(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 108345789 B
(45)授权公告日 2019.02.22

(21)申请号 201710213086.X

(22)申请日 2017.04.01

(65)同一申请的已公布的文献号
申请公布号 CN 108345789 A

(43)申请公布日 2018.07.31

(73)专利权人 清华大学
地址 100084 北京市海淀区清华园

(72)发明人 刘雷波 罗奥 魏少军

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 贾磊 王涛

(51)Int.Cl.
G06F 21/55(2013.01)
G06F 16/17(2019.01)

(56)对比文件
CN 106407063 A,2017.02.15,
CN 101561775 A,2009.10.21,
CN 103970512 A,2014.08.06,

审查员 张文波

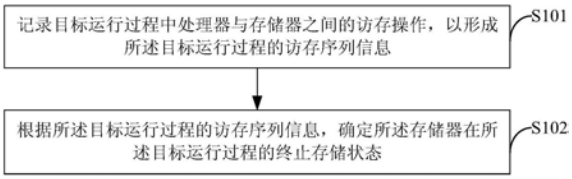
权利要求书4页 说明书12页 附图5页

(54)发明名称

记录访存操作信息的方法及装置

(57)摘要

本发明提供了一种记录访存操作信息的方法及装置，该方法包括：记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，该访存序列信息中的各访存操作信息包括访存类型、访存地址和访存数据；根据目标运行过程的访存序列信息，确定存储器在目标运行过程的终止存储状态。本发明实施例使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。



CN 108345789 B

1.一种记录访存操作信息的方法,其特征在于,包括:

记录目标运行过程中处理器与存储器之间的访存操作,以形成所述目标运行过程的访存序列信息,所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据;

根据所述目标运行过程的访存序列信息,确定所述存储器在所述目标运行过程的终止存储状态,

其中所述终止存储状态为所述处理器在所述目标运行过程中所操作的存储空间的最终存储状态。

2.根据权利要求1所述的方法,其特征在于,所述根据所述目标运行过程的访存序列信息,确定所述存储器在所述目标运行过程的终止存储状态,包括:

获取所述访存序列信息中的第一访存操作信息;

当所述第一访存操作信息的访存类型为写操作时,将所述第一访存操作信息写入第一缓冲器;

从所述第一缓冲器中获取所述终止存储状态。

3.根据权利要求2所述的方法,其特征在于,当所述第一访存操作信息的访存类型为写操作时,将所述第一访存操作信息写入第一缓冲器,包括:

确定所述第一缓冲器中是否记载有所述第一访存操作信息的访存地址;

当所述第一缓冲器中已记载所述第一访存操作信息的访存地址时,将所述第一访存操作信息写入所述第一缓冲器以覆盖先前的访存操作信息;

当所述第一缓冲器中未记载所述第一访存操作信息的访存地址时,将所述第一访存操作信息插入所述第一缓冲器。

4.根据权利要求2或3所述的方法,其特征在于,还包括:

从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息;

将所述首次读操作对应的访存操作信息中的访存数据作为检测装置的输入信息或初始运行状态,使所述检测装置以符合预定义行为的方式执行所述目标运行过程中的任务,所述预定义行为是是处理器的硬件行为标准。

5.根据权利要求4所述的方法,其特征在于,所述从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息,包括:

获取所述访存序列信息中的第二访存操作信息;

当所述第二访存操作信息的访存类型为读操作时,将所述第二访存操作信息写入第二缓冲器;

从所述第二缓冲器中获取所述首次读操作对应的访存操作信息。

6.根据权利要求5所述的方法,其特征在于,还包括:

当所述第二访存操作信息的访存类型为读操作时,确定所述第一缓冲器中是否记载有所述第二访存操作信息的访存地址;

当所述第一缓冲器中未记载所述第二访存操作信息的访存地址时,将所述第二访存操作信息写入第一缓冲器;

在所述检测装置执行所述目标运行过程中的任务时,将所述检测装置的输出数据写入所述第二缓冲器;

依次遍历比较所述第二缓冲器与所述第一缓冲器中相同访存地址的访存数据及访存类型，确定所述处理器是否安全。

7.根据权利要求5所述的方法，其特征在于，还包括：

在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器；

确定所述第一缓冲器中是否记载有所述输出数据的访存地址；

当所述第一缓冲器中已记载所述输出数据的访存地址时，根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全。

8.根据权利要求7所述的方法，其特征在于，所述根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全，包括：

遍历所述第一缓冲器中的访存操作信息，确定所述第二缓冲器是否记载有相同访存地址对应的相同访存数据；

当所述第二缓冲器中已记载相同访存地址对应的相同访存数据时，确定所述处理器安全；

当所述第二缓冲器中未记载相同访存地址对应的相同访存数据时，确定所述处理器不安全。

9.根据权利要求1至3中任一项所述的方法，其特征在于，在所述记录目标运行过程中处理器与存储器之间的访存操作之前，还包括：

获取待检测的地址范围；

根据所述待检测的地址范围，选择在所述目标运行过程中记录的访存操作。

10.一种记录访存操作信息的装置，其特征在于，包括：

访存操作记录单元，用于记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据；

数据组织单元，用于根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态，

其中所述终止存储状态为所述处理器在所述目标运行过程中所操作的存储空间的最终存储状态。

11.根据权利要求10所述的装置，其特征在于，所述数据组织单元包括：第一访存操作信息获取模块、第一处置模块、第一缓冲器及终止存储状态获取模块；其中，

所述第一访存操作信息获取模块，用于获取所述访存序列信息中的第一访存操作信息；

所述第一处置模块，用于当所述第一访存操作信息的访存类型为写操作时，将所述第一访存操作信息写入第一缓冲器；

所述终止存储状态获取模块，用于从所述第一缓冲器中获取所述终止存储状态。

12.根据权利要求11所述的装置，其特征在于，所述第一处置模块用于：

确定所述第一缓冲器中是否记载有所述第一访存操作信息的访存地址；

当所述第一缓冲器中已记载所述第一访存操作信息的访存地址时，将所述第一访存操作信息写入所述第一缓冲器以覆盖先前的访存操作信息；

当所述第一缓冲器中未记载所述第一访存操作信息的访存地址时，将所述第一访存操作信息插入所述第一缓冲器。

13.根据权利要求11或12中所述的装置，其特征在于，还包括：

首次读操作获取单元，用于从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息；

所述首次读操作对应的访存操作信息中的访存数据用于作为检测装置的输入信息或初始运行状态，使所述检测装置以符合预定义行为的方式执行所述目标运行过程中的任务，所述预定义行为是是处理器的硬件行为标准。

14.根据权利要求13所述的装置，其特征在于，所述首次读操作获取单元包括：第二访存操作信息获取模块、第二处置模块、第二缓冲器及首次读操作获取模块；其中，

所述第二访存操作信息获取模块，用于获取所述访存序列信息中的第二访存操作信息；

所述第二处置模块，用于当所述第二访存操作信息的访存类型为读操作时，将所述第二访存操作信息写入第二缓冲器；

所述首次读操作获取模块，用于从所述第二缓冲器中获取所述首次读操作对应的访存操作信息。

15.根据权利要求14所述的装置，其特征在于，还包括：判断单元、同步单元、输出数据获取单元及安全判断单元；其中，

所述判断单元，用于当所述第二访存操作信息的访存类型为读操作时，确定所述第一缓冲器中是否记载有所述第二访存操作信息的访存地址；

所述同步单元，用于当所述第一缓冲器中未记载所述第二访存操作信息的访存地址时，将所述第二访存操作信息写入第一缓冲器；

所述输出数据获取单元，在所述检测装置执行所述目标运行过程中的任务时，用于将所述检测装置的输出数据写入所述第二缓冲器；

所述安全判断单元，用于依次遍历比较所述第二缓冲器与所述第一缓冲器中相同访存地址的访存数据及访存类型，确定所述处理器是否安全。

16.根据权利要求15所述的装置，其特征在于，在所述检测装置执行所述目标运行过程中的任务时，所述输出数据获取单元将检测装置的输出数据写入所述第二缓冲器；

所述判断单元还用于确定所述第一缓冲器中是否记载有所述输出数据的访存地址；

当所述第一缓冲器中已记载所述输出数据的访存地址时，所述安全判断单元还用于根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全。

