(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118339542 A
(43)申请公布日 2024.07.12

(21)申请号 202280078994.1
(22)申请日 2022.04.28
(30)优先权数据
2117274.7 2021.11.30 GB
(85)PCT国际申请进入国家阶段日
2024.05.29
(86)PCT国际申请的申请数据
PCT/GB2022/051073 2022.04.28
(87)PCT国际申请的公布数据
WO2023/099860 EN 2023.06.08
(71)申请人 ARM有限公司
地址 英国剑桥
(72)发明人 理查德·罗伊·格里森思怀特
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
专利代理师 杨佳婧
(51)Int.Cl.
G06F 12/109(2016.01)
G06F 12/14(2006.01)
G06F 9/455(2018.01)

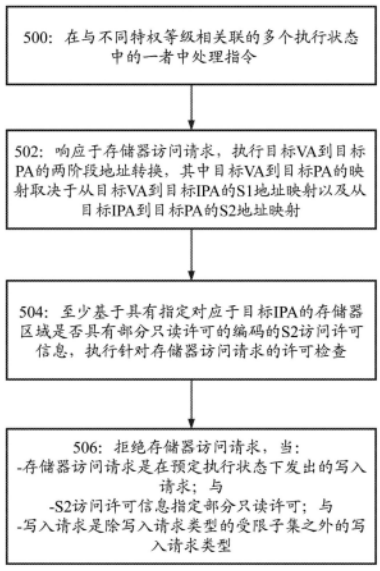
权利要求书5页 说明书38页 附图19页

(54)发明名称

两阶段地址转换

(57)摘要

存储器管理电路(28)支持基于阶段1和阶段2转换表结构的两阶段地址转换。由阶段2转换表条目指定的阶段2访问许可信息具有指定对应存储器区域是否具有部分只读许可的编码,该部分只读许可指示当处理电路(4)处于预定执行状态时发出的针对对应于目标中间地址的存储器区域的写入请求对于写入请求类型的受限子集(包括用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求)被许可,但是对于其他写入请求类型被禁止。当对应的阶段2转换表条目的该阶段2访问许可信息指定该部分只读许可,并且存储器访问请求是在该预定执行状态下发出的除了该写入请求类型的受限子集之外的写入请求时,该存储器管理电路(28)拒绝该存储器访问请求。



CN 118339542 A

1.一种装置,所述装置包括:

处理电路,所述处理电路用于在与不同特权等级相关联的多个执行状态中的一者中处理指令;和

存储器管理电路,所述存储器管理电路用于响应于所述存储器访问请求而将由所述存储器访问请求指定的目标虚拟地址转换成指示待访问的存储器系统位置的目标物理地址;其中:

所述存储器管理电路被配置为支持基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从所述目标虚拟地址到所述目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,所述阶段1地址映射包括从所述目标虚拟地址到由对应阶段1转换表条目指定的对应于所述目标虚拟地址的目标中间地址的映射,并且所述阶段2地址映射包括从所述目标中间地址到由对应阶段2转换表条目指定的对应于所述目标中间地址的所述目标物理地址的映射;

所述存储器管理电路被配置为至少基于由所述对应阶段2转换表条目指定的阶段2访问许可信息来执行针对所述存储器访问请求的许可检查,所述阶段2访问许可信息具有指定对应于所述目标中间地址的存储器区域是否具有部分只读许可的编码,所述部分只读许可指示当所述处理电路处于所述多个执行状态中的预定执行状态时发出的针对对应于所述目标中间地址的所述存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了所述受限子集之外的写入请求类型被禁止,所述写入请求类型的受限子集包括由所述存储器管理电路生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;并且

所述存储器管理电路被配置为响应于确定所述存储器访问请求是在所述预定执行状态下发出的写入请求、所述阶段2访问许可信息指定对应于所述目标中间地址的所述存储器区域具有所述部分只读许可、并且所述存储器访问请求是除了所述写入请求类型的受限子集之外的写入请求类型,拒绝所述存储器访问请求。

2.根据权利要求1所述的装置,其中所述写入请求类型的受限子集还包括响应于由所述处理电路在所述预定执行状态中执行的至少一个预定类型的转换表条目更新指令而发出的写入请求。

3.根据任一前述权利要求所述的装置,其中所述写入请求类型的受限子集排除响应于由所述处理电路在所述预定执行状态中执行的至少一种类型的存储指令而发出的写入请求。

4.根据任一前述权利要求所述的装置,其中每个阶段1转换表条目具有编码,所述编码指定所述阶段1转换表条目是否是受保护条目,与未被编码为受保护条目的阶段1转换表条目相比,所述受保护条目的更新受限。

5.根据权利要求4所述的装置,所述装置包括受保护条目检查电路,所述受保护条目检查电路用于基于给定的阶段1转换表条目是否被标记为受保护条目来检查是否将更新限制到由所述给定的阶段1转换表条目指定的访问许可或地址映射。

6.根据权利要求4和5中任一项所述的装置,所述装置包括受保护条目检查电路,所述受保护条目检查电路用于响应于所述处理电路执行用于请求对给定存储器系统位置的更新的受保护条目检查类型的读取检查写入指令,而:

从所述给定存储器系统位置读取数据,

检查从所述给定存储器系统位置读取的所述数据是否具有与被指定为受保护条目的阶段1转换表条目一致的值,以及

响应于确定从所述给定存储器系统位置读取的所述数据具有与被指定为受保护条目的阶段1转换表条目一致的值,防止所述阶段1转换表条目的更新受限位子集响应于所述读取检查写入指令而被更新。

7.根据权利要求6所述的装置,其中当响应于所述受保护条目检查类型的读取检查写入指令而执行对所述给定存储器系统位置的所述更新时,所述受保护条目检查电路被配置为控制待作为原子操作执行的以下操作:从所述给定存储器系统位置读取所述数据、检查所述数据是否具有与被指定为受保护条目的阶段1转换表条目一致的值、以及更新所述给定存储器系统位置。

8.根据权利要求6和7中任一项所述的装置,其中当响应于当所述处理电路处于所述预定执行状态时执行的所述受保护条目检查类型的读取检查写入指令而执行对所述给定存储器系统位置的所述更新时,所述受保护条目检查电路被配置为禁止对所述给定存储器系统位置的所述更新改变存储在所述给定存储器系统位置处的阶段1转换表条目是否被指定为受保护条目。

9.根据权利要求6至8中任一项所述的装置,其中响应于所述受保护条目检查类型的读取检查写入指令而发出的写入请求是所述写入请求类型的受限子集中的一者。

10.根据权利要求6至9中任一项所述的装置,其中所述更新受限位子集包括以下中的一者:

所述阶段1转换表条目的所有位;和

所述阶段1转换表条目的适当位子集,包括用于对所述阶段1转换表条目是否被指定为受保护条目进行编码的一个或多个位,选择哪些位在所述适当位子集中是以下中的一者:

不可编程的;和

可编程的,取决于存储在控制寄存器中的软件可编程的选择值。

11.根据权利要求6至10中任一项所述的装置,其中:

每个有效的阶段1转换表条目具有指定所述阶段1转换表条目是否是受保护条目的编码;并且

响应于确定从所述给定存储器系统位置读取的所述数据具有与无效的阶段1转换表条目一致的值,所述受保护条目检查电路被配置为允许所述无效的阶段1转换表条目的更新,不同于使得所述给定存储器系统位置处的所述数据变为被指定为受保护条目的有效的阶段1转换表条目的更新。

12.根据权利要求6至10中任一项所述的装置,其中有效和无效的阶段1转换表条目都具有指定所述阶段1转换表条目是否是受保护条目的编码;

响应于确定从所述给定存储器系统读取的所述数据具有与被指定为受保护条目的无效的阶段1转换表条目一致的值,所述受保护条目检查电路被配置为防止所述给定存储器系统位置的无效条目更新受限位子集响应于所述读取检查写入指令而被更新;并且

响应于确定从所述给定存储器系统读取的所述数据具有与被指定为受保护条目的有效的阶段1转换表条目一致的值,所述受保护条目检查电路被配置为防止所述给定存储器

系统位置的有效条目更新受限位子集响应于所述读取检查写入指令而被更新。

13.根据权利要求12所述的装置,其中:

有效的阶段1转换表条目包括指示所述有效的阶段1转换表条目是否是受保护条目的第一位字段;并且

无效的阶段1转换表条目包括指示所述无效的阶段1转换表条目是否是受保护条目的第二位字段;并且

所述第一位字段和所述第二位字段位于阶段1转换表条目编码内的不同位位置。

14.根据权利要求6至13中任一项所述的装置,其中所述受保护条目检查电路被配置为通过以下中的一者抑制对所述更新受限位子集的所述更新:

当所请求的更新将引起对所述更新受限位子集中的至少一个位的更新时,拒绝对所述给定存储器系统位置的所述更新;以及

当所述更新受限位子集是所述给定存储器系统位置的适当位子集时,响应于所述读取检查写入指令,抑制对所述更新受限位子集的所述更新,同时允许对所述给定存储器系统位置的至少一个其他位的更新。

15.根据权利要求6至14中任一项所述的装置,其中响应于所述受保护条目检查类型的读取检查写入指令,所述处理电路被配置为设置至少一个条件状态值以指示基于对从所述给定存储器系统读取的所述数据是否是被指定为受保护条目的阶段1转换表条目的检查,是否抑制由所述受保护条目检查类型的读取检查写入指令请求的所述更新的至少一部分。

16.根据权利要求6至15中任一项所述的装置,其中所述受保护条目检查类型的读取检查写入指令是以下中的一者:

所述受保护条目检查类型的读取检查写入指令的交换变体,响应于所述交换变体,所述处理电路被配置为将从所述给定存储器系统位置读取的所述数据写入到目的地寄存器以供后续指令用作操作数;

所述受保护条目检查类型的读取检查写入指令的存储变体,针对所述存储变体,所述处理电路被配置为处理所述存储变体而不将从所述给定存储器系统位置读取的所述数据写入到目的地寄存器;

指定比较操作数的所述受保护条目检查类型的读取检查写入指令的比较和交换变体,针对所述比较和交换变体,所述受保护条目检查电路被配置为确定从所述给定存储器系统位置读取的所述数据与所述比较操作数的比较是否满足比较条件,在不满足所述比较条件时抑制对所述给定存储器系统位置的所述更新,并且将从所述给定存储器系统位置读取的所述数据写入到目的地寄存器以供后续指令用作操作数;和

位设置/清除指令,针对所述位设置/清除指令,对所述给定存储器系统位置的所述更新包括设置或清除在所述给定存储器系统位置处的所述数据的至少一个选定位。

17.根据权利要求5至16中任一项所述的装置,其中对应于给定中间地址的给定的阶段2访问转换表条目具有指定对应于所述给定中间地址的存储器区域是否具有指示以下要求的抗混叠性质的编码:针对将被允许的对与所述给定中间地址相对应的存储器区域的访问,将在所述阶段1转换结构的转换表遍历中被访问以定位指定从给定虚拟地址到所述给定中间地址的阶段1地址映射的对应阶段1转换表条目的一个或多个遍历的阶段1转换表条目中的每一者被要求满足抗混叠条件,

当满足以下任一项时,满足给定的遍历的阶段1转换表条目的所述抗混叠条件:

所述给定的遍历的阶段1转换表条目被指定为受保护条目,并且所述部分只读许可由针对相关阶段2转换表条目的所述阶段2访问许可信息指定,所述相关阶段2转换表条目提供用于导出存储所述给定的遍历的阶段1转换表条目的所述存储器系统位置的物理地址的所述阶段2地址映射;或者

只读许可由针对所述相关阶段2转换表条目的所述阶段2访问许可信息指定;

并且

所述存储器管理电路被配置为响应于确定所述对应的阶段2转换表条目指定对应于所述目标中间地址的所述存储器区域具有所述抗混叠性质并且所述一个或多个遍历的阶段1转换表条目中的任一者未能满足所述抗混叠条件而拒绝所述存储器访问请求。

18.根据任一前述权利要求所述的装置,其中所述存储器管理电路被配置为基于阶段1转换表基地址寄存器中的值来确定所述阶段1转换表结构的阶段1顶层转换表的阶段1顶层基地址。

19.根据权利要求18所述的装置,其中当启用阶段1顶层表部分只读检查时,所述存储器管理电路被配置为响应于确定所述阶段1顶层基地址对应于相关联的阶段2转换表条目未指定所述部分只读许可的中间地址而发信号通知故障。

20.根据权利要求19所述的装置,其中所述存储器管理电路被配置为基于存储在控制寄存器中的阶段1顶层部分只读检查启用控制值来确定是否启用所述阶段1顶层表部分只读检查。

21.根据权利要求18至20中任一项所述的装置,其中:

当阶段1顶层表存在许可检查被启用时,所述存储器管理电路被配置为确定对应于所述阶段1顶层基地址的给定存储器区域是否与指示允许所述给定存储器区域被分配用于存储所述阶段1转换表结构的阶段1顶层表的阶段1顶层表存在许可相关联,并且在对应于所述阶段1顶层基地址的所述给定存储器区域不具有所述阶段1顶层表存在许可时触发故障。

22.根据权利要求21所述的装置,其中所述存储器管理电路被配置为基于对应于所述阶段1顶层基地址的相关联的阶段2转换表条目的编码来确定所述给定存储器区域是否与所述阶段1顶层表存在许可相关联。

23.根据权利要求21和22中任一项所述的装置,其中所述存储器管理电路被配置为基于存储在控制寄存器中的阶段1顶层表存在许可检查启用控制值来确定是否启用所述阶段1顶层表存在许可检查。

24.一种方法,所述方法包括:

在与不同特权等级相关联的多个执行状态中的一者中处理指令;以及

响应于所述存储器访问请求而执行由存储器访问请求指定的目标虚拟地址到指示待访问的存储器系统位置的目标物理地址的两阶段地址转换,所述两阶段地址转换基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从所述目标虚拟地址到所述目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,所述阶段1地址映射包括从所述目标虚拟地址到由对应阶段1转换表条目指定的对应于所述目标虚拟地址的目标中间地址的映射,并且所述阶段2地址映射包括从所述目标中间地址到由对应阶段2转换表条目指定的对应于所述目标中间地址的所述目

标物理地址的映射;

至少基于由所述对应阶段2转换表条目指定的阶段2访问许可信息来执行针对所述存储器访问请求的许可检查,所述阶段2访问许可信息具有指定对应于所述目标中间地址的存储器区域是否具有部分只读许可的编码,所述部分只读许可指示当所述处理电路处于所述多个执行状态中的预定执行状态时发出的针对对应于所述目标中间地址的所述存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了所述受限子集之外的写入请求类型被禁止,所述写入请求类型的受限子集包括由存储器管理电路生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;以及

