[19]中华人民共和国专利局

[51]Int.Cl[6]
H04N 7/167

[12]发明专利申请公开说明书

[21]申请号 96193603.7

[43]公开日 1998年5月27日

[11]公开号 CN 1183198A

[22]申请日 96.4.2

[30]优先权

[32]95.4.3 [33]US[31]08/415,617

[86]国际申请 PCT/US96/04165 96.4.2

[87]国际公布 WO96/31982 英 96.10.10

[85]进入国家阶段日期 97.10.29

[71]申请人 亚特兰大科技公司

地址 美国乔治亚

[72]发明人 霍华德G·平德

安东尼J·瓦斯莱维斯特

[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

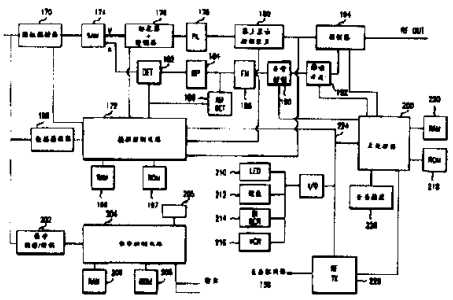
代理人 范本国

权利要求书 3 页 说明书 19 页 附图页数 12 页

[54]发明名称 具有可重构存储器的信息终端

[57]摘要

本发明的信息终端包括保密微处理器及保密非易失存储器。按照其来源验证授权数据及用于收费信息服务的其他与服务提供者有关的数据之类的数据，并根据需要由保密处理器按照服务提供者的密钥对其中的部分数据进行解密，然后装入保密非易失存储器。由多服务提供者或由用户本身装入保密数据，对各服务提供者适当分配具有预定长度的若干个非易失存储单元。按照这种方式，可保存不充裕的非易失存储器资源，并能使多信息服务提供者按照需要或根据需求的变化更容易地得到存储器资源。



权 利 要 求 书

1. 一种信息终端，包括：数据接收器，用于接收命令和数据；处理器，用于解释该命令和数据；及可重构存储器，用于响应处理器，并根据信息提供者的要求将多个数据块存储在存储块内；对上述各信息提供者至少分配一个存储块，并将所有未被分配的存储块与一个空表链接。

2. 根据权利要求 1 所述的信息终端，其特征在于：上述可重构存储器由非易失存储器构成。

3. 根据权利要求 1 所述的信息终端，其特征在于：上述处理器由保密微处理器构成。

4. 根据权利要求 1 所述的信息终端，其特征在于：上述数据接收器接收分别按该信息终端编址的数据。

5. 根据权利要求 1 所述的信息终端，其特征在于：上述至少一个存储块包含与服务提供者有关的数据。

6. 根据权利要求 5 所述的信息终端，其特征在于：上述与服务提供者有关的数据包含从实体接收的服务提供者密钥。

7. 根据权利要求 5 所述的信息终端，其特征在于：上述与服务提供者有关的数据包含服务提供者标识符。

8. 根据权利要求 5 所述的信息终端，其特征在于：上述与服务提供者有关的数据包含对信息服务用户的服务授权数据。

9. 根据权利要求 1 所述的信息终端，其特征在于：上述命令和数据包含用于接收和存储对服务提供者的认证密钥数据的第 1 命令。

10. 根据权利要求 9 所述的信息终端，其特征在于：上述命令和数据包含授权该终端从服务提供者接收编址信息的第 2 命令。

11. 根据权利要求 1 所述的信息终端，其特征在于：上述各存储块具有预定长度。

12. 根据权利要求 1 所述的信息终端，其特征在于：上述可重构存储器还用于存储与电子签名的验证有关的数据。

13. 根据权利要求 1 所述的信息终端，还包括一个信息发送器，其特征

在于: 上述处理器用于对通过上述信息发送器输出的各信息产生电子签名。

14. 一种用于重新配置用户信息终端存储器的方法, 包括以下步骤:

接收用于存储对服务提供者的密钥认证的第 1 命令;

将上述密钥认证存储在终端存储器;

接收授权该信息终端从服务提供者接收信息的第 2 命令;

接收用于存储用于服务提供者的公用密钥的第 3 命令; 及

将上述公用密钥存储在用于服务提供者的终端存储器的一个存储块内, 该存储块从空存储块表获得。

15. 根据权利要求 14 所述的方法, 其特征在于: 将上述第 3 命令及随后的用于写入授权数据的命令以编址的方式从服务提供者向用户终端发送。

16. 根据权利要求 14 所述的方法, 其特征在于: 上述存储器是保密的, 上述授权数据用电子签名接收, 上述电子签名在存储前通过一个保密处理器验证。

17. 一种保密终端存储器, 包括: 多个具有预定长度的非易失存储单元, 各存储单元彼此用指针链接, 对该存储器的访问由保密处理器控制, 对特定的提供者至少分配一个上述的非易失存储单元, 并将未被分配的上述各个存储单元保存在一个空表内。

18. 根据权利要求 17 所述的包括保密终端存储器的保密处理器, 上述保密处理器用于从包括电子签名的特定服务提供者接收通信, 并根据通信认证将授权数据写入该保密终端存储器。

19. 根据权利要求 17 所述的包括保密终端存储器的保密处理器, 该处理器用于将以用户电子签名传输的与服务提供者有关的数据输出到该特定的服务提供者。

20. 根据权利要求 19 所述的保密处理器, 其特征在于: 上述与服务提供者有关的数据包含服务购买数据。

21. 一种传送用于收费信息系统的与收费信息服务有关的数据的通信方法, 包括以下步骤:

由受托实体存储密钥认证;

对收费信息终端验证收费信息服务提供者的身份识别符; 及

响应验证步骤，由收费信息终端从该信息服务提供者接收信息。

22. 根据权利要求21所述的方法，其特征在于：来自信息服务提供者的上述信息包括按照该信息服务提供者的密钥加密的数据，并且，上述信息的解密在该收费信息终端的保密处理器内进行。

23. 根据权利要求21所述的方法，还包括产生用于向该信息服务提供者传输的信息的步骤，该信息包括用户的电子签名。

24. 根据权利要求21所述的方法，还包括以下步骤：由服务提供者从该终端接收信息；按照其来源验证该信息；及对所接收信息的加密部分进行解密。

说　　明　　书

具有可重构存储器的信息终端

本发明总的来说是涉及具有可重构存储器的信息终端，更具体地说是包括具有可在多信息服务提供者的控制下通过中央单元重构的保密授权存储器这样的用户终端单元的收费信息系统。

在收费电视系统之类的信息系统中可由用户利用的信息容量和专题节目的数量在不断地增加着。例如，光纤网络的出现及与电信系统的链接几乎能够向用户提供无限的信息和专题节目。收费电视系统已经使用于编址信息传输、按收视付费编程、即兴式按收视付费编程、最受欢迎的信道专题节目、及亲体控制。有线电视系统的工作人员还可以提供图文服务，如象新闻报道、体育比赛比分、证券市场行情、及天气预报等。也可以提供相当新的专题节目，例如，提供电视游戏演示、数字音响服务、广域网访问、家庭购物、旅游预约服务、家庭银行、能量消耗监视、电视会议、防盗防火报警、以及其他服务项目。

各种各样的每一项服务可以由不同的服务提供者提供，例如. 能量消耗监视由公用事业部门(煤气/水/油)、数字音响服务由数字音响服务提供者、游戏服务由游戏服务提供者、证券报价服务由证券行情自动收录机服务提供者、家庭购物服务由商品目录供货商、电影服务由按收视需求服务的供给商提供等。这些服务中的每一种都可以提供以记账方式收费的服务，因此就需要有允许或拒绝向用户提供服务的能力。此外，这些服务的某些提供者，可能需要更有刺激性地向用户授权他们的服务的能力。例如，应使用户能观看他们选择的电影而不必事先从服务提供者预订该电影。

这种即兴的按收视付费服务，一般需要一条通向服务提供者的回程通道，以通报所购买的信息服务。在直接入户、直播卫星、有线电视或其他熟知的系统中，一般使用电话回线。美国专利 No. 4792848 、 5053883(终端轮询法)、以及 5270809 说明了电话回程通道。在同轴电缆、光纤系统及其组合中，其电缆可以例如以射频提供回程通道。在一个由美国专利

No. 5109286、5142690、5155590、5225902、5235619、5251324、及5255086说明的这样的系统中，利用了从用户到有线电视总端的的上游信道的一个或多个波段。对数据信道进行选择，以避开有噪声的信道或波段。仅在美国专利No. 5341425中说明了为传输到接收位置而在多个发射位置加密的数据。

所有这些服务最好能得到保护，以防可能存在的非法服务接收者的侵害。在过去，一般采用加扰和加密法来保护所提供的服务不受非法接收者的侵害。为提供这样的服务保护，例如有线电视终端设备的制造商在设备中安装了微处理器和非易失存储器，其中有一个授权存储器可以保存或用新接受的服务等更新。虽然可以保护服务和编址命令的传输不受非法接收者的侵害，但非法接收者通常会找到破译服务项目的方式，例如通过设法访问非易失存储器来达到。但是，现有技术的这类系统，不能提供分别对多家希望他们的服务进入市场的服务提供者的访问。总是假定对所提供的例如有线电视服务等所有的服务只有一家供给商。另外，每家服务提供者都从一条或多条该服务提供信道沿着分设的数据通信信道单独地访问各独立的终端单元。

提供保密授权终端的一个解决方案是以必须用智能形式方能解密的加密格式发送授权数据。目前，已知有利用所谓的公用密钥/专用密钥加密系统和算法，在美国专利No. 4405829和5231668中分别说明了其中的两种，即RSA(在专利上署名的各发明人的最后首字母)和数字签名算法(DSA)。

另外，由于加密和加扰已成为保护服务不受非法接收者侵害的主要方法，所以最好是能保证有关的授权信息等按其来源验证。例如在Houser等的题为“电子文件检验系统和方法”的申请号为08/306447的未决美国申请书中说明了一种方法，利用它可以通过在签名电子文件中嵌入保密对象来验证和检验一个文件。由一个检验处理器验证或检验该电子文件中的“签名”。文件本身和(或)保密信息可以加密以保护该保密信息，或也可以不加密。此外，保密信息还可以包括文件摘要和(或)签名摘要，前者包括一个散列值，而后者、即保密系列号对每个保密对象是唯一的。

