[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680004442.7

[43] 公开日 2008 年 2 月 13 日

[11] 公开号 CN 101124584A

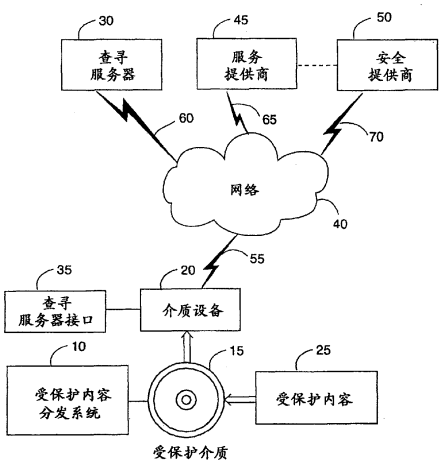
[22] 申请日 2006.2.16
[21] 申请号 200680004442.7
[30] 优先权
[32] 2005. 3. 7 [33] US [31] 11/072,943
[86] 国际申请 PCT/EP2006/060018 2006.2.16
[87] 国际公布 WO2006/094880 英 2006.9.14
[85] 进入国家阶段日期 2007.8.9
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 小多纳尔德·里克
杰夫里·B.·罗茨皮奇
斯特凡·纽塞尔
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李 颖
权利要求书 3 页 说明书 18 页 附图 12 页

[54] 发明名称

实现受保护媒体上的分发内容的授权使用的系统、服务和方法

[57] 摘要

受保护内容分发系统利用基于介质的复制保护以安全并且合法的方式支持受保护内容的在线分发。 通过利用根据广播加密的基于介质的复制保护方案，受保护内容分发系统实现诸如音频文件、电影之类受保护内容的在线分发，通过把唯一的加密密钥传送给受保护介质，许可未经授权内容的消费。 这种交易快速，涉及加密绑定密钥的传送，而不是受保护内容的传送。 通过经由与介质驱动器分离的设备访问的受保护介质上的唯一加密密钥，允许操作所述内容。



1、一种能够实现受保护介质上的分发内容的授权使用的方法，包括:

辨别分发内容未正确地与受保护介质相关联;

根据加密密钥的有效性，有条件地防止分发内容的解密;

确定加密密钥的有效性; 和

如果对于受保护介质来说，加密密钥无效，那么访问受保护介质上的链接信息，从而获得加密密钥，以便实现受保护介质上的分发内容的授权使用。

2、按照权利要求 1 所述的方法，其中访问链接信息包括把用户引导到查寻服务器。

3、按照权利要求 2 所述的方法，还包括把分发内容的唯一标识符发送给查寻服务器，以便识别提供加密密钥的来源。

4、按照权利要求 3 所述的方法，其中发送包含通过网络传送唯一标识符。

5、按照权利要求 3 所述的方法，其中所述唯一标识符包含分发内容独有的加密标题密钥。

6、按照权利要求 3 所述的方法，其中分发内容被加密; 并且

其中所述唯一标识符包含加密内容的密码散列。

7、按照权利要求 3 所述的方法，其中识别所述来源包含选择被授权提供加密密钥的多个可用来源中的至少一个。

8、按照权利要求 7 所述的方法，还包括用户选择一个可用来源以获得加密密钥。

9、按照权利要求 8 所述的方法，其中获得加密密钥包括购买加密密钥。

10、按照权利要求 8 所述的方法，其中获得加密密钥包括租用加密密钥。

11、按照权利要求 8 所述的方法，其中获得加密密钥包括接收加

密密钥来交换非货币因素。

13、按照权利要求 1 所述的方法，还包括把加密密钥独立于受保护内容保存在受保护介质软件狗上。

14、按照权利要求 13 所述的方法，还包括如果在受保护介质软件狗上没有找到加密密钥，那么访问从受保护介质软件狗到授权来源的链接信息，以便获得加密密钥。

15、按照权利要求 1 所述的方法，还包括把受保护内容保存在硬盘驱动器上。

16、按照权利要求 1 所述的方法，还包括把受保护内容保存在独立的受保护介质上。

17、按照权利要求 1 所述的方法，还包括保存指示用于从至少一个授权来源获得至少一个加密密钥的预算的值。

18、按照权利要求 17 所述的方法，还包括减少所述预算，以反映加密密钥的获得。

19、按照权利要求 1 所述的方法，其中受保护介质包含一个订购容器；并且

其中拥有可唯一识别的可记录介质授权受保护介质上的预定数目的受保护内容的使用。

20、按照权利要求 19 所述的方法，还包括通过根据介质 IS 在服务器系统中追踪，实施并存的内容对象；

还包括在把新内容记录到介质上之前，强制消除旧的内容。

21、按照权利要求 19 所述的方法，还包括根据介质的容量，强制实施并存的内容对象。

22、一种具有多条指令代码的计算机程序产品，所述多条指令代码用于实现受保护介质上的分发内容的授权使用，所述计算机程序产品包含用于执行权利要求 1-21 任意之一的步骤的指令代码。

23、一种能够实现受保护介质上的分发内容的授权使用的系统，包括：

基于分发内容未正确地与受保护介质关联的辨别，介质驱动器根

据加密密钥的有效性，有条件地防止分发内容的解密；

介质驱动器确定加密密钥的有效性；和

如果对于受保护介质来说，加密密钥无效，那么访问保存在受保护介质上的链接信息，从而获得加密密钥，以便实现受保护介质上的分发内容的授权使用。

24、一种能够实现受保护介质上的分发内容的授权使用的服务，包括：

基于分发内容未正确地与受保护介质关联的辨别，根据加密密钥的有效性，有条件地防止分发内容的解密的实用程序；

所述实用程序确定加密密钥的有效性；和

如果对于受保护介质来说，加密密钥无效，那么所述实用程序访问保存在受保护介质上的链接信息，从而获得加密密钥，以便实现受保护介质上的分发内容的授权使用。

实现受保护媒体上的分发内容的授权使用的系统、服务和方法

技术领域

本发明涉及实现受保护媒体上的分发内容的授权使用的系统、服务和方法。

背景技术

娱乐业处于数字革命的中心。音乐、电视和电影正在日益变得数字化，在质量和灵活性方面向消费者提供新的优越性。同时，数字革命也包含威胁，因为数字数据能够被完美并且快速地复制。如果消费者能够随意复制娱乐内容，并且在因特网上提供该内容，那么娱乐内容的市场会消失。

通过因特网发行数字内容，比如 MP3 和 DivX 编码电影的快速增长尤其令内容所有者担忧。这些争议极大并且未被授权的发行渠道已造成娱乐业对保护他们的价值数百万美元的内容的方法的需求增加。随着通过因特网共享的内容的数量每年按指数规律增长，开发一种内容保护系统变得日益重要，所述内容保护系统向内容所有者提供一种他们可用于安全地发行其受版权保护内容的端对端解决方案。

通过网络基础结构发行电子内容的一种传统方法使用预付费媒体(参见美国专利 No.6434535B1)。用户获得包含唯一密钥的预付费媒体。用户利用所述唯一密钥和预付费媒体的剩余余额联系指定的服务器。如果媒体和剩余余额有效，那么用户能够把选择的一项用所述唯一密钥加密的受保护内容下载到所述媒体。但是，这种方法不允许用户从除指定服务器之外的来源获得受保护内容，这种方法也不向用户提供获得使用通过未经授权的来源得到的一项受保护内容的授权的方法。

最近，消费电子产品方面的发展已产生对传统的数字产权管理系统的替换物。使用这种新方法(称为可记录介质的内容保护)技术的新的记录和播放设备已投入市场。现在能够直接把用 CPRM 保护的内容记录到可写介质中。如果在服务器中准备记录，那么客户端不需要任何特殊的密钥或者抗窜改。这种内容保护方法利用广播加密。设备不必进行会话来确定公用密钥。广播加密方面的最新进展使其在撤消能力方面和公钥密码学一样强大。由于广播加密的单向性，广播加密固有地适于保护存储器上的内容。

一旦客户端利用 CPRM 收到加密内容，内容服务器和客户端模块之间的交互作用就结束。服务器现在能够自由地集中在其它请求上。在客户端，CPRM 要求加密内容被记录在物理介质上，例如可记录光盘上。按照当加密内容位于该特定物理介质上的时候，所述加密内容只能由顺应设备播放的方式进行这种记录。从而，复制到另一物理介质上的加密内容不能被顺应设备播放。

CPRM 设备使用通常位于空白 DVD 可记录光盘上的介质密钥块和介质 ID 计算介质唯一密钥。介质唯一密钥被用于对标题密钥加密。标题密钥再对保存在 DVD 上的内容加密。用介质唯一密钥加密标题密钥导致标题密钥加密地与烧录内容的特定物理介质捆绑在一起。这可防止从任何其它物理介质解密和访问加密内容。

尽管这种技术被证明是有用的，不过提供进一步的改进是合乎需要的。受保护内容的常规复制保护技术通过超级分发，即文件共享防止受保护内容的使用。例如，用户具有受保护内容的许可副本，比如 DVD 上的电影。用户通过因特网与另一用户，比如一位朋友共享该内容。该朋友把所述内容复制到诸如 DVD-RAM 之类的受保护介质上。常规的复制保护技术阻止该朋友播放所述内容。但是，常规的复制保护技术并不允许该朋友购买使用所获得内容的许可证。通过把受保护介质的响应限制为“不要播放”，常规的复制保护技术限制了受保护内容通过诸如超级分发之类渠道的销售。

于是，需要一种使消费者能够以安全并且合法的方式利用受保护

介质分发受保护内容的系统、服务、计算机程序产品和相关方法。迄今为止，对这种解决方案的需要仍然没有得到满足。

发明内容

本发明设法满足上述需要的一个或多个方面，提供一种能够实现受保护介质上的分发内容的授权使用的系统、服务、计算机程序产品和相关方法(这里总称为“系统”或“本系统”)。本系统利用基于介质的复制保护以安全并且合法的方式支持受保护内容的在线分发。

通过利用以广播加密为基础的基于介质的复制保护方案，本系统实现诸如音频文件、电影之类受保护内容的在线分发。这里，受保护内容也被称为数字内容、受版权保护的内容或内容。目前，利用广播加密的标准包括视频内容保护系统(VCPS)，记录介质的内容保护(CPRM)和高级访问内容系统(AACS)。虽然在 CPRM 方面来说明本系统，不过显然本系统可应用于利用广播加密的任何复制保护系统，或者使数字内容被加密并且与物理介质关联的任何内容保护系统。

