(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 1647484 B
(45)授权公告日 2010.09.01

(21)申请号 03808512.7
(22)申请日 2003.03.06
(30)优先权数据
02/02969 2002.03.08 FR
(85)PCT申请进入国家阶段日
2004.10.15
(86)PCT申请的申请数据
PCT/FR2003/000721 2003.03.06
(87)PCT申请的公布数据
WO2003/077500 FR 2003.09.18
(73)专利权人 维亚塞斯公司
地址 法国巴黎
(72)发明人 克洛迪娅·贝克尔 安德烈·科代 皮埃尔·费夫里耶 尚塔尔·吉奥内
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘炳胜
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 5748732 A,1998.05.05, 全文.
CN 1183841 A,1998.06.03, 全文.
VAN SCHOONEVELD D.Standardization of conditional access systems for digital paytelevision.PHILIPS JOURNAL OF RESEARCH50 1.1996,50(1),217-225.
审查员 张巍

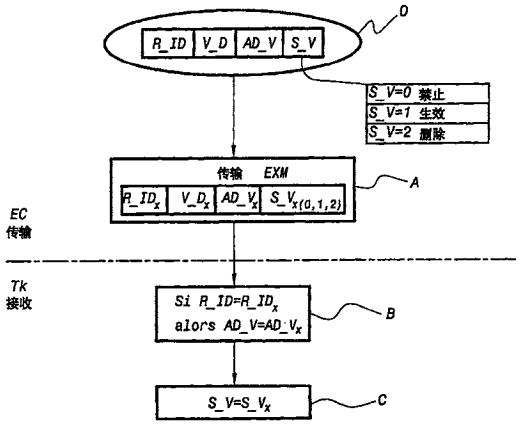
权利要求书 2 页 说明书 13 页 附图 5 页

(54)发明名称

加扰数据存取权限注册、禁止与/或删除协议及相应存取控制模块

(57)摘要

本涉及一种用于禁止/删除对加扰数据的存取权限的协议。根据本发明,在存取控制模块中注册的访问权限包括下列变量:权限标识变量(RAD)、作用日期变量(AD V)以及权限状态变量(S V)。该状态变量可以具有三个编码值之一:即生效、禁止、或删除权限。本发明的协议包括:(A)发送至少一个存取权限管理消息,该消息包括权限标识变量(R IDx)、作用日期变量(AD Vx)以及状态赋与变量(S Vx),后者对应于一个生效的、禁止的或删除权限;(B)将该消息的作用日期(AD Vx)赋与注册的权限的作用日期(AD V);以及(C)将该消息的、对应于生效、禁止、或删除权限的状态赋与变量(S Vx)分配给注册的存取权限的状态变量(S V)。本发明特别适用于付费电视。



CN 1647484 B

1. 一种注册、禁止或删除加扰数据存取权限的方法，其中该加扰数据由发射中心发送到至少一个解扰终端，该解扰终端连接一个配备了安全处理器的存取控制模块，这些存取权限在所述存取控制模块中注册，所述加扰数据通过周期性发送存取控制消息实现控制存取，传送周期性改变并用操作密钥加密的控制密钥密文和存取规范，然后在每个安全处理器中，通过用所述操作密钥解密控制密钥密文，参照所述存取规范验证至少一个注册的存取权限的真值，根据情况发送复原的控制密钥到解扰终端，使用所述复原的控制密钥解扰所述加扰数据，其特征在于包括以下过程：

- 将所述存取控制模块中注册的所有存取权限构成为一组独立变量和链接变量，除了存取权限识别变量外，还至少包括一个已注册存取权限的作用日期变量，一个代表权限生效、权限禁止、权限删除三个编码值之一的状态变量，

- 存取权限管理消息从所述发射中心发送到每个解扰终端和存取控制模块，至少一个存取权限管理消息连接到该存取控制模块，该存取权限管理消息除了一个注册的存取权限识别变量外，还至少包括一个作用日期变量和一个状态赋与变量，对应于生效的存取权限、禁止的存取权限、或者删除的存取权限的编码值；以及在接收到所述存取权限管理消息时，在所述存取控制模块处，将所述作用日期赋与和所述存取权限管理消息的存取权限识别变量对应的、已注册的存取权限，然后将对应于生效的存取权限、禁止的存取权限、或者删除的存取权限的状态赋与变量赋与所述相应已注册的存取权限的状态变量。

2. 如权利要求 1 中所述的方法，其特征在于，对于在存取控制模块中注册已确定的存取权限的操作，所述存取权限管理消息的所述作用日期变量对应于注册日期，状态赋与变量是一个对应于生效存取权限的编码值，所述注册操作包括在所述存取控制模块中注册一个已确定的存取权限，该存取权限的作用日期是所述的注册日期，并且该存取权限的状态变量是一个对应于生效权限的状态变量。

3. 如权利要求 2 中所述的方法，其特征在于，在正确地注册所确定的存取权限的操作之前，在所述的存取控制模块中，所述方法还包括以下操作：

- 在所述的存取控制模块中校验对应于所确定的存取权限的已注册存取权限的存在性，以及状态变量是否对应于权限生效或者权限禁止的编码值，在得到该校验的肯定答复后：

- 参照同一个所述已注册存取权限的作用日期，校验对应于一注册日期的所述作用日期变量的滞后特征，在针对该校验得到肯定答复后，

- 利用对应于注册日期的作用日期，更新所述同一个已注册存取权限的作用日期的变量，

- 将对应于生效权限的编码值赋予所述同一个已注册存取权限的状态变量，从而允许所述已注册存取权限被生效。

4. 如权利要求 3 中所述的方法，其特征在于，在上述关于同一存取权限的存在性的校验结果为否定后，进一步包括执行对该存取权限的首次注册的更新，其作用日期对应于注册日期。

5. 如权利要求 1 中所述的方法，其特征在于，对于存取控制模块中禁止一个已注册的存取权限的操作，所述存取权限管理消息的所述作用日期变量对应于一个禁止日期，并且状态赋与变量是一个对应于禁止存取权限的编码值；该禁止操作包括已注册的存取权限状

态变量赋值为一个对应于禁止权限的编码值，以及利用所述禁止日期更新所述已注册存取权限的作用日期。

6. 如权利要求 5 中所述的方法，其特征在于，在所述禁止操作之前，进一步包括：

- 在所述的存取控制模块中，校验对应于所述管理消息中的所述存取权限的、已注册的存取权限，该权限的存在性；

- 参照所述已注册存取权限的作用日期变量，校验对应于所述禁止日期的作用日期变量滞后特征。

7. 如前面权利要求之一中所述的方法，其特征在于，对于对应于已删除权限的管理消息的任一状态赋与变量，以及对于存取控制模块中注册的、对应于生效权限或者禁止权限的任一存取权限，至少包括：

- 更新所述已注册存取权限的作用日期；

- 将所述管理消息的对应删除存取权限的状态赋与变量赋给所述的已注册存取权限的状态变量，对于所述已注册存取权限，该赋与操作包括虚拟删除操作。

8. 如权利要求 7 中所述的方法，所述已注册存取权限的更新和虚拟删除步骤之前存在以下步骤：在所述存取控制模块内校验对应于所述管理消息的存取权限的已注册存取权限的存在性；参照所述已注册存取权限的作用日期变量，校验所述管理消息的作用日期变量的滞后性。

9. 如权利要求 7 中所述的方法，其中所述虚拟删除操作之后是物理删除所述存取权限的操作。

10. 如权利要求 9 中所述的方法，其中所述物理删除立即或者延迟执行。

11. 如权利要求 2 或 3 中所述的方法，其特征在于，对于具有其状态赋与变量对应于删除的存取权限的已注册存取权限，进一步包括执行一个该存取权限首次注册的更新，对应于一个生效权限的状态变量被赋与该存取权限，并且其作用日期对应于注册日期。

