(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 102549594 B
(45)授权公告日 2015.04.08

(21)申请号 201080046403.X
(22)申请日 2010.09.24
(30)优先权数据
12/577846 2009.10.13 US
(85)PCT国际申请进入国家阶段日
2012.04.13
(86)PCT国际申请的申请数据
PCT/US2010/050275 2010.09.24
(87)PCT国际申请的公布数据
WO2011/046731 EN 2011.04.21
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 S. 索姆 C.M. 伊拉克
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 董宁 刘鹏
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 13/14(2006.01)
(56)对比文件
CN 101470789 A,2009.07.01, 权利要求1,说明书第6页2－26行,第7页1－5行,说明书附图3.
CN 101470789 A,2009.07.01, 权利要求1,说明书第6页2－26行,第7页1－5行,说明书附图3.
CN 101496337 A,2009.07.29,
CN 101441601 A,2009.05.27, 全文.
CN 1474279 A,2004.02.11,
CN 101369254 A,2009.02.18, 全文.
审查员 谢永坚

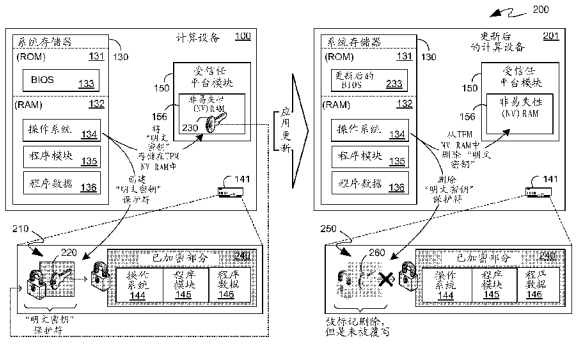
权利要求书2页 说明书12页 附图6页

(54)发明名称

临时秘密的安全存储

(57)摘要

可以把临时的敏感信息存储在TPM的非易失性存储中,并且可以从该处将其安全且不可复原地删除。此外,存储在TPM中的信息可以保护存储在可在通信方面断开的存储介质上的信息打安全,从而当在通信方面断开时,存储在这样的介质上的信息就不可访问。可以通过存储在TPM中的密钥来保护整体容量加密服务密钥,并且即使在保护符保持可访问的情况下,通过从TPM中安全地删除所述密钥也会防止对于整体容量加密服务密钥的未经授权的泄露。此外,只有在计算设备处于由PCR决定的特定状态时才可以释放在TPM中存储的数据。可以对休眠镜像进行加密并且把密钥存储在TPM中,从而只有在其状态在休眠期间没有发生重大改变的情况下才释放所述密钥来解密镜像以及恢复活跃计算。



CN 102549594 B

1. 一种用于临时暂停现有安全性机制的方法，该现有安全性机制把与该现有安全性机制关联的第一密钥绑定到计算设备的状态，该计算设备包括受信任平台模块 TPM（150），该方法包括以下步骤：

生成第一密钥的已加密版本以及解密已加密的第一密钥所需要的第二密钥，所述生成导致现有安全性机制的临时暂停；

把已加密的第一密钥存储在第一存储介质（141）上，该第一存储介质与该计算设备通信地耦合且在 TPM 外部；

把所述第二密钥存储在第二存储介质（156）上，该第二存储介质在 TPM 内部，其中对所述第二密钥的访问能自由地被 TPM 准许而不需要被限制到该计算设备的状态；

把标识在该第二存储介质（156）内存储所述第二密钥的位置的索引与已加密的第一密钥一起存储在该第一存储介质（141）上；

在把所述第二密钥存储在该第二存储介质（156）上之后，向 TPM（150）请求所述第二密钥，所述请求指定所述索引；

利用响应于所述请求而从 TPM（150）获得的第二密钥来对已加密的第一密钥进行解密；以及

当现有安全性机制被重新激活时，指示 TPM（150）从该第二存储介质（156）中删除所述第二密钥；其中，通过指示 TPM（150）删除第二密钥而导致从该第二存储介质（156）中不可复原地擦除所述第二密钥，从而即使在从该第一存储介质（141）获取了已加密的第一密钥的情况下，也无法从已加密的第一密钥获得所述第一密钥。

2. 权利要求 1 的方法，其中，把第二密钥存储在第二存储介质上的所述步骤包括：指示 TPM 响应于请求所述第二密钥来从第二存储介质提供所述第二密钥，而不管 TPM 的任何平台配置寄存器（PCR）的数值如何。

3. 权利要求 1 的方法，其中，在把第二密钥存储在第二存储介质上之后向 TPM 请求所述第二密钥的所述步骤也在计算设备的状态改变之后发生，预期到所述计算设备的状态改变而施行现有安全性机制的临时暂停。

4. 一种保护休眠镜像的方法，包括以下步骤：

在休眠之前加密包括与计算设备的状态关联的信息的休眠镜像，该计算设备包括受信任平台模块 TPM；

把已加密的休眠镜像存储在第一存储介质（141）上，该第一存储介质与该计算设备通信地耦合且在 TPM 外部；

把能利用来对所述已加密的休眠镜像进行解密的密钥存储在第二存储介质（156）上，该第二存储介质在 TPM 内部，使得如果在计算设备处于休眠状态时计算设备的状态发生重大改变，则 TPM 拒绝提供所述密钥；

把标识在该第二存储介质（156）内存储所述密钥的位置的索引与已加密的休眠镜像一起存储在该第一存储介质（141）上；

在把该密钥存储在该第二存储介质（156）上之后，向 TPM（150）请求所述密钥，所述请求指定所述索引；

利用响应于所述请求而从 TPM（150）获得的密钥来对已加密的休眠镜像进行解密；以及

当在休眠之后继续执行活跃操作时，指示 TPM（150）从该第二存储介质（156）中删除所述密钥；其中，通过指示 TPM（150）删除密钥而导致从该第二存储介质（156）中不可复原地擦除所述密钥，从而即使在从该第一存储介质（141）获取了已加密的休眠镜像的情况下，也无法从已加密的休眠镜像获得所述休眠镜像。

5. 权利要求 4 的方法，其还包括以下步骤：指示 TPM 只有在 TPM 的一个或更多平台配置寄存器 PCR 包括预期数值的情况下，才响应于请求所述密钥来从第二存储介质提供所述密钥。

6. 权利要求 5 的方法，其中，所述一个或更多 PCR 的预期数值等效于在生成休眠镜像时的 PCR 的数值。

7. 一种用于临时暂停现有安全性机制的装置，该现有安全性机制把与该现有安全性机制关联的第一密钥绑定到计算设备的状态，该计算设备包括受信任平台模块 TPM（150），该装置包括：

用于生成第一密钥的已加密版本以及解密已加密的第一密钥所需要的第二密钥的模块，所述生成导致现有安全性机制的临时暂停；

用于使已加密的第一密钥存储在第一存储介质（141）上的模块，该第一存储介质与该计算设备通信地耦合且在 TPM 外部；

用于使所述第二密钥存储在第二存储介质（156）上的模块，该第二存储介质在 TPM 内部，其中对所述第二密钥的访问能自由地被 TPM 准许而不需要被限制到该计算设备的状态；

用于使标识在该第二存储介质（156）内存储所述第二密钥的位置的索引与已加密的第一密钥一起存储在该第一存储介质（141）上的模块；

用于在把所述第二密钥存储在该第二存储介质（156）上之后，向 TPM（150）请求所述第二密钥的模块，所述请求指定所述索引；

用于利用响应于所述请求而从 TPM（150）获得的第二密钥来对已加密的第一密钥进行解密的模块；以及

用于当现有安全性机制被重新激活时，指示 TPM（150）从该第二存储介质（156）中删除所述第二密钥的模块；其中，通过指示 TPM（150）删除第二密钥而导致从该第二存储介质（156）中不可复原地擦除所述第二密钥，从而即使在从该第一存储介质（141）获取了已加密的第一密钥的情况下，也无法从已加密的第一密钥获得所述第一密钥。

临时秘密的安全存储

背景技术

[0001] 随着计算设备变得更加普及，更多敏感信息被存储在这样的计算设备上并且由其利用。因此，这样的计算设备的用户可能投入大量时间和精力来保护这种敏感信息的安全。在用于保护敏感信息的安全的各种机制当中，基于口令的机制已经变得普遍。正如本领域技术人员将认识到的那样，基于口令的保护技术可以依赖于加密技术来施行其保护。更具体来说，基于口令的保护技术在传统上对数据集合进行加密，并且只有在提供适当口令的情况下才提供对这样的数据的访问。如果没有提供适当的口令，则所述数据保持已加密形式，从而被保护免于未经授权的泄露。

[0002] 利用基于口令的保护的普遍性和易于使用的特点的一种技术是整体容量加密，从而对存储在给定容量上的所有或几乎所有数据进行加密。因此，即使恶意实体获得对于其上存储有这样的数据的存储介质的物理访问，所述容量的数据仍然将保持受到保护，这是因为这种数据将按照已加密形式被存储。正如本领域技术人员将知道的那样，整体容量加密技术在传统上依赖于一层或更多层密钥来施行有效且高效的密钥管理。因此，例如可以利用“更高”层密钥来解密“更低”层密钥，并且最终可以利用最低层密钥来解密存储在所述存储介质上的数据本身。作为一种保护措施，可以把对于一层或更多层密钥的解密绑定到计算设备本身的状态，从而使得例如在把存储介质从计算设备中去除并且可通信地耦合到不同的计算设备的情况下，所述数据不可被解密，这是因为存储介质与之可通信地耦合的计算设备的状态将已发生改变。

[0003] 在计算设备的操作期间，即使是已经被配置成用于进行安全操作的计算设备，仍然可能存在这样的情况或情形：在其期间可能必须以容易访问的形式存储敏感信息。举例来说，在对计算设备进行可能对计算设备的状态造成重大影响的更新的过程中，可能需要以容易访问的形式存储在整体容量加密机制中利用的一个或更多密钥，比如其解密在传统上被绑定到计算设备的状态的那些密钥。对于这种容易访问的信息的后续去除应当改进与按照容易访问的形式存储这种信息相关联的潜在的安全性问题。