有线电视设备制造商通过提供扩充存储器、例如以包括这类存储器的所谓的灵巧卡的形式解决存储容量有限的问题。通常，当存储要求增加时，

按这种方式能使存储器的大小变得适用。例如,Bowen 等于 1994 年 11 月提出的美国专利 No. 5367571 说明了一种带有扩充槽的收费终端,该扩充槽适合于安放这种包括可编程存储器的灵巧卡。该存储器例如可以用于特殊制图功能、控制软件或其他功能。在 1992 年 12 月 1 日提出的题为“可重编程序的用户终端”的申请号为 07/983909 的未决美国专利申请书中,说明了一种可重编程序的用户终端,其中,每个 EEPROM 存储器的 16 个 24 字节容量页面可以由有线电视总端编程。

在 Kauffman 等的美国专利 No. 5003591 中公开了现有技术的可重构终端的一例。该专利说明了一种带有可远程修改功能的有线电视转换器。固件可沿有线电视网络下载。如果不向终端下载固件,则可将非易失存储器与一个用于存储缺省操作程序的处理器联接。建议用于指令按收视付费程序的方法可以通过可下载固件修改,或可以通过增加一个异步数据端口并通过可下载固件控制公用数据的检索,提供公用计数器读数。

在信息译码设备中,还已知通过可插入译码器的所谓灵巧卡进行解密的方法。在美国专利 No. 5029207 和 5237610 中说明了用于使服务解密的灵巧卡。

在上述参考资料中没有任何一份资料涉及到保护有价值的非易失存储器,也没有一份资料提出具体的实现性解决方法,能以有效的方式适应多家服务提供者的不同需要和要求。如果多家服务提供者能够单独地访问和利用在收费信息终端的同一存储器资源,显然是最为理想的。此外,这种存储器资源最好能得到保护,不使其受到那些极力地想找机会不花钱就得到服务的非法接收服务者们的侵害。

本发明涉及将在有线电视总端的控制下能以可编址方式重构的存储器包括在信息终端内。该存储器最好是保密的和非易失的,并且其访问由保密处理器控制。并且,该保密终端存储器可以由多家服务提供者分别访问,以便能使其各自只需使用为其目的所需的存储容量。正如本文将说明的,一个服务提供者只要由受托实体对用户终端进行了验证,则该服务提供者就直接与该用户终端进行信息通信,而无需有线电视总端或受托实体的介入。此外,当服务提供者和用户各自分别提出他们的改变要求时,可以通过被称作链接表的处理对存储器分别进行分配和重新配置。在这种处理中,按照要

求将存储块从分配给空表的状态恢复。

因此，按照本发明的信息终端包括：数据接收器，用于从一个实体和信息提供者接收命令和数据；处理器，用于解释该命令和数据；及可重构存储器，用于响应处理器，并根据信息提供者的要求将多个数据块存储在存储块内；对上述各信息提供者至少分配一个存储块，并将所有未被分配的存储块与一个空表链接。存储块最好具有预定的长度，例如，包括状态和指针的 4 个字节在内其数量级约为 40 个字节。存储块的一个类型字段为一个服务提供者指明下一个存储块、为下一个服务提供者指明第 1 个存储块、或指明存储块的空表。存储块可以包含服务提供者的描述性信息，内容包括签名数据和加密/解密密钥、大型等级图、大型程序图、小型程序图，其中还包括单个程序授权及用户启用的事务处理数据，例如，即兴式按收视付费事件的授权。按这种方式，可以将一个容量不充裕的资源、即保密微处理器的非易失存储器动态地重新分配，以满足服务提供者的变化的要求。

通过配合附图阅读以下的详细说明，将能深入地理解本发明的上述和其他特点及优点。

图 1 是本发明的信息系统的概括性的框图。

图 2A、 2B、 2C 和 2D 是可在其中实现本发明的收费电视系统的框图。

图 3 是图 2C 所示的用户终端单元 160 的详细框图。

图 4A 示出包括类型/状态字节的典型的基本存储块或非易失存储器的存储单元(NVSC)；图 4B 提供一个包含类型字节和状态字节的数据的例；图 4C 提供一个类型字节的类型值的例；图 4D 提供状态数据的典型值。

图 5 是表示作为例子提供的多个存储块类型的每一个的定义的图表。

图 6 是多家服务提供者访问图 3 的用户终端单元用的典型链接表的框图。

图 7 是表示图 6 的特定存储器的结构例和其他例的图表。

图 1 本发明的信息系统 10 的概括性的框图。信息系统 10 可以是模拟的、数字的或表示模拟和数字技术的组合。该信息系统 10 包括一个信息分配中心 12，用于接收来自一个或多个远距离设置的信息服务提供者(SP) 14-1、...、 14-n 的信息，并将该信息向终端单元 16 提供或播放。本文中所用

的“信息”包括(但不限于)模拟视频;模拟声频;数字视频;数字声频;诸如新闻报道、体育比赛比分、证券市场行情、及天气预报等图文服务;电子信息;电子程序指南;数据库信息;包括游戏程序的软件;家庭购物商品目录;能量消耗监视服务;报警服务及广域网数据。此外,信息分配中心 12 还可以局部产生信息并将该局部产生的信息提供给终端单元 16 。

按照本发明,信息分配中心 12 可假定是一个所谓的受托实体,用于登记为服务提供者所专用的信息。尤其是,假定服务提供者分别将密钥认证和公用密钥委托给受托实体。该密钥认证用于验证密钥的有效性。该受托实体应以保密的形式保护该信息不受其他服务提供者和非法服务接收者的侵害。在受托实体与一个特定用户的收费信息终端之间的开始的一两次事务处理中,该受托实体向该终端证实服务提供者的身份及他们的密钥,并传送一个传输数据流标识符,沿着该数据流进行预期的通信。从受托实体到该家庭通信终端的信息,最好由受托实体签名,并通过在系列号 08/306447 的美国申请书中说明的处理或其他已知的处理验证他们的签名。所有这些信息或从中选择的部分,可以加密通信,并由本发明的保密微处理器进行解密。有关服务提供者的其他信息可以明文传输(他们的地址、标识和图形数据等),但为开始提供或授权服务并不需要这种数据。按照这种方式,根据服务提供者的被证实的公用密钥及相应的用户个人的专用密钥,可以接收由各服务提供者向特定的服务用户发出的授权、验证他们的签名、进行部分解密并存储数据。

由信息分配中心 12 向终端单元 16 发送的信息,包括编址的信息,该编址信息包含由终端单元 16 接收和解释的命令和数据。该命令和数据可以包含例如由受托实体为新的服务提供者存储密钥认证的命令。上述密钥认证最好是保存在非易失的保密存储器内。

信息分配中心在第 1 命令和数据之后接着发送一个授权该终端直接从该服务提供者接收信息的命令。可以由该命令规定最多分配给该服务提供者的终端存储器的的存储块数。

在这之后,服务提供者可以通过编址的通信信道与该用户终端直接通信。这种通信可以如图 2b 所示通过受托实体提供,或如图 2C 所示通过公用或专用的交换或非交换网络、或网络的组合提供。服务提供者通过信息分

配中心12向终端发送一个在本文中有时称作多重会晤密钥(MSK)的密钥，存储在终端存储器内，最好是存储在保密的非易失存储器内。

随后从服务提供者发来的命令，最好是指令提供某些带有签名的服务授权，并可以有选择地以用户的公用密钥加密。然后，在接收这些命令时，仍使用用户的专用密钥解密，并将授权数据存储在保密存储器内。

图2A、2B、2C和2D是可在其中引入本发明的收费电视系统的框图，可以是模拟的、数字的或者是模拟和数字技术的组合。当然，本发明可以应用于不同于收费电视系统的信息系统，而且本发明在这一点上不受限制。收费电视系统100向多个用户位置、例如120-1、...、120-n(见图2C)提供信息。该信息可以包括(但不限于)模拟视频；模拟声频；数字视频；数字声频；诸如新闻报道、体育比赛比分、证券市场行情、及天气预报等专题服务；电子信息；电子程序指南；数据库信息；包括游戏程序的软件；及广域网数据。参照图2A，收费电视系统100包括多个信息提供者114-1、...、114-n，其中每一个都可以提供一个或多个用于进行上述识别的信息类型。例如，信息提供者114-2包含一个信息源115，用于向发送器118提供模拟电视信号。发送器118与发射模拟电视信号122-2的卫星上行链路121联接。信息提供者114-1和114-3分别从信息源115向产生用于发送编码数据流的各编码器116提供数字信息。信息提供者114-1和114-3的信息源115可以是用于存储信息的光存储器之类的存储器。如果各信息提供者114-1和114-3的任何一个提供各种信息，例如，多个不同的游戏程序、或不同类型的图文服务、或多个数字电视或声频程序，则编码器116可以多路复用该信息，以产生用于发送的多路复用数据。来自编码器116的数据流供给发送器118，进而供给到卫星上行链路121。作为图2A的例子，由信息提供者114-1操作的编码器116产生数字信号122-1，由信息提供者114-3操作的编码器116产生数字信号122-3。各信号122-1、122-2、122-3通过卫星123发送到有线电视总端装置125(见图2B)。在本发明的系统中，当然可以有许多信息服务提供者，因此，可以通过卫星123向有线电视总端装置125所在的位置发送多个信号。在图中虽未示出，但也可以在有线电视总端装置以外的位置接收信号，例如，在直播卫星(DBS)的用户位置。此外，虽然在信息提供者与有线电视总端装置之间的链接如卫星链路所示，但本发明在这一点上并

不受限制。因此,例如,该链路可以是同轴电缆、电话网络、卫星系统、射频(RF)链路、或光纤或者是其任意的组合。另外,虽然图 2A 的信息提供者的位置远离有线电视总端装置 125,但其中一个或多个信息提供者实际上也可以与有线电视总端装置 125 位于同一地点。

