(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 1735194 B
(45)授权公告日 2011.05.25

(21)申请号 200510091120.8

(22)申请日 2005.08.08

(30)优先权数据
04300532.1 2004.08.11 EP

(73)专利权人 汤姆森许可贸易公司
地址 法国布洛里

(72)发明人 埃里克·迪尔
让－皮埃尔·安德烈奥斯
路易斯－格扎维埃·卡博内尔
阿兰·迪朗

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 罗松梅

(51)Int.Cl.
H04N 21/4623(2011.01)

(56)对比文件
WO 03/075570 A1,2003.09.12, 全文.

审查员 李熙

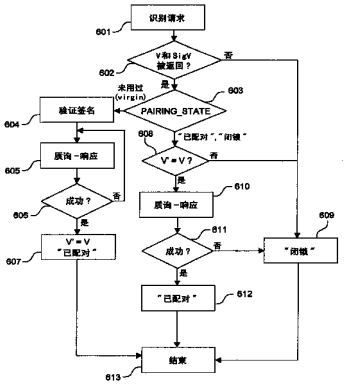
权利要求书 1 页 说明书 7 页 附图 5 页

(54)发明名称

用于设备配对的装置和方法

(57)摘要

本发明涉及将从设备与主设备配对，如条件访问系统中的解码器。提出了用于存储指示解码器将作为主解码器还是从解码器的设备状态的安全模块。还提出了在条件访问系统中向设备提供安全模块上所存储的设备状态的方法。检测安全模块是否正与所述设备相连，并将设备状态从安全模块传送到所述设备。还提出了将从设备与主设备配对的方法。从设备要求主设备识别其自身，主设备返回标识，如果从设备还未与主设备配对，则检查主设备的身份，如果验证了身份，则与主设备配对。还提出了与第二、主设备配对的第一、从设备。第一设备包括：接口，向主设备发送识别命令以及从主设备接收识别消息；以及处理器，检查第二设备的身份并将第一设备与第二设备配对。



CN 1735194 B

1. 一种用于使第一设备 (41) 与第二设备 (42) 配对的安全模块 (30,43,44),所述安全模块 (30,43,44) 具有处理器 (31) 和存储器 (32),所述存储器 (32) 存储了用于指示所述第一设备 (41) 将作为主设备还是从设备的可变的设备状态 (34),所述安全模块 (30,43,44) 的特征在于 :与所述第一设备 (41) 相连接,所述处理器 (31) 接收和处理专用权利管理消息 (EMM),并根据所述专用权利管理消息中包含的指令来改变所述设备状态 (34)。

2. 一种用于使第一设备 (41) 与第二设备 (42) 配对的安全模块 (30,43,44),所述安全模块 (30,43,44) 具有处理器 (31) 和存储器 (32),所述存储器 (32) 存储了用于指示所述第一设备 (41) 将作为主设备还是从设备的可变的设备状态 (34),所述安全模块 (30,43,44) 的特征在于 :与所述第一设备 (41) 相连接,所述处理器 (31) 在使用预定时间之后如果未接收和处理专用权利管理消息 (EMM),则改变所述设备状态 (34)。

用于设备配对的装置和方法

技术领域

[0001] 本发明通常涉及设备的配对，更具体地，涉及在其中向终端提供对内容的条件访问的系统中对设备的配对。有利地，本发明应用于付费电视系统中的解码器的配对。

背景技术

[0002] 这里所使用的、将用作终端的典型实现的术语“解码器”可以是指与接收机物理上分离的解码器；组合的接收机和解码器，例如在机顶盒（解码器）中；或者具有附加功能的解码器，例如记录设备、显示器或万维网浏览器。还将假定条件访问系统的一般概念是公知的，由此，将不需要在下面对其进一步进行描述，其对于本发明的理解而言是不必要的。

[0003] 在该描述中将使用的诸如付费电视等条件访问系统已经在许多国家赢得了广泛的接受。许多家庭具有解码器，且大部分家庭具有多于一台的电视机。当前，利用一个解码器，订户经常仅可以在一台电视机上访问付费电视节目。已经提出了两种主要的解决方案来解决该问题。

[0004] 第一种方案是在家庭内部分配所接收到的内容。现有技术的当前状态是使用无线模拟传输。不利地，视频质量较差，且仅能够在所有相连的电视机上观看同一节目。

[0005] 第二种方案是简单地在家庭内提供多个解码器。许多广播商向已经订阅的家庭提供第二次较为便宜的订阅。然而，由于广播商害怕邻居或亲戚将“共享”两次订阅以为其订阅获得平均起来较低的价格，因此广播商要求两个解码器应该配对。图 1 示出了基本的现有技术概念。两个解码器 11、12 通过双向数字连接 13 相连。一个解码器 11 充当主解码器而另一解码器 12 充当从解码器。主解码器 11 总是能够访问通过订阅已授权的节目，而从解码器 12 仅当其与主解码器 11 相连时，能够访问通过订阅已授权的节目。

[0006] 存在多种方法来验证两个解码器被一起使用。

[0007] 由一些条件访问 (CA) 提供商提出的一种方案是使用专用权利管理消息 (EMM)。除了指向其的 EMM 之外，主解码器 11 还接收从解码器 12 所需的 EMM，并且通过数字连接 13 将后一个 EMM 发送到从解码器 12。尽管存在另一更为复杂的方案，但是将会意识到，即使这个相对简单的方案暗示着对 CA 系统的较大修改和广播商的事务部门的较强关联，并且由于这些理由，其对于水平市场而言非常不切实际（如果并非不可用）。