响应于确定所述存储器访问请求是在所述预定执行状态下发出的写入请求、所述阶段2访问许可信息指定对应于所述目标中间地址的所述存储器区域具有所述部分只读许可、并且所述存储器访问请求是除了所述写入请求类型的受限子集之外的写入请求类型,拒绝所述存储器访问请求。

25.一种计算机程序,所述计算机程序包括用于控制主机数据处理装置以提供用于执行目标代码的指令执行环境的指令,所述计算机程序包括:

处理程序逻辑,所述处理程序逻辑用于模拟在与不同特权等级相关联的多个执行状态中的一者中处理目标代码的指令;和

存储器管理程序逻辑,所述存储器管理程序逻辑用于响应于所述存储器访问请求而将由所述目标代码触发的模拟存储器访问请求所指定的目标虚拟地址转换成指示待访问的模拟存储器系统位置的目标物理地址;其中:

所述存储器管理程序逻辑被配置为支持基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从所述目标虚拟地址到所述目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,所述阶段1地址映射包括从所述目标虚拟地址到由对应阶段1转换表条目指定的对应于所述目标虚拟地址的目标中间地址的映射,并且所述阶段2地址映射包括从所述目标中间地址到由对应阶段2转换表条目指定的对应于所述目标中间地址的所述目标物理地址的映射;

所述存储器管理程序逻辑被配置为至少基于由所述对应阶段2转换表条目指定的阶段2访问许可信息来执行针对所述模拟存储器访问请求的许可检查,所述阶段2访问许可信息具有指定对应于所述目标中间地址的存储器区域是否具有部分只读许可的编码,所述部分只读许可指示当所述处理程序逻辑处于所述多个执行状态中的预定执行状态时发出的针对对应于所述目标中间地址的所述存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了所述受限子集之外的写入请求类型被禁止,所述写入请求类型的受限子集包括由所述存储器管理程序逻辑生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;并且

所述存储器管理程序逻辑被配置为响应于确定所述模拟存储器访问请求是在所述预定执行状态下发出的写入请求、所述阶段2访问许可信息指定对应于所述目标中间地址的所述存储器区域具有所述部分只读许可、并且所述模拟存储器访问请求是除了所述写入请求类型的受限子集之外的写入请求类型,拒绝所述模拟存储器访问请求。

两阶段地址转换

[0001] 本申请涉及数据处理领域。更具体地,本申请涉及存储器管理。

[0002] 数据处理装置可以具有存储器管理电路,以基于地址映射和在转换表中定义的访问许可信息来执行地址转换并且控制是否允许对特定地址的访问。存储器管理电路可支持两阶段地址转换,其中从虚拟地址到物理地址的转换取决于从虚拟地址到中间地址的阶段1映射和从中间地址到物理地址的阶段2映射。这可用于支持虚拟化,其中多个客户操作系统可共存于同一硬件平台上,其中阶段1映射主要由客户操作系统控制并且阶段2映射主要由管理程序控制,使得中间地址(从客户操作系统的观点看来似乎是指物理存储器)可被重新映射到不同物理地址。两阶段地址转换可用于避免由不同客户操作系统设定的冲突中间地址之间的冲突,并且可用于在客户操作系统所看到的硬件资源的虚拟化视图与处理装置中所提供的实际硬件资源之间进行映射。

[0003] 至少一些示例提供了一种装置,该装置包括:处理电路,该处理电路用于在与不同特权等级相关联的多个执行状态中的一者中处理指令;和存储器管理电路,该存储器管理电路响应于存储器访问请求而将由存储器访问请求指定的目标虚拟地址转换成指示待访问的存储器系统位置的目标物理地址;其中:存储器管理电路被配置为支持基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从目标虚拟地址到目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,阶段1地址映射包括从目标虚拟地址到由对应阶段1转换表条目指定的对应于目标虚拟地址的目标中间地址的映射,并且阶段2地址映射包括从目标中间地址到由对应阶段2转换表条目指定的对应于目标中间地址的目标物理地址的映射;存储器管理电路被配置为至少基于由对应阶段2转换表条目指定的阶段2访问许可信息来执行针对存储器访问请求的许可检查,阶段2访问许可信息具有指定对应于目标中间地址的存储器区域是否具有部分只读许可的编码,部分只读许可指示当处理电路处于该多个执行状态中的预定执行状态时发出的针对对应于目标中间地址的存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了受限子集之外的写入请求类型被禁止,写入请求类型的受限子集包括由存储器管理电路生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;并且存储器管理电路被配置为响应于确定存储器访问请求是在预定执行状态下发出的写入请求、阶段2访问许可信息指定对应于目标中间地址的存储器区域具有部分只读许可、并且存储器访问请求是除了写入请求类型的受限子集之外的写入请求类型,拒绝该存储器访问请求。

[0004] 至少一些示例提供了一种方法,该方法包括:在与不同特权等级相关联的多个执行状态中的一者中处理指令;以及响应于存储器访问请求而执行由存储器访问请求指定的目标虚拟地址到指示待访问的存储器系统位置的目标物理地址的两阶段地址转换,该两阶段地址转换基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从目标虚拟地址到目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,阶段1地址映射包括从目标虚拟地址到由对应阶段1转换表条目指定的对应于目标虚拟地址的目标中间地址的映射,并且阶段2地址映射包括从目标中

间地址到由对应阶段2转换表条目指定的对应于目标中间地址的目标物理地址的映射;至少基于由对应阶段2转换表条目指定的阶段2访问许可信息来执行针对存储器访问请求的许可检查,阶段2访问许可信息具有指定对应于目标中间地址的存储器区域是否具有部分只读许可的编码,部分只读许可指示当处理电路处于该多个执行状态中的预定执行状态时发出的针对对应于目标中间地址的存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了受限子集之外的写入请求类型被禁止,写入请求类型的受限子集包括由存储器管理电路生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;响应于确定存储器访问请求是在预定执行状态下发出的写入请求、阶段2访问许可信息指定对应于目标中间地址的存储器区域具有部分只读许可、并且存储器访问请求是除了写入请求类型的受限子集之外的写入请求类型,拒绝该存储器访问请求。

[0005] 至少一些示例提供了一种计算机程序,该计算机程序包括用于控制主机数据处理装置以提供用于执行目标代码的指令执行环境的指令,该计算机程序包括:处理程序逻辑,该处理程序逻辑用于模拟在与不同特权等级相关联的多个执行状态中的一者中处理目标代码的指令;以及存储器管理程序逻辑,该存储器管理程序逻辑用于响应于存储器访问请求而将由目标代码触发的模拟存储器访问请求所指定的目标虚拟地址转换成指示待访问的模拟存储器系统位置的目标物理地址;其中:存储器管理程序逻辑被配置为支持基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从目标虚拟地址到目标物理地址的映射取决于阶段1地址映射和阶段2地址映射,阶段1地址映射包括从目标虚拟地址到由对应阶段1转换表条目指定的对应于目标虚拟地址的目标中间地址的映射,并且阶段2地址映射包括从目标中间地址到由对应阶段2转换表条目指定的对应于目标中间地址的目标物理地址的映射;存储器管理程序逻辑被配置为至少基于由对应阶段2转换表条目指定的阶段2访问许可信息来执行针对模拟存储器访问请求的许可检查,阶段2访问许可信息具有指定对应于目标中间地址的存储器区域是否具有部分只读许可的编码,部分只读许可指示当处理程序逻辑处于该多个执行状态中的预定执行状态时发出的针对对应于目标中间地址的存储器区域的写入请求对于写入请求类型的受限子集被许可,但是对于除了受限子集之外的写入请求类型被禁止,写入请求类型的受限子集包括由存储器管理程序逻辑生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求;并且存储器管理程序逻辑被配置为响应于确定模拟存储器访问请求是在预定执行状态下发出的写入请求、阶段2访问许可信息指定对应于目标中间地址的存储器区域具有部分只读许可、并且模拟存储器访问请求是除了写入请求类型的受限子集之外的写入请求类型,拒绝模拟存储器访问请求。

[0006] 计算机程序可存储在计算机可读存储介质上。该记录介质可以是非暂态存储介质。

[0007] 本技术的另外的方面、特征和优点将从结合附图阅读的示例的以下描述中显而易见,在这些附图中:

[0008] 图1示出了具有处理电路和存储器管理电路的数据处理装置的示例;

[0009] 图2示出了处理电路的执行状态的示例;

[0010] 图3示出了两阶段地址转换;

[0011] 图4和图5分别示出了针对阶段1和阶段2地址转换的转换表遍历的示例;

[0012] 图6示出了当考虑到在阶段1确定的每个表基地址和最终中间地址将使用相应的阶段2转换被转换成物理地址时,针对阶段1和阶段2转换两者的全转换表遍历执行的表查找;

[0013] 图7示出了用于控制存储器管理的存储器管理电路和控制寄存器的示例;

[0014] 图8示出了针对阶段1和阶段2地址转换的转换表条目的示例;

[0015] 图9示出了被允许和被禁止向由阶段2转换表条目限定的部分只读存储器区域写入的写入请求的类型;

[0016] 图10示出了用于执行地址转换和许可检查的方法;

[0017] 图11是示出基于部分只读许可的检查的流程图;

[0018] 图12、图13和图14示出了受保护条目检查类型的读取检查写入指令的不同变体的处理;

[0019] 图15示出了将虚拟地址混叠到相同中间地址上;

[0020] 图16示出了抗混叠检查;

[0021] 图17示出了阶段1顶层表存在检查和阶段1顶层部分只读检查;并且

[0022] 图18示出了可以使用的模拟器具体实施。

[0023] 部分只读阶段2访问许可

[0024] 一种装置具有处理电路和存储器管理电路,该处理电路用于在与不同特权等级相关联的多个执行状态中的一者中处理指令;该存储器管理电路用于响应于存储器访问请求而将由存储器访问请求指定的目标虚拟地址转换成指示待访问的存储器系统位置的目标物理地址。存储器管理电路支持基于包括阶段1转换表条目的阶段1转换表结构和包括阶段2转换表条目的阶段2转换表结构的两阶段地址转换,其中从目标虚拟地址到目标物理地址的映射取决于阶段1地址映射和阶段2地址映射。阶段1地址映射包括从目标虚拟地址到由对应阶段1转换表条目指定的对应于目标虚拟地址的目标中间地址的映射。阶段2地址映射包括从目标中间地址到由对应阶段2转换表条目指定的对应于目标中间地址的目标物理地址的映射。

[0025] 在支持两阶段地址转换的系统中,阶段1地址映射通常由操作系统控制,而阶段2地址映射通常由管理程序控制。因此,用于存储阶段1地址映射的存储器系统位置通常可由操作系统写入,使得操作系统可维持由阶段1转换表条目表示的地址映射和许可。现代操作系统软件可相对较大,并且因此可具有涉及对存储器的写入的许多代码行,如果存储指令的地址操作数被设置为对应于用于保存阶段1转换表条目的存储器区域,则可能能够引起对阶段1转换表条目的更新。因此,操作系统可呈现大的攻击表面,其可由攻击者使用以试图获得对敏感数据或代码的访问或破坏在装置上执行的软件的功能,这是通过使得操作系统代码破坏阶段1转换表条目中的一些条目以便改变访问许可或地址映射并且规避旨在使用阶段1转换表条目实现的存储器管理控制来实现的。因此,可能需要提供防范措施以防止某些阶段1转换表条目的损坏(可能不必将此防范措施应用于所有阶段1转换表条目,因为某些阶段1转换表条目可对应于用于保存非敏感信息的存储器区域)。

[0026] 已经提出的用于强化阶段1转换表对抗攻击的一种方法是提供与用于指向常规阶段1转换表的基地址分开的另选基地址。另选基地址指向一组另选阶段1转换表。另选转换表基地址和一组另选阶段1转换表可由管理程序而非操作系统控制,并且可用于控制对地

址空间的敏感区域的特定子集的访问。另选转换表结构的每一级处的转换表条目可以指定重新开始指示符,该重新开始指示符指示一组另选阶段1转换表的转换表遍历是否应当被停止并且改为使用常规阶段1转换表来重新开始。如果在另选转换表结构遍历期间没有遇到重新开始转换表遍历的指示,则最终到达地址映射(由作为另选转换表的一部分的管理程序控制),并且这可以用于标识保存敏感信息的存储器区域的中间地址。然而,如果重新开始指示符指定转换表遍历应当在转换表结构的给定级别处停止并重新开始,则从用于由操作系统控制的常规阶段1转换表的基地址开始发起另一转换表遍历。该方法允许基于不能被操作系统篡改的另选转换表结构来控制对某些敏感存储器区域的访问,而不需要被保护以免受攻击的其他存储器区域可以基于由操作系统设置的一组常规阶段1转换表来控制它们的访问。然而,该方法的问题在于,对于对非敏感存储器区域的访问,由于执行两个单独的转换表遍历操作,使得已经缓慢的转换表遍历操作甚至更慢(长达两倍时长):首先遍历另选转换表结构,其次在停止另选结构的遍历之后遍历常规转换表结构。这可能对性能具有显著影响,尤其是如果大多数地址空间不旨在是敏感的并且因此使用常规阶段1转换表。

[0027] 另一种方法可以是使用为对应于用于存储阶段1转换表条目的存储器区域的阶段2转换表条目设置的阶段2访问许可来将该存储器区域标记为只读,这将防止操作系统能够更新阶段1转换表条目。然而,这种方法的问题在于,对于操作系统来说,能够更新阶段1转换表条目中的访问跟踪元数据以记录关于访问或写入给定存储器区域的频繁程度的信息通常是有用的。例如,元数据可以包括访问标记和/或脏标记,该访问标记被设置为跟踪对应存储器区域自从访问标记先前被清除以来已经被访问过至少一次,该脏标记被设置为指示自从脏标记被清除以来已经发生了针对对应存储器区域的至少一次写入。访问跟踪元数据的另一示例可以是对于针对对应给定存储器区域的访问的次数进行计数的访问计数器。此类访问跟踪元数据可用于允许操作系统更有效地管理存储器区域调出到外部存储装置(例如,允许操作系统标识作为调出到外部存储装置的最佳候选的最不频繁访问的页)。因此,如果使用阶段2访问许可信息将用于存储阶段1转换表条目的存储器区域标记为只读,则这将防止对访问跟踪元数据的更新,并且因此可能导致对由操作系统管理的分页和其他操作的较低效管理,这冒着性能损失的风险,因为频繁访问的数据由于关于访问频率的信息的丢失而被分页到外部存储器。

