



[12] 发明专利说明书

[21] ZL 专利号 97182181.X

[45] 授权公告日 2004 年 12 月 1 日

[11] 授权公告号 CN 1178504C

[22] 申请日 1997.4.25 [21] 申请号 97182181.X

[30] 优先权

[32] 1997. 3. 21 [33] EP [31] 97400650.4

[86] 国际申请 PCT/EP1997/002111 1997.4.25

[87] 国际公布 WO1998/043431 英 1998.10.1

[85] 进入国家阶段日期 1999.11.11

[71] 专利权人 卡纳尔股份有限公司

地址 法国巴黎

[72] 发明人 J-C·萨尔法蒂 J·梅里克

审查员 龚锦玲

[74] 专利代理机构 中国专利代理(香港)有限公司

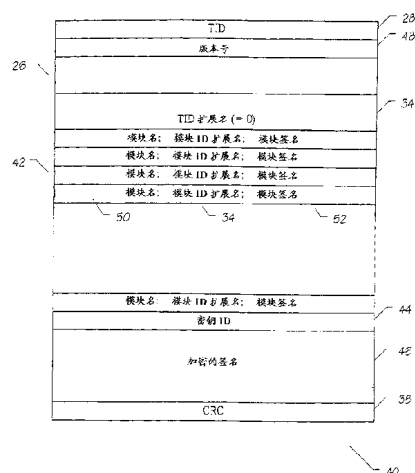
代理人 王 岳 王忠忠

权利要求书 3 页 说明书 21 页 附图 9 页

[54] 发明名称 向 MPEG 接收/译码器下载数据的方法和 MPEG 传输系统

[57] 摘要

在一种数字卫星电视系统中, 电视机通过一个诸如机顶盒的接收/译码器来接收信号, 可以下载交互式的作业并且在接收/译码器上运行。将作业代码设置成模块, 并且在下载模块之前在一个特定的本地地址内部检索一个目录模块。为模块加上标记, 还要为目录模块加上标记并且加密, 从而将一个密码用于构成一项作业的所有模块。在接收/译码器的 ROM 中存储多个公用密钥, 以便从不同的来源产生这种作业, 而这些来源不需要互相知道对方的私人密钥。可以将密钥便利地暂存在接收/译码器的 RAM 中, 让接收/译码器的制造商能够检查它的功能。可以将目录的签名隐藏在目录模块的伪数据块中的一个可变的位置上。准备下载的作业需要经过存储在接收/译码器中的一个作业确认位图的核查。



权 利 要 求 书

1. 向 MPEG 接收/译码器下载数据的方法, 该方法包括以下步骤:
为准备下载的数据产生一个签名;
按照一个数据块的起点和该签名的起点之间的一个选定的偏移将该签名和其他数据纳入该数据块中;
用私人密钥对该数据块加密;
将准备下载的数据及加密的数据块格式化成一个 MPEG 表;
发送该 MPEG 表; 和
在接收/译码器上:
接收该 MPEG 表;
使用对应着私人密钥的一个公用密钥对接收的 MPEG 表中加密的数据块执行解密;
在接收/译码器的存储器保护区内查找至少一个存储的偏移;
使用上述查找的偏移, 从解密的数据块的起点开始从解密的数据块中提取所述签名;
为接收的 MPEG 表中的数据产生一个签名; 和
将从解密数据块中提取的签名与接收/译码器上为接收的数据产生的签名进行比较。
2. 按照权利要求 1 的方法, 其特征不在于, 上述存储器保护区中具有至少两个这种存储的偏移, 如果提取的签名和产生的签名在比较步骤中彼此不符, 就进一步包括以下的步骤: 用另一个存储的偏移重复查找、提取和比较签名。
3. 按照权利要求 1 或 2 的方法, 其特征不在于, 在数据块中的上述其他数据至少有一些属于伪数据或随机数据。
4. 按照权利要求 1 或 2 的方法, 其特征不在于, 数据以多种数据模块的形式下载, 并且包括以下的步骤:
为准备下载的每个数据模块产生一个模块签名;
将各数据模块格式化成各自的模块 MPEG 表;
产生一个包括每一模块 MPEG 表的识别符和各自的签名在内的目录, 并且

在接收/译码器上:

为接收的模块 MPEG 表中的每个模块产生各自的模块签名; 和
将接收的目录 MPEG 表中的每个模块签名与接收/译码器上产生的各自的模块签名相比较。

5. 按照权利要求 4 的方法, 其特征在于, 进一步包括以下步骤:
在模块签名比较步骤中, 如果接收的目录 MPEG 表中的模块签名与接收/译码器中为该模块产生的相应模块签名彼此不符, 就禁止或是中止下载这种数据模块。

6. 按照权利要求 1 或 2 的方法, 其特征在于, 进一步包括以下步骤:
在比较步骤中, 如果该解密的签名与产生的签名彼此不符, 就禁止或是中止下载这种数据。

7. 一种用于向 MPEG 接收/译码器下载数据的方法的 MPEG 接收/译码器, 该方法包括以下步骤:

为准备下载的数据产生一个签名;

按照一个数据块的起点和该签名的起点之间的一个选定的偏移将该签名和其他数据纳入该数据块中;

用私人密钥对该数据块加密;

将准备下载的数据及加密的数据块格式化成一个 MPEG 表; 其特征
在于, 所述 MPEG 接收/译码器包括:

用来接收这种 MPEG 表的装置;

用来存储一个公用密钥和这一公用密钥的识别符的装置;

用来存储至少一个偏移的存储器保护区; 和

被编程的处理装置, 采用对应着私人密钥的存储的公用密钥对这种接收的 MPEG 表中加密的数据块进行解密; 在存储器保护区内查找上述的一个存储的偏移; 使用上述查找的偏移, 从解密的数据块的起点开始从解密的数据块中提取签名; 为接收的 MPEG 表中的数据产生一个签名; 并且将从解密的数据块中提取的签名与接收/译码器中为接收的数据所产生的签名相比较。

8. 按照权利要求 7 的接收/译码器, 其特征在于, 在存储器保护区内存储着至少两个这种偏移, 如果提取的签名和产生的签名彼此不符, 处理装置就采用存储的偏移中的另一个存储的偏移重复地查

找、提取和比较签名。

9. 按照权利要求 8 的接收/译码器，其特征在于，用来存储偏移的存储器是由可重写的非易失性存储器构成的。

10. 权利要求 7 到 9 之一的接收/译码器，其特征在于，所述被编程的处理装置为接收的模块 MPEG 表中的每一个模块产生各自的一个模块签名，并且将接收的目录 MPEG 表中的每一个模块签名与接收/译码器中产生的各自的模块签名相比较。

11. 按照权利要求 10 的接收/译码器，其特征在于，如果接收的目录 MPEG 表中的模块签名与接收/译码器中为该模块产生的相应的模块签名彼此不符，所述被编程的处理装置就禁止或是中止下载这种数据模块。

12. 按照权利要求 7 到 9 之一的接收/译码器，其特征在于，如果该解密的签名与产生的签名彼此不符，所述程序处理装置就禁止或是中止下载这种数据。

说明书

向 MPEG 接收/译码器下载数据的方法和
MPEG 传输系统

5 技术领域

本发明涉及到:

· 向 MPEG (动画专家组 (moving picture expert group)) 接收/译码器下载数据的方法;

· 这样的一种 MPEG 接收/译码器; 以及

10 · 一种 MPEG 传输系统。

数字传输系统的出现原来是用于广播电视信号的, 特别是不排除卫星电视系统在内的此类系统都具有用于开发其他目的的可能性。这其中就包括为终端用户提供交互式作业。

背景技术

15 一种途径就是在用来接收电视信号的接收/译码器上运行一项作业。作业的代码可以永久性地存储在接收/译码器中。然而, 这样可能会形成一种限制。最好是让接收/译码器能够下载所需作业的代码。按照这种方式可以提供更多的灵活性, 并且可以根据需要来更新作业, 用户部分不需要做任何动作。

20 在一个 MPEG 系统中, 可以从一个 MPEG 表中下载作业代码。然而, 对于借助单个的 MPEG 表下载的代码来说, 其大小是受到限制的。另外, 如果需要在运行一项作业之前下载完整的作业, 这种方式所造成的延迟是用户无法接受的。因此就需要有一种能够以许多模块的形式下载一项作业的方法。然而, 由此所产生的问题是如何从 MPEG 比特流中识别和提取一项特定作业中所需的模块。本发明的第一方面就涉及到这个问题。

发明内容

按照本发明的第一方面, 提供了一种向 MPEG 接收/译码器下载一项作业的至少一部分的方法, 该方法包括以下步骤: 将作业划分成许多模块; 将每个模块格式化成各自的 MPEG 表, 在表中具有相同的表识别符
30 (“TID”) 和除了一个预定的 TID-扩展名之外各自不同的表识别符扩展名 (“TID-扩展名”); 为具有相同的上述 TID 和上述预定的 TID 扩展名

的模块产生一个目录 MPEG 表,在目录中包含每个模块的模块名和各自的 TID-扩展名;在 MPEG 比特流中循环发送目录 MPEG 表和模块 MPEG 表;并且在 MPEG 接收/译码器上:接收 MPEG 比特流;下载具有预定的 TID 扩展名的一个 MPEG 表,从而下载其目录 MPEG 表;从目录 MPEG 表的内容确定模块 MPEG 表的 TID-扩展名;以及下载至少一个模块 MPEG 表,它与下载的目录 MPEG 表具有相同的 TID 和一个由下载的目录 MPEG 表确定的 TID-扩展名。

也就是说,一项作业是由许多模块构成的,如果能按照要求正确地运行就可以下载。目录表是很容易识别的,因为它具有特定的 TID 扩展名,并且一旦完成了下载,接收/译码器就能够从它们各自的 TID-扩展名中识别出模块表。

该方法还应该包括以下的步骤:在发送的目录 MPEG 表中包括其版本识别符;并且在接收/译码器上:确定当前发送的目录 MPEG 表的版本识别符是否比当前下载的目录 MPEG 表的版本识别符更新,如果是,就重复下载目录 MPEG 表,确定 TID-扩展名,以及下载至少一个模块 MPEG 表的步骤。

因此,如果一项作业被改变了,就可以自动地检测和更新目录,并且可以下载任何更新的模块。

至少有一个模块 MPEG 表可以被格式化成在 MPEG 比特流中单独发送的许多 MPEG 段,在每个 MPEG 段的预定部位包含该 MPEG 段在 MPEG 表中的识别符,以及对 MPEG 表中段数的一个指示。

