(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102402657 A
(43)申请公布日 2012.04.04

(21)申请号 201010286283.2

(22)申请日 2010.09.15

(71)申请人 联想（新加坡）私人有限公司
地址 新加坡新加坡市新技术园区

(72)发明人 戴维·C.·查利纳
约翰·H.·尼克尔森三世
约瑟夫·庞尼斯 罗德·D.·沃特曼

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 曾贤伟

(51)Int.Cl.
G06F 21/00(2006.01)

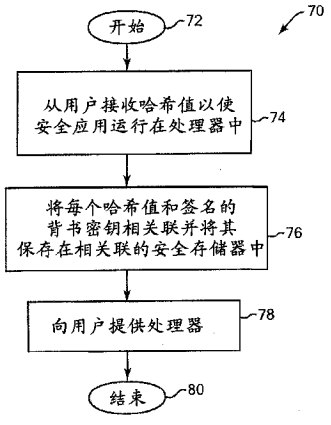
权利要求书 3 页 说明书 10 页 附图 4 页

(54)发明名称

用于使能安全处理器上的应用的装置和方法

(57)摘要

使能计算机系统的安全处理器中的应用的方法和装置。在一个方面，安全处理器装置包括处理器和与处理器连接的存储器，并可操作地保存安全表。安全表保存不同的核准的背书密钥和不同值，每个值都关联于一个背书密钥。每个保存值是从处理器中将被执行的关联背书密钥核准的不同应用获得的。



CN 102402657 A

1. 一种提供安全处理器的方法，所述方法包括：

接收多个值，每个值用于识别能够在所述安全处理器上执行的不同应用；和

通过在所述安全处理器能够访问的存储器中保存背书密钥和接收到的所述多个值关联不同的核准的背书密钥和每个接收到的值，其中使用所保存的背书密钥和关联值中的至少一个来允许在所述安全处理器上执行不同应用中的一个。

2. 根据权利要求 1 所述的方法，其中，

所述不同应用包括不同的安全架构应用，每一个安全架构应用能够在所述安全处理器上实现不同的安全架构，其中每一个安全架构与至少一个哈希算法和至少一个加密算法相关联。

3. 根据权利要求 2 所述的方法，其中，

所述安全架构应用包括可信平台模块应用，每一个可信平台模块应用能够在所述安全处理器上实现不同的 TPM 架构。

4. 根据权利要求 1 所述的方法，其中，

所述不同应用包括不实现安全架构的应用。

5. 根据权利要求 1 所述的方法，其中，

每一个值是哈希值，所述哈希值是通过对由所述哈希值识别的应用施加哈希算法而获得的。

6. 根据权利要求 1 所述的方法，其中，

在所述安全处理器访问的非易失性存储器的安全表中保存所述背书密钥和关联值。

7. 根据权利要求 1 所述的方法，进一步包括：

在所述存储器中保存至少一个无关联值的额外核准的背书密钥，其中用户能够将所述额外核准的背书密钥与所述用户提供的值相关联。

8. 一种安全处理器装置，包括：

处理器；和

存储器，连接于所述处理器并可操作地保存安全表，所述安全表保存了多个不同的核准的背书密钥和多个不同的值，每个值关联于一个背书密钥，其中每个保存的值是通过由处理器将要执行的关联背书密钥核准的不同应用获得的。

9. 根据权利要求 8 所述的安全处理器装置，其中，

所述不同应用包括不同的安全架构应用，每一个安全架构应用能够在所述处理器上实现不同的安全架构，每一个安全架构使用不同组的加密和解密算法。

10. 根据权利要求 9 所述的安全处理器装置，其中，

所述安全架构应用包括可信平台模块应用，每一个可信平台模块应用能够在所述安全处理器上实现不同的 TPM 架构。

11. 根据权利要求 9 所述的安全处理器装置，其中，

所述不同应用包括不实现安全架构的应用。

12. 根据权利要求 8 所述的安全处理器装置，其中，

所述不同的值是不同的哈希值，每一个哈希值是通过对应用施加哈希算法而从不同应用获得的。

13. 根据权利要求 12 所述的安全处理器装置，其中，

当所请求的应用将被加载到所述处理器中时，所述处理器比较通过对所请求的应用进行哈希获得的哈希值和所述安全存储器中保存的哈希值，以确定所请求的应用是否被核准在所述处理器中执行。

14. 根据权利要求 13 所述的安全处理器装置，其中，

当基于用户将所请求的应用加载到所述处理器中的请求而所述从处理器卸载已加载的应用时，处理器可操作地对所述已加载的应用进行以获得新的哈希值，对于所述已加载的应用在所述安全表中保存所述新的哈希值，并且将已加载的应用加密并存储到连接到所述处理器的存储设备。

15. 根据权利要求 8 所述的安全处理器装置，其中，

所述存储器是安全的、非易失性存储器。

16. 根据权利要求 8 所述安全处理器装置，其中，

在所述存储器中保存了至少一个无关联值的额外核准的背书密钥，其中能够将额外核准的背书密钥与用户提供的哈希值相关联。

17. 一种在安全处理器中安全地提供应用的方法，所述方法包括 ：

接收在所述安全处理器中加载所请求的应用的请求 ；

比较通过处理所请求的应用获得的值和在所述安全处理器的存储器中保存的多个保存值中的至少一个，其中保存值和获得的值之间的匹配表示所请求的应用被核准在所述安全处理器中执行 ；以及

如果在获得的值和保存值之间发现匹配则在安全处理器中执行所请求的应用。

18. 根据权利要求 17 所述的方法，其中，

所述安全存储器中保存的每个值关联于所述安全存储器中保存的不同的核准的背书密钥。

19. 根据权利要求 18 所述的方法，其中，

获得的值是通过对所请求的应用进行哈希获得的哈希值，而保存值是哈希值。

20. 根据权利要求 17 所述的方法，进一步包括 ：

在加载所请求的应用之前，在处理器中卸载已加载的应用。

21. 根据权利要求 20 所述的方法，其中，

当所请求的应用不适合于与所述处理器连接的当前可利用的存储器时，从所述处理器卸载已加载的应用。

22. 根据权利要求 20 所述的方法，其中，

所述已加载的应用是当所请求的应用需要执行不同的安全架构应用时从所述处理器卸载的安全架构应用。

23. 根据权利要求 20 所述的方法，其中，

卸载所述已加载的应用包括 ：通过对所述已加载的应用进行哈希并对于所述已加载的应用在所述安全表中保存新的哈希值，获得所述新的哈希值。

24. 根据权利要求 23 所述的方法，其中，

卸载所述已加载的应用包括 ：将所述已加载的应用加密并保存到与所述安全处理器连接的存储设备。

25. 根据权利要求 24 所述的方法，其中，

所述已加载的应用是安全架构应用，而加密使用与所述安全架构相关联的加密算法。

26. 根据权利要求 19 所述的方法，进一步包括 ：

接收安装用于所述安全处理器的新的应用的请求，其中对所述新的应用进行哈希以获得新的哈希值 ；和

在所述安全处理器的所述存储器中保存所述新的哈希值，其中所述新的哈希值关联于所述存储器中保存的背书密钥。

27. 一种计算机系统，包括 ：

输入设备，可操作地提供从用户接收到的对计算机系统的输入，所述输入设备包括用于识别所述用户的安全输入设备 ；

安全处理器，连接于所述输入设备，可操作地从用户接收输入并运行对于所述处理器核准的应用 ；和

存储器，连接于所述安全处理器，可操作地保存安全表，所述安全表保存多个不同的核准的背书密钥和多个不同的哈希值，每一个哈希值关联于一个背书密钥，其中每一个哈希值是从将被加载到处理器中的关联背书密钥核准的不同应用获得的，并且其中所述不同应用包括每一个在所述安全处理器中实现不同安全架构的不同安全架构应用。