[0028] 在下文讨论的示例中,存储器管理电路至少基于由对应于存储器访问的目标中间地址的对应阶段2转换表条目指定的阶段2访问许可信息来执行对存储器访问请求的许可检查。阶段2访问许可信息具有指定对应于目标中间地址的存储器区域是否具有部分只读许可的编码。部分只读许可可能是可用于选择给定存储器区域的另一许可选项,作为诸如只读、读/写、执行、读取/执行等其他类型许可的替代。虽然只读许可可以禁止对对应存储器区域的所有写入,但是与此相反,部分只读许可指定在处理电路处于该多个执行状态中的预定执行状态时发出的针对对应于目标中间地址的存储器区域的写入请求当中,对于写入请求类型的受限子集被许可,但是对于除了受限子集之外的写入请求类型被禁止的写入请求。写入请求类型的受限子集至少包括由存储器管理电路生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求。存储器管理电路响应于确定存储器访问请求是在预定执行状态下发出的写入请求、阶段2访问许可信息指定对应于目标中间地址的存储

器区域具有部分只读许可、并且存储器访问请求是除了写入请求类型的受限子集之外的写入请求类型,拒绝该存储器访问请求。

[0029] 因此,利用这种方法,控制阶段2访问许可的管理程序可以将用于存储阶段1转换表条目的存储器区域设置为具有部分只读许可,这仍然允许发生对访问跟踪元数据的更新(这将趋向于通过增加诸如对外部存储的分页之类的操作的控制效率来帮助改善性能),但是防止至少一些其他请求类型写入到对应存储器区域。通过将对与部分只读许可相关联的区域的写入能力限制到写入请求类型的受限子集,这减少了攻击者可利用的攻击表面,从而增加了针对此类攻击的保护。

[0030] 在一些示例中,元数据更新写入请求可以是受限子集内的唯一类型的写入请求。在这种情况下,如果操作系统需要更新存储在由阶段2访问许可信息标记为部分只读的存储器区域中的阶段1转换表条目,则更新可能失败并且捕获到管理程序,管理程序然后可以确定由操作系统请求的更新是否适当并且然后可以在将控制返回到操作系统之前对更新进行仿真。

[0031] 然而,在实践中,对阶段1转换表条目的更新可能相对频繁,并且因此在每次更新时捕获到管理程序可能影响性能。因此,写入请求类型的受限子集还包括响应于由处理电路在预定执行状态中执行的至少一个预定类型的转换表条目更新指令而发出的写入请求可能是有用的。另一方面,响应于由处理电路在预定执行状态中执行的至少一种类型的存储指令而发出的写入请求可以从写入请求类型的受限子集中排除。因此,通过限制允许写入到部分只读区域的写入请求的类型,这减少了攻击者修改存储指令的行为以导致阶段1地址转换表条目的损坏的机会。由于写入部分只读区域的能力被限制于旨在更新转换表条目的专用指令类型的受限子集,这意味着在操作系统代码的部分中使用的其他类型的通用存储指令(不是由代码作者旨在更新转换表条目)不能被黑客攻击以使得它们破坏存储在存储器的部分只读区域中的转换表条目。转换表条目更新指令可使得处理电路执行至少一个附加检查,其将不响应于用于触发对存储器的写入的其他类型的存储指令而执行,以增加安全性。

[0032] 预定执行状态可以是与操作系统特权等级相关联的执行状态。例如,在下面的示例中,预定执行状态可以是异常层级EL1。在一些示例中,由预定执行状态强加的写入限制可仅在处理电路处于该预定执行状态或较低特权执行状态时应用。另选地,不管当前执行状态如何,可以应用针对被标记为部分只读的区域的写入限制,使得它们应用在包括预定执行状态的所有执行状态中。然而,由于至少对于在预定执行状态中发出的存储器访问请求,基于部分只读许可来施加对写入能力的限制,使得在该预定执行状态中发出的一些写入请求类型可以被允许而其他写入请求类型可以不被允许,这提供了与也被实现的任何基于特权的控制正交的附加控制,其可以允许对操作系统更新用于存储阶段1转换表条目的某些存储器区域中的数据的能力的进一步限制,而不损害存储器管理电路发出用于更新转换表条目中的访问跟踪元数据的写入的能力。

[0033] 在一些实施方案中,存储器管理电路被配置为允许响应于由处理电路在比预定执行状态更具特权的执行状态中执行的该至少一种类型的存储指令而发出的写入请求写入到具有部分只读许可的存储器区域。然而,在实践中,这不是必要的,因为通常在更具特权的执行状态中操作的管理程序在任何情况下可以使用与由操作系统在预定执行状态下使

用的阶段2转换表不同的一组转换表,使得即使用于存储阶段1转换表条目的存储器区域在由操作系统使用的阶段2转换表中被标记为部分只读,这也不意味着相同的存储器区域必须在由管理程序使用的转换表中被标记为部分只读。该存储器区域可以被定义为在由管理程序使用的转换表中是可写入的,并且因此即使由操作系统使用的阶段2转换表将该区域标记为部分只读,管理程序仍然能够在对应阶段1转换表条目中设置信息(诸如阶段1地址映射本身和/或定义受保护条目的位字段,如在以下示例中进一步讨论的)。

[0034] 阶段2访问许可信息可以由对应阶段2转换表条目直接或间接(或两者的组合)指定。通过直接指定,阶段2转换表条目的编码本身指定阶段2访问许可信息。通过间接指定,阶段2转换表条目的编码可以指定引用存储在与阶段2转换表条目分离的结构中的多组阶段2访问许可信息中的一组的值。例如,可以提供许可间接寄存器,其包括多个许可字段,每个许可字段可以被设置为指示对应许可类型的编码。阶段2转换表条目的一部分可被解释为索引值,该索引值用于选择许可间接寄存器的许可字段中的哪一者为该阶段2转换表条目提供阶段2访问许可信息。因此,在一些示例中,指定部分只读许可的信息可以直接在阶段2转换表条目中指定。在其他示例中,指定部分只读许可的信息可由阶段2转换表条目间接指定,该阶段2转换表条目指定到阶段2许可间接寄存器(或其他数据结构)的字段中的索引,该索引被编码为指示部分只读许可。使用访问许可的间接指定可以是有用的,因为其允许软件通过对间接寄存器的同一字段的单次写入来更新若干不同转换表条目的许可,而不需要单独地更新每个转换表条目,该若干不同转换表条目各自参考间接寄存器的该字段。在一些具体实施中,使用间接寄存器还可以帮助支持比可以在转换条目本身中编码的更多数量的许可类型选项。

[0035] 受保护的阶段1转换表条目

[0036] 一些具体实施可以假设存储在由阶段2访问许可标记为部分只读的存储器区域内的所有转换表条目应当被认为对于不是在预定执行状态中发出的请求类型的受限子集中的一者的写入请求是只读的。然而,在实践中,对应于阶段2转换条目的给定存储器区域可存储包括对应于不同存储器区域的大量不同阶段1转换表条目的转换表,并且并非所有那些存储器区域都可能需要保护对应阶段1转换表条目以免被来自操作系统的不适当写入访问请求损坏。例如,由不同的阶段1转换表条目表示的存储器区域可以对应于敏感信息和非敏感信息的混合。如果仍然希望允许操作系统更新与非敏感信息相关联的阶段1转换表条目,尽管对应存储器区域在阶段2访问许可中被设置为具有部分只读许可,则一种方法可以是将每个更新捕获到可以决定更新是否被许可的管理程序。然而,此类更新请求可能相对频繁,并且因此这可能导致性能的损失。

[0037] 因此,在下文讨论的示例中,每个阶段1转换表条目可具有指定该条目是否是受保护条目的编码,与未被编码为受保护条目的阶段1转换表条目相比,该受保护条目的更新受限。这使得能够将对应于敏感信息和非敏感信息的条目彼此区分开,以允许与非受保护条目相比对那些受保护条目的更新进行更严格的检查。例如,允许向部分只读存储器区域写入的上述预定类型的转换表条目更新指令可以包括检查存储在写入请求所针对的存储器区域处的数据是否被编码为受保护条目,并且当发现存储器区域的内容被编码为受保护条目时抑制对存储器区域的至少一些位的写入。另一方面,对于非受保护条目,可允许响应于转换表条目更新指令而写入(假定满足任何其他访问许可检查)。因此,通过提供对将阶段1

转换表条目编码为受保护条目的支持,从而区别于其他非受保护条目,这可使得能够在无管理程序干预的情况下更新非受保护条目,这可帮助改进性能。

[0038] 该装置可以具有受保护条目检查电路,该受保护条目检查电路用于基于给定的阶段1转换表条目是否被标记为受保护条目来检查是否将更新限制到由给定的阶段1转换表条目指定的访问许可或地址映射。在转换表条目指定访问跟踪元数据的情况下,可以不基于该条目是否被保护来限制对访问跟踪元数据的更新,并且因此即使当正在更新的阶段1转换表条目是受保护条目时,也可以允许由硬件中的存储器管理电路生成的元数据更新写入请求(例如在页表遍历操作期间)。

[0039] 当与单独使用任一特征相比时,在阶段2访问许可信息中定义的部分只读许可和用于阶段1转换表条目的受保护条目编码的组合可以是特别有效的。尽管有可能在阶段2处支持部分只读许可而不支持受保护的阶段1转换表条目的编码,但是如上所述,这将趋向于需要频繁捕获到管理程序。因此,这些特征的组合可以是特别有效的。

[0040] 在一些示例中,阶段1转换表条目的编码该条目是否是受保护条目的信息可为专用位或字段,其被视为指示该条目在处理电路的所有模式或操作状态下是否是受保护条目。然而,根据处理电路的操作模式或根据存储在控制寄存器中的控制状态,以不同方式解释用于对条目是否是受保护条目进行编码的阶段1转换表条目的信息也是可能的。例如,控制寄存器中的控制值可以指示阶段1转换表条目的特定位或位字段是否将被解释为指示该条目是受保护条目,或者以另一种方式(例如,根据在不支持受保护条目编码的系统中使用的传统编码)被解释。因此,虽然装置可支持在至少一种操作状态下将阶段1转换表条目编码为受保护条目,但阶段1转换表条目编码其是否在处理电路的所有操作状态中受保护并非必要。在一些示例中,阶段1转换表条目是否受保护可部分地取决于条目本身的编码,并且部分地取决于存储在控制寄存器中的控制值。

[0041] 受保护条目检查类型的读取检查写入指令

[0042] 处理电路可支持用于请求对给定存储器系统位置的更新的受保护条目检查类型的读取检查写入(RCW)指令。受保护条目检查电路可响应于处理电路执行受保护条目检查类型的RCW指令而:从给定存储器系统位置读取数据,检查从给定存储器系统位置读取的数据是否具有与被指定为受保护条目的阶段1转换表条目一致的值,并且响应于确定从给定存储器系统位置读取的数据具有与被指定为受保护条目的阶段1转换表条目一致的值,防止阶段1转换表条目的更新受限位子集响应于读取检查写入指令而被更新。因此,通过在由处理电路支持的指令集架构中支持触发待更新的数据是否具有与受保护的阶段1转换表条目的编码一致的值的检查的指令,这避免了每次更新捕获到管理程序的需要,并且因此提供用于操作系统在没有管理程序干预的情况下更新非受保护的阶段1转换表条目以改善性能的机制。

[0043] 需注意,对所读取的数据的检查可能不能肯定地区分该数据实际上是旨在作为阶段1转换表条目还是仅仅是具有为了其他目的而设置的值的一些数据。该检查可确定数据的值是否与被指定为受保护条目的阶段1转换表条目的编码一致(例如,检查数据的某些位是否匹配在受保护的阶段1转换表条目存储于给定存储器系统位置处的情况下那些位将具有的值)。

[0044] 受保护条目检查类型的RCW指令可以是允许写入到存储器的部分只读区域的写入

请求类型的受限子集中的一者,使得当存储器的区域被标记为部分只读时,其可通过阶段2访问许可检查。

[0045] 指定给定的阶段1转换表条目是否是受保护条目的信息的设置可由以比预定执行状态更高的特权等级执行的软件(诸如,管理程序)来控制。例如,当初始化对应操作系统时,管理程序可以在首先将一组阶段1转换表条目写入存储器时指定特定受保护的阶段1转换表条目。这是可能的,因为由管理程序使用的转换表结构的阶段2转换表条目可以不限制对对应存储器结构的写入被管理程序写入。虽然随后可允许操作系统更新非受保护的阶段1转换表条目,但受保护条目可具有不可响应于由操作系统执行的指令而改变的至少一些位。

[0046] 受保护条目检查类型的RCW指令的读取、检查和写入可以由受保护条目检查电路作为原子操作来执行。因此,读取、检查和写入可被视为结果被完全观察到或根本未观察到的不可分的一组操作,使得在数据处理装置上执行的其他软件进程不可能看到执行受保护条目检查类型的RCW指令的部分结果,或不可能在针对RCW指令执行的读取与写入之间的时段中写入到正由RCW指令读取/写入的存储器位置。这防止了在响应于受保护条目检查类型的RCW指令而执行的读取与写入之间的时段中另一软件进程可能对给定存储器系统位置进行写入的情况下可能发生的竞争条件的出现。

[0047] 在对受保护条目编码的检查之后允许对存储器系统位置的更新并且因此响应于受保护条目检查类型的RCW指令而更新给定存储器系统位置的至少一个位的情况下,受保护条目检查电路可禁止对给定存储器系统位置的更新改变存储在给定存储器系统位置处的阶段1转换表条目的受保护规范。因此,虽然对于非受保护条目,可以允许操作系统更新该条目的部分,但是操作系统不能使用RCW指令来使得该条目成为受保护条目。此外,不能通过执行受保护条目检查类型的RCW指令来将受保护条目转换为非受保护条目。这确保了由管理程序对某些阶段1转换表条目施加的保护不能被执行RCW指令的操作系统规避,并且攻击者不能使得由攻击者创建的任意转换表条目被标记为受保护,这可能使得依赖于受保护条目被管理程序授权的假设的其他安全检查被规避。

[0048] 不同的具体实施可以具有用于控制对受保护的阶段1转换表条目的更新被限制的程度的不同机制。

[0049] 在一些示例中,更新受限位子集可以包括阶段1转换表条目的所有位。因此,在执行受保护条目检查类型的RCW指令并且发现从给定存储器系统位置读取的数据具有与受保护阶段1转换表条目一致的值的情况下,则可整体抑制对给定存储器系统位置处的数据的所请求更新。然而,这并不阻止阶段1转换表条目中的访问跟踪元数据响应于在我们的转换表遍历期间由存储器管理电路在硬件中生成的元数据更新写入请求而被更新(用于限制响应于RCW指令的更新的受保护条目检查不适用于元数据更新写入请求)。

