[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 11/30 (2006.01)
G06F 11/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580006770.6

[45] 授权公告日 2009 年 5 月 20 日

[11] 授权公告号 CN 100489805C

[22] 申请日 2005.1.21
[21] 申请号 200580006770.6
[30] 优先权
[32] 2004. 3. 1 [33] US [31] 10/791,171
[86] 国际申请 PCT/US2005/001752 2005.1.21
[87] 国际公布 WO2005/091757 英 2005.10.6
[85] 进入国家阶段日期 2006.9.1
[73] 专利权人 飞思卡尔半导体公司
地址 美国得克萨斯
[72] 发明人 劳伦斯·L·卡塞
马克·D·雷德曼
托马斯·E·特卡奇克
乔尔·D·费尔德曼
[56] 参考文献
CN1155700A 1997.7.30
US6587947B1 2003.7.1
US6098171A 2000.8.1
JP10-326126A 1998.12.8
CN87107775A 1988.8.10
审查员 郑嘉青
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 黄启行 穆德骏

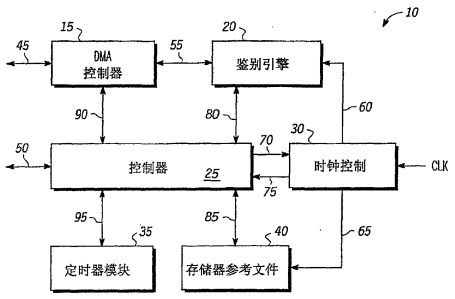
权利要求书 3 页 说明书 10 页 附图 4 页

[54] 发明名称

运行时间安全保证的自动存储器检测器及其方法

[57] 摘要

为电子设备的运行时间安全保证提供自动存储器检测器的方法和装置。 自动存储器检测器包括控制器、耦合至控制器的存储器参考文件以及耦合至控制器的鉴别引擎。 在电子设备运行时间操作期间执行检测。 自动存储器检测器生成对应于存储于存储器中的可信信息的运行时间参考值。 运行时间参考值被与存储在存储器参考文件中的存储器参考值进行比较。 存储器参考值从存储器中存储的可信信息生成。 当运行时间参考值与存储器参考值不相同时，生成错误信号，由此指示可信信息已经被修改。



1. 一种电子设备，包括用于运行时间安全保证的自动存储器检测器，该自动存储器检测器耦合至主机处理器，所述自动存储器检测器包括：

DMA 控制器；

耦合至所述DMA控制器并适于请求所述DMA控制器从存储器的一部分提取第一存储器内容的控制器；

耦合至所述控制器的存储器参考文件，该存储器参考文件适于存储对应于所述第一存储器内容的至少一个存储器参考值；以及

耦合至所述控制器的鉴别引擎，该鉴别引擎适于通过将至少一个运行时间参考值与所述至少一个存储器参考值进行比较来在所述电子设备的运行时间操作期间执行运行时间检测，其中所述至少一个运行时间参考值对应于所述控制器在所述电子设备的所述运行时间操作期间从存储器的所述部分提取的第二存储器内容，其中所述自动存储器检测器是允许从存储器提取所述第二存储器内容而无需从所述主机处理器请求准许的总线主控器。

2. 权利要求 1 的所述电子设备，其中所述检测在所述电子设备的运行时间操作期间周期性地执行。

3. 权利要求 1 的所述电子设备，其中所述检测在所述电子设备的运行时间操作期间在随机时刻执行。

4. 权利要求 1 的所述电子设备，在所述电子设备的所述运行时间操作期间，所述自动存储器检测器独立于来自所述主机处理器的命令操作。

5. 权利要求 1 的所述电子设备，其中所述控制器响应于来自所述主机处理器的进入初始存储器参考模式的信号而提取所述第一存储器

内容。

6. 权利要求 1 的所述电子设备，其中所述第一存储器内容包括可以由所述主机处理器在所述电子设备上执行的软件。

7. 一种操作具有存储器以及耦合至所述存储器的主机处理器的电子设备以用于运行时间安全保证的方法，包括以下步骤：

在所述电子设备的所述存储器中的特定存储器位置存储可信信息，其中所述可信信息包括可由所述主机处理器在所述电子设备上执行的软件；

从所述特定存储器位置提取所述可信信息，并且向鉴别引擎提供所述可信信息；

对应于从所述特定存储器位置提取的所述可信信息生成存储器参考值；

在存储器参考文件中存储所述存储器参考值；

在所述存储器参考文件中存储所述存储器参考值之后，以操作的运行时间模式操作所述电子设备；

在所述电子设备操作的运行时间模式期间，从所述特定存储器位置提取存储器内容，并且向所述鉴别引擎提供对应于所述存储器位置的所述存储器内容，其中无需从所述主机处理器请求准许即可执行所述从所述特定存储器位置提取所述存储器内容；