[0008] WO 2004/019296 的“Secure Electric Anti-Theft Device, Anti-Theft System Comprising One Such Device and Method ofMatching Electric Devices”描述了一种确保多个网络设备之间的配对的方法。为了全面操作，设备需要存在在初始化期间对其留下印记的安全装置。尽管该方法可以用于对解码器进行配对，但是将意味着要对主解码器和从解码器进行区分，这对于制造商、零售商和售后人员而言是一个问题。

[0009] WO 03/10547 的“Method, System and Terminal for ReceivingContent with Authorized Access”描述了确保在多个联网设备之间进行配对的另一方法。仅当其已被配对时，辅助设备（即从设备）能够访问内容，并且能够与最初已经与其配对的预定主终端（即，主设备）进行通信。在一些情形下，该方法还受到以下限制：由于例如必须将从解码器

与特定主解码器进行配对以使其工作，因此缺乏特定的灵活性。如前所述，这对于制造商、零售商和售后人员而言存在问题。

发明内容

[0010] 因此，能够意识到，需要一种灵活的方案，能够以受控和可靠的方式将解码器变为主解码器或从解码器。优选地，该变换应该发生在订户的家中（或同等场所）。另外，该方案还应该确保主解码器和从解码器之间的配对。本发明提出了一种这样的解决方案。

[0011] 在第一方案中，本发明涉及一种用于使第一设备与第二设备配对的安全模块，所述安全模块具有处理器和存储器，所述存储器存储了用于指示所述第一设备将作为主设备还是从设备的可变的设备状态，所述安全模块的特征在于：与所述第一设备相连接，所述处理器接收和处理专用权利管理消息，并根据所述专用权利管理消息中包含的指令来改变所述设备状态。

[0012] 因此，所述安全模块能够提供设备状态，并且由于设备状态可以改变，改善了使用的灵活性。

[0013] 在优选实施例中，所述设备状态是可变的，并且可以在接收和处理专用权利管理消息（EMM）之后发生改变。

[0014] 因此，可以通过广播网络来改变设备状态，这意味着可以远程地改变设备状态。

[0015] 在可选的优选实施例中，新安全模块的设备状态是可变的，并且如果所述安全模块在此之前未接收到专用权利管理消息（EMM），则在使用预定时间之后发生改变。

[0016] 因此，在该改变可能在广播网络上被禁用的同时，所述设备状态可以自动发生改变，这意味着所述设备状态可以自动地或远程地发生改变。

[0017] 在第二方案中，本发明涉及一种在条件访问系统中向设备提供设备状态的方法，所述设备状态存储在安全模块上，并且用于通知设备其应该充当主设备还是从设备，检测安全模块是否正与所述设备相连；以及将设备状态从安全模块传送到所述设备。

[0018] 该方法提出了一种向设备提供设备状态的简单方式。

[0019] 在优选实施例中，为了传送设备状态，所述设备向安全模块发送识别数据和随机数。安全模块利用所述识别数据和所存储的主密钥来计算导出密钥，以及根据导出密钥、随机数和设备状态来计算散列值，并且将设备状态和散列值从安全模块发送到所述设备。所述设备利用散列值、导出密钥、随机数来验证所述设备状态。

[0020] 因此，将设备状态安全地从安全模块传送到所述设备。

[0021] 在优选实施例中，所述设备还存储了设备状态。

[0022] 在第三方案中，本发明涉及一种将从设备与主设备配对的方法。由从设备发送用于要求主设备识别主设备自身的命令；从主设备向从设备发送识别了主设备的消息；所述方法的特征在于：确定从设备是否已与主设备配对，如果确定了从设备还未与主设备配对，则由从设备利用所接收到的消息来检查主设备的身份；并且如果验证了所述身份，则将从设备与主设备配对。

[0023] 因此，本发明的成功执行使得从设备与主设备配对。

[0024] 在另一优选实施例中，与主设备配对的从设备验证第二设备的身份是否等于先前所存储的第二设备的身份；以及，如果该验证成功，则将从设备与主设备配对。

[0025] 在另一优选实施例中，如果需要，通过运行至少一个质询－响应协议，在使设备配对之前要求每一个协议均获成功，进一步增强了安全性。

[0026] 在第四方案中，本发明涉及一种用于与第二设备配对的第一设备。所述第一设备充当从设备且所述第二设备充当主设备。所述第一设备包括接口，用于发送用于要求第二设备识别其自身的命令；以及从第二设备中接收识别了第二设备的消息。所述第一设备还包括：接口，用于：发送用于要求第二设备识别第二设备自身的命令；以及从第二设备中接收识别了第二设备的消息；所述第一设备的特征在于其还包括：处理器，如果第一设备还未与主设备配对，则所述处理器检查第二设备的身份；并且如果已验证了身份，则将第一设备与第二设备配对。

