[19]中华人民共和国专利局

[51]Int.Cl[6]
H04N 7/24
H04N 5/44

[12] 发明专利申请公开说明书

[21] 申请号 96110548.8

[43]公开日 1997 年 3 月 26 日

[11] 公开号 CN 1146122A

[22]申请日 96.7.8

[30]优先权

[32]95.7.7 [33]US[31]499280

[71]申请人 汤姆森消费电子有限公司

地址 美国印第安纳州

[72]发明人 P·罗哈吉

V·杜劳

[74]专利代理机构 中国专利代理(香港)有限公司

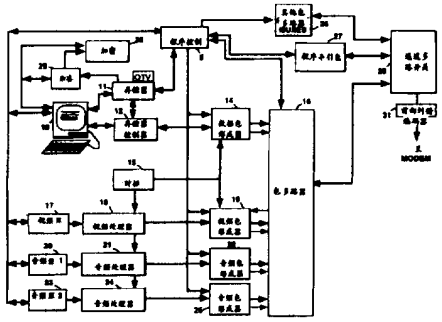
代理人 吴增勇 傅 康

权利要求书 6 页 说明书 24 页 附图页数 8 页

[54]发明名称 交互信息系统中鉴别发送应用的装置和方法

[57]摘要

把可执行交互程序与传送用音频/视频结合。程序分成模块，并建立连接程序模块的目录模块。通过将签了字的许可证附在目录模块来提供可执行应用的加密。通过各模块的杂凑处理和把杂凑值加入目录模块来监视模块完整性。含有其他杂凑值的目录模块杂凑值被产生、加密并附于目录模块。在接收机将许可证解码，检查提供的真实性。若许可证真实，且只有当接收机产生的程序模块杂凑等于目录模块所含的相应的杂凑值时，程序才可执行。



权 利 要 求 书

1.一种用于接收以模块形式发送的可执行应用的装置，所述模块包括其中含有关于其他模块的信息的目录模块，所述目录模块至少具有加了密的对目录模块的杂凑值和加了密的后附的许可证，所述许可证包括应用提供者的识别符，所述装置的特征在于包括:

存储器(88),

用于检测传送的所述模块并将检测出的模块储存在存储器中的检测器(84),

用于将所述许可证从检测出的目录模块分离出来的装置(89 ， μPC),

用于将所述许可证及加了密的杂凑值解密的解密器(97),

用于对检测出来的所述目录模块进行杂凑处理以产生其他杂凑值的杂凑函数元件(96),

处理器(μ PC)，它在程序控制下对解了密的所述许可证进行授权鉴定，并将解了密的杂凑值和所述其他杂凑值进行比较，若所述解了密的杂凑值与所述其他杂凑值相等，而且所述许可证是有效的，则允许所述应用执行。

2. 权利要求 1 所提出的装置，其中目录模块还包括其他模块的杂凑值，所述装置的特征还在于

用于从所述检测出的目录模块访问其他模块的杂凑值的装置，

用于将各所述其他程序模块加到所述杂凑函数元件以产生对其他程序模块的杂凑值的装置，以及其中

规定所述处理器将从所述目录模块取出的其他程序模块的杂凑值，与由所述杂凑函数元件产生的相应的杂凑值比较，如果相应的杂凑值中至少预定的一个相等，则允许所述程序执行。

3. 权利要求 1 所提出的装置，其特征在于所述发送的目录模块是

加了密的，而规定所述解密器用应用提供者的公共密钥对所述目录模块进行解码。

4. 权利要求 2 所提出的装置，其特征在于所述处理器包括用于从所述存储器删除相应杂凑值不等的模块的装置。

5. 权利要求 1 所提出的装置，其特征在于所述解密器和所述杂凑函数元件包含在所述处理器中。

6. 权利要求 1 所提出的装置，其特征在于所述监测器包括前向纠错线路。

7. 权利要求 1 所提出的装置，其特征在于传送的所述可执行的应用是以传送分组的形式传送的，每个传送分组包括服务通道识别符和扰频标志，而所述检测器包括:

用于从多路传送分组流中选择具有预定服务通道识别符的传送分组的可编程服务通道识别符检测器，而所述装置还包括:

用于响应所述扰频标志，按照所述扰频标志的各种状态，对各传送分组进行反扰频用的反扰频器。

8. 权利要求 1 所提出的装置，其特征还在于用于产生表明检测到由未经授权的应用提供者提供的信号的显示的装置。

9. 权利要求 1 所提出的装置，其特征还在于

预定正文数字版本的来源，

用于将所述预定正文数字版本加在包括目录模块的所述模块中至少一个的前面的装置，并且其中

规定所述杂凑函数元件要对前面加有所述预定正文数字版本的所述至少一个模块进行杂凑处理。

10. 权利要求 9 所提出的装置， 其特征在于所述预定的正文是 OpenTV(TM)。

11. 权利要求 1 所提出的装置，其特征在于所述目录模块包括利用 RSA 算法、以模数 N 和指数 e 算出的签字 S，还包括用模数 N 除签字 S 而得的商 Q1 和 Q2，所述处理器规定要利用商 Q1 和 Q2，不

必做除法即可校验所述签字 S 。

12. 一种用于处理作为模块以多路分组的格式发送的可执行的应用的方法，所述模块包括含有连接其他各应用模块的信息的目录模块，所述目录模块具有加了密的附加的许可证，所述许可证含有有关应用提供者的信息，而其许可证用系统提供者私人密钥加密，所述方法的特征在于:

检测和选择包括所希望的应用的分组，将作为各模块的各个分组的有效载荷储存起来，

选择具有附加的加了密的许可证的目录模块，

将带有系统提供者公共密钥的许可证解密，

将解了密的所述许可证中的信息与储存的相应数据加以比较，

对所述应用模块之中的几个进行杂凑处理，以产生模块的杂凑值，

将所述模块的杂凑值与目录模块中传送的相应模块杂凑值加以比较，以及

如果产生的和传送的相应的杂凑值相同，而在所述许可证中所含解了密的信息与所存相应的数据相当，则执行一个应用。

13. 权利要求 12 所提出的方法，其中所述许可证包括应用提供者的公共密钥，而所述目录模块具有附于所述目录模块的杂凑值，所述杂凑值用所述应用提供者的私人密钥加密，所述方法的特征还在于下列步骤:

从解了密的所述许可证中提取所述应用提供者的公共密钥，并从所述目录模块中分离出加了密的杂凑值，

用所述应用提供者的公共密钥对加了密的所述杂凑值进行解密，

将解了密的所述加密杂凑值与检测出的所述目录模块的杂凑值进行比较。

14. 权利要求 12 所提出的方法，其特征还在于，在对所述目录模块进行杂凑处理之前，在所述目录模块之后附加数字形式的正文

OpenTv(Tm)，然后对后附了数字形式的所述正文 OpenTv(Tm)的目录模块进行杂凑处理。

15.用于发送可执行的应用的装置，其特征在于:

用来产生可执行应用，并将所述应用形成含有所述应用的一部分的模块，和含有将模块连接成应用用的连接信息的目录模块用的处理器(10，11，12),

用于对所述应用的模块完成单向杂凑处理功能，以产生相应杂凑值，并协同所述处理器将所述杂凑值插入所述目录模块的杂凑功能元件(29，30),

用于应用提供者公共密钥和许可证的来源(10)，所述许可证是用系统控制器的私人密钥签字的，并包含应用提供者的识别符和与产生时间和许可证有效时间有关的时戳,

用于将应用提供者的公共密钥和所述许可证附在所述目录模块后面的装置(11，12)；以及

用于形成所述应用的所述模块的时分多路信号的传送处理器(14，16)。

16. 权利要求 15 所提出的装置，其特征还在于

用应用提供者的私人密钥对含有所述应用模块杂凑值的目录模块的杂凑值进行加密用的加密装置；以及

将加了密的所述目录模块的杂凑值附在所述目录模块后面用的装置。

17. 权利要求 15 所提出的装置，其特征在于所述模块之中，有一些是其中所含数据预期在所述应用的执行过程中会改变的数据模块，而所述处理器给各个模块加上版本号，而当这样的模块改变时，改变模块的版本号，

所述杂凑功能元件对每一个改变了版本号的模块进行杂凑处理，产生新的杂凑值，并与所述处理器合作，将所述新杂凑值附在与之对应的模块后面。

18. 权利要求 15 所提出的装置，其特征还在于:

预定正文的数字版本的来源，

多路器，用来将所述预定正文的数字版本与所述目录模块一起进行多路切换，其中规定所述杂凑功能元件要对所述预定正文的数字版本与所述目录模块的组合体进行杂凑处理。

19.用于发送可执行的应用的方法，其特征在于:

产生可执行的应用，并将其分成模块，

形成含有将各应用模块连接起来用的信息的目录模块，

对具有单向杂凑处理功能的所述各模块进行杂凑处理，产生与各模块对应的杂凑值，

把各模块的杂凑值列入所述目录模块中，

访问包括应用提供者识别符的许可证，所述许可证是用系统控制器私人密钥来加密的，

将所述许可证附在所述目录模块的后面，并将所述应用发送出去。

20. 权利要求 19 所提出的方法，其特征还在于:

对其中含有杂凑值的目录模块进行杂凑处理，

对目录模块的杂凑值进行加密，

将加了密的所述目录模块杂凑值附在所述目录模块的后面。

21. 权利要求 19 所提出的方法，其特征还在于:

产生另一种包含第三方提供者识别信息的许可证，

用应用提供者私人密钥对另一种许可证进行加密，

将加了密的所述另一种许可证附在所述目录模块的后面。

22. 权利要求 20 所提出的方法，其特征还在于:

用应用提供者的私人密钥对所述目录模块进行加密，并将所述加了密的目录模块发送出去，以及

以明文形式发送其余的应用模块。

23. 权利要求 19 所提出的方法，其特征在于将杂凑值加入目录模

块之中的步骤加入长 128 位的各个杂凑值，以及

把许可证附在所述目录模块后面的所述步骤包括附加一个包括下列各项的许可证:

32 位许可证描述符或标志，

32 位识别符，

32 位有效期描述符，

32 位文件储存限制，

128 位姓名，

32 位公共密钥。

说　明　书

交互信息系统中鉴别发送应用的装置和方法

本发明涉及一种用于保证交互电视系统所接收的数据是得到授权的数据的方法和设备。

交互电视(TV)系统可从例如，美国专利 No.5,233,654 得知。交互电视系统通常都涉及向各接收设备发送编程和/ 或控制数据(下文记为 PC 数据，即，程控数据)以及音频和视频信息。接收设备将程控数据解码，并将其应用于控制设备，供接收器自动使用，或由接收器的用户选择使用。控制设备可以采取计算机的形式，而所述使用可以包括将选择性的，例如财务数据下载，供用户以后处理。

正如这里预期的，交互电视系统(ITVS)是以压缩的数字形式发送的。该系统的接收端包括集成接收解码器(IRD)，用来接收发送来的信息，并将其解压，向各处理器提供已解码的音频和视频信息，以及程控数据。音频和视频处理器可以是音频和视频重放装置或电视接收机，而程控数据处理器可以是计算机。最理想的是，系统只提供由授权服务提供者所提供的经过充分测试的程控数据，而在这样的条件下，发送的信息实际上不大可能破坏各接收机。但是，如果大量的服务提供者被授权使用该系统，就很容易 a)被未经授权的用户侵入和有意地使系统用户受到损害， b)不细心地准备的程控数据和随之无意地使系统用户受到损害。同时向成千上万集成接收解码器广播程控数据的能力，使软件不良行为造成系统崩溃的潜在可能性加大许多倍。这就有必要采取措施，保证各交互电视系统接收机不受不良行为和未经授权的程控数据损害。

