[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)
G11B 20/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 02801621.1

[45] 授权公告日 2009 年 2 月 4 日

[11] 授权公告号 CN 100458640C

[22] 申请日 2002.1.28 [21] 申请号 02801621.1

[30] 优先权

[32] 2001.3.12 [33] EP [31] 01200898.3

[86] 国际申请 PCT/IB02/00245 2002.1.28

[87] 国际公布 WO2002/073378 英 2002.9.19

[85] 进入国家阶段日期 2003.1.13

[73] 专利权人 皇家菲利浦电子有限公司

地址 荷兰艾恩德霍芬

[72] 发明人 H·J·贝尔

G·C·P·洛克霍夫

M·R·布罗伊戈姆

D·V·R·恩格伦 P·范德佩尔

[56] 参考文献

WO0052558A1 2000.9.8

EP087896A2 1998.11.18

审查员 张 坦

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 杨 凯 王 勇

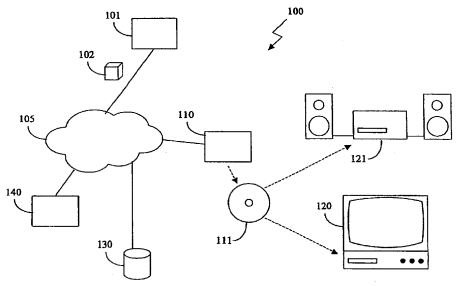
权利要求书 3 页 说明书 14 页 附图 4 页

[54] 发明名称

安全存储内容项目的接收设备和重放设备

[57] 摘要

一种用于把内容项目(102)安全存储在存储介质(111)上的接收设备(110)。 内容项目(102)以安全格式存储并具有关联的特许文件(141)。 利用与一组重放设备(120，121)相关联的公开密钥加密特许文件(141)，以便使所述组中的每台设备(121)都可解密所述特许文件(141)并播放内容项目(102)，而组外的设备则不能。 重放设备(121)可以向内容分发管理系统(CDMS)提供每台装置特有的公开密钥。 然后内容分发管理系统(CDMS)就返回用于由重放设备(121)的公开密钥加密的这一组的秘密密钥。 重放设备(121)于是安全地获得了所述组的秘密密钥，随后就能解密特许文件(141)。



1. 一种用于安全存储内容项目(102)的接收设备，包括:

下载装置(201)，用于下载内容项目(102)，

写入装置(203)，用于将所述下载的内容项目(102)写入存储介质(111)，

特许装置(204)，用于从特许服务器(140)获得特许文件(141)，所述特许文件(141)包含访问所述内容项目所需的多个许可以及解密密钥，和

特许锁定装置(205)，用于利用与一组重放设备相关联的加密密钥来加密所述特许文件(141)，对应的解密密钥可在是所述组的成员的重放设备中获得，并且用于将所述加密的特许文件(141)提供给所述写入装置(203)，以便将所述加密的特许文件(141)写入所述存储介质(111)。

2. 如权利要求 1 所述的接收设备，其中所述特许锁定装置(205)配置成: 利用称为特许锁定加密密钥的会话密钥来加密所述特许文件(141)，利用与所述重放设备组相关联的加密密钥来加密所述特许锁定加密密钥，并且另外将所述加密的特许锁定加密密钥提供给所述写入装置(203)，以便将所述加密的特许锁定加密密钥写入所述存储介质(111)。

3. 如权利要求 1 所述的接收设备，其中所述加密密钥是公开/秘密密钥对中的公开密钥。

4. 如权利要求 1 所述的接收设备，其中所述内容项目(102)包含声频和视频数据中的至少一种。

5. 如权利要求 1 所述的接收设备，其中所述特许锁定装置(205)还配置成: 用于接收所述组的标识符的选择，并且用于从密钥服务器(130)获得与所述选择相关联的加密密钥。

6. 如权利要求 1 所述的接收设备，还包括:

代码转换装置（202），用于将下载的内容项目（102）转换为适合用于存储在存储介质（111）上的格式。

7. 如权利要求 1 所述的接收设备，其中所述存储介质（111）是固态存储卡。

8. 一种用于播放存储在存储介质(111)上的内容项目(102)的重放设备，包括:

重放装置(305)，用于根据特许文件(141)中对所述内容项目(102)的许可来重放所述内容项目(102)，并利用包括在所述特许文件中的解密密钥对所述内容项目进行解密，所述特许文件(141)被加密存储在所述存储介质(111)上，

所述重放设备内用于存储一个或多个解密密钥的安全存储装置(309)，每一个存储在所述安全存储装置中的解密密钥与相应的重放设备组相关联，

解码装置(302)，用于检查存储在所述安全存储装置中的解密密钥是否适合用于解密所述加密的特许文件(141)，并且如果适合的话，则

利用存储在所述安全存储装置中的解密密钥来解密所述特许文件(141)，并将所述解密的特许文件(141)提供给所述重放装置(305)。

9. 如权利要求 8 所述的重放设备，其中所述特许文件(141)利用称为特许锁定加密密钥的会话密钥进行加密存储，所述特许锁定加密密钥利用用于特许锁定加密密钥的加密密钥进行加密存储在所述存储介质(111)上，存储在所述安全存储装置中的一个或多个解密密钥是用于特许锁定加密密钥的解密密钥，并且所述解码装置（302）配置成用于检查存储在所述安全存储装置中的解密密钥是否适合用于解密所述加密的特许锁定加密密钥，并且如果适合的话，则利用存储在所述安全存储装置中的用于特许锁定加密密钥的解密密钥从所述加密的特许锁定加密密钥中获得所述特许锁定加密密钥，并且利用所述特许锁定加密密钥来解密所述特许文件(141)。

10. 如权利要求 8 所述的重放设备，其中所述内容项目(102)包含声频和视频数据中的至少一种。

11. 如权利要求 8 所述的重放设备，其中存储在所述安全存储装置中的解密密钥是公开/秘密密钥对中的秘密密钥。

12. 如权利要求 8 所述的重放设备，还包括登记装置(306)，用于在称为内容分发管理系统(310)的远程服务器上登记与所述重放设备(121)相关联的公开/秘密密钥对中的公开密钥，所述公开/秘密密钥对中的秘密密钥被存储在所述安全存储装置(309)中，并且所述登记装置(306)还用于接收与一组重放设备相关联的利用所述公开密钥加密的解密密钥、解密利用所述公开密钥加密的解密密钥并将所述解密的解密密钥存储在所述安全存储装置(309)中。