28. 根据权利要求 27 所述的安全计算机系统，其中，

所述安全输入设备包括指纹读取器和智能卡读取器中的至少一个，其中所述不同应用包括不实现安全架构的应用和用于与所述安全输入设备接口的应用。

29. 根据权利要求 27 所述的安全计算机系统，其中，

当所请求的应用将被加载到所述处理器中时，所述处理器比较通过对所请求的应用进行哈希而获得的哈希值和所述安全存储器中保存的哈希值，以确定所请求的应用是否被核准加载到所述处理器中。

30. 一种计算机可读介质，包括由计算机实现的程序指令并用于安全地提供在安全处理器中加载的应用，所述程序指令用于 ：

接收在所述安全处理器中加载所请求的应用的请求 ；

比较通过处理所请求的应用获得的值和在所述安全处理器的存储器中保存的多个保存值中的至少一个，其中保存值和获得的值之间的匹配表示所请求的应用被核准在所述安全处理器中执行 ；以及

如果在获得的值和保存值之间发现匹配则在安全处理器中执行所请求的应用。

用于使能安全处理器上的应用的装置和方法

技术领域

[0001] 本发明涉及安全地保护计算机数据，尤其涉及计算机系统中提供的用于实现安全特征的安全处理器。

背景技术

[0002] 十分关心计算机系统上保存的信息的安全性。已经实施了许多不同的技术以确保这些信息，这些技术涉及访问信息所需的从计算机系统中安装的安全应用软件到的硬件密钥。

[0003] 另一种确保信息安全的方法公知为来自可信计算组 (TCG) 的可信平台模块 (TPM) 规范。在这个规范中，在制造过程中在计算机的电路板上提供包括可编程微控制器在内的标准芯片集，并且该标准芯片集被用来保存所期望受保护的计算机系统的信息及确保其安全，即使能有效的可信计算特征。在微控制器中运行的安全框架（即，功能和应用程序接口 (API)）可被称为 TPM。TPM 可提供各种特征，包括随机数生成器、用于密码密钥的安全生成的设施、以及限制密钥的使用（例如，签名及验证、和 / 或加密及解密）的能力。

[0004] 当电子商务、电子政府和电子商业随着网络犯罪的威胁增大而成长时，出现了使用安全技术来保护数据并认证身份和交易的应对措施。涉及这些身份和交易的处理的信息技术拥有者期望使用为他们自身环境和威胁概况所定制的特定加密算法。他们期望使用与期望的加密算法相关联的 TPM 的特定特征组实现方式以支持他们的端到端系统和操作模型的所需安全等级。例如，标准的通用 TPM 可使用包括先进加密标准 (AES) 的特别组的加密算法。然而，特别的政府组织可使用不同于 AES 的其他算法，诸如使用 GOST(Gosudarstvennyi 标准）加密的俄罗斯政府或使用 SMS4 加密的中国政府。诸如美国国家安全局等其他组织则使用他们不希望向公众披露的他们自己的算法。

[0005] 不同对象的这种不同需求典型地需要每个 TPM 芯片集都按照他的特定终端用户所期望的安全架构和算法而特殊地被定制。因此，实施特定的哈希及加密算法和其他功能的不同的安全架构将会必须在交付给终端用户之前在不同的 TPM 芯片集上被加载。这需要针对每个不同的用户规范来制作不同的 TPM 芯片，这将会极大地增加 TPM 的制造成本和由此带来的用户在他们的系统上安装这种类型的安全性方面的成本。

[0006] 此外，TPM 芯片的现有实现方式不允许 TPM 架构从微控制器中被安全地卸载以允许在芯片上加载其他的应用，另外他们也不允许将最新版本的已卸载的 TPM 架构安全地重新加载到芯片中。

[0007] 相应地，期望一种灵活及安全地使用安全的可编程微控制器的方法，以支持各种安全架构和他们的加密算法，并将这些包括在 TPM 硬件的不同实例的仿真当中。本发明解决了上述需求。

发明内容

[0008] 本申请的发明涉及在计算机系统的安全处理器提供的应用。在本发明的一个方面

中，一种提供安全处理器的方法包括接收多个值，每个值用于识别能够在所述安全处理器上执行的不同应用。通过在所述安全存储器能够访问的存储器中保存背书密钥和所述多个值来关联不同的核准的背书密钥和每个接收到的值，其中使用所保存的背书密钥和关联值中的至少一个来允许在所述安全处理器上执行不同应用中的一个。

[0009] 在本发明的另一方面，一种安全处理器装置包括：处理器和连接于所述处理器并可操作地保存安全表的存储器。所述安全表保存了多个不同的核准的背书密钥和多个不同的值，每个值关联于一个背书密钥，其中每个保存的值是通过由处理器将要执行的关联背书密钥核准的不同应用获得的。

[0010] 在本发明的另一方面，一种在安全处理器中安全地提供应用的方法包括：接收在所述安全处理器中加载所请求的应用的请求，比较通过处理所请求的应用获得的值和在所述安全处理器的存储器中保存的多个保存值中的至少一个，其中保存值和获得的值之间的匹配表示所请求的应用被核准在所述安全处理器中执行。如果在获得的值和保存值之间发现匹配则在安全处理器中执行所请求的应用。

[0011] 在本发明的另一方面，一种计算机系统包括：可操作地提供从用户接收到的对计算机系统的输入的输入设备，所述输入设备包括用于识别用户的安全输入设备。安全处理器连接于所述输入设备，可操作地从用户接收输入并运行对于所述处理器核准的应用。存储器，连接于所述安全处理器，可操作地保存安全表，所述安全表保存多个不同的核准的背书密钥和多个不同的哈希值。每一个哈希值关联于一个背书密钥，其中每一个哈希值是从将被加载到处理器中的关联背书密钥核准的不同应用获得的。不同应用包括每一个都在安全处理器中实现不同安全架构的不同安全架构应用。

[0012] 本发明提供了在支持各种核准的安全架构和他们的算法方面的灵活性的安全处理器，并允许用户选择在处理器中执行的应用。这允许提供商产生能够满足期望使用不同架构和算法的众多不同用户的需求的一种处理器。本发明还允许应用从安全处理器被卸载并加载到安全处理器中，以及安装用于安全处理器中，从而保持了应用的安全性和最新更新。

附图说明

[0013] 图 1 是示出了适用于本发明的计算机系统 10 的方框图；

[0014] 图 2 是能够在与图 1 的安全处理器相连的非易失性存储器中保存的、本发明的安全表的示意图；

[0015] 图 3 是示出了用于为用户准备并提供安全处理器的本发明的方法的流程图；

[0016] 图 4 是示出了用于将应用加载到安全处理器中的本发明的方法的流程图；以及

[0017] 图 5 是示出了用于安装安全处理器所使用的新的应用的本发明的方法的流程图。

具体实施方式

[0018] 本发明涉及安全地保护计算机数据，尤其涉及计算机系统中提供的用于实现安全特征的安全处理器。提供如下的具体实施方式以使得本领域普通技术人员可以制作并使用本发明，并考虑专利申请及其需求的上下文来提供具体实施方式。对于这里所说明的优选实施方式和总的原理和特征的修改将会对于本领域技术人员而言是明显的。因此，本发明