按照本发明的第二方面,提供了一种用来部分执行本发明第一方面的方法的 MPEG 接收/译码器,它包括:用于接收 MPEG 比特流的接收机;一个存储装置;以及处理装置,为其编制的程序可以将接收到的具有预定的 TID-扩展名的一个 MPEG 表下载到存储装置中,根据目录 MPEG 表的内容来确定模块和 MPEG 表的 TID 扩展名,并且将与下载的目录 MPEG 表及其所确定的一个 TID-扩展名具有相同 TID 的至少一个模块 MPEG 表下载到存储装置中。

为处理装置编制的程序应该是这样的,确定当前发送的目录 MPEG 表的版本识别符是否比下载的目录 MPEG 表的版本识别符更新,如果是,就重复下载目录 MPEG 表,确定 TID-扩展名,并且下载至少一个模块 MPEG 表。

在采用接收/译码器来接收被格式化成许多独立发送段的至少一个模块表的情况下,就应该用处理装置的程序将 MPEG 段重复下载到存储装置中,直至处理装置根据段识别符和用来指示已下载段的段号确定了所有这些段都已经被下载时为止。

- 5 接收/译码器中应该进一步包括一个并行端口和/或一个串行端口,用来接收采用至少一种 MPEG 表格式的作业,在这种情况下最好是采用短 MPEG-2 格式,而用于诸如卫星或是电缆的远程接收则应该采用长 MPEG-2 格式。

这种特点在制造商希望测试接收/译码器的具体特性时是非常有用的,因为在下下载作业时不需要通过卫星电视系统进行发送。

按照本发明的第三方面所提供的一种 MPEG 传输系统包括:

- 用来将准备下载到 MPEG 接收/译码器上的一项作业划分成许多模块的装置;将每个模块格式化成各自的一个 MPEG 表的装置,在表中具有相同的 TID 和除了一个预定的 TID-扩展名之外各自不同的 TID-扩展名;为具有相同的上述 TID 和上述预定的 TID 扩展名的模块产生一个目录 MPEG 表的装置,在目录中包含每个模块的模块名和各自的 TID-扩展名;以及

用 MPEG 比特流循环发送目录 MPEG 表和模块 MPEG 表的装置。

- 系统中应该进一步包括用于为目录 MPEG 表产生版本识别符的装置;并且可以用其中的目录 MPEG 表产生装置将产生的版本识别符纳入目录 MPEG 表中。

可以用模块格式化装置将至少一个模块 MPEG 表格式化成许多的 MPEG 段,在每段中的预定部位包含该 MPEG 段在 MPEG 表中的识别符,以及该 MPEG 段在 MPEG 表中的指示号。

- 25 理想的接收/译码器应该能够受到保护,避免下载有可能包含病毒的非法作业。因此,应该考虑到至少为一部分作业代码加密和签名的问题。

- 按照本发明的第四方面所提供的一种向 MPEG 接收/译码器下载数据的方法包括以下步骤:为准备下载的数据产生一个签名;用私人密钥对签名加密;将准备下载的数据,加密的签名和私人密钥的识别符格式化成 MPEG 表;发送 MPEG 表;并且在接收/译码器上:接收 MPEG 表;按照接收的 MPEG 表中的密钥识别符来选择多个公用密钥其中的一个;

用选定的公用密钥对接收的 MPEG 表中加密的签名执行解密;为接收的 MPEG 表中的数据产生一个签名;以及将解密的签名与接收/译码器上为接收的数据产生的签名进行比较。

这样就可以用接收/译码器从一个以上的来源下载具有加密签名的作业,而这些来源并不需要互相知道对方的私人密钥。

该方法可以进一步包括以下步骤:向接收/译码器下载一项作业,该作业具有用带有预定的密钥识别符的私人密钥加密的签名;在接收/译码器上运行上述作业,让接收/译码器接收另一个密钥;将另一个密钥存储在接收/译码器的一个易失性存储区内。在这种情况下,在运行作业的步骤中可以从本地向接收/译码器提供另一个密钥,例如是通过接收/译码器的一个并行端口,串行端口或是智能卡读卡器。如果接收/译码器是连接到调制解调器的,则应该避免通过调制解调器向接收/译码器提供另一个密钥。

这种特点使得制造商能够在希望测试接收/译码器时向接收/译码器下载一个密钥。

该方法可以进一步包括以下步骤:在接收/译码器上从接收/译码器的存储器中的一个被保护区中查找用于选定的公用密钥的一个确认标志,如果没有设定被查找的标志,就禁止或是中止下载数据。

因此,尽管在接收/译码器的存储器中可以永久性地提供多个公用密钥,在必要的情况下可以有选择地禁止使用任何一个密钥,例如是在对联系着特定的公用密钥的一个私人密钥解除秘密的情况下,或是在原来使用着同一个密钥的两个操作员决定采用各自的密钥的情况下。

如果接收/译码器按照上述的方式来下载一项作业,该作业具有采用具有预定的密钥识别符的私人密钥加密的签名,在接收/译码器的存储器保护区内具有预定的密钥识别符的私人密钥就要有一个可以被上述作业改变的确认标志,并且根据这一确认标志的状态来确定能不能接收上述的另一个密钥。

为公用密钥提供确认标志的这些附属的特征与本发明的第四方面并没有直接的联系。因此,本发明的第五方面提供了一种向 MPEG 接收/译码器下载数据的方法,该方法包括以下步骤:为准备下载的数据产生一个签名;用私人密钥对签名加密;将准备下载的数据,加密的签名和私人密钥的识别符格式化成一个 MPEG 表;发送 MPEG 表;以及在接收/译码

器上:接收 MPEG 表;在接收/译码器的一个存储器保护区内查找一个公用密钥的确认标志,该公用密钥对应着在接收的 MPEG 表中验明的私人密钥;以及如果设定了查找的标志:就用对应着在接收的 MPEG 表中验明的私人密钥的那个公用密钥对接收的 MPEG 表中加密的签名执行解密,提供一个解密的签名;为接收的 MPEG 表中的数据产生一个签名;以及将解密的签名与接收/译码器上为接收的数据产生的签名进行比较。

本发明第四和第五方面的方法还应该进一步包括以下步骤:为准备下载的数据产生一个确认代码,在加密步骤中用签名为确认代码加密,并且在解密步骤中用签名为其进行解密;

10 在接收/译码器的存储器保护区内查找存储的确认代码;以及将查找的确认代码与解密的确认代码相比较。

这样就能将接收/译码器设置成仅仅能接收某些作业或是某种类型的作业。

这些附属的特征与本发明的第四和第五方面并没有直接的联系。

15 因此,本发明的第六方面提供了一种向 MPEG 接收/译码器下载数据的方法,该方法包括以下步骤:为准备下载的数据产生一个确认代码;为准备下载的数据或是其中的一部分产生一个签名;用私人密钥对确认代码和签名加密;将准备下载的数据及加密的确认代码和签名格式化至少一个 MPEG 表;发送每一个 MPEG 表;以及在接收/译码器上:接收每一个 MPEG 表;用对应着私人密钥的一个公用密钥对接收的 MPEG 表中加密的确认代码和签名执行解密;在接收/译码器的一个存储器保护区内查找存储的确认代码;将查出的确认代码与解密的确认代码相比较;

为接收的 MPEG 表或是其上述一部分中的数据产生一个签名;以及将解密的签名与接收/译码器上为接收的数据产生的签名进行比较。

25 该方法应该进一步包括以下步骤,如果查出的确认代码与解密的确认代码在确认代码比较步骤中彼此不符,就禁止或是中止下载数据。

按照本发明的第四到第六方面,可以在一个包括其他数据的数据块内为准备下载的数据的签名加密,在数据块的起点和签名的起点之间有一个选定的偏移,并且在解密步骤中在接收/译码器上为加密的数据块解密,并且在接收/译码器上进一步包括以下步骤,在接收/译码器的存储器保护区内查找至少一个存储的偏移,以及用上述的一个查出的偏移从解密的数据块的起点开始从解密的数据块中提取上述签名。

因此,可以将签名隐藏在其他伪数据当中,从而更难以确定签名的位置。这一特征也有可能使数据仅仅能在一或多组特定的接收/译码器上使用。

这些特征与本发明的第四到第六方面并没有直接的联系。因此,本
5 发明的第七方面提供了一种向 MPEG 接收/译码器下载数据的方法,该方法包括以下步骤:为准备下载的数据产生一个签名;按照数据块的起点和签名的起点之间的一个选定的偏移将签名和其他数据纳入一个数据块中;用私人密钥对数据块加密;将准备下载的数据及加密的数据块格式化成一个 MPEG 表;发送 MPEG 表;以及在接收/译码器上:接收 MPEG 表;
10 用对应着私人密钥的一个公用密钥对接收的 MPEG 表中加密的数据块执行解密;在接收/译码器的存储器保护区内查找至少一个存储的偏移;用上述的一个查出的偏移从解密的数据块的起点开始从解密的数据块中提取签名;为接收的 MPEG 表中的数据产生一个签名;以及将从解密数据块中提取的签名与接收/译码器上为接收的数据产生的签名进行比较。

15 如果在上述存储器保护区中具有至少两个存储的偏移,如果提取的签名和产生的签名在比较步骤中彼此不符,该方法就可以进一步包括以下的步骤:用另一个存储的偏移重复查找,提取和比较的步骤。

在数据块中的上述其他数据至少有一些属于伪随机数据,但是,如果是这样,伪数据段与签名之间应该没有重复。

20 按照本发明的第四到第七方面,可以按照许多数据模块的形式下载数据,并且还可以包括以下的步骤:为准备下载的每个数据模块产生一个模块签名;将数据模块格式化成各自的模块 MPEG 表;产生一个包括每一模块 MPEG 表的识别符和各自的签名在内的目录,对这种目录执行上述的产生签名的步骤;并且在接收/译码器上:为接收的模块 MPEG 表中的
25 的每个模块产生各自的一个模块签名;以及将接收的目录 MPEG 表中的每个模块签名与接收/译码器上产生的各自的模块签名相比较。

因此,尽管准备下载的数据是由许多模块构成的,为了对模块加密,仅仅需要执行一次加密程序,并且在需要核查签名时仅仅需要执行一次解密程序。

30 这些特征与本发明的第四到第七方面并没有直接的联系。因此,本发明的第八方面提供了一种向 MPEG 接收/译码器下载许多数据模块的方法,该方法包括以下步骤:为准备下载的每个数据模块产生一个模块