[0050] 在其他示例中,更新受限位子集可包括阶段1转换表条目的适当位子集,使得即使对于受保护条目,一些位仍可由受保护条目检查类型的RCW指令更新,而其他位被禁止更新。更新受限位子集可包括用于对阶段1转换表条目是否是受保护条目进行编码的至少任何一个或多个位,以防止操作系统能够将受保护条目转换为非受保护条目,或反之亦然,如上文所讨论。然而,应认识到,可能存在阶段1转换表条目的其他位,其可由操作系统更新而没有规避由管理程序预期的保护的风险,并且因此即使该条目是受保护条目也允许更新一

些位可以是有用的。

[0051] 在更新受限位子集包括适当位子集(其中至少一个其他位不具有响应于受保护条目检查类型的RCW指令而受限的更新)的示例中,一些具体实施可以固定对哪个位子集是更新受限位子集的选择。因此,选择哪些位在适当位子集中可以是不可编程的。例如,对更新限制位的选择可以是由处理电路支持的指令集架构所规定的硬连线架构选择。

[0052] 另选地,取决于存储在控制寄存器中的软件可编程的选择值,选择哪些位在更新受限位子集中可以是可编程的。这可以允许某些软件根据该软件的需要编程哪些特定位应当使其更新受限。例如,更新存储在控制寄存器中的软件可编程的选择值的能力可限于在具有至少特定阈值特权等级(其可例如为管理程序的特权等级)的执行状态中执行的软件。在上述预定执行状态中执行的软件可以不被允许写入软件可编程的选择值。

[0053] 在一些具体实施中,每个有效的阶段1转换表条目可具有指定该条目是否是受保护条目的编码。然而,无效的阶段1转换表条目可能不能被编码为受保护或非受保护,并且可以默认地被假定为非受保护条目。在这种情况下,可允许无效条目由RCW指令更新,只要更新不使得条目变为有效且受保护,则允许更新条目的任何部分。因此,响应于确定从给定存储器系统位置读取的数据具有与无效的阶段1转换表条目一致的值,受保护条目检查电路可以允许无效的阶段1转换表条目的更新,不同于使得给定存储器系统位置处的数据变为被指定为受保护条目的有效的阶段1转换表条目的更新。

[0054] 然而,在其他具体实施中,有效和无效的阶段1转换表条目都可以具有指定该条目是否是受保护条目的编码。在这种情况下,响应于确定从给定存储器系统读取的数据具有与被指定为受保护条目的无效的阶段1转换表条目一致的值,受保护条目检查电路可以防止给定存储器系统位置的无效条目更新受限位子集响应于读取检查写入指令而被更新;并且响应于确定从给定存储器系统读取的数据具有与被指定为受保护条目的有效的阶段1转换表条目一致的值,受保护条目检查电路可以防止给定存储器系统位置的有效条目更新受限位子集响应于读取检查写入指令而被更新。这种方法可以是有用的,因为它允许管理程序初始化一组阶段1转换表条目,其中一些条目受保护,包括一些无效条目,这些无效条目当前不能用于允许对存储器的访问,但是稍后可以使其有效,同时在转换表条目还无效的时段内仍然受保护以防止未经授权的更新。

[0055] 在一些具体实施中,有效条目更新受限位子集可以与无效条目更新受限位子集处于相同的位位置。另选地,与无效条目更新受限位子集相比,有效条目更新受限位子集可以是转换表条目编码的不同的位子集。根据存储在控制寄存器中的软件可编程的有效条目更新受限位选择值,有效条目更新受限位子集可以是阶段1转换表条目的所有位、阶段1转换表条目的非可编程选择的适当位子集、或阶段1转换表条目的可编程选择的适当位子集。相似地,根据存储在控制寄存器中的软件可编程的无效条目更新受限位选择值,无效条目更新受限位子集可以是阶段1转换表条目的所有位、阶段1转换表条目的非可编程选择的适当位子集、或阶段1转换表条目的可编程选择的适当位子集。用于选择哪些位是有效条目更新受限位子集所采取的方法可以与用于选择哪些位是无效条目更新受限位子集所采取的方法相同或不同。例如,有效受保护条目的所有位可使其更新受限,而无效受保护条目的仅位子集可使其更新受限。另选地,更新受限位可以被可编程地选择用于无效/有效条目中的一者而不是另一者。例如,一个示例性具体实施可以提供掩码寄存器来选择哪些位是有效条

目更新受限位子集,但是选择哪些位是无效条目更新受限位子集可以是由指令集架构规定的固定选择。因此,应当理解,存在用于选择在有效和无效的阶段1转换表条目中哪些位更新受限的多种选项。

[0056] 在一些示例中,有效的阶段1转换表条目可包括指示该有效的阶段1转换表条目是否是受保护条目的第一位字段;并且无效的阶段1转换表条目可包括指示该无效的阶段1转换表条目是否是受保护条目的第二位字段。第一位字段和第二位字段可处于阶段1转换表条目编码内的相同位位置处,或处于阶段1转换表条目编码内的不同位位置处。在一些情况下,将第一位字段和第二位字段定位在不同位位置处可为软件在其如何布置其数据方面提供更多灵活性。无效的转换表条目编码由软件用于任何任意非转换表数据。在有效的转换表条目编码中,可能仅存在可用于对"受保护状态"进行编码的有限位。因此,如果用于对受保护状态进行编码的位字段在有效和无效条目中的相同位位置处,则这可约束软件可如何使用其在并非旨在用作转换表条目的存储器位置中的数据。通过允许第一位字段和第二位字段的位字段位置不同,无效的阶段1转换表条目编码内的第二位字段可以位于不太可能导致软件使用正常数据的不便的位置处,即使该位置由于已经为有效的阶段1转换表条目内的其他信息分配的位位置而不适于有效的阶段1转换表条目。

[0057] 可以以不同方式允许对(有效或无效)受保护的阶段1转换表条目的更新受限位子集的更新的抑制。在一些示例中,如果确定更新受限位子集中的至少一者正被请求更新且从给定存储器系统位置读取的数据具有与表示受保护条目的数据一致的编码,则受保护条目检查电路可简单地整体抑制对给定存储器系统位置的更新,包括对除了更新受限位子集以外的位的任何更新。在这种情况下,如果试图写入任何更新受限位,则写入失败。

[0058] 在其他示例中,仅可抑制对更新受限位子集的更新,而仍可允许对给定存储器系统位置的至少一个其他(非更新受限)位的更新。在这种情况下,对于受保护条目,写入成功地更新到允许写入更新的位,但是即使基于RCW指令的操作数请求这样做,也不改变更新受限位。

[0059] 响应于受保护条目检查类型的读取检查写入指令,处理电路可以设置至少一个条件状态值以指示基于对从给定存储器系统读取的数据是否是被指定为受保护条目的阶段1转换表条目的检查,是否抑制由受保护条目检查类型的读取检查写入指令请求的更新的至少一部分。该至少一个条件状态值可由后续条件指令(例如条件比较指令或条件分支指令)测试以允许根据由RCW指令请求的更新是否成功的条件而进行后续操作。在知道RCW指令是成功还是失败是有用的情况下,这可以帮助改善性能,因为这意味着不需要执行另一组指令来确定写入是否成功。

[0060] 受保护条目检查类型的RCW指令可以以各种方式实现。例如,处理电路可以支持受保护条目检查类型的RCW指令的以下变体中的任何一者或多者:

[0061] ●受保护条目检查类型的读取检查写入指令的交换变体,响应于交换变体,处理电路被配置为将从给定存储器系统位置读取的数据写入到目的地寄存器以供后续指令用作操作数。该变体可以是有用的,使得后续指令可以在更新之前以转换表条目的先前状态为条件执行操作。

[0062] ●受保护条目检查类型的读取检查写入指令的存储变体,针对存储变体,处理电路被配置为处理存储变体而不将从给定存储器系统位置读取的数据写入到目的地寄存器。

如果后续操作不需要依赖于给定存储器系统位置的旧内容,则该变体可以是有用的,以避免不必要地消耗目的地寄存器。在一些示例中,交换变体和存储变体可具有共同编码,并且当交换变体的目的地寄存器说明符指定预定值时,这可使得将指令视为不需要返回从给定存储器系统位置读取的数据的存储变体。其他架构可以将存储变体提供为与交换变体分离的独立指令。

[0063] ●指定比较操作数的受保护条目检查类型的读取检查写入指令的比较和交换变体,针对该指令,受保护条目检查电路被配置为确定从给定存储器系统位置读取的数据与比较操作数的比较是否满足比较条件,在不满足比较条件时抑制对给定存储器系统位置的更新,并且将从给定存储器系统位置读取的数据写入到目的地寄存器以供后续指令用作操作数。比较和交换变体还可致使状态信息被设置用于指示是否满足比较条件(例如,设置可由后续条件指令测试的一个或多个条件标志)。响应于比较和交换变体,与在满足比较条件但所请求的写操作的至少一部分被抑制时相比,当未满足比较条件时,状态信息可被设置为不同状态,这是因为当写入正在请求对更新受限位的更新时,读取数据被编码为受保护阶段1转换表条目。

[0064] ●位设置/清除指令,针对该指令,给定存储器系统位置的更新包括设置或清除在给定存储器系统位置处的数据的至少一个选定位。例如,位设置/清除指令的操作数可指定位掩码,该位掩码指示将在给定存储器系统位置处的数据中设置或清除的位的位置。任选地,位设置/清除指令还可致使从给定存储器系统位置读取的数据返回到目的地寄存器以供后续指令用作操作数,类似于交换变体及比较和交换变体。

[0065] 应当理解,并非所有这些变体都需要在数据处理装置的任何给定具体实施中得到支持。

[0066] 抗混叠

[0067] 以上讨论的技术可用于允许在恶意方的攻击下保护阶段1转换表条目的特定集合免于被操作系统破坏。这可保护将特定虚拟地址映射到特定中间地址的条目免于被破坏。然而,有可能提供将不同虚拟地址映射到相同中间地址的两个或更多个不同的阶段1转换表条目。因此,即使特定的阶段1转换表条目被保卫免于破坏(通过使用部分只读许可和任选地使用受保护条目编码),也可能存在以下风险:攻击者可能尝试设置将另一虚拟地址映射到由受保卫的阶段1转换表条目指定的相同中间地址的另一阶段1转换表条目以规避应用于该受保卫条目的保护。用于解决该问题的一种方法可以是在设置或使用阶段1转换表条目时引入检查以检查它们没有映射到已经使用受保护的阶段1转换表条目来映射的中间地址,但是这在性能方面是极其昂贵的并且在实践中难以实现。

[0068] 在下文讨论的示例中,对应于给定中间地址的给定的阶段2访问转换表条目具有指定对应于给定中间地址的存储器区域是否具有指示以下要求的抗混叠性质的编码:针对将被允许的对与给定中间地址相对应的存储器区域的访问,将在阶段1转换结构的转换表遍历中被访问以定位指定从给定虚拟地址到给定中间地址的阶段1地址映射的对应阶段1转换表条目的一个或多个遍历的阶段1转换表条目中的每一者被要求满足抗混叠条件。在以下情况下认为满足针对给定的遍历的阶段1转换表条目的抗混叠条件:(a)给定的遍历的阶段1转换表条目被指定为受保护条目,并且部分只读许可由针对相关阶段2转换表条目的阶段2访问许可信息指定,该转换表条目提供用于导出存储给定的遍历的阶段1转换表条目

的存储器系统位置的物理地址的阶段2地址映射,或(b)只读许可由针对相关阶段2转换表条目的阶段2访问许可信息指定。存储器管理电路响应于确定对应的阶段2转换表条目指定对应于目标中间地址的存储器区域具有抗混叠性质并且一个或多个遍历的阶段1转换表条目中的任一者未能满足抗混叠条件而拒绝存储器访问请求。

[0069] 该方法保护免于以上讨论的基于阶段1转换表条目的混叠的攻击。如果存在对应于需要被保护免于攻击的敏感信息的给定中间地址,针对该给定中间地址,用于标识虚拟地址到该中间地址的映射的阶段1转换表条目通过将该条目存储在部分只读存储器中并且将该阶段1转换表条目编码为受保护条目来进行保护,则控制阶段2转换表条目的管理程序还可将对应于给定中间地址的给定阶段2转换表条目标记为具有抗混叠性质。这意味着即使攻击者致使操作系统代码创建映射到相同中间地址的新阶段1转换表条目,或者修改通过转换表遍历的遍历路径上的现有阶段1转换表条目以使得不同虚拟地址变为映射到相同中间地址,攻击者也将不能够引起以下两者:新的/经修改的阶段1转换表条目被存储在存储器的部分只读区域中(因为攻击者不能控制阶段2访问许可),并且新条目被编码为受保护条目(如果攻击者写入的区域已经被指示为部分只读区域,则攻击者将需要使用写入请求的受限子集来执行写入,例如使用上述RCW指令,并且此类写入请求类型可能具有强加的限制,即它不能致使被写入的值变为受保护的阶段1转换表条目)。此外,攻击者不能将新混叠条目写入到只读区域。因此,通过在对针对其在对应的阶段2转换表条目中定义了抗混叠性质的存储器区域的访问中检查所遍历的阶段1转换表条目中的每一者(其将在阶段1转换表结构的遍历中被遍历以到达从给定虚拟地址到给定中间地址的阶段1地址映射)是否满足抗混叠条件(基于在阶段2处设置的PRO或只读许可,并且如果指定了PRO,即阶段1条目也是受保护条目),这防止攻击者能够使用混叠作为规避以上讨论的使用部分只读许可和受保护的阶段1条目特征的保护的手段。

[0070] 类似于上文所讨论的部分只读许可和受保护条目编码,抗混叠性质可由阶段2访问转换条目直接或间接地指定,并且可由专用位或位字段或由再用位或位字段指示,该再用位或位字段的解译取决于处理电路的操作状态或控制寄存器中指定的控制信息。

[0071] 阶段1顶层基地址保护检查

[0072] 存储器管理电路可基于阶段1转换表基地址寄存器中的值来确定阶段1转换表结构的阶段1顶层转换表的阶段1顶层基地址。尽管上述特征可保护免于特定阶段1转换表条目的破坏,但是攻击者可尝试规避这些保护的另一种方式可以是修改阶段1顶层基地址以指向与旨在用于授权使用的地址不同的地址,以便用由攻击者定义的另选阶段1转换表集合替换受保护的阶段1转换表集合。