并不应局限于所示的实施例，而是包括与这里所描述的原理和特征相一致的最大范围。

[0019] 以特定实施方式中提供的特定系统和方法来主要地描述了本发明。然而，本领域普通技术人员可以理解的是，在其他实施方式中有效地操作这些方法和系统。例如，本发明所使用的计算机系统实施方式可采用几种不同的形式。

[0020] 为了更加特别地描述本发明的特征，请结合图 1 至图 5 参考下面的讨论。

[0021] 图 1 是示出了适用于本发明的计算机系统 10 的方框图。系统 10 是具有多种形式中的任一种的计算机系统。例如，计算机系统 10 可以是大型计算机、台式计算机、工作站、便携式计算机、或电子设备。系统 10 包括诸如来自可信计算组 (TCG) 的可信平台模块 (TPM) 等安全架构、或是适用于本发明的其他安全系统，以确保系统 10 的数据和功能安全不受到未授权的访问和操纵。系统 10 包括输入部分 12、安全部分 14 和标准部分 16。

[0022] 输入部分 12 可包括允许用户向系统 10 输入数据并认证用户对系统的身份的多种不同的输入设备。例如，在所示出的实施例中，系统 10 中包括卡读取器 20、键盘 22、和 / 或指纹读取器 24。卡读取器 20 可读取诸如智能卡等处理器卡，其包括用于识别用户并保存用户的关联信息的安全信息。键盘 22 可用来输入识别用户的密码。指纹读取器 24 可读取用户的唯一的指纹图案以识别用户。这些输入设备因此可被用于用户认证用途，以允许已授权的用户访问系统 10 中的安全数据。这里，术语“用户”是指系统 10 的任意用户，无论是否授权。TPM 标准中的术语“拥有者”是指已加载特定的 TPM 架构并具有访问该架构的最高认证的用户。

[0023] 系统 10 的安全部分 14 用来确保仅由已授权的用户访问及使用系统的数据和应用。在所述的实施例中，系统中包括的可编程安全处理器 26 是专用于安全功能的（在某些实施例中还可用于其他功能）。处理器可执行在处理器中加载的各种应用。处理器 26 典型地实现了“安全架构”，其在这里被称为由处理器 26 中加载的安全架构应用所确定的、系统 10 中实现的特别安全特征和功能（例如，API 功能、算法）。通常以硬件实现的安全架构的实例在本发明中可以软件方式仿真，以使得处理器 26 支持不同的架构。

[0024] 例如，处理器 26 可实现 TPM 安全架构，这是用于确保计算机数据安全而公知的标准。TPM 架构可在由制造商包含在计算机的主板或其他电路上的、安全的、专用芯片集上实现。在其他实施例中，TPM 架构可以在计算机系统 10 的另一现有的芯片上实现。其他的实施例还可使用不同的标准或所有权安全架构以实现安全特征。TPM 的典型安全功能包括随机数生成、加密密钥的安全生成、安全存储、限制密钥的使用的能力（诸如签名及验证）、和 / 或加密及解密。例如，在一个实施例中，处理器 26 可以是运行 IBM 公司的 Java 卡开放式平台 (JCOP) 操作系统的 H8 处理器，一种实现适用于本发明的许多安全特征的公知操作系统。TPM 应用可被加载到处理器 26 当中并被 JCOP 操作系统所实施以使能安全架构。

[0025] 处理器 26 可典型地加载有不同的安全架构，其中各架构可使用不同的安全算法和与该架构相关联的密钥，并实现不同组的安全功能。在本发明中，可从系统 10 的部分 16（或是其他的安全源）将不同的安全架构加载到处理器 26 上。

[0026] 此外，在处理器 26 上还可加载及运行不实现安全架构的其他应用。参考在处理器 26 中正在加载的特定安全架构的应用的依赖，这些应用可与特定的安全架构进行“绑定”。这个特征将会在下面更加详细地说明。

[0027] 非易失性存储器 28 包含在安全部分 14 当中并与处理器 26 相连接。例如，存储

器 28 可以是快闪存储器、电擦除可编程只读存储器 (EEPROM)、或是其他类型的存储器。在所述实施例中，存储器 28 是不易受到篡改而读取其数据内容的安全存储器。在某些实施例中，非易失性存储器 28 可包含在与处理器 26 的相同集成电路芯片中或处理器 26 的封装当中。

[0028] 在本发明中，如下面将会更加详细地说明，非易失性存储器 28 保存用于确定加载到处理器 26 中的应用是否被认证的哈希值和背书密钥 (endorsement key) 的安全表，并使能灵活地及安全地支持处理器 26 中的各种不同的安全架构和程序。存储器 28 还保存关于执行处理器的安全架构的安全功能的其他安全数据。某些实施例中的非易失性存储器还可用于保存已加载的安全架构和 / 或处理器 26 中加载的应用。

[0029] 在其他实施例中，额外的存储器 (未示出) 可与处理器 26 相连接，用于保存已加载的安全架构、已加载的应用、或是其他程序。例如，可连接安全的随机访问存储器 (RAM)、额外的非易失性存储器等。

[0030] 系统 10 的标准部分 16 可与处理器 26 相连接并包括系统的剩余标准部件。这样的部件典型地包括微处理器或 CPU 30、存储器 32(随机访问存储器 (RAM)、只读存储器 (ROM) 等)、输出设备 34(视频监视器、音频扬声器、打印机等)、以及其他类型的计算机部件。微处理器可与存储器设备和其他部件接口以控制系统 10 的操作，包括执行数据操纵、计算、输入 / 输出、以及其他典型的功能。

[0031] 还可典型地包含诸如硬盘驱动器等存储设备 36，以保存将要被系统 10 使用的数据和应用。在本发明中，利用加密和其他安全方法，在存储设备 36 上安全地保存将被加载到处理器 26 当中的安全应用和处理器 26 和微处理器 30 使用的其他应用等应用。在其他实施例中，替代硬盘驱动器还可使用不同的存储设备 36，诸如存储器、磁带、光学存储器 (CD-ROM、DVD-ROM) 等。在所述实施例中，系统 10 的标准部分 16 与处理器 26 相连接，而输入部分 12 与处理器 26 相连接，从而向部分 16 提供的输入可首先被安全部分 14 检查用于认证和安全性。

[0032] 图 2 是关于在与安全处理器 26 相连接的非易失性存储器 28 中保存的本发明的安全表 50 的示意图。表 50 可保存关于允许经核准的应用在处理器 26 上被执行并确定将要加载及执行哪一种安全架构的信息。

[0033] 在所述实施例中，表 50 包括大量的背书密钥 (EK) 值 52。例如，在 TPM 标准中，背书密钥 (例如，在制造期间内对于 TPM 架构随机生成的) 被用来允许安全交易的执行并识别在处理器 26 中将被加载的真实的 TPM 架构。背书密钥是包括公有密钥和私有密钥的密钥对 ；背书密钥的私有部分被保存在表 50 中。可选的，背书密钥的公有和私有部分被保存在表 50 中。尽管术语“背书密钥”用在 TPM 架构中使用的 TPM 标准中，但是这个术语在这里可笼统地用于任何标准中的相似使用并可与任何应用一起使用。