17.根据权利要求16所述的装置，其特征在于，当所述第一缓冲器中已记载所述输出数据的访存地址时，所述安全判断单元根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全，包括：

遍历所述第一缓冲器中的访存操作信息，确定所述第二缓冲器是否记载有相同访存地址对应的相同访存数据；

当所述第二缓冲器中已记载相同访存地址对应的相同访存数据时，确定所述处理器安全；

当所述第二缓冲器中未记载相同访存地址对应的相同访存数据时，确定所述处理器不

安全。

18.根据权利要求10至12中任一项所述的装置,其特征在于,

所述访存操作记录单元还用于,获取待检测的地址范围,并根据所述待检测的地址范围,选择在所述目标运行过程中记录的访存操作。

记录访存操作信息的方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种记录访存操作信息的方法及装置。

背景技术

[0002] 随着网络信息化等新技术的大规模应用，信息安全成为日益严峻的问题。人们通常讨论的信息安全都局限于网络安全、软件安全等方面，但是随着近年来研究表明，硬件安全也应受到关注。

[0003] 硬件设计的规模随着硬件设计水平的提升日渐提升，使得硬件木马成为可能：在当前以CPU(中央处理器)为代表的大规模电路中，用到的硬件IP(知识产权)的来源多样化，硬件设计的流程复杂化，设计制造流程分工细化等因素造成了硬件最终产品的安全可控性下降。在设计中被注入恶意木马或者漏洞(下文简称木马)的可能性增加，同时硬件规模的增加也增加了木马被识别和发现的困难。近年来，随着信息安全概念的发展，硬件的安全性逐渐成为信息安全的研究热点。

[0004] 因此，在检测硬件安全性的过程中，如何设计方案以降低软硬件开销成为了重要课题。

发明内容

[0005] 为解决现有技术中的上述问题，本发明的一个目的在于提出一种记录访存操作信息的方法及装置，使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。

[0006] 本发明实施例一方面提供了一种记录访存操作信息的方法，该方法包括：

[0007] 记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据；

[0008] 根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态。

[0009] 本发明实施例另一方面还提供了一种记录访存操作信息的装置，该装置包括：

[0010] 访存操作记录单元，用于记录目标运行过程中所述处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据；

[0011] 数据组织单元，用于根据所述目标运行过程的访存序列信息，确定存储器在所述目标运行过程的终止存储状态。

[0012] 根据本发明的上述实施例，记录目标运行过程中处理器与存储器之间的访存操作，并借由访存序列信息确定处理器的终止运行状态。这样，仅使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。

附图说明

[0013] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0014] 图1为本发明实施例提供的记录访存操作信息的方法的流程图；

[0015] 图2为本发明实施例确定终止存储状态的流程图；

[0016] 图3为本发明一实施例的基于访存操作信息确定处理器是否安全的流程示意图；

[0017] 图4为本发明另一实施例的基于访存操作信息确定处理器是否安全的流程示意图；

[0018] 图5为本发明实施例提供的记录访存操作信息的装置的结构示意图；

[0019] 图6为本发明实施例数据组织单元502的结构示意图；

[0020] 图7为本发明实施例基于访存操作信息确定处理器安全性的装置的结构示意图；

[0021] 图8为本发明实施例首次读操作获取单元503的结构示意图；

[0022] 图9为本发明另一实施例基于访存操作信息确定处理器安全性的装置的结构示意图；

[0023] 图10为本发明实施例的电子设备的系统构成的示意框图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0025] 硬件安全是软件安全的基石。所有的软件安全实现方法都是基于硬件可信的假设，即硬件应该按照其手册所定义的行为进行工作。目前大多情况是在设计环节、出厂环节对硬件进行检测，由于硬件出场后是以黑盒子的面目出现在用户的系统中(不像软件木马，其代码是存在于系统中的，可以被读取和分析)，硬件的行为是很难监控或感知的。此外，由于难以判断硬件行为的合理性，目前很少针对硬件安全性的研究。发明人发现，在处理器安全检测过程中，存储器的存储状态是重要指标之一。为获得存储器镜像，最简单的方法是拷贝整个存储器的内容，进而获得检测区间中存储器的存储状态。但是，这种方式效率很低，并且占用了较多的资源。

[0026] 本发明提出的记录访存操作信息的方法和装置，记录目标运行过程中处理器与存储器之间的访存操作，并借由访存序列信息确定处理器的终止运行状态。这样，仅使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。本发明实施例中记录访存操作信息的方法可以由记录访存操作信息的装置执行。应理解的是，记录访存操作信息的装置可以实现为检测装置(基于访存操作信息确定处理器安全性的装置)的一部分。具体地，该装置可以与处理器集成在同一个芯片上，也可以实现为独立的芯片，还可以实现为其它的装置形式，本发明对此不作限定。例如，可以将本发明实施例的一部分功能与被测处理器集成在同一个芯片上，而剩余的其它功能实现为独立的一个或多个

芯片，这些变化例都应落入本发明的保护范围。

[0027] 图1为本发明一实施例的记录访存操作信息的方法的流程示意图。如图1所示，该方法包括：

[0028] 步骤S101，记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据。

[0029] 通常地，此处所述的存储器包括片上存储器和片外存储器，片上存储器例如可以是处理器芯片的内存等，片外存储器例如可以是硬盘、U盘和内存等，本发明并不作限制。应理解的是，访存类型包括读操作和写操作，访存地址是指本次访存操作的地址，访存数据是指本次访存操作所读取的数据或写入的数据。

[0030] 步骤S102，根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态。其中，在一个实施例中，所述终止存储状态可以用于确定所述处理器在所述目标运行过程中是否安全。例如，检测装置可以根据存储器的终止存储状态确定处理器在目标运行过程中是否安全。

[0031] 应理解的是，本发明提出记录访存操作信息的方法及装置不仅可以应用到上述硬件安全检测领域，只要不脱离本发明的精神和宗旨，即使应用到其它技术领域也应落在本发明的保护范围内。

[0032] 应理解的是，存储器在目标运行过程中的终止存储状态是指，处理器在目标运行过程中所操作的存储空间的最终存储状态。处理器所操作的存储空间可以包括只读存储空间、只写存储空间，以及既读又写的存储空间。其中，只读存储空间是指处理器在目标运行过程中仅对该存储空间执行了读操作。同理，只写存储空间是指处理器在目标运行过程中仅对该存储空间执行了写操作，而既读又写的存储空间是指处理器在目标运行过程中对该存储空间既执行了读操作又执行了写操作。在一个实施例中，终止存储状态可以仅包括只写存储空间以及既读又写的存储空间中的最终存储状态。在另一实施例中，终止存储状态可以包括只读存储空间、只写存储空间，以及既读又写的存储空间中的最终存储状态。