[0004] 但是现今的存储介质常常利用这样的技术和科技：其虽然把特定数据集合标记为已删除，但是并不实际破坏存储介质本身上的这种数据。举例来说，现今的基于磁性的存储介质常常包括这样的存储容量：被标记为删除的数据可能在很长时间内都不会被实际覆写从而不会被不可恢复地破坏。在其间的时间内，所述数据可能仍然可以通过已知的数据恢复机制来访问。通过类似的方式，利用固态存储技术的现今的存储介质常常实施耗损均衡技术。作为这种技术的结果，现今的基于固态的存储介质可能直到在应当把数据不可复原地去除之后的很长时间才会实际覆写被标记为删除的数据。与基于磁性的存储介质一样，由于基于固态的存储介质无法正确地删除这样的敏感信息，因此可能会导致显著更弱的安全性状况。

发明内容

[0005] 现有的受信任平台模块(TPM)可以包括少量的安全存储容量。这样的 TPM 存储可

以被利用来存储要被不可复原地去除的敏感信息集合当中的一些或全部。与其他现今的存储介质不同，TPM 的设计规范特别要求 TPM 在被指示从其存储中去除数据时按照安全且不可复原的方式这样做。

[0006] 在一个实施例中，可以例如在特定的更新操作期间暂停整体容量加密机制，这是通过生成与所述整体容量加密机制相关联的一个或更多密钥的保护符并且随后把解锁该保护符的密钥存储在 TPM 的安全存储中而实现的。所生成的保护符可以包括元数据，所述元数据可以标识出 TPM 的安全存储内的其中存储解锁所述保护符的密钥的位置。随后，比如在完成更新操作之后，可以删除保护符和存储在 TPM 中的密钥。由于所述密钥将被不可复原地去除，因此即使在所生成的保护符本身没有被不可复原地去除的情况下（比如在其上存储所述保护符的存储介质的存储机制不提供对于被请求删除的数据的立即且不可复原的去除的情况下），所述整体容量加密仍然可以保持安全。

[0007] 在另一个实施例中，由密钥保护的信息（比如已加密信息）可以被存储在可能不提供或保证安全且不可复原的擦除的存储设备上。保护这样的信息的密钥可以被存储在 TPM 的安全存储中。如果要不可复原地去除受保护的信息，则可以把密钥安全地并且不可复原地从 TPM 去除，并且受保护信息从而可以变得不可访问，即使在存储所述受保护信息的存储设备无法保证其安全且不可复原的去除的情况下也是如此。类似地，如果受保护信息被混叠、拷贝或者以某种其他形式被存储设备保留，则仍然可以通过单独保留在 TPM 中的密钥来实现对于这样的信息的控制（包括其不可复原的去除）。

[0008] 在又一个实施例中，如果存储介质被物理地去除并且因此与其先前可通信地耦合的计算设备断开通信，则存储在所述存储介质上的数据可以保持安全并且变为不可访问。为了提供正确的计算设备对数据的鲁棒访问，可以利用整体容量加密机制来加密存储在这样的存储介质上的数据，并且可以由存储在 TPM 中的密钥保护与所述整体容量加密机制相关联的一个或更多密钥，但是对于存储在 TPM 中的密钥的访问不需要受到限制，诸如例如通过把对于该密钥的访问绑定到计算设备的特定配置。但是如果存储介质被物理地盗窃并且从而与计算设备断开通信，则无法从该计算设备的 TPM 获取这样的密钥，并且因此存储在所述存储介质上的数据将保持加密并且从而不可访问。

[0009] 在另一个实施例中，在计算设备处于休眠状态时，建立在所述计算设备上的计算环境的各个方面可以受到保护。当计算设备休眠时，可以独立于可能或者可能不由这样的计算设备利用的任何其他加密机制对所生成的休眠镜像进行加密。用于解密这样的已加密休眠镜像的密钥可以被存储在 TPM 中，并且可以将其从 TPM 到后续请求处理的释放绑定到休眠时的计算设备的特定配置。随后，当计算设备的操作从休眠中继续执行时，只有在计算设备的配置在其休眠时没有发生重大改变的情况下才能解密并访问所述已加密休眠镜像。此外，当计算设备从休眠中继续执行时可以从 TPM 中删除用于对已加密休眠镜像进行解密的密钥，从而防止针对在其配置已发生重大改变的计算设备上访问并恢复所述已加密休眠镜像的多次尝试。

[0010] 提供本概要是为了以简化的形式介绍在下面的详细描述中进一步描述的一部分概念。本概要不意图标识出所要求保护的主题内容的访问控制特征或本质特征，也不意图被用来限制所要求保护的主题内容的范围。

[0011] 通过下面参照附图做出的详细描述，附加的特征和优点将变得显而易见。

附图说明

[0012] 结合附图可以最好地理解下面的详细描述，其中：

[0013] 图 1 是包括 TPM 的示例性计算设备的图示；

[0014] 图 2 是示例性利用 TPM 来存储并且随后安全地删除被存储限定时间段的敏感信息的方框图；

[0015] 图 3 是示例性利用 TPM 来防止由于存储介质的物理失窃而导致数据散播的方框图；

[0016] 图 4 是示例性利用 TPM 在休眠期间保护计算设备的方框图；

[0017] 图 5 是示例性利用 TPM 来存储并且随后安全地删除被存储限定时间段的敏感信息的流程图；以及

[0018] 图 6 是示例性利用 TPM 在休眠期间保护计算设备的流程图。

具体实施方式

[0019] 下面的描述涉及利用现有的受信任平台模块（TPM）来存储或者以其他方式保留敏感信息，其中包括利用 TPM 的安全且不可复原地删除存储在 TPM 中的信息的能力，以及利用 TPM 的把敏感信息的释放绑定到与所述 TPM 相关联的计算设备的特定配置的能力。在在其期间可能适当的做法是暂停整体容量加密机制的情况下，可以在保护符中加密与所述整体容量加密机制相关联的一个或更多密钥，并且可以把用以解锁这样的保护符的相关联的密钥存储在 TPM 中。随后，当可以重新激活所述整体容量加密机制时，可以由 TPM 安全且不可复原地删除用于所述保护符的密钥。类似地，存储在 TPM 处的信息可以使得被存储在与无法保证安全且不可复原的擦除的存储设备相关联的存储介质中的数据不可访问，或者在这样的存储介质与计算设备断开通信的情况下也是如此。此外，当对休眠镜像进行加密并且把密钥存储在 TPM 中并且将其释放绑定到计算设备的特定状态（比如可以通过 TPM 的一个或更多平台配置寄存器（PCR）的值来表达）时，在计算设备上活跃的处理可以在所述计算设备处于休眠状态时仍然得到保护。在休眠之后继续执行活跃计算时，如果计算设备的状态在休眠期间没有发生重大改变，则 TPM 中的密钥可以被利用来解密休眠镜像。

[0020] 这里描述的技术集中于（但不限于）整体容量加密机制。实际上，下面的技术同样适用于将按照不可复原的方式施行其后续删除的任何安全信息，或者其访问受到与特定计算设备的通信连接限制的任何安全信息。因此，下面的描述不意图把所列举的实施例限制到所提到的具体示例性情况。

[0021] 虽然不作要求，但是下面的描述将在由计算设备执行的计算机可执行指令（比如程序模块）的一般情境中进行。更具体来说，除非另行声明，否则下面的描述将涉及由一个或更多计算设备或外设施行的动作和操作的象征性表示。因此应当理解的是，这样的动作和操作（其有时被称作由计算机执行）包括由处理单元操纵以结构化形式代表数据的电信号。该操纵对数据进行变换或者在存储器中的一些位置处保持所述数据，其以本领域技术人员很好理解的方式重新配置或者以其他方式改动计算设备或外设的操作。在其中保持数据的数据结构是具有由数据的格式定义的特定属性的物理位置。

[0022] 一般来说，程序模块包括例程、程序、对象、组件、数据结构等等，其施行特定任务

或者实施特定抽象数据类型。此外，本领域技术人员将认识到，计算设备不需要被限制到传统的个人计算机，而是可以包括其他计算配置，其中包括手持式设备、多处理器系统、基于微处理器的或可编程的消费电子装置、网络PC、小型计算机、大型计算机等等。类似地，计算设备不需要被限制到单体式计算设备，这是因为还可以在通过通信网络链接在一起的分布式计算环境中实践所述机制。在分布式计算环境中，程序模块既可以位于本地也可以位于远程存储器存储设备中。

[0023] 参照图 1，其中示出了示例性的计算设备 100，其部分地包括在下面描述的方法中进一步提到的各个硬件元件。示例性计算设备 100 可以包括（但不限于）一个或更多中央处理单元（CPU）120、系统存储器 130、受信任平台模块（TPM）150 以及把包括系统存储器在内的各个系统组件连接到处理单元 120 的系统总线 121。系统总线 121 可以是几种类型的总线结构当中的任一种，其中包括存储器总线或存储器控制器、外围总线以及使用多种总线体系结构当中的任一种的局部总线。取决于具体的物理实现方式，CPU 120、系统存储器 130 和 TPM 150 中的一个或更多可以在物理上位于一处，比如位于单个芯片上。在这种情况下，系统总线 121 的一部分或全部可以不过是单个芯片结构内的硅路径，并且其在图 1 中的图示可以不过是为了说明目的的标记方便。