签名;将数据模块格式化成各自的模块 MPEG 表;产生一个目录,在目录
中包括每个 MPEG 表的识别符和各自的签名;为目录产生一个目录签名;
用私人密钥对目录签名加密;将目录和加密的目录签名格式化成一个目
录 MPEG 表;发送目录和模块 MPEG 表;以及在接收/译码器上:接收目录
5 和模块 MPEG 表;用对应着私人密钥的公用密钥对接收的目录 MPEG 表中
加密的目录签名进行解密;为接收的 MPEG 表中的目录产生一个目录签
名;将解密的目录签名与接收/译码器中产生的目录签名相比较;为接收
的模块 MPEG 表中的每一个模块产生各自的模块签名;以及将接收的目
录 MPEG 表中的每一个模块签名与接收/译码器中产生的各自的模块签
10 名相比较。

该方法进一步包括以下步骤:在模块签名比较步骤中,如果接收的
目录 MPEG 表中的模块签名与接收/译码器中为该模块产生的各自的模
块签名彼此不符,就禁止或是中止下载这种数据模块。

上述的方法还可以进一步包括以下步骤:在比较步骤中,如果解密
15 的签名与产生的签名彼此不符,就禁止或是中止下载这种数据模块。

按照本发明的第九方面提供了一种用于部分执行本发明第四方面
所述方法的一种 MPEG 接收/译码器,其特征是包括:用来接收这种 MPEG
表的装置;用来存储多个公用密钥和每个公用密钥的一个识别符的装置;
以及一个程序处理装置,用于按照接收的 MPEG 表中的密钥识别符来选
20 择一个存储的公用密钥;用选定的公用密钥对接收的 MPEG 表中加密的
签名解密,提供一个解密的签名;为接收的 MPEG 表中的数据产生一个签
名;以及将解密的签名与接收/译码器中为接收的数据所产生的签名相
比较。

密钥存储装置最好是由 ROM 构成的,并且可以由公用密钥在密钥存
25 储装置中的存储位置来提供每个公用密钥的识别符。

这种接收/译码器还可以进一步包括一个易失的存储区,处理装置
可以向这一存储区中下载一项作业,该作业具有一个用带有预定的密钥
识别符的私人密钥加密的签名,运行这种作业,让接收/译码器接收另一
个密钥,并且将另一个密钥存储在易失的存储区中。

30 接收/译码器还可以进一步包括用来接收从本地提供给接收/译码
器的这种另一个密钥的装置,例如是接收/译码器的一个并行端口,串行
端口和/或智能卡读卡器。易失的存储器是由 RAM 构成的。同样,如果

(2)

接收/译码器是连接到调制解调器的,则应该避免通过调制解调器向接收/译码器提供另一个密钥。

接收/译码器还可以进一步包括一个存储器的保护区,用来存储至少是某些公用密钥的各自的确认标志,并且可以用程序处理装置在保护区内查找选定的每个公用密钥的这种确认标志,如果没有设定被查找的标志就禁止或是中止下载数据。

接收/译码器还可以进一步包括一个存储器的保护区,用来存储具有预定的密钥识别符的私人密钥的一个确认标志,并且其中的程序处理装置在运行上述作业时可以改变这种确认标志,并且可以按照这一标志的状态来存储另一个密钥。

这些附属的特征与本发明的第九方面并没有直接的联系。因此,本发明的第十方面提供了一种 MPEG 接收/译码器,它包括:用来接收这种 MPEG 表的装置;用来存储一个公用密钥和这一公用密钥的识别符的装置;用来存储这一公用密钥的确认标志的一个存储器保护区;以及一个程序处理装置,用于在接收/译码器的存储器保护区内查找与接收的 MPEG 表中识别到的私人密钥相对应的这一公用密钥的确认标志;如果设定了被查找的标志,就用对应着从接收的 MPEG 表中识别出来的私人密钥的那个公用密钥对接收的 MPEG 表中加密的签名进行解密,提供一个解密的签名,为接收的 MPEG 表中的数据产生一个签名;并且将解密的签名与接收/译码器中为接收的数据所产生的签名相比较。

用来存储密钥确认标志的存储器应该是由可重写的非易失性存储器构成的。

如果存储了多个这种公用密钥,就应该将用来存储确认标志的存储器设置成一个位图。

按照本发明第十方面的接收/译码器可以进一步包括一个用来存储确认代码的存储器保护区,并且用其中的程序处理装置对接收的 MPEG 表中的确认代码进行解密,查找存储的确认代码,并且将查出的确认代码与解密的确认代码相比较。

这些附属的特征与本发明的第九或第十方面并没有直接的联系。因此,本发明的第十一方面提供了一种 MPEG 接收/译码器,它包括:用来接收这种 MPEG 表的装置;用来存储一个公用密钥和这一公用密钥的识别符的装置;用来存储一个确认代码的一个存储器保护区;以及程序处

理装置,采用对应着私人密钥的存储的公用密钥对这种接收的 MPEG 表中加密的确认代码和签名进行解密;在存储器保护区内查找存储的确认代码;将查出的确认代码与解密的确认代码相比较;为接收的 MPEG 表或是其上述部分中的数据产生一个签名;并且将解密的签名与接收/译码器中为接收的数据所产生的签名相比较。

如果查出的确认代码与解密的确认代码彼此不符,程序处理装置就应该禁止或是中止下载数据。

用来存储确认代码的存储器应该是由可重写的非易失性存储器构成的,并且将其设置成一个位图。

按照本发明第九到十一方面的接收/译码器还可以进一步包括用来存储至少一个偏移的存储器保护区,并且用其中的程序处理装置对这种接收的 MPEG 表中加密的数据块进行解密,在存储器保护区内查找上述的一个存储的偏移,并且从解密的数据块的起点开始用查出的偏移从解密的数据块中提取签名。

这些附属的特征与本发明的第九到第十一方面并没有直接的联系。因此,本发明的第十二方面提供了一种 MPEG 接收/译码器,它包括:用来接收这种 MPEG 表的装置;用来存储一个公用密钥和这一公用密钥的识别符的装置;用来存储至少一个偏移的存储器保护区;以及

程序处理装置,采用对应着私人密钥的存储的公用密钥对这种接收的 MPEG 表中加密的数据块进行解密;在存储器保护区内查找上述的一个存储的偏移;从解密的数据块的起点开始用查出的偏移从解密的数据块中提取签名;为接收的 MPEG 表中的数据产生一个签名;并且将从解密的数据块中提取的签名与接收/译码器中为接收的数据所产生的签名相比较。

用来存储偏移的存储器最好是由可重写的非易失性存储器构成的。

在按照本发明第九到第十二方面的接收/译码器中,可以用程序处理装置为接收的模块 MPEG 表中的每一个模块产生各自的一个模块签名,并且将接收的目录 MPEG 表中的每一个模块签名与接收/译码器中产生的各自的模块签名相比较。

这些附属的特征与本发明的第九到第十二方面并没有直接的联系。因此,本发明的第十三方面提供了一种 MPEG 接收/译码器,它包括:

用来接收这种目录和模块 MPEG 表的装置;

用来存储一个公用密钥和这一公用密钥的识别符的装置;以及程序处理装置,采用对应着私人密钥的存储的公用密钥对接收的目录 MPEG 表中加密的目录签名进行解密;为接收的目录 MPEG 表中的目录产生一个目录签名;将解密的目录签名与接收/译码器所产生的目录签名相比较;为接收的模块 MPEG 表中的每一个模块产生各自的一个模块签名;并且将接收的目录 MPEG 表中的每一个模块签名与接收/译码器所产生的各自的一个模块签名相比较。

如果接收的目录 MPEG 表中的模块签名与接收/译码器中为该模块产生的各自的一个模块签名彼此不符,程序处理装置就应该禁止或是中止下载这种数据模块。

在本发明第九到第十三方面的任何一种接收/译码器中,如果各自的一个解密的签名与产生的签名彼此不符,程序处理装置就应该禁止或是中止下载数据。

附图说明

以下要参照附图通过举例的方式说明本发明的最佳特征,在附图中:

图1表示一个数字电视系统的总体结构;

图2表示图1的数字电视系统中的一个交互系统的结构;

图3是构成图1和2所示系统中一部分的一个接收/译码器的接口示意图;

图4是这种数字电视系统中使用的一个遥控器的示意图;

图5表示下载到交互式接收/译码器的存储器中的一个模块内部的文件结构;

图6表示MPEG数据流的许多分量之间的内部关系;

图7说明了如何用模块/表来构成一项作业,模块/表又可以由许多段构成;

图8表示一个目录模块的内容;

图9表示目录模块内容中更具体的部分;以及

图10表示在电视系统的接收/译码器的存储器中的各个区。

具体实施方式

在图1中表示了按照本发明的数字电视系统1000的概况。本发明包括使用公知的MPEG-2压缩系统来发送压缩数字信号的最普通的数字电视系统2000。具体地说,用广播中心的MPEG-2压缩器2002接收一个数字信号流(通常是视频信号流)。通过链路2006将压缩器2002连接到一个复用和扰频器2004。复用器2004另外还要接收多个经过扰频或是比较透明的输入信号流,并且通过包括电信线路在内的各种形式的链路2010向广播中心的发射机2008发送压缩的数字信号。发射机2008通过上行线路2012向卫星转发器2014发送电磁信号,在卫星上经过电子处理之后通过国内下行线路2016向诸如终端用户所拥有或是租赁的抛物面天线一类的地面接收机2018广播。接收机2018接收到的信号被发送给终端用户所拥有或是租赁的一个集成的接收/译码器2020,并且连接到终端用户的电视机2022上。用接收/译码器2020对压缩的MPEG-2信号译码,变成电视机2022的电视信号。

将部分位于广播中心且部分设在其他广播供应商处的一个条件存取系统3000连接到复用器2004和接收/译码器2020。可以将一个能够对涉及商业来源(也就是由广播供应商出售的一或多个电视节目)的信息解密的智能卡插入接收/译码器2020。终端用户使用这种译码器2020和智能卡就可以按照订阅方式或是每次观看时付费的方式从商业来源采购。

同样也是部分位于广播中心且部分设在译码器中的一个交互系统4000也被连接到复用器2004和接收/译码器2020,让终端用户能够通过调制解调反向信道4002执行各种交互式作业。

图2表示本发明的数字电视系统1000的交互式电视系统4000的总体结构。

例如,交互式系统4000允许终端用户按照屏幕上的目录采购物品,根据需要查阅本地新闻和气象地图以及通过他的电视机玩游戏。

交互式系统4000总体上包括四个主要部件:

- 设在广播中心等处的一个编辑工具4004,供广播供应商来产生,开发,调试和测试作业;

- 在广播中心连接到编辑工具4004上的一个作业和数据服务器4006,供广播供应商对供给复用和扰频器2004的作业和数据进行制备,鉴定和

格式化,以便插入准备广播给终端用户的MPEG-2传送数据流(通常是其中的私人片段);