本系统能够以安全并且合法的方式实现内容的基于介质的超级分发。例如，用户拥有诸如电影之类的内容的许可副本。该用户通过因特网与一位朋友共享所述电影。该朋友把所述电影复制到诸如 DVD-RAM 之类的受保护介质上。常规的复制保护系统仅仅阻止播放所述电影，因为在受保护介质上并不存在“绑定密钥”(唯一的加密密钥)。相反，本系统把该朋友引导到一个或多个网站，从所述一个或多个网站可购买内容的使用许可证，并且可获得绑定密钥。这样，在保护内容所有者的权利的同时，本系统允许以安全并且合法的方式超级分发内容，从而能够通过超级分发实现受保护内容的新的营销技术。

本系统使用相对于许可服务器的简单交易流来实现受保护内容的授权超级分发。用户接收一项未经许可的内容，并把所述未经许可的内容转移到受保护介质。另一方面，用户得到未经许可的内容已存在于其上的受保护介质。用户试图在介质设备上播放所述未经许可的内容。所述介质设备把用户引导到一个网站，所述网站提供一个或多

个到能够进行交易，从而允许所述未经授权内容的电子商务企业的链接。通过经因特网把加密的绑定密钥传送给受保护介质，未经许可的内容被授权。

未经许可的内容在常规的内容经销商控制的渠道之外分发。从而，所述网站提供从用户到未经许可内容的授权经销商的链接。介质设备把未经许可内容的内容 ID 提供给所述网站。网站查寻未经许可内容的电子零售商的名单，并把该名单提供给用户。用户随后能够根据其个人喜好选择一个电子零售商。由于用户已拥有未经许可的内容，因此该交易只涉及加密的绑定密钥的传递。从而，交易快速，在服务器方需要适中的带宽能力。

通过由播放器呈现给用户的消息上的链接，用户可被引导到所述网站，这要求用户点击所述链接以便导航到所述网站。媒体播放器可自动为用户启动该网站。所述网站还可起可向其购买或租用内容的电子商务企业的作用。超级分发模型允许对等文件共享服务的操作，所述对等文件共享服务使用户能够按照安全并且合法的方式通过网络交换内容。作为一个优点，只需要一个保护机制就可在分发和基于介质的重放期间保护所述内容。

在一个实施例中，通过硬件复制保护设备，比如软件狗（dongle）上的绑定密钥允许内容。这种软件狗模型并不依赖于超级分发模型。在常规术语中，软件狗是连接在计算机上，控制用户对特定应用程序或其它内容的访问的装置。在本实施例中，受保护介质(这里还被称为受保护介质软件狗)被用作软件狗。例如，PC 包含 SD 卡适配器；SD 卡充当受保护介质软件狗。通过加密，受保护内容被绑定到当允许所述受保护内容时，要求提供的受保护介质软件狗上。受保护介质软件狗代表消费内容的许可证的物理权标。所述许可证表示内容的购买，内容的租用，内容的推销赠送等。

用户通过下载，通过电子邮件附件，通过从另一介质复制等，接收受保护内容。受保护内容被复制到诸如硬盘驱动器之类的存储设备上。应用程序或媒体播放器播放或以其它方式“消费”内容。为了消费

内容，应用程序需要一个密钥。所述密钥被加密并被保存在受保护介质软件狗上。从而，对于应用程序来说，为了获得和解密所述密钥，需要受保护介质软件狗的存在。借助这里所述的超级分发模型，可获得该密钥，或者可作为常规记录操作的一部分获得所述密钥。这样，用户可在许多地方具有所述内容的许多副本，但是只能够使用或者消费可以获得受保护介质软件狗上的密钥的那个副本。在本实施例中，内容包含在 PC 或者其它媒体播放器上消费的任何内容，比如多媒体内容，诸如游戏之类的可执行内容等等。与受保护介质软件狗无关地加密分发所述密钥，并利用绑定机制把所述密钥绑定到受保护介质软件狗上。

例证的受保护介质软件狗是 SD 卡。常规 SD 卡的存储容量为 64 MB、256 MB 等。尽管 SD 卡太小以至于不能保存应用程序，不过 SD 卡能够保存许多不同的密钥。典型的密钥约为 20 字节。从而，容量为 64 MB 的 SD 卡能够包含 3 百万份不同内容，比如游戏、电影、应用程序、数据库、视频、音频或者要求保密分发的任意其它类型的内容的密钥。

本实施例利用由受保护介质提供的廉价的复制保护特征来保护 PC 上的任意形式的内容。本实施例保护受保护介质软件狗上的密钥，而不是设法保护 PC 上的内容。从而，本实施例把受保护介质的复制保护能力扩展到 PC 和硬盘驱动器。

本实施例还提供可移植性特征，因为内容可被复制到另一台 PC。但是，在任意时刻使用每份副本都需要受保护介质软件狗上的密钥；即，如果用户购买了内容的一个副本的许可证，那么每次只可使用该内容的一个副本。例如，用户可能具有度假住所。用户可产生他的整个视频和音频文件库的副本，并把该副本保存在他的度假住所中。用户把受保护介质软件狗随身带到他的度假住所，并且可以访问所述整个文件库。但是，在没有受保护介质软件狗的情况下，他的常住住所中的内容不能被播放。在任一时刻只能播放所述文件库的副本之一。播放文件库的另一副本的能力要求获得所述文件库的内容的其它密

钥，并把这些其它密钥保存在另一个受保护介质软件狗上。

在另一实施例中，本系统起电子钱夹的作用。电子钱夹使用受保护介质的保护能力来管理预算信息。预算信息能够实现预定次数的交易或者可花在交易上的预定美元值。保存在受保护介质上的受保护内容是可用的预算。受保护介质管理预算的状态，防止所述预算被复制到其它介质。受保护介质还保护预算不被“退回重来”（roll back）；即，防止用户产生处于初始值的电子钱夹的副本，消费一部分的电子钱夹，并利用备份把电子钱夹恢复到初始值。

电子钱夹可由用户购买，或者作为推销赠送给予用户。利用电子钱夹进行的交易在用户方可以是匿名的，或者可包含关于用户的信息。通过在线交易，可以补充电子钱夹上的预算的值。和电子钱夹上的预算的值有关的信息被保存在电子钱夹上，而不是保存在中央处理系统上，这使受保护钱夹可在连接被切断的环境中使用。为了向电子钱夹充值，服务器需要通过诸如因特网之类的网络访问电子钱夹。

利用受保护介质的电子钱夹包含复制保护和状态管理。复制保护防止电子钱夹的复制，消除用户简单地无限次复制电子钱夹，以便无限次地访问电子钱夹上的预算的可能性。状态管理防止用户利用电子钱夹的副本恢复电子钱夹的预算，从而把电子钱夹的预算“退回到”以前的值。

例如，用户得到一个电子钱夹，作为一种推销，所述电子钱夹装有三次播放的初始信用量（credit）。用户随后可下载受保护电影，并使用在电子钱夹上管理的余额播放所述内容三次。当试图获得比所述推销允许的次数更多的电影播放次数时，用户产生在电子钱夹的预算中具有三次播放的电子钱夹的副本。受保护介质包含操作电子钱夹，从而操作所述电影所需的密钥。当电子钱夹的内容被复制到任意形式的介质上时，电子钱夹不能得到出自受保护介质的密钥；从而，电子钱夹的副本不起作用。

在另一获得比所述推销允许的次数更多的电影播放次数的尝试中，用户播放所述电影三次，随后试图用以前产生的电子钱夹的副本

代替电子钱夹起作用。

存在于电子钱夹上的余额由具有记录能力的应用程序减少。在一个实施例中，减少余额由所述应用程序执行，只要该应用程序可以访问用于修改电子钱夹的加密密钥。在另一实施例中，利用可以访问用于修改电子钱夹的加密密钥的服务器在线减少余额。即使电子钱夹由服务器在线修改，用现金购买的电子钱夹也不需要来自用户的任何个人信息。交易可以是匿名的，因为采取受保护介质形式的电子钱夹的存在足以确认电子钱夹上的预算。从而，电子钱夹利用能够以匿名方式实现匿名交易的廉价受保护介质的复制保护特征。

电子钱夹的状态表示可由本系统减少的任意值。电子钱夹的状态可由与授权服务器或者验证的应用程序的交易增加。任意应用程序能够“再装”电子钱夹，只要该应用程序具有对受保护介质进行写操作所必需的设备密钥。

电子钱夹可被用于内容的世代管理，限制用户能够产生的内容的副本数目。电子钱夹可用于从可接入用于购买的因特网的电子商务或标准零售店的被用于向用户提供自多次购买或者购买值。

在另一实施例中，本系统起受保护介质订购容器(container)的作用。在订购过程中，受保护介质上的介质 ID 把该受保护介质指定为与特定用户关联的租用介质。用户能够远程或者本地把内容从租用服务复制到租用介质。例如，用户可通过因特网把内容从租用服务下载到租用介质。用户还可本地把内容从诸如出租零售店中的信息亭之类的设备复制到租用介质。

租用介质是租用内容的“容器”。订购条款能够限制用户在任意时刻只能拥有三项内容。为了拥有另一项内容，用户重写租用介质中的三项内容之一。用户被允许对向租用内容的提供商登记的租用介质进行次数不限的下载。但是，用户限于在任意时候只能拥有预定项数的租用内容。另一方面，并存租用的最大数目强制服从于介质本身的容量。这种情况下，用户可对登记为租用容器的介质进行次数不限的下载。但是，由于介质的容量有限，当下载新内容时，因此用户将不得

不重写旧内容。

本系统使用受保护介质的唯一标识来提供一种安全并且合法的经营内容租赁企业的方法，而不需要可信时钟来限制可消费所述内容的时间窗。此外，订购租赁模型允许以安全并且合法的方式使用内容的因特网下载，而不需要把内容寄给用户和寄回内容租赁企业。