[0073] 用于针对此类攻击进行管制的一种方法可以是捕获由操作系统请求的对阶段1转换表基地址寄存器的任何更新,以致使管理程序检查由操作系统请求的更新是否适当。因此,可能不必需的是提供对于对阶段1转换表基地址寄存器的更新的任何硬件强制检查。

[0074] 然而,在实践中,操作系统对阶段1转换表基地址寄存器的更新可能是相对频繁的(例如,操作系统可在每个上下文切换时这样做),并且因此将每个更新捕获到管理程序可能招致性能成本。因此,一些附加检查可用于改进性能。

[0075] 此类附加检查的一个示例可为阶段1顶层表部分只读检查,其实施阶段1顶层基地址应当对应于针对其相关联的阶段2转换表条目指定上文所讨论的部分只读许可的存储器

区域的要求。因此,当启用阶段1顶层表部分只读检查时,存储器管理电路响应于确定阶段1顶层基地址对应于针对其相关联的阶段2转换表条目未指定部分只读许可的中间地址而发信号通知故障。例如,可在基于存储在阶段1顶层基地址寄存器中的第阶段1顶层基地址执行转换表遍历时执行该检查。该检查意味着管理程序可将保持被许可由操作系统使用的阶段1顶层转换表(其可能已经由管理程序验证为安全)的存储器区域定义为部分只读。攻击者不能在存储器的某个其他区域中定义任意的阶段1顶层转换表并且不能够致使该任意的阶段1顶层转换表被用于页表遍历,并且因此不能使用基地址的重新编程作为用于绕过受保护映射和部分只读保护的手段,该受保护映射和部分只读保护被定义用于经由映射到由管理程序在对应的阶段2转换表条目中定义的部分只读区域的正确基地址可访问的正确阶段1转换表。

[0076] 在一些具体实施中,阶段1顶层部分只读检查可被视为永久启用,使得可能不存在对该检查是被启用还是禁用的任何可编程控制。

[0077] 然而,在其他具体实施中,存储器管理电路可基于存储在控制寄存器中的阶段1顶层部分只读检查启用控制值来确定是否启用阶段1顶层表部分只读检查。写入到控制寄存器中的阶段1顶层部分只读检查启用控制值的能力可限于在阈值特权等级或更高特权等级下执行的软件(例如,阈值特权等级可为管理程序特权等级,比与先前提及的预定执行状态相关联的特权更具特权)。通过提供启用或禁用阶段1顶层表部分只读检查的能力,这允许与未被设计成使用部分只读许可的传统软件的向后兼容性。

[0078] 用于对于对阶段1转换表基寄存器的不适当更新进行管制的检查的另一示例可以是基于使用阶段1或阶段2转换表结构为存储器区域设置的阶段1顶层表存在许可的阶段1顶层表存在许可检查。阶段1顶层表存在许可意味着允许对应存储器区域被分配用于存储阶段1顶层转换表,该转换表可有效地用作基于阶段1顶层基地址寄存器中的地址在阶段1转换表遍历中访问的顶层转换表。因此,当阶段1顶层表存在许可检查被启用时,存储器管理电路确定对应于阶段1顶层基地址的给定存储器区域是否与指示允许给定存储器区域被分配用于存储阶段1转换表结构的阶段1顶层表的阶段1顶层表存在许可相关联,并且在对应于阶段1顶层基地址的给定存储器区域不具有阶段1顶层表存在许可时触发故障。

[0079] 阶段1顶层表存在许可检查帮助针对另一类型的攻击进行管制,其中攻击者可更新阶段1顶层基地址寄存器中的地址以指向用于存储旨在阶段1转换表结构的除顶层之外的另一层级处使用的另一层阶段1转换表条目中的一者的存储器区域。换句话说,不是试图创建全新的转换表条目,攻击者还可通过致使转换表结构的稍后层级处的条目被视为转换表结构的较早层级处的条目来导致对存储器的不适当访问,使得用于从该转换表条目中进行选择的目标地址的位不是预期位子集(表的不同层级由输入地址的不同位子集索引到转换表遍历),从而致使由转换表结构的稍后层级处的不适当访问的条目指定的地址映射或访问许可被应用于与建立转换表结构的一方所预期的虚拟地址不同的虚拟地址。可使用阶段1顶层表存在许可来防止这种攻击,因为用于保持除顶层转换表条目之外的阶段1转换表条目的存储器区域可被定义为不具有阶段1顶层表存在许可,并且因此如果攻击者更新阶段1顶层基地址以指向此类条目,则检测到缺乏存储顶层条目的许可,并且这可致使发信号通知故障。

[0080] 在一些具体实施中,其中提供至少两个阶段1顶层基地址寄存器以存储阶段1顶层

基地址以供在不同存储器访问场景中使用,可支持阶段1顶层表存在许可的至少两个变体,每一变体对应于多个阶段1顶层基地址寄存器的相应子集。当针对给定存储器区域指定阶段1顶层表存在许可的给定变体时,对应存储器区域被指示为被允许分配用于存储使用用于给定变体的阶段1顶层基地址寄存器的对应子集中的一者来访问的阶段1顶层转换表,但是不被允许分配用于存储使用不是用于给定变体的对应子集的成员的阶段1顶层基地址寄存器来访问的阶段1顶层转换表。因此,如果尝试使用特定的阶段1顶层基地址寄存器来执行页表遍历,则可触发故障,该寄存器指定被分配阶段1顶层表存在许可的存储器区域中的地址,针对该地址,阶段1顶层基地址寄存器的对应子集不包括特定的阶段1顶层基地址寄存器。通过支持指示针对基地址寄存器的相应特定子集使用阶段1顶层转换表的对应存储器区域的许可的不同的阶段1顶层表存在许可,这允许更精确的控制,例如使得可防止旨在用于在一个基地址寄存器中使用的基地址被用于另一基地址寄存器。

[0081] 例如,在支持第一阶段1顶层基地址寄存器和第二阶段1顶层基地址寄存器的具体实施中,阶段1顶层表存在许可的变体可包括以下中的至少两者:

[0082] ●第一变体,其中对应子集包括第一阶段1顶层基地址寄存器但不包括第二阶段1顶层基地址寄存器;

[0083] ●第二变体,其中对应子集包括第二阶段1顶层基地址寄存器但不包括第一阶段1顶层基地址寄存器;并且

[0084] ●第三变体,其中对应子集包括第一和第二阶段1顶层基地址寄存器两者。

[0085] 在一个示例中,当针对给定虚拟地址执行阶段1页表遍历时,存储器管理电路可基于给定虚拟地址的最高有效位的一部分是否全为零来选择第一和第二阶段1顶层基地址寄存器中的哪一者用于访问阶段1顶层转换表。被考虑用于该选择的最高有效位的数量可以是固定的,或者可使用由软件配置的控制值来编程。该方法可用于例如允许使用不同转换表集合来转换虚拟地址空间的上限和下限范围。例如,都被设置为零的地址的最高有效位的下限地址范围可用于用户地址空间,并且地址的最高有效部分中的至少一个非零位的上限地址范围可用于内核地址空间。

[0086] 可能的是,给定存储器区域的阶段1顶层表存在许可被编码在对应于该给定存储器区域的阶段1转换表条目的阶段1访问许可内,但是在该情况下,可能期望实现至少一个进一步的保护机制以防止用于编码阶段1顶层表存在许可的位被在具有操作系统特权等级的执行状态下执行的指令修改。

[0087] 相反,可能更方便的是,存储器管理电路基于对应于阶段1顶层基地址的相关联的阶段2转换表条目的编码来确定给定存储器区域是否与阶段1顶层表存在许可相关联。通过使用相关联的阶段2转换表条目来表示给定存储器区域是否被允许保持阶段1顶层转换表,这简化了对由操作系统代码触发的对阶段1转换表条目的更新的控制,该操作系统代码通常将不能够更新阶段2转换表条目。

[0088] 再次,在一些具体实施中,阶段1顶层表存在许可检查可被认为是永久启用的。

[0089] 另选地,存储器管理电路可基于存储在控制寄存器中的阶段1顶层表存在许可检查启用控制值来确定阶段1顶层表存在许可检查是否被启用。写入到控制寄存器中的阶段1顶层表存在许可检查启用控制值的能力可限于在阈值特权等级或更高特权等级下执行的软件(例如,阈值特权等级可为管理程序特权等级)。通过提供启用或禁用阶段1顶层表部分

只读检查的能力,这提供了与不使用阶段1顶层表存在许可的传统软件的向后兼容性。

[0090] 而且,在其中如上文所讨论的那样支持了对应于基地址寄存器的不同子集的阶段1顶层表存在许可的两个或更多个变体的具体实施中,可存在由存储在控制寄存器中的至少一个控制值定义的至少一个进一步控制,其指示阶段1顶层表存在许可的不同变体是否应被视为仅使得能够将对应存储器区域用于阶段1顶层基地址寄存器的对应子集,或每个变体是否可用于使得能够将对应存储器区域用于阶段1顶层基地址寄存器中的任一者。因此,在用于提供阶段1顶层基地址的基地址寄存器不是由针对包括阶段1顶层基地址的存储器区域指定的阶段1顶层表存在许可的变体启用的基地址寄存器子集中的一者时触发的上述故障可基于至少一个另外的控制而被启用或禁用。在一些示例中,可提供单独的控制以用于配置是否针对所使用的阶段1顶层基地址寄存器与阶段1顶层表存在许可的变体的特定组合生成故障。例如,可提供一个控制值,该控制值用于在包括基地址的存储器区域具有上述的阶段1顶层表存在许可的第一变体时,使用第二阶段1顶层基地址寄存器中的基地址来控制是否在页表遍历上生成故障,并且可提供第二控制值,该第二控制值用于在包括基地址的存储器区域具有阶段1顶层表存在许可的第二变体时,使用第一阶段1顶层基地址寄存器中的基地址来控制是否在页表遍历上生成故障。

[0091] 在支持阶段1顶层表部分只读检查和阶段1顶层表存在许可检查两者的一些示例中,可以使用单独启用控制值来分别单独地启用或禁用这些检查。另选地,单个控制值可一起启用/禁用两个检查,使得所支持的选项可以是两个检查都被启用或者两个检查都被禁用,但是可能不能启用一个检查而不能启用另一个。

[0092] 其他具体实施可不支持这两种类型的检查。例如,在一些具体实施中,这些检查的一个检查或另一检查可被认为是足够的。

[0093] 对于部分只读许可,阶段1顶层表存在许可可由转换表条目直接或间接(或两者的组合)指定,例如使用在转换表条目的编码中直接指定的信息和/或参考许可寄存器由转换表条目间接指定的信息。

[0094] 架构模拟

[0095] 上文所讨论技术可以在数据处理装置内实现,该数据处理装置具有提供用于实现指令解码器和上文所讨论的处理电路的硬件电路。

[0096] 然而,同样的技术也可以在计算机程序内实现,该计算机程序在主机数据处理装置上执行以提供用于执行目标代码的指令执行环境。此类计算机程序可以控制主机数据处理装置来模拟将在硬件装置上提供的架构环境,该硬件装置实际上支持根据特定指令集架构的目标代码,即使主机数据处理装置本身不支持该架构。计算机程序可具有处理程序逻辑和存储器管理程序逻辑,其模拟上文所讨论的处理电路和存储器管理电路的功能,包括对上文所讨论的部分只读许可和各种检查的支持。例如,当在支持不同指令集架构的主机处理器上执行针对一种指令集架构编写的遗留代码时,此类模拟程序可以是有用的。另外,模拟可以允许在支持新架构版本的处理硬件准备好之前开始针对指令集架构的较新版本的软件开发,因为软件在模拟执行环境上的执行可以使得软件测试与支持该新架构的硬件设备的正在进行的开发并行地进行。模拟程序可以存储在存储介质上,该存储介质可以是非暂态存储介质。

[0097] 数据处理装置的特定示例

[0098] 图1示意性地示出了数据处理装置2的示例。数据处理装置具有包括多个流水线阶段的处理流水线4。在该示例中,该流水线阶段包括:提取级6,该提取级用于从指令高速缓存8中提取指令;解码级10,该解码级用于解码所提取的程序指令,以生成要由流水线的其余级处理的微操作(经解码指令);发布级12,该发布级用于检查微操作所需的操作数在寄存器文件14中是否可获得,并且一旦给定微操作所需的操作数可用就发布供执行的微操作;执行级16,该执行级用于通过处理从寄存器文件14读取的操作数以生成结果值来执行对应于微操作的数据处理操作;以及写回级18,该写回级用于将处理的结果写回到寄存器文件14。应当理解,这仅仅是可能的流水线架构的一个示例,并且其他系统可具有附加阶段或不同的阶段配置。例如,在乱序处理器中,可以包括寄存器重命名级,该寄存器重命名级用于将由程序指令或微操作指定的架构寄存器映射到标识寄存器文件14中的物理寄存器的物理寄存器指定符。在一些示例中,在由解码级10解码的程序指令与由执行级处理的对应微操作之间可存在一对一关系。还可能的是,程序指令与微操作之间还可能存在一对多或多对一关系,使得例如可将单个程序指令拆分为两个或多于两个微操作,或者可将两个或多于两个程序指令融合,作为单个微操作来处理。

[0099] 执行级16包括用于执行不同类别的处理操作的多个处理单元。例如,执行单元可包括标量算术/逻辑单元(ALU)20,该标量ALU用于对从寄存器14读取的标量操作数执行算术或逻辑操作;浮点单元22,该浮点单元用于对浮点值进行操作;分支单元24,该分支单元用于评估分支操作的结果并且相应地调整表示当前执行点的程序计数器;以及加载/存储单元26,该加载/存储单元用于执行加载/存储操作以访问存储器系统8、30、32、34中的数据。提供了作为存储器管理电路的示例的存储器管理单元(MMU)28,该MMU用于执行由加载/存储单元26基于数据访问指令的操作数指定的虚拟地址与标识数据在存储器系统中的存储位置的物理地址之间的地址转换。MMU具有转换后备缓冲器(TLB)29,该TLB用于高速缓存来自存储在存储器系统中的页表的地址转换数据,其中页表的页表条目限定地址转换映射和管控是否允许流水线上执行的给定进程读取、写入或执行给定存储器区域的指令的访问许可。

