(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 105027097 B
(45)授权公告日 2018.01.16

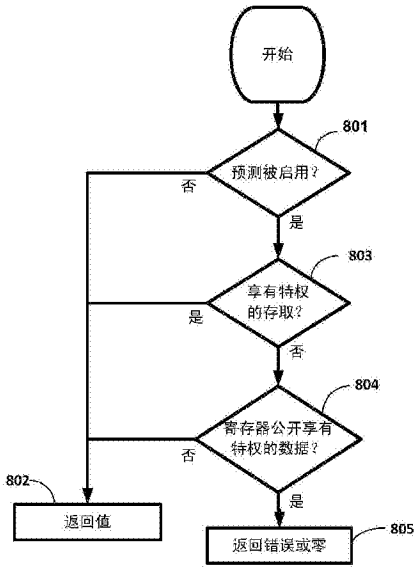
(21)申请号 201480011829.X
(22)申请日 2014.03.04
(65)同一申请的已公布的文献号
申请公布号 CN 105027097 A
(43)申请公布日 2015.11.04
(30)优先权数据
13/785,979 2013.03.05 US
(85)PCT国际申请进入国家阶段日
2015.09.01
(86)PCT国际申请的申请数据
PCT/US2014/020185 2014.03.04
(87)PCT国际申请的公布数据
WO2014/138005 EN 2014.09.12
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 T·曾 A·托兹尼 T·R·曾
P·J·博斯特利
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张立达 王英
(51)Int.Cl.
G06F 12/14(2006.01)
G06F 9/455(2006.01)
G06F 21/79(2013.01)
G06F 12/1027(2016.01)
(56)对比文件
US 2006206687 A1,2006.09.14,
US 2005125628 A1,2005.06.09,
WO 2011156021 A2,2011.12.15,
US 7124170 B1,2006.11.17,
CN 1278244 C,2006.10.04,
US 2007283123 A1,2007.12.06,
审查员 周静奇
权利要求书3页 说明书9页 附图8页

(54)发明名称

用于在某些情况下当执行硬件表移动(HWTW)时防止对寄存器的内容进行未授权的存取的方法和装置

(57)摘要

一种安全装置和方法具有安全算法，该安全算法防止对由于在硬件表移动期间执行预测算法而已经被加载到计算机系统的存储元件中的物理地址(PA)的内容进行未授权的访问，所述预测算法使用预测器基于虚拟地址(VA)来预测PA。当预测器被启用时，具有系统知识的人员可能配置预测器来使被存储在主存储器的安全部分的PA处的内容被加载到TLB中的寄存器中。以这种方式，不应当使用被存储在主存储器的安全部分中的内容的人员能够间接地获得对这些内容的未授权的存取。该装置和方法通过在某些情况下遮掩该内容来防止这样的对内容的未授权的存取。



CN 105027097 B

1.一种用于防止对在执行硬件表移动(HWTW)期间已经被加载到计算机系统的存储元件中的物理地址的内容进行未授权的存取的所述计算机系统的装置,所述装置包括:

内存管理单元(MMU),其被配置为当读事务指导所述MMU通过中间物理地址来定位物理地址时断言预测使能位,所述MMU还被配置为当在检查转换旁路缓冲器(TLB)时所述读事务的执行结果为未中时断言类别使能位;

预测器,其被配置为启用预测算法,所述预测算法将物理地址作为所述中间地址的函数和虚拟机标识符的函数进行预测,所述预测器被配置为响应于所述预测使能位和所述类别使能位来禁用HWTW控制逻辑单元;以及

安全逻辑单元,其被配置为当所述预测算法当前被启用时,防止所述存储元件的内容被无特权的实体存取。

2.根据权利要求1所述的装置,其中,所述存储元件是所述TLB的寄存器,如果所述预测算法当前被启用,则预测的物理地址的内容已经被加载到所述TLB的寄存器中,并且其中,所述安全逻辑单元包括:

第一判定逻辑单元,其确定所述预测算法当前被启用的时间,并且其中,所述第一判定逻辑单元还确定是享有特权的实体还是无特权的实体在尝试存取所述寄存器的内容,如果所述第一判定逻辑单元确定所述预测算法当前被启用并且享有特权的实体在尝试获得对所述寄存器的内容的存取,则所述第一判定逻辑单元输出第一判定,如果所述第一判定逻辑单元确定所述预测算法当前未被启用或者无特权的实体在尝试获得对所述寄存器的内容的存取,则所述第一判定逻辑单元输出第二判定;以及

选择逻辑单元,其被配置为如果所述第一判定逻辑单元输出所述第二判定,则利用掩码值来使所述寄存器的内容被盖写,如果所述第一判定逻辑单元输出所述第一判定,则所述选择逻辑单元被配置为保持所述寄存器的内容。

3.根据权利要求2所述的装置,其中,所述安全逻辑单元还包括:

第二判定逻辑单元,其被配置为确定所述物理地址是与主存储器的安全部分相对应还是与所述主存储器的非安全部分相对应,或者所述第一判定逻辑单元是输出所述第一判定还是输出所述第二判定,其中,如果所述第二判定逻辑单元确定所述物理地址与主存储器的安全部分相对应,则所述第二判定逻辑单元输出第一判定,并且其中,如果所述第二判定逻辑单元确定所述物理地址与主存储器的非安全部分相对应或所述第一判定逻辑单元输出所述第二判定,则所述第二判定逻辑单元输出第二判定;以及

其中,如果所述第二判定逻辑单元输出所述第一判定,则所述选择逻辑单元被配置为使所述寄存器的内容被遮掩,并且其中,如果所述第二判定逻辑单元输出所述第二判定,则所述选择逻辑单元被配置为保持所述寄存器的内容。

4.根据权利要求1所述的装置,其中,所述安全逻辑单元是所述计算机系统的所述MMU的一部分。

5.根据权利要求4所述的装置,其中,所述MMU是所述计算机系统的中央处理单元(CPU)的一部分。

6.根据权利要求5所述的装置,其中,所述CPU是所述计算机系统的CPU集群的一部分。

7.根据权利要求1所述的装置,其中,所述计算机系统是移动电话的一部分。

8.一种在计算机系统中被执行、用于防止对在执行硬件表移动(HWTW)期间已经被加载

到所述计算机系统的存储元件中的物理地址的内容进行未授权的存取的方法，所述方法包括：

提供预测器，所述预测器被配置为当内存管理单元(MMU)接收读事务时启用预测算法，所述预测算法将物理地址作为中间物理地址的函数和虚拟机标识符的函数进行识别，所述预测器还被配置为响应于当检查转换旁路缓冲器(TLB)时所述读事务的执行结果为未中，来禁用HWTW控制逻辑单元；以及

提供安全逻辑单元；

利用所述安全逻辑单元来防止所述存储元件的内容被无特权的实体存取。

9.根据权利要求8所述的方法，其中，所述存储元件是所述TLB的寄存器，如果所述预测算法当前被启用，则所预测的物理地址的内容已经被加载到所述TLB的寄存器中，并且其中，所述方法还包括：

利用所述安全逻辑单元的第一判定逻辑单元确定所述预测算法当前被启用的时间，并且其中，所述第一判定逻辑单元还确定是享有特权的实体还是无特权的实体在尝试存取所述寄存器的内容；

如果所述第一判定逻辑单元确定所述预测算法当前被启用并且享有特权的实体在尝试获得对所述寄存器的内容的存取，则利用所述第一判定逻辑单元输出第一判定；

如果所述第一判定逻辑单元确定所述预测算法当前未被启用或无特权的实体在尝试获得对所述寄存器的内容的存取，则利用所述第一判定逻辑单元输出第二判定；

如果所述第一判定逻辑单元输出所述第二判定，则通过利用掩码值使所述寄存器的内容被盖写来利用所述安全逻辑单元的选择逻辑单元防止所述寄存器的内容被存取；以及

如果所述第一判定逻辑单元输出所述第一判定，则利用所述选择逻辑单元来保存所述寄存器的内容。

10.根据权利要求9所述的方法，还包括：

利用所述安全逻辑单元的第二判定逻辑单元来确定所述物理地址是与主存储器的安全部分相对应还是与所述主存储器的非安全部分相对应，或者所述第一判定逻辑单元是输出所述第一判定还是输出所述第二判定；

如果所述第二判定逻辑单元确定所述物理地址与主存储器的安全部分相对应，则利用所述第二判定逻辑单元来从所述第二判定逻辑单元输出第一判定；

如果所述第二判定逻辑单元确定所述物理地址与主存储器的非安全部分相对应或所述第一判定逻辑单元输出所述第二判定，则利用所述第二判定逻辑单元从所述第二判定逻辑单元来输出第二判定；

如果所述第二判定逻辑单元输出所述第一判定，则利用所述选择逻辑单元来使所述寄存器的内容被遮掩；以及

如果所述第二判定逻辑单元输出所述第二判定，则利用所述选择逻辑单元来使所述寄存器的内容被保持。

11.根据权利要求8所述的方法，其中，所述安全逻辑单元是所述计算机系统的所述MMU的一部分。

12.根据权利要求11所述的方法，其中，所述MMU是所述计算机系统的中央处理单元(CPU)的一部分。

13.根据权利要求12所述的方法，其中，所述CPU是所述计算机系统的CPU集群的一部分。

14.根据权利要求8所述的方法，其中，所述计算机系统是移动电话的一部分。

15.一种非暂时性计算机可读介质，具有存储于其上以由计算机系统的一个或多个处理器执行的、用于防止对在执行硬件表移动(HWTW)期间已经被加载到所述计算机系统的存储元件中的物理地址的内容进行未授权的存取的计算机代码，所述计算机代码包括：

