



(12) 发明专利

(10) 授权公告号 CN 101965570 B

(45) 授权公告日 2013. 09. 18

(21) 申请号 200980106728. X

(22) 申请日 2009. 02. 27

(30) 优先权数据

102008011925. 3 2008. 02. 29 DE

12/186, 821 2008. 08. 06 US

(85) PCT申请进入国家阶段日

2010. 08. 27

(86) PCT申请的申请数据

PCT/US2009/001289 2009. 02. 27

(87) PCT申请的公布数据

W02009/108371 EN 2009. 09. 03

(73) 专利权人 格罗方德半导体公司

地址 开曼群岛大开曼岛

(72) 发明人 R·芬代斯 M·格雷尔 T·E·铂利

M·E·约内斯 F·许克

(74) 专利代理机构 北京戈程知识产权代理有限公司 11314

代理人 程伟 胡冰

(51) Int. Cl.

G06F 21/57(2013. 01)

G06F 21/72(2013. 01)

(56) 对比文件

EP 1659472 A1, 2006. 05. 24, 全文.

CN 1822013 A, 2006. 08. 23, 全文.

CN 1900939 A, 2007. 01. 24,

审查员 马毓昭

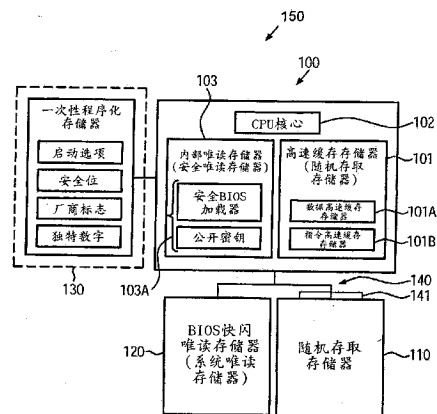
权利要求书2页 说明书10页 附图5页

(54) 发明名称

具有安全启动机制的计算机系统

(57) 摘要

本发明提供一种安全启动处理,可基于属于中央处理单元(100)之不可或缺部分的非易失性存储器(103)而达成,且一旦于预启动信息被程序化于非易失性存储器(103)中之后,该非易失性存储器即无法任意更改。在重启事件或开机事件的期间,可从该内部非易失性存储器(103)开始执行,其中该内部非易失性存储器可包含公开解密密钥(public decryption key),作为验证启动程序片段的签名之用。启动程序之个别片段的验证,可通过使用内部随机存取存储器(101)而完成,藉此避免在验证启动程序期间发生外部存取的情形。因此本发明可得到高度抗篡改性,举例而言,对于通过交换基本输出入系统(BIOS)芯片而进行的BIOS修改具备高度抗篡改性。



CN 101965570 B

1. 一种启动计算机系统的方法,包括以下执行步骤:

存取储存在中央处理单元的非易失性存储器区内的第一组数据,该第一组数据包含第一指令,该第一指令使得该中央处理单元的核心电路初始化该中央处理单元的随机存取存储器并且通过利用包含在该第一组数据中的解密密钥来验证该第一指令的至少第一部分的完整性;

执行该第一指令的第二部分来验证该第一指令的该至少第一部分的该完整性;

响应验证该第一指令的该第一部分的该完整性而从非易失性存储器将第二组数据的镜像加载至该经初始化的随机存取存储器,该第二组数据包括用以验证该第二组数据的完整性的签名,该第二组数据还包括第二指令,该第二指令使得该中央处理单元初始化该计算机系统的系统存储器;

利用该签名及包含在该第一组数据中的该解密密钥来验证该第二组数据的该完整性;以及

于成功验证该第二组数据时,利用该第二指令初始化该系统存储器。

2. 如权利要求 1 所述的方法,还包括:

从该非易失性存储器区执行该第一指令的该第二部分来验证该第一指令的该第一部分的该完整性。

3. 如权利要求 1 所述的方法,还包括:

从该非易失性存储器区执行该第一指令的该第一部分来初始化该随机存取存储器;

将该第一组数据的散列值复制至该经初始化的随机存取存储器;以及

利用复制至该经初始化的随机存取存储器的该第一组数据的该散列值,执行该第一指令的该第一部份来验证该第一指令的该第一部分的该完整性。

4. 如权利要求 1 所述的方法,还包括:

从该非易失性存储器将第三组数据加载至该系统存储器,并且验证该第三组数据的完整性;以及

执行包含于该第三组数据中的第三指令,该第三指令使得操作系统从连接至该计算机系统的可启动装置加载至该系统存储器。

5. 如权利要求 4 所述的方法,其中,验证该第三组数据的完整性包括判定该第三组数据的散列值,并且将该判定的散列值与包含于该第二组数据中的该第三组数据的初始散列值相比较。

6. 如权利要求 1 所述的方法,其中,初始化该随机存取存储器包括初始化该中央处理单元的数据高速缓存及指令高速缓存,且其中,该第二组数据加载至该数据高速缓存中,且该方法还包括于已经成功验证该第二组数据的完整性时将该第二组数据复制至该指令高速缓存,以执行该第二指令。

7. 如权利要求 1 所述的方法,其中,加载该第二组数据至该随机存取存储器包括执行散列算法以判定该第二组数据的散列值,且验证该第二组数据的完整性包括将该第二组数据的该散列值与通过应用加密密钥至该签名所取得的初始散列值相比较。

8. 如权利要求 1 所述的方法,其中,该第一组数据是每当该中央处理单元重启或开机时被存取。

9. 如权利要求 1 所述的方法,还包括重映像该第一组数据的地址于该中央处理单元的

虚拟地址空间中,以使成功验证该第二组数据后得以从外部存取至少该解密密钥。

10. 如权利要求 1 所述的方法,还包括提供至少该第二组数据的验证状态的状态信息。

11. 如权利要求 4 所述的方法,还包括复制该第一组数据至该系统存储器。

12. 如权利要求 1 所述的方法,其中,该第一组数据包括预启动指令及数据值,用以初始化该中央处理单元的该随机存取存储器,且该第二组数据包括启动指令及启动数据值。

具有安全启动机制的计算机系统

技术领域

[0001] 本发明系关于加强完整性的计算机系统及于其中执行之相关机制；本发明可提升安全标准，进而增进需要安全性计算机平台的应用程序之效能。

背景技术

[0002] 随着计算机系统的普及，于电子计算系统上进行之信息处理量亦显著增加，进而导致大量数字数据的产生、分配与处理。以数据储存容量与增加之处理速度的角度而言，可用之计算机系统资源变大，随此，越来越多的人能够进行声音数据、电影等大型数据组的复制 (reproduction)，且此等复制系经常地被实施而无视于与以电子形式提供之许多数据结合的保护权利。因此，电子数据之非法复制、储存及重新分配，会造成重大的经济损失。再者，应用程序系于诸如因特网 (internet) 之分布广泛的网络四处散播，此将制造散布恶意软件应用程序的机会，其可随后被用于篡改个别计算机平台之数据及 / 或组构。举例而言，由于导入不当的软件应用程序，使得例如储存档案被篡改、信息在实际使用者不知情的情形下经由因特网传播、启动阻绝服务攻击从而导致需要在特殊状态之平台上执行的专属应用程序无法使用该平台，因而可能对私人环境、特别是对产业造成严重伤害。

