(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 101819612 B
(45)授权公告日 2013.09.25

(21)申请号 200910211956.5
(22)申请日 2005.12.21
(30)优先权数据
60/638,804 2004.12.21 US
11/314,053 2005.12.20 US
11/314,052 2005.12.20 US
(62)分案原申请数据
200580048275.1 2005.12.21
(73)专利权人 桑迪士克科技公司
地址 美国德克萨斯州
(72)发明人 法布里斯·约刚-库仑
迈克尔·霍尔茨曼 巴赫曼·卡瓦米
罗恩·巴尔齐莱
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 刘国伟
(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/78(2013.01)
(56)对比文件
CN 1300068 A,2001.06.20, 全文.
EP 0919904 A2,1999.06.02, 全文.
EP 1467312 A1,2004.10.13, 全文.
审查员 徐淑娴

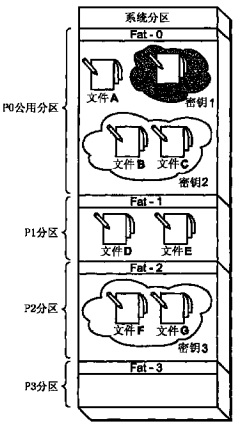
权利要求书2页 说明书22页 附图15页

(54)发明名称

具有分区的通用内容控制

(57)摘要

本发明涉及具有分区的通用内容控制。在一些移动存储装置中，通过将存储器划分为多个独立区域来提供内容保护，在所述独立区域中，存取受保护区域需要在先认证。尽管此特征提供某种保护，但其却不能保护免受通过非法途径获得口令的用户存取。因此，本发明的另一方面是基于以下认识的：可提供一种机制或结构来将存储器划分为多个分区，且使得所述分区中的至少一些数据可用密钥来加密，以使得除了存取某些所述分区所要求的认证之外，可能需要存取一个或一个以上密钥来解密此类分区中经加密的数据。在一些应用中，可更方便地使得用户能够通过使用一个应用程序来登录存储器系统，且接着能够使用不同应用程序来存取受保护内容而无需再次登录。在此类情况下，可将用户想要以此方式存取的所有内容与第一帐户进行关联，以使得可经由不同应用程序（例如，音乐播放器、电子邮件、蜂窝式通信等）来存取所有此类内容而无需多次登录。接着，可将不同组的认证信息用于进行登录，以存取在与所述第一帐户不同的账户中的受保护内容，即使所述不同帐户是针对相同用户或实体的。



CN 101819612 B

1. 一种供在存储装置上使用的安全存储方法，所述存储装置包括：非易失性存储器，其具有分区且含有包括认证证书和账户许可的账户；以及控制器，其与所述非易失性存储器通信，并存储将所述存储器划分为多个逻辑地址分区的结构，其中第一组的一个或多个分区中的数据可在无需认证的情况下存取，且第二组的一个或多个分区中的数据基本上仅可由经授权的实体存取，其中使用一个或多个密钥来加密所述第二组中的一个或多个所述分区中的数据；所述方法包括：

接收存取所述分区的请求，所述请求包括对话 ID，在实体被认证给所述账户之后，所述对话 ID 与所述账户许可相关联，其中在认证所述实体之前，所述存储装置存储所述账户许可；

使用包括在所述请求中的所述对话 ID 以在所述存储装置中查询与所述对话 ID 相关联的所述账户许可；

确定所述账户许可是否授权对存取所述分区的所述请求；如果所述账户许可授权对存取所述分区的所述请求，则授予对存取所述分区的所述请求。

2. 根据权利要求 1 所述的方法，其中所述存储器包括额外分区，且其中所述方法进一步包含许可经认证的实体存取在所述额外分区中的数据。

3. 根据权利要求 1 所述的方法，其中对所述分区的一种存取独立于用于将所述实体认证给所述账户的任何认证。

4. 根据权利要求 1 所述的方法，其中多个账户能被授权给对所述分区的一种存取。

5. 根据权利要求 1 所述的方法，其中关于所述账户的信息在认证阶段由所述控制器从所述非易失性存储器取出。

6. 根据权利要求 1 所述的方法，其中所述分区包括一个连续范围的地址。

7. 一种供在存储装置上使用的安全存储方法，所述存储装置包括：非易失性存储器，其具有分区且含有包括认证证书和账户许可的账户；以及控制器，其与所述非易失性存储器通信，并存储将所述存储器划分为多个逻辑地址分区的结构，其中第一组的一个或多个分区中的数据可在无需认证的情况下存取，且第二组的一个或多个分区中的数据基本上仅可由经授权的实体存取，其中使用一个或多个密钥来加密所述第二组中的一个或多个所述分区中的数据；所述方法包括：

无需认证而允许读取和写入中的一者存取所述非易失性存储器中的所述分区；

仅在实体被认证给所述账户之后允许对所述分区的所述读取和写入存取中的另一者，其间将认证对话 ID 提供给所述实体且其与所述账户许可相关联，其中在认证所述实体之前，所述存储装置存储所述账户许可，以及仅发生在以下之后：

接收执行对所述分区的所述读取和写入存取中的另一者的请求，所述请求包括所述对话 ID；

使用包括在所述请求中的所述对话 ID 以在所述存储装置中查询与所述对话 ID 相关联的所述账户许可；以及

确定所述账户许可是否授权对所述分区的所述读取和写入存取中的另一者。

8. 根据权利要求 7 所述的方法，其中基于至少一个其它账户来控制对所述分区的存取。

9. 根据权利要求 7 所述的方法，其中所述非易失性存储器包括至少一个额外分区。

10. 根据权利要求 7 所述的方法，其中所述账户包括存取控制记录。

11. 根据权利要求 7 所述的方法，其中关于所述账户的信息在认证阶段由所述控制器从所述存储器取出。

12. 根据权利要求 7 所述的方法，其中所述分区包括一个连续范围的地址。

具有分区的通用内容控制

[0001] 本申请是国际申请日为 2005 年 12 月 21 日，国际申请号为 PCT/US2005/046689，发明名称为“具有分区的通用内容控制”的 PCT 申请进入中国国家阶段申请号为 200580048275.1 的专利申请的分案申请。

技术领域

[0002] 本发明大体上涉及存储器系统，更明确地说，涉及一种具有通用内容控制特征的存储器系统。

背景技术

[0003] 计算装置市场正朝向在移动存储装置上包括内容存储以便通过产生较多数据交换来增加平均收入的方向发展。这意味着在将移动存储媒体中的内容用于计算装置上时需要保护所述内容。内容包括有价值的数据，此可为除了制造或出售所述存储装置的人之外的群体所拥有的数据。

[0004] 在第 6,457,126 号美国专利中描述一种具有加密能力的存储装置。然而，此装置所提供的能力非常有限。因此，需要提供一种具有较多通用内容控制特征的存储器系统。

发明内容

[0005] 移动存储媒体中的内容保护可涉及加密媒体中的数据，以使得仅授权用户或应用程序可存取用于加密存储在媒体中的数据的密钥。在一些现有系统中，用于加密和解密数据的密钥存储在移动存储媒体外部的装置中。在此类情况下，拥有内容所有权权益的公司或个人可能对媒体中内容的使用没有很多控制。由于用于加密媒体中数据的密钥存在于媒体外部，因而可用不受内容所有者控制的方式将此密钥从一个装置传递到另一个装置。根据本发明的一个特征，如果加密 - 解密密钥存储在媒体自身中且实质上不可由外部装置存取，那么所有者权益的拥有者将占据控制存取媒体中内容的较佳位置。

[0006] 通过使得基本上不可从媒体外部存取密钥，此特征对安全内容提供可携性。因此，含有以此类密钥来加密的安全内容的存储装置可用于由各种主机装置来存取，而没有破坏安全性的危险，因为所述装置具有对存取密钥的专有控制。只有那些具有适当证书的主机装置才能够存取所述密钥。

[0007] 为了增强存储在移动存储媒体中的内容的商业价值，需要内容所有权权益的拥有者能够将不同许可授权给不同实体以用于存取内容。因此，本发明的另一特征基于以下认识：可存储用于授权不同许可（例如，给不同经授权实体）以存取存储在媒体中的数据的存取策略。并入有所述两个上述特征的组合的系统尤其有利。一方面，内容拥有者或所有者具有通过使用实质上外部装置不可存取的密钥来控制存取内容的能力，且同时具有授权用于存取媒体中内容的不同许可的能力。因此，即使在外部装置获得存取的情况下，其存取仍可受记录在存储媒体中的由内容拥有者或所有者设定的不同许可支配。

[0008] 又一特征基于以下认识：当在快闪存取器中实施上述策略（其中将不同许可授权

给不同经授权实体）时，这导致对内容保护尤其有用的媒体。

[0009] 许多存储装置不知道文件系统，而许多计算机主机装置以文件形式读取和写入数据。根据另一特征，主机装置提供密钥参考或 ID，而存储器系统作为响应产生与所述密钥 ID 相关联的密钥值，其中所述密钥值用于密码处理与所述密钥 ID 相关联的文件中的数据。主机将所述密钥 ID 与待由存储器系统密码处理的文件进行关联。因此，密钥 ID 由计算装置和存储器用作句柄，存储器通过所述句柄保持对用于密码处理的密钥值的产生和使用的完全且专有控制，而主机保持对文件的控制。

[0010] 在例如智能卡的一些移动存储装置中，卡控制器管理文件系统。在例如快闪存储器、磁碟或光碟的许多其它类型的移动存储装置中，装置控制器不知道文件系统；而是，装置控制器依赖主机装置（例如，个人计算机、数码相机、MP3 播放器、个人数字助理、蜂窝式电话）来管理文件系统。本发明的各种方面可容易地并入到此些类型的存储装置中，其中所述装置不知道文件系统。这意味着可在各种各样的现有移动存储装置上实践本发明的各种特征而无需重新设计此类装置来使得此类装置中的装置控制器变得知道且能够管理文件系统。

[0011] 存储媒体中所存储的树结构提供对于实体在恰好获得存取之后可进行什么的控制。树的每个节点指定对于已通过树的此节点获得入口的实体的许可。一些树具有不同等级，其中在树的一节点处的一个或多个许可与在同一树中较高或较低或相同等级的另一节点处的一个或多个许可具有预定关系。通过要求实体遵守在每个节点处如此指定的许可，此应用程序的树特征允许内容拥有者控制哪些实体可采取行动和每个实体可采取哪些行动，这与树是否具有不同等级无关。

[0012] 为了增强可由移动存储媒体提供的商业价值，需要移动存储装置能够同时支持一个以上应用程序。当两个或两个以上应用程序正同时存取移动存储装置时，可能重要的是能够分离所述两个或两个以上应用程序的操作，以使得其不会以本文称为串话的现象而彼此干扰。因此，本发明的另一特征基于以下认识：可提供优选地为分级的两个或两个以上树以用于控制存取存储器。每个树在不同等级包含节点以用于控制相应组实体对数据的存取，其中每个树的节点指定所述一个或多个相应实体用于存取存储器数据的一个或多个许可。在每个树的节点处的所述一个或多个许可与在同一树中较高或较低等级的另一节点处的一个或多个许可具有预定关系。优选地，在所述树的至少两者之间不存在串话。

[0013] 根据上文，将显然看到树是可用于内容安全性的强有力结构。所提供的一个重要控制是控制树的创建。因此，根据本发明的另一特征，移动存储装置可具备能够创建至少一个分级树（其在不同等级处包含节点以用于由相应实体控制存取存储在存储器中的数据）的系统代理。树的每个节点指定一个或多个相应实体用于存取存储器数据的一个或多个许可。在每个树的节点处的所述一个或多个许可与在同一树中较高或较低或相同等级的节点处的一个或多个许可具有预定关系。因此，可在尚未创建任何树的情况下发行移动存储装置，以使得装置的购买者可以自由地创建分级树，所述分级树适用于购买者所考虑的应用程序。或者，可在已创建树的情况下发行移动存储装置，以使得购买者不必经历创建树的麻烦。在这两种情况下，优选地，树的特定功能性在装置制成之后变得固定，以使得不能进一步改变或修改所述功能性。这提供内容拥有者对装置中内容存取的较强控制。因此，在一个实施例中，可优选地禁用系统代理，以使得不会创建额外的树。

[0014] 在一些移动存储装置中，通过将存储器划分为多个独立区域来提供内容保护，其中存取受保护区域要求在先认证。尽管此特征提供某种保护，但其不能保护以免通过非法途径获得口令的用户存取。因此，本发明的另一方面基于以下认识：可提供一种机制或结构来将存储器划分为多个分区，且使得所述分区中的至少某些数据可用密钥来加密，以使得除了存取某些所述分区所需要的认证之外，可能需要存取一个或一个以上密钥来解密此类分区中经加密的数据。

[0015] 在一些应用中，可更方便地使得用户能够使用一个应用程序登录存储器系统，且接着能够使用不同应用程序来存取受保护内容而无需再次登录。在此类情况下，用户想要以此方式存取的所有内容可与第一帐户相关联，以使得可经由不同应用程序（例如，音乐播放器、电子邮件、蜂窝式通信）来存取所有此类内容而无需多次登录。接着可将不同组认证信息用于登录以存取在与第一帐户不同的帐户中的受保护内容，即使所述不同帐户是针对相同用户或实体的。

[0016] 在存储系统中可单独使用上述特征或可以任何组合来组合上述特征，以提供内容拥有者的控制和 / 或保护的较强通用性。

附图说明

[0017] 图 1 是可用于说明本发明的与主机装置通信的存储器系统的方框图。

[0018] 图 2 是存储器的不同分区和存储在不同分区中的未加密和加密文件的示意图，其中存取特定分区和加密文件由存取策略和认证程序控制，所述示意图用以说明本发明的实施例。

[0019] 图 3 是说明存储器中不同分区的存储器的示意图。

[0020] 图 4 是用于图 3 所示的存储器的不同分区的文件位置表的示意图，其中所述分区中的某些文件经加密以说明本发明的实施例。

[0021] 图 5 是存取受控记录群组中的存取控制记录和相关联密钥参考的示意图，其用以说明本发明的实施例。

[0022] 图 6 是由存取受控记录群组和存取受控记录形成的树结构的示意图，其用于说明本发明的实施例。

[0023] 图 7 是说明存取受控记录群组的三个分级树的树的示意图，其用以说明所述树的形成过程。

[0024] 图 8A 和 8B 是说明由主机装置和存储器装置（例如，用于创建和使用系统存取控制记录的存储卡）执行的过程的流程图。

[0025] 图 9 是说明使用系统存取控制记录来创建存取受控记录群组的过程的流程图，其用以说明本发明。

[0026] 图 10 是说明用于创建存取控制记录的过程的流程图。

[0027] 图 11 是可用于说明分级树的特定应用程序的两个存取控制记录群组的示意图。

[0028] 图 12 是说明用于授权特定权利的过程的流程图。

[0029] 图 13 是存取受控记录群组和存取控制记录的示意图，其用以说明图 12 的授权过程。

[0030] 图 14 是说明用于创建用于加密和 / 或解密目的的密钥的过程的流程图。

[0031] 图 15 是说明用于根据存取受控记录来取消存取权利和 / 或针对数据存取的许可的过程的流程图。

[0032] 图 16 是说明当存取权利和 / 或存取许可已被删除或已期满时请求存取的过程的流程图。

[0033] 图 17A 和图 17B 是说明用于认证的规则结构和用于授权存取密码密钥的策略的组织的示意图，其用以说明本发明的另一实施例。

[0034] 图 18 是说明当打开一些对话时认证和存取对话的流程图。

[0035] 图 19-22 是说明不同认证过程的流程图。

[0036] 为了简化说明，在此申请案中，用相同数字标注相同元件。

具体实施方式

[0037] 图 1 的方框图说明其中可实施本发明各种方面的实例性存储器系统。如图 1 所示，存储器系统 10 包括中央处理单元 (CPU)12、缓冲器管理单元 (BMU)14、主机接口模块 (HIM)16 和快闪接口模块 (FIM)18、快闪存储器 20 和外围存取模块 (PAM)22。存储器系统 10 通过主机接口总线 26 和端口 26a 与主机装置 24 通信。可以是 NAND 类型的快闪存储器 20 为主机装置 24 提供数据存储。也可将 CPU 12 的软件代码存储在快闪存储器 20 中。FIM 18 通过快闪接口总线 28 和端口 28a 连接到快闪存储器 20。HIM16 适于连接到例如数码相机、个人计算机、个人数字助理 (PDA)、数字媒体播放器、MP-3 播放器、蜂窝式电话或其它数字装置的主机系统。外围存取模块 22 选择例如 FIM、HIM 和 BMU 的适当控制器模块以用于与 CPU 12 通信。在一个实施例中，可将虚线框内的系统 10 的所有元件装入例如存储卡或棒 10’ 的单个单元中且优选地将其密封。

[0038] 尽管本文参考快闪存储器来说明本发明，但本发明也可适用于其它类型的存储器，例如磁碟、光学 CD 以及其它类型的可重写非易失性存储器系统。

[0039] 缓冲器管理单元 14 包括主机直接存储器存取 (HDMA)32、快闪直接存储器存取 (FDMA)34、仲裁器 36、缓冲器随机存取存储器 (BRAM)38 和密码引擎 40。仲裁器 36 是共享总线仲裁器，以使得仅一个主导装置或启动器 (其可以是 HDMA 32、FDMA34 或 CPU 12) 可在任何时间起作用，且从属装置或目标装置是 BRAM 38。仲裁器负责将适当启动器请求引导到 BRAM 38。HDMA 32 和 FDMA 34 负责在 HIM 16、FIM 18 与 BRAM 38 或 CPU 随机存取存储器 (CPU RAM)12a 之间传送的数据。HDMA 32 和 FDMA34 的操作是常规的，且不需要在本文详细描述。BRAM 38 用于存储在主机装置 24 与快闪存储器 20 之间传递的数据。HDMA 32 和 FDMA 34 负责在 HIM 16/FIM 18 与 BRAM 38 或 CPU RAM 12a 之间传送数据且指示扇区完成。

[0040] 针对存储在存储器 20 中的内容的改进安全性，存储器系统 10 产生用于加密和 / 或解密的密钥值，其中此值实质上不可由例如主机装置 24 的外部装置存取。然而，通常逐个文件地进行加密和解密，因为主机装置以文件的形式读取数据和将数据写入存储器系统 10。如同许多其它类型的存储装置，存储器装置 10 不知道文件或文件系统。尽管存储器 20 存储其中识别文件的逻辑地址的文件分配表 (FAT)，但所述 FAT 通常由主机装置 24 而并非由控制器 12 存取和管理。因此，为了加密特定文件中的数据，控制器 12 将必须依赖主机装置来发送存储器 20 中的文件中的数据的逻辑地址，以使得可由系统 10 找到特定文件的数据并使用仅系统 10 可获得的密钥值对其进行加密和 / 或解密。