本发明的接收机的实施例包括集成接收解码器，后者响应发送来的程序导引(program guide) ，选择程控数据的信号分组。集成接收解码器将所选择的程控数据临时储存起来。得到授权的程控数据将包含

许可证。程控数据处理器将该许可证分离出来，并检查其授权性。该处理器将一部分程控数据进行杂凑分类，并将产生的杂凑值与随该程控数据发送来的并与同一部分程控数据对应的杂凑值进行比较。若杂凑值相等，而且许可证是经授权的，便使系统能够执行发送来的程序。

发送器的实施例包括用于提供交互程序的软件发生装置。程序分成模块，并产生目录模块。各模块都进行杂凑分类，并将产生的模块杂凑值包括在目录模块内。然后使模块处于准备发送的状态。

下面将参照附图对本发明进行说明。

图 1 是一个体现本发明一个方面的交互电视信号编码系统的方块图。

图 2 是作为例子举出的音频、视频及交互信号一部分的图解。

图 3 是作为例子举出的传送包的图解。

图 4 是对描述本发明有用的作为例子举出的音频、视频及交互应用的格式的图解。

图 5 是作为例子举出的发送单元标题的内容一览表。

图 6 是体现本发明的作为例子举出的音频、视频及交互应用的目录模块内容一览表。

图 7 是说明体现本发明的对音频、视频及交互应用进行加密/保护的过程的流程图。

图 8 是体现本发明的接收装置方块图。

图 9 是可用来实现图 8 装置的处理器的作为例子举出的处理器扩大的方块图。

图 10 是流程图， 说明图 8 接收装置的一部分操作，并描述本发明一个接收机实施例。

图 11 是作为例子举出的许可证鉴别过程的流程图，它是本发明的实施例。

图 12 是本发明的最佳目录模块格式的图解。

本发明将在压缩数字传送系统，例如卫星直播系统的环境下进行

描述.假定单个卫星发送－应答器适配多个采用时分多路格式的不同的电视节目.

参照图 1，分组多路器 16 在其出口处提供一个音频、视频、交互程序(AVI)．与此类似的装置 26 产生替代的音频、视频及交互程序.程序导引包括通过服务通道识别符(SCID)与各个音频、视频及交互程序的音频、视频及交互成份关联的信息.该程序导引由处理元件 27 以类似于音频、视频及交互程序的传送格式提供.程序导引和各个音频、视频及交互程序，以传送分组的形式加在通道多路器 28 的各个输入口.通道多路器 28 可以是已知结构的多路器，以相等的时分将各个分组信号多路切换成单一的信号流，或者它也可以是以统计方式控制的多路器.该多路器 28 耦合到前向纠错编码(FEC)和信号交错装置 31，该装置可包括 Reed-Solomon 及 Trellis 编码器.前向纠错编码装置 31 的输出耦合到调制解调器，在这里经过多路切换之后的信号被处理，以便应用于，例如，卫星传送－应答器上.作为例子举出的的统计控制多路切换后的分组信号在图 2 加以说明，而作为例子举出的各种分组的格式在图 3 中说明.

音频、视频及交互信息由系统程序控制器 5 控制.程序控制器 5 可以有用户接口，用以选择特定的程序和各程序信号成份.程序控制器给各个程序的各个音频、视频及交互成份分配相应的服务通道识别符.假定各个接收机可以读取程序导引，以确定哪一个服务通道识别符关联音频、视频及交互程序成份，然后从传送的信息流中选取含有该关联的服务通道识别符的传送分组.给音频、视频及交互成份赋予不同的服务通道识别符，使得一个音频、视频及交互程序的一个或多个成份可以方便地用来形成交替的音频、视频及交互程序.利用不同的服务通道识别符也便于把从一个节目来的音频信号与从另一个节目来的视频信号编辑在一起.

给定的音频、视频及交互程序可以包括不同的信号成份源.图 1 所示是，交互成份源 10 、视频信号源 17 和第一及第二音频信号源

20 和 23(双语种音频)。控制器 5 与各个源通信，起时间管理和/或使能的作用。视频信号源 17 耦合到视频信号压缩装置 18，后者按照运动图像专家组(MPEG)提出的视频压缩标准对信号进行压缩。类似地，来自源 20 和 23 的各个音频信号加在各个压缩装置 21 和 24 上。这些压缩装置按照运动图像专家组(MPEG)提出的音频压缩标准对各个音频信号进行压缩。按照 MPEG 提出的规程压缩了的相关的音频和视频信号采用由定时元件 15 提供的播放时标进行同步。为了深入了解音频和视频如何在时间上关联起来，建议读者参阅“ INTERNATI ONAL ORGANIZATION FOR STANDARDIZATION , I S O/I E C JTC1/SC29/WG11 ; NO531 , CODING OF MOVING PICTURES AND SCCOCIATED AUDIO , MPEG91 , SEPTEMB ER , 1993 。”

压缩了的音频和视频信号加到传送分组形成器或处理器 19，22 和 25 上。音频和视频传送分组处理器是已知的，这里不再叙述。只要指出传送分组处理器将压缩了的数据分割成一定字节数的有效载荷，并附上图 3 所示的包括服务通道识别符的识别标题。为了得到关于视频信号传送分组处理器的详细信息，建议读者参阅美国专利 No.5,168,356 。传送分组处理器耦合到传送分组多路器上，后者对信号成份进行时分多路切换。传送分组处理器可以包括用于临时储存分组化的数据以适配正在为其他成份服务的多路器的缓冲内存。传送分组处理器包括耦合到多路器，在传送分组可用时向多路器发出指示用的 PACKET READY(分组就绪)信号线。

交互程序由操作可能是一台个人计算机的交互成份源或编程元件 10 的程序员用已知的技术建立。在形成所述应用时，编程元件 10 与存储器 11 及存储器控制器 12 接口，完成了的应用储存在存储器 11 内。完成后，把所述应用浓缩或翻译成某种本机编码，以节省信号的频带宽度。

如图 4 所示，在形成所述应用时，程序的一部分格式化为模块、传送单元及分组。这种分组类似于上述的传送分组。一个传送单元包

括多个传送分组。每个传送单元包括含有描述传送单元内容的信息的标题分组，以及多个包括一部分应用码字的基本分组。模块分割成传送单元，以便对来自不同模块的信息进行交替。最好允许传送单元的交替，但不允许来自不同传送单元的传送分组的交替。为了获得对应用及传送单元的信息的更详细的描述，建议读者参阅美国专利No.5,448,568。

模块类似于计算机的文件，并且具有不同的类型。第一种类型的模块是目录模块，含有作为一种应用的有关各个传送单元及模块的信息。第二种类型的模块是编码模块，包含对接收机的计算装置进行编程以完成或执行该应用所必须的可执行编码。第三种类型的模块是数据模块。数据模块包括执行该应用所用的不可执行的“数据”。数据模块往往比编码模块更具有动态性，就是说，在一个程序中，数据模块往往会变化，而编码模块一般不。第四种类型的模块称为信号模块。这种模块是一种特殊的分组，包括用来触发接收机中断的信息，可以用来进行例如视频与应用程序特点的同步，或者使应用暂停，或者重新允许程序运行等等。同步是通过加入播放时标实现的。数据、目录、编码及信号模块是程控数据的一些例子。

各个模块可以由编程元件10进行错误编码。例如，可以对整个模块进行循环盈余编码CRC，并在模块结尾处加上错误检查位。

每个传送单元TU配上一个标题，后者分组包括有关该传送单元的信息。图5所列表1作为例子列出包括在每个传送单元标题包中的信息类型。标题包括版本号。加入版本号用来指示在播放音频、视频及交互程序时何时对应用进行改变。可以这样安排接收机的解码器使得当检测出版本号发生变化时，作出响应，修改正在执行的应用。模块识别符类似于计算机文件的识别符，并由应用的程序员提供。模块传送字节偏移量是一个数字，它指明本传送单元有效载荷第一个编码或数据字节在模块中的字节位置。传送单元长度说明传送单元的大小或者传送单元最后一个编码或数据字节的位置。

图 6 表 II 列出包括在目录模块中的有代表性的数据类型。 目录模块包括带有下列内容的标题: 应用识别符 AID 、说明应用类型的字段、包括类型描述符的字段、指明储存和执行该应用所需内存数量的字段、说明该应用所包含的模块数的字段、以及一个或多个(第一加密信息)可以包括诸如授权识别数据等加密数据的字段。应该指出，上列的各个字段，或者以后的字段，都不一定要按照所列的顺序排列。目录模块的数据部分包括类似于各个模块的标题数据的每一个模块的数据。此外，还有一个字符串表，它是各个应用模块名的 ASCII 格式的表格。 每个模块的数据段还包含一个或多个(其他加密信息)可以包括诸如授权识别数据等加密数据的字段。作为另一方案，这个数据也可以以更一般的目录数据列在第一加密信息字段中。模块加密信息字段的内容在下面将要更详细的讨论。

对于传送分组的信息，交互成份源 10 可以编程来产生实际的传送单元或传送分组，但在图 1 的实施例中，包括了单独的编码/数据分组处理器 14 。该编码/数据分组处理器通过存储器控制器 12 存取存储器 11 的各区，并顺序地产生代表各个应用的包(图 4)。

分组多路器 16 按照特定的时间表提供分组。该时间表一般是由音频、视频及交互成份的带宽要求确定的。当各成份之间出现多路切换竞争时，最好给最不经常出现的分组的信号成分赋予较高的多路切换优先级。

这里不再叙述分组多路器的细节了，因为多路器是一种成熟的技术，而对于熟识数字信号处理的人来说，很容易设计出满足他们特定要求的多路器。只要指出分组多路器 16 利用三态逻辑开关进行安排，将输入口耦合到各成分的信号上，而将其输出口耦合到多路器的输出口就够了。 可以安排一个状态机，按照由控制器 5 建立的优先级以及由分组形成器提供的各个分组就绪信号来控制逻辑开关。

音频、视频及交互系统的加密是建立在音频、视频及交互系统控制器所执行的技术和存在于音频、视频及交互系统从属接收机中的密

码之间的紧密结合上。加密是建立在使用 Rivest, Shimir 和 Adleman, RSA 算法的公共密钥加密法或数据加密标准 DES 的基础上的。 本发明者推荐的算法是 RSA 算法， 利用分别是 4(8 位)字节的倍数的模数和指数大小。一般类型的加密保护驻留在用目录模块提供的许可证的鉴别和在相应的其他应用模块上产生的杂凑(分类)值中。

一类特殊的 RSA 规程在于公共指数是 3 。优越性在于，签名检查的速度由于加入了下述类型的“帮助”信息而得到加强。

现在来考虑检查一台接收机， 对数据 D 的 RSA 签字是 S ，其中公共的模数和指数分别为 N 和 3 。为检查，接收机本上质显示出 $S^3 = D(\mathrm{mod}\ N)$。一般，这要作计算困难而费时的除法/对 N 取模的运算。因为乘法是计算比较简单速度较快的运算，所以依靠乘法而不依靠除法的检查运算会大大加快运算速度。

考虑如下定义的商 Q1 和 Q2 :