[0003] 基于上述原因，已投入相当大的努力在发展各种机制以加强计算机平台之完整性，以降低例如恶意软件形式、阻绝服务攻击、测录 (sniffing)、电子诈欺 (spoofing) 等「成功的」外部攻击，并同时增加计算机平台内部调处 (internal manipulation) 所相关的数据完整性。举例而言，已有多种加密技术可运用，例如对称型 / 非对称型之加密 / 解密技术，其可能使数据交换过程中具有高度的抗篡改性，防止第三方在传输或储存数据时篡改数据。举例而言，以非对称型加密技术来说，一对私密密钥和公开密钥系可用来以其中一密钥来加密数据，并使用另一密钥来解密数据，且其中一密钥为可公开存取。虽然此技术能够在数据交流及数据储存方面，提供较佳的完整性，但所考虑之计算机平台之实际组构仍可能遭受复数种攻击，特别是因为许多意欲提升计算机安全性的应用程序系依赖于可信赖平台组构 (trusted platform configuration) 之故。

[0004] 可信赖平台组构可视为一计算机系统，其中的硬件组构硬件组构与软件应用程序皆被假定为处于专属组构的状态。然而安全性平台组构可能仅通过一连串可信任平台阶层的建立而建立，其中，只有当后续阶层的完整性经过验证，才能由前一阶层来启动各后续阶层。如此一来，于系统阶层的完整性可透过以一连串之完整性验证步骤维持，而这些一连串验证步骤的基础必须具备高度抗篡改性，使得最高阶层（例如使用者应用程序）被初始化后，仍能高度信赖系统的完整性。

[0005] 在典型的计算机平台中，系统初始化需要不同程度的「提取」(abstraction) 处理，如关于中央处理单元 (central processing unit ;CPU) 的初始化，系统存储器的初始化（其通常设置于中央处理单元外部），从外部的大量数据储存装置将操作系统加载系统存储器中，最后再执行使用者应用程序。由加强系统整体的完整性而言，要假定加载操作系统之前的各种系统活动皆具有安全性而可依赖操作系统及使用者应用程序之完整性，可能

有所不足之处,这是因为操作系统可能是由「不可信赖」的程序所引动,进而提供通过更改硬件或软件组件而篡改基础平台组构的机会。因此,计算机系统之各种硬件组件(如系统存储器)的初始化程序以及包含于其中之用以启动较高系统阶层之指令的执行(其可被称为启动 (boot strapping 或 booting),皆必须并入一连串「可信赖」的环节中,方可提升系统整体的完整性。

[0006] 在施加电源后或重启事件后用以初始化计算机系统之典型的第步骤为使中央处理单元执行「开机自我测试」(power on self-test),于此过程中处理器亦于专属进入地址 (dedicated entry address) 开始执行指令,其中该地址系由处理器之重启向量所指示。换句话说,于初始处理器自我测试 (initial processor self-test) 之后,指令所开始执行的进入地址通常为常被称为基本输出系统 (BIOS) 之软件程序的地址,而该 BIOS 可储存于计算机平台之专属外部非易失性存储器。在 BIOS 控制之下,可进行其余的自我测试步骤,且可判定或「测量」平台的硬件组构。接着,将搜寻如大量数据储存装置等可启动装置(举例而言,计算机系统之硬盘、磁盘、光盘及扩充卡等),并从该可启动装置将主要启动区块 (primary boot block) 加载系统存储器中,同时转移控制至主要启动区块,而该主要启动区块可加载操作系统于系统存储器。

[0007] 尽管在提升整个启动过程的安全性方面亦已投入相当大的努力,然而针对启动程度提供可靠之可信赖测量之核根 (core root of trust for measurement ;CRTM) 仍面临困难。举例而言,以平台改变 (platform modifications ;例如更换包含 BIOS 软件之非易失性存储器芯片) 来说,由于相关的芯片更换可能会因此中断信任链 (chain of trust),因此可能使所有之后续验证步骤成为不可信赖。

[0008] 本发明揭露的方法及装置,可避免或至少可减少上述习知技术衍生的问题。

发明内容

[0009] 以下之具体实施例,仅系用以例释本发明之特点及功效,而非用以限定本发明之可实施范畴,在未脱离本发明上揭之精神与技术范畴下,任何运用本发明所揭示内容而完成之等效改变及修饰,均仍应为下述之申请专利范围所涵盖。

[0010] 大致上,本发明系关于加强完整性的计算机系统及其执行之相关机制,通过建立信赖测量的静态根 (static root of trust for measurement) 达成,其中可提供特定数据组,该数据组包含可执行指令及数据值,此指令及数据值由微处理器于开机时存取,并确保任何情况下皆可避免专属数据组被入侵的可能性,因此可获得平台启动用的定义根 (defined root);另外,执行该数据组的方式可达到高度抗篡改性。于包含在该数据组中的指令之执行过程中,不能改变或中断相关的程序,藉此可提供该组数据之高度完整性,因此其可被考虑为预启动指令及数据值。由于预启动数据之个别指令的处理于该系统开机时为强制者,故可开始一连串可信赖软件,从而得以建立高度的系统完整性,这是因为专属预启动数据组即表示用于后续验证步骤之静态根。为此目的,该预启动数据组可保存在该中央处理单元核心的非易失性存储器中,以实质避免更换 BIOS 芯片等时的攻击行为。

[0011] 本发明之一实施例系关于计算机系统之开启方法,包括:存取储存在中央处理单元 (CPU) 的非易失性存储器内的第一组数据,该第一组数据包含第一指令,该第一指令使得该中央处理单元的核心电路初始化该中央处理单元的随机存取存储器。该方法还包括从

非易失性存储器将第二组数据的镜像 (image) 加载至该经初始化的随机存取存储器, 该第二组数据包括用以验证该第二组数据的完整性的签名, 该第二组数据还包括第二指令, 该第二指令使得该中央处理单元初始化该计算机系统的系统存储器。此外, 该方法包括通过利用该签名及包含在第一组数据中的解密密钥而验证该第二组数据的该完整性。最后, 该方法包括于已经成功验证该第二组数据时, 利用该第二指令初始化该系统存储器。

[0012] 本发明之另一实施例系关于计算机系统之开启方法, 包括: 于开机及重启事件之其中至少一者后, 存取中央处理单元的内部非易失性存储器, 该非易失性存储器包含预启动指令及数据值, 用以初始化该中央处理单元的内部易失性存储器并验证储存于非易失性存储器之启动指令及启动数据值的至少一部分之完整性。该方法还包括通过执行该预启动指令将该启动指令及启动数据值的至少一部分从该非易失性存储器加载至该内部易失性存储器中。此外, 通过执行该预启动指令验证该启动指令及启动数据值的至少一部分之完整性。最后, 于成功验证该启动指令及启动数据值的至少一部分之完整性后, 执行该启动指令。