13. 如权利要求 8 所述的重放设备，其中所述存储介质（111）是固态存储卡。

14. 如权利要求 8 所述的重放设备，其中所述安全存储装置(309)是可移动存储介质。

15. 如权利要求 8 所述的重放设备，还包括登记装置（306），用于在服务器（310）上登记与所述重放设备（121）有关的公开/秘密密钥对中的公开密钥，所述服务器（310）被配置为：利用登记的公开密钥对存储在所述安全存储装置中的解密密钥进行加密，该存储在所述安全存储装置中的解密密钥与所述重放设备（121）是其中一个成员的一个组有关；以及将利用登记的公开密钥加密的解密密钥发送给所述重放设备（121），所述重放设备（121）被配置为接收利用登记的公开密钥加密的解密密钥，对所述利用登记的公开密钥加密的解密密钥进行解密，以便将所述解密的解密密钥存储在所述安全存储装置(309)中。

安全存储内容项目的接收设备和重放设备

本发明涉及用于安全存储内容项目的接收设备，它包括：用于下载内容项目的下载装置；用于将下载的内容项目写入存储介质的写入装置；以及用于从特许服务器获得特许文件的特许装置，所述特许文件至少包括将下载的内容项目写入存储介质的许可。

本发明还涉及重放设备，用于播放在存储介质上存储的内容项目，所述重放设备包括用于根据在特许文件中对内容项目的许可重放存储在存储介质上的内容项目的重放装置。

文件共享服务，例如 Napster (http://www.napster.com)或 Gnutella (http://www.gnutella.co.uk/) 在互联网上已广为人知。成百万用户使用它们来交换内容项目，例如音乐，特别是以 MP3 为格式的音乐。每个用户可以提供他自己的收集的音乐给其他任何一个人，这就使每个人可有大量的音乐选择下载。但在这些共享服务中提供的音乐通常是流行音乐，而且提供时没有得到版权持有人的许可。为了保证版权持有人得到他们应得的版税，某些文件共享服务已开始向其用户收取预订费。来自预订费的部分收入可用来支付给版权持有人。

为了避免用户以未经授权的方式将他们下载的内容项目分发出去，需使这些项目以安全方式提供。例如，他们可以以加密格式分发，而接收设备上的软件可允许重放但不能以未加密方式存储。保证内容项目安全的一种技术是例如由美国专利 5892900 可知的 Intertrust “Digifile”技术。按照所述专利，音乐存储在安全的数字容器--Digifile 中。接收人必须从特许服务器获得特许。所述特许文件提供一组许可，例如许可重放音乐，或许可将内容项目存

储在存储介质上。用户当然需为每种许可支付一定数量的钱。特许文件也含有解密密钥或存取 Digifile 中的音乐所必需的其它信息。当重放设备得到了特许之后，它就可将音乐解密并向用户播放。用户可以把所述 Digifile 分发给其他人，但其他人不买他们自己的特许文件就不能将此音乐解密。保证内容项目安全的其它技术以类似方式工作。

许可可以和 Digifile 一起转发给另一台设备，这样另一台设备就可重放内容。但这通常需要这另一台设备连接到所述接收器上才可转发 Digifile 和许可。或者，可以将特许文件连接到用户，但其缺点是用户必须在每一台他想重放内容的设备上鉴别他自己。

已知的设备都有缺点，即它们不符合用户当前习惯的购买和听音乐的期望。如果用户在商店里购买了一张 CD 盘，他付了一次钱，就可在他拥有的任何设备上，甚至在别人的设备上播放这张 CD。他不希望每播放一次音乐就付一次钱，或者进行繁杂的操作把音乐以及关联的许可转发到其它设备上。而且，每次使用付费的方案要求重放设备连接到网络上，这样才可付费和提供特许文件。这样，就很难使用便携式设备。

本发明的一个目的就是提供一种根据前言的接收设备，它允许持续控制存储介质上内容项目的使用而且符合用户的使用期望。

此目的是根据本发明在一种接收设备中实现的，其特征是具有特许锁定装置，用于利用与一组重放设备相关联的加密密钥来加密特许文件，并且用于将所述加密特许文件提供给写入装置以便将所述加密特许文件写入存储介质。由所述存储装置在其上存储了内容项目的存储介质可以不受限制地复制，但这些内容项目仅可在加密密钥与之相关联的那组重放设备中按照特许文件播放。

根据本发明，提供了一种用于安全存储内容项目的接收设备，它包括：用于下载内容项目的下载装置，用于将所述下载的内容项

目写入存储介质的写入装置，以及从特许服务器获得特许文件的特许装置，所述特许文件包含访问所述内容项目所需的多个许可和一个解密密钥，以及特许锁定装置，用于利用与一组重放设备相关联的一个加密密钥来加密所述特许文件，对应的解密密钥能够从作为所述组的成员的重放设备中获得，并且用于将所述加密的特许文件提供给所述写入装置，以便将所述加密的特许文件写入所述存储介质。

用户只需定义一次他想播放内容项目的重放设备。例如他可在购买每一个重放设备之后直接就把它加入到一组中。然后他就可自由地使用接收设备所写入的存储介质。用户买了新的重放设备总可以扩大这个组，因为它们可以被随时加入，且内容项目是这样存储的、使得组内的任何装置都可以存取它，以下将做说明。

众所周知，对数据这样加密、使得某一特定设备才可读出它，例如用所述特定设备的公开密钥，最好是用会话密钥来加密数据。这意味着，特许文件可以用多个公开密钥多次加密，每一次对应于组中的一个重放设备。这样做的缺点是存储介质上的数据量多少会有增加，但更重要的是不能在组中加入新的设备并使它也能存取内容项目。在这种情况下特许文件加密的方式是只有在加密时已存在于组中的重放设备才能对它解密，因此接收设备不可能用新加入设备的公开密钥来获得加密用的特许文件。利用组密钥，就不需要在接收设备中有额外的步骤，也不需要对存储介质作任何更改。新加入的重放设备只需获得所述组的解密密钥，然后就能解密特许文件。