[0033] 还应理解的是，可以根据存储器的终止存储状态得到处理器的最后一次写操作。例如，当终止存储状态仅包括只写存储空间以及既读又写的存储空间中的最终存储状态时，终止存储状态等于处理器的最后一次写操作。具体地，访存序列信息中的各项访存操作信息的排序可以表示各项访存操作的时间先后。这样，依据各访存操作的时间先后，依次遍历各项访存操作信息，可以得到存储器的终止存储状态。或者说，可以得到处理器对各存储空间的最后一次写操作，进而使用终止存储状态/最后一次写操作来判断处理器是否安全。

[0034] 在一个实施例中，确定处理器是否安全时，可以将被测处理器的运行过程划分为一个或多个检测区间。例如，可以将被测处理器从开机到关机的整个运行过程作为一个目标运行过程，也可以将整个运行过程划分为多个检测区间对应的多个目标运行过程。这样，在确认处理器的安全性时，可以实现为对处理器在某一检测区间中的运行过程(即，目标运行过程)的安全性检测。

[0035] 在一个实施例中，根据所述目标运行过程的访存序列信息，获取所述存储器在所述目标运行过程的终止存储状态时，可以按照图2所示步骤获取：

[0036] 步骤S201，从所述访存序列信息中获取第一访存操作信息。应理解的是，此处的第

一访存操作信息为一种代称，可以用以代指访存序列信息中的任意一项访存操作信息。

[0037] 步骤S202，当该第一访存操作信息的访存类型为写操作时，将该第一访存操作信息写入一缓冲器。为与后面的缓冲器以示区别，将此处的缓冲器记为第一缓冲器。

[0038] 步骤S203，依次遍历访存序列中的各项访存操作信息，在将所述访存序列信息中的所有写操作对应的访存操作信息写入第一缓冲器后，可以从第一缓冲器中获取所述终止存储状态。

[0039] 在上述实施例中，步骤S202中将第一访存操作信息写入第一缓冲器时，可以不将写操作对应的访存操作信息与第一缓冲器中的内容作比较，而直接写入到第一缓冲器中，这种情况可能导致第一缓冲器中记录的信息量变大。例如，同一个地址可能对应多条访存记录。这样，在获取终止存储状态时需要获取同一个地址中最后一条写入操作的内容。

[0040] 而对同一访存地址，只需要取用最后一条记录即可。因此，在将写操作对应的访存操作信息写入第一缓冲器时，可以先与第一缓冲器中记录的内容作比较，通过覆盖或插入的方式写入第一缓冲器。这样可以保证第一缓冲器中同一个地址对应一条记录，减少了第一缓冲器中记录的信息量。

[0041] 在一个实施例中，当第一访存操作信息的访存类型为写操作，在将该第一访存操作信息写入第一缓冲器时，通常先确定第一缓冲器中是否记载有该第一访存操作信息的访存地址。如果第一缓冲器中已记载该第一访存操作信息的访存地址，则将该第一访存操作信息写入第一缓冲器以覆盖先前的访存操作信息；如果第一缓冲器中未记载该第一访存操作信息的访存地址，则将该第一访存操作信息插入第一缓冲器。

[0042] 在一个实施例中，根据步骤S101中得到的访存序列信息，获取所述目标运行过程中所涉及的访存地址的首次读操作对应的访存操作信息，然后将各访存地址的首次读操作对应的访存操作信息中的访存数据作为检测装置的输入信息或初始运行状态，使所述检测装置以符合预定义行为的方式执行所述目标运行过程中的任务。应理解的是，首次读操作是针对同一地址而言的，不同地址的首次读操作不同。例如，对于某一特定存储地址而言，处理器可能有多次读操作，其中的第一次读操作是本发明所称的首次读操作。

[0043] 所述预定义行为是处理器的硬件行为标准，其中硬件行为标准是指在解析与执行软件指令流的过程中处理器的行为标准。在一个实施例中，处理器的硬件行为标准可以是处理器说明书或其它规范化文档中规定的行为标准。例如，对于指令集处理器而言，预定义行为可以包括：处理器所实现的指令集中规定的指令行为，对中断的响应和处理行为，以及处理器的输入输出端口的行为等行为。在一个实施例中，可以预先根据处理器的硬件行为标准设计检测装置中的处理器，进而使检测装置在运行过程中符合预定义行为。

[0044] 由于被测处理器对于用户来说是个黑盒子，它在实际运行过程中是否以符合预定义行为的方式来执行目标运行过程中的任务是未知的。因此，比较在执行相同任务时被测处理器与检测装置两者的硬件执行轨迹的异同，是判断硬件安全性的重要依据。其中，预定义行为是可以被用户所定义和修改的，具有很好的可移植性，可以应用于不同型号处理器的安全检测，解决了处理器硬件黑盒的难题。

[0045] 在一个实施例中，从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息时，可以先从所述访存序列信息中获取第二访存操作信息。然后，判断该第二访存操作信息的访存类型是否为读操作；如果是读操作，则将该第二访存操作信息

写入一缓冲器，此处记为第二缓冲器。这样，在检测装置执行目标运行过程中的任务时，可以从所述第二缓冲器中获取首次读操作的访存数据，以作为输入信息。或者说，检测装置获取该首次读操作作为检测区间的初始运行状态。应理解的是，此处的第二访存操作信息与上述的第一访存操作信息都是代称，它们可以指向同一个访存操作信息。还应理解的是，检测装置可以实时地从第二缓冲器中获取首次读操作的访存数据，而不必等到目标运行过程结束。

[0046] 在一个实施例中，由于检测装置的输入信息为首次读操作对应的访存操作信息中的访存数据，因此从第二缓冲器中获取所述首次读操作对应的访存操作信息时，可以只读取各个首次读操作对应的访存操作信息中的访存数据，而不必读取各个首次读操作对应的访存操作信息中的访存地址和访存类型。

[0047] 在一个实施例中，在第二访存操作信息的访存类型为读操作时，可以先判断第二缓冲器中是否已记载有与该第二访存操作信息相同的信息，如果已记载与该读操作对应的访存操作信息相同的访存操作信息，那么可以将该第二读操作对应的访存操作信息丢弃，不再写入第二缓冲器。

[0048] 在一个实施例中，在记录访存操作信息之后，检测装置基于访存操作信息对上述处理器进行安全性检测时，该方法还包括以下步骤(见图3)：

[0049] 步骤S301，当第二访存操作信息的访存类型为读操作时，还要确定第一缓冲器中是否记载有所述第二访存操作信息的访存地址。

[0050] 步骤S302，当第一缓冲器中未记载所述第二访存操作信息的访存地址时，将所述第二访存操作信息写入第一缓冲器。当第一缓冲器中已记载所述第二访存操作信息的访存地址时，可将所述第二访存操作信息丢弃(步骤S303)。

[0051] 总结地说，可以依次遍历访存序列信息中的各项访存操作信息，如果为写操作将其写入第一缓冲器。如果为读操作将其写入第二缓冲器，同时判断第一缓冲器中是否记载有对应的访存地址，如果没有的话还要将其写入第一缓冲器。

[0052] 步骤S304，在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器。这样，第二缓冲器不仅用于存储访存操作信息，还可以被检测装置复用，以存储检测装置的输出信息，因此节省了存储资源。应理解的是，检测装置也可将输出数据写入到其它存储器中，本发明实施例的保护范围并不限于此。