[0027] 因此，提出了一种使用根据本发明的方法来与另一设备相配对的设备。

附图说明

[0028] 现在将参考附图，纯粹作为示例来描述本发明的优选特征，其中：

[0029] 图 1 示出了根据现有技术的解码器的配对的基本概念；

[0030] 图 2 示出了根据本发明的解码器的结构；

[0031] 图 3 示出了典型的安全模块；

[0032] 图 4 示出了根据本发明的配对后的解码器；

[0033] 图 5 示出了涉及根据本发明的解码器和相关安全模块的状态验证的方法；

[0034] 图 6 示出了根据本发明在两个解码器之间进行配对的方法；以及

[0035] 图 7 示出了根据现有技术的典型质询－响应协议。

具体实施方式

[0036] 图 2 是根据本发明的解码器 20 的优选实施例的结构的简化图。解码器 20 包括中央处理单元 (CPU)24、视频单元 23、优选为符合 ISO-7816 的智能卡接口形式的安全模块接口 26、串行接口 27 和存储器 25（优选地，以安全、非易失性存储器 25a、非易失性存储器 25b 和随机存取存储器 (RAM)25c 的形式）。视频单元 23 通过输入连接 21 来接收视频流，提取权利控制消息 (ECM) 和权利管理消息 (EMM)，并将其传递给 CPU 24 以将其经由安全模块接口 26 转发到安全模块（图中未示出）。如果已由安全模块授权，则视频单元 23 还对视频流进行解扰并在连接 22 上进行输出，所述连接 22 通常与显示器（未示出）相连。安全模块接口 26 实现了与安全模块的物理接口和电接口。RS 232 串行接口 27 尤其允许通过数字连接 13 与另一解码器的连接，如先前参考图 1 所讨论的，例如，这可以采用有线连接或蓝牙® 连接的形式。

[0037] 图 3 是根据本发明的典型安全模块 30 的简化图，如图 4 中的安全模块 43、44。安全模块 30 包括中央处理单元 (CPU)31、存储器 32 和通信单元 33。其是符合 ISO-7816 的通信单元 33，与主机解码器（图 2 中的 20）的安全模块接口（图 2 中的 26）进行通信。假定 CPU 31 的存储器 32 和 RAM（未示出）是安全的，即，难以或甚至不可能由攻击者访问。安全模块 30 可以诸如为智能卡或 PC 卡，这均为本领域内所公知的。

[0038] 为了执行如以下所述的根据本发明的配对方法，在优选实施例中，安全模块和解码器存储特定数据且能够执行如现在将描述的特定功能。

[0039] 安全模块 30 的存储器 32 最好同时存储以下信息：

[0040] • 主对称密钥 MK；以及

[0041] • 状态 CAM_STATE 34，可以取两个逻辑值：“主”或“从”；以及

[0042] • 用于计算和验证的临时变量。

[0043] 安全模块 30 的 CPU 31 用于执行：

[0044] • 密钥推导算法 KeyDevAlgo，例如高级加密标准 (AES) 算法，根据诸如主密钥 MK 和标识值来推导密钥参见 FIPS 公布 197：“Advanced Encryption Standard”；国家标准和技术学会，2001；以及

[0045] • 消息认证码 (MAC) 产生算法 MACGenerate，例如 HMAC-SHA1 参见 FIPS 公布 198：“The Keyed-Hash Message Authentication Code(HMAC)”；国家标准和技术学会，2001，用于计算散列值。

[0046] 优选地，解码器 20 不必同时将以下内容存储在由其括号内的参考数字表示的存储器中（安全非易失性存储器 25a、非易失性存储器 25b 和 RAM 25c）：

[0047] • 识别数据 ID(25b)；

[0048] • 导出对称密钥 (DK)，满足等式

[0049] DK = KeyDevAlgo{MK}(ID)(25c)；

[0050] • 状态 decoder_STATE，可以取两个逻辑值：“主”或“从”(25a)；

[0051] • 超大数 S，对于每一个解码器是唯一的 (25a)；

[0052] • 公开号 n，对于每个型号的解码器、制造商或系统均是相等的，其中 n 是两个超大、私密、质数的乘积 (25b)；

[0053] • 数值 V，从而使$S = \sqrt{V} \bmod n$ (25b)；

[0054] • V 的签名 SigV，由广播商签名 (25b)；

[0055] • 广播商的公用密钥 K_{pub_sig}，用于校验该签名 (25a)；

[0056] •状态 PAIRING_STATE 28，能够取三种逻辑值：“未用过”、“配对”或“闭锁”(25a)；

[0057] • 随机数 R(25c)；

[0058] • 用于计算和验证的临时变量 (25c)；以及

[0059] • 数 V’，稍后将进一步描述其 (25c)。

[0060] 解码器 20 的 CPU 24 能够执行：

[0061] • 消息认证码 (MAC) 验证算法 MACVerify；以及

[0062] • 产生随机数，实际上是伪随机数 (PRNG)。

[0063] 图 4 示出了根据本发明优选实施例的配对的解码器。在条件接入系统 40 中，解码器 41、42 配备有可拆卸安全模块 43、44（还被称为 CA 模块），或者具有智能卡的形式，或者是 PCMCIA（个人计算机存储卡国际联合会）形式的代管模块（还被称为 PC 卡）。尤其地，安全模块 43、44 处理权利管理消息 (EMM) 和权利控制消息 (ECM)，并且由解码器使用其中的信息对已加扰传输进行解密。

[0064] 根据本发明，新制造的相同型号的解码器在许多方面是相同的，特别是尽管其既非主解码器也非从解码器，但是其能够变为任一个（或者甚至是两者，如以下将会看到的，尽管并非同时，但是至少并未处于单一解码器对内）。

[0065] 当第一次安装解码器 41、42 时，解码器询问其安全模块 43、44 其是应该充当主解

码器还是从解码器，而安全模块 43、44 返回其已经存储的 CAM_STATE 45、46。如果安全模块 43、44 回答为主解码器，则解码器 41、42 将充当主解码器 41。相反，如果安全模块 43、44 回答为从解码器，则解码器 41、42 将充当从解码器 42。如果其安全模块 43 返回了适当的解扰（还被称为解密）密钥，主解码器 41 对内容进行解扰（还被称为解密），针对与订阅相对应的服务（包括节目）无差错地进行此操作。仅当两个解码器 41、42 经由数字连接 13 相连且适当配对时，从解码器 42 利用由其安全模块 44 提供的解扰密钥对内容进行解扰。

