

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 9/445 (2006.01)

G06F 1/00 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200510128890.5

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1801091A

[22] 申请日 2005.12.7

[74] 专利代理机构 上海专利商标事务所有限公司

[21] 申请号 200510128890.5

代理人 李 玲

[30] 优先权

[32] 2005.1.7 [33] US [31] 11/031,161

[71] 申请人 微软公司

地址 美国华盛顿州

[72] 发明人 小 J · A · 舒瓦茨 J · 亨特
J · D · 舒瓦茨 K · D · 雷
P · 英格兰德 R · 汉弗莱斯
S · 汤姆

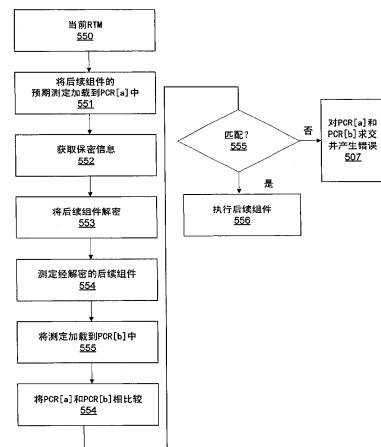
权利要求书 3 页 说明书 23 页 附图 9 页

[54] 发明名称

用可信处理模块安全地引导计算机的系统和方法

[57] 摘要

在具有可信平台模块(TPM)的计算机中，引导组件的期望散列值可被放在平台配置寄存器(PCR)中，该 PCR 允许 TPM 拆封保密信息。该保密信息随即被用来将引导组件解密。然后可计算经解密的引导组件的散列，并将结果放到一 PCR 中。然后可比较这两个 PCR 。如果它们不匹配，则可撤消对系统操作的重要保密信息的访问。同样，一第一保密信息仅在第一个 PCR 值现存时可被访问，而一第二保密信息仅在第一个 PCR 值中的一个或多个已被新值所替换以后才可被访问，从而为准许对第二保密信息的访问必然撤消了对第一保密信息的进一步访问。



1. 一种承载了具有硬件安全模块（HSM）的计算机上的安全引导过程所用的指令的计算机可读介质，所述 HSM 包含记录下来的值、将所提交的值与所记录的
5 值进行比较、并且在所提交的值正确的情况下发放保密信息，所述计算机可读介质包括：

用于向所述 HSM 提交至少一个值的指令，其中，如果所述值是正确的，则所述 HSM 可发放保密信息；

用于检索所述保密信息的指令；

10 用于使用由于检索所述保密信息而可被访问的信息来对数据解密的指令，其中，所述用于解密的指令的执行产生经解密的数据；

用于计算机引导过程的至少一部分的指令，其中，所述计算机引导过程在没有所述经解密的数据的情况下不能完成正常引导。

2. 如权利要求 1 所述的计算机可读介质，其特征在于，所述 HSM 是一可信
15 平台模块（TPM），且所述至少一个值被放在至少一个平台配置寄存器（PCR）中。

3. 如权利要求 1 所述的计算机可读介质，其特征在于，所述经解密的数据包括所述计算机引导过程中所使用的软件组件。

4. 如权利要求 1 所述的计算机可读介质，其特征在于，所述经解密的数据包括所述计算机引导过程中所使用的软件组件继续所述计算机过程所需的信息。

20 5. 如权利要求 1 所述的计算机可读介质，其特征在于，所述经解密的数据包括访问存储在计算机可读介质上的数据所需的信息。

6. 如权利要求 1 所述的计算机可读介质，其特征在于，还包括用于从存储器中移除所述保密信息的指令。

7. 一种包括硬件安全模块（HSM）的计算机，所述 HSM 包含记录下来的值、
25 将所提交的值与所记录的值进行比较、并且在所提交的值正确的情况下发放保密信息，所述计算机还包括：

用于向所述 HSM 提交至少一个值的装置，其中，如果所述值是正确的，则所述 HSM 可发放保密信息；

用于检索所述保密信息的装置；

30 用于使用由于检索所述保密信息而可被访问的信息来对数据解密的装置，其

中，所述用于解密的装置的操作产生经解密的数据；

包括计算机引导过程的至少一部分的装置，其中，所述计算机引导过程在没有所述经解密的数据的情况下不能完成正常的引导。

8. 如权利要求 7 所述的计算机，其特征在于，所述 HSM 是可信平台模块
5 (TPM)，且所述至少一个值被放在平台配置寄存器 (PCR) 中。

9. 如权利要求 7 所述的计算机，其特征在于，所述经解密的数据包括所述计
算机引导过程中所使用的软件组件。

10. 如权利要求 7 所述的计算机，其特征在于，所述经解密的数据包括所述计
算机引导过程中所使用的软件组件继续所述计算机过程所需的信息。

10 11. 如权利要求 7 所述的计算机，其特征在于，所述经解密的数据包括访问
存储在计算机可读介质上的数据所需的信息。

12. 如权利要求 7 所述的计算机，其特征在于，还包括用于从存储器中移除
所述保密信息的装置。

13. 一种承载了具有多个分区和硬件安全模块 (HSM) 的计算机上的安全引
15 导过程所用的指令的计算机可读介质，所述 HSM 包含记录下来的值、将所提交的
值与所记录的值进行比较、并且在所提交的值正确的情况下发放保密信息，所述计
算机可读介质包括：

用于向所述 HSM 提交至少一个值的指令，其中，如果所述值是正确的，则所
述 HSM 可发放保密信息；

20 用于检索第一保密信息的指令；

用于从存储器位置移除所述第一保密信息的指令；

用于向所述 HSM 提交至少一个第二值的指令，其中，如果所述第二值是正
确的，则所述 HSM 可发放第二保密信息而不发放所述第一保密信息。

14. 如权利要求 13 所述的计算机可读介质，其特征在于，所述 HSM 是可信
25 平台模块 (TPM)，且所述至少一个值和所述至少一个第二值被放在平台配置寄
存器 (PCR) 中。

15. 如权利要求 13 所述的计算机可读介质，其特征在于，还包括计算机引导
过程的至少一部分所用的指令，其中，所述计算机引导过程在没有所述第一保密信
息的情况下不能完成正常引导。

30 16. 如权利要求 13 所述的计算机可读介质，其特征在于，所述第二保密信息
是访问存储在计算机可读介质的至少一个分区上的实际所有数据所需的。

17. 如权利要求 13 所述的计算机可读介质，其特征在于，所述第一值包括计算机引导过程中所使用的软件组件的散列。

18. 如权利要求 13 所述的计算机可读介质，其特征在于，所述第二值包括解密密钥的散列。

5 19. 如权利要求 13 所述的计算机可读介质，其特征在于，所述第一保密信息和所述第二保密信息中的至少一个是二进制大对象（BLOB）。

20. 如权利要求 13 所述的计算机可读介质，其特征在于，所述第一保密信息和所述第二保密信息中的至少一个是解密密钥。

用可信处理模块安全地引导计算机的系统和方法

5 技术领域

本发明一般涉及计算领域。更特别地，本发明提供通过预防对引导期间所使用的数据未经授权的修改、以及通过预防对只在引导期间所需资源的引导后访问来增强计算机安全的系统和方法。

10 背景技术

安全已成为计算机用户普遍关注的问题。病毒、蠕虫、特洛伊木马、身份窃取、软件和媒体内容盗版、以及使用数据破坏恐吓的敲诈十分猖獗。操作系统可提供许多安全特征来防止此类攻击。但是，如果操作系统的安全特征被禁用，则它们将无效。如果试图禁用此类安全特征，很可能是在操作系统的引导期间进行尝试。
15 在引导以后，操作系统可能使许多特征就位以保护其自身及其所管理的数据和进程。但是，在引导期间，那些特征可能尚未被初始化，并且容易被旁路和/或篡改。

操作系统当前所使用的示例性安全特征有加密文件系统（EFS）、以及可信平台模块（TPM）。EFS 特征将所选择的敏感数据加密。在用户登录以前，操作系统无需访问 EFS 数据。在操作系统引导以后，用户可向登录进程提供密码。由密码
20 授予对能够将 EFS 数据解密的解密密钥的访问。作为示例，微软 WINDOWS® 操作系统使用系统密钥，或称“SYSKEY”，使用该系统密钥，通过令各个进程的正确执行依赖于 SYSKEY 的可用性来保护那些进程。例如，可从 SYSKEY 导出将由操作系统以加密的形式存储的 EFS 数据解密所需的密钥。

因此，执行受限操作所需的密钥受登录过程保护。通常，用户在开始使用系
25 统以前必须正确地验证自己。仅当用户正确地验证时才允许使用密钥。但是，使用登录过程来保护对密钥的访问是假定了操作系统已加载了正确的登录程序，且并非由可能运行的欺诈代码允许密钥的使用。如果在引导期间使用了欺诈操作系统加载器而不是正确的操作系统加载器，则欺诈加载器可能令欺诈登录程序随操作系统被加载。欺诈登录程序可能进而允许无须输入正确密码即可使用 EFS 密钥。因为操
30 作系统的加载提供了破坏安全的机会，在此类情况中密钥的保护要求操作系统的加

载在可证明其会正确发生的情况下发生。

因为 EFS 是被引导的操作系统所支持的特征，所以它在保护引导过程期间所泄露的某些数据方面是无效的。EFS 不能保护用户登录以前所需的用户数据，诸如某些系统服务所需的保密信息；网络服务（例如，个人或公共 web 服务器）所使用的数据库；以及用于连接到公司域的 RAS 凭证。

可信处理模块（TPM）确保计算机上所运行的软件的可信赖性。一般而言，这是通过向 TPM 提交可信数据度量，并依靠 TPM 来确定该度量是否符合来实现的。计算机安全常常依赖于能够预测软件组件的行为。一般而言，系统的安全来自从已知的好状态而来的、行为被理解的已知程序将以可预测的方式行动这一前提。

反过来，阻碍安全——这可能涉及令计算机系统以超出其设计者构想范围的方式运作——一般可通过替换或改变已知程序、或在其行为不被理解的状态下运行已知程序来实现。由此，为计算环境提供安全的一个方面包括证明所使用的是已知程序，且它是从已知的好状态而来。TPM 通过验证该数据因诸如数据的散列等度量匹配先前密封在 TPM 中的值而符合来实现此方面。

和 EFS 一样，TPM 已被成功用来为被引导的计算机上所运行的应用程序的完整性提供某种程度的保证。TPM 也存在许多其它限制。例如，以标准方式使用 TPM 的机器不能在现场被重新配置（例如，在开会的同时将网卡插入到膝上型计算机中）。TPM 造成已初始化的操作系统的严重限制和复杂性。

现今的大多数 TPM 符合 TRUSTED COMPUTER GROUP® (TCG) 标准，该标准目前在<http://www.trustedcomputinggroup.org/home>可用，题为“Trusted Platform Module (TPM) Specification Version 1.2.”（可信平台模块 (TPM) 规范 1.2 版）TPM 是可以并入计算平台中来为平台所执行的代码建立信任的子系统。用于建立可信任代码的机制的标准化是有益的，因为它允许安全和加密共同体访问用于提供安全的机制，还因为它促进顾客对新的软件特征的理解和信任。它还鼓励在实现和改进标准中的革新，如 TCG® 所构想和鼓励的。如 TCG® 规范中所陈述，“[m]anufacturers will compete in the marketplace by installing subsystems with varying capabilities and cost points”（制造商将通过安装具有可变能力和成本点的子系统而在市场中竞争）。

一些用于安全引导的技术补充了操作系统所使用的上述示例性安全机制。机器密码验证可被用于使用机器全局密码来保护保密信息。但是，这需要密码在机器引导以前被输入。该密码必须由机器的多个用户共享，这是第一个安全缺陷。第二

个缺陷是引入了可使用性问题，因为不能为密码输入呈现通常的用户界面。这对平板PC而言特别不方便。机器全局密码常常可能被写在一张纸上并被留在机器边上。因此，密码是有效的，但不允许常被期望的类型的复杂的用户保护。

其次，保密信息可能被存储在可移动介质上。同样，从安全的角度出发，理论上此特征是有效的，但是实际上它常常是有问题的。此情形中的根本问题是，为确保可使用的工作系统，可移动介质将几乎总是被留在机器内。