代码，其被配置为当内存管理单元(MMU)接收读事务时启用预测算法，所述预测算法将物理地址作为中间物理地址的函数和虚拟机标识符的函数进行识别，所述代码还被配置为响应于当检查转换旁路缓冲器(TLB)时所述读事务的执行结果为未中，来禁用HWTW控制逻辑单元；

第一计算机代码部分，用于确定所述预测算法当前是否被启用；以及

第二计算机代码部分，用于如果所述第一计算机代码部分确定所述预测算法当前被启用，则防止所述存储元件的内容被无特权的实体存取。

16.根据权利要求15所述的非暂时性计算机可读介质，其中，所述存储元件是所述TLB的寄存器，如果所述预测算法当前被启用，则所预测的物理地址的内容已经被加载到所述TLB的寄存器中，并且其中，所述第一计算机代码部分还确定是享有特权的实体还是无特权的实体在尝试存取所述寄存器的内容，并且其中，如果所述第一计算机代码部分确定所述预测算法当前被启用并且享有特权的实体在尝试获得对所述寄存器的内容的存取，则所述第一计算机代码部分输出第一判定，并且其中，如果所述第一计算机代码部分确定所述预测算法当前未被启用或者无特权的实体在尝试获得对所述寄存器的内容的存取，则所述第一计算机代码部分输出第二判定；并且其中，如果所述第一计算机代码部分输出所述第二判定，则所述第二计算机代码部分通过利用掩码值使所述寄存器的内容被盖写来防止所述寄存器的内容被存取；并且其中，如果所述第一计算机代码部分输出所述第一判定，则所述第二计算机代码部分使所述寄存器的内容被保持。

17.根据权利要求16所述的非暂时性计算机可读介质，其中，所述计算机可读介质是所述计算机系统的所述MMU的一部分。

18.根据权利要求17所述的非暂时性计算机可读介质，其中，所述MMU是所述计算机系统的中央处理单元(CPU)的一部分。

19.根据权利要求18所述的非暂时性计算机可读介质，其中，所述CPU是所述计算机系统的CPU集群的一部分。

用于在某些情况下当执行硬件表移动(HWTW)时防止对寄存器的内容进行未授权的存取的方法和装置

技术领域

[0001] 本发明涉及计算机系统，而更具体地说，涉及一种用于在某些情况下防止对在硬件表移动(HWTW)期间已经被加载到寄存器中的物理内存地址的内容进行未授权的存取的方法和装置。

背景技术

[0002] 现代计算机系统使用内存管理单元(MMU)来管理向一个或多个物理存储设备(诸如例如固态存储设备)写数据以及从一个或多个物理存储设备读取数据。计算机系统的MMU向计算机系统的中央处理单元(CPU) 提供虚拟内存，其允许CPU在其自己专用的、连续的虚拟内存地址空间上运行每一个应用程序，而不是使所有的应用程序共享物理内存地址空间，所述物理内存地址空间经常是成碎片的或非连续的。MMU的目的是针对 CPU将虚拟内存地址(VA)转化成物理内存地址(PA)。CPU通过直接地对MMU读和写VA来间接地读和写PA，所述MMU将VA转化成PA，并且然后写或读PA。

[0003] 为了执行该转化，MMU存取被存储在系统主存储器中的页表。该页表由页表的条目组成。该页表的条目是由MMU使用来将VA映射成PA的信息。MMU通常包括转换旁路缓冲器(TLB)，其是被用于缓存最近使用的映射的高速缓冲存储器单元。当MMU需要将VA转化成PA时，MMU首先检查TLB以确定是否存在针对该VA的匹配。如果有，则MMU使用在 TLB中找到的映射来计算PA，并且然后存取PA(即，读或写PA)。这被称为TLB“命中”。如果MMU没有在TLB中找到匹配，则这被称为TLB “未中”。

[0004] 在TLB未中事件中，MMU执行被称为硬件表移动(HWTW)的操作。HWTW是耗时的且计算上开销很高的过程，所述过程涉及执行“表移动”，以在MMU中查找相应的页表，并且在页表中读取多个位置，以查找相应的VA-至-PA的地址映射。然后，MMU使用该映射来计算相应的PA，并且将该映射写回到TLB。

[0005] 在实现操作系统(OS)虚拟化的计算机系统中，将虚拟内存监视器 (VMM)(通常还被称为系统管理程序)插入到计算机系统的硬件与计算机系统的系统OS之间。系统管理程序在特权模式下执行，并且能够主管一个或多个客户高级OS。在这样的系统中，运行在OS上的应用程序使用虚拟内存的第一层的VA来对内存寻址，以及运行在系统管理程序上的OS使用虚拟内存的第二层的中间物理地址(IPA)来对内存寻址。在MMU中，执行阶段1(S1)转化，以将每一个VA转化成IPA，以及执行阶段2(S2) 转化，以将每一个IPA转化成PA。

[0006] 如果在执行这样的转化时发生TLB未中，则执行多级的、二维(2-D) 的HWTW，以获得计算相应的IPA和PA需要的表条目。执行这些多级的、 2-D的HWTW，能够引起MMU的大量计算开销，其通常导致性能代偿。

[0007] 图1是当执行读事务时发生TLB未中时执行已知的、三级的、2-D的 HWTW的插图。图1中示出的HWTW表示针对三级的、2-D的HWTW的最坏情况的场景，需要十五次表查找的执行来在数据被存储在物理内存中的地方获得PA。针对这个示例，计算机系统的MMU正在运行主

管至少一个客户高级OS(HLOS)的系统管理程序，继而，其正运行至少一个应用程序。在这样的配置中，正被客户HLOS分配的内存不是系统的真实的物理内存，而是上述的中间物理内存。系统管理程序分配真实的物理内存。因此，将每一个VA转化成IPA，然后，将IPA转化成读取的数据实际被存储的地方的真实物理内存的PA。

[0008] 该过程开始于MMU接收S1页全局目录(PGD)IPA 2。针对这个最坏情况场景的示例，将假设的是，在MMU针对匹配检查TLB时发生TLB未中。因为该未中，MMU必须执行HWTW。HWTW涉及执行三次S2表查找3、4和5，以获得将IPA 2转变成PA所需的映射，以及一次额外的查找6来读取PA。表查找3、4和5分别涉及读取S2 PGD、页中间目录(PMD) 和页表条目(PTE)。在查找6处读取PA为MMU提供S1 PMD IPA 7。针对这个最坏情况场景的示例，将假设的是，当MMU针对匹配利用S1 PMD IPA 7来检查TLB时发生TLB未中。因为该文中，所以MMU必须执行另一HWTW。该HWTW涉及执行三次S2表查找8、9和11，以获得将S1 PMD IPA 7转变成PA所需的映射，以及一次额外的查找12来读取PA。表查找8、 9和11分别涉及读取S2 PGD、PMD和PTE。在查找12处读取PA为MMU 提供S1 PET IPA 13。

[0009] 针对这个最坏情况场景的示例，将假设的是，当MMU针对匹配利用 S1 PTE IPA 13来检查TLB时发生TLB未中。因为该未中，MMU必须执行另一HWTW。该HWTW涉及执行三次S2表查找14、15和16，以获得将 S1 PTE IPA 13转变成PA所需的映射，以及一次额外的查找17来读取PA。表查找14、15和16分别涉及读取S2 PGW、PMD和PTE。在查找17处读取PA为MMU提供真实的IPA 18。针对这个最坏情况场景的示例，将假设的是，当MMU针对匹配利用真实的IPA 18来检查TLB时发生TLB未中。因为该未中，MMU必须执行另一HWTW。该HWTW涉及执行三次S2表查找19、21和22，以获得将真实的IPA 18转变成PA所需的映射。表查找 19、21和22分别涉及读取S2 PGD、PMD和PTE。然后，读取PA来获得相应的读数据。在查找18处读取PA为MMU提供S1 PTE IPA 13。

[0010] 因此，能够看出的是，在针对三级的、2-D的HWTW的最坏情况场景下，执行了12次S2表查找和三次S1表查找，其是消耗大量时间并导致性能代偿的大量计算开销。已经使用各种各样的技术和架构来降低在执行 HWTW中涉及的时间和处理开销的量，包括，例如，增加TLB的大小，使用多个TLB，使用平面嵌套的页表，使用影子分页或推测的影子分页，以及使用页移动高速缓冲存储器。虽然所有的这些技术和架构能够降低与执行HWTW相关联的处理开销，但是，它们经常导致计算机系统中别的地方的处理开销的增加。

[0011] 因此，存在针对降低执行HWTW需要的时间和计算资源的量的计算机系统和方法的需求。还存在针对用于防止对在HWTW期间已经被加载到 TLB中的PA的内容进行未授权的存取的方法和装置的需求。

发明内容

[0012] 本发明针对一种用于防止对在执行HWTW期间已经被加载到计算机系统的存储元件中的PA的内容进行未授权的存取的安全装置和方法。该安全装置和方法检测某些条件，以确定是否应当防止对该内容进行存取，包括检测是否使用预测算法来基于PA预测VA。