[0041] 为了为主机装置 24 和存储器系统 10 两者提供句柄以参考用于密码地处理文件中的数据的相同密钥，主机装置提供针对由系统 10 产生的每个密钥值的参考，其中此参考可简单地是密钥 ID。因此，主机 24 将由系统 10 密码地处理的每个文件与密钥 ID 进行关联，且系统 10 将用于密码地处理数据的每个密钥值与由主机提供的密钥 ID 进行关联。因此，当主机请求密码地处理文件时，其将把具有密钥 ID 的请求连同待从存储器 20 取出或存储在存储器 20 中的数据的逻辑地址发送到系统 10。系统 10 产生密钥值，并将由主机 24 提供的密钥 ID 与此值进行关联，且执行密码处理。以此方式，不需要对存储器系统 10 操作且同时允许其使用密钥完全控制加密处理（包括对密钥值的专有存取）的方式作出改变。换句话说，系统 10 继续允许主机 24 通过具有对 FAT 的专有控制来管理文件，而其维持对产生和管理用于密码处理的密钥值的专有控制。主机装置 24 不参与产生和管理用于数据的密码处理的密钥值。

[0042] 由主机 24 提供的密钥 ID 和由存储器系统产生的密钥值形成两个数量属性，下文在一个实施例中称为“内容加密密钥”或 CEK。尽管主机 24 可将每个密钥 ID 与一个或一个以上文件进行关联，但主机 24 也可将每个密钥 ID 与未组织数据或以任何方式组织的数据（且不限于组织成完整文件的数据）进行关联。

[0043] 为了使用户或应用程序能够存取系统 10 中的受保护内容或区域，将需要使用预先向系统 10 注册的证书来认证。证书与以此证书授予特定用户或应用程序的存取权利绑定。在预先注册过程中，系统 10 存储身份记录和用户或应用程序的证书以及与由用户或应用程序确定且通过主机 24 提供的此识别和证书相关联的存取权利。在完成预先注册过程之后，当用户或应用程序请求将数据写入存储器 20 时，将需要通过主机装置提供其身份和证书、用于加密数据的密钥 ID 和将存储已加密数据的逻辑地址。系统 10 产生密钥值，且将此值与由主机装置提供的密钥 ID 进行关联，且将用于加密待写入数据的密钥值的密钥 ID 存储在其针对此用户或应用程序的记录或表中。其随后加密数据且将已加密数据存储在由主机指定的地址处，以及存储其产生的密钥值。

[0044] 当用户或应用程序请求从存储器 20 读取已加密数据时，其将需要提供其身份和证书、先前用于加密所请求数据的密钥的密钥 ID 和存储已加密数据的逻辑地址。系统 10 接着将由主机提供的用户或应用程序身份和证书与存储在其记录中的那些进行匹配。如果它们匹配，那么系统 10 接着将从其存储器取出与由用户或应用程序提供的密钥 ID 相关联的密钥值，使用密钥值来解密存储在由主机装置指定的地址处的数据，且将已解密数据发送到用户或应用程序。

[0045] 通过将认证证书与用于密码处理的密钥管理分离，接着能够在不共享证书的情况下共享存取数据的权利。因此，具有不同证书的一群组用户或应用程序可存取用于存取相同数据的相同密钥，而此群组之外的用户不能存取。虽然一群组内的所有用户或应用程序可存取相同数据，但是其仍可具有不同权利。因此，一些可具有只读存取，而其它可具有只写存取，而另一些可具有两者。因为系统 10 维持用户或应用程序身份和证书、其可存取的密钥 ID 和针对每个密钥 ID 的相关联存取权利的记录，因而系统 10 能够增加或删除密钥 ID 且改变针对特定用户或应用程序的与这些密钥 ID 相关联的存取权利、使存取权利在用户或应用程序之间彼此授权、或甚至删除或增加针对用户或应用程序的记录或表，这所有动作均由适当认证的主机装置来控制。所存储的记录可指定需要安全通道来存取特定密钥。

可使用对称或不对称算法以及口令来进行认证。

[0046] 尤其重要的是存储器系统 10 中的安全内容的可携性。由于密钥值是由存储器系统产生的且实质上外部系统不可获得，因而当将存储器系统或并入有所述系统的存储装置从一个外部系统转移到另一者时，存储在其中的内容的安全得以维护，且外部系统不能存取此内容，除非其已经被以完全由存储器系统控制的方式认证。即使在如此认证之后，存取也完全由存储器系统控制，且外部系统仅可以根据存储器系统中的预设记录控制的方式来存取。如果请求不遵守这些记录，那么将拒绝请求。

[0047] 为了在保护内容时提供较大灵活性，构思仅可由经适当认证的用户或应用程序存取存储器的以下称为分区的某些区域。当与以基于密钥的数据加密的上述特征组合时，系统 10 提供较大数据保护能力。如图 2 所示的本发明的 SanDisk 新一代卡的实施例，快闪存储器 20 可将其存储能力划分为若干分区 :用户区域或分区和定制分区。用户区域或分区 P0 可在无需认证的情况下由所有用户和应用程序存取。尽管可由任何应用程序或用户读取或写入存储在用户区域中的数据的所有位值，但如果数据读取被加密，那么没有解密权限的用户或应用程序将不能存取由存储在用户区域中的位值所表示的信息。这通过（例如）存储在用户区域 P0 中的文件 102 和 104 说明。同样存储在用户区域中的还有未加密文件（例如 106），其可由所有应用程序和用户读取和理解。因此，以符号表示的方式，用与例如文件 102 和 104 的文件相关联的闭锁来展示已加密的文件。

[0048] 尽管未经授权的应用程序或用户不能理解用户区域 P0 中的加密文件，但是这些应用程序或用户仍可能够删除或破坏文件，这可对于一些应用程序来说是不良的。为此目的，存储器 20 也可包括例如分区 P1 和 P2 的受保护定制分区，所述分区不能在无先前认证的情况下进行存取。下文解释此申请案的实施例中所允许的认证过程。

[0049] 同样如图 2 说明，多种用户或应用程序可存取存储器 20 中的文件。因此，图 2 中展示用户 1 和 2 以及应用程序 1 到 4（在装置上运行）。在允许这些实体存取存储器 20 中的受保护内容之前，这些实体首先由认证过程用下文解释的方式来认证。在此过程中，需要在主机侧识别请求存取的实体以进行基于任务的存取控制。因此，请求存取的实体首先通过提供例如“我是应用程序 2 且我想要读取文件 1”的信息来自我识别。控制器 12 接着将身份、认证信息和请求与存储在存储器 20 或控制器 12 中的记录进行匹配。如果满足所有要求，那么接着对此实体授权存取。如图 2 说明，允许用户 1 从分区 P1 中的文件 101 读取或写入到文件 101，但是除了用户 1 具有无限制权利来从 P0 中的文件 106 读取和写入到文件 106 之外，仅可读取文件 102 和 104。另一方面，不允许用户 2 存取文件 101 和 104，但用户 2 能够读取和写入文件 102。如图 2 指示，用户 1 和 2 具有相同登录算法 (AES)，而应用程序 1 和 3 具有不同登录算法（例如，RSA 和 001001），这些算法也不同于用户 1 和 2 的那些算法。

[0050] 安全存储应用程序 (SSA) 是存储器系统 10 的安全性应用程序，且说明本发明的可用于实施许多上述特征的实施例。可用存储器 20 或 CPU 12 中的非易失性存储器（未图示）中所存储的数据库来将 SSA 实施为软件或计算机代码，且将其读取到 RAM 12a 中并由 CPU 12 执行。在下表中阐述关于 SSA 而使用的首字母缩写 :

[0051] 定义、首字母缩写 & 缩略语

[0052]

ACR	存取控制记录
AGP	ACR 群组
CBC	链式区块密码
CEK	内容加密密钥
ECB	电子密码本
ACAM	ACR 属性管理
PCR	许可控制记录
SSA	安全存储应用程序
实体	具有登录 SSA 且因此利用其功能性的真实且单独存在（主机侧）的任何事物

[0053] SSA 系统描述

[0054] 数据安全性、完整性和存取控制是 SSA 的主要任务。所述数据是原本将简单地存储在某类型的大容量存储装置上的文件。SSA 系统位于存储系统上且增加用于所存储的主机文件的安全层。

[0055] SSA 的主要任务是管理与存储器中的所存储（且安全）内容相关联的不同权利。存储器应用程序需要管理多个用户和内容权利以成倍增加所存储的内容。来自其侧的主机应用程序看见此类应用程序可见的驱动器和分区以及管理并描绘存储装置上的所存储文件的位置的文件分配表 (FAT)。

[0056] 在此情况下，存储装置使用划分为多个分区的 NAND 快闪芯片，但也可使用其它移动存储装置且这些其它装置属于本发明范围内。这些分区是逻辑地址的连续线程，其中开始和结束地址界定其边界。因此，如果需要的话，可对隐藏分区的存取加上限制，这借助于将此类限制与此类边界内的地址进行关联的软件（例如，存储在存储器 20 中的软件）来进行。分区可完全由 SSA 通过其逻辑地址边界（由 SSA 管理）来识别。SSA 系统使用分区来在实体上保护数据免受未授权的主机应用程序存取。对于主机，分区是界定存储数据文件的所有权空间的机制。这些分区可以是共享的，其中存取存储装置的任何人可以看见且知道装置上分区的存在，或者这些分区可为私有的或隐藏的，其中仅选定的主机应用程序可存取且知道存储装置中分区的存在。

[0057] 图 3 是说明存储器的分区 P0、P1、P2 和 P3（明显地，可采用少于或多于四个分区）的存储器的示意图，其中 P0 是可由任何实体在无需认证的情况下存取的公用分区。

[0058] 私有分区（例如 P1、P2 或 P3）隐藏对其内的文件的存取。通过防止主机存取所述分区，快闪装置（例如，快闪卡）提供对分区内的数据文件的保护。然而，此种保护通过对存取存储在所述分区内的逻辑地址处的数据加以限制来吞没驻存在隐藏分区中的所有文件。换句话说，所述限制与一个范围的逻辑地址相关联。能够存取所述分区的所有用户 / 主机将能无限制地存取其内部的所有文件。为了将不同文件 - 或文件群组 - 彼此隔离，SSA 系

统使用密钥和密钥参考或密钥 ID 对每个文件 - 或文件群组 - 提供另一等级的安全性和完整性。可将用于加密在不同存取器地址处的数据的特定密钥值的密钥参考或密钥 ID 比喻为含有已加密数据的容器或领域。鉴于此原因，在图 4 中，将密钥参考或密钥 ID（例如，“密钥 1”和密钥“2”）以图形方式展示为使用与密钥 ID 相关联的密钥值加密的文件周围的区域。

[0059] 参看图 4，举例来说，文件 A 可由所有实体存取而无需任何认证，因为文件 A 经展示为未由任何密钥 ID 包围。即使公用分区中的文件 B 可由所有实体读取或重写，文件 B 也含有用具有 ID“密钥 1”的密钥来加密的数据，以使得文件 B 中所含有的信息不可由实体存取，除非此实体能存取此密钥。以此方式，使用密钥值和密钥参考或密钥 ID 仅提供逻辑保护，这与由上述分区所提供的保护类型相反。因此，可存取分区（公用或私有）的任何主机能够读取或写入整个分区中的数据，包括经加密的数据。然而，由于数据被加密，因而未经授权的用户仅可将其破坏。其优选地不能在没有检测的情况下改变数据或使用数据。通过限制对加密和 / 或解密密钥的存取，此特征可仅允许经授权的实体使用数据。也可使用 PO 中具有密钥 ID “密钥 2”的密钥来加密文件 B 和 C。

[0060] 可通过使用内容加密密钥 (CEK) 的对称加密方法（每个 CEK 对应一种方法）来提供数据机密性和完整性。在 SSA 实施例中，通过仅内部使用的快闪装置（例如，快闪卡）来产生 CEK，且将 CEK 保持为不为外界所知的秘密。经加密或密码化的数据也可被散列或者密码被链式组块，以确保数据完整性。

[0061] 并非分区中的所有数据均由不同密钥来加密且与不同密钥 ID 相关联。公用或用户文件中或操作系统区域（即，FAT）中的某些逻辑地址可以不与任何密钥或密钥参考相关联，且因此可由自身可存取所述分区的任何实体获得。

[0062] 要求获得创建密钥和分区以及将数据写入分区或从分区读取数据或使用密钥的能力的实体需要通过存取控制记录 (ACR) 登录 SSA 系统。SSA 系统中的 ACR 的特权被称为动作。每个 ACR 可具有用以执行以下三个种类的动作的许可 ：创建分区和密钥 / 密钥 ID、存取分区和密钥以及创建 / 更新其它 ACR。

[0063] ACR 被组织成称为 ACR 群组或 AGP 的群组。一旦已成功认证 ACR，SSA 系统便打开对话，通过所述对话可执行任何 ACR 动作。

[0064] 用户分区

[0065] SSA 系统管理一个或一个以上公用分区（也称为用户分区）。此分区存在于存储装置上，且是可通过存储装置的标准读取写入命令存取的分区。获得关于分区大小以及其存在于装置上的信息优选地不能向主机系统隐藏。

[0066] SSA 系统使得能够通过标准读取写入命令或 SSA 命令来存取此（些）分区。因此，存取分区优选地不能只限于特定 ACR。然而，SSA 系统可使得主机装置能够限制对用户分区的存取。可单独启用 / 禁用读取和写入存取。允许所有四个组合（例如，只写、只读（写入保护）、读取和写入以及无存取）。

[0067] SSA 系统使得 ACR 能够将密钥 ID 与用户分区内的文件进行关联并使用与这些密钥 ID 相关联的密钥来加密各个文件。将使用 SSA 命令组（关于 SSA 命令的详细描述请参考附录 A——在附录中，密钥 ID 称为“领域”）来进行存取用户分区内的加密文件以及设定对所述分区的存取权利。以上特征也适用于未经组织成文件的数据。

[0068] SSA 分区

[0069] 这些是可仅通过 SSA 命令来存取的隐藏（向主机操作系统或 OS 隐藏）分区。除了通过由登录到 ACR 而建立的对话（下文描述）外，SSA 系统将优选地不允许主机装置存取 SSA 分区。类似地，SSA 优选地将不提供关于 SSA 分区的存在、大小和存取许可的信息，除非此请求从所建立的对话传出。

[0070] 从 ACR 许可中导出对分区的存取权利。一旦 ACR 登录到 SSA 系统中，其便可与其它 ACR（下文描述）共享分区。当创建分区时，主机提供用于所述分区的参考名称或 ID（例如，图 3 和 4 中的 P0-P3）。此参考用于对所述分区的进一步读取和写入命令。

[0071] 存储装置的分区

[0072] 优选地，将装置的所有可用存储容量分配给用户分区和当前配置的 SSA 分区。因此，任何重新分区操作可涉及对现有分区的重新配置。装置容量（所有分区的大小总和）的净改变将为零。通过主机系统来界定装置存储空间中的分区的 ID。

[0073] 主机系统可将一个现有分区重新分区为两个较小分区，或将两个现有分区（可以是相邻或不相邻的）合并为一个。由主机决定，可擦除经划分或合并分区中的数据或使其未受影响。

[0074] 由于存储装置的重新分区可造成数据损失（或者因为其在存储装置的逻辑地址空间中被擦除或四处移动），因而由 SSA 系统管理对于重新分区的严格限制。仅允许驻留在根 AGP（下文解释）的 ACR 发出重新分区命令且其仅可参考其拥有的分区。由于 SSA 系统不知道如何将数据组织成分区 (FAT 或其它文件系统结构)，因而主机负责在对装置进行重新分区的任何时候重建这些结构。

[0075] 用户分区的重新分区将改变主机 OS 所看见的此分区的大小和其它属性。

[0076] 在重新分区之后，主机系统负责确保 SSA 系统中的任何 ACR 不参考非现有分区。如果这些 ACR 未被适当删除或更新，那么将由系统检测和拒绝存取非现有分区的未来努力（以这些 ACR 的名义）。对于已删除密钥和密钥 ID，采用类似照管。

[0077] 密钥、密钥 ID 和逻辑保护

[0078] 当将文件写入到特定隐藏分区时，将其向公众隐藏。但是，一旦实体（敌对或非敌对的）获得对此分区的认识和存取，文件便变得可用且易于看见。为了进一步保护文件，SSA 可在隐藏分区中对其加密，其中用于存取用于解密文件的密钥的证书优选地不同于用于存取所述分区的那些证书。由于文件不为 SSA 所知（由主机完全控制和管理）的事实，将 CEK 与文件进行关联是一个问题。将文件链接到 SSA 知道的某事物 - 密钥 ID- 对此进行调整。因此，当由 SSA 创建密钥时，主机将用于此密钥的密钥 ID 与使用由 SSA 创建的密钥来加密的数据进行关联。

[0079] 密钥值和密钥 ID 提供逻辑安全性。使用相同内容加密密钥 (CEK)（其参考名称或密钥 ID 在创建时由主机应用程序唯一提供）来加密与给定密钥 ID 相关联的所有数据，而不管其位置如何。如果实体获得对隐藏分区的存取（经由通过 ACR 认证），且希望读取或写入此分区内的加密文件，那么其需要能够存取与文件相关联的密钥 ID。当授权存取针对此密钥 ID 的密钥时，SSA 加载与此密钥 ID 相关联的 CEK 中的密钥值，且在将数据发送到主机之前将其解密或在将数据写入到快闪存储器 20 之前将其加密。与密钥 ID 相关联的 CEK 中的密钥值由 SSA 系统随机创建一次且接着由其维护。SSA 系统外部没有装置知道或存取

CEK 中的此密钥值。外界仅提供和使用参考或密钥 ID，而并非 CEK 中的密钥值。密钥值由 SSA 完全管理且仅可由 SSA 存取。

[0080] SSA 系统使用以下加密模式中的任何一者来保护与密钥 ID 相关联的数据（所使用的实际密码算法以及 CEK 中的密钥值受系统控制且不向外界展现）：

[0081] 块模式 - 将数据划分为块，分别对其每一者进行加密。通常认为此模式较不安全且易受字典攻击。然而，其将允许用户随机存取数据块中的任何一者。

[0082] 链模式 - 将数据划分为块，其在加密过程中被链接。将每个块用作下个块的加密过程的一个输入。尽管认为此模式较安全，但此模式要求从开始到结束总是按序写入和读取数据，从而造成总是不为用户接受的额外开销。

