(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1897526 B
(45)授权公告日 2012.07.04

(21)申请号 200610105405.7
(22)申请日 2001.01.11
(30)优先权数据
00400912.2 2000.04.03 EP
(62)分案原申请数据
01810646.3 2001.01.11
(73)专利权人 汤姆森许可公司
地址 法国布洛涅－比扬古
(72)发明人 J·-B·G·M·伯奎 P·普莱恩
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 程天正 陈景峻
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
CN 1276613 C,2006.09.20,6-8,29-31,44.
US 5867578 A,1999.02.02, 全文.
US 5745574 A,1998.04.28, 全文.
US 5956408 A,1999.09.21, 全文.

审查员 王国纲

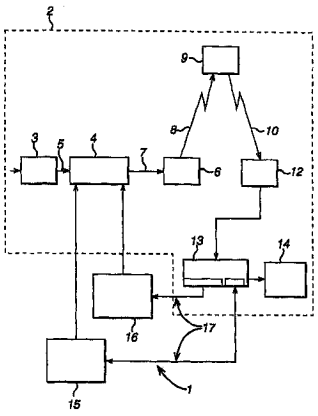
权利要求书 2 页 说明书 15 页 附图 11 页

(54)发明名称

数字传输系统中发送的数据的鉴权

(57)摘要

在数字传输系统中发送的数据的鉴权方法，其中方法包括以下步骤，在传输之前，确定对于至少某些数据的至少两个加密的数值，每个加密数值可通过使用各个加密算法的密钥来确定，以及连同所述数据一起输出所述至少两个加密的数值。



CN 1897526 B

1. 一种对在数字传输系统 (1) 中所发送的数据 (130) 进行鉴权的方法，其特征在于，所述方法包括在传输之前进行以下步骤：

为至少一些数据 (130) 确定至少两个加密的数值 (146)，每个加密数值 (146) 是使用相应加密算法的密钥而为相同的数据确定的；

确定要被撤销的公共密钥的识别符 (140)；以及

连同所述数据 (130) 一起输出所述至少两个加密数值和要被撤销的公共密钥的所述识别符 (140)，

其中在数字传输系统 (1) 中所发送的数据 (130) 包括替代根证书。

2. 权利要求 1 的方法，其中识别符 (140) 包括数字证书的识别符。

3. 权利要求 2 的方法，其中所述数字证书的识别符是根证书序列号。

4. 权利要求 1 的方法，其中在数字传输系统 (1) 中所发送的数据 (130) 包括对于撤销的时间和数据。

5. 一种对在数字传输系统中所发送的数据 (130) 进行验证的方法，其特征在于，所述方法包括以下步骤：

接收所述数据 (130)、要被撤销的公共密钥的识别符 (140)、和为至少一些该数据而确定的至少两个加密的数值 (146)，每个加密数值 (146) 是使用相应的加密算法的密钥而为相同的数据确定的；

使用所述相应的加密算法的已存储的密钥来处理 (204) 每个加密数值从而形成得到的数值；

把每个得到的数值与所述至少一些数据 (130) 进行比较 (206)，以鉴权所述至少一些数据；以及

存储 (208) 要被撤销的公共密钥的所述识别符 (140)。

6. 权利要求 5 的方法，其中识别符 (140) 包括数字证书的识别符。

7. 权利要求 6 的方法，其中所述数字证书的识别符是根证书序列号。

8. 权利要求 5 的方法，其中数据 (130) 包括替代根证书。

9. 权利要求 5 的方法，其中数据 (130) 包括对于撤销的时间和数据。

10. 对在数字传输系统 (1) 中所发送的数据 (130) 进行鉴权的设备，其特征在于，所述设备包括：

用于为至少一些所述数据 (130) 确定至少两个加密的数值 (146) 的装置，每个加密数值 (146) 是使用相应的加密算法的密钥而为相同的数据确定的；

用于确定要被撤销的公共密钥的识别符 (140) 的装置；以及

用于连同所述数据 (130) 一起输出所述至少两个加密数值和要被撤销的公共密钥的所述识别符 (140) 的装置，

其中所述数据 (130) 包括替代根证书。

11. 权利要求 10 的设备，其中识别符 (140) 是数字证书的识别符。

12. 权利要求 11 的设备，其中所述数字证书的识别符是根证书序列号。

13. 权利要求 10 的设备，其中所述数据 (130) 包括对于撤销的时间和数据。

14. 一种接收机 (13)，包括：

用于存储多个密钥的装置 (20)；

该接收机的特征在于，它还包括：

用于接收包括替代根证书的数据（130）、要被撤销的公共密钥的识别符（140）、和为至少一些数据（130）而确定的至少两个加密的数值（146）的装置（31；32；30；20），每个加密数值是使用相应的加密算法的密钥而为相同的数据确定的；

用于使用所述相应加密算法的已存储的密钥来处理每个加密数值从而形成得到的数值的装置（20）；

用于把每个得到的数值与所述至少一些数据（130）进行比较（206）以鉴权所述至少一些数据的装置（20）；

用于存储（208）要被撤销的公共密钥的所述识别符（140）的装置（20）；

用于撤销相应于要被撤销的公共密钥的所述识别符的公共密钥的装置（20）；以及

用于存储该替代根证书的装置。

15. 权利要求 14 的接收机，其中识别符（140）是数字证书的识别符。

16. 权利要求 15 的接收机，其中所述数字证书的识别符是根证书序列号。

17. 权利要求 14 的接收机，其中该数据（130）包括对于撤销的时间和数据。

数字传输系统中发送的数据的鉴权

[0001] 本申请是申请号为 01810646.3 专利申请的分案申请。

[0002] 本发明涉及数字传输系统中发送的数据的鉴权方法。

[0003] 数字数据的广播传输在付费电视系统领域中是熟知的，在该系统中扰码的音频视频信息通常通过卫星或卫星 / 电缆链路被发送到多个预订用户，其中每个用户具有一个译码器，能够解扰传输的节目，以供以后观看。地面数字广播系统也是已知的。最新的系统也使用广播链路来发送除了音频视频数据以外的其他数据（诸如计算机程序或交互应用项目）到译码器或连接的 PC 机。

[0004] 应用数据的传输的一个具体的问题在于需要验证任何这样的数据的整体性和起源点。由于这种数据可被使用来重新配置译码器，以及实施任意数目的交互的应用，重要的是接收数据是完全的以及被识别为从已知的源发起的。否则，可能引起与下载不完全的数据相联系的运行问题，以及有译码器成为开放的因而受到第三方等的攻击的风险。

[0005] 验证这样的数据的整体性，可以通过验证由译码器直接接收的分组数据流而进行。在发送之前，通过把散列算法施加到分组中至少某些数据上，分组典型地被加以标记。所得出的散列数值被存储在分组中。在接收数据分组后，译码器把同样的散列算法施加到数据上，以及把由译码器计算的散列数值与被存储在接收的分组中的散列数值进行比较，以便验证接收的数据的完整性。例如，在传输中出现故障或损坏的事件中，计算的散列数值将与接收的散列数值不同。于是，译码器被提醒 :在现在的数据分组中存在可能的错误，以及将重新装载有故障的数据分组。与熟知的散列算法（诸如消息摘要算法 MD5）的使用有关的问题是，散列数值的计算是按照众所周知的一系列计算步骤实行的，结果是任何人都可以计算数据分组的散列数值。所以，不可能验证由译码器接收的数据分组的起源点。这在用接收的数据修正译码器的运行数据文件时是特别重要的。

[0006] 为了克服这个问题，不使用散列算法来计算对于至少某些数据的散列数值，数据分组的签名数值可以通过使用只有广播者知道的密钥数值被计算。这个密钥可以通过使用对称密钥算法（诸如数据加密标准算法，或 DES 算法）被得出，其中利用译码器存储等价的密钥。然而，通过使用非对称公共 / 专用密钥算法（诸如 Rivest，Shamir 和 Adleman 算法，或 RSA 算法）可以提供更大的方便性，在这些算法中公共和专用密钥形成数学公式的互补部分。

[0007] 负责产生数据分组的广播者存储了专用密钥，以及通过使用专用密钥来计算签名值。公共密钥被存储在译码器中，后者通过在制造期间把公共密钥硬编码到译码器的存储器中以便接收数据。在接收数据分组后，译码器使用存储的公共密钥，通过把接收的数据与把公共密钥算法施加到接收的签名数值上得到的结果进行比较，从而验证签名数值。

[0008] 即使在这样的保安系统中，公共密钥的数值有可能通过非法地公开地散布而被泄漏。在这样的情形下，广播者必须快速地撤销等价的公共密钥，以便阻止对数据分组未许可的接收。另外，也进而必须使用新的公共 / 专用密钥。所以，广播者将需要用新的公共密钥代替被存储在合法的用户的译码器中的公共密钥。取决于公共密钥的敏感度，这可能需要广播者费钱和费事地返还这些译码器给制造商，以便把新的公共密钥硬编码到这些译码器

的存储器中。

[0009] 至少在本发明的优选实施例中，本发明寻求解决这些问题和其他问题。

[0010] 本发明的第一方面提供数字传输系统中发送的数据的鉴权方法，所述方法包括以下步骤，在传输之前：

[0011] 确定对于至少某些数据的至少两个加密的数值，每个加密数值是通过使用一个相应的加密算法的密钥对于同一个数据被确定的；以及

[0012] 连同所述数据一起输出所述至少两个加密的数值。

[0013] 本发明具体地应用于，但并不限于，其中希望更新对安全敏感的数据，诸如在新的加密算法中要使用的密钥的情形，以便确保数据“如同发布的那样”被接收。为了提供这样的保密性，要确定对于至少某些、优选地大多数、更优选地全部数据的至少两个加密的数值。每个加密数值是通过使用一个相应的加密算法的密钥被确定的。如果密钥之一被泄漏，则“黑客”有可能截取数据以及改变数据的内容和通过使用泄漏的密钥计算的加密的数值。然而，黑客不可能改变通过使用未泄漏的密钥计算的加密的数值。所以，在通过使用等价于被使用来计算加密数值的密钥的密钥验证加密数值时，使用等价密钥的两个数值将是不同的，这表示数据已成为不可靠的。

[0014] 数据和加密的数值优选地被输出，以便传输到接收机/译码器。优选地，所述数据和所述加密的数值被接收机/译码器接收，其中每个加密的数值通过使用所述相应的加密算法的密钥被处理，以及每个以后得到的数值与所述至少某些数据进行比较，以便鉴权所述至少某个数据。如果该数据已成为不可靠的，则接收机/译码器可选择忽略该数据，这样，泄漏的或不可靠的新的密钥将不存储在译码器的存储器中。优选地，如果至少一个以后得到的数值与所述至少某个数据不同，则所述接收的数据被接收机/译码器拒绝。

[0015] 所以，本发明扩展成数字传输系统中一种发送的数据的鉴权方法，所述方法包括以下步骤：

[0016] 接收所述数据和对于至少某些该数据而确定的至少两个加密的数值，每个加密数值是通过使用一个相应的加密算法的密钥对于同一个数据被确定的；

[0017] 存储多个密钥；

[0018] 通过使用所述相应的加密算法的存储的密钥处理每个加密的数值；

[0019] 把所述以后得到的数值与所述至少某些数据进行比较，以便鉴权所述至少某些数据。

[0020] 优选地，每个算法是非对称的。在优选实施例中，每个加密的数值相应于通过使用相应的加密算法的专用密钥计算的数字签名，每个签名是可以通过使用所述加密算法的公共密钥进行处理的。

[0021] 优选地，所述方法包括连同每个签名一起输出一个要被使用来处理该签名的公共密钥的识别号的步骤。这使得接收机/译码器能够容易识别要被使用来验证该签名的密钥

[0022] 优选地，所述数据包括密钥。在优选实施例中，该数据包括至少一个数字证书，优选地，至少一个数字根证书，它包含一个用于处理数据的加密算法的公共密钥。该至少一个数字证书可包括通过使用被包含在该证书中的公共密钥的加密算法的专用密钥而被计算的数字签名。因此，数字证书可被安全地发送到译码器，而译码器不必被返回到制造商那里以便把新的证书硬编码到译码器的存储器中。

[0023] 优选地，所述数据包括一个撤销的公共密钥的识别号。识别号可包括数字证书的识别号，优选地是数字根证书，它包含所述撤销的公共密钥。所述数据可包括多个所述识别号，每个识别号标识各个撤销的公共密钥。因此，撤销的密钥的识别号清单可被安全地发送到译码器。