各信息服务提供者最好本身具有其唯一的服务提供者标识符,还要有自己的公用密钥,即如上所述,委托给能够操作有线电视总端装置 125 的受托实体的密钥。此外,服务提供者保留有自己的专用密钥。同样,各用户亦具有公用密钥和专用密钥。彼此间发送的信息可以签名或精确验证。应按用户分别编址的数据最好采用使非法服务接收者不可能复制的密钥加密。该数据可以包括用密钥加密的服务授权数据,最终由保密微处理器接收、解密后,存储在保密的非易失存储器内,按照本发明,即存储在预定长度的各非易失存储单元(NVSC)内。

概括地说,服务提供者或用户可能关心两个问题:(1)通信的保密(例如,为防止非法接收等)和(2)验证,即无损害地接收文件、信息或数据,并按其来源进行验证(或检验)。按照本发明,家庭通信终端的同一保密微处理器或控制器,能够以经济地利用程序存储器的方式同等地用来达到验证和保密目的。

参照图 2B,在有线电视总端装置 125 处的卫星下行链路 124,提供接收的信号 122-1、122-2 和 122-3。有线电视总端装置 125 用作通信中枢,与各信息提供者接口联系,并根据附加条件的基础将其与用户位置 120-1、...、120-n 连通。此外,有线电视总端 125 可以是上面提到的受托实体的位置。例如,所接收的数字数据信号 122-1 供给接收器 126-1,然后供给到调制器 128-1,在这里将其调制到相异的电缆信道。调制器 128-1 可采用任何适用的调制方法,如象正交部分响应(QPR)调制。所接收的模拟电视信号 122-2 供给接收器 126-2,然后供给用于加扰的加扰器 130,进而供给到调制器 128-2,在这里将其调制到相异的电缆信道。正如将在下文中讨论的,加扰器 130 还将带内数据插入模拟电视信号 122-2。显然,对于从其他本地的或远程的信息提供者(图中未示出)接收的数字和模拟信号,同样可以提供另外的接收器、调制器,也可以有选择地提供加扰器。此外,虽然在有线电视终端的范围内说明了本发明,但本发明也可以适用于直接入户卫星终端、直

播卫星终端、数字声频服务终端或其他用户信息终端。

所接收的数字数据信号122-3提供给信息信号处理器(ISP)142,使其可用所谓的带内或带外传输方式传输。来自其他信息提供者的其他数据流(未示出)也可以提供给ISP142。ISP142用于接收一个或多个数据信号,然后如下文所述将数据传输到用户终端位置。ISP142将数据提供给加扰器130。ISP142可以根据要传输的数据量及提供和更新数据时所应有的速度等因素,将数据提供给其他加扰器。数据由加扰器130反复发送。如果只有一个加扰器而数据量很大,则重复速率将变得缓慢。使用一个以上的加扰器,可以使数据的重复速率提高。

具体地说,加扰器130在对相关的模拟电视信号122-2加扰的同时,将数据置于带内,以便向用户传输。在一种配置中,将数据置于电视信号的垂直消隐期内,但也可将数据置于其他位置,而在这一点上本发明不受限制。例如,一种熟知的方式是将数据按伴音载波调幅。如本文所述,带内传输意味着数据在由声频和视频载波组成的视频电视信道内传输。因此,来自ISP142的数据可以通过按伴音载波调幅进行传输,即下文中的带内声频数据,也可在模拟电视信号的垂直或水平消隐期内传输,即下文中的带内视频数据。ISP142也可以配置成在供给数据时在未用部分中传输一个数字数据流,例如MPEG压缩视频数据流。

ISP142也可以局部接收和(或)产生传输到用户的涉及即将到来的事件或服务中断或改变的信息。这类信息不需要加密。如从信息提供者接收信息,则由ISP142按收到时的状态或更改后的格式传送信息,然后供给加扰器130,以便传输到用户。此外,按照本发明,特别敏感的信息,如象服务授权信息,最好在传输到用户之前,以服务提供者规定的前提进行加密。

ISP142也可将信息传送到与加扰器130及带外传输器134连接的有线电视总端控制器(“HEC”)132。虽然HEC132如图所示连接于同一个加扰器130,但事实上HEC132可以连接于一个或几个不同的加扰器。HEC132可以简便地采用Scientific-Atlanta8658型,用于控制向加扰器130及带外传输器134的数据传输。如上所述,加扰器130将数据置于带内,以便向用户传输。带外传输器134按分立的载波、即不是在信道内传输信息。在一种实施方案中,带外载波为108.2MHz,但也可采用其他带外载波。在HEC132

控制下传输的信息,例如可以是解扰数据。在一种配置中,将信息插入各垂直消隐期,用于指示在下一视频字段中采用的加扰形式。加扰系统在技术中是众所周知的。例如,可采用同步抑制加扰、视频反转加扰等,或采用加扰技术的某种组合。

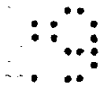
按照本发明,授权信息可采用电子签名,而加密传输部分由保密终端处理器接收。授权信息允许用户接收某些信道、事件、程序或服务等级。如本文所采用的,程序通常是指具有预定信道和时隙的收费信息服务,但该概念可以推广到包括销售计划等信息服务。等级用来规定服务的水平,例如,包含多路数据信道和时隙。等级的一个例子可以是拱廊游乐中心式游戏播放,使用户能在较长的时间、例如星期六玩任何电视游戏(多路游戏信道)。事件可以以信道和时隙等的形式规定,而信道可以是低速数据信道(用于证券行情自动收录机服务)或用于高分辨率电视和环绕声的高速数据信道。

来自 ISP142 和 HEC132 的信息,也可以作为带内声频或视频数据通过数据重发器、例如 Scientific-Atlanta8556-100 型数据重发器沿着不加扰信道传输。

某些传输信息是全局的,即传送到每一个用户。例如,解扰数据可以是全局传输。应注意到,并不能只是由于每个用户可接收解扰数据就意味着每个用户都能对所收到的信号解扰。相反,只有被授权的用户终端单元才能对所收到的信号解扰。另一方面,某些信息传输可以是编址传输。例如,授权信息通常可以对单个的用户编址。就是说,当传输时,数据具有与之相关的地址(例如,用户终端单元系列号)。被编址的用户终端单元接收信息并当其地址与信息中所含地址相符时,作出相应的响应。其他用户终端单元不能接收该数据。另外,还可以有成组编址数据,将影响到成组的用户终端单元。

调制器 128-1 、 128-2 、任何其他调制器、及带外传输器 134 的输出,供给组合器 136,该组合器 136 将各单个信道组合成一个单一的宽带信号,然后通过分配网络 138 发送到多个用户位置 120-1 、...、 120-n(见图 2C)。分配网络 138 例如可以包括一个或多个光发送器 140 、一个或多个光接收器 142 、及同轴电缆 144 。

如图 2B 所示,收费电视系统 100 包括分别向特定城市或地理区域中的地点提供信息的多个有线电视总端装置。可以提供中央控制装置 146 配合



收费电视系统 100 中的各个有线电视总端装置的操作。中央控制装置 146 往往与多服务操作员的中央局相联系，可以与许多城市中的有线电视总端装置通信并对其进行控制。中央控制装置146包括一台系统控制计算机148，用于指挥中央控制装置146的其他部件。按照本发明，控制计算机146一般对任何信息提供者的专用信息、例如密钥认证、密钥及标识符进行保密，而且，同样可以与有线电视总端装置125组成本发明的受托实体。系统控制计算机148的一个例子是Scientific-Atlanta系统管理程序10的网络控制器。中央控制装置146，例如可以为服务提供者提供记账服务，包括按收视付费事件的记账。用一台记账计算机150存储记账数据，并可以按不同格式打印帐单。在系统控制计算机148与HEC132之间的通信，可以通过调制解调器进行，尽管本发明并不受这一点的限制。授权数据可以从系统控制计算机148传送到HEC132。然后，HEC132将授权数据编排格式，并如上所述，通过加扰器130以带内形式或通过带外数据传输器134以带外形式将格式化的授权数据传输到用户终端单元。

有线电视总端装置125还包括一个RF处理器152，用于从用户位置120-1、...、120-n接收回程通道的数据通信。另外，回程数据通信可以通过电信设施接收，并可利用电话处理器(图中未示出)。这些数据通信可以包括对购买即兴式按收视付费的记账信息，可以直接送到系统控制计算机148，还可以包括对由有线电视总端装置125保持的数据库信息的请求。例如，数据库服务程序154、例如Oracle(商标名)数据库服务程序可以提供对诸如百科全书、图册、词典等的访问。用户请求可从RF处理器152送到信息请求出器156，以便访问该请求信息的数据库154，并如上所述将该请求信息例如通过编址的带内或带外事务送到请求用户。此外，信息请求处理器156还可以访问通信网络158，以便提供用户对因特网等服务的访问。

随着在有线电视总端装置125与用户位置之间所传输的数据量的增加，所增加的使用量将可能由带外和数字传输组成。例如，可将50MHz的带宽专用于正向信道(至用户终端单元)和反向信道(自用户终端单元)两者的数字数据(非视频)传输。也可将200MHz或200MHz以上分配给数字视频，而将300MHz～500MHz分配给模拟视频。因此，尽管以上举例说明了各种传输方法，但本发明在任何方面都不受在有线电视总端装置与用户位置之间的传

