[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 7/167
H04N 5/00

[12] 发明专利申请公开说明书

[21] 申请号 03824668.6

[43] 公开日 2005 年 11 月 9 日

[11] 公开号 CN 1695374A

[22] 申请日 2003.9.19 [21] 申请号 03824668.6
[30] 优先权
[32] 2002. 9.27 [33] CH [31] 1623/02
[32] 2002.12. 4 [33] CH [31] 2048/02
[86] 国际申请 PCT/IB2003/004121 2003.9.19
[87] 国际公布 WO2004/030363 法 2004.4.8
[85] 进入国家阶段日期 2005.4.26
[71] 申请人 纳格拉影像股份有限公司
地址 瑞士洛桑
[72] 发明人 希尔万 - 维克托 · 内厄姆
菲利浦 · 斯特兰斯凯
[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 郭思宇

权利要求书 2 页 说明书 10 页 附图 1 页

[54] 发明名称 条件访问数据解密系统

[57] 摘要

本发明涉及一种条件访问数据解密系统，具体地用于付费数字电视广播中。 所述系统包括一个被设计为广播由各控制字(cw)加密的数据的广播中心(1)，至少一个被设计为广播涉及对加密数据的访问权利的各个人消息(ECM，EMM)和管理所述访问权利的管理中心(11)，一个用于使所述加密数据成为可用的操作器件(12)以及一个用于将至少一部分加密数据解密的解码器(13)。 所述解码器位于广播中心(10)和操作器件(12)之间。 所述解码器(13)包括一个用于接收加密数据的模块(14)和一个用于管理访问所述数据的权利的模块(15)。 接收模块(14)连至或集成于操作器件(12)中，以及管理模块(15)被设计为与接收模块通信。 管理模块(15)包括一个安全模块(16)，它被设计为验证个人消息(ECM，EMM)的内容以及根据个人消息内容允许或阻止将各控制字(cw)解密。 接收模块从广播中心(10)接收加密数据以及管理模块从管理中心(11)接收允许消息(EMM)。

ISSN1008-4274

1. 一种条件访问数据解密系统，此系统包括:

. 一个传播中心（10），被安排为把由至少一个控制字(cw)所加密的数据加以传播，

. 至少一个管理中心（11），被安排为将与访问装置的管理相关的个人消息(ECM, EMM)传播给加密的数据，

. 一个操作器件（12），用于给出可用的所述加密数据，及

. 一个解码器（13），被安排为将放置于传播中心（10）和操作器件（12）之间的至少一部分加密数据加以解密，

其特征在于

. 解码器（13）包括一个用于接收和解密所加密数据的模块（14）和一个用于管理对此数据的访问权利的模块（15），这些模块在物理上是不同的，接收模块（14）连至操作器件（12），以及管理模块（15）被安排为与接收模块通信，

. 管理模块（15）包括一个安全模块（16），它包括一个独一的标识号（UA）和用于保证所述管理中心（11）与安全模块（16）之间连接的安全性的数据，此安全模块被安排为验证个人消息(ECM, EMM)的内容以及根据个人消息内容允许或阻止将（各）控制字(cw)解密，

并且在于: 接收模块(14)接收来源于传播中心(10)的经由第一通信线的加密数据，以及管理模块(15)通过管理中心(11)并经由第二通信线接收个人消息(ECM, EMM)。

2.根据权利要求 1 的数据解密系统，其特征在于接收模块（14）和管理模块（15）之间的通信是借助于波进行的。

3.根据权利要求 1 的数据解密系统，其特征在于权利管理模块（15）是一个移动电话。

4.根据权利要求 3 的数据解密系统，其特征在于安全模块（16）包括电话和至少一个关于管理中心（11）的存储区所需的鉴别功能，此存储区包括用于接收所述管理中心的授权消息(EMM)的各安全参数。

5.根据各权利要求 1 至 4 的系统，其特征在于传播中心（10）被安排为传播包括（各）控制字(cw)的控制消息（ECM），以及在于由管理中心（11）广播的个人消息对应于一个授权消息(EMM)。

6.根据各权利要求 1 至 4 的系统，其特征在于管理中心（11）被安排为传播包括（各）控制字(cw)的个人消息，管理模块（15）的安全模块（16）具有用于确定此消息是否准备用于所述安全模块的装置和将此控制字(cw)传输至接收模块（14）的装置。