12. 如权利要求 5 或 6 中所述的方法，其特征在于，对于其状态赋与变量对应于已删除的存取权限的已注册存取权限，进一步包括执行一个该存取权限首次注册的更新，对应于禁止权限的状态变量被赋与所述存取权限，并且其作用日期为注册日期。

13. 如权利要求 6 中所述的方法，其特征在于，如果上述校验相应存取权限存在性的结果为否，则进一步包括执行一个该存取权限首次注册的更新，所述存取权限的作用日期对应于一个禁止日期，并且对应于一个禁止权限的状态变量被赋与该存取权限。

加扰数据存取权限注册、禁止与/或删除协议及相应存取控制模块

[0001] 在当前加扰数据存取控制领域，为了确保提供流畅和灵活的服务管理，加扰数据存取权限的注册、禁止与/或删除协议至关重要。

[0002] 付费电视领域更是这样。付费电视领域的服务以及提议条款往往拥有最复杂多变的服务以及条款。

[0003] 而且在上述领域中，用户订阅的周期性更新需要增加和注册新数据以实现用户提出的范围扩展或者新申请。

[0004] 当前对每个用户申请及分配的存取权限管理与控制完全无关。这是因为存取权限管理是能够携带存取权限的管理消息(EMM)进行处理；存取控制通过发送存取控制消息(ECM)处理，ECM消息包含一个加密的存取控制字作为服务密钥或者存取规范，这种更新包括注册新数据到安全处理器的内存。安全处理器连接到解码器或者存取控制模块。

[0005] 由于存取控制模块通常由一块类似银行卡的微处理器卡构成，其内存资源相当有限。

[0006] 因此，上述注册权限过程同时伴随着一个删除过期权限的功能。而删除过期权限功能的唯一目的是释放存取控制模块或微处理器卡的内存空间，以避免导致最终资源耗尽。

[0007] 但是在分配给用户的存取控制模块或者卡中进行存取权限管理时，这样的一个注册/删除过程并不能提供必要的灵活性、安全和流畅性。

[0008] 例如这样一个例子中：用户一方付账失误，甚或是在一个灵活的提供方式环境中用户改变他/她申请的服务提供方式。

[0009] 考虑到安全规范，假定当前删除过程中的某种恶劣情况：任意恶意的用户可能过滤或者拦截那类用来降低或者控制他们权限的删除消息。

[0010] 而且不能防止一个恶意进程可能存储正确的注册权限EMM消息，然后非法地提交到一个重放进程；

[0011] 最后如果发生未料及的适当EMM消息序列，其EMM消息引发的当前注册与/或删除权限进程可能引起这些管理操作失误。

[0012] 本发明的目标是实现一种加扰数据存取权限的注册、禁止与/或删除协议，一方面提供一个非常灵活和流畅的存取权限控制及管理协议，另一方面大幅提高其具备的安全水平。

[0013] 本发明的一个特别目的是实现一个加扰数据存取权限的注册禁止与/或删除协议时，每一个注册，禁止，与/或删除操作附有条件，需要得到一个预先的基准，例如作用时间。

[0014] 本发明的另一个目的是实现一个加扰数据存取权限的注册禁止与/删除协议时，注册、禁止与/或删除操作能够被加密，以提高安全水平，防止重放相应的被拦截命令消息。

[0015] 最后，本发明的另一个目的是实现一个能够在其可编程内存中注册存取权限和电

子钱包的加扰数据存取控制模块，实现本发明的目标协议。

[0016] 在加扰数据从一个发射中心发送到至少一个解扰终端时实现本发明的目标协议，加扰数据存取权限的注册禁止与/或删除协议。终端连接了一个带有安全处理器的存取控制模块。存取权限在存取控制模块中注册，通过周期性的存取控制消息控制加扰数据的存取。存取控制消息携带存取规范和用一个操作密钥加密的周期性改变的一个密码。然后在每一个安全处理器中，根据操作密钥解密得到的存取规范来校验至少一个已注册存取权限的实值，最后将解密的控制字发送到解扰终端，并对加扰数据进行解扰。

[0017] 值得注意，在存取控制模块中任何已注册存取权限都由一组独立变量和链接变量组成：除了一个存取权限识别变量外，还至少包括一个注册存取权限作用日期变量，和一个标志存取权限生效、终止和删除三个编码值之一的状态变量。从发射中心传送至少一个存取权限管理消息到每一个解扰终端以及相应的存取控制模块。管理消息除了存取权限识别变量外，至少包括一个作用日期变量和一个生效、终止、删除存取权限的相应编码值之一的状态赋与变量。

[0018] 接收到存取权限管理消息后，在存取控制模块中最终将作用日期赋与对应于存取权限管理消息存取权限识别变量的相应已注册存取权限，将生效、禁止、删除的存取权限相应的状态指定变量赋值到相应的已注册存取权限状态变量。

[0019] 从发射中心到至少一个解扰终端的加扰数据通过连接到解扰终端的存取控制模块实现控制存取。本发明的目标协议明确在这个存取控制模块的内存中包括了至少一个由一组独立变量和链接变量代表的存取权限。除了一个注册存取权限标识变量和一个生效日期变量外，这组变量还至少包括一个标识存取权限生效、禁止、删除三种编码值之一的状态变量。

[0020] 作为本发明的目标，协议和存取控制模块不仅能够应用在加扰数据的点到多点发送中，而且能够应用在付费电视领域中点到点的视频图像数据或者在如 IP 协议网络中服务执行数据的发送中。

[0021] 为了更易于理解，可以参见下面各图的描述和说明：

[0022] - 图 1 给出实现本发明目标协议的通用步骤流程图。

[0023] - 图 2a 给出了在配置给用户的存取控制模块中注册生效权限操作中，实现本发明目标协议的特定步骤流程图。

[0024] - 图 2b 给出了在配置给用户的存取控制模块中执行已注册权限禁止操作中，实现本发明目标协议的特定步骤流程图。

[0025] - 图 2c 给出了在执行已注册权限删除操作中，实现本发明目标协议的特定步骤流程图。该删除操作实际上是一个虚拟操作，实际上的物理删除有短暂延迟。

[0026] - 图 2d 给出了对于特定规范如面象时间的规范时有条件地对注册的存取权限引入物理删除时实现本发明目标协议的特定步骤流程图；

[0027] - 图 3a 和图 3b 根据发明，描述了一个存取控制模块。

[0028] 作为发明目标的加扰数据存取权限的注册、禁止与/或删除协议，将结合图 1 及后面的图进行给出更详细的描述。

[0029] 作为通用规则，应该记住本发明的目标协议可以管理由一个发射中心发送到多个解扰终端的加扰数据的存取权限。每一个终端 Tk 都与一个安装了安全处理器的相应存取

控制模块相关联。

[0030] 习惯上，每一个存取控制模块由一个包含上述安全处理器、以及保存译码密钥的安全内存和任一种验证检查操作的微处理器卡组成。每个存取控制模块安装了一个非易失可编程内存，在存取控制模块中加扰数据存取权限注册到上述非易失可编程内存。

[0031] 加扰数据的存取控制通过周期性发射存取控制消息，即 ECM 消息实现。这些存取控制消息携带存取规范和一个周期性改变并用一个操作密钥加密的控制字密文。

[0032] 在每个安全处理器中，一般参照存取控制消息携带的存取规范，对至少一个已注册权限的真值进行验证，实现存取控制需要使用操作密钥解密控制字的密文，然后存储到安全处理器的非易失内存，然后将存取控制模块恢复的控制字发送到解扰终端，使用上述解扰终端中的恢复的控制字对加扰数据进行解扰。