输方式的限制。

以上对图 2B 系统的说明意味着本发明可以适用于所说明的模拟/数字系统的组合。同样,本发明可以修改为早已熟知的可看作是模拟系统的系统。现在来参照图 2C,图中所示的数字系统,通过公用或专用的交换或非交换的交互式数据网络、或这类网络的组合进行在服务提供者与受托实体之间、服务提供者与用户(家庭通信终端)之间的通信以及其他的可能通信的组合。按照图 2C,多个服务提供者 SP1 、...、 SPn 通过以云状图示出的交换或非交换的交互式数据网络与受托实体及多个家庭通信终端 HCT1 、...、 HCTn 进行通信。一般,在这类网络中,例如可从 SP1 至 HCT2 编址传输例如在异步传输模式(ATM)标准下的那些操作及包括标题的数据包,而不特别重视该数据包到达其目的的方向和路径。在接收器、例如家庭通信终端中,在接收数据包时,应验证签名、按需要解密、并根据嵌入的控制数据或在程序存储器内存储的预定算法进行适当地操作。此外,可收集多个数据包,并重新修改其顺序,使其可以作为一个信息按该顺序一起中断,然后再进行操作。换句话说,先发送的数据包 1 事实上是否是相对于有关的数据包 2 最后接收的,这对一个接收器来说没有任何关系。接收器可以编程,使其收集所有相关的数据包的数据,并在数据包丢失时或不能按 ATM 或其他协议精确验证时,确认不能接收。当然,除 ATM 以外,也可以采用从本发明的角度来看更为有利的其他数据通信协议。此外,应该知道,任何受托实体、服务提供者位置、或家庭通信终端位置都可以是发送器或接收器;而且,可能包括多个数据包的信息可以按组或以全局方式编址。

参照图 2D,各用户位置 120-1 、...、 120-n 包括与分配网络连接的用户终端单元 160 。本文中使用的“用户位置”,是指相对于有线电视总端装置 125 位于远距离的任何位置。按照本发明,用户终端,例如可以位于家庭、教室、医务室、或办公室。各用户终端单元 160 可以与一个或多个装置 162-1 、...、 162-n 联接。装置 162-1 、...、 162-n 可以包括能够按照用户提供的命令操作的装置,但本发明在这一点上并不受限制。因此,该装置可以包括电视机、立体声接收机、盒式磁带录像机(VCR)、盒式录音机、光盘(CD)播放机、视盘播放机、电视游戏机、个人计算机、能量控制器等。这些装置中的某些装置可以连接在一起操作。因此,如图 2D 所示,装置 162-1

与装置162 -2连接。例如,装置162-2可以是电视机,而装置162-1可以是盒式录像机。为进行讨论,将假定装置162-1是盒式录像机而装置162-2是电视机。一个或多个装置162-1、...、162-n可以与用户终端单元160的开关电源插座连接,从而使用户终端单元160能够从内部对这些装置进行通断切换。远距离控制单元166沿着通信链路168将信息传送到用户终端单元160。通信链路168可以是(比方说)红外链路。

图3是表示出模拟和数字技术的组合的用户终端单元160的详细框图。图3的终端只是一个能有效利用本发明的终端的典型例。一个典型的全数字终端是将所有模拟信道的调谐去掉并通过ATM、时分多路复用(TDM)、脉码调制(PCM)、频分多路复用/TDM组合系统、及其他有关的数据传输装置或其组合接收数字服务数据及相关数据的终端。

来自通信网络138的宽带信号供给模拟调谐器170、数据接收器198、及数字调谐器202。模拟调谐器170和数字调谐器202可按由用户所选信道调谐。例如,模拟调谐器170可在54MHz的频率范围上调谐,并能调谐到预定的"未用信道",以便在关掉电视机160-2时接收带内数据。这种所谓的未用信道可以由系统控制计算机148(见图2B)预先设定,识别预定信道的数据可以用上述的任何一种数据传输方法传送到用户终端单元160。未用信道识别数据可以存储在用户终端单元160的存储器内。在给定时间内最好仅使模拟调谐器和数字调谐器中的一个工作。

模拟调谐器170使用在模拟控制电路172控制下的锁相环路,用于将所选的或预定的未用信道信号转换为45.75MHz的中频(IF)信号。模拟控制电路172,例如可以是专用的集成电路(ASIC),用来将多个用户终端单元的控制与数据处理功能合并成一个单一的电路。当然,模拟ASIC可以包括单个控制电路的任意组合。另外,也可使用其他控制电路,例如微处理器。模拟控制电路172具有相联的RAM196和ROM197。

滤波器174、例如SAW滤波器用于对来自模拟调谐器170的IF信号进行滤波,将该信号分成用于处理的独立的视频和声频部分。该视频部分由在模拟控制电路172控制下的视频解调器和解扰器176进行解调和解扰。例如,如采用了同步抑制加扰,则视频解调器和解扰器176可以进行视频恢复。然后,将该视频信号通过带通滤波器178传送到幕上显示控制装置180,

如需要时，在这里使视频反转加扰反转(解扰)。视频信号的解扰，不管是同步抑制、同步反转、视频线反转等，都在模拟控制电路172控制下进行。因此，模拟控制电路172向幕上显示控制装置180供给任何必要的定时信号、反转轴电平、及该视频是否反向的信息，并向视频解调器和解扰器176供给任何必要的定时信号、恢复电平、及所恢复的同步脉冲的识别。模拟控制电路172，例如从作为带内声频数据的脉冲或从在垂直消隐期间按视频调制的数据接收用于实现这种控制的解扰数据。

在另一通道，由同步检测器182将该声频信号转换为4.5MHz的内部调制频率。对同步检测器182的自动增益控制的反馈由带通滤波器184的输出供给。调幅检测器186进行脉冲检测，以便将调幅后的带内声频数据恢复为声频载波。所检测的带内声频数据供给模拟控制电路172。除了解扰数据外，该带内声频数据为进行缓冲而存储在RAM196内。解扰数据则直接由模拟控制电路172访问，以进行上述的解扰操作。来自带通滤波器184的声频信号由FM解调器188解调。声频信号的音量控制，例如可在作为参考引用的、和本发明一共转让的美国专利No.5054071中说明的音量控制电路190及主处理器200的控制下进行。在音量控制后，将该声频信号供给在主处理器200控制下的静噪开关192。静噪开关192的输出供给调制器194。

幕上显示控制装置180的输出供给模拟控制电路172，用于从该信号的消隐期间检测带内视频数据。模拟控制电路172将该检测数据在由主处理器200处理之前存储在RAM196内。如上所述，任何解扰数据可由模拟控制电路172直接访问，以便进行上述的解扰操作。在已知的于1994年4月提出的题为“可同时显示多种服务的收费电视系统及终端”的系列号08/229805的未决申请书中，可以找到检测这种带内视频数据的其他详细说明。另外，可从有线电视总端装置125发送日历数据，并存储在例如RAM196内。例如，可以按照在作为参考引用的已知美国专利No.4994908中所说明的，根据卫星时间标准周期地进行全球日历传输。因此，主处理器200可访问当前的日历信息。

幕上显示控制装置180有选择地产生幕上字符和图形显示，以代替或覆盖视频信号。例如，可以将存储在RAM196或ROM197内的信息读出到幕上显示控制装置180，并用于产生幕上字符和(或)图形。调制器194将幕上显示

控制装置180的输出和来自静噪开关192的输出端的声频信号组合，并将该组合信号转换为由主处理器200选择的信道频率，例如信道3或4。将该组合并重新调制的信号作为RF输出以众所周知的方式供给到VCR162-1和(或)电视机162-2。

输入宽带信号还供给带外数据接收器198，用于接收命令和数据。带外数据接收器198将所接收的带外信号供给模拟控制电路72。该数据可存储在可由主处理器200访问的RAM196内。

输入宽带信号还供给可在例如从400到750MHz的范围调谐的数字调谐器/解调器202，并按照用户的选择进行调谐。数字调谐器/解调器202用于调谐到数字数据信道。一个可以包括数字ASIC的数字控制电路204用于恢复和处理在被调谐数字数据信道上的数字数据，并将对应的模拟和(或)数字输出信号供给装置162-1、...162-n中的一个。另外，该被恢复的数字数据可以由装置162-1、...162-n中的一个进行访问。例如，如果该数字数据包括数字声频数据，则可以将对应的模拟输出信号供给扬声器。如果该数字数据是电视游戏数据，则电视游戏机例如可通过电视游戏机端口(未示出)访问存储在RAM206内的该被恢复的数字数据。如果该数字数据包括数字电视数据，则可将对应的模拟输出信号供给VCR162-1和(或)电视机162-2。如果该数字数据包括软件程序，则个人计算机可以通过一个串行端口访问被恢复的软件程序。可以用于恢复和处理数字数据的数字控制电路的细节，可在以下文献中找到：Rovira的已知美国专利No.5239540；题为“用于游戏演示服务的保密授权、控制方法及仪器”的申请号08/352162的共同被转让的美国申请书；及题为“用于远距离传输的多个数字程序服务的多路复用系统和方法”的系列号07/970918的共同被转让的美国申请书。这里引用这些专利和申请书分别供参考之用。数字控制电路204还具有相联的RAM206和ROM208。

数字控制电路204还联接着包括保密非易失存储器的保密处理器205。一般，由公用密钥支持的保密微处理器具有大约4　字节的板上非易失存储器。这种容量值作为例子用于说明本发明的特点，从而使上述非易失存储器是可重构的并能有效地利用。本发明对保护较大或较小的存储器都同样能有效地利用。在作为例子的4千字节存储器中，有些留作存储专用密

钥、控制算法等。剩下的空间留给大约 80 个预定长度、例如 40 字节的非易失存储单元(NVSC)。此外,这种分配只作为例子,也可以大于或小于 80 单元,每个单元可以大于或小于 40 字节(可以是 100 单元、每单元 32 字节;60 单元、每单元 50 字节,或根据本发明的应用场合的其他配置)。此外,程序存储器对例如在信息验证上的电子签名及密钥解密都能有效地进行分配。

处理器 205 最好是与图 3 的终端的其余部分设置在同一外壳内,但在另一实施例中,可以包括一个如作为参考引用的已知美国专利 No. 5029207 及 5237610 中所说明的灵巧卡或另外的保密处理器/存储器。这种灵巧卡可插在适合于其插入的槽内,并能以磁、光或其他方式读出或写入。

数字调谐器 202 、数字控制电路 204 、 RAM206 、及 ROM208 是按与其他电路集成在一起示出的,但这些部件也可以按单个、组合、子组合的形式作为添加单元或附带单元提供,并通过连接于处理器总线 224 的扩充槽与主处理器 200 连接。在任何灵巧卡、附带单元或终端实施例的内部部件中,命令和数据的加密和解密都在处理器 205 内进行,其中的数据以明文形式存储。保密处理器的特征之一是,只要非法接收者企图侵入处理器试图得到其中的数据,则存储器可能受到损失,而当然该处理器在功能上可以使其不工作。