若 $S^3 = D(\mathrm{mod}\ N)$， 则 $S^2/N = Q1 + R1$； $S * R1/N = Q1 + Q2$； $R2 = D$。就是说，数值 Q1 和 Q2 是签字除以 N 而得的整数商。而 R1 和 R2 是分别除剩的余数。给定最多 T 位大小的 D 任何 N, S 和，其中： $S < N$ 及 $D < N$， 则利用下面马上要描述的算法，便会有能够检查 $S^3=D(\mathrm{mod}\ N)$ 的最多 T 位大小的商 Q1 和 Q2 。如果数值 Q1 和 Q2 是由应用程序员(例如非实时地) 计算出来的，并在目录模块内与签字 S 一起发送，就可以看出，对签字的快速检查可按下列步骤完成。在计算机上， 从目录模块取出 S， Q1 和 Q2 ;

1.计算 $A = S2$

2.计算 $B = Q1$ 乘以 N

3.比较 $A > B$; 若 $A < B$ 则退出， 无法检查签字

否则 若 $A > B$ 则

4.计算 $C = A - B$

5.比较 $C < N$; 若 $C > N$ 则退出， 无法检查签字

否则 若 $C < N$ 则

6.计算　　E＝C 乘以 S

7.计算　　F＝Q2 乘以 N

8.比较　　E＜F；若 E＜F 则退出，　无法检查签字

否则 若 E＞F 则

9.计算　　G＝E - F

10.比较　　G＝D；若不，则不检查签字

请注意，　所有算法运算都是简单的乘法或者减法。可以在 3, 5, 8 或 10 步查出错误签字。　如果在 3 或 5 步查出错误签字，所花的时间是非常少的。

音频、视频及交互接收机装有各个系统提供者的公共密钥(以及要求的帮助商 Q1 和 Q2)，用来解密包括程控数据的签了字的许可证，以确定程序的真实性。如果程序的真实性得不到证实，则立即将接受到的程序应用从接收机废弃掉。这种加密系统的中心是给应用提供者和系统控制器或服务器赋予唯一的识别符。系统控制器给每个受托音频、视频及交互应用提供者分配唯一的例如，32 位的识别符，另外给应用提供者公共密钥发布许可证。许可证基本上就是系统控制器对应用提供者公共密钥的数字签字，它包括诸如许可证截止日期、提供者的识别符以及具有识别符的应用在接收机的文件系统中可以使用的存储器数量限度等字段。系统控制器可以使用许多对私人－公共密钥，而许可证包括一些标志来指定在多个公共密钥中接收机应该使用哪一个来给各个许可证解密。

一般，应用提供者的许可证包括:

CERTIFICATION FLAGS (许可证标志)(它识别许可证的类型，并且可以包括系统控制器公共密钥标志)

PROVIDER_ID (提供者密钥)(它指出提供者识别符的长度)

PROVIDER_EXPRE (提供者截止日期)(它指示应用寿命)

PROVIDER_AUTHORIZATION_FLAGS (提供者授权标志)

PROVIDER_STORAGE_LIMIT (它指出给提供者分配的存储限度)

PROVIDER_NAME (应用提供者的姓名)

PROVIDER_FIXED_CERT (这是提供者的公共密钥).

上列许可证信息以 128 为模进行杂凑分类，并将杂凑值附于其后。

上述许可证标志包括授权标志， 它准许/不准许接收机处理器采取特权行动。通过该标志采取的具有代表性的特权例子列于此后:

1.从广播链路下载的能力;

2.从本地链路(例如通过本地集成接收解码器口连接的)下载的能力;

3.从本地远程链路(例如通过电话链路)下载的能力;

4.根据同一程序的上下文给应用转换频道(例如在电视第一和第二频道之间切换)的能力;

5.建立广播联接(例如改变电视节目和频道)的能力;

6.建立本地联接的能力;

7.建立远程联接的能力;

8.控制外部装置的能力;

9.下载非检查的模块的能力;

10.应用使用加密特点的能力;

11.应用请求用户允许使用用户加有限制的文件的能力;

12.启动常驻 OCODE 监视器进行远程查错的能力。

这些标志既是提供者许可证的一部分，又是应用授权字段目录的一部分。一个应用必须在这两个地方的授权标志都设置了，才允许执行特权行动。各个接收机在非易失存储器内都含有一个 BOX 授权屏蔽，

在程序控制下允许采取特定的特权行动，或者禁止采取某些特权行动。

每个应用提供者选择他自己的加密用公共一私人密钥对，并具有他的（例如，通过公证请求）被音频、视频及交互系统控制器认可的

公共密钥。在选择公共密钥方面，应用提供者受到某些规则的限制。这些限制涉及接收机硬件的能力。更具体地说，目前的消费者电子接收机包括最小内存和相对不太高级的处理器，这些因素影响鉴别授权处理速度和时间，从而影响公共密钥的大小和形式。限制的例子可能是公共密钥为512位或更小，位数是2的若干次方。

可以把一组音频、视频及交互系统专用识别符保留下来，供完成接收机或系统维护的程序用。这个系统识别符将附加在服务提供者识别符上。如果一个程序既含有专用识别符，又含有经授权的提供者识别符，则依特定提供者识别符的不同，相应维护程序可以含有对接收机比较机密的部分的访问。例如，应用提供者可以是系统控制器，而所附的应用可以用来修改智能卡的权限，或者完成系统性能检查。或者，应用提供者可以是商品促销商，而程序可以是有关检查用户的借方和贷方，或者用来简化税收手续等等。另一方面，如果一组识别符不是该组音频、视频及交互系统专用识别符，那么对该应用可用的功能就只限于对所有应用均可使用的功能。

可以给特定的接收机装置的制造商分配特殊制造商识别符。具有制造商识别符的任何应用，都可以通过驻留在接收机中并在接收机装配过程中由制造商实现的的特殊的鉴别过程来进行鉴别。含有制造商识别符的程序，只可以访问该特定的制造商所生产的接收机，而其功能只能访问制造商装在接收机内的特定的一组功能。这类应用可以用来把接收机的操作软件升级。

还可以有网络操作者， 他在特定的接收机中驻留有软件/硬件。还可以给这些网络操作者分配专用的识别符，以允许选择性地访问所有网络接收机的软件/硬件。网络操作者可以包括他们自己的驻留在网络接收机上软件/硬件中的鉴别过程。

一个应用属于专用系统型、制造商型还是属于网络型，是在目录模块(表II)的应用类型字段中指出的。应用描述符字段可以包括识别制造商、或者网络操作者等的信息。

对应用的加密过程如下。应用提供者产生一个应用，并形成各种模块，包括目录模块之后，他决定所述应用的那些部分要保护。在任何情况下，目录模块都是要保护的。此外，每个含有入口的模块也是要保护的。不含入口的模块是否要保护、数据模块是否要保护，这要由提供者决定。应该认识到，数据模块中的数据部分是经常变化的，因此如果对数据模块进行保护，就会给编码器和接收机造成比较沉重的加密处理负担。所以，数据模块常常是不加保护地发送的。选择了要保护的模块之后，提供者编制一个选出进行加密保护的模块清单及各模块的保护模式，将这个清单输入目录模块中标为加密信息的字段。在一个特定的音频、视频及交互系统中，这个模块清单加入一般性的目录信息中，亦即目录模块的第一加密信息部分。在另一方案的音频、视频及交互系统中，指出一个特定的模块是否保护，只可以包括在目录中的各模块的其他加密信息字段。接收机系统编程的一部分，将包括用来检查目录，以获得模块加密信息，并按照这些信息对各个模块进行加密处理的例行程序。

模块的保护可以采取几种形式。第一种是用应用提供者的私人密钥对选定的模块进行加密处理。第二种方法是对模块执行“杂凑”处理功能，并把“杂凑”值填入目录模块中用于该模块的其余加密信息字段。第三种方法是对模块执行杂凑处理功能，并把杂凑值填入目录模块，再用应用提供者的私人密钥对选定的模块进行加密处理。第四种方法是对选定的模块执行杂凑处理功能，并把杂凑值附于该模块之后，对模块及其杂凑值进行加密处理，将加了密的杂凑值复制在目录模块中。在上述每一个例子中，目录模块都是在其他全部模块都处理过并将各模块的加密信息都填入目录模块之后，才进行加密处理的。

最佳的方法包括对各模块执行杂凑处理功能，并把各杂凑值插入目录模块的其余加密信息字段，然后对目录模块进行杂凑处理功能。然后用应用提供者的私人密钥对目录模块的杂凑值进行加密处理。

给信得过的应用提供者分配一个签了字的许可证，它包括诸如提

供者公共密钥、提供者的识别符、许可证的有效日期、或许还有接收机为提供者分配的存储器数量等项目。这个许可证用系统控制器的私人密钥签字。经过加密的杂凑值附在签了字的许可证后面，并将两者的组合附在目录模块的后面。目录模块和其他模块以未经加密的正文形式提供给系统控制器。选出来进行保护的而且经常变动的数据模块，通过提供者在该数据模块上的杂凑值上的签字来保护，该签字变成各模块的一部分。

事实上，应用提供者可能是较小的应用提供者小组的监督者。在这种情况下，该应用提供者可以提供用该应用提供者的私人密钥签字的副许可证，其中包括副提供者公共密钥、副提供者的识别符、许可证的有效日期、或许还有接收机为提供者分配的存储器数量等。这个副许可证还可以和由该应用提供者签了字的许可证一起附在目录模块后面。

该最佳保护模式并不保证排除试图检测/解释所传送的信息的窥探目光。然而，该保护方法，亦即包括许可证和对数据进行杂凑处理，有完成起来简单的优点，并且确实能够保证数据都来自权威的出处，而收到的数据的完整性是有保证的(如果在接收机上证实进行鉴别的话)。

对于信不过的应用提供者，亦即产生应用不细心，并可能威胁音频、视频及交互服务完整性的提供者，不提供许可证来附在他们的应用的后面。由信不过的提供者提供的应用，要交由信得过的鉴定权威鉴定。鉴定权威可以检查该应用的完整性，然后为保护目的对信不过的应用提供者的应用进行处理，最后将处理过的应用交给系统控制器。

下面参照图 1 和 5 进一步描述加密过程。包括各别的杂凑元件和加密元件 29 和 30，但是熟识数字信号处理本行的人都不难认识到，这两个功能都可以用软件由包括在元件 10 中的微处理机或者数字信号处理器 DSP 完成。一旦应用产生出来，并存入存储器 11{40}，程

序员将准备进行加密保护的模块选出/确定{41}。这些模块标以索引号(i)。给目录模块分配最高的索引号，以便最后进行处理。给每个准备处理的模块都分配一个置成 1 的“改变” 标志。在音频、视频及交互程序过程中，音频、视频及交互系统反复地发送该应用。一般，编码模块和某些数据模块在该程序过程中是不变的，但是，某些模块，例如数据模块会变化。在所述应用的反复发送过程中，没有变化的模块最好不要再进行加密处理，而仅仅再处理那些确实变化了的模块。建立“改变”标志是用来通知加密处理功能哪些模块在该程序进行的过程中应该再处理。开始时，每个准备加密保护的模块，其“改变”标志都设置成改变方式。元件 10 还确定系统控制器是否还有许可证可用。