在一个实施例中，特许锁定装置做成用特许锁定加密密钥(LLEK)来加密特许文件，用与一组重放设备关联的加密密钥来加密 LLEK，并将加密的 LLEK 提供给写入装置以将所述加密的 LLEK 写入存储介质。能解密所述加密 LLEK 的重放设备也能解密特许文件。然后就可利用所述特许文件按照其中的许可重放内容项目。这就提供了附加的灵活性。

在另一实施例中，加密密钥是公开/秘密密钥对中的公开密钥。相应的秘密密钥在组内的重放设备中也可使用，这样可轻易地解密已加密的特许文件。这样做还有一个优点是现在加密密钥不需要作安全保护，因此接收设备不需要采取任何措施来保护所述密钥，如果加密密钥是个秘密(对称)密钥，恶意的用户可能会从接收设备中偷窃所述密钥，然后解密特许文件并在任何装置上播放内容项目。

在又一实施例中，内容项目包括至少一种声频或视频数据。诸如 Napster 等音乐共享服务的普及清楚说明了对于分发音乐和其它声频内容有着巨大的需求。一旦网络带宽足够大而允许大量分发视频数据时，视频的情况也会一样。有了根据本发明的能够便于存储介质的安全分发的接收设备，在人群中分发就成为可能。

在又一实施例中，还设置一种特许锁定装置，用于接收对所述组的标识符的选择并用于从密钥服务器获得与所述选择相关联的加密密钥。如果用户定义了多个组，那么，最好在把内容项目写入存储介质时他能选择使用哪一个。在密钥服务器上为所述组提供公开密钥，用户就可以安全存储另一用户能重放的内容项目。这样，例如，用户可以利用已登记给一个朋友的那一组的公开密钥下载一组歌曲并将其存储在存储介质上。然后把存储介质例如作为礼物送给朋友，朋友则可在他的那组中的任何装置上播放。这样用户可以只收录他知道他的朋友会喜欢的内容项目，成为一种非常个性化的礼物。

本发明还有一个目的就是提供一种根据前言的重放设备，它可持续控制存储介质上内容项目的使用而且符合用户的使用期望。

此目的是用根据本发明的一种重放设备来达到的，其特征是特许文件是加密存储在存储介质上的，并且重放设备还包括：安全存储装置，用于存储一个或多个解密密钥，每个解密密钥与一组重放设备相关联；解码装置，用来检查存储的解密密钥是否适合于解密已加密的特许文件，如果适合，就用存储的解密密钥解密特许文件

并将已解密的特许文件提供给重放装置。由于特许文件是加密存储的，只有能解密它的重放设备才可存取和使用所述内容项目。如果重放设备是在正确的组中，如在内容项目写入存储介质时用户所选择的，则在安全存储装置中提供正确的解密密钥。

根据本发明，提供了一种用于播放存储在存储介质上的内容项目的重放设备，它包括：重放装置，用于根据特许文件中对所述内容项目的许可，播放所述内容项目，并利用包括在所述特许文件中的一个解密密钥对所述内容项目进行解密，所述特许文件被加密存储在所述存储介质上，存储一个或多个解密密钥到重放设备中的安全存储装置，每一个解密密钥与相应的重放设备组相关联，解码装置，用于检查存储的解密密钥是否适合用于解密所述加密的特许文件，如果适合，则利用所述存储的解密密钥解密所述特许文件，并将所述解密的特许文件提供给所述重放装置。

在一个实施例中，特许文件用特许锁定加密密钥(LLEK)加密存储，所述 LLEK 是存储在用 LLEK 加密密钥加密的存储介质上的，所述一个或多个解密密钥是 LLEK 解密密钥，设置解码装置、用来检查存储的 LLEK 解密密钥是否适合于解密已加密的 LLEK，如果适合，就用存储的 LLEK 解密密钥从已加密的 LLEK 获得 LLEK，并利用 LLEK 解

密特许文件。利用 LLEK 作为会话密钥提供了更多的灵活性。

在另一实施例中，解密密钥是公开/秘密密钥对中的秘密密钥。利用公共密钥加密使加密密钥的分发容易得多，因为他们不需要保密。加密密钥可以不受限制地发送到接收设备，接收设备就用它来加密特许文件。只有具有相应的秘密解密密钥的重放设备才能解密所述特许文件并存取所述特许文件。

在另一实施例中，重放设备还包括登记装置，用于在内容分发管理系统(CDMS)上登记与所述重放设备关联的公开/秘密密钥对中的公开密钥，所述公开/秘密密钥对中的秘密密钥存储在安全存储装置中，所述登记装置还用于接收用所述公开密钥加密的解密密钥，解密所述加密的解密密钥并将解密密钥存储在安全存储装置中。通过以这种方式便于分发秘密密钥到重放设备组，就可做到使秘密密钥在任何时候都不会暴露给恶意的用户，而且任何重放设备不经登记就不能存取秘密密钥。

本发明还涉及一种计算机程序产品，用于使可编程的设备在执行所述计算机程序产品时起本发明的接收设备的作用。

本发明还涉及一种计算机程序产品，用于使可编程的设备在执行所述计算机程序产品时起本发明的重放设备的作用。

本发明的这些以及其他方面从结合附图所示的实施例的说明中便可一目了然，附图中：

图 1 示意地示出根据本发明的方案的第一实施例；

图 2 更详细地示出本发明的接收设备；

图 3 更详细地示出本发明的重放设备；以及

图 4 示意地示出根据本发明的方案的第二实施例。

在所有的图中，相同的标号表示类似或相应的特征。图中示出的某些特征是用软件实现的，它们代表软件实体，例如软件模块或

对象。

图 1 示出方案 100，它包括发射设备 101 和接收设备 110，它们通过网络 105 (例如互联网)相连接。连接到网络上的还有密钥服务器 130 和特许服务器 140，它们的工作在下面说明。方案 100 使接收设备 110 能从发射设备 101 下载内容项目，例如内容项目 102。在一个优选实施例中，发射设备 101 和接收设备 110 以对等关系方式连接，允许它们相互共享文件。在此实施例中，可以设置目录服务器(未示出)，使接收设备 110 无需直接接触发射设备 101 就可找出发射设备 101 上哪些文件可用。当发射设备是多个相互连接的发射设备之一且以对等关系方式连接到接收设备 110 时，这就特别有用。在这种情况下，还可以把接收设备 110 设置成对本方案中其他设备而言以对等方式起发射设备的作用。在另一实施例中，发射设备 101 是一个文件服务器，接收设备 110 可以从它那里下载内容项目。