通过从所述特定存储器位置提取的所述存储器内容生成运行时间参考值；以及

将所述运行时间参考值与所述存储器参考值进行比较。

8. 权利要求 7 的所述方法，进一步包括以下步骤：

当所述运行时间参考值与所述存储器参考值相同时，继续所述电子设备操作的所述运行时间模式；以及

当所述运行时间参考值与所述存储器参考值不相同时，发出错误

信号。

9. 一种操作具有主机处理器的电子设备以用于运行时间安全保证的方法，包括以下步骤：

从所述电子设备的存储器的一部分提取可信信息，其中所述可信信息包括可由所述主机处理器在所述电子设备上执行的软件；

在所述电子设备操作的引导时间模式期间，向自动存储器检测器提供所述可信信息；

在所述引导时间模式期间，指示所述自动存储器检测器散列所述可信信息；

通过所述自动存储器检测器，从所述可信信息生成参考散列值；

将所述参考散列值存储到存储器参考文件；

在所述电子设备操作的运行时间模式期间，从之前提取所述可信信息的存储器的所述部分中提取存储器内容；

通过所述自动存储器检测器，利用在运行时间模式期间得到的所述存储器内容生成运行时间散列值，其中在操作的所述运行时间模式期间，所述自动存储器检测器独立于来自所述主机处理器的命令操作；

将所述参考散列值与所述运行时间散列值进行比较；以及

当所述参考散列值与所述运行时间散列值不同时，发送错误信号，指示所述可信信息已经被修改。

运行时间安全保证的自动存储器检测器及其方法

技术领域

本发明主要涉及软件的安全保证，更具体地，本发明涉及向运行时间软件增加安全保证的硬件方法。

背景技术

确保嵌入系统软件代码完整性正成为嵌入电子设备日益重要的安全问题。确保存储于存储器中软件的完整性是有利的大量例证是个人数字助理（PDAs）和手机。主要地，这些设备利用内部微处理器分两个阶段执行指令：引导时间和运行时间。可信计算机系统利用加密的软件在执行软件前鉴别每个阶段。

在引导时间期间，嵌入的处理器执行基本硬件和存储在非易失性存储器中的软件初始化指令（引导代码），如电可擦除只读存储器（如闪盘永久性存储器）、只读存储器（ROM）、或电可编程只读存储器（EPROM）。引导代码的目的是确认和配置硬件及与硬件相关的数据，为系统软件提供已知的执行环境和用户界面。对于可信的计算机操作，引导代码也在引导时间确认和鉴别程序应用及操作系统（OS）存储器，确保该存储器包含期望的并因此可信的代码。一旦引导时间指令对鉴别进行了检测，则系统控制进入经确认的 OS/应用程序执行图像并进入运行时间模式。

在运行时间期间，处理器执行来自 OS/应用程序图像的代码。OS 通常将建立多处理运行时间执行环境，装载任何启动或嵌入式应用程序，为正常运行时间过程作准备。在此稍后时间期间，当运行时间环境完全建立时，不可信的用户应用代码或下载的动态代码可能运行，并且存储器故障可能出现在原来可信和鉴别的代码上，这是由于非引

导时间因素造成的，如计算机病毒或内部程序缺陷。此外，在引导时间确认的OS/应用程序存储器可被运行时间存储器恶意替换，而变得与在引导时间鉴别的完全不同。这被称为“背负式（piggy back）”攻击，它向嵌入式系统软件构成相当大的安全威胁难题。请求对产品平台的物理访问，运行时间存储器件被背负在初始确认的存储器件上。在引导过程结束并将控制传递至外部存储器之后，它完全替换确认的引导设备，从此创建完全不同的、未经检测的运行时间环境。

系统软件中确认指令代码的传统方法只鉴别指令存储器一次。利用密码算法生成单向存储器参考签名或不对称密钥数字签名执行一次确认。执行前，消息鉴别代码或类似的数字签名在指令寄存器中生成。如果生成的结果与存入系统其它地方或加密的不对称数字签名内的预定值匹配，则指令被允许执行。然而，目前的解决方法不解决在初始鉴别后篡改指令存储器内容的风险。在运行时间期间，指令代码易受背负式即软件攻击，这些攻击将替换已鉴别的指令存储器或数据。初始鉴别代码的完整性可因存储器的物理替换或处理器的转移而受到破坏，从未经初始鉴别的存储器范围执行代码。例如，计算机病毒可在引导时间期间保持隐匿，然后导致处理器异常，以执行不同的指令集。

在设备的操作过程当中，控制电子设备的大部分系统软件不会改变。即使通过初始鉴别将系统软件高可靠性地装入存储器中，在数百万时钟循环和不断向不可信代码暴露后，系统恶化的可能性会上升。如果系统遭破坏，执行自我检测功能是不可信的。事实上，用于执行自检的参考数据/存储器是安全目标或弱点，并且是安全敏感的和决不应改变的数据的示例。其它安全敏感数据可以是配置寄存器，该配置寄存器控制内部数据对嵌入设备或OS敏感数据的外部的可见度，如中断服务例程（ISR）地址，或特定存储器管理单元（MMU）页面表，或特定文件系统数据，如用户和组标识符以及口令。