[0033] 上述加扰数据存取控制过程的上下文环境中，值得注意的是，根据本发明的目标协议，至少构成和定义已在存取控制模块中注册的所有权限作为一组独立变量和链接变量，这些变量至少包括：除了一个存取控制权限标识变量和一个生效日期变量外，还至少包括一个存取控制模块中已注册存取权限的作用日期变量，以及一个包括表示存取权限生效、禁止、删除三个编码值之一的状态变量。

[0034] 参考上述图 1，定义了下列符号：

[0035] -R_ID：存取权限标识变量；

[0036] -V_D：生效日期变量；

[0037] -AD_V：已注册存取权限作用日期变量；

[0038] -S_V：状态变量，代表存取权限生效、禁止、删除三个编码值中的一个。

[0039] 给出一个例子但并不局限于本例，三个编码值可以按照这种方式实现取值：

[0040] - 禁止权限 S_V = 0；

[0041] - 生效权限 S_V = 1；

[0042] - 删除权限 S_V = 2；

[0043] 给定上述安排，可以自然的理解前面描述的存取权限定义和构成是本发明目标协议的基础。图 1 的步骤 0 描述了该步骤，每个存取权限 AR 可以相应表示为下列语法：

[0044] AR = [V_D] R_ID [R_SID] AD_V S_V (1)

[0045] 对于该关系，根据前面存取权限的特定编码，上面方括号内的各个变量都是可选的。

[0046] 当生效日期变量 V_D 是一个独立变量时，在特定编码情况下它是可选的。例如一个缺少生效日期变量的已注册存取权限可能对应于一个特定的权限值。

[0047] 相反，权限标识子变量 R_SID 是一个链接到存取权限识别变量 R_ID 的链接变量。

[0048] 在这种条件下，独立的存取权限标识变量 R_ID，作用日期变量 AD_V 和状态变量 S_V 的提出对实现本发明的目标协议是必需的，主要用来实现注册存取权限和包含一个生效日期变量（尽管可选）。

[0049] 因此，参考上面关系 (1)，这些变量可以这样理解：

[0050] V_D：指明一个效力日期间隔，能够用存取权限的开始日期和终止日期来设置及表示，或者转动并定义为一个日期数，或者失效日期，例如，效力间隔能够根据第一次使用日期转化为一个固定值。

[0051] R_ID 和 R_SID：已注册权限的相应标识和子标识变量，在存取控制消息 ECM 携带的存取规范中自然用来作为参照；

[0052] AD_V：表述注册权限已经执行的日期。更特殊的情况下，当智能卡中没有执行操作时，变量表示为卡中注册权限的注册日期，或者相反，表示为上次操作执行日期和作用日期，甚至是将在以后描述到的再生效、禁止、删除日期。

[0053] S_V：表示为状态变量的编码值。参考图 1，这个编码值有前面提到的 0、1、2 三个值，或者其他任何明文或加密值。

[0054] 参照图 1，根据以上描述可以完成组成和定义存取权限的步骤。

[0055] 在前述步骤 0 之后，本发明的目标协议由步骤 A 组成：至少一个存取权限管理消息，标识为 EXM 消息，从发射中心传送到每一个解扰终端 Tk，自然，传送到与其相连的存取控制模块。

[0056] 见图 1，这个消息由至少一个表示为 R_ID_x 的注册存取权限标识变量和一个表示为 AD_V_x 的作用日期变量。作用日期对应于管理消息的发送日期，也就是说，对已经注册的存取权限所执行的管理操作的日期，其中的标识变量 R_ID 对应于包含在管理消息中的标识变量 R_IDx，后面将进一步解释。这个消息可以进一步包含一个表示为 V_D_x 的生效日期变量，最后，该管理消息 EXM 包括由对应于存取权限生效、禁止或者删除的一个编码值的状态赋与变量 S_V_x。变量 S_V_x 能够象前面描述的那样取值 0，1，2。

[0057] 在连接到解扰终端的存取控制模块内接收到 EXM 消息后，按照本发明的目标协议包括，在步骤 B 中，将作用日期赋与与存取权限管理消息的存取权限识别变量对应的已注册存取权限；步骤 C 中，将对应于一个存取权限生效、禁止、删除的状态赋与变量 S_V_x 分配给已注册存取权限的状态变量 S_V。

[0058] 考虑在步骤 B 中的实现过程，这个过程可以使用一个逻辑 IF...Then... 命令来实现。

[0059] 这种条件下，如图 1，上述步骤 B 将已注册存取权限标识变量 R_ID 的值与 EXM 消息中注册存取权限标识变量即变量 $R\text{-}ID_x$ 进行匹配比较。这个比较过程包括对很多变量的连续比较，例如权限子识别变量 R_SID 和生效日期变量或者其他适当变量。

[0060] 当进行匹配校验时，根据情况，作用日期变量 AD_V 被赋予 EXM 消息的作用日期变量 AD_V_x 的值。这种情况包括校验变量 AD_Vx 相对于变量 AD_V 的滞后性。然后将 EXM 管理消息中的状态赋与变量 S_Vx 赋与已注册权限的状态变量 S_V。该操作在步骤 C 中执行，并按照下式将已注册存取权限的权限状态变量 S_V 进行实例化：

[0061] $S\_V = S\_V_x$

[0062] 下面结合图 2a 到 2d，通过注册一个生效权限，禁止权限，和删除权限的操作步骤的环境中，给出本发明目标协议实现的详细描述。

[0063] 对于在存取控制模块中所定义的注册存取权限的操作，EXM 管理消息中的作用日期变量 AD_Vx 对应于该存取权限的注册日期，赋与变量 S_Vx 是一个编码值，对应于一个生效权限，也就是说，这里编码值 S_Vx = 1。

[0064] 注册存取权限的操作包括在存取控制模块中特别是它的非易失内存中注册一个权限，其作用日期是上述的注册日期，状态变量 S_Vx = 1。

[0065] 参见图 2a，注册操作开始于步骤 B_{0a}，即在解扰终端处接收到 EXM 消息。

[0066] 在EXM消息解扰之后，存取控制模块从EXM消息中获得了变量R_IDx，V_Dx，AD_Vx，S_Vx ＝ 1，还得到了存取模块中已注册权限的R_ID，V_D，AD_V，S_V变量（如果这些权限已经注册的话）。

[0067] 实现上述的注册操作，本发明的目标协议包括：如图2描述的步骤B_{1a}，校验一个相应的已注册权限的存在性。该测试表示为：

[0068] $\exists R\_ID = R\_ID_x$。

[0069] 同时完成S_V ≠ 2测试确保这个权限不属于删除的权限，以允许执行处于禁止状态或者注册状态的权限的执行，并且以后可以重新执行注册操作。所以步骤B_{1a}中实现的测试将验证该式：

[0070] $\exists R_ID = R_ID_x$且S_V ≠ 2

[0071] 步骤B_{1a}的测试得到肯定响应后，本发明的目标协议验证对应于注册日期的作用日期变量相对于相应的存取权限的作用日期的滞后性特征，这一操作可在步骤B_{2a}中执行，通过比较包含在消息EXM中的作用日期变量A_V_x与作用日期相对于已注册权限的作用日期AD_V的超前性来完成。