[0066] 除了在安装时向其安全模块询问有关动作之外，每一次当解码器检测到安全模块已经插入到其中（或者与其相连）时，该解码器也询问相同的内容，并且还可以在随机时间或间隔处这样做，优选地，利用以下方法，如图 5 所示。然而，应该注意，还可以使安全模块直接向解码器发送动作信息。

[0067] 根据本发明，当解码器向其安全模块询问相关动作时，可以使用两种方法。最简单的方法是通过简单的命令进行请求。然而，该方法具有以下缺陷：可以诸如由黑客容易地再现该回答。一种优选的且更安全的方法是根据解码器和安全模块之间的会话密钥来建立安全信道。对于安全信道所需的信息，所有解码器可以共享相同的全局密钥，尽管这使得系统易受逆向工程的损坏。优选地，每一个解码器具有其自身的密钥，则极大地降低了该易损性。

[0068] 在步骤 51 中，解码器使用其 PRNG 来获取随机（实际上为伪随机）值 R。解码器将该随机值 R 与其 ID 一起通过安全信道、作为消息 52 发送到安全模块。在步骤 53，安全模块利用 KeyDevAlgo，根据接收到的 ID 和 MK 来计算 DK，并且在步骤 54，利用 MACGenerate，根据其状态 CAM_STATE、推导的密钥 DK 和随机 R 来计算散列值 H。然后，该安全模块将其状态 CAM_STATE 和散列值 H 作为消息 55 发送到解码器。最终，在步骤 56，解码器使用 MACVerify，利用数据 H、R 和 DK 来验证 CAM_STATE。如果验证了 CAM_STATE，则 decoder_STATE 取值 CAM_STATE，否则 decoder_STATE 保持不变。按照该方式，解码器可以根据需要在主解码器和从解码器之间改变。然而，如果解码器并未从安全模块接收到回答，或者如果其检测到其不再与安全模块相连，则优选地，将主解码器自动地改变为“从解码器”，优选为立即改变，但是也能够在与安全模块联系的一定数量的不成功的尝试之后或特定时间之后这样做。

[0069] 安全模块可能已经按照不同的方式接收到针对该回答的信息。

[0070] 一种方案是 CA 提供商提供两种类型的安全模块，主卡和从卡，其中主卡总是返回回答“主”，而从卡总是返回回答“从”。

[0071] 另一优选的方案是 CA 提供商提供一种唯一类型的安全模块，默认为返回一种类型的回答，即或者“从”或者“主”。然后，通过传送专用 EMM，广播商可以改变该回答。可以采用更为复杂的策略，例如使安全模块以回答“主”开始，并且在使用了预定时间之后，例如两星期，如果在此之前其没有接收到告诉其保持为“主”的 EMM，则将该回答改变为“从”。详细说明后一个策略。

[0072] 图 6 示出了用于验证从解码器位于与其配对的主解码器的面前的方法。无论何时当解码器变为从解码器时，以及 / 或者在随机时间处，可以执行该方法。在步骤 601 处，从解码器 42 通过链路 13 来发送命令，要求另一解码器识别自己。如果解码器存在且其 decoder_STATE 是主解码器，则其返回 V 和 SigV，否则其不返回任何值。在步骤 602，验证是否存在响应。如果未返回任何值，则将从解码器的 PAIRING_STATE 设置为“闭锁”，之后该方法结

束，但是如果给出了响应，则在步骤603，校验从解码器的PAIRING_STATE，并且存在三种可能性：

[0073] • 从解码器的PAIRING_STATE是“未用过”（即，从未配对过）：

[0074] 从解码器的CPU使用公用密钥K_{pub_sig}，利用签名SigV来校验V。如果在步骤604中成功地验证了签名，则在步骤605，开始与主解码器的L个连续质询－响应协议，有利地，所述主解码器为本领域内所公知的零知识型的（诸如Fiat-Shamir)（在图7中示出了其典型实施例），其中L的典型值在10和20之间，包含这两个值。如果所有质询－响应协议成功，则在步骤607，CPU将V存储为V’，将其PAIRING_STATE设置为“已配对”，且解码器变为完全操作从解码器，之后，在步骤613该方法结束。然而，一旦质询－响应协议失败，则解码器不会改变其PAIRING_STATE，并保持为不能够对内容进行解扰。然后，立即或者在预定或随机时间之后，解码器重新开始图6中所示的方法，并且要求解码器重新开始所述质询－响应协议的序列。

[0075] • 从解码器的PAIRING_STATE是“已配对”（即，其已经成功配对）或“闭锁”（即，至少部分的解码器功能是禁用的）：

[0076] 在步骤608，其CPU验证所接收到的V等于所存储的V’。如果情况并非如此（例如，情况为用户尝试与除了与其配对的解码器之外的其他解码器关联），则在步骤609，将PAIRING_STATE设置为“闭锁”，并且该解码器变得（或者取决于情况，保持为）不能够对内容进行解扰。然而，如果V和V’相匹配，则在步骤610，该CPU开始质询－响应协议的序列，并且如果所有协议均成功，则在步骤612，从解码器的PAIRING_STATE变为“已配对”，并且其变为完全操作从解码器，之后，在步骤613处，该方法结束。如果另一方面，协议失败，则在步骤609，从解码器的PAIRING_STATE变为（或保持为）“闭锁”，并且解码器变得（或保持为）不能够对内容进行解扰，之后，在步骤613处，该方法结束。