用户终端单元 160 还包括用于显示例如信道数等信息的 LED 显示器 210 、用于输入用户命令的键盘 212 、用于从远距离控制装置 166 接收命令的红外接收器 214 、及利用例如 IR 信号向 VCR162-1 发送命令的 VCR 控制装置 216 。 RF 发送器可由主处理器 200 控制,用于沿着分配网络发送回程传输数据。这些回程传输数据可以根据用户供给的输入产生,用于从有线电视总端装置 125 处的数据库请求信息,并用于将有关即兴式按收视付费服务的购买记账信息传送到系统控制计算机 148,而后者最好按照本发明进行加密,并存储在处理器 205 内。开关电源插座 226 可以有选择地向所插入的一个或多个装置 162-1 、...162-n 供电。

主处理器 200 最好采用 PoworPC(商标名)微处理器,并用在存储器(例如,ROM218 和 RAM220)内存储的程序代码及从有线电视总端装置 125 下装的数据控制用户终端单元 160 的整个操作。

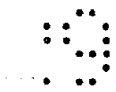
现在来参照图 4A ~ 4D,进一步详细说明图 3 的保密处理器 205 的保密

非易失存储单元(NVSC)。首先参照图 4A,图中示出一典型的 NVSC 或预定长度的存储块,例如 40 字节非易失存储器,例如保密微处理器 205 的 EEPROM。这是一种可以预定为任意长度的软件结构,40 字节只是一个例子。为便于存储器的存取,NVSC 最好是一组相连字节。一个字节可以包含一个将结合图 4B 进一步说明的用于类型和状态的共享字节。另一字节可以作为备用或保留字节。后面接着的是数据的 36 个字节。最后是指向所分配的或空存储块表中的下一个 NVSC 的指针。

全部有效的 NVSC 彼此链接。总是存在一个保持在最好是相连的 NVSC 阵列之外的指向第 1 个有效 NVSC 的指针,而每个有效 NVSC 都指向表中的下一个 NVSC。在最后的 NVSC 中的指针保持 0xFFFF 的值。同样,所有空 NVSC 彼此链接,带有一个指向空表上的第 1 个空存储块的外部指针。表上的第 1 空单元用外部地址指针查找。除了在存储块内已经存有数据时外,状态数据字段改为“写入”,然后其状态是“切换”。在 NVSC 被写入之后,状态数据字段改为“有效”。通过用后一单元的地址代替前一单元的指针,可将一个单元(NVSC)从链接表中去掉。

现在来参照图 4B,图中示出包含 8 个字节的典型的类型/状态字节。4 个字节包含将用图 4C 进一步说明的类型信息,另 4 个字节包含将用图 4D 进一步说明的状态信息。

参照图 4C,类型字段指示该块是什么类型的 NVSC 数据。存储块(NVSC)可以包括服务提供者 SP 描述符块、多重会晤密钥(MSK)块、大型等级图、(小型等级图)、大型程序图、小型程序图、单个程序授权表(例如,最多 8 个程序)或即兴式按收视付费事件表(例如,8 个事件)。数据的 4 个字节最多可提供 16 种选择。其他可能的服务授权及购买的 NVSC 可以考虑到用于不同的服务,例如数字游戏服务或数字声频服务。这些保密数据中的某些数据包括应防止非法服务接收者的侵害的授权和服务验收数据,并且必须返回服务提供者,供记账之用。本发明的一个优点是,用户的电子签名及以用户的密钥对这类与服务验收有关的数据进行的加密,可以在保密处理器内完成,并且,由于进行了加密,非法服务接收者可以接近的任何数据对该非法接收者来说都是难于破译的。在图 4C 中示出一种典型的配置,其中,类型值 0001 表示可由服务提供者提供的最多 256 级服务的大型等级图。分配给该大型



等级图 32 字节、 SP 标识符 2 字节、传输数据标识型符 2 字节，大型等级图利用 1 个 NVSC 。其他只是作为例子给出的 NVSC 类型值是用同样的方式定义的。类型值 0000 是错误指示器。类型值 0011 表示 4096 信道授权图的一小部分，相当于该图的 1/16 。其他配置可以考虑到本发明的不同应用。一种修改的 NVSC 类型表示于图 5 。

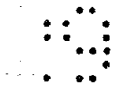
参照图 4D，状态字段指示存储块在给定时刻的状态。该状态可以是切换、可以是有效(即在使用中)、写入或空表的一项。在另一实施例中，类型和状态字节可以适当地例如允许类型数据的 5 位和状态数据的 3 位共享。此外，该字节共享的例仅仅是按照本发明的原理可以适用的一个例子。如本发明的例所示，状态值的最高位部分是无效的，因而可以是空位。

下面，将参照图 5 、 6 、 7 说明本发明的一例，首先，图 5 示出典型的 NVSC 类型。例如，服务提供者(SP)描述符块包含由标识符(2 字节)、 16 位的公用散列密钥、最多两个信道的授权(分别用 8 个字节、 4 个字节标识的两个信道)、其他 SP 特征(8 字节)及 2 个字节的指向下一个 NVSC 的 NVSC 指针。另外，信道授权可以位映射到用于服务提供者的预定数据信道，并可包括最多用于 64 个信道的位授权图。

另一个存储块可以用于存储对特定服务提供者的多重会晤密钥(MSK)。奇偶 MSK 可以进一步挫败非法接收者，如在技术中众周知的那样，各为 16 字节长度。在该同一存储块中可以存储服务提供者 ID 、及 2 个字节的传输数据流识别符(TS ID)，用于识别沿传输数据流接收的数据。

其他存储块的定义如图 5 所示(或在变形例中的图 4C)，例如，用于定义 256 级服务(大型等级图)、 4096 信道(大型)或 256(小型)、事先购买的事件及即兴式按收视付费事件。所购买的即兴式按收视付费事件是收费信息服务验收数据的典型例，最好是加密后例如通过回程通道装置、 RF 或电话以保密的方式传输。使用者或用户通过图 3 的终端在例如包括个人签名或个人话音识别的远程控制下登记服务验收数据(可以是家庭购物数据)。在已通过记账计算机 150(图 2B)得到确认、即服务验收数据已由该记账计算机成功地登记之前，这类数据最好不要擦去。

现在来参照图 6，图中示出一个链接表的例，用于说明可以怎样分配或重新分配容量不充裕的存储器。至此为止我们假定备有 80 个 NVSC，各具有



40 字节的预定长度。从受托实体接收一个单命令或命令集，以装入服务提供者描述块，并等待来自服务提供者的进一步的命令。来自受托实体的这些第 1 事务用于向收费信息终端证实该服务提供者是有效服务提供者，只要信息的完整性及受托实体的签名得到认证，就授权该终端直接从被验明的服务提供者接收通信。

一般，至少将空表中的一个存储块分配给在初步事务中的服务提供者。初次和系列的服务提供者验证事务的通信内容有服务提供者标识符、服务提供者密钥认证、服务提供者密钥、传输数据流或服务提供者进行通信时的数据流、及服务提供者将使用的非易失存储器的 NVSC 的最大数目。同样，当服务提供者不想再通过受托实体提供服务时，由保密处理器 205 接收一个或多个命令并进行操作，以将用于该服务提供者的存储块擦除，并将该存储块返回空表。如上所述，表的末端可由十六进制的指针 0xFFFF 预先定义。

在图 6 的上部进入服务提供者表，服务提供者指针可与第 1 服务提供者描述符块的服务提供者标识符对照。如果不一致，则在该表中依次对服务提供者#2 、#3 进行。在本例中，假定只有 3 个有效服务提供者。

服务提供者#1 是使用多重会晤密钥块、大型等级图块及信道(程序)授权图(4 个 NVSC)的服务提供者。

图 6 假定服务提供者#2 是使用多重会晤密钥、及在本例中包括 17 个存储块的极大型信道图的服务提供者。

图 6 还假定服务提供者#3 是不具有等级结构、没有预购或有即兴购买能力等的所谓播放服务提供者。服务提供者#3 仅需要两个存储块。总之，处理器 205 的包含 80 个存储块或 NVSC 的非易失存储器，仅使用到 25 个存储块左右，而 55 个存储块留在空表内。

图 7 在第 1 列中给出这种结果。第 2 列给出本发明的原理对最近发布的在工业中称作 USWset Omaha Triail 的有线电视服务的现场试验的应用。在该最近发布的例子中，总共有 23 个服务提供者(分别具有密钥块，共需 46 个 NVSC)。大型等级图需要其中的 14 个。我们还假定有 9 个 8 信道授权图，用于对 72 个信道授权。然后将 11 个 NVSC 留在空表内。

另外的例子用于说明直接入户服务提供器(Ex #3)及其他典型的模型。

按照这种方式，并作为一例，给出由多服务提供者以保密、有效的方式使用的仅4千字节的保密非易失存储器，该存储器可根据要求并在服务提供者和服务用户的控制下重构，而无需受托实体介入（只要该实体已确认了二者的关系）。接收所有用于装入图内的数据，包括被认证的电子签名、在保密存储器中的任何加密和解密的部分或全部信息，该信息存储在保密存储器内使任何非法的服务接收者不能得到。留在保密微处理器 205 内的任何数据同样由用户以存储在保密存储器内的唯一保密对象签字，并以用户密钥对部分或全部信息加密，从而使服务提供者能够很方便地验证该信息和恢复其包含的数据，并能判定企图干扰回程通信的非法服务接收者的存在。本发明在实践中的任何收费服务终端、直接入户、直播卫星、以及仅作为例子的有线电视中都证明是有用的。

另外，虽已根据图 3 所示的所谓模拟/数字或全数字收费信息服务终端对本发明进行了说明，但本发明经修改后可适用于某些现有的有线电视终端，例如Scientific-Atlanta 8600型和8600X型以及其他厂商的其他的类似终端，而不管是否有厂商的参与。

本发明已参照附图作了详细说明，但本发明在范围上仅受权利要求的限制。此外，本文中引用的任何应用均应看作是针对被认为对本发明的公开来说是实质性的任何要点而作为参考之用引入的。