此外，许多嵌入系统，如手机 及PDA，只有在它们被从电源断开

时才进入引导模式。因此，在运行时间模式的嵌入设备的初始指令代码的完整性，在设备运行下载的应用程序和在与外部设备通信时，面临逐渐增加的风险。因此，在通常不断开电源和直到电源故障才重新引导进行鉴别的设备中，风险特别大。而且，操作系统和应用软件被存储于存储器的不同区域。事实上，软件被存储在不同的区域，并且软件还可能被从许多源接收，一些是确实存在的，其它是不能被证实，这会引起长期跟踪和安全问题。

由此，期望为软件的运行时间安全保证设计存储器检测器，在引导时间期间装入存储器。如果存储器检测器是自动地确保检测出现，那将是有利的。如果该设备节能并且在频繁请求总线访问而不明显影响运行时间系统性能，那将更是有利的。

发明内容

根据本发明的一个方面，提供了一种电子设备，包括用于运行时间安全保证的自动存储器检测器，该自动存储器检测器耦合至主机处理器，所述自动存储器检测器包括：DMA 控制器；耦合至所述 DMA 控制器并适于请求所述 DMA 控制器从存储器的一部分提取第一存储器内容的控制器；耦合至所述控制器的存储器参考文件，该存储器参考文件适于存储对应于所述第一存储器内容的至少一个存储器参考值；以及耦合至所述控制器的鉴别引擎，该鉴别引擎适于通过将至少一个运行时间参考值与所述至少一个存储器参考值进行比较来在所述电子设备的运行时间操作期间执行运行时间检测，其中所述至少一个运行时间参考值对应于所述控制器在所述电子设备的所述运行时间操作期间从存储器的所述部分提取的第二存储器内容，其中所述自动存储器检测器是允许从存储器提取所述第二存储器内容而无需从所述主机处理器请求准许的总线主控器。

根据本发明的另一个方面，提供了一种操作具有存储器以及耦合至所述存储器的主机处理器的电子设备以用于运行时间安全保证的方

法，包括以下步骤：在所述电子设备的所述存储器中的特定存储器位置存储可信信息，其中所述可信信息包括可由所述主机处理器在所述电子设备上执行的软件；从所述特定存储器位置提取所述可信信息，并且向鉴别引擎提供所述可信信息；对应于从所述特定存储器位置提取的所述可信信息生成存储器参考值；在存储器参考文件中存储所述存储器参考值；在所述存储器参考文件中存储所述存储器参考值之后，以操作的运行时间模式操作所述电子设备；在所述电子设备操作的运行时间模式期间，从所述特定存储器位置提取存储器内容，并且向所述鉴别引擎提供对应于所述存储器位置的所述存储器内容，其中无需从所述主机处理器请求准许即可执行所述从所述特定存储器位置提取所述存储器内容；通过从所述特定存储器位置提取的所述存储器内容生成运行时间参考值；以及将所述运行时间参考值与所述存储器参考值进行比较。

根据本发明的还一个方面，提供了一种操作具有主机处理器的电子设备以用于运行时间安全保证的方法，包括以下步骤：从所述电子设备的存储器的一部分提取可信信息，其中所述可信信息包括可由所述主机处理器在所述电子设备上执行的软件；在所述电子设备操作的引导时间模式期间，向自动存储器检测器提供所述可信信息；在所述引导时间模式期间，指令所述自动存储器检测器散列所述可信信息；通过所述自动存储器检测器，从所述可信信息生成参考散列值；将所述参考散列值存储到存储器参考文件；在所述电子设备操作的所述运行时间模式期间，从之前提取所述可信信息的存储器的所述部分中提取存储器内容；通过所述自动存储器检测器，利用在运行时间模式期间得到的所述存储器内容生成运行时间散列值，其中在操作的所述运行时间模式期间，所述自动存储器检测器独立于来自所述主机处理器的命令操作；将所述参考散列值与所述运行时间散列值进行比较；以及当所述参考散列值与所述运行时间散列值不同时，发送错误信号，指示所述可信信息已经被修改。

附图说明

此后将结合下面给出的附图描述本发明，其中相同的引用标记表示相同的元件，并且

图 1 是根据本发明一个实施例的自动存储器检测器框图；

图 2 是根据本发明的一个实施例的第一流程图，说明用于运行时间安全保证的自动存储器检测器的操作步骤；

图 3 是示出了耦合至主机处理器和存储器块的自动完整性检测器的系统方框图；以及

图 4 是根据本发明的一个实施例的第二流程图，说明用于运行安全保证的自动存储器检测器的操作步骤。

具体实施方式

下面的详细描述仅为特性示例，并非意图限制本发明，及其本发明的应用及使用。此外，也无意图因对前述技术领域、背景技术、发明内容及后面的详细描述使任何表述或隐含的理论受到限制。