操作索引号"i"设置为 0{42}，从存储器 11 访问第一个模块 M(0)。测试该模块的“改变”标志{44}，然后将其清零{45}。如果以前处理过，而且“改变”标志表明没有变化，系统就跳到{56}步，将索引号加一，访问下一个模块。如果“改变”标志表明该模块发生了变化，就将其提交给杂凑函数处理器 29{46}。该特定的杂凑函数维持的比较简单，以便限制对各个接收机提出的处理要求。该函数可能是单向函数。杂凑函数应该是计算上快速的，但又极难解密或击破。作为例子举出的杂凑函数是基于一个 256 码字的矢量 W，每个码字 128 位长。准

备进行杂凑处理的数据，分段成唯一的 256 位数据块 D，其中 D = d1,

d2, d3, d4...d256。一个基本杂凑函数 BH（D）定义如下:

$$BH(D) = \sum_{x=1}^{256} dx\, Wx \bmod 2^{128}$$

如果有 n 个数据块 D，则由函数 BH（D）便产生 n 个值，B1, B2, B3,... Bn，每个 128 位长。为了计算整个数据的杂凑值，将立即结果

Bi 按如下方式组合：令<Bi, Bj>代表 128 位块 Bi 和 Bj 串合并而得的 256 位数，则将对整个数据的杂凑值 H(D)定义为：

H(D) = BH(<BH(...(<BH(<BH(<B1,B2>),B3>),B4>),...),Bn>)

作为另一方案，函数 H(D)可以具有如下形式：

H(D) = B1 XOR B2 XOR B3 XOR ... Bn

对模块进行杂凑的推荐的杂凑函数是众所周知的函数 MD5(MD 代表 Message Digest(信息摘要), 而 MD5 是 R. Rivest 在 RFC， 1992，四月， 1321，题为"The MD5 Message Digest Algorithm"一文中描述的)。一旦模块进行了杂凑处理，就要测试{47}确定该模块在该程序运行的过程中预期是否变化。如果预期要变化，则杂凑值 H(D)不放在目录中，而附在放在存储器 11 中的模块后面{48}。(另一方案是，用提供者的私人密钥对该杂凑值进行签字(加密)，然后附在放在存储器 11 中的模块后面)。将索引值加一{56}，从存储器访问下一个模块。如果在步{47}确定模块是不变化的，则进行测试{49}，以确定该模块是否目录模块。如果不是，则将模块 M(i)的杂凑值 H(M(i))放在目录模块{50}，不是放在第一加密信息字段，就是放在各模块的其他信息字段中。将索引值加一{56}，从存储器访问下一个模块。

如果在测试步{49}确定该模块是目录模块， 则把索引值 H(M(i))加在编码器 30 上，用提供者的私人密钥进行加密。(如有要求，这时可将整个目录模块加在编码器 30 上，进行加密。)取出许可证{52}，将加了密的杂凑值附于其后{53}，并将后附了杂凑值的许可证附在存储器 11 中的目录模块后面{54}。设置一个标志{55}，向数据分组处理器/编码控制器表明， 该程序已经准备好发送。系统跳到{42}步，将索引值清零。系统进一步检查模块是否发生了变化，并且在该程序运行的过程中在该应用反复发送时，只对变化了的模块进行再杂凑。正如前面已经指出的， 应用提供者可以加入签了字的信息/许可证，附在目录模块的后面。签字在编码器 30 中用提供者的私人密钥进行。

在一个替代的实施例中，可以取消加密步 51 。在再一个实施例

中，所有进行杂凑处理的模块的全部杂凑值都进行加密。

图 12 说明推荐的目录模块的格式。该目录模块采取未经加密的正文形式。只有目录的签字（杂凑值）和许可证是加密的。前者用提供者的密钥加密，后者用系统控制器进行加密。另外，当各模块进行杂凑处理时， 进行杂凑之前，在每一个这样的模块前面，加上 ASCII 形式的某些与系统控制器/提供者有关的预定的正文，例如正文 "OpenTV (TM) "，所以各模块的签字是例如， H(OpenTV(TM)+模块)，而目录模块的签字是加了密的杂凑值 H(OpenTV(TM) +目录模块)。这一点在图 1 中用附在存储器 11 的方框 OTV 表示，其涵意是，这里存有正文"OpenTV (TM) "的数字形式，当读出时，它可以与各模块一起进行多路切换，并加在杂凑函数元件 29 上。

在图 12 中的目录模块表示由 Thomsom Comsumer Eletronics Inc (汤姆森日用电子公司）开发的商标为 OpenTV TM 的音频、视频及交互系统推荐的格式。下面立即要描述其中所用的许可证、公共密钥、及其中所用的签字的格式。

所有的许可证、密钥和签字都是 BIG - ENDIAN 格式的多字节字段。这种与结构无关的格式便于在各种不同接收机结构之间移植。 任何 OpenTV 许可证都是固定结构后跟变长部分的组合，后者包括有待证实的公共密钥和 OpenTV 控制器的签字。

有两种许可证将由 OpenTV 控制器发布。

1.发给应用生产者的生产者(提供者)许可证。

2.专门发给交易服务器的服务器(系统控制器)许可证，生产者(提供者)将应用交给交易服务器，后者建立加密通信。

另外，控制器可以发用户许可证。 OpenTV 从不在内部对这种许可证进行分解，而只供外界使用。 OpenTV 系统只知道这种许可证的大小。除了 OpenTV 规定的 4 字节的标题之外， 许可证的其余部分可以保密，并且可以是标准的 X.509 许可证。

下列是许可证公用部分的大小。

CERTIFIDATE_FLAG_LENGTH (4 字节) (可证标志长度)

PUBLIC_KEY_SIZE_LENGTH (4 字节) (公共密钥长度)

一个 OpenTV 控制器发的许可证从 32 字节描述许可证的标志结构开始。不同标志的位置和意义描述如下。对于 OpenTV 许可证结构可能扩展的标志是为 OpenTV 基本许可证设置的，而不是为扩展设置的。该标志的定义如下。

BASIC_CERTIFICATE (0X80000000) (基本许可证)

可以准确地设置成下列 3 个标志之一。

SERVER_CERTIFICATE (0X40000000) (服务器许可证)

PRODUCER_CERTIFICATE (0X20000000) (生产者许可证)

USER_CERTIFICATE (0X10000000) (用户许可证)

在对这 32 位字段的解释方面，服务器/生产者许可证与用户许可证之间是不同的。如果许可证具有用户许可证的外表，则该字段的最后 16 位在实际上是其大小，包括开始的 32 位。

至于服务器/生产者标志，检查头 4 位之后，就已经知道正在被检验的实体，否则该许可证就被认为是扩展到当前系统以外。下面 4 位指出使用哪一种 OpenTV 控制器公共密钥来产生签字。它们代表 0-15 的数字 N。如果 0<=N<=14，则采用第 N 个嵌入的公共密钥。如果 N=15，则所用的公共密钥是通过外部受托信道接收的最后一个密钥。在系统内部，密钥数字只能增加。就是说，如果在内部密钥是 5，而且出现带有密钥 6 的许可证，并被检验通过，则内部密钥变成 6，密钥小于 6 的许可证将不被接受。最后，如果而且当全部内部密钥都击破，则公共密钥只能从外部受托信道接收。

下一字节保留用于描述许可证。当前不使用。下两个字节提供关于生产者/服务器的信息和有待检查的密钥。头一个字节含有描述有关公共密钥的算法的标志。这对服务器和生产者都是共用的。下一个和最后一个字节对于服务器和生产者是不同的，故分别描述。

算法字节标志是:

RSA_3_WITH_MD5 (0X00008000)

RSA_WITH_MD5 (0X00004000)

对于生产者许可证最后字节目前尚无标志定义。对于服务器许可证最后字节目前只定义了一个标志，用来表明服务器是否是受约束的。从功能的观点来看，受约束的服务器在第一次建立机密链路时，不要求连接对方的任何信息。这使链路的建立大大加快。

SERVER_CONSTRAINED (0X00000080) (服务器受约束)

生产者签字可供外部使用的固定部分由一个规定签字的类型的两字节标志字段和一个给出签字大小的 2 字节标志字段组成。

PRODUCER_SIGNATURE_FLAGS_LENGTH (2 字节) (生产者签字标志长度)

PRODUCER_SIGNATURE_SIZE_LENGTH (2 字节) (生产者签字尺寸长度)

当前只有一个标志是有意义的，即帮助标志。如果如在生产者许可证中规定的，生产者签字算法是 RSA_3_WITH_MD5，则该生产者在签字后面有一个加入附加帮助数据以加快检查的选项，并将其标出。

PRODUCER_SIGNATURE_ASSIST (0X8000) (生产者签字帮助)

现描述生产者、服务器和 OpenTV 框的公共密钥的结构(RSA 用)。为了移植性，模数和指数的大小必须是 4 字节的倍数。OpenTV 还要求，若将模数的大小表示为 S 字节，则模数表达为 BIG_ENDIAN 格式时，其前 32 为必须为非零。这并不是一个限制，因为该大小可以表述为 S-4 或更小。

公共密钥包括

fixed_public._key_t (固定公共密钥_t)

后跟

指数 (采用 BIG_ENDIAN 格式)

后跟

模数（采用 BIG_ENDIAN 格式）

生产者/服务器许可证包括含有 OpenTV 控制器对许可证的描述的明文(未加密的正文)部分，后跟数据类型如上述的生产者/服务器的公共密钥，另外还有密文部分，它是取决于明文数据的 OpenTV 控制器对数据的数字签字 S。在这一阶段，生产者/服务器有权选择只用 S，或者除签字以外，再加入附加数据(亦即 Q1 和 Q2)，以便使检查变得容易。

生产者/服务器需要在明文与签字 S 之间加入 4 字节信息，或许在 S 以外加入某些信息以协助检查。这 4 字节信息包括标志字段和构成签字和帮助信息的数据总量的大小。这两个字段的大小是 L

CERTIFICATE_SIGNATURE_INFO_FLAGS_LENGTH (2 字节)

(许可证签字信息标志长度)

CERTIFICATE_SIGNATURE_SIZE_LENGTH (2 字节)

(许可证签字大小长度)

目前只定义了一个标志，RSA_3_ASSIST(RSA_3_帮助)标志。如果设置，则除签字 S 之外还有帮助信息，这是前述的两个商 Q1 和 Q2。这个标志定义为:

RSA_3_ASSIST　(0X8000)　(RSA_3_帮助)

上面描述了模块一级的加密情况。在传送分组一级这可能会被其他加密方法覆盖。就是说，当各模块分成传送分组的有效载荷以便传送时，有效载荷会被加密，而这与授权检验过程无关。

回到对系统的一般描述来，通过例如，电话 MODEM(调制解调器)在提供者与接收机之间进行双向通信，将涉及利用 RSA 或数据加密标准 DES 加密法的加密通信问题。应用必须提交它希望与之通信的服务器的检验合格的公共密钥版本。只要应用提供者识别符与许可证上的服务器的识别符匹配，就建立交谈密钥，而密钥的交换将使用许可证上得到的密钥。

图 8 以框图的形式表示音频、视频及交互信号接收机或集成接收

解码器的一部分，包括反相传送分组处理器的元件。信号由天线 80 检测出来，加在调谐检波器 81 上，后者将收到信号的特定频带取出，提供基带多路分组信号。频带由用户利用普通的方法通过集成接收解码器系统控制器 89（这里是集成接收解码器控制器）选择。一般，广播的音频、视频及交互信号是例如利用 Reed-Solomon 前向纠错编码法(FEC)进行纠错编码的。这样，基带信号加在 FEC 译码器 82 上。FEC 译码器 82 使收到的视频信号同步，并提供图 3 所示类型的信号分组流。FEC 12 可以以相等的间隔，或者按要求，例如，按存储器控制器 87 的要求提供分组。不论是在哪一种情况下，FEC 线路都提供分组框或同步信号，指出各分组信息从 FEC 82 传送次数。