[0083] 散列 - 具有可用于验证数据完整性的数据摘要的额外创建的链模式

[0084] ACR 和存取控制

[0085] SSA 经设计以处理多个应用程序，其中将每个应用程序表示为系统数据库中的节点树。通过确保树分枝之间没有串话来实现应用程序之间的相互排斥。

[0086] 为了获得对 SSA 系统的存取，实体需要经由系统 ACR 中的一者来建立连接。由 SSA 系统根据嵌入在用户选择与其连接的 ACR 中的定义来管理登录程序。

[0087] ACR 是到 SSA 系统的各个登录点。ACR 持有登录证书和认证方法。同样驻存在记录中的还有 SSA 系统内的登录许可，在所述许可当中是读取和写入特权。这在图 5 中说明，图 5 说明相同 AGP 中的 n 个 ACR。这意味着所述 n 个 ACR 中至少一些可共享对相同密钥的存取。因此，ACR#1 和 ACR#n 共享对具有密钥 ID“密钥 3”的密钥的存取，其中 ACR#1 和 ACR#n 是 ACR ID，且“密钥 3”是针对用于加密与“密钥 3”相关联的数据的密钥的密钥 ID。也可使用相同密钥来加密和 / 或解密多个文件或多组数据。

[0088] SSA 系统支持若干类型的到系统的登录，其中认证算法和用户证书可发生变化，同样一旦用户成功登录其在系统中的特权也可变化。图 5 再次说明不同登录算法和证书。ACR#1 要求口令登录算法和口令作为证书，而 ACR#2 要求 PKI（公用密钥基础结构）登录算法和公用密钥作为证书。因此，为了登录，实体将需要出示有效 ACR ID 以及正确的登录算法和证书。

[0089] 一旦实体登录到 SSA 系统的 ACR 中，便在与 ACR 相关联的许可控制记录 (PCR) 中定义其许可（其使用 SSA 命令的权利）。在图 5 中，根据所展示的 PCR，ACR#1 对与“密钥 3”相关联的数据授予只读许可，且 ACR#2 对与“密钥 5”相关联的数据授予读取和写入许可。

[0090] 不同 ACR 可共享系统中（例如，用来进行读取和写入的密钥中）的共同权益和特权。为了实现此目的，将具有共同处的 ACR 分组为 AGP(ACP 群组）。因此，ACR#1 和 ACR#n 共享对具有密钥 ID“密钥 3”的密钥的存取。

[0091] 以分级树来组织 AGP 和其内的 ACR，且因此除了创建保持敏感数据安全的安全密钥之外 ;ACR 可优选地还创建对应于其密钥 ID/ 分区的其它 ACR 实体。这些 ACR 子代将具有与其父代（创建者）相同或比其少的许可，且可被给予针对父代 ACR 自身创建的密钥的许可。不用说，子代 ACR 获得对其创建的任何密钥的存取许可。这在图 6 中说明。因此，AGP 120 中的所有 ACR 由 ACR 122 创建，且两个此类 ACR 从 ACR 122 处继承对与“密钥 3”相关联的数据的存取的许可。

[0092] AGP

[0093] 通过指定 AGP 和 AGP 内的 ACR 来登录到 SSA 系统上。

[0094] 每个 AGP 具有唯一 ID（参考名称），其用作其在 SSA 数据库中的入口的索引。当创建 AGP 时，向 SSA 系统提供 AGP 名称。如果所提供的 AGP 名称已经存在于系统中，那么 SSA 将拒绝创建操作。

[0095] 使用 AGP 来管理对于授权存取和管理许可的限制，如将在以下部分中描述。由图 6 中的两个树提供的功能之一是管理由完全分离的实体（例如两个不同应用程序或两个不同计算机用户）的存取。出于此类目的，其对于实质上彼此独立（即，实质上无串话）的两个存取过程来说是重要的，即使两个过程同时发生。这意味着每个树中的认证、许可以及额外 ACR 和 AGP 的创建未连接到其它树的那些且不依赖于其它树的那些。因此，当在存储器 10 中使用 SSA 系统时，这允许存储器系统 10 同时服务多个应用程序。其也允许所述两个应用程序彼此独立地存取两个分离组的数据（例如，一组照片和一组歌曲）。这在图 6 中说明。因此，与用于经由图 6 的顶部部分的树中的节点 (ACR) 进行存取的应用程序或用户的“密钥 3”、“密钥 X”和“密钥 Z”相关联的数据可包含照片。与用于经由图 6 的底部部分的树中的节点 (ACR) 进行存取的应用程序或用户的“密钥 5”和“密钥 Y”相关联的数据可包含歌曲。仅当 AGP 没有 ACR 实体时，创建 AGP 的 ACR 才具有将其删除的许可。

[0096] 实体的 SSA 入口点 :存取控制记录 (ACR)

[0097] SSA 系统中的 ACR 描述许可实体登录到系统中的方式。当实体登录到 SSA 系统中时，其需要指定对应于将要执行的认证过程的 ACR。ACR 包括许可控制记录 (PCR)，所述 PCR 说明用户一旦经认证（如图 5 所说明的 ACR 中定义）便可执行的经授权动作。主机侧实体提供所有 ACR 数据字段。

[0098] 当实体已成功登录到 ACR 上时，实体将能够询问所有 ACR 分区和密钥存取许可和 ACAM 许可（下文解释）。

[0099] ACR ID

[0100] 当 SSA 系统实体初始化登录过程时，其需要指定对应于登录方法的 ACR ID（如当创建 ACR 时由主机所提供），以使得当已满足所有登录要求时 SSA 将建立正确的算法且选择正确的 PCR。当创建 ACR 时，向 SSA 系统提供 ACR ID。

[0101] 登录 / 认证算法

[0102] 认证算法指定实体将使用哪种登录程序和需要哪种证书来提供用户身份的证明。SSA 系统支持若干种标准登录算法，这基于对称或不对称密码从无程序（和无证书）和基于口令的程序到双向认证协议。

[0103] 证书

[0104] 实体的证书对应于登录算法且由 SSA 使用来验证和认证用户。证书的实例可以是用于口令认证的口令 /PIN 编号、用于 AES 认证的 AES 密钥等。证书的类型 / 格式（即，PIN、对称密钥等）经预先定义且得自认证模式 ;当创建 ACR 时，将其提供给 SSA 系统。SSA 系统不参与定义、分配和管理这些证书，除了基于 PKI 的认证之外，其中可使用装置（例如，快闪卡）来产生 RSA 密钥对且可输出公用密钥以用于凭证产生。

[0105] 许可控制记录 (PCR)

[0106] PCR 展示在实体登录到 SSA 系统中并成功通过 ACR 认证过程之后向实体授予什么。存在三个类型的许可种类 :用于分区和密钥的创建许可、对分区和密钥的存取许可和用于

实体 -ACR 属性的管理许可。

[0107] 存取分区

[0108] PCR 的此部分含有实体在成功完成 ACR 阶段之后可存取的分区（使用其提供给 SSA 系统的 ID）的列表。对于每个分区来说，存取类型可限于只写或只读，或者可指定全部写入 / 读取存取权利。因此，图 5 中的 ACR#1 能够存取分区 #2 而并非分区 #1。PCR 中指定的限制适用于 SSA 分区和公用分区。

[0109] 可由到主导 SSA 系统的装置（例如，快闪卡）的常规读取和写入命令或由 SSA 命令存取公用分区。当根 ACR（下文解释）经创建为具有用以限制公用分区的许可时，他可将所述许可传递给他的子代。ACR 可优选地仅限制常规读取和写入命令存取公用分区。SSA 系统中的 ACR 可仅在其创建方面受到限制。一旦 ACR 具有用以读取 / 写入公用分区的许可，则优选地其不能被取走。

[0110] 存取密钥 ID

[0111] PCR 的此部分含有与当实体的登录过程已符合 ACR 策略时实体可存取的密钥 ID 列表（如由主机提供给 SSA 系统）相关联的数据。所指定的密钥 ID 与驻存在出现于 PCR 中的分区中的一个或多个文件相关联。由于密钥 ID 不与装置（例如，快闪卡）中的逻辑地址相关联，因而当一个以上分区与特定 ACR 相关联时，文件可在任何一个所述分区中。PCR 中所指定的密钥 ID 可每一者具有不同组的存取权利。存取由密钥 ID 指向的数据可限于只写或只读，或者可指定全部写入 / 读取存取权利。

[0112] ACR 属性管理 (ACAM)

[0113] 这部分描述在某些情况下可如何改变 ACR 的系统属性。

[0114] 可在 SSA 系统中许可的 ACAM 动作为：

[0115] 创建 / 删除 / 更新 AGP 和 ACR。

[0116] 创建 / 删除分区和密钥。

[0117] 授予对密钥和分区的存取权利

[0118] 父代 ACR 优选地不能编辑 ACAM 许可。这将优选地要求删除和重新创建 ACR。同样，优选地不能取走由 ACR 创建的对密钥 ID 的存取许可。

[0119] 创建 / 删除 / 更新 AGP 和 ACR

[0120] ACR 可具有创建其它 ACR 和 AGP 的能力。创建 ACR 也可意味着授予其由其创建者所拥有的 ACAM 许可中的一些或所有。具有用以创建 ACR 的许可意味着具有用于以下动作的许可：

[0121] 1. 定义和编辑子代的证书——优选地，认证方法一旦由创建 ACR 设定便不能被编辑。可在已经针对子代定义的认证算法的边界内改变证书。

[0122] 2. 删除 ACR。

[0123] 3. 将创建许可授予子代 ACR（因此具有孙代）。

[0124] 具有用以创建其它 ACR 的许可的 ACR 具有用以将解锁许可授予其创建的 ACR 的许可（尽管其很可能不具有用以解锁 ACR 的许可）。父代 ACR 将在子代 ACR 中放置对其解锁者的参考。

[0125] 父代 ACR 是具有用以删除其子代 ACR 的许可的唯一 ACR。当 ACR 删除其创建的较低等级 ACR 时，那么由此较低等级 ACR 产生的所有 ACR 同样被自动删除。当 ACR 被删除时，

那么其创建的所有密钥 ID 和分区被删除。

[0126] 存在 ACR 可由此更新其自身记录的两个例外 :

[0127] 尽管口令 /PIN 由创建者 ACR 设定,但仅可由包括其的 ACR 来更新。

[0128] 根 ACR 可将其自身和其所驻存的 AGP 删除。

[0129] 授予对密钥和分区的存取权利

[0130] 将 ACR 和其 AGP 组合成分级树,其中根 AGP 和其内的 ACR 位于树的顶部 (例如,图 6 中的根 AGP 130 和 132)。在 SSA 系统中可存在若干 AGP 树,尽管其完全彼此分离。AGP 内的 ACR 可将对其密钥的存取许可授予其所在的同一 AGR 中的所有 ACR 以及由其创建的所有 ACR。用以创建密钥的许可优选地包括用以授予存取许可以使用密钥的许可。

[0131] 将对密钥的许可划分为三个种类 :

[0132] 1. 存取 - 此定义针对密钥的存取许可,即读取、写入。

[0133] 2. 拥有权 - 创建密钥的 ACR 从定义上来说是其拥有者。可将此拥有权从一个 ACR 授予给另一个 ACR(只要其在相同 AGP 中或在子代 AGP 中)。密钥的拥有权提供用以将其删除的许可以及向其授予许可。

[0134] 3. 存取权利授予 - 此许可使得 ACR 能够授予其持有的权利。

[0135] ACR 可将存取许可授予其创建的分区以及其对此具有存取许可的其它分区。

[0136] 通过将分区名称和密钥 ID 添加到指定 ACR 的 PCR 来进行许可授予。授予密钥存取许可可通过密钥 ID 或通过规定存取许可是针对授权 ACR 的所有所创建密钥的来进行。

[0137] ACR 的封锁和解锁

[0138] ACR 可具有封锁计数器,其在系统对于实体的 ACR 认证过程不成功时递增。当达到不成功认证的特定最大数目 (MAX) 时,ACR 将由 SSA 系统封锁。

[0139] 经封锁的 ACR 可由另一 ACR 解锁,其由所述经封锁的 ACR 参考。对于解锁 ACR 的参考由其创建者设定。解锁 ACR 优选地与经封锁 ACR 的创建者位于相同的 AGP 中且具有“解锁”许可。

[0140] 系统中没有其它 ACR 可解锁经封锁的 ACR。ACR 可经配置具有封锁计数器而没有解锁器 ACR。在此情况下,如果此 ACR 受到封锁,那么其不能被解锁。

[0141] 根 AGP- 创建应用程序数据库

[0142] SSA 系统经设计以处理多个应用程序和隔离每个应用程序的数据。AGP 系统的树结构是用于识别和隔离专用数据的主要工具。根 AGP 位于应用程序 SSA 数据库树的尖端且遵守稍有不同的行为规则。可在 SSA 系统中配置若干个根 AGP。在图 6 中展示两个根 AGP 130 和 132。显然,可使用较少或较多 AGP,且这在本发明的范围内。

[0143] 通过将新的 AGP/ACR 树添加到装置的过程来进行向所述装置 (例如,快闪卡) 注册所述装置的新应用程序和 / 或新应用程序的发布证书。

[0144] SSA 系统支持三种不同模式的根 AGP 创建 (以及根 AGP 的所有 ACR 和其许可) :

[0145] 1. 开放 :未请求任何种类的认证的任何用户或实体或通过系统 ACR(下文解释) 认证的用户或实体可创建新的根 AGP。所述开放模式使得能够在无需任何安全措施且同时在开放通道上 (即,在发布机构的安全环境中) 进行所有数据传送的情况下创建根 AGP,或者通过经由系统 ACR 认证 (即,无线 (OTA) 和后发布程序) 建立的安全通道来创建根 AGP。

[0146] 如果未配置系统 ACR(这是可选特征) 并将根 AGP 创建模式设定为开放,那么仅开

放通道选择可用。

[0147] 2. 受控：只有通过系统 ACR 认证的实体可创建新的根 AGP。如果未配置系统 ACR，那么不可将 SSA 系统设定为此模式。

[0148] 3. 锁定：禁用根 AGP 的创建且不可向系统添加额外的根 AGP。

[0149] 控制此特征的两个 SSA 命令（这些命令可用于任何用户 / 实体而无需认证）：

[0150] 1. 方法配置命令 - 用于将 SSA 系统配置为使用所述三个根 AGP 创建模式中的任何一者。仅允许以下模式改变：打开 -> 受控、受控 -> 锁定（即，如果当前将 SSA 系统配置为受控，那么可仅将其改变为锁定）。

[0151] 2. 方法配置锁定命令 - 用于禁用方法配置命令和永久地锁定当前所选择的方法。

[0152] 当创建根 AGP 时，其具有特殊初始化模式，所述模式实现其 ACR 的创建和配置（使用适用于根 AGP 的创建的相同存取限制）。在根 AGP 配置过程的末端，当实体明确地将其切换到操作模式时，不再能够更新现有 ACR 且不再能够创建额外的 ACR。

[0153] 一旦将根 AGP 置于标准模式中，仅可通过使其通过指派有用以删除根 AGP 的许可的其一个 ACR 登录到系统中来将其删除。除了特殊初始化模式之外，这是根 AGP 的另一例外；其优选地是可含有具有用以删除其自身 AGP 的许可的 ACR 的唯一 AGP，这与下一个树等级中的 AGP 相反。

[0154] 根 ACR 与标准 ACR 之间的第三个也是最后一个区别在于，其是系统中可具有用以创建和删除分区的许可的唯一 AGP。

[0155] SSA 系统 ACR

[0156] 可将系统 ACR 用于以下两个 SSA 操作：

[0157] 1. 在敌对环境内在安全通道的保护下创建 ACR/AGR 树。

[0158] 2. 识别和认证主导 SSA 系统的装置。

[0159] 优选地，可在 SSA 中仅存在一个系统 ACR，且一旦经定义，其便优选地不可改变。当创建系统 ACR 时不需要系统认证；仅需要 SSA 命令。可禁用创建系统 ACR 特征（类似于创建根 AGP 特征）。在创建系统 ACR 之后，创建系统 ACR 命令没有效果，因为优选地，仅允许一个系统 ACR。

[0160] 当在创建过程中时，系统 ACR 不操作。当完成时，需要发布特殊命令来指示系统 ACR 得以创建且准备好运行。在此点之后，系统 ACR 优选地不能被更新或取代。

[0161] 系统 ACR 在 SSA 中创建根 ACR/AGP。其具有用以增加 / 改变根等级直到满足主机且主机将其封锁为止的许可。封锁根 AGP 实质上切断其与系统 ACR 的连接，且致使其防扰。在此点处，没有一者能改变 / 编辑根 AGP 和其内的 ACR。此通过 SSA 命令进行。禁用创建根 AGP 具有持久效应且不可逆。图 7 中说明以上涉及系统 ACR 的特征。系统 ACR 用于创建三个不同根 AGP。在创建这些之后的某个时间，从主机发送 SSA 命令以封锁来自系统 ACR 的根 AGP，借此禁用创建根 AGP 特征，如图 7 中将系统 ACR 连接到根 AGP 的虚线指示。这致使所述三个根 AGP 防扰。在封锁根 AGP 之前或之后，所述三个根 AGP 可用于创建子代 AGP 以形成三个单独树。

[0162] 上述特征为内容拥有者在用内容配置安全产品中提供较大灵活性。安全产品需要“经发布”。发布是放置识别密钥（装置可通过这些密钥来识别主机且反之亦然）的过程。识别装置（例如，快闪卡）使得主机能够决定其是否可将其秘密委托给所述装置。另一方面，

识别主机使得装置能够在仅当主机被允许时实施安全策略（授予并执行特殊主机命令）。

[0163] 经设计以服务多个应用程序的产品将具有若干识别密钥。产品可以“先发布”（在发货之前在制造期间存储密钥）或“后发布”（在发货之后添加新密钥）。对于后发布来说，存储器装置（例如，存储卡）需要含有某类型的用于识别被允许向装置添加应用程序的实体的主导装置或装置等级密钥。

[0164] 上述特征使得产品能够经配置以启用 / 禁用后发布。另外，可在发货之后安全地进行后发布配置。可将装置作为零售产品来购买，其中在装置上除了上述主导装置或装置等级密钥之外没有其它密钥，且接着由新拥有者配置所述装置以启用另外的后发布应用程序或将其禁用。

[0165] 因此，系统 ACR 特征提供用以实现上述目标的能力：

[0166] - 不具有系统 ACR 的存储器装置将允许无限制且不受控地添加应用程序。

[0167] - 不具有系统 ACR 的存储器装置可经配置以禁用系统 ACR 创建，这意味着没有方法来控制新应用程序的添加（除非同样禁用创建新根 AGP 的特征）。