图 1 是根据本发明一个实施例的自动存储器检测器 10 的框图。主机处理器（未示出）首先设定可编程参数，如存储器起始地址、长度、直接存储器访问（DMA）读频率、最大突发大小、以及存储器块使能。主机经过主机总线 50 发送指令到自动存储器检测器 10 的控制器 25，启动初始存储器参考模式。在初始存储器参考模式，控制器 25 请求 DMA 控制器 15 经过 DMA 主控总线 45 提取存储器内容。存储器内容是可信的信息。鉴别引擎 20 经内部总线 55 接收存储器内容，生成适当的存储器参考。鉴别引擎 20 生成存储器参考值，如大块数据的散列函数、少量数据的简单复制，或大量数据快速处理的循环冗余校验（CRC）。从鉴别引擎 20 输出的存储器参考值，经过内部总线 80 和 85，被存储于存储器参考文件 40 中。在引导时间模式期间，存储器参考文件 40 在存储器中存储存储器参考值。这些存储器参考值被重复地与在运行时间模式生成的运行时间参考值进行比较，以确保可信信息的完整性，这些存储器参考值在引导时间模式启动后不应当被改变。

可信信息的一个示例是对电子设备的操作非常关键的软件。制造商在电子设备中装入软件。由于制造商或其它受可信实体向电子设备提供该软件，则该软件是可信的信息。总之，现有技术的电子设备只检测在引导时间模式期间可信信息的完整性。该可信信息易受修改，而无需电子设备用户的认可。由外部代理而没有用户认可的可信信息修改会造成严重后果。利用软件程序检测可信信息是自相矛盾的，因为存储器中信息的完整性有问题。换句话说就是软件检测程序可能会像可信信息一样被修改。可以理解，可信信息可是任何类型的信息，该信息不应被改变或修改，并且也不限于软件。

在运行时间期间，自动存储器检测器 10 可主动监测经确认的存储器内容的真实性。它可从存储器取值并执行多种监测方案。一种可能的方法是“点检测”，点检测从一个隔离的存储器位置检索数据。另一方法设计包括“漫游检测”，该检测从某位置读取值，然后与前面存储的值进行比较。如果两个值匹配，指针增加，新的值被读并存储。这个存储的值之后被与从相同的存储器位置读取的值进行比较。在分配空间的边界内，漫游检测自我重复。

另一常用方案是“块检测”。该方法通常被称为“散列”或 CRC。块检测对特定的数据块执行压缩型功能，并且存储不同的代表值（即离散数学函数输出），为之后比较之用。

其它监测功能包括写-读检测，主动等待检测，以及软件到硬件切换检测。写-读检测将任意值装入存储器位置，之后再重新取得。存储值的任何改变均表明可能的数据破坏。读-写方式要求 DMA 控制器 15 具备向期望的存储器位置既能读又能写的能力。

主动等待检测要求系统软件周期性地“check-in”以进行比较。最后，软件到硬件的切换检测阻止缓冲区溢出攻击在子例程中的出现，

该子例程给缓冲区分配的空间小于写入其中的字的数量。溢出的字落入为诸如为程序计数器的关键数据而分配的栈空间。当子例程返回，程序计数器将是不正确的。一种防止缓冲区溢出攻击的方式是命令正常软件在安全状态下初始化硬件检测。处于正常状态的软件告知硬件将要在子例程中分配缓冲区以及关键数据位于特定地址。硬件缓冲鉴别的值。之后不久，硬件要看处于缓冲区边缘的值是否没有改变。尽管软件到硬件的切换检测包括一些开销，但对高敏感数据，它明显地增加了安全保证。

如果在运行时间期间出现参考失配，地址/长度错误，或出现监视超时，自动存储器检测器 10 停止操作，并且发出适当的中断，以表明经确认的存储器内容的可能恶化。可以理解，自动存储器检测器 10 独立操作，并在其操作期间不能由其它逻辑块或程序关闭。这就确保了可信信息在运行时间模式期间总被检测。在运行时间期间的任何错误将引起自动存储器检测器 10 中断，并向主机发错误信号。在系统实施例中，要求硬件复位，以退出错误状态。

自动存储器检测器 10 也包括定时器模块 35 以及时钟控制 30。定时器模块 35 在自动存储器检测器的各个阶段关闭自动存储器检测器 10 的特定逻辑块，以提供节能。定时器模块 35 不断地、部分地控制时钟控制 30、控制器 25、鉴别引擎 20 及其它块的操作。定时器模块 35 包含总线监视定时器，该定时器确保 DMA 控制器 15 被准许在可接受的时间量内的总线访问。如果时钟控制 30 处于活动模式，则时钟控制 30 向控制器 25、鉴别引擎 20 以及存储器参考文件 40 提供时钟信号。

DMA 控制器 15 允许自动存储器检测器 10 是总线主控器。自动存储器检测器 10 可提取存储器内容，而在任何时候无需向主机请求准许。DMA 控制器 15 具备读能力。DMA 控制器 15 的直接存储器访问能力允许自动存储器检测器 10 在由于软件损坏而使主处理器不可信的情况下是可靠的。