[0024] 借助于以上方法，数据可被安全地更新，只要泄漏的密钥的数目低于与数据一起存储的加密的数值的数目。所以，所述数据和所述至少两个加密的数值可被组织在数据文件中，它可包括要被存储在以后产生的数据文件中的加密数值的最小数目的指示。这使得如果密钥被泄漏以使得加密数值的最小数目保持大于泄漏的密钥的数目的话，则加密数值的最小数目能够被改变，例如，被增加。

[0025] 优选地，数据文件被接收机 / 译码器接收，它把被存储在所述数据文件中的加密数值的数目与所述最小数目进行比较，以及如果被存储在所述数据文件中的加密数值的数目小于所述最小数目，则拒绝所述数据文件。

[0026] 数据文件可以在数据模块中被发送。对于在所述模块中的至少某些数据的模块加密数值可以通过使用发射机加密算法的密钥而被计算，以及被存储在所述数据模块。数据模块可以被接收机 / 译码器接收，它通过使用发射机加密算法的密钥来处理所述模块加密数值，以及把以后得到的数值与在模块中的所述至少某些数据进行比较，以便鉴权在所述模块中的所述至少某些数据。

[0027] 对于在所述模块中至少某些数据的加密数值可以相应于通过使用发射机加密算法的专用密钥计算的数字签名，以及是可通过使用所述加密算法的公共密钥进行处理的。

[0028] 数字传输系统可以是数字广播系统，诸如电视或音频系统。

[0029] 本发明也提供用于鉴权在数字传输系统中要被发送的数据的设备，所述设备包括 ：

[0030] 用于确定对于至少某些数据的至少两个加密的数值的装置，其中每个加密数值是通过使用相应的加密算法的密钥对于同一个数据被确定的 ；以及

[0031] 用于连同所述数据一起输出所述至少两个加密的数值的装置。

[0032] 本发明也提供用于鉴权在数字传输系统中要被发送的数据的系统，所述系统包括上述的设备。该系统优选地还包括接收机 / 译码器，后者包括用于接收所述数据和所述加密数值的装置，用于通过使用所述相应的加密算法的密钥处理每个加密的数值的装置，以及用于把每个以后得到的数值与所述至少某些数据进行比较以便鉴权所述至少某些数据的装置。

[0033] 本发明推广到一种接收机 / 译码器，它包括 ：

[0034] 用于接收包括所述数据的数据文件和对于至少某些数据确定的至少两个加密的数值的装置，每个加密数值是通过使用相应的加密算法的密钥被确定的 ；

[0035] 用于存储多个密钥的装置 ；

[0036] 用于通过使用所述相应的加密算法的存储的密钥处理每个加密的数值的装置 ；

[0037] 用于把所述以后得到的数值与所述至少某些数据进行比较以便鉴权所述至少某些数据的装置。

[0038] 本发明也推广到一种用于鉴权在数字传输系统中发送的数据的系统，所述系统包括上述的设备和上述的接收机 / 译码器。

[0039] 本发明还推广到一种信号，它包括数据和对于至少某些数据而确定的至少两个加密数值，每个加密数值是通过使用相应的加密算法的密钥被确定的。

[0040] 本发明还推广到基本上如这里参照附图描述的、用于鉴权数据的方法或设备，接收机／译码器，或信号。

[0041] 术语“接收机／译码器”或这里使用的“译码器”可以指用于接收编码的或未编码的信号（例如，电视和／或无线电信号）的接收机，这些信号可被某些其他装置广播或发送。术语也可以指用于译码接收的信号的译码器。这样的接收机／译码器的实施例可包括与用于在“机顶盒”中译码被接收的信号的接收机集成在一起的译码器，诸如与在物理上分开的接收机组合地起作用的译码器，或包括附加功能（诸如网络浏览器）的译码器，或与其他设备（诸如视频记录器或电视机）集成在一起的译码器。

[0042] 正如这里使用的，术语“数字传输系统”包括用于发射或广播主要音频视频的或多媒体数字数据的任何传输系统。虽然本发明特别可应用于广播数字电视系统，但本发明也可应用于用于多媒体互联网应用的固定电信网、闭路电视等等。

[0043] 正如这里使用的，术语“数字电视系统”包括任何的卫星、地面、电缆和其他系统。

[0044] 在本发明中使用的、用于产生专用／公共密钥的适当的算法可包括 RSA、Fiat-shamir，或 Diffie-Hellman，以及适当的对称密钥算法可包括 DES 型算法。然而，除非其内容方面所必须的，或除非另外规定的，在与对称算法有关的密钥和与公共／专用算法有关的密钥之间一般没有什么不同之处。

[0045] 为了语言简明起见，术语“扰码的”和“加密的”，以及“控制字”和“密钥”被使用于文本中的各种部分。然而，将会看到，在“扰码的数据”和“加密的数据”，以及“控制字”和“密钥”之间没有根本的不同。

[0046] 另外，为了语言简明起见，术语“加密的”和“加标记的”，以及“解密的”和“验证的”被使用于文本中的各种部分。然而，将会看到，在“加密的数据”和“加标记的数据”，以及“解密的数据”和“验证的数据”之间没有根本的不同。

[0047] 同样地。术语“等价的密钥”被使用来指适合于解密由第一个提到的密钥加密的数据的密钥，或反之亦然。

[0048] 涉及到本发明的方法方面的以上的特性也可被应用于设备方面，以及反之亦然。

[0049] 现在仅仅通过例子参照附图描述本发明的优选实施例，其中：

[0050] 图 1 显示连同本发明使用的数字电视系统的示意图；

[0051] 图 2 显示图 1 的系统的译码器的结构；

[0052] 图 3 显示 MPEG 广播输送流内多个组成成分的结构；

[0053] 图 4 显示把软件应用划分成多个 MPEG 表；

[0054] 图 5 显示在 DSM-CC 数据文件与最终产生的 MPEG 表之间的关系；

[0055] 图 6 显示如在 DSM-CC 环境下规定的客户机、服务器、网络管理程序的关系；

[0056] 图 7 显示鉴权的目录、子目录和文件对象；

[0057] 图 8 显示广播者证书、证书管理机构证书和根证书管理机构证书的格式；

[0058] 图 9 显示证书撤销清单的格式；

[0059] 图 10 显示根证书管理消息 (RCMM) 的格式；

[0060] 图 11 显示在译码器进行接收后，在 RCMM 处理中涉及的步骤。

[0061] 图 1 上显示按照本发明的数字电视系统 1 的总貌。本发明包括大多数传统的、使用已知的 MPEG-2 压缩系统来发送压缩的数字信号的数字电视系统 2。更详细地，在广播中心的 MPEG-2 压缩器 3 接收数字信号流（典型地是视频信号流）。压缩器 3 通过链路 5 被连接到复用器和扰码器 4。

[0062] 复用器 4 接收多个另外的输入信号，组合输送的数据流，以及把压缩的数字信号通过链路 7 发送到广播中心的发射机 6，链路 7 当然可以采取各种各样的形式，包括电信链路。发射机通过上行链路 8 向卫星转发器 9 发送电磁信号，在卫星转发器上该信号被处理和通过理论上的下行链路 10 广播到地面接收机 12，在传统上是通过由最终用户拥有的或租用的碟形天线。由接收机 12 接收的信号被发送到由最终用户拥有的或租用的集成的接收机 / 译码器 13 以及被连接到最终用户的电视机 14。接收机 / 译码器 13 把压缩的 MPEG-2 信号译码成用于电视机 14 的电视信号。

[0063] 用于传输数据的其他的输送信道当然是可能的，诸如，地面广播，电缆传输，组合的卫星 / 电缆链路，电话网等等。

[0064] 在多信道系统中，复用器 4 处理从多个并行源接收的音频和视频信息，以及与发射机 6 进行交互以便沿着相应的数目的信道广播信息。除了音频视频信息以外，消息或应用或任何其他种类的数字数据可被引入到某些或全部这些信道，与发送的数字音频和视频消息交织。在这样的情形下，具有 DSM-CC（数字贮存媒体命令和控制）格式软件文件和消息的形式的数字数据流将被压缩器 3 压缩和被打包成 MPEG 格式。下面更详细地描述软件模块的下载。

[0065] 条件接入系统 15 被连接到复用器 4 和接收机 / 译码器 13，以及部分位于广播中心和部分位于译码器。它使得最终用户能够接入来自从一个或多个广播提供者的数字电视广播。能够解密涉及商业提供的消息（也就是，由广播提供者销售的一个或几个电视节目）的智能卡，可被插入到接收机 / 译码器 13。通过使用译码器 13 和智能卡，最终用户可以以预订模式或以每次观看付费模式购买商业出售品。实际上，译码器可被配置成能处理同时密码 (Simulcrypt) 或多个密码 (Multicrypt) 设计的多个接入控制系统。如上所述，由系统发送的节目在复用器 4 中被扰码，加到给定的传输上的条件和加密密钥由接入控制系统 15 确定。这样的扰码数据的传输在付费电视系统领域是熟知的。典型地，扰码的数据连同用于数据扰码的控制字一起被发送，控制字本身通过所谓的操作密钥被加密，以及以加密的方式被发送。

[0066] 扰码数据和加密的控制字然后被译码器 13 接收，访问被存储在插入到译码器中的智能卡上的所述操作密钥的等价物，以便解密加密的控制字，然后解扰码发送的数据。付费的用户将在每月广播的 EMM（权利管理消息）中接收对于解密加密的控制字所必须的操作密钥，以许可观看所述传输内容。除了它们在解密音频视频电视节目中使用以外，类似的操作密钥可被产生和被发送，供验证其他数据（诸如将在下面描述的软件模块）时使用。

[0067] 交互系统 16，也被连接到复用器 4 和接收机 / 译码器 13，以及也部分地位于广播中心和部分地位于译码器中，它使得最终用户能够通过调制解调器返回信道 17 与各种应用交互。调制解调器返回信道也可被应用于在条件接入系统 15 中使用的通信中。交互系统可被使用来使得观众能够立即与传输中心通信，以便要求授权观看特定的事件、下载和应用等等的合法权。

[0068] 接收机 / 译码器的物理单元

[0069] 参照图 2，现在概略地描述适合于在本发明中使用的接收机 / 译码器 13 或 1 机顶盒的物理单元。图上显示的单元将按功能块进行描述。

[0070] 译码器 13 包括中央处理器 20，它包括相关的存储器单元，适用于接收来自串行接口 21、并行接口 22 和调制解调器 23（被连接到图 1 的调制解调器返回信道 17）的输入数据。

[0071] 译码器另外还适合于通过控制单元 26 以及从译码器的前面板上的开关接触点 24 接收来自红外遥控器 25 的输入。译码器也具有两个智能卡读卡器 27，28，分别适合于读出银行卡和预订智能卡 29，30。输入也可通过红外键盘（未示出）被接收。预订智能卡读卡器 28 接受插入的预订卡 30 和接受条件接入单元 29，以便提供必要的控制字给解复用器 / 解扰码器 30，使得加密的广播信号能够被解扰。译码器还包括传统的调谐器 31 和解调器 32，以便接收和解调卫星传输，然后被单元 30 滤波和被解复用。

[0072] 在译码器内处理数据，通常是由中央处理器 20 来管理的。中央处理器的软件结构相应于这样一种虚拟机，它与用译码器的硬件部件实施的较低级别的操作系统交互。

[0073] 发送的数据的分组结构

[0074] 现在参照图 3 和 4 描述在从发射机发送到译码器的、在广播的 MPEG 输送数据流内的数据的分组结构。正如将会看到的，虽然说明是集中在 MPEG 标准中使用的表格格式，但相同的原理同样应用于其他分组的数据流格式。

[0075] 具体参照图 3，MPEG 比特流包括节目接入表（“PAT”）40，它具有为 0 的分组标识（“PID”）。PAT 包含对于多个节目的节目对应表（“PMT”）41 的 PID 的参考。每个 PMT 包含对于该节目的音频 MPEG 表 42 和视频 MPEG 表 43 的数据流的 PID 的参考。具有为零的 PID 的分组（也就是，节目接入表 40）提供对于所有的 MPEG 接入的入口点。