内容项目这个词是指人们想要下载的任何种类的材料。它特别是指诸如电视节目，电影，音乐，文章或书籍等项目。可以在发射设备上以安全方式使用内容项目 102。在一个优选实施例中，由美国专利 5892900 可知，可以以 Intertrust “Digifile” 的格式使用内容项目 102。其它保证内容项目安全的技术，例如 CD-2 格式，也可以使用。安全格式的内容项目 102 也可任选地伴有代表内容项目的非安全格式的引题(teaser)。这样用户观看引题就可先不必购买就能查明他们是否喜欢所述内容项目。

接收设备 110 能够下载以这种安全格式可用的内容项目 102，像如下说明的那样。接收设备 110 可以是例如机顶盒，个人计算机，连接到本地网络的网关，或消费类电子(CE)装置。有了适当的许可，它就可重放内容项目 102，也可能借助于单独的重放设备(未示出)。例如，接收设备 110 可以是一台机顶盒，它下载内容项目 102 并将它发送到个人娱乐系统，由个人娱乐系统为用户播放。

用户可以从特许服务器 140 购买使用内容项目 102 的特许文件。

特许文件提供一组许可，例如许可重放音乐，许可把内容项目存储在存储介质上等。用户当然需为获得每种许可支付一定数量的钱。钱的提供可以采用以下方法：要用户提供信用卡信息，或识别用户并在用户的帐户上收取费用，或通过网络上处理付款的其他已知途径。特许文件还包括解密密钥或存取内容项目 102 所需的其它信息。

用户购买了存储内容项目 102 的许可后，接收设备 110 就可将内容项目 102 写入存储介质 111 上，最好是可录制的 CD，当然其他存储介质，例如可录制的 DVD，硬盘或固态存储卡等也可以。内容项目 102 以安全方式(例如以它被下载的同样的安全格式)写入存储介质 111。但最好是用一种不同的技术安全分发内容，例如要从存储介质 111 读出内容项目 102 的装置不能处理内容项目 102 被下载时的安全格式。

用户可对适当的重放设备，例如声频重放设备 120 或声频重放设备 121，提供存储介质 111，最好是可更换的存储介质。然后这些重放设备就从存储介质 111 读出内容项目 102 并播放给用户。为此，它需要在内容项目 102 的特许文件中提供的重放许可。它们如何得到所述许可下面将结合图 3 加以说明。

图 2 详细示出了接收设备 110。内容项目 102 由下载模块 201 下载，如上述。下载模块 201 可以是，例如，众所周知的 Napster 文件共享客户端的下载组件。代码转换模块 202 处理下载的内容项目 102，将它转换成适合于在存储介质 111 上存储的格式。这可能涉及到解密内容项目 102 和用不同的加密技术来加密它。但是，如果原来的安全格式可以接受，就不需要代码转换模块 202。然后写入模块 203 将内容项目 102 写入存储介质 111。

特许模块 204 从特许服务器 140 获得特许文件 141。所述特许文件 141 必须至少包含将内容项目 102 写入存储介质 111 的许可。如果存储许可并不含有存储的内容项目 102 的重放许可，则特许文件 141 必须也包含重放许可。特许模块 204 是特许服务器 140 和用户之间

的接口，可以用已知的特许模块实现，例如在 Intertrust 装置中提供的特许模块。特许模块为用户提供接口，用户可以利用它来为内容项目 102 挑选特许条件，例如，付少量钱的一次重放许可，免费一次重放，以填写问题单作为回报，或付较多的钱重放一个月等。

特许模块 204，如果已获得适当许可，将特许文件 141 提供给特许锁定模块 205，它产生特许文件 141 的加密版本，以下称为特许锁定件。特许文件 141 最好用会话密钥加密，以下称为特许锁定加密密钥(LLEK)。LLEK 可以用产生会话密钥的已知技术产生，例如散列伪随机数发生器的输出以获得所需长度的序列，例如在加密特许文件 141 时使用 128 比特加密算法时获得像 MD5 那样的 128 比特的散列函数。

特许锁定模块 205 将特许锁定件提供给写入模块 203，写入模块 203 把特许锁定件同内容项目 102 一起写入存储介质 111。在某些存储介质中，例如可录制 CD，需要一次性把全部数据写入存储介质。使用这种存储介质时，写入模块 203 可能需要缓冲被写入的数据直到获得全部数据，对于例如可更换硬盘来说，当然不需要这样做。

LLEK 然后也写入存储介质 111，但是以加密的形式写入。能从存储介质 111 读出 LLEK 并解密它的重放设备可以从特许锁定件解密特许文件 141，然后就能重放内容项目 102。以这种方式提供内容项目 102 和特许文件 141，本发明就可做到让用户在不需连接到网络 105 的情况下就可以在的重放设备上重放存储的内容项目 102。

或者，利用会话密钥，也可直接用加密密钥来加密特许文件 141，加密密钥对应的解密密钥可以用于以后将访问存储介质 111 的重放设备。加密可以是对称的，或是不对称的。

最好内容项目 102 的重放限于一定数量的重放设备，因为这样可使版权持有人控制内容项目 102 的使用。但对于能重放内容的装置的管理应与内容项目 102 在存储介质 111 本身的存储分离开，以使方案 100 符合用户的期望。通常内容的买主不但自己播放，而且

他的家庭成员也会在他家庭的各种设备上播放。朋友和邻居也想听一听内容项目 102。一般来说，应对一组人群，或对所述组人群拥有的一组装置许可重放内容项目 102。为了区别装置组，每一组分配一个组 ID。内容项目 102 与组 ID 链接，这样组内的装置就可从存储介质 111 重放内容项目 102。为此目的，特许文件应加密成组内的装置都可解密它，而组外的装置就不行。

在一个优选实施例中，LLEK 用与所述组关联的公开/秘密密钥对中的公开密钥加密，从而所述组内的所有装置都能存取相应的秘密密钥。或者也可使用秘密密钥加密方案。特许锁定模块 205 提醒用户从例如连接到接收设备 110 的显示器上显示的列表中选择一个组 ID，并且，例如从密钥服务器 130 中检索以获得所述组的公开密钥。然后用所述组的公开密钥加密 LLEK 并将加密的 LLEK 提供给写入模块 203，用于在存储介质 111 上写入。然后将存储介质提供给重放设备，例如视频重放设备 120 或声频重放设备 121。