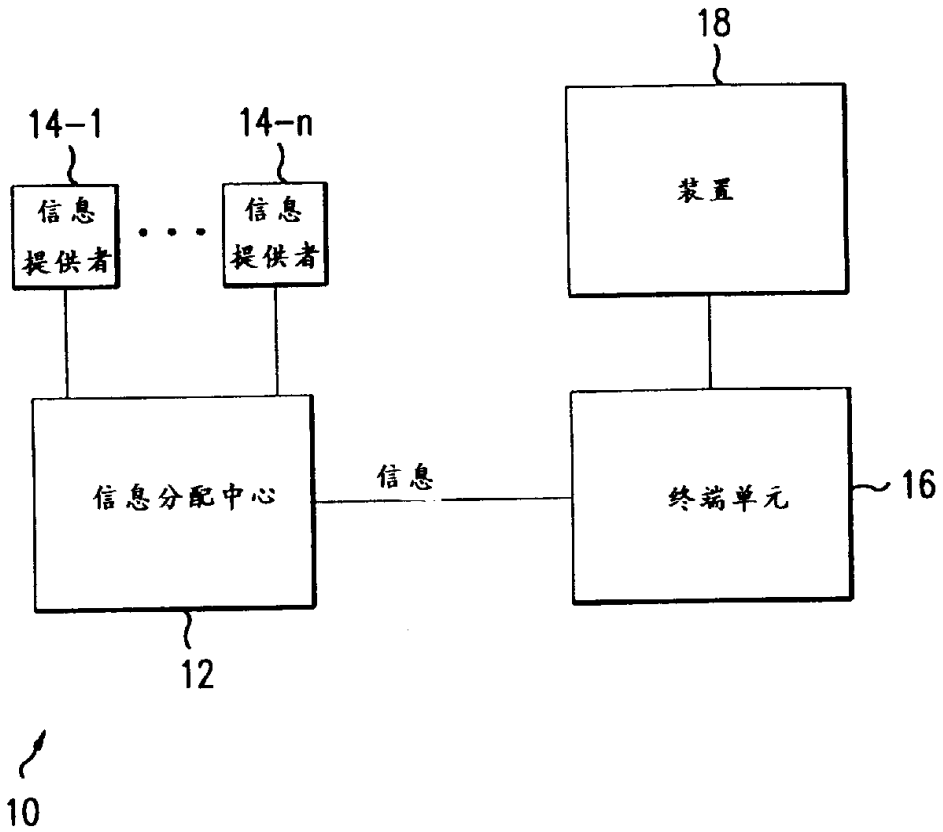


图 1

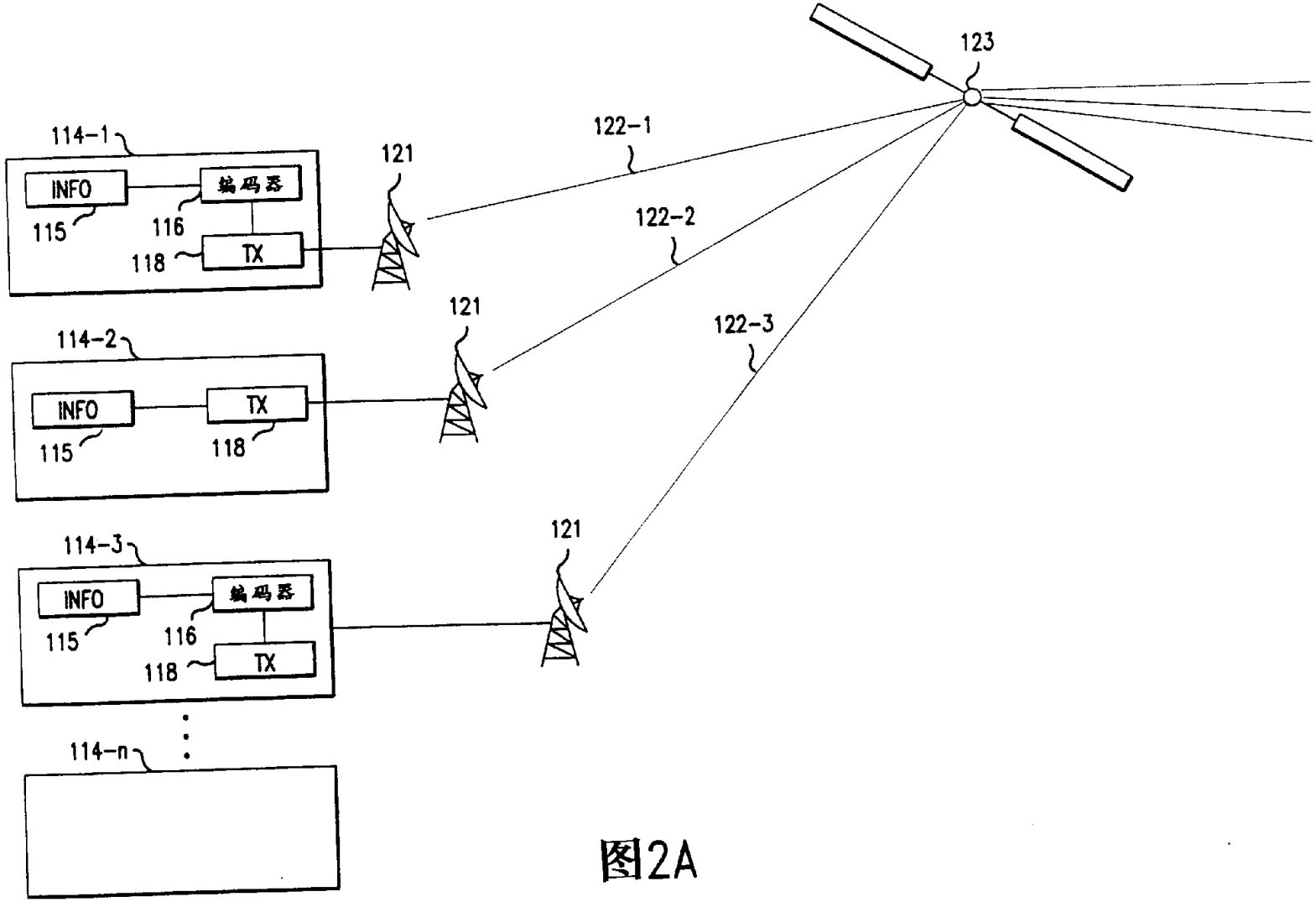

123
122-1
122-2
122-3
114-1
INFO
编码器
115
116
118
TX
121
114-2
INFO
TX
115
118
121
114-3
INFO
编码器
115
116
118
TX
121
114-n

图2A

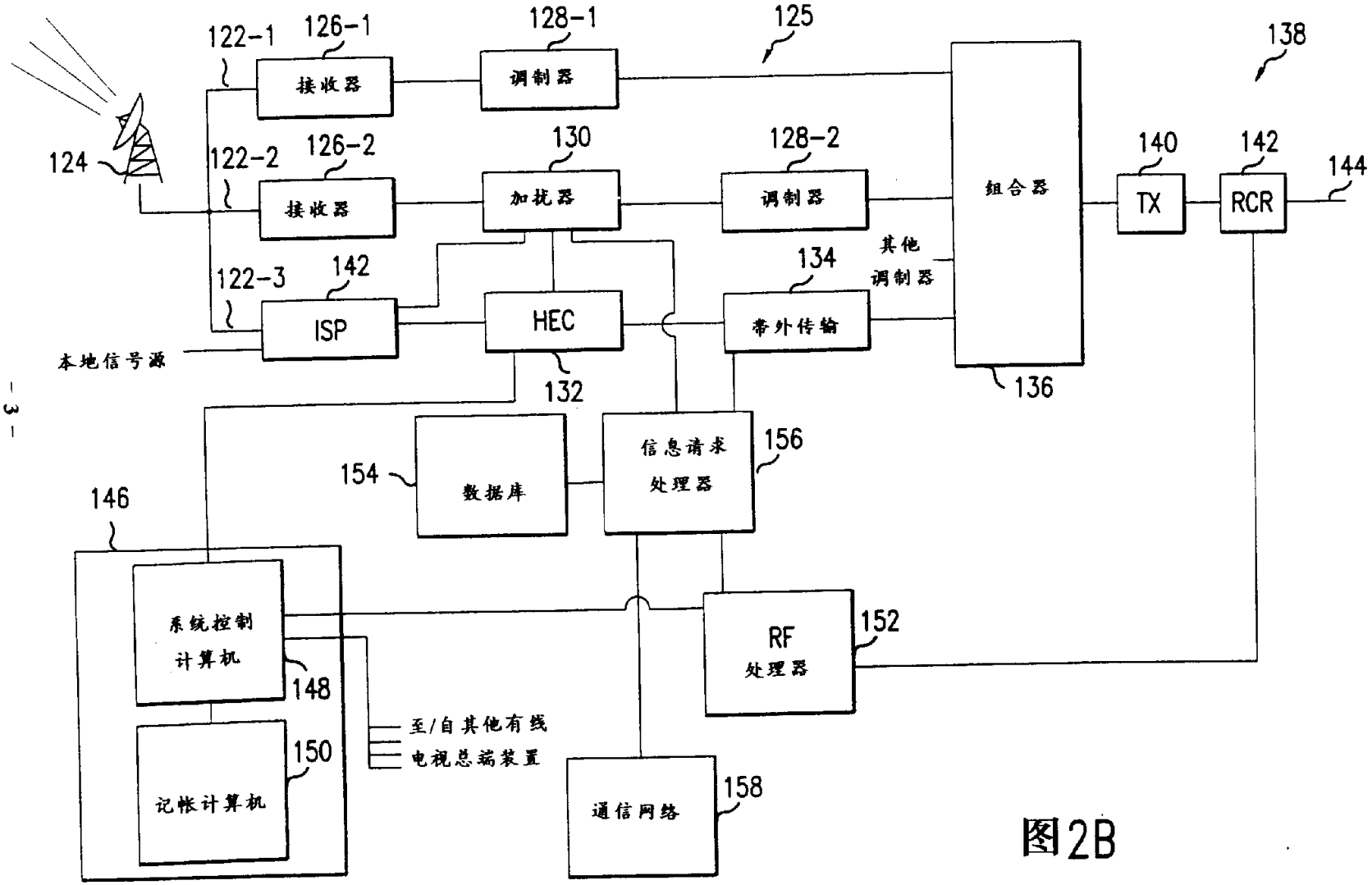

122-1
126-1
接收器
128-1
调制器
125
138
124
122-2
126-2
接收器
130
加扰器
128-2
调制器
组合器
140
TX
142
RCR
144
122-3
142
ISP
HEC
134
带外传输
其他
调制器
本地信号源
132
136
154
数据库
信息请求
处理器
156
146
系统控制
计算机
148
RF
处理器
152
至/自其他有线
电视总端装置
150
记帐计算机
通信网络
158