[0024] TPM 150 可以包括用于对提供给它的信息进行加密和解密的加密密钥 151。在传统上，TPM 150 包括不可变的公共和私有加密密钥的初始集合，其可以按照已知的、已确立的方式被利用来获得可丢弃的公共和私有加密密钥。此外，TPM 150 可以包括平台配置寄存器（PCR）155，其可以安全地存储与计算设备 100 的状态唯一地相关联的数值或其他数据。这样的数值在传统上由 CPU 120 通过系统总线 121 提供给 TPM 150。在一些实施例中，只有由 CPU 120 执行的特定代码才将被允许向 TPM 150 发送数据，其将修改存储在 PCR 155 中的数值。TPM 150 还可以包括非易失性存储容量，比如非易失性 RAM 156，TPM 可以在其中安全地存储由计算设备的其他元件（比如 CPU 120）通过系统总线 121 提供给它的至少少量信息。

[0025] 除了前面描述的元件之外，计算设备 100 通常还包括计算机可读介质，其可以包括能够由计算设备 100 访问的任何可用介质。作为举例而非限制，计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括按照任何方法或技术所实施的用于存储诸如计算机可读指令、数据结构、程序模块或其他数据之类的信息的介质。计算机存储介质包括（但不限于）RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字通用盘（DVD）或其他光盘存储、磁带盒、磁带、磁盘存储或其他磁性存储设备或者可以被用来存储所期望的信息并且可以由计算设备 100 访问的任何其他介质。通信介质通常在诸如载波之类的已调数据信号或其他传输介质中具体实现计算机可读指令、数据结构、程序模块或其他数据，并且包括任何信息递送介质。作为举例而非限制，通信介质包括诸如有线网络或直接连线连接之类的有线介质，以及诸如声学、RF、红外和其他无线介质之类的无线介质。前述各项的任意组合也应当被包括在计算机可读介质的范围内。

[0026] 在使用通信介质时，计算设备 100 可以通过去到一个或更多远程计算机的逻辑连接而操作在联网环境中。图 1 中描绘的逻辑连接是去到网络 180 的通用网络连接 171，所述网络 180 可以是局域网（LAN）、广域网（WAN）或其他网络。计算设备 100 通过网络接口或适配器 170 连接到通用网络连接 171，所述网络接口或适配器 170 又连接到系统总线 121。在

联网环境中，关于计算设备 100 描绘的程序模块或者其一些部分或外设可以被存储在通过通用网络连接 171 可通信地耦合到计算设备 100 的一个或更多其他计算设备的存储器中。应当认识到，所示出的网络连接是示例性的，并且可以使用建立计算设备之间的通信链接的其他措施。

[0027] 在计算机存储介质当中，系统存储器 130 包括具有易失性和 / 或非易失性存储器形式的计算机存储介质，其中包括只读存储器（ROM）131 和随机存取存储器（RAM）132。特别包含用于引导计算设备 100 的代码的基本输入 / 输出系统 133（BIOS）通常被存储在 ROM 131 中。RAM 132 通常包含由处理单元 120 立即可访问以及 / 或者当前正由其操作的数据和 / 或程序模块。作为举例而非限制，图 1 把操作系统 134、其他程序模块 135 和程序数据 136 显示为驻留在 RAM 132 中。RAM 132 还可以包括可能与 TPM 150 的操作有关的数据，比如 TCG 事件日志 190。在一个实施例中，TCG 事件日志 190 可以包括自从加电以来或者自从其上一次重启以来由计算设备 100 所加载或执行的所有模块的唯一标识；也就是其加载或执行可能已经得到了当前由 TPM 150 保持在一个或更多 PCR 155 中的数值的相同模块。

[0028] 计算设备 100 可以附加地包括其他可移除 / 不可移除、易失性 / 非易失性计算机存储介质。仅仅作为举例，图 1 示出了从 / 向不可移除、非易失性磁性或固态介质进行读取或写入的硬盘驱动器 141。可以与所述示例性计算设备一起使用的其他可移除 / 不可移除、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、数字通用盘、数字视频带、固态 RAM、固态 ROM 等等。硬盘驱动器 141 通常经由诸如接口 140 之类的不可移除存储器接口连接到系统总线 121。

[0029] 前面讨论的并且在图 1 中示出的驱动器及其相关联的计算机存储介质提供对于计算机可读指令、数据结构、程序模块以及用于计算设备 100 的其他数据的存储。在图 1 中，例如硬盘驱动器 141 被显示为存储操作系统 144、其他程序模块 145 和程序数据 146。应当提到的是，这些组件可以与操作系统 134、其他程序模块 135 和程序数据 136 相同或不同。操作系统 144、其他程序模块 145 和程序数据 146 在此被给出不同的编号以便表明其至少是不同的拷贝。

[0030] 在一个实施例中，操作系统 144、其他程序模块 145 和程序数据 146 可以按照已加密形式被存储在硬盘驱动器 141 上。举例来说，硬盘驱动器 141 可以实施或者与整体容量加密机制一起利用，从而可以按照已加密格式来存储被存储在硬盘驱动器 141 上的所有或基本上所有数据。参照图 2，在示例性系统 200 中，硬盘驱动器 141 被显示为包括已加密部分 240，其可以包括操作系统 144、程序模块 145 和程序数据 146 的至少很多部分。密钥 220 可以由计算设备 100 或者由与硬盘驱动器 141 相关联的硬件利用来解密来自已加密部分 240 的数据，从而使得计算设备能够有意义地访问操作系统 144、程序模块 145 和程序数据 146。

[0031] 正如本领域技术人员所知，整体容量加密机制可以利用多个级别和层次的密钥，比如密钥 220。举例来说，为了避免不得不利用不同的密钥再加密诸如操作系统 144、程序模块 145 或程序数据 146 之类的数据，可以通过另一个密钥来对密钥 220 本身进行加密。密钥 220 的已加密版本以及与这样的已加密密钥相关联的任何元数据可以被称作“密钥保护符”。同样地，正如本领域技术人员所知，对于单个密钥可以生成多个密钥保护符，其中每一个密钥保护符与不同的认证或其他安全性机制相关联。因此，举例来说，可以解密存储在硬盘驱动器 141 的已加密部分 240 中的数据的密钥 220 可以利用与用户口令相关联的密钥

而被加密到一个密钥保护符中，并且可以利用与 PCR 155 的具体数值相关联的密钥而被加密到另一个密钥保护符中。按照这种方式，如果经过授权的用户输入其口令，或者如果 PCR 155 的数值表明计算设备处于受信任状态，则可以通过计算设备 100 来解密并访问已加密部分 240。

[0032] 如前所示，可以利用多个层次的密钥来提供各种访问替换方案。此外，可以将多个层次的密钥用于其他密钥管理目的，其中例如包括提高可靠性、提供安全性保障、提高性能、提供对于例如可能忘记其密钥的用户的第三方帮助或支持或者其他目的。因此，在下面的描述中，在提到与整体容量加密机制相关联的密钥(比如密钥 220)时，意图涉及任何层次的密钥，而不意图排他性地仅仅涉及例如直接对已加密部分 240 进行解密的特定密钥。

[0033] 在某些情况下，可能需要临时暂停通常由整体容量加密机制提供的保护。举例来说，在可能影响计算设备 100 的受信任状态的更新期间，可能需要暂停整体容量加密，这是因为可能难以或者不可能预先确定 PCR 155 的适当数值，而没有这样的确定，可能就无法访问使得能够访问存储在已加密部分 240 中的数据所需要的并且与 PCR 的具体数值相关联的密钥。为了避免这样的困难，可以在预期到对于计算状态的改变的情况下临时地暂停整体容量加密或其他安全性机制，这例如是通过生成“明文密钥”保护符 210 而实现的，所述“明文密钥”保护符 210 可以同时包括密钥 220 的已加密版本以及对密钥 220 的所述已加密版本进行解密所需要的密钥。可以看出，这样的“明文密钥”保护符 210 可以使得有能力访问所述“明文密钥”保护符的任何处理能够访问受保护的密钥本身(比如密钥 220)，所述受保护的密钥又可以使得这样的处理能够访问已加密部分 240 中的所有数据。因此，例如硬盘驱动器 141 上的“明文密钥”保护符 210 的存在有效地暂停或禁用实施在这样的驱动器上的整体容量加密的安全性方面。为了重新启用比如实施在图 2 的系统 200 的硬盘驱动器 141 上的整体容量加密机制的安全性方面，可以按照无法复原的方式从硬盘驱动器中删除“明文密钥”保护符 210。

[0034] 为了提供对于敏感信息(诸如例如可以规避整体容量加密机制的安全性方面的明文密钥保护符)的不可复原的删除，可以把特定信息存储在 TPM 150 的 NV RAM 230 中。因此，在一个实施例中，如图 2 的系统 200 中所示，操作系统 134 或其他处理可以创建可以被存储在硬盘驱动器 141 上的明文密钥保护符 210，但是与明文密钥保护符 210 相关联的密钥 230 不是像前面描述的那样与明文密钥保护符存储在一起，而是被存储在 TPM 150 的 NV RAM 156 中。因此，操作系统 134 被图示为向两个不同的存储介质提供数据。具体来说，操作系统 134 可以把明文密钥保护符 210 存储在硬盘驱动器 141 上，并且可以把与明文密钥保护符 210 相关联的密钥 230 存储在 TPM 150 的 NV RAM 156 中。

[0035] 图 2 的系统 200 的明文密钥保护符 210 可以包括指向存储在 TPM NV RAM 156 中的密钥 230 的指针而不是密钥 230 本身。更具体来说，在一个实施例中，明文密钥保护符 210 可以包括密钥 230 被存储在 TPM 150 的 NV RAM 156 中的 NV 索引。正如本领域技术人员所知，对于明文密钥保护符 210 的后续访问将揭示与之存储在一起的 NV 索引，从而允许进行访问的处理向 TPM 150 请求密钥 230。作为响应，TPM 150 可以向发出请求的处理提供密钥 230，并且发出请求的处理可以利用这样的密钥 230 从明文密钥保护符 210 获得密钥 220，并且访问已加密部分 240 中的信息。