在不能充分保证安全操作系统引导的情况下，用户保护计算机上的数据的能力受到关放这类计算机的建筑的安全限制，而不是该计算机上所运行的操作系统的安全功能的限制。随着膝上型计算机的流行，以及计算机盗窃、特别是膝上型计算机盗窃上升趋势的增长，需要一种在计算机进入窃贼手中时允许操作系统的安全不受危及的解决方案。

使用 TPM 来保护引导过程的系统和方法还远未被探索完全。除了在引导过程中使用 TPM 以外，用于执行引导过程的维护以及用于控制对此类计算机上的数据的访问的系统和方法可能会证明是有用的。对这些系统和方法的描述可在于 _____
15 提交的、题为 “Systems and Methods for Boot Recovery in a Secure Boot Process on a Computer with a Hardware Security Module”（带有硬件安全模块的计算机上的安全引导过程中引导恢复的系统和方法）、代理卷号为 MSFT 4634/311226.01 的美国专利申请第 _____ 号，于 _____ 提交的、题为 “Systems and Methods for Updating a Secure Boot Process on a Computer with a Hardware Security Module”（更新带有硬件安全模块的计算机上的安全引导过程的系统和方法）、代理卷号为 MSFT
20 4784/312086.01 的美国专利申请第 _____ 号，以及于 _____ 提交的、题为 “Systems and Methods for Controlling Access to Data on a Computer with a Security Boot Process”（控制对带有安全引导过程的计算机上的数据的访问的系统和方法）、代理卷号为 MSFT 4635/311227.01 的美国专利申请第 _____ 号中找到。于 2004 年
25 6 月 30 日提交的、题为 “System and method for protected operating system boot using state validation”（使用状态验证的受保护的操作系统引导的系统和方法）的美国专利申请第 10/882,134 号也一般涉及本发明。

发明内容

30 考虑到以上背景，本发明提供以用于验证软件组件的完整性度量的可信平台模块（TPM）安全地引导计算机的系统和方法。配合本发明使用的 TPM 可将保密

信息密封到多个平台配置寄存器 (PCR) 值中。PCR 值可通过测定引导组件来获得。如果引导组件从保密信息被密封的时间起未被修改，则可为适当的系统引导获得保密信息。可将引导组件预期的散列值放到 PCR 中，如果预期值是正确的，则将保密信息拆封。该保密信息随即可能被用来将实际的引导组件从其在磁盘上的位置解密。然后可计算经解密的引导组件的散列，并将结果与预期值相比较。另一个示例需要使用被密封到可在引导过程中的不同点获得的 PCR 值的两个保密信息。第一个保密信息仅在第一多个 PCR 值被加载时可被访问，而第二个保密信息仅在第一多个值中的一个或多个已被新的值所替换以后可被访问，从而为准许对第二保密信息的访问必然撤消了对第一保密信息的进一步访问。本发明的其它优点和特征在以下描述。

附图说明

参考附图进一步描述根据本发明安全引导计算机的系统和方法，其中：

图 1 阐述适于实现与本发明相关联的软件和/或硬件技术的计算环境。

图 2 提供对来自图 1 的基本计算环境的扩展，以着重强调可在多个联网的设备上执行现代计算技术。

图 3 示出利用可信平台模块 (TPM) 的计算平台。

图 4 示出一种示例性引导过程，其中在过渡到后续过程之前多个软件组件测定该后续过程。

图 5 示出使用诸如 TPM 等硬件安全模块 (HSM)，在允许后续组件执行以前确保该后续软件组件或过程的完整性的一般技术。

图 5a 示出用于确保在只有在 TPM 验证了引导过程中所使用的数据的情况下引导过程才能继续进行的系统和方法。

图 6 演示图 5a 中所示的系统和方法的一个示例，其中计算机的成功引导依赖于示例性组件——引导管理器的成功解密和测定。

图 7 图解一种用于提供对资源仅可进行有限持续期的访问的引导组件、然后在运行操作系统以前撤消对这些资源的访问的体系结构的操作。

图 8 提供在诸如图 7 等体系结构中要执行的示例性步骤的流程图。

30 具体实施方式

在以下描述和附图中阐述某些特定细节，以提供对本发明的各个实施例的详

尽理解。但是，在以下揭示中不对常常与计算和软件技术相关联的某些公知细节进行阐述，以避免不必要的混淆本发明的各个实施例。此外，相关领域普通技术人员将会理解，他们无需以下所描述的一个或多个细节就能够实践本发明的其它实施例。最后，尽管参考以下揭示中的步骤和顺序来描述各种方法，但是如下描述是为 5 提供本发明的实施例的清楚的实现，且不应将各步骤及其顺序视为实践本发明所必须。

以下详细描述大体上将贯彻上述发明内容，并在必要时进一步解释和扩展本发明的各个方面和实施例的定义。为此目的，此具体实施方式首先阐述图 1 中的计算环境，它适于实现与本发明相关联的软件和/或硬件技术。在图 2 中示出一种联网的计算环境作为基本计算环境的扩展，以着重强调可在多个离散设备上执行现代 10 计算技术。

接下来，结合图 3 提供利用硬件安全模块（HSM）的计算平台的概述，以解释如何将测定提交给 HSM，且 HSM 可被配置成在那些测定正确的情况下向系统资源返回密钥。注意，图 3 中所示的 HSM 是 TPM，它是本领域技术人员已知的一种 15 HSM。同样，可令引导中或其后所涉及的软件组件的进一步处理随附于拆封受 TPM 保护的保密信息。然后在图 4 中示出在引导过程中软件组件对 TPM 的使用。图 5 示出诸如图 4 中等软件组件使用 TPM 的一个一般模式，其中下一个软件组件的加载和执行随附于对下一个组件的可执行代码的散列的证明。

在图 5a、6、7 和 8 中，更加详细地解释了在引导过程中被称为平台配置寄存器（PCR）的 TPM 寄存器的使用的各个方面。图 5a 示出用于确保只有在特定的引导组件集合就位的情况下引导过程才能继续进行的系统和方法。图 6 演示图 5a 中所示的系统和方法的一个示例，其中计算机的成功引导依赖于示例性组件——引导管理器的成功解密和测定。图 7 和 8 示出一种用于在引导过程成功运行操作系统且不再需要引导所需的系统资源（通常驻留在一个或多个磁盘分区上）以后防止对那些 25 资源进行访问的机制。

示例性计算和联网环境

图 1 中的计算系统环境 100 只是适用的计算环境的一个示例，并不试图对本发明的使用范围或功能提出任何限制。也不应将计算环境 100 解释为具有涉及示例性操作环境 100 中所示出的任一组件或其组合的任何依赖性或要求。

30 本发明可配合许多其它通用或专用计算系统环境或配置操作。适用于本发明的公知计算系统、环境、和/或配置的示例包括，但不限于，个人计算机、服务器

计算机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境、等等。

本发明可在计算机所执行的诸如程序模块等计算机可执行指令的通用上下文中实施。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构、等等。本发明还可在分布式计算环境中实践，其中任务是由通过通信网络连接的远程处理设备执行。在分布式计算环境中，程序模块可位于包括记忆存储设备在内的本地和远程计算机存储介质中。

参考图 1 用于实现本发明的示例性系统包括计算机 121 形式的通用计算设备。计算机 121 的组件可包括，但不限于，处理单元 101、系统存储器 103、以及将包括系统存储器在内的各个系统组件耦合到处理单元 101 的系统总线 102。系统总线 102 可以是若干种类型的总线结构中的任何一种，包括存储器总线或存储器控制器、外围总线、以及使用各种总线体系结构中的任何一种的局部总线。作为示例，而非限制，此类体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强型 ISA (EISA) 总线、视频电子标准协会 (VESA) 局部总线、以及也称为 Mezzanine 总线的外围组件互连 (PCI) 总线。

图 1 中未示出 HSM，但这类设备可以是实现本发明的计算机的一部分。图 3 示出与计算机的组件集成的 HSM (图 3 的实施例中的 TPM)，如以下参考图 3 所讨论。在经典实施例中，HSM 可以是为提供一定范围的安全功能的目的而被焊接到母板、或者集成到诸如图 1 等计算机的芯片组或其它硬件组件中的硬件芯片。但是，为此说明书目的，应当理解 HSM 可在硬件或软件中实现，并被宽泛地定义为可提供本发明的操作所需的那些可信功能 (即，对向其提交的测定的比较和证明，以及用于访问经加密的存储器资源的密钥的发放) 的功能单元。TPM 还可提供一定范围的其它功能，如工业标准 TPM 的 TCG® 规范中所描述。

计算机 121 通常包括各种计算机可读介质。计算机可读介质可以是可由计算机 121 访问的任何可用介质，并包括易失性和非易失性、可移动和不可移动介质。作为示例，而非限制，计算机可读介质可包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括，但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术，CD-ROM、数字多功能盘 (DVD) 或其它光盘存储器，磁带盒、磁带、磁盘存储

器或其它磁存储设备，或可用于存储所需信息并可由计算机 121 访问的任何其它介质。通信介质通常具体化为诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据。术语“已调制数据信号”是指以在信号中将信息编码的这样一种方式设置或改变其一个或多个特征的信号。作为示例，
5 而非限制，通信介质包括诸如线网络或直接连线连接等有线介质，以及诸如声学、RF、红外线及其它无线介质等无线介质。以上任何组合也应被包括在计算机可读介质的范围之内。

系统存储器 103 包括诸如只读存储器 (ROM) 104 和随机存取存储器 (RAM)
106 等易失性和/或非易失性存储器形式的计算机存储介质。包含诸如在启动期间帮助
10 在计算机 121 内部各元件之间传递信息的基本例程的基本输入/输出系统 105
(BIOS) 通常存储在 ROM 104 中。RAM 106 通常包含可由处理单元 101 即时访问和/或正由其操作的数据和/或程序模块。作为示例，而非限制，图 1 示出操作系统
107、应用程序 108、其它程序模块 109、以及程序数据 110。

计算机 121 还可包括其它可移动/不可移动、易失性/非易失性计算机存储介质。
15 仅作为示例，图 1 示出读或写不可移动、非易失性磁介质的硬盘驱动器 112，读或
写可移动、非易失性磁盘 119 的磁盘驱动器 118，以及读或写诸如 CD ROM 或其它光
介质等可移动、非易失性光盘 253 的光盘驱动器 120。示例性操作环境中可使用的其它可
20 移动/不可移动、易失性/非易失性计算机存储介质包括，但不限于，磁带盒、闪存卡、数字多功
能盘、数码录像带、固态 RAM、固态 ROM、等等。硬盘驱动器 112 通常通过诸如接口 111 等不可
移动存储器接口连接到系统总线 102，而磁盘驱动器 118 和光盘驱动器 120 通常由诸如接口 117 等可
移动存储器接口连接到系统总线 102。

以上所讨论并在图 1 中示出的各设备及其相关联的计算机存储介质为计算机
121 提供计算机可读指令、数据结构、程序模块和其它数据的存储。例如，在图 1
25 中，示出硬盘驱动器 112 存储了操作系统 113、应用程序 114、其它程序模块 115、
以及程序数据 116。注意，这些组件可以和操作系统 107、应用程序 108、其它程
序模块 109 以及程序数据 110 相同或不同。此处赋予操作系统 113、应用程序 114、
其它程序模块 115、以及程序数据 116 不同标号以说明至少它们是不同的副本。用
户可通过诸如键盘 128 和定位设备 127（通常指鼠标、轨迹球或触摸垫）等输入设
备将命令和信息输入到计算机 121 中。其它输入设备（未示出）可包括话筒、操纵
杆、游戏垫、圆盘式卫星天线、扫描仪、等等。这些及其它输入设备常常通过耦合

到系统总线的用户输入接口 126 连接到处理单元 101，但也可由诸如并行端口、游戏端口或通用串行总线（USB）等其它接口和总线结构连接。监视器 139 或其它类型的显示设备也经由诸如视频接口 232 等接口连接到系统总线 102。除了监视器以外，计算机还可包括诸如扬声器 138 和打印机 137 等其它外围输出设备，它们可通过输出外围接口 123 连接。

计算机 121 可使用到诸如远程计算机 131 等一台或多台远程计算机的逻辑连接在联网环境中操作。远程计算机 131 可以是个人计算机、服务器、路由器、网络 PC、对等设备、或其它普通网络节点，并通常包括以上相对于计算机 121 所描述的许多或所有元件，尽管图 1 中仅示出了记忆存储设备 132。图 1 中所示的逻辑连接包括局域网（LAN）135 和广域网（WAN）130，但也可包括其它网络。这些网络环境常见于办公室、企业范围的计算机网络、内联网、以及因特网。

