] 在541，如果所请求的节目事件既是通过预定服务又是通过PPV服务提供的，则服务提供商向所有的请求用户（订户和PPV用户都是一样的）传输分组寻址的多播ECM，其携带了预定服务和PPV服务二者所需的那些字段。因而，分组寻址的多播ECM携带了用于所请求的节目事件的公共访问规则、用于PPV用户的任何附加的访问规则、用于订户的用服务密钥230加密的节目密钥240、在至少已加密的节目密钥240和公共访问规则之上用于订户的第一MAC，以及在至少公共访问规则和任何附加的访问规则之上的第二MAC。第一MAC从用于订户的服务密钥230得到。第二MAC从用于PPV用户的节目密钥240得到。因此，接收分组寻址的多播ECM的请求用户中的每一个均能够取决于特定的请求用户是订户还是PPV用户而检验不同的MAC。在543，服务提供商进一步向PPV用户中的每一个传输单独的、单元寻址的ECM，其含有用相应的设备单元密钥220加密的、必要的节目密钥240，该单元寻址的ECM由此不再携带公共访问规则或任何附加的访问规则，以便为PPV用户最优化带宽使用和时间开销。

[0047] 在另一实施例中，为了进一步减少用于传输公共访问规则的ECM带宽，有可能将公共访问规则划分或归类成两组：需要在较高速率以分组访问的多播ECM发送给用户的第一组访问规则（这样的访问规则的例子包括内容等级），以及可以在较低速率以分组访问的多播ECM发送给用户的第二组访问规则（这样的访问规则的例子包括记录许可，由此可接受在发送访问规则以禁止任何进一步的记录之前用户记录几秒钟的节目事件）。因而，可以在较低速率以分组访问的多播ECM向用户发送整组公共访问规则，包括第一和第二组访问规则，并且可以在较高速率以附加的、分组访问的多播ECM发送第一组访问规则。

[0048] 为了促进从一个服务密钥230到下一服务密钥的无缝转换（例如，对于相同的服务但具有不同的截止日期），EMM可操作以包括当前服务密钥和下一服务密钥。当计划向下一服务密钥进行转换时，在使用下一服务密钥之前的某个预定的时间重复EMM，且随当前和下一服务密钥相应的密钥ID呈现当前和下一服务密钥二者。一旦进行开关，当前服务密钥就过期，并且下一服务密钥就成为当前服务密钥且直到期望时才需要包括随后的下一服务密钥。

[0049] 相同的方案应用于为设备单元密钥120调度的密钥改变。然而，该方案不应用于节目密钥240。节目密钥240仅仅对应于特定的PPV事件ID，而不是当前密钥或下一密钥的概念，并且接收机为所有的非过期PPV事件保留其已接收的所有节目密钥的列表。

[0050] 因为并不假设IP多播传输是可靠的并且不保证返回路径，所以周期性地向接收机重传EMM和ECM。为了进一步最小化消息带宽利用，可以用简单二进制编码方法对EMM和ECM进行高效率格式化，例如MIKEY(IETF RFC 3830)，其是用于可应用于IP多播的应用层密钥管理的因特网工程任务组(IETF)标准。例如在MIKEY:MultimediaInternet KEYing，RFC 3830，J.Arkko，E.Carrara，F.Lindholm，M.Naslund，K.Norman，August 2004中找到完整的MIKEY描述和说明。

[0051] 根据另一实施例，EMM包括附加权限，该附加权限提供诸如域ID、域密钥和域限制（例如关于设备数的限制）的信息，以便寻址通过其在多个设备上共享内容的个人域。通过个人域提供内容保密性的密钥管理协议通常是基于IP的点对点双向。因而，这样的协议不需要使用保护初始内容传送的相同密钥管理层次200。

[0052] 将对应于各自的内容服务（预定服务或PPV事件）的各ECM流映射到各自的IP多

播地址，其同样分离于相应的IP内容地址。这使得能够在接收机的IP层高效实现将ECM分组过滤并分离于内容分组以支持快速信道获取。用与早先所描述的相同方式对携带了已加密的节目密钥240的ECM进行格式化；也就是说，各节目密钥240仅仅对应于特定的PPV事件ID，并且接收机保留其已接收的且具有非过期的相关节目事件的所有节目密钥的列表。

[0053] 根据一个实施例，作为额外的加强，可在单个的背景低速率多播IP流中传输用于许多服务的ECM。在设备存储器准许时，预先获取并存储ECM以进一步减少信道获取时间。

[0054] 图6说明了用于不采用节目密钥240的DRM结构的密钥管理层次600的可选实施例。DRM结构可操作为编码于计算机可读介质上的计算机可读数据结构。在该实施例中，设备单元密钥610、数字证书615以及设备单元密钥620分别操作如早先所述的密钥管理层次200（图2）中的设备单元密钥210、数字证书215以及设备单元密钥220。然而，在没有节目密钥的情况下，与如早先所述的从节目密钥和CKID得到内容解密密钥不同，两种不同的服务密钥现在用于对内容解密密钥进行加密。因而，可以在分组寻址的ECM中将内容解密密钥发送给用户的接收机。

[0055] 因此，如图6中所示，在仅是预定服务的情况下，服务提供商向所有的订户传输EMM，其中EMM包括用于预定服务的预定服务密钥630。该EMM包括了如早先对用于图2中的密钥管理层次200的EMM所描述的其它信息和功能。服务密钥630操作如早先对图2中的服务密钥230所描述的。接下来，服务提供商向所有的订户传输分组寻址的多播ECM，其包括公共访问规则以及用预定服务密钥630加密的内容解密密钥650的副本。