可用诸如受保护内容分发系统实用程序之类的实用程序具体体现本发明。本发明还向用户提供获得消费受保护介质上的受保护内容的许可证的手段。用户调用受保护内容分发系统实用程序，从而在获得受保护内容的加密密钥之后能够实现受保护内容的使用。本发明还向用户提供通过保存在受保护介质上的加密密钥，在介质设备上实现受保护内容的使用或消费的手段。用户调用受保护内容分发系统实用程序，从而能够从在其上操作受保护内容的介质设备外部的软件狗介质设备实现受保护介质作为受保护介质软件狗的使用。此外，本发明向用户提供获得和消费受保护介质上的预算的手段。用户调用受保护内容分发系统实用程序，从而管理受保护介质上的预算。本发明还向用户提供把受保护介质操作为租用容器的手段。用户调用受保护内容分发系统实用程序来管理受保护介质上的租用的受保护内容。

附图说明

下面参考附图，举例详细说明本发明的实施例，其中：

图 1 是例证运行环境的示意图，其中本发明的优选实施例的受保护内容系统可被用于实现通过超级分发获得的受保护内容的使用；

图 2 由图 2A 和 2B 组成，表示图 1 的受保护内容分发系统在许可通过超级分发获得的受保护内容方面的操作方法的处理流程图；

图 3 是例证运行环境的示意图，其中本发明的优选实施例的受保护内容分发系统可被用于通过受保护介质软件狗实现受保护内容的可选择使用；

图 4 是图解说明图 3 的受保护内容分发系统在使用图 3 的受保护介质软件狗方面的操作方法的处理流程图；

图5是图解说明图3的受保护内容分发系统在消费受保护内容方面的操作方法的处理流程图;

图6是例证运行环境的示意图,其中本发明的优选实施例的受保护内容分发系统可被用作受保护介质电子钱夹;

图7由图7A和7B组成,表示图解说明图7的受保护内容分发系统的操作方法的处理流程图;

图8是例证运行环境的示意图,其中本发明的优选实施例的受保护内容分发系统可被用作受保护介质租赁容器;

图9由图9A和9B组成,表示图解说明起用于受保护内容的租赁的受保护介质租赁容器作用的图1的受保护内容分发系统的操作方法的处理流程图。

具体实施方式

下面的定义和解释提供与本发明的技术领域相关的背景信息,意图帮助理解本发明,而不是限制本发明的范围:

内容:在电子设备上以数字格式呈现的受版权保护的内容,比如音乐、电影、音频文件、电子书籍、数据库、应用程序、游戏等。

软件狗:连接在计算机上,控制对特定应用程序或者受保护内容项目的访问的装置。

因特网:依据一组标准协议,由路由器连接在一起,从而形成分布式全球网络的许多互连公共和专用计算机网络。

受保护介质:任意形式的具有复制保护技术的介质,比如保密MMC、闪速存储卡、保密数字存储卡(SD卡)、具有随机存取存储器的数字通用光盘、具有读/写能力的数字通用光盘(DVD-R/W、DVD+RW)、高清晰度数字通用光盘和硬盘数字通用光盘(HD-DVD)等。

超级分发:通过除从商业实体销售给消费者之外的渠道,从一个用户到另一用户的内容分发,例如当用户与一位朋友共享内容的副本时。超级分发的例子包括诸如Napster®、Kazaa®之类的文件共享方

案。

URL(统一资源定位符): 完全指定内容对象在因特网上的位置的唯一地址。URL 的一般形式是协议://server-address/path /filename。

万维网(WWW，也称为 Web): 一种因特网客户端-服务器超文本分发信息检索系统。

图 1 描绘例证的总体环境，其中可以使用按照本发明的利用受保护介质分发受保护内容的系统、服务、计算机程序产品和相关方法("系统 10")。系统 10 包括一般嵌入介质设备 20 内或者安装在介质设备 20 上的软件编程代码或者计算机程序产品。

介质设备 20 可以读写受保护介质 15。介质设备 20 是能够播放或执行受保护介质 15 上的受保护内容 25 的任意设备。用户接收受保护内容 25; 受保护内容 25 是未经许可的受版权保护数字内容的副本。例如，用户可通过从文件共享网站下载受保护内容 25，作为电子邮件中的附件等，接收受保护内容 25。用户把受保护内容 25 复制到空的受保护介质 15 上。另一方面，用户可从另一来源得到受保护介质，同时受保护内容 25 已存在于受保护介质 15 上。

用户试图在介质设备 20 中播放受保护介质 15 上的受保护内容 25。为了播放、读取、执行或以其它方式消费受保护内容 25，介质设备需要受保护介质 15 上的加密密钥，所述加密密钥与该特定介质绑定在一起。一般来说，绑定的加密密钥存在于包含授权受保护内容的受保护介质上，指示作为授权事务的结果，用户已获得消费该受保护介质上的受保护内容的权限。

当介质设备 20 访问受保护介质 15 上的受保护内容 25 时，找不到该特定介质的有效加密密钥。介质设备 20 访问受保护介质 15 上的系统 10。系统 10 包括链接，比如到查寻服务器 3 的 URL。用户借助查寻服务器接口 35 和系统 10 访问查寻服务器 30。通过网络 40，介质设备 15 能够访问查寻服务器 30。

系统 10 向查寻服务器 30 提供受保护内容 25 的唯一标识符或者说明，所述说明包括例如标题、作者、作曲者、制作者、产权所有者

等。所述唯一标识符也可由加密内容的密码散列组成。查寻服务器 30 查寻被准许销售使用受保护内容的许可证的零售商或其它服务提供商。用户通过选择链接或 URL，利用查寻服务器接口 35 选择服务提供商之一。

介质设备 20 能够通过网络 40 访问服务提供商 45(可用来源)。用户完成与服务提供商 45 的交易，服务提供商 45 向用户转让消费受保护介质 15 上的受保护内容的权限。所述交易可以采取购买、租赁或者允许用户消费受保护内容 25 的推销活动的形式。介质服务 20 能够通过网络 40 访问安全提供商。介质设备 20 把与服务提供.45 的交易的证据提供给安全提供商 50。作为回报，安全提供商 50 把受保护介质 15 上的受保护内容 25 的加密密钥提供给用户。加密密钥把受保护内容 25 绑定在受保护介质 15 上，使用户能够在与服务提供商 45 的交易的条款内消费受保护介质 15 上的受保护内容 25。

介质设备 20 包括使用户可以安全地与查寻服务器 30、服务提供商 45 和安全提供商 50 连接的软件。介质设备 20 通过通信链路 55，比如电话、电缆或者卫星链路与网络 40 连接。查寻服务器 30 可通过通信链路 60 与网络 40 连接。服务提供商 45 可通过通信链路 65 与网络 40 连接。安全提供商 50 可通过通信链路 70 与网络 40 连接。虽然用网络 40 来描述系统 10，不过介质设备 20 可本地而不是远程访问查寻服务器 30、服务提供商 45 或安全提供商 50。

图 2(图 2A、2B)图解说明系统 10 在许可通过超级分发获得的受保护内容方面的方法 200。用户通过某种未经批准的分发方法接收受保护内容 20(步骤 205)。用户把受保护内容 20 写入受保护介质 15(步骤 210)。用户试图在介质设备 20 上播放受保护内容 20(步骤 215)。介质设备 20 发现受保护介质 15 并不包含所需的加密密钥(步骤 220)。介质设备 20 访问受保护内容分发系统(系统 10)(步骤 225)。系统 10 通过查寻服务器接口 35 把用户引导到查寻服务器 30，并把受保护内容 25 的描述提供给查寻服务器 30(步骤 230)。

查寻服务器 30 查寻准许向用户销售、出租或者赠送消费受保护

内容 25 的许可证的零售商或者其它服务提供商，比如服务提供商 45(步骤 235)。查寻服务器 30 通过查寻服务器接口 35 把寻找到的服务提供商列表提供给用户(步骤 240)。用户通过选择到某一服务提供商，比如服务提供商 45 的链接，选择服务提供商(步骤 245)。用户购买、租借或者免费接收消费受保护内容 25 的许可证(步骤 250)。服务提供商 45 批准把加密密钥传送给介质设备 20(步骤 255)。所述批准包括把购买的证据提供给介质设备 20；介质设备 20 把所述购买证据提供给安全提供商以交换加密密钥。另一方面，服务提供商 45 把购买证据直接发送给安全提供商 50；安全提供商 50 随后把加密密钥传送给介质设备 20。

介质设备 20 把加密密钥记录在受保护介质 15 上(步骤 260)。加密密钥把受保护内容 25 绑定在受保护介质 15 上，要求受保护内容 25 只能从受保护介质 15 被消费。介质播放器 20 播放受保护介质 15 上的受保护内容 25(步骤 265)。

图 3 图解说明系统 10 的一个实施例，系统 10A(它大体类似于系统 10)，其中受保护介质 15 被用作受保护介质软件狗。显然可独立于这里描述的任何其它模型，比如超级分发模型实现软件狗模型。

受保护介质 15A 大体类似于受保护介质 15。这里，受保护介质 15A 还被称为受保护介质软件狗 15A。受保护内容 25A 被保存在介质设备 20A 上。受保护内容 25A 大体类似于受保护内容 25。介质设备 20A 大体类似于介质设备 20。介质设备 20A 还包含用于执行、播放或者以其它方式消费受保护内容 25A 的应用程序 305。在本实施例中，介质设备 20A 是能够保存和访问受保护内容 25A，并能通过软件狗介质设备 30 访问关于受保护介质软件狗 15A 的信息的任意设备。例证的介质设备 20A 是个人计算机。

系统 10A 把受保护内容 25A 的加密密钥保存在受保护介质软件狗 15A 上。为了执行或者以其它方式操作受保护内容 25A，介质设备 15A 需要获得受保护内容 25A 的加密密钥。从而，只有当受保护介质软件狗 15A 被插入软件狗介质设备 310 中时，受保护内容 25A 才能

被消费。例证的受保护介质软件狗 15A 是 SD 卡。例证的受保护介质软件狗设备 310 是 SD 卡读/写器。受保护介质软件狗设备 310 是能够读写受保护介质软件狗 15A 的任意设备。

图 4 图解说明系统 10 的使用受保护介质软件狗 15A 来安全、合法地使用保存在介质设备 20A 上的受保护内容 25A 的方法 400。用户获得受保护内容 25A(步骤 405)。就步骤 405 来说，获得受保护内容 25A 包括获得消费受保护内容 25 的许可证。通过在与受保护内容 25A 的授权来源，比如服务提供商 45 的交易中下载受保护内容 25A，可获得所述许可证。另一方面，可如图 2 中步骤 205-步骤 255 中所述那样为未经授权内容获得许可证。与服务提供商 45 的交易的结果是使介质设备 15A 能够执行或者以其它方式消费受保护内容 25A 的加密密钥。受保护介质软件狗设备 310 把加密密钥记录在受保护介质软件狗 15A 上(步骤 410)。