[0053] 在执行步骤S304之前，第二缓冲器中已经记载了访存序列信息中访存操作类型为读操作的访存操作信息。因此，将检测装置的输出数据写入第二缓冲器时，如果第二缓冲器中记载了与输出数据的访存地址(写入地址)相同的访存操作，那么将输出数据写入第二缓冲器时，会覆盖第二缓冲器先前记载的内容。而如果第二缓冲器中未记载与输出数据的访存地址(写入地址)相同的访存操作，可以在第二缓冲器中增加写入地址项，进而将输出数据插入至第二缓冲器中。在利用本发明实施例确定所述处理器在所述目标运行过程中是否安全时，可以按照步骤S305进行判断。

[0054] 步骤S305，依次遍历比较所述第二缓冲器与所述第一缓冲器中相同访存地址的访存数据及访存类型，确定所述处理器是否安全。例如，可以先判断第二缓冲器与第一缓冲器中是否记载了相同的访存地址，如果没有记载相同的访存地址，则认为处理器不安全(步骤S306)。如果两个缓冲器中记载的访存地址相同，则还需要判断各访存地址对应的访存操作

信息中的访存数据及访存类型是否一致，如果存在不一致的情况，则认为处理器不安全(步骤S307)。例如，还可以将第一缓冲器作为比较基准，依次遍历比较第二缓冲器中所记载的各项访存操作信息的访存地址、访存数据及访存类型是否与第一缓冲器一致。如有不一致的情况，则认为处理器不安全。如果完全一致，则认为处理器安全。

[0055] 应理解的是，本说明书中所认定的处理器安全是一个暂时安全的概念。通常地，检测处理器是否安全时，需要对处理器的多项参数进行比较。这种情况下，本说明书中所认定的“处理器安全”是一个暂态的安全，需要比较完所有的参数时，才能最终确定处理器是安全的。下面举例说明完备的处理器安全检测过程。

[0056] 根据处理器在目标运行过程的初始运行状态信息设置检测装置的初始运行状态，将处理器在目标运行过程中的输入信息作为检测装置的输入信息。使检测装置以符合预定义行为的方式执行目标运行过程中的任务，得到检测装置的输出信息和/或终止运行状态信息。其中，预定义行为是处理器的硬件行为标准。根据检测装置的输出信息和/或终止运行状态信息，确定处理器在目标运行过程中是否安全。目标运行过程的初始运行状态信息为，所述目标运行过程起始处特征状态集合对应的存储器中存储的数据。所述目标运行过程的终止运行状态信息为，所述目标运行过程终止处特征状态集合对应的存储器中存储的数据。其中，根据所述目标运行过程的当前运行状态、输入信息以及所述特征状态集合，能够确定所述目标运行过程的输出信息与下一运行状态。

[0057] 其中，本发明所称的存储器的终止存储状态可用于表示处理器对存储器的最后一次写操作，因此相当于处理器的输出信息。这样，图3所示的安全检测方法是根据输出信息确定处理器是否安全的一个具体实施例。可选地，可以实时地根据输出信息判断处理器是否安全，也可以在检测装置执行完目标运行过程中的任务时，再根据输出信息判断处理器是否安全。那么，在检测装置执行完目标运行过程中的任务时，需要比较完输出信息和终止运行状态，才能最终确定处理器是安全的。

[0058] 在另一个实施例中，在检测装置对上述处理器进行安全性检测时，作为图3所示实施例的替换实现方式，其与图3所示实施例相比，不需要将读操作类型的访存操作信息写入第一缓冲器。例如，在依次遍历访存序列信息中的各项访存操作信息时，如果为写操作将其写入第一缓冲器。如果为读操作将其写入第二缓冲器，但不需要判断第一缓冲器中是否记载有对应的访存地址并将其写入第一缓冲器。这种情况下，该方法还包括以下步骤(见图4)：

[0059] 步骤S401，在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器。

[0060] 步骤S402，确定所述第一缓冲器中是否记载有所述输出数据的访存地址。

[0061] 其中，检测装置的输出数据可能携带除访存类型和访存数据以外的其它信息，在将其写入第二缓冲器时，需保证该输出数据与第二缓冲器的存储格式相同，例如从该输出数据中至少提取出访存类型和访存数据写入第二缓冲器。

[0062] 当第一缓冲器中已记载所述输出数据的访存地址时，根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全，具体操作见步骤S403。当第一缓冲器中未记载所述输出数据的访存地址时，则认为所述处理器不安全(步骤S404)。也就是说，当第一缓冲器中未记载所述输出数据的访存地址时，表明被测处理器比检测装置少写入了

数据，此时可认定被测处理器不安全。

[0063] 步骤S403，遍历第一缓冲器中的访存操作信息，确定所述第二缓冲器是否记载有相同访存地址对应的相同访存数据。当所述第二缓冲器中已记载相同访存地址对应的相同访存数据时，确定所述处理器安全(步骤S405)。而当所述第二缓冲器中未记载相同访存地址对应的相同访存数据时，确定所述处理器不安全(步骤S404)。

[0064] 从上述实施例可以看出，若第一缓冲器中的访存地址和访存数据与第二缓冲器中的访存地址和访存数据一致时，确定所述处理器安全。当第二缓冲器中未记载与第一缓冲器中相同的访存地址或者其中的访存数据不同时，判定处理器不安全。

[0065] 在一个实施例中，在记录目标运行过程中所述处理器与存储器之间的访存操作之前，获取待检测的地址范围。这种情况下，根据所述待检测的地址范围，选择在所述目标运行过程中记录的访存操作。其中，待检测的地址范围可由用户自定义，并预先存储在检测装置或其它检测装置可读取的位置。这样，用户可以根据安全检测的需要自定义安全检测的存储器范围，提高了检测效率和灵活性。

[0066] 利用本发明提出的记录访存操作信息的方法和装置，记录目标运行过程中处理器与存储器之间的访存操作，并借由访存序列信息确定处理器的终止运行状态。这样，仅使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。

[0067] 此外，根据本发明的上述实施例，通过记录目标运行过程中处理器与存储器之间的访存操作，并根据所获得的存储器的终止存储状态确定处理器在目标运行过程中是否安全，可以有效检验处理器在目标运行过程中的行为是否有异常，降低硬件安全检测的难度，提高硬件使用的安全性。同时，检测内容可以由用户自定义设置，具有很好的可移植性，能够应用于不同型号处理器的硬件安全检测，解决了处理器硬件黑盒的难题，降低了检测难度。

[0068] 基于与图1所示的记录访存操作信息的方法相同的发明构思，本发明实施例还提供了一种记录访存操作信息的装置，具体如下面实施例所述。由于该装置解决问题的原理与图1中的方法相似，因此该装置的实施可以参见图1所示方法的实施，重复之处不再赘述。

[0069] 如图5所示实线部分，本发明实施例还提供了一种记录访存操作信息的装置，其主要包括访存操作记录单元501和数据组织单元502。其中，访存操作记录单元501用于记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据。数据组织单元502用于根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态。所述终止存储状态用于确定所述处理器在所述目标运行过程中是否安全。

[0070] 本发明实施例中的访存操作记录单元501可以设置在处理器与存储器之间，也可以设置在处理器芯片上，本发明不做限制。为方便描述，在图5中将检测装置作为独立的单元示出。应理解的是，访存操作记录单元501和数据组织单元502可以实现为检测装置的一部分，与检测装置的其它部分协作完成安全检测过程。同理，下文中所述的各个单元都可实现为检测装置的一部分。

[0071] 在一个实施例中，数据组织单元501的结构如图6所示(图中实线部分)，包括：第一访存操作信息获取模块601、第一处置模块602、第一缓冲器603及终止存储状态获取模块