图2B

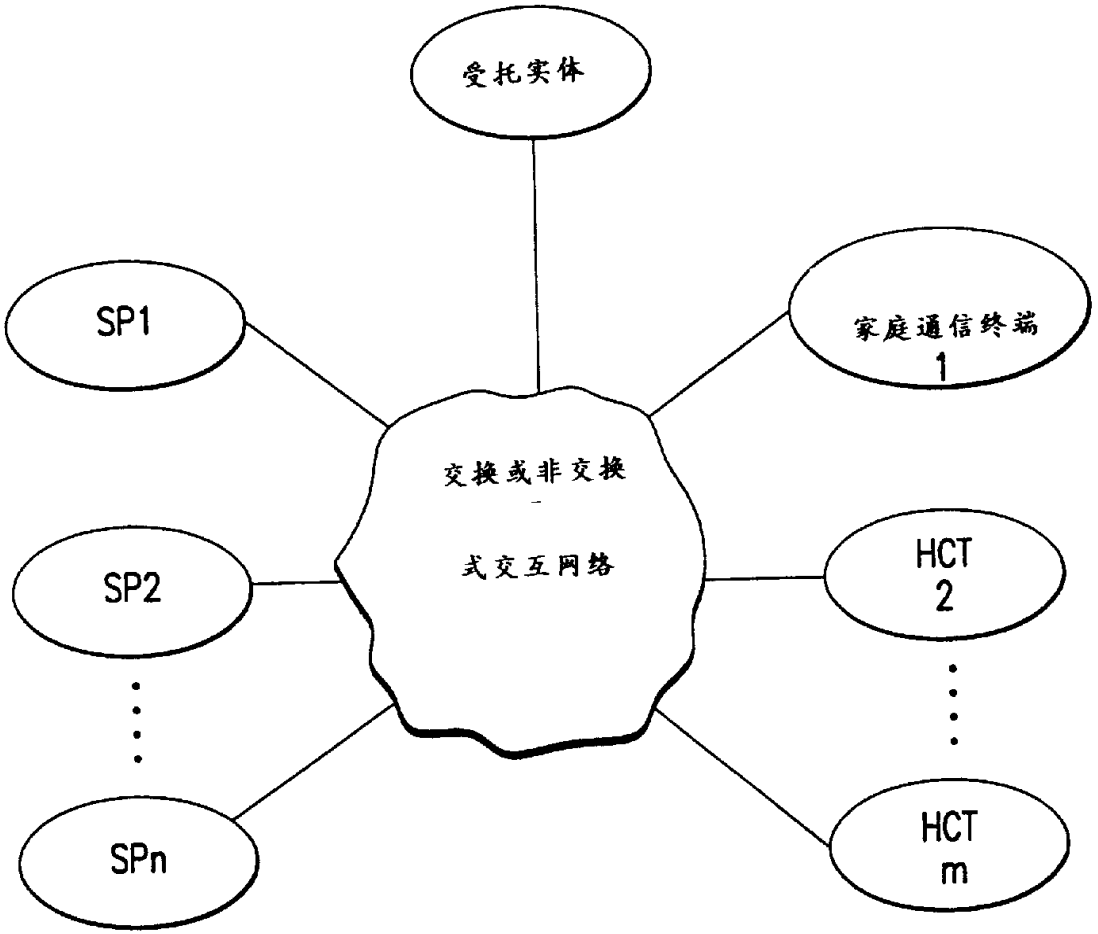


图2C

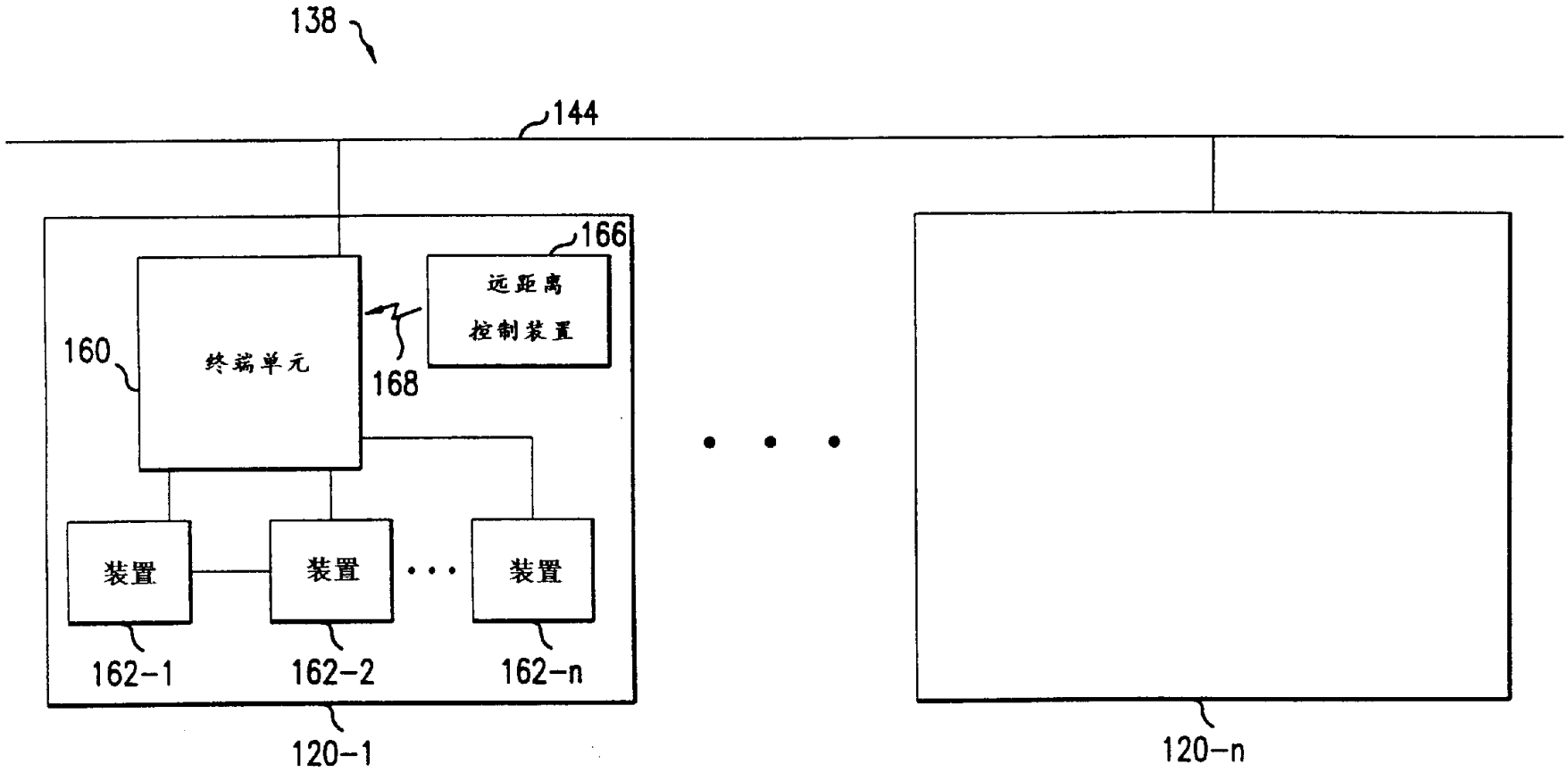

138
144
166
远距离
控制装置
160
终端单元
168
装置
装置
装置
162-1
162-2
162-n
120-1
120-n

图2D

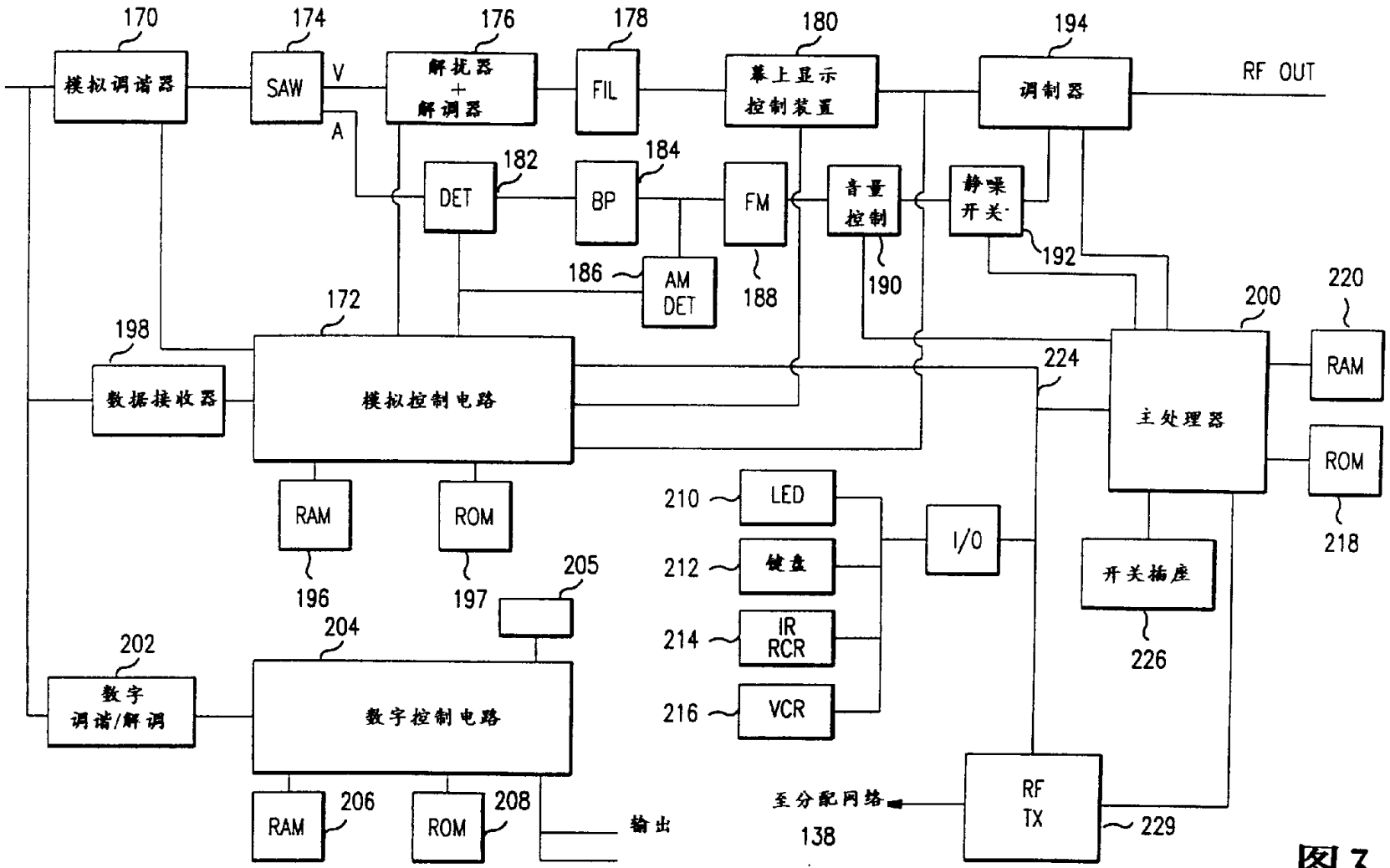

170
模拟调谐器
174
SAW
V
A
176
解扰器
+
解调器
178
FIL
180
幕上显示
控制装置
194
调制器
RF OUT
182
DET
184
BP
FM
音量
控制
静噪
开关
192
186
AM
DET
188
190
172
198
数据接收器
模拟控制电路
224
200
220
主处理器
RAM
ROM
218
RAM
ROM
196
197
205
210
LED
212
键盘
214
IR
RCR
216
VCR
I/O
开关插座
226
202
数字
调谐/解调
204
数字控制电路
RAM
206
ROM
208
输出
至分配网络
138
RF
TX
229

图3

NVSC 项目	尺寸（字节）
类型/状态	1
保留	1
数据	36
下一个 NVSC 指针	2

图4A

位 7	6	5	4	3	2	1	位 0
状态				类型			

图4B

类型值…	指示数据的类型	各NVSC最多可保持…
0000	错误－本NVSC块无效，不应使用	
0001	大型等级图（256级，位映射为32字节，SP号 2 字节，TS ID 2字节）	1
0010	小型等级图（16级，位映射为2字节，SP ID 2字节，TS ID 2字节）	6
0011	位映适时程序授权图的部分（4096信道）	1/16
0100	单个程序授权（程序数2字节，SP ID 2字节， TS ID 2 字节）	6
0101	用于服务提供者的MSK（128字节，奇/偶）	1
0110	即兴式按收视付费事件（事件数2字节，SP ID2字节， TS ID 2字节）	6
0111	TBD	
1000	TBD	
	…	
1111	空，备用。	

图 4C

状态值	含义
0000	错误－本NVSC块无效，不应使用。
1000	切换－另一块正在写入，取代本块的信息。
1100	有效－本块正在使用中，其内容有效。
1110	写入－本块正在写入
1111	空，备用
其它	无效

图 4D

NVSC 类型	说明	需用量