图 5 图解说明应用程序 305 执行、播放或以其它方式消费由保存在受保护介质软件狗 15A 上的加密密钥保护的受保护内容 25A 的操作方法 500。用户启动应用程序 305 执行受保护内容 25A(步骤 505)。应用程序 305 从受保护介质软件狗 15A 上的系统 10 取回受保护内容 25A 的加密密钥(步骤 510)。

应用程序 305 确定受保护内容 25A 是否和受保护介质软件狗 15A 上的加密密钥匹配(判定步骤 515)。如果受保护内容 25A 不匹配加密密钥，那么该应用程序执行图 4 图解说明的方法 400，从而获得加密密钥(步骤 520)。否则，应用程序 305 强制执行由受保护介质软件狗 15A 上的系统 10 管理的受保护内容 25A 的使用条件(步骤 525)。使用条件包括受保护内容 15A 可被执行的次数。应用程序 305 使用加密密钥在介质设备 20A 上对受保护内容 15A 解密(步骤 530)，并执行或以其它方式消费受保护内容 25A(步骤 535)。

图 6 图解说明系统 10 的另一实施例，系统 10B(它大体类似于系统 10 或 10A)，其中受保护介质 15B 被用作电子钱夹。受保护介质 15B 大体类似于受保护介质 15。这里，受保护介质 15B 还被称为受保护

介质电子钱夹 15B。受保护内容 25B 被保存在受保护介质电子钱夹 15B 上。受保护内容 25B 大体类似于受保护内容 25。受保护内容 25B 包含用户可用于购买、租借或以其它方式获得诸如受版权保护内容之类产品的预算或状态。受保护介质电子钱夹 15B 包含用于维护受保护介质电子钱夹 15B 的状态或预算的系统 10B。

进一步参考图 6，图 7(图 7A、7B)图解说明受保护介质电子钱夹 15B 上的系统 10B 的方法 700。用户进行交易，从而获得预装预定预算的受保护介质电子钱夹 15B(步骤 705)。所述交易可包含购买、订购、租借或者推销赠送。另一方面，用户可在零售店中的信息亭选择受保护介质电子钱夹 15B 的初始预算或状态；信息亭中的安全提供商把选择的初始预算或状态烧录在受保护介质电子钱夹 15B 上。

用户把受保护介质电子钱夹 15B 插入介质设备 20B 中(步骤 710)。介质设备 20B 大体类似于介质设备 20。介质设备 20B 可位于零售店中，用户的家中，或者介质设备 20B 可以访问诸如服务提供商 45 之类的服务提供商和诸如安全提供商 50 之类的安全提供商的其它地方。用户利用电子钱夹接口 605 在受保护介质电子钱夹 15B 上的系统 10 引导下访问服务提供商 50(步骤 715)。用户从服务提供商 50 提供的产品中选择诸如应用程序、音频文件、视频文件、电影、电子书籍、数据库之类的受保护内容产品(步骤 720)。

服务提供商 45 确定受保护介质电子钱夹 15B 的预算或状态的剩余值是否足以完成选择的交易(判定步骤 725)。如果否，那么服务提供商 45 拒绝该交易(步骤 730)。如果是，那么安全提供商批准该交易(步骤 735)。安全提供商把反映受保护介质电子钱夹 15B 上的新余额的加密密钥更新发给介质设备，所述新余额反映所述交易的价格(步骤 740)。

用户以加密文件的形式把受保护内容 25B 下载到受保护介质电子钱夹 15B(步骤 745)。介质设备记录反映受保护介质电子钱夹的预算或状态的减少值的新加密信息，所述减少值反映所述交易(步骤 750)。受保护介质电子钱夹 15B 包含受保护介质电子钱夹 15B 的预算或状

态，和下载的受保护内容 25B。用户可下载另外的下载受保护内容 25B，直到受保护介质电子钱夹 15B 的预算或状态被用尽为止。通过利用电子钱夹接口 605 与服务提供商 45 和安全提供商 50 进行交易，用户可增加受保护介质电子钱夹 15B 的预算或状态的值。显然下载的受保护内容 25B 可出现在硬盘驱动器或者不同的受保护介质上，钱夹(即，预算数据)和实际内容不一定被组合在相同的受保护介质上。

另一方面，用户可能已通过其它来源，比如通过超级分发获得了受保护内容 25B，并且已把受保护内容写入受保护介质电子钱夹 15B。这种情况下，用户按照和前面关于图 1 和图 2 说明的处理类似的方式，获得用于播放受保护内容 25B 的加密密钥。

例如，服务提供商 45 向消费者提供利用受保护介质电子钱夹 15B 购买受保护内容的能力。用户购买预装 60 信用量的受保护介质电子钱夹 15B。受保护介质电子钱夹 15B 具有 50 首歌曲的容量。受保护介质电子钱夹 15B 包含介质 ID 139。服务提供商 45 以 6 个信用量出售一首最新发行的歌曲，而其它歌曲价值为 3 个信用量。用户可从中选择购买的歌曲的例证列表示于表 1 中。

表 1：供利用受保护介质电子钱夹 15B 租用的歌曲的例证列表

电影 ID	音乐标题	信用成本
1	歌曲 A	6
2	歌曲 B	3
3	歌曲 C	3

表 2 举例说明在购买三首歌曲之后，用户对受保护介质电子钱夹 15B 的使用历史。每次用户按照歌曲的价格购买歌曲时，受保护介质电子钱夹 15B 的预算余额被减少。每次购买一首歌曲时，所得到的余额用加密密钥加密，并被写入受保护介质电子钱夹 15B 中。

表 2：利用受保护介质电子钱夹 15B 的歌曲购买的例证历史

先前余额	新余额	歌曲 ID
60	54	1
54	51	3
51	48	2

图 8 图解说明系统 10 的另一实施例，系统 10C(它大体类似于系统 10)，其中受保护介质 15 被用作租赁容器。受保护介质 15C 大体类似于受保护介质 15。这里，受保护介质 15 还被称为受保护介质租赁容器 15C。受保护内容 25C 被保存在受保护介质租赁容器 15C 上。受保护内容 25C 大体类似于受保护内容 25。受保护介质租赁容器 15C 包含可被用于租用受版权保护的内容的预算或状态。受保护介质租赁容器 15C 还包含用于维护受保护介质租赁容器 15C 的状态或预算的系统 10C。

进一步参考图 8，图 9(图 9A、9B)图解说明受保护介质租赁容器 15C 上的系统 10C 的方法 900。用户订购受保护内容租用服务，并收到受保护介质租赁容器 15C(步骤 905)。用户把受保护介质租赁容器 15C 插入介质设备 20C 中(步骤 910)。介质设备 20C 大体类似于介质设备 20。在一个优选实施例中，为管理特定的租用提供物（offering）而需要的只是介质 ID。

用户选择供下载的租用内容(步骤 915)。作为基本订购的一部分，或者作为推销赠送，租用服务可出于额外的费用把受保护介质租赁容器 15C 的其它副本提供给用户。表 4 中举例说明了例证的介质表格，所述介质表格列举受保护介质租赁容器 15C 的副本的例证介质 ID。

表 4：列举介质 ID 的例证介质表格

介质 ID
123
456

租用服务的服务提供商 45 确定该介质 ID 是否被准许出租当前插入介质设备 20C 中的受保护介质租赁容器 15C 上的受保护内容 25C(判定步骤 920)。如果该介质 ID 未被批准，那么服务提供商 45 提出对订购增加另外的介质(判定步骤 925)。如果用户拒绝该提议，那么服务提供商 45 拒绝交易(步骤 930)。如果用户接受该提议，那么用户开始与服务提供商 45 交易，并升级介质订购，以包括当前插入介质设备中的受保护介质租赁容器(步骤 935)。

用户选择供租用的产品(步骤 940)。另外，如果介质 ID 被批准(步骤 920)，那么用户将被准许选择供租用的所需产品。

产品包括受版权保护的内容，例如电影、音频文件、视频文件、电子书籍、数据库、游戏、应用程序等。例如，租用服务可向订购租用服务的用户出租电影。可供租用的电影的例证列表示于表 5 中。

表 5: 列举可向租用服务租借的每部电影的电影 ID 的例证电影表格

电影 ID	电影标题
1	电影 A
2	电影 B
3	电影 C
4	电影 D

例如，用户选择电影 C。服务提供商 45 确定用户的订购是否允许所选产品的租用(判定步骤 945)。例如，订购可允许用户在任一时刻租用三部电影。受保护介质租赁容器 15C 包含用户当前租用的三部电影。这种情况下，用户能够升级他的订购，以便在受保护介质租赁容器 15C 上租用更多的电影，选择受保护介质租赁容器 15C 上的一部电影以便用新选择的电影重写，或者取消交易。

如果受保护介质租赁容器 15C 包含的产品的数目少于在任一时刻可租用的产品的最大许可数目，那么订购允许选择的产品(判定步骤 945)。服务提供商 45 允许介质设备 20C 把选择的产品和安全提供商 50 准备的加密密钥下载到受保护介质租赁容器 15C。加密密钥包含受保护介质租赁容器 15C 上可供用户消费的每项受保护内容的介质 ID。

用户 ID“psuedo”租用的电影和相关介质 ID 的例证表格示于表 6 中。用户选择电影 D，以便下载到具有介质 ID 123 受保护介质租赁容器 15C。用户的订购允许在具有介质 ID 123 的受保护介质租赁容器 15C 上，在任一时刻租用两部电影。该订购并不允许用户只是把电影 D 增加到具有介质 ID 123 的受保护介质租赁容器 15C 中(判定步骤 945)。

表 6：到特定日期，比如 8 月 22 日为止，用户“pseudo”租用的电影和相关介质 ID 的例证列表

用户 ID	介质 ID	电影 ID	下载日期
psuedo	123	1	8 月 15 日
psuedo	456	3	8 月 15 日
pseudo	123	2	8 月 22 日