[0056] 在仅是PPV服务的情况下，服务提供商首先向用户的接收机传输EMM，其中EMM包括用于PPV服务的PPV服务密钥640。该EMM另外包括了如早先对用于图2中的密钥管理层次200的EMM所描述的其它信息和功能。PVV服务密钥640操作类似于预定服务密钥630，除了PPV服务密钥640具有对应于PPV节目事件而不是对应于预定服务的使用期，并且各PPV用户并不自动获得下一PPV服务密钥640，除非该PPV用户购买了另一PPV节目事件。接下来，服务提供商向所有的PPV用户传输分组寻址的多播ECM，其包括公共访问规则以及用PPV服务密钥640加密的内容解密密钥660的副本。

[0057] 在节目事件既可通过预定服务又可作为PPV事件获得的情况下，服务提供商传输两种不同的EMM，具有预定服务密钥630的一种用于订户，而具有PPV服务密钥640的一种用于PPV用户。接下来，服务提供商向订户和PPV用户均传输分组寻址的多播ECM，其包括公共访问规则以及（用两种不同的服务密钥加密的）相同内容解密密钥的两份不同的副本650和660。因而，为了优化ECM带宽和时间开销，将相同内容解密密钥的两份加密的副本650和660包括在相同的分组访问的多播ECM中，用于传输给订户和PPV用户二者以避免重复访问规则（PPV用户可以获得包括在多播ECM中的附加的访问规则，如以下进一步描述的）。

[0058] 再次参照图3，如同密钥管理层次200（图2）的情况那样，有可能将密钥管理层次600实现为在诸如保密硬件模块350中的存储器360这样的一个或多个CRM上实现的计算机可读数据结构。再者，这确保了保密硬件模块350内各种加密/解密密钥的保密性。在可选的实施例中，公/私钥对和关联的数字证书存储于智能卡上，并且得到诸如设备单元密钥这样的较低层级的密钥、两种不同的服务密钥，以及内容解密密钥并存储于存储器360中。

[0059] 图 7 说明了基于用户所请求的节目事件的类型向用户传送不具有节目密钥的分组寻址的多播 ECM 的流程。在 710，确定所请求的节目事件是通过预定服务、PPV 服务还是二者来提供的。在 721，如果所请求的节目事件是通过仅是预定服务提供的，则服务提供商向订户传输分组寻址的多播 ECM，其携带了所请求的节目事件的公共访问规则、用预定服务密钥 630 加密的内容解密密钥的第一副本 650，以及在至少预定内容解密密钥 650 和访问规则之上的 MAC，该 MAC 由此是从预定服务密钥 630 得到的对称密钥。

[0060] 在 731，如果所请求的节目事件是通过仅是 PPV 服务提供的，则服务提供商向请求 PPV 用户传输分组寻址的多播 ECM，其携带了所请求的节目事件的公共访问规则、可由请求用户（即使他们已经是 PPV 用户）购买的任何附加的访问规则（增量访问规则）或选项、用 PPV 服务密钥 640 加密的相同内容解密密钥的第二副本 660，以及在至少访问规则和任何附加的访问规则之上的 MAC，该 MAC 由此是从 PPV 服务密钥 640 得到的对称密钥。

[0061] 在 741，如果所请求的节目事件既是通过预定服务又是作为 PPV 事件提供的，则服务提供商向所有的请求用户（订户和 PPV 用户都是一样的）传输分组寻址的多播 ECM，其携带了预定和 PPV 服务二者所需要的那些字段。因而，该分组寻址的多播 ECM 携带了所请求的节目事件的公共访问规则、如早先对 PPV 用户所提及的任何附加的访问规则、相同内容解密密钥的第一和第二加密副本 650 和 660、在至少公共访问规则和用于订户的内容解密密钥的第一加密副本 650 之上的第一 MAC，以及在至少公共访问规则、任何附加的访问规则以及用于 PPV 用户的相同内容解密密钥的第二加密副本 660 之上的第二 MAC。第一 MAC 是从预定服务密钥 630 得到的对称密钥，并且第二 MAC 是从 PPV 服务密钥 640 得到的对称密钥。因此，接收分组寻址的多播 ECM 的请求用户中的每一个均能够取决于特定的请求用户是订户还是 PPV 用户而检验不同的 MAC。订户和 PPV 用户还分别使用其自己的服务密钥 630 和 640 来对已加密的内容解密密钥的适当副本进行解密。

[0062] 根据一个实施例，图 2 和图 6 中所说明的密钥管理层次可操作以向漫游移动接收机提供内容访问。在移动多播的情况下，漫游指的是携带移动接收机的用户在预定的服务区外且进入了不同的区域（“漫游区”），在那里用户不能够从该用户预定的服务提供商接收广播（预定或 PPV）服务，但在那里却存在候选的本地服务提供商。因而，临时向访问移动接收机提供在漫游区从本地服务提供商接收广播。漫游还指的是用户进入了这样的区域（“漫游区”），即在该区域中用户不被提供接收广播（预定或 PPV）服务并且不能够自动接收和解密 ECM，即使该用户实际上对该漫游区内的服务是授权的（例如，该漫游区由相同的服务提供商所操作的不同网络覆盖）。当用户在漫游区中时，该用户可以联系服务该漫游区的本地服务提供商以便临时接收权限。如果用户的移动接收机具有双向通信能力，则这可以交互完成。可选地，用户可以通过电话联系本地服务提供商。