服务提供者 （SP）描述符	特定SP的全面说明，包括公用散列密钥（16字节），SP ID（2字节），NVSC指针（2字节）、SP特征（8字节）、及最多2个信道授权（8字节）。	1
用于服务 提供者的MSK	每个服务提供者具有其自己的MSK，对ECM加密， 具有奇偶MSK，各16字节。	1
大型等级图	使SP根据256级对信道授权。该等级被位映射为32字节。 SP ID 2字节，TS ID 2字节。	1
大型程序图	用于4096个道的位映射程序授权图。每信道需要1位，加上开销。	17
小型程序图	用于256个信道的位映射程序授权图，每信道需要1位 （32字节），SP ID 2字节，TS ID 2字节。	1
单个程序授权（8）	由单一的SP用于对最多8个播放信道或PPV事件授权。 每个程序对信道号需要2字节，对TS ID 2字节。	1
即兴式按收视 付费事件（8）	由单一的SP用于存储IPPV事件。 各事件对事件号需要2字节，对长度需要2字节。	1

图 5

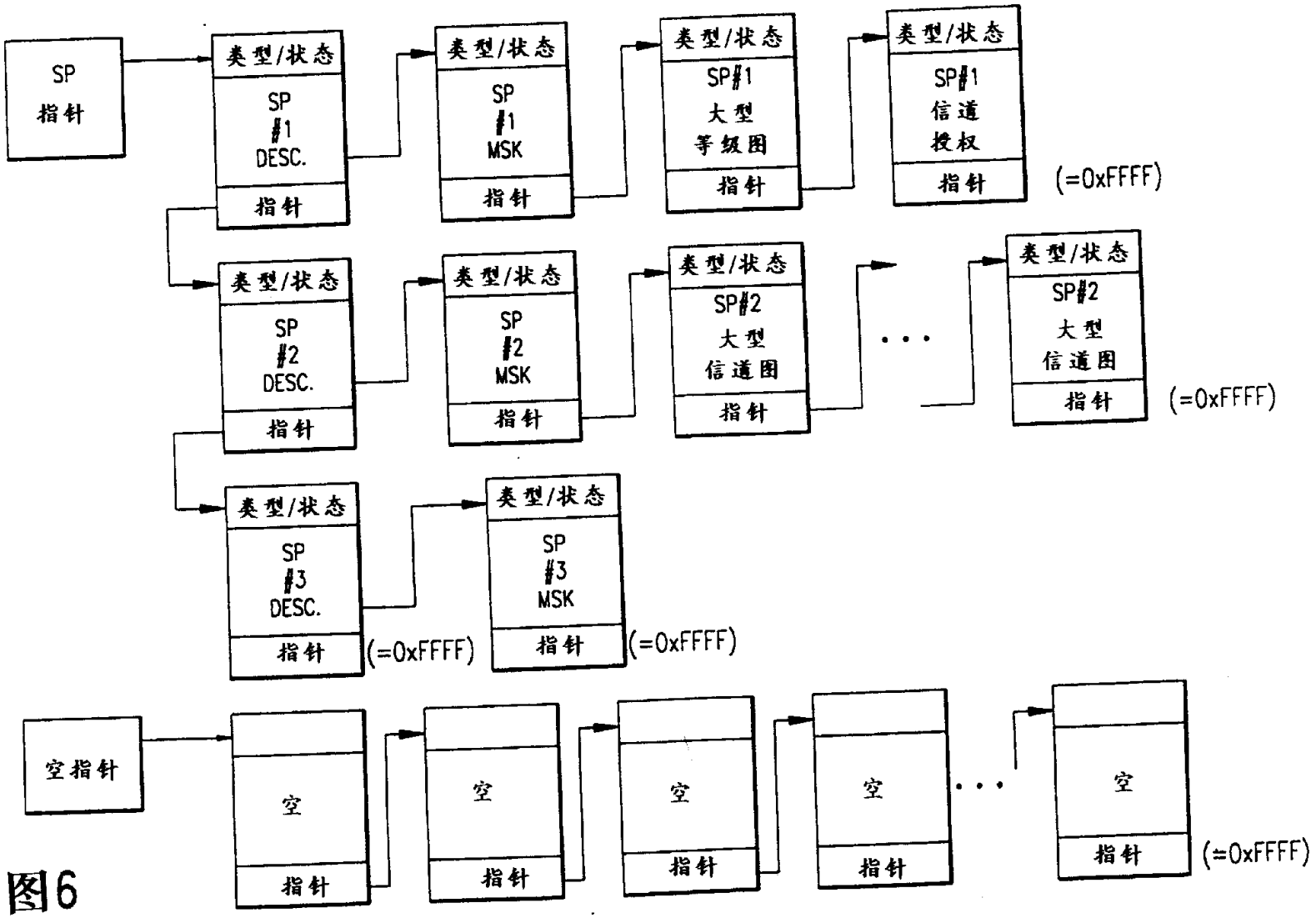

SP
指针
类型/状态
SP
#1
DESC.
指针
类型/状态
SP
#1
MSK
指针
类型/状态
SP#1
大型
等级图
指针
类型/状态
SP#1
信道
授权
指针
(=0xFFFF)
类型/状态
SP
#2
DESC.
指针
类型/状态
SP
#2
MSK
指针
类型/状态
SP#2
大型
信道图
指针
类型/状态
SP#2
大型
信道图
指针
(=0xFFFF)
类型/状态
SP
#3
DESC.
指针
(=0xFFFF)
类型/状态
SP
#3
MSK
指针
(=0xFFFF)
空指针
空
指针
空
指针
空
指针
空
指针
空
指针
(=0xFFFF)

图6

	EX #1: 图6的例	EX #2: USWEST OMAHA TRIAL	EX #3: DIRECT TV 型	EX #4: SAVANNAH 型	EX #5: 强交互式	EX #6: 多个小SP
服务提供者总数	3 (6 NVSC'S)	23	2	5	35	35
具有大型 等级图的SP		14	2	4	5	1
具有大型 信道图的SP	1 (17 NVSC'S)			1		
具有小型 信道图的SP						
8信道授权	1	9 (总计72个)	20 (总计160个)	10 (总计80个)	5 (总计40个)	
8 IPPV 事件			6 (总计48个)	10 (总计80个)		
空NVSC (从总数80个留出)	55	11	48	29	0	9

图 7