当在 LAN 网络环境中使用时，计算机 121 通过网络接口或适配器 134 连接到 LAN 135。当在 WAN 130 网络环境中使用时，计算机 121 通常包括调制解调器 129 或用于通过 WAN（诸如因特网）建立通信的其它装置。可以是内置或外置的调制解调器 129 可经由用户输入接口 126 或其它适当机制连接到系统总线 102。在联网环境中，相对于计算机 121 所描述的程序模块或其部分可存储在远程记忆存储设备中。作为示例，而非限制，图 1 示出远程应用程序 133 驻留在存储设备 132 上。可以认识到，所示网络连接是示例性的，并且可以使用在计算机之间建立通信链路的其它装置。

应当理解，本文中所描述的各种技术可结合硬件、软件、或在适当情况下结合这两者的组合来实现。因此，本发明的方法和装置，或其部分的某些方面可表现为具体化为诸如软盘、CD-ROM、硬盘驱动器、或任何其它机器可读的存储介质等可触知介质中的程序代码（即，指令）的形式，其中当程序代码被加载到诸如计算机等机器中并由其执行时，该机器即变为用于实践本发明的装置。在程序代码在可编程计算机上的执行的情形中，计算设备一般包括处理器、该处理器可读的存储介质（包括易失性和非易失性存储器和/或存储元件）、至少一个输入设备、以及至少一个输出设备。可实现或利用结合本发明所描述的过程的一个或多个程序，例如，通过使用 API、可重复使用的控件、等等。较佳的是，用高层过程或面向对象编程语言实现这些程序来与计算机系统通信。但是，如果需要的话，可用汇编或机器语言实现这（些）程序。在任何情况下，语言都可以是已编译或已解释的语言，并可与硬件实现相结合。

尽管示例性实施例涉及在一个或多个独立计算机系统的上下文中使用本发明，但是本发明不受此限制，而是可结合诸如网络或分布式计算环境等任何计算环境来实现。此外，本发明可在多个处理芯片或设备中或之上实现，而存储也可类似地在多个设备上实现。这些设备可包括个人计算机、网络服务器、手持式设备、超 5 型计算机、或集成到诸如汽车或飞机等其它系统中的计算机。

图 2 中提供一种示例性联网计算环境。本领域普通技术人员可以认识到，网络可连接任何计算机或其它客户机或服务器设备，或者是在分布式计算环境中。就此而言，具有任何数量的处理、记忆或存储单元，以及任何数量的同时发生的应用程序和进程的任何计算机系统或环境被认为适合结合所提供的系统和方法使用。

10 分布式计算通过计算设备和系统之间的交换来提供计算机资源和服务的共享。这些资源和服务包括信息的交换、文件的高速缓存和磁盘存储。分布式计算利用网络连接性，从而允许客户机调节它们集体的力量以益于整个企业。在这点上，各种设备可具有涉及本文中所描述的过程的应用程序、对象或资源。

15 图 2 提供示例性联网或分布式计算环境的示意图。该环境包括计算设备 271、272、276 和 277，以及对象 273、274 和 275，及数据库 278。这些实体 271、272、273、274、275、276、277 和 278 中的每一个都可包括或利用程序、方法、数据存储、可编程逻辑、等等。实体 271、272、273、274、275、276、277 和 278 可以跨 20 越诸如 PDA、音频/视频设备、MP3 播放器、个人计算机等相同或不同的设备的各个部分。每个实体 271、272、273、274、275、276、277 和 278 可通过通信网络 270 与另一实体 271、272、273、274、275、276、277 和 278 通信。就此而言，任一实体都可负责数据库 278 或其它存储元件的维护和更新。

25 此网络 270 本身可包括向图 2 的系统提供服务的其它计算实体，且本身可表示多个互连的网络。根据本发明的一个方面，每个实体 271、272、273、274、275、276、277 和 278 可包含离散的功能程序模块，它们可利用 API 或其它对象、软件、固件和/或硬件，来请求其它实体 271、272、273、274、275、276、277 和 278 中 30 的一个或多个的服务。

还可认识到，诸如 275 等对象可主宿在另一计算设备 276 上。因此，尽管所示的物理环境可能将所连接的设备示为计算机，但是此类图示仅仅是示例性的，且该物理环境可被替换地图示或描述为包括诸如 PDA、电视机、MP3 播放器等各种数码设备、诸如接口、COM 对象等软件对象、等等。

有各种支持分布式计算环境的系统、组件和网络配置。例如，计算系统可由

有线或无线系统、由局域网或广域网连接到一起。目前，许多网络被耦合到因特网，它为广泛分布的计算提供基础结构，并且包括许多不同的网络。任何此类基础结构，无论其是否被耦合到因特网，都可结合所提供的系统和方法来使用。

5 网络基础结构可允许诸如客户/服务器、点对点、或混合体系结构等许多网络拓扑结构。“客户”是一个类或组群的成员，它使用其不相关的另一个类或组群的服务。在计算中，客户是请求另一程序所提供的服务的进程，即，大致上是指令或任务的集合。客户进程无须“知道”关于另一程序或服务本身的工作细节即可使用所请求的服务。在客户/服务器体系结构中，特别是在联网系统中，客户通常是访问另一台计算机（例如，服务器）所提供的共享的网络资源的计算机。在图 2
10 的示例中，取决于情况，任何实体 271、272、273、274、275、276、277 和 278 都可被视为客户机、服务器、或这两者。

尽管不是必须，但服务器通常是，通过诸如因特网等远程或本地网络可访问的远程计算机系统。客户进程可能在第一计算机系统上活动，而服务器进程可在第二计算机系统上活动，它们通过通信介质相互通信，从而提供分布式功能，并允许
15 多个客户利用该服务器的信息收集能力。任何软件对象都可以分布在多个计算设备或对象上。

客户机和服务器使用协议层所提供的功能相互通信。例如，超文本传输协议（HTTP）是结合万维网（WWW，或称“Web”）使用的公共协议。通常，可使用诸如因特网协议（IP）地址等计算机网络地址或诸如统一资源定位器（URL）等
20 其它引用来向服务器或客户计算机标识彼此。网络地址可被称为 URL 地址。可在通信介质上提供通信，例如，客户机和服务器可经由 TCP/IP 连接相互耦合以进行高容量的通信。

按照可根据图 1 的一般框架来构建的多种不同的计算环境，以及在诸如图 2 等网络环境里的计算中可能发生的其它多样性，本文中所提供的系统和方法在任何
25 情况下都不能被解释为被限制于特定的计算体系结构。本发明不应被限制于任何单个实施例，相反是应根据所附权利要求书的广度和范围来解释。

示例性 TPM 保护的引导序列

本发明的实施例在安全引导过程中使用 TPM。在图 3 中的计算机体系结构的
30 上下文中示出 TPM。尽管构想在本发明的实施例中使用的 TPM 可以是遵守 TCG®1.2 的，但可使用用于验证诸如被放在 PCR 中的测定等测定、并在这些测定

是正确的情况下拆封保密信息的任何 HSM。

就此而言，图 3 给出诸如图 1 等计算机的高度一般化的视图中可访问存储器 305 的 CPU 300。CPU 300 可依靠 TPM 301 提供某些安全功能。一般而言，CPU 300 可首先执行引导过程中所涉及的数据的测定，而那些测定可被安全地存储在 TPM 5 301 中，如密封的 PCR 值 304 所示。注意，在各个实施例中，本文附图中所示的各 PCR 值 304 和 303 实际上可被存储在由代数方程扩展的一个或多个单个存储位置中，如 TCG®1.2 规范所定义。

10 保密信息 302 可被密封到 TPM 301 中的特定 PCR 值 304。为从 TPM 301 检索保密信息 302，正确的 PCR 值必须被输入到 PCR 303 中。这些正确的值可通过测定与获得密封在 TPM 301 中的 PCR 值 304 所测定的数据相同的数据来获得。多个保密信息 302 可被密封到各个 PCR 304。例如，为检索第一保密信息 A，可能要求正确的值被存储在 PCR[1]、PCR[2]和 PCR[3]中。为获得第二保密信息 B，PCR[4] 中可能要求第四正确值。

15 如果被放到 PCR 303 中的测定不匹配密封在 TPM 301 中的那项测定的值，则当请求 TPM 301 拆封保密信息 302 时，拆封将失败。如果正确的测定被放到 PCR 303 中，则当请求 TPM 301 拆封保密信息 302 时，TPM 301 可信以执行此操作。因此，为此应用程序目的，“正确的”测定，或正确的值是保密信息 302 被密封到的测定，由此允许由 TPM 301 拆封保密信息 302。注意，在一些实施例中，正确的测定可能是恶意代码的测定。例如，当密封在 TPM 301 中的初始测定 304 被破坏时，便出现这种情况。

20 密封到特定测定的保密信息可以是任何数据。通常，保密信息 302 会表现为解密密钥和/或二进制大对象（BLOB）的形式。一般而言，密钥提供可用来将数据解密的信息。密封的 BLOB 可包含密钥以及可能有用的其它数据。就此而言，可通过用密钥来替换 BLOB 来构造本文中所讨论的各种技术的等效方案，反之亦然，如本领域技术人员将会认识到。因此，如果 CPU 300 向 303 中的 PCR 提交正确的测定，则当请求诸如密钥等对应的保密信息 302 时，TPM 301 可拆封该保密信息 302。来自 302 的密钥随即可能被用来将计算机 300 可访问的存储器 305 的部分解密。在本发明的实施例中，TPM 301 可被配置成授予对三个保密信息 A、B 和 C 的访问，如图 3 中所示。保密信息 302 可被密封到各个被请求的 PCR 值，因此仅在执行了某些测定以后才可被访问。这三个密钥，或三个保密信息，在本文中将被称为，第一个，只供引导访问保密信息，第二个，卷绑定保密信息，以及第三个，密码保

密信息。

TPM 相关活动可被存储在日志 307 中。在一些实施例中，日志 307 可由计算机的 BIOS 维护。任何其它进程也可负责维护日志 307。因此，如果诸如软件组件 308 或其它数据 309 等数据被测定到 PCR 303 中，则被测定的数据可在日志 307 中加以标识。如果作出保密信息拆封的请求，则该请求事件可在日志 307 中被标识。这些只是将 TPM 有关的活动存储到日志 307 中的两个示例，日志中可包含广大范围的其它事件和活动的记录。

通常，TPM 301 与信任测定的静态根（SRTM）协同操作，以执行可信测定并将它们提交给 TPM 301。但是，有诸如通过使用 DRTM 关系等进行安全测定的其它过程可用。本发明的实施例能以此方式使用诸如 SRTM 等可信测定过程，并且就此而言，SRTM 可以是本文中所讨论的各种软件组件用以测定初始的基于盘的引导代码的 BIOS 标准 SRTM（也称为过程和 RTM）。该系统还可扩展 SRTM 以测定引导操作程序的早期阶段中所涉及的其它代码和关键性数据，以使操作系统引导的任何早期阶段可被测定。注意，PCR 303 可包含从任何地方获得的值。这些值可以是诸如软件组件 308 或其它数据 309 等数据的测定。本发明不局限于被放在 PCR 303 中的数据测定或其它值的任何排它性组合。

在 TPM 保护的引导过程中，图 3 中所显示的安排可被用来测定图 4 中所示的示例性软件组件，并将这些测定存储在 PCR 303 中。已知图 4 中所示的、被选择由本发明的实施例测定的引导组件，特别是基于盘的代码组件是很少改变且易受攻击的。因此，强加这些特定引导组件仍然保持不变，除非通过本文中所描述的合格的维护和更新过程，使显著增强数据安全所要付出的代价相对很小。

参考图 4，示出一系列软件组件 400 – 407 以提供计算机的示例性引导过程。本发明不局限于所示的特定组件，也不局限于各组件的顺序。所示组件可被顺序加载，以测定的信任内核根（CRTM）400 开始，并以本文中被一般化为单个软件组件 407 的操作系统（OS）407 的组件结束。加载组件使得给予组件对诸如存储器和 CPU 等计算机资源的访问、以使该组件的指令可由 CPU 执行成为必须。如果图 4 中的组件是恶意的或被破坏的，则一旦它被加载即会被用来规避安全测定。因此，一种根据本发明引导计算机的过程包括在允许一个或多个组件执行以前，将它（们）测定到一个或多个 PCR 303 中。可令成功的引导随附于被密封到测定 304 的可信集合的保密信息 302，而测定 304 的可信集合被密封到 TPM 中。但是注意，本发明也可能将恶意代码的测定密封到 TPM 中。如果恶意代码在密封的时候运行，则