[0013] 该装置包括安全逻辑单元，其被配置为如果当针对PA的内容检查TLB 时发生未中，则确定预测算法当前是否被启用，其中该预测算法将PA作为 IPA的函数进行预测。该安全逻辑单元被配置为当预测算法当前被启用时，防止存储元件的内容被无特权的实体存

取。

[0014] 该方法包括：

[0015] 提供安全逻辑单元；

[0016] 如果当针对PA的内容检查TLB时发生未中，则利用安全逻辑单元确定预测算法当前是否被启用，所述预测算法将PA作为IPA的函数进行预测；以及

[0017] 如果安全逻辑单元确定预测算法当前被启用，则安全逻辑单元防止存储元件的内容被无特权的实体存取。

[0018] 本发明还针对非暂时性计算机可读介质(CRM)，其具有存储于其上以由计算机系统的一个或多个处理器执行的用于防止对在执行HWTW期间已经被加载到计算机系统的存储元件中的PA的内容进行未授权的存取的计算机代码。该计算机代码包括第一计算机代码部分和第二计算机代码部分。如果当针对PA的内容检查TLB时发生未中，则第一计算机代码部分确定预测算法当前是否被启用，所述预测算法将PA作为IPA的函数进行预测。如果第一计算机代码部分确定预测算法当前被启用，则第二计算机代码部分防止存储元件的内容被无特权的实体存取。

[0019] 根据下面的描述、附图和权利要求，这些和其它特征和优点将变得显而易见。

附图说明

[0020] 图1是根据本发明的说明性的实施例的计算机系统的框图。

[0021] 图2示出了根据被配置为执行用于降低执行HWTW需要的时间和计算资源的量的方法的说明性的、或示例性的实施例的计算机系统的框图。

[0022] 图3是根据说明性的实施例来表示被图2中示出的系统管理程序执行的、以降低执行HWTW读事务需要的时间和处理开销的量的方法的流程图。

[0023] 图4是根据说明性的实施例来展示在其中使用由图3中示出的流程图表示的方法来执行HWTW读事务的方式的示意图。

[0024] 图5是根据说明性的实施例执行由图3中示出的流程图表示的方法的硬件预测器的框图。

[0025] 图6示出在其中并入了图2中示出的计算机系统的移动智能手机的框图。

[0026] 图7是根据说明性的实施例用于当图5中示出的预测器被启用时执行防止对已经被加载到TLB中的寄存器中的PA的内容进行未授权的存取的安全算法的安全逻辑单元的框图。

[0027] 图8是根据说明性的实施例描述由图7中示出的安全逻辑单元执行的过程的流程图。

具体实施方式

[0028] 根据本文描述的说明性实施例，提供了一种计算机系统和一种供在计算机系统中使用的方法，用于降低执行HWTW需要的时间和计算资源的量。如果当执行S2HWTW以查找存储S1页表的PA时发生TLB未中，则 MMU执行使用IPA来预测相应的PA的预测算法，由此避免执行S2表格查找中的任一个的需求。这极大地降低了当执行这些类型的HWTW读事务时需要被执行的查找的数量，其极大地降低了与执行这些类型的事务相关联的处理开销和性能代

偿。

[0029] 此外，提供了用于执行防止对由于启用预测算法而已经被加载到存储元件(例如，TLB的寄存器)中的PA的内容进行未授权的存取的安全算法的安全装置和方法的说明性实施例。当预测算法被启用时，对于具有系统知识的人员来说，可能配置预测算法来使被存储在主存储器的安全部分的 PA处的内容被加载到TLB中的寄存器中。以这种方式，不应当使用被存储在主存储器的安全部分中的内容的人员能够间接地获得对这些内容的未授权的存取。该安全装置和方法通过在某些环境下遮掩该内容来防止这样的未授权的存取发生。在描述该安全装置和方法的说明性实施例之前，将关于图2-6描述用于执行预测算法的计算机系统和方法的说明性实施例。然后，将关于图7和8描述该安全装置和方法的说明性实施例。

[0030] 图2根据被配置为执行用于降低执行S2HWTW以在存储S1页表的位置处查找PA需要的时间和计算资源的量的方法的说明性的、或示例性的实施例示出了计算机系统100的框图。图2中示出的计算机系统100的示例包括CPU集群110、主存储器120、摄像机显示器130、图形处理单元(GPU) 140、外围连接接口快速(PCIe)输入/输出(I/O)设备150、多个IO TLB(IOTLB)160以及系统总线170。计算机集群110具有多个CPU核110a，其中的每一个CPU核110a具有MMU 110b。每一个CPU核110a可以是微处理器或任意其它合适的处理器。摄像机显示器130具有系统MMU (SMMU)130a。GPU 140具有其自己的SMMU 140a。同样地，PCIe IO 设备150具有其自己的SMMU 150a。

[0031] 处理器核110a的MMU 110b被配置为执行将VA转化成IPA以及将IPA 转化成PA的任务。将页表存储在主存储器120中。MMU 110b和SMMU 130a、140a和150a中的每一个具有其自己的TLB(出于清楚的目的，未示出)，所述TLB存储被存储在主存储器120中的页表的子集。根据这个说明性的实施例，在发生TLB未中之后，MMU 110b执行处理IPA以预测PA 的预测算法。在数学上，可以将该预测算法表示为：

[0032] PA＝f(IPA)， (等式1)

[0033] 其中，f表示数学函数。下文关于图5详细地描述可以被用于这个目的的函数f。短语“以预测”，如该短语在本文被使用的，表示“以确定”的意思，并且尽管随机的或概率的确定不必然地被排除在本发明的范围之外，但是，该短语并不意味随机的或概率的确定。由预测算法进行的预测通常是确定性的，但是，不必然地是确定性的。

[0034] CPU集群110运行系统OS 200和虚拟机监视器(VMM)或系统管理程序210。系统管理程序210管理转化任务，所述转化任务除去执行转化之外包括更新被存储在MMU 110b和SMMU 130a、140a和150a中的页表。系统管理程序210还运行客户HLOS 220和/或客户数字版权管理器(DRM) 230。可以将HLOS 220与摄像机显示器130相关联，以及可以将DRM 230 与GPU 140相关联。系统管理程序210管理HLOS 220和DRM 230。

[0035] 在发生TLB未中之后，系统管理程序210配置MMU 110b和SMMU 130a、140a和150a，以执行预测算法来将IPA转变成PA。在这样的情况下，以在其中S1转化正常开始的典型方式，从CPU集群110的硬件基址寄存器(出于清楚的目的，未示出)获得针对与TLB未中相关联的VA的起始 IPA。然后，如下文将更详细地描述的，预测算法根据等式1预测PA。为了管理和更新SMMU 130a、140a和150a，CPU MMU 110b在总线170上向SMMU 130a、140a和150a发送分布式虚拟内存(DVM)消息。MMU 110b 和SMMU 130a、140a和150a访问主存储器120，以执行

HWTW。

[0036] 根据说明性的实施例，CPU MMU 110b将MMU业务分成三个事务类别，即：(1)S2HWTW读事务，以查找存储S1页表的PA；(2)客户端事务；以及(3)地址故障(AF)/脏标志写事务。根据这个说明性的实施例，对于类别1事务(即，HWTW读事务)，预测算法针仅将IPA转变成PA。针对所有其它的事务类别，根据这个说明性的实施例，MMU 110b和SMMU 130a、140a和150a以典型的方式执行所有其它的转化(例如，S1和客户端事务S2转化)。

[0037] 图3是根据说明性的实施例来表示由CPU MMU 110b执行以降低执行 HWTW读事务需要的时间和处理开销的量的方法的流程图。框301表示方法开始，通常在CPU集群110启动并开始运行系统OS 200和系统管理程序210时发生。如由框302指示的，MMU 110b将业务分成上述的事务类别(1)、(2)和(3)。分类过程可以将事务分成比这三个类别要多或要少的类别，但是，分类中的至少一个分类将是类别(1)事务，即，S2HWTW 读事务，以查找存储S1页表的PA。在由框303表示的步骤处，对在执行类别(1)的事务时是否已经发生TLB未中进行确定。如果未发生，则该方法进行到框306，在框306处，MMU 110b或SMMU 130a、140a或150a 以正常的方式执行HWTW。

[0038] 如果在由框303表示的步骤处CPU MMU 110b确定当执行类别(1) 事务时发生未中，则该方法进行到由框305表示的步骤。在由框305表示的步骤处，执行上述预测算法，以将IPA转变或转化成PA。

[0039] 图4是根据说明性的实施例来展示在其中执行HWTW读事务的方式的示意图。针对这个说明性的实施例，出于示例性的目的，假设页表是三级页表并且HWTW是2-D的HWTW。该示例还假设TLB未中的最坏情况场景。该过程开始于MMU接收VA，以及然后从控制寄存器(出于清楚的目的，未示出)检索S1 PGD IPA 401。然后，MMU针对与S1 PGD IPA 401 的匹配来检查TLB。针对这个最坏情况场景的示例，将假设的是，当MMU 针对匹配来检查TLB时发生TLB未中。因为这个未中，MMU执行预测算法，以将S1 PGD IPA 401转变成存储S1 PMD IPA 403的PA 402。因此，使用单个查找来将S1 PGD IPA 401转变成PA 402。