· 包括运行时间工具(RTE)4008在内的一个虚拟计算机,它是一种安装在终端用户所拥有或是租赁的接收/译码器2020中的执行代码,让终端用户能够对作业进行接收,鉴定,解压缩,并且将其装入译码器2020的工作存储器中执行。工具4008还可以运行驻留的通用作业。工具4008的硬件和操作系统是独立的;以及

· 处在接收/译码器2020与作业和数据服务器4006之间的调制解调反向信道4002,可以按照终端用户的要求用信号指令服务器4006在MPEG-2传送数据流中插入数据和作业。

交互式电视系统使用“作业”来控制接收/译码器和装在其内的各种设备的功能。作业以“资源文件”的形式存在于工具4008中。一个“模块”是一组资源文件和数据。接收/译码器的一个“存储体”是指供模块使用的存储空间。模块可以从MPEG-2传送数据流中下载到接收/译码器2020。

接收/译码器2020的物理接口被用来下载数据。参见图3,译码器2020中例如包含了六个下载设备;MPEG-2数据流调谐器4028,串行接口4030,并行接口4032,调制解调器4034和两个读卡器4036。

为了便于说明,一项作业是指用来控制接收/译码器2020的高级功能的一段计算机代码。例如,当终端用户将一个遥控器2026(图4中表示了它的细节)的聚焦位置放在从电视机2022的屏幕上可以看到的一个按钮目标上并且按下有效键时,就开始运行与这一按键相应的指令序列。

交互式作业可以推荐菜单并且按照终端用户的要求执行指令,并且提供关于作业用途的数据。作业可以是驻留的,也就是存储在接收/译码器2020的ROM(或是FLASH或者是其他非易失性存储器)中的作业,或者是广播和下载到接收/译码器2020的RAM(或是FLASH)中的作业。

作业的例子有:

· Initiating Application. 接收/译码器2020装备有驻留的初始化作业,适合用来收集让接收/译码器2020立即进入MPEG-2操作环境的模块(以下还要具体定义这一术语)。该作业提供了广播供应商在需要时可以进行修改的核心特征。它还可以在驻留的作业和下载的作业之间提供一个接口。

· Startup Application. 起动作业可以使下载或是驻留的一切作业在接收/译码器2020上运行。这种作业是在开始起动一项业务的作业时执行的一种引导程序。将起动作业下载到RAM中以便于更新。这样就可以直接在下载之后或是预装之后选择和运行各个频道上的交互式作业。在预装的情况下,将作业下载到存储器2024中并且在需要时通过起

5 动作业来起动。

· Program Guide. 节目向导是一种交互式作业,它可以提供关于节目的充分信息。例如可以提供在数字电视供应商的每个频道上的一周电视节目的有关信息。只要按下遥控器2026上的一个按键,终端用户

10 就可以进入一个重叠在电视机2022屏幕上显示的图像之上的一个添加屏幕。这种添加屏幕是一个浏览器,给出了数字电视供应商在各个频道上提供的当前和后续节目的信息。只要按下遥控器2026上的另一个按键,终端用户就可以进入一个作业,显示一周节目信息的目录。终端用户也可以直接按照习惯对节目进行检索和分类。终端用户还可以直接

15 进入一个选定的频道。

· Pay Per View Application. 每次观看时付费的作业是数字TV供应商配合着条件存取系统3000在每个PPV频道上提供的一种交互式业务。终端用户可以通过TV引导或是频道浏览器进入这种作业。另外,一旦在PPV频道上检测到一个PPV项目时就自动起动这种作业。终端用户

20 可以通过他的子智能卡3020或是通过通信服务器3022(使用调制解调器,电话和DTME代码,MINITEL等等)购买当前的项目。作业可以驻留在接收/译码器2020的ROM中,或是下载到接收/译码器2020的RAM中。

· PC Download 作业。终端用户可以用PC下载作业下载计算机软件。

25 · Magazine Browser 作业。杂志浏览器作业包括一个循环播放的电视图象,通过屏幕上的按钮来引导终端用户。

· Quiz 作业。问答作业应该与广播问答节目是同步的,例如将多种选择的问题显示在电视机2022的屏幕上,用户可以用遥控器2026来选择一个答案。问答作业可以告知用户他的答案是否正确,并且保存用户的

30 成绩。

· Teleshopping 作业。在电子购物作业的一个例子中,出售物品的售价被发送给接收/译码器2020并且显示在电视机2022上。用户可以

用遥控器2026来选购特定的物品。通过调制解调的反向信道4002将采购命令发送给作业和数据服务器4006或是一个独立的销售系统,其电话号码可以事先下载到接收/译码器上,还可以用一条命令将帐单记入已经被插在接收/译码器2020的一个读卡器4036中的信用卡。

5 · Telebanking 作业。在电子银行事物作业的一个例子中,用户将银行卡插入接收/译码器2020的一个读卡器4036中。接收/译码器2020用存储在银行卡上或是接收/译码器中的电话号码向用户的银行拨号,然后由作业来提供许多可以用遥控器2026选择的便利项目,例如是通过电话线路下载一个财务报表,在帐户之间转帐,请求支票簿等等。

10 · Internet Browser 作业。在 Internet 浏览器作业的一个例子中,来自用户的一个指令例如是请求查阅具有特定 URL 的一个网页通过遥控器 2026 被输入,然后通过调制解调的返回信道 4002 发送给作业和数据服务器 4006。然后将适当的网页纳入广播中心的传输中,由接收/译码器 2020 通过上行线路 2012,转发器 2014 和下行线路 2016 来接收,
15 并且显示在电视机 2022 上。

作业以资源文件的形式被存储在接收/译码器2020的本地存储器中。在资源文件中包括图形目标描述单元文件,可变块单元文件,指令序列文件,作业文件和数据文件。

20 图形目标描述单元文件描述了屏幕,也就是作业的人-机接口。可变块单元文件描述了作业所采取的数据结构。指令序列文件描述了作业的处理程序。作业文件提供了作业的入口点。

如此构成的作业可以使用数据文件,例如图标库文件,图象文件,字体文件,配色表文件,以及ASCII文本文件。一项交互式作业还可以通过执行输入和/或输出而获得在线的数据。

25 工具4008只有在给定的时间才装入需要的那些资源文件的存储器中。从图形目标描述单元文件,指令序列文件和作业文件当中读出这些资源文件;可变块文件随着对模块加载程序的一次调用被存储在存储器中并且保持锁定状态,一直保持到出现对模块卸载程序的特定调用时为止。

30 参见图3,模块4010例如是电子购物模块是一组资源文件和数据,这其中包括以下内容:

一个单一的作业文件4012;

图形目标描述单元文件4014的一个不确定的编码;

可变块单元文件4016的一个不确定的编码;

指令序列文件4018的一个不确定的编码;以及

适当的数据文件4020,诸如图标库文件,图象文件,字体文件,配色表文件,以及ASCII文本文件。

参见图5,模块4010例如是电子购物模块是一组资源文件和数据,这其中包括以下内容:

一个单一的作业文件4012;

图形目标描述单元文件4014的一个不确定的编码;

可变块单元文件4016的一个不确定的编码;

指令序列文件4018的一个不确定的编码;以及

适当的数据文件4020,诸如图标库文件,图象文件,字体文件,配色表文件,以及ASCII文本文件。

模块4010的概念和下载少量代码的概念是为了便于作业的变化。

它们可以下载到译码器2020的永久性FLASH存储器中作为驻留的软件,或是仅仅在终端用户需要时才通过广播下载到译码器2020的RAM中。

为了从载波信号上下载一个模块4010,首先要下载载波信号上的目录接入口。在目录中直接列出了可以从载波信号上下载模块4010的名称。只要下载了这种目录,就可以下载作业的一或多个模块4010。

在采用MPEG数据流的情况下,目录被转移到一个单一的MPEG表中。进而将一个模块4010转移到一个单一的MPEG表中。如果模块是发送给MPEG调谐器4028的,就采用长MPEG-2格式,具有一个长的字头和一个CRC代码。这种情况同样适用于五种其他的接口(串行接口4030,并行接口4032,调制解调器4034和两个读卡器4036),除非是采用具有短字头且没有CRC的“短”MPEG-2格式。

参见图6,众所周知,MPEG-2比特流包括一个程序入口表(“PAT”)10,它的分组识别符(“PID”)是0。PAT中包含了许多程序的程序图表(“PMA”)12的PID标记。每个PMT中包含这一程序的伴音MPEG表14和电视MPEG表16的数据流中的PID标记。分组的PID是0,它就是程序入口表10,用来为所有的MPEG表提供入口点。

为了从中下载作业,限定了两种新的数据流,并且相关的PMT中也要包含作业MPEG表18(或是其一部分)和数据MPEG表20(或是其一部分)的数据流的PID标记。

参见图7,为了下载一项作业22,将作业划分成各自由一个MPEG表构成的模块24,有些模块是由单个的段18构成的,而其他模块可能有许多个段18。典型的段18具有一个字头,它包含一字节的表识别符(“TID”)28,该段在表中的段号30,表中的段的总数32,以及二字节的TID扩展名34。每段中还包括一个数据部分36和一个CRC38。对于一个特定的模块/表24来说,构成表24的所有段18都具有相同的TID28和相同的TID扩展名34。

10 对于一项特定的作业22来说,构成作业22的所有的表24都具有相同的TID28,但是各自的TID扩展名是不同的。

每一项作业22都有一个单独被用作目录的MPEG表24,在图8中表示了这种表的细节。目录表40包括一个字头26,目录部分42,密钥识别符44,加密的签名46,以及一个CRC38。从上文中可以看出,在目录表40的字头26中的TID28与构成这一作业的其他模块/表24是相同的。然而,目录表具有一个预定的TID扩展名34,也就是零,并且所有其他的模块都具有非零的TID扩展名。在字头中还包括目录表40的版本号48。在目录部分42中包括构成作业22的每个其他模块/表24的模块名50,模块的TID扩展名34,以及这一模块的签名52。目录部分42中还可以包括每个其他模块/

15 表24的模块长度和模块的版本号。

回到图6,在操作中,PAT10,PMT12以及作业和数据流分量18,20是循环发送的,并且根据需要进行更新。发送的每个作业都具有其预定的TID28。在下载一项作业时具有适当的TID并且TID扩展名为零的这种MPEG表下载到接收/译码器2020上。这种表就是所需要的作业的目录表