[0063] 一旦漫游区内的本地服务提供商检验并授权用户在其中接收服务，则本地服务提供商向用户的接收机传输具有用于漫游服务的漫游设备单元密钥的 EMM，该漫游设备单元密钥是用来自如早先所述的接收机的公 / 私钥对中的公钥加密的。如早先所提及的，对于本地服务提供商来说，有可能从全局可访问的证书目录定位用于接收机的公 / 私钥的对应的数字证书（基于接收机的设备 ID）。因此，用户能够用该用户的接收机接收用于漫游服务的 EMM 和 ECM，就好像该用户是常规订户一样，除了接收机将要接收用于漫游预定服务的 EMM 中的短期服务密钥（例如，仅一天有效）。因此，为了支持漫游接收机，本地服务提供商

生成两组独立的ECM：a) 一组正常的ECM，其具有用该区域中具有预定服务的常规用户的常规服务密钥加密的节目密钥，以及b) 一组独立的漫游ECM，其具有用前述该区域中具有预定服务的漫游用户的短期服务密钥加密的节目密钥。另外，漫游用户能够请求或购买PPV事件，该用户的接收机由此将接收具有用该接收机的漫游设备单元密钥而不是长期单元密钥加密的节目密钥的ECM。这里也可应用如早先所描述的对ECM带宽和时间开销的优化。

[0064] 因为没有对用于在生成和传送EMM和ECM中所涉及的各种网络服务器之间通信的服务提供商的IP网络的保密性进行假设，所以这样的消息有可能在这样的IP网络内受到未授权的记录或捕获。先前所传输和捕获的EMM然后可用于对用户产生相当大的拒绝服务问题，尤其是在并未频繁改变用户接收机的服务密钥230和设备单元密钥220的时候（例如，对服务密钥230一月一次而对设备单元密钥220一年一次）。当稍后将先前所捕获的EMM重新插入IP广播流（例如用于传输EMM的IP多播流）时，利用使接收机接收并成功解密随后的密钥管理消息的能力失效的、旧的和废弃的设备单元密钥220或服务密钥230重新初始化接收机。因而，根据一个实施例，通过顺序增加用于设备单元密钥220的密钥标识符和使用MAC来提供消息完整性，提供了对EMM的重放保护。例如，当接收机检测到特定的EMM含有比上一个接收到的密钥标识符小的密钥标识符时，这样的EMM就被丢弃并被忽略为可能的重放攻击。EMM的合法发送者决不减少在相同设备单元密钥220下加密的密钥标识符。

[0065] 如早先所讨论的，并不频繁改变设备单元密钥220和服务密钥230。因而，4字节的密钥标识符数千年也不会翻转到0，并且没有任何根据去关心当密钥标识符翻转到0时会发生什么。然而，为了避免当出于某种原因将密钥标识符设为FFFF时的任何偶然误差，有可能对接收机进行程序设计以检验新的密钥标识符并未从先前的值跳跃超过某一合理数量（例如100）。

[0066] 根据一个实施例，对于服务提供商来说为了增加可扩缩性有可能通过向用户提供称为存储和转发PPV或即时PPV(IPPV)的内容购买模型来促进密钥管理层次200，其中所有参与的接收机均托付于节目密钥，在物理上都足够保密，即使在购买关于该IPPV服务的任何内容之前。然后向各接收机分派任务以在该接收机本地记录用户实际选择查看哪些IPPV节目并且周期性地将这些购买报告给服务提供商的计费系统，该计费系统然后相应地向用户收费。该IPPV模型可应用于具有返回路径的接收机。

[0067] 因而，在密钥管理层次200的情况下，通过允许所有用户免费预定IPPV服务而易于启用IPPV。与此同时，在接收机内部记录了关于IPPV服务所进行的对节目事件或服务的任何本地购买，并且然后将累积成组的购买报告回给服务提供商。当然，在各接收机与服务提供商的主机系统之间需要双向点到点安全协议，因为后者要向各接收机查询在预定的过去的时期（例如，上一计费周期）内已进行的IPPV购买的列表。此外，有可能对接收机设计程序代码以对可以进行的IPPV购买数或总计直到接收机向服务提供商报告了购买的整个列表为止的全部“现金花费”量加以限制。为了对不一定有返回路径能力的接收机支持IPPV服务，对于关联于那些接收机的用户来说有可能从购物亭预购积分。一旦使用了积分，用户就能够返回购物亭、报告回购买以及买到更多的积分。

[0068] 根据一个实施例，密钥管理层次200和600可操作以支持免费预览PPV节目。在这样的实施例中，在注册后不久服务提供商便在EMM中向各用户的接收机传输免费预览节

目密钥。对免费预览节目密钥的分发基于另外一个授权准则，例如年龄或地理位置。当免费预览发生时，服务提供商在相应的频道（IP 多播地址）上向用户传输免费预览内容数据分组。每个免费预览内容分组包括具有至少免费预览节目 ID（或者用于免费预览节目密钥的一些其它类型的标识符）的应用层标题。因而，对免费预览授权的所有接收机均能够用从免费预览节目密钥得到的密钥对免费预览内容分组进行解密，该密钥由分组标题中的免费预览节目 ID 标识。一旦免费预览结束，服务提供商就可以传输不是用于免费预览的内容分组以指示不同的节目 ID，基于早先所描述的机制，其然后需要通过预定、PPV 或 IPPV 购买而获得的节目密钥。

