[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

专利号 ZL 200380108103.X

[45] 授权公告日 2007 年 12 月 5 日

[11] 授权公告号 CN 100353273C

[22] 申请日 2003.11.21
[21] 申请号 200380108103.X
[30] 优先权
[32] 2002.12.30 [33] EP [31] 02080568.5
[86] 国际申请 PCT/IB2003/005725 2003.11.21
[87] 国际公布 WO2004/059451 英 2004.7.15
[85] 进入国家阶段日期 2005.6.30
[73] 专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 F·L·A·J·坎佩曼
G·J·施里詹
S·A·F·A·范登霍伊维尔
[56] 参考文献
CN 1322312A 2001.11.14
WO 0163387A2 2001.8.30
EP 0930556A2 1999.7.21
审查员 石 岗
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 王 勇

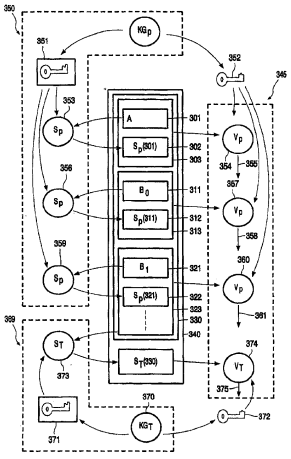
权利要求书 3 页 说明书 12 页 附图 8 页

[54] 发明名称

在授权域内划分的权利

[57] 摘要

为了确保数字权利不能被伪造或篡改，可以数字地对所述数字权利加以签名。 然而，这意味着不可能再更新所述数字权利，因为这会使所述数字签名无效。 本发明提出数字权利的发行者发布在基本块中而不是从总体上来签名的权利。 取代发布用于播放内容块的权利三次，供应者例如在特定的 AD 中一次发布用于播放所述内容的三个权利，可以把其中的两个转送到其它域。 用签名来各自地保护所述数字权利，因而不再可能伪造数字权利。 作为增强，照此表明可以被转送的权利并且将其可靠地存储以防止篡改。 当转送所述权利时，所述权利必须由原始接收它的人来签名。



1. 一种在包括一组设备的系统中对访问内容项进行控制的方法，

所述方法包括把至少一个使用权利与所述内容项相关联的步骤，

其特征在于，

所述方法还包括把所述使用权利分解为一组部分权利，

并且随后独立地签名所述一组部分权利中的每一个，产生一组独立的已签名的部分权利。

2. 如权利要求 1 所述的方法，其中在所述系统中的至少一个设备在验证所述相对应的签名之后，能够访问并行使至少一个部分权利。

3. 如权利要求 1 所述的方法，其中与所述内容项相关联的一个部分权利包括再现权利、转送权利、要约权利、派生工作权利和实用权利之一。

4. 如权利要求 1 所述的方法，其中至少一个部分权利只可以被行使有限的次数。

5. 如权利要求 1 所述的方法，其中所述方法还包括如下的步骤，其中所述一组设备中的一个设备在行使所述部分权利之前验证所述部分权利及其发行者是否都没有被撤消。

6. 如权利要求 1 所述的方法，其中所述系统包括一组设备，用于构成一个域，所述域包括与家庭或有限的消费者组有关的设备。

7. 如权利要求 1 所述的方法，其中至少一个部分权利的最小要求保护级别被与所述部分权利一起指示。

8. 如权利要求 1 所述的方法，其中至少一个部分权利的最小要求保护级别隐含地从所述部分权利的类型导出。

9. 如权利要求 6 所述的方法，其中所述方法还包括允许在所述系统中的至少一个第一设备识别一个第二设备，

以便随后签名包括至少一个部分权利和下列项至少之一的组合的信息：

所述域的标识，

所述第二设备的标识，和

关于所述部分权利的长度和有效性的信息，

并且随后把该签名的组合转送到所述第二设备。

10. 如权利要求 6 所述的方法，其中所述方法还包括允许在所述系统中的至少一个第一设备识别一个第二设备，

以便随后签名至少一个部分权利；

并且随后把所签名的部分权利转送到所述 第二设备。

11. 如权利要求 9 所述的方法，其中所述第二设备参与表示不同的域。

12. 如权利要求 11 所述的方法，其中向所述第二设备的转送只被允许在所述第一设备和所述第二设备中的至少一个已经被其它设备验证为应允的和未撤消中的至少一个之后发生。

13. 如权利要求 11 所述的方法，其中由把所述权利转送到所述第二设备的设备来撤消或删除所述部分权利。

14. 如权利要求 6 所述的方法，

其中由内容供应商把所述使用权利与所述内容项相关联，

其中所述使用权利包括用于某一特定权利的要约权利，

所述方法还包括请求所述内容供应商执行所述要约权利并把所述特定的权利递送给指定的第三方，

接着所述内容供应商在验证可以应用的条件之后，把所述特定权利直接递送给所述指定的第三方。

15. 一种包括一组通过网络连接的设备的客户系统，所述客户系统包含对某一内容项进行控制的装置，以及用于与所述内容项相关联的使用权利的处理装置，其特征在于，所述使用权利是一组各自签名的部分权利，并且所述客户系统包含各自验证并各自处理所述部分权利的装置。

16. 一种被安排成对访问内容项执行控制的服务器系统，所述服务器系统还把至少一个使用权利与所述内容项相关联，其特征在于，所述服务器系统具有用于把所述使用权利分解为一组部分权利的装置，所述服务器系统还具有签名部件，所述签名部件被安排成随后独立地签名所述一组部分权利中的每一个，并且所述服务器系统被安排成把各自签名的部分权利捆为一组各自签名的部分权利。

17. 一种被安排成对访问内容项执行控制的设备，能够处理与

所述内容项相关联的使用权利，其特征在于，所述设备还被安排成处理所述使用权利，所述使用权利已经被分成部分权利，每个所述部分权利具有数字签名。

在授权域内划分的权利

本发明涉及一种用于在包括一组设备的系统中控制对内容项访问的方法，所述方法包括把至少一个使用权利与所述内容项相关联的步骤。

本发明还涉及一种包括一组设备的客户端系统，所述客户端系统被安排成执行对内容项的访问控制，并具有用于与所述内容项相关联的使用权利的处理设备。

本发明还涉及一种服务器系统，被安排成执行对内容项的访问控制，所述服务器系统还把至少一个使用权利与所述内容项相关联。

本发明还涉及一种用于携带使用权利的信号。

本发明还涉及一种设备，被安排成执行对内容项的访问控制，能够处理与所述内容项相关联的使用权利。

电视及其它内容越来越变得数字化。在通常能够彼此通信的设备之间还可以容易地转送数字内容。这向终端用户呈现了用户界面友好的系统，其中对内容的访问不再限于单个设备，所述内容可以被从连接到某种（家庭）网络的任何设备加以访问。

这还给内容所有者带来了威胁，即它的内容将被无限制地拷贝或转送。数字权利管理（Digital Right Management DRM）系统被设计成用于保护并管理对内容的访问。对于所述内容所有者（他们常常想要对内容的数字转送强制严格的规则以便防止无限制的数字拷贝）而言，对于向消费者家庭分发数字内容的认可接受来说，由 DRM 系统所提供的保护内容是重要的条件。