引导可能需要那些测定。理想的是，保密信息被密封到可信代码的测定 304 中。如果被放到 PCR 303 中的测定是正确的，则来自 302 的保密信息可被拆封，以允许机器继续进行安全引导。图 5 中示出拆封保密信息 302 的过程。

- 在某些使用情形中，机器的所有者可能确定他们想要“锁定”机器的配置，
5 以确保除先前被验证的代码以外绝没有其它基于 ROM 的代码被执行。在此情形中，
机器的所有者可通过选择其它要使用的 PCR 302 来将更多软件组件配置成涉及验
证过程（BIOS、选项 ROM）。所有者还可确定他们还想要使用经 TPM 301 验证
的机器密码。这允许在本发明的标准实施例中通常提供的安全之上进行安全扩展，
并允许用户在机器安全和使用方便之间进行权衡。
10 图 5 示出一种在加载后续组件以前使用 TPM 来确保该后续软件组件的完整性
的技术。可通过将适当的指令放到诸如图 4 的组件等一系列组件中来执行图 5 的步
骤。就此而言，图 5 的过程可以 CRTM 组件 508 的执行开始。诸如 CRTM 及图 4
的部分或所有其它组件等组件可承载用于测定另一个组件并将诸如来自图 3 中的
303 的结果放到 PCR 中的指令。承载此类指令的组件有时被称为测定的信任根
15 （RTM），并可包含利用如上文所提及的 SRTM 的指令。因此，如果引导块测定
引导管理器，则引导块起到引导管理器的 RTM 的作用。

RTM 可将后续组件加载到存储器 500 中，然后对后续组件 501 执行测定，并
将测定添加到 PCR 502 中。如果 RTM 需要诸如来自 TPM 503 的密钥或 BLOB 等
保密信息，则它可请求此类保密信息，且仅当为访问该保密信息所需的所有 PCR
20 都加载了正确的 PCR 值时，TPM 才会发放被请求的保密信息。因此，可能基于从
TPM 504 检索到的信息，试图拆封保密信息。如果在步骤 505 中拆封成功，则可
能采取额外步骤，可包括加载后续组件，以及以下所描述的其它动作。如果拆封不
成功，则 PCR 中的值很可能是不正确的，因此执行代码可能是被破坏了的。可在
步骤 507 产生一个错误，并采取适当测定来确保不会对存储在计算机上的敏感信息
25 提供任何访问，例如通过使用计算机盘上数据的加密，以及避免公开解密密钥。或者，
可实现例如通过将系统恢复到会产生正确 PCR 值的状态，或通过认证用户以
在图 3 的值 302 中授权新的密封 PCR 值来维护系统的过程。以下解释这些过程。
如果在步骤 503 不需要任何保密信息，则无需要求任何保密信息即可加载后续组
件，如图所示。

30 可共同参考图 4 和图 5 来示出根据本发明的系统和方法的示例性引导过程。
首先 CRTM 400 可被加载，它加载并测定基本输入/输出系统（BIOS）401。例如

可通过在 BIOS 上执行散列，然后将散列测定值提交给 PCR 来进行此测定。BIOS 随即可被允许执行，并起到主引导记录（MBR）402 的 RTM 的作用。MBR 可被测定到 PCR 中，然后 MBR 402 可被允许执行。MBR 可测定引导扇区组件 403，后者随即被允许执行。可由每一个组件 404、405、406 和 407、以及必要的话由操作系统 407 中的任何组件重复此加载、测定、写到 PCR、然后过渡到后续组件的模式。本发明的其它方面包括此过程的变更，它们可能在沿此过程的任何点请求和使用保密信息，如图 5 中示出此类请求。就此而言，本发明的实施例通过可在过渡到后续组件以前执行的额外步骤来提供提高的安全。这些额外的步骤可令成功的机器引导随附于通过测定正确的 PCR 值获得的保密信息，从而确保引导中所使用的部分或全部数据在保密信息被密封时都是符合的。这些额外步骤还可用于避免对引导期间所需但其后不再需要的资源的引导后访问。

图 4 和图 5 的基本过程可通过请求组件 400 – 406 中的一部分在过渡到后续组件以前检索保密信息（可以是密钥、BLOB、或允许访问解密密钥等的其它受保护信息）来增强。因此本发明的实施例可通过操作系统在引导过程中的战略点访问一个或多个保密信息来调节有用操作的性能。如果发现经测定的代码模块 401 – 406（本文中也称为组件和/或软件过程）中的任何一个改变了，则可扣留关键性的保密信息。可被扣留的保密信息的示例有“SYSKEY”（由 LSASS 用来将诸如服务所使用的密码等本地保密信息加密）、实质上用于将存储在计算机硬盘驱动器或磁盘分区上的任何信息解密的卷加密密钥、以及诸如 EFS 等较高层系统保护所需的保密信息。较高层保护随即以比 SRTM 丰富得多的方式使用目录来进行验证。

为将机器修复到其可成功引导的状态，可实现以下所描述的系统和方法，作为对本文中所描述的安全引导过程的补充。

示例性附加引导保护技术

在诸如参考图 4 和 5 所能理解的引导序列等引导序列中（其中多个软件组件可被配置成在过渡期到下一组件以前测定下一组件），可采取一些附加的预防措施以进一步增强存储在计算机上的数据的安全。这些附加预防措施是此章节的主题。本文中所描述的任一或所有预防措施可被结合到本发明的实施例中。在一个较佳的实施例中，使用了本文中所解释的所有预防措施，如以下将会解释。但是本发明不局限于这些实现。

首先参考图 5a，通过调节这类平台完整性上的保密信息的发布，可令计算机

的引导依赖于这些先于操作系统的组件的完整性。首先提供图 5a 的概念综览，然后提供图 5a 的更详细描述。

首先，可用诸如引导管理器等软件组件的公知散列来扩展 PCR。这导致引导保密信息成为不可拆封的，如果所有在先的软件组件都是可信的，则这是令人满意的。
5 所有在先的组件都可被信任，引导保密信息可被拆封。在此交汇点，例如引导管理器等软件组件的状态是未知的。

接下来，可将引导保密信息解密，并可使用卷对称密钥将未决系统分区解密，以将引导管理器读入存储器中。

第三，预认证步骤可通过对照公知散列来证明当前正被解密并在存储器中的
10 引导管理器的散列来巩固。如果两个散列匹配，则引导可正常进行。如果散列不正确，则可使 PCR 无效。至少有以下几种检查散列是否正确的方法：

a. 对照公知散列检查引导管理器的散列。如果系统能够拆封引导保密信息，则我们知道公知散列是有效的，因此意味着如果引导管理器的散列匹配用来拆封引
导 blob 的散列，则我们知道引导管理器的散列是有效的。

15 b. 对照存储在密封保密信息中的散列检查引导管理器的散列。

c. 用引导管理器的公知散列扩展不同的 PCR，并比较这两个散列。

现在更详细地参考图 5，在步骤 550 执行当前组件，或 RTM。当前 RTM 可执行以下步骤以过渡到下一个软件组件。后续组件的预期测定可被加载到 PCR 中，
20 例如 PCR[a] 551。然后 RTM 组件可尝试检索保密信息 552。如果没有用正确的值加载 PCR[a]，则当前 RTM 可能无效，而对该保密信息的访问可能被拒绝，从而阻塞了正常的引导，如参考图 5 所解释。该保密信息可用来将后续组件 553 解密。因为后续组件已被解密，所以想要成为攻击者的人要逆向工程和将后续组件修改为以非预期方式执行是不可能的。已被解密的后续组件可被测定 554，且测定可被放到诸如 PCR[b] 555 等 PCR 中。RTM 接下来可比较 PCR[a] 和 [b] 的值。如果它们匹配，
25 则 RTM 可过渡到下一组件，它可以是后续组件 556。如果它们不匹配，则例如通过将存储器的某个预定部分测定到那些 PCR 中来将 PCR[a] 和 [b] 求交运算为终值，而正常引导可被中止 557。

参考图 6，所示流程图示出图 5a 中所介绍的系统和方法的一个实施例，实现用于在先组件的成功操作以及关键性引导组件的完整性的前提下调节对该关键
30 性引导组件的访问的系统和方法的若干步骤。图 6 中所使用的示例性引导组件是引导管理器，尽管任何组件都可以是图 6 中所演示的技术的主题。为此解释的目的，

可在图 4 的上下文中理解图 6 的步骤。可用串行方式执行多个软件组件，且其中一个或多个可在过渡到下一组件以前测定下一组件。

在此上下文中，诸如引导扇区等第一组件可在引导过程中的某个点被加载，如步骤 612 中所示。根据图 5a 中所阐述的技术，引导扇区随即可能被测定到 PCR 中。

5 步骤 611 中使用的示例性 PCR 是 PCR[8]，尽管本发明并不局限于任何特定 PCR。然后计算机可过渡到引导扇区 612 的执行。现在引导扇区可起到引导块的 RTM 的作用，就此而言，可将引导块测定到 PCR[9]中 608。计算机随即可能过渡到引导块 600 的执行。现在引导块可起到引导管理器的 RTM 的作用，并能执行以下步骤中的附加安全测定。

10 由此，引导块可将引导管理器的期望测定值加载到 PCR 601 中。图 6 中所使用的示例性 PCR 是 PCR 10。如果加载到 PCR[8]、[9]和[10]，以及任何在先或后续的被配置以进行控制的 PCR 中的值是正确的，则 TPM 可在引导块请求保密信息时授予对这类保密信息的访问。该保密信息可以是用于解密存储器中存储了引导管理器的一个部分（诸如硬盘的一个部分等）的解密密钥。此密钥可由引导块组件检索，
15 如步骤 602 中所示。注意，请求引导块为引导管理器产生正确的期望测定提供了第一层安全：如果提供了不正确的值，则 TPM 可拒绝对将引导管理器解密所需的密钥的访问。

当正确的期望值被提供时，加密密钥可被检索，它随即可能在步骤 603 中被用来将引导管理器组件解密。然后引导块可被配置成永久清除用来将引导管理器解密的“只供引导访问”密钥 604。通过在加载引导管理器以前清除只供引导访问密钥，一层安全被添加，因为如果引导管理器或后续加载的组件是被破坏的，则它将不能访问该密钥，从而在它可访问的数据中将被严格限制。当计算机的硬盘几乎完全被加密时，这尤其为真，如本发明的各个实施例所构想。

接下来，可对引导管理器组件进行测定，诸如计算该组件的散列值 605。该测定可被存储在另一个 PCR 中，诸如 PCR 13 606。可比较存储在 PCR 10 和 PCR 13 中的值，以确定它们是否匹配，如步骤 607 中所示。如果它们不匹配，则可推断引导管理器已经改变，并可能包含被破坏的或恶意的代码。记住尚未过渡到引导管理器组件的执行，因此它还不能产生任何危害。如果引导管理器已被破坏，则引导块可采取适当的安全测定。由此，可令计算机的引导随附于诸如引导管理器等关键性
30 软件组件的成功解密和测定。

参考图 7 和 8，示出一种示例性系统和方法，可用来密封引导期间所使用的保

密信息，使其与稍后控制计算资源的进程隔绝。图 7 和 8 中所揭示的过程在计算机硬盘驱动器上现有多个盘分区的情况下特别有用，尽管可认识到它们有在各种设置中有用的其它优点。图 7 和 8 中所示的过程的一个优点是它们可被用来将软件组件的访问限制在单个分区中。尽管在引导的早期阶段组件常常要求访问所有盘分区，
5 但是稍后阶段以及引导以后的组件可被限制于单个分区。图 7 和 8 示出用于确保此类限制的示例性系统和方法。