[0100] 在该示例中,存储器系统包括一级数据高速缓存30、一级指令高速缓存8、共享二级高速缓存32和主系统存储器34。应当理解,这仅为可能的存储器分级结构的一个示例,并且还可以提供其他高速缓存布置方式。在执行级16中示出的处理单元20至26的具体类型仅为一个示例,并且其他具体实施可具有一组不同的处理单元或可包括同一类型的处理单元的多个实例,使得可以并行处理同一类型的多个微操作。应当理解,图1仅仅是可能的处理器流水线具体实施的一些组件的简化表示,并且处理器可包括其他许多为简洁起见未示出的元件。虽然图1示出了具有对存储器34的访问的单个处理器核,但是装置2还可具有共享对存储器34的访问的一个或多个另外的处理器核,其中每个核具有相应高速缓存8、30、32。

[0101] 图2是示出处理电路4在执行指令时可在其中操作的不同执行状态(也称为异常层级)的示图。在该示例中,存在四个异常层级EL0、EL1、EL2、EL3,其中异常层级EL0是最低特权的异常层级,并且异常层级EL3是最高特权的异常层级。一般来说,当在更具特权的异常层级中执行时,处理电路可访问较低、较不具特权的异常层级不可访问的一些存储器位置或寄存器14。

[0102] 在该示例中,异常层级EL0用于执行由在异常层级EL1处执行的对应操作系统或虚

拟机管理的应用程序。在多个虚拟机共存于相同物理平台上的情况下,则可提供在EL2处操作的管理程序以管理相应虚拟机。虽然图2示出了其中管理程序管理虚拟机并且虚拟机管理应用程序的示例,但是管理程序也可能直接管理EL0处的应用程序。

[0103] 尽管不是必要的,但是一些具体实施可实现针对处理电路的单独的硬件划分的安全和非安全操作域。数据处理系统2可具有在处理器和存储器系统内实现的硬件特征以确保与在安全域中操作的软件进程相关联的数据和代码与在非安全域中操作的进程的访问隔离。例如,可使用诸如由英国剑桥的Arm®有限公司提供的TrustZone®架构的硬件架构。另选地,可使用其他硬件强制的安全划分架构。安全应用程序(可信服务)可在安全域中的异常层级EL0中操作,并且安全(可信)操作系统或虚拟机可在安全域中的异常层级EL1中操作。在一些具体实施中,在安全状态中不存在对EL2的支持,并且管理程序可仅在非安全EL2中执行。在其他具体实施中,可支持在安全EL2中执行的安全管理程序,如图2中的星号所指示的。在一些示例中,可提供用于管理非安全域和安全域之间的转变的安全监测程序,其在异常层级EL3中执行。其他具体实施可管制硬件中的安全域之间的转变,使得可不需要安全监测程序。

[0104] 地址转换

[0105] 由MMU 28执行的一个任务是虚拟地址(VA)与物理地址(PA)之间的地址转换。在处理电路4上执行的软件使用虚拟地址来指定存储器位置,但这些虚拟地址可由MMU 28转换成标识待访问的存储器系统位置的物理地址。使用虚拟地址的益处在于其允许管理软件(诸如操作系统(OS))控制呈现给软件的存储器的视图。OS可控制什么存储器是可见的、该存储器可见的虚拟地址、以及允许对该存储器进行什么访问。这允许OS将应用程序沙箱化(将一个应用程序的资源从另一应用程序进行隐藏)并且提供从底层硬件的抽象。使用虚拟地址的另一益处在于OS可将存储器的多个经分段物理区作为单个连续虚拟地址空间呈现给应用程序。虚拟地址还有益于软件开发者,软件开发者在编写他们的应用程序时将不知道系统的确切存储器地址。利用虚拟地址,软件开发者不需要自己关注物理存储器。应用程序知道由OS和硬件一起工作以执行地址转换。

[0106] 在实践中,每个应用程序可使用其自身的虚拟地址集,该虚拟地址集将被映射到物理系统中的不同位置。当操作系统在不同应用程序之间切换时,其对映射进行重新编程。这意味着当前应用程序的虚拟地址将映射到存储器中的正确物理位置。

[0107] 通过映射将虚拟地址转换为物理地址。虚拟地址与物理地址之间的映射被存储在转换表(有时称为页表)中。转换表被存储在存储器中并由软件(通常是OS或管理程序)管理。转换表不是静态的,并且可根据软件改变的需要来更新表。这改变了虚拟地址和物理地址之间的映射。

[0108] 对于在处理电路4处于特定执行状态子集中时(具体地,在处理电路4处于非安全EL0或非安全EL1中时)执行的存储器访问,如图3所示使用两阶段地址转换(对于其他执行状态,使用阶段1页表的一个地址转换级是足够的)。因此,使用两个表集合来转换来自非安全EL0和非安全EL1的虚拟地址。这些表支持虚拟化并且允许管理程序虚拟化由给定虚拟机(VM)(对应于客户操作系统和由该客户操作系统控制的应用程序的虚拟机)看到的物理存储器的视图。我们将由OS控制的转换集称为阶段1。阶段1表将虚拟地址转换为中间物理地址(IPA-先前提到的中间地址的示例)。在阶段1中,OS认为IPA是物理地址空间。然而,管理

程序控制第二转换集,其被称为阶段2。该第二转换集将IPA转换为物理地址。

[0109] 阶段1和阶段2转换表被实现为分层表结构,该分层表结构包括如图4和图5中分别针对阶段1和阶段2所示的转换表的多个层级。在该示例中,阶段1表和阶段2表两者可具有至多4个页表层级,即层级0(L0)、层级1(L1)、层级2(L2)和层级3(L3)。

[0110] 为了定位给定地址的物理地址映射,执行转换表遍历,包括一个或多个转换表查找。转换表遍历是将虚拟地址转换为物理地址所需的查找集合。对于非安全EL1和0转换体系,该集合包括对阶段1转换和阶段2转换两者的查找(参见下面示出的图6)。由使用阶段1和阶段2查找的成功转换表遍历返回的信息是:

[0111] ●所需的物理地址(基于到中间地址的阶段1映射和到物理地址的阶段2映射而转换)。

[0112] ●目标存储器区域的访问许可和/或存储器属性,其提供关于如何控制对该存储器区域的访问的信息。这些可包括在阶段1表结构中定义的阶段1访问许可和/或属性以及在阶段2表结构中定义的阶段2访问许可和/或属性。

[0113] 为了遍历阶段1和阶段2结构中的给定一者,基于在转换表基地址寄存器(用于阶段1的TTBR,用于阶段2的VTTBR_EL2)中指定的地址,遍历开始于对用于初始查找的顶层(L0)转换表的读取。每个转换表查找返回描述符,该描述符指示以下中的一者:

[0114] ●条目是阶段1或阶段2结构的遍历的最终条目,其提供所寻求的地址映射。如果条目在最终L3中,则该条目被称为页描述符(D_Page),而如果提供遍历的最终条目的条目处于较高层级中的一者处,则其被称为块描述符(D_Block)。遍历的最后条目包含输出地址(OA,即用于阶段1的IPA或用于阶段2的PA)以及针对访问的许可和属性。如果在转换表结构的较高层级处找到块描述符,则这意味着块描述符表示大小比由L3处的单个条目表示的4kB存储器页大的存储器区域(由L1和L2处的块描述符表示的特定大小取决于用于索引到L1或L2表中的索引位的数目—在该示例中,L1和L2块描述符分别表示1GB和2MB区域)。

[0115] ●需要附加查找层级。在该情况下,条目被称为表描述符(D_Table),因为它为表的另一层级中的查找提供了转换表基地址。表描述符还可任选地提供可应用于最终转换的其他分层属性。层级1和2处的转换表条目的编码将块描述符与表描述符区分开。

[0116] ●描述符是无效的。在该情况下,存储器访问生成转换故障。

[0117] 图4示出了使用作为用于表查找的输入地址而提供的虚拟地址的相应位来索引阶段1转换表。从TTBR读取顶层表L0的基地址,并且L1、L2、L3表的基地址分别由存储在L0、L1、L2表中的索引表描述符中的地址指示(如果在L1或L2表中没有标识出块描述符—如果在L1或L2的索引条目中找到块描述符,则由于已经找到输出地址映射,因此在该层级处停止遍历)。基于对应于作为用于查找的输入地址而提供的虚拟地址的特定位子集的索引值a、b、c、d来确定要在阶段1转换表的给定层级内选择的特定条目。图4示出了在一个特定示例中的输入地址的哪些位用于每个索引值a、b、c、d。给定表中的相关条目的地址通过将索引位a、b、c或d的倍数添加到如基于TTBR确定的该给定表的基地址或先前层级处的表描述符中指定的地址来获得(乘数应用于与一个转换表条目的大小相对应的索引值)。

[0118] 类似地,图5示出了使用作为用于阶段2表查找的输入地址而提供的中间地址的相应位来索引阶段2转换表。索引类似于图4所示的用于阶段1的索引,但是使用不同的基地址寄存器VTTBR_EL2以提供L0表的基地址。如图5的示例中所示,对于阶段2查找,可以基于控

制寄存器VTCR_EL2.SL0中存储的值(其可指定查找应当在L0或L1处开始)来改变阶段2转换表的遍历开始于的开始层级。如果阶段2查找在L0处开始,则等级0、1、2、3的索引分别使用类似于阶段1的图4的索引值a、b1、c、d。如果阶段2查找在L1处开始,则以类似方式执行索引,但现在在查找的顶部层级(L1)处使用较大数量的索引位b2,如图5中所示。提供可变开始层级不是必要特征并且如果需要的话可被省略。尽管在图4中未示出,但也可以提供用于在阶段1处的查找的可变开始层级。

[0119] 如图6所示,在实践中,当执行包括阶段1和阶段2转换两者的完整转换表遍历时,则从TTBR以及在阶段1L0、L1、L2转换表中访问的表描述符获得的每个阶段1表基地址将是中间地址,其本身需要使用阶段2转换表来转换。因此,在转换表遍历没有遇到任何块描述符,而是一路前进到发现页描述符的L3的情况下,则全页表遍历过程可包括以下面的顺序访问页表的多个层级:

[0120] ●阶段1L0页表的基地址到物理地址的阶段2转换(阶段1L0基地址通常是中间物理地址,因为阶段1转换由操作系统配置)。阶段2转换包括4个查找(阶段2L0;阶段2L1;阶段2L2;阶段2

[0121] L3)。

[0122] ●在基于目标虚拟地址的L0索引部分“a”和经转换的阶段1L0基地址来获得的地址处的条目的阶段1L0查找,以获得阶段1L1基地址(中间物理地址)

[0123] ●使阶段1L1基地址成为物理地址的阶段2转换(同样包括4个查找)。

[0124] ●在基于目标虚拟地址的L1索引部分“b”和经转换的阶段1L1基地址来获得的地址处的条目的阶段1L1查找,以获得阶段1L2基地址(中间物理地址)

[0125] ●使阶段1L2基地址成为物理地址的阶段2转换(同样包括4个查找)

[0126] ●在基于目标虚拟地址的L2索引部分“c”和经转换的阶段1L2基地址来获得的地址处的条目的阶段1L2查找,以获得阶段1L3基地址(中间物理地址)

[0127] ●使阶段1L3基地址成为物理地址的阶段2转换(同样包括4个查找)。

[0128] ●在基于目标虚拟地址的L3索引部分“d”和经转换的阶段1L3基地址来获得的地址处的条目的阶段1L3查找,,以标识对应于目标虚拟地址的目标中间物理地址。

[0129] ●使目标中间物理地址成为目标物理地址的阶段2转换,该目标物理地址表示对应于原始目标虚拟地址的存储器中要访问的位置(同样包括4个查找)。

[0130] 因此,在没有任何高速缓存的情况下,并且假设阶段2的开始层级是L0,转换将总共包括24个查找。如果阶段2的开始层级是L1,则这可将查找的数量减小到19(对于所执行的5个阶段2转换中的每一者少一个查找)。然而,从上述顺序可以看出,执行整个页表遍历过程可能非常慢,因为对于地址转换的阶段中的每个阶段,其可能需要对存储器的大量访问来逐步通过页表的各层级中的每个层级。这就是通常期望在MMU 28的TLB 29中高速缓存从转换表遍历导出的信息的原因。高速缓存的信息不仅可包括从VA到IPA的最终阶段1地址映射、从IPA到PA的最终阶段2映射、或从VA直接到PA的组合阶段1和阶段2映射(从阶段1和阶段2结构的先前查找导出),而且可在MMU 28的TLB 29内高速缓存来自阶段1和阶段2表的较高层级页表的条目。即使给定目标地址的末级地址映射当前不在地址转换高速缓存中,这也可以允许绕过完整页表遍历的至少一些步骤。

[0131] 图6通过指定特定许可或性质的信息来注释,该特定许可或性质可针对两阶段地

址转换中涉及的转换表条目中的一些来定义。一旦这些许可和性质已经在下面解释,这将在后面更详细地描述。

[0132] 存储器管理单元示例

[0133] 图7更详细地示出了存储器管理单元28。虽然为了简洁,图1和图7示出了单个MMU 28,但是也可以提供分开的指令侧和数据侧MMU以分别处理用于由提取级6发起的指令提取访问和由加载/存储单元26发起的数据访问的存储器管理操作—在该情况下,指令侧和数据侧MMU都可具有图7中示出的部件。与TLB 29一样,MMU 28包括访问控制电路50,其用于检查在所查找的转换表条目中指定的访问许可并且根据那些访问许可来控制存储器访问请求的处理。例如,访问控制电路50可实现用于确定特定类型的存储器访问请求(例如,基于请求为读取、写入还是指令提取请求,或基于致使发出请求的所执行的指令的类型)是否满足针对正被访问的给定存储器区域的对应转换表条目中指定的许可的检查。MMU还包括转换表遍历控制电路52,在来自转换表的所需信息在TLB 29中还不可用的情况下,该转换表遍历控制电路向存储器发出存储器访问请求以请求在转换表遍历过程期间读取转换表条目,如以上在图4至图6中所示。转换表遍历控制电路52可负责生成待读取的存储器系统位置的地址以获得阶段1或阶段2转换表结构中的相关转换表条目。此外,在执行转换表遍历时,转换表遍历控制电路52可生成元数据更新写入请求,其请求对在转换表遍历中正被遍历的特定转换表条目内的访问跟踪元数据的更新。这些元数据更新写入请求可更新访问跟踪元数据以反映特定存储器区域已被访问,这可用于管理诸如分页的操作。在硬件中生成元数据更新写入请求,以指定不是直接指定为指令提取地址的地址,或者从由处理电路4执行的加载/存储指令的操作数导出的加载/存储目标地址,因为元数据更新写入请求的地址是在转换表遍历中访问的转换表条目的地址,而不是正在访问的数据或指令的地址。