604。第一访存操作信息获取模块601用于获取所述访存序列信息中的第一访存操作信息；第一处置模块602用于当所述第一访存操作信息的访存类型为写操作时，将所述第一访存操作信息写入第一缓冲器603；终止存储状态获取模块604，用于从所述第一缓冲器中获取所述终止存储状态。

[0072] 在一个实施例中，上述的第一处置模块602用于确定第一缓冲器603中是否记载有所述第一访存操作信息的访存地址，并当第一缓冲器603中已记载所述第一访存操作信息的访存地址时，将第一访存操作信息写入第一缓冲器603中，以覆盖先前的访存操作信息；当第一缓冲器603中未记载所述第一访存操作信息的访存地址时，将第一访存操作信息插入第一缓冲器603中。

[0073] 在一个实施例中，图5所示的装置还包括一首次读操作获取单元503(详见图7)，用于从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息。其中，所述首次读操作对应的访存操作信息中的访存数据可作为检测装置的输入信息或初始运行状态，使检测装置以符合预定义行为的方式执行所述目标运行过程中的任务。所述预定义行为是是处理器的硬件行为标准。在另一场景中，当存储器与处理器集成在一起时，首次读操作对应的访存数据可以作为检测装置初始运行状态的一部分。

[0074] 在一个实施例中，首次读操作获取单元503的结构如图8中的实线部分所示，包括：第二访存操作信息获取模块801、第二处置模块802、第二缓冲器803以及首次读操作获取模块804。其中，第二访存操作信息获取模块801用于获取所述访存序列信息中的第二访存操作信息；第二处置模块802用于当所述第二访存操作信息的访存类型为读操作时，将所述第二访存操作信息写入第二缓冲器803；首次读操作获取模块804用于从所述第二缓冲器中获取所述首次读操作对应的访存操作信息。

[0075] 在一个实施例中，记录访存操作信息的装置还包括一判断单元504、同步单元505、输出数据获取单元506及安全判断单元507，其结构如图9所示。

[0076] 其中，判断单元504用于当第二访存操作信息的访存类型为读操作时，确定第一缓冲器603中是否记载有第二访存操作信息的访存地址；同步单元505用于当所述第一缓冲器中未记载所述第二访存操作信息的访存地址时，将第二访存操作信息写入第一缓冲器；在上述检测装置执行所述目标运行过程中的任务时，输出数据获取单元506用于将所述检测装置的输出数据写入第二缓冲器803；安全判断单元507用于依次遍历比较第二缓冲器803与第一缓冲器603中相同访存地址的访存数据及访存类型，确定处理器是否安全。

[0077] 在一个实施例中，在检测装置执行所述目标运行过程中的任务，输出数据获取单元506将检测装置的输出数据写入第二缓冲器803时，判断单元504还用于确定第一缓冲器603中是否记载有所述输出数据的访存地址，并在第一缓冲器603中已记载所述输出数据的访存地址时，利用安全判断单元507根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全。

[0078] 在一个实施例中，利用安全判断单元507根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全时，可以遍历第一缓冲器603中的访存操作信息，并确定第二缓冲器803是否记载有相同访存地址对应的相同访存数据，当第二缓冲器803中已记载相同访存地址对应的相同访存数据时，确定处理器安全；当第二缓冲器803中未记载相同访存地址对应的相同访存数据时，确定处理器不安全。

[0079] 在一个实施例中，访存操作记录单元501还用于，获取待检测的地址范围，并根据所述待检测的地址范围，选择在所述目标运行过程中记录的访存操作。

[0080] 本发明提出的记录访存操作信息的方法和装置，记录目标运行过程中处理器与存储器之间的访存操作，并借由访存序列信息确定处理器的终止运行状态。这样，仅使用较少的存储资源就可获得存储器在目标运行过程中的终止存储状态，降低了硬件开销。

[0081] 此外，本发明的上述实施例通过记录目标运行过程中处理器与存储器之间的访存操作，并根据所获得的存储器的终止存储状态确定处理器在目标运行过程中是否安全，可以有效检验处理器在目标运行过程中的行为是否有异常，降低硬件安全检测的难度，提高硬件使用的安全性。同时，检测内容可以由用户自定义设置，具有很好的可移植性，能够应用于不同型号处理器的硬件安全检测，解决了处理器硬件黑盒的难题，降低了检测难度。

[0082] 应理解的是，本发明所称的缓冲器可以实现为任何类型的存储器，本发明实施例并不限于此。

[0083] 本发明实施例还提供了一种电子设备，该电子设备可以是台式计算机等，本实施例不限于此。在本实施例中，该电子设备可以参照图1所示方法的实施及图5所示装置的实施，其内容被合并于此，重复之处不再赘述。

[0084] 图10为本发明实施例的电子设备的系统构成的示意框图。如图6所示，该电子设备可以包括处理器1001和存储器1002，存储器1002耦合至处理器1001。值得注意的是，该图是示例性的，还可以使用其他类型的结构来补充或替代该结构，以实现通信、检测功能或其他功能。

[0085] 在一个实施例中，记录目标运行过程中处理器与存储器之间的访存操作的功能可以被集成到处理器1001中。其中，处理器1001可以被配置为进行如下控制：记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息，所述访存序列信息中的各项访存操作信息包括访存类型、访存地址和访存数据；根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态。其中，在一个实施例中，所述终止存储状态用于确定所述处理器在所述目标运行过程中是否安全。

[0086] 其中，根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态，包括：获取所述访存序列信息中的第一访存操作信息；当所述第一访存操作信息的访存类型为写操作时，将所述第一访存操作信息写入第一缓冲器；从所述第一缓冲器中获取所述终止存储状态。

[0087] 其中，当第一访存操作信息的访存类型为写操作时，将第一访存操作信息写入第一缓冲器包括：确定所述第一缓冲器中是否记载有所述第一访存操作信息的访存地址；当所述第一缓冲器中已记载所述第一访存操作信息的访存地址时，将所述第一访存操作信息写入所述第一缓冲器以覆盖先前的访存操作信息；当所述第一缓冲器中未记载所述第一访存操作信息的访存地址时，将所述第一访存操作信息插入所述第一缓冲器。

[0088] 其中，处理器1001还可以被配置为进行如下控制：从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息；将所述首次读操作对应的访存操作信息中的访存数据作为检测装置的输入信息或初始运行状态信息，使所述检测装置以符合预定义行为的方式执行所述目标运行过程中的任务，所述预定义行为是是处理器的硬件行为标准。

[0089] 其中，从所述访存序列信息中获取所述目标运行过程中的首次读操作对应的访存操作信息，包括：获取所述访存序列信息中的第二访存操作信息；当所述第二访存操作信息的访存类型为读操作时，将所述第二访存操作信息写入第二缓冲器；从所述第二缓冲器中获取所述首次读操作对应的访存操作信息。

[0090] 其中，处理器1001还可以被配置为进行如下控制：当所述第二访存操作信息的访存类型为读操作时，确定所述第一缓冲器中是否记载有所述第二访存操作信息的访存地址；当所述第一缓冲器中未记载所述第二访存操作信息的访存地址时，将所述第二访存操作信息写入第一缓冲器；在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器；依次遍历比较所述第二缓冲器与所述第一缓冲器中相同访存地址的访存数据及访存类型，确定所述处理器是否安全。

[0091] 其中，处理器1001还可以被配置为进行如下控制：在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器；确定所述第一缓冲器中是否记载有所述输出数据的访存地址；当所述第一缓冲器中已记载所述输出数据的访存地址时，根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全。