[0013] 本发明亦揭露一中央处理单元包括: 基板, 具有形成于其上的电路组件, 该电路组件定义中央处理单元核心、易失性随机存取存储器、非易失性存储器及总线系统, 其中该总线系统用以连接该中央处理单元核心、该易失性随机存取存储器及该非易失性存储器。此外, 该中央处理单元包括储存于该非易失性存储器的预启动信息, 该预启动信息包含用以初始化该易失性随机存取存储器与验证启动程序的至少一部分而可被该中央处理单元核心执行的指令、以及数据值。

[0014] 本发明进一步揭露一面向, 上述中央处理单元可为计算机系统的一部分, 该计算机系统除中央处理单元之外, 还包括系统存储器、包含启动程序之记忆装置、以及将该系统存储器及包含该启动程序之记忆装置与该中央处理单元予以连接之接口系统。

附图说明

[0015] 本发明所揭露之内容可通过以下图标简单说明配合图标加以了解; 各图标组件符号代表不同组件:

[0016] 图 1a 为根据本发明实施例之中央处理单元的示意图, 其中包含随机存取存储器 (高速缓存)、中央处理单元核心以及包含预启动信息的非易失性存储器;

[0017] 图 1b 为根据本发明实施例具有中央处理单元之计算机系统的示意图, 该中央处理单元包含内部预启动信息;

[0018] 图 1c 为根据本发明实施例之用以在制造启动信息第一部分的签名之程序期间操控启动数据步骤的示意图, 该启动程序数据包含指令及数据值;

[0019] 图 1d 为根据本发明实施例验证该启动信息一部分的签名步骤之示意图;

[0020] 图 1e 为根据本发明实施例之流程图, 描述图 1b 的计算机系统之运作; 以及

[0021] 图 1f 为根据本发明实施例之流程图, 描述包含中央处理单元的计算机系统之运作, 该中央处理单元可为图 1a 的中央处理单元。

[0022] 虽然本发明可容许各种修饰及替代形式, 但在此已经由附图中之范例显示并描述特定之实施例。然而, 应了解的是, 本发明并非意欲限制至所揭露之特定形式。相反地, 本发明系意欲涵盖落在由所附申请专利范围所界定之精神与范畴内之所有修饰、等效及替代

者。

具体实施方式

[0023] 以下将描述多个例举实施例。为了清楚起见,并未将实际实施之所有特征皆描述于本说明书中。吾人将当然体会到,于任何此种实际实施例的研发中,必须做出许多特定之实施决定以达到研发人员之特定目标,例如遵从与系统相关或与商业相关之限制条件,该限制条件随着实施之不同而有所变化。此外,吾人将体会到此种研发之投入非常复杂且耗时,但对于在所属技术领域中具有通常知识而可由本发明所揭露之内容得益者而言,其仅属于惯常程序。

[0024] 本发明之内容将参照附图进行描述。该等图标中之多个结构、系统及装置仅为了说明起见而示意地描绘,以免因所属技术领域人员所熟知之细节而模糊本发明之内容。但是,该等附图系被包含以描述并说明本发明内容之说明范例。下文中所用之用字和措辞应被了解及理解为与熟习相关技术领域之人士对于该些字辞的了解具有一致之意义。下文中该等名词或措辞之一致性用法并不会想意者名词或措辞之特别定义(亦即与熟习相关技术领域之人士所了解之通常和惯用意义不同之定义)。欲具有特别意义如特别定义之名词或措辞,也就是不同于熟习此技艺之人士所理解之意义(如特殊定义),将于本说明书中以定义方式特别提出以直接且明确地提供该等名词或措辞之特殊定义。

[0025] 大致而言,本发明揭露一种系统及机制,该系统及机制于开机(start up)、重启或其它需要初始化系统之运作状态下,执行储存于非易失性存储器之指令及利用储存于非易失性存储器之数据,其中该非易失性存储器代表中央处理单元之一部分。藉此,可显著降低非易失性存储器中的数据组遭到篡改之可能性。因而,可确保在开机或CPU的重启后第一个指令系自非易失性存储器所提取,藉此在初始化中央处理单元与整体计算机系统的期间,非易失性存储器之内容可做为信赖测量的静态根(static root of trust for measurement)。因此,包含于其中之数据组可作为预启动或预BIOS组件,其可初始化诸如内部随机存取存储器等进一步的系统组件,而这些系统组件可作为储存用以执行部分BIOS软件的例如变量、堆栈(stack)或指令等运作数据之用。举例而言,属于随机存取存储器区域之一部份的数据高速缓存、以及指令高速缓存,可藉内部非易失性存储器之预启动数据初始化,以有效避免包含于其中之数据于初始化过程中由外部存取的可能性。也就是说,该随机存取存储器区域(即该数据高速缓存与该指令高速缓存)为中央处理单元内部组件,因此极难发生不想要之数据篡改,尤其是此时外部系统存储器尚未初始化。取决于随机存取存储器的储存容量,BIOS程序可被分割为两个部分以上,以便可针对该第一部分(其大小系经设计为符合指令高速缓存之容量)于随机存取存储器中执行一或多个签名的验证,以确定BIOS之完整性。如此,在完整性的验证完成后,此部份之启动信息可直接从随机存取存储器执行。因此,在通过执行预启动指令而使随机存取存储器初始化及加载部分启动信息之期间,预启动信息即无法由外部存取,藉此可实质避免对第一签名验证程序进行任何数据篡改的情形。在一些示范性实施例中,预启动信息在签名验证后可由外部应用程序存取,例如存取解密密钥,以评估BIOS升级版本等之完整性。

[0026] 因此,在启动信息第一部分的签名验证完成后,流程控制可交由该第一部分,使接下来的启动处理得以继续,其步骤包括:初始化系统存储器、复制其余之启动信息,同时验

证该启动信息其它部份的完整性。因此,储存于非易失性存储器(其系设置成中央处理单元之必要部分)中之该数据(即指令及数据值)可使用作为信赖测量的静态根,藉此提供一计算机平台,于其中可达成具有抗篡改性之硬件与软件组构。特别是,在考虑到诸如更换 BIOS 芯片等攻击时,于此所述之实施例之机制可针对依据可信赖计算机平台而以金融交易或数字权限管理为主体使用平台之一般应用程序提供加强之安全性。

[0027] 图 1a 示意性地显示根据本发明之实施例之中央处理单元(CPU)100,其中可信赖测量之核根(CRTM)以高度抗篡改性的方式实施。中央处理单元 100 可包括具有用于数据处理之组件之中央处理单元核心 102,该数据处理例如为实行算术运算或逻辑运算等。该中央处理单元核心 102 系功能性地连接于随机存取存储器 101,该随机存取存储器 101 可包括复数个静态随机存取存储器单元或其它类似单元,其与中央处理单元 100 的整体组构兼容。于一示范性实施例中,该随机存取存储器 101 可包括第一记忆区(亦表示为数据高速缓存 101A)以及第二记忆区(亦表示为指令高速缓存 101B)。例如,该随机存取存储器 101 可利用快速存储器技术来实施以增加中央处理单元 100 之整体效能,此技术在复杂集成电路中通常为必要者。然而应当了解的是,任何适当的存储器技术皆可应用于存储器 101,只要在初始化中央处理单元 100 之期间可透过中央处理单元核心 102 达成存储器 101 之直接控制,而无外部存取的可能性即可。