图 7 提供图 8 中所示过程的设置。图的左边示出多个盘分区，包括分区 A 700、分区 B 702、以及分区 C 704。如本领域技术人员可以理解，每个分区都可被完全加密，除了引导的早期阶段所需的信息，它们通常被存储在诸如 701、703 和 705 等保留区中。沿着图 7 的底部是软件组件，包括引导块 706、引导管理器 707、以及可如参考图 4 所述进行串行加载的操作系统 (OS) 加载器 708。图 7 中心示出多个 PCR，包括 PCR x 709、PCR y 710、t1 时的 PCR z 711、以及 t2 时的 PCR z 712。这些 PCR 通常用数字而不是字母来标识，但这里使用字母来着重强调本发明不局限于所使用的特定 PCR，尽管一些实施例可能使用图 8 中所讨论的 PCR。图 7 的
10 PCR 起到参考图 5 所描述的功能的作用——可将值放在其中，且 TPM 713 可被信任以指示该值是否正确，和/或在正确的值被输入时授予对保密信息的访问。
15

在对图 8 所反映的实施例进行更详细的解释以前，可参考图 7 阐述一般概念。可能需要一个或多个 PCR 的第一值，诸如 t1 时的 PCR z 711 的值，以通过 TPM 713 来获得对诸如密钥或 BLOB 714 等只供引导保密信息的访问。只供引导密钥或
20 BLOB 714 可能可用于将来自多个分区的信息解密，如计算机引导的早期阶段中所要求的。可能需要一个或多个第二 PCR 值，诸如 t2 时的 PCR z 712 的值，以获得对卷绑定密钥或 BLOB 715 的访问。卷绑定密钥或 BLOB 可能只可用于分区的一个子集，诸如仅可用于将来自分区 A 700 的数据解密。由此，通过使用同一 PCR 在不同时间的不同值，并调节对那些多个值上的适当密钥的密钥或 BLOB 访问，
25 可阻塞下游软件组件访问对引导组件可用的信息。为使引导正确发生，卷绑定密钥或 BLOB 715 必须被访问，这确保只供引导密钥或 BLOB 714 不再可被访问。此系统的其它优点对本领域技术人员将会是显而易见的，特别是结合图 6 中所示的系统和方法考虑以后。

参考图 8，示出用于实现诸如图 7 中所图解等系统的各种实施例。由此，在步骤 30 800 引导管理器组件可被加载。在结合了图 6 的技术的系统中，可根据本文中所演示的过程加载引导管理器。例如，在步骤 801，引导管理器的散列可被测定到

PCR 10 中。接下来，可不仅基于所有先前测定的值（如 TPM 用途中典型的）而且还基于 PCR[y]和[z]的值（例如 PCR[11]和[12]，且尚未被用测定加载，因此仍保持它们的初始值，该初始值通常为零）来从 TPM 检索只供引导访问的密钥。由此，在步骤 802，可基于 PCR[y]和[z]的初始值检索保密信息。

5 参考图 8，此外在步骤 803 和 804，OS 加载器组件可被加载到存储器中，并由引导管理器测定。OS 加载器的散列可被放到 PCR[y]中 805。注意对 PCR[y]的这一改变有效地撤消将来对只供引导访问保密信息的访问，因此如果该保密信息被引导管理器清除，则下游组件不能再找到它。然后可将 PCR[y]与存储在只供引导访问的保密信息中的值相比较 806。例如，如果只供引导访问保密信息是 BLOB，则
10 可随该 BLOB 存储该 PCR 值。如果比较成功，则可从只供引导访问 BLOB 提取卷绑定密钥 807。卷绑定密钥可被测定到 PCR[z]中 808。通过 PCR[z]，TPM 可被配置成基于新的 PCR 值授予对卷绑定保密信息的访问 809。因此，在步骤 809 中，可在只供引导访问 BLOB 的不可访问基础上调节卷绑定 BLOB 的获得。在使用此技术的本发明的实现中，所有后续进程可被有效限制于与卷绑定密钥或 BLOB 相
15 关联的分区子集。

用于保护系统数据的示例性引导验证过程

本发明的实施例可提供一种引导验证过程，它可通过用户界面（UI）在用户的命令下被开启和配置。由此，使用诸如控制面板小应用程序等程序，可令允许用户启用根据本发明的引导保护过程的操作的 UI 可用。如果机器的用户尚未接管该机器的 TPM 的所有权，则该 UI 可首先呈现接管所有权或取消的选项。可呈现类似的选项以要求用户选择特定的引导分区。如果受保护的引导被配置成仅随诸如新技术文件系统（NTFS）等特定文件系统操作，则可要求用户选择使用该文件系统的引导分区。
20

一旦从 UI 启用了受保护的引导，一自动过程即可确保要保护的顶层保密信息在可能处被重新生成，然后被密封到拆封该保密信息所需的期望的 PCR 寄存器值。较佳的实施例可将 PCR[4]、PCR[8]到（可能地）PCR[15]用于此操作。可为拆封操作委派密码，并将其存储在公共可见的位置。因此，所选择的密码可能与密封操作所用的密码不同。较佳的是用 TCG® 1.2 TPM 来支持此操作。此过程一可提供更高安全的变更允许指定更多 PCR，并且允许由机器所有者指定拆封密码，并在引导过程的早期输入该拆封密码。
30

在传统的 PC 或 AT 计算机 (PCAT) 系统上，即在使用常规 BIOS 的基于 x86 的系统中，可使用 MBR 引导扇区、NTFS 引导扇区、NTFS 引导块和引导管理器来确定期望的 PCR 值。以下结合示例性引导顺序来描述期望 PCR 值的更多细节。在可扩展固件接口 (EFI) 系统上，EFIU 系统分区 (ESP) 中的有关文件被测定。

5 在本发明一包括引导卷加密的变更中，盘解密密钥可被密封到 PCR，用于引导中直至并包括 NTFS 引导块的各早期部分。

为在恢复情形中起到帮助，上述保密信息的其它副本可被密封到涉及经由 CDROM 的恢复；经由特定恢复分区（如果这一分区存在）的恢复；以及经由第二种认证方法（诸如可移动介质和/或密码）的恢复的引导中。

10 以下提供 PCAT 系统的一种示例性引导过程。还可参考图 8 和 9 来理解本文中所演示的过程：

- 如 TCG® 1.2 规范所要求，可执行负责将 BIOS 测定到 PCR[0]中的 ROM 只读部分。
- BIOS 配置参数被测定到 PCR[1]中
- 15 • 选项 ROM 被测定到 PCR[2]中
- 选项 ROM 参数被测定到 PCR[3]中
- MBR 被测定到 PCR[4]中
- 分区表被测定到 PCR[5]中
- 在测定 MBR 以后，BIOS 将执行移交给 MBR
- 20 • MBR 加载活动分区的 NTFS 引导扇区，并将其测定到 PCR[8]中。MBR 随即将执行移交给此引导扇区。
 - 引导扇区将引导块加载到存储器中（通常 8K）。引导块被测定（除了加密信息以外）到 PCR[9]中。如果该卷是加密的，则加密信息在这个点被拆封并用来将从盘上加载的任何将来的扇区解密。
- 25 • 将引导管理器从盘中读到存储器中。它被测定到 PCR[10]中。执行被移交给引导管理器。（如上所述，一种变更可将期望的 PCR[10]测定存储在被密封的数据中间，并使用其来验证所测定的是正确的引导管理器）。
- 引导管理器将关键性数据测定到 PCR[11]中。关键性数据可包括可影响安全（诸如调试器是否将被启用等）的信息。在一些实施例中，直至用此信息扩展了
- 30 PCR[11]才能够对其进行作用。
 - 引导管理器选择一个 OS 加载器进入存储器，将其测定到 PCR[12]中，并

将执行移交给它。

- OS 加载器将关键性数据测定到 PCR[13]中。
- OS 加载器使用 PCR[4]、PCR[8-13]以及可选地任何其它 PCR，来拆封 OS 加载器所使用的保密信息。

- 5
 - OS 加载器移交到“代码完整性”来执行系统的进一步验证。
 - 代码完整性验证系统所加载的每个将来的二进制码，诸如 0 阶段驱动程序、NTKRNL 以及 HAL。

- NTKRNL 开始初始的系统进程，包括 LSASS 和 WinLogon。
- LSASS 使用 PCR[4]、PCR[8-13]以及可选地任何其它 PCR 来拆封 SYSKEY。

- 10 如果拆封失败，则 LSASS 确定原因，并提议纠正的行动，和/或由第二方法请求复原信息以获得保密信息。

- 所有访问加密的引导卷的代码使用 PCR[4]、PCR[8-9]以及任何其它指定的 PCR 来拆封引导卷解密保密信息。

- 15 在 EFI 系统中，对以上过程的数次变更可能是有益的。例如，可采取以下行动，而不是测定 MBR 并将执行移交给它：

- 除了选项 ROM 以外，基于 ROM 的驱动程序被测定到 PCR[2]中。
- 包括引导管理器在内的基于盘的驱动程序和模块被测定到 PCR[4]中
- 任何理解 NTFS 的 EFI 驱动程序都具有拆封引导卷解密保密信息的附加能力。

- 20 以上过程及其变更可被用于实现超越标准计算机引导的目的。特别地，构想了另外两个目的，尽管本发明的其它用途也是可能的，并且本发明不局限于特定设置或目的。首先，上述过程可被扩展为包括对休眠文件的保护。第二，上述过程可被扩展为包括对引导卷以及操作系统的操作所需的其它卷的保护。

- 25 就对休眠文件的保护而言，这可通过将休眠文件加密和解密密钥存储在启用保密信息中间来实现。加密和解密密钥可以是单个对称密钥，或可以是用来密封另一对称密钥的非对称密钥。当机器休眠时，休眠文件可被加密。除非机器经由经验证的引导代码路径来引导，否则休眠文件是不可解密的，因此存储在休眠文件中的任何保密信息将会被维护。如果机器经由经验证的代码路径引导，则休眠文件将由经验证的代码解密，而执行将在定义良好的执行路径中重新开始，以恢复到运行环境的安全中。

30 对引导卷以及操作系统的操作所需的其它卷的保护也可被实现。在此情形中，

整个引导卷可被加密和/或包含全面的完整性检查。解密所需的密钥仅对经验证的引导代码可用；而经验证的引导代码随即将使用这些密钥来将恢复系统的引导所需的其它代码和数据解密。更新盘的完整性信息所需的密钥也将仅对经验证的引导代码可用。一旦确保包括全面的完整性检查的系统是在运行经验证的代码，它就能够只选择完整性经验证的代码和数据进行其它操作。攻击者无法欺骗这类系统使其相信它的完整性是有效的，因为只有经验证的代码才能拆封这些启用位。

用于修理和升级受保护的引导过程的示例性系统和方法

本发明的实施例可结合诊断和修理以及升级用于安全引导计算机的系统和方法的过程。为此目的，用于诊断引导过程中的问题的第一观测是，在上述受保护的引导过程中，拆封保密信息的过程提供一种确定测定是否正确的手段。因此可能有两种状态：或者保密信息将拆封，这指示正被测定的代码中仅经验证的代码已被执行；或者保密信息将不被拆封，这指示可能未经验证的代码已被执行。对于诊断而言，就能通过检查遵守 TCG 的 BIOS 所创建的日志来确定什么出了故障。此信息随即即可被用来诊断问题，以在错误是意外而非故意的时候给出更多信息反馈。

上述受保护的引导过程依靠利用 TPM 的系统自验证。在一些实施例中，这类系统能够在其实际仍然有效时表现为无效。当系统表现为无效时，有两条解决路径，可在本发明的各个实施例中使其中任一或两者可用：第一，使用从检查日志获得的信息，可将系统返回到可被视为有效的状态。第二，用户可验证系统是否应被视为有效。

为将系统返回到可被视为有效的状态，可使用日志信息来诊断 TPM 为何将测定视为无效。改变了的任何代码可被恢复到其原始状态。或者，如果用户以不同寻常的方式引导，诸如在引导出系统盘以前试图进行网络引导等，则计算机可被重新引导，以试图按期望方式进行引导。

有许多其它特征可被结合到产品中，以对将系统返回到有效状态的实施例进行补充。例如，如果机器上的硬件坏了，而盘被移到另一个原本完全相同的机器中；则 TPM 的保密密钥可能不同。在此情形中，可认证用户而不是认证机器。称为次级认证的若干机制可实现该特征。这里使用的凭证无需轻易可得，而是可要求例如电话呼叫，以重新启用该机器。次级认证可提供与主 TPM 方法所解密的保密信息相同的保密信息，而该保密信息可用另一种方式获得。和使用与主认证方法相同的方法相比，这些实施例可提供更强的安全。例如，机器密码可纯粹随机生成，而无