25 40。然后由接收/译码器2020处理目录中的数据,从中确定构成所需作业的那些模块表的TID扩展名34,然后就可以下载与目录表具有相同TID和一个从目录中确定的TID扩展名的那些所有需要的模块。

接收/译码器2020被用来核查目录表中的任何更新。例如可以通过每隔30秒或是一到五分钟为周期再次下载目录表而完成这种工作,并且

30 将新近下载的目录表的版本号与先前下载的目录表的版本号进行比较。如果新近下载的版本号靠后,就拆除那些有靠后的版本号的与先前的目录表相联系的模块或是任何这种模型,并且下载和安装靠后的模

块。按照另一种方式,采用一种对应着TID,TID扩展名和版本号的屏蔽,按照为作业的TID,TID扩展名为零,并且版本号比当前下载的目录更高的一级而设定的值对输入的比特流进行滤波。这样就能检测出版本的升级,一旦检测到升级,按照上述方式就下载目录并且对作业进行更新。这种滤波方法的进一步细节请参见(代理编号为PC/ASB/19716)的未决专利申请。如果要结束一项作业,就发送具有下一个版本号的一个空的目录,但是在目录中没有列出任何模块。如果接收到这种空的目录,接收/译码器2020的程序就拆除此项作业。

以下要详细说明对作业表签名和加密的作用。

10 如上所述,目录表40中每个模块的入口都包括模块签名。模块签名是用公知的MD5签名产生程序在各个模块表的数据上产生的。

另外,目录表40还包括一个加密的签名46,它是按照下文中参照图9所述的方法来产生的。产生一个64字节的数据块54。第一字节56是零。接着的三个字节58可以包括伪随机数据。下面的八个字节60构成了一个下文中还要进一步解释的作业确认位图。最后四个字节62是保留的。剩下的32字节中包含16字节的签名64,在它的开头紧接着作业确认位图60之后的第一字节后面有一个0到31之间的偏移。在作业确认位图60和签名64之间和/或签名64与保留字节62之间插入伪数据66。签名64是用公知的MD5签名产生程序在目录表40的目录入口42上产生的。然后用公知的加密程序和一个专用的私人密钥对数据块54加密,产生加密的签名和作业确认位图46。将这种数据块46纳入目录表40,并且将用来为数据块加密的私人密钥的1-字节识别符当作密钥识别符44纳入目录表40。

将作业的产生和发送过程总结如下,它包含下列的步骤:

- 产生由许多模块构成的作业;
- 25 · 为作业注明预定的TID28;
- 为模块分配名称和非零的TID扩展名34;
- 将每个模块格式化成一个MPEG表24或是MPEG表中的段18;
- 产生每个模块的MD5签名52;
- 产生目录42;
- 30 · 为目录产生一个MD5签名64;
- 选择一个作业确认比特60;
- 选择一种偏移;

- 产生数据块54;
- 用选定的私人密钥对数据块54加密;
- 用分配的TID28, 零值的TID扩展名, 目录42, 私人密钥的识别符44, 以及加密的签名46产生目录MPEG表40;

5 · 发送目录表40和模块表24或是各个段18。

以下要详细说明在下载作业的过程中在接收/译码器2020上执行的签名的解密操作。参见图10, 接收/译码器2020包括EEPROM68, ROM70和RAM72。EEPROM68包括一个供虚拟计算机使用的保护区74, 只有虚拟计算机(而不是普通的作业)才能在其中写入。保护区74包括一个16或256
10 比特的密钥确认位图76, 一个64比特的作业确认位图78, 和一个32比特的偏移位图80。在一个实施例中, ROM70中包括十六个公用密钥82, 在这种情况下采用一个16-比特的密钥确认位图, 而在另一个有256个公用密钥的实施例中则采用256-比特的密钥确认位图。根据公用密钥在ROM70中的具体位置来进行识别, 或者将它们纳入一个查询表中, 用一种特
15 定的密钥识别符来产生对应的公用密钥。RAM72可以被用来存储临时密钥84。

如上所述, 在下载一项作业时, 首先要下载具有该作业的预定TID和一个零值的TID扩展名的目录表。然后从目录表中提取密钥识别符44, 并且在受保护的存储器74中核查密钥确认位图76中的比特是不是
20 按照提取的密钥识别符44来设定的。如果不是, 就中止进一步下载作业。然而, 如果设定了适当的密钥, 就按照提取的密钥识别符44从ROM70中选择一个公用密钥82。然后用选定的公用密钥和公知的解密程序对目录表40中加密的数据块46执行解密, 产生一个数据块54。然后从数据块54中提取作业确认位图60, 并且与存储在受保护的存储器74中的作业
25 确认位图78执行AND运算。如果AND运算的结果是零, 就中止进一步下载作业。然而, 如果AND运算的结果不是零, 就核查受保护的存储器74中的偏移位图所包含的偏移, 或者是在设置了一个以上偏移比特的情况下依次核查每一个偏移比特, 并且从作业确认位图60之后的第一字节开始用查出的偏移开始从解密的数据块54中提取十六字节的数据, 将这十
30 六字节当作用目录表40发送的签名。利用公知的MD5程序计算出目录表40的目录42中的入口的签名, 并且将这一签名与从数据块54中提取的签名相比较。如果针对每一个查出的偏移的这两个签名彼此不符, 就中止

进一步下载作业。然而,如果签名相符,就可以下载目录42中规定的模块。如上所述,为了下载一个特定的模块,从目录42中获得该模块的TID扩展名,并且下载与目录表具有相同的TID并且带有获得的TID扩展名的MPEG表24或是段18。只要是已经下载了模块MPEG表,接收/译码器2020就能用公知的MD5程序计算出下载的表的签名,然后将计算出的签名与从目录入口中获得的签名相比较。如果签名相符,就接收这一模块,如果彼此不符,就拒绝这一模块。

这样就能用上述的方法下载作业中的所有模块,并且在接收/译码器2020上运行这种作业。

以上所述的下载操作的特征是一般的使用方式,而下文要说明在设置接收/译码器2020以及改变其设置时使用的某些特征。

接收/译码器2020的程序可以改变受保护的存储区74,但是仅限于采用一个特定的密钥识别符例如是密钥15的一项已经下载的作业,并且有一个特定的偏移,例如是从作业确认位图60之后的第一字节开始有字节的偏移。如果已经使用着同一个公用密钥的两个操作员决定要使用不同的公用密钥,或者是私人密钥的内容已经泄漏了,也可能不需要改变受保护的存储区74,在这种情况下可以在密钥确认位图76中给对应的公用密钥加上无效的标记。

接收/译码器2020可以让某一个密钥例如密钥15永远有效,在这种情况下,在密钥确认位图76中不需要这一密钥的比特。因而可以将这个比特用于其他用途。具体地说,已经被授权使用密钥15的一项作业可以将这一特定的比特设定为1,在这种情况下,接收/译码器2020的程序允许在RAM72中装入一个临时密钥84,但是仅仅能通过串行接口4030,并行接口4032或是两个读卡器4036其中的一个输入临时密钥。接收/译码器2020的制造商可以利用这种便利来使用一项作业,将一个临时密钥装入接收/译码器2020,以便对作业进行测试。

上述的加密和签名方式提供了许多重要的特征:

- 只有当存储在接收/译码器2020的存储器中的适当的公用密钥与下载的目录表中的密钥识别符相对应时才能下载一项作业;

- 除了一个密钥之外,只有当接收/译码器2020的存储器中的密钥确认位图76被设定在允许使用该密钥时才能下载一项作业;

· 只有当存储在接收/译码器2020的存储器内的偏移位图80中的一个设定的比特与产生目录表时使用的偏移相对应时才能下载一项作业;

· 只有当接收/译码器2020的存储器中的作业确认位图78被正确地设置在允许下载作业的状态时才能下载一项作业;

5 · 只有为目录表最初产生的签名在此后没有受到破坏的情况下才能下载一项作业;

· 只有为各个模块表最初产生的签名在此后没有受到破坏的情况下才能下载一项作业的每一个模块;

· 即使作业是由若干个MPEG表构成的,在准备下载一项作业时仍然
10 仅需要一次加密操作,并且在接收/译码器2020上仅仅需要一次解密操作就能够下载完整的作业;

· 可以采用多个密钥,从而使不同的业务供应商可以采用不同的私人密钥;

· 制造商可以使用临时密钥进行测试。

15 需要指出的是,上文中对本发明的描述仅仅是一些例子,在本发明的范围内还可以对其细节进行修改。

在说明书,(适当的)权利要求书和附图中揭示的每一个特征都是可以独立存在的,或是采用任何适当的组合。

在上述的最佳实施例中已经用计算机软件实现了本发明的某些特
20 征。然而,本领域的技术人员显然都明白这些特征是可以硬件来实现的。另外还很容易理解,由硬件,计算机软件等等执行的功能都是用电和类似的信号来执行的。

本文与我们于同日提出的以下各项未决专利申请是相互参照的,这些申请的名称是:Signal Generation and Broadcasting(信号的发生和
25 广播)(代理编号为PC/ASB/19707),Smartcard for use with a Receiver of Encrypted Broadcast Signals,and Receiver(用于加密广播信号接收机的智能卡和接收机)(代理编号为PC/ASB/19708),Broadcast and Reception System and Conditional Access System therefor(广播和接收系统及其条件存取系统)(代理编号为PC/ASB/19710),Downloading
30 a Computer File from a Transmitter via a Receiver/Decoder to a Computer(通过接收/译码器从发射机到计算机下载计算机文件)(代理编号为PC/ASB/19711),Transmission and Reception of Television

Programmes and Other Data(电视节目和其它数据的传输和接收)(代理编号为PC/ASB/19712), Downloading Data(下载数据)(代理编号为PC/ASB/19713), Computer Memory Organisation(计算机存储结构)(代理编号为PC/ASB/19714), Television or Radio Control System
 5 Development(电视或无线电控制系统体系)(代理编号为PC/ASB/19715), Extracting Data Sections from a Transmitted Data Stream(从发送数据流中提取数据段)(代理编号为PC/ASB/19716), Access Control System(存取控制系统)(代理编号为PC/ASB/19717), Data Processing System(数据处理系统)(代理编号为
 10 PC/ASB/19718), 以及 Broadcast and Reception System, and Receiver/Decoder and Remote Contrller therefor(广播和接收系统及其接收/译码器和遥控器)(代理编号为PC/ASB/19720)。这些文献所公开的内容都可供本文参考。在申请的目录中包括了本项申请。