[0036] 如图 2 的系统 200 中所示，一旦计算设备 100 以更新后的计算设备 201 的形式被

更新，操作系统 134 或其他有关处理就可以删除被生成来规避例如实施在硬盘驱动器 141 上的整体容量加密的安全性方面的信息。因此，如图所示，可以向硬盘驱动器 141 提供针对删除明文密钥保护符 210 的指令，并且可以向 TPM 150 提供针对删除密钥 230 的指令。如前所示，可能无法从硬盘驱动器 141 的存储介质中不可复原地去除明文密钥保护符 210。举例来说，如果硬盘驱动器 141 由磁性存储介质构成，则明文密钥保护符 210 可能保持在这样的磁性存储介质上，直到其实际上被提供来存储在硬盘驱动器 141 上的其他数据覆写为止。虽然传统的基于磁性存储介质的存储设备可以实施可能随机覆写被标记为删除的数据的安全删除功能，但是磁性存储介质的性质使得即使其被覆写几次也仍然有可能恢复先前存储的信息。类似地，如果硬盘驱动器 141 由基于固态的存储介质构成，则明文密钥保护符 210 在被标记为删除之后也仍然可能保持在这样的基于固态的存储介质上。更具体来说，基于固态的存储介质通常与耗损均衡技术相结合地利用，所述耗损均衡技术可以避免对于特定节段的写入次数多于任何其他节段。其结果是，存储在某些节段上的数据（即使是应被删除的数据）也可能在一个很长的时间段内保持可访问状态。

[0037] 在图 2 的系统 200 内，明文密钥保护符 250 和密钥 260 意图说明处于已删除但是可恢复状态的明文密钥保护符 210 和受保护密钥 220。但是从图 2 中可以看出，通过从 TPM NV RAM 156 不可复原地去除密钥 230 可以重新建立实施在硬盘驱动器 141 上的整体容量加密的安全性方面。更具体来说，如果密钥 230 与明文密钥保护符 210 被存储在一起，则即使在删除之后，仍然可能从硬盘驱动器 141 的存储介质恢复明文密钥保护符 250，并且可能获得密钥 260 并且利用其来访问存储在硬盘驱动器 141 的已加密部分 240 内的信息。但是由于密钥 230 被存储在 TPM 150 内，而 TPM 150 在得到指令这样做时可以遵循要求安全地删除存储在其 NV RAM 156 内的信息的规范，因此从硬盘驱动器 141 的存储介质恢复明文密钥保护符 250 将不会得到密钥 260，这是因为访问保护符 250 及获得密钥 260 所需要的密钥 230 将不再可用或可复原。其结果是，即使在没有安全地或者不可复原地删除明文密钥保护符 210 的情况下，存储在已加密部分 240 内的信息也可以保持受到保护。

[0038] 虽然前面的描述和图 2 中提供的图示提到了保护密钥 220 的保护符并且密钥 220 被显示为直接负责解密已加密部分 240，但是本领域技术人员将认识到，前面的描述和图示同样适用于传统上由诸如整体容量加密机制的安全机制生成并且与之相结合地使用的多个层次的密钥当中的任一个。因此，举例来说，受保护密钥 220 不需要直接能够解密已加密部分 240，而是可以替换地是中间级别的密钥，其可以替换地解密另一个密钥，所述另一个密钥可以随后解密已加密部分 240。

[0039] 此外，虽然前面的描述和图 2 中提供的图示特别是针对安全地删除与整体容量加密机制相关联的未受保护的或者“明文密钥保护符”，其例如可以在诸如计算设备 100 之类的计算设备的状态改变期间被临时利用，但是前面描述的原理同样适用于安全地删除存储在与不能保证安全删除的存储设备相关联的存储介质上的任何受保护数据。更具体来说，如果信息以受保护方式被存储，从而可以利用某项其他数据（其在这里按照传统被称作“密钥”）来访问该信息，则为了提供对于这样的信息的安全且不可复原的去除，可以把受保护信息存储在任何存储介质上，并且可以把密钥存储在 TPM NV RAM 156 中，正如前面所详细描述的那样。即使存储介质以及与这样的存储介质相关联的存储设备无法提供或保证对于受保护信息的安全且不可复原的去除，可以由 TPM 150 提供的对于所述密钥的安全且不可

复原的删除实际上也可以像前面详细描述的那样导致对于受保护信息的不可复原的去除，而不管在其上存储这样的受保护信息的存储介质或设备的能力如何。

[0040] 在许多情况下，存储介质以及与所述介质相关联的存储设备由于基于硬件的机制而无法保证不可复原的去除，所述基于硬件的机制可能混叠、拷贝、复制或者以其他方式倍增存储在所述存储介质上的受保护信息，从而使得对于受保护信息的一份拷贝或方面的安全去除可能无法保证对于所有这样的方面或拷贝的安全去除。在这种情况下，受保护信息可能作为存储硬件的一部分而扩散，通过把单个密钥保留在TPM NV RAM 156中可以提供一种单一性措施以及对于受保护信息的控制。此外，虽然并不要求，但是如果需要不可复原地去除受保护信息，则可以通过从TPM NV RAM 156中安全且不可复原地去除密钥来实现这一点，正如前面所详细描述的那样。

[0041] 在另一个实施例中，把诸如密钥230之类的密钥存储在TPM NV RAM 156中的做法可以被利用来提供一种针对诸如硬盘驱动器141之类的存储设备的物理失窃的保护措施，或者替换地针对从例如出于维护原因而被合法地移除的存储设备窃取信息而提供保护。参照图3，其中示出了包括计算设备100的系统300，所述计算设备100具有可以与计算设备在物理和通信方面分离的硬盘驱动器141。如前所述，可以创建保护密钥220的密钥保护符210并且将其存储在硬盘驱动器141上。与之前一样，密钥220可以被直接地或间接地利用来解密并访问硬盘驱动器141的已加密部分240。通过把密钥230存储在TPM NV RAM 156中并且与密钥保护符210一起提供指向密钥230的指针，在试图访问存储在硬盘驱动器141的已加密部分240中的信息时，计算设备100以及在其上执行的处理遵循来自密钥保护符210的指针去到TPM NV RAM 156中的存储密钥230的位置，并且可以随后从TPM 150获得这样的密钥并且利用其来最终访问硬盘驱动器的已加密部分。

[0042] 此外，在一个实施例中，对于密钥230的访问或者更具体来说对于TPM NV RAM 156的存储密钥230的特定索引的访问可以自由地被TPM 150准许，而不需要被限制到PCR 155的特定数值，或者与计算设备100的状态相关联的其他类似信息。因此，执行在计算设备100上的处理可以自由地访问存储在硬盘驱动器141的已加密部分240内的信息而不管对于计算设备或者由其执行的处理的总体安全性可能无关紧要的计算设备的状态的各个方面。这样的环境在传统上可以配备有基于硬件的安全性(比如有限访问物理环境)的服务器计算设备中可能特别有用，所述基于硬件的安全性可以最小化服务器计算设备100的状态以不安全方式发生改变的几率，但是应当尝试保持尽可能多的操作正常运行时间。

[0043] 但是如果这样的计算设备(或者更具体来说是这样的计算设备的组件)被盗，则通过如前所述把必要的信息存储在TPM NV RAM 156中可以防止利用来自被盗硬盘驱动器141或其他类似的被盗存储介质的已加密部分240的信息。替换地，如果硬盘驱动器141发生了可能导致必须更换所述硬盘驱动器的故障，则一旦把硬盘驱动器或任何其他类似的存储介质在物理和通信方面与计算设备100分离之后，可能就无法访问存储在硬盘驱动器141的已加密部分240内的信息。实际上，存储在硬盘驱动器141的已加密部分240内的信息可以足够地不可访问，从而一旦硬盘驱动器与计算设备100在通信方面分离，其可以满足各种安全性标准而不需要对硬盘驱动器或存储在其上的信息进行高成本并且耗时的擦除或其他破坏。

[0044] 从图3的系统300可以看到，如果硬盘驱动器141与计算设备100在通信方面分

离，例如如果硬盘驱动器 141 被从服务器计算设备 100 物理地移除（例如作为经过授权的维护的一部分或者由于被盗）并且随后可通信地耦合到不同的计算设备，则执行在这样的不同计算设备上的处理将不能访问存储在计算设备 100 的 TPM 150 的 NV RAM 156 中的密钥 230。由于无法访问这样的密钥 230，因此执行在硬盘驱动器 141 随后与之可通信地耦合的不同计算设备上的处理将不能从保护符 210 获得密钥 220，因而将不能有意义地访问存储在硬盘驱动器 141 的已加密部分 240 内的信息。由于执行在计算设备 100 外部的计算设备上的处理不管是通过电子通信机制还是通过对 TPM 150 本身的物理访问都无法容易地从 TPM 150 获得存储在 NV RAM 156 内的信息，因此通过把诸如密钥 230 之类的必要信息存储在 TPM NV RAM 中，可以在不对计算设备 100 的操作正常运行时间造成负面影响的情况下，针对存储在可以与计算设备 100 在通信方面断开的存储介质上的数据提供一种安全性措施，其中包括针对盗窃的安全性以及针对作为经过授权的维护的一部分被更换的存储介质的后续访问的安全性。

[0045] 虽然在前面没有特别列举出来，但是正如本领域技术人员所知，TPM 150 可以把存储在其中（比如存储在 TPM NV RAM 156 上）的信息的释放限制到计算设备 100 的比如在传统上将由一个或更多 PCR 155 的数值代表的特定状态。因此，在另一个实施例中，TPM 150 的这种看门功能可以被利用来在计算设备 100 可能处于易受攻击状态时（诸如比如当计算设备处于休眠或其他暂停状态时）保护信息。