服务提供商询问用户是否想要升级订购(判定步骤 955)。如果是，那么用户与服务提供商 45 开始交易，并升级所述订购以允许选择的产品(步骤 960)，处理进入步骤 950。如果用户不想升级订购(判定步骤 955)，那么服务提供商 45 询问用户是否想要用新电影重写具有介质 ID 123 的受保护介质租赁容器 15C 上的一部电影(判定步骤 965)。如果是，那么用户选择一部电影，比如电影 A(电影 ID 1)，以便由新电影(具有电影 ID 4 的电影 D)重写(步骤 970)，处理进入步骤 94。如果用户拒绝选择供重写的一部电影，那么服务提供商 45 拒绝租用交易(步骤 975)。

显然上面说明的本发明的具体实施例只是举例说明本发明的原理某些应用。在不脱离本发明的范围的情况下，可对这里描述的利用受保护介质分发受保护内容的系统、服务和方法做出许多修改。此外，虽然用 CPRM 来说明本系统，不过显然本系统可应用于利用广播加密的任何复制保护系统。此外，虽然仅仅出于举例说明的目的，关于 WWW 说明了本发明，不过显然本发明也适用于可通过其分发内容的任何网络。

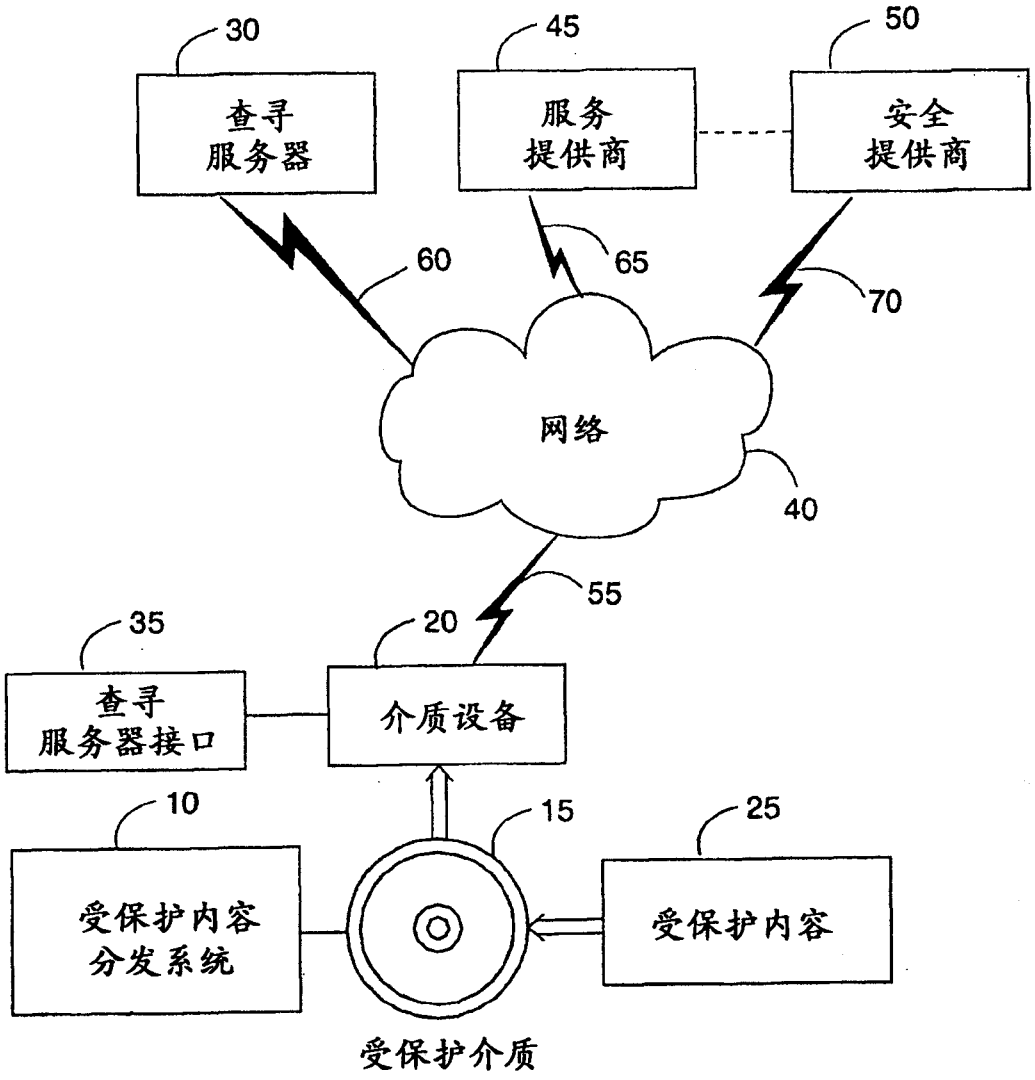

30
查寻
服务器
45
服务
提供商
50
安全
提供商
60
65
70
网络
40
55
35
查寻
服务器接口
20
介质设备
10
受保护内容
分发系统
15
25
受保护内容
受保护介质

图1

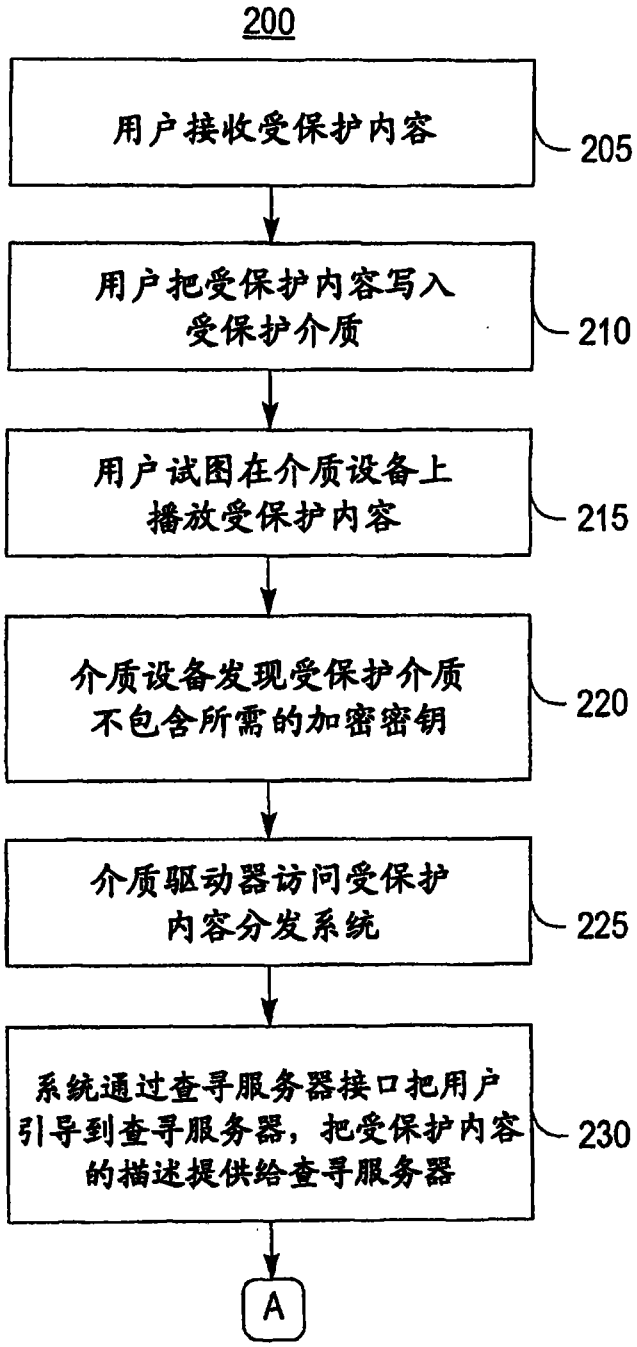

200
用户接收受保护内容
205
用户把受保护内容写入受保护介质
210
用户试图在介质设备上播放受保护内容
215
介质设备发现受保护介质不包含所需的加密密钥
220
介质驱动器访问受保护内容分发系统
225
系统通过查寻服务器接口把用户引导到查寻服务器，把受保护内容的描述提供给查寻服务器
230
A

图2a

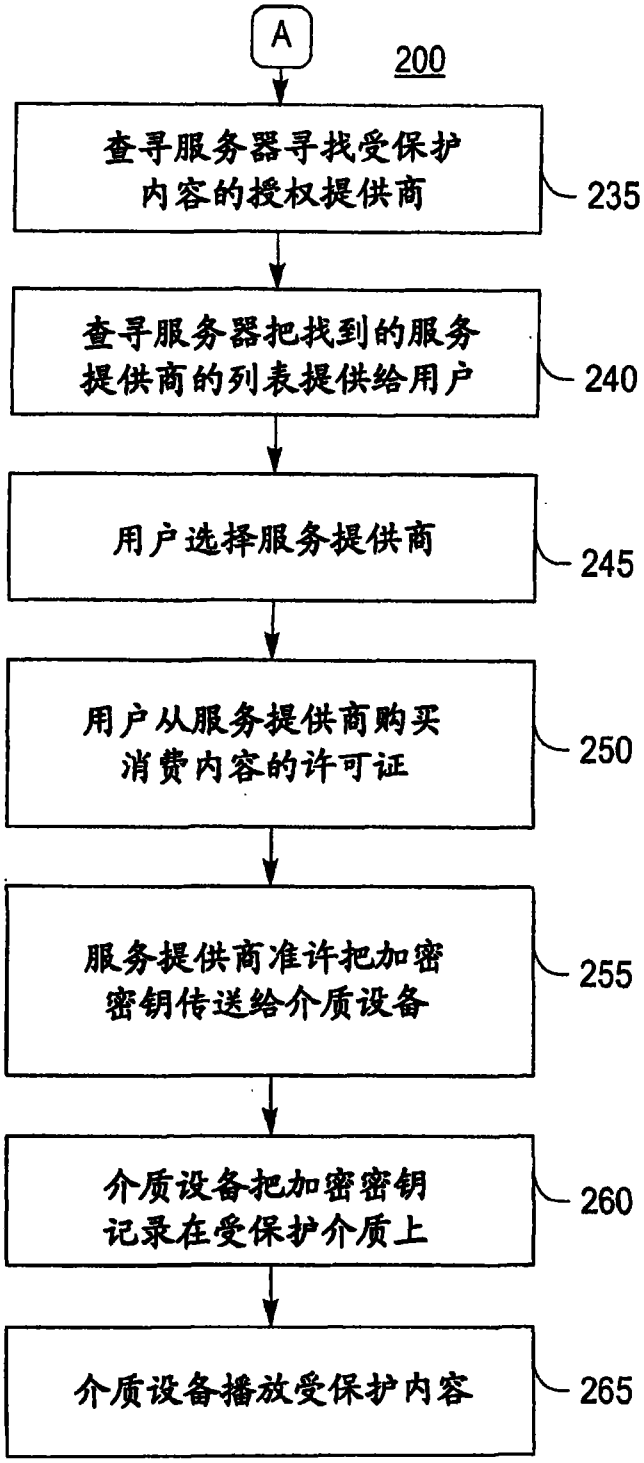

A
200
查寻服务器寻找受保护内容的授权提供商
235
查寻服务器把找到的服务提供商的列表提供给用户
240
用户选择服务提供商
245
用户从服务提供商购买消费内容的许可证
250
服务提供商准许把加密密钥传送给介质设备
255
介质设备把加密密钥记录在受保护介质上
260
介质设备播放受保护内容
265