[0028] 另外,该中央处理单元 100 可包含非易失性存储器 103,其可利用适当之存储器技术(例如以闪存之形式或其它只读存储器技术等)来设置;这些技术可避免外部存取造成之存储器 103 内容之更改。如此一来,存储器 103 可视为一安全的存储器区域,其内容可因此代表可信赖的静态根。为此目的,本发明系至少于存储器 103 的一部分之中提供数据组 103A,该数据组 103A 将被理解为可被中央处理单元核心 102 执行之指令以及代表该指令之操作数或类似数据的数据值数据组,并且,于一旦程序化存储器 103 的各个部分后,该数据组 103A 不会被新数据覆写。包含该数据组 103A 的存储器 103 可透过总线系统 104 与该中央处理单元核心 102 相连接,俾使于开机或重启后,可跳越至存储器 103 的特定地址。藉此可提供用于中央处理单元核心 102 之重启向量的硬连接(hard-wired)目标,以确保至少在开机事件或重启事件时,指令系由具备安全性之存储器 103 开始执行。

[0029] 应当了解的是,该中央处理单元 100 可基于精密半导体制程技术形成,其中可于半导体基材等适合的载体材料中,容置基于 CMOS 制程等相关技术形成的复数个电路组件,其中可根据中央处理单元 100 之特定装置架构来形成晶体管、电容器、电阻器等组件。于本实施例中,可因而在共通制造流程中在共通基板上形成中央处理单元 100 的各种组件,以提供存储器 101 及 103 作为装置 100 之内部或构成整体所必要的构件。例如,能够与中央处理单元核心 102 所需之非易失性存储器单元及高效能逻辑闸一起形成易失性及快速存储器单元的各个制程技术目前已相当成熟。此外,可提供适当的机制以避免在程序化存储器 103 或至少其一部分(包括数据组 103A)后,数据位被进一步之存取更改,而可提供该数据组 103A 一个受到保护的环境。

[0030] 图 1b 系为包含如上述可提供数据组 103A 一个受到保护的环境之中央处理单元 100 的计算机系统 150,其中,于所示之实施例中,该中央处理单元 100 可包括随机存取存储器 101,而该随机存取存储器 101 可为数据高速缓存 101A 及指令高速缓存 101B 之形式,其大小(例如 64kB)可容纳启动信息的一部分,并当实行数据组 103A 的指令时,担任「系统随机

存取存储器」之角色。同样地,该指令高速缓存 101B 可具有 64kB 之大小,惟应了解任何其它适当之存储器大小皆适用,只要其兼容于验证过程中将由存储器 101 执行之启动信息之个别部份的大小即可。类似地,内部非易失性存储器 103 可具有任何适当大小,例如 32kB,以兼容于代表计算机系统 150 可信赖测量之核根的数据组 103A 之需求。举例而言,数据组 103A 可包括代表一安全加载程序的指令及数据值,其中该安全加载程序系用于加载启动信息个别部分于内部存储器 101 中以执行验证程序。此外,该数据组 103A 可包括一或多个解密密钥,其可代表非对称型加密/解密算法的公开密钥,以在存储器 101 中验证启动信息之经签名的部分。应理解的是,数据组 103A 之公开密钥的数目可依照安全考虑而选择,例如考虑到维持用以提供各密钥配对之适当架构具备高度完整性等。

[0031] 计算机系统 150 可进一步包含系统存储器 110,该系统存储器可例如为包含随机存取存储器单元(例如动态随机存取存储器单元等)之任何适当的存储器装置。系统存储器 110 的大小可调适成符合于考虑到该计算机系统 150 之效能与储存容量的需求。并且,该计算机系统 150 可包含如闪存等之非易失性存储器 120,其可包含亦称为 BIOS 信息的信息,其至少一部分可为签名部分;换句话说,签名部分可包括基于适当的散列算法(hash algorithm)并结合加密机制而获得的签名,并且如上所述,可在该数据组 103A 中包含一个或多个适合的解密密钥。

[0032] 于一示范性实施例中,该非易失性存储器 120 可包括分为两部分的启动信息,其中第一部分可包含用于初始化其它系统组件(例如系统存储器 110)的数据及指令,而该其它系统组件系用以容纳启动信息的第二部分,并于第一部分在该中央处理单元 100 提供的受保护环境被验证后执行该第二部分。关于在非易失性存储器 120 中的启动信息之详细结构将参考图 1c 及图 1d 稍后描述。

[0033] 该计算机系统 150 可另外包含接口系统 140,其系设为将该系统存储器 110、非易失性存储器 120 与该中央处理单元 100 运作性地予以连接。于一示范性实施例中,该系统 150 可进一步包括一次性程序化存储器(one-time programmable memory) 130,其可包括平台特定性信息(platform-specific information),例如关于启动源及相关参数者。举例而言,如图所示,一次性程序化存储器 130 可包含关于启动选项的信息,用以指示中央处理单元 100 自内部存储器 103 启动与否。另外,于该存储器 130 中所提供之安全位可包括用以判定要将重启后该中央处理单元 100 的初始指令提取导向何处的个别位。例如,该位设为“1”时,可将执行转移至内部存储器 103,从而进入安全启动处理之程序。某些情况下,例如为了开发程序或除错,可能需要关闭安全启动功能。其它情形下,可能根据平台需求,需要关闭或略过可信赖平台功能。此时,于安全启动处理期间系不允许该位状态的改变。为此目的,所以除错模式(例如 JTAG……)至少在启动期间将全部被关闭。在关闭个别的除错模式之后,可执行安全启动程序,详细说明如后。同样地,该存储器 130 可包括在安全启动程序期间控制除错功能的位,其中,该除错功能于开发程序期间系有帮助,而在生产时系关闭个别的除错功能控制。除这些安全位之外,该存储器 130 还可包括其它信息,例如厂商标志或可用于数字权利管理应用程序等之任何独特的数字。应理解的是,在其它实施例中,该一次性程序化存储器 130 可被省略,或可于开发程序或实际应用时被提供以包含用以控制该安全启动处理的其它信息。

[0034] 图 1c 系示意性地显示启动信息 121 之结构,且该启动信息 121 可储存于非易失性

存储器 120 中。在图 1c 所显示之实施例中,该启动信息 121 (亦可称为 BIOS) 可包括第一部分 121A,且该第一部分 121A 可表示包含指令及数据值的数据组,其中该指令及数据值的大小如前述系与存储器 101 之大小兼容。举例而言,就上文中所给定之各随机存取存储器区域 101A、101B 为 64kB 之例示大小而言,第一部分 121A 容量的极大值系限制为约 32kB。然而应理解的是,本发明可依据随机存取存储器 101 内可用之储存容量使用任何其它适合大小的第一部分。另外应理解的是,当启动信息 121 大于存储器 101 之容量时,必须提供第一部分 121A,这是因为一般而言启动程序可能占用数十万个位或以上之大小,故启动信息 121 超出存储器 101 之容量时整个启动处理可能无法基于存储器 101 而执行之故。在其它情形,当在储存容量足够时,启动信息 121 整体可于安全启动处理期间使用,详细内容描述于后。