7.根据权利要求 6 的系统，其特征在于接收和解密模块（14）包括一个应用于控制字(cw)的独一解密密钥，此密钥用于在各控制字被向管理模块（15）传输之前在管理中心（11）处将各控制字加密。

8.根据权利要求 1 的数据解密系统，包括至少两个管理中心（11），其特征在于管理模块（15）的安全模块（16）包括用于接收来源于不同管理中心（11）的授权消息(EMM)的各安全参数。

9.根据各权利要求 1 至 8 的数据解密系统，传播中心（10）被安排为传输加密数据的描述性信息，其特征在于所述数据包含为建立与负责对这些数据授权的管理中心（11）的通信所需的标示，并且所述数据被传输至管理模块（15），后者被安排为建立与所考虑的管理中心（11）的通信，从而获取授权消息(EMM)。

10.根据上述权利要求中任一项的数据解密系统，其特征在于接收和解密模块（14）被集成于操作器件（12）内。

11.根据权利要求 1 的数据解密系统，其特征在于接收和解密模块（14）包括具有管理模块（15）的标准化通信装置，以使一个接收和解密模块（14）能够与多个管理模块（15）交互操作。

12.根据上述权利要求中任一项的数据解密系统，其特征在于管理模块（15）包括用于建立一个与接收模块（14）匹配的密钥的装置，此密钥准备用于向接收模块（14）加密和解密至少传输至管理模块（15）的各控制字(cw)。

条件访问数据解密系统

技术领域

本发明涉及一种条件访问数据解密系统。

背景技术

这类系统具体地用于数字付费电视领域。在此情况下，向电视机传输的数字数据流被加密以便能够控制使用并决定此类用途的条件。得益于以一定间隔（虽然可用较长的间隔，但通常在 5 至 30 秒之间）改变的控制字而完成这种加密操作，从而阻止任何旨在发现此控制字的侵犯。

为使接收机能够使用这些控制字将被加密的流解密，后者使用一个密钥加密并且独立于控制消息（ECM）流之外而被发送，该密钥属于一个管理中心和一个用户单元的安全模块之间的传输系统。事实上，在一个安全模块（SC）中执行该安全操作，该安全模块通常具有一个智能卡的形式并享有不会损坏的声誉。此模块可以是可移动类型，也可直接集成于接收机内。

在将控制消息（ECM）解密时，它在安全模块（SC）中被证实具有访问该流的权利。此权利能被授权消息（EMM）进行管理，它将此权利装入该安全模块。也可想象其它可能的操作，例如发送解密密钥。

在后面，“事件”系指按照已知控制字方法进行加密的视频或音频（例如 MP3）的内容或数据（例如游戏程序），每个事件能用一个或多个控制字加密，每个控制字具有一个确定的有效期。

目前使用这些事件的记账是根据订阅、根据购买事件或者按照时间单元付费的原则的。

订阅允许限定与一个或多个传输这些事件的传播频道相关联的权利，以及如果在用户的安全模块中存在该权利，则允许他/她获得用明文

表示的这些频道。

类似地，有可能为一个事件例如一个影片或一场足球比赛限定各权利。用户能够获得（例如购买）此权利，然后由此权利专门安排此事件。此方法已知被称为“付费观看节目”（PPV）。

关于按照时间单元付费，该安全模块包括一个信贷，它按照用户的实际消费来记入借方。因此，例如，无论所考虑的频道或事件如何，每分钟都向贷方将一个单元记入借方。有可能根据技术实施方式随着持续时间或者所占时间值或者甚至通过将这两个参数合并而改变记帐单元，以便适用于对所传输事件的不同类型开出发票。

控制消息（ECM）不但包含控制字，还具有为将此控制字送回接收机/解码器所需的条件。在控制字解密期间，如果在安全模块中存在一个与该消息中给定的访问条件相关联的权利，它将被证实。