图2b

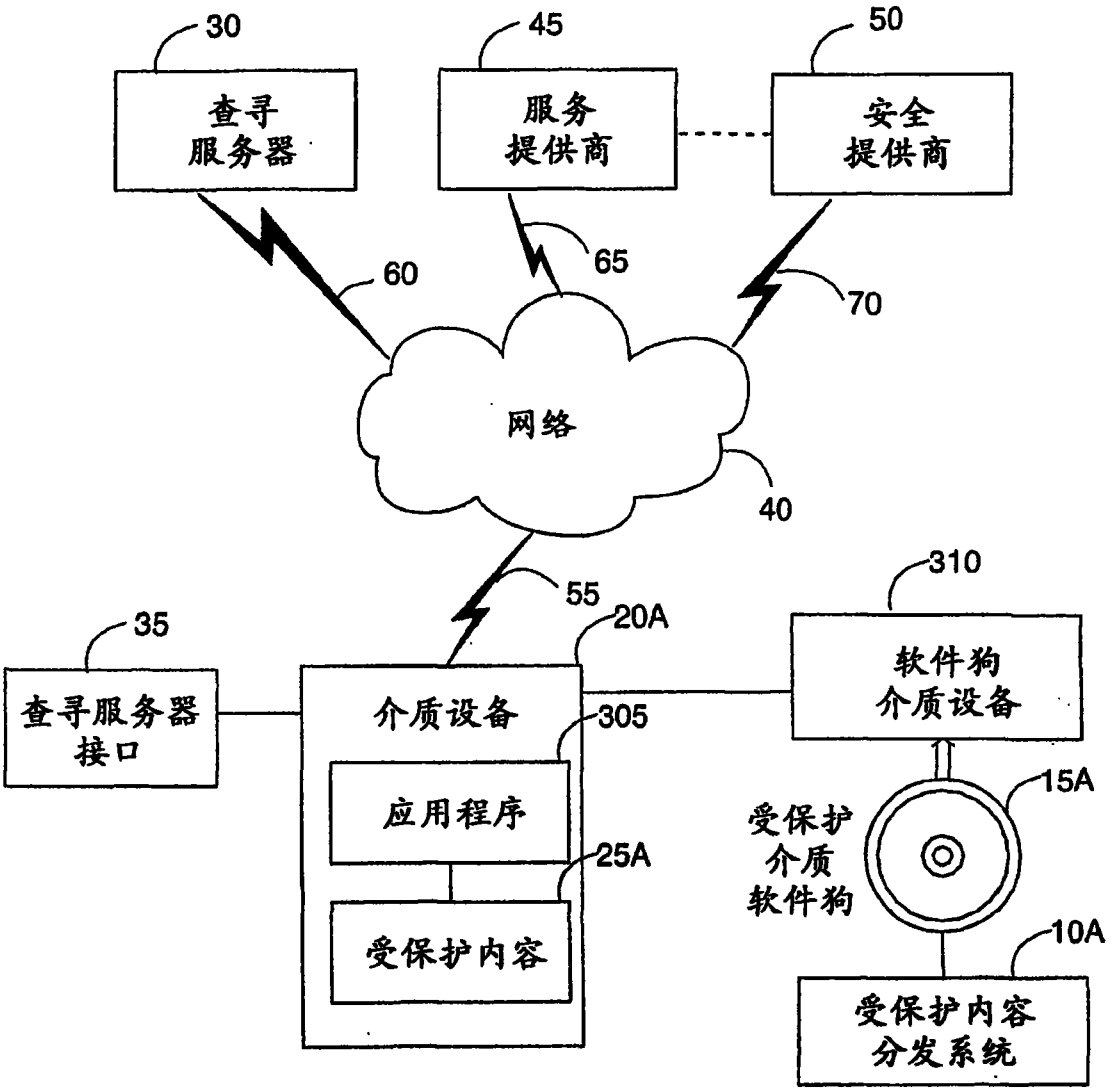

30
查寻
服务器
45
服务
提供商
50
安全
提供商
60
65
70
网络
40
55
20A
310
35
查寻服务器
接口
介质设备
305
软件狗
介质设备
应用程序
25A
15A
受保护
介质
软件狗
受保护内容
10A
受保护内容
分发系统

图 3

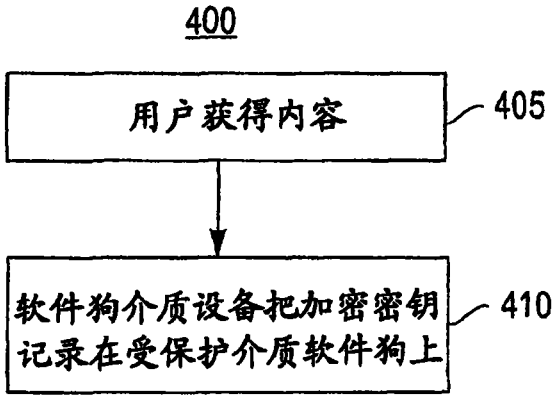


图4

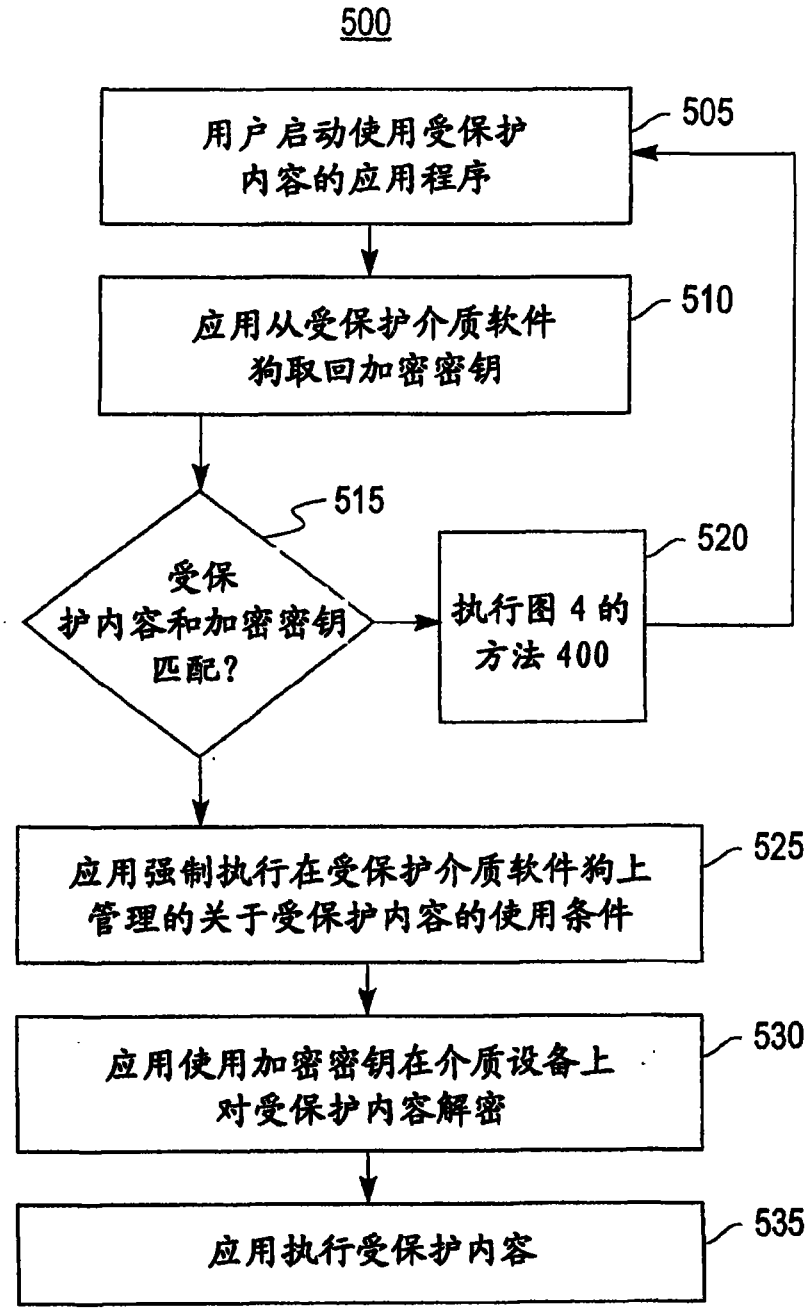

500
用户启动使用受保护内容的应用程序
505
应用从受保护介质软件狗取回加密密钥
510
受保护内容和加密密钥匹配?
515
执行图 4 的方法 400
520
应用强制执行在受保护介质软件狗上管理的关于受保护内容的使用条件
525
应用使用加密密钥在介质设备上对受保护内容解密
530
应用执行受保护内容
535