[0040] 针对该最坏情况场景的示例，将假设的是，当MMU针对匹配利用S1 PMD IPA 403来检查TLB时发生TLB未中。因为该未中，MMU执行预测算法，以将S1 PMD IPA 403转变成存储S1 PTE IPA 405的PA 404。因此，使用单个查找来将S1 PMD IPA 403转变成PA 404。针对这个最坏情况场景的示例，将假设的是，当MMU针对匹配利用S1 PTE IPA 405来检查TLB 时发生TLB未中。因为该未中，MMU执行预测算法，以将S1 PTE IPA 405 转变成存储IPA1 407的PA 406。一旦已经获得IPA1 407，就执行三次查找 408、409和411，以获得存储要读取的数据的最终PA 412。

[0041] 因此，根据这个实施例，能够看出的是，已经将查找的总次数从十五 (图1)降低到了六，其表示处理开销降低了60％。当然，本发明不限于具有特定级数或特定数量的HWTW维度的MMU配置。本领域技术人员将理解的是，应用本发明的概念和原理，而不管页表的配置。同样地，尽管本文关于IPA-至-PA转变描述了方法和系统，但是，它们同样可应用于不使用IPA的系统中的直接的VA-至-PA的转变。

[0042] 图5是执行预测算法的预测器500的说明性实施例的框图。通常在 MMU 110b中和SMMU 130a、140a和150a中实现预测器500。如上文指示的，根据说明性的实施例，仅当执行类别1的读事务时执行预测算法。图5 中示出的预测器500的配置是允许针对类别1的事务

启用预测器500和针对所有其它的事务类别(包括类别2和3的事务)禁用预测器500的一个配置的示例。

[0043] 图5中示出的预测器500的配置还允许预测器500选择被用在上文等式1中的函数f,以基于IPA来计算PA。每一个虚拟机(VM)可以使用不同的函数f的集合,所以,重要的是,被使用的函数的集合确保在IPA的范围上的IPA与PA之间存在一一对应的映射。系统管理程序210可以管理多个HLOS或DRM,所述多个HLOS或DRM中的每一个将具有运行在系统管理程序210中的相应的VM。被使用的函数的集合确保预测的PA不与被分配给另一VM的预测的PA重叠。

[0044] 函数f的示例是:

[0045] PA=IPA;

[0046] PA=IPA+Offset_function(VMID),其中,VMID是跨越所有VM标识与 HWTW读事务相关联的VM的唯一标识符,Offset_function是具有基于与 VMID相关联的特定的偏移值选择的输出的函数;以及

[0047] PA=IPA XOR Extended_VMID,其中,XOR表示异或操作,以及Extended_VMID是扩展的VMID。系统管理程序210选择函数f,从而避免 VM之间的冲突。

[0048] 在图5中,假设函数f是多项式,并且系统管理程序210从多个多项式选择要被用作函数f的多项式。可以基于例如针对其执行HWTW读事务的 VM的VMID来选择多项式。预测器500的配置寄存器510存储一个或多个预测使能比特510a和一个或多个多项式选择比特510b。预测器500的多项式计算硬件520包括基于从寄存器510接收的多项式选择比特510b的值来选择多项式函数的硬件。多项式计算硬件520还接收IPA-至-PA的转化请求,并根据选择的多项式函数来处理该请求,以生成预测的PA。

[0049] 在与门530的输入处接收预测使能比特510a和类别1使能比特。当在执行类别1的读事务时已经发生未中时,断言类别1的使能比特。预测器 500的复用器(MUX)540在MUX 540的选择器端口处接收与门530的输出,并且接收以正常方式获得的预测的PA和IPA-至PA的转化结果。当预测使能比特510a和类别1的使能比特均被断言时,S2WALK控制逻辑与状态机550被禁用,并且MUX 540选择要从MUX 540输出的预测的PA。

[0050] 当预测使能比特510a和/或类别1的使能比特被解除认定时,S2移动控制逻辑与状态机550被启用。当S2移动控制逻辑与状态机550被启用时,可以由S2移动控制逻辑与状态机550在主存储器120中执行其它类型的S2 移动(例如,类别2和类别3)。因此,当S2移动控制逻辑与状态机550 被启用时,MUX 540输出IPA-至-PA的转化结果,所述IPA-至-PA的转化结果是根据S2移动控制逻辑与状态机550输出的。

[0051] 应当注意到的是,预测器500可以具有多个不同的配置。图5中示出的预测器500的配置仅是用于执行预测算法的多个合适的配置中的一个配置。本领域技术人员将理解的是,可以使用除了图5中示出的之外的多个配置来执行预测算法。

[0052] 可以在执行内存虚拟化的任意类型的系统(包括例如,台式计算机、服务器和移动智能手机)中实现图2中示出的计算机系统100。图6示出并入了计算机系统100的移动智能手机600的框图。除了智能手机600必须能够执行本文描述的方法之外,智能手机600不限于任意特定类型的智能手机或具有任意特定的配置。同样地,图6中示出的智能手机600旨在是具有情境感知和用于执行本文描述的方法的处理能力的蜂窝电话的简化示例。具有本领

域普通技术的人员将理解，已经省略了智能手机的操作和结构，以及由此的实现方式的细节。

[0053] 根据这个说明性的实施例，智能手机600包括在系统总线612上被连接在一起的基带子系统610和射频(RF)子系统620。系统总线612通常包括将上述元件耦合在一起并启用它们的互操作性的物理的和逻辑的连接。RF子系统620可以是无线收发机。尽管为了清楚未示出细节，但是，RF子系统620通常包括具有用于为发送准备基带信息信号的调制、上变频和放大电路的发送(Tx)模块630，包括具有用于接收RF信号并将RF信号下变频到基带信息信号以恢复数据的放大、滤波和下变频电路的接收 (Rx)模块640，以及包括前端模块(FEM) 650，所述前端模块(FEM) 650包括天线共用器电路、双工器电路或如对本领域技术人员来说是已知的能够将发送信号与接收信号分离的任意其它电路。将天线660连接至FEM 650。

[0054] 基带子系统610通常包括经经由系统总线612电耦合在一起的计算机系统100、模拟电路元件616和数字电路元件618。系统总线612通常包括物理连接和逻辑连接，以将上述元件耦合在一起并启用它们的互操作性。

[0055] 经由连接624将输入/输出(I/O)元件621连接至基带子系统610。I/O 元件621通常包括，例如，麦克风、小键盘、扬声器、定点设备、用户接口控制元件和允许用户提供输入命令并从智能手机600接收输出的任意其它设备或系统。经由连接629将存储器628连接至基带子系统610。存储器 628可以是任意类型的易失性或非易失性存储器。可以将存储器628永久地安装在智能手机600中，或可以是诸如可移动存储卡的可移动存储元件。

[0056] 模拟电路616和数字电路618包括信号处理、信号转变和将由I/O元件 621提供的输入信号转变成要被发送的信息信号的逻辑单元。类似地，模拟电路616和数字电路618包括被用于生成包含从接收的信号恢复的信息的信息信号的信号处理元件。数字电路618可以包括，例如，数字信号处理器(DSP)、现场可编程门阵列(FPGA)或任意其它处理设备。因为基带子系统610包括模拟元件和数字元件，所以其可以被称为混合信号设备 (MSD)。

[0057] 智能手机600可以包括各种各样的传感器中的一个或多个传感器，例如照相机661、麦克风662、全球定位系统(GPS)传感器663、加速计665、陀螺仪667和数字罗盘668。这些传感器经由总线612与基带子系统610相通信。

[0058] 使计算机系统100嵌入到智能手机600中允许多个OS和多个各自的 VM运行在智能手机600上。在这个环境下，计算机系统100的系统管理程序210(图2)在智能手机600的硬件与被VM执行的应用软件之间提供安全隔离。

[0059] 根据说明性的实施例，提供了一种安全方法和装置，其检测是否执行上文关于图5描述的预测算法，以及如果是，则采取防止某些寄存器和/或缓冲器的内容被无特权的实体或未授权的实体可存取的预防措施。需要这个安全方法和装置的原因是，当预测算法被启用时，具有系统知识的人员可能会配置预测算法来使被存储在物理主存储器120(图2)的安全部分的 PA处的内容被加载到TLB中的寄存器中。以这种方式，不应当使用被存储在物理主存储器120的安全部分中的内容的人员可能间接地获得对那些PA 的未授权的存取。该方法和装置防止这样的未授权的或无特权的存取。

[0060] 图7是根据说明性的实施例用于当预测算法被启用时执行防止对已经被加载到TLB中的寄存器中的PA内容进行未授权的存取的安全算法的装置700的框图。该框图本质上是概念性的，并且可以单独地在硬件中、或在硬件与软件或固件的组合中实现。装置700是

被配置为执行安全算法的安全逻辑单元。安全逻辑单元700通常是CPU核110a的一部分，并且可以是MMU 110b和SMMU 130a、140a和150a(图2)的一部分。本发明针对安全逻辑单元700在计算机系统100中所处的位置不进行限制。