[0072] 如果上述步骤B_{2a}的测试得到一个否定答复，注册操作终止于结束注册步骤B_{3a}，注册权限的操作没有能够完成。

[0073] 相反，如果B2a的测试得到一个肯定答复，进入步骤B_{4a}，包括根据对应注册日期的作用日期更新相应存取权限的作用日期。操作由下式表示：

[0074] $$AD\_V = AD\_V_x。$$

[0075] 更新步骤之后执行赋值步骤C，将一个生效的权限相应编码值，S_Vx ＝ 1，赋于同一个存取权限的状态变量S_V。存取控制模块中以前已注册存取权限得到更新或修改。

[0076] 对于注册权限操作，本发明的目标协议自然能够实现在存取控制模块中注册第一个权限的操作。

[0077] 这种情况下，对应于EXM消息中存取权限识别变量R_IDx没有已注册存取权限，步骤B1a执行的关系匹配比较得不到验证。

[0078] 从而，上述步骤校验关系$\exists R_ID = R_ID_x$和S_V ≠ 2得到一个否定答复时，本发明的目标协议执行该存取权限的首次注册更新，其作用日期等于注册日期。

[0079] 图2中，该操作在表示为在步骤B_{1a}的失败响应后，更新步骤AD_V ＝ AD_Vx的存取。

[0080] 该存取能够通过将EXM管理消息中的R_IDx值赋给步骤B5a执行的已注册权限变量R_ID完成，然后在步骤B6a中，将生效日期变量V_Dx赋予生效日期变量V_D。

[0081] 在该例中步骤C中的赋值操作对应于首次注册。

[0082] 同样，参见图2a，对于这样一个注册的存取权限，其状态赋与变量对应于已经删除但是物理上还存在的权限，即相应的状态赋与变量S_V ＝ 2的注册存取权限，也同样包括步骤B1a得到失败反映后的步骤B5a，B6a，和B4a，进行权限的更新。然后步骤C中为注册的存取权限赋与一个对应于生效权限状态变量。

[0083] 结合图2b对本发明的目标协议在存取控制模块中实现禁止一个已有存取控制权限进行更详细的描述解释。

[0084] 这时，存取权限管理消息的作用日期变量对应于一个禁止日期，状态赋与变量S_

Vx 是对应于禁止权限的编码值，即前面说明中的 0 值。

[0085] 该情况中，在存取控制模块中禁止已注册权限的操作包括将对应于禁止权限的编码值，即 S_Vx ＝ 0 赋与注册存取权限状态变量 A_V，自然，利用禁止操作日期更新已注册存取权限的作用日期。

[0086] 如图 2b 中表示的那样，禁止操作开始于解扰终端 Tk 接收到这次操作的 EXM 管理消息。

[0087] 该步骤中，参见图 2b 中的 B_{0b}，EXM 消息中包括存取权限识别变量 R_IDx，生效日期变量 V_Dx，作用日期变量 AD_Vx，状态赋与变量 S_Vx ＝ 0 ；存取控制模块中已注册权限包括权限赋与变量 R_ID，生效日期变量 V_D，作用日期变量 AD_V，状态变量 S_V。

[0088] 这种情况下，本发明的目标协议如图 2b 所示，在执行禁止操作之前，如同图 1a 中的测试步骤 B_{1a} 一样，在存取控制模块的步骤 B_{1b} 中包括一个相应注册存取权限存在性的验证步骤。

[0089] 而且，在不限定模式中，类似图 1a 中的测试步骤 B1a，该测试可以验证对应的注册权限是一个生效的还是禁止的权限，对于该禁止的权限，应当执行了禁止操作。

[0090] 因此，步骤 B1b 执行的测试校验下式 ：

[0091] $\exists R\_ID = R\_IDx$ 并且 S_V ≠ 2

[0092] 步骤 B1b 得到肯定结果后，进入步骤 B2b，参照已注册权限的作用日期变量校验对应于一个禁止日期的作用日期变量的滞后性特征。该操作在步骤 B2b 中依下式执行 ：

[0093] AD_Vx ＞ AD_V。

[0094] 如果步骤 B2b 得到否定结果，如图 2b 所示，调用步骤 B3b 结束禁止操作。这个操作可用来为正确执行禁止操作提供一种安全措施。

[0095] 相反，如果步骤 B2b 得到肯定结果，在步骤 B4b 中执行作用日期更新操作。该更新操作执行和图 2a 中注册生效权限的更新步骤 B4a 类似的关系。

[0096] 步骤 B4b 接下来是禁止步骤 C，包括赋与相应禁止权限编码值 S_Vx ＝ 0 到已注册存取权限的状态变量 S_V。

[0097] 参见图 2b，本发明的目标协议还能实现禁止一个还在存取控制模块上已删除的存取权限，即 S_V ＝ 2。这时，在上述步骤 B_{1b} 得到否定结果时，执行更新步骤 B_{4b}，然后在步骤 C 中进行禁止操作，S_V ＝ S_V ＝ 0。如同图 2a 中的步骤 B_{5a} 和 B6a 情形，步骤 B_{4b} 接下来是 B_{5b} 和 B_{6b}。

[0098] 上述环境中，本发明的目标协议通过注册一个其作用日期对应于禁止日期的存取权限来实现更新。该注册的存取权限被分配了一个对应于禁止权限的状态变量。

[0099] 上述操作通过一个带有较早作用日期的消息来放置或者注册禁止状态的权限，防止后来的注册。

[0100] 下面结合图 2c 和 2d 更详细地描述本发明的目标协议实现删除已注册权限的操作。

[0101] 删除已注册权限的操作执行，是始于对应于删除权限的状态赋与变量 S_Vx ＝ 2 的 EXM 消息。

[0102] 如图 2c 所示，删除操作开始于一个解扰终端 Tk 接收到 EXM 消息，然后在描述中描述前述的变量，以便注册和禁止操作，但是状态赋与变量 S_Vx ＝ 2。

[0103] 对于存取控制模块中其状态变量对应于无效权限生效权限的存取权限执行删除操作。

[0104] 这里，步骤B0c接收到EXM消息，然后是测试步骤B1c，在存取控制模块内校验相应的已注册存取权限的存在性。前面步骤B1c类似于图2a中的B_{1a}或者图2b中的B1b，校验相同的关系。步骤B1c得到一个否定答复后，调用删除终止步骤B2c。步骤B1c得到肯定结果时进入步骤B3c，校验管理消息作用日期变量AD_Vx相对于已注册权限作用日期变量AV_V的滞后性。该步骤按照下式执行前后关系的比较：

[0105] AD_Vx ＞ AD_V

[0106] 校验步骤B3c得到否定结果时，返回到调用删除终止步骤B2c，这个类似于图2b中禁止一个权限的相似情况。

[0107] 相反，校验步骤B3c得到肯定结果时，根据本发明的目标协议，执行下式，删除操作包括调用已注册权限的作用日期更新步骤B4c：

[0108] AD_V ＝ AD_Vx

[0109] 在步骤C中，上述更新步骤之后是一个删除步骤，执行已注册权限的一个虚拟删除操作。

[0110] 作为本发明的目标协议特定优越性的一个体现，虚拟删除操作将对应于一个已删除的存取权限即S_Vx ＝ 2的管理消息状态赋与变量S_V赋予给已注册权限的状态赋与变量S_V。

[0111] 虚拟删除操作概念实际上在存取控制模块的非易实行内存中保持存取权限的物理存在，但是通过分配一个对应于已删除权限的编码值简单地使权限不再起作用。

[0112] 作为本发明的目标协议特定优越性的一个体现，一个已注册权限的虚拟删除状态可对应于该权限完全不能使用，尽管存取控制模块的非易实行内存中物理上还保存着该权限。对任何已注册权限完全的删除操作即物理删除，可以随后系统地执行，完全独立于存取控制和用户对与相关权限对应的加扰数据的存取。