[0077] 主解码器可以一直对内容进行解扰，但是仅当从解码器正确地配对时，其才可以这样做；如果例如，其并未与主解码器相连，则解扰变为不可能。还应该注意，如果其decoder_STATE是“主”，则解码器仅回答质询和其他消息、以及由从解码器发送来的请求；从解码器不作任何回答。

[0078] 图7示出了根据现有结束在两个解码器（图4中的41和42）之间的典型质询－响应协议。在该描述中，术语主解码器和从解码器用作示例，这是事情的常态。在步骤71处，从解码器发起协议，并通过连接13发送消息72，向主解码器要求委托。在步骤73，主解码器选择现在的r，并且计算委托$G = r^2$，其在消息74中发送到从解码器。在步骤75，从解码器利用PNRG选择随机质询b，并且在消息76中将其发送到主解码器。然后，在步骤77，主解码器计算响应$A = rS^b$，其作为消息78被返回到从解码器。在步骤79，从解码器通过检查A^2实际上等于GV^b来验证响应。如果验证成功，则质询－响应协议成功；否则其不成功。

[0079] 因此，可以意识到，这里所描述的本发明提供了一种增强两个解码器的配对的方法，具有以下优点：

[0080] • 在制造时，不存在对解码器的区分。解码器可以变为主解码器或从解码器，并且仅在解码器安装之后发生该区分。

[0081] • 本发明至多需要对条件访问系统的些微改变。如果CA提供商在个性化时对卡进行区分，则可以利用已经存在的消息来执行该方法。

[0082] • 可以通过对专用 EMM 的传输来无线地更新解码器的状态。

[0083] • 事务部门不需要跟踪和列出权利和解码器的关联，这简化了售后维护。

[0084] 将会理解，纯粹作为示例描述了本发明，并且在不脱离本发明的范围的情况下可以对细节进行修改。特别地，本发明可以应用于诸如移动电话等其他设备的配对，并且可以应用于其中提供对终端的条件访问的其他类型系统，例如用于访问音乐或计算机文件的系统。

[0085] 可以独立地或者以任意适当的组合来提供所述描述和（适当地话）和权利要求与附图中所公开的每一个特征。也可以用软件来实现如硬件中所实现的所述特征，反之亦然。

[0086] 在权利要求中所出现的参考符号仅是说明性的，而不应该具有对权利要求的范围的限定效果。还应该知道，术语“主解码器”应该解释为至少暂时充当主解码器的解码器；相反，“从解码器”应该解释为至少暂时充当从解码器的解码器。