[0134] MMU 28具有对用于控制转换表遍历和存储器管理操作的其他方面的各种控制寄存器的访问。例如,控制寄存器可包括阶段1和阶段2基地址寄存器TTBR_EL1、VTTBR_EL2,如先前相对于图4和图5所提及的。响应于在异常层级EL1、EL2或EL3处执行的指令,寄存器TTBR_EL1中的阶段1基地址是可写入的。响应于在异常层级EL2或EL3处执行的指令,寄存器TTBR_EL2中的阶段2基地址是可写入的。在一些情况下,可以设置控制值以指示由在EL1处执行的指令触发的对TTBR_EL1的写入应当被捕获到EL2,使得在EL2处操作的管理程序可检查正由操作系统请求的更新并且在必要时防止更新。控制寄存器还包括用于指定各种控制状态值的寄存器TCR_EL1、VTCR_EL2,这些控制状态值影响执行阶段1和阶段2转换和访问许可检查的方式。例如,可在VTCR_EL2中指定了指定用于阶段2遍历的开始层级的控制值。此外,TCR_EL1或VTCR_EL2控制寄存器可指定控制值,该控制值指定启用/停用何种类型的安全检查。如下面更详细讨论的,控制寄存器还可包括用于指定更新受限位子集的掩码寄存器(标记为RCWMask_Valid_EL2和RCWMask_Invalid_EL2),对于该更新受限位子集,更新被限制在分别用于有效和无效条目的受保护的阶段1转换表条目中。应当理解,还可提供另外的控制寄存器,并且用于控制寄存器的标记可变化。例如,可提供一个或多个许可间接寄存器来指定间接访问许可信息,该间接访问许可信息可由给定转换表条目引用以指定针对给定转换表条目的访问许可信息。同样可能的是,相同信息以不同格式布置在控制寄存器内,使得信息到一个控制寄存器或另一控制寄存器的特定分配不是必要特征。

[0135] 如图7所示,装置可具有受保护条目检查电路54,其用于在请求对被编码为受保护

条目的阶段1转换表条目的更新时执行受保护条目检查(这将在下面更详细地描述)。如图7中的虚线所示,可在处理系统内的不同位置处实现受保护条目检查电路54。例如,受保护条目检查电路54可以是MMU 28的访问控制电路50的一部分。另选地,可在存储器系统部件56内实现受保护条目检查电路,其较靠近将使用受保护条目检查电路54来检查的给定存储器访问请求所访问的物理存储器系统位置。例如,存储器系统部件56可以是高速缓存30、32、用于管理多个处理器核对共享存储器的访问的互连、或与特定存储器存储单元相关联的存储器控制器。此外,受保护条目检查电路54可包括系统中的多个位置处的分布式逻辑(例如,MMU 28、加载/存储单元26和/或存储器系统部件56)。

[0136] 转换表访问许可和属性

[0137] 图8示出了阶段1和阶段2转换表结构中的转换表条目的示例性格式。应当理解,相同信息可以不同布置来表示并且因此描述符内的字段的特定排序和布局可与图8中所示的不同。

[0138] 在该示例中,有效转换表描述符具有设置为1的最低有效位并且无效转换表描述符具有设置为0的最低有效位。对于在转换表结构的层级0、1、2中的一者处读取的有效描述符,第二最低有效位区分描述符是表描述符(第二最低有效位被设置为1)还是块描述符(第二最低有效位被设置为0)。在阶段1或阶段2结构的L3处的页描述符可将第二最低有效位设置为1以允许区分页描述符与块描述符。当然,有效/无效条目以及表/块/页描述符也可通过其他编码方法来区分。

[0139] 对于阶段1和阶段2条目两者,有效表描述符提供下一级表地址60,其指示阶段1或阶段2转换表结构的下一级处的转换表的基地址。有效的阶段1块或页描述符提供与用于索引阶段1转换表结构的虚拟地址相对应的中间地址映射62。有效的阶段2块或页描述符提供与用于索引阶段2转换表结构的中间地址相对应的物理地址映射64。

[0140] 阶段1块和页描述符还提供用于控制对于对应存储器区域的访问的阶段1访问许可66。例如,阶段1访问许可66(通常由EL1处的OS设定)可指定是否允许读取、写入和/或使用区域以用于可执行指令的指令提取。

[0141] 类似地,阶段2块和页描述符提供用于控制对于对应存储器区域的访问的阶段2访问许可68。同样,阶段2访问许可68(通常由EL2处的管理程序设定)可指定是否允许读取、写入和/或使用区域以用于可执行指令的指令提取。如果在阶段1访问许可66与阶段2访问许可68之间存在冲突,则更具限制性的属性集合可优先。

[0142] 阶段1或阶段2块/页描述符还可指定与存储器区域相关联的其他属性(图8中未示出)。例如,这些属性可指定诸如是否允许高速缓存来自对应存储器区域的数据、区域是否被定义为设备存储器以使得不允许对设备存储器的不同存储器访问的重新排序或合并等的性质。

[0143] 阶段1块/页描述符还可指定访问跟踪元数据,其可由操作系统使用以跟踪对给定存储器区域的访问的频率。例如,元数据可包括访问标志(AF)70和脏位修改器(DBM)72。

[0144] 操作系统可周期性地清除对应于待监测的存储器区域集合的条目中的访问标志。当对这些存储器区域中的一者进行读访问时,可在对应的阶段1块或页描述符中设置访问标志70(如果在较早访问之后还没有设置)(致使访问标志70被设置的存储器访问请求可以是由较早提及的转换表遍历控制电路52生成的元数据更新写入请求中的一者)。在监测时

段之后,操作系统然后可检查访问标志70以辅助可从关于访问某些页的频率的信息中获益的操作。例如,操作系统可在存储器中维持另外的跟踪数据结构,其中每个存储器区域的条目跟踪存储器区域已经被访问了多少次,并且因此在每个监测时段的结束时,可递增该另外的跟踪结构的对应于访问标志70被设置的存储器区域的条目。在多个监测时段之后,该另外的跟踪结构因此将提供对于对应存储器区域的访问的相对频率的指示。这可提供用于控制诸如分页的操作的有用信息,其中可能有用的是知道存储器的最不频繁访问的页,与其他更频繁访问的页相比,针对该最不频繁访问的页,对应数据可被优先化以用于分页到外部存储装置。

[0145] 类似地,DBM 72辅助跟踪哪些页已经受写入。如果操作系统希望跟踪给定页是否已被写入,则当页被映射时或在监测时段的开始时,操作系统可将该页的访问许可设置为“只读”(即使页旨在被允许写入)并且设置DBM位72。当DBM位72被设置时,对于由对只读页的写入引起的访问许可故障,操作系统可根据被设置的DBM位72确定这不是只读许可的“真实”违反,并且替代地致使操作系统更新跟踪经受写入请求的页的存储器中存储的数据结构,并且还更新页的写入访问许可以指示页现在可被写入而不触发故障。在监测时段之后,软件可使用存储器中的跟踪数据结构来确定在分页出特定区域时是否有必要将经修改数据从该区域写回到外部存储装置,或者(如果没有发生写入)在分页出区域时是否可简单地丢弃存储在片上存储器中的数据,因为如果数据是干净的,则可假设外部存储器中的对应数据仍然相同。

[0146] 访问标志70和脏位修改器72仅是可存储在转换表条目内的可能访问跟踪数据的一些示例,并且其他示例可提供其他类型的访问跟踪元数据。例如,在另一示例中,可提供多位访问计数器作为访问跟踪元数据。而且,在另一示例中,代替DBM位72用于对于写入请求修改只读访问许可违反的处置并且触发写入许可的更新,DBM标志72可替代地响应于在清除DBM标志72之后对页的第一次写入而直接被更新,其方式类似于如先前所描述在对页的第一次访问时更新访问标志70的方式。

[0147] 如图8中所示,各种转换表描述符还可包括可用于保护阶段1转换表条目以在攻击者的攻击下不被操作系统代码破坏的多条其他信息。典型操作系统代码可包括可能难以完全验证为免于攻击的安全的许多代码行,并且因此期望提供用于保护以免于攻击者可以能够修改操作系统代码的行为以引起对用于存储转换表条目的存储器区域的写入(从而尝试修改这些条目中的地址映射或许可以便给予攻击者以未经授权方式访问存储器区域的权利)的可能性的架构机制。

[0148] 如图8中所示,以下描述的用于针对攻击来硬化阶段1转换表的附加属性和许可包括以下:

[0149] ●阶段2块/页描述符指定阶段2访问许可68,其具有指示对应存储器区域是否具有部分只读(PRO)许可的编码(部分只读许可还可被称为“主要只读”许可);

[0150] ●在阶段1转换表结构的所有层级处的有效阶段1描述符(包括表描述符和块/页描述符)具有指定该转换表条目是否为“受保护”条目的编码,与非受保护条目相比,针对该“受保护”条目提供了针对未授权更新的附加保护。例如,有效阶段1描述符内的位字段76可表示条目是否为受保护条目。

[0151] ●在阶段1转换表结构的所有层级处的无效阶段1描述符还可具有指定该转换表

条目是否为“受保护”条目的编码。这可使用位字段78来指示,与用于表示有效阶段1转换表条目的受保护条目的位字段76相比,该位字段可在转换表条目编码内的不同位置处。

[0152] ●阶段2块/页描述符可具有指定对应存储器区域是否具有抗混叠性质的指示符79。在一些示例中,可在组合位字段中编码抗混叠性质的存在或不存在,该组合位字段也可发信号通知其他类型的性质,或另选地,抗混叠位字段可为不发信号通知任何其他信息的独立位字段。如果被指定,则抗混叠性质指示了针对要被允许的对于对应物理地址的访问,在转换表遍历中访问以获得用于访问该阶段2描述符的中间地址的所有阶段1转换表条目将需要使用位字段76来指定为受保护条目并且将被存储在针对其对应阶段2块/页描述符指示部分只读许可74的存储器区域中。

[0153] ●阶段2块/页描述符还可在阶段2访问许可68中指定阶段1顶层条目存在许可80,其指示对应存储器区域是否被允许保持用于阶段1转换的顶层转换表(即,图4和图6的示例中的阶段1L0表)。在一个示例中,阶段2访问许可68的编码可使得阶段1顶层条目存在许可被编码为PRO许可的另一属性,从而使得被允许针对阶段2访问许可68编码的值可包括指示以下的值:

[0154] o没有阶段1顶层条目存在许可的PRO许可;

[0155] o具有阶段1顶层条目存在许可的PRO许可;或者

[0156] o不具有PRO许可或阶段1顶层条目存在许可的一个或多个其他类型的许可(例如,只读许可、读取/写入许可和/或执行许可)。

[0157] 在该情况下,可能无法独立于PRO许可来指定阶段1顶层条目存在许可。然而,其他具体实施可独立于PRO许可来编码阶段1顶层条目存在许可,使得即使不提供PRO许可也可指定阶段1顶层条目存在许可。

[0158] 下面将更详细地讨论这些属性和许可的使用。应当理解,并非所有这些属性和许可都需要在每个具体实施中得到支持。虽然图8示出了在转换表条目的编码中直接指定S1和S2访问许可的示例,但是也可以使用许可寄存器中指定的许可来间接指定相同信息。例如,S1或S2许可字段66、68可指定索引值,该索引值选择许可寄存器的多个许可字段中的哪一者为对应转换表条目指定访问许可。取决于存储在控制寄存器中的控制状态,还能够以不同方式解释转换表条目的一些字段。例如,当存储在控制寄存器中的控制值具有第一值时,阶段1转换表条目的受保护条目字段76可被解释为指示阶段1转换表条目是否受保护,并且当控制值具有第二值时,该受保护条目字段可以不同方式来解释。类似地,当存储在控制寄存器中的控制值具有第一值时,阶段2转换表条目的抗混叠性质字段79可被解释为指示阶段2转换表条目是否具有抗混叠性质,并且当控制值具有第二值时,该抗混叠性质字段可以不同方式来解释。

[0159] 部分只读许可

[0160] 图9总结了由阶段2访问许可68标记为具有部分只读(PRO)许可的存储器区域的写入访问控制行为。至少对于在当前执行状态是EL1(其中期望执行操作系统代码的状态)时发出的写入请求,具有PRO许可的存储器区域针对写入请求类型的受限子集是可写的,但是针对写入请求类型被视为只读。由于仅一些写入请求类型将存储器区域看作只读,因此该许可被描述为部分只读许可。

[0161] 图9总结了被允许和禁止写入到存储器区域的写入请求的类型,针对该存储器区

域,对应阶段2转换表条目将该区域定义为具有PRO许可。当在EL1处发出写入时被允许写入到PRO区域的写入请求类型的受限子集包括由MMU 28生成的元数据更新写入请求以在脏位修改器72被设置的情况下更新转换表条目中的访问跟踪元数据(诸如访问标志70或写入许可),如上文所讨论。此外,受限子集可包括在异常状态EL1处执行的至少一个预定类型的转换表条目更新指令,其可以是旨在用于更新转换表条目的专用类型的指令,以表达将用于更新转换表条目的此类写入与用于更新除转换表条目之外的数据的写入区分开的程序代码的意图。例如,预定类型的转换表条目更新指令可包括下面相对于图12至图14讨论的受保护条目检查读取检查写入(RCW)指令的变体。如图9所示,禁止响应于在异常状态EL0和EL1中的一者中执行的至少一个其他类型的存储指令而发出的写入请求写入到存储器的PRO区域。例如,所禁止的写入请求类型可包括处理电路4所支持的指令集架构中的大多数存储指令。通过在用PRO许可标记区域时将用于更新转换表条目的能力限于一组有限指令类型,这减少了可供攻击者在尝试破坏阶段1转换表条目时利用的攻击表面,例如,篡改不是写入请求的受限子集中的一者的通用存储的地址操作数将不允许访问存储器的PRO区域。

[0162] 任选地,响应于在执行状态EL2或EL3中的一者中执行的存储指令而发出的写入请求可被允许写入到部分只读区域,即使它们是如果在执行状态EL0或EL1处执行则将被禁止写入该区域的存储指令类型。然而,如上所述,这不是必需的。