图5

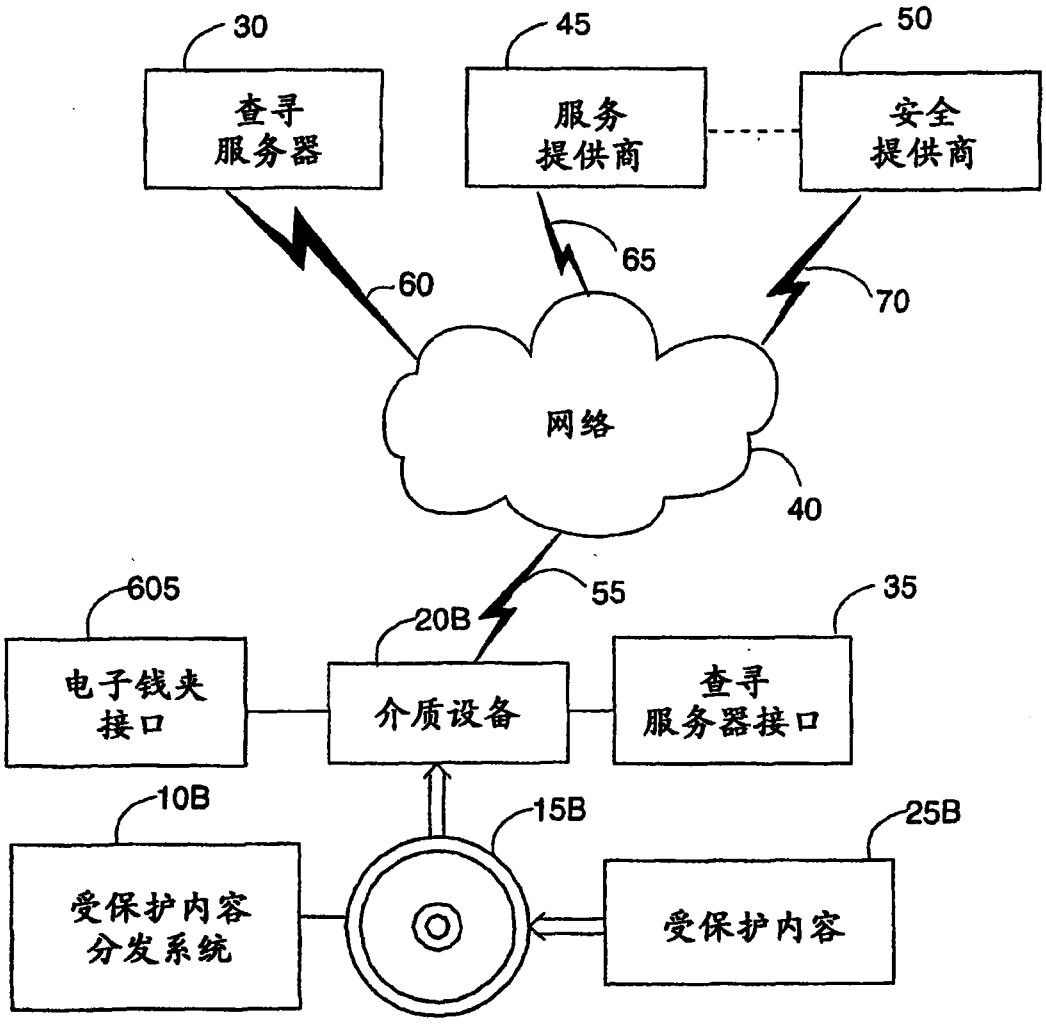

30
查寻
服务器
45
服务
提供商
50
安全
提供商
60
65
70
网络
40
605
电子钱夹
接口
20B
介质设备
55
35
查寻
服务器接口
10B
受保护内容
分发系统
15B
25B
受保护内容
受保护介质电子钱夹

图6

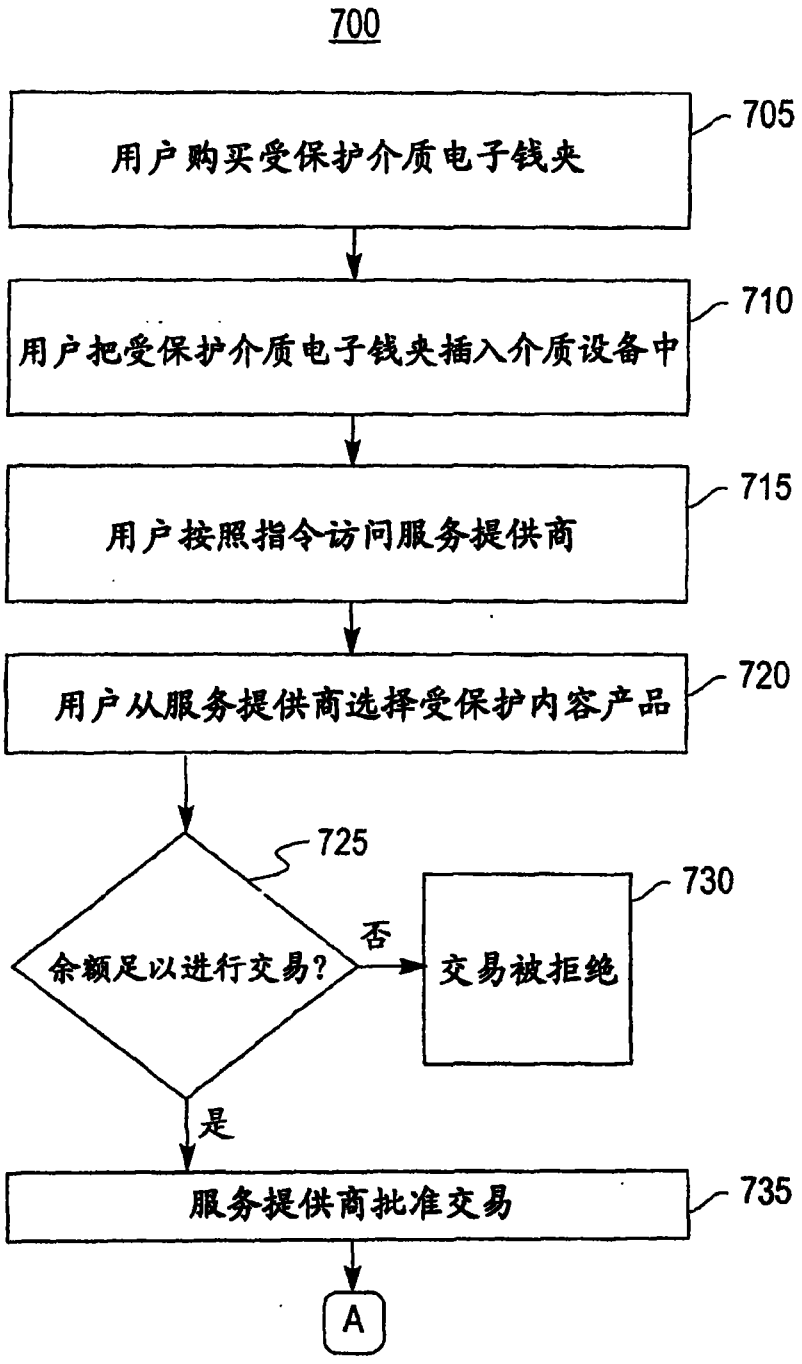

700
用户购买受保护介质电子钱夹
705
用户把受保护介质电子钱夹插入介质设备中
710
用户按照指令访问服务提供商
715
用户从服务提供商选择受保护内容产品
720
725
余额足以进行交易?
否
730
交易被拒绝
是
服务提供商批准交易
735
A

图7a

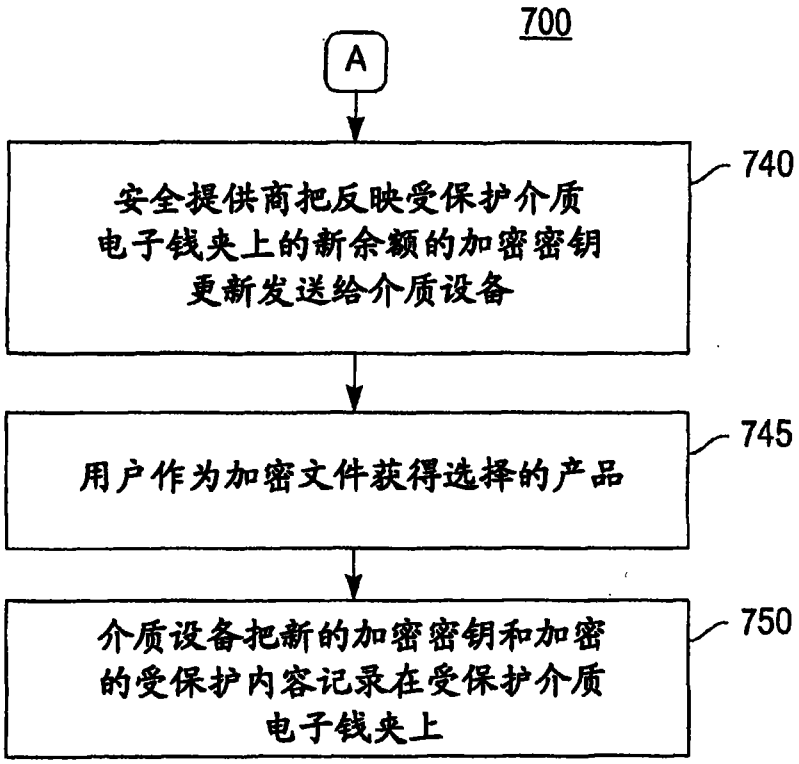
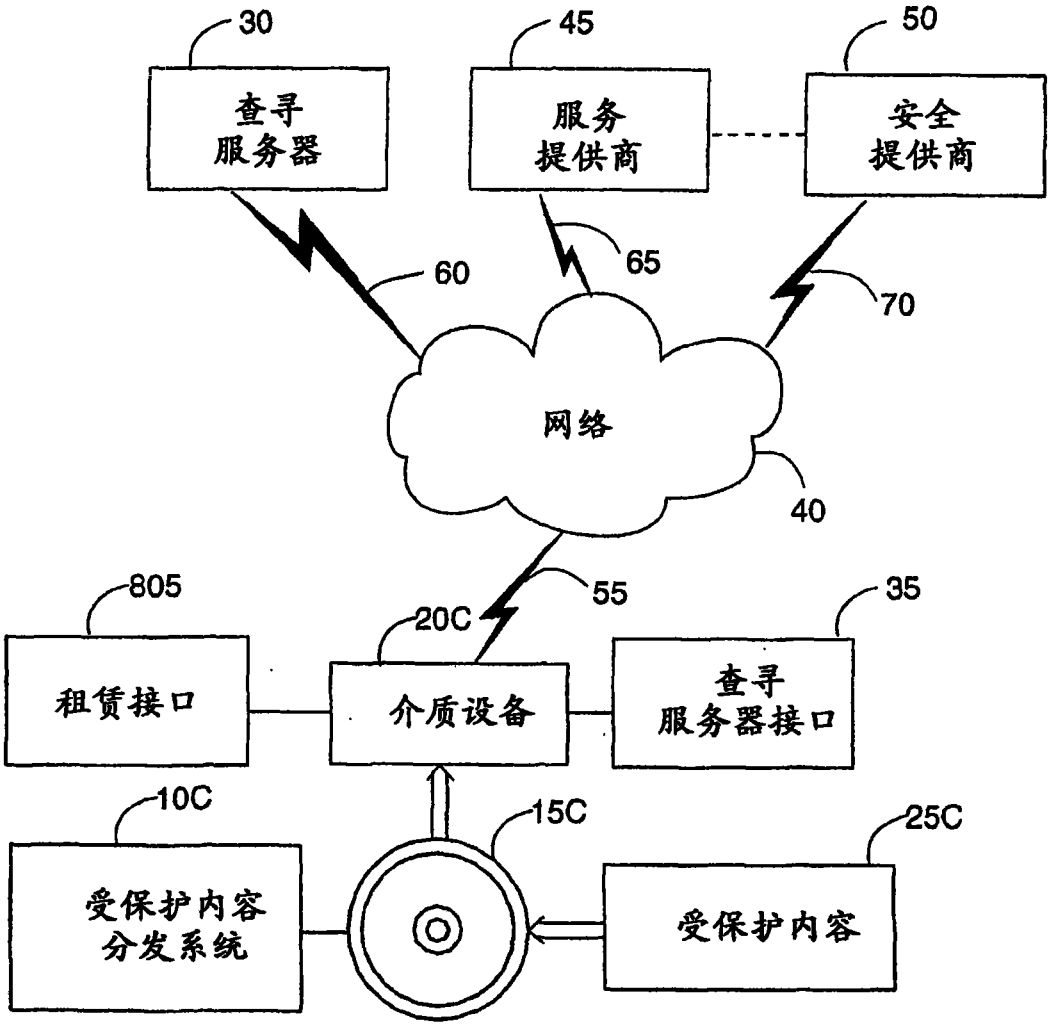