需是容易记住的形式。当机器通过此次级方法请求验证时，该机器的用户呼叫其 IT 部门。IT 部门使用其所选择的系统来验证呼叫者的身份，并向呼叫者读出密码。当输入密码时，在此情形中可使用上述迁移机制来将保密信息重新密封到新的 TPM PCR 值中。此外，这一系统可使用产生只可使用一次的密码、而将保密信息 5 重新密封到次级认证机制的新密码中需要新的电话呼叫的密码系统。

用于安全引导计算机的系统和方法的实施例可被配置成能很容易被升级。尽管受本发明的实施例监视的代码很少改变，但是无可避免的是这些代码模块中的一个最终会被改变。此外，安全引导过程中所使用的保密信息可在最初配置系统的时候，或在如上述的恢复以后被密封到 TPM 中。

10 升级一个或多个引导组件的第一方法可利用恢复以后或代码修改以后可用的迁移，并可在确定 TPM PCR 值以前存储在临时存储器中。在许多实施例中，这无需重新引导，因为 PCR 值在当前引导中是已知的。但是，如果代码模块被改变了，则重新引导将确保新的代码模块被测定，且值被存储在 TPM PCR 中。

15 升级一个或多个引导组件的第二方法可在代码修改的受控环境中使用。在此情形中，由于新的代码修改的缘故，期望的 PCR 值是预定的，而保密信息在系统被重新引导以前可被密封到预期的 PCR 值中。

运行中的系统可根据以下选项的非限制性列表中的一项或多项来执行上述的迁移：

- 例如在改变以前，服务组件可知道它将改变 OS 加载器。
- 20 • 例如在刚刚改变以后，在盘已被格式化以后。
- 在经验证系统上的改变检测以后。例如，在关机时，系统可能注意到组件已被正当修改，并无声地执行迁移。
- 作为恢复的一部分。例如，在系统启动时，系统可确定恢复是否已被执行，并可执行迁移，以使下一次引导以后不再需要恢复机制。

25 维护安全引导过程的又一种系统可提供在 TPM 外部创建的多个不同的密钥。这些密钥中的每一个都可使用相同的 RSA 密钥编制素材，但每个密钥的使用可被绑定到不同的 PCR 集合和/或密码。实际上，这些附加密钥可不被绑定到任何事物。在这些实施例中，因而至少可令一个 BLOB 与每个未被绑定到任何事物的盘卷（例如，分区）相关联。每个密钥可从一不同的引导组件使用，并确保 BLOB 的保密 30 性。密码选通的密钥可用于恢复，而 RSA 密钥编制素材可由第三方保管。

尽管此方法和上述安全引导过程仅有细微差异，但维护和服务中的显著好处

变得清楚：这是由于 RSA 密钥编制素材是在 TPM 外部生成的并且在每个密钥中都是完全相同的这一事实，如今可为诸如部门或整个组织中的雇员等多个用户更大范围地使用此 RSA 素材。结果是，可创建允许打开和服务组织中的任何机器的主密钥。这些密钥仍然受每个 TPM 的 SRK 保护，因此这些密钥仍可被视为是安全的。

5 但是，在此实施例中，诸如信息技术（IT）部门等中央部门无须每个机器存储一个密钥，而是每个逻辑分组存储一个密钥。此方法在引导块中还要求略少的存储空间来存储多个 BLOB 上的多个密钥。

最后，在上述实施例中，管理员如今可下推策略和新的 RSA 密钥，因此每个机器上密钥都经常改变。这将减少维护此特征的成本。

10

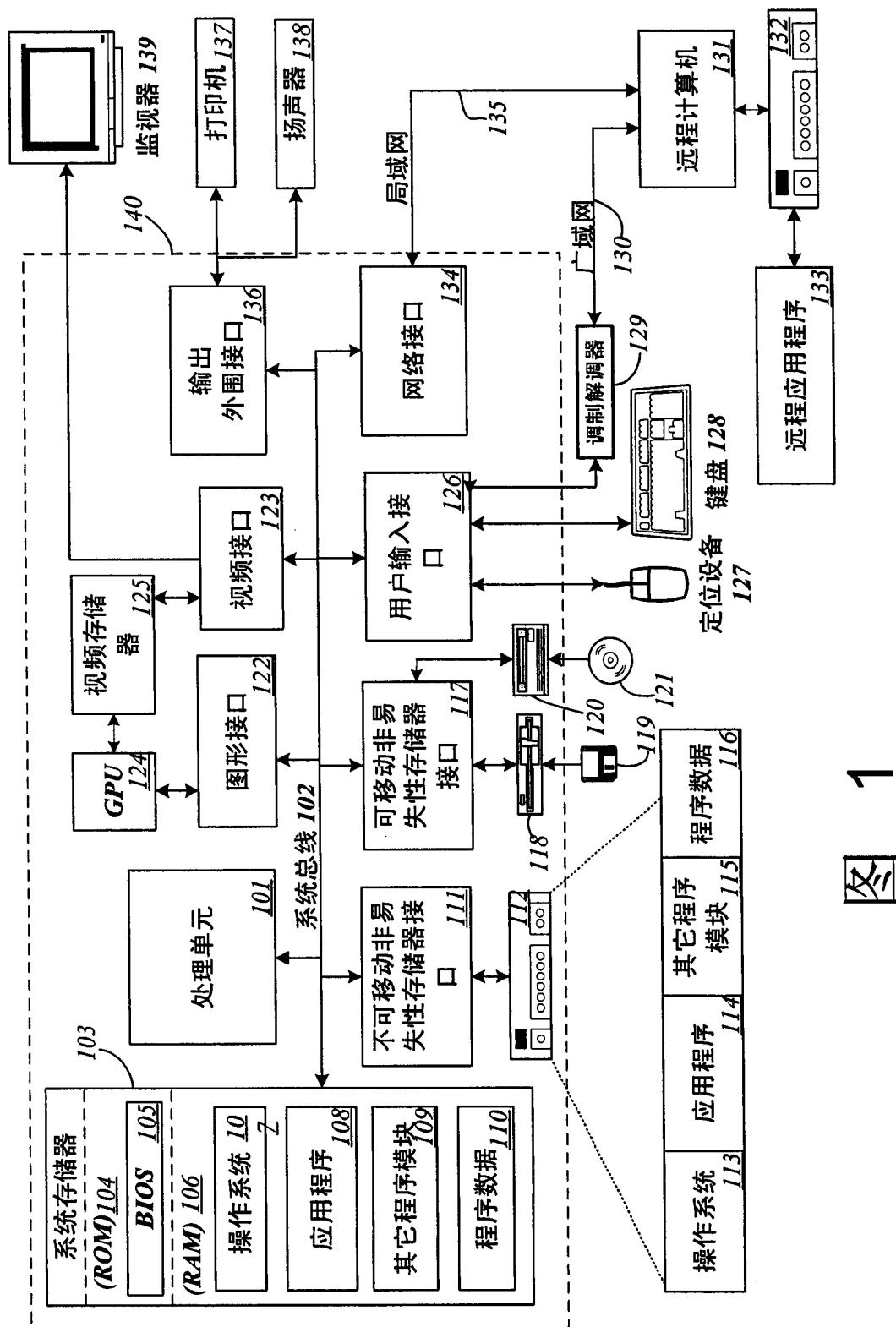
使用全卷加密和受保护引导以永久破坏对数据的访问

上述安全引导过程的一个副产品是全卷加密（即，对分区中几乎所有数据的加密）可被高效率且有效地支持。这可令摧毁保密信息并由此摧毁访问计算机上的数据所需的关键性信息所要求的工作量微不足道。数据的这种有效的摧毁在某些设置中可能是有价值的，特别是在希望清除敏感数据，尤其是迅速清除此类数据的时候。

20 消除操作实现本发明的计算机所需的保密信息无须重新安装软件即可可令这些计算机不可使用，并可永久防止对其上的数据进行访问。为实现此特征，存储在 TPM 内部的保密信息可被重置。这可通过改变 TPM 的所有权来轻松完成。该 TPM 所密封的任何保密信息将不再有效。次级恢复机制也必须被摧毁。但是，就目前直至此机制被摧毁为止而言，当将恢复机制保存在关位置时，它可规定一种临时禁用机器，然后在稍后恢复该机器的方法。

25 当存储在 TPM 内的保密信息和任何恢复机制都被改变时，机器的内容（代码和数据两者）变为不可获得。这非常迅速地实现机器的安全扫除。这类高效率的安全扫除的一个优点是它令机器的转售更加切实可行。