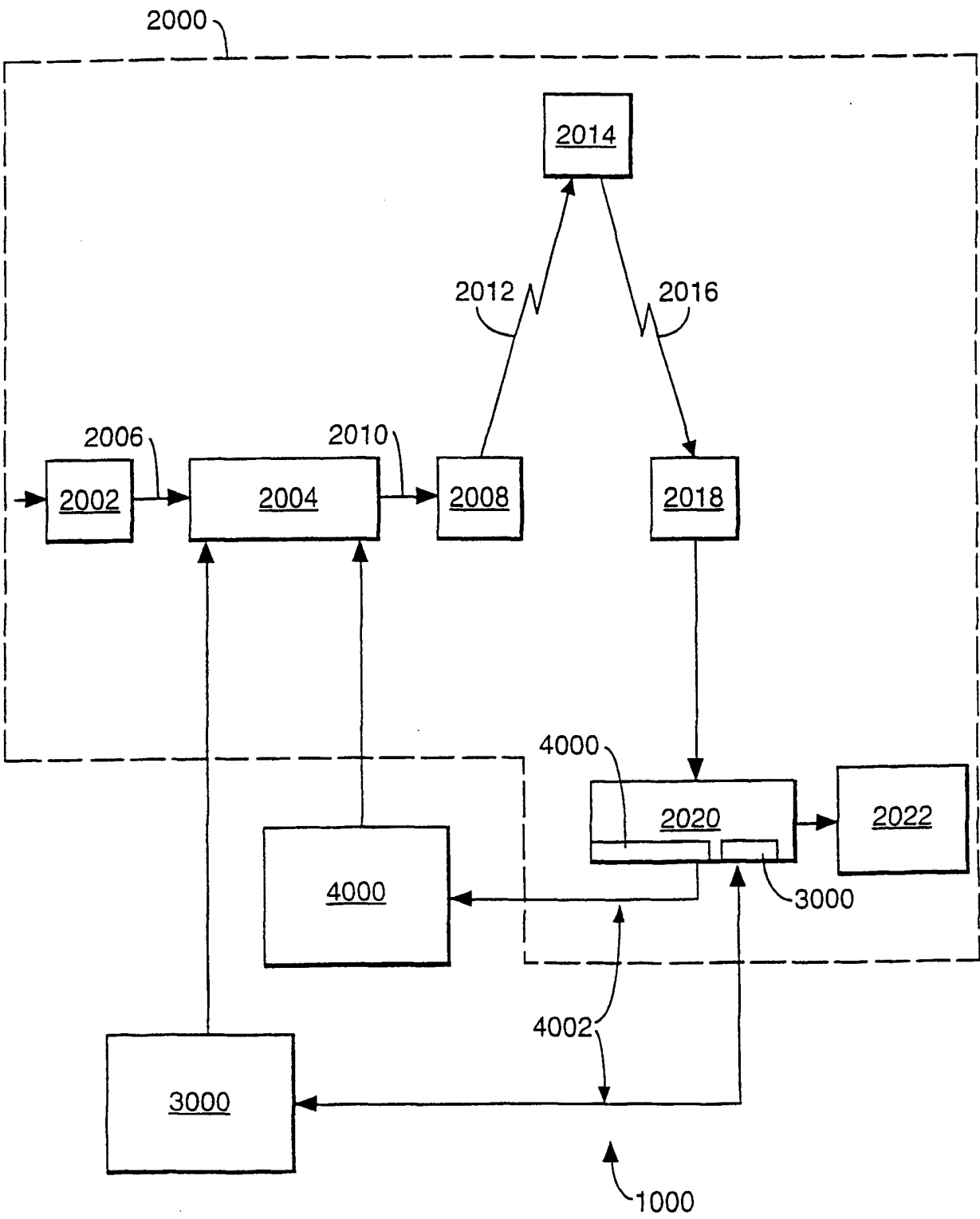


图 1

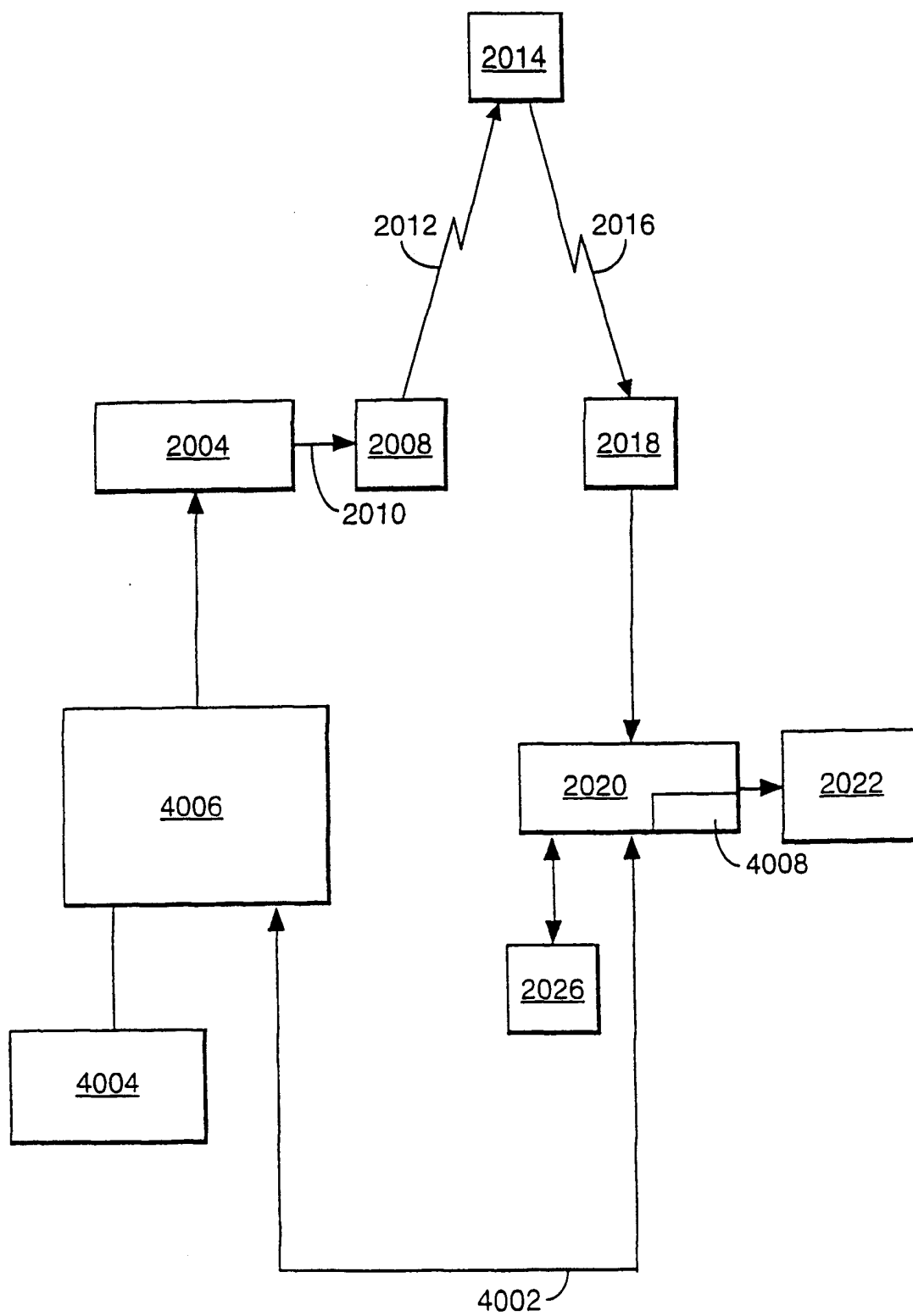


图 2

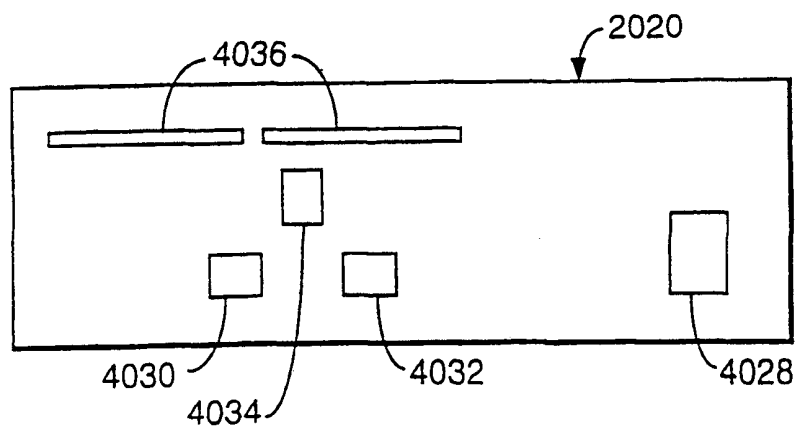


图 3