在几个论坛中，像 CPTWG（Copy Protection Technical Working Group(拷贝保护技术工作组),http://www.cptwg.org)、DVB(Digital VideoBroadcasting（数字视频广播），http://www.dvb.org）和 TV-Anytime（随时电视）（http://www.tv-anytime.org），继续论述当由消费者在与它们的家庭网络连接的设备上访问价值高的数字内容时，怎样确保所述高位值数字内容不可以被非法地重新分发。

在 DVB-CPT（Copy Protection Technical Module 拷贝保护技术模块）和 TV-Anytime RMP（Rights Management and Protection 权

利管理和保护）内的最近论述中，在标题*授权域*（AD）下解决上述问题。从消费者能够在所述 AD 内自由访问并分发所述内容这个意义上讲，AD 尊重了内容供应商和消费者这两个方面的利益，而同时通过引入严格的导入导出口规则来防止对内容进行穿过域的、不受限的数字拷贝，来保护所述内容所有者和服务提供者的权利。

DVB-CPT 组把 AD 定义为一组 DVB-CPCM（Copy Protection and Copy Management 拷贝保护和拷贝管理）适应的功能单元，其控制内容的流动和内容格式。所述 AD 表示对于授权使用版权内容信任的环境。所述 AD 可以由用户家庭网络的几个且可能拆接的部分组成。这包括移动设备的暂时连接和由便携式介质所进行的不同网络段（可能在不重叠的时间操作）的虚拟“连接”。

AD 向消费者提供了对于在所述 AD 内合法地获得的内容的不限制并且不复杂的访问。消费者将期望它们可以向所述域增加设备、权利和内容。消费者还将期望他们可以在任何地方、任何时候并且在他们的任何一个设备上访问他们的内容。另外，这还可以适用于移动设备，或适用于在房间外的终端，诸如在旅馆客房中的电视。另外，可以从一个域中增加并删除用户，例如因为他们在家庭之间改变。其它用户还期望可以访问所述内容，例如因为他们在访问期间是朋友，或者由于合理使用提供。

另一方面，内容供应商要求对内容交换-尤其是经由因特网重新分发所进行的内容交换给予有力的限制。因此，应该清楚地定义并保护内容的权利。例如，在电视系统域中，内容权利（在付费电视环境中也称为 ECM)描述了对所述内容而言什么是被允许的，并且使用权利(在付费电视环境中也称为 EMM）授权人们使用确定的内容权利，并且还可以描述允许用户怎么处理所述内容。

实例性的使用权利是用于播放内容的权利、用于制作一个生成拷贝的权利等。

内容权利和使用权利还可以都包含密码密钥。

对于在家庭网络中使用 DRM 的更广泛的介绍，参见 F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, M.H. Verberkt, Digital Right Management In Home Network（在家庭网络中的数字权利管理），Philips Research（菲利浦研究），荷兰 IBC 2001conference

publication vol.I,pages 70-77（会议出版卷 I，第 70 - 77 页）。

显然内容权利和使用权利表示一定量的价值，并且应该防止不希望有的复制或未经授权的创建。这可以使用安全和加密的通信以及安全存储这些权利来完成，这仅仅要由抗篡改的软件和／或硬件来处理。

内容权利并没有被个性化的，从而可以连同所述内容一起被转送或由不同的服务器来提供。

然而，使用权利却被个性化了。根据商业模型或保护模式，可以把使用权利依赖到设备、依赖到诸如 CD 的介质、依赖到 AD 或人。对于抗篡改处理的需求使例如在设备之间或当旅行时难于自由地使用或转送所述使用权利。

更好的解决方案是用数字签名来保护使用权利。由所述内容供应商或不同的授权源使用众所周知的公钥签名技术来签名所述使用权利。在这种解决办法中，所述内容供应商具有私有／公钥对。在把签名增加到所述公共权利的过程中要求私钥。由所述内容供应商完全秘密地保存所述私钥。可以使用相应的公钥来检查用于保护所述公共权利的完整性的所述签名的有效性。因为由数字签名来保护使用权利，所以可以在抗篡改的环境外允许所述使用权利。

为了防止对内容的非法访问，只在能够（使用设备的公钥来）检查所述设备来源于授权源的情况下，才应当由该（应允的）设备接受使用权利证书。另外，在接受证书之前还能够检查其它条件，诸如所述证书是否属于打算把所述权利送到的 AD，或者在基于人的 AD 情况下，是否存在相关联的人。

一些数字使用权利只可以使用有限的次数，例如用于播放内容块三次的权利，或者用于把所述内容转送到不同的域两次的权利。这要求所述使用权利本身包含某种计数或撤销机制，每当使用所述权利时触发该机制。然而，由于在所述使用权利中实现所述计数机制所导致的任何改变会使所述签名无效。所述签名只可以由信任的第三方来计算，这无疑是一个缺点。

另外，所述使用权利还可以包含用于把内容转送到不同的域或用户一次的权利。在已经使用这种转送权利之后，需要撤消这种转送权利。撤销或删除这种转送权利也会使其余使用权利的签名无效。

本发明的目的是提供一种方法，其允许可以在不使数字签名无效的情况下来处理使用权利。

借此由依照序文的方法来实现该目的，所述方法还包括把所述使用权利分解为一个部分权利组，并且随后分别独立地签名所述部分权利组中的每一个，产生对应的签名。

该方法有下列好处即，现在在基本块中而不是总体上来签名使用权利。例如，用于把所述内容转送到不同的域的权利，和用于在特定的 AD 中播放所述内容一次的权利都被各自地签名。当使用或转送部分权利时，其仍然被数字地签名，对于任何其余权利也是如此。

本说明书中 描述了依照本发明的方法的实施例：

在所述系统中的设备能够访问这种签名的部分权利，并且验证其有效性，而不要求对完整的使用权利的访问。随后，在成功确认之后可以行使所述权利。

一个依照本发明的方法的实施例为：

一些部分权利只可以行使有限的次数，允许控制可以访问所述内容项的次数。如果只可以行使权利一次，这有下列好处：该权利能够被分别独立地撤消、删除或被立即标记为已在使用。

另一个依照本发明的方法的实施例为：

所述设备可以在行使权利之前检查该权利的撤销，由此增强了防止使用过期的权利的健壮性。

这种检查允许可靠地撤销权利，在所述检查中可以参考在所述域内的抗篡改设备。

一个依照本发明的方法的实施例为：

设备的系统可以组成例如如下设备的如上所述的域，所述设备属于单个家庭的成员，或在所述设备或他们的所有者之间具有某种其它的关系。可以允许人们进入并离开域。例如可以用个人智能卡来识别用户。

一个依照本发明的方法的实施例为：

在所述域中的至少一个设备被允许将其签名增加到一个部分权利和至少包含其本身和／或不同的设备或域的标识、有效性信息（长度，类型）的信息的组合，并且被允许随后把该权利转送到不同的设备，所述设备可能是不同域的一部分或表示不同的域。

这有下列好处即，可以跟踪已转送权利的历史记录、重新分发渠道和原始的发行者。

类似地，可以允许设备局限于只签名所述部分权利 。

一个依照本发明的方法的实施例为:

可以要求用于转送所述权利的设备验证接收所述权利的设备的应允性。还可以同第三方检查所述接收设备是否还没被撤消。所述接收设备可以对始发设备执行类似的检查。

一个依照本发明的方法的实施例为:

把所述权利转送到不同设备的设备可以在本地撤消或删除所述部分权利。

一个依照本发明的方法的实施例为:

引入一种使用权利，称作要约（offer）权利，该要约权利表示来自内容供应商的要约。该要约权利可以包含许诺: 即，当请求使用权利时，把签名的使用权利从所述内容供应商直接转送到第三方，所述第三方以后指定。这允许所述要约权利的所有者以后“转送”使用权利，同时它允许所述内容供应商验证所述权利的使用。可以引入附加限制，诸如在要约权利和转送时间之间的最小或最大延迟。

第三方可以是不同的域,但是其还可以是由不是或不总是所述域的一部分的用户拥有的设备之一。所述第三方还可以是由其他人拥有的设备，但是由所述转送的所有者例如在访问期间、旅游时或在旅馆客房中当前在使用。

本发明的进一步目的是提供一种依照序文的客户端系统,所述使用权利是一个各自被签名的部分权利组，并且所述客户端系统被安排成各自验证并且各自处理所述部分权利。

本发明的进一步的目的是提供一种依照序文的服务器系统,所述服务器系统具有用于把所述使用权利分解为一个部分权利组的设备，所述服务器系统还具有签名部件，所述签名部件被安排成随后分别独立地签名所述部分权利组中的每一个，并且被安排成把各自签名的部分权利捆为一组。

本发明的进一步的目的是提供一种依照序文的信号,其中把所述使用权利分成被各自签名的部分权利。

本发明的进一步的目的是提供一种依照序文的设备，其中所述设备还被安排成处理已经被分成部分权利的使用权利，所述部分权利中的每一个具有数字签名。

将要参考附图并以举例形式进一步描述本发明的这些及其它方面，其中：

图 1 示意地示出了包括经由网络互连的设备的系统，

图 2 是依照现有技术的数字签名的权利，

图 3 是依照本发明被各自签名的一个部分权利组，

图 4 是依照本发明已经由所述发行者转送并签名的权利，

图 5 示出了在两个域之间转送所述权利，

图 6 示出了与每个权利相关联的、用于表明所要求保护级别的字段，

图 7 示出了把各自签名权利传送到家庭网络之外位置的传送，和

图 8 示出了要约权利，使用所述要约权利来请求把使用权利从供应商转送到在所述家庭网络外的位置。

在所有附图中，相同的附图标记表明相似的或相应的特征。代表性地，用软件来实现在附图中显示的一些特征，而这些特征本身又代表软件实体（例如软件模块或对象）。

图 1 示意地示出家庭（in-home）网络系统 100。这种系统一般包括许多设备，例如收音机、调谐器／解码器、CD 播放器、一对扬声器、电视、VCR、磁带机、个人计算机等等。通常互连这些设备以便允许例如电视之类的一个设备控制例如 VCR 之类的另一个设备。诸如调谐器／解码器或机顶盒（STB）之类的一个设备通常是中央设备，对其它设备提供中央控制。

例如经由 PC 106 或住宅内网关或机顶盒 101 来接收内容 130，所述内容 130 一般包括像音乐、歌曲、电影、TV 节目、图片、节目指南信息等等之类的东西。源可以与宽带电缆网络、因特网连接、卫星下行链路等等连接。所述机顶盒 101 或在所述系统 100 中的任何其它设备，可以包括诸如适当地大硬盘之类的存储介质 S1，以便允许记录并稍后播放所接收的内容。所述存储介质 S1 可以是某种个人数字记录器（Personal Digital Recorder PDR），例如 DVD+RW 记录器，所述机顶盒 101 与其连接。还可以向所述系统 100 提供内容，所述内容存储

在诸如光盘（CD）或数字多功能盘（DVD）之类的载体 120 上。然后可以经由网络 110 向接收端转送所述内容以便再现。

接收端例如可以是电视显示器 102、便携式显示设备 103、移动电话 104 和／或音频播放设备 105。再现内容项所采用的确切方式取决于设备的类型和内容的类型。例如，在收音机中，再现包括产生音频信号并把它们馈送到扬声器。对于电视机，再现通常包括产生音频与视频信号并且把这些信号馈送到显示屏和扬声器。对于其它类型的内容，必须采取类似适当的动作。再现还可以包括诸如解密或解扰所接收信号、同步音频与视频信号等之类的操作。

在一定条件下，个人计算机 106 还可以作为源、存储介质和／或接收端操作。

所述便携式显示设备 103 和移动电话 104 使用基站 111 来无线连接（例如使用蓝牙或 IEEE 802.11b）到网络 110。使用常规的有线连接来连接其它设备。为了允许设备 101 - 106 相交互，几个互操作性标准是可用的，其允许不同的设备交换消息和信息并且彼此控制。一种众所周知的标准是家庭音频/视频互操作性（Home Audio/Video Interoperability HAVi）标准，其版本 1.0 在 2000 年 1 月问世，并且在因特网网址 http://www.havi.org/上可查到。其它众所周知的标准是在 IEC 1030 和通用即插即用（http://www.upnp.org）中描述的家用数字总线（Demestic digital Bus D2B）标准。

确保在家庭网络中的设备 101 - 106 不会对内容进行未经授权的拷贝常常是重要的。为此，需有一个安全架构，典型地称为数字版权管理（Digital Rights Management DRM）系统。这种系统典型地使用权利。不同类型的权利是内容权利和使用权利。

内容权利描述了对于所述内容什么是被允许的，而使用权利授权人们使用确定的内容权利，并且还可以描述允许用户怎样处理所述内容。

实例性的使用权利是用于播放内容的权利，用于制作一个生成拷贝的权利等。

内容权利和使用权利还可以都包含密码密钥。

可以在抗篡改模块 108 中完成权利的安全处理和存储，所述抗篡改模块 108 例如位于中央控制器 101 中。

图 2 示出了依照现有技术可以怎样签名使用权利。所述使用权利例如可以包括再现权利（render right）、转送权利（transfer right）、派生工作权利（derivative）或实用权利（utility right）。一些权利在时间上或在次数上具有有限的有效性。在该例子中，使用权利 201 可以包含：再现权利 202 和转送权利 203，所述再现权利 202 规定用户对某块内容具有播放的权利，所述转送权利 203 规定所述用户具有把一定量内容转送到不同的域恰好两次的权利。签名过程利用众所周知的公钥加密，是基于一对私钥和公钥的存在的。所述私钥由签名并使用该私钥身份验证消息的一方来保密，并且为了验证该消息的确被签名并且自从由原始方签名以来没有被改变过，可以把对应的公钥分发给任何第三方并由其使用。

在该例子中，私有／公钥对产生器 210 为使用权利的发行者产生一对私钥 211 和公钥 212，所述发行者可以是内容供应商本身，我们把所述内容供应商称为 P。P 在所述使用权利 201 的签名过程 213 期间使用其私钥 211 并计算签名 204。使用权利 201 和签名 204 的组合构成所签名的使用权利 205，所签名的使用权利 205 可以被存储并发送，而对于未检出的篡改没有风险。任何第三方能够使用所述公钥 212 来执行验证过程 214 以便判断消息 205 是否是可信的。所述应答可用作输出 215。

然而，因为只有权利的发行者能够签名这种使用权利 201，所以不能分别独立地删除或处理来自这一组的权利，因为这会使所述签名 204 无效。因为没有控制（非法）拷贝部分权利，所以也不能可靠地撤消在安全环境的保护之外已经可用的这种部分权利。