[0168] - 具有系统 ACR 的存储器装置将仅允许经由安全通道受控地添加应用程序以通过使用系统 ACR 证书的认证程序来建立。

[0169] - 在添加应用程序之前或之后，具有系统 ACR 的存储器装置可经配置以禁用应用程序添加特征。

[0170] 密钥 ID 列表

[0171] 对每个特定 ACR 请求创建密钥 ID；然而，在存储器系统 10 中，仅由 SSA 系统使用这些密钥 ID。当创建密钥 ID 时，由创建 ACR 提供或向创建 ACR 提供以下数据：

[0172] 1. 密钥 ID。所述 ID 由实体通过主机提供且用于参考密钥和在所有进一步读取或写入存取中使用密钥加密或解密的数据。

[0173] 2. 密钥密码和数据完整性模式（上述块、链和散列模式，且如下文解释）

[0174] 除了主机提供的属性之外，由 SSA 系统维护以下数据：

[0175] 1. 密钥 ID 拥有者。作为拥有者的 ACR 的 ID。当创建密钥 ID 时，创建者 ACR 是其拥有者。然而，可将密钥 ID 拥有权转移给另一 ACR。优选地，仅允许密钥 ID 拥有者转移密钥 ID 的所有权和授权密钥 ID。将存取许可授予相关联密钥和撤销这些权利可由密钥 ID 拥有者或分配有授权许可的任何其它 ACR 来管理。无论何时试图实行这些操作中的任何一者，SSA 系统将仅在批准请求 ACR 时向其授权。

[0176] 2. CEK。这是用于加密与密钥 ID 相关联的内容或由密钥 ID 指向的内容的 CEK。CEK 可以是由 SSA 系统产生的 128 位 AES 随机密钥。

[0177] 3. MAC 和 IV 值。用于链接块密码 (CBC) 加密算法中的动态信息（消息认证代码和初始向量）。

[0178] 还参考图 8A-16 中的流程图来说明 SSA 的各种特征，其中步骤左侧的“H”意味着操作由主机执行，且“C”意味着操作由卡执行。为了创建系统 ACR，主机向存储器装置 10 中的 SSA 发布用以创建系统 ACR 的命令（方框 202）。装置 10 通过检查系统 ACR 是否已经存在来作出响应（方框 204，菱形 206）。如果已经存在，那么装置 10 返回失败结果并停止（椭圆形 208）。如果不存在，那么存储器 10 检查以查看是否允许系统 ACR 创建（菱形 210），且如果不允许则返回失败状态（方框 212）。因此，可存在装置发布者不允许创建系统 ACR 的

情况，例如在已预先确定了所需要的安全性特征以使得不需要系统 ACR 的状况下。如果这不被允许，那么装置 10 返回 OK 状态且等待来自主机的系统 ACR 证书（方框 214）。主机检查 SSA 状态和装置 10 是否已指示允许创建系统 ACR（方框 216 和菱形 218）。如果不允许创建或如果系统 ACR 已经存在，那么主机停止（椭圆形 220）。如果装置 10 已指示允许创建系统 ACR，那么主机发出 SSA 命令以定义其登录证书并将其发送到装置 10（方框 222）。装置 10 用所接收的证书来更新系统 ACR 记录并返回 OK 状态（方框 224）。响应于此状态信号，主机发出指示系统 ACR 已准备好的 SSA 命令（方框 226）。装置 10 通过锁定系统 ACR 以使得其不能被更新或取代来作出响应（方框 228）。这锁定了系统 ACR 的特征和其用于向主机识别装置 10 的身份。

[0179] 通过在装置中配置这些功能的方式来确定用于创建新树（新的根 AGP 和 ACR）的程序。图 9 解释所述程序。主机 24 与存储器系统 10 两者均遵守其。如果完全禁用添加新根 AGP，那么不能添加新的根 AGP（菱形 246）。如果其被启用但需要系统 ACR，那么主机通过系统 ACR 来认证并建立安全通道（菱形 250，方框 252），且之后发出创建根 AGP 命令（方框 254）。如果不需要系统 ACR（菱形 248），那么主机 24 可发出创建根 AGP 命令而无需认证，并进入方框 254。如果系统 ACR 存在，那么即使不需要，主机也可使用其（流程图中未图示）。如果禁用该功能，那么装置（例如，快闪卡）将拒绝任何创建新根 AGP 的试图，且如果需要系统 ACR，那么其将拒绝在没有认证的情况下创建新根 AGP 的试图（菱形 246 和 250）。现在将方框 254 中的新创建的 AGP 和 ACR 切换到操作模式，以使得这些 AGP 中的 ACR 不能被更新或改变，且不能将任何 ACR 添加到其（方框 256）。接着视情况将系统锁定，以使得不能创建额外的根 AGP（方框 258）。虚线框 258 是指示此步骤为可选步骤的常规方式。此应用程序的图式的流程图中以虚线表示的所有框均是可选步骤。这允许内容拥有者阻断出于其它非法目的的装置 10 的使用（其可模仿具有合法内容的真正存储器装置）。

[0180] 为了创建 ACR（除了上述根 AGP 中的 ACR），可用具有创建 ACR 权利的任何 ACR 来开始（方框 270），如图 10 所示。实体可试图通过提供实体点 ACR 身份和具有其希望创建的所有必要属性的 ACR 而经由主机 24 进入（方框 272）。SSA 检查与 ACR 身份的匹配且具有此身份的 ACR 是否具有创建 ACR 的许可（菱形 274）。如果请求被验证为经授权的，那么装置 10 中的 SSA 创建 ACR（方框 276）。

[0181] 图 11 展示两个 AGP，其说明可用于使用图 10 的方法的安全应用程序的树。因此，营销 AGP 中具有身份 m1 的 ACR 具有用以创建 ACR 的许可。ACR m1 还可具有用以将密钥用于读取和写入与密钥 ID “营销信息”相关联的数据和与密钥 ID “价格列表”相关联的数据的许可。通过使用图 10 的方法，其创建具有两个 ACR 的销售 AGP：s1 和 s2，其对用于存取与密钥 ID “价格列表”相关联的定价数据的密钥而不是对存取与密钥 ID “营销信息”相关联的数据所必要的密钥的只读许可。以此方式，具有 ACR s1 和 s2 的实体仅可读取而不能改变定价数据，且将不能存取营销数据。另一方面，ACR m2 不具有用以创建 ACR 的许可，且具有对用于存取与密钥 ID “价格列表”和密钥 ID “营销信息”相关联的数据的密钥的只读许可。

[0182] 因此，可用上文解释的方式授予存取权利，其中 m1 向 s1 和 s2 授予用以读取定价数据的权利。这对于涉及较大营销和销售群组尤其有用。在仅存在一个或少数销售人员的情况下，可能不需要使用图 10 的方法。而是，可由 ACR 向在同一 AGP 内较低或相同等级处

的 ACR 授予存取权利，如图 12 说明。首先，实体通过经由主机用上文描述的方式在树中指定 ACR 来进入此 AGP 的树（方框 280）。接着，主机将指定 ACR 和授予其的权利。SSA 检查此 ACR 的树和是否 ACR 具有将权利授予所指定的另一 ACR 的许可（菱形 282）。如果具有，那么授予权利（方框 284）；如果没有，那么停止。所述结果在图 13 中说明。在此情况下，ACR m1 具有授予 ACR s1 读取许可的许可，以使得 s1 将能够在授权之后使用密钥来存取定价数据。如果 m1 具有用以存取定价数据的相同或较大权利和如此授权的许可，那么可执行这项操作。在一个实施例中，m1 在授权之后维持其存取权利。优选地，可在例如有限时间、有限数目的存取等的受限条件下（而并非永久地）授予存取权利。

[0183] 图 14 中说明用于创建密钥和密钥 ID 的过程。实体通过 ACR 来认证（方框 302）。实体请求创建具有由主机指定的 ID 的密钥（方框 304）。SSA 检查并查看所指定的 ACR 是否具有这样做的许可（菱形 306）。举例来说，如果将要把密钥用于存取特定分区中的数据，那么 SSA 将检查并查看 ACR 是否可存取此分区。如果 ACR 被认证，那么存储器装置 10 创建与由主机提供的密钥 ID 相关联的密钥值（方框 308），且将密钥 ID 存储在 ACR 中并将密钥值存储在其存储器中（在与控制器相关联的存储器或存储器 20 中），且根据由实体提供的信息分派权利和许可（方框 310）并修改具有这些所分派的权利和许可的此 ACR 的 PCR（方框 312）。因此，密钥的创建者具有所有可用权利，例如读取和写入许可、授予及与同一 AGP 中其它 ACR 或较低等级处的 ACR 共享的权利和转移密钥拥有权的权利。

[0184] ACR 可改变 SSA 系统中另一 ACR 的许可（或连同存在），如图 15 说明。实体可如同以前那样通过 ACR 进入树；在一种情况下，实体经认证，且接着其指定 ACR（方框 330、332）。其要求删除目标 ACR 或目标 ACR 中的许可（方框 334）。如果所指定的 ACR 或此时活动的 ACR 具有这样做的权利（菱形 336），那么删除目标 ACR，或改变目标 ACR 的 PCR 以删除此许可（方框 338）。如果这未被认证，那么系统停止。

[0185] 在上述过程之后，目标将不再能够存取其在所述过程之前能够存取的数据。如图 16 所示，实体可试图在目标 ACR 处进入（方框 350）并发现认证过程失败，因为先前存在的 ACR ID 不再存在于 SSA 中，以使得存取权利被否定（菱形 352）。假定尚未删除 ACR ID，那么实体指定 ACR（方框 354）和特定分区中的密钥 ID 和 / 或数据（方框 356），且 SSA 接着根据此 ACR 的 PCR 检查以查看密钥 ID 或分区存取要求是否被许可（菱形 358）。如果许可已被删除或已期满，那么再次拒绝请求。否则，授权请求（方框 360）。

[0186] 上述过程描述装置（例如，快闪卡）如何管理存取受保护数据，而不管 ACR 和其 PCR 是否刚由另一 ACR 改变或经如此配置以开始。

[0187] 对话

[0188] SSA 系统经设计以处理同时登录的多个用户。此特征要求由 SSA 接收的每个命令与特定实体相关联且仅在用于认证此实体的 ACR 具有针对所请求行动的许可时被执行。

[0189] 通过对话概念支持多个实体。在认证过程期间建立对话，且所述对话由 SSA 系统分派对话 id。所述对话 id 内在地与用于登录到系统中的 ACR 相关联，且经输出给实体以用于所有进一步 SSA 命令。

[0190] SSA 系统支持两个类型的对话：开放对话和安全对话。在 ACR 中界定与特定认证过程相关联的对话类型。SSA 系统将以类似于其自身实施认证的方式来实施对话建立。由于 ACR 界定实体许可，因而此机制使得系统设计者能够将安全隧穿与存取特定密钥 ID 或调

用特定 ACR 管理操作（即，创建新 ACR 和设定证书）进行关联。

[0191] 开放对话

[0192] 开放对话是用对话 id 而没有总线加密来识别的对话，所有命令和数据被不受阻碍地传递。此操作模式优选地用于多用户或多实体环境中，其中实体既不是威胁模型的一部分，也不在总线上窃听。

[0193] 尽管既不保护数据的传输，也不启用主机侧上应用程序之间的有效防火墙功能，但开放对话模式使得 SSA 系统能够允许仅存取允许用于当前经认证 ACR 的信息。

[0194] 开放对话也可用于分区或密钥需要保护的情况。然而，在有效认证过程之后，将存取授予主机上的所有实体。为了获得经认证 ACR 的许可，各种主机应用程序需要共享的唯一事物是对话 id。这在图 17A 中说明。线 400 上的步骤是由主机 24 执行的那些步骤。在针对 ACR1 认证实体（方框 402）之后，其要求存取存储器装置 10 中与密钥 ID X 相关联的文件（方框 404、406 和 408）。如果 ACR1 的 PCR 允许此存取，那么装置 10 授权所述请求（菱形 410）。如果不允许，那么系统返回到方框 402。在完成认证之后，存储器系统 10 仅通过所分派的对话 id（而并非 ACR 证书）来识别发出命令的实体。一旦 ACR1 获得存取与其 PCR 中的密钥 ID 相关联的数据，那么在开放对话中，任何其它应用程序或用户可通过指定正确对话 ID（其在主机 24 上的不同应用程序之间共享）来存取相同数据。此特征在更方便地使得用户能够仅登录一次且能够存取与通过其为不同应用程序执行登录的帐户有关的所有数据的应用中是有利的。因此，蜂窝式电话用户可以能够存取存储器 20 中存储的电子邮件和听存储器 20 中存储的音乐而无需登录多次。另一方面，不由 ACR1 所包含的数据将为不可存取的。因此，同一蜂窝式电话用户可具有可通过单独帐户 ACR2 存取的有价值内容（例如游戏和照片）。这是他不希望借其电话的其他人存取的数据，尽管他不介意其他人通过其第一帐户 ACR1 存取可用的数据。将数据存取分为两个单独帐户，而允许在开放对话中存取 ACR1 提供使用方便性以及提供对有价值数据的保护。

[0195] 为了更进一步方便在主机应用程序当中共享对话 id 的过程，当 ACR 请求开放对话时，其可特别地请求向所述对话分派“0（零）”id。如此，应用程序可经设计以使用预定义对话 id。显然，唯一限制是在特定时间仅可认证请求对话 0 的一个 ACR。认证请求对话 0 的另一 ACR 的试图将被拒绝。

[0196] 安全对话

[0197] 为了添加安全层，可使用对话 id（如图 17B 所示）。存储器 10 接着还存储活动对话的对话 id。在图 17B 中，举例来说，为了能够存取与密钥 ID X 相关联的文件，实体将需要在其被允许存取文件之前还提供对话 id（例如，对话 id “A”）（方框 404、406、412 和 414）。以此方式，除非请求实体知道正确的对话 id，否则其不能存取存储器 10。由于在对话结束之后删除对话 id 且对话 id 对于每个对话是不同的，因而实体可仅在其已能够提供对话号码时获得存取。

[0198] 除了通过使用对话号码之外，SSA 系统没有其它方法来确保命令确实来自经正确认证的实体。对于其中存在攻击者将试图使用开放通道来发送恶意命令的威胁的应用程序和使用情况来说，主机应用程序使用安全对话（安全通道）。

[0199] 当使用安全通道时，使用安全通道加密（对话）密钥来加密对话 id 以及整个命令，且安全水平与主机侧实施方案一样高。

[0200] 终止对话

[0201] 在任何一种以下情形中，终止对话且退出 ACR：

[0202] 1. 实体发出明确的结束对话命令。

[0203] 2. 通信超时。特定实体未对定义作为一个 ACR 参数的时间周期发出命令。

[0204] 3. 在装置（例如，快闪卡）复位和 / 或功率周期之后终止所有打开对话。

[0205] 数据完整性服务

[0206] SSA 系统验证 SSA 数据库（其含有所有 ACR、PCR 等）的完整性。此外，通过密钥 ID 机制为实体数据提供数据完整性服务。

[0207] 如果将散列用作其加密算法来配置密钥 ID，那么将散列值连同 CEK 和 IV 一起存储在 CEK 记录中。在写入操作期间计算和存储散列值。在读取操作期间再次计算散列值并将其与在先前写入操作期间存储的值进行比较。每次实体存取密钥 ID 时，将额外数据连接（以密码形式）到旧数据和经更新的适当散列值（用于读取或用于写入）。

[0208] 由于只有主机知道与密钥 ID 相关联或由密钥 ID 指向的数据文件，因而主机明确地用以下方式管理数据完整性功能的若干方面：

[0209] 1. 从开始到结束写入或读取与密钥 ID 相关联或由密钥 ID 指向的数据文件。任何存取部分文件的试图将使其混乱，因为 SSA 系统正使用 CBC 加密方法且产生整个数据的散列消息摘要。

[0210] 2. 无需处理相连流（数据流可与其它密钥 Id 的数据流交错且可在多个对话上分裂）中的数据，因为中间散列值由 SSA 系统维持。然而，如果重新开始数据流，那么实体将需要明确指示 SSA 系统重设散列值。

[0211] 3. 当完成读取操作时，主机必须明确请求 SSA 系统通过将读取散列与在写入操作期间计算出的散列值进行比较来验证所述读取散列。

[0212] 4. SSA 系统同样提供“虚拟读取”操作。此特征将使得数据串流通过密码引擎，但将不会把其发送出到主机。此特征可用于在将数据实际从装置（例如，快闪卡）读出之前验证数据完整性。

[0213] 随机号码产生

[0214] SSA 系统将使得外部实体能够利用内部随机号码产生器并请求将随机号码在 SSA 系统外部使用。此服务可用于任何主机且不需要认证。

[0215] RSA 密钥对产生

[0216] SSA 系统将使得外部用户能够利用内部 RSA 密钥对产生特征并请求将 RSA 密钥对在 SSA 系统外部使用。此服务可用于任何主机且不需要认证。

[0217] 替代实施例

[0218] 代替使用分级方法，可使用数据库方法来实现类似结果，如图 18 说明。

[0219] 如图 18 所示，可将实体的证书、认证方法、失败试图的最大数目和需要解锁的证书的最小数目的列表输入到存储在控制器 12 或存储器 20 中的数据库中，这使得这些证书要求与数据库中由存储器 10 的控制器 12 执行的策略（读取、写入存取密钥和分区、安全通道要求）相关。同样存储在数据库中的还有对存取密钥和分区的约束和限制。因此，一些实体（例如，系统管理者）可在白名单上，这意味着这些实体可始终存取所有密钥和分区。其它实体可在黑名单上，且其对存取任何信息的试图将被阻断。限制可以是全局的或密钥

和 / 或分区特定的。这意味着仅某些实体可始终存取某些特定密钥和分区，且某些实体始终不能存取。可对内容本身进行约束，而不管内容所在的分区或用于将其加密或解密的密钥。因此，某些数据（例如，歌曲）可具有其仅可由存取其的前面五个主机装置来存取或其它数据（例如，电影）仅可被读取有限次数（而不管哪些实体已进行存取）的属性。

[0220] 认证

[0221] 口令保护

[0222] •口令保护意味着需要出示口令以存取受保护区域。除非其不能是一个以上口令，否则口令可与例如读取存取或读取 / 写入存取的不同权利相关联。

[0223] • 口令保护意味着装置（例如，快闪卡）能够验证由主机提供的口令，即装置也具有存储在由装置管理的安全存储区域中的口令。

[0224] 问题和限制

[0225] •口令常遭受重放攻击。因为口令在每次出示之后不发生改变，所以其可被同样地再次发送。这意味着如果待保护的数据是有价值的，且通信总线可易于存取，那么照现在的样子不能使用口令。