[0035] 如图 1c 所示,若设置有第一部分 121A 时,第一部分 121A 可作为用于第二部分 121B 的初始 BIOS「加载器」,其中该第一部分 121A 可包含经由整个该第二部分 121B 所得到的散列值 (hash value)。用于该第二部分 121B 的散列值亦可由基于经由整个第一部分 121A 所得到的散列值而包含于第一部分 121A 中的签名所保护,且此步骤可在一专属可信中心之中完成。因此该第二部分散列值的加密可为非必要。该第一部分 121A 散列值的签名可用于在安全启动处理期间验证第一部分 121A。因此该第一部分 121A 可设定为实行必要的平台初始化动作,例如存储器控制器的初始化等,并接着将该第二部分 121B 自存储器 120 映照 (shadowing) 至启动系统存储器 110。

[0036] 在执行第一部分 121A 后,散列值可经由复制至系统存储器 110 的整个影像 121B 计算之,且所得的散列值可与最初包含在第一部分 121A 的散列值相互比较。如此,可依据包含在第一部分 121A 的散列值,验证第二部分 121B 的完整性,从而提供完整性的信任炼。因此如图 1c 所示,可通过处理第一部分 121A 获得签名,且此步骤可基于适当的可信环境在适当之信任中心完成。为此,可应用安全散列算法以提供一或多个散列值,例如散列值 0、散列值 1、散列值 2 同时结合适当的控制数据。其后可应用任何适当之加密技术,例如使用合适之私密密钥的 RSA (Rivest, Schamir, Adelman) 算法,以获得如图 1c 右侧字段所示之加密散列值。如前述,合适数目之公开密钥可包含在数据组 103A 中,从而在如图 1c 所示的流程中所产生之已加密的散列值或签名可被解密。

[0037] 图 1d 为验证第一部分 121A 中所包含的签名之流程示意图;此流程可于启动系统 150 之期间依据数据组 103A 实行之。该验证步骤可基于例如使用一公开密钥之 RSA 算法完成,以获得经初始地产生的散列值,如散列值 0、散列值 1、散列值 2。该等经初始地产生的散列值可随后与经由对整个第一部分 121A 施加适当散列算法所得到的个别散列值进行比较,其中,该第一部分 121A 系经复制至随机存取存储器 101。若计算所得的散列值与通过解密第一部分 121A 的签名所得的初始产生的散列值匹配时,则第一部分 121A 可视为通过验证,如图 1d 左侧字段所示。

[0038] 以下将参考图 1e 及图 1f 更详细地说明依据本发明实施例之于安全启动处理期间的系统 150 的运作。如前述,为提供一安全平台,应执行可信的静态根 (static root of trust),以使该计算机系统开机或重启后,操作系统能够安全启动。举例而言,可信之 BIOS 信息 121 之经定义的执行可通过根据可信数据组 103A 而验证至少第一部分 121A 来完成,其中该可信数据组 103A 实质上可抵抗任何外部篡改。因此每次启动该系统时,系

初始化一安全启动程序,其中,通过密码方法,可达初始硬件及软件组构的完整性验证。因此,于通过启动信息 121(即图标的第一部分 121A 与第二部分 121B)之完整性验证后,可确认整体启动程序之完整性,藉此使操作系统能够可信赖地被初始化,进而可被用以实行对安全性敏感(security sensitive)之应用程序。另一方面,一旦无法通过完整性测试时,则例如在验证第一部分 121A 或第二部分 121B 期间,可应用合适的政策(policy)以限定由该系统所提供的服务;或在其它实施例中,实际上关闭启动处理。

[0039] 本发明所揭露之安全启动架构可避免「等级突破」(class break)的发生,所谓等级突破系指会与一给定安全系统之每个情况作对的攻击。举例而言,由外部来源所产生之软件片段可视为一等级突破,此软件片段可轻易安装且容许对安全/保护措施规避(circumvention),进而容许平台之未授权使用。在数字版权管理(DRM)的环境中,当经 DRM 保护之数据文件曾经被突破时,则等级突破可能已经发生,从而容许未受保护之档案的重新散布。本发明所揭露的机制及系统可针对等级突破提高安全性,这是由于可基于中央处理单元本身中之不可或缺的部份而得到受保护环境之故,因此系需要中央处理单元本身之篡改、或用于签署启动信息与维持秘密密钥之架构上的各个缺陷,而在上述两种情形皆需要耗费相当的时间与金钱。

[0040] 图 1e 为示意性地描述该系统 150 运作之流程图。在步骤 S100 中,该系统 150 可被重启、或电源可被供应至系统、抑或其它任何其它需要安全启动处理的事件可能发生。因此可由中央处理单元核心 102 执行适当的自我测试,且可初始化个别组件(如缓存器等)。应理解的是,在某些实施例中,可能不会进行安全启动处理,而该系统 150 可能由处于操作系统仍受控制的作业状态。在步骤 S110 中,第一指令系取自内部非易失性存储器 103,其可通过映像(mapping)该内部存储器 103 至相对应之重启向量地址而达成。因此,该中央处理单元 100 在因任何外部事件导致跳越至重启向量的任何事例中会开始进行依据安全数据组 103A 之执行。于步骤 S120 中,会因包含在数据组 103A 中的指令被执行而使得该内部随机存取存储器 101 被启动。于步骤 S130 中,至少一部分之启动信息 121,例如包含其签名的第一部分 121A,可被加载至该内部随机存取存储器 101 中。于步骤 S140,启动信息 121 或第一部分 121A 的完整性可通过利用包含在数据组 103A 中的解密密钥验证之。

[0041] 换句话说,在初始化存储器 101 之后,即开始执行启动信息 121 或至少第一部分 121A 的签名检验。为此目的,在某些实施例中,可依据安全散列算法计算散列值,该安全散列算法系例如 SHA1,其中一或多个用于启动信息 121 或第一部分 121A 的签名可被略过。另外,例如包含于一次性程序化存储器 130 中之厂商标志等其它信息可适用于某些情形,且可用于计算一或多个散列值。接着一或多个计算得到的散列值,可与一或多个包含在数据 121 或 121A 之专属地址的散列值相比较,如前述参照图 1b 之说明。为止目的,来自一或多个签名的散列值可通过数据组 103A 中的公开解密密钥而取得,以得到初始散列值。若计算所得的散列值与初始散列值匹配,则于步骤 S 150 中将启动信息 121 或第一部分 121A 视为可信赖,并接着于步骤 S160 继续启动处理。于一示范性实施例中,若于步骤 S150 中未通过完整性检验,则于步骤 S170 中,可指示相对应之启动失败,并伴随着终止启动处理且发出相对应之错误代码。

[0042] 在上述实施例中,在将执行交由启动信息 121 或第一部分 121A 之前,该安全启动程序(即步骤 S100-S150 表示之流程)不会将重启程序适用于该系统 150 之任何组件,藉