[0046] 参照图 4，系统 400 示出了可以在计算设备 100 处于休眠状态时借以保护休眠镜像 410 的一种示例性机制。最初，在计算设备 100 启动休眠之后，可以创建休眠镜像 410。正如本领域技术人员所知并且如图 4 中的虚线所示，诸如休眠镜像 410 之类的休眠镜像可以包括与计算设备在休眠之前的状态相关联的信息。举例来说，休眠镜像 410 可以包括在休眠时存在于计算设备 100 的 RAM 132 中的操作系统 134、程序模块 135 和程序数据 136 的状态，从而在从休眠状态继续执行之后，计算设备 100 可以把信息从休眠镜像 410 加载到 RAM 132 中，从而允许操作系统和程序模块继续执行其之前的动作或执行。

[0047] 由于休眠镜像 410 可以包括与处于执行状态下的处理和应用相关联的信息，因此其可以包括可能只有在可能已经施行了特定的与安全性有关的动作之后才可用的信息。举例来说，可能只有在确定了计算设备 100 处于受信任状态之后才把操作系统 134 或程序模块 135 的某些方面加载到 RAM 132 中。但是操作系统 134 或程序模块 135 的这些方面现在可能驻留在 RAM 132 中而没有任何进一步的保护。如果将要收集并存储这样的信息以作为休眠镜像 410 的一部分，则诸如例如在计算设备 100 处于休眠状态时对于所述休眠镜像的后续访问可能会提供对于所述信息的访问，而没有意图保护这样的信息免于未经授权的访问的通常的安全性限制。

[0048] 因此，在一个实施例中，为了保持休眠镜像 410 的完整性和计算设备 100 的状态，可以对休眠镜像进行加密并且存储为如图 4 的系统 400 中所示的已加密休眠镜像 415。虽然图 4 的系统 400 示出了对于休眠镜像 410 的加密由操作系统 134 施行，但是本领域技术人员将认识到，这样的加密同样可以由其他处理施行，其中例如包括作为程序模块 135 的一部分执行的处理。除了对休眠镜像 410 进行加密并且将其作为已加密休眠镜像 415 存储在存储设备（诸如例如硬盘驱动器 141）上之外；操作系统 134 或其他有关处理还可以在 TPM NV RAM 156 中存储密钥 430，所述密钥 430 可以解锁已加密休眠镜像 415 或者以其他方式

提供对于休眠镜像 410 的访问。

[0049] 在一个实施例中，可以结合针对 TPM 150 的指令将密钥 430 存储在 TPM NV RAM 156 中，所述指令指示 TPM 除非在发出针对密钥 430 的请求时的 PCR 155 的数值当中的一个或更多个与计算设备 100 休眠时相同，否则不要释放或者以其他方式提供密钥 430。更具体来说，如前所示，一个或更多 PCR 155 的数值可以与计算设备 100 的状态唯一地相关联。因此，在计算设备 100 休眠时，一个或更多 PCR 155 的数值可以反映计算设备 100 在休眠时的状态，以及当计算设备从休眠中继续执行时所述计算设备应当具有的状态。因此，可以参照一个或更多 PCR 155 的数值来确保计算设备 100 的状态从其休眠时到其随后继续执行时为止没有发生重大改变，因此，可以把如前所示地能够提供对于休眠镜像 410 的访问的密钥 430 的释放绑定到计算设备休眠时的一个或更多 PCR 155 的数值。

[0050] 随后，当计算设备 100 从休眠中继续执行时，正如本领域技术人员所知可以作为操作系统 134 的部件的引导加载器 434 可以尝试访问休眠镜像 410 并且将其加载到 RAM 132 中。但是在能够实现这一点之前，引导加载器 434 可以首先从 TPM NV RAM 156 获得密钥 430。按照前面描述的方式，已加密休眠镜像 415 可以包括例如针对 TPM NV RAM 156 中的密钥 430 的位置的 NV 索引的参照。于是例如可以在引导加载器 434 尝试从 TPM 150 获取密钥 430 时利用这样的参照。

[0051] 但是由于 TPM 150 对密钥 430 的释放可能已被绑定到一个或更多 PCR 155 的数值，因此 TPM 可以首先把计算设备从休眠中继续执行并且请求密钥 430 时的 PCR 155 的数值与把密钥 430 存储在 TPM NV RAM 156 中时指定的 PCR 的数值进行比较。如果计算设备 100 的状态的一个或更多重大方面与计算设备休眠时相比发生了改变，则密钥 430 的释放所绑定到的一个或更多 PCR 155 的数值将不等效于其在密钥 430 被存储于 TPM NV RAM 156 中时的数值，并且 TPM 150 将不提供密钥。因此，例如当计算设备 100 处于休眠状态时，如果恶意的或者以其他方式未知的或不受信任的计算机可执行指令或其他处理被暗中插入在所述计算设备 100 中或者以其他方式被准备在所述计算设备上执行，则这样的计算机可执行指令或处理的执行或激活将被记录在 TCG 事件日志 490 中，并且将被反映在 PCR 155 的数值中。更具体来说，这样的处理或指令的暗中插入将导致 PCR 155 的数值不同于在休眠之前把密钥 430 存储在 TPM NV RAM 156 中时所述密钥 430 的释放与之绑定的数值，其结果是将导致 TPM 150 拒绝向发出请求的处理（例如引导加载器 434）提供密钥 430。

[0052] 其结果是，已加密休眠镜像 415 将不能被解密，并且计算设备 100 将不能利用暗中插入的新的指令或处理从休眠中继续执行操作。相反，本领域技术人员将认识到，计算设备 100 可以被完全重启，从而去除或者以其他方式抵消任何暗中插入的指令或处理的效果，并且其结果是保护了计算设备 100，更具体来说是确保可能已经例如由操作系统 134 或程序模块 135 加载并利用的敏感信息不会受到危害。

[0053] 下面通过图 5 和 6 的流程图进一步详述前面描述的机制的操作。参照图 5，流程图 500 示出了可以被施行来提供对于敏感信息的安全且不可恢复的删除的一系列示例性步骤，所述敏感信息可能需要诸如例如在更新处理期间被临时存储在存储介质上。流程图 500 中示出的步骤至少部分地也适用于按照把信息不可分离地绑定到计算设备的方式来存储所述信息，并且在存储介质与计算设备在通信方面断开的情况下利用该信息来保护存储在所述存储介质上的其他信息。

[0054] 最初，在步骤 510 中，可以发起对于计算设备的更新或其他改变，其例如可能会影响计算设备的引导处理，或者以其他方式导致计算设备的操作状态的重大改变。随后，在步骤 515 中，可以例如为与整体容量加密机制相关联的密钥生成明文密钥保护符。可以在步骤 520 中把“明文密钥”存储在 TPM 的 NV RAM 中，所述“明文密钥”可以访问在步骤 515 中生成的明文密钥保护符。在步骤 525 中，把指向存储在 TPM 的 NV RAM 中的密钥的指针（诸如例如与所述密钥在 TPM 的 NV RAM 中的存储位置相关联的 NV 索引）与明文密钥保护符存储在一起，以其他方式与之相关联。在步骤 530 中，可以施行与可能对计算设备的状态造成重大影响的更新或其他改变的施行相关联的一个或更多步骤。此外，作为步骤 530 的一部分，可以重新引导或者以其他方式重启计算设备。

[0055] 随后，在步骤 535 中，可以作为解密或者以其他方式访问受保护信息的努力的一部分来访问在步骤 515 中生成的明文密钥保护符，所述受保护信息诸如例如是作为整体容量加密机制的一部分而受到保护的信息。从在步骤 535 中访问的明文密钥保护符，可以在步骤 540 中获得指针（比如 NV 索引），并且利用所述指针来获得密钥，该密钥可以解密或者以其他方式访问由所述明文密钥保护符保护的密钥。如果在步骤 540 中成功获得所述密钥，则可以访问在步骤 535 中获得的明文密钥保护符，并且可以在步骤 545 中利用所得到的密钥来解锁所述容量。

[0056] 如前所示，在步骤 530 中施行的更新或其他改变可能影响了把例如与整体容量加密机制关联的密钥绑定到计算设备的状态的现有机制。因此，在步骤 545 中解锁了由整体容量加密服务保护的容量之后，可以在步骤 550 中可选地生成对应于可以访问已加密容量的密钥的一个或更多新的保护符。此外，可以在步骤 555 中把步骤 515 中生成的明文密钥保护符从其所被存储的存储介质中删除，并且在步骤 560 中可以指示 TPM 从 TPM NV RAM 中删除密钥。正如前面详细描述的那样，即使应当在步骤 555 中已被删除的明文密钥保护符实际上没有被不可复原地去除，根据 TPM 所遵守的规范，在步骤 560 中指示 TPM 从 TPM NV RAM 中删除密钥的指令也可以导致所述密钥被安全且不可复原地删除。本领域技术人员将认识到，在 555 中对于明文密钥保护符的删除和步骤 560 中指示 TPM 从 TPM NV RAM 中删除密钥的指令不需要精确地按照图 5 的流程图 500 的所示顺序发生，而是可以在步骤 545 的容量解锁期间或之后的任何时间发生。随后，在步骤 565 中，有关的处理可以结束。

[0057] 正如前面详细描述的那样，图 5 的流程图 500 中所示的步骤不需要都被执行，比如在把一段关键信息存储在 TPM NV RAM 内以便在其他存储介质被盗或者其他通信分离时保护信息的安全。举例来说，步骤 530 对计算系统的更新或其他改变、在步骤 550 中相应地生成新的保护符以及随后在步骤 555 和 560 中分别从存储介质删除明文密钥保护符并且从 TPM NV RAM 中删除密钥，可以只适用于特定实施例，并且在仅仅尝试在被盗或者存储介质与计算设备的其他通信分离的情况下保护存储介质上的信息时不需要被施行。