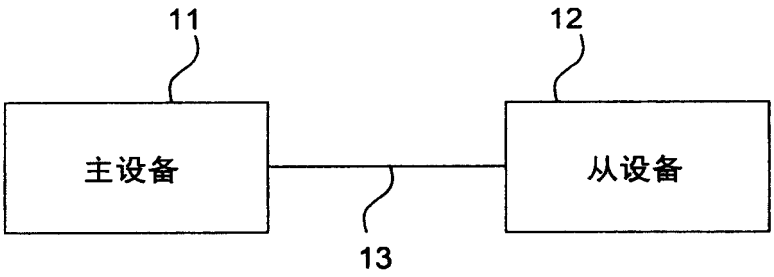

11
12
主设备
从设备
13

图 1

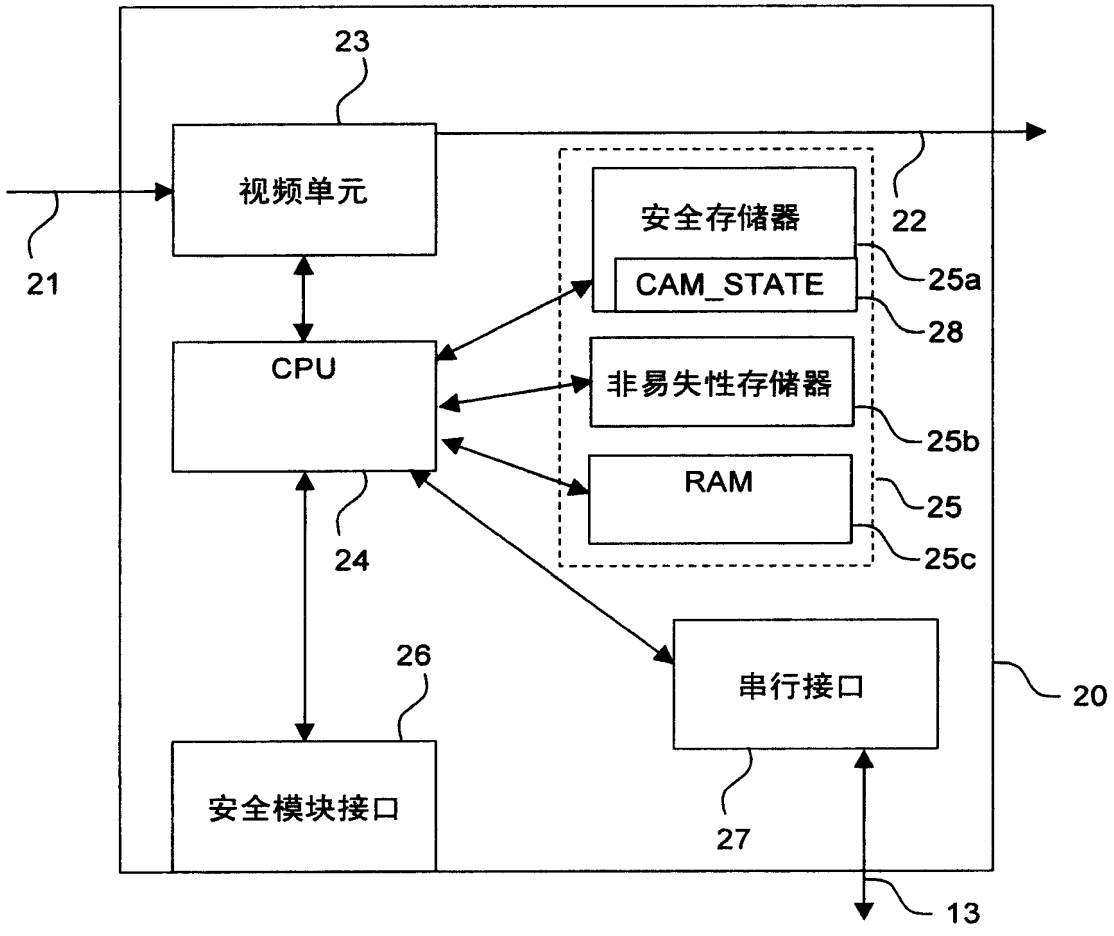

23
视频单元
21
22
安全存储器
CAM_STATE
25a
28
CPU
非易失性存储器
25b
RAM
25
25c
24
26
串行接口
20
安全模块接口
27
13