[0076] 为了下载应用及其数据，规定两种新的数据流类型，相关的 PMT 也包含对于应用 MPEG 表 44（或它们的分段）和数据视频 MPEG 表 45（或它们的分段）的数据流的 PID 的参考。实际上，虽然在某些情形下规定分开的用于可执行的应用软件的数据流类型和由这样的软件处理的数据可能是方便的，但这不是本质的。在其他的实现方案中，数据和可执行的代码可被组装在通过 PMT 接入的单个数据流中。

[0077] 参照图 4，为了在数据流 44 内下载应用，应用 46 被划分成模块 47，每个模块由 MPEG 表形成。这些表中的某些表包括单个分段，而其他表由多个分段 48 组成。典型的分段 48 具有一个标题，它包括一字节表识别符（“TID”）50、表中的该分段的分段号 51、该表中分段总数 52、以及二字节 TID 扩展参考 53。每个分段也包括数据部分 54 和 CRC 55。对于特定的表 47，组成该表 47 的所有的分段 48 具有相同的 TID 50 和相同的 TID 扩展 53。对于特定的应用 46，组成该应用 46 的所有的表 47 具有相同的 TID 50，但具有不同的 TID 扩展。

[0078] 对于每个应用 46，单个 MPEG 表被使用作为目录表 56。目录表 56 在它的标题中具有与组成应用的其他的表 47 相同的 TID。然而，为了识别目的和由于对于目录中的信息只需要单个表的事实，目录表具有为零的预定的 TID 扩展。所有的其他的表 47 通常具有非零 TID 扩展，以及它们由多个相关的分段 48 组成。目录表的标题也包括要被下载的应用的版本号。

[0079] 回过来参照图 3,PAT 40,PMT 41 以及应用和数据流分量 44,45 被循环地发送。被发送的每个应用具有各自的预定的 TID。为了下载应用,具有适当的 TID 和为零的 TID 扩展的 MPEG 表被下载到接收机 / 译码器。这是用于需要的应用的目录表。目录中的数据然后被译码器进行处理,以便去确定组成需要的应用的表的 TID 扩展。此后,具有与目录表相同的 TID 和从目录中确定的 TID 扩展的任何需要的表可被下载。

[0080] 译码器被安排来检验目录表,以用于对它进行任何的更新。这可以通过再次周期地(例如,每 30 秒,或每 1 分或 5 分钟)下载目录表以及对比先前下载的目录表的版本号而被完成。如果新下载的版本号是较新的版本的号码,则与先前的目录表有关的表被删除,以及与新的版本有关的表被下载和被汇编。

[0081] 在替换的安排中,输入的比特流通过使用相应于 TID、TID 扩展和版本号的屏蔽被滤波,它们具有对于应用的 TID、为零的 TID 扩展和比当前下载的目录的版本号大 1 的版本号设置的数值。因此,版本号的增量可被检测,以及一旦被检测,该目录被下载以及应用被更新,如上所述。如果应用要被终结,具有下一个版本号的空的目录被发送,但不带有被列出在目录中的任何模块。响应于这样的空的目录的接收,译码器 2020 被编程来删除应用。

[0082] 实际上,在译码器中实施应用的软件和计算机程序可以通过译码器的任何部件被引入,具体地是在通过所描述的无线链路接收的数据流中,但也通过串行端口、智能卡链路等等。这样的软件可包括高的级别的应用,被使用来在译码器内实施交互应用,诸如网络浏览器、小测验应用、节目指南等等。软件也可借助于“插入码 (patches)”等被下载来改变译码器软件的工作配置。

[0083] 应用也可以通过译码器被下载,以及被发送到连接到译码器的 PC 等等。在这样的情形下,译码器起到用于软件的通信路由器的作用,该软件最终在连接的设备上运行。除了这个路由功能以外,译码器也可用来在路由到 PC 之前把 MPEG 分组化的数据变换成按照 DSM-CC 协议组织的计算机文件软件(见下面)。

[0084] 数据文件中数据的组织

[0085] 图 5 显示在一组 DSM-CC U-U(用户到用户)数据文件 60 中,在被汇编的应用 46 中组织的、和被包容在一系列 MPEG 表 47 内的数据之间的关系。这样的关系在 WO99/49614 中被描述,它的内容在此引用,以供参考。

[0086] 在发送之前,数据文件被汇编成应用 46,此后,被 MPEG 压缩器分组为 MPEG 表或模块 47,如上所述,其中包括对于 MPEG 分组数据流特定的标题 49,以及包括表 ID,版本号等等。正如将会看到的,在数据文件 61 和最终 MPEG 表 47 中组织的数据之间可能没有固定的关系。在被译码器接收和滤波后,分组标题 49 被丢弃,以及从表 47 的有用负载中重新构建的应用 46。

[0087] 用于数据文件的 DSM-CC 格式是特别适合于多媒体网络的标准,它规定用于在客户机用户 70,服务器用户 71,与网络资源管理者 72 之间通信的一系列消息格式和会话命令,如图 6 所示。网络资源管理者 72 可被看作为一个逻辑实体,用来管理网络内的资源的属性。

[0088] 在客户机与服务器之间的通信由一系列会话建立,第一消息序列在用户(客户机 70 或服务器 71)和网络管理者 72 之间交换,以便配置客户机和 / 或服务器用于通信。这样的消息按照所谓的 DSM-CC U-N(从用户到网络)协议被格式化。这个协议的子集已被具体

地定义以用于广播下载数据。

[0089] 一旦通信链路被建立，以后就按照DSM-CC U-U协议在客户机70和服务器71之间交换消息。这种消息序列相应于图5的数据文件60。在DSM-CC U-U消息的情形下，数据被组织在按照BIOP或广播轨道间(Inter Orb)协议分组的消息序列61中。

[0090] 每个消息或对象61包括标题62，子标题63和包含数据本身的有用负载64。按照BIOP协议，标题62特别地包含消息类型和BIOP版本的指示，而子标题表示由系统结构规定的对象和其他信息的类型。

[0091] 在DSM-CC U-U文件的有用负载内的数据对象64通常可被规定为三种类型中的一种类型；目录对象、文件对象和数据流对象。目录对象规定根目录或子目录，被使用来参考包含实际应用数据的一系列相关的文件对象。

[0092] 数据流对象可被使用来使得能够在被包含在数据文件和MPEG分组数据流本身中的数据之间建立暂时的关系。这可在被包含在数据文件中和被设计来与由译码器接收和处理的基本视频或音频数据流同步的交互应用的情形下被使用。如上所述，在MPEG分组化的数据和数据文件之间可能没有直接的关系。

[0093] 不像其中的单个目录参考只具有单个分级级别的一组表的MPEG表，数据文件60可以以更复杂的分级形式被组织。正如对于被存储在PC或服务器中的文件，主目录或根目录可以参照一个或多个子目录，这些子目录进而又参考第二级别的数据文件。甚至可以参考与另一个组的应用数据有关的第二根目录。

[0094] 数据文件组的文件结构

[0095] 参照图7，图上显示数据文件组的文件结构的例子。用75表示的根目录DIR A0参考对象文件77的子目录组A1。为了简明起见，图上只显示与子目录A4有关的单个组的对象文件F1，F2等等。实际上，多组的对象文件可被子目录A1到A4中的每一个参考。

[0096] 在每个目录和子目录内，对于链接到该目录的文件引入一组鉴权步骤。参照根目录75，子标题63包括通过把散列算法施加到被存储在被表示为76的子目录文件A1到A4中的某些或全部数据而得到的散列数值。所使用的散列算法可以具有任何已知的类型，诸如消息摘要算法MD5。

[0097] 在一个实现方案中，算法可被各个地施加到每个相关的文件或子目录上，以及在发送之前施加到一个对于被存储在根目录75中的每个子目录76的散列数值表上。然而，虽然这样的解决方案在验证每个子目录方面能够提高检验分辨率程度，这个解决方案在对于译码器计算相应的签名所必须的处理时间方面，是相当不够的。因此，目录79的子标题63优选地包括通过把MD5散列算法施加到组合的子标题和子目录76的有用负载分段63，64而计算出的累积的散列数值79，也就是，不用标题62。具体地，被包含在子目录76内并且涉及到文件对象层77的散列数值82被包括在这个散列计算中。

[0098] 在图7所示的子目录A4的情形下，这个子目录本身关系到以77表示的一组对象文件F1-Fn。在这种情形下，累积的散列数值82是对于对象文件77的组合的内容而产生的。这个数值被包括在能导致散列数值79的散列处理过程中。所以，不可能不改变子目录76的散列数值82而改变任何对象文件77，而这将会进而改变目录75的散列数值79。

[0099] 在本例中，组合的散列数值是对于目录中所有的子目录A1-A4计算的。这个散列数值连同从其中取数据的子目录组的识别号一起被存储。在其他的实施例中，一系列组合

的或单独的散列数值和相应的识别号可被存储在目录的子标题中。

[0100] 例如，第二组子目录（它也是与根目录有关的，但涉及到不同的组的数据或可执行代码）也可一起被编组，并且对于这些子目录而计算的积累的散列数值被加以计算和被存储在子标题根目录中。与单个目录有关的单个散列数值可相等地被存储在根目录的子标题中。

[0101] 数据文件组或单独的数据文件的鉴权当然不阻止根目录（或实际上，任何其他文件）也去参照未验证的或未散列的数据文件，但对于这个文件的任何运行，将需要考虑这样的文件的缺少验证。在这方面，不一定必须鉴权数据流对象。

[0102] 在这种情形下散列函数的使用主要使得译码器能够验证下载的数据文件的整体性或完整性。在传输时故障或损坏的情形下，积累散列算法对于接收的非独立的文件的运行将不会给出与被存储在根目录中的这些文件的散列数值相同的结果。译码器然后被提示：在下载的数据中存在可能的错误，以及将重新下载有故障的数据文件。

[0103] 用于根目录的签名数值

[0104] 为了增强的安全性，根目录 75 的签名数值被加以计算。在本实施例中，使用专用/公共密钥算法，诸如 Rivest，Shamir 和 Adleman 或 RSA 算法，负责产生数据文件的广播者具有专用密钥数值，并且公共密钥数值由译码器保持。替换地，秘密密钥可相应于通过对称密钥算法（诸如数据加密标准或 DES 算法）得到的密钥。

[0105] 如图 7 所示，根目录 75 包括广播者识别号 80，它向译码器表示在验证级要被连同通过使用广播者的专用密钥产生的计算的签名数值 81 一起使用的公共密钥。在这种情形下，签名数值 81 是通过把由广播者保持的专用密钥施加到目录 75 内某些或全部数据（优选地，包括有用负载 64 和/或积累的散列数值 79）而被产生的。然后，译码器通过使用由广播者识别号 80 标识的相应的公共密钥来验证这个签名数值 81。

[0106] 在本例中，目录 75 中的数据被解密，以及专用密钥只被使用来提供由公共密钥可验证的签名数值。在替换的实施例中，目录的某些或所有的内容可被专用密钥加密，此后由相应的密钥解密。

[0107] 在任一种情形下，签名数值或由加密密钥使用的加密码块的产生使得译码器能够验证目录 75 的整体性和起源点，也就是由这个根目录所联系到的文件的整体性和起源点。由于所联系到的文件的积累的散列数值被包括在签名 81 的计算中，如果在验证级中没有检测到这一点，就不可能改变这些数值。由于每个散列数值通常对于给定的数据组是唯一的，所以，如果不改变任何依赖的散列文件的特征的散列数值，就不可能改变这些散列文件的内容，以及从而改变目录的最终的签名数值。

[0108] 正如将会看到的，有可能具有多个变例，特别是为了减小在每级散列的或加标记的数据量。具体地，在目录或子目录中被使用来验证较低的级别的数据文件的签名或散列数值的情形下，目录签名或散列数值可以通过只使用较低的级别的散列数值而不使用其他数据被产生。

[0109] 例如，在 A0 目录 75 中的组合的散列数值 79 可以通过使用被表示为 76 的每个 A1-A4 子目录的组合的散列数值被产生。由于这些数值正好是与子目录的有用负载中的数据一样独特的，组合的散列数值 79 对于所讨论的子目录仍旧是独特的。而且，仍旧可假设较低的级别的对象和目录文件 77，78 的整体性，因为散列数值 82 仍旧在计算中被使用。