[0058] 参照图 6，流程图 600 示出了可以在休眠或其他暂停状态期间施行来保护计算设备的一系列示例性步骤。首先，从流程图 600 中可以看出，在步骤 610 中，用户或其他处理可以发起计算设备的休眠或暂停。随后，在步骤 615 中，根据传统的休眠机制，可以生成例如包括来自计算设备的 RAM 的有关信息的休眠镜像。在步骤 620 中，可以对该休眠镜像进行加密，以便在计算设备处于休眠或其他暂停状态时保护休眠镜像免受访问或修改。在步骤 625 中，可以把与已加密休眠镜像相关联并且可以被利用来对已加密休眠镜像进行解密

的密钥存储在 TPM NV RAM 中。

[0059] 如前所述，在步骤 625 中把密钥提供给 TPM NV RAM 时，可以指示 TPM 除非在发出针对密钥的请求时的 TPM 的 PCR 数值当中的一个或更多个与计算设备在步骤 625 中休眠时相同，否则不要向发出请求的处理释放密钥。一旦在步骤 620 中对休眠镜像进行了加密并且在步骤 625 中把密钥存储在 TPM NV RAM 中，计算设备就可以完成休眠并且在步骤 630 中进入休眠状态。在也由步骤 630 包含的后来的某一时间点，可以指示计算设备继续执行活跃操作。此时正在计算设备上执行的有关处理(比如引导加载器或休眠管理器)可以尝试从 TPM 获得存储在 TPM NV RAM 中的密钥并且利用该密钥来解密并访问在步骤 620 中加密的休眠镜像，从而把计算设备恢复到其紧接在休眠之前正在其中执行的执行情境。

[0060] 在步骤 635 中，TPM 可以参照针对释放密钥所指定的数值来检查一个或更多 PCR 的当前数值。如果在步骤 635 中有关的 PCR 数值等效于针对释放密钥所指定的数值，则所述处理可以进行到步骤 640，并且由 TPM 向发出请求的处理提供密钥。发出请求的处理于是可以在步骤 645 中利用所述密钥来解锁在步骤 615 和 620 中生成的已加密休眠镜像，并且重新建立活跃计算状态。有关的处理可以随后在步骤 660 中结束。

[0061] 但是如果在步骤 635 中有关的 PCR 数值不等效于针对释放密钥所指定的数值，则所述处理可以进行到步骤 650，此时 TPM 可以拒绝向发出请求的处理提供密钥。在这种情况下，由于无法对已加密休眠镜像进行解密，因此计算设备将不能继续执行活跃处理，并且可以在步骤 655 中施行完全重启或者以其他方式将其自身关机并且在某一后续时间点施行引导处理。因此，如果在计算设备处于休眠状态时计算设备的状态已经发生了重大改变，诸如例如如果恶意的或者以其他方式未知的计算机可执行指令或者对于计算设备的其他改变被暗中插入，或者被设置成在恢复执行活跃处理时执行，则 TPM 可以例如在步骤 650 中拒绝提供密钥，并且通过在步骤 655 中施行完全重启或重新引导规程可以擦除或者以其他方式抵消在计算设备处于休眠状态时对所述计算设备暗中施行的任何改变。有关的处理随后可以在步骤 660 中结束。

[0062] 从前面的描述中可以看出，给出了用于通过利用 TPM 的存储能力安全地存储并且不可复原地擦除敏感信息的机制。鉴于这里所描述的主题内容的许多可能变型，可能落在所附权利要求书及其等效表述的范围内的所有这样的实施例都应当作为本发明而被要求保护。

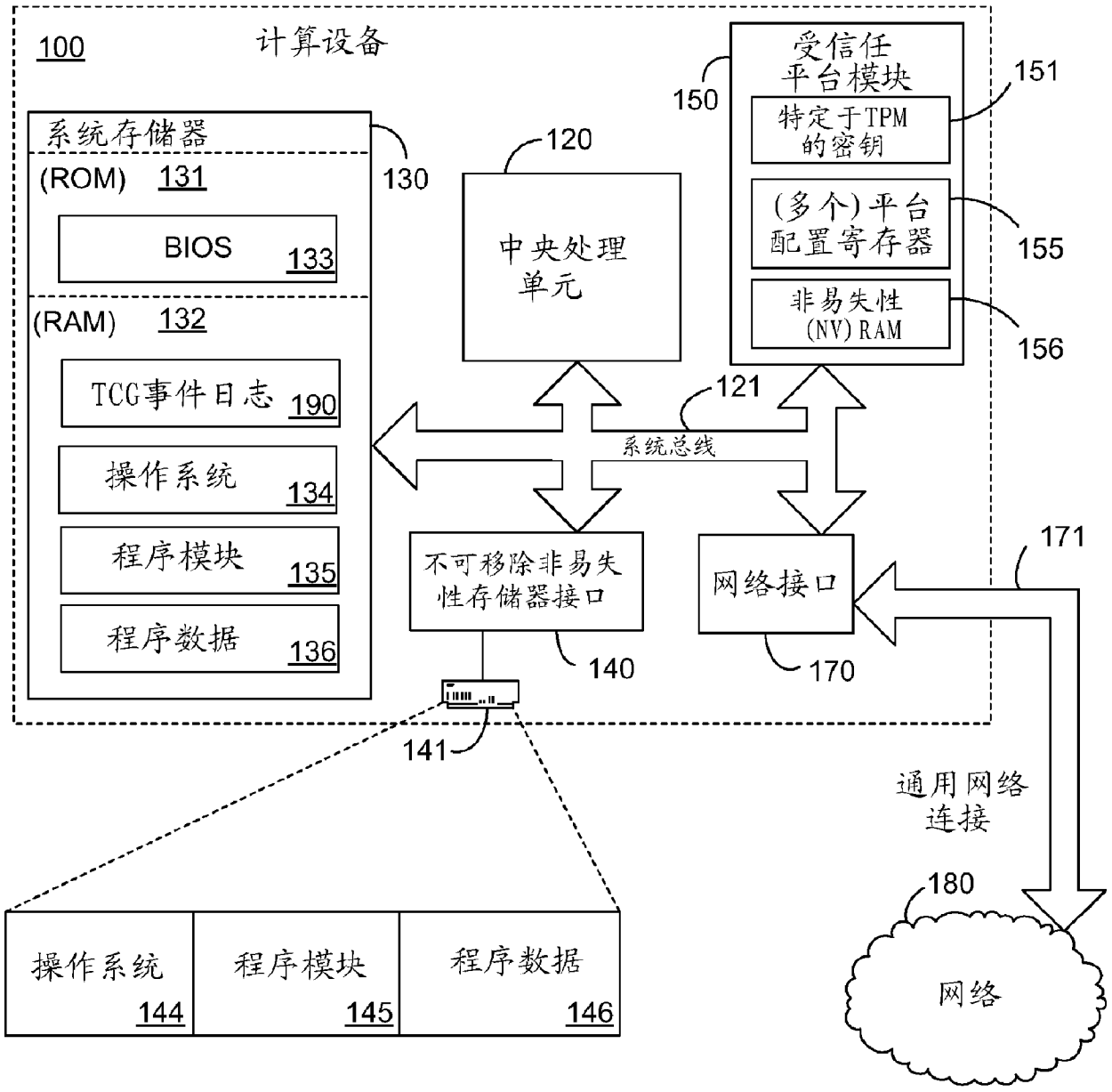

100
计算设备
系统存储器
(ROM) 131
BIOS 133
(RAM) 132
TCG事件日志 190
操作系统 134
程序模块 135
程序数据 136
130
120
中央处理单元
受信任平台模块
150
151
特定于TPM的密钥
(多个)平台配置寄存器
155
非易失性(NV) RAM
156
121
系统总线
不可移除非易失性存储器接口
140
网络接口
170
171
141
通用网络连接
180
网络
操作系统 144
程序模块 145
程序数据 146