图 2

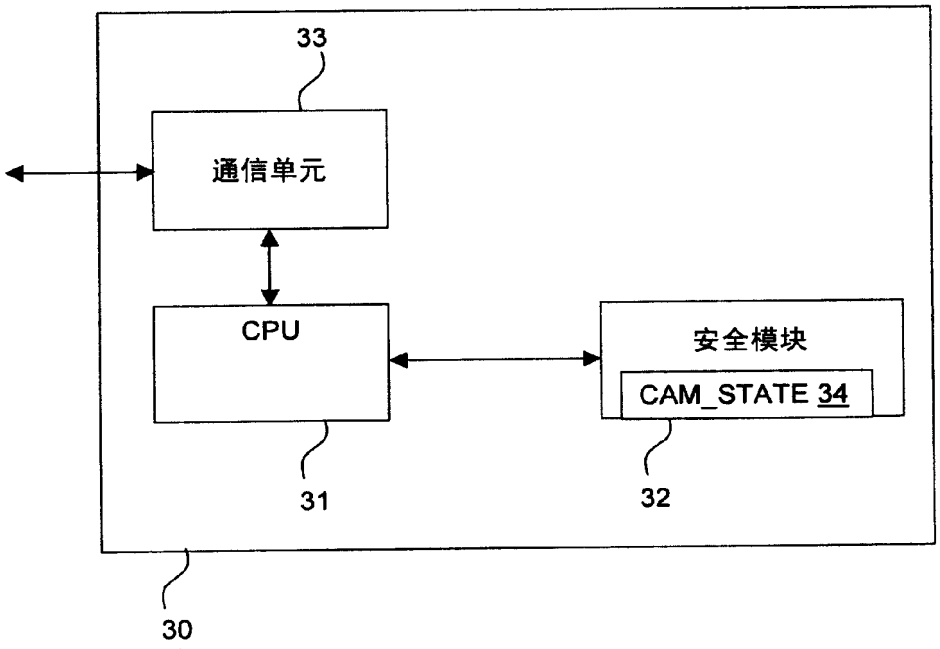

33
通信单元
CPU
安全模块
CAM_STATE 34
31
32
30

图 3

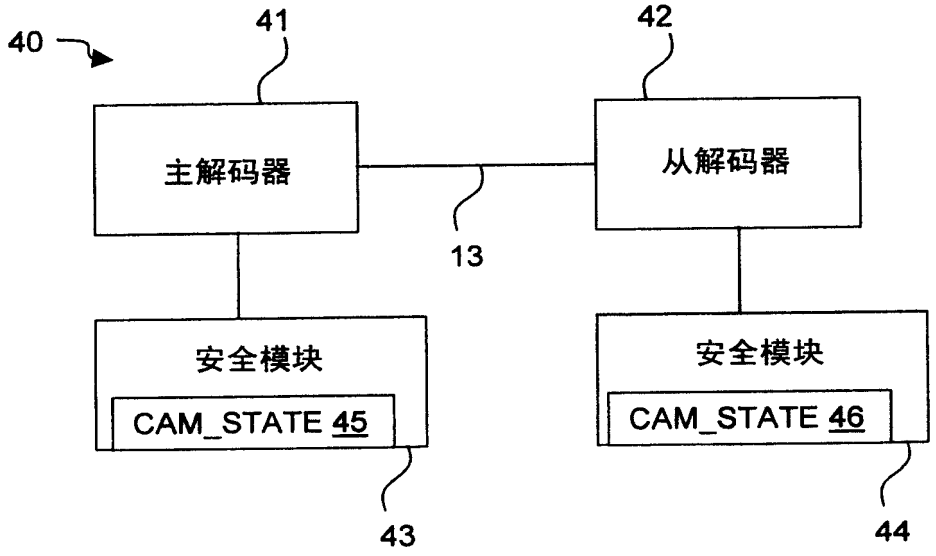

40
41
42
主解码器
从解码器
13
安全模块
CAM_STATE 45
安全模块
CAM_STATE 46
43
44

图 4

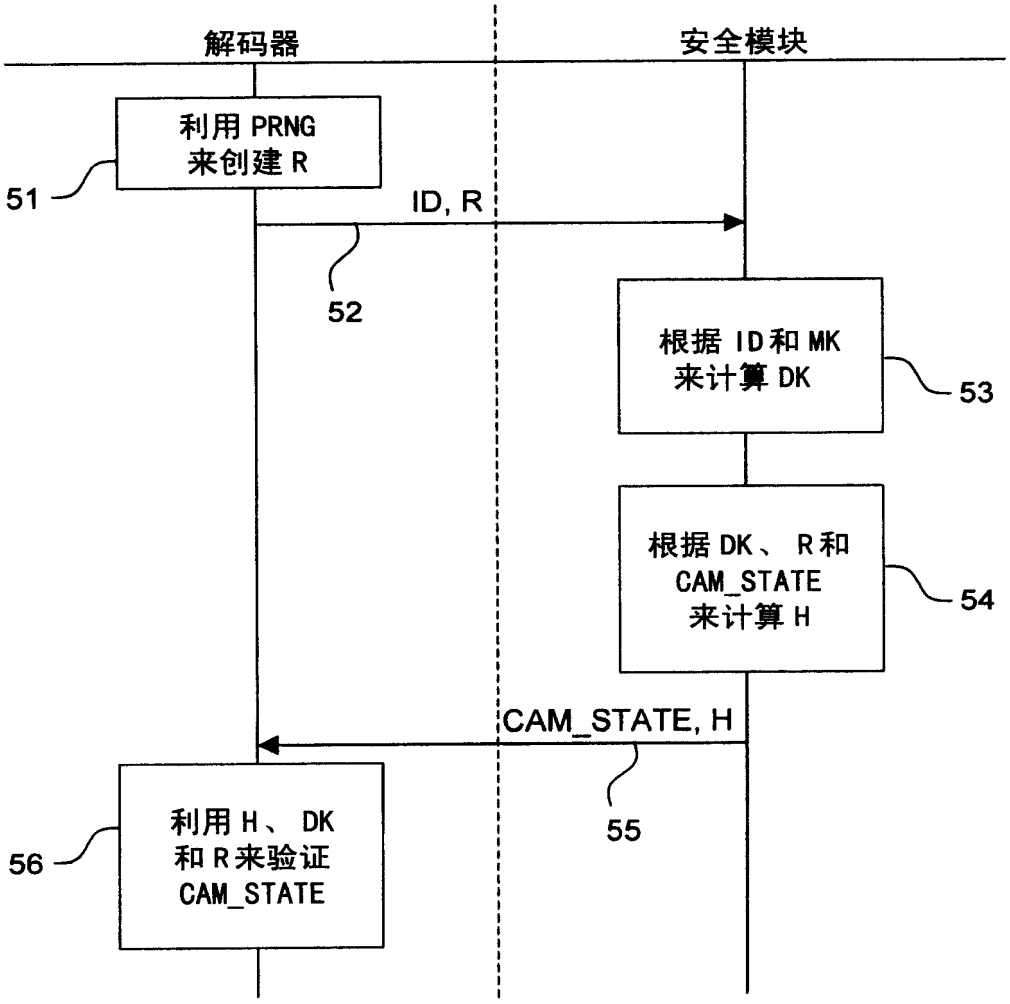

解码器
安全模块
利用 PRNG
来创建 R
51
ID, R
52
根据 ID和 MK
来计算 DK
53
根据 DK、 R和
CAM_STATE
来计算 H
54
CAM_STATE, H
55
利用 H、 DK
和 R来验证
CAM_STATE
56