只有从单一的音频、视频及交互信号中来的分组才可以被接收机处理一次。在这个例子中，用户不知道要选择哪一个分组。这个信息含在程序指引中。这是一种特殊的程序，后者由通过它们各自的服务通道识别符与程序信号成分有关的数据组成。程序导引是每个程序的列表，包括各个程序的音频、视频和数据成份的服务通道识别符。分配给程序导引(图 2 中分组 D4) 的是一个固定的服务通道识别符。当接收机加电时，集成接收解码器控制器 89 在程序控制下将与该程序导引相关的服务通道识别符装入服务通道识别符检测器 84，后者可以是一排匹配的滤波器。检测到程序导引的服务通道识别符时，存储器控制器 87 控制得使相应的分组有效载荷引导到由集成接收解码器控制器使用的存储器 88 的预定位置。

集成接收解码器控制器等待用户通过界面 90 发来的编程命令，界面在图中所示是键盘，但可以是普通的遥控器，或者接收机面板开关。用户可以请求看看通道 4 上演播的节目(用模拟电视系统的行话来说)。集成接收解码器控制器 89 在程序控制下扫描已经装入存储器 88 的通道 4 节目成分的各服务通道识别符用的程序导引列表，并将该服务通道识别符装入服务通道识别符检测器 84。

对于要看的节目，接收的音频、视频或数据节目成分分组，最后

必须分别被送到各音频 93 、视频 92 或辅助数据 91(94)信号处理器。数据是以相对恒定的速率接收到的，但是，信号处理器一般要求输入数据呈脉冲串形式（例如， 按照各解压类型）。图 8 作为例子举出的系统，首先将各分组送至存储器 88 内的预定存储器位置。此后，各处理器 91 — 94 从存储器 88 请求成分分组。通过存储器发送各成分，提供了一种要求的信号数据速率缓冲或节流的措施。

音频、视频或数据分组装入存储器各预定的位置，以便使信号处理器能够容易地访问该成分数据。各成分分组的有效载荷，根据相应服务通道识别符和服务通道识别符检测器提供的控制信号，装入存储器适当位置。这种联系可以通过存储器控制器 87 内的硬接线实现，或者通过程序实现。

各信号分组从 FEC 82 通过一个信号反扰频器 86 耦合到存储器控制器 87 。只有信号的有效载荷才进行扰频，而分组的标题是不加改变地通过反扰频器的。一个分组是否要反扰频，取决于分组前缀中的 CF 标志(图 3)，而如何进行反扰频，则由 CF 标志指导。这个分组的扰频过程与上述应用模块的加密处理无关。反扰频装置可用一般解密装置实现，根据需要可以用来对接收到的许可证和其他数据进行解密。但是，在下面对发送应用的处理的描述中，解密是用其他装置完成的。

音频、视频及交互系统可以包括若干个能够操作音频、视频及交互信号的程控数据部分的装置。例如，在图 8 中， AUX1 和 AUX2 处理器都可以响应音频、视频及交互信号的程控数据部分。 AUX1 处理器可以是一台安排来检测发送的股票市场数据、并以发送的交互应用来处理该种数据的个人计算机。 AUX2 可以是一个电视系统，安排来在发送交互商业方面的交互促销。 应该指出，交互性可以借助与图 8 系统连接的电话调制解调器(未示出)来使之易于实现。另外，可以通过编程使集成接收解码器控制器 89 处理和执行发送来的应用，特别是系统维护。与发送的交互应用有关的接收机功能，将在能与发送的应用一起操作的集成接收解码器控制器 89 的情况下进行描述。(应该指

出，交互性并不一定意味着用户与提供者交互，虽然这是交互性的一个方面。交互性还包括用户能够按照发送的应用，在用户端影响信号/系统，特别是在教育节目领域)。

图 9 比较详细地显示图 8 的集成接收解码器控制器。所示的集成接收解码器控制器 89，包括杂凑函数处理器 96、解密器 97、调制解调器 98 和 EPROM 99。杂凑函数发生器 96 和解密器 97，可以用硬件或者软件实现。控制器处理器(μ PC)可以包括随机存储器 RAM 和一般系统指令编程用的只读存储器 ROM。其他系统指令包含于 EPROM 99 中。ROM 和 FPROM 是在制造时编程的，所以系统是可操作的。但是，在这个例子中，EPROM 可以通过交互发送程序再编程，以改进系统功能。

假定，在制造时，通过编程使系统在上午 1：00 和上午 4：00 之间早上接收机不使用时，查找系统维护服务通道识别符，使得系统提供者能够用新的系统增强来改进各个接收机。早上 1：00 和 4：00 之间接收机不使用，μ PC 将编程服务通道识别符检测器，查找含有系统维护服务通道识别符的分组，并准备存储器 88 接收程序数据。程序模块检测的一个例子示于图 10。

服务通道识别符检测的编程和存储器的准备是启动过程的一部分{100}。一旦服务通道识别符监测器的程序编好，系统空运行{102}，直至检测到一个含有系统服务通道识别符的分组。一旦检测出这样的分组，检测该分组{104}，以确定它是否含有发送单元或模块标题。若非如此，将该包弃置，系统等待{102}下一个应用分组。假定装入任何一个应用程序所需的信息本身包含在程序中(发送单元的标题或者目录模块的标题)，因此，系统被迫不得装入任何一个检测出的分组，直至有一个带有相应标题信息的分组可用为止。当监测到一个适当的分组将其有效载荷装入存储器 88{106}。系统等待{108}下一个系统维护分组，而当监测到时将其{110}装入存储器 88。每个分组装入存储器 88 后，进行测试{112}，以确定是否整个模块都装入了。如果模块尚

未装完，系统跳回到{108}步，等待下一个分组。如果模块已经完成，则列出模块清单{114}。

进行下一个测试{116}，确定完成的模块是否目录模块。若是，则立即试图确定应用提供者的有效性。将附于目录模块后面的许可证解密{122}，并检查其内容{124}。如果许可证的内容无效，启动警告显示，通知用户检测出未经授权的提供者。在这一点上，可以采取多个方案，包括 a)在步{100}处从新启动该过程； b)关闭该过程 24 小时；c)弃置该目录模块并等待下一个目录模块等。图 11 表示更详细的鉴别过程。如果在测试步{16}检测出目录模块，则访问许可证及附在模块后面的加了密的杂凑值{122}。将许可证加到解密器 97，利用预先分发给各接收机并存于接收机中的音频、视频及交互系统控制器公共密钥进行解密{1222}。将解了密的许可证加到μ PC 上{1241}。μ PC 从 EPROM 访问相应的项目，{1242}与有关项目比较。例如，许可证中含有识别符，将其与授权的识别符清单进行比较。另外，许可证可以包括截止时间和日期与当前的时间和日期比较等。如果项目与储存在接收机中的项目对比一致{1243}，则将在许可证中发送来到应用提供者公共密钥加在解密器上，并用来解密附在目录模块后面的加了密的杂凑值，或者解密应用提供者提供的任何加了密的数据。(在这方面，如果整个目录模块都加了密，则可从存储器访问，并在将应用提供者的私人密钥加在解密器的情况下进行解密。)另一方面，如果比较的项目证实是无效的，或者许可证已经过期，则显示报警信息{130}。

如果应用提供者证实是有效的，则将目录模块加在杂凑函数元件 96 上，进行杂凑处理{126}，并在μ PC 中将杂凑值与加了密的附在目录模块后面的目录模块杂凑值比较{128}。在最佳的实施例中，某些与系统控制器/提供者有关的预先确定的正文的 ASCII 版本，例如"OpenTV(TM)"等，在进行杂凑处理之前加在各模块的前面，所以各杂凑值等于例如，H(OpenTv(TM)+模块)。这在图 9 中，用附在存储器 88 上面的 OTV 框表示，其涵意是正文"OpenTV(TM)"的数字版本，例如

可以储存在存储器 88 中，当其从存储器读出时，与目录模块一起进行多路切换。如果杂凑值不相同，即认为目录模块含有错误，并将其从存储器弃置，先前装入的模块从清单中删除{134}{114}，系统返回{108}步，等待下一个分组。

如果目录模块中的杂凑值与附后的杂凑值一致，则从目录中取出各程序模块的杂凑值{129}，用来检查接收到的程序模块的完整性。系统跳到{118}步，测试是否全部程序模块都已装入存储器。如果还没有，安排{120}下一个模块的存储器地址，系统返回{108}步，等待下一个适当的分组。

如果{118}处的测试表明，应用程序已经完全装入存储器，则检查各程序模块的传输完整性。{136}从存储器访问各模块，加到杂凑函数元件 96 上，{138}进行杂凑处理。在μ PC 中{140}，将各杂凑值与目录模块中发送的相应的杂凑值，或者附在正在受试的特定模块后面的杂凑值进行比较。如果杂凑值不一致，则认为该模块含有错误，并弃置之{150 ， 152}， 或者进行测试{142}，以确定是否全部模块都检查过了。如果全部检查过，则进行测试{146}，以确定是否一个完全的加密检查的应用驻留的存储器中。若非如此，系统返回{120}步，开始装载一个新的模块。如果应用是完整性的，则执行之{148}。在这个例子中，程序将指令μ PC 去访问程序数据模块中特定的数据，并用发送来到数据来对 EPROM 重新编程。

一旦开始执行，程序就让系统继续从发送的信号中提取程序分组。接收到时，检查各标题的版本号，如果一个特定模块的版本号发生变化，这个模块要进行杂凑处理，如果杂凑值检查通过，则带有新版本号的模块将代替原先的相应模块。

接受装置中的各种不同的装置可以采用特定的发送的应用，并可以在执行该应用之前通过编程完成要求的加密处理。在最佳实施例中，为了避免编程或硬件的重复，加密处理有集成接收解码器控制器完成。当加密处理需要用程序导引中所含的信息来完成时，集成接收