接收设备 110 可以用能使处理器执行上述步骤的计算机软件产品 200 来实现。计算机软件产品 200 能使可编程装置在执行所述计算机程序产品时起接收设备 110 的作用。由于接收设备 110 不需存取任何秘密密钥，在使用公开密钥加密方案时，就可以计算机软件产品 200 的形式完全实现所述接收设备，计算机软件产品 200 可以，例如作为文件共享程序(如 Napster)的补充，被下载并在个人计算机上运行。这就扩展了 Napster 客户端，用户用它可以下载并分发音乐文件，而不失去版权持有人需要的控制。

图 3 详细示出了声频重放设备 121。其他重放设备，例如视频重放设备 120，也可以类似方式实现。用户可向重放设备 121 提供存储介质 111，例如将它插入接收单元 301。解码模块 302 从存储介质 111 中读出加密的特许文件 141 并用存储在安全存储模块 309 中的秘密密钥将其解密。在一优选事实施例中，解码模块 302 从存储介质 111 中读出加密的 LLEK 并用存储的秘密密钥解密这个加密的 LLEK。解码

模块 302 然后利用这样得到的 LLEK 解密特许锁定件而得到特许文件 141。

也可能发生这种情况，即解密步骤需要的秘密密钥并未存储在安全存储模块 309 中。此时，解码模块 302 就不能解密特许文件 141。另外，重放设备 121 也可能被包括在不止一个组中。此时，在其安全存储模块中就会存储有多个解密密钥，每一个对应于它所在的一个组。所以，解码模块 302 首先要检查正确的秘密密钥是否存储在安全存储模块 309 中，并且根据检查的结果解密特许文件 141 或通知用户由于没有解密密钥故不可能获得特许文件 141。

这项检查可以用多种方式进行，例如将存储的秘密密钥的密钥识别符与加密特许文件 141 一起存储的识别符加以比较。或者，特许文件 141 可以包括一条已知信息，例如版本号或固定的正文串。此时，解码模块 302 可试着解密特许文件 141，然后将输出与预期的已知信息进行比较。如果在输出中没有预期的已知信息，则所用的解密密钥不正确。或者，秘密密钥可包括它们所属的那一组的识别符，且存储介质 111 可包括特许文件 141 已加密的那一组的识别符。然后解码模块 302 检索后一种识别符，并在安全存储模块 309 中搜索含有匹配识别符的秘密密钥。解码模块 302 也可用每一个解密密钥试着解密特许文件 141，直到找到一个可以用来获得有效的特许文件的解密密钥为止。

解密步骤可以用多种途径实现，部分取决于秘密密钥是如何存储在安全存储模块 309 中的。所述模块 309 可以用具有嵌入式解密软件的硬件模块来实现，这样解码模块 302 可将加密的特许文件 141 提供给模块 309，模块 309 用适当的解密密钥将其解密，再以未加密形式将特许文件 141 返回给解码模块 302。这样做就十分安全，因为实际的秘密密钥现在存储在防止窜改的硬件中，恶意用户是无法读出的。或者，安全存储模块 309 就是一个只读存储器(ROM)，解码模块 302 从中读出秘密解密密钥并自己解密特许文件 141。模块 309 可

以设置在智能卡上。

解码模块 302 把特许文件 141 提供给重放模块 305。重放模块 305 从存储介质 111 读出存储的内容项目 102 并验证在特许文件 141 中确有重放许可。确认后，它就播放内容项目 102，例如在扬声器 306 产生声频信号。

安装在重放设备 121 的安全存储模块 309 中的秘密密钥可以是与接收器 111 所用的公开密钥相对应的所述组的秘密密钥，如以上结合图 2 所述。这就要求所述组的秘密密钥必须分发到所述组中所加入的每一台装置，这既不实际可行，又肯定不安全，除非使用诸如智能卡等高度防窜改的硬件。但这需要用户获得许多张智能卡，每一张用于所述组的每一台装置，这就非常麻烦。

所以最好每台重放设备具有与自己关联的公开/秘密密钥对，这样秘密密钥就可安全地安装在重放设备内。这可以例如在制造重放设备的工厂中完成。为更加安全起见，装置的公开/秘密密钥对可以由一个独立的实体产生，例如一个证明机构 (Certifying Authority) (CA)，并提供给工厂由制造商安装。

重放设备 121 具有登记模块 306，它可以向内容分发管理系统 310(CDMS)提供用于登记的公开密钥，以及所述重放设备的唯一识别符。所述唯一识别符可以包括例如制造商编号，型号以及系列号等。登记可以在用户要求时，或重放设备 121 第一次接通时或其他适宜的时刻进行。或者，公开密钥可以在制造商安装密钥对时由 CA 登记。

从以下结合图 4 的说明可见，CDMS310 利用所述装置的登记公开密钥加密所述组的秘密密钥，一次加密所述组的一台装置。这些加密的秘密密钥再发回重放设备的登记模块，于是登记模块就可利用它们各自的秘密密钥来解密。然后它们将秘密密钥存储在其安全存储模块中。以后，它们就可利用所述组相应的秘密密钥来解密用所述组的公开密钥加密的特许文件 141。用这种方式方便地分发所述组的秘密密钥后，秘密密钥任何时候都不会暴露给恶意用户，而且未

经登记的任何装置都不能得到秘密密钥。这样，当用户想得到将内容项目 102 分发给一大组装置的许可时，就可以例如向用户收取较高的费用。而且，所述组中的装置数量可以按照版权持有人的愿望加以限制。

重放设备 120 可以用能使处理器执行上述步骤的计算机程序产品 300 来实现。计算机程序产品 300 使可编程的装置在执行所述计算机程序产品时起重放设备 120 的作用。必须小心确保秘密密钥不被另外的装置复制，因为这会允许其它装置假冒重放设备 120，从而破坏了对每一台播放存储的内容项目 102 的装置收费的可能性。

图 4 示出了方案 100 的另一实施例，说明了登记各组和装置的过程。CDMS310 保存组 G1，G2，G3 以及每组中的装置 D1...D9 的列表 402。用户可要求在 CDMS310 上建立新组。CDMS 310 为所述组产生公开/秘密密钥对。然后可以在密钥服务器 130 上设置所述组的公开密钥，供接收设备 110 下载。通过在密钥服务器 130 上设置所述组的公开密钥，用户就有可能安全存储另一用户能够重放的内容项目。这样，例如用户可利用朋友登记的公开密钥把一组歌曲下载并存储到存储介质 111 上。然后他把所述存储介质 111 例如作为礼物送给朋友，朋友就可在他的组中的每一台装置上播放。用户仅把他知道他的朋友会喜欢的内容项目包括在内，并用他的朋友的组来存储，他就创造了一个非常个性化的礼物。