[0061] 将图5中示出的预测使能位510a连接至安全逻辑单元700的与门710 的输入。将特权存取位应用于与门710的另一个输入。如果尝试访问多个寄存器720中的一个寄存器的实体被给予特权来访问特定的寄存器720，则该特权访问位被断言。出于示例性的目的，假设寄存器720在TLB中。将与门710的输出应用于或门730的输入之一。将从寄存器访问表740输出的访问标识符位应用于或门730的另一个输入。如果被访问的寄存器720 包含来自其在主存储器120(图5)的安全的或享有特权的部分中的PA的内容，则该访问标识符位被断言。寄存器访问表740跟踪哪些PA在主存储器120的安全部分中，并相应地对访问标识符位断言或去断言。被用来选择寄存器720中的一个寄存器的寄存器选择地址750还被用来选择寄存器地址表740中的相应条目。因此，如果由寄存器选择地址750选择的寄存器720是享有特权的，则被输入到或门730的相应的访问标识符位被断言。

[0062] 将或门730的输出应用于MUX 760的选择器接线端。将通过寄存器选择地址750寻址的寄存器720的内容应用于MUX 760的输入端的第一集合。MUX 760的输入端的第二集合均接收逻辑0。当预测算法被启用并且特权访问位被断言时，MUX 760选择通过寄存器选择地址750寻址的寄存器720 的内容要从MUX 760输出并被加载到结果寄存器770中。当预测算法被禁用、或特权访问位被去断言、以及访问标识符位被去断言(指示被存取的内容是来自主存储器120的非安全部分)时，MUX 760选择由寄存器选择地址750寻址的寄存器720的内容要从MUX 760输出并被加载到结果寄存器770。当访问标识符位被断言(指示被存取的内容是来自主存储器120的安全部分)时，MUX 760选择逻辑全0要从MUX 760输出并被加载到结果寄存器770中。

[0063] 因此，除了在以下两种情况中的任一种情况下之外，通过寄存器选择地址750寻址的寄存器720的真实内容将从MUX 760输出并被加载到结果寄存器770中：(1)预测算法被启用，并且特权访问位被断言；或(2)访问标识符位被断言。在这两种情况中的任一种情况下，将逻辑全0加载到结果寄存器770中，以防止寄存器720的真实内容在寄存器770中可存取。

[0064] 图8是描述由上文关于图7描述的安全逻辑单元700执行的判定过程的流程图。在框801处进行关于预测算法是否被启用的确定。如果未被启用，则如框802指示的，返回寄存器720的真实内容。如果被启用，则在框803处进行关于尝试存取内容的实体是否是享有特权的确定。如果享有特权，则在框802处返回寄存器720的真实内容。如果不享有特权，则在框804处进行关于寄存器720是否公开享有特权的数据的确定。如果不公开，则在框802处返回寄存器720的真实内容。如果公开，则如由框805 指示的，返回逻辑0。

[0065] 能够从对安全逻辑单元700的描述看出，如果无特权的实体(例如，除了系统管理程序之外的实体)尝试使用图5中示出的预测器500来获得对被存储在主存储器120的未授权的PA中的内容的存取，则将利用0来盖写真实内容，以防止未授权的实体或无特权的实体存取真实内容。在本发明的范围内，可以对图7中示出的安全逻辑700和对图8中示出的过程进行多种修改。例如，关于图8，能够通过消除框803、留下框801、802、804 和805来修改该过程。替代地，能够消除框804，留下框801、802、803和 805。如将被本领域技术人员理解的，能够容易地修改图7中示出的安全逻辑单元700，以实现修改的过程。

[0066] 应当注意到的是，当已经检测到未授权的存取尝试时，还可以实现除了或除了上文关于图5、7和8描述的那些之外的安全功能。利用逻辑0来盖写寄存器的内容仅是提供安全的一种方式的示例。替代的示例包括利用逻辑1或隐藏真实内容的某个其它二进制值来盖写该内容，利用相等长度的某个其它二进制值来异或该内容，返回错误消息而不是真实内容，发出中断，重置处理器110a、MMU 110或SMMU 130a、140a或150a等。鉴于本文提供的讨论，本领域技术人员将理解在其中可以实现对本文描述的说明性实施例的这些和其它合适的替代的方式。

[0067] 可以单独地在硬件中、或在硬件与软件的组合中、或在硬件与固件的组合中实现上文关于图3和8描述的过程。同样地，可以单独地在硬件中、或在硬件与软件或固件的组合中实现图2中示出的计算机系统100的组件中的多个组件。例如，可以单独地在硬件中、或在硬件与软件或固件的组合中实现系统管理程序210。在软件或固件中实现图3和8中示出的过程或图2中示出的计算机系统100的组件的情况下，将相应的代码存储在是计算机可读介质的主存储器120中(图2)。主存储器120通常是固态的计算机可读介质，例如，非易失性随机存取存储器(RAM)、动态RAM(DRAM)、只读存储器(ROM)设备、可编程ROM(PROM)、可擦除PROM(EPROM) 等。然而，可以使用其它类型的计算机可读介质来存储代码，诸如例如，磁性存储设备和光学存储设备。

[0068] 应当注意到的是，本文描述的说明性实施例旨在展示本发明的原理和概念。鉴于本文提供的描述，如将被本领域技术人员理解的，本发明不限于这些实施例。还应当注意到的是，在不偏离本发明的保护范围的情况下，可以对上文关于图2-8描述的方法和系统进行多种变型。例如，鉴于本文提供的描述，如将被本领域技术人员理解的，可以以多个方式修改图7中示出的安全逻辑单元700的配置，同时仍实现上文描述的目标。同样地，图6 中示出的智能手机600仅是具有用于执行该方法的合适的配置和功能的移动设备的一个示例。鉴于本文提供的描述，本领域技术人员将理解的是，在不偏离本发明的保护范围的情况下，可以对图6中示出的智能手机600 进行多种变型。这些变型和其它变型在本发明的范围内。

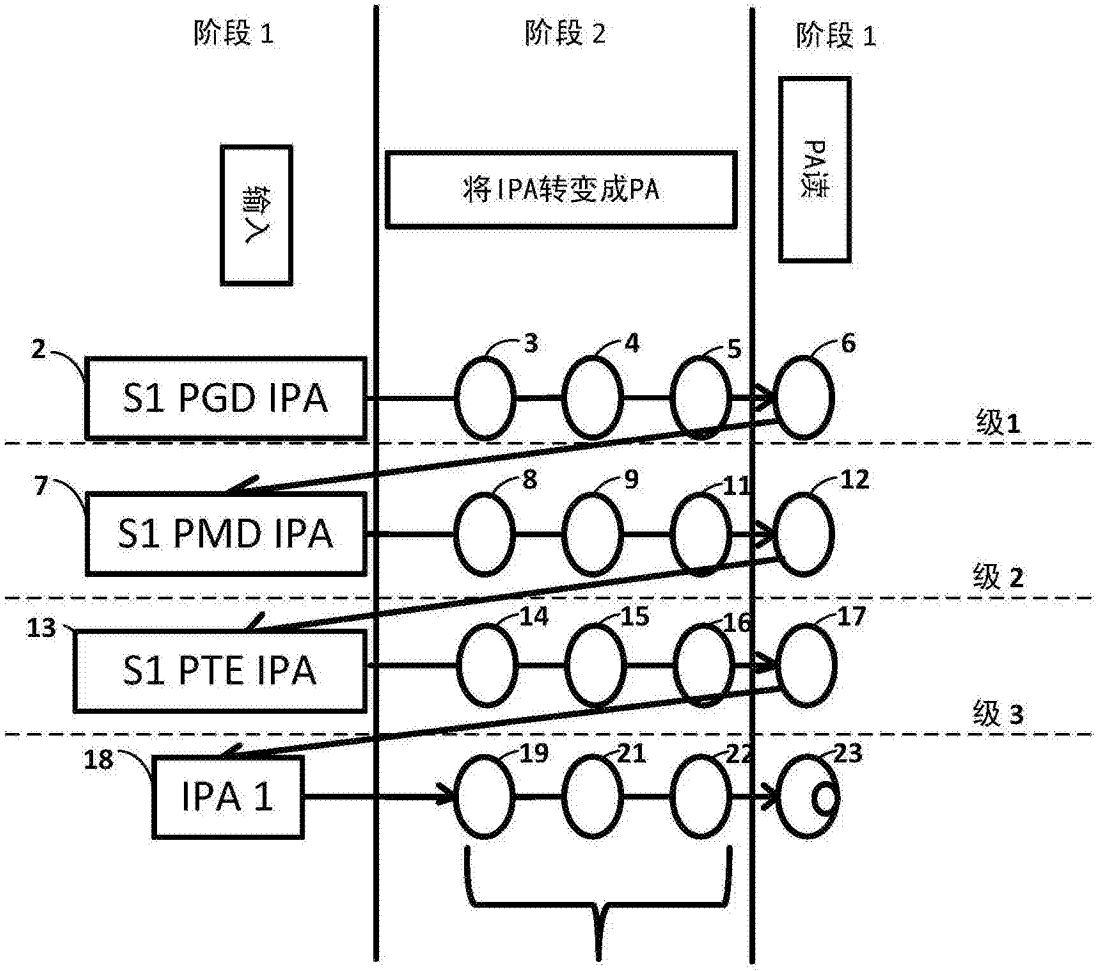

阶段 1
阶段 2
阶段 1
输入
将IPA转变成PA
PA读
2
S1 PGD IPA
3
4
5
6
级1
7
S1 PMD IPA
8
9
11
12
级 2
13
S1 PTE IPA
14
15
16
17
级 3
18
IPA 1
19
21
22
23