[0092] 其中，根据所述存储器在所述目标运行过程中的终止存储状态，确定所述处理器是否安全，包括：遍历所述第一缓冲器中的访存操作信息，确定所述第二缓冲器是否记载有相同访存地址对应的相同访存数据；当所述第二缓冲器中已记载相同访存地址对应的相同访存数据时，确定所述处理器安全；当所述第二缓冲器中未记载相同访存地址对应的相同访存数据时，确定所述处理器不安全。

[0093] 其中，处理器1001在被配置为记录目标运行过程中处理器与存储器之间的访存操作之前，还被配置为进行如下控制：获取待检测的地址范围；根据所述待检测的地址范围，选择在所述目标运行过程中记录的访存操作。

[0094] 在另一个实施例中，记录访存操作信息的装置可以与处理器1001分开配置，例如可以将记录访存操作信息的装置配置为与处理器1001连接的芯片，通过处理器1001的控制来实现对访存操作信息的记录。

[0095] 如图10所示，该电子设备还可以包括：输入单元1003、显示单元1004和电源1005。值得注意的是，该电子设备也并不是必须要包括图10中所示的所有部件。此外，电子设备还可以包括图10中没有示出的部件，可以参考现有技术。

[0096] 如图10所示，处理器1001有时也称为控制器或操作控件，可以包括微处理器或其他处理器装置和/或逻辑装置，该处理器1001接收输入并控制电子设备的各个部件的操作。

[0097] 其中，存储器1002例如可以是缓存器、闪存、硬驱、可移动介质、易失性存储器、非易失性存储器或其它合适装置中的一种或多种，可存储上述处理器1001的配置信息、处理器1001执行的指令、记录的访存序列信息等信息中的一种或多种。处理器1001可以执行存储器1002存储的程序，以实现信息存储或处理等。在一实施例中，存储器1002中还包括缓冲存储器，即缓冲器，以存储中间信息。

[0098] 输入单元1003例如可以为按键输入装置或触摸输入装置，用于向处理器1001提供输入。显示单元1004用于进行图像或文字等显示对象的显示，该显示单元例如可以为LCD显示器，但本发明并不限于此。电源1005用于向电子设备提供电力。

[0099] 本发明实施例还提供一种计算机可读指令，其中当在电子设备中执行所述指令时，所述程序使得电子设备执行如图1所示的记录访存操作信息的方法。

[0100] 本发明实施例还提供一种存储有计算机可读指令的存储介质，其中所述计算机可读指令使得电子设备执行如图1所示的记录访存操作信息的方法。

[0101] 应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0102] 还应理解，在本发明实施例中，术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系。例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0103] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0104] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0105] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口、装置或单元的间接耦合或通信连接，也可以是电的，机械的或其它的形式连接。

[0106] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本发明实施例方案的目的。

[0107] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0108] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0109] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

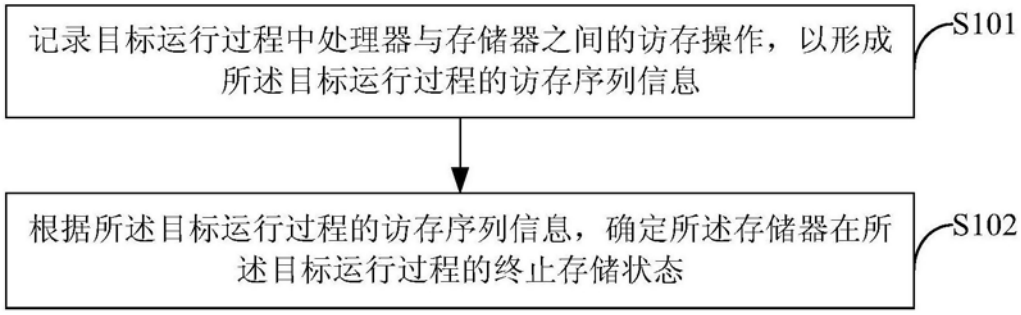

记录目标运行过程中处理器与存储器之间的访存操作，以形成所述目标运行过程的访存序列信息
S101
根据所述目标运行过程的访存序列信息，确定所述存储器在所述目标运行过程的终止存储状态
S102

图1

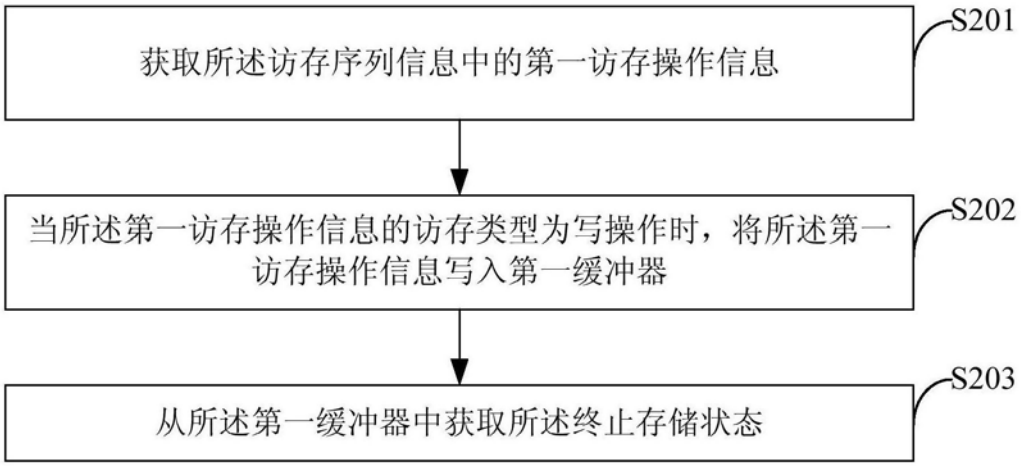

获取所述访存序列信息中的第一访存操作信息
S201
当所述第一访存操作信息的访存类型为写操作时，将所述第一访存操作信息写入第一缓冲器
S202
从所述第一缓冲器中获取所述终止存储状态
S203