[0110] 广播者数字证书

[0111] 参照图8，公共密钥91和广播者识别号80在数字证书中优选地以熟知的国际标准组织(ISO)X.509标准的形式提供给译码器的用户，它在制造期间被硬编码到译码器的存储器中。这样的证书通过受信任的第三方（它们通常被称为证书管理机构(CA)）分配给译码器的制造商。这样的证书的使用，主要由于通过用于保障在万维网(WWW)上的信用卡交易的Netscape Communications开发的和标准化的安全插口层(SSL)安全输送协议，从而变成为更广泛的。

[0112] 除了公共密钥91和广播者识别号80以外，与广播者有关的数字证书、或广播者证书90还包括：

[0113] • 广播者证书90的版本号92；

[0114] • 广播者证书90的串号93；

[0115] • 分发广播者证书90的CA的CA识别号94；

[0116] •广播者证书90的有效性期限95，用于表示需要使用证书的时间期间的开始点和结束点；以及

[0117] • 广播者证书90的签名数值96。

[0118] 正如从上面看到的，广播者证书包括两个不同的识别号：相应于证书的分发者的识别号94的第一“分发者名称”识别号，和相应于标识公共密钥91的识别号80的第二“主题名称”识别号。

[0119] CA通过把CA的专用密钥或CA专用密钥施加给广播者证书内的至少某些或全部的数据，从而计算出广播者证书90的签名数值96。然后，译码器可以通过使用由CA识别号94标识的相应的CA公共密钥101而处理签名，以便确定证书的内容在由CA进行签名后没有被修改，从而验证这个签名数值96。

[0120] 译码器可以存储用于不同的各个广播者的多个这样的证书。

[0121] 证书管理机构数字证书

[0122] 还参照图8，相应的CA公共密钥101和CA识别号94在CA证书100中被提供给译码器的用户，它也是在制造期间被硬编码到译码器中的。CA证书100还包括：

[0123] • CA证书100的版本号102；

[0124] • CA证书100的串号103；

[0125] •分发CA证书100的根证书管理机构(RCA)（诸如欧洲电信标准局(ETSI)）的RCA识别号104；

[0126] • CA证书100的有效性期限105；以及

[0127] • CA证书100的签名数值106。

[0128] 正如从上面看到的，CA证书也包括两个不同的识别号：相应于证书的分发者的识别号104的第一“发布者名称”识别号，和相应于标识公共密钥101的识别号94的第二“受主名称”识别号。

[0129] RCA通过把RCA的专用密钥或RCA专用密钥施加给CA证书内至少某些或全部的数据，从而计算CA证书100的签名数值106。然后，译码器可以通过使用由RCA识别号104标识的相应的RCA公共密钥111而处理签名，以便确定证书的内容在由进行RCA签名后没有被修改，从而验证这个签名数值106。

[0130] 译码器可以存储用于不同的各个 CA 的多个这样的证书。

[0131] 根证书管理机构数字证书

[0132] 相应的 RCA 公共密钥 111 和 RCA 识别号 104 在 RCA 或根证书 110 中被提供给译码器的用户，它也是在制造期间被硬编码到译码器的存储器中的。每个译码器典型地包括一组两个或多个根证书。每个根证书 110 还包括：

[0133] • 根证书 110 的版本号 112；

[0134] • 根证书 110 的串号 113；

[0135] • 根证书 110 的有效性期限 114；以及

[0136] • 根证书 110 的签名数值 115。

[0137] 正如从上面看到的，根证书只包括单个识别号，即，证书的分发者的识别号 104。这个识别号 104 也标识公共密钥 111。因此，根证书可被定义为其中发布者名称是与受主名称相同的证书。

[0138] 由于根证书是在广播者证书 90-CA 证书 100- 根证书 110 的链中的最终的证书，根证书是本身加标记的，也就是，签名数值是通过使用等价于公共密钥 111 的专用密钥而被计算出的。所以，要关心的是根证书的内容不变成为公开地可提供的。

[0139] 当然，有可能 RCA 把广播者证书 90 直接提供给译码器的制造商，在这种情形下，广播者证书将包含 RCA 识别号 111，以及通过使用 RCA 专用密钥而被加标记。

[0140] 证书撤销清单

[0141] 如果相应于被存储在证书中的公共密钥的的专用密钥被泄漏，则任何的广播者证书 90 和 CA 证书 100 可以在其中规定的有效期限时间到之前通过删除而被撤销。这样的撤销可以通过发送包含要被撤销的证书的串号 92、102 的清单的证书撤销清单给译码器而被实施。在撤销后，优选地通过从译码器的存储器中删除证书而使得证书不能起作用，由此阻止下载任何未批准的和可能恶意的、使用泄露的专用密钥加标记的数据分组。

[0142] CRL 由 CA 或 RCA 分发给广播者，后者通过调制解调器返回信道 17 把 CRL 发送到译码器或通过 MPEG 输送流广播 CRL。广播者把 CRL 插入到从发射机发送到译码器的所有的输送流中并不是重要的；广播者把 CRL 插入到非常可能由译码器调谐到的那些输送流就足够了。例如，CRL 可以作为数据文件被插入到从发射机广播到译码器的一组数据文件的根目录 75 或子目录 76 中。

[0143] 参照图 9，CRL 典型地包括：

[0144] • 分发 CRL 120 的 CA 或 RCA 的识别号 94 或 104；

[0145] • 发布 CRL 120 的日期 122；

[0146] • 下一个 CRL 预期要被发布的日期 124；

[0147] • 要被撤销的证书的串号的清单 125，其中包括对于每个被撤销的证书、该证书的撤销的时间和日期；以及

[0148] •CRL 的签名数值 126，它是通过使用发布 CRL 120 的 CA 或 RCA 的专用密钥而被计算的。

[0149] 在接收 CRL 后，译码器把发布该 CRL 120 的日期 122 与由先前接收的 CRL 建议的该 CRL 预期要被发布的日期 124 进行比较。如果新接收的 CRL 的日期 122 不迟于该 CRL 预期要被发布的日期 124，则 CRL 被忽略。

[0150] 如果新接收的CRL的日期122迟于该CRL预期要被发布的日期124，则CRL的签名通过使用CA的发布者的公共密钥（它是通过使用被包含在CRL中的识别号94或104被标识的）而被验证。

[0151] 如果CRL的整体性被这样地验证，则CRL被加以处理以便附加上日期124，并且把下一个CRL预期要被发布的日期124存储在永久存储器中，以及存储撤销的证书的串号的清单125。接收的撤销证书清单125也被存储在译码器的永久存储器中。为了性能上的原因，CRL 120优选地被超高速缓存在译码器的存储器中。优选地，译码器的超高速缓存器以树状的方式存储CRL 120，并且RCA的CRL位于“树”的顶部以及该RCA分布的CA的CRL位于“树”的底部。

[0152] 在撤销广播者证书90的事件中，如果广播者的专用密钥被泄露，则用于该广播者的证书管理机构把广播者证书90的串号93附加到它的CRL 120上。证书管理机构随后分发新的CRL 120给所有的广播者，这些广播者也接受所分发的用于广播的广播者证书90。只要译码器例如在对广播者的信道攻击后下载新的CRL 120，CRL超高速缓存器就被更新，以及在CRL 120的清单125中标识的任何证书将被撤销。

[0153] 替代广播者证书90由证书管理机构100产生，以及在文件的目录75或76中被广播给用户。替代广播者证书将包括新的公共密钥91、更新的版本号92、更新的有效性期限95、以及通过使用CA的专用密钥计算出的新的签名数值96。广播者识别号80和CA识别号94将保持不变。在接收替代广播者证书90后，译码器通过使用被包含在由CA识别号94标识的CA证书中的相应的CA公共密钥处理证书而验证证书。

[0154] 在撤销CA证书100后，该CA的CRL从译码器的存储器中被去除。所以，如果该CA的CRL的尺寸变得太大而不能贮存在译码器的超高速存储器中，则可能希望自动地撤销CA证书100。在这种情形下，分发CA证书100到该CA的RCA将把该CA证书100的串号103附加到它的CRL中。根证书管理机构随后把新的CRL分发给所有的广播者，这些广播者也接受由该RCA分发的用于广播的CA证书。只要译码器例如通过广播者的信道下载新的CRL 120，CRL超高速缓存器就被更新，以及在CRL 120的清单125中标识的任何证书将进行撤销。

[0155] 在撤销证书管理机构的CA证书100后，除了把对于该证书管理机构的新的CA证书贮存到译码器以外，必须对所有的广播者的广播者证书90进行替换，这些广播者是接受该证书管理机构分发的证书的广播者，因为，由于用于该证书管理机构的专用密钥不再有效，所以将需要通过使用加标记的新的广播者证书90。替代的CA证书100由根证书管理机构110产生，以及在文件的目录75或76中被广播给用户。类似于替代的广播者证书，替代的CA证书将包括新的CA公共密钥101、更新的版本号102、更新的有效性期限105、以及通过使用RCA的专用密钥计算出的新的签名数值106。CA识别号94和RCA识别号104将保持不变。在接收替代的CA证书100后，译码器通过使用被包含在由RCA识别号104标识的RCA证书110中的相应的RCA公共密钥去处理证书，从而验证证书。

[0156] 根证书管理消息

[0157] 在撤销根证书管理机构的RCA证书110后，必须用新的RCA代替撤销的RCA证书。如上所述，RCA证书是本身加标记的，所以不希望把RCA证书包括在CRL中，因为有可能黑客会占有证书，如果他知道被使用来标记CRL的专用密钥的话。所以，在RCA证书每次要被

更新时，例如当它已经成为过时的或被撤销时，必须把译码器返回到制造商。

[0158] 为了克服这个问题，由根证书管理机构产生根证书管理消息 (RCMM)，以便由广播者广播到译码器。正如下面更详细地说明的，类似于 CRL，RCMN 包含要被撤销的根证书的串号的清单 125，其中包括对于每个撤销的根证书，撤销该证书的时间和日期，连同对于已成为过时的或在清单 125 中表示的那些证书的一个或多个替代的根证书。

[0159] 正如将会看到的，从 RCMM 的敏感的内容（新的根证书）看来，重要的是确保 RCMM "在被发布"给广播者时被译码器接收，也就是，确保 RCMM 的内容在分发与接收之间没有改变。也是重要的是确保 RCMM 只被 RCMM 寻址到的译码器接入。

[0160] 为了增强安全性，对于被包括在其中的至少某些数据（优选地是全部数据）。RCMM 包含至少两个签名数值，这与 CRL 不同。每个签名数值是通过使用相应的加密算法的密钥（诸如公共 / 专用密钥对的专用密钥）而被计算的。

[0161] 当 RCMM 被根证书管理机构 (RCA) 发布以及包括新的根证书 110 时，RCMM 包括至少两个签名数值。每个签名数值是通过使用由接受该 RCA 提供的证书的证明的相应的专用密钥被计算的（虽然可以选择与译码器存储的密钥等价的任何密钥）。如果那些证书管理机构之一未知的，它的专用密钥被泄漏，有可能"黑客"截取广播者的广播，以及如果他知道广播者和证书管理机构的专用密钥，则他可能改变 RCMM 的内容和通过使用证书管理机构的专用密钥计算出的 RCMM 的签名数值。然而，黑客不可能改变通过使用其他证书管理机构的专用密钥计算出的签名数值，因为这个密钥没有被泄漏。所以，在由译码器通过使用两个证书管理机构的公共密钥验证签名数值后，由译码器通过使用各个公共密钥计算出的两个数值将不是相同的。所以，译码器将被提示：缺乏 RCMM 的内容的整体性，以及将拒绝 RCMM，或不进行 RCMM 的处理。

[0162] 因此，根证书被安全地更新，只要泄漏的证书的数目低于被包含在 RCMM 中的签名的数目。所以，RCMM 的签名的数目是由分发 RCMM 的根证书管理机构确定的变量。