图 2 是示出图 1 的自动存储器检测器 10 的操作概念性步骤的第一流程图。在复位后的引导时间期间，自动存储器检测器 10 从主机接收进入初始存储器参考模式 110 的信号。在初始存储器参考模式 110 中，自动存储器检测器 10 通过 DMA 控制器 15 从存储器中提取特定内容，并通过鉴别引擎 20 为期望的存储器位置或块生成存储器参考值。典型的鉴别方案包括，但不限于，安全散列算法 1（SHA-1）及消息分类算法 5（MD5）。存储器参考值表示特定存储器内容的特有值。每个存储器参考值被存于存储器参考文件 40，以为之后比较之用。处理 115 及 117 重复，直到自动存储器检测器 10 从主机接收到进入运行时间检测模式 120 的另一个信号。

在运行时间检测模式 120 中，可调时间随机函数发生器初始化存储器参考比较 130。当定时器模块 35 唤醒自动存储器检测器 10 中的其余电路时，控制器 25 向 DMA 控制器 15 发出信号，以从特定块和地址中提取存储器内容。提取的存储器内容馈入鉴别引擎 20，以生成运行时间参考值。运行时间参考值被与存储器参考文件 40 中存储的值比较。比较的运行时间和存储参考值对应于相同的存储器块和地址。如果运行时间和存储器参考值匹配，那么无论何时可调时间随机函数发生器初始化另一个存储器参考比较，处理 130 和 140 重复。如果存储器参考值不匹配，那么，自动存储器检测器 10 进入错误模式 155，硬件采取动作。

一旦错误出现，自动存储器检测器 10 具有可采取的几个硬件动作。一个可能的动作是进入硬件的、降低的系统状态。该线路将把系统功能带入非安全状态，如手机的 E-911。外部提醒是用于通知错误的硬件动作的另一方法。这像 LED 一样简单，指示设备的存储器内容的完整性不能被信任。对于非常敏感数据，硬件动作也可包括自动清除包含敏感信息的存储器。

图 3 示出了耦合至主机处理器 210 的自动存储器检测器 205 的系统方框图。自动存储器检测器 205 具有主总线 245，该主总线用于从内部存储器块 215 和外部存储器块 220 及 225 读数据。自动存储器检测器 205 由主机处理器 210 通过从主线 255 编程。自动存储器检测器 205 具有 DMA 功能，一旦它被编程，它将不向主机处理器 210 请求任何动作。如果写-读检测被执行，自动存储器检测器 205 也能够向存储器块 215、220 和 225 写入。

自动存储器检测器 205 还具备监测外围设备 260 及 265 中寄存器内容的功能。在引导时间期间，自动存储器检测器 205 可鉴别设备寄存器的内容，并在其存储器参考文件 40 中存储寄存器参考值。然后，自动存储器检测器 205 可将设备 260 和 265 中的实时寄存器值与在运行时间期间存储的值进行比较。

图 4 是展示自动存储器检测器 205 操作步骤的第二流程图 300。在本系统实施例中，自动存储器检测器 205 由块检测方案实施，采用散列函数生成存储器参考值。首先，主机处理器 210 为需要被散列的存储器块装入地址和长度对，如过程框图 310 示出。主机处理器 210 设置控制寄存器中的单一散列存储器使能并且设置命令寄存器中的“散列一次”位，如过程框图 320 示出。

在本阶段，自动存储器检测器 205 进入初始存储器参考模式，如前图 2 所示例。自动存储器检测器 205 散列存储器，在散列寄存器文件中置入散列值，并生成“完成”中断，如过程框图 330 示出。主机处理器 210 从自动存储器检测器 205 中读取生成的散列值，然后校验存储器的数字签名，如过程框图 340 示出。如果数字签名不正确，那么存在代码完整性错误，如判定框图 350 示出。如果值匹配，主机处理器 210 告诉自动存储器检测器 205，在运行时间期间，存储器块比较是否应当起作用，如判定框图 360 示出。否则，在运行时间代码散列期间，如框图 360 的 NO 判定示出，存储器块比较将被跳过。如果主机

处理器 210 要自动存储器检测器 205 处理块比较，那么主机处理器 210 将设置控制寄存器的运行时间散列存储器使能并且设置指令寄存器中的“运行时间散列”位，如过程 370 示出。

此时，自动存储器检测器 205 不能被关闭并且与主机处理器 210 的指令无关地操作。在运行时间期间，自动存储器检测器 205 在运行时间期间频繁地将来自于存储器块 215、220 及 225 的散列结果与散列寄存器文件中存储的值进行比较。设备在无限循环 380 中操作，直到存储器参考失配出现。检测周期性地或随机地被执行。随机的方法使得攻击变得非常困难，如背负式攻击，这里，存储器或存储器内容被调出更加困难，因为检测不以任何规律的时间顺序进行。

尽管在前面的详细描述中，至少展示了一个示例实施例，但应当认识到，有大量变形存在。还应当认识到，具体示例实施例或各个示例实施例仅为示例，无意限制本发明任何形式的范围、适用性，或构造。相反地，前面的详细描述将向本领域普通技术人员提供方便的方法图，以实施特定示例实施例或各个示例实施例。应当理解，在具体功能和元件安排上各种变化可能出现，而不脱离由所附权利要求和法律等效阐明的本发明的范围。