解码器控制器会发出通知。

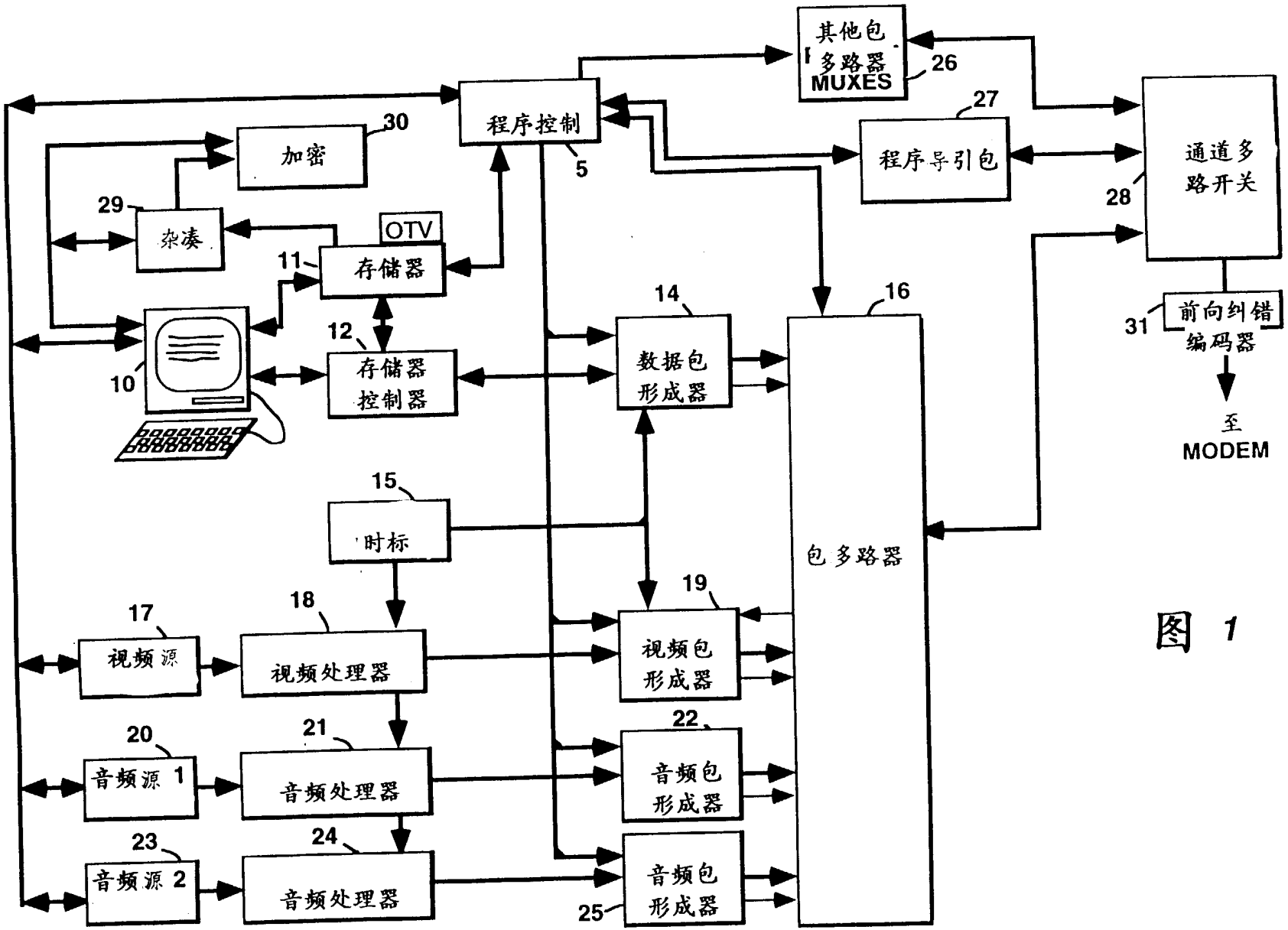
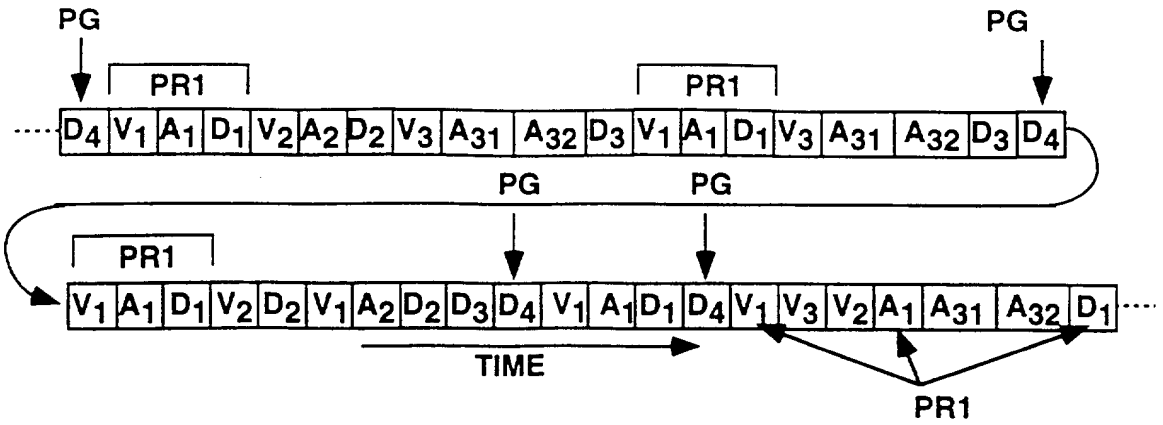

其他包多路器 MUXES
26
程序控制
5
27
程序导引包
通道多路开关
28
30
加密
29
杂凑
OTV
11
存储器
12
存储器控制器
10
14
数据包形成器
16
31
前向纠错编码器
至 MODEM
15
时标
包多路器
19
视频包形成器
17
视频源
18
视频处理器
20
音频源 1
21
音频处理器
22
音频包形成器
23
音频源 2
24
音频处理器
25
音频包形成器