[0034] 在生成了应用的背书密钥之后，提供商 (或其他认证的实体) 发行证书，该证书包括背书密钥的公有部分并提供用于识别与背书密钥相关联的应用的信息。例如，这个信息可以是应用的哈希值，或也可以描述应用 (例如，关于安全架构应用，指定所使用的算法等)。提供商利用提供商密钥的私有部分签名证书，这允许提供商密钥的公有部分被用来验证证书信息是否为真实的及是否来自提供商。因此，例如，证书可利用加密和解密算法的关联组测试已识别的 TPM 架构是否为特定类型的 TPM 架构。

[0035] 在本发明中，多个背书密钥的多个背书密钥值52可被保存在表50中，以允许多个不同的安全架构或应用中的任意一个被加载到处理器26中。表50中的每个背书密钥都是唯一的并与发行的证书中指定为特定应用的使用相关联。

[0036] 表50还可保存哈希值54，其中每个哈希值都与对应保存的背书密钥值52相关联。哈希值54是对特定的应用和/或数据应用的加密的哈希函数的结果，并唯一地识别哈希后的应用/数据。由提供商将哈希值与背书密钥值52相关联表示应用/数据已经被授权并核准在处理器26中使用。用于生成列54中的哈希值的特定哈希算法与所使用的特定安全架构相关联，并依赖于该所使用的特定安全架构。

[0037] 例如，本发明的处理器26的提供商可在表50中保存背书密钥值，其中背书密钥值中的每一个都与用于授权及指定处理器26中所使用的不同类型的安全架构的证书相关联。提供商还可保存制造商已经授权并核准用于处理器26中保存的的背书密钥的应用的哈希值。此外，用户能够在表50中保存新的哈希值、和/或与用户签名的证书相关联的新的背书密钥。这些特征将会在下面更加详细地说明。

[0038] 图3是示出了用于准备并提供用户的安全处理器26的本发明的方法70的流程图。方法70是由处理器26的制造商或是可提供处理器26中已核准的背书密钥的授权实体所使用；所有这样的制造商或授权实体被统称为处理器26的“提供商”。

[0039] 方法开始于72，并在步骤74，提供商接收希望使用处理器26的用户（例如，客户）的哈希值。每个哈希值都代表特定的应用（诸如TPM应用等安全架构应用）和期望被加载到安全处理器26中并在其上运行的任意关联数据。每个哈希值都利用对于提供商而言未知的哈希算法获得的；因此，应用和应用所使用的算法的实现对于提供商而言是未知的，这正是某些用户所期望的。可选的，提供商还可对期望由处理器26支持的应用应用哈希算法以获得某些或是全部的哈希值。

[0040] 在步骤76，提供商将每个不同的哈希值与由处理器26为该哈希值（例如，可由处理器26签名的、用于形成背书密钥对的随机数）生成的背书密钥相关联，并保存背书密钥和哈希值。在认证机构发布的证书中能够提供背书密钥的公有部分。对于每个不同的哈希值，在与处理器26相连的安全非易失性存储器28的安全表50中保存背书密钥值和相关联的哈希值。所保存的背书密钥值可以是背书密钥的私有部分（或可选的，公有部分或两部分）。每个背书密钥对于哈希值而言可以是不同的；或是，在可选实施例中，对于多个哈希值表项可使用相同的背书密钥。每个所保存的哈希值用于识别用户所期望的不同应用；如果在步骤74中两个或更多个用户提供了相同的哈希值，则对于那个应用在表50中仅需要保存一个哈希值和背书密钥。在某些实施例中，相同的应用的不同实例可提供不同的哈希值（例如，当具有不同的设定、数据等），从而每个不同的实例可具有在安全表50中保存的、对应的不同哈希值和背书密钥表项。与特定安全架构绑定的应用可通过多种方法的任意一种表示在安全表50中具有那种关系，例如，绑定应用具有包括安全架构应用所需的链接或指针的哈希值，或是其他的状态指示器或指针等。在某些实施例中，在安全表50的每个表项中保存额外的标识符，其用于匹配表项与所请求的应用，这将会在下面描述。

[0041] 在步骤78，提供商向用户提供处理器26（或使得处理器26被提供给用户）。处理器26可被包括在提供给用户的计算机系统10当中。用户可随后在处理器26中加载他或她所期望的应用，如参考图4更加详细地描述的。在步骤80，处理随后完成。

[0042] 在某些实施例中，提供商还可在表 50 中保存额外的核准的背书密钥值，其尚未与任何的哈希值相关联。这使得用户可以加载他或她自己的哈希值并将其与所保存的、核准的背书密钥相关联。在某些实施例中，提供商还可允许用户在表 50 中保存他或她自己的背书密钥和哈希值。

[0043] 利用图 3 的方法，本发明允许提供商提供计算机系统中的安全处理器，而不使得提供商知晓将被加载到处理器 26 中的应用的特定的实现和 / 或算法。用户无需给出用户期望在期望的安全架构中实现或与用于期望的安全架构的任何实际的应用或算法，而仅仅需要向提供商给出哈希值。通过将每个应用哈希值和背书密钥相关联，这实现了提供商认证已授权给处理器 26 使用的应用。

[0044] 本发明允许提供商节省在为提供商的客户所期望的每个类型的安全架构提供不同的处理器 26 的制造成本。提供商可为多种不同类型的安全架构（或其他应用）保存哈希值和背书密钥，其中通过在加载时对安全架构应用进行哈希而使得用户可选择他或她所期望的架构，这将会匹配表 50 中的正确的哈希值和背书密钥。提供商可由此向所有的用户提供相同的处理器 26，并使得用户选择所期望的安全架构或应用以及与该应用相关联的特定算法。

[0045] 图 4 是示出了用于将应用加载到安全处理器 26 中的本发明的方法 100 的流程图。可利用处理器 26 的操作系统中运行的应用通过处理器 26 实现方法 100（和下面的方法 200）。可选的，可利用硬件（电路、逻辑门电路等）或硬件和软件的组合来实现方法 100 和 / 或 200。在计算机可读介质上保存实现本发明的全部或部分的程序指令，并可以对该计算机可读介质访问，该计算机可读介质诸如是电子、磁性、光学、电磁、红外或半导体介质，这样的例子包括存储器（随机访问存储器 (RAM)、只读存储器 (ROM) 等）、硬盘驱动器、光盘 (CD-ROM、DVD-ROM 等）。

[0046] 方法开始于 102，在步骤 104，处理器 26 接收用于加载应用到处理器 26 当中的请求。典型的，这个应用被安全地例如以加密形式保存在诸如硬盘驱动器 36 等存储设备或其他设备中，或是从诸如相连接的计算机网络等一些其他的源提供。这个请求可包括期望被加载的应用的标识符和应用的大小。例如，加密后的应用的现有哈希值可被提供为应用文件中的签名、和 / 或另一标识符或对保持应用的特定文件的参考。例如，请求可将 TPM 应用加载到当前没有已加载的 TPM 架构的处理器 26 当中。在另一例子中，请求可将 TPM 应用加载到处理器 26 当中，以安装将替换不同的当前加载的 TPM 架构的架构。在再一例子中，请求可将非 TPM 应用加载到处理器 26 当中。例如，当应用加载请求被发送到提供将被加载的应用的存储设备 36（或其他的源）时，可接收到请求；可通过处理器 26 的操作系统的滤波器驱动器解析这个加载请求。例如，可通过将加载请求中指定的应用和安全表 50 中列出的应用进行比较来识别加载请求中指定的应用，例如，可比较加密后的应用文件中的哈希值和表 50 中的哈希值，或是比较不同的应用标识符和表 50 中保存的标识符。