图1
(现有技术)

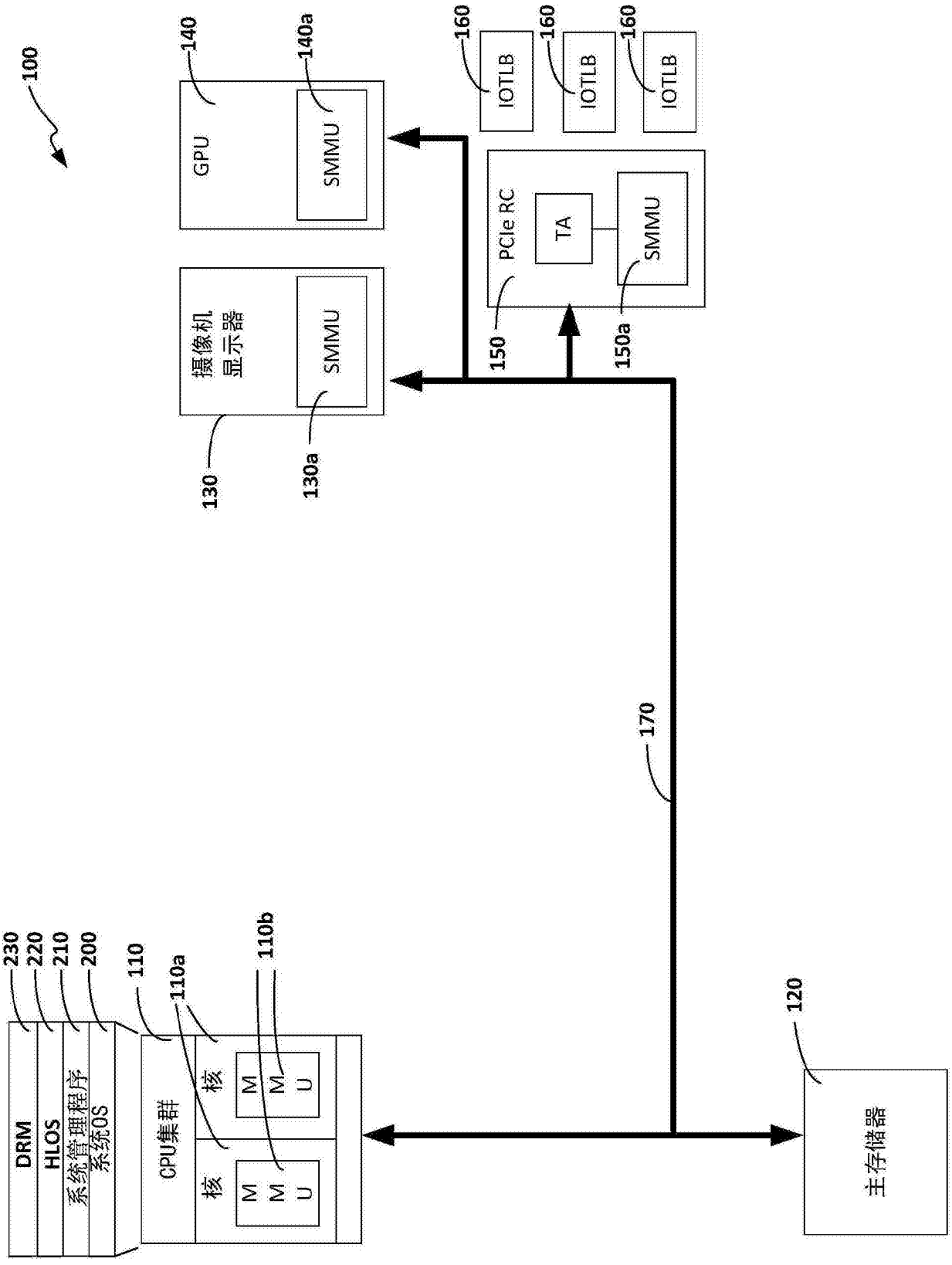

100
140
140a
GPU
SMMU
160
160
160
IOTLB
IOTLB
IOTLB
PCIe RC
TA
SMMU
150
150a
摄像机
显示器
SMMU
130
130a
170
230
220
210
200
110
110a
110b
DRM
HLOS
系统管理程序
系统OS
CPU集群
核
核
M
M
U
M
M
U
120
主存储器

图2

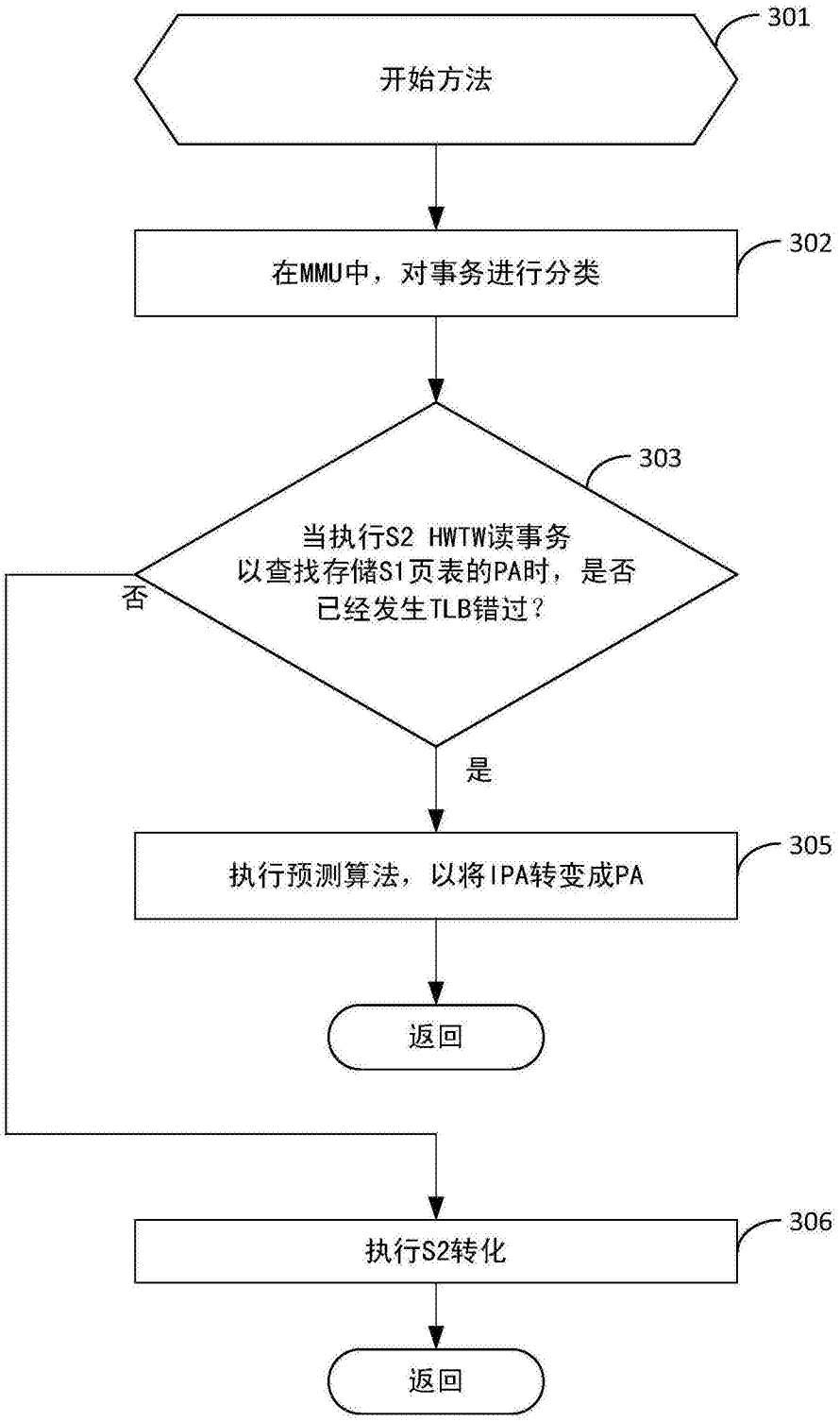

301
开始方法
302
在MMU中，对事务进行分类
303
当执行S2 HWTW读事务
以查找存储S1页表的PA时，是否
已经发生TLB错过？
否
是
305
执行预测算法，以将IPA转变成PA
返回
306
执行S2转化
返回