[0069] 根据另一实施例，如果允许节目访问规则包括保密的或已验证的时间服务限制，例如“内容可以被记录在 PVR 上或在本地被使用有限的时段”，则接收机有可能保护时间源以便将临时存储的内容设为保密期满。为了实现该方案，向具有持久存储内容广播节目的能力（例如 PVR 或 DVR）的接收机的特定 IP 多播地址重复发送时间消息或分组。每个时间消息包括 UTC 时间中预定长度（例如 4 字节）的时间戳、序号以及诸如 RSA 或 ECDSA 的数字签名。

[0070] 为了确认各时间消息，然后向接收机提供（例如，在 EMM 消息中）时间服务器的当前序号以及证书链。一个时间消息中的序号必须大于或等于先前时间消息的序号。在序号相同的情况下，较新的时间戳必须大于或等于上一个所接收到的时间戳。因而，该序号可操作用于使得反向时间调整如所期望的或所需要的。只要时间戳严格增加，就永远不需要改变该序号。

[0071] 如果大量接收机访问返回路径，那么可实现在可扩缩性和内容获取时间方面额外的改进。只要服务提供商已知各接收机的双向能力，周期性重复的 EMM 流和单元寻址的 ECM 流就不需要包括寻址到那些双向接收机的任何消息。具有双向能力的接收机可操作以发送上行消息来请求其 EMM 或单元寻址的 ECM 并且等待返回响应。如果响应由于不可靠传送而没有返回，则接收机可操作以在预定的超时周期之后重试。只要服务提供商没有看到来自双向接收机的明确请求，服务提供商就不需要多播为该设备专门加密的任何消息。

[0072] 文中已描述和说明的是各种实施例连同其变体中的一些。文中所使用的术语、描述和附图仅是作为举例说明来阐述的而并不意味着作为限制。本领域的工作人员将认识到许多变体在本主题的精神和范围内是可能的，本主题的精神和范围将由下面的权利要求 - 及其等同物进行限定，其中所有术语除非另有说明均具有其最广泛合理意义上的意思。