700
A
安全提供商把反映受保护介质电子钱夹上的新余额的加密密钥更新发送给介质设备
740
用户作为加密文件获得选择的产品
745
介质设备把新的加密密钥和加密的受保护内容记录在受保护介质电子钱夹上
750

图7b



受保护介质租赁容器

图8

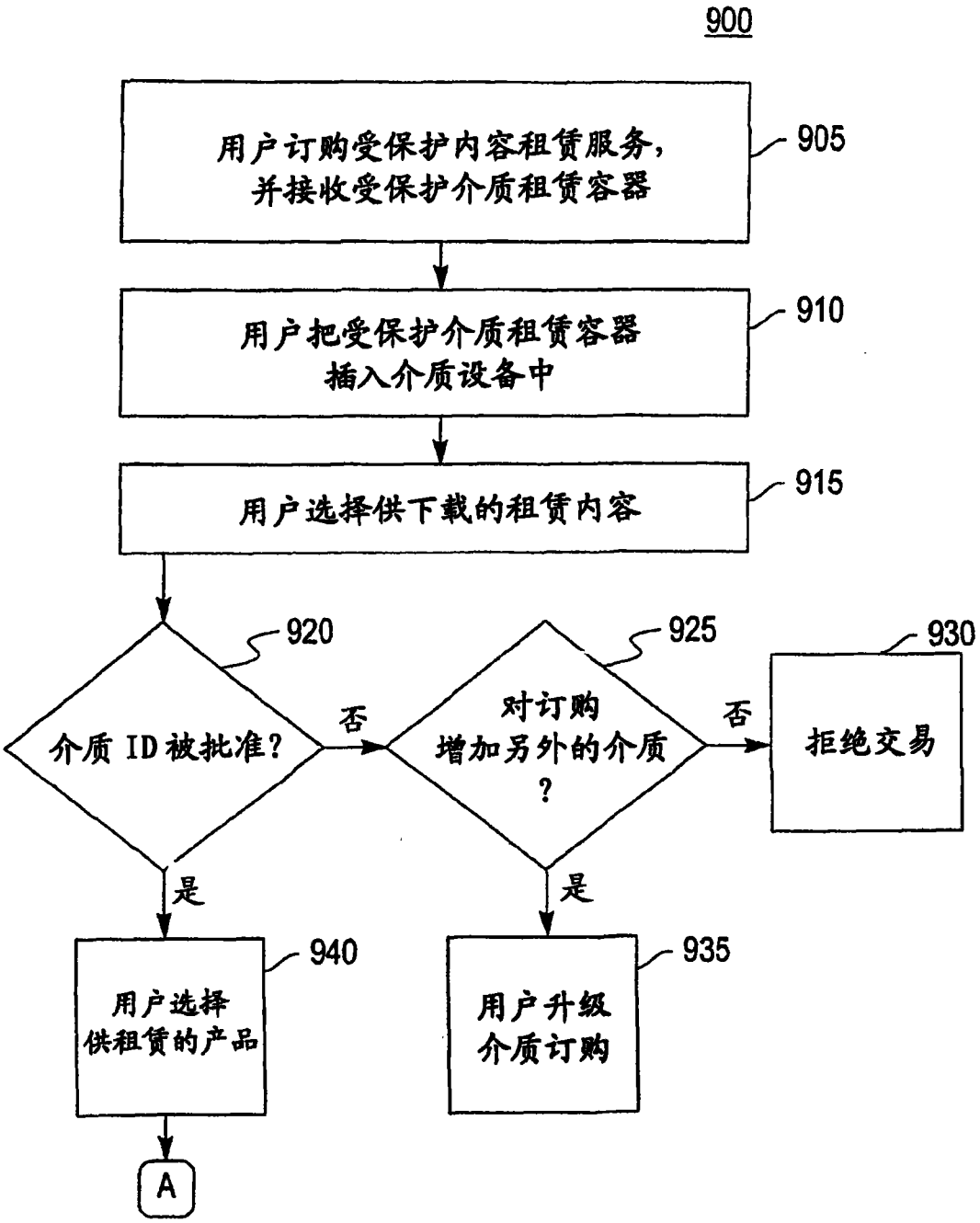

900
用户订购受保护内容租赁服务，并接收受保护介质租赁容器
905
用户把受保护介质租赁容器插入介质设备中
910
用户选择供下载的租赁内容
915
介质 ID 被批准？
920
否
对订购增加另外的介质？
925
否
拒绝交易
930
是
是
用户选择供租赁的产品
940
用户升级介质订购
935
A

图9a

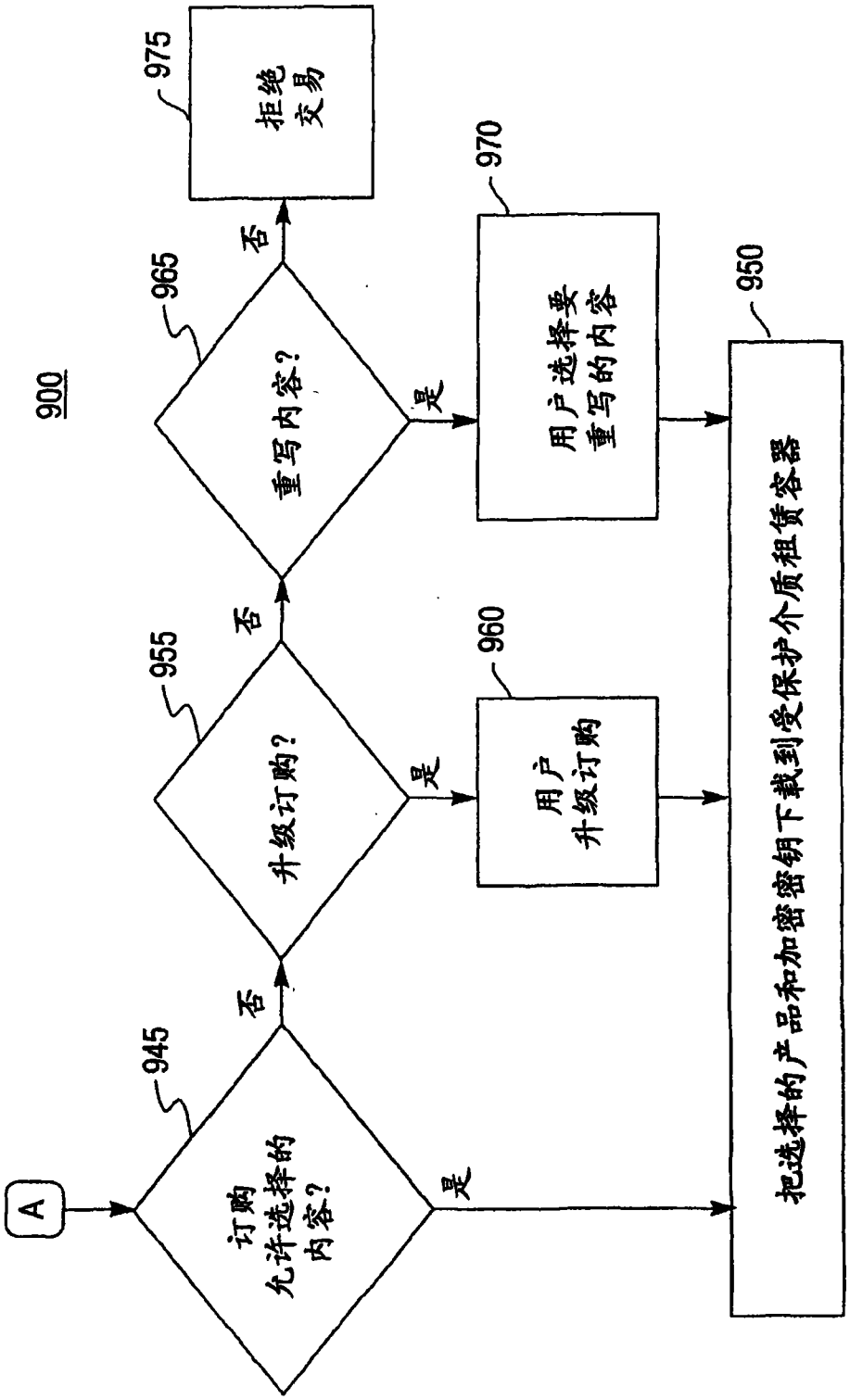

900
A
945
订购
允许选择的
内容?
否
是
955
升级订购?
否
是
960
用户
升级订购
965
重写内容?
否
是
970
用户选择要
重写的内容
975
拒绝
交易
950
把选择的产品和加密密钥下载到受保护介质租赁容器

图9b