[0047] 在下一个步骤 106，处理核对所请求的加载是否需要处理器切换当前加载的应用（在某些情形下，包括已加载的安全架构）。典型的，如果所请求的应用需要比处理器 26 当前可以利用的存储器更多的存储器，则需要卸载处理器 26 的当前加载的应用。或是，如果所请求的应用是安全架构应用并且存在不同的当前加载的安全架构，则已加载的安全架构需要被去除，这是因为在某些实施例中一次仅一个安全架构可在处理器 26 上运行。在其他

的可选实施例中，处理器 26 能够同时运行两个或更多个安全架构，在这种情形下，如果存在充足的存储器可以被利用，则无需卸载不同的当前加载的安全架构（除非是用户请求卸载）。在其他的实施例中，已加载的安全架构可以被指定为“单个使用”、和 / 或处理器 26 在硬件或软件中设置具有“保险”或旗标，这表示当前加载的安全架构不允许被从处理器 26 中卸载。例如，步骤 106 的核对可包括核对所请求的应用是否与当前没有被加载的、特定的安全架构绑定（需要在特定的安全架构下运行）（例如，通过核对表 50 中是否存在任何这样的绑定链接）。某些应用可以不与任何的安全架构绑定，并与其并行地被执行。

[0048] 如果当前加载的应用将被从处理器中卸载，则处理继续前进到可选步骤 108，其中识别用户。例如，通过处理器 26 的操作系统可请求用户以安全的、认证的方式识别他们自己，诸如向智能卡读取器 20 中插入智能卡，该智能卡保存有用于识别用户的数据；或是利用手指接触指纹读取器 24；或是利用键盘 22 输入密码；或是通过另一安全识别技术（或通过上述这些的任意组合）。所请求的加载可依赖于用户的身份；例如，只有 TPM 处理器 26 的拥有者被允许切换 TPM 架构或加载应用。如果在步骤 108 中没有识别出合适的用户，则放弃方法 100。在其他的实施例中，无需执行用户识别步骤。

[0049] 处理继续前进至步骤 110，其中根据已知的加密哈希算法对当前加载的应用和任何相关联的数据进行哈希，并且利用这个应用的相关联的背书密钥在安全表中保存哈希值。利用当前的哈希值可覆写表中保存的这个应用的先前保存的哈希值。当前的哈希值可不同于先前保存的值，这是因为保存了自从先前哈希值以来应用或它的数据发生的改变。例如，存在与 TPM 应用相关联的新的密码和 / 或新的存储根密钥 (SRK)，其不同于在该应用的先前哈希值中包括的密码或 SRK。因此，本发明可防止在处理器 26 中加载并执行未授权的、较旧版本的应用，这是因为仅最新版本将会匹配当加载应用时表 50 中保存的哈希值（见下面的步骤 116-118）。在某些实施例中，可在安全表 50 中维护应用的原始哈希值；例如，如果被授权，这允许原始形式的应用被重新安装。

[0050] 在下一个步骤 112，处理利用与应用的安全架构相关联的加密算法加密已加载的应用。例如，对于加密可使用对称算法。此外，例如，还可在这个应用的加密文件中保存步骤 110 中在表 50 中保存的并从这个应用生成的哈希值，以便当加载应用时识别及使用。在诸如硬盘驱动器等系统 10 的存储设备 36 中保存已加密的应用。处理随后继续前进到步骤 114。

[0051] 如果在步骤 106 中确定无需从处理器 106 中去除当前加载的应用以加载所请求的应用，则处理继续前进至步骤 114。如上步骤 108-112 所述，步骤 114 也可以在当前加载的应用被卸载并在存储器中归档之后或过程中被执行。在步骤 114，所选择的应用被加载到处理器 26 的存储器（诸如非易失性存储器 28 或其他可利用的存储器）当中，利用与所请求的应用的安全架构相关联的合适算法将其解密，并利用与所请求的应用的安全算法相关联的合适加密哈希函数对其进行哈希（例如，通过如上所述的安全表 50 中的查找识别应用、它的对应的解密及哈希算法）。

[0052] 利用哈希算法执行哈希以得到用于识别这个特定应用和数据的哈希值。例如，用于 TPM 标准的标准哈希算法包括 SHA-1、SHA-256 或类似算法，并且所使用的加密 / 解密算法是先进加密标准 (AES)。

[0053] 根据不同的情况，步骤 114 中处理的“所选择的应用”可以是步骤 104 的所请求的

应用，或是不同的应用。例如，所选择的应用可以是步骤 104 中请求被加载的应用。或者，如果所请求的应用需要不是当前被加载的安全架构，则所选择的应用可以是所需求的安全架构应用（诸如 TPM 应用），随后在步骤 114 的后续迭代中，所选择的应用就是所请求的应用。

[0054] 在下一个步骤 116，处理比较关于所选择的应用的获取的哈希值和安全表 50 中一个或更多个保存的哈希值。在步骤 118，处理核对在所获取的哈希值和表中的哈希值之间是否发现了匹配。如果在比较了表 50 中的全部哈希值之后仍未发现匹配，则处理继续前进至步骤 120 以拒绝所选择的应用（例如，不激活应用、和将其从存储器中卸载），并使处理在 128 结束。

[0055] 如果发现了哈希值的匹配，则所选择的应用被认为是关联于表中保存的核准的背书密钥，因此核准并授权应用加载到这个特定处理器 26 当中并被其所使用。如上所述，每个背书密钥都关联于用于说明 / 识别应用的公有证书（诸如通过提供应用的哈希值）；由此可从表 50 中的背书密钥得知应用规范（诸如所使用的算法，除非这是机密的）。

[0056] 例如，如果所选择的应用是如上面步骤 108-112 中所述的已经先前被卸载的应用，则在表 50 中保存当前版本的应用的更新的哈希值。因此当被重新加载时，所卸载的应用将会匹配表 50 中的哈希值，而较旧版本的应用将不会匹配表 50 中的哈希值，这提供了额外的安全性。

[0057] 在步骤 122，在处理器 26 上激活所选择的应用，由此允许执行应用并使其可以被用户访问。如果所选择的应用是诸如 TPM 应用等安全架构应用，则激活新的架构。例如，如在表 50 中保存的，关联于匹配的哈希的背书密钥 (EK) 被设定或加载到处理器 26 当中作为有效的背书密钥。此外，还可生成用于初始化应用所需的任何其他数据并将其加载到处理器 26 的存储器当中；例如，当激活 TPM 架构时，可生成存储根密钥 (SRK) 并将其保存在安全的非易失性存储器 28 当中，并且用户可访问 TPM 架构并成为它的“拥有者”。