当该比较结果为正时，该控制字只被送回至用户。此控制字被包含于一个由一个传输密钥所加密的控制消息 ECM 中。

为使该权利存在于该安全模块中，通常由一个授权消息（EMM）将它装载入此模块，由于安全理由，该授权消息通常由不同的称为权利密钥（RK）的密钥进行加密。

根据付费 TV 传播的一个已知形式，以下三个元素是在给定时间内将一个事件解密时所需的：

- 与由一个或多个控制字（CW）所加密的事件相关的数据；
- 包含控制字（CW）和访问条件（AC）的（各）控制消息 ECM；
- 存于安全模块内并允许对所述访问条件进行证实的相应权利。

现在上述类型的解密系统都由相对大的设备组成。它们连至一个运行的或是可视化的器件例如有线电视。它们并不被提供为能被容易地移动。因此，不可能移动用户自己的解码器并将它简单地连至另一个电视机而获取确切权利。此外，在现有系统中，相对少的装备具有一条回线，允许从解码器向一个管理中心通信。这些具有一条回线的装备通常没有一个允许与管理中心进行用户友好通信的接口。事实上，该回线被提供为在解码器和管理中心之间进行通信，但不在用户和此中心之间通信。

因此难于简单地和快速地获取确切权利。在所有已知系统中，包含数据、控制消息和授权消息的各流来源于一个独一来源，它用于管理它自己的订户但不能提供来自不同来源的订阅范围。

在允许装载确切权利的系统中已经改善了与管理中心的通信。这类系统被描述于美国专利5,901,339中。此文件描述的一个系统包括用于数据或加密事件的数个传播中心，意在将这些事件传输至一个操作的系统例如一个电视机或其它显示装置。这些事件一方面与一个独一标识号而另一方面与一个解密码相关联。该系统还包括一个装载中心，在传播这些事件之前，每个事件的与该解密码相关联的标识号被传输至该装载中心。当一个用户希望获取将一个加密事件进行解密的权利时，他/她通过一个通信设备例如电话访问该装载中心，并且标示他/她希望获取的识别号。该装载中心将所考虑的事件的解密码传输至通信设备。然后该装载中心将此码传输至用户的解码器。当该事件被广播时，该解码器具有该解密码以及该事件能被解密和加以可视化。

此系统涉及一定数量的约束。具体地，由于解密码是在用户请求下接收的，为相同事件使用数个解密码是不方便的。在此事件的整个持续期间，此码必须保持不变。从安全的观点看，这是一个缺点。作为比较，在现有系统中，为加密和解密事件所用控制字每隔一定间隔就改变，该间隔可在大约2至30秒之间变化。

在根据美国 5,901,339 的系统中，数个传播中心只连至一个装载中心。这具体地意味着所有传播中心必须将它们的密码装置放置于相同的装载中心内，但从安全角度看这不是最佳情况。

此系统还具有安全方面的其它缺点。一方面，在装载中心和用户解码器之间的解密码的传输是通过电话的一条电话线而不是安全装置进行的。这意味着要想非法地获取此码并且将它与另一个解码器一起使用是相对地容易的。另一方面，由于装载中心并不清除任何与请求该解密码的解码器相关的信息，有可能在任何解码器上使用此码。这意味着一旦它已经被合法地获得，该解密码能被容易地传输至其它解码器而非法地将一个事件或数据解密。

名为“一个条件访问系统的功能模型”的文件“EBU 技术回顾” Winter 1995 No. 266 描述了具体地用于付费 TV 的条件访问系统的不同变量，这些系统使用双级解密操作，也即通过控制消息 ECM 来实现的第一级安全性，以及使用授权消息 EMM 的第二级。在这些变量中的一个中，该条件访问系统意欲同时地供数个条件访问数据传播器使用。所述系统具体包括一个权利管理系统，负责生成和发送授权消息 EMM 以及一个授权管理系统为将传播器数据加密而负责生成控制字。

在此文件中所呈现和描述的所有例子中，每个传播器与一个权利管理系统单义地相关联。不可能只将一个传播器与数个权利管理系统相关联。在根据此文件的系统中，一个或数个服务供应商的使用是对用户完全透明的。事实上，后者不能选择一个操作者或另一个，他/她只能选择一个具有一个或多个操作者的服务。

此系统并不解决与解码器的简单放置和确切权利的获取相关联的问题，也无法解决用户和管理中心之间通信的问题。

发明内容

本发明意在避免现有技术中这些系统的缺点，所产生的系统能够容易地在实际中任何选择的操作器件中被放置和使用。此外，这类系统在传播中心的级别上简化访问权利的管理，并且通过保证最佳安全性从而阻止将一个用户为确定的解码器所获取的数据用于另一个解码器上，从而给用户提供更大灵活性。