[0113] 而且，如图2d所示的，前面对虚拟删除状态的已注册权限实现物理删除可以立即执行或者延迟执行。

[0114] 物理删除状态可以适当的根据某个规范，例如基于时间的规范。结合图2d进行更详细的讨论。

[0115] 参考前面的图，按照结合前面图2c的说明书中所描述和展示实现形式，在实施本发明的目标协议后，将一个已注册存取权限看作处于虚拟删除状态。

[0116] 这种条件下，接收到连同S_Vx ＝ 2的一个EXM消息，虚拟删除条件对应于前面描述的关系S_V ＝ S_Vx ＝ 2。在图2d的状态C0d中展现了虚拟删除状态。

[0117] 已注册权限的物理删除的执行可以在步骤C1d中进行测试，例如基于时间的测试。

[0118] 作为一个非限定性例子，上述测试可以比较EXM消息的作用日期变量AD_Vx（即AD_V_x变量）是否先于已注册权限的效力终止日期变量V_D。但是并不局限于该例，

[0119] 校验步骤C1d得到肯定结果后，由于删除作用日期晚于已注册权限的效力日期，通过调用相应步骤C3d立即执行物理删除。

[0120] 相反，校验步骤C1d得到否定结果后，由于删除作用日期早于已注册权限的效力

日期 V_D，执行相应延迟物理删除步骤 C2d。删除延迟到所有相继 EXM 消息作用日期 AD_Vx 小于或等于已注册权限的效力终止日期。延迟物理删除的保持标志为退回校验步骤 C1d。

[0121] 由于上述延迟删除，可以理解，可以确保系统管理这些注册存取权限的物理删除，尽管这些权限还物理的保存在卡上，但是由于其相应权限被置于虚拟删除的环境下，因此用户是不能使用的。

[0122] 下面将给出根据现有技术以及按照本发明的目标协议的一个实现权限删除的对比例，其中假设一个给定用户没有存取模块，也就是说在用户的解扰终端或者解码器没有处理卡，或者说在相对管理消息（现有技术中的 EMM 消息，本发明的 EXM 消息）发送周期的一个时间段内解码器不能运行。

[0123] 该例子考虑到现有技术中处理器的 EMM 消息或 E 根据本发明协议的 EXM 消息的周期性广播特性。

[0124] 根据与现有技术的处理器相关的表 1，按照周期 1 的 EMM 型管理消息周期发射（如表所示），而在相应的作用日期期间，根据表中周期 1 的区 A 的各单元，解扰终端或存取控制模块失效。

[0125] 表 1

[0126]

	消息类型	作用日期	卡上的动作	
周期 1	.../...	01/12/01	早于 01/12/01	
	R_ID1 注册 EMM		注册权限 R_ID1	
	R_ID1 删除 EMM	02/12/01	删除权限 R_ID1	
	R_ID2 注册 EMM	12/12/01	注册权限 R_ID2	
	R_ID3 注册 EMM	13/12/01		A
	R_ID4 注册 EMM	12/12/01		
	EMM .../...	.../...		
周期 2	R_ID5 注册 EMM	31/12/01	注册权限 R_ID5	
	R_ID5 删除 EMM	01/01/02	删除权限 R_ID5	
	R_ID6 注册 EMM	12/01/02	注册权限 R_ID6	
	EMM .../...			
N 周期 1	R_ID1 注册 EMM	01/12/01	注册权限 R_ID1	
	R_ID1 删除 EMM	02/12/01	删除权限 R_ID1	
	R_ID2 注册 EMM	12/12/01	权限已经存在	B
	R_ID3 注册 EMM	13/12/01	注册权限 R_ID3	
	R_ID4 注册 EMM	12/12/01	注册权限 R_ID4	
	EMM .../...			

[0127] 上面表 1 中，应该明白作用日期代表消息发送日期，但是不像实现本发明的目标协议适用的 EXM 消息那样，该消息不包含作用日期。

[0128] 周期 1 之后是带有不同日期的周期 2，然后是一批周期 1，表示为 n 周期 1。

[0129] 在发送第一个周期 1 的时候，除了表格中区域 A 的部分外，注册或者删除一个权限的执行都要在存取控制模块也就是处理卡或者解扰终端不失效的情况下。

[0130] 不同于周期 1，发送周期 2 时，考虑到已注册权限的识别变量，需要存取控制模块和 / 或终端的服务，相应的操作按照相同的方式执行。

[0131] 相反，在周期 1 的重复阶段，也就是表 1 标识的 n 周期 1 的表格单元，对应于区域 B 的单元，这些区域表示连续注册和删除的广播权限 R_ID_1 不能在存取控制模块也就是卡中建立，因为没有作用日期的控制被执行。

[0132] 现有技术的处理器不允许控制非重新注册或者删除权限，和本发明的目标协议相联系的表 2 在类似的环境下，减少了 EXM 消息带来失误的机会。

[0133] 表 2

[0134]

	消息类型	作用日期	卡上权限状态
周期 1	…/…	01/12/01	
	R_ID1 注册 EXM		注册权限
	R_ID1 禁止 EXM	02/12/01	禁止权限
	R_ID2 注册 EXM	12/12/01	注册权限
	R_ID3 注册 EXM	13/12/01	
	R_ID4 注册 EXM	12/12/01	
	R_ID4 禁止 EXM	13/12/01	
	EXM …/…	…/…	
周期 2	R_ID5 注册 EXM	31/12/01	注册权限
	R_ID5 禁止 EXM	01/01/02	禁止
	R_ID6 注册 EXM	12/01/02	注册权限
	EXM …/…		
N 周期 1	R_ID1 注册 EXM	01/12/01	注册权限
	R_ID1 禁止 EXM	02/12/01	删除权限
	R_ID2 注册 EXM	12/12/01	权限已经存在
	R_ID3 注册 EXM	13/12/01	注册权限
	R_ID4 注册 EXM	12/12/01	注册权限
	R_ID4 禁止 EXM	13/12/01	禁止
	EMM …/…		

A

[0135] 在这种条件下，存取控制模块的处理规则如下：

[0136] - 禁止时，权限被标记为禁止 I；

[0137] - 一个禁止的权限在某些条件下可以生效；

[0138] - 如果作用日期，也就是 EXM 消息中的作用日期变量小于或者等于已注册权限的作用日期，消息的作用在卡 I 中被忽略；

[0139] - 如果 EXM 消息中的作用日期变量大于已注册权限的作用日期，已注册权限被重新更新，也就是被刷新为禁止或者删除；

[0140] 如同表 1，表 2 中区域 A 对应于周期 1 中存取控制模块或者处理卡失效或停用阶段。

[0141] - 区域 I 表示已注册权限被禁止消息所禁止，即 S_V = S_Vx = 0；

[0142] - 区域 I 的单元的表格指这样的环境，如果 EXM 消息中的作用日期小于或者等于已有但已禁止权限的作用日期，相应的动作被存取控制模块忽略。

[0143] 这表明在存取控制模块中有一个对所有已注册存取权限更加灵活和流畅的处理和管理方式。

[0144] 为了实现本发明的目标协议，有一个解扰终端，连接到一个对由发射中心发送到上述解扰终端的加扰数据实现存取控制的存取控制模块，自然很重要。

[0145] 如图 3a 所示，连接到相应解扰终端的存取控制模块包括至少一个由一组相关和独立变量组成的存取权限，注册到存取控制模块的内存中。除了已注册权限的识别变量 R_ID，这组变量还包括一个已注册权限作用日期变量 AD_V，和一个表示前面提到的代表生效权限、禁止权限甚至删除权限三个编码值之一的状态变量。存取控制模块还能包括一个生效日期变量 V_D。