本发明使在不使数字签名无效的情况下可以处理使用权利成为可能。

在本发明的第一实施例中，把使用权利 201 分解为部分权利，随后各自地签名所述部分权利。

图 3 示出了依照本发明的一个各自地签名的部分权利组 330。其包含了许多示例性部分权利 301、311、321，并且可能更多。在 P 控制之下的系统 350 中，签名部分权利。在过程 353 中再次使用 P 的私钥 351 来签名部分权利 301 以便计算签名 302。使用相同的签名过程 356 来计算 P 的部分权利 311 的签名 312 等等。这些签名的权利连同可选

的其它签名的权利，形成了一个新的各自签名的部分权利 330 组。现在在系统 345 中可以像在检验过程 354、357 和 360 中一样来各自地检验每个部分权利，以便计算所述签名是否有效（分别是输出 355、358 和 361）。可以由在访问部分权利的域内的任何设备来完成该验证。这种设备可以检查所述权利是否没有被所述发行者撤消，或所述发行者本身是否没有被撤消。

通过把所述部分权利作为组来处理，就在事务大小和数目上最小化通信，并且维持在所述使用权利和所述内容项之间的概念关系。

可选地，可以在过程 373 总体上来签名一个完整的各自签名的部分权利 330 组，以便验证所述权利组的完整性。在系统 369 中签名可以由服务提供者再次完成，而且如图 3 所示，还可以由受不同信任的第三方 T 用其自己的私有／公钥对 371/372 来完成，所述私有／公钥对 371/372 由密钥对产生器 370 产生。验证 374 产生输出应答 375，表明签名的权利组 340 是否是完整的。

本发明第一实施例的优点是由签名各自地保护所述部分权利，并且从而可以在所述域内自由并各自地流动。现在可以各自地处理它们，例如撤消。

在第一实施例的变形中，在过程 373 可以由权利组的接收器（例如，所述用户）本身的私有／公钥对 371/372 来签名各自签名的部分权利的完整组。可以把结果送回到例如所述权利组的发行者。这可以是事务的一部分，以便发行者能够证明完整的权利组已经到达了预期的接收器。

在本发明的第二实施例中，允许一些或所有签名的部分权利从一个域（始发域）转送到不同的域（接收域）。

图 4 示出了怎样给诸如在图 3 中所描述的部分权补充附加信息和签名，并且随后签名所述部分权利以便形成要加以转送的权利，还被称为可转送的权利。优选地是，从所提及的抗篡改模块内部构成可转送的权利，所述模块诸如在图 1 中的模块 108。其包含部分权利 311，它还包含由 P 按照签名过程 356 创建的原始的并仍然有效的签名 312。另外，增加元数据 411，其包含关于但不局限于下列项的信息：始发域的标识符、接收域的标识符、转送的原因或目的、转送的时间和有效性的长度。对于始发和接收域的标识符，优选使用它们各自的公钥。

部分权利 311、对应的签名 312 和附加信息 411 一起组成信息 430，并且随后在过程 463 中由所述始发域用其自己的私钥 461 来签名以便形成签名 431。所述可转送的权利 440 包含信息 430 和签名 431，并且可以在过程 464 中由任何第三方通过使用所述始发域的公钥 462 来检验所述可转送权利的有效性和真实性。

图 5 示出了两个域 500 和 550，都与在图 1 中的系统 100 相似。还示出了在过程 540 中可转送的权利 440 被转送到域 500 外，可以使用安全通信来转送到不同的域 550，优选地是在各自域中的通信设备 101 和 501 已经彼此验证是应允的并且没有被撤消之后进行。所述始发域 500 可以在本地撤消或删除所述转送的权利。

本发明的实施例具有进一步的优点：可以从包含在可转移权利中的元数据和签名来可靠地获取被转送权利的目标域和始发域。这使得能够跟踪内容。

在本发明的第三实施例中，在对不同类型权利的不同保护级别及其处理之间有区别。

一些部分权利在域内可以被自由地使用，即便是在加密的传输或安全存储的保护之外也是如此，诸如用于播放确定内容块的本地权利。这些权利将被称为“安全权利”。安全权利可以在授权域（AD）内自由地流动。诸如只能转送内容块恰好一次的权利之类的其它权利，在被使用之后必须立即要加以撤消或删除。将把这些权利称为“弱权利”。弱权利需要防止未经授权的复制和篡改，以便例如强迫它们只能被发布有限的次数。例如在还负责把权利转送到不同域的抗篡改模块中（可能在中央控制器中），例如可以通过不允许弱权利在安全环境的保护之外来提供这种保护。当然还可以定义两个以上的保护级别。

用于表明对某个权利所要求的最小保护级别的潜在方法是：添加具有所述信息的字段。图 6 示出了一个修改的权利组 640，与在图 3 中各自签名的部分权利 340 的签名组相似。在其最简单的形式中，附加的单个位字段 601/611 表明所述权利 301/311 是否必须被压缩在安全存储中。例如，权利 301 可以是不要求安全存储（在位字段 601 中示例内容是 0）的播放权利，而权利 311 要求安全存储（在位字段 611 中示例内容是 1）。用于表明所要求最小保护级别的可选择的方法包括

但不局限于：一种设备根据权利的类型来决定获得的保护级别，或一种设备具有表明对于每个权利所要求保护级别的（可更新的）列表。

可以使用所述最小要求保护级别来确定应该怎样处理所述部分权利。

在本发明的第四实施例中，描述为了（或许暂时地）用位于靠近所述用户／所有者的设备来扩展家庭网络而把权利转送到所述域外。所述扩展还可以是不同所有者的设备，所述所有者由于在部分权利中被指定或其它原因（诸如合法使用），所以有权访问所述内容。

在申请号为 02079390.7（代理人文档号 NL021063）的欧洲专利申请中，描述了 AD 架构的扩展，其允许人们在原始定义的家庭网络外，例如当旅行时，远程地查看或使用其个人内容。在所述应用中，通过加密内容，通过安全存储对应的解密密钥，并且通过个性化的使用权利来获得安全性，由信任的第三方创建的签名来保护所述个性化的使用权利。

在这种情况下，能够只传递所述使用权利的一部分是有益的，依照本发明所述使用权利还可以使用单个签名。图 7 举例说明了经由网关 751 把可转移权利 731 从系统 100（如图 1 所示）转送到远程旅馆电视系统 770 的转送过程 730，例如转送到位于接近所述授权用户的收音机 753 或电视 752。这些设备可以位于旅馆房间、大厅等。

在本发明的第五实施例中，所述转送权利被保持在所述服务提供者，并且所述所有者向所述服务提供者通知应该把所述权利转送到另一人或域。

为了表明所述转送权利的存在，在本申请正文中已经引入要约权利。

在这种情况下，因为所述服务提供者可以监视只可以做出允许数目的拷贝，所以不要求安全存储来防止非授权复制。

图 8 示出了由家庭网络系统 100 对要约权利的使用。在通信过程 820 期间，把要约权利 821 发送到提供商 810 以便请求把使用权利 831 转送 830 到在家庭网络外的系统 550。所述服务提供者可以在存储器 811 保存转送权利或者当要求时用产生器 812 来产生所述转送权利。