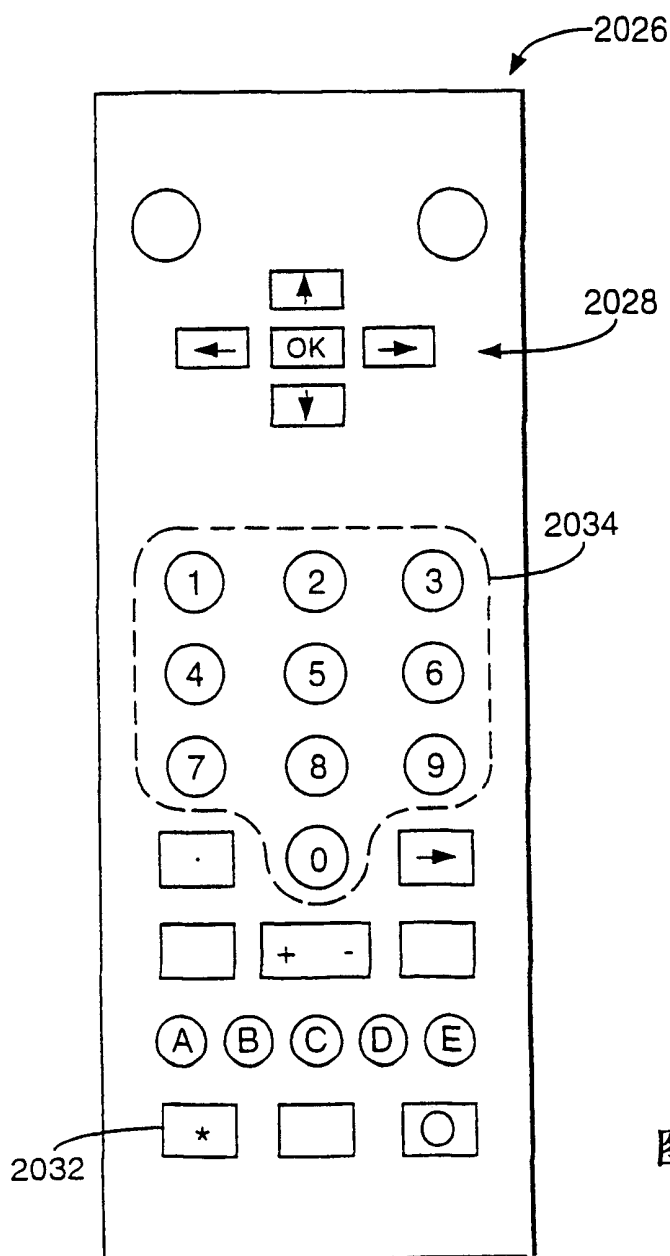


图 4

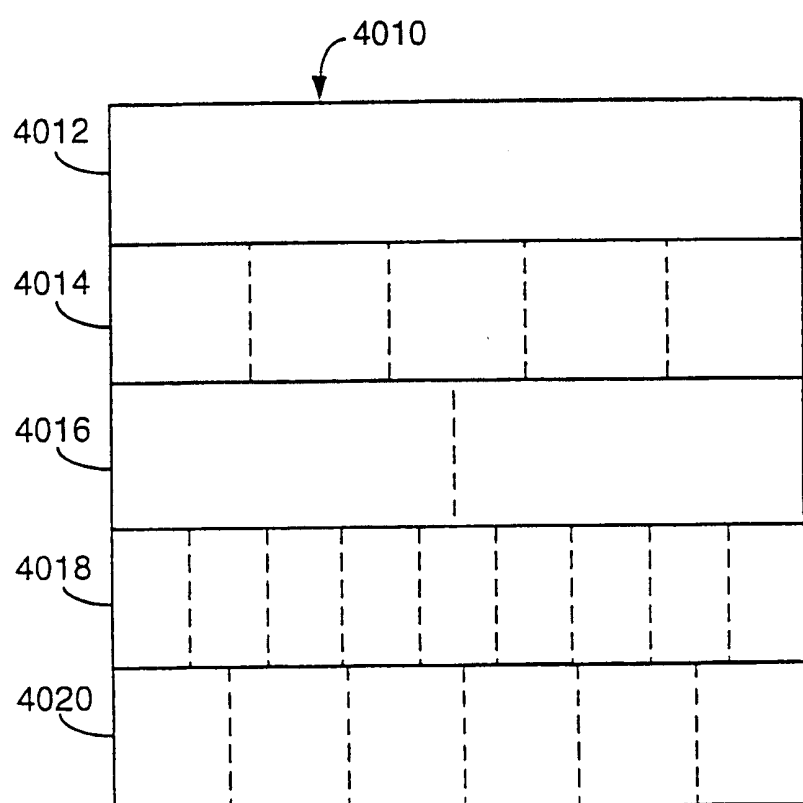


图 5

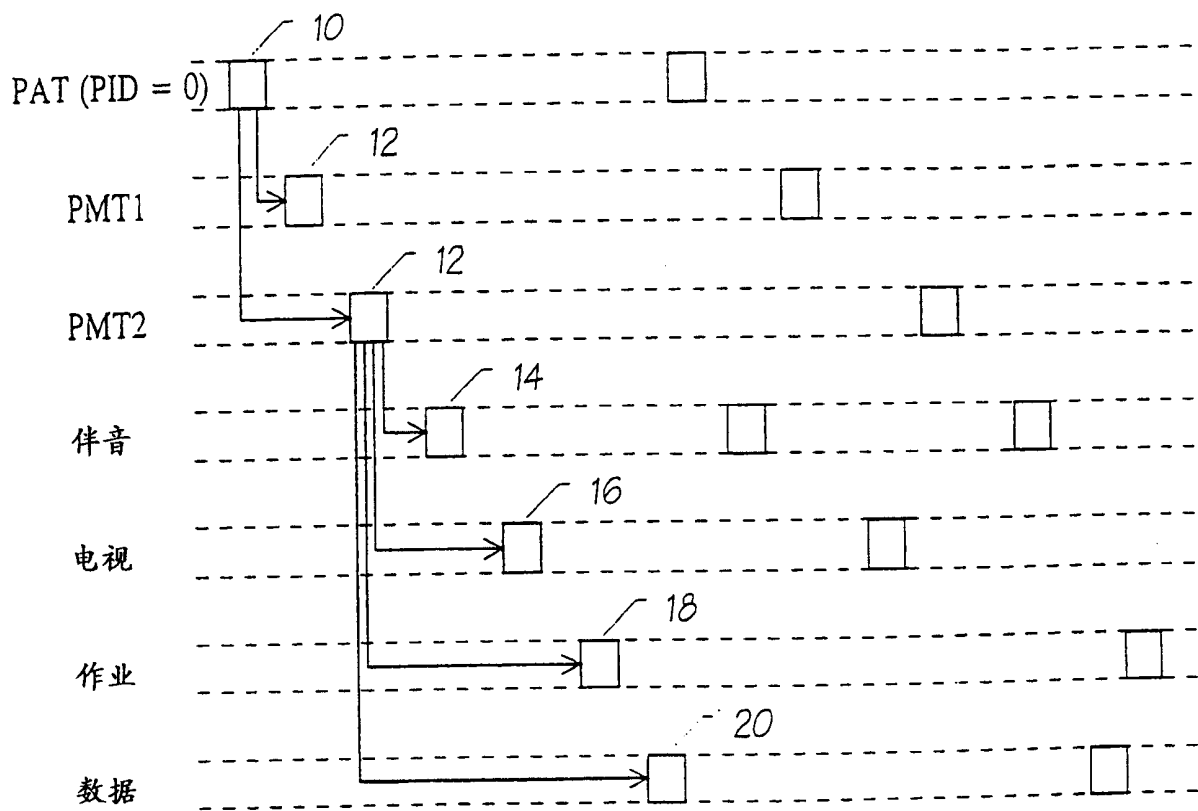


图 6

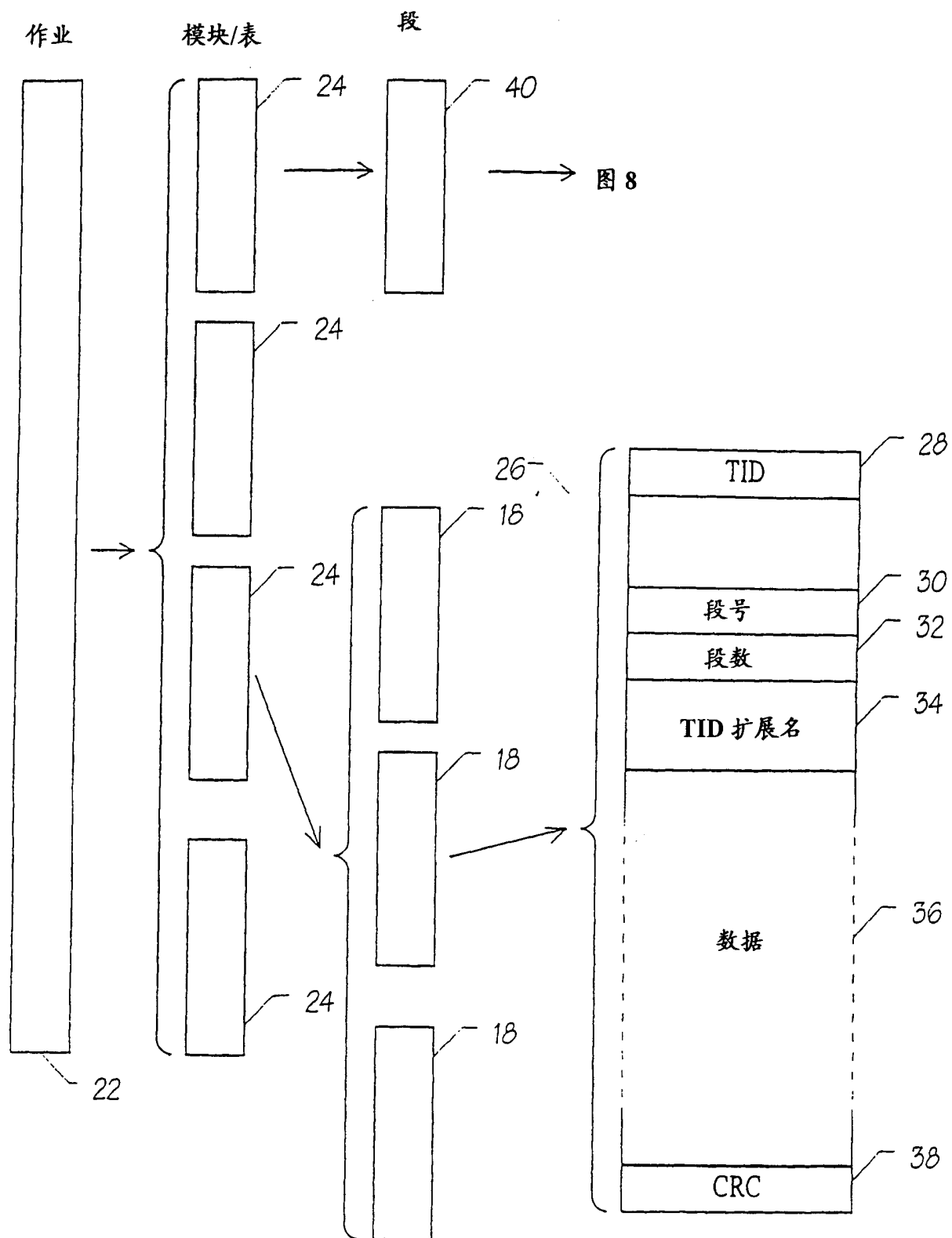