一种条件访问数据解码系统能达到这些目的，此系统实施：

. 一个传播中心，被安排为把由至少一个控制字所加密的数据加以传播，

. 至少一个管理中心，被安排为将与访问装置的管理相关的个人消息传播给加密的数据，

. 一个操作器件，用于给出可用的所述加密数据，及

. 一个解码器，被安排为将放置于传播中心和操作器件之间的至少一部分加密数据加以解密，

其特征在于

．该解码器包括一个用于接收和解密所加密数据的模块和一个用于管理对此数据的访问权利的模块，这些模块在物理上是不同的，该接收模块连至操作器件以及该管理模块被安排为与接收模块通信，

．该管理模块包括一个安全模块，后者包括一个独一的标识号和用于保证所述管理中心与安全模块之间连接的数据，此安全模块被安排为验证个人消息的内容以及根据个人消息内容允许或阻止将（各）控制字解密，

并且在于：该接收模块接收来源于传播中心的经由第一通信线的加密数据，以及该管理模块通过该管理中心并经由第二通信线接收个人消息。

附图说明

参照不同实施例和附图，将能更好地理解本发明及其优点，附图中：

．图 1 表示根据本发明的系统的第一实施例的一个总图；及

．图 2 是本发明的第二实施例的一个总图。

具体实施方式

参照这些图的涉及本发明的系统主要包括一个被安排为传播加密数据的传播中心 10，至少一个被安排为传播授权消息（EMM）和对加密数据的访问权利进行管理处理的管理中心 11，一个使该加密数据可用的操作器件 12 以及一个被安排为将至少一部分加密数据解密的解码器 13。

用于加密数据的传播中心 10 可以是一个使用电缆的常规器件或是卫星。该中心以加密形式传输数据。当然，这些数据的性质决定于它必须被使用的方式。在下面将能理解，这些数据用于一个条件访问电视系统中。因此这些数据由视频内容 CT 组成，也就是说，由图像和声音组成。如业内人员所熟知的，也可包括专用于此用途的其它数据。所述数据或其中至少一部分通过控制字进行加密，并在图中标以 cw（CT）。

根据第一实施例，由传播中心在传播加密数据的同时以加密形式传播控制字 cw。根据另一个实施例，这些控制字能被管理中心 11 作为控制消息的密码进行传播，该控制消息包括该控制字并根据适合于每个管理中心的协议而被专门管理。

当控制消息（ECM）不是专用时，“个人消息”这一名称代表一个授权消息（EMM），这些个人信息允许通过存储一个权利而访问这些数据。该控制字从该消息中提取并通常以加密形式发送至接收模块，从而使该控制字不能在此级上被复制和送至另一个用户。

管理中心或者更一般的是各管理中心 11 负责管理对数据的访问权利。它们可以各管理不同类型的权利，具体为订阅、确切访问、不同频道组合。为做到此点，它们也传播相应的供所考虑的各解码器使用的授权消息（EMM）。

当然操作器件 12 也适用于将被传输的数据。在所选择的条件访问电视系统中，该操作器件是一个电视机。

解码器 13 包括一个用于接收和解密数据的模块 14 以及一个用于管理访问这些数据权利的模块 15。权利管理模块的生产方式是它易于移动。能够通过一个移动电话来明智地实现这点。该管理模块还包括一个安全模块 16。此接收和解密模块能够包括具有管理模块的标准化通信装置。因此该接收模块能够与任何管理模块交互操作。

一个被开发的安全模块能够包括关于（pertaining to）每个管理中心的各存储区。在移动电话的情况下，电话操作者能够分配各存储区，然后由各参数为每个管理中心将它们激励。这些参数例如是授权消息（EMM）的解密密钥、根据关于所述管理中心的系统的订户的鉴别操作或者甚至一个信贷。

当不同操作者不希望将他们的安全性集成为一个公共模块或简单地增加使用的灵活性时，有可能提供连接器技术，它允许安全模块或者容易地改变，或者数个同时使用。这些模块能够以与管理模块的一个合适的阅读器合作的智能卡的形式生产，或者以更紧凑形式将数个安全模块同时实施。在此情况下，每个芯片管理来源于管理中心中的一个的各