还可以有可选择的实施例。在上面的描述中，“包括”不排除其它元件或步骤，“一个”或“一种”不排除多个，并且单个处理器或

其它单元也可以实现在权利要求中所列举的几个装置的功能。

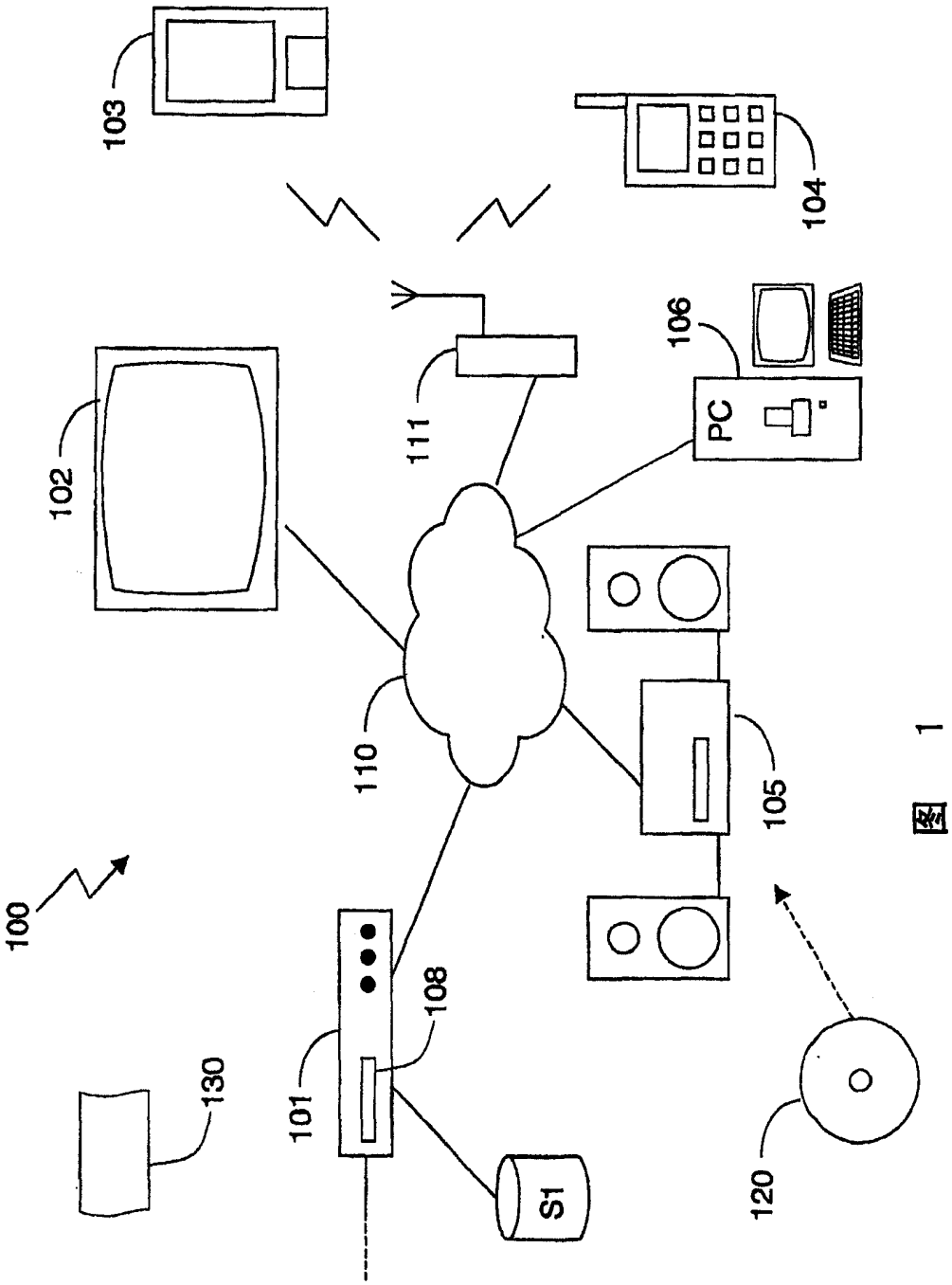


图 1

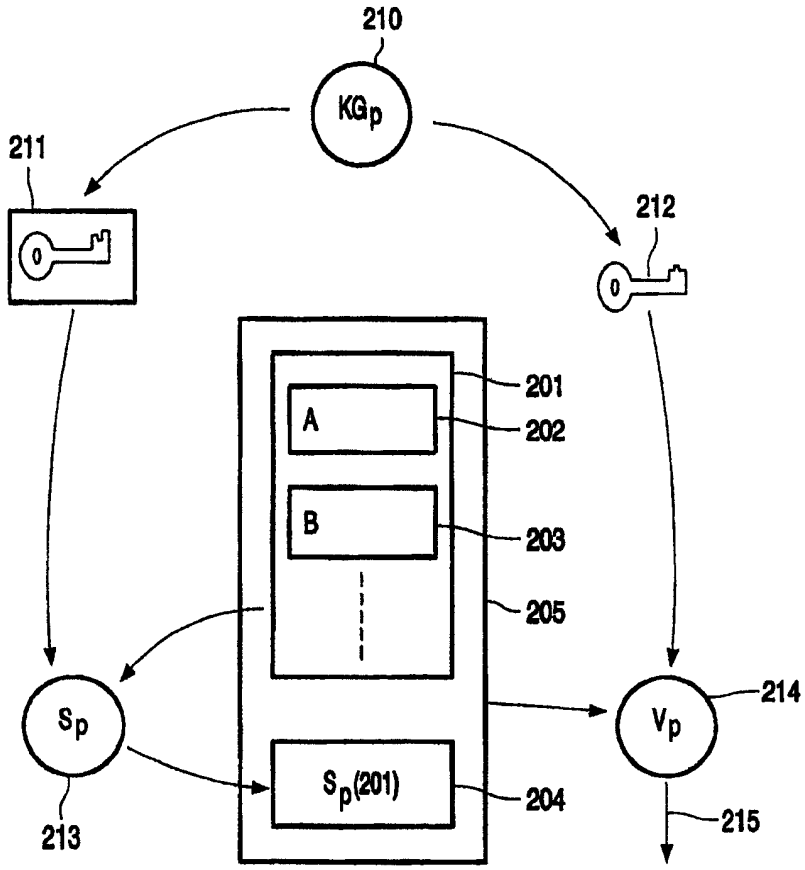


图 2

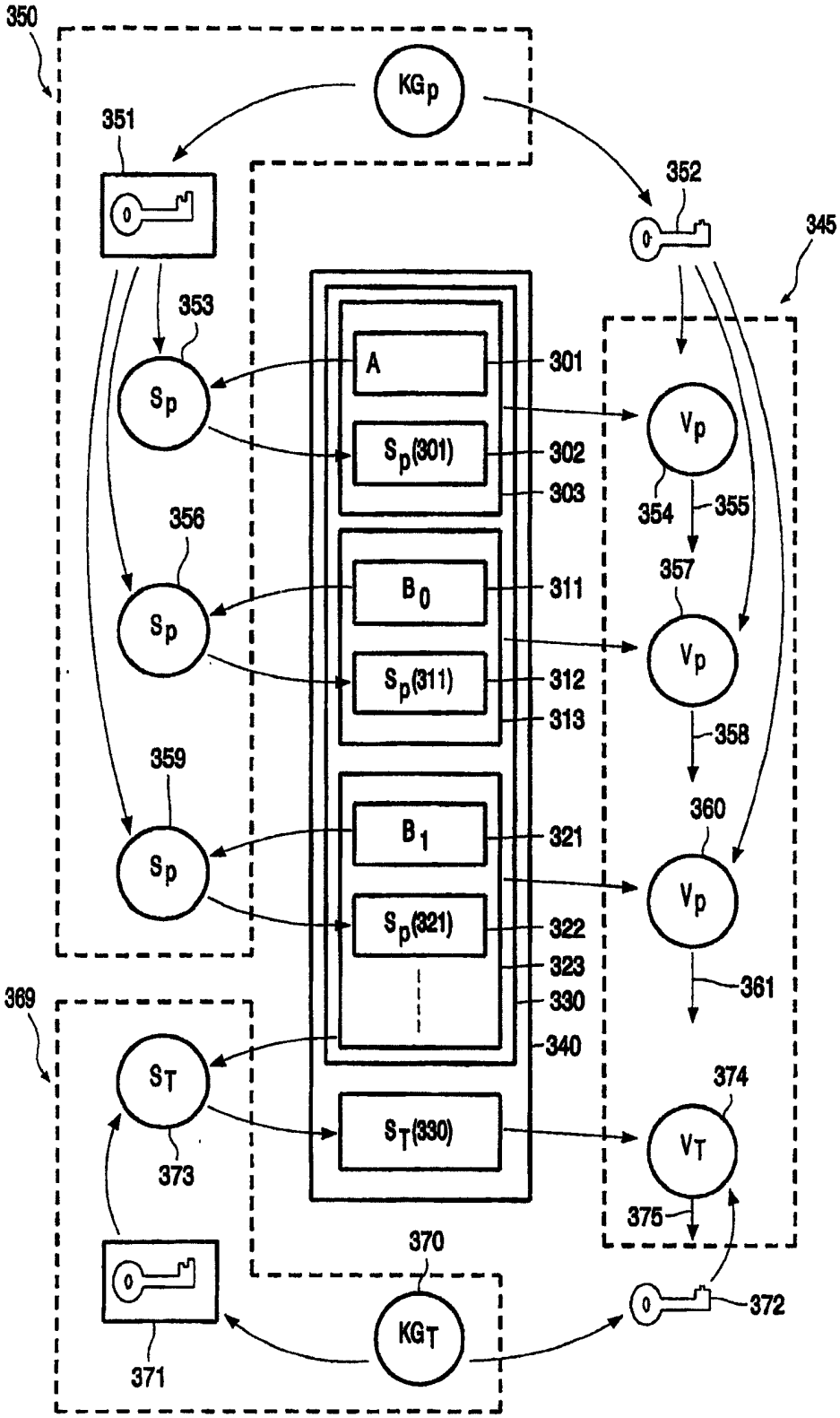

350
KGp
351
352
345
353
A
301
Sp
Vp
Sp(301)
302
303
354