[0163] 现在参照图 10 更详细地描述 RCMM 的格式。

[0164] RCMM130 包括：

[0165] • 分发 RCMM 130 的 RCA 的识别号 132；

[0166] • 发布 RCMM 130 的日期 134；

[0167] • 以后的 RCMM 将包含的签名数值的数目 136；

[0168] • 包含了要被存储在译码器中的一个或多个更新的或替换根证书的域 138；

[0169] • 要被撤销的根证书的串号的清单 140，其中包括：对于每个被撤销的根证书、该证书的撤销的时间和日期；以及

[0170] • 至少两个签名域 142，其中每个包含：

[0171] 被存储在译码器中的证书的识别号 144，它包含公共密钥、要被使用来验证被包含在由签名区中的签名数值；以及

[0172] RCMM 的签名数值，它是通过使用等价于被包含在由识别号 144 识别的证书中的公共密钥的专用密钥而被计算的。

[0173] 签名域 142 的数目应当等于或大于如在先前接收的 RCMM 中建议的签名域的数目 136。

[0174] 优选地，RCMM 通过 MPEG 输送流被发送，因为调制解调器返回信道可被容易地断开

连接或可能完全不存在。优选地，RCMM 被广播者作为数据文件插入到根目录 75 中，以便确保 RCMM 被译码器下载。

[0175] 根证书管理消息的处理和产生

[0176] 现在参照图 11 描述由译码器对 RCMM 的接收和处理。

[0177] 在接收 RCMM 后，在步骤 200，译码器比较该 RCMM 130 被发布的日期 134 与先前发布的 RCMM 的日期。如果新接收的 RCMM 的日期 134 不迟于先前的 RCMM 发布的日期，则 RCMM 被拒绝。

[0178] 如果新接收的 RCMM 的日期 134 迟于先前的 RCMM 的接收的日期，则新接收的 RCMM 要包含的签名数值的数目 136（正如由先前接收的 RCMM 建议的那样）在步骤 202 与实际上被包含在新接收的 RCMM 中的签名数值的数目进行比较。如果被包含在新接收的 RCMM 中的签名数值的数目低于预期的，则 RCMM 被拒绝。这可阻止 RCMM 由于黑客抹除了与未泄漏的专用 / 公共密钥对有关的签名而要被进行处理。

[0179] 如果被包含在新接收的 RCMM 中的签名数值的数目等于或大于预期的签名数目，则在步骤 204，被包含在 RCMM 中的每个签名数值 146 通过使用由被包含在与该签名数值相同的签名区 142 中的识别号 144 标识的公共密钥而被验证。在步骤 206，译码器确定通过使用公共密钥计算出的至少一个数值是否与通过使用不同的公共密钥计算的任何其他的数值不同。如果至少一个计算的数值不同于至少一个其他计算的数值，则 RCMM 被拒绝。

[0180] 如果在步骤 206 证明了 RCMM 的整体性，则 RCMM 被处理，在步骤 208 把撤销的根证书的串号的清单 140 存储在译码器的永久存储器中，以使得这些证书可以从译码器的存储器中被删除，在步骤 210 把被包含在域 138 中的每个根证书存储在译码器的永久存储器中，以及在步骤 212 把 RCMM 的日期 134 存储在永久存储器中。如果根证书管理机构的证书被删除，则由该管理机构发布的任何 CRL 也被删除。

[0181] 优选地，被包含在 RCMMZ 中的数据的永久贮存的整体性被保持，如果在 RCMM 消息的处理期间译码器被关断的话。所以，如果在 PCMM 处理期间打算关断功率，则与被存储在译码器中的、先前处理的 RCMM 有关的清单 140 被保持，就好像新的接收的 RCMM 消息完全没有被处理那样。

[0182] 如前所述，根证书管理机构 (RCA) 典型地具有至少两个 RCA 证书 RC0 和 RC1，它们被存储在每个译码器中。在这些证书之一（比如说 RC0）被泄漏的情形下，必须替换被存储在译码器中的所有的 CA 证书（它们已通过使用等价于被存储在 RC0 中的公共密钥的专用密钥而被加标记），以及产生新的 RCA 证书 RC2 来替代 RC0。

[0183] 参照图 12，为了替换这些 CA 证书，首先在步骤 300，由 RCA 发布表示要被撤销的 CA 证书的串号的适当的 CRL 消息。其次，在步骤 302，通过使用非泄漏的证书 RC1 的专用密钥加标记的替代的 CA 证书被发布给广播者，以便广播到译码器。

[0184] 然后就删除泄漏的 RCA 证书 RC0 以及用新的 RCA 证书 RC2 替换这个证书。在步骤 304，RCA 产生新的公共 / 专用密钥对，把新的公共密钥插入到证书 RC2 中以及通过使用新的专用密钥去标记证书。

[0185] 在步骤 306，RCA 产生 RCMM，它在域 138 中包含证书 RC2，以及在清单 140 中包含 RC0 的串号。在步骤 308，RCMM 被分发给广播者，以便发送到译码器，以便删除泄漏的证书 RC0 和用新的证书 RC2 替代它。

[0186] RCA 证书 RC1 和 RC2 随后将被提供给译码器制造商，以便硬编码到新的译码器的存储器中。

[0187] 将会看到，以上纯粹作为例子描述了本发明，以及可以在本发明的范围内作出细节的修正。

[0188] 例如，除了新的 RCA 证书以外，RCMM 可包括新的 CA 证书 100 和 / 或新的广播者证书 90，以及清单 140 可包括要被撤销的 CA 证书和 / 或广播者证书的识别号。这可以使得能避免由 RCA 产生分开的 CRL 消息。

[0189] 在说明书中以及（在适合的情形下）权利要求和附图揭示的每个特征可以独立地或以任何适当的组合而被提供。

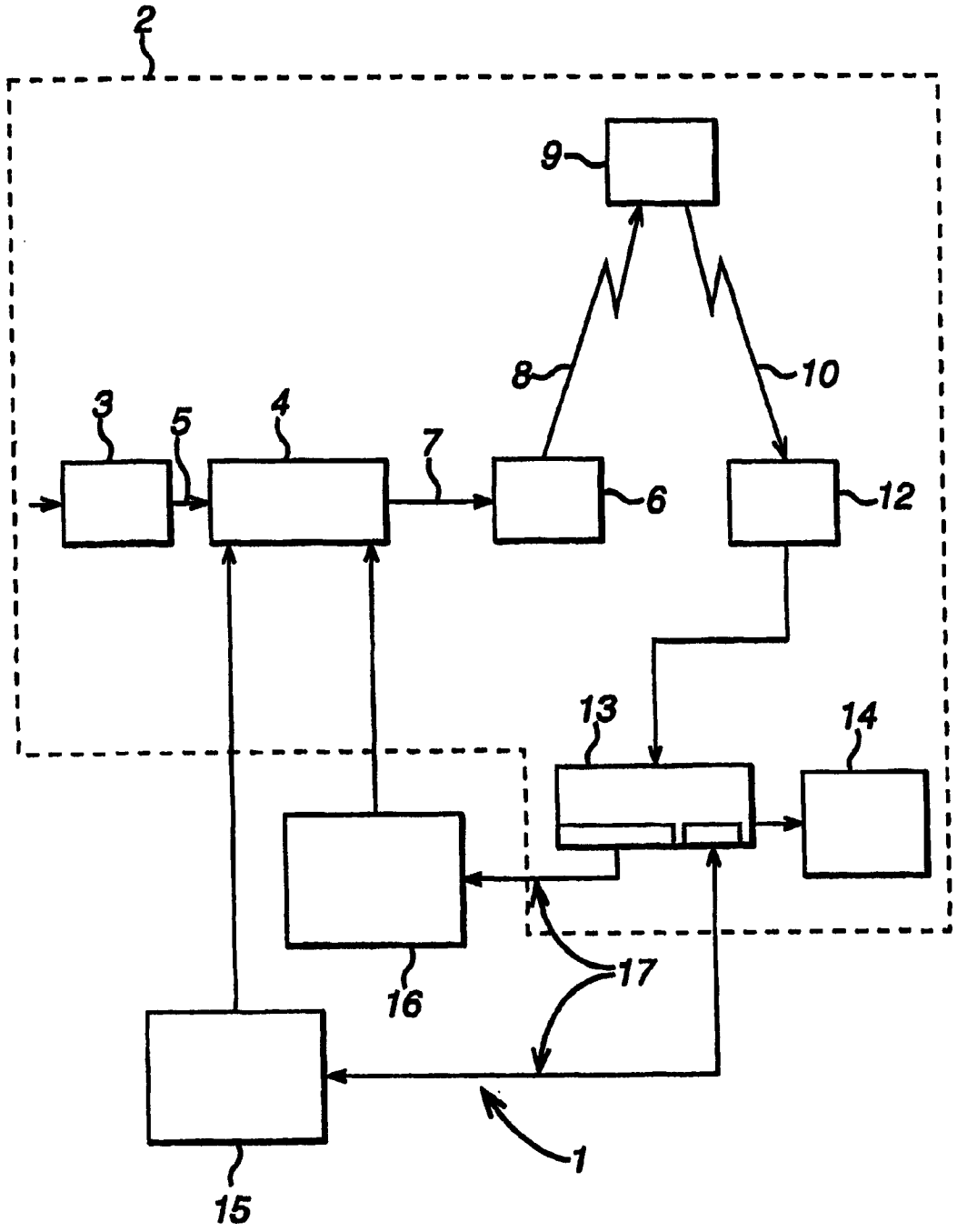


图 1

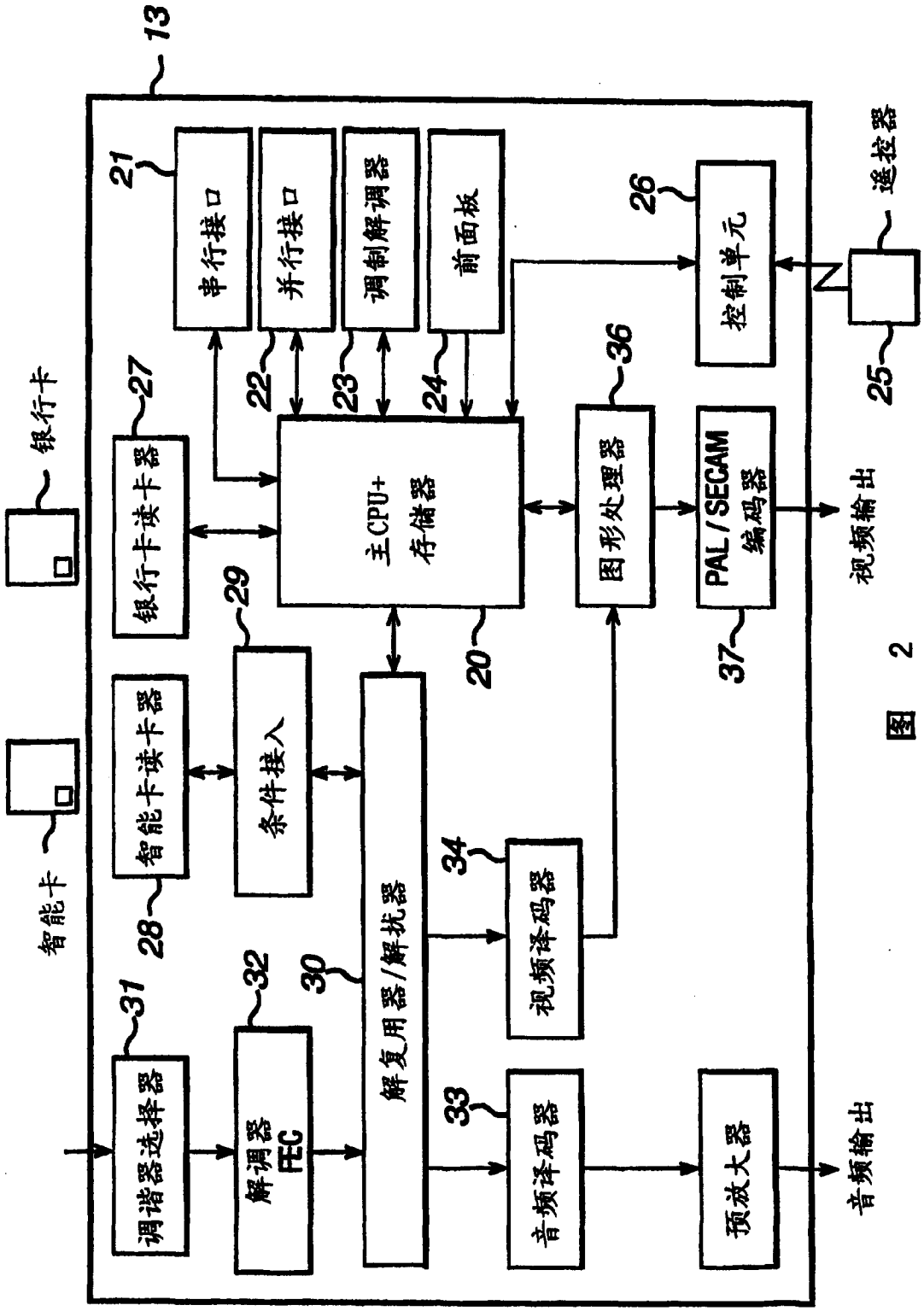

13
21
串行接口
并行接口
调制解调器
前面板
26
控制单元
遥控器
25
22
23
24
27
银行卡读卡器
主CPU+
存储器
图形处理器
36
PAL / SECAM
编码器
视频输出
银行卡
29
智能卡读卡器
条件接入
20
37
智能卡
28
34
视频译码器
30
解复用器/解扰器
31
32
调谐器选择器
解调器
FEC
33
音频译码器
预放大器
音频输出