此能达成该系统 150 硬件组构硬件组构之可信赖「测量」。

[0043] 图 1f 为依据本发明其它实施例之安全启动处理的示意图。如图所示,于步骤 S101 中,将决定一安全启动处理是否应启动。可通过设定被包含在存储器 130 中之个别的安全位,而取得个别的指示。如前述,于步骤 S100 中,由非易失性存储器 103 开始执行。在步骤 S102 中,可提供状态信息,以例如用于适当地设定一输出埠。举例而言,于步骤 S102 中,可指示安全启动处理系在内部自我测试期间被启动。于步骤 S120 中,该系统 150、特别是中央处理单元 100 可被初始化,其可例如包含一或多个步骤 S121-S129。例如在步骤 S121 中,该存储器 103 的地址可作适当的重映像,以确保第一个指令将提取自该存储器 103。于步骤 S122 中,可侦测启动源,并于步骤 S123 中初始化该启动源。此外,该存储器 101 (即数据高速缓存 101A 及指令高速缓存 101B) 可在步骤 S124、S125 中被初始化,且数据高速缓存之非真实模式 (unreal mode) 可于步骤 S126 中建立。再者,启动信息 121 或第一部分 121A 之镜像 (image) 可复制至数据高速缓存 101A 中,且于步骤 S128 中,数据高速缓存 101A 中之储存空间可指派予变量。最后若需要,可于步骤 S129 中取得厂商标志。

[0044] 在步骤 S141 中读取启动信息 121 或第一部分 121A 的区块,接着在步骤 S142 中,可执行各个散列算法以得到第一散列值。于步骤 S143 中,可决定先前读取之数据区块是否为最后的区块。若否,流程将回到步骤 S141 以读取另一数据区块,并于下一步骤 S142 中,计算散列值并更新之前取得的散列值。当于步骤 S143 中读取最后的区块时,系于步骤 S144 中储存计算得到的散列值,并于步骤 S145 中读取数据 121 或 121A 的相关部分以取得包含于其中的签名。例如,信息 121 或第一部分 121A 的标头区块 (header block) 可用于此目的。于步骤 S146 中,一或多个签名被取得,并于步骤 S147,使用一或多个公开密钥以辨读于步骤 S146 中所取得的签名。于步骤 S150,将在步骤 S144 中所储存的散列值与通过执行步骤 S147 所得之原始散列值进行比较,以决定数据 121 或 121A 是否被视为可信赖。

[0045] 当步骤 S150 中散列值匹配时,之前所初始化的指令高速缓存可利用启动数据 121 或 121A 被更新 (该启动数据此时储存于数据高速缓存 101A 中),以验证其中之启动数据。在步骤 S162 中,可指示安全启动程序的状态,最后于步骤 163 中,通过实行来自指令高速缓存的指令,使启动程序继续,其中该指令可包括系统存储器 110 的初始化、启动数据 121 任何剩余部分 (如第二部分 121B) 之取得、以及通过计算散列值并将所计算的散列值与第一部分 121A 中所包含的原始散列值相比较而进行其完整性的验证。当步骤 S150 中的完整性未确认通过时,于步骤 S171 将提供一相对应的状态信息 (例如,0xCD)。于一示范性实施例中,于步骤 S172 终止执行。

[0046] 因此,本发明所揭露的系统及机制可通过提供安全启动处理,而提升计算机平台之完整性,其中安全启动处理系基于包含在非易失性存储器中的预启动程序者,且其中,一旦数据被程序化至非易失性存储器后即无法被覆写。由于非易失性存储器属于中央处理单元的一部分,故系统初始化可依据储存在非易失性内部存储器之预启动信息而完成,同时其中尚可包含适当之解密密钥,其可用于已签名之启动信息、或至少启动信息之已签名的部分。用于计算启动信息或其一部分之适当散列值的程序、以及与以加密方式储存在启动信息中的原始散列值的比较,系可通过使用中央处理单元的内部随机存取存储器来完成,藉此可防止外部存取的可能性,进而防止系统设定遭篡改的可能性。因此,储存在内部的预启动信息可使用为系统初始化时的信赖测量之核根。

[0047] 上文中揭露的特定实施例系仅为例示性者,对该技术领域中具有通常知识者而言,本发明可被更改,且能以不同但等效之方式施行。例如,上述之程序步骤可用不同的顺序来执行。再者,除非为于申请专利范围中所描述者,否则无意限制为于此所示之架构或设计的细节。因此明显地,该等实施例可能会有变动,而任何的变动或等效性的替换系被视为在本发明之精神及范围内。因此,于此所寻求之保护系于后述之申请专利范围中提出。