一旦用户登记了一个组，他就可向所述组加入重放设备。如果他想加的装置尚未登记，用户必须例如启动所述装置的登记模块 306 先将它登记，使它加入到设备列表 403 中。设备加入到一个组里以后，CDMS 310 就用所述设备的公开密钥加密其秘密密钥。例如，用户把设备 D6 加入组 G1，CDMS310 就用公开密钥 PK6 加密 G1 的秘密密钥。所述加密的秘密密钥是设备 D6 的解码模块 302 所需要的。一旦用户想加入的装置已在 CDMS 310 登记，用户就可简单地从 CDMS310 提供的，包括设备识别符 UID1，.....UID9 并与公开密钥 PK1，...PK9

相关联的设备列表 403 中选择所述设备并将其加入到组中。

用户也可以从所述组的列表中去掉一些设备，例如在各组的设备数量受 CDMS 310 限制时让出地方给新设备。这样一来，有可能用户从所述组的列表中取消一个设备，但仍能在所述设备上播放所述组的内容项目。之所以可能这样是因为所述装置仍具有用以解密 LLEK 的所述组的秘密密钥，所以特许文件 141 可以被解密，内容项目 102 仍可以播放。要避免这种情况可以例如定期更换所述组的公开/秘密密钥对且仅对当时在所述组列表上的设备提供新的秘密密钥。另外，对每台加入一组或从一组中取消的设备收取登记费也可减少用户频繁操作他那一组列表的兴趣。

为了确保由密钥服务器 130 提供的公开密钥是确有授权的，可以由认证机构 CA 认证之后才使它们可以在密钥服务器 130 上使用。接收设备 110 可配以 CA 的证书，使它能验证证书的确实性，从而验证所述组公开密钥的确实性。CA 的证书或公开密钥可以由制造商加载到接收设备 110 中，或在需要时从密钥服务器 130 下载。但由制造商把 CA 证书加载到接收设备 110 更为安全，因为这样一来恶意用户更换证书的机会就比较少。

以这种方式将内容项目 102 存储在存储介质 111 上的另一优点是不处在适当组内的重放设备如果获得了新的特许文件也可以存取内容项目 102。终究内容项目 102 是以一种安全格式存储的，只要有适宜的特许文件就可以存取。所以，建立了具有其喜爱的音乐纹迹的存储介质 111 的用户把所述存储介质 111 借给一个朋友，但朋友的设备不属于用户的组。那么朋友可以购买一次播放特许并访问存储介质 111 上的纹迹就可知道用户的爱好。如果他也喜欢，他可以要求用户把他也加入到他的组中，或自己来下载这些音乐纹迹。用户也可以建立一个包括他和他的朋友拥有的设备的新组，然后建立一个含有他们两人都喜爱的纹迹的新存储介质。