图 1

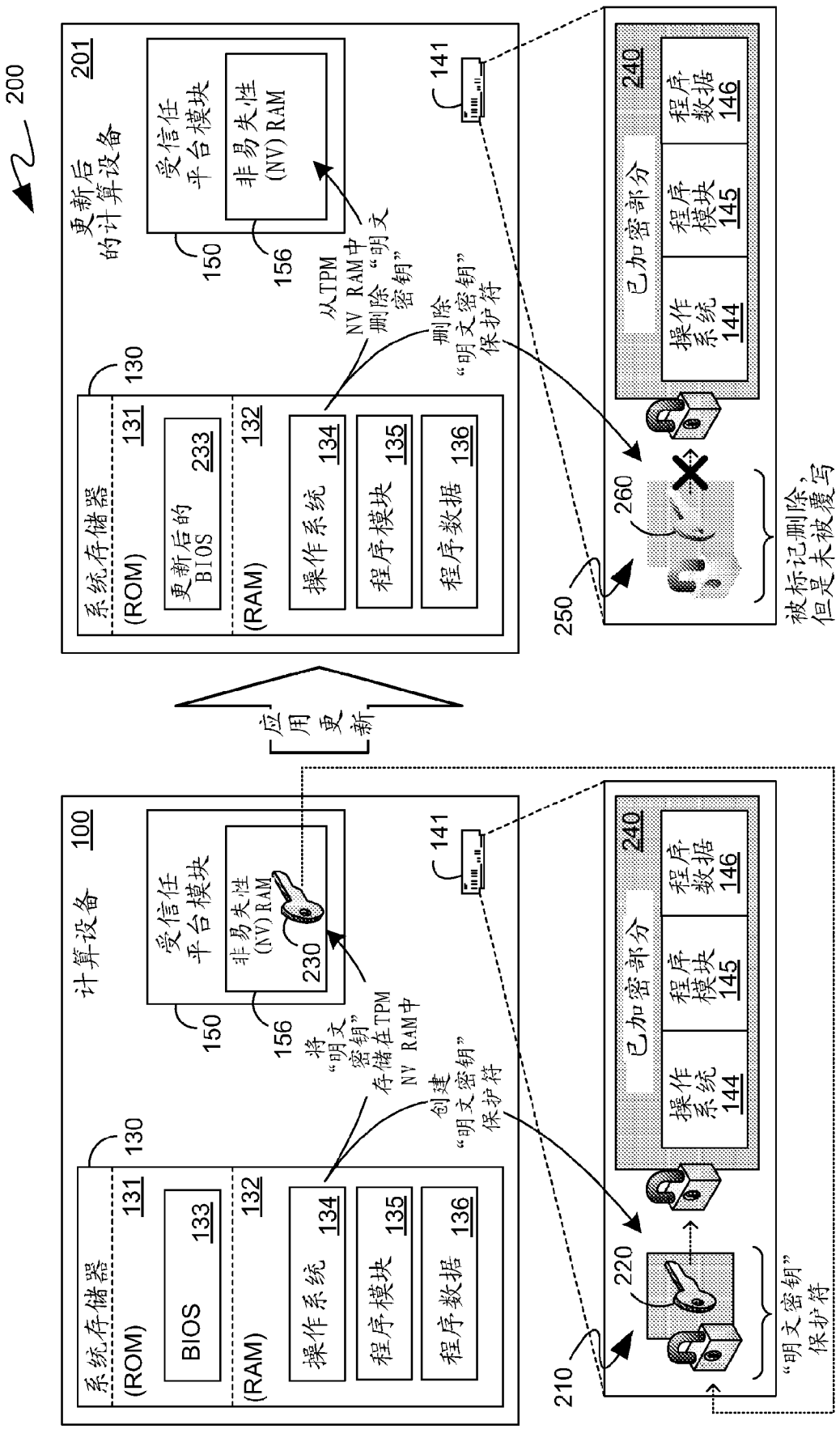

200
201
更新后的计算设备
系统存储器
(ROM)
131
更新后的BIOS
233
(RAM)
132
操作系统
134
程序模块
135
程序数据
136
130
受信任平台模块
150
非易失性(NV) RAM
156
141
从TPM NV RAM中删除“明文密钥”
删除“明文密钥”保护符
已加密部分
240
操作系统
144
程序模块
145
程序数据
146
250
260
被标记删除，但是未被覆写
应用更新
100
计算设备
BIOS
133
230
将“明文密钥”存储在TPM NV RAM中
创建“明文密钥”保护符
210
220
“明文密钥”保护符

图 2

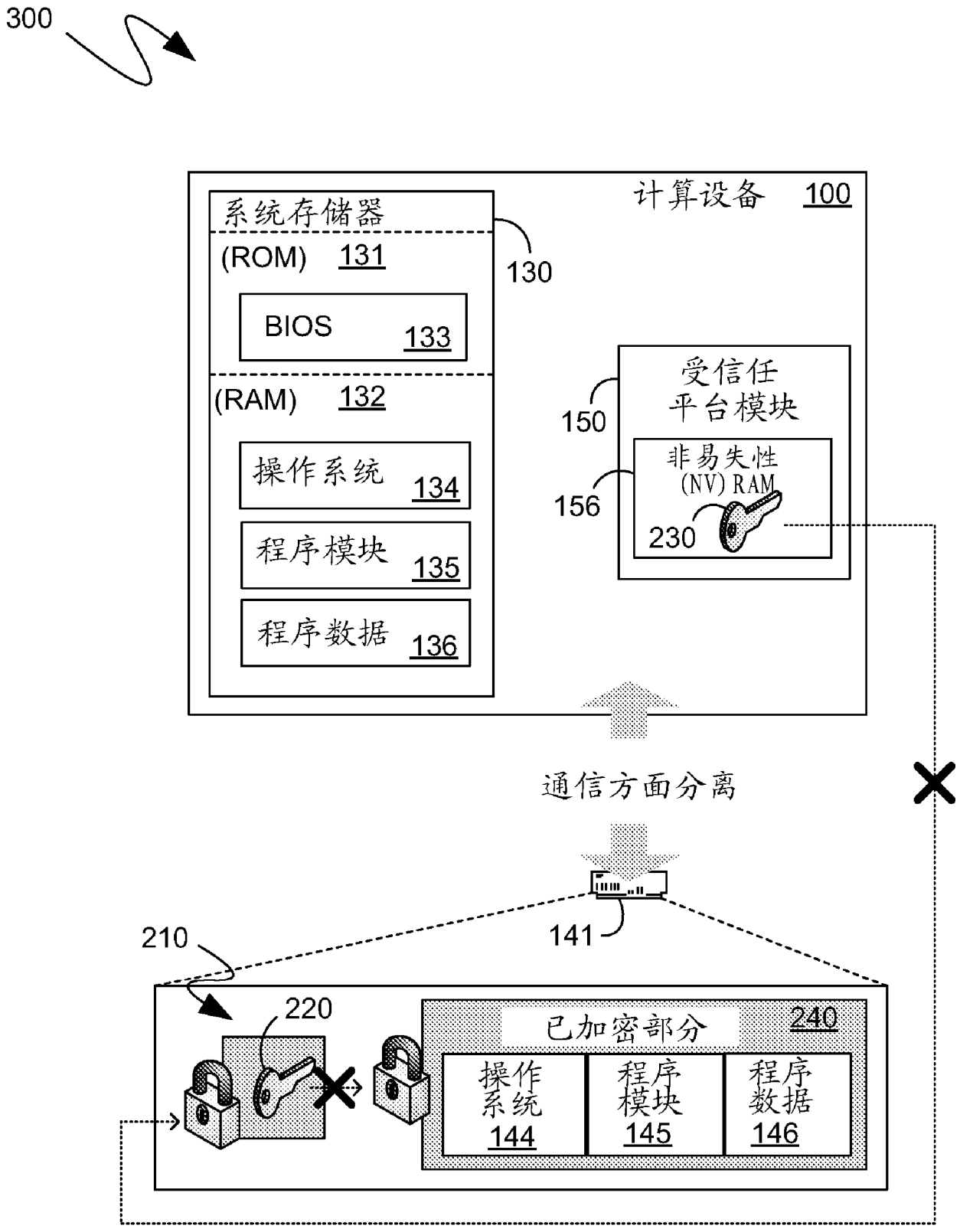

300
计算设备 100
系统存储器
(ROM) 131
130
BIOS 133
(RAM) 132
操作系统 134
程序模块 135
程序数据 136
受信任
平台模块
150
非易失性
(NV) RAM
156
230
通信方面分离
141
210
220
已加密部分
240
操作
系统
144
程序
模块
145
程序
数据
146

图 3

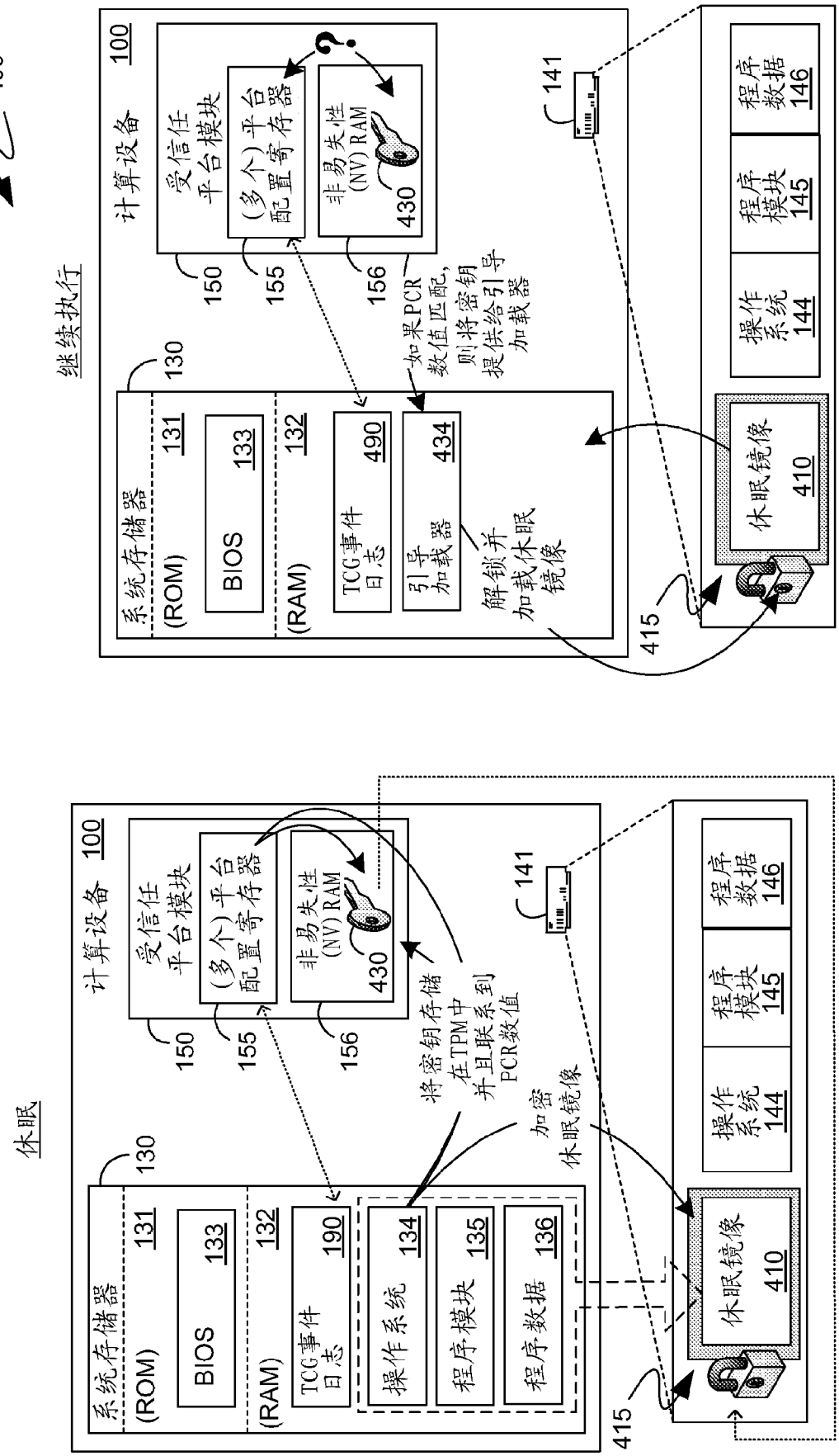

400
休眠
计算设备 100
系统存储器 130
(ROM) 131
BIOS 133
(RAM) 132
TCG事件日志 190
操作系统 134
程序模块 135
程序数据 136
受信任平台模块 150
(多个)平台配置寄存器 155
非易失性(NV)RAM 156
430
将密钥存储在TPM中并且联系到PCR数值
加密休眠镜像
141
415
休眠镜像 410
操作系统 144
程序模块 145
程序数据 146
继续执行
TCG事件日志 490
引导加载器 434
如果PCR数值匹配，则将密钥提供给引导加载器
解锁并加载休眠镜像