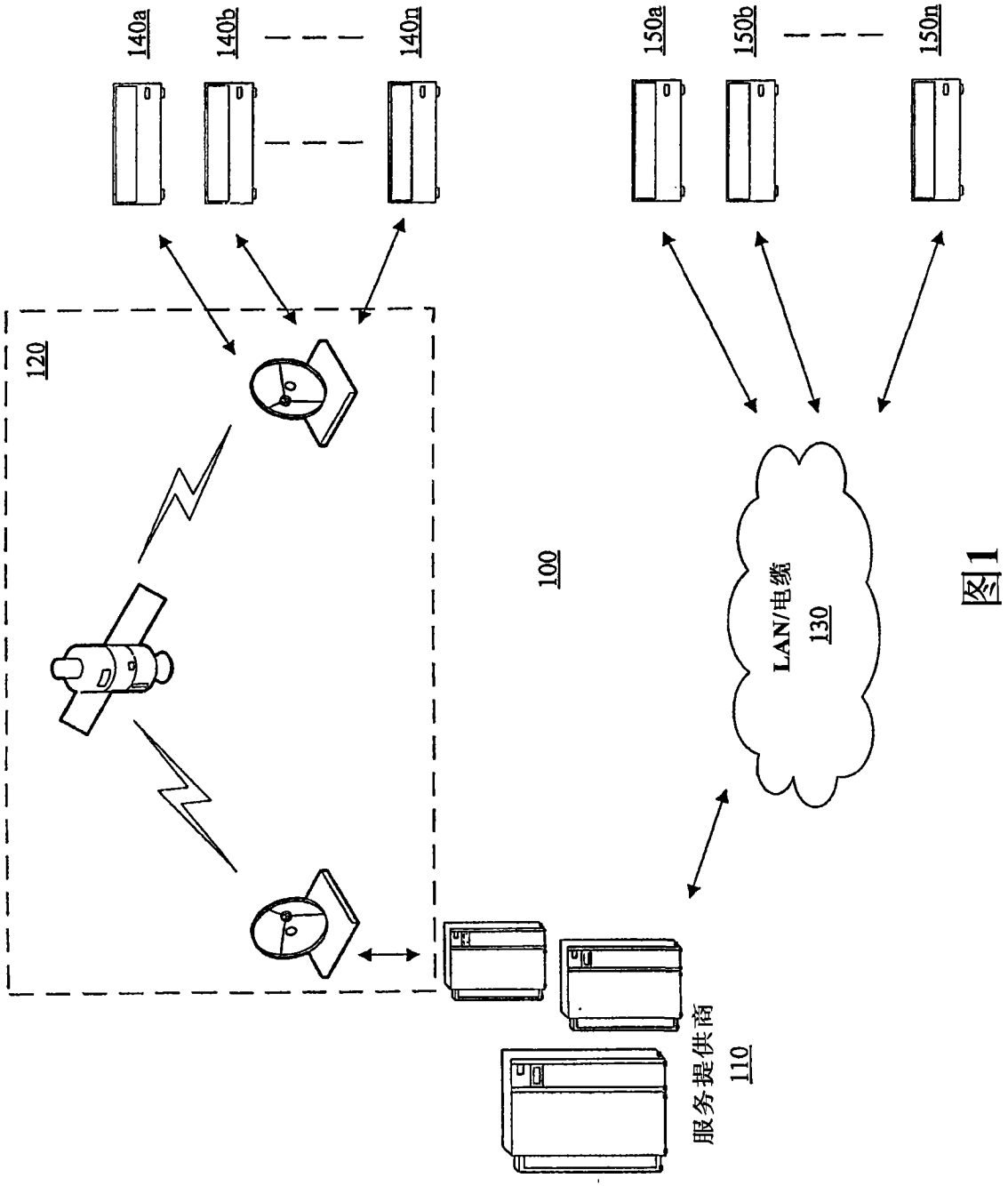


图1

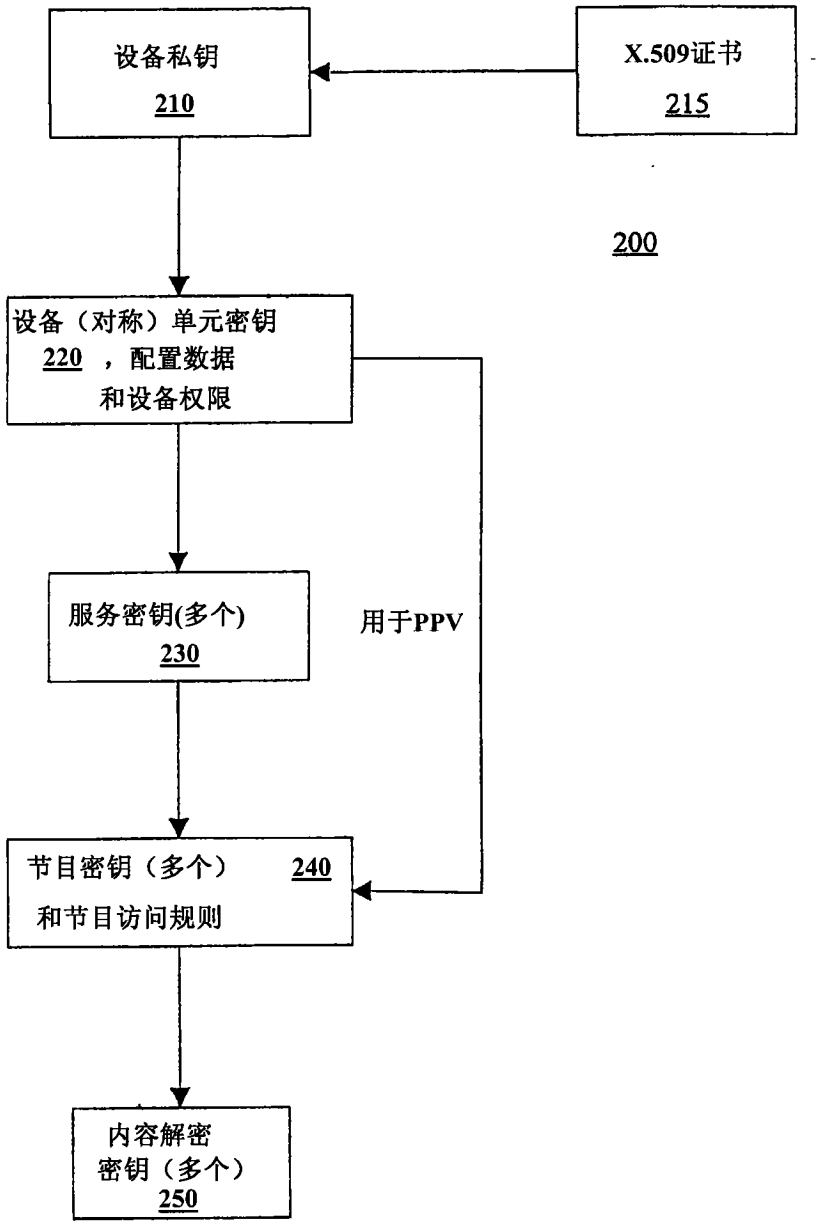

设备私钥
210
X.509证书
215
200
设备（对称）单元密钥
220 ，配置数据
和设备权限
服务密钥(多个)
230
用于PPV
节目密钥（多个） 240
和节目访问规则
内容解密
密钥（多个）
250