图 2

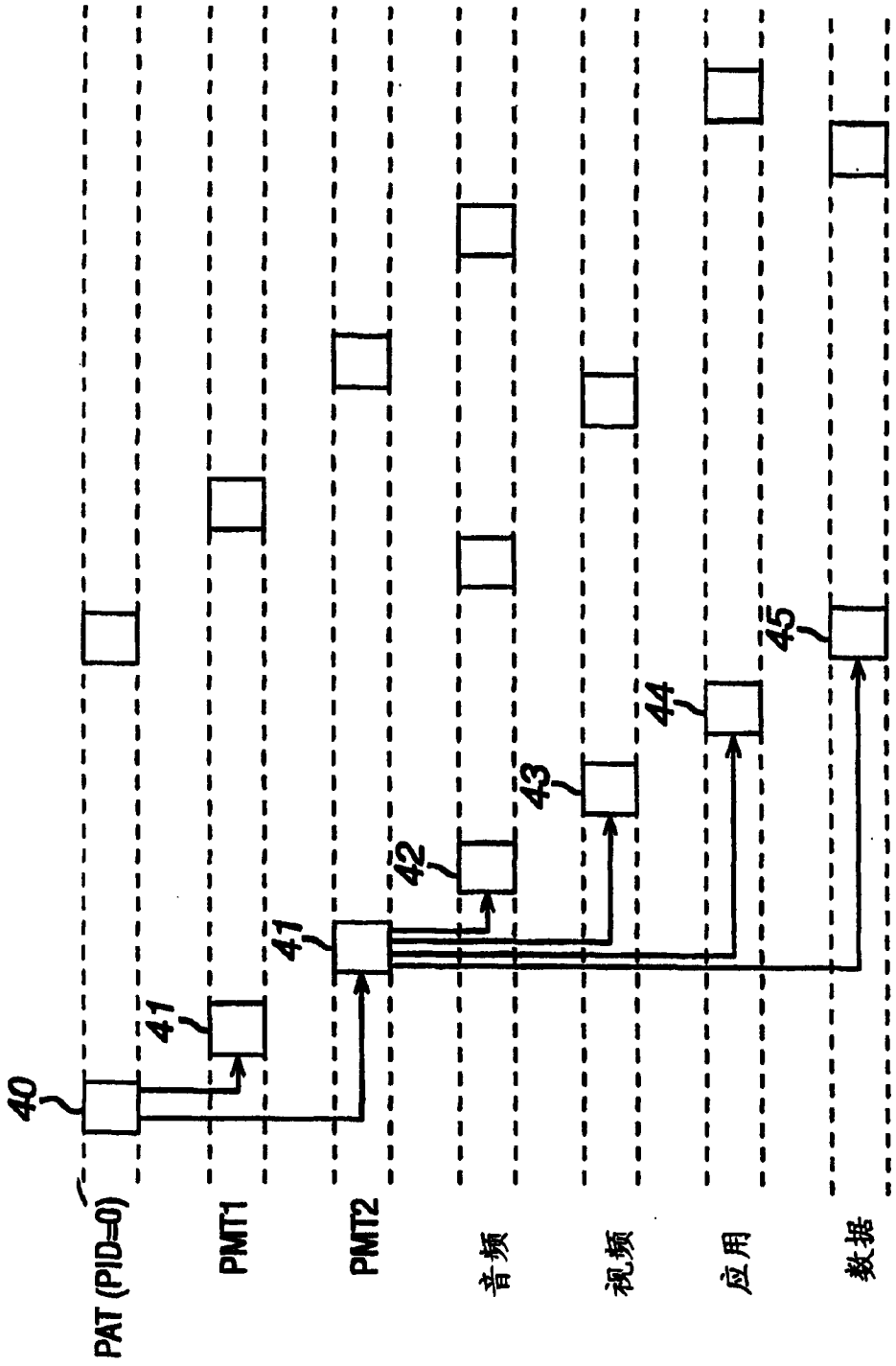


图 3

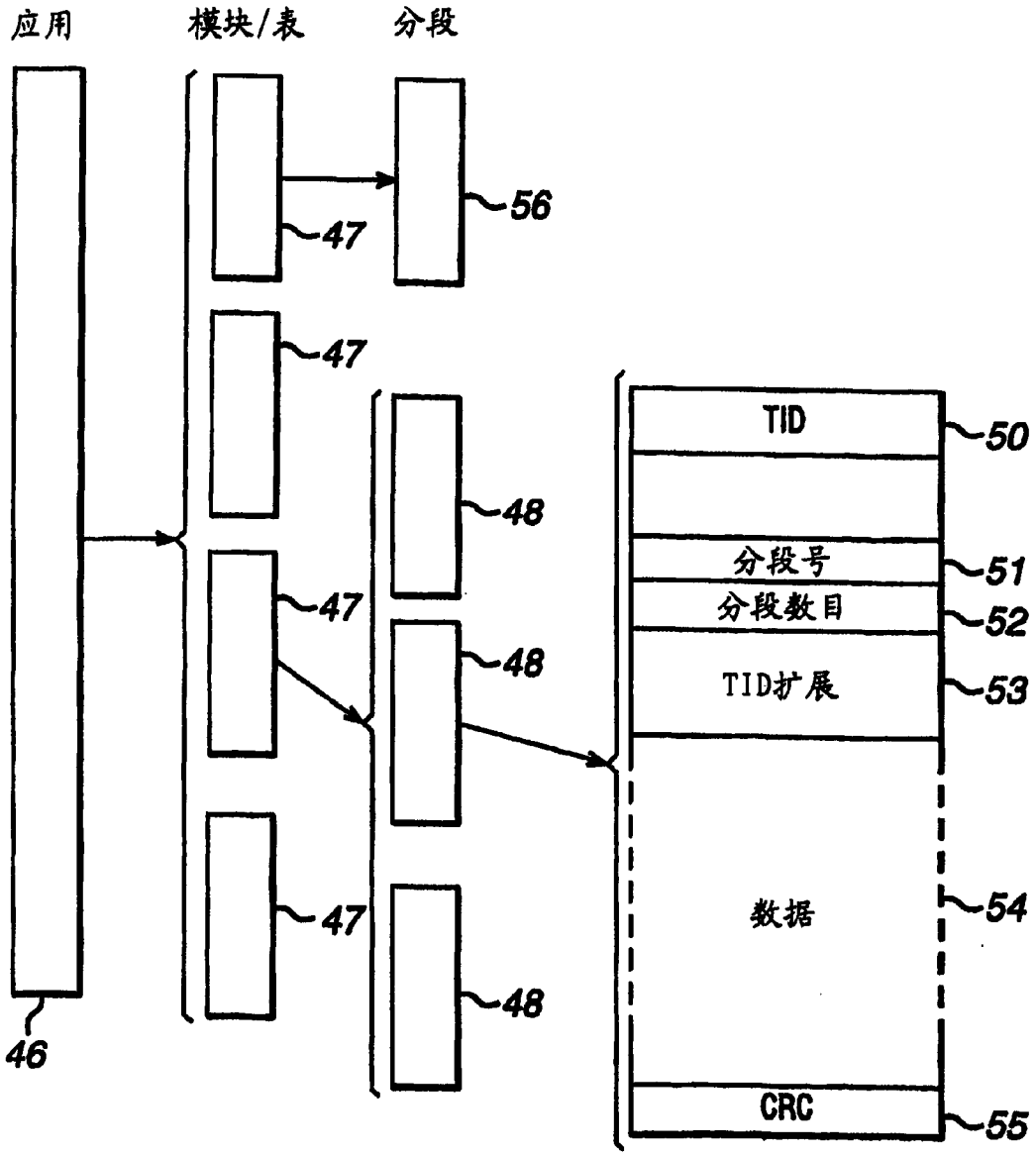

应用
模块/表
分段
47
56
47
48
47
48
47
48
46
TID
50
分段号
51
分段数目
52
TID扩展
53
数据
54
CRC
55