计算环境 100



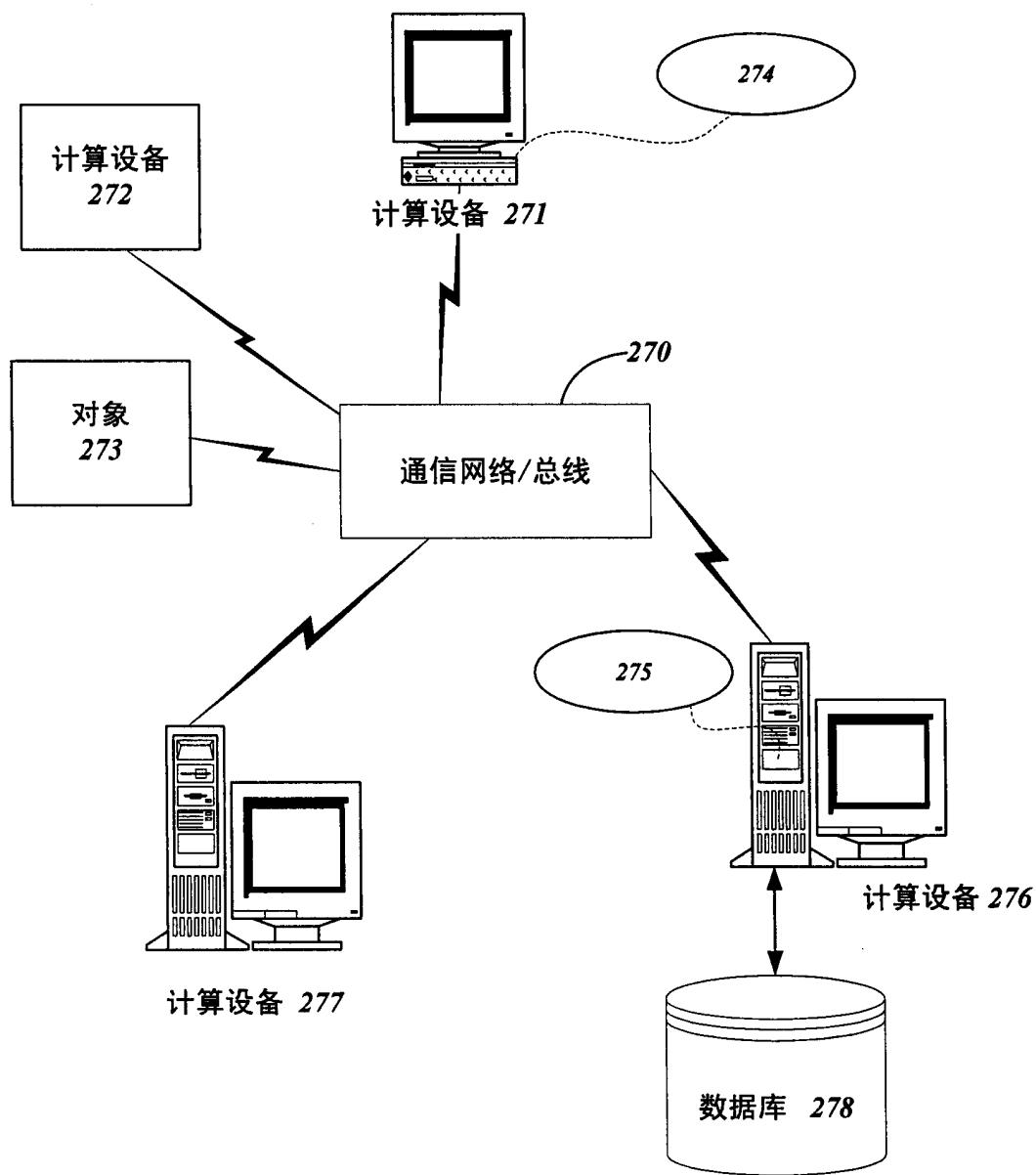


图 2

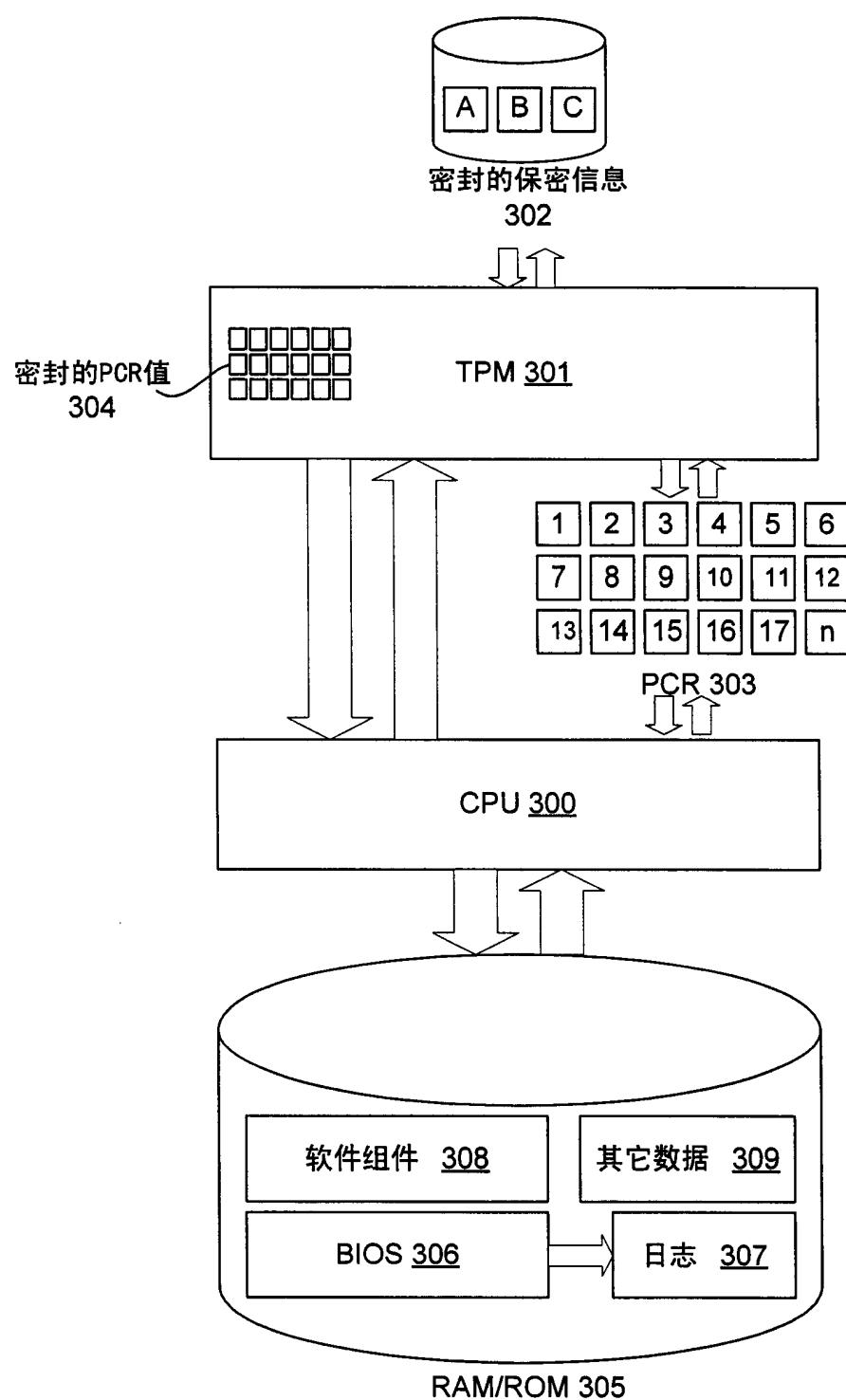


图 3

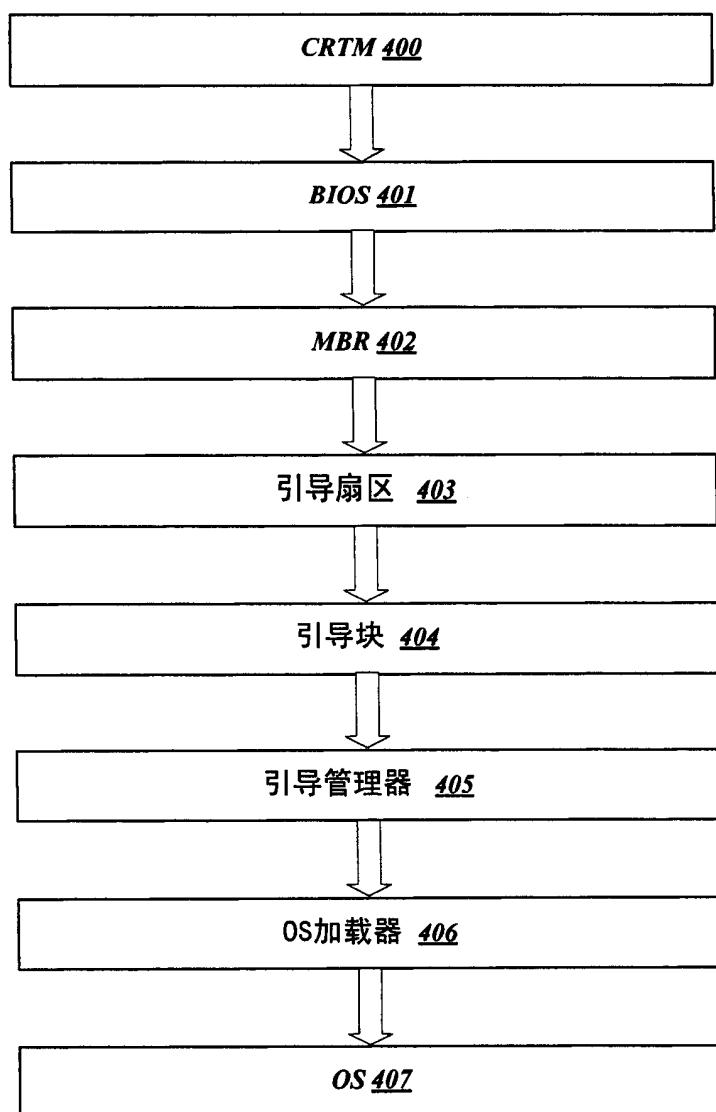


图 4

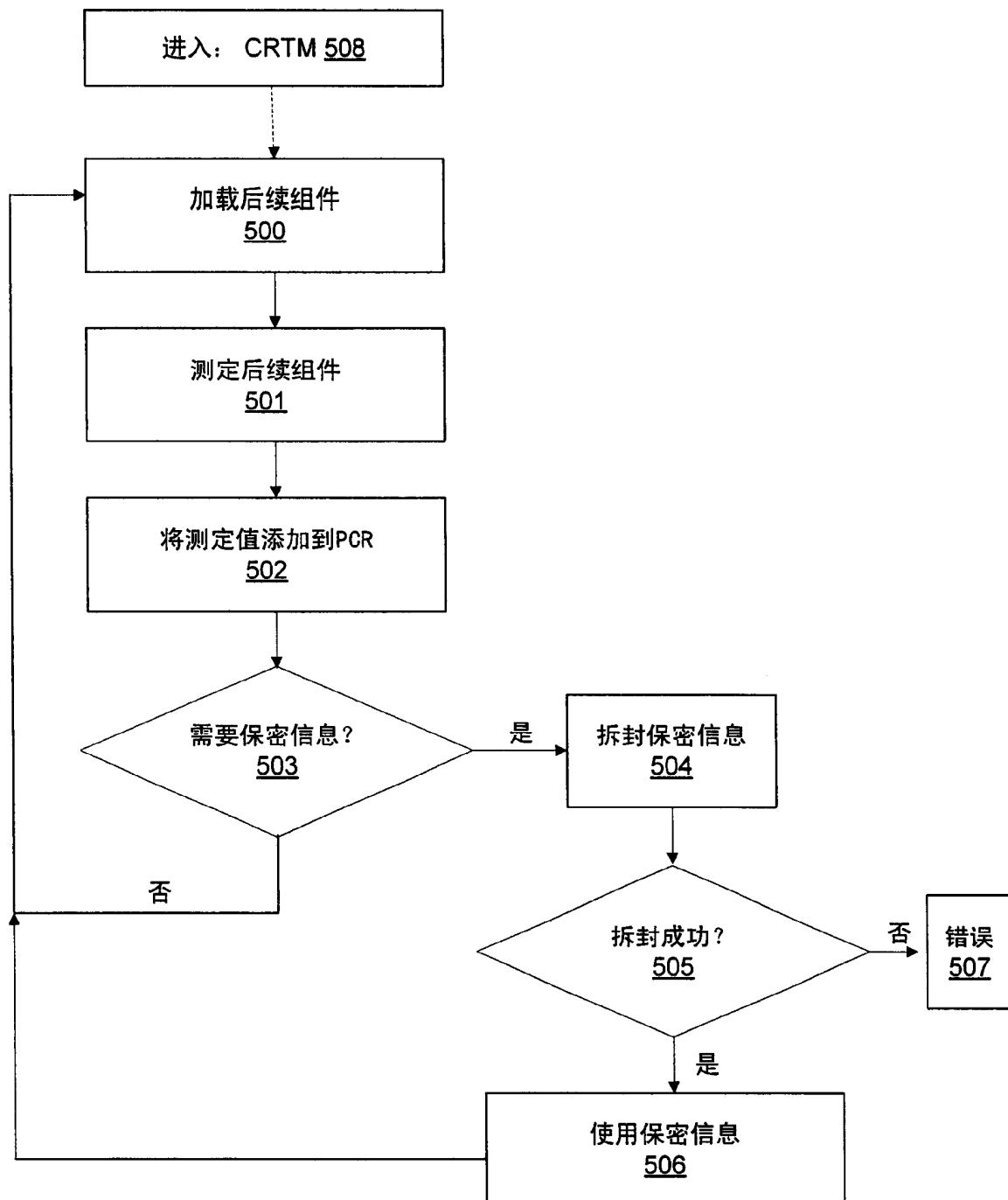