[0226] • 口令可保护对所存储数据的存取，但不应用于保护数据（并非密钥）

[0227] • 为了增加与口令相关联的安全等级，可使用主密钥来使口令多样化，这导致一个口令被黑 (hack) 不会破坏整个系统。基于对话密钥的安全通信通道可用于发送口令。

[0228] 图 19 是说明使用口令的认证的流程图。实体向系统 10（例如，快闪存储卡）呈报帐户 id 和口令。系统检查以查看所述口令是否与其存储器中的口令匹配。如果匹配，那么返回受认证状态。否则，针对那个帐户递增错误计数器，且要求实体重新输入帐户 id 和口令。如果计数器溢出，那么系统返回拒绝存取的状态。

[0229] 质询响应

[0230] 图 20 是说明使用质询 / 响应型方法的认证的流程图。实体呈报帐户 id，且从系统 10 请求质询。系统 10 产生随机号码并将其呈现给主机。主机从所述号码计算出响应，并将其发送给系统 10。系统 10 将所述响应与所存储的值进行比较。剩余步骤类似于图 19 中用于确定是否授权存取的步骤。

[0231] 图 21 是说明使用另一质询 / 响应型方法的认证的流程图。图 21 与图 20 的不同之处在于，除了要求主机由系统 10 认证之外，其还要求系统 10 由质询 / 响应认证，其中系统 10 也从主机请求质询且返回响应以由主机检查。

[0232] 图 22 是说明使用另一质询 / 响应型方法的认证的流程图。在此情况下，只有系统 10 需要被认证，其中主机将质询发送给系统 10，系统 10 计算出响应，所述响应由主机检查以确定与系统 10 的其记录的匹配。

[0233] 对称密钥

[0234] 对称密钥算法意味着在两侧上使用 SAME 密钥来进行加密及解密。其意味着在通信之前密钥必须被预先同意。而且，每侧应实施彼此反向的算法，即，一侧上是加密算法而另一侧上是解密算法。所述两侧不需要实施两个算法来通信。

[0235] 认证

[0236] •对称密钥认证意味着装置（例如，快闪卡）与主机共享相同密钥且具有相同加密算法（直接和反向，例如 DES 和 DES-1）。

[0237] • 对称密钥认证意味着质询 - 响应（保护以免受重放攻击）。受保护装置产生对于另一装置的质询，且两者均计算响应。认证装置发送回响应，且受保护装置检查响应且因此验证认证。接着可授权与认证相关联的权利。

[0238] 认证可以是：

[0239] • 外部的：装置（例如，快闪卡）认证外界，即，装置验证给定主机或应用程序的证书

[0240] • 相互的：在两侧上产生质询

[0241] • 内部的：主机应用程序认证装置（例如，快闪卡），即，主机检查装置对于其应用程序来说是否是真实的

[0242] 为了增加整个系统的安全等级（即，破坏一者不会破坏所有）

[0243] • 通常可将对称密钥与使用主密钥的多样化结合

[0244] • 相互认证使用来自两侧的质询以确保质询是真实质询

[0245] 加密

[0246] 对称密钥密码术也用于加密，因为其是非常有效的算法，即，其不需要强大 CPU 来处理密码术。

[0247] 当用于保护通信通道时：

[0248] • 两个装置必须知道用以保护通道（即，加密所有传出数据和解密所有传入数据）的对话密钥。通常使用预先共享的秘密对称密钥或使用 PKI 来建立此对话密钥。

[0249] • 两个装置必须知道并实施相同密码算法

[0250] 签名

[0251] 对称密钥也可用于签署数据。在所述情况下，签名是加密的部分结果。保持结果不完整允许签署进行所需要的次数而不会暴露密钥值。

[0252] 问题和限制

[0253] 对称算法是非常有效且安全的，但其基于预先共享的秘密。发布以动态方式秘密地共享此秘密且可能使其为随机的（如同对话密钥）。此想法在于，共享秘密难以长期保持安全且几乎不可能与多人共享。

[0254] 为了有利于此操作，已发明公用密钥算法，因为其允许交换秘密而无需共享秘密。

[0255] 公用密钥密码术

[0256] 不对称密钥算法通常指公用密钥密码。其是非常复杂且通常 CPU 密集的数学实施。已发明其来解决与对称密钥算法相关联的密钥分布的问题。其也提供用于确保数据完整性的签署能力。

[0257] 不对称密钥算法使用分别被称为私有密钥和公用密钥的具有私有和公用元素的密钥。私有密钥与公用密钥两者以数学方式链接在一起。公用密钥可被共享，而私有密钥需要保密。至于所述密钥，不对称算法使用两个数学函数（一个用于私有密钥且一个用于公用密钥）来提供包裹及解开或签署和验证。

[0258] 密钥交换和密钥分配

[0259] 密钥交换通过使用 PK 算法而变得非常简单。装置将其公用密钥发送给其它装置。其它装置用所述公用密钥来包裹其秘密密钥，且将已加密的数据返回到第一装置。第一装置使用其私有密钥来解开数据，且检索两侧现都知道且可用于交换数据的秘密密钥。因为

可容易地交换对称密钥，所以其通常是随机密钥。

[0260] 签名

[0261] 由于其本性的缘故，公用密钥算法通常仅用于签署少量数据。为了确保数据完整性，其接着与提供消息的单向足迹的散列函数组合。

[0262] 私有密钥用于签署数据。公用密钥（可自由获得）允许验证签名。

[0263] 认证

[0264] 认证通常使用签名：质询经签署并返回以供验证。

[0265] 密钥的公用部分用于验证。因为任何人可产生密钥对，所以需要证实公用密钥的拥有者以便证明这是使用正确密钥的合适人。凭证授权方提供凭证，且将在签署凭证中包括公用密钥。凭证由授权方自身签署。接着使用公用密钥来验证签名意味着信任发出含有所述密钥的凭证的授权方且能够验证所述凭证尚未被黑掉，即，由授权方签署的凭证散列是正确的；意味着用户具有授权方公用密钥凭证并信任所述授权方公用密钥凭证。

[0266] 提供 PK 认证的最普通方法是信任授权方或根凭证且间接信任由给定授权方证实的所有密钥对。那么认证是通过签署质询和提供质询响应和凭证来证明所具有的私有密钥与凭证匹配的事项。接着，检查凭证以确保其尚未被黑掉且其由受信任的授权方签署。接着，验证质询响应。如果凭证被信任且质询响应正确，那么认证成功。

[0267] 装置（例如，快闪卡）中的认证意味着对装置加载受信任的根凭证且装置能够验证质询响应以及凭证签署的散列。

[0268] 文件加密

[0269] PK 算法并不用于加密大量数据，因为其是过于 CPU 密集的，但 PK 算法通常用于保护经产生以加密内容的随机化加密 / 解密密钥。举例来说，SMIME（安全电子邮件）产生接着用所有接受者的公用密钥加密的密钥。

[0270] 问题和限制

[0271] 因为任何事物可产生密钥对，所以其必须被证实以确保其来源。在密钥交换期间，一者可能想要确保秘密密钥被提供给正确的装置，即，将需要检查所提供的公用密钥的来源。那么凭证管理成为安全性的一部分，因为其可通知关于密钥的有效性和密钥是否已被撤销。

[0272] 尽管上文已参考各种实施例描述了本发明，但将了解，可在不脱离本发明范围的情况下，对本发明作出各种改变和修改，本发明的范围应仅由所附权利要求书和其等效物界定。本文所提到的所有参考均以引用方式并入本文中。

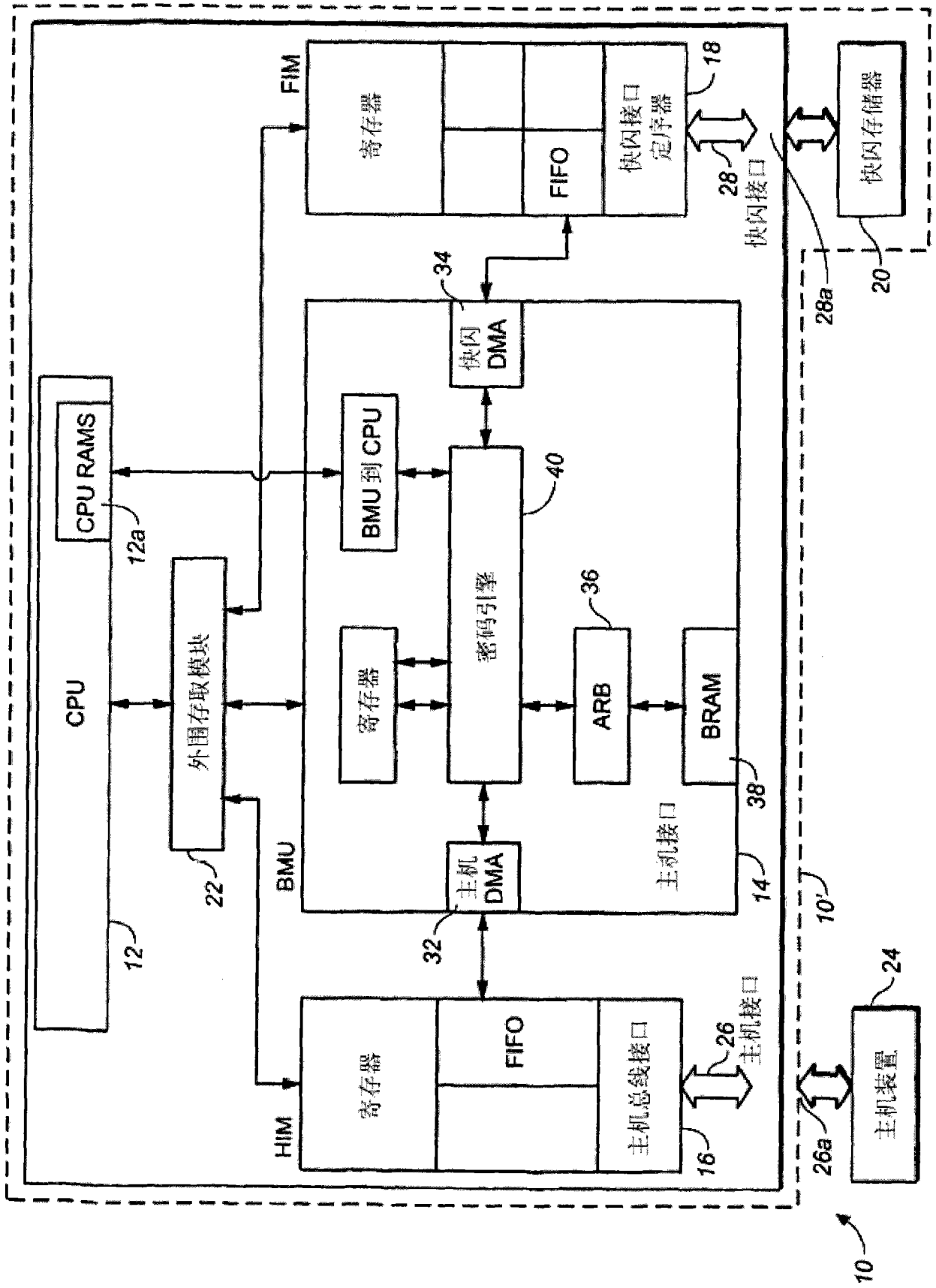

FIM
寄存器
FIFO
快闪接口定序器
18
28
快闪接口
快闪存储器
20
28a
34
快闪 DMA
BMU 到 CPU
40
CPU RAMS
12a
CPU
外围存取模块
寄存器
密码引擎
36
ARB
BRAM
38
22
BMU
主机 DMA
主机接口
14
10
32
12
HIM
寄存器
FIFO
主机总线接口
26
主机接口
24
16
26a
主机装置
10

图 1

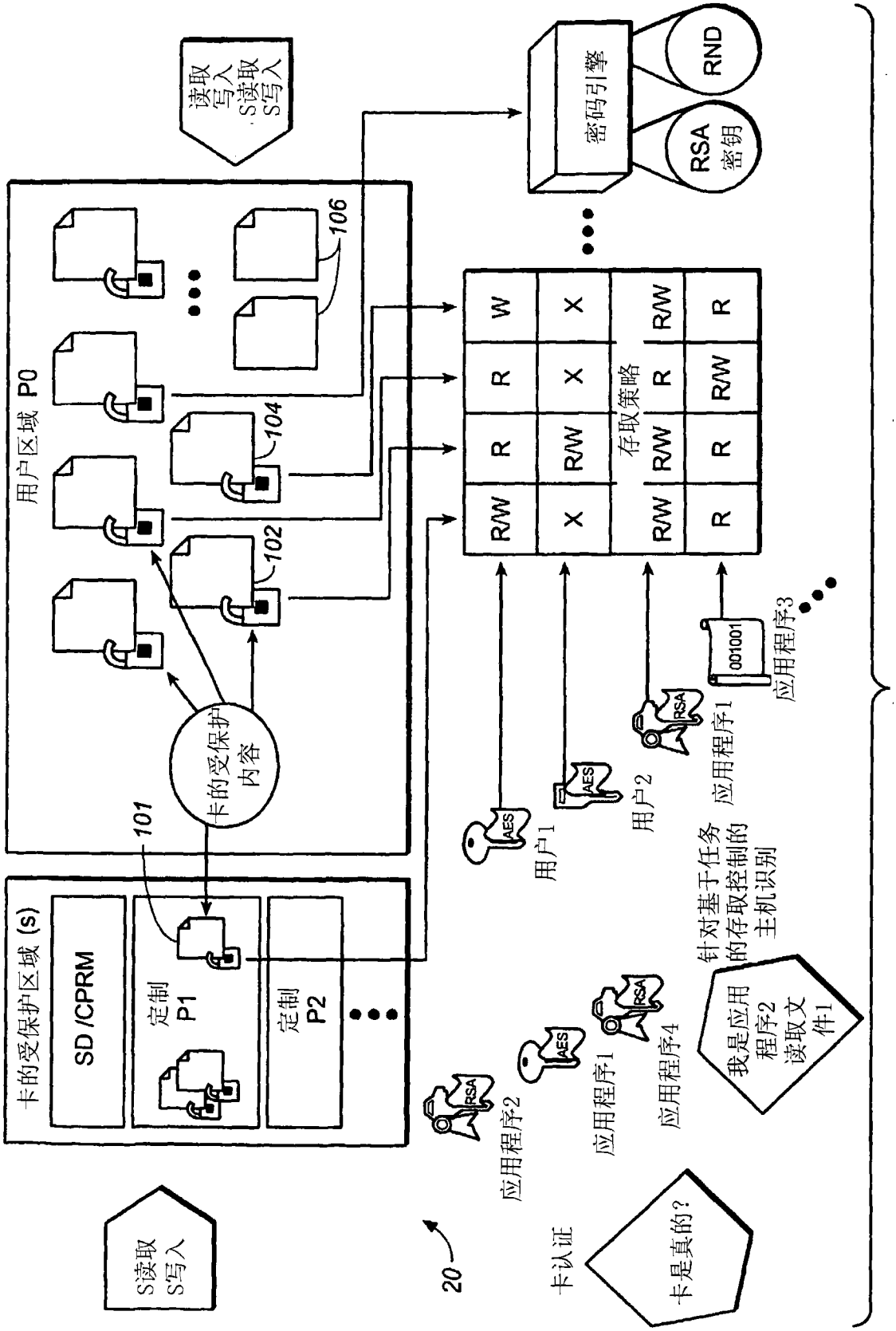

读取
写入
S读取
S写入
密码引擎
RND
RSA
密钥
用户区域 P0
106
104
102
101
卡的受保护
内容
卡的受保护区域 (s)
SD /CPRM
定制
P1
定制
P2
存取策略
R/W
R
X
W
用户1
用户2
应用程序1
应用程序3
针对基于任务
的存取控制的
主机识别
应用程序2
应用程序1
应用程序4
我是应用
程序2
读取文
件1
卡认证
卡是真的?
S读取
S写入
20

图 2

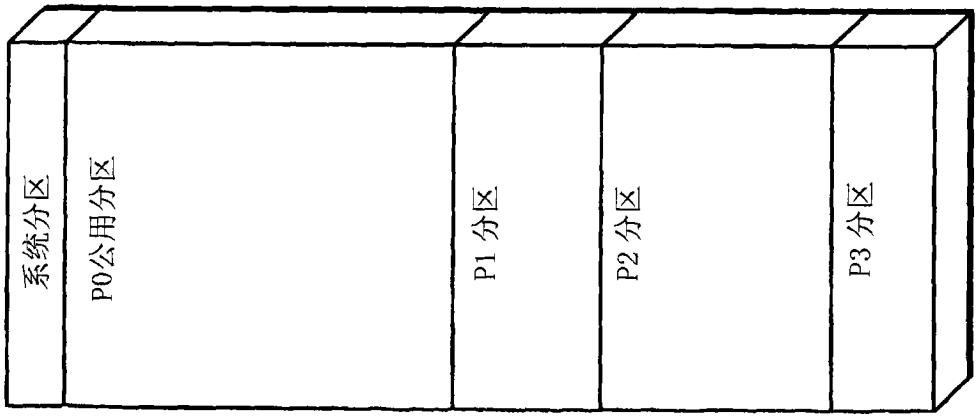

系统分区
P0公用分区
P1 分区
P2 分区
P3 分区

图 3

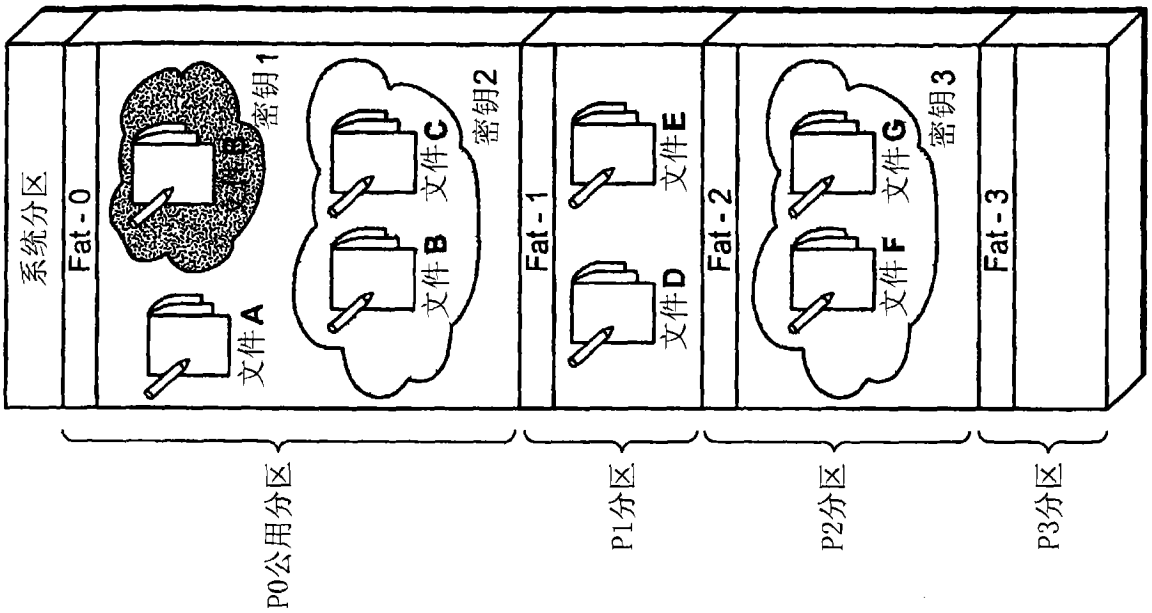

系统分区
Fat - 0
密钥1
文件A
文件B
密钥2
文件C
Fat - 1
文件D
文件E
Fat - 2
密钥3
文件F
文件G
Fat - 3
P0公用分区
P1分区
P2分区
P3分区