图3

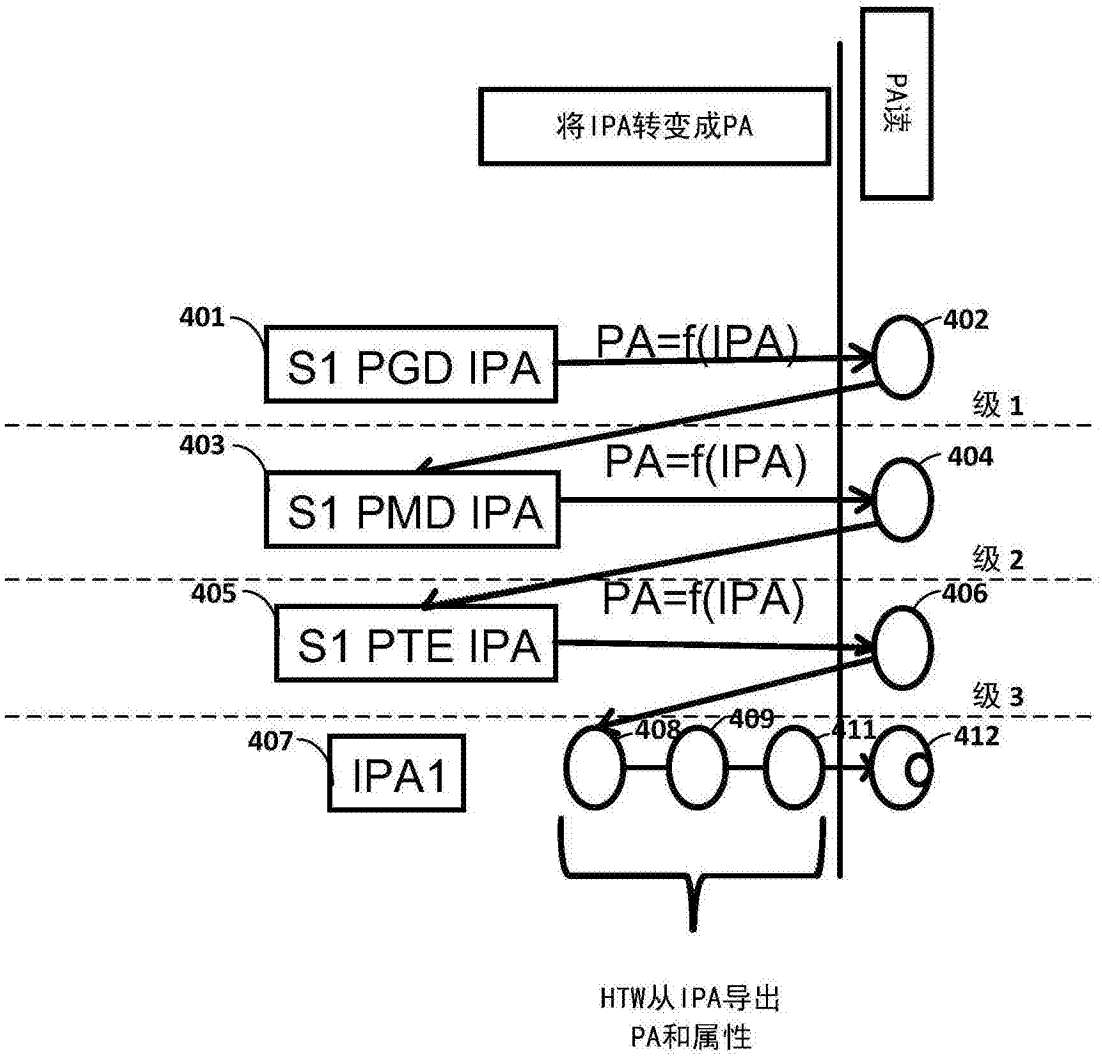

PA读
将IPA转变成PA
401
S1 PGD IPA
PA=f(IPA)
402
级 1
403
S1 PMD IPA
PA=f(IPA)
404
级 2
405
S1 PTE IPA
PA=f(IPA)
406
级 3
407
IPA1
408
409
411
412
HTW从IPA导出
PA和属性

图4

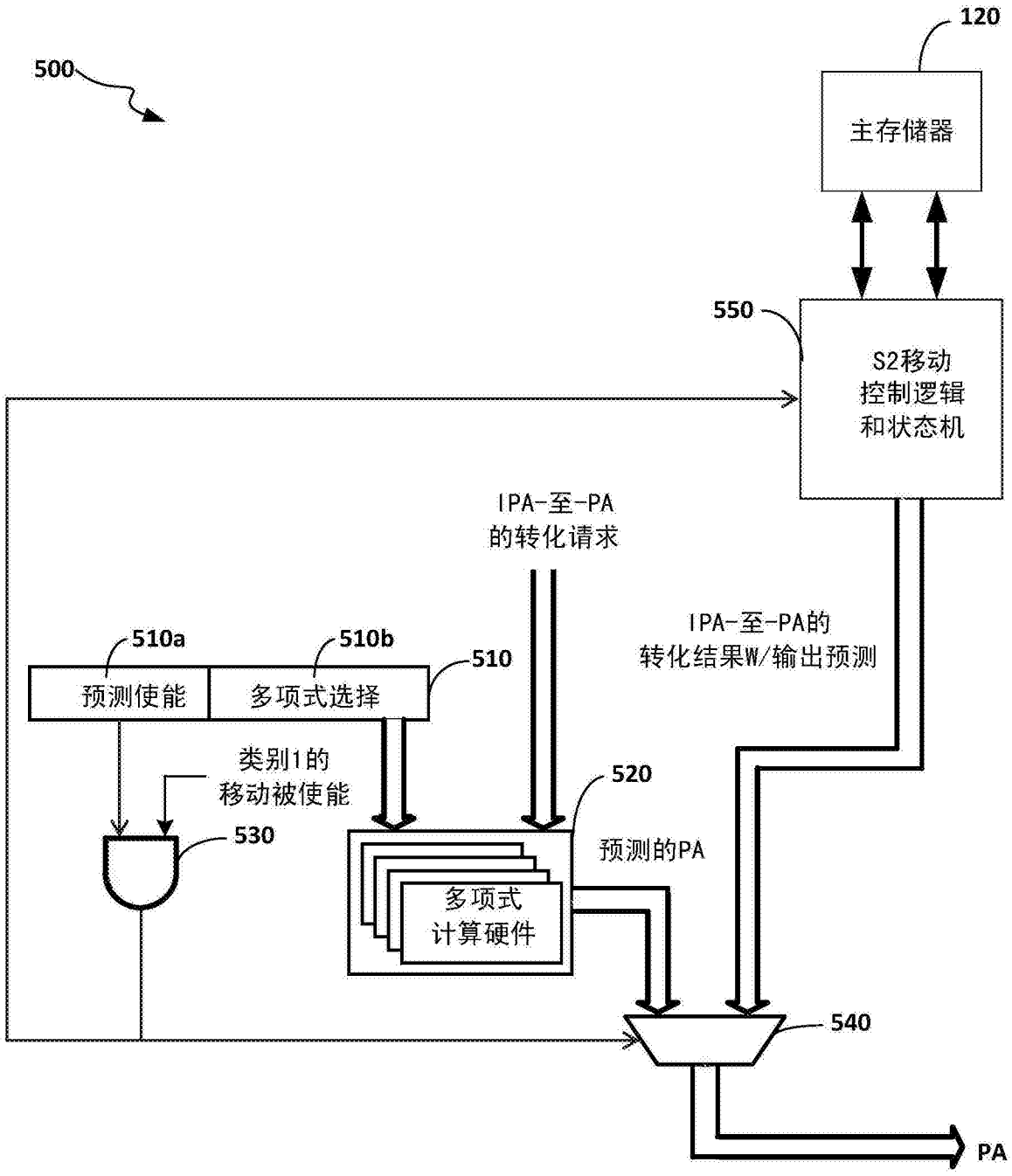

500
120
主存储器
550
S2移动
控制逻辑
和状态机
IPA-至-PA
的转化请求
IPA-至-PA的
转化结果W/输出预测
510a
510b
510
预测使能
多项式选择
类别1的
移动被使能
530
520
预测的PA
多项式
计算硬件
540
PA