图 5

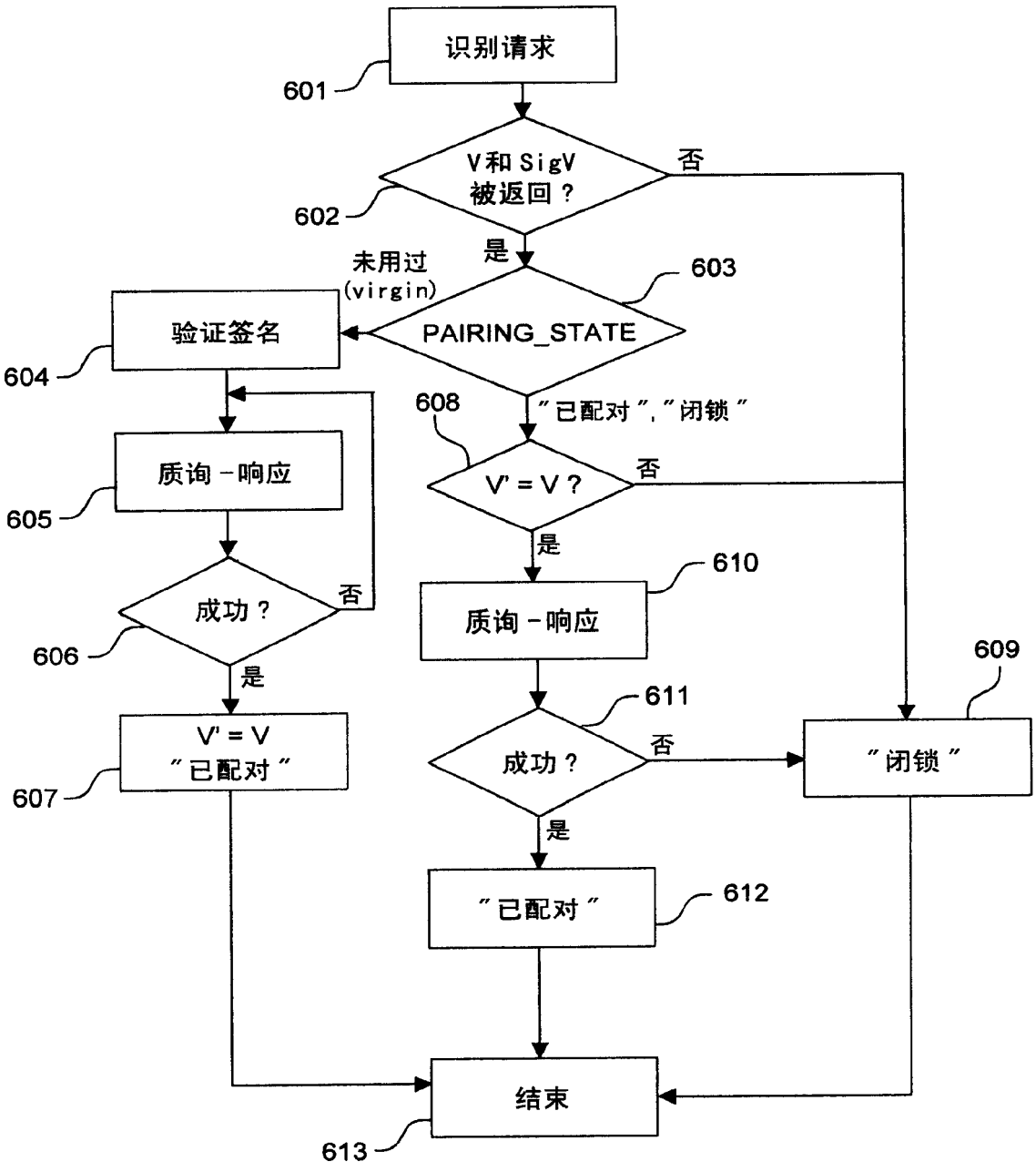

识别请求
601
V和 SigV
被返回？
602
否
是
未用过
(virgin)
603
PAIRING_STATE
验证签名
604
"已配对","闭锁"
608
质询－响应
605
V' = V？
否
是
成功？
606
否
610
是
质询－响应
609
611
V' = V
"已配对"
607
成功？
否
"闭锁"
是
"已配对"
612
结束
613

图 6

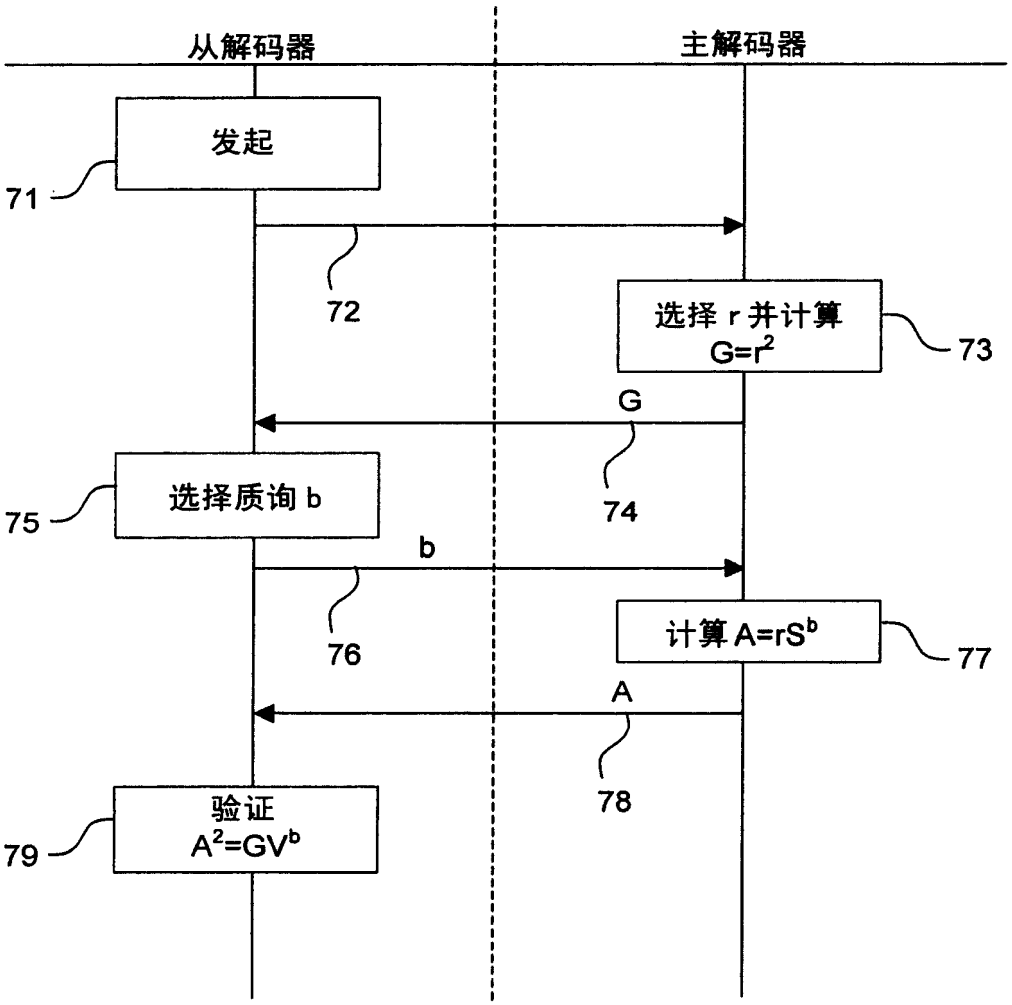

从解码器
主解码器
发起
71
72
选择 r 并计算
$G=r^2$
73
G
74
选择质询 b
75
b
76
计算 $A=rS^b$
77
A
78
验证
$A^2=GV^b$
79

图 7