[0058] 在步骤 124，处理核对所请求的应用是否仍需要被加载。例如，这可以发生在当步骤 104 所请求的应用是需要（绑定于）与当前加载的安全架构不同的安全架构应用时；以这样的情形下，步骤 122 中激活的第一应用是所需要的安全架构应用。因此，如果所请求的应用仍需要在步骤 124 中被加载，则处理返回到步骤 114-122，以对所请求的应用进行哈希，确定是否被授权加载，并且激活应用。如果在步骤 124 中所请求的应用已经被加载并被激活，则处理结束于 128。

[0059] 应该值得注意的是，图 4 中的许多步骤无需以所示的顺序执行。例如，在步骤 108-112 从处理器卸载任何当前加载的应用之前，处理可首先在步骤 116-118 核对所选择的或所请求的应用的哈希值是否匹配表 50 中的哈希值，如果对于以这种顺序执行存在充足的可以利用的存储器空间的话。

[0060] 图 5 是示出了用于安装处理器 26 所使用的新的应用的本发明的方法 200 的流程图。方法开始于 202，并在步骤 204，处理器 26 接收关于安装新的应用的请求。这可以发生在当用户希望在存储设备（诸如硬盘驱动器 36 等）上安装应用并且应用可以被加载到处理器 26 中并在其上运行时。将被安装的应用可以是享用处理器 26 及其操作系统的安全特征的非安全架构应用。例如，实现蜂窝式电话的客户识别模块 (SIM) 卡或与其接口的应用、或是实现用户的指纹匹配的应用，都期望被安装用于处理器 26 及其安全加强的操作系统

和内存存储器使用。例如，当应用写请求发送到将会保存新的应用的存储设备 36 时，可检测请求；这个写请求可以被处理器 26 的操作系统的过滤器驱动器拦截。

[0061] 在安装应用的请求中，可提供应用的标识信息和大小。在可选的步骤 206，类似于上面参考图 4 所述的步骤 108，可识别用户以确定是否授权用户安装用于处理器 26 的新的应用。

[0062] 在某些实施例中，执行步骤 208，其中处理核对是否卸载当前加载的安全架构并使用不同的安全架构替代当前加载的安全架构。例如，可通过核对由处理器的过滤器驱动器拦截的写请求来执行上述核对，并且这个核对可包括例如比较应用和安全表 50 以发现与绑定于当前加载的安全架构的应用的匹配，这类似于关于图 4 所描述的。例如，某些绑定的应用可使用对于特定安全架构所特定的密钥或其他特征，由此仅在这个架构下可以被安装。因此，如果新的应用绑定于与当前加载的安全架构不同的安全架构，则当前加载的安全架构应该被卸载并加载所需要的安全架构。在不允许安全架构被卸载或改变的那些实施例中可跳过步骤 208。在允许两个或更多个安全架构同时地在处理器 26 上运行的其他可选实施例中，可能不需要执行步骤 208 的核对，也不需要安全架构被卸载。

[0063] 如果已加载的安全架构应该被卸载（例如，新的应用没有绑定于当前加载的安全架构），则处理继续前进至步骤 210，其中对已加载的安全架构应用进行哈希、加密及卸载至存储设备 36。这个步骤类似于如上所述的图 4 中的步骤 108-112。在步骤 212，所需要的（新的应用所绑定的）安全架构被加载、解密、与表中的哈希值进行比较、以及激活。这个步骤类似于如上所述的图 4 中的步骤 114-124。一旦新的应用被激活，则处理继续前进至步骤 214。如图 4 所示，如果新的安全架构的哈希值不匹配表 50 中的哈希值，则新的架构应用将不会被加载并且处理结束。

[0064] 如果在步骤 208 将不卸载已加载的安全架构（例如，新的应用绑定于当前加载的安全架构），或是在步骤 210-212 已经加载了所需要的安全架构，则处理继续前进至步骤 214，其中新的应用被加载到处理器 26 的存储器中（例如，从与计算机系统 10 相连的任何源，例如，磁盘、光学存储介质、网络等）。如果新的应用已经被加密，则利用与安全架构相关联（或是与应用绑定的安全架构相关联）的算法对其进行解密，并利用与这个安全架构相关联的哈希算法（例如，通过应用文件中保存的标识符或现有的哈希值识别的算法，这类似于图 4）对新的应用进行哈希。通过在与背书密钥相关联的安全表 50 中保存所得到的哈希值，在处理器 26 中注册所得到的哈希值。这个背书密钥可已经存在于表中作为处理器提供商提供并保存的非关联密钥并将被关联于用户最新安装的应用。或者，通过生成背书密钥的私有部分并将其保存在表 50 中，并生成将发行或提供给用户的密钥的公有部分，由处理器 26 的操作系统最新生成背书密钥。例如，诸如 JCOP 等操作系统具有它们自己的背书密钥，其中操作系统可对应用生成新的背书密钥并利用它自己的背书密钥的私有部分对密钥的公有部分签名。可选的，用户可签名新的背书密钥的公有部分并提供证书。

[0065] 在注册新的应用之后，在某些实施例中，可利用处理器 26 的操作系统的背书密钥重新签名整个安全表 50，这表示表是安全的。

[0066] 在步骤 216，利用相关联的加密算法加密新的应用，并在处理器 26 的存储器或系统 10 的存储设备 36 中安装或保存新的应用。处理随后结束于 218。

[0067] 尽管已经根据所示的实施例描述了本发明，但是本领域普通技术技术应该可以理

解的是，对于实施例存在各种变化并且这些变化都应包含在本发明的精神和范围之内。相应地，在不脱离所附的权利要求的精神和范围的前提下，本领域普通技术人员可以做出许多改变。