图 2

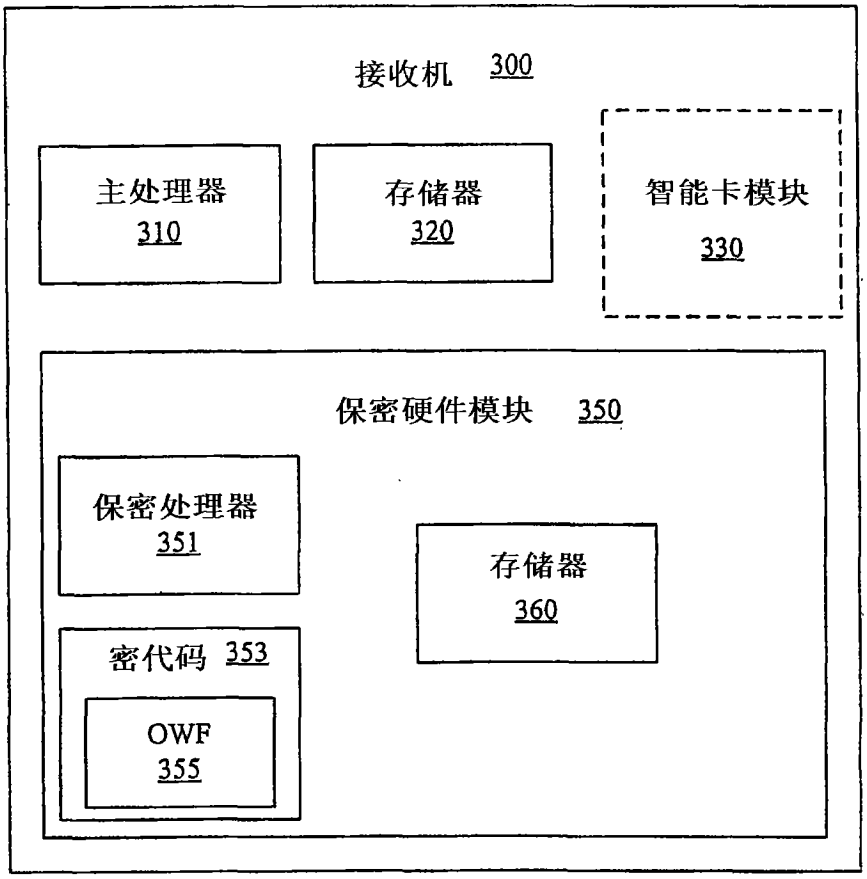

接收机 300
主处理器 310
存储器 320
智能卡模块 330
保密硬件模块 350
保密处理器 351
存储器 360
密代码 353
OWF 355

图3

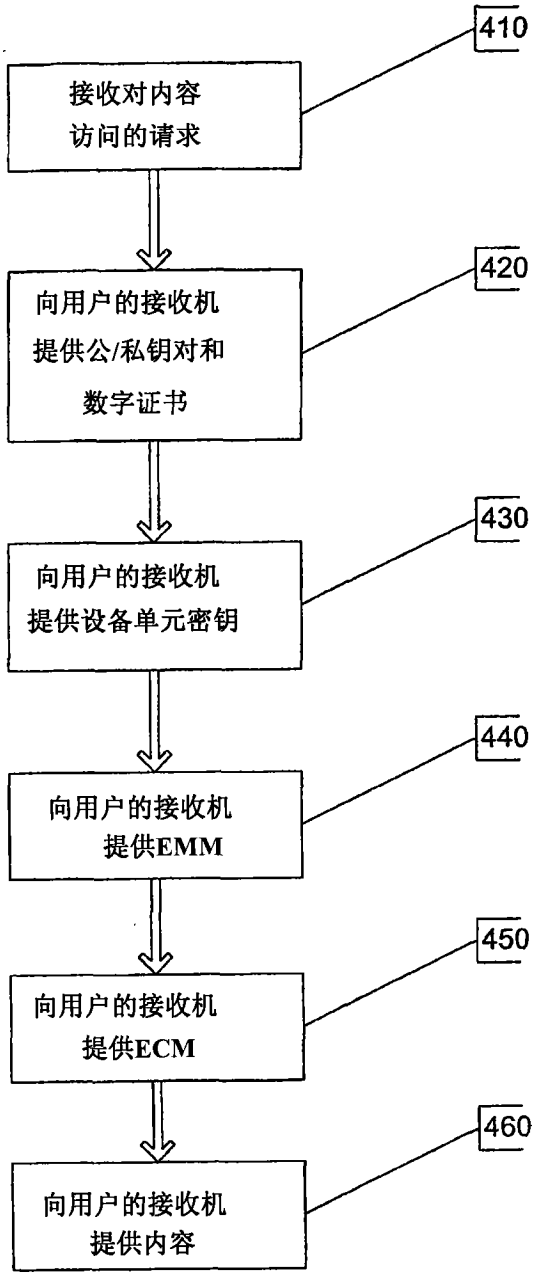

410
接收对内容
访问的请求
420
向用户的接收机
提供公/私钥对和
数字证书
430
向用户的接收机
提供设备单元密钥
440
向用户的接收机
提供EMM
450
向用户的接收机
提供ECM
460
向用户的接收机
提供内容