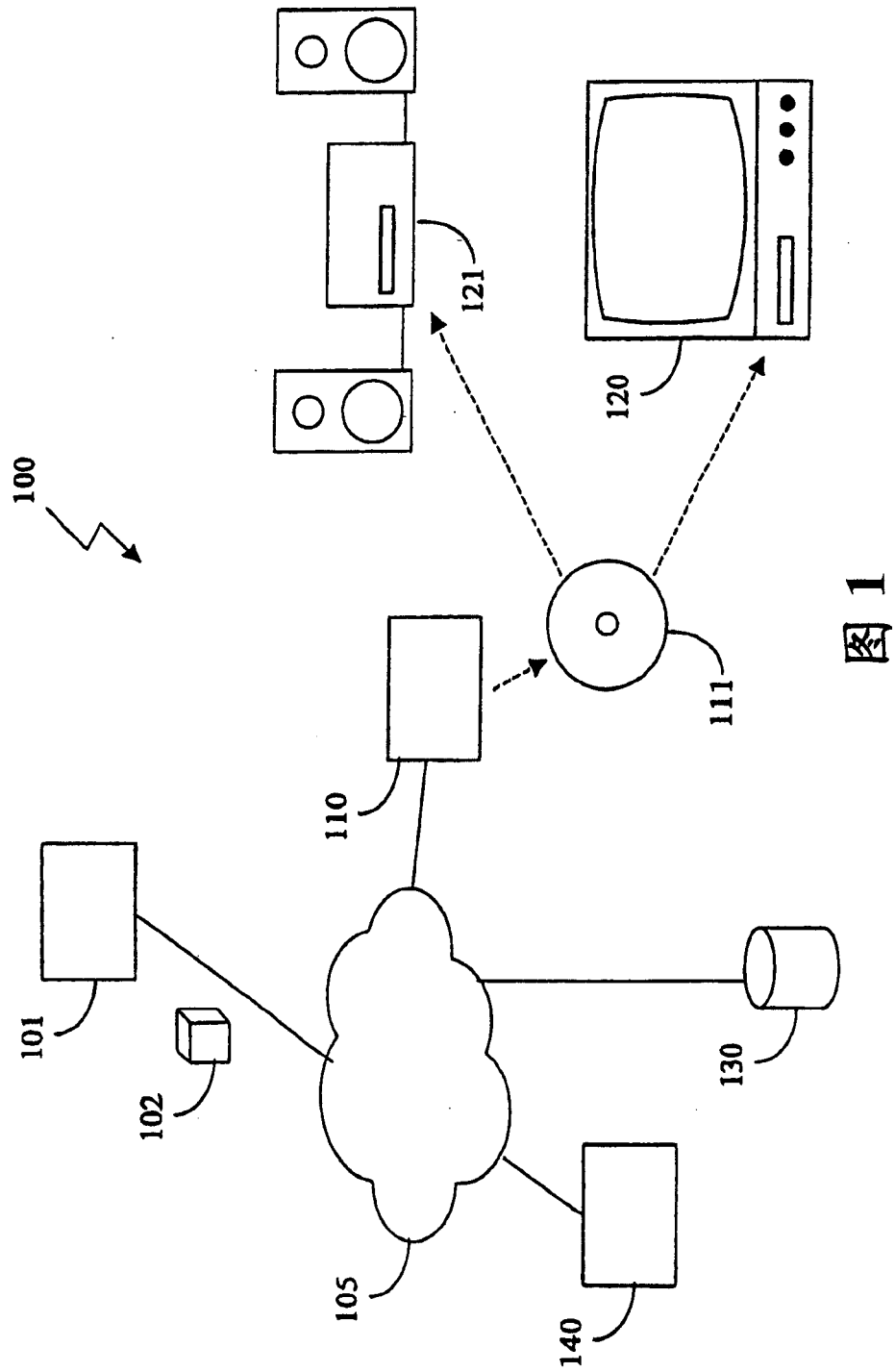


图 1

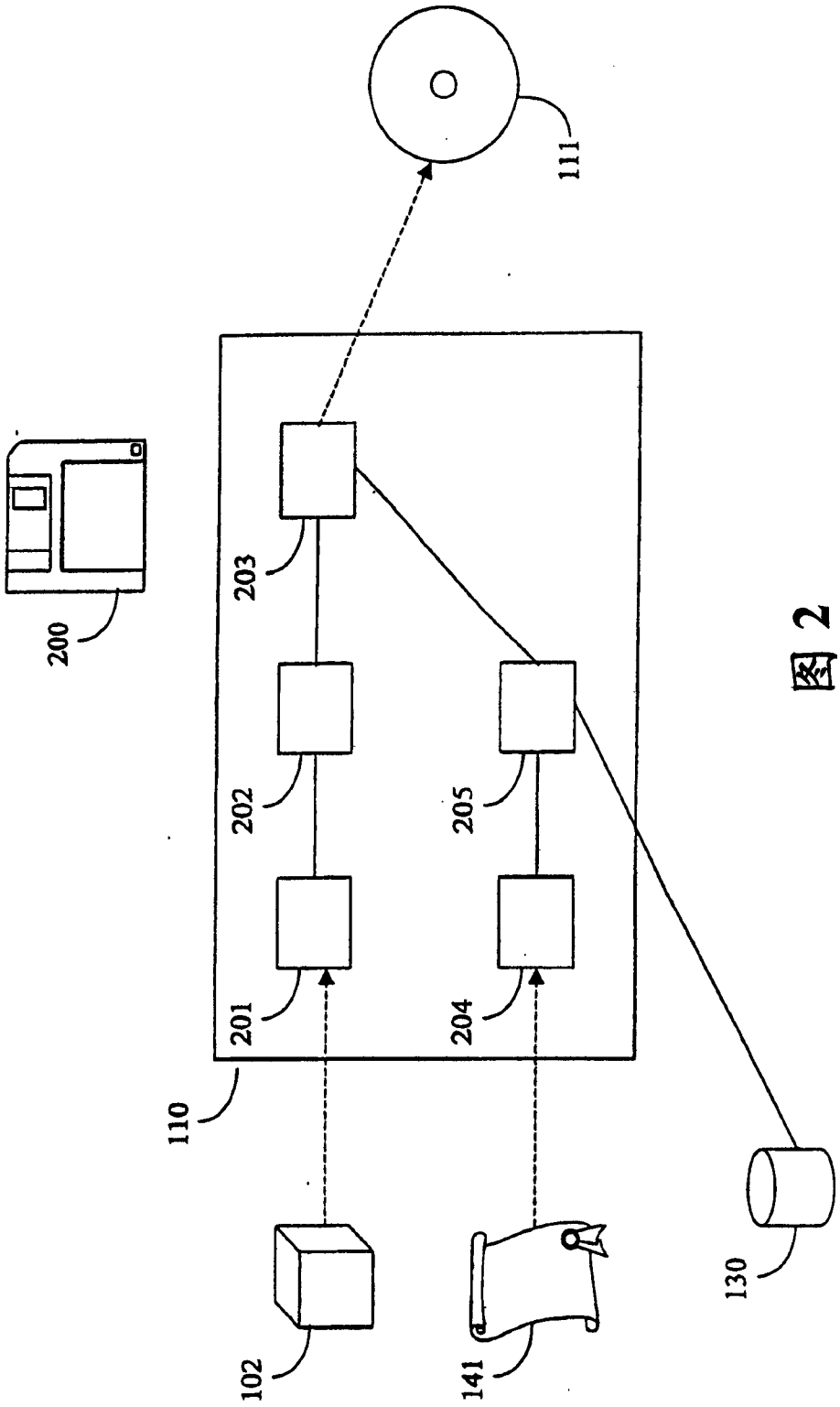


图 2

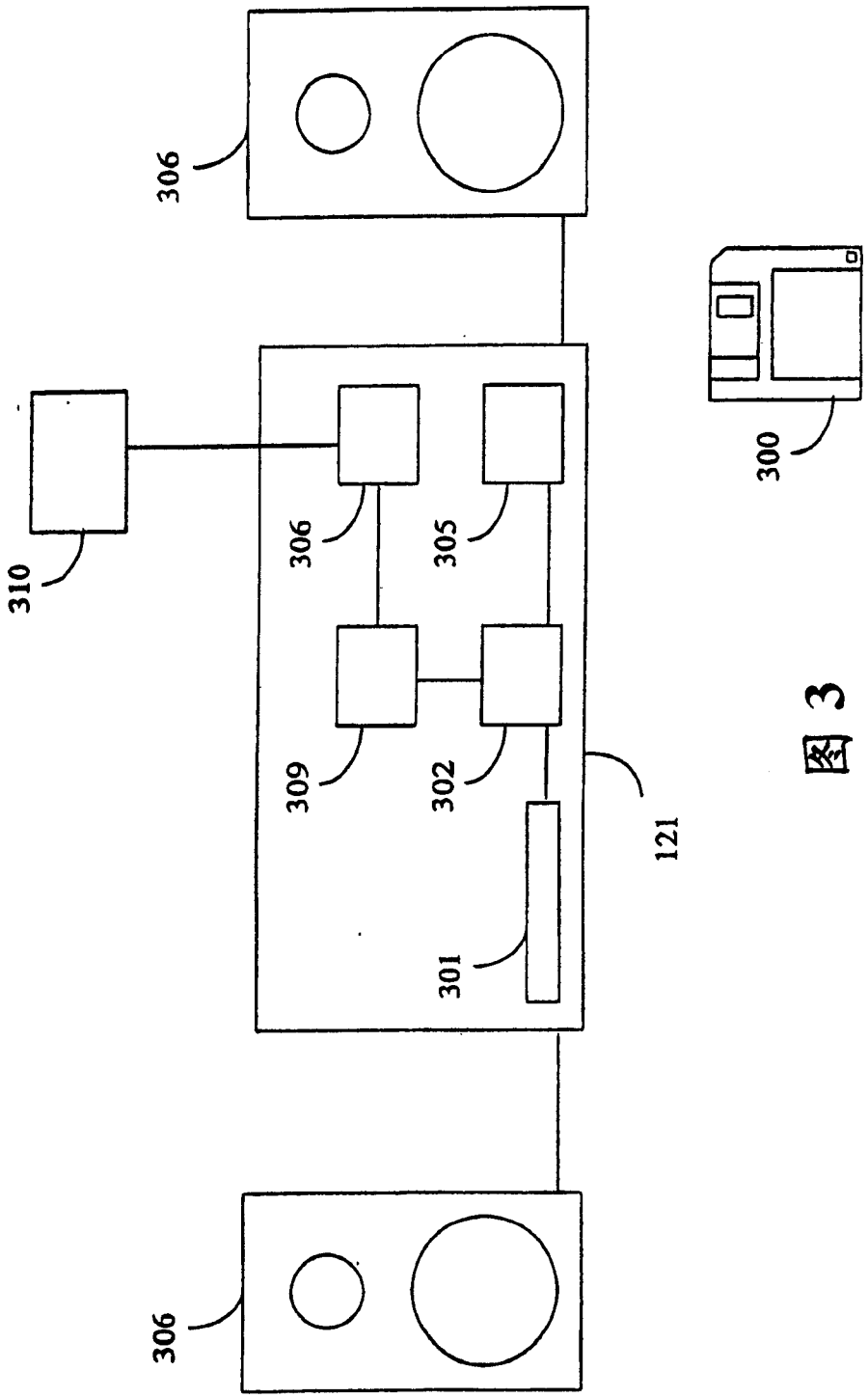


图 3

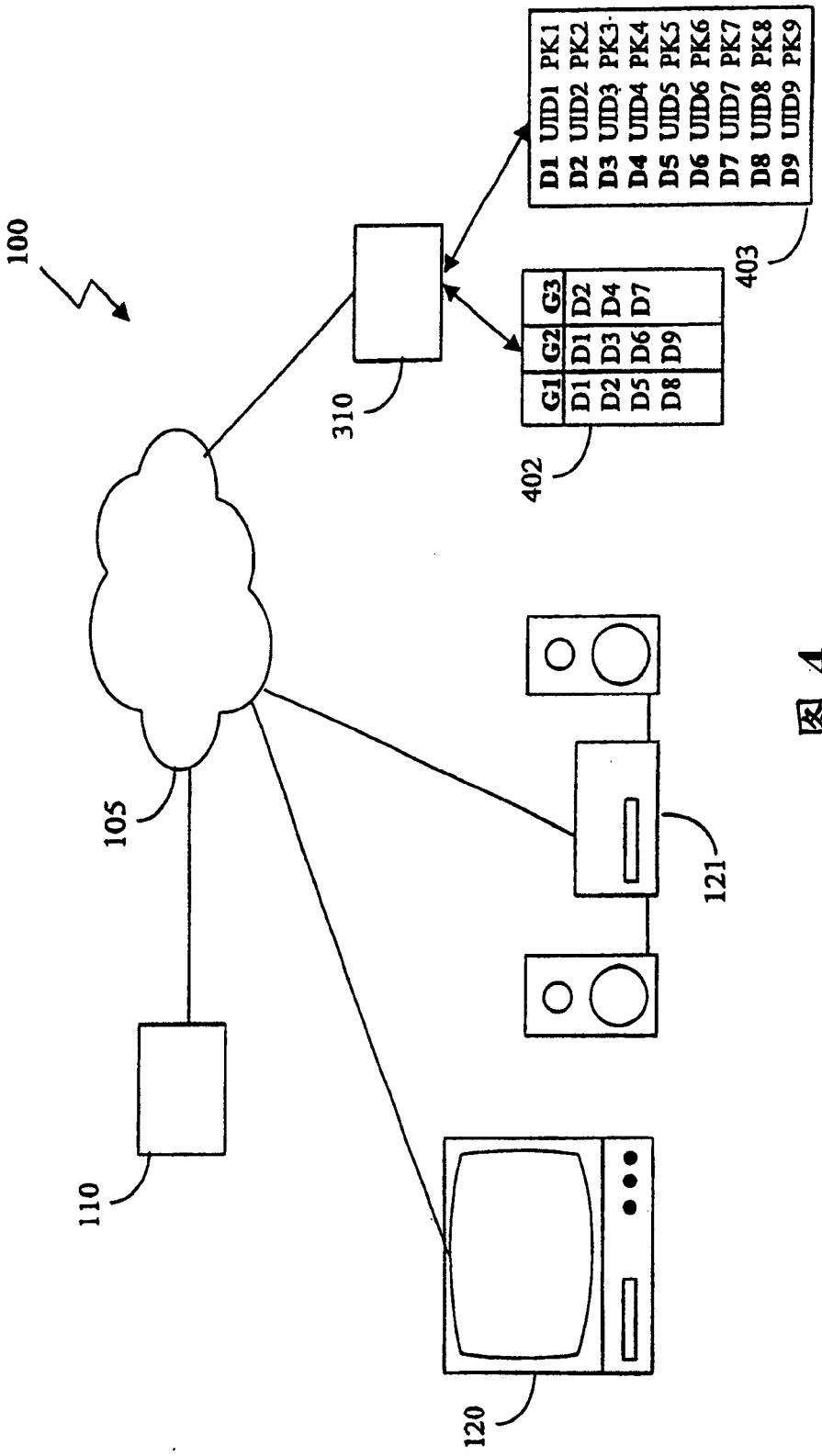

100
310
105
110
120
121
402
403
D1 UID1 PK1
D2 UID2 PK2
D3 UID3 PK3
D4 UID4 PK4
D5 UID5 PK5
D6 UID6 PK6
D7 UID7 PK7
D8 UID8 PK8
D9 UID9 PK9
G1 G2 G3
D1 D1 D2
D2 D3 D4
D5 D6 D7
D8 D9

图 4