[0146] 作为通用规则，存取控制模块可以包括一个软件单元，也可以是一个硬件单元，甚至是一个包含上述软件单元的虚拟处理卡，或者前面描述的一个带有安全处理器的微处理器卡。

[0147] 例如，当存取控制模块是一个软件单元时可以放置在解扰终端里。如图 3a 所示，由上述相关和独立变量组成的存取权限可以存储在例如硬盘这样的永久存储器里。图中没有显示出它们，以及可以系统地装入解扰终端的工作内存，而工作内存自然连接到解扰终端的安全处理器 CPU_S。

[0148] 相反，如果存取控制模块是一个带有安全处理器的微处理器卡，如图 3b，这块微处理器卡也可安装一个与安全处理器相连的非易失可编程内存。这时，如上图 3b 所示，由上述相关和独立变量组成的存取权限注册到安全的非易失可编程内存。

[0149] 而且可以理解，借助于该卡输入 / 输出电路的总线连接，即指示的 I/O，从解扰终端来的、用于在非易失可编程内存中注册存取权限或禁止存取权限或者相反用于删除权限的交易指令，可以由前面提到的安全处理器 CPU_S 控制下输入 / 输出电路 I/O 实现。

[0150] 最后，同样在图 3b 中，加扰数据控制服务更特殊的情况中，对数据的存取要受支付情况影响，例如在付费电视服务，由链接和独立变量组成并且定义加扰数据存取模式的存取权限概念以及，覆盖了拥有存取控制模块的用户分配的电子钱包。

[0151] 因此，图 3b 展示了一个和存取权限 AR 类似编码的电子钱包，同样电子钱包可能包括下例变量：

[0152] - 电子钱包识别变量，表示 Puese SubID（钱包标识）；

[0153] - 生效日期变量 V_D；

[0154] - 电子钱包的作用日期变量 AD_V；

[0155] - 状态变量 S_V。

[0156] 最后，一个备用的单元变量，表示为 Puese Units（钱包单元）。

[0157] 电子钱包识别变量可以连接到一个链接变量，例如，Puese SubID（钱包子标识）。根据关于存取权限 AR 实体的前述描述，该变量也是可选的。

[0158] 这里，可以理解对以一个给定电子钱包，参照钱包 ID，对于特定应用或者特殊服务可能通过 Puese SubID 定义子钱包。

[0159] 同样，相同的情况下对于钱包单元变量可以连接到一个可选的连接变量 RE，连接变量 RE 能指定一个“携带”变量，用来携带超出相关电子钱包的内容或者信用余额到一个相同类型的电子钱包，或者到有同样标识符的相同电子钱包。

[0160] 在和存取权限 AR 同样的情况下，类似于存取权限 AR，电子钱包的加密语法采用以下形式：

[0161] PU ＝ PurseID[Purse SubID]V_D AD_V S_V Purse Units[RE]。

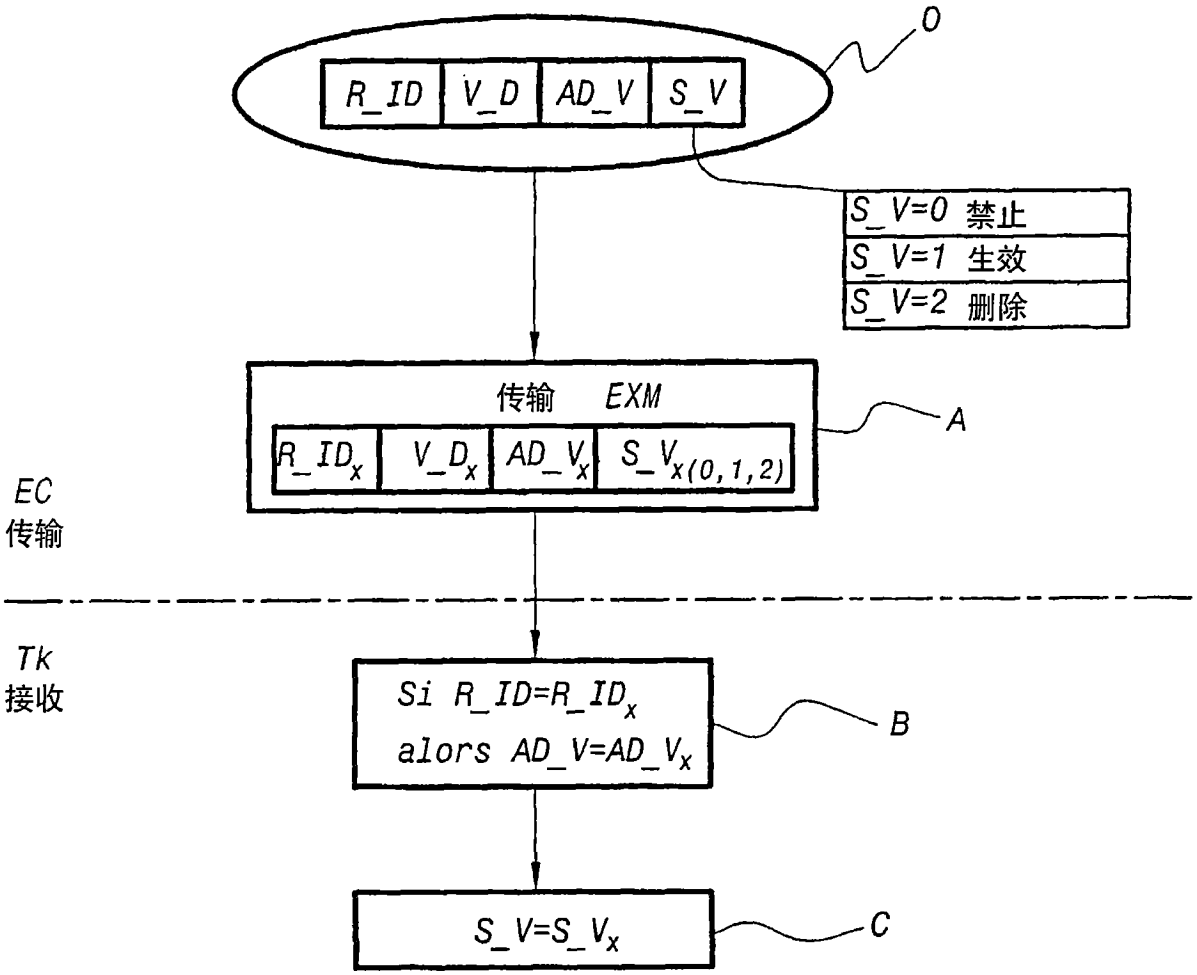

O
R_ID
V_D
AD_V
S_V
S_V=0 禁止
S_V=1 生效
S_V=2 删除
传输 EXM
R_ID_x
V_D_x
AD_V_x
S_V_x(0,1,2)
A
EC
传输
Tk
接收
Si R_ID=R_ID_x
alors AD_V=AD_V_x
B
S_V=S_V_x
C