图 1

说 明 书 附 图



V_1 A_1 D_1 程序 # 1 信号成份包

V_2 A_2 D_2 程序 # 2 信号成份包

V_3 A_{31} A_{32} D_3 程序 # 3 信号成份包

D_4 程序指引包

图 2

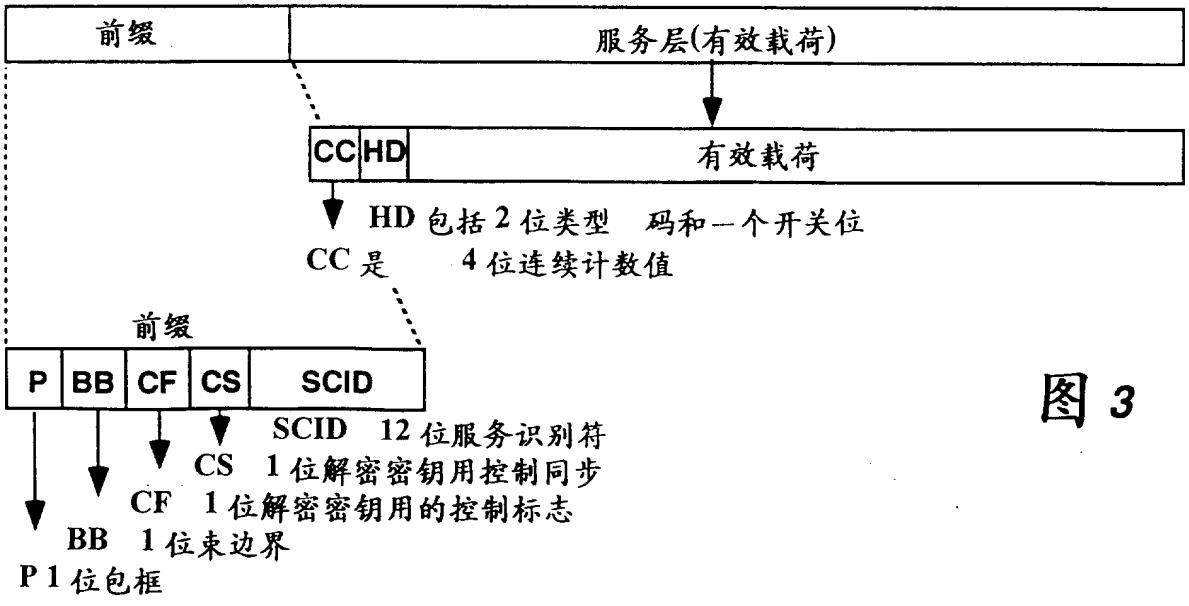


图 3

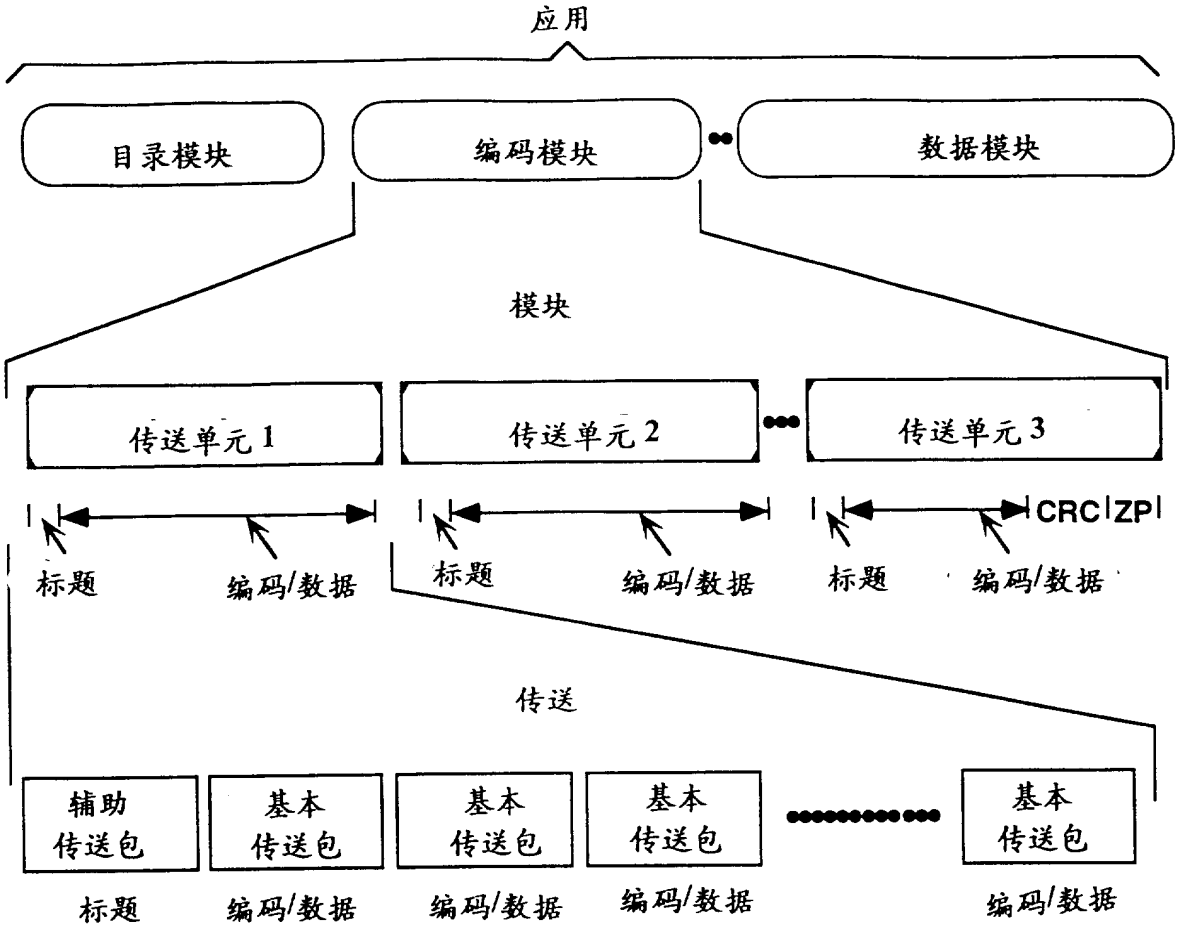


图 4

表 1

位	功能
16	模块识别符
32	包括 CRC 模块总字节数
32	模块版本号
32	模块传送单元字节偏移量
32	传送单位字节长度
XX	保留

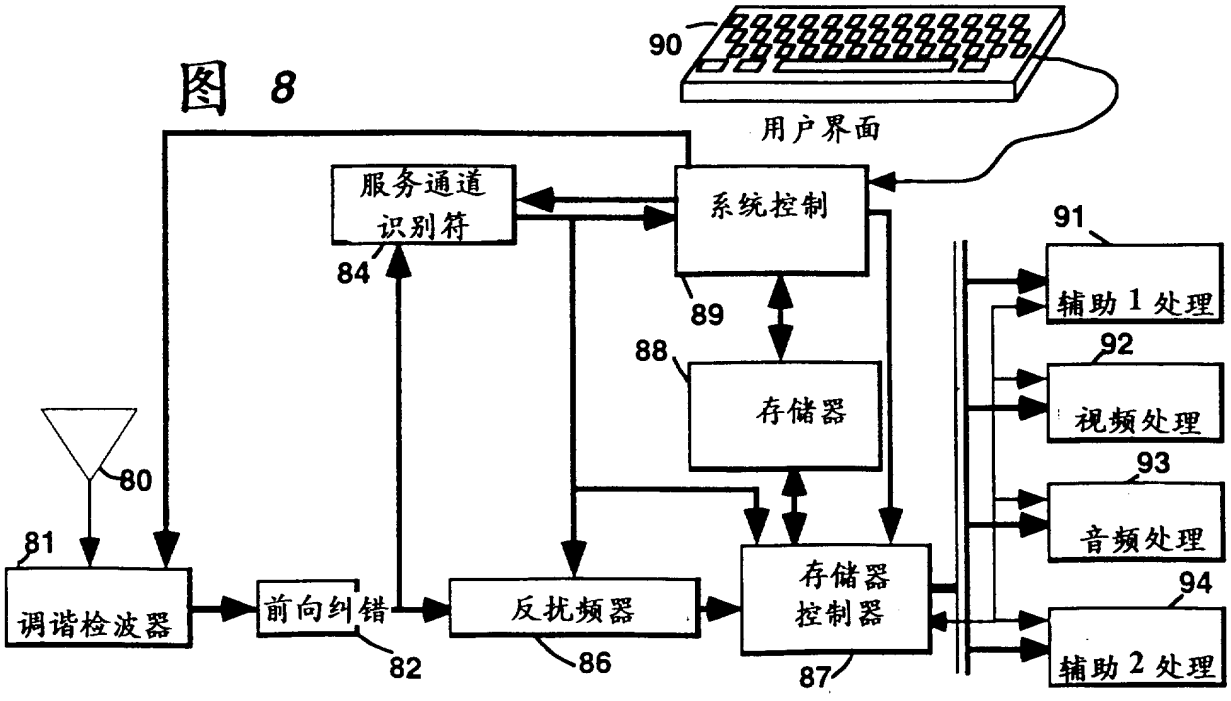
图 5

图 6

表 2

位	功能
32	应用识别符
YY	应用类型
ZZ	应用描述符
32	应用解密内存需求
16	总模块计数
XX	第一加密信息
	各模块
16	指向模块串表的指针
16	模块识别符
32	模块版本号
32	包括 CRC 的模块长度
32	译码器内存需求(若为编码模块)
32	其他标志
XX	模块名串表、串以空字符结尾
NN	第二加密信息
签字的许可证	
杂凑	

图 8



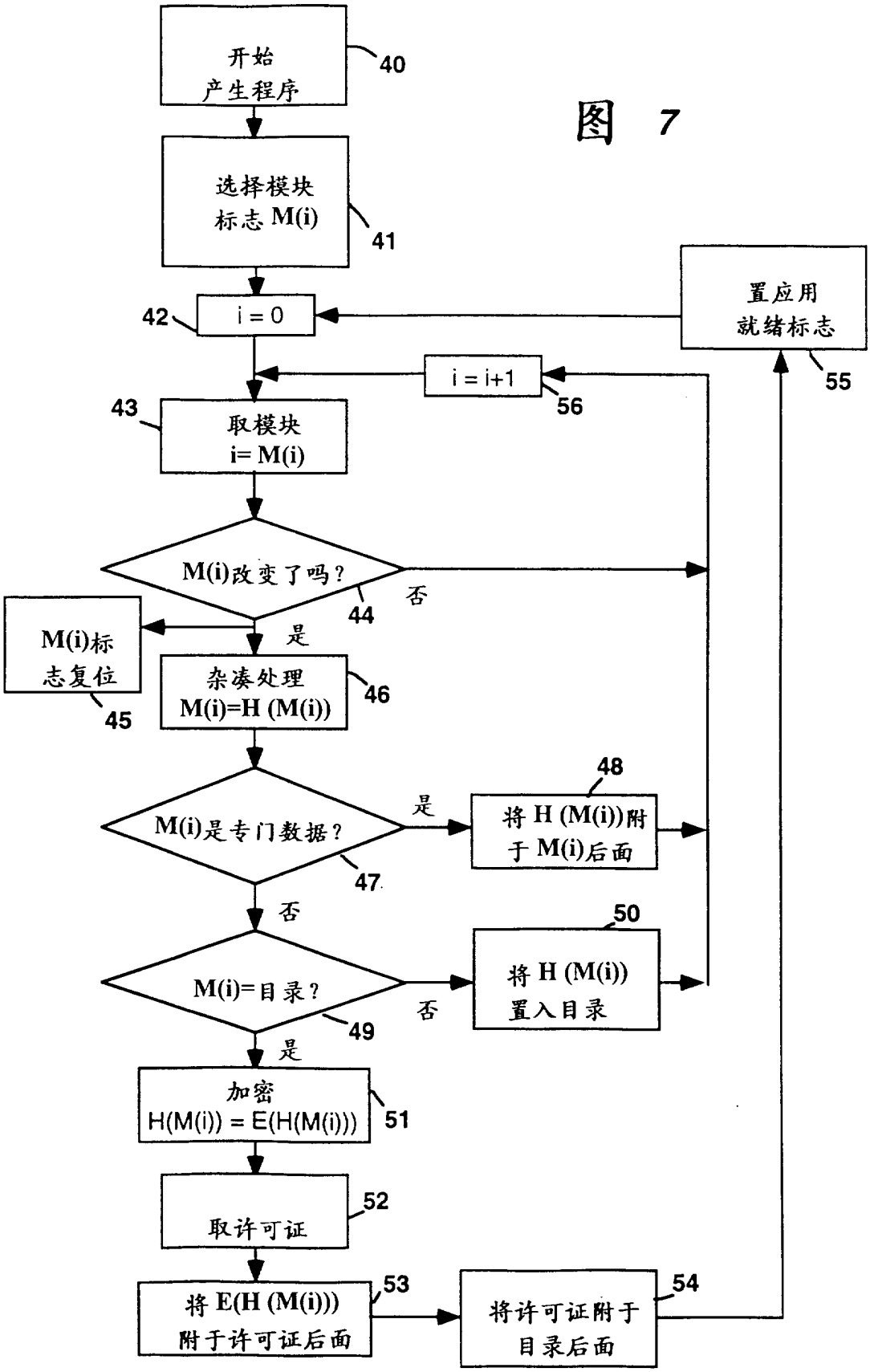
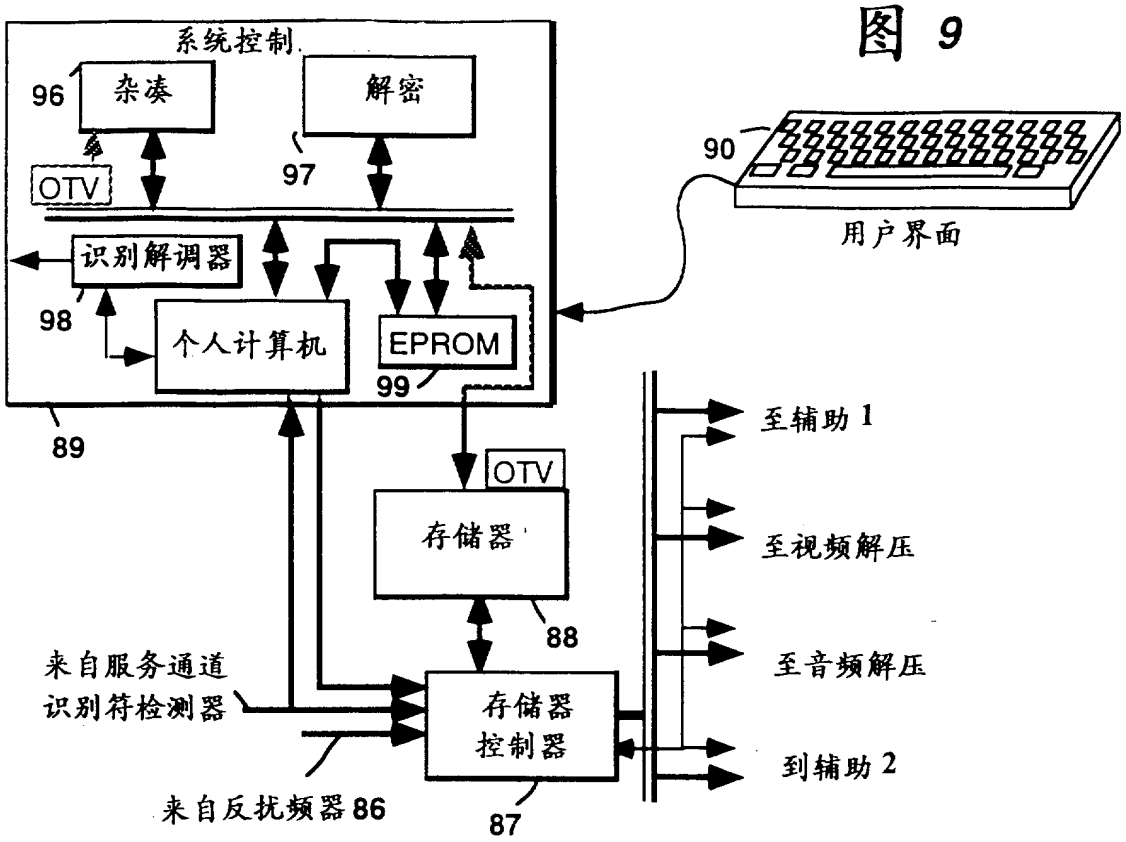

开始
产生程序
40
选择模块
标志 M(i)
41
置应用
就绪标志
55
42
i = 0
i = i+1
56
43
取模块
i= M(i)
M(i)改变了吗？
44
否
是
M(i)标
志复位
45
杂凑处理
M(i)=H (M(i))
46
48
M(i)是专门数据？
47
是
将 H (M(i))附
于 M(i)后面
否
50
M(i)=目录？
49
否
将 H (M(i))
置入目录
是
加密
H(M(i)) = E(H(M(i)))
51
取许可证
52
将 E(H (M(i)))
附于许可证后面
53
54
将许可证附于
目录后面

图 7

图 9


系统控制
96
杂凑
解密
97
OTV
90
用户界面
识别解调器
98
个人计算机
EPROM
99
89
至辅助 1
OTV
存储器
至视频解压
88
来自服务通道
识别符检测器
存储器
控制器
至音频解压
到辅助 2
来自反扰频器 86
87