355
356
357
B0
311
Sp
Vp
Sp(311)
312
313
358
359
360
B1
321
Sp
Vp
Sp(321)
322
323
330
340
361
369
374
ST
ST(330)
VT
373
375
370
372
KGT
371

图 3

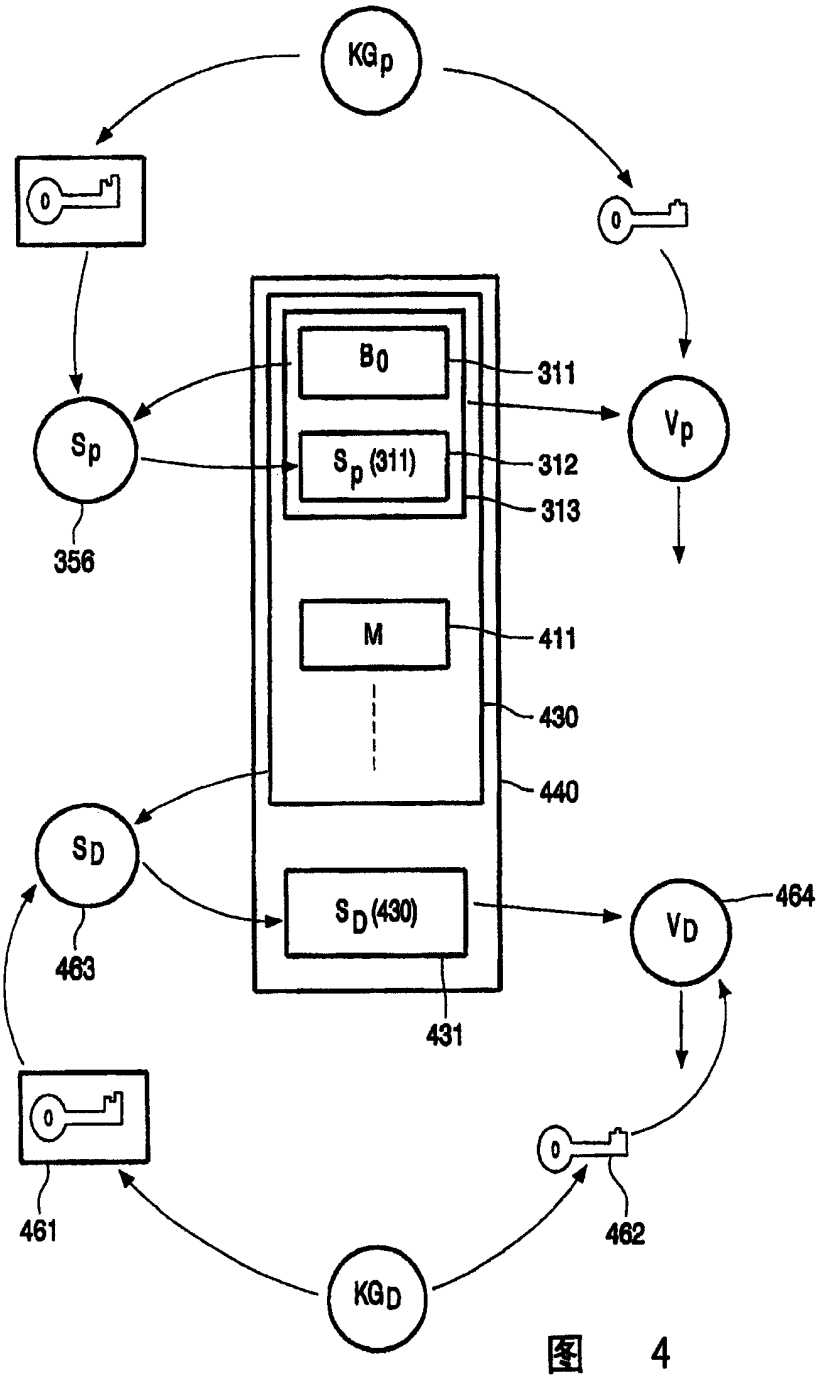

KGp
B0
311
Sp
Sp (311)
312
313
Vp
356
M
411
430
440
SD
SD (430)
464
VD
463
431
461
462
KGD