图 1

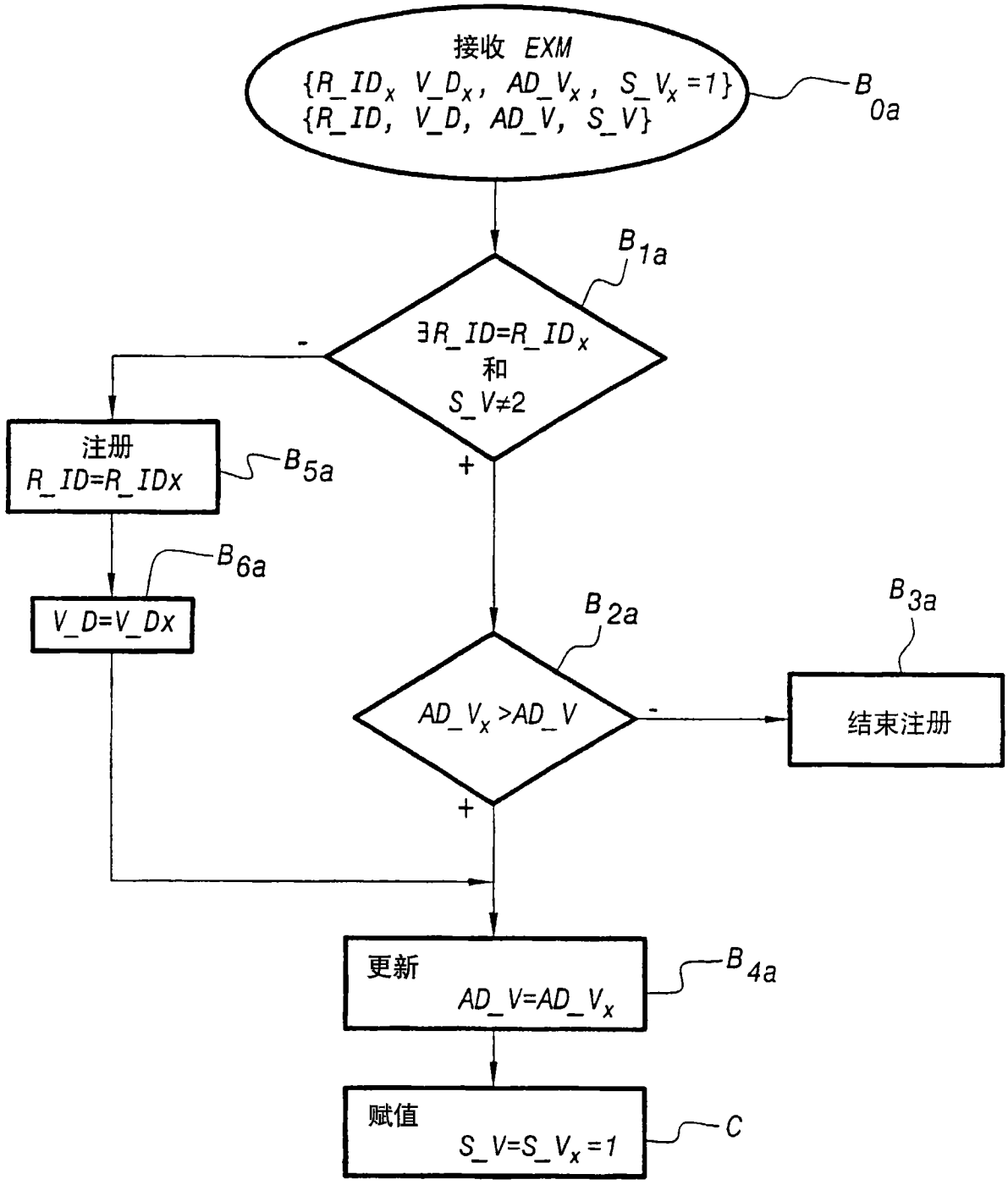


图 2a 注册一个有效权限

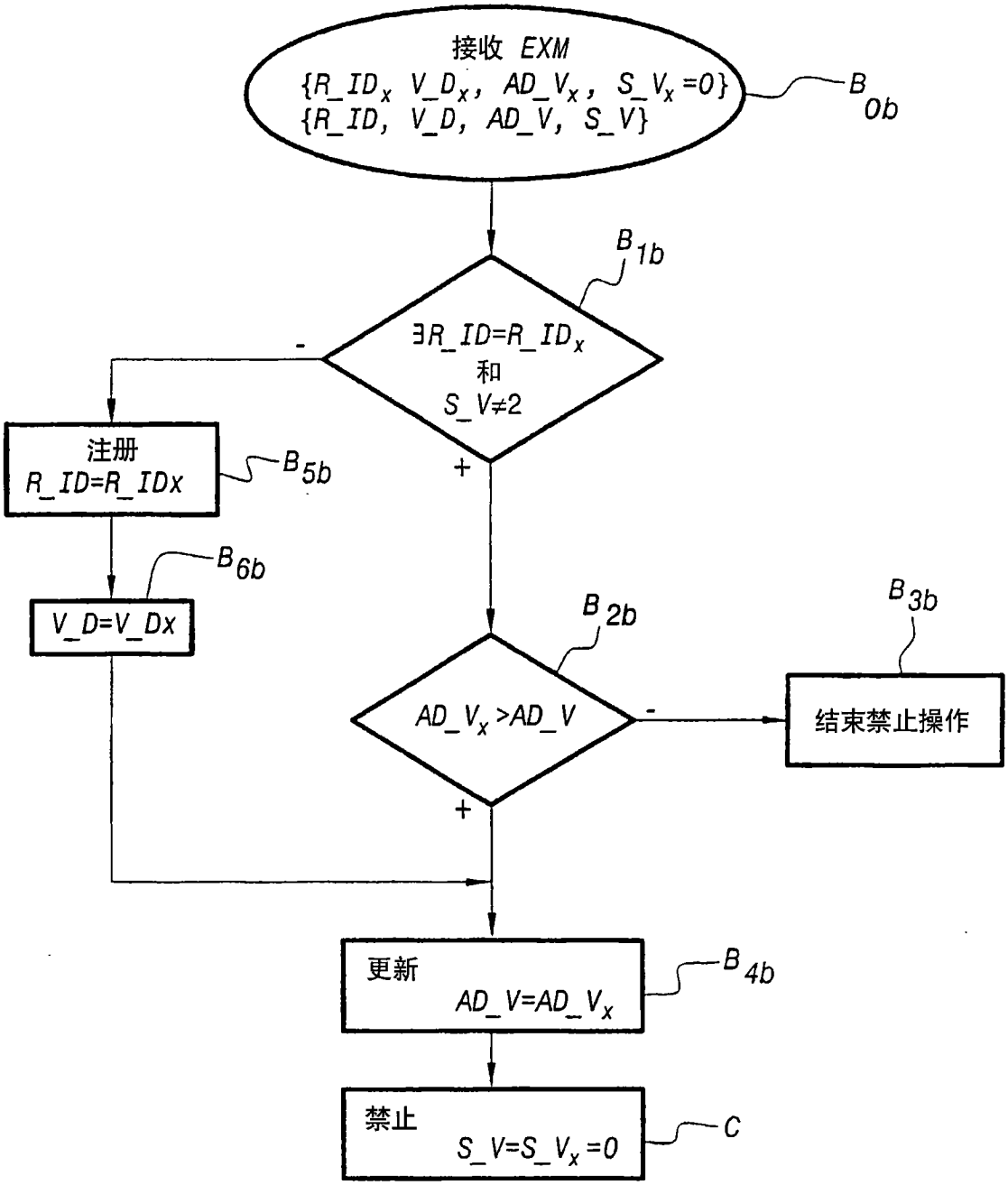

接收 EXM
{R_ID_x V_D_x, AD_V_x, S_V_x =0}
{R_ID, V_D, AD_V, S_V}
B 0b
B 1b
∃R_ID=R_ID_x
和
S_V≠2
-
+
注册
R_ID=R_IDx
B 5b
B 6b
V_D=V_Dx
B 2b
AD_V_x >AD_V
B 3b
结束禁止操作
更新
AD_V=AD_V_x
B 4b
禁止
S_V=S_V_x =0
C