图 4

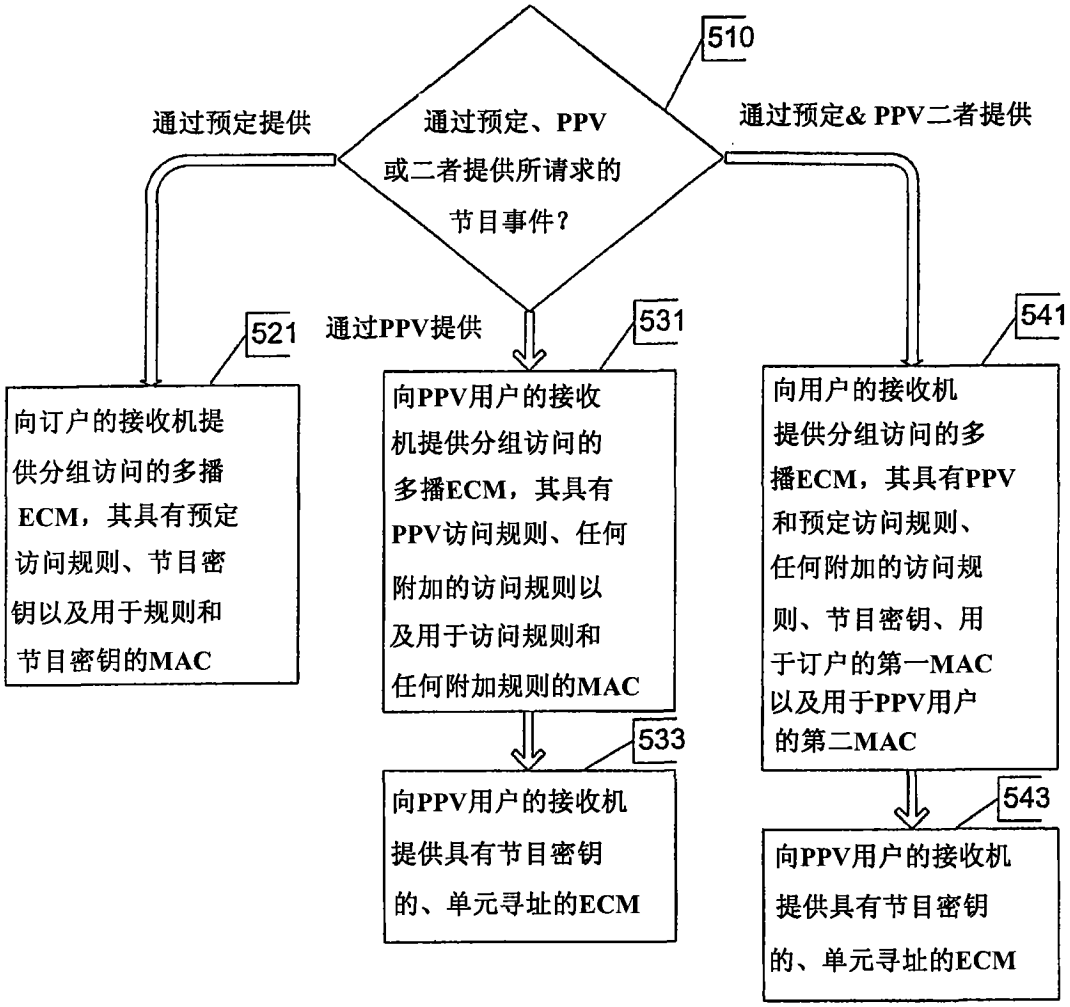

510
通过预定、PPV或二者提供所请求的节目事件？
通过预定提供
通过预定& PPV二者提供
通过PPV提供
521
向订户的接收机提供分组访问的多播ECM，其具有预定访问规则、节目密钥以及用于规则和节目密钥的MAC
531
向PPV用户的接收机提供分组访问的多播ECM，其具有PPV访问规则、任何附加的访问规则以及用于访问规则和任何附加规则的MAC
533
向PPV用户的接收机提供具有节目密钥的、单元寻址的ECM
541
向用户的接收机提供分组访问的多播ECM，其具有PPV和预定访问规则、任何附加的访问规则、节目密钥、用于订户的第一MAC以及用于PPV用户的第二MAC
543
向PPV用户的接收机提供具有节目密钥的、单元寻址的ECM