授权。

还可能提供一个卡或另一个包括数个芯片的支持，它们中的每一个管理来源于管理中心中的一个的各授权。这类安全模块被公开于图 2 中，由参考标号 16 标记。

该安全模块或数个模块中的每一个都包含一个独一的标识号（UA）和关于管理中心 11 的数据，这些模块被授权利用所述数据通信。这意味着，在能够获取和解密一个来源于一个管理中心的授权消息（EMM）之前，与此管理中心相关的数据必须首先被装载入该安全模块。关于该管理中心的数据例如是一个加密密钥或一个允许形成一个加密密钥的代码，这些数据允许在管理中心和将被保证安全的安全模块之间进行连接。根据一个优选实施例，该授权消息（EMM）以一种加密形式通过一个密钥被送至该安全模块，其中该密钥既决定于相关的管理中心，又决定于安全模块的独一的标识号 UA。依此方式，由一个安全模块接收的授权消息不能由另一个模块使用。此外，一个伪造的不包含关于该管理中心的数据的模块无法使用该授权消息，因为它不能将所述消息解密。

该管理模块 15 优选地包括一个智能卡阅读器，准备用于一个信用卡或一个预付费卡 17。依此方式，当请求一个事件时，能保证管理该支付。此外，这允许将该管理模块用作一个电子钱包。此类卡被显示于图 2 中，以参考标号 17 标记。

根据用于实施向接收模块传播数据的数个管理中心的一个实施例，提供向所述加密数据增加描述性信息，从而允许用户与合适的管理中心连接。此描述性信息从接收模块传输至管理模块，并被显示于所述模块上。用户能够做出他/她的选择并启动一个与一个中心的通信，只要他/她的安全模块支持此管理中心所要求的安全功能即可。除描述视频或音频产品外，此描述性信息包括一个电话或因特网类型的地址。此地址将被用于交互操作，以便发送用于允许接收为访问（存取）加密数据所需的权利或密钥的个人消息。

数据的接收和解密模块 14 能够被直接集成入电视设备 12。在此情况下，为能在此类电视设备上阅读加密数据，具有管理模块 15 和对应于

所需事件的权利就已足够。因此该事件能够在任何合适地装配的电视机上被可视化。此实施例被原理地阐述于图 2 中。根据另一个优选实施例，它能由一个盒子组成，该盒子通过一条连接电缆或直接通过电视机上的输出口连至该电视机。这允许将本发明简单地应用于现有电视机上。

根据本发明的系统用以下方式运行:

如前所述，由加密数据的传播中心 10 来传播视频内容 CT。同时，此第一中心还将已经用于将数据加密的（各）控制字 cw 进行传播。当一个用户希望使用条件访问系统的数据例如希望观看一个事件例如一个影片或一场足球赛而访问它们需要一定权利时，用户首先需要获取此权利。后者能由管理模块 15 中的一个预付卡给出，或者得益于该模块和用于管理访问权利的管理中心 11 中的一个之间的通信装置，它能被装载入此模块。

为获取允许将解密数据所需的控制字 cw 解密并将该事件可视化的各授权消息 EMM，接收和解密模块 14 与管理中心中的一个建立通信联系。如前所述，该接收模块可以是一个移动电话。在此情况下，通过拨通一个对应于该传播中心的电话号而建立一个连接。通过一个预先纪录的“菜单”来选择用户希望为其获取权利的事件，其中该菜单的每个选项与移动电话键盘上的一个具体号码相关。在电话键盘上按下一个有效键之后，将对应于所选事件的授权消息下载。通过一个既取决于安全模块的独一标识号 UA 又取决于关于该管理中心的数据的一个键来优选地将此授权消息加密。

接收和解密模块 14 连至电视机，例如连至后者的一个输出口或直接集成于该电视机内。

在第一实施例中，接收模块 14 通过各控制字以及控制字 cw 本身接收来源于第一传播器件 10 的加密数据 cw（CT）。它还接收来源于管理中心 11 中的一个的授权消息 EMM。接收模块 14 将控制字 cw 传输至权利管理模块。可通过例如红外或无线电波进行传输。此权利管理模块验证是否已经正确地获取了对应于所选事件的权利。如果情况属实，则在安全模块中处理控制消息 ECM，从而提取控制字 cw。后者然后使用一