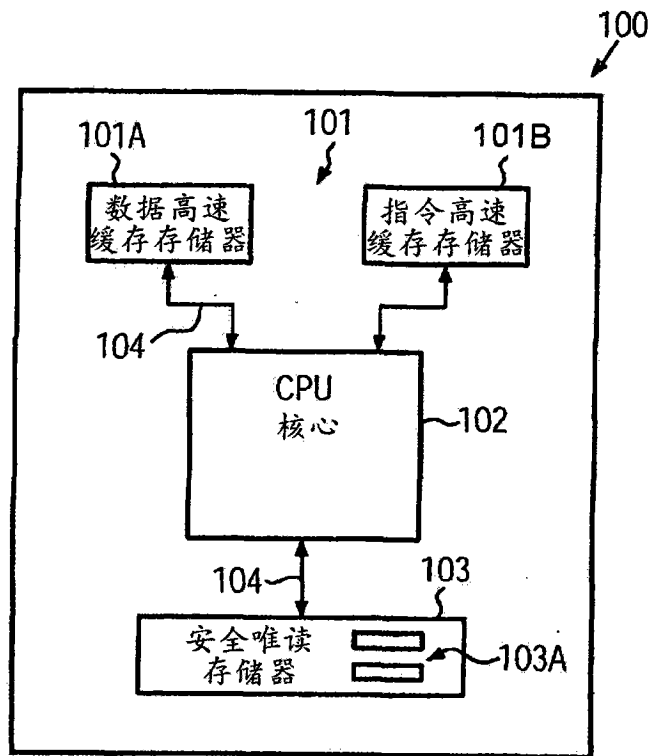


图 1a

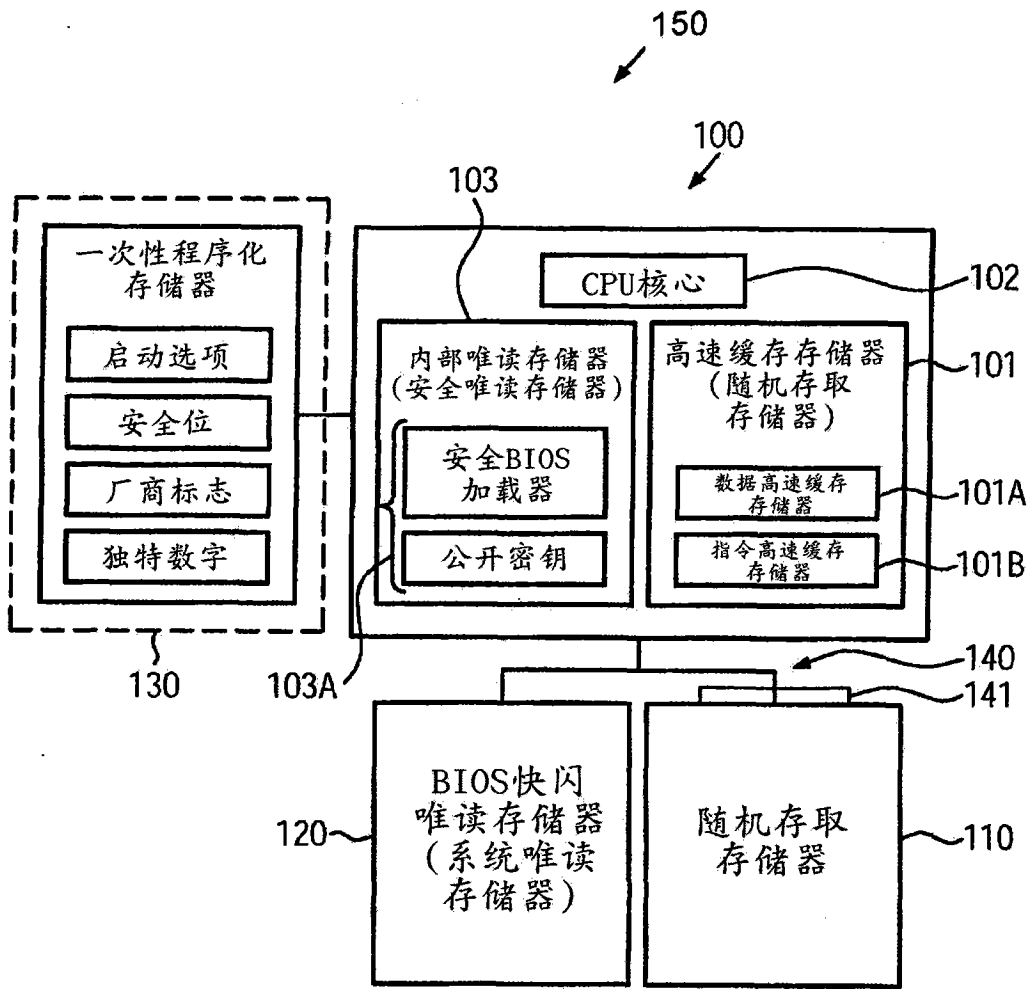


图 1b

BIOS镜像于可信中心签名：

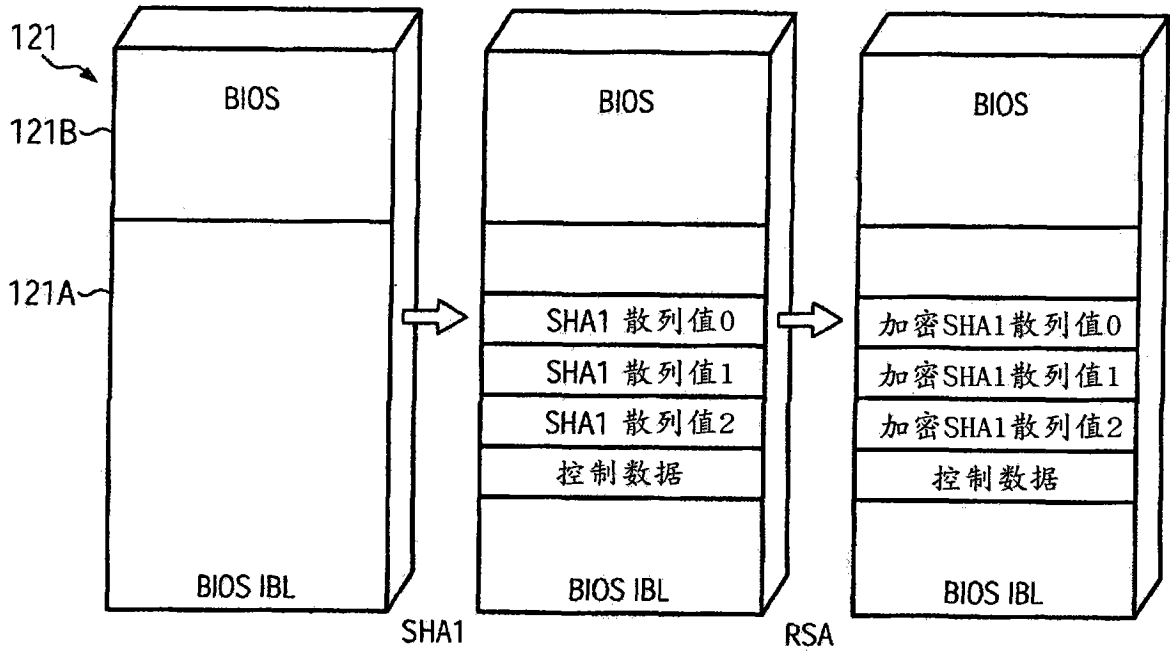


图 1c