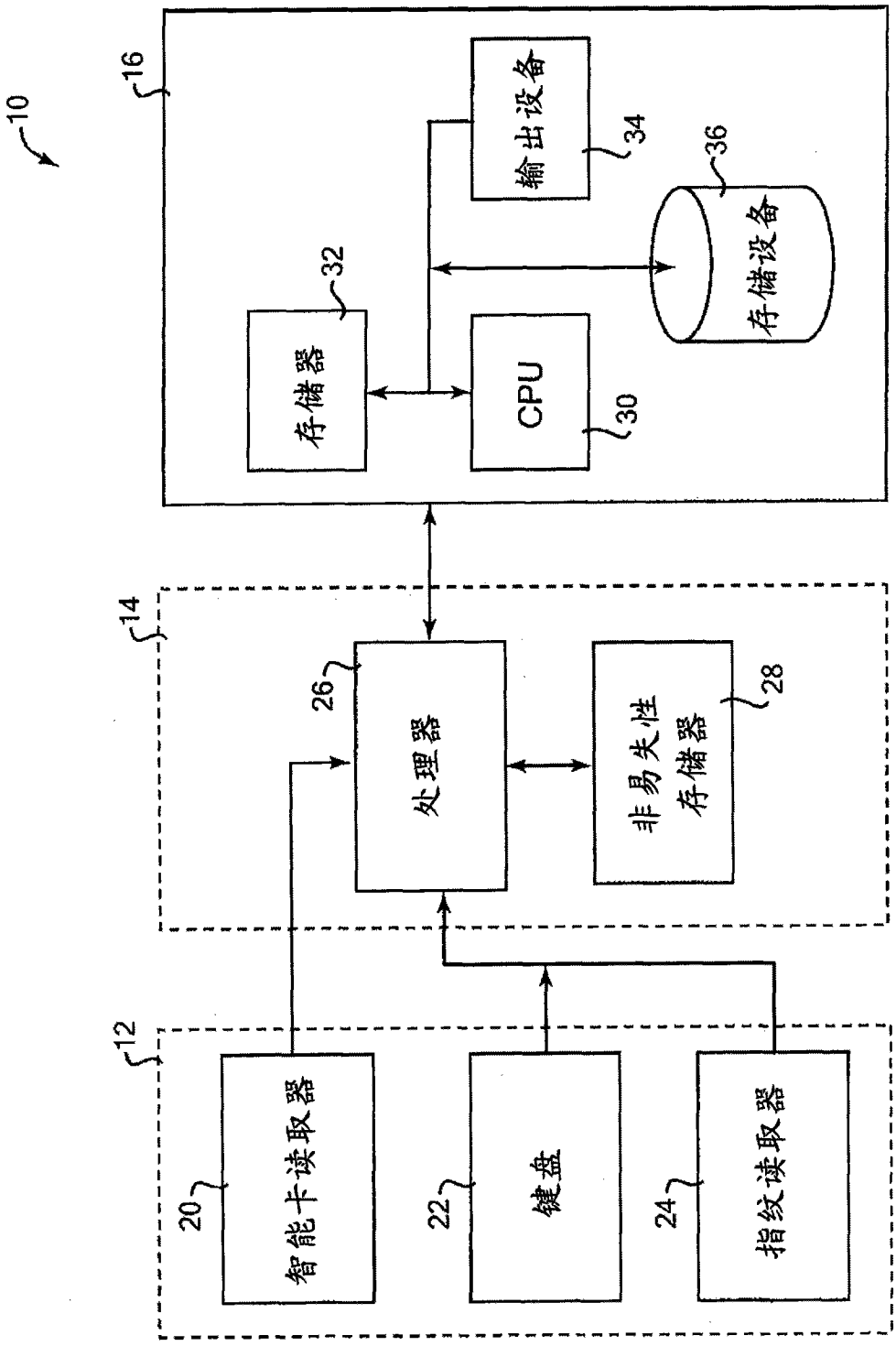

10
16
输出设备
34
36
存储设备
32
存储器
CPU
30
14
26
处理器
非易失性
存储器
28
12
智能卡读取器
20
22
键盘
24
指纹读取器

图 1

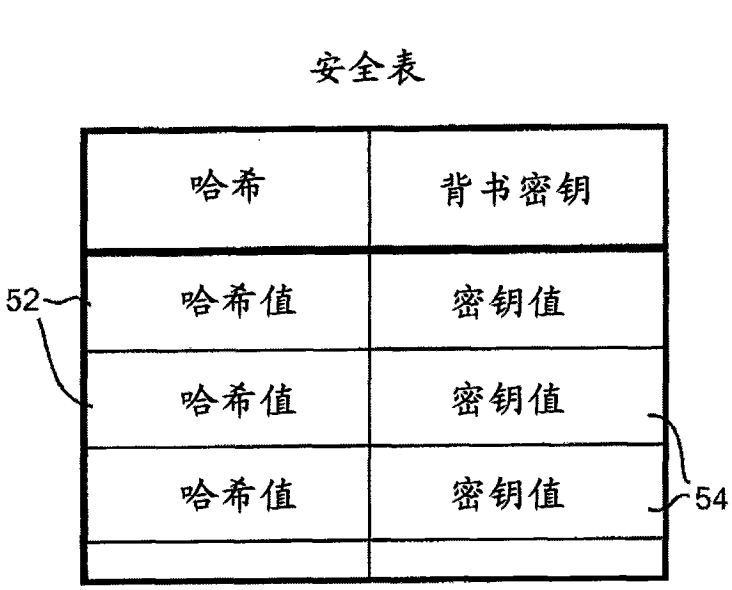

50
安全表
哈希
背书密钥
52
哈希值
密钥值
哈希值
密钥值
哈希值
密钥值
54

图 2

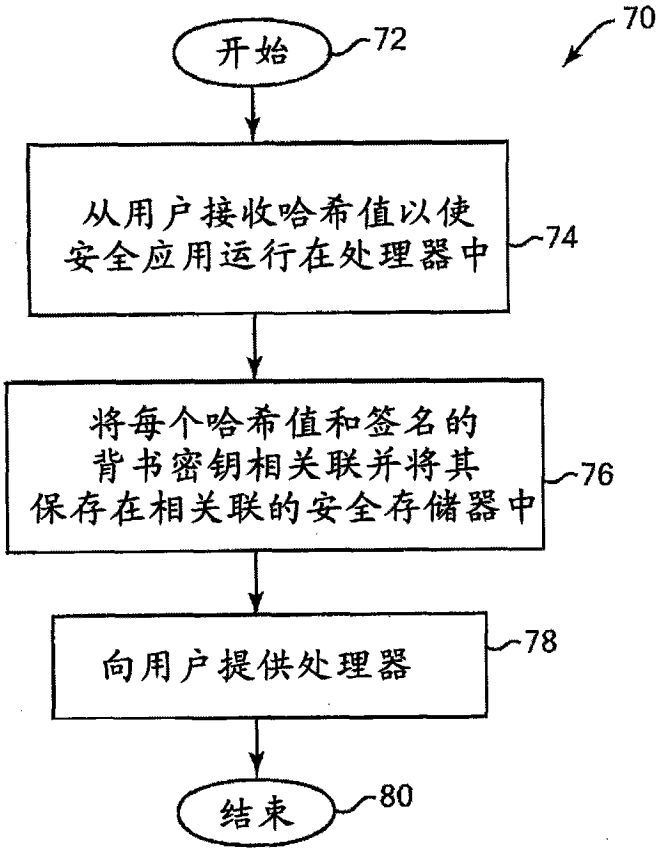

70
开始
72
从用户接收哈希值以使
安全应用运行在处理器中
74
将每个哈希值和签名的
背书密钥相关联并将其
保存在相关联的安全存储器中
76
向用户提供处理器
78
结束
80