个对应于数据加密所用频率的合适频率被传输至接收模块 14，接收模块 14 然后使用所述控制字将数据解密并使该事件成为可视。

在一个原理地阐述于图 2 中的第二实施例中，权利管理器件 15 接收包含加密数据、控制消息和授权消息的流。这些流被如前一样地处理以及解密的数据用明文传输至接收器件。

此系统允许生产一个容易地运输的并能用于任何电视机上的解码器。当数据接收模块 14 被集成入电视机中时，已足以安排管理模块 15 访问一个事件。依此方式，可消除对用户的约束。此外，由于使用不同于数据传播中心的管理中心来管理授权消息，此事实增加了提供给用户的选择，并且便于使用条件访问系统。

由于各控制字在管理模块中被解密并传输至接收模块，将能优选地保证这两个模块之间的通信。为此，有许多不同配对过程，它们通常适用于由安全单元和解码器所形成的各对。在此情况下，这些过程应用于接收模块和管理模块之间。这类配对的例子被描述于申请 WO 02/052515 中。

为保证这些控制字不被散布至其它接收和解密模块，在一个具有双级的图中，当控制消息是个人类型时，管理中心能够要求一个属于解密模块的加密密钥。此密钥被直接编码于解密模块中，对于每个模块此密钥是独一的。

当包含控制字 cw 的控制消息 ECM 通过管理中心被发送时，或类似地当一个事件通过单个由管理中心送至安全模块的密钥被加密时，此管理中心在一个给定的控制字上施加一个关于解密模块的独一密钥的加密操作以及还有一个关于管理中心和安全模块之间的电讯系统的加密操作。因此，如果此消息被一个伪造的安全模块所截获，则该被获取的控制字将无法用于另一个解密模块，因它是由此模块的独一密钥所加密的。

根据一个实施例，在管理模块和管理中心之间的连接是一个被保障的点对点连接。因此有可能将与由传播中心所传播的图像和事件相关的命令进行传播。此功能用于通过管理模块作出命令或对请求作出响应。

在一个应用中，向解码器传播的图像是来源于娱乐场游戏例如转盘

或“二十一点”牌戏的真实图像，并且此类管理模块的主人，无论他或她在何处，都能交互地实时地玩耍。为有条件地访问所广播数据而实施的安全装置也能用于此类应用。在此类应用中，娱乐场连至管理中心，以便确定管理模块携带者的身份或者至少确定此携带者是有偿还能力的。管理中心为此携带者分配一个信贷并将此信息传送给娱乐场。

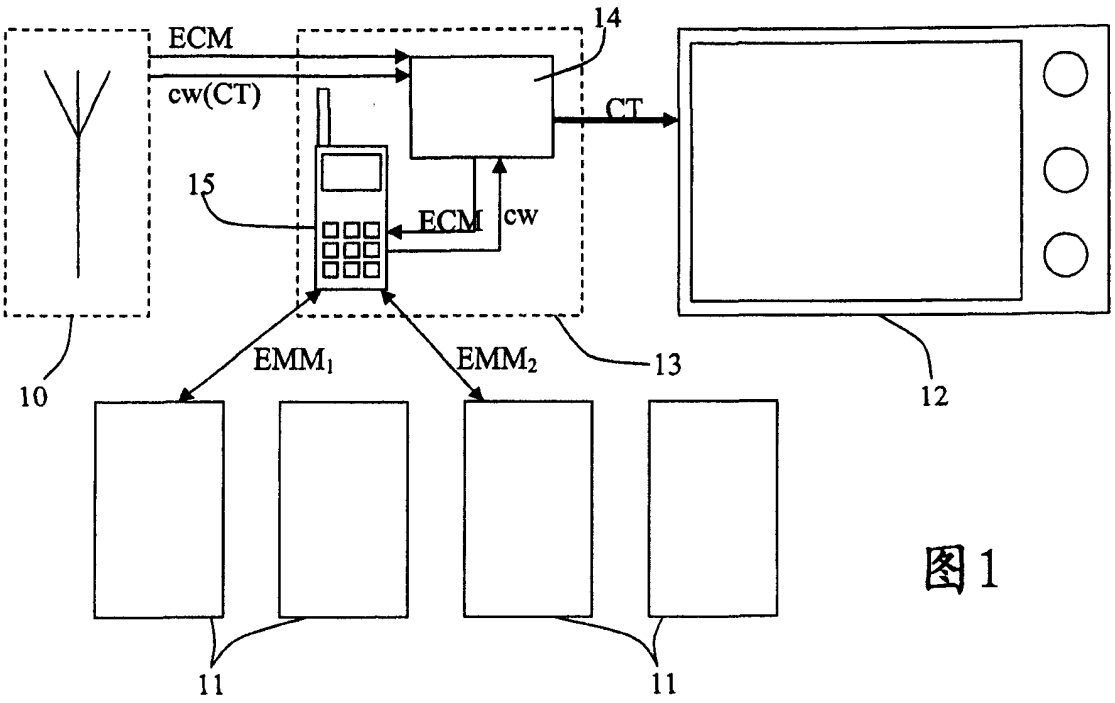
ECM
cw(CT)
14
CT
15
ECM
cw
EMM1
EMM2
13
10
12
11
11