图 4

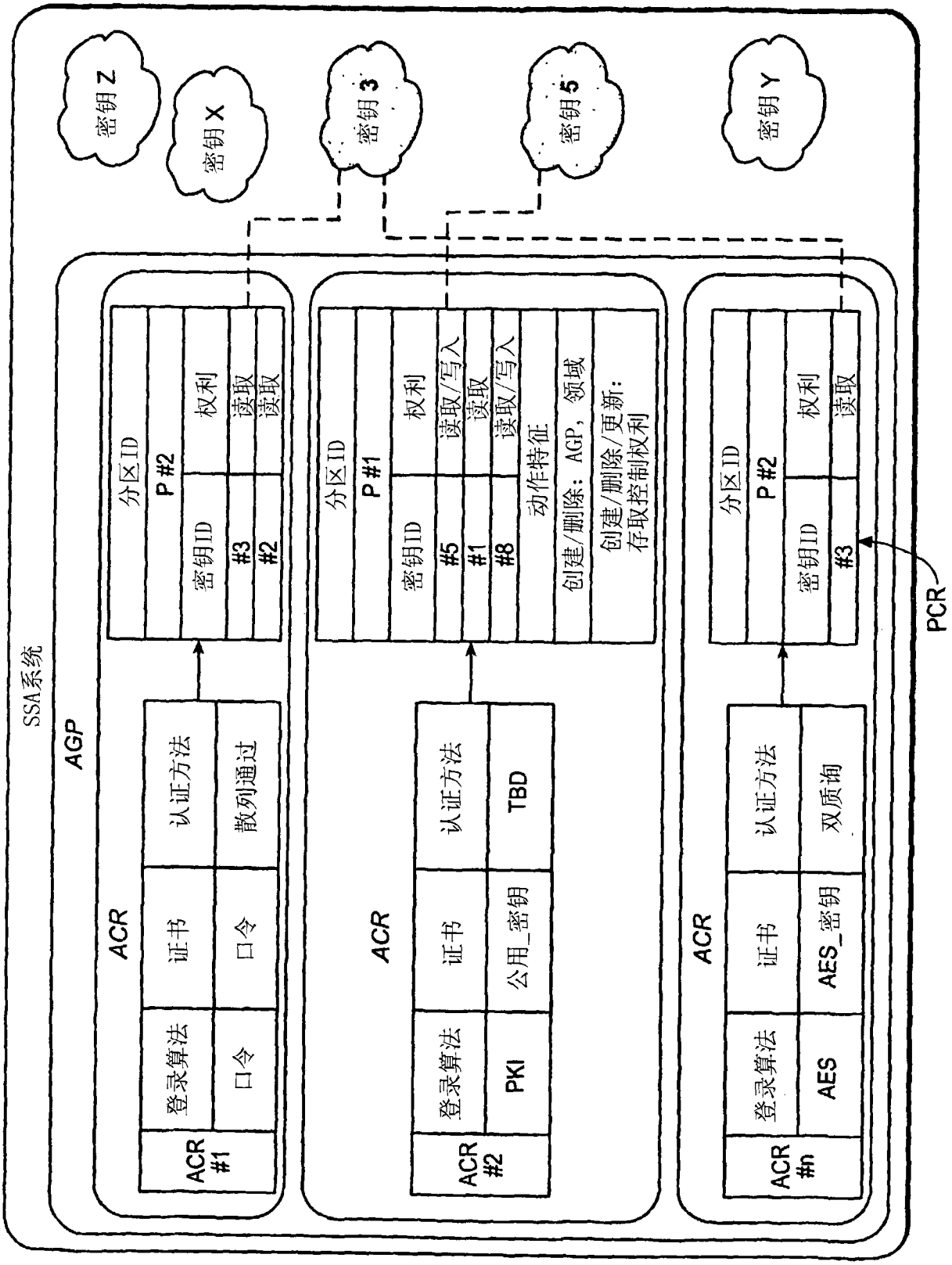

SSA系统
AGP
ACR
ACR #1
登录算法
口令
证书
口令
认证方法
散列通过
分区ID
P #2
密钥ID
权利
#3
读取
#2
读取
密钥 Z
密钥 X
密钥 3
密钥 5
密钥 Y
ACR
ACR #2
登录算法
PKI
证书
公用_密钥
认证方法
TBD
分区ID
P #1
密钥ID
权利
#5
读取/写入
#1
读取
#8
读取/写入
动作特征
创建/删除：AGP，领域
创建/删除/更新：
存取控制权利
ACR
ACR #n
登录算法
AES
证书
AES_密钥
认证方法
双质询
分区ID
P #2
密钥ID
权利
#3
读取
PCR

图 5

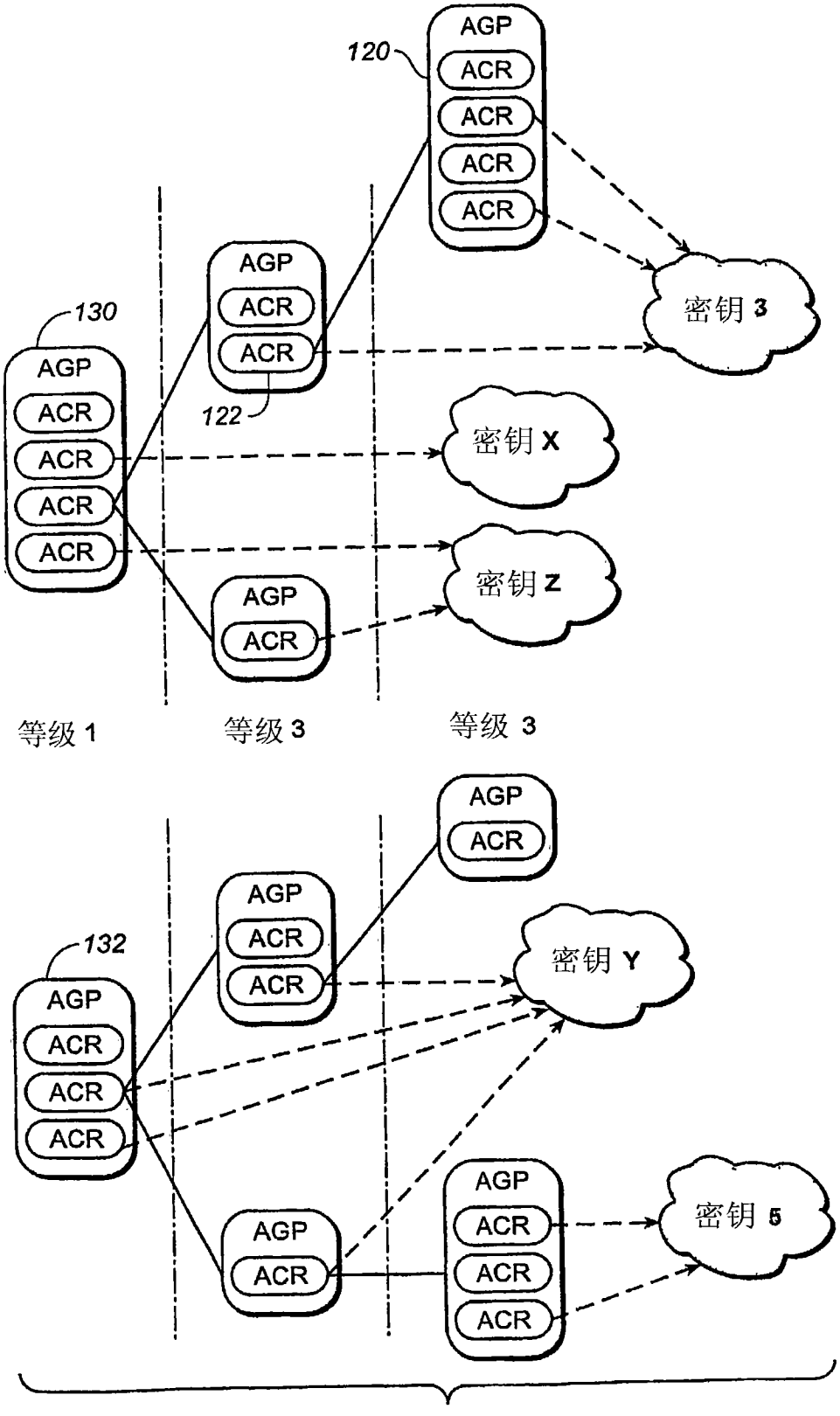

120
AGP
ACR
ACR
ACR
ACR
密钥 3
130
AGP
ACR
ACR
ACR
ACR
AGP
ACR
ACR
122
密钥 X
密钥 Z
AGP
ACR
等级 1
等级 3
等级 3
132
AGP
ACR
ACR
ACR
AGP
ACR
ACR
密钥 Y
AGP
ACR
AGP
ACR
ACR
ACR
密钥 5

图 6

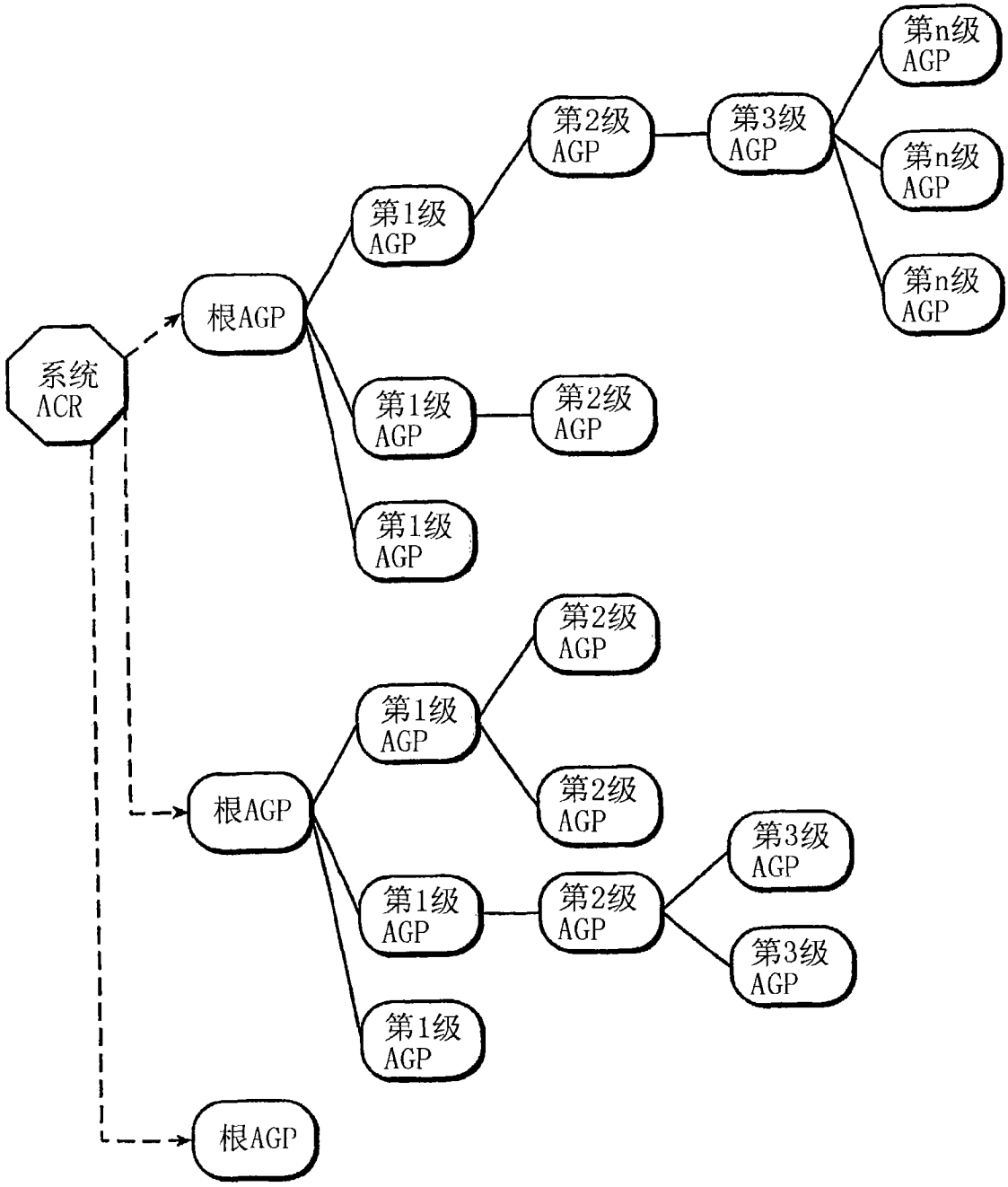

系统
ACR
根AGP
第1级
AGP
第2级
AGP
第3级
AGP
第n级
AGP
第n级
AGP
第n级
AGP
第1级
AGP
第2级
AGP
第1级
AGP
根AGP
第2级
AGP
第1级
AGP
第2级
AGP
第1级
AGP
第2级
AGP
第3级
AGP
第3级
AGP
第1级
AGP
根AGP

图 7

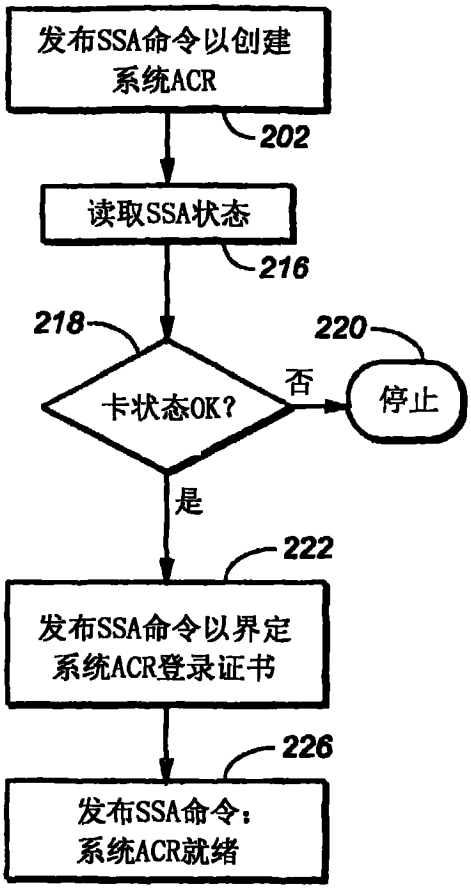

发布SSA命令以创建系统ACR
202
读取SSA状态
216
218
卡状态OK?
否
220
停止
是
222
发布SSA命令以界定系统ACR登录证书
226
发布SSA命令：系统ACR就绪

图 8A

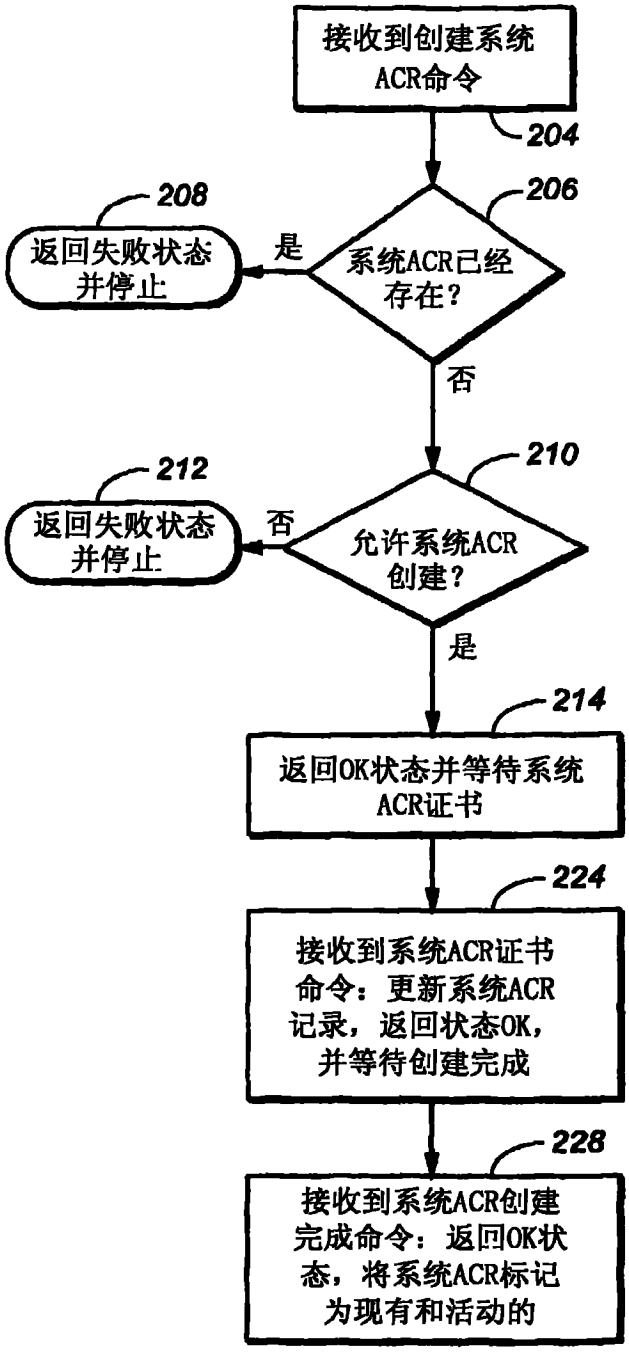

接收到创建系统ACR命令
204
206
208
返回失败状态并停止
是
系统ACR已经存在?
否
210
212
返回失败状态并停止
否
允许系统ACR创建?
是
214
返回OK状态并等待系统ACR证书
224
接收到系统ACR证书命令：更新系统ACR记录，返回状态OK，并等待创建完成
228
接收到系统ACR创建完成命令：返回OK状态，将系统ACR标记为现有和活动的