图 7

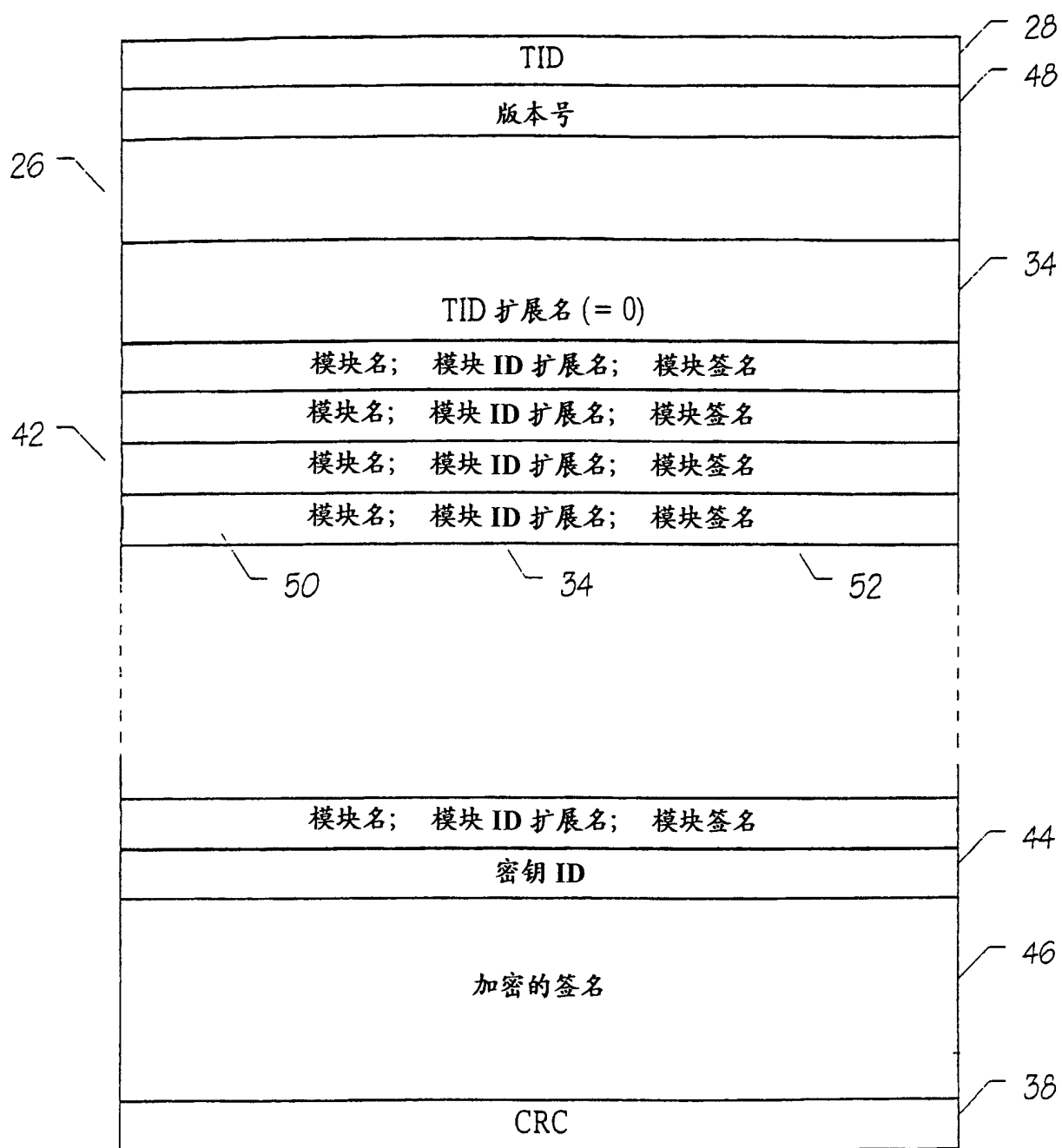


图 8

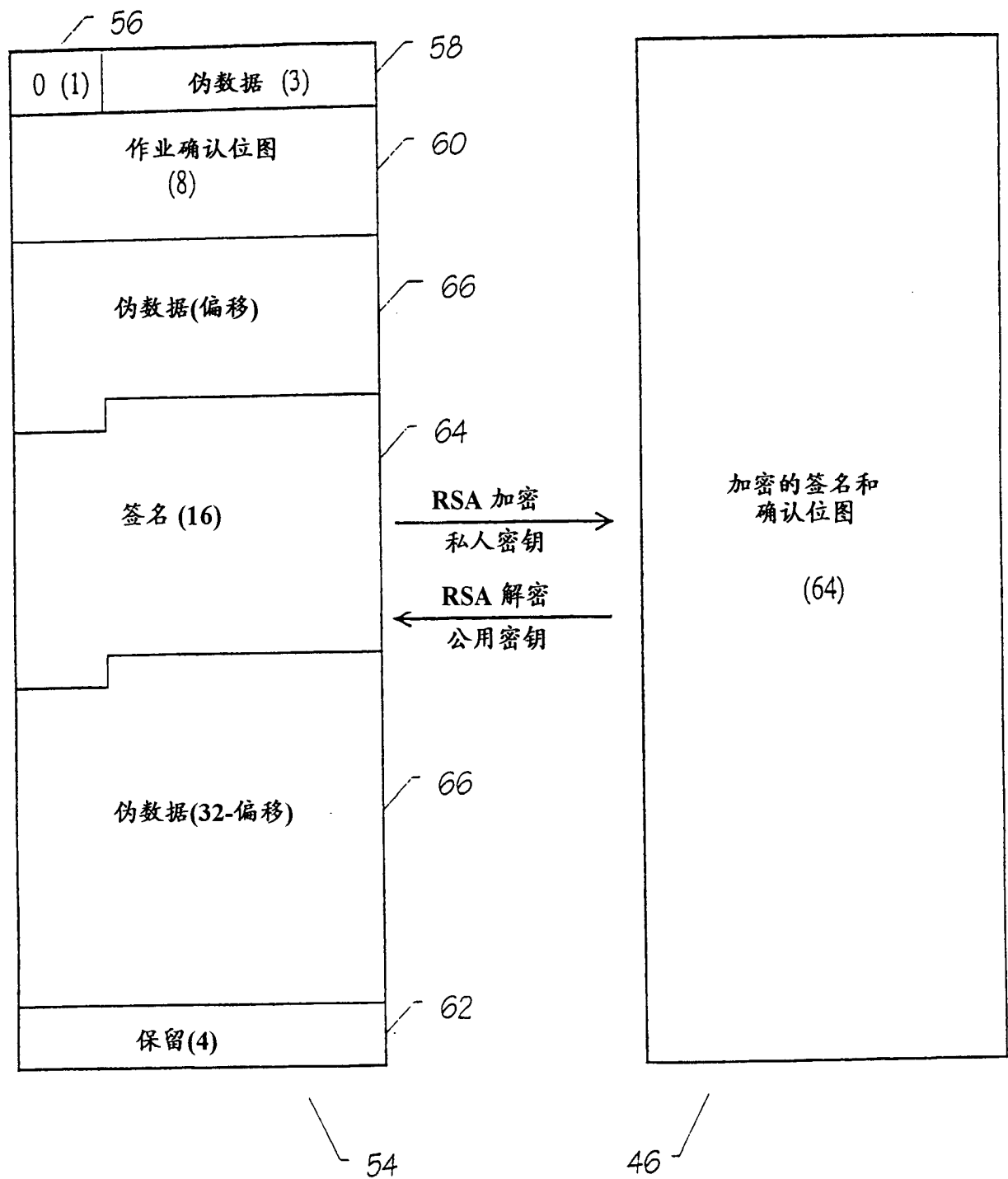


图 9

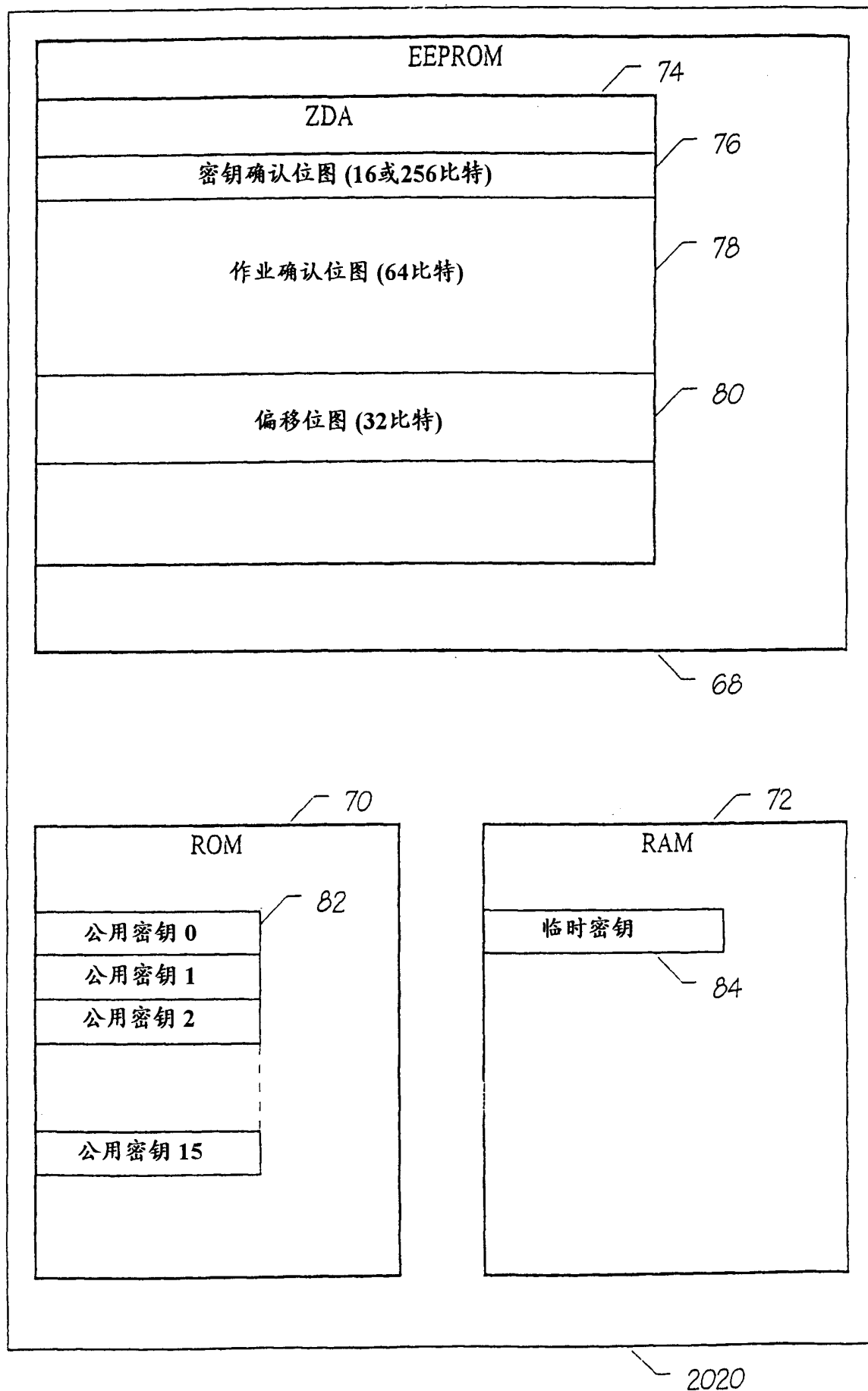


图 10