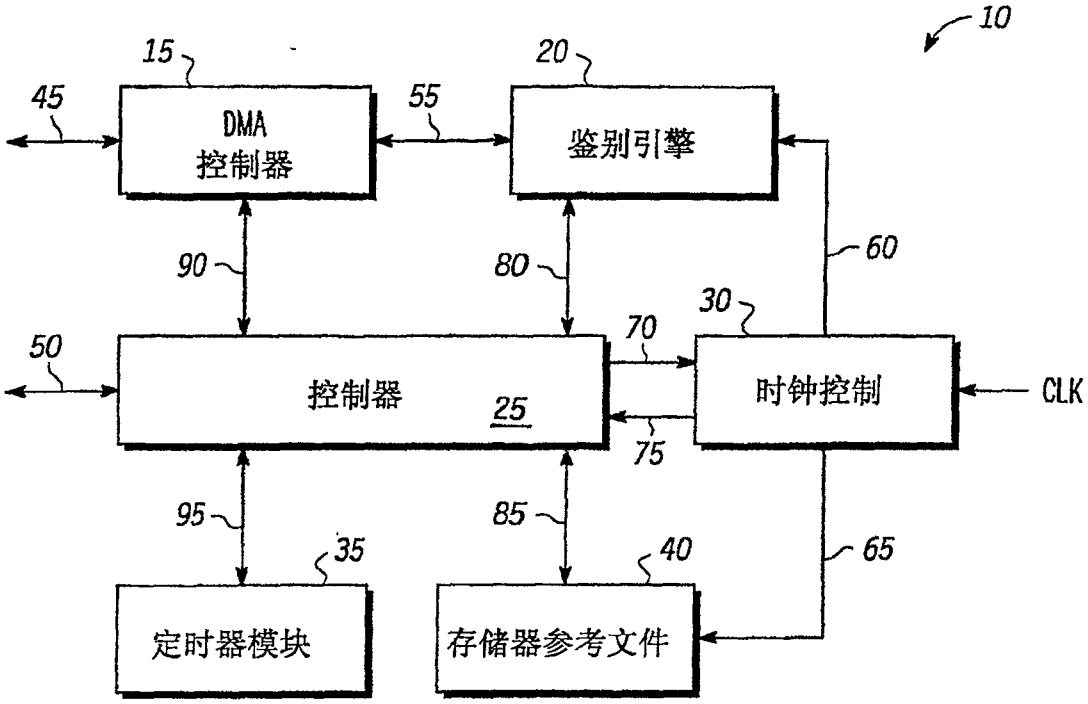

10
15
20
45
55
DMA
控制器
鉴别引擎
90
80
60
30
70
50
控制器
25
时钟控制
CLK
75
95
85
65
35
40
定时器模块
存储器参考文件