图 3

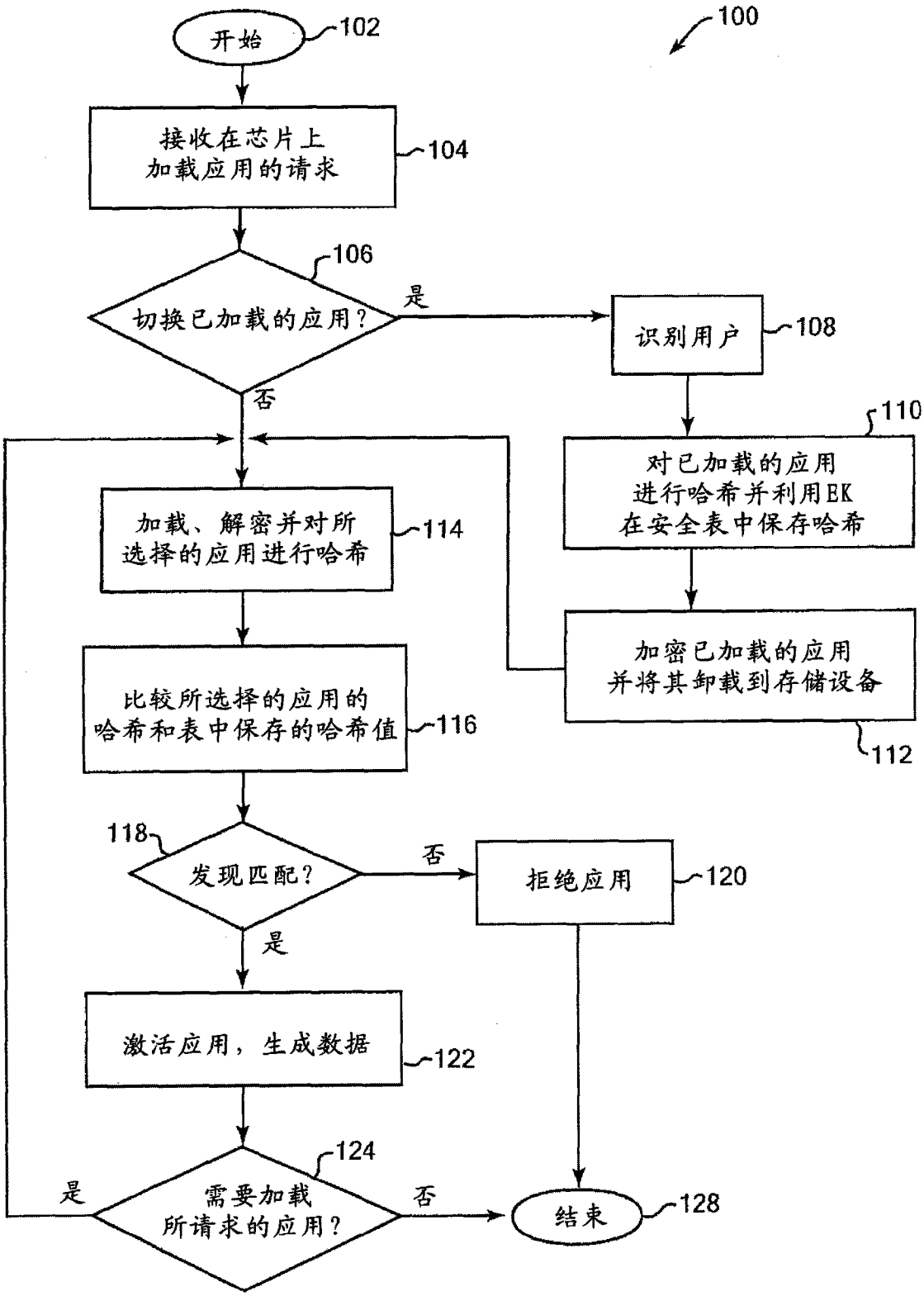

100
开始
102
接收在芯片上
加载应用的请求
104
106
切换已加载的应用？
是
否
识别用户
108
110
对已加载的应用
进行哈希并利用EK
在安全表中保存哈希
加密已加载的应用
并将其卸载到存储设备
112
加载、解密并对所
选择的应用进行哈希
114
比较所选择的应用的
哈希和表中保存的哈希值
116
118
发现匹配？
否
拒绝应用
120
是
激活应用，生成数据
122
124
需要加载
所请求的应用？
是
否
结束
128

图 4

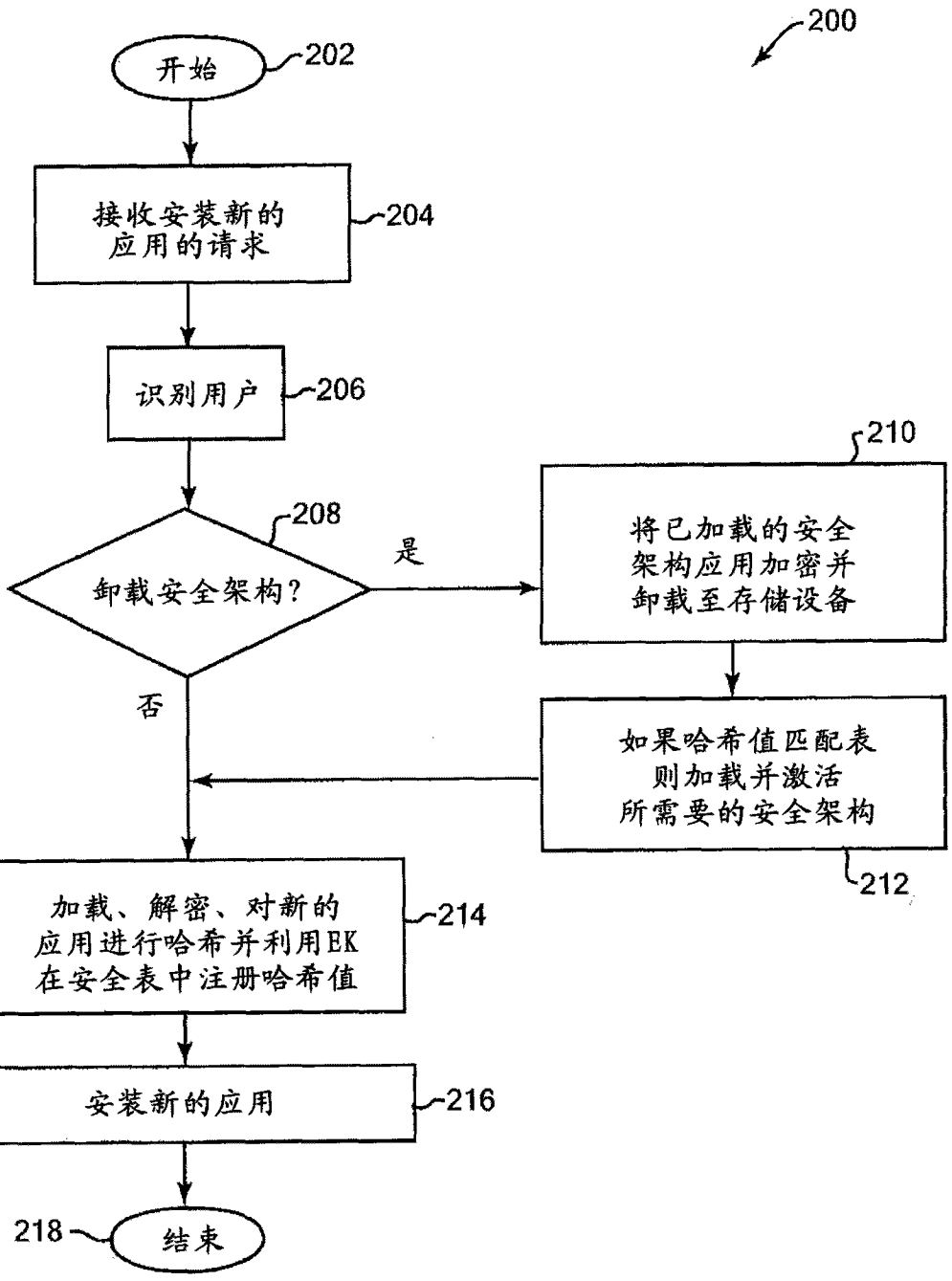

200
开始
202
接收安装新的
应用的请求
204
识别用户
206
208
卸载安全架构?
是
否
210
将已加载的安全
架构应用加密并
卸载至存储设备
如果哈希值匹配表
则加载并激活
所需要的安全架构
212
加载、解密、对新的
应用进行哈希并利用EK
在安全表中注册哈希值
214
安装新的应用
216
218
结束

图 5