图1

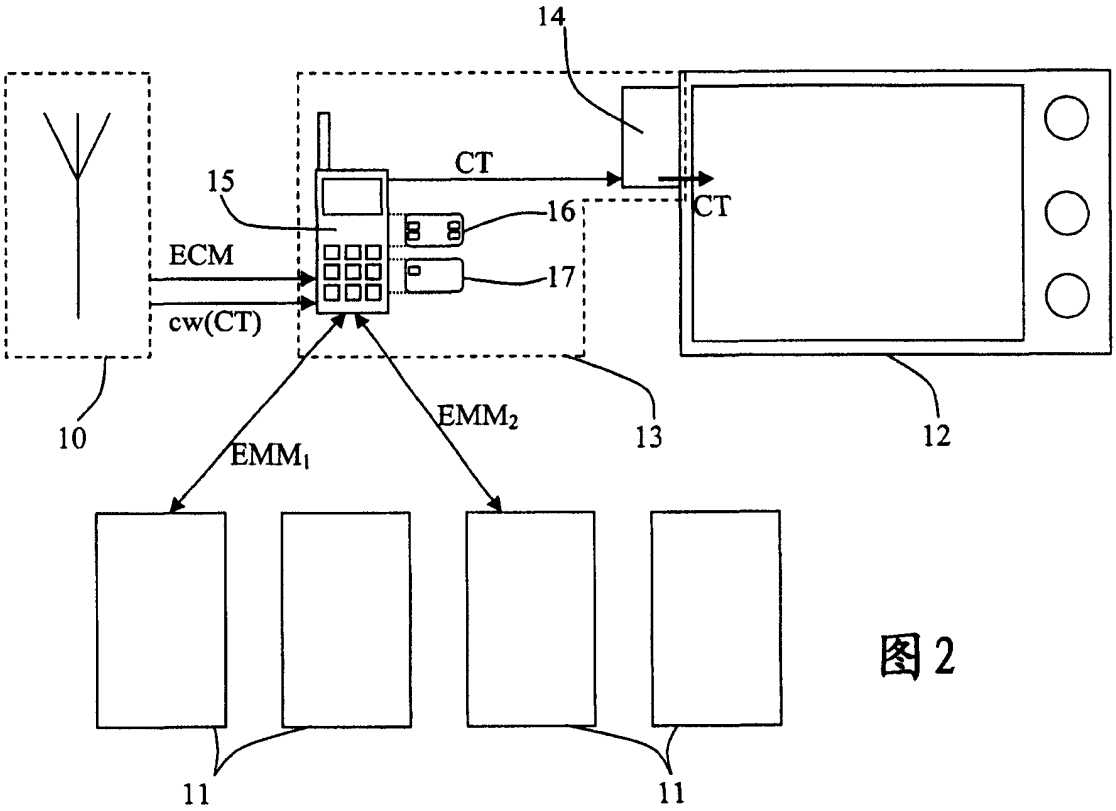
14
CT
15
16
CT
ECM
17
cw(CT)
EMM2
EMM1
10
13
12
11
11

图2