图2

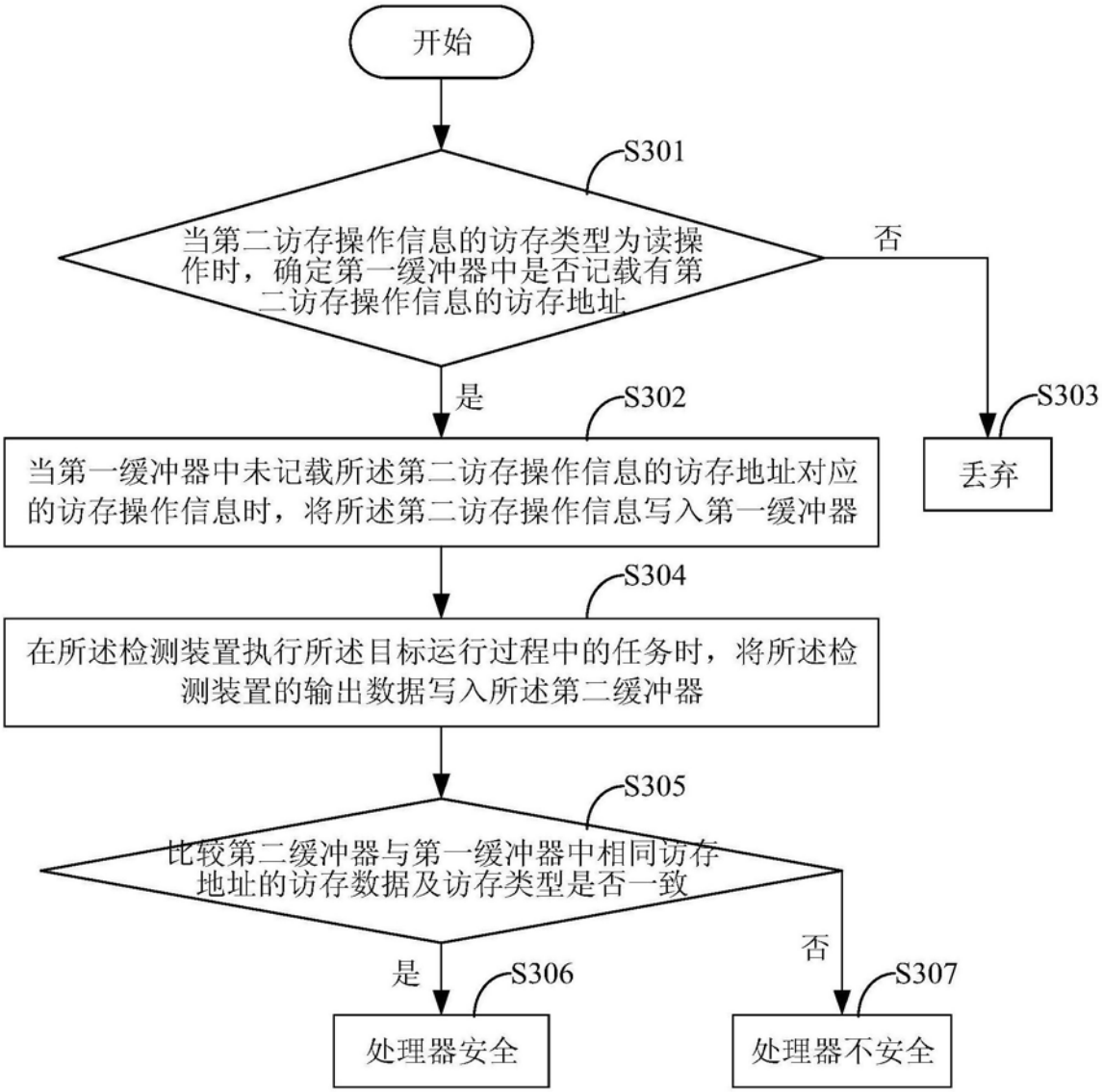

开始
S301
当第二访存操作信息的访存类型为读操作时，确定第一缓冲器中是否记载有第二访存操作信息的访存地址
否
是
S302
S303
当第一缓冲器中未记载所述第二访存操作信息的访存地址对应的访存操作信息时，将所述第二访存操作信息写入第一缓冲器
丢弃
S304
在所述检测装置执行所述目标运行过程中的任务时，将所述检测装置的输出数据写入所述第二缓冲器
S305
比较第二缓冲器与第一缓冲器中相同访存地址的访存数据及访存类型是否一致
否
是
S306
S307
处理器安全
处理器不安全

图3

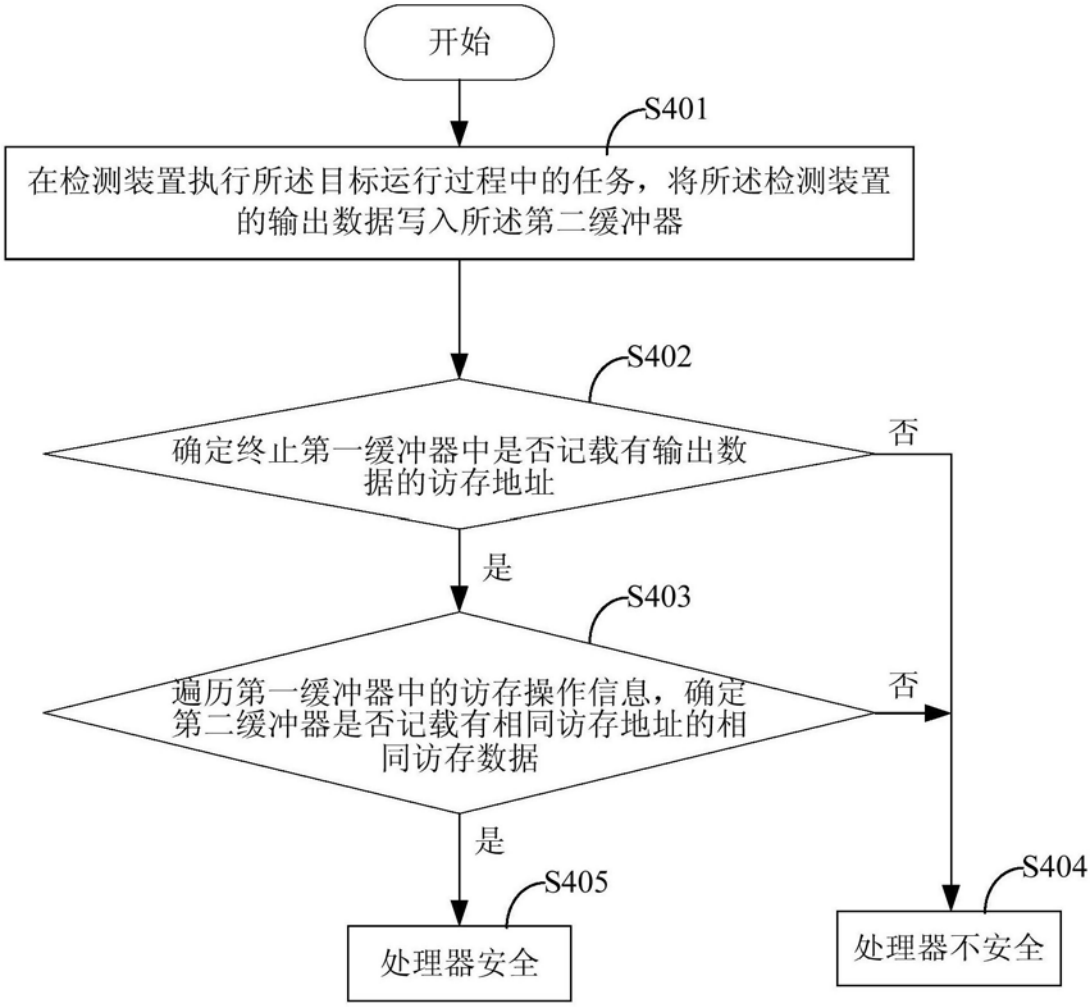

开始
S401
在检测装置执行所述目标运行过程中的任务，将所述检测装置的输出数据写入所述第二缓冲器
S402
确定终止第一缓冲器中是否记载有输出数据的访存地址
否
是
S403
遍历第一缓冲器中的访存操作信息，确定第二缓冲器是否记载有相同访存地址的相同访存数据
否
是
S405
处理器安全
S404
处理器不安全