图5

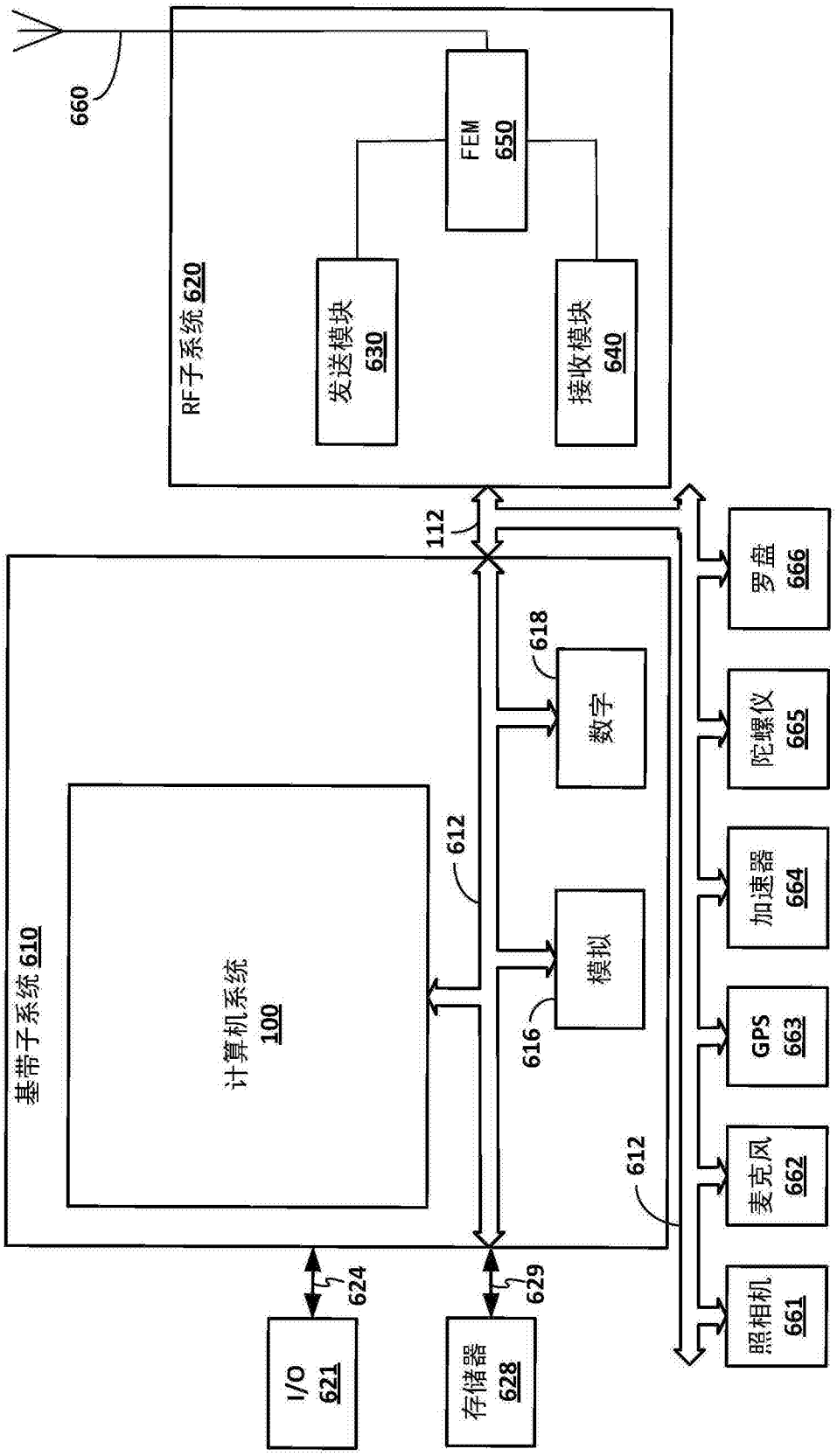

660
RF子系统 620
FEM 650
发送模块 630
接收模块 640
112
基带子系统 610
计算机系统 100
618
数字
612
模拟
616
612
624
629
I/O 621
存储器 628
罗盘 666
陀螺仪 665
加速器 664
GPS 663
麦克风 662
照相机 661

图6

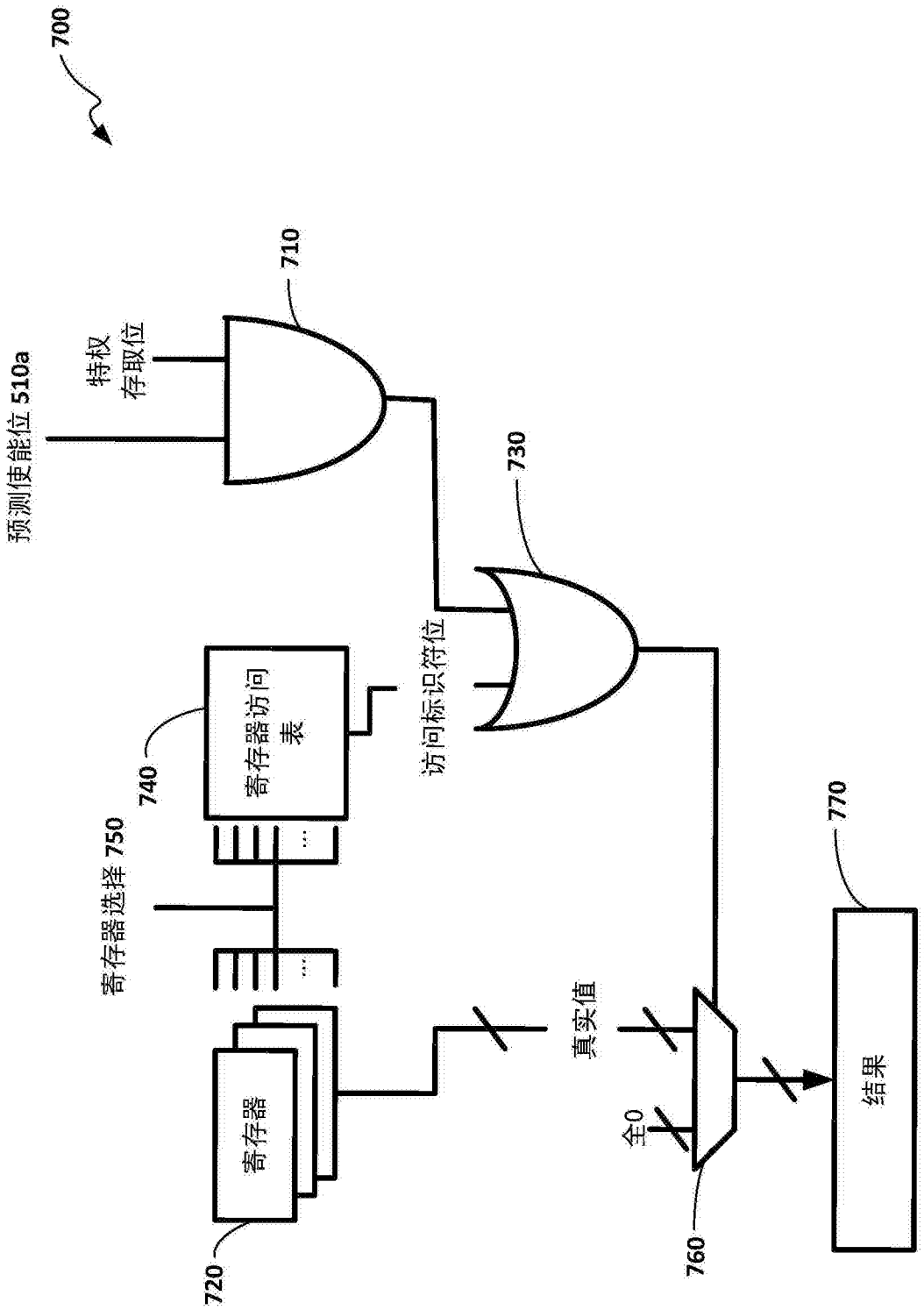

700
710
特权
存取位
预测使能位 510a
730
访问标识符位
740
寄存器访问
表
寄存器选择 750
真实值
770
结果
全0
寄存器
720
760

图7

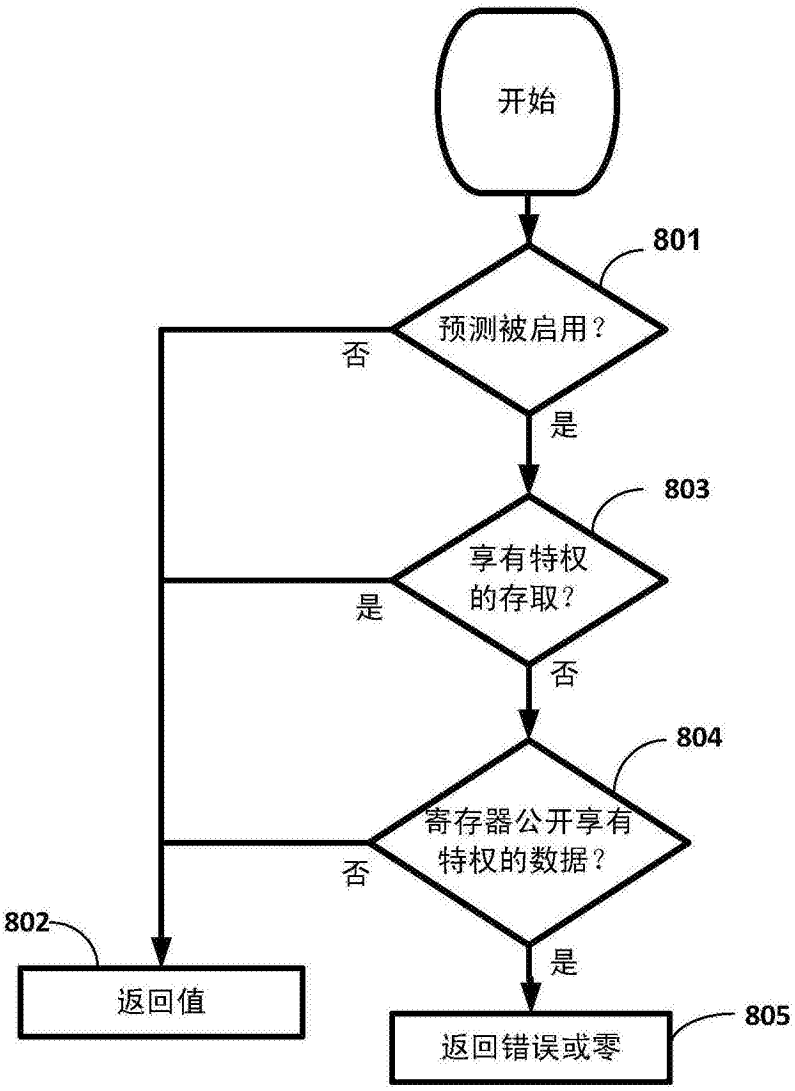

开始
801
预测被启用？
否
是
803
享有特权
的存取？
是
否
804
寄存器公开享有
特权的数据？
否
是
802
返回值
805
返回错误或零

图8