图 4

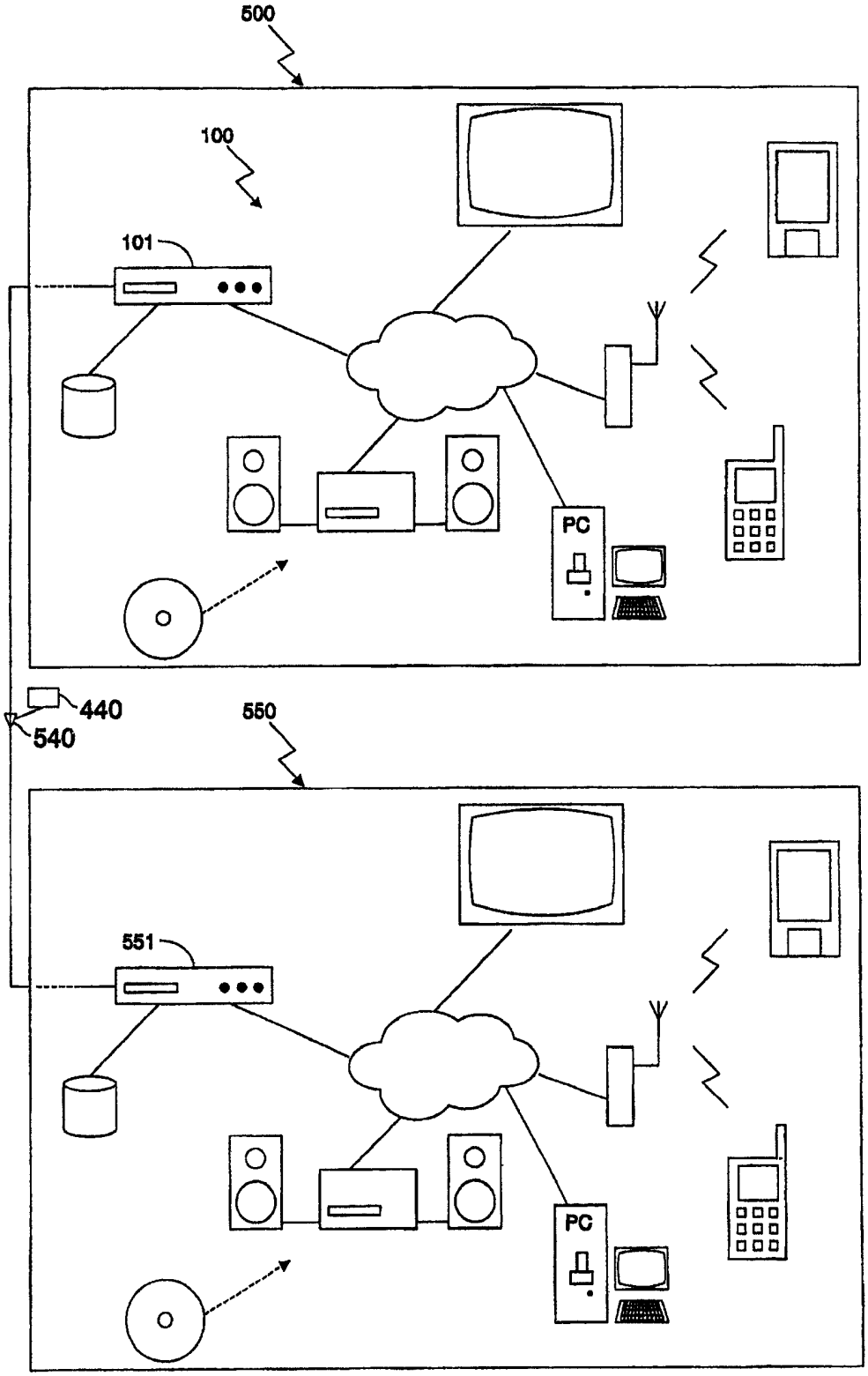


图 5

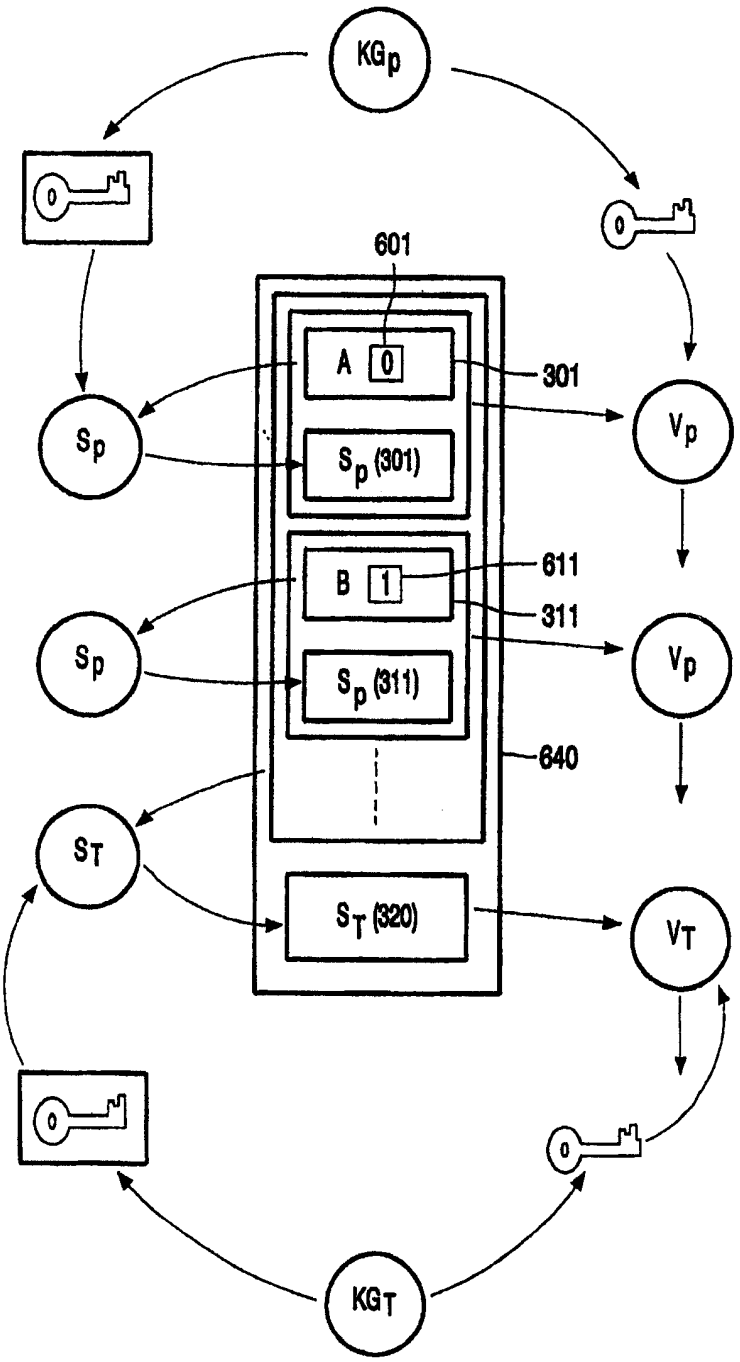

KGp
601
A 0
301
Sp
Vp
Sp (301)
B 1
611
311