图4

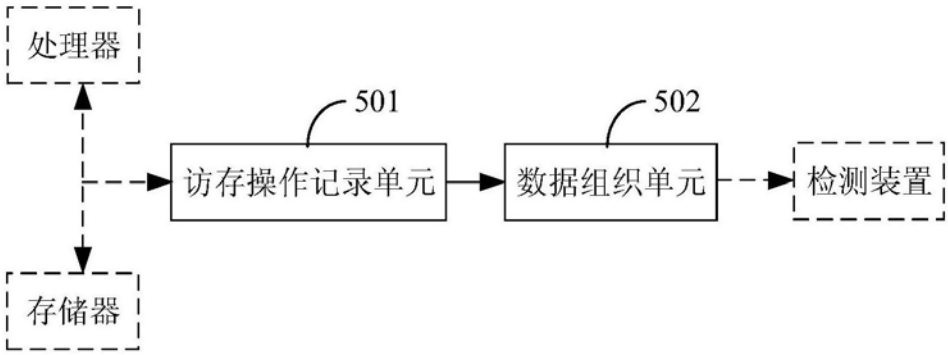

处理器
501
访存操作记录单元
502
数据组织单元
检测装置
存储器

图5

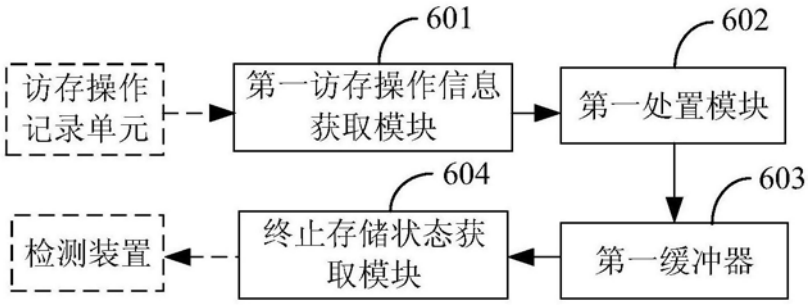

601
602
访存操作记录单元
第一访存操作信息获取模块
第一处置模块
604
603
检测装置
终止存储状态获取模块
第一缓冲器

图6

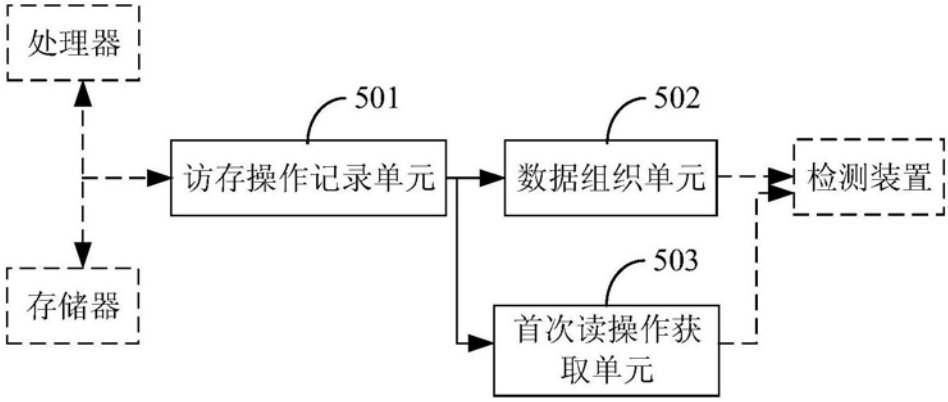

处理器
501
502
访存操作记录单元
数据组织单元
检测装置
503
存储器
首次读操作获取单元

图7

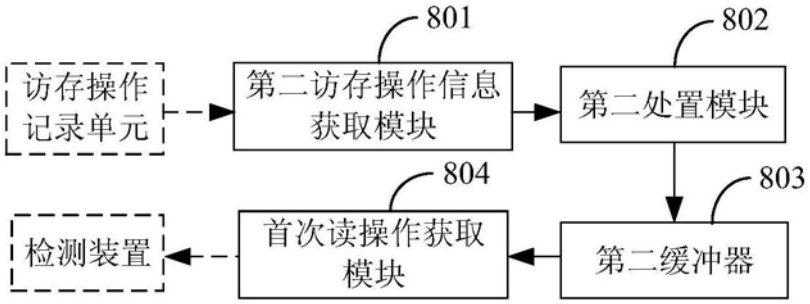

801
802
访存操作记录单元
第二访存操作信息获取模块
第二处置模块
804
803
检测装置
首次读操作获取模块
第二缓冲器

图8

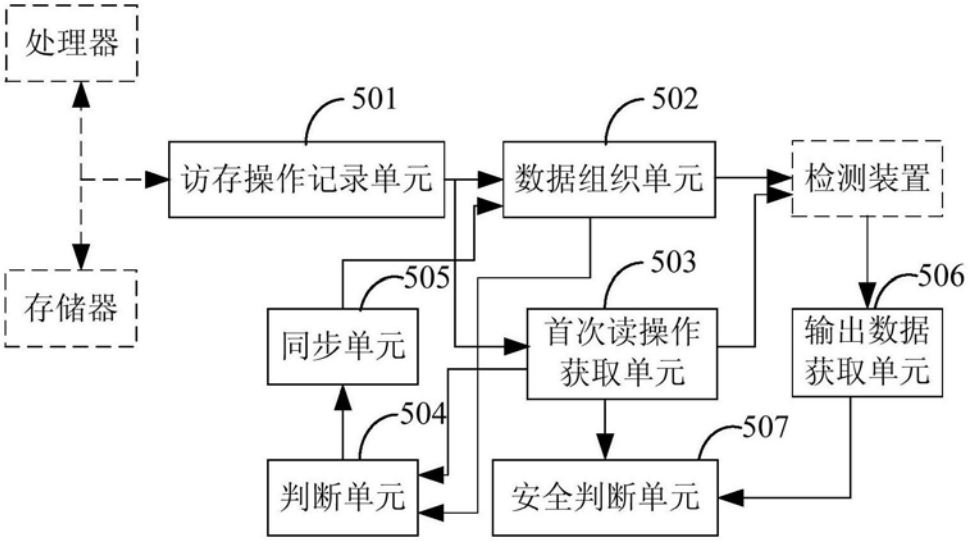

处理器
存储器
501
访存操作记录单元
502
数据组织单元
检测装置
505
同步单元
503
首次读操作
获取单元
506
输出数据
获取单元
504
判断单元
507
安全判断单元

图9

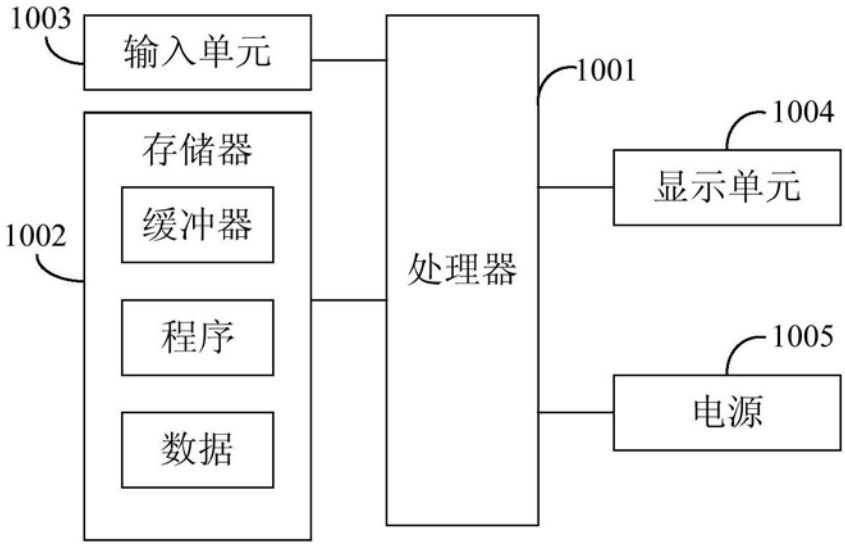

1003
输入单元
存储器
缓冲器
1002
程序
数据
处理器
1001
1004
显示单元
1005
电源

图10