BIOS于CPU100的完整性检验：

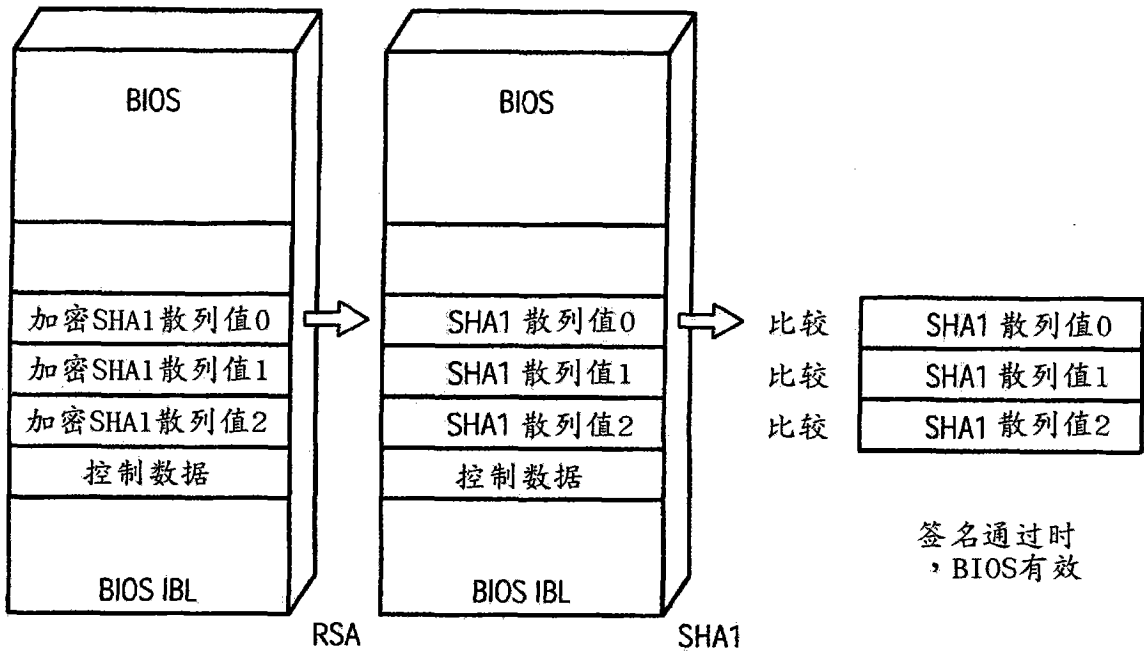


图 1d

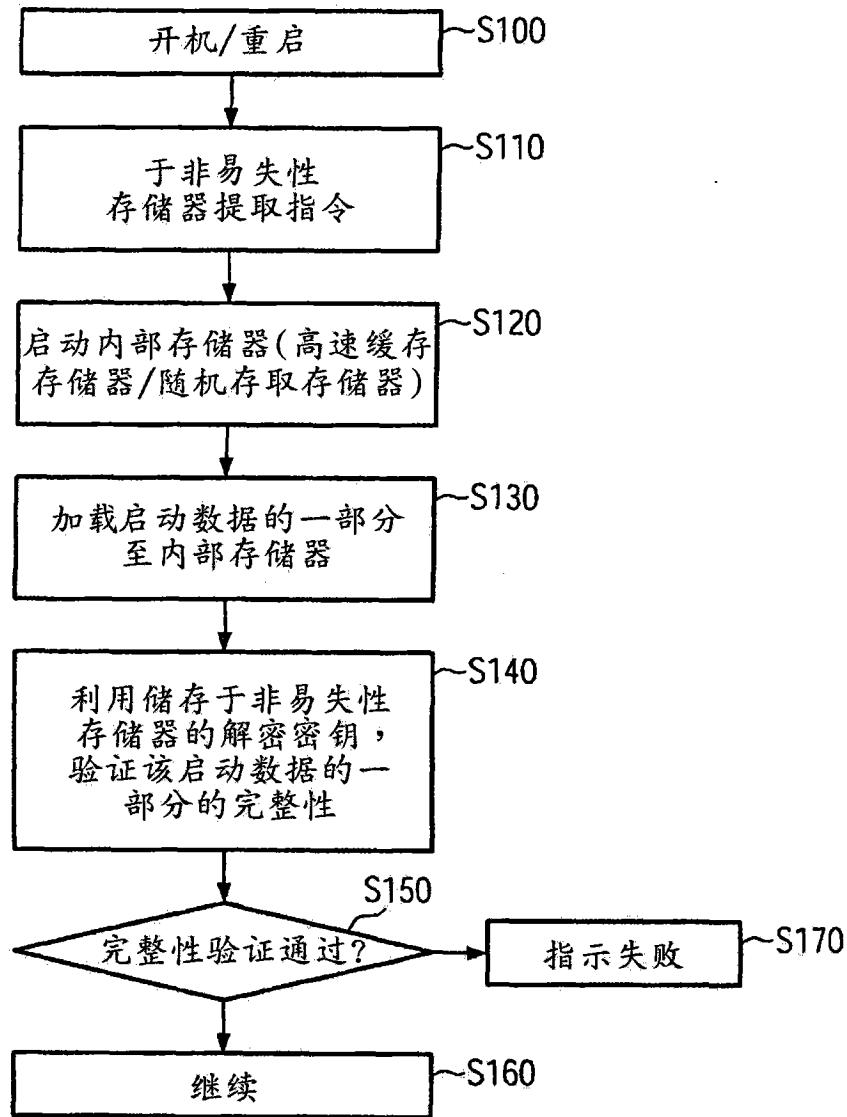


图 1e

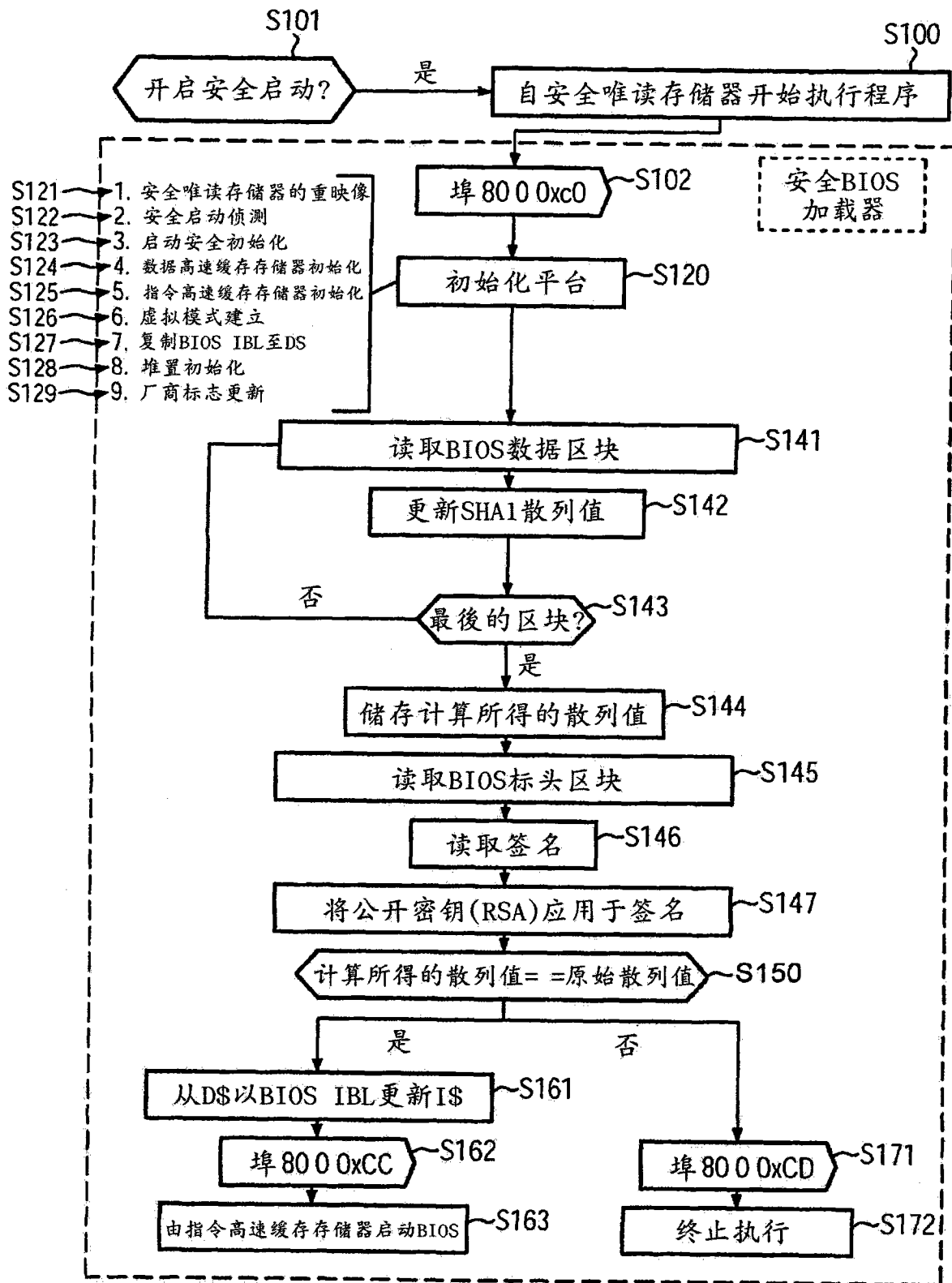


图 1f