图 8B

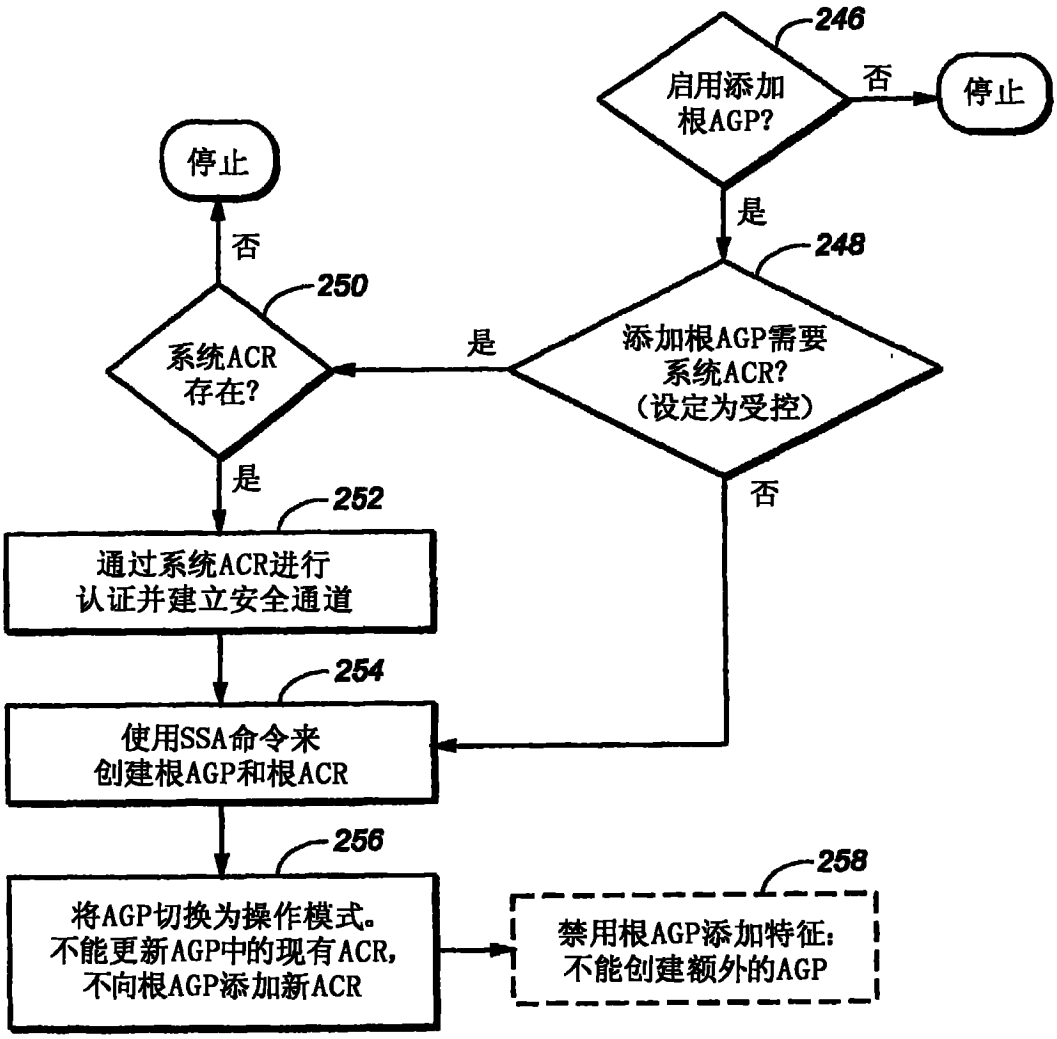

246
启用添加根AGP?
否
停止
是
248
添加根AGP需要系统ACR?（设定为受控）
是
250
系统ACR存在?
否
停止
是
252
通过系统ACR进行认证并建立安全通道
254
使用SSA命令来创建根AGP和根ACR
256
将AGP切换为操作模式。不能更新AGP中的现有ACR，不向根AGP添加新ACR
258
禁用根AGP添加特征：不能创建额外的AGP

图 9

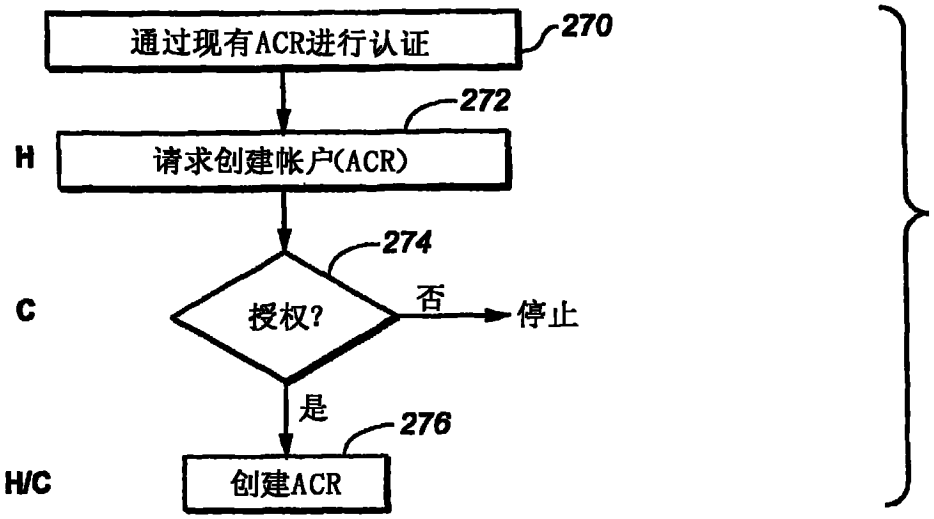

通过现有ACR进行认证
270
272
H
请求创建帐户(ACR)
274
C
授权?
否
停止
是
276
H/C
创建ACR

图 10

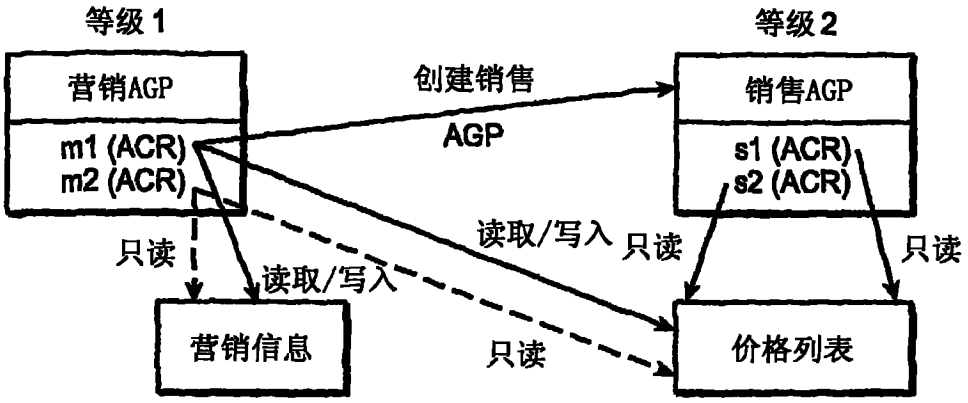


图 11

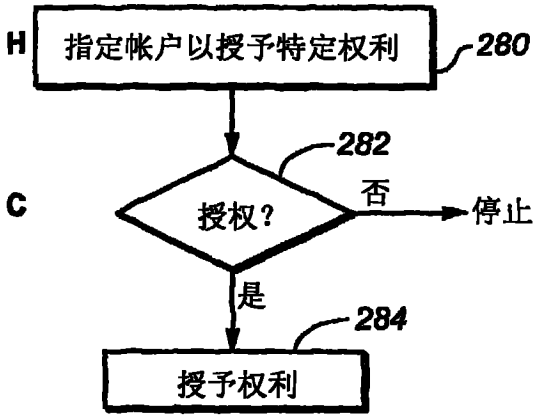


图 12

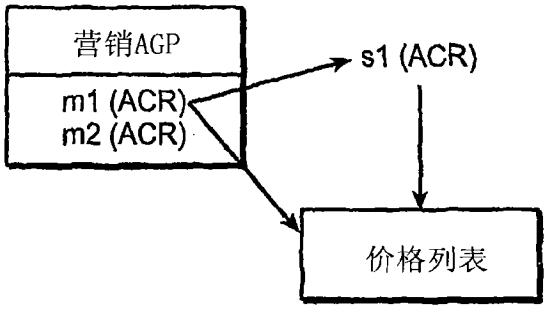


图 13

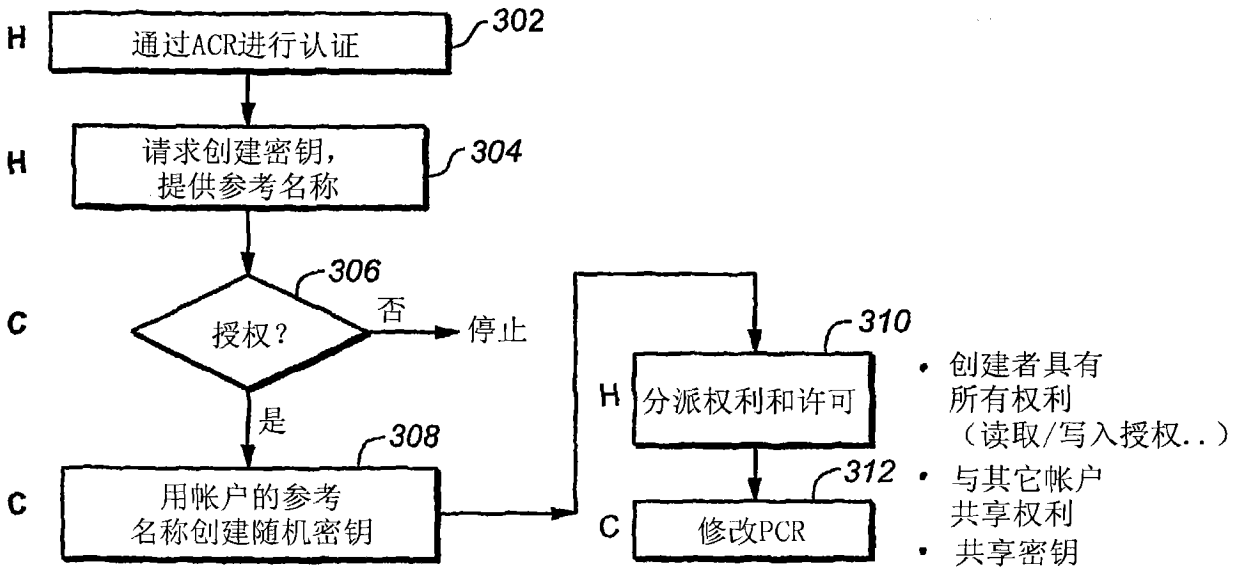


图 14

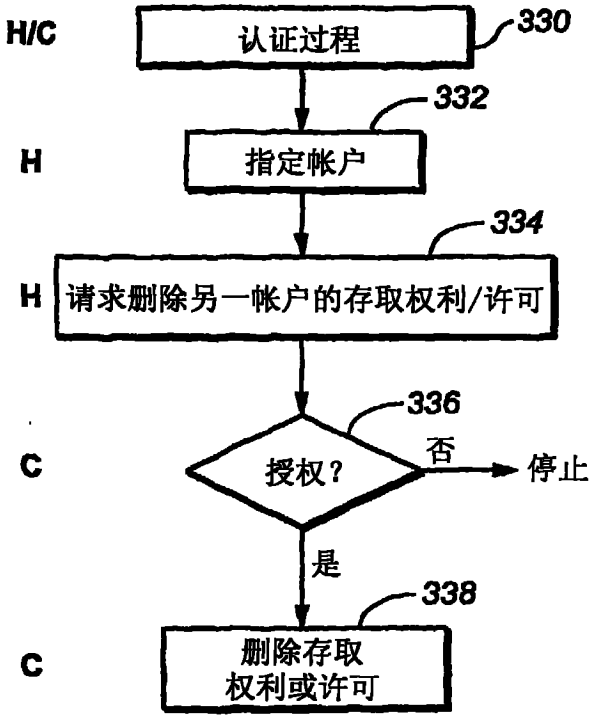

H/C
认证过程
330
332
H
指定帐户
334
H
请求删除另一帐户的存取权利/许可
336
C
授权？
否
停止
是
338
C
删除存取
权利或许可

图 15

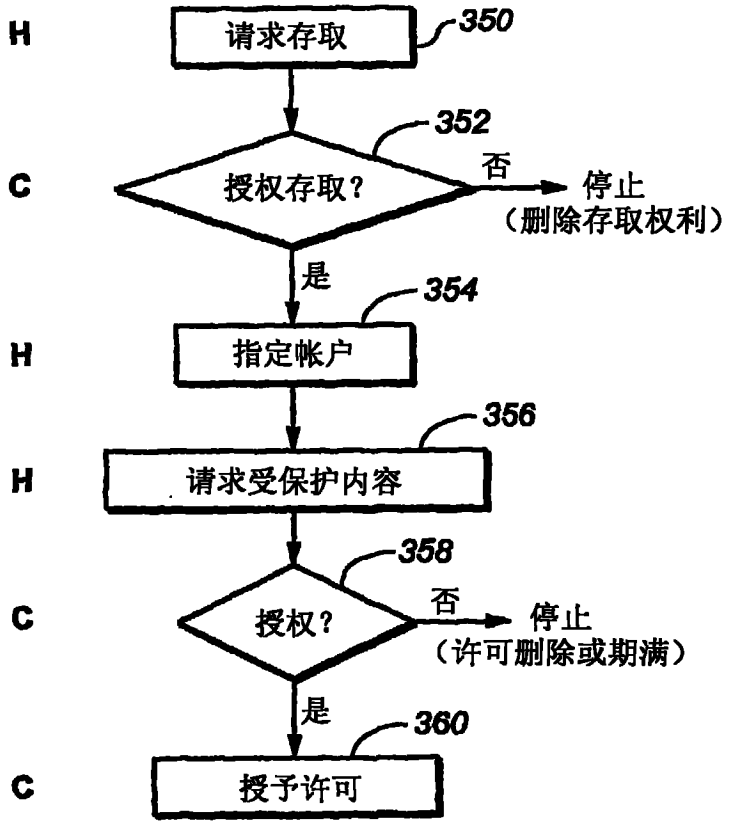

H
请求存取
350
352
C
授权存取？
否
停止
（删除存取权利）
是
354
H
指定帐户
356
H
请求受保护内容
358
C
授权？
否
停止
（许可删除或期满）
是
360
C
授予许可

图 16

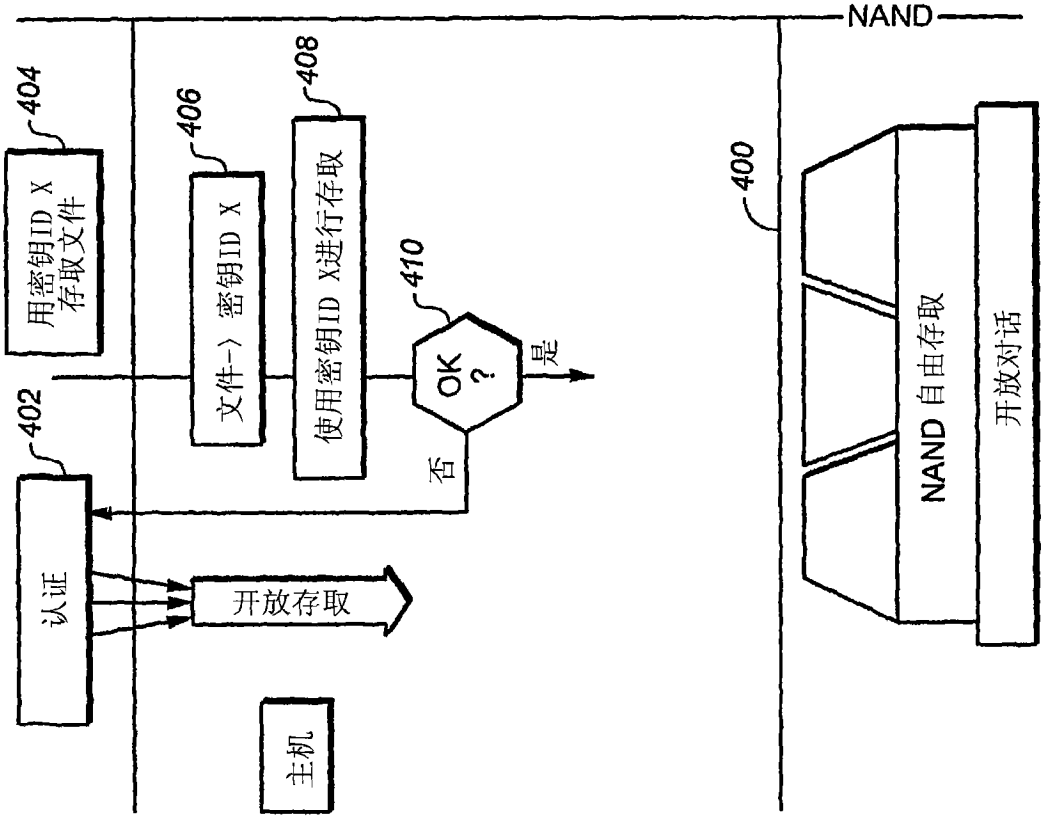

NAND
404
用密钥ID X存取文件
406
文件-> 密钥ID X
408
使用密钥ID X进行存取
410
OK ?
是
否
400
NAND 自由存取
开放对话
402
认证
开放存取
主机