图1

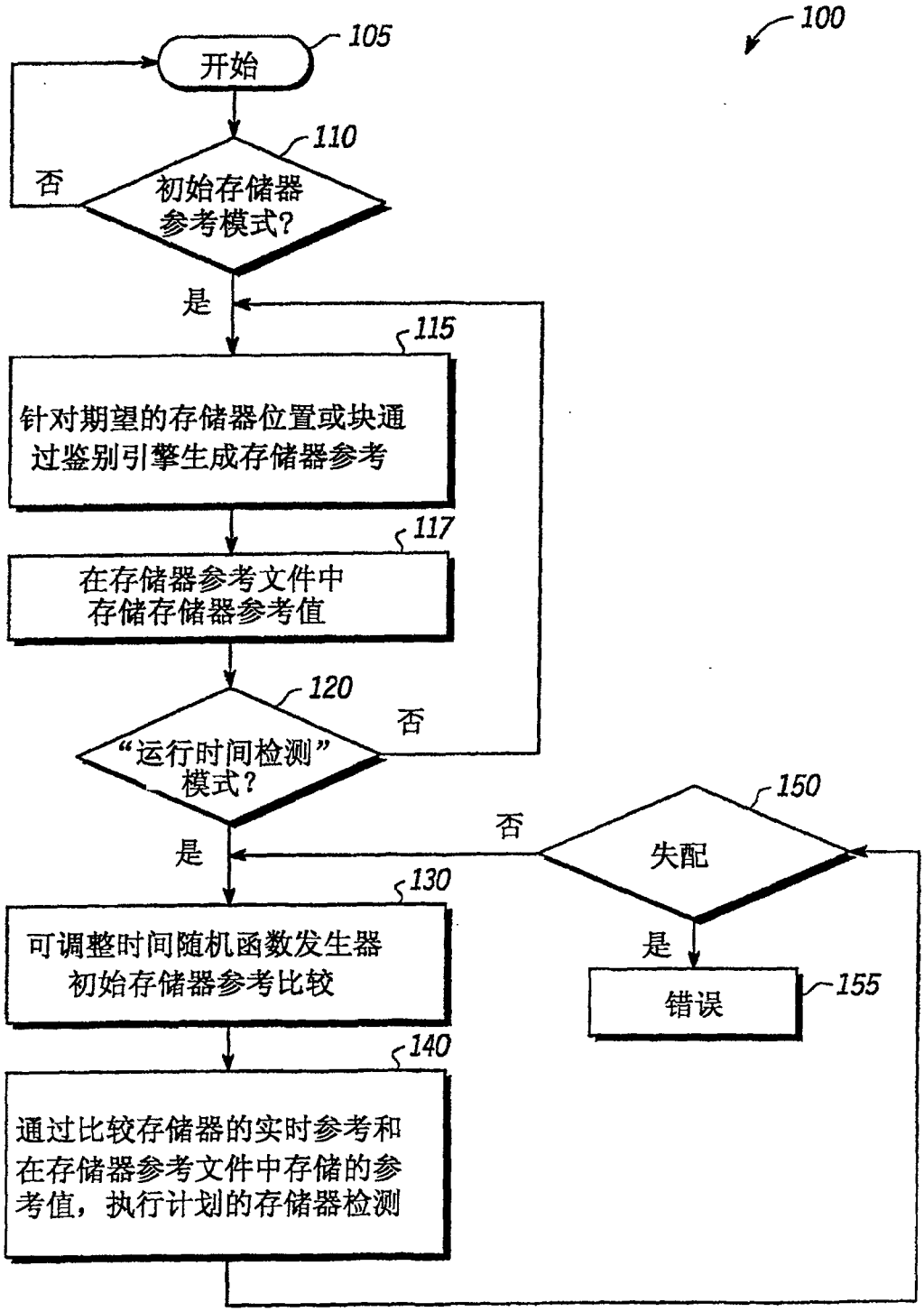

100
105
开始
110
初始存储器
参考模式?
否
是
115
针对期望的存储器位置或块通
过鉴别引擎生成存储器参考
117
在存储器参考文件中
存储存储器参考值
120
“运行时间检测”
模式?
否
是
150
失配
否
是
155
错误
130
可调整时间随机函数发生器
初始存储器参考比较
140
通过比较存储器的实时参考和
在存储器参考文件中存储的参
考值，执行计划的存储器检测

图2

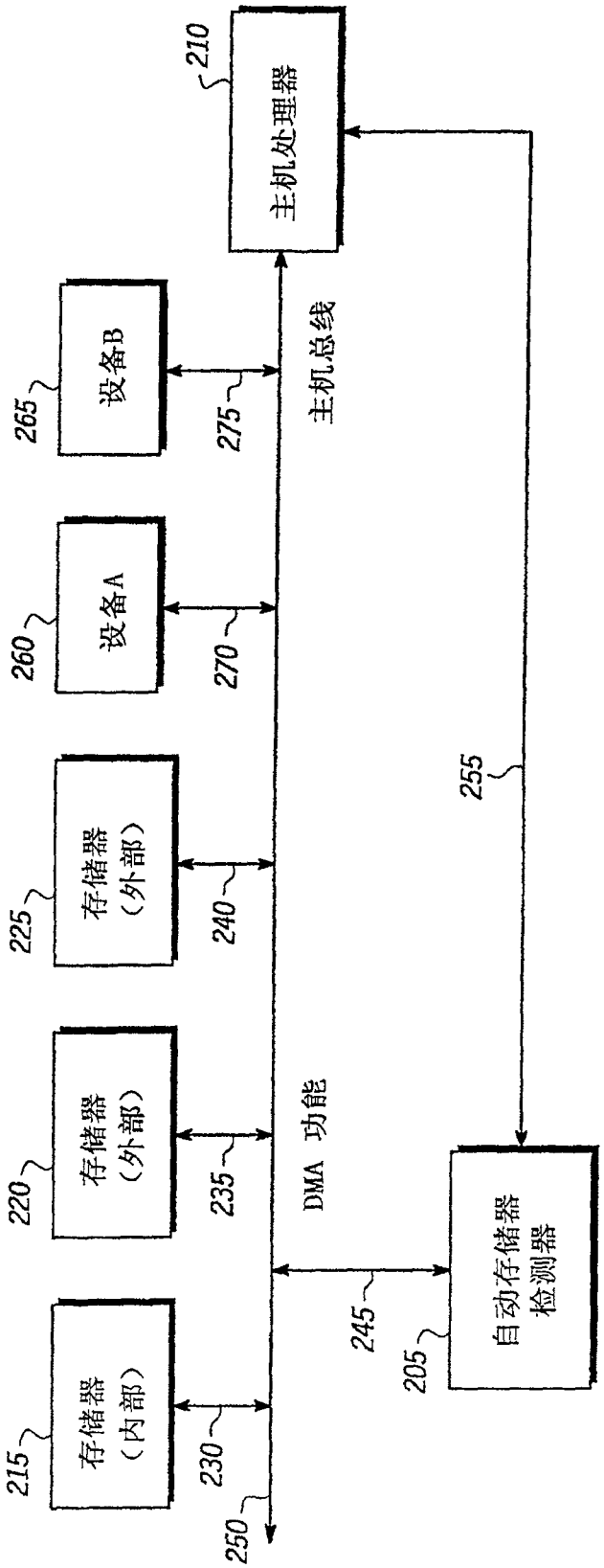

200
210
主机处理器
265
设备B
275
主机总线
260
设备A
270
225
存储器（外部）
240
255
220
存储器（外部）
235
DMA 功能
245
205
自动存储器检测器
215
存储器（内部）
230
250