图 4

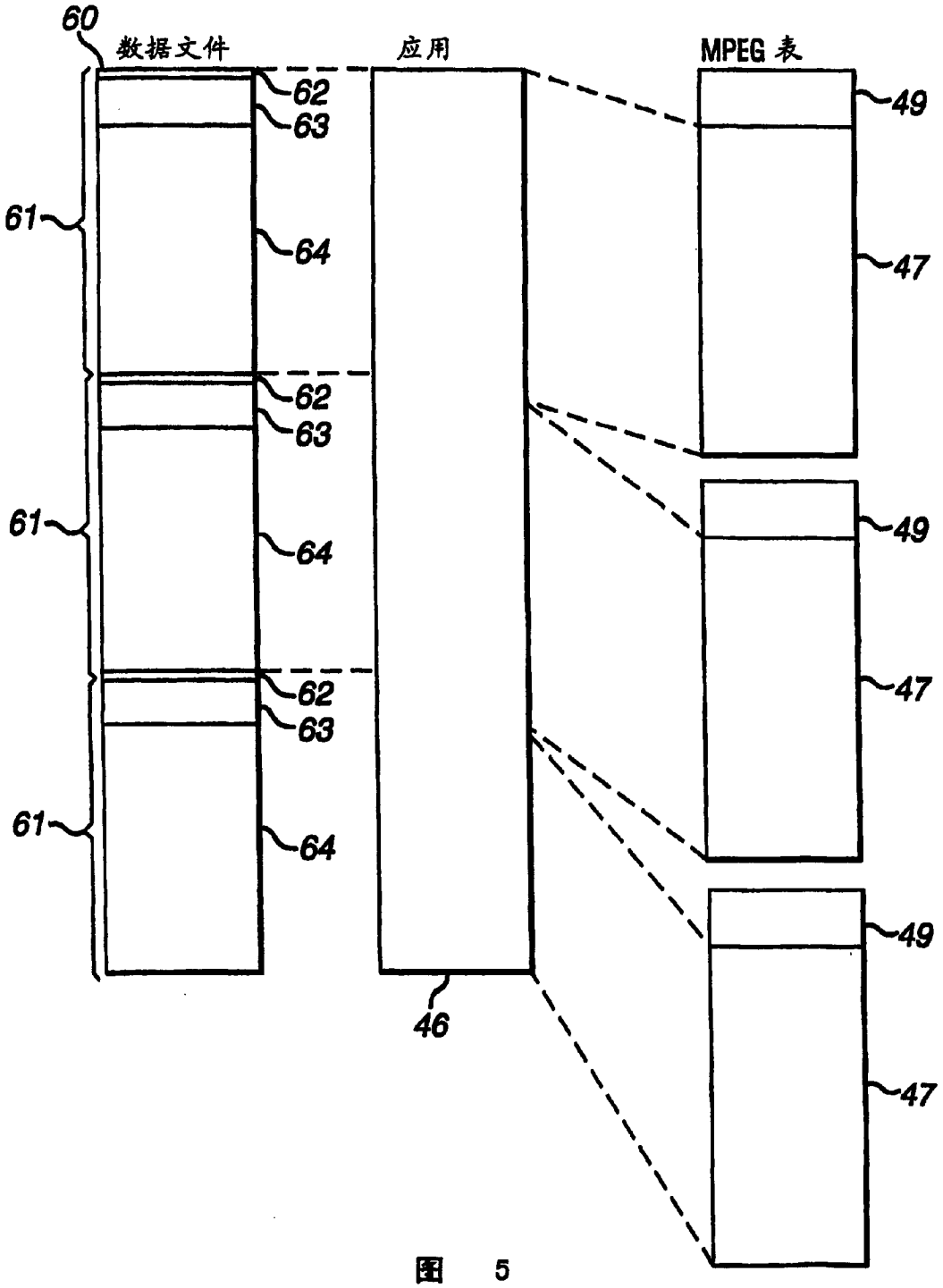


图 5

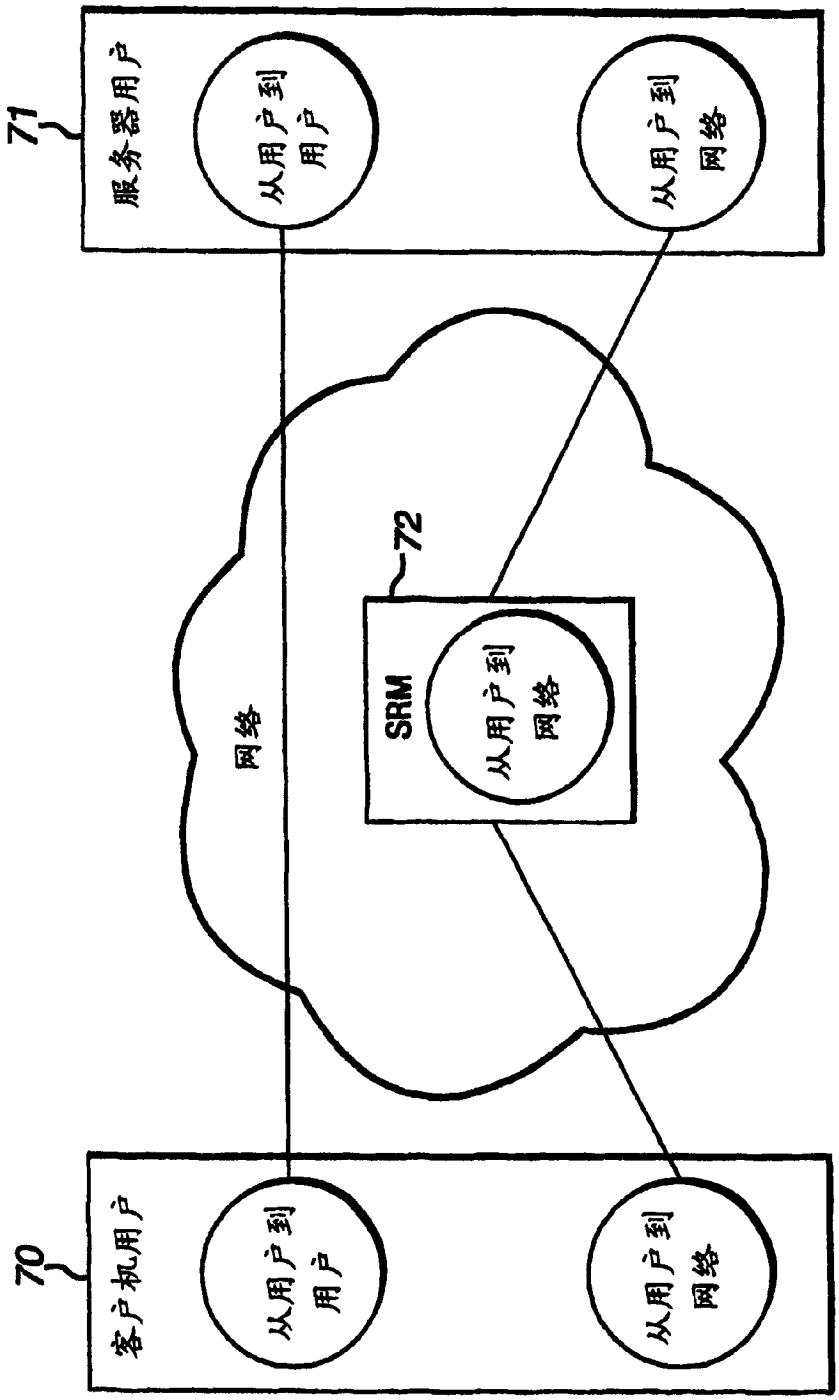

71
服务器用户
从用户到用户
从用户到网络
网络
72
SRM
从用户到网络
70
客户机用户
从用户到用户
从用户到网络

图 6

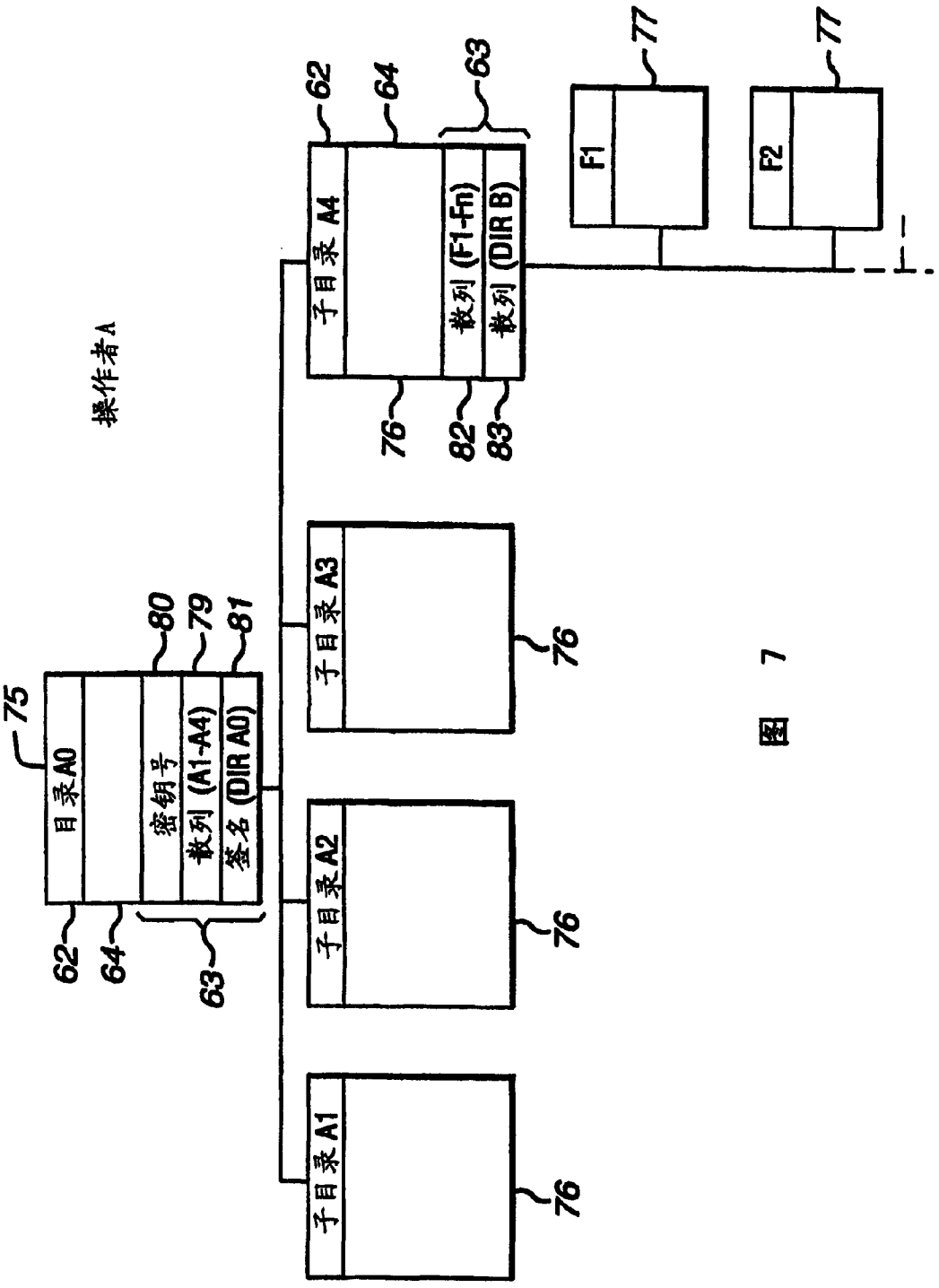

操作者A
目录A0
密钥号
数列 (A1-A4)
签名 (DIR A0)
75
80
79
81
62
64
63
子目录A4
数列 (F1-Fn)
数列 (DIR B)
62
64
63
76
82
83
F1
F2
77
77
子目录A3
子目录A2
子目录A1
76
76
76

图 7

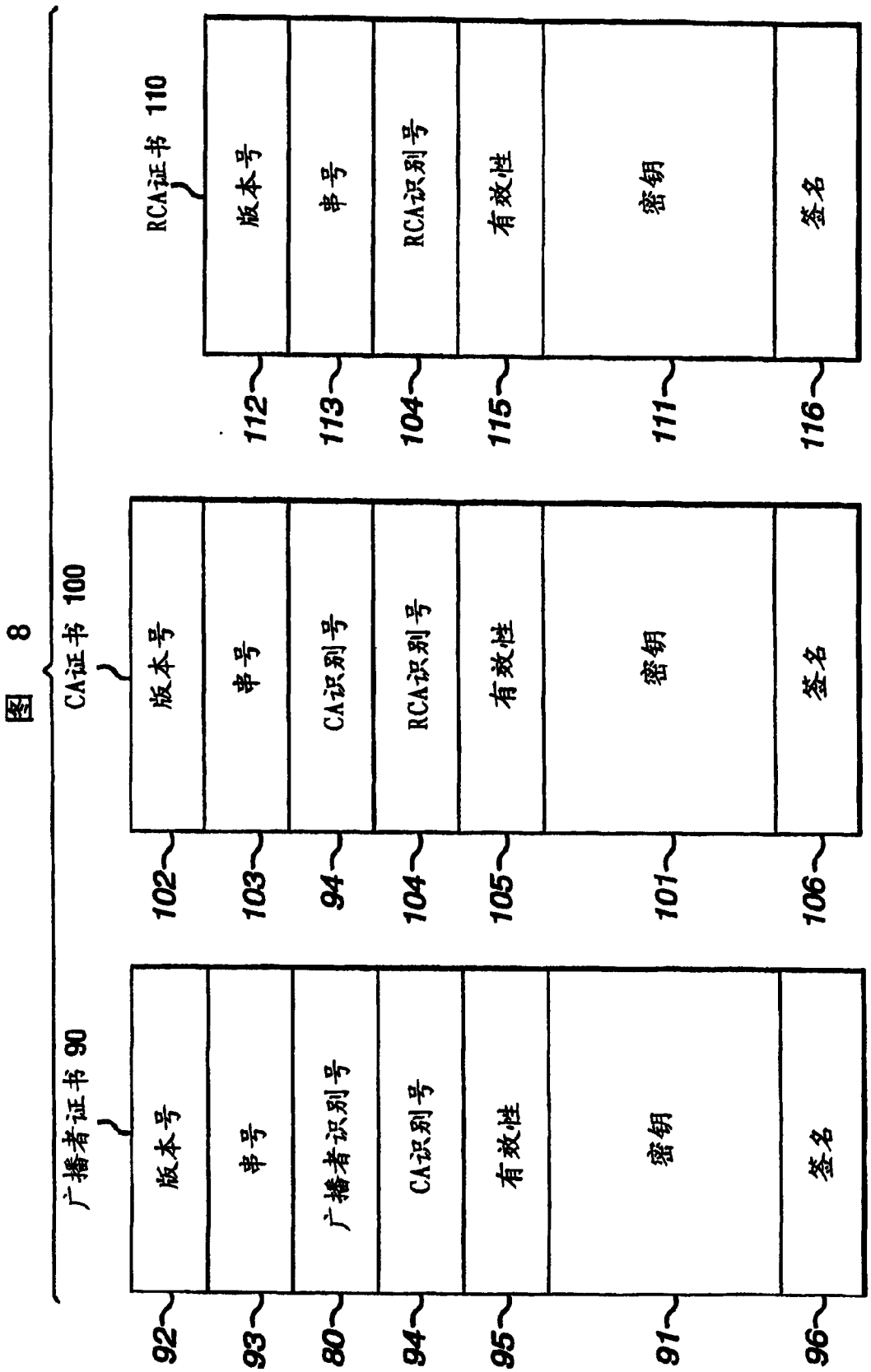


图 8
广播者证书 90
版本号
串号
广播者识别号
CA识别号
有效性
密钥
签名
92
93
80
94
95
91
96
CA证书 100
版本号
串号
CA识别号
RCA识别号
有效性
密钥
签名
102
103
94
104
105
101
106
RCA证书 110
版本号
串号
RCA识别号
有效性
密钥
签名
112
113
104
115
111
116