图 17A

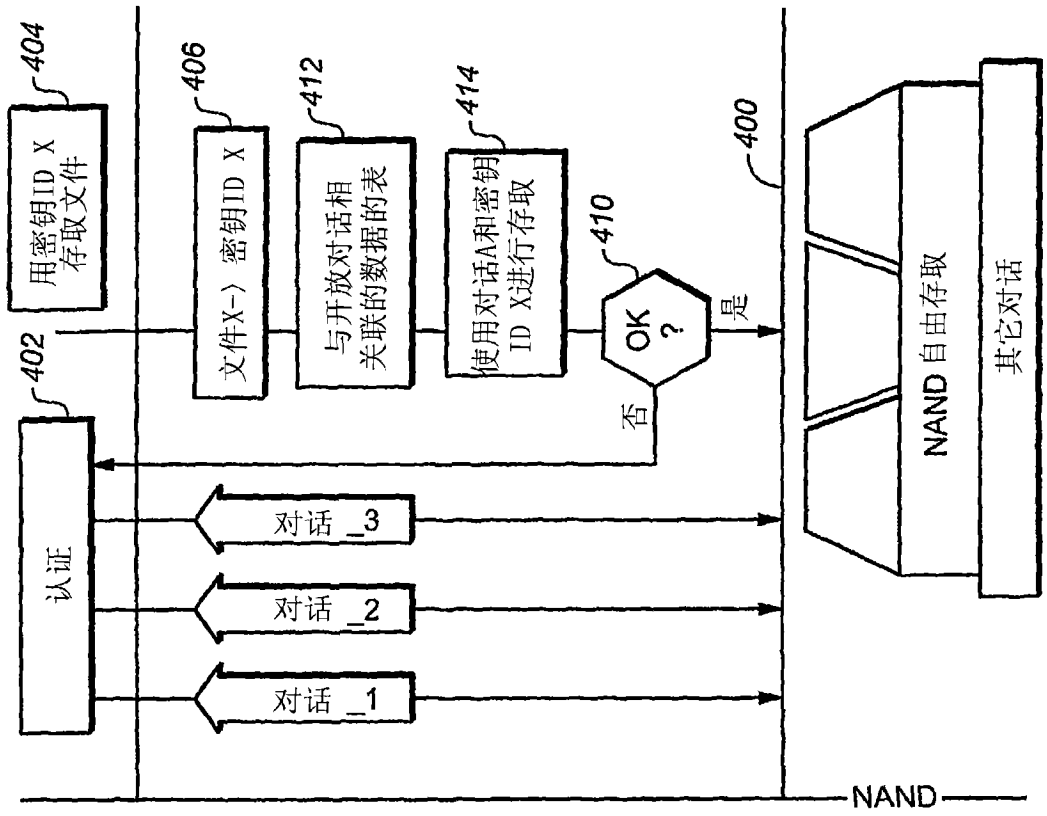

404
用密钥ID X
存取文件
406
文件X-〉密钥ID X
412
与开放对话相
关联的数据的表
414
使用对话A和密钥
ID X进行存取
410
OK
?
是
否
400
402
认证
对话 _3
对话 _2
对话 _1
NAND 自由存取
其它对话
NAND

图 17B

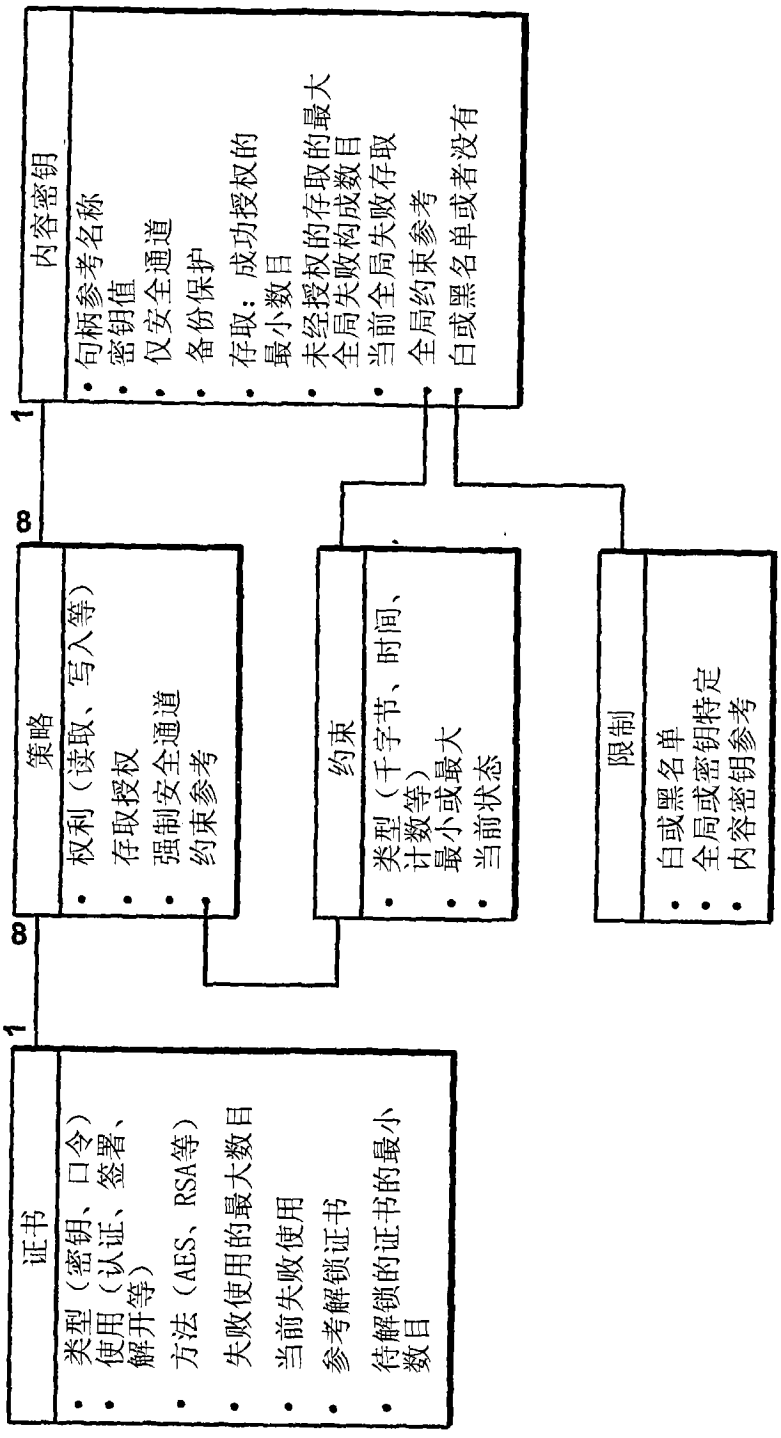

内容密钥
• 句柄参考名称
• 密钥值
• 仅安全通道
• 备份保护
• 存取：成功授权的最小数目
• 未经授权的存取的最大全局失败构成数目
• 当前全局失败存取
• 全局约束参考
• 白或黑名单或者没有
1
8
策略
• 权利（读取、写入等）
• 存取授权
• 强制安全通道
• 约束参考
约束
• 类型（千字节、时间、计数等）
• 最小或最大
• 当前状态
限制
• 白或黑名单
• 全局或密钥特定
• 内容密钥参考
8
1
证书
• 类型（密钥、口令）
• 使用（认证、签署、解开等）
• 方法（AES、RSA等）
• 失败使用的最大数目
• 当前失败使用
• 参考解锁证书
• 待解锁的证书的最小数目

图 18

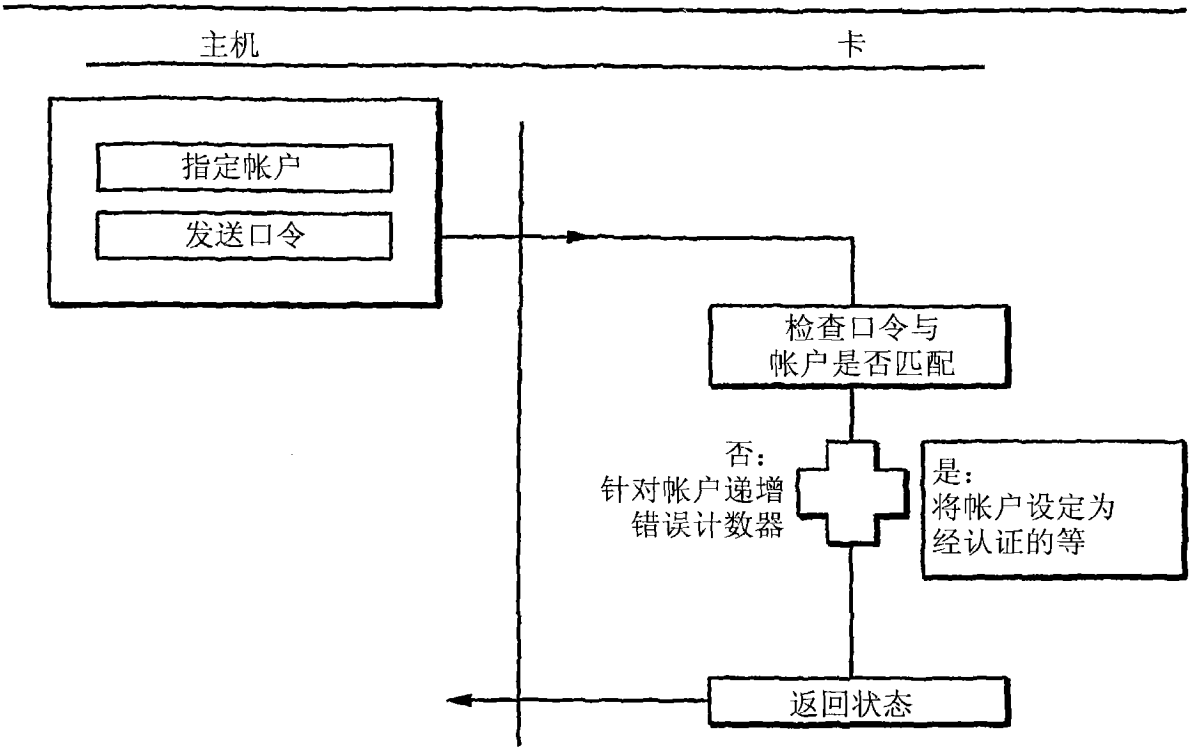

主机
卡
指定帐户
发送口令
检查口令与
帐户是否匹配
否：
针对帐户递增
错误计数器
是：
将帐户设定为
经认证的等
返回状态

图 19

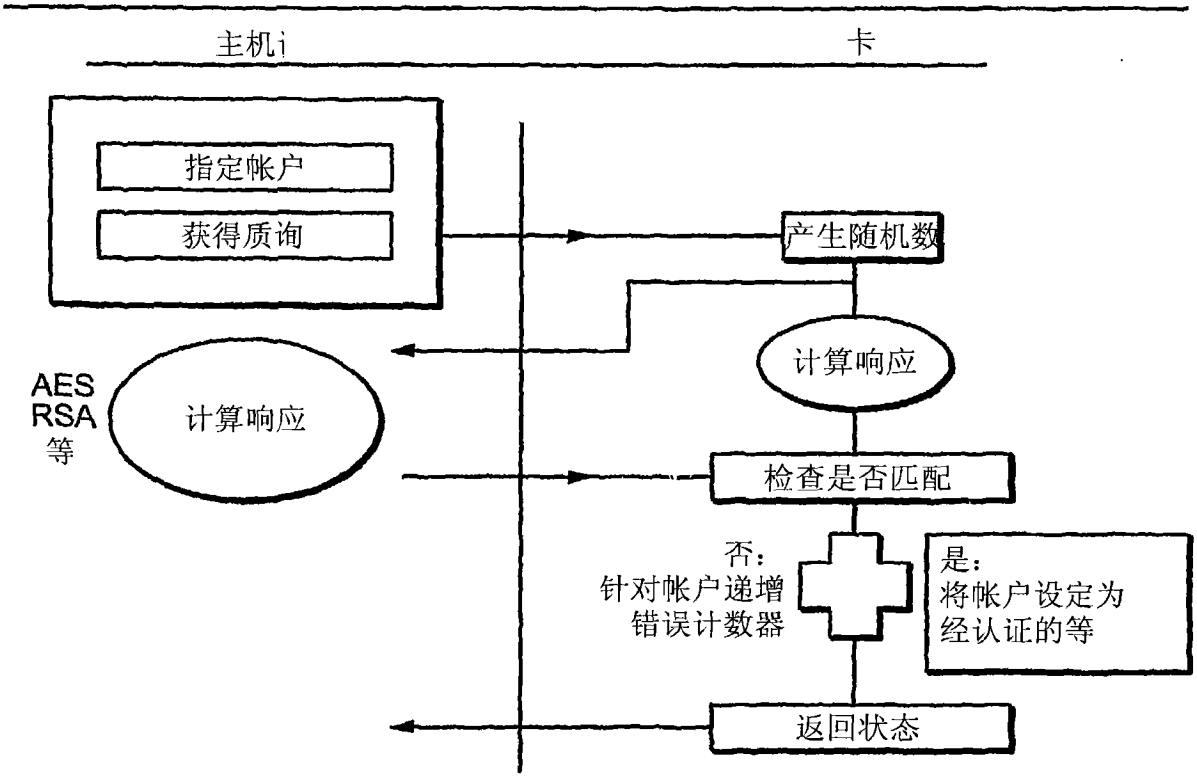

主机i
卡
指定帐户
获得质询
产生随机数
计算响应
AES
RSA
等
计算响应
检查是否匹配
否：
针对帐户递增
错误计数器
是：
将帐户设定为
经认证的等
返回状态

图 20

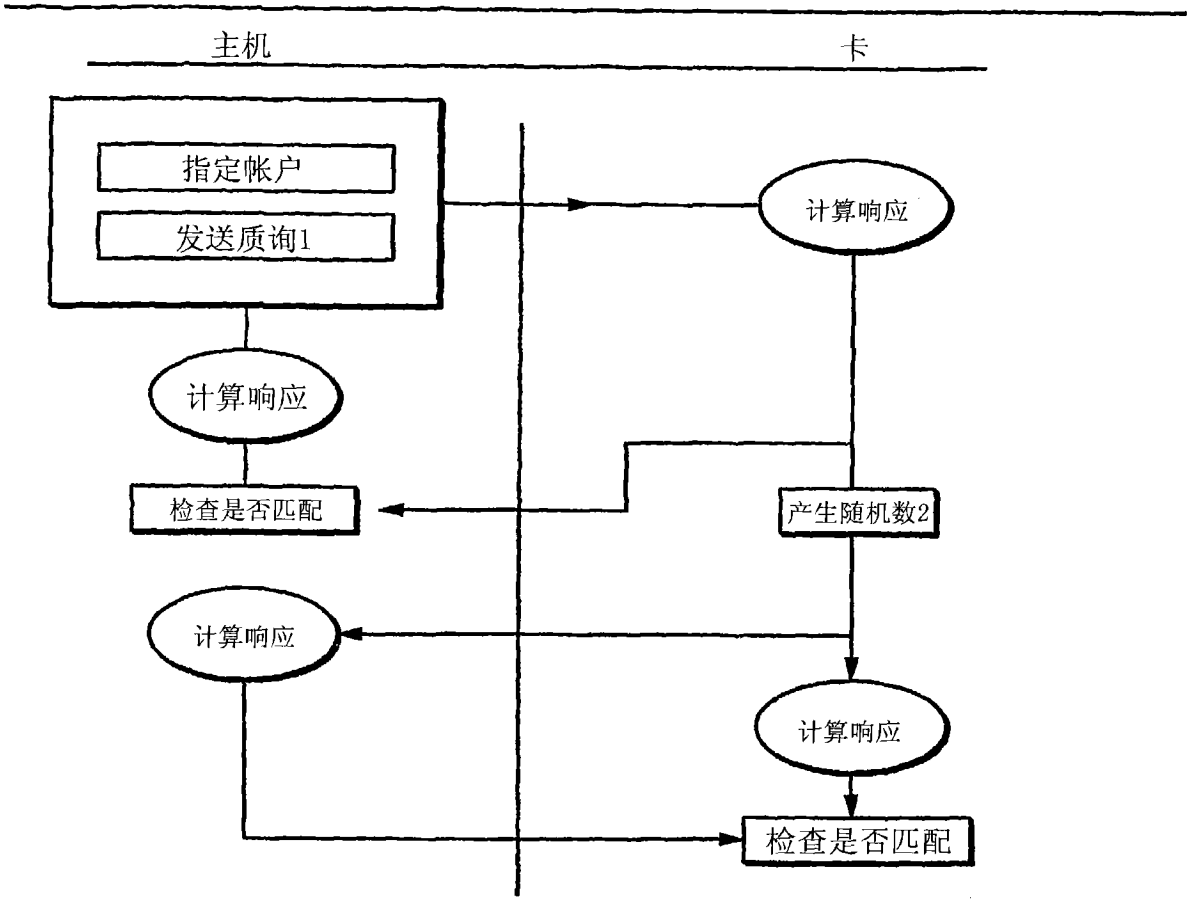

主机
卡
指定帐户
发送质询1
计算响应
计算响应
检查是否匹配
产生随机数2
计算响应
计算响应
检查是否匹配

图 21

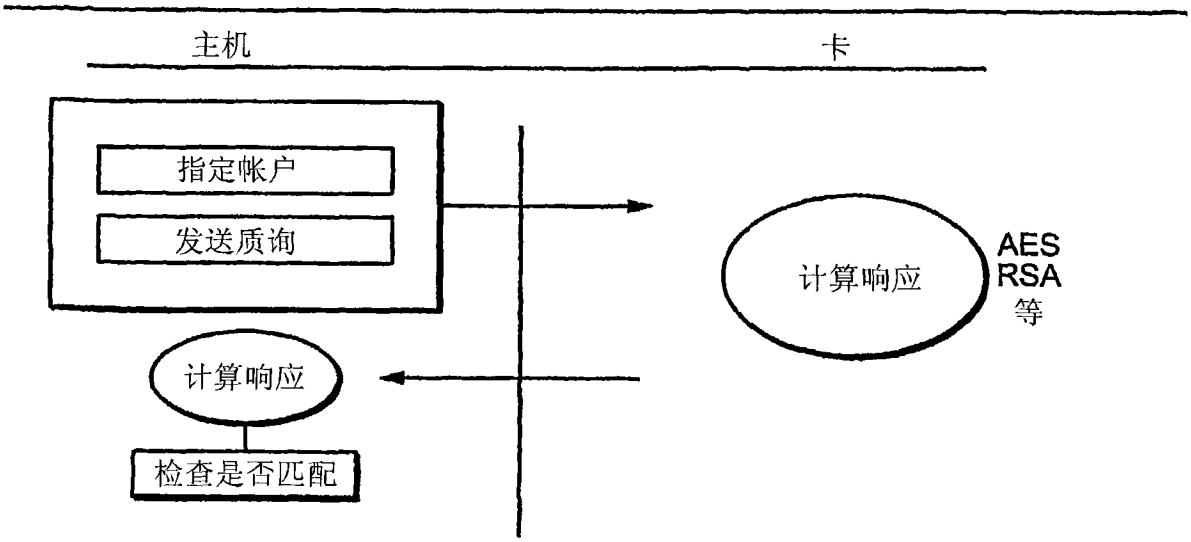

主机
卡
指定帐户
发送质询
计算响应
AES
RSA
等
计算响应
检查是否匹配

图 22