图 5

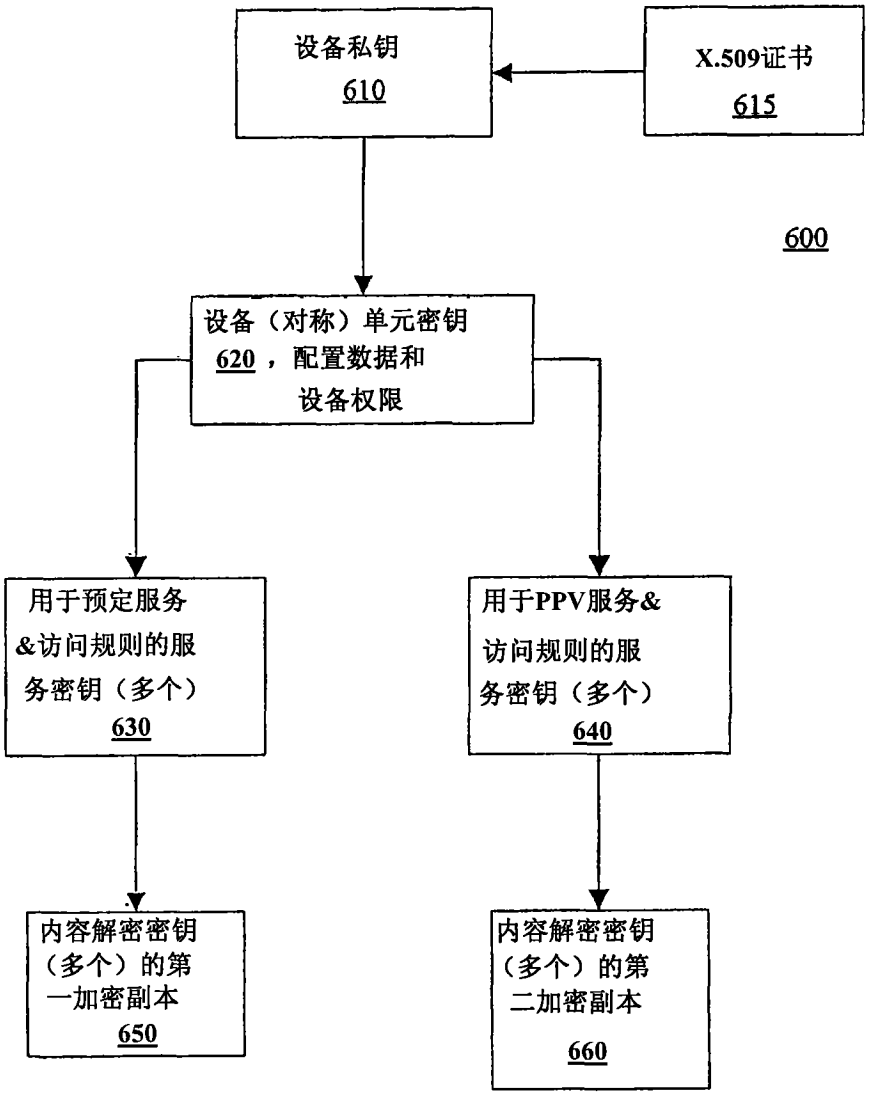

设备私钥
610
X.509证书
615
600
设备（对称）单元密钥
620，配置数据和
设备权限
用于预定服务
&访问规则的服
务密钥（多个）
630
用于PPV服务&
访问规则的服
务密钥（多个）
640
内容解密密钥
（多个）的第
一加密副本
650
内容解密密钥
（多个）的第
二加密副本
660

图 6

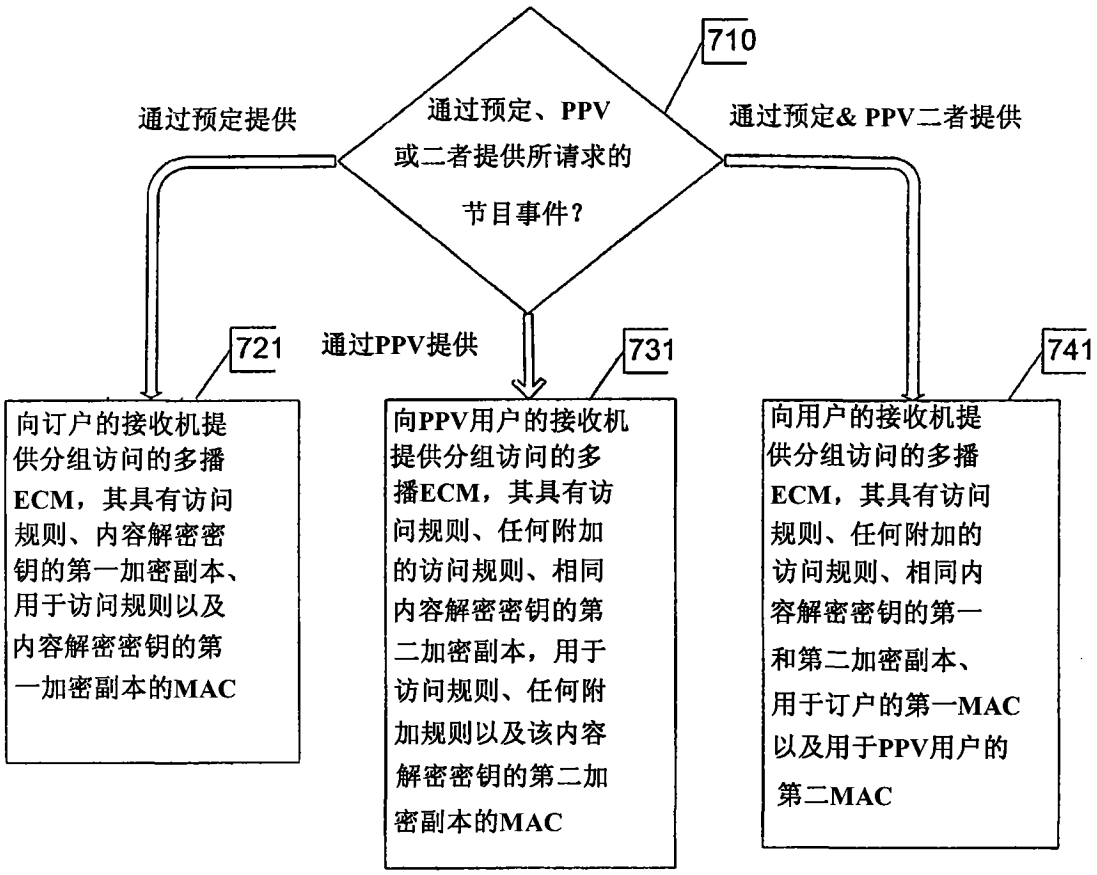

710
通过预定、PPV或二者提供所请求的节目事件？
通过预定提供
通过预定& PPV二者提供
通过PPV提供
721
731
741
向订户的接收机提供分组访问的多播ECM，其具有访问规则、内容解密密钥的第一加密副本、用于访问规则以及内容解密密钥的第一加密副本的MAC
向PPV用户的接收机提供分组访问的多播ECM，其具有访问规则、任何附加的访问规则、相同内容解密密钥的第二加密副本，用于访问规则、任何附加规则以及该内容解密密钥的第二加密副本的MAC
向用户的接收机提供分组访问的多播ECM，其具有访问规则、任何附加的访问规则、相同内容解密密钥的第一和第二加密副本、用于订户的第一MAC以及用于PPV用户的第二MAC

图 7