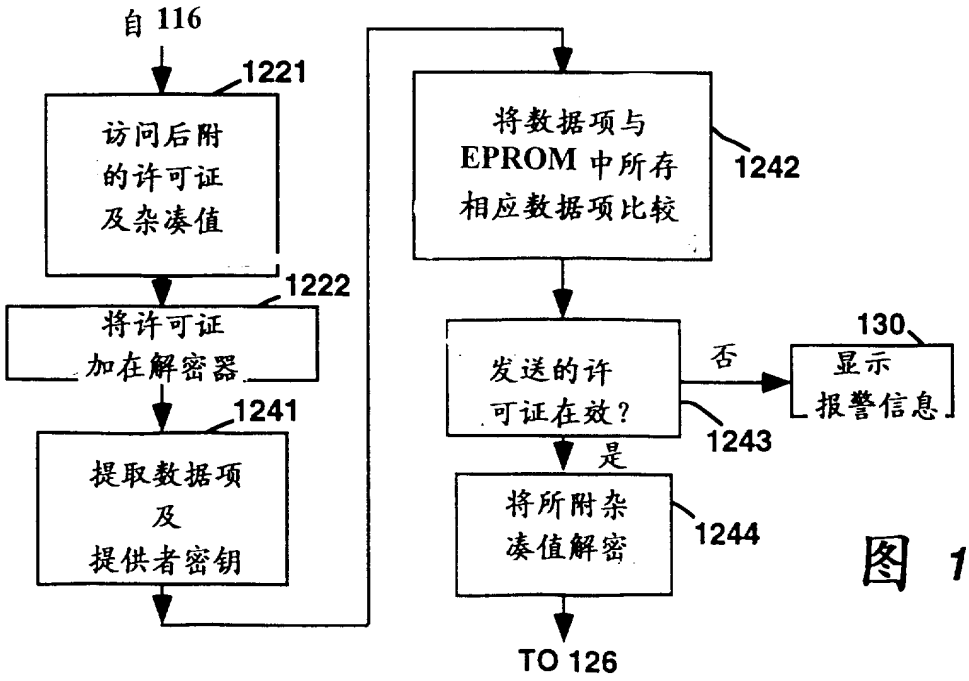

自 116
1221
访问后附
的许可证
及杂凑值
1222
将许可证
加在解密器
1241
提取数据项
及
提供者密钥
将数据项与
EPROM 中所存
相应数据项比较
1242
发送的许
可证在效?
否
130
显示
报警信息
1243
是
将所附杂
凑值解密
1244
TO 126

图 11

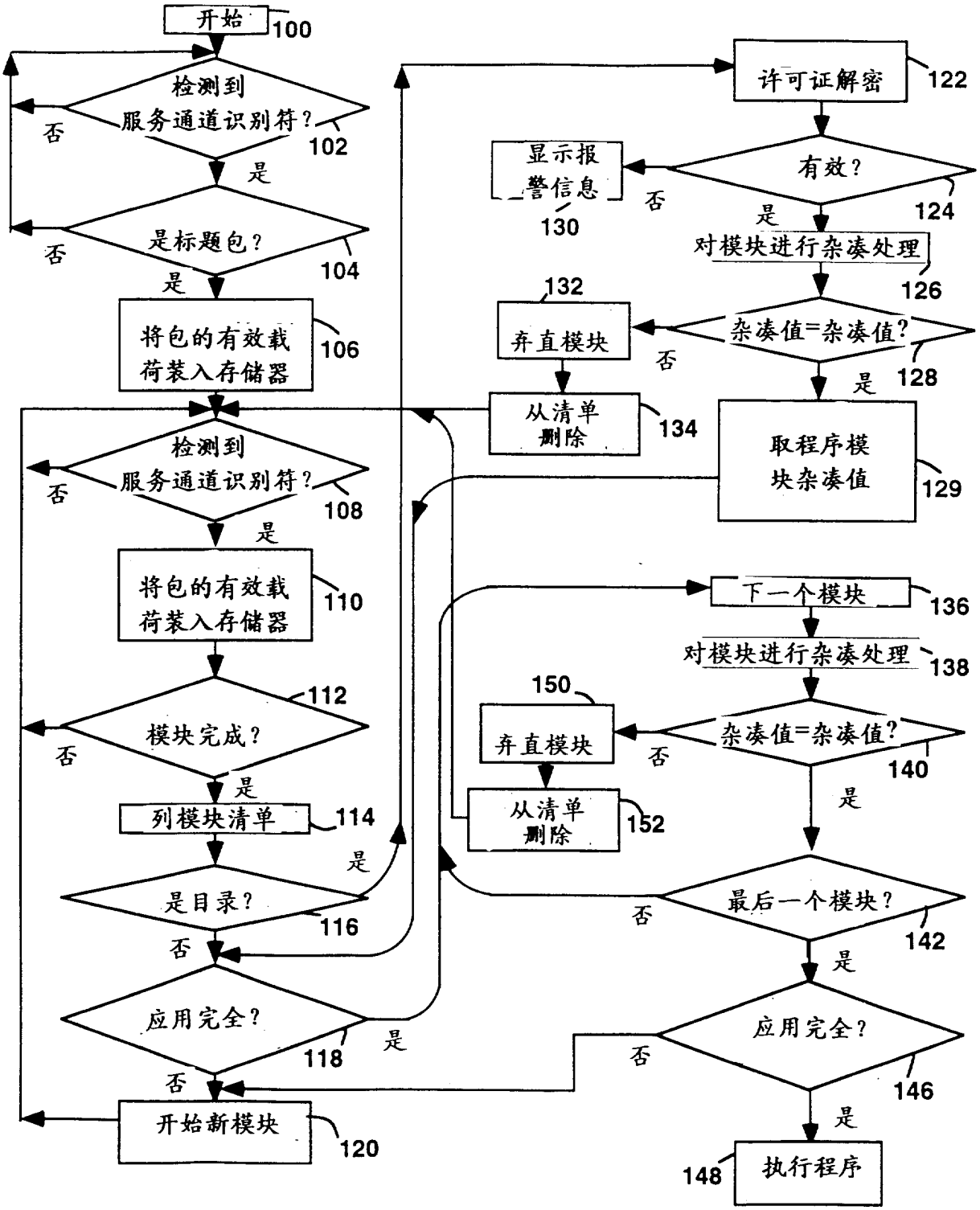

开始
100
检测到服务通道识别符?
102
否
是
是标题包?
104
否
是
将包的有效载荷装入存储器
106
检测到服务通道识别符?
108
否
是
将包的有效载荷装入存储器
110
模块完成?
112
否
是
列模块清单
114
是目录?
116
是
否
应用完全?
118
是
否
开始新模块
120
许可证解密
122
有效?
124
否
是
显示报警信息
130
对模块进行杂凑处理
126
132
弃直模块
杂凑值=杂凑值?
128
否
是
从清单删除
134
取程序模块杂凑值
129
下一个模块
136
对模块进行杂凑处理
138
150
弃直模块
杂凑值=杂凑值?
140
否
是
从清单删除
152
最后一个模块?
142
否
是
应用完全?
146
否
是
执行程序
148

图 10

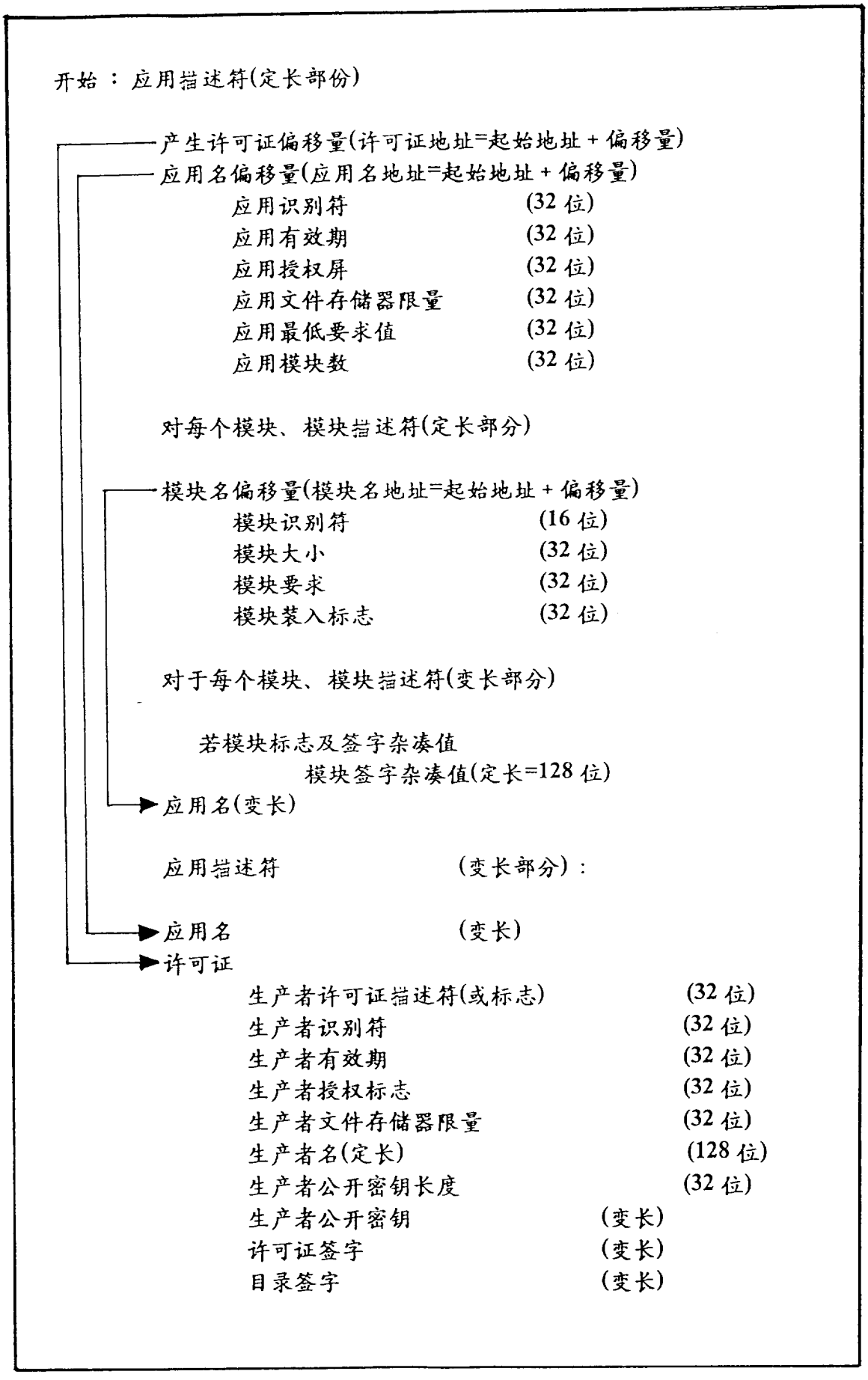

开始：应用描述符(定长部份)
产生许可证偏移量(许可证地址=起始地址+偏移量)
应用名偏移量(应用名地址=起始地址+偏移量)
应用识别符 (32 位)
应用有效期 (32 位)
应用授权屏 (32 位)
应用文件存储器限量 (32 位)
应用最低要求值 (32 位)
应用模块数 (32 位)
对每个模块、模块描述符(定长部分)
模块名偏移量(模块名地址=起始地址+偏移量)
模块识别符 (16 位)
模块大小 (32 位)
模块要求 (32 位)
模块装入标志 (32 位)
对于每个模块、模块描述符(变长部分)
若模块标志及签字杂凑值
模块签字杂凑值(定长=128 位)
应用名(变长)
应用描述符 (变长部分)：
应用名 (变长)
许可证
生产者许可证描述符(或标志) (32 位)
生产者识别符 (32 位)
生产者有效期 (32 位)
生产者授权标志 (32 位)
生产者文件存储器限量 (32 位)
生产者名(定长) (128 位)
生产者公开密钥长度 (32 位)
生产者公开密钥 (变长)
许可证签字 (变长)
目录签字 (变长)

图 12