图 4

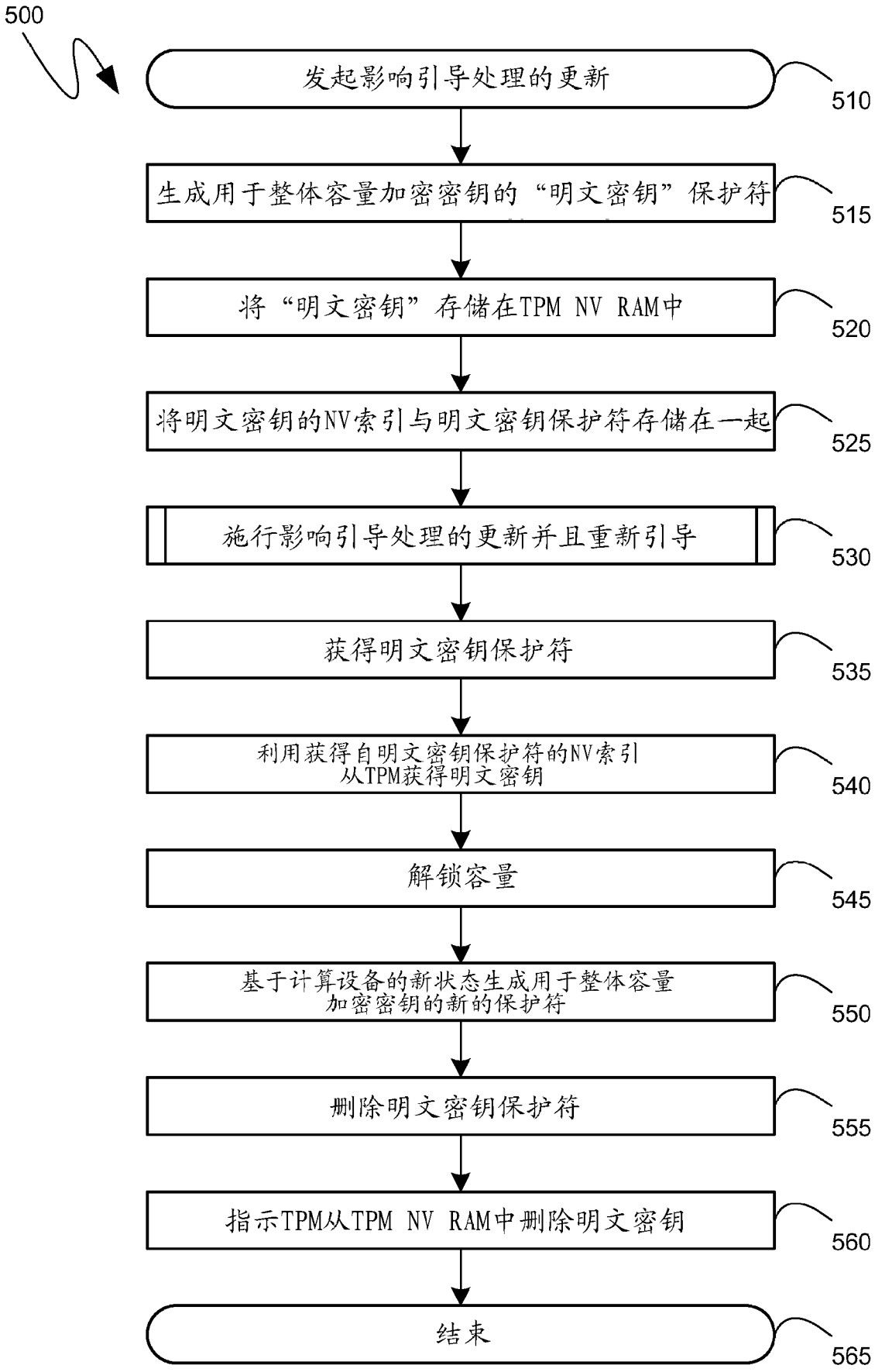

500
发起影响引导处理的更新
510
生成用于整体容量加密密钥的“明文密钥”保护符
515
将“明文密钥”存储在TPM NV RAM中
520
将明文密钥的NV索引与明文密钥保护符存储在一起
525
施行影响引导处理的更新并且重新引导
530
获得明文密钥保护符
535
利用获得自明文密钥保护符的NV索引
从TPM获得明文密钥
540
解锁容量
545
基于计算设备的新状态生成用于整体容量
加密密钥的新的保护符
550
删除明文密钥保护符
555
指示TPM从TPM NV RAM中删除明文密钥
560
结束
565

图 5

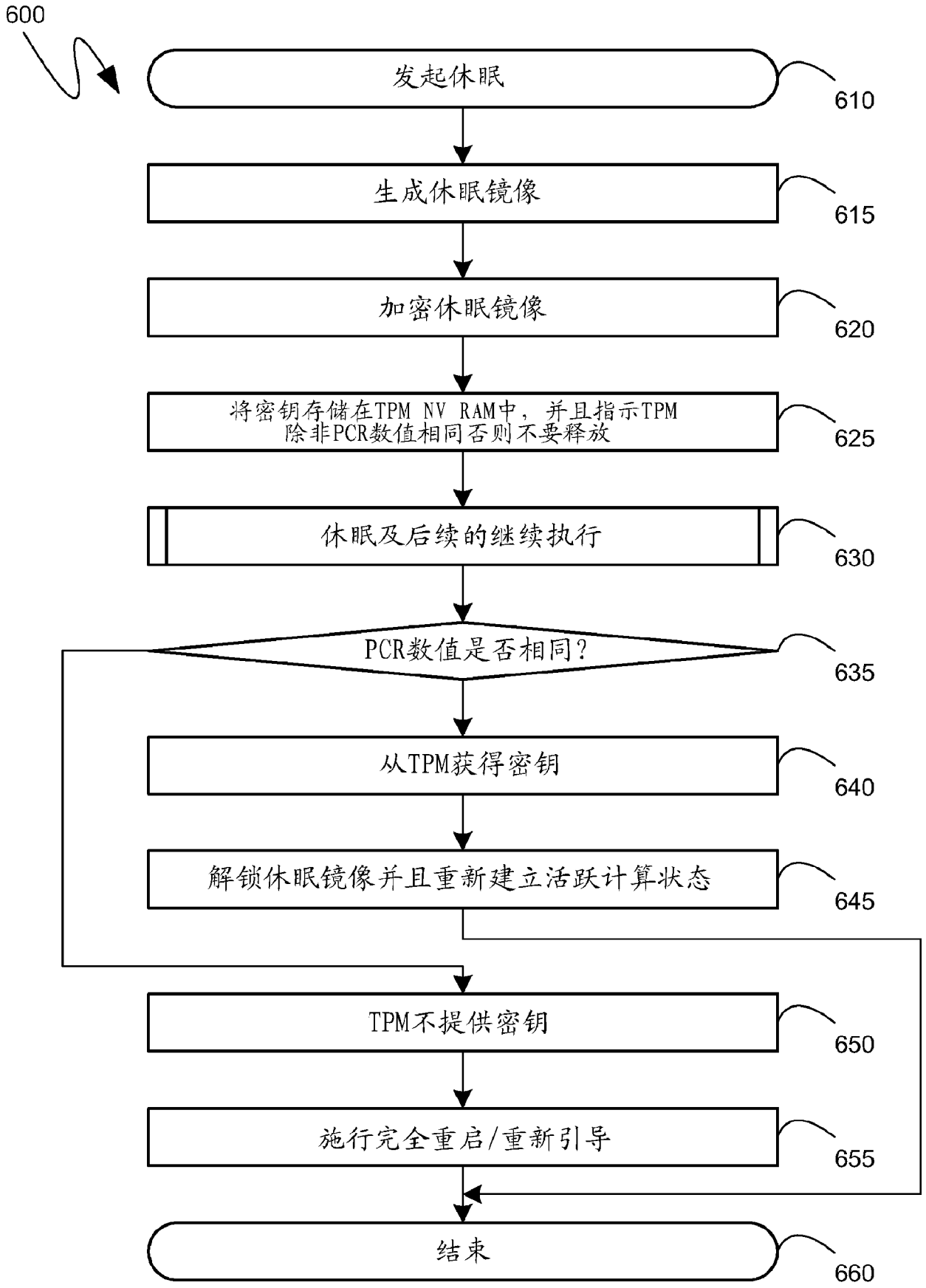

600
发起休眠
610
生成休眠镜像
615
加密休眠镜像
620
将密钥存储在TPM NV RAM中，并且指示TPM
除非PCR数值相同否则不要释放
625
休眠及后续的继续执行
630
PCR数值是否相同？
635
从TPM获得密钥
640
解锁休眠镜像并且重新建立活跃计算状态
645
TPM不提供密钥
650
施行完全重启/重新引导
655
结束
660

图 6