Sp
Vp
Sp (311)
640
ST
ST (320)
VT
KGT

图 6

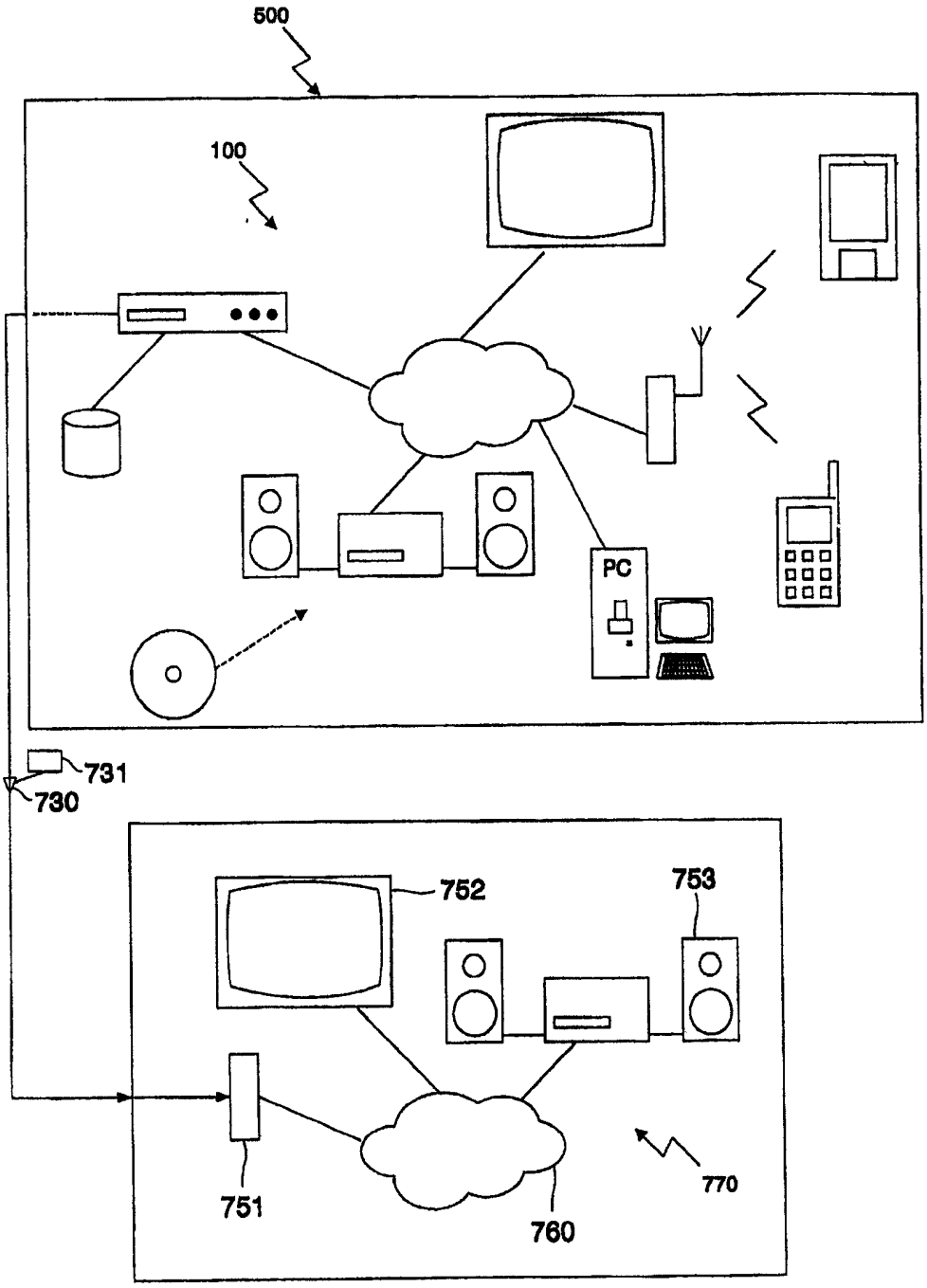


图 7

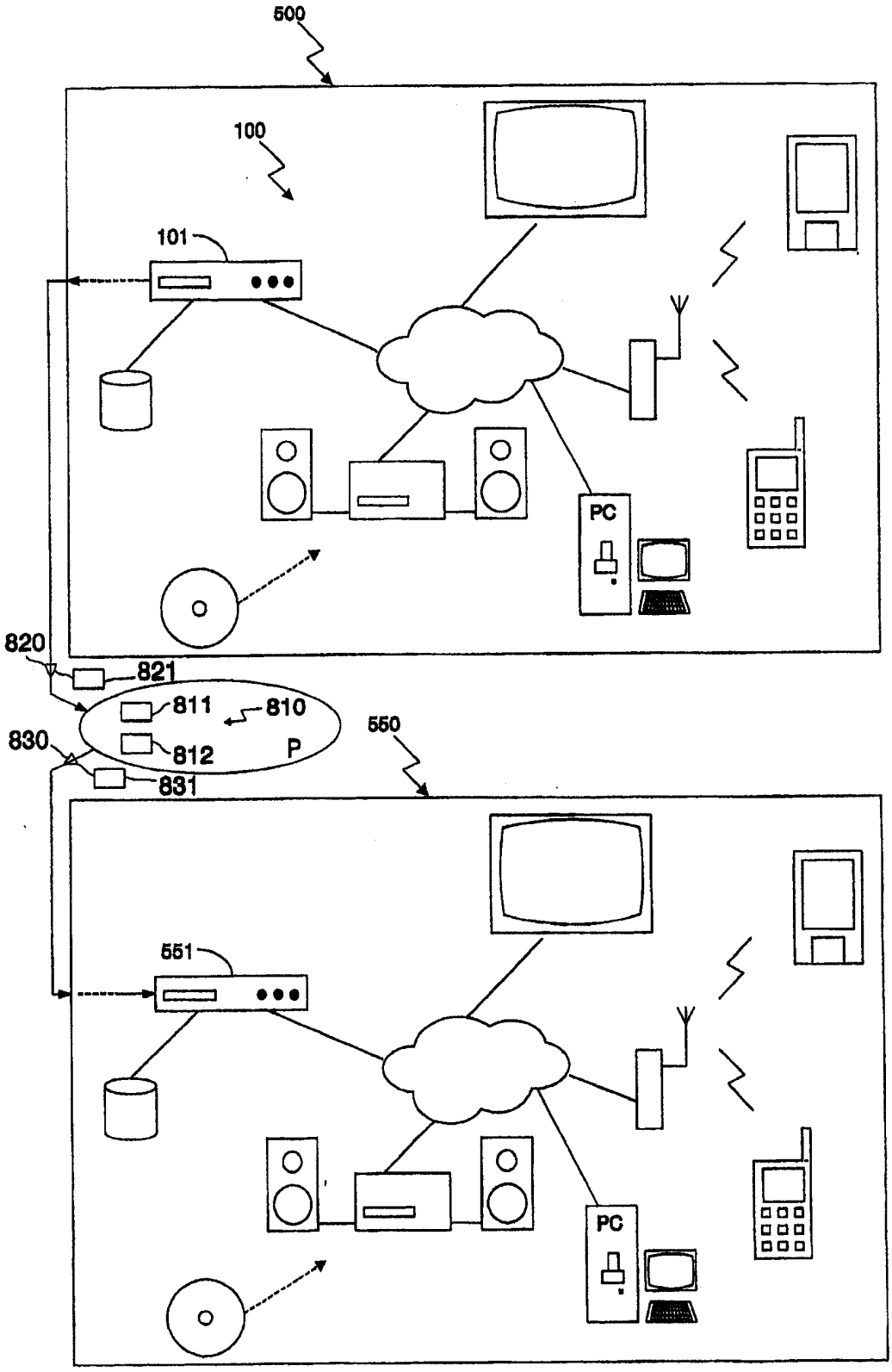


图 8