图3

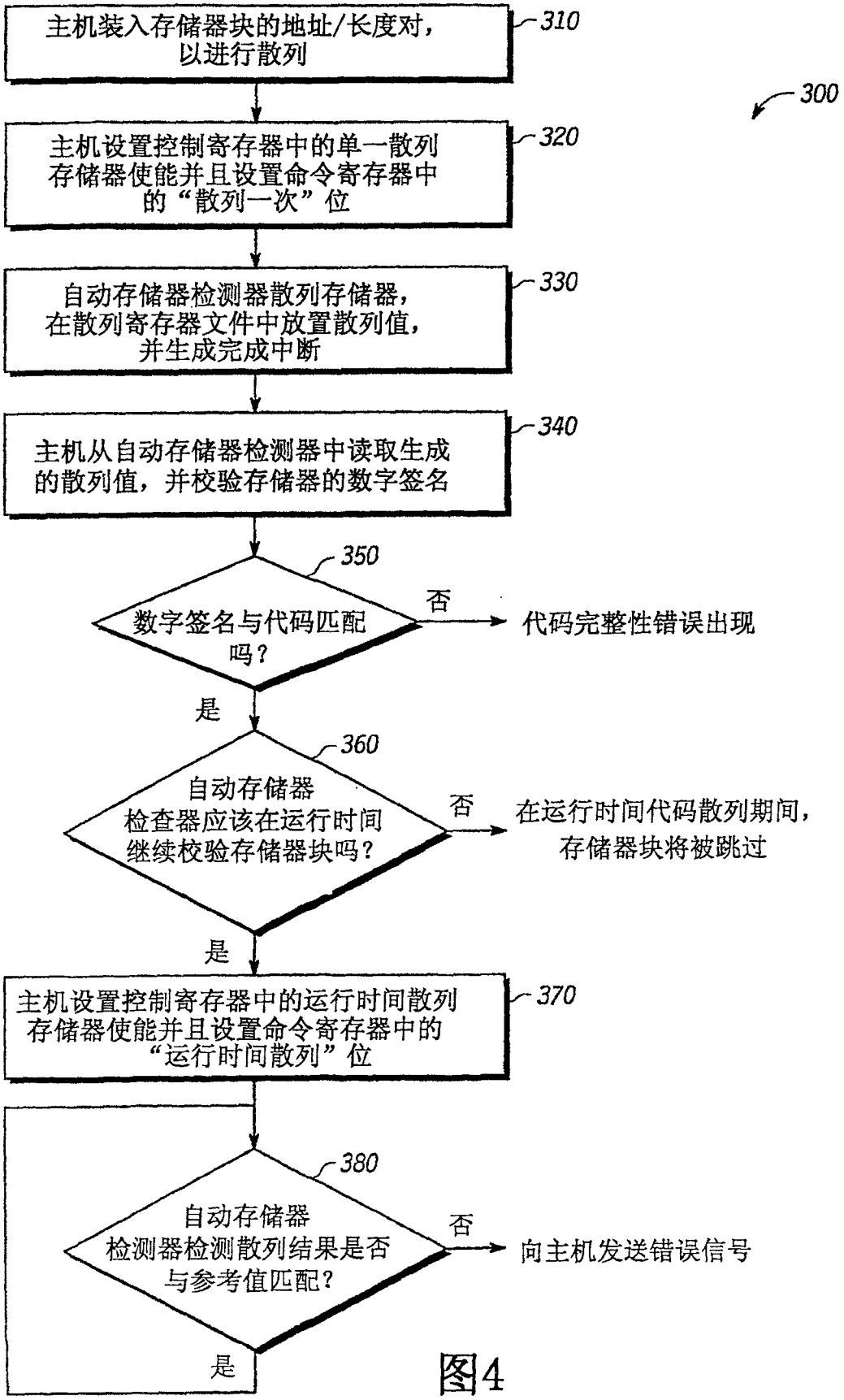

主机装入存储器块的地址/长度对，以进行散列
310
300
主机设置控制寄存器中的单一散列存储器使能并且设置命令寄存器中的“散列一次”位
320
自动存储器检测器散列存储器，在散列寄存器文件中放置散列值，并生成完成中断
330
主机从自动存储器检测器中读取生成的散列值，并校验存储器的数字签名
340
350
数字签名与代码匹配吗？
否
代码完整性错误出现
是
360
自动存储器检查器应该在运行时间继续校验存储器块吗？
否
在运行时间代码散列期间，存储器块将被跳过
是
主机设置控制寄存器中的运行时间散列存储器使能并且设置命令寄存器中的“运行时间散列”位
370
380
自动存储器检测器检测散列结果是否与参考值匹配？
否
向主机发送错误信号
是

图4