图 2b 禁止一个权限

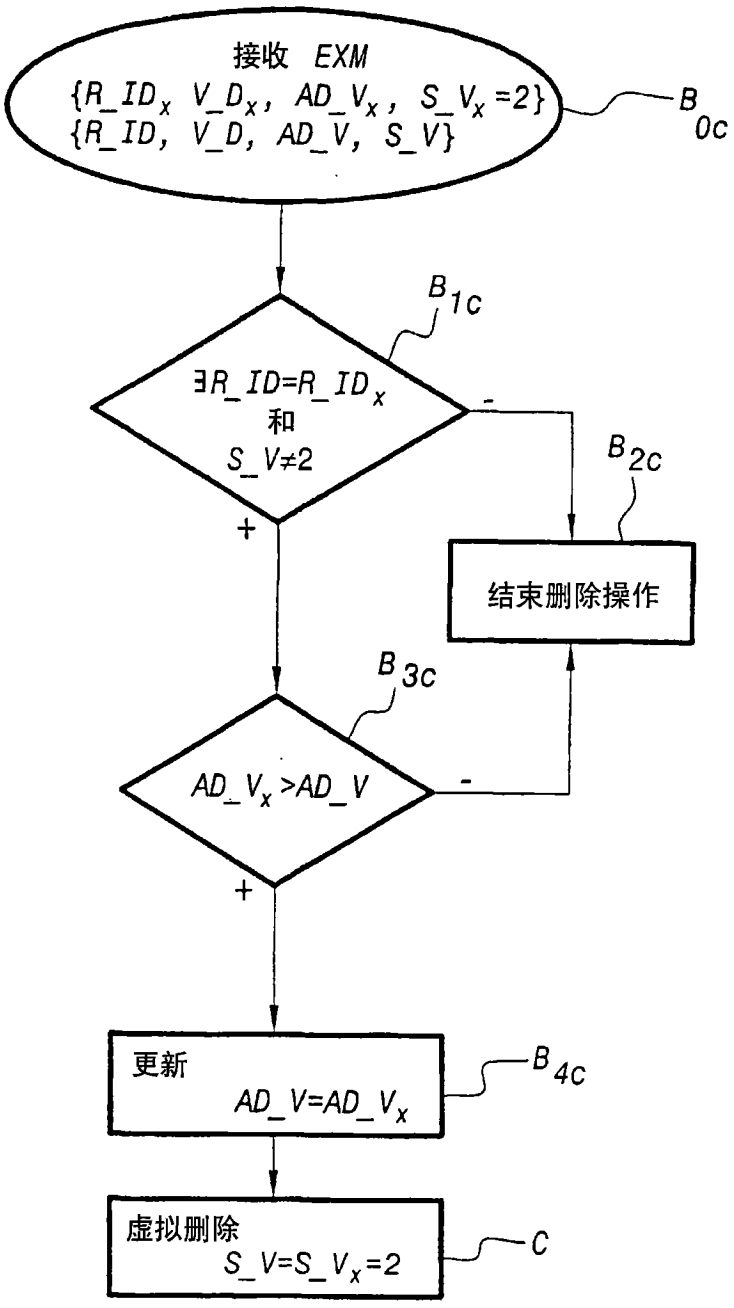


图 2c 虚拟删除一个权限

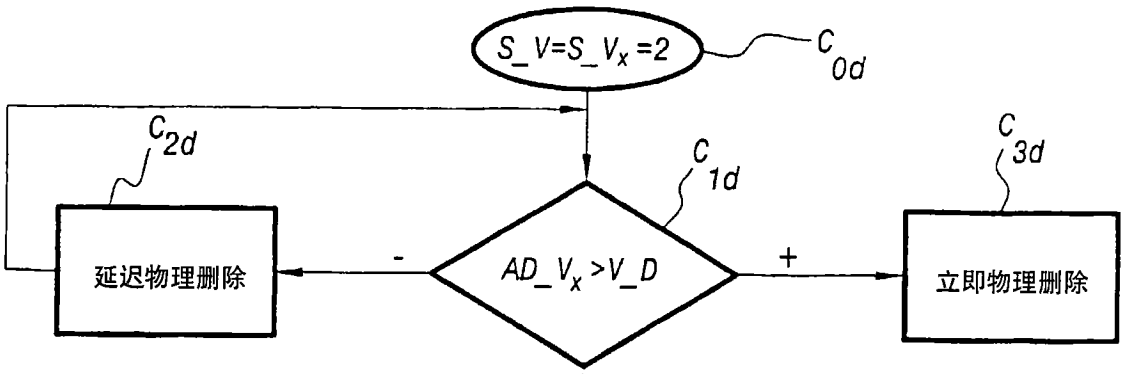


图 2d 物理删除

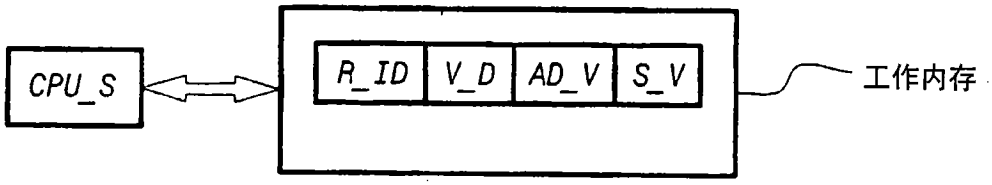


图 3a

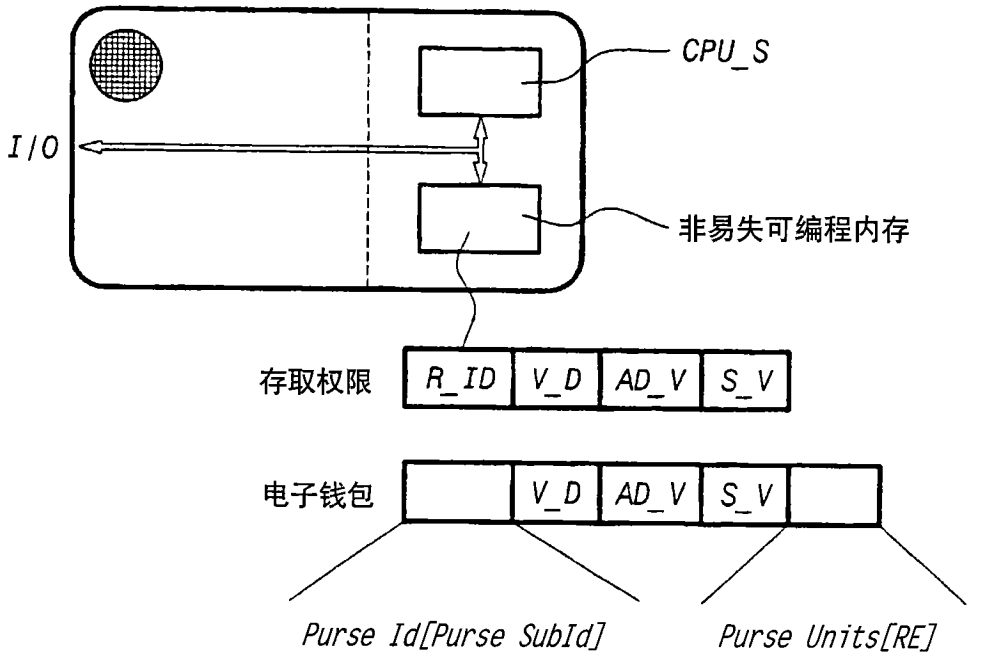


图 3b