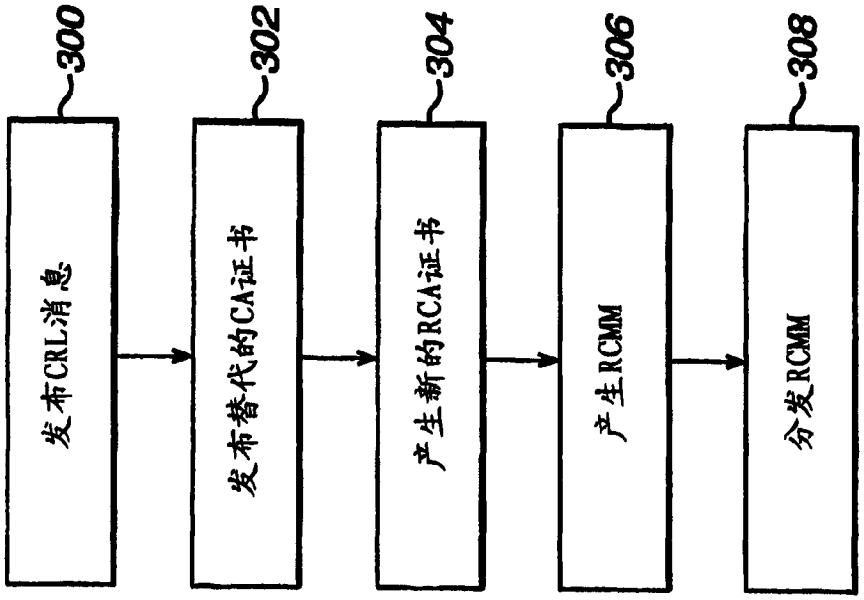

300
发布CRL消息
302
发布替代的CA证书
304
产生新的RCA证书
306
产生RCMM
308
分发RCMM

图 12

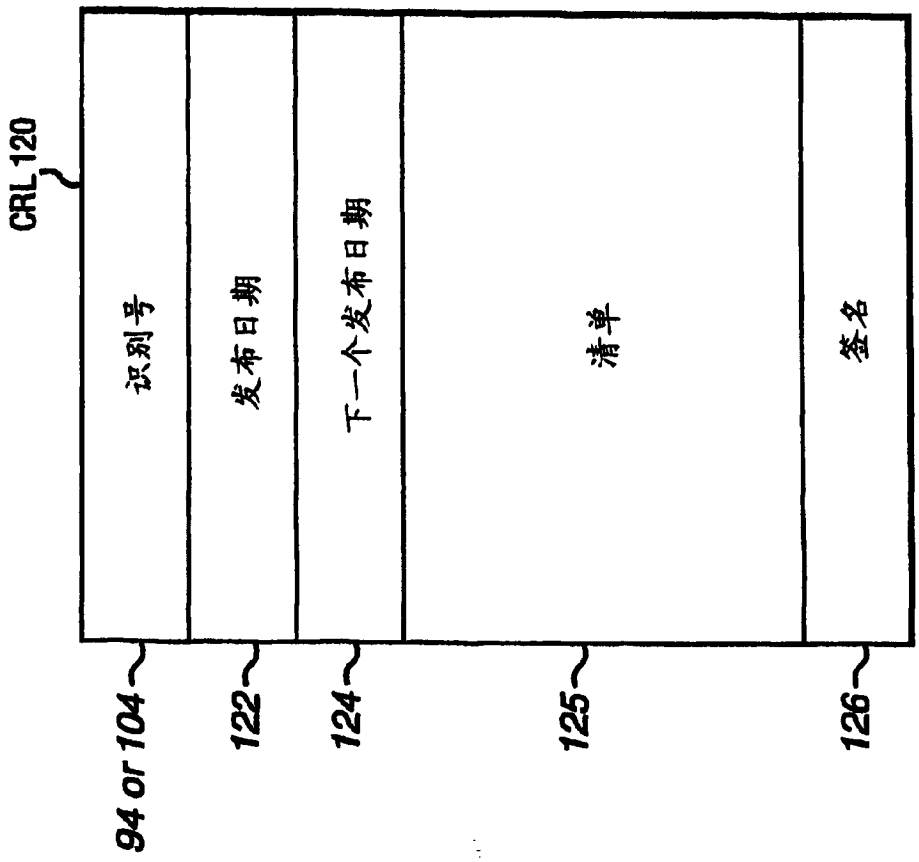

CRL 120
识别号
发布日期
下一个发布日期
清单
签名
94 or 104
122
124
125
126

图 9

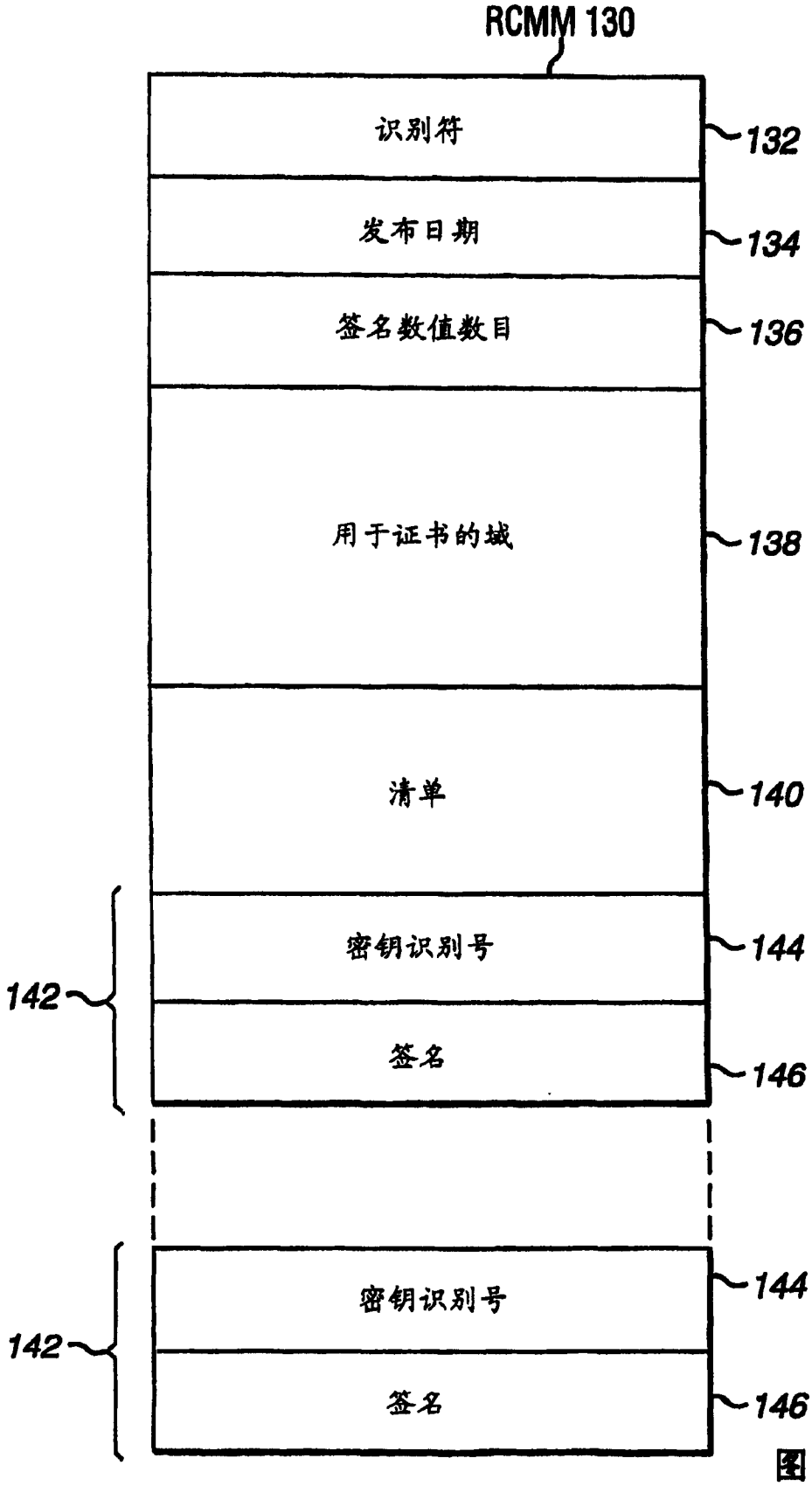

RCMM 130
识别符
132
发布日期
134
签名数值数目
136
用于证书的域
138
清单
140
142
密钥识别号
144
签名
146
142
密钥识别号
144
签名
146

图 10

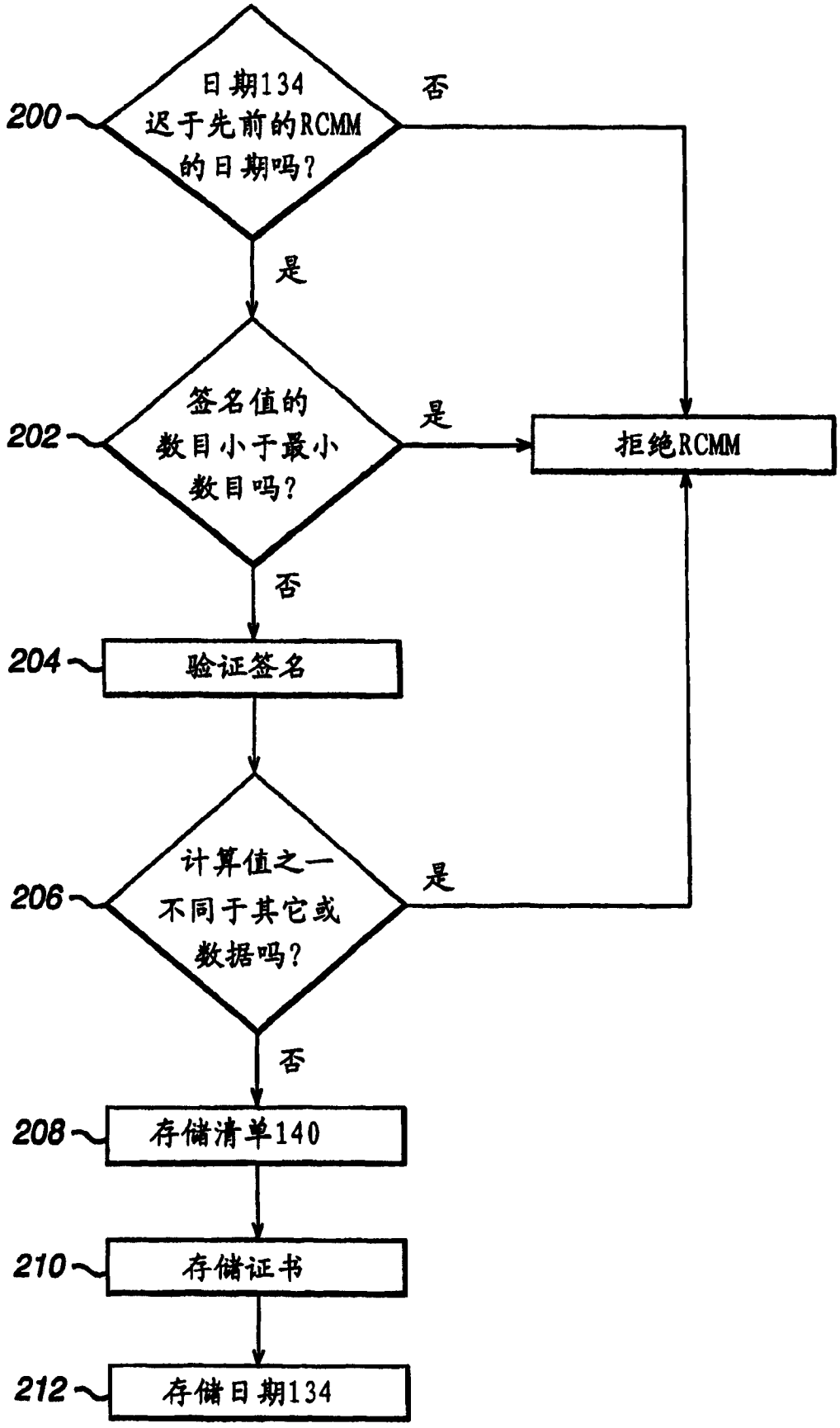

200
日期134
迟于先前的RCMM
的日期吗?
否
是
202
签名值的
数目小于最小
数目吗?
是
拒绝RCMM
否
204
验证签名
206
计算值之一
不同于其它或
数据吗?
是
否
208
存储清单140
210
存储证书
212
存储日期134

图 11