图 5

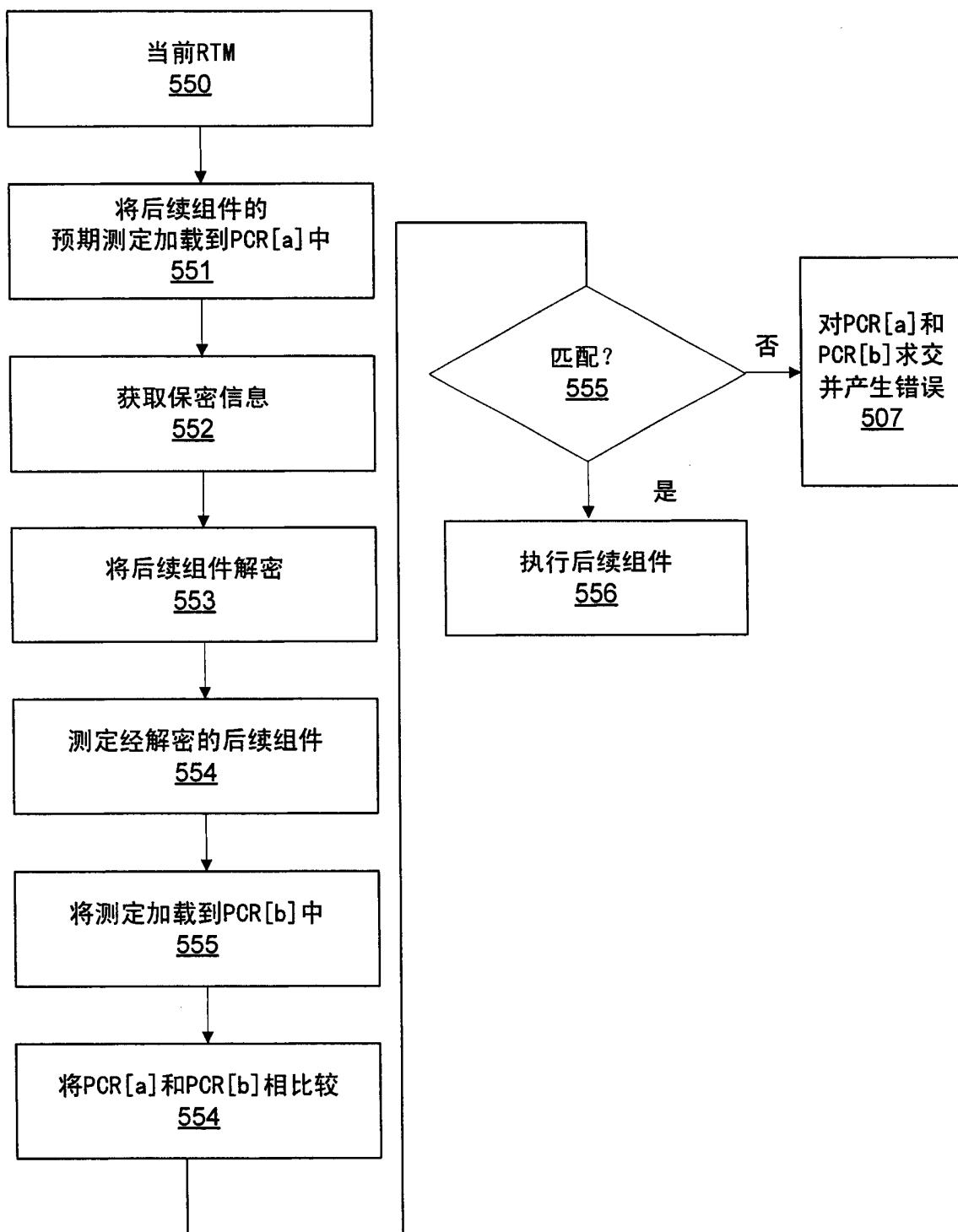


图 5a

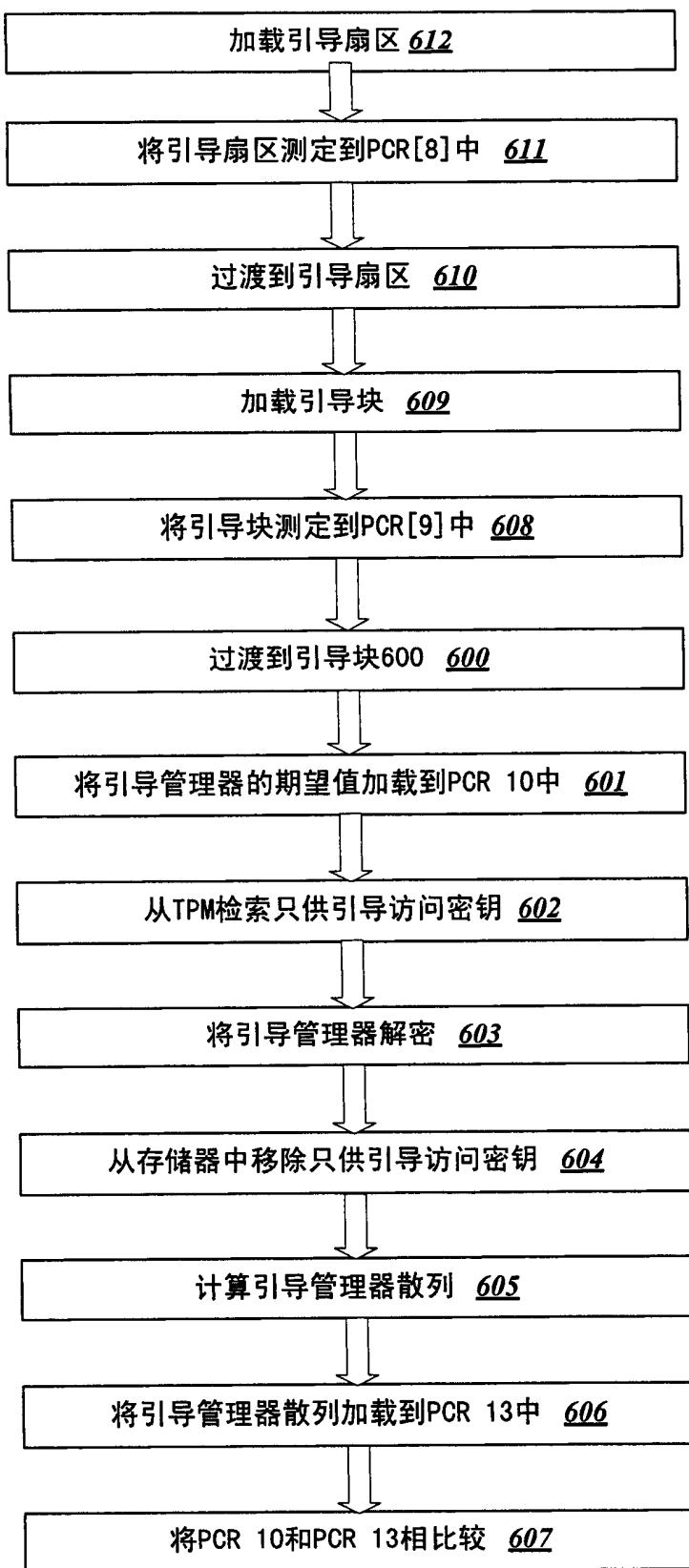
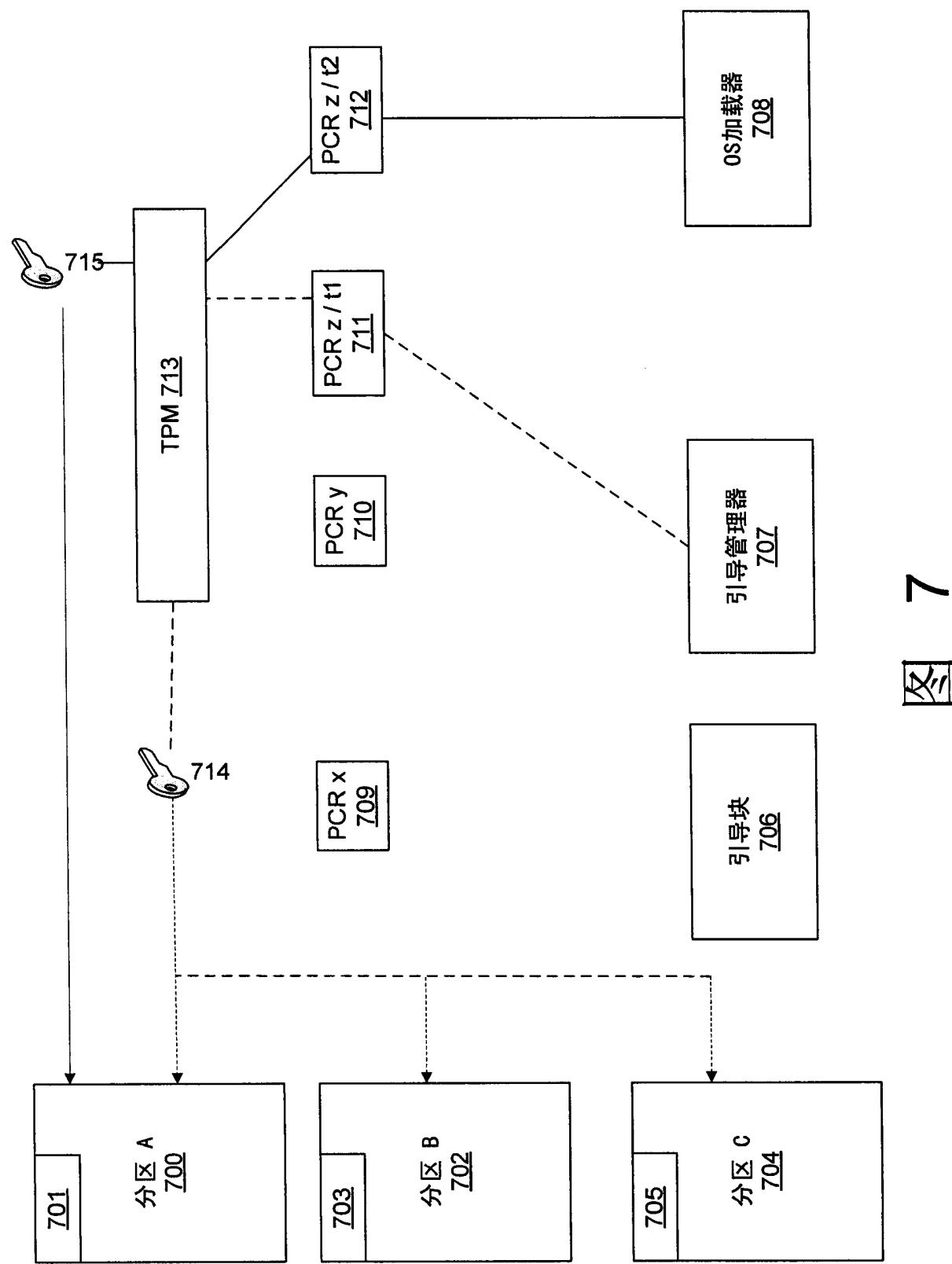


图 6



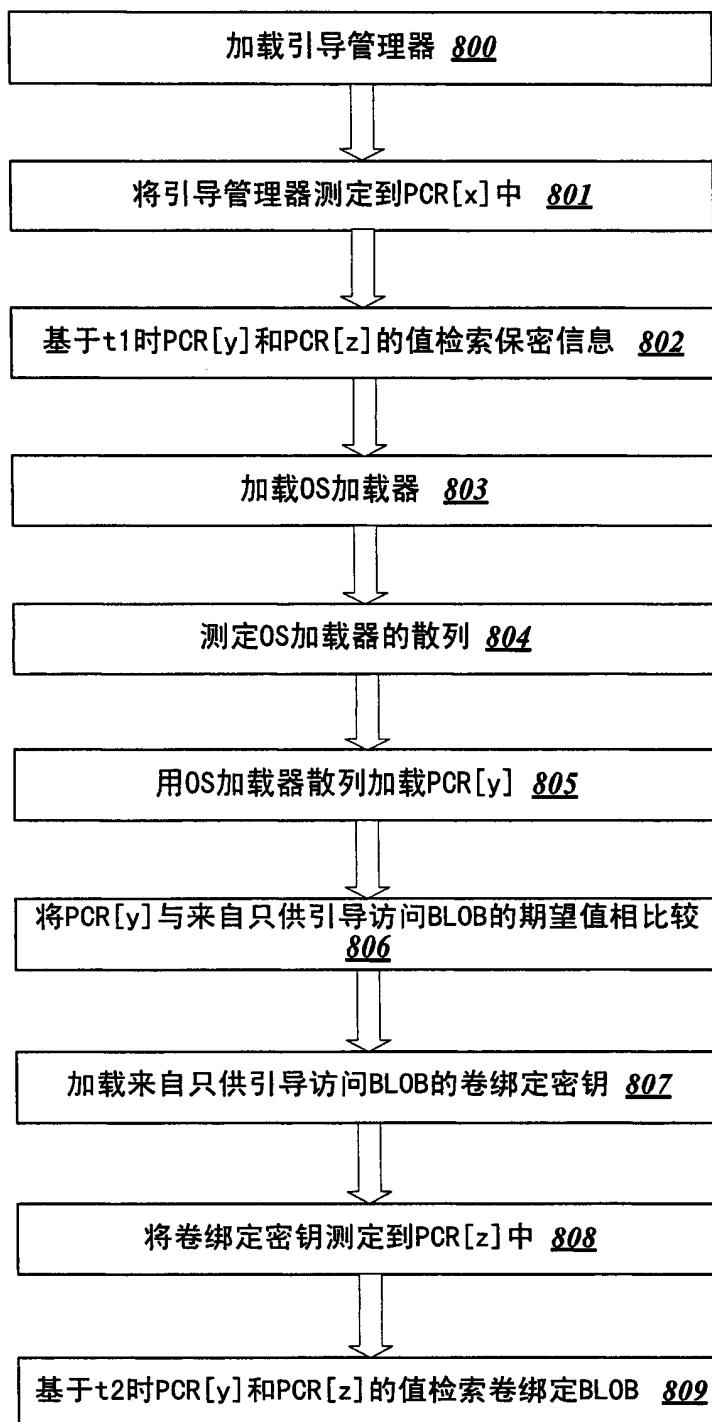


图 8