[0163] 图10是示出了处理指令和控制存储器管理操作的方法的流程图。在步骤500处,处理电路4处理与不同特权等级相关联的多个执行状态EL0-EL3中的一者中的指令。在步骤502处,响应于存储器访问请求,MMU 28执行使由存储器访问请求指定的目标虚拟地址(VA)成为目标物理地址(PA)的两阶段地址转换,其中目标VA到目标PA的映射取决于从目标VA到目标中间地址(IPA)的阶段1地址映射及从目标IPA到目标PA的阶段2地址映射。在步骤504处,MMU 28的访问控制电路50至少基于在对应的阶段2转换表条目中指定的阶段2访问许可信息68,执行针对存储器访问请求的许可检查。许可检查也可基于阶段1访问许可信息66。阶段2访问许可信息66具有指定对应于目标IPA的存储器区域是否具有PRO许可的编码。在步骤506处,当存储器访问请求是在预定执行状态(例如EL1)下发出的写入请求,阶段2访问许可信息指定PRO许可,并且写入请求是除了被允许写入到存储器的PRO区域的写入请求类型的受限子集之外的写入请求类型时,MMU 28拒绝存储器访问请求。任选地,当存储器访问请求是在除了预定执行状态的执行状态(例如,EL0)中发出的写入请求时,MMU 28也可拒绝该存储器访问请求,此时PRO许可由阶段2访问许可信息指定并且写入请求类型不是写入请求类型的受限子集中的一者。

[0164] 图11更详细地示出了由MMU 28的访问控制电路50执行的部分只读检查。在步骤600处,当处理电路4处于预定执行状态(EL1)时,发出写入存储器访问请求。写入请求指定目标VA。写入请求可由处理电路4的加载/存储单元26响应于由处理电路执行的加载/存储指令而发出,或者在请求指令提取时由提取级6发出。写入请求还可以是由MMU 28发出的元数据更新写入请求以在转换表遍历过程期间更新转换表条目中的访问跟踪元数据。

[0165] 在步骤602处,将目标VA转换成标识待访问的存储器系统位置的目标PA。为了执行转换,MMU 28可在TLB 29内查找目标VA,并且如果从目标VA到目标PA的映射已经在TLB 29中可用,则不需要转换表遍历。否则,可能需要图6中所示的转换表遍历过程的至少一部分,

尽管如果从针对转换表遍历的该部分的对应转换表条目导出的信息已经被高速缓存在TLB29中,则一些部分可以能够被跳过。对于从非安全EL1发出的写入存储器访问请求,基于在阶段1和阶段2转换表两者中定义的映射将转换执行为两阶段地址转换,尽管这不一定意味着需要执行两个单独的转换,因为有可能提供组合的阶段1/阶段2TLB,其高速缓存直接从目标VA到目标PA的映射(取决于阶段1和阶段2映射两者)连同对应的阶段1和阶段2许可信息,以避免需要明确地确定目标IPA。

[0166] 在步骤604处,访问控制电路检查对应阶段2(S2)转换表条目(指定从目标IPA到目标PA的映射的阶段2条目)是否指定PRO许可。如果是,则在步骤606处,访问控制电路检查正被处理的写入请求是否是写入请求类型的受限子集中的一者。如果当前写入请求不是写入请求类型的受限子集(至少包括元数据更新写入请求)中的一者,则在步骤608处拒绝存储器访问请求并且发信号通知故障。如果写入请求是写入请求类型的受限子集中的一者,则部分只读检查通过并且因此方法行进到步骤610。而且,如果在步骤604处,对应阶段2转换表条目没有指定PRO许可,则可省略步骤606处的部分只读检查并且因此方法从步骤604直接行进到步骤610。

[0167] 在步骤610处,访问控制电路确定是否满足允许写入存储器访问请求继续进行所需的任何其他检查。例如,这些检查可包括使用阶段1访问许可66的检查、在未指定PRO许可的情况下使用其他阶段2访问许可68的检查、基于请求是从安全还是非安全状态发出的安全检查(在支持安全状态的具体实施中)、以及专用于特定指令类型的其他检查,诸如以下相对于图12至图14讨论的关于目标存储器位置处的数据是否为受保护转换表条目的检查。如果不满足这些其他检查的任一者,则再次在步骤608处拒绝存储器访问请求并且发信号通知故障。故障症状信息可被设置为区分故障的原因。如果满足在步骤610处执行的检查,则在步骤612处,可允许存储器访问请求继续进行,并且因此可通过由写入请求指定的写入数据来更新与目标PA相关联的存储器系统位置。

[0168] 因此,如先前讨论的图6中所示,可在阶段2转换表条目的阶段2访问许可68中指定PRO许可,该条目用于提供保持在阶段1表结构的遍历使用以获得包含敏感信息的存储器区域的中间地址的阶段1转换表的各种层级的存储器系统位置的物理地址。这保护了那些阶段1转换条目免于在恶意方的攻击下被错误起作用代码或操作系统代码破坏,因为PRO许可将向对应存储器区域进行写入的能力限于指令类型的有限子集,从而极大地减小可能易受阶段1转换表的破坏的代码行的数量。然而,用于更新转换表条目中的访问跟踪元数据的硬件生成的写入请求仍然可被允许用于此类区域以避免损害操作系统的分页操作的效率。

[0169] 尽管图11示出了针对在预定执行状态EL1中发出的写入存储器访问请求执行部分只读检查,但也可针对其他执行状态执行部分只读检查。然而,这可能不是必要的,因为对于在最低特权的执行状态EL0中发出的写入请求,有可能的是,保持阶段1转换表的存储器区域在任何情况下将被阶段1访问许可66标记为对于在EL0处操作的应用程序级代码不可访问,因此阶段1许可检查可能已经防止此类写入请求破坏阶段1转换表。此外,对于在EL2或EL3处执行的代码,转换表将不使用两阶段地址转换,并且不太可能限制对存储阶段1转换表条目的区域的写入,因为管理程序或监测代码可以是正控制对允许对于阶段1转换表的更新的限制的代码。因此,一些具体实施可将部分只读检查限制为仅在当前执行状态是EL1时才执行。无论哪个执行状态是当前执行状态,其他具体实施都可应用部分只读检查。

[0170] 用于阶段1转换表条目的受保护条目编码

[0171] 使用PRO许可以将特定存储器区域标记为针对除写入类型的受限子集之外的写入请求只读有助于保护阶段1表免于破坏。然而,如图6中所示,典型地,在转换表结构的给定层级处的给定转换表占据存储器中的整页,并且因此PRO许可将应用于在阶段1转换表结构的给定层级处的整个转换表,其可包括用于各种存储器区域的转换表条目,该存储器区域可包括用于需要被保护以免于未授权访问的敏感信息的一些存储器区域,以及仅包含不需要该保护的非敏感信息的其他存储器区域。

[0172] 有可能的是,提供不支持将受保护条目编码用于阶段1转换表条目的具体实施,如下面进一步讨论的。在该情况下,为了允许操作系统更新与包含非敏感信息的非受保护区域相关联的特定阶段1转换表条目,在不是被允许写入到PRO区域的写入请求类型之一的对PRO区域的写入访问时生成的故障可导致捕获到在EL2处操作的管理程序,并且管理程序然后可在软件中确定针对其操作系统希望更新阶段1转换表条目的区域是否应当被保护以免于被操作系统更新,并且如果区域不需要被保护,则可允许由操作系统请求的更新继续进行。然而,在实践中,操作系统可能需要相对频繁地改变用于存储器的非受保护区域的转换表条目,并且因此每次需要更新时对管理程序的捕获在性能方面可能是缓慢的。

[0173] 用于阶段1转换表条目的受保护条目编码(例如,使用位76、78)帮助允许操作系统在没有管理程序干预的情况下对非受保护条目进行更新(并且任选地对于一些具体实施,在没有管理程序干预的情况下对受保护条目的非更新受限位进行更新)。这有助于改进性能,因为即使当给定阶段1转换表被存储在存储器的PRO区域中时,也可更频繁地避免管理程序参与,因为它包含受保护条目和非受保护条目的混合。处理电路4的指令解码器10和执行级16支持至少一种类型的指令,被称为受保护条目检查类型的读取检查写入(RCW)指令,其可用于请求对给定存储器系统位置的更新,其中以受保护条目检查为条件进行更新,该受保护条目检查会检查存储在所访问的存储器系统位置处的数据以检查其是否具有与受保护的阶段1转换表条目的编码一致的值。如果发现了所访问的存储器系统位置处的数据具有与作为受保护的阶段1转换表条目的数据一致的值,则抑制对给定存储器系统位置的至少更新受限位子集的更新。RCW指令被允许由在EL1处执行的操作系统执行。RCW指令是被允许通过对应的阶段2转换表条目更新用PRO许可标记的存储器区域中的数据的受限指令子集中的一者。

[0174] 受保护条目检查由受保护条目检查电路54在硬件中执行,如图7中所示,该受保护条目检查电路可在MMU 28内实现或较靠近存储数据的存储器系统位置实现(例如,在诸如高速缓存、互连或存储器控制器的存储器系统部件56内)。还可以使用分布式逻辑集合,其中受保护条目检查电路54的一些部分在MMU 28(或流水线的执行级16)中实现并且其他部分在较靠近存储器存储装置处实现。在受保护条目检查中执行的读取、检查和写入操作作为原子(不可分)操作来执行,使得当由在与执行RCW指令的线程相同的处理器电路上执行的另一线程或由另一处理器核请求对给定存储器系统位置的访问时,另一访问看到在处理RCW指令之前的给定存储器系统位置的值或在处理RCW指令之后的给定存储器系统位置的值,而不是RCW指令的任何部分效应,并且还不可能使对给定存储器系统位置的写入在受保护条目检查读取给定存储器系统位置处的数据与响应于RCW指令而对给定存储器系统位置处的数据的后续更新之间的时段中更新给定存储器系统位置。可使用用于对存储器系统位

置实施原子读取/写入操作的任何已知技术来强制原子性(例如,锁定存储器位置以免于在读取与写入之间的时段中由其他操作访问,或在该时段中允许冲突访问但在读取与写入之间的时段中检测到冲突访问的情况下重新开始RCW操作)。通过强制读取、检查和写入的原子性,这避免了可能导致不正确处理结果的竞争条件。当以原子方式执行读取、检查和写入操作时,与如果读取数据必须一直返回到MMU 28或处理器流水线4的另一元件以用于在写入可继续进行且将写入数据返回到存储数据的存储器系统位置之前执行检查的持续时间相比,可能有用的是,使受保护条目检查电路54在存储器系统部件56内较靠近正在更新的存储位置实现以减小读取与写入之间的时段的持续时间。

[0175] 在图8中所示的示例中,有效和无效阶段1转换表条目都具有允许条目被指定为受保护条目的编码。然而,无效条目能够被指定为受保护不是必要的,并且其他示例可从无效条目格式中省略受保护条目编码位字段78。此外,不同具体实施可针对受保护条目的多少位响应于RCW指令而使其更新被抑制来选择不同选项。一些具体实施可防止响应于RCW指令的对受保护条目的任何更新,其中仅在给定存储器系统位置处的数据未被编码为受保护条目的情况下响应于RCW指令而允许更新。其他具体实施可指定更新受限位子集和非更新受限位子集,并且因此即使对于受保护条目,也可允许对非更新受限位子集的更新。例如,可能存在对于安全性不是关键的一些字段,诸如访问标志70和脏位修改器72,其甚至在受保护条目中也可被允许更新。哪些位是更新受限的或非更新受限的可针对给定架构以不可编程的方式固定,或者可通过软件使用存储在控制寄存器中的选择值来编程。例如,选择值可从若干不同模式中的一个模式中选择,每个模式与哪些位是更新受限的不同设置相关联。然而,在图7的示例中,选择值被编码为标识更新受限位的位置的位掩码,其中选择值被存储在掩码寄存器中(例如,图7所示的RCWMask_Valid_EL2和RCWMask_Invalid_EL2寄存器,用于分别为有效和无效条目选择更新受限位—在其中无效条目不能被编码为受保护条目的具体实施中,可省略RCW_Mask_Invalid_EL2寄存器)。对选择值的更新可限于以阈值特权等级或更高特权等级执行的程序指令,例如仅在EL2或EL3处执行的指令可被允许更新选择值。不管选择值的状态如何,可能存在被强制为更新受限的一些位。例如,用于编码条目是否为受保护条目的位字段76、78可不被允许更新,而不管哪些其他位能够被更新。一般来说,可禁止RCW指令改变特定条目是受保护还是不受保护的状态。位字段76、78的设置将改为由以较高特权等级(诸如EL2或EL3)执行的程序代码控制,该程序代码可使用阶段2转换表的不同集合来访问存储器,该不同集合不将存储受保护条目的存储器区域标记为部分只读,并且因此可使用标准通用存储指令来设置受保护阶段1条目的位字段76、78。

[0176] 存在可实现受保护条目检查的多种方式。在一个示例中,如果存储在所访问的存储器系统位置处的条目有效且受保护,则其不能被更改,并且如果其无效,则其可被更改,包括使其有效(只要也不使条目受保护)。另选地,在有效条目中可存在受保护位字段76,并且在无效条目中可存在受保护位字段78,并且可不允许对受保护条目的改变,否则允许对非受保护(有效或无效)条目进行更新(除了改变条目是否受保护的状态)。另一示例可在有效条目中提供受保护位字段76,并且在无效条目中提供受保护位字段78,并且可允许RCW指令在不受保护的情况下对条目作出任何改变(除了使其受保护),而如果其被保护,则RCW指令可对如针对有效条目所描述的一些位作出改变,并且对无效条目中的一些位作出改变。在一些示例中,用于描述哪些位被保护的机制是除了保护或有效字段之外的任何字段的硬

连线架构选择。另选地,用于描述哪些位在有效条目中被保护的机制可使用EL2所拥有的掩码寄存器,和/或用于描述哪些位在无效条目中被保护的机制是EL2所拥有的掩码寄存器。用于定义更新受限位的不同选择分别对于有效和无效条目而言是可能的一例如,一种方法可以是定义用于定义有效条目的更新受限位的掩码寄存器,但是硬连线无效条目的更新受限位。

[0177] 当允许更新受保护条目中的一些字段时,如何应用检查也可有变化,两个示例性选项是:

[0178] A)受保护条目检查电路54读取当前条目以检查条目是否为有效和/或受保护的,并且然后仅存储允许被写入的位(而不检查RCW指令是否正尝试改变不允许被写入的更新受限位)。

[0179] B)受保护条目检查电路54读取当前条目以检查条目是否为有效和/或受保护的。如果它被保护,并且RCW指令没有尝试改变不允许被写入的任何位,则写入可发生,但是如果RCW指令尝试更新任何更新受限位,则写入失败并且什么都不被写入。

[0180] A和B都是可行的替代方案。

[0181] 响应于RCW指令,写入是成功还是失败的指示可被写入到存储在处理电路4的控制寄存器中的条件状态标志。例如,条件状态寄存器可包括多个条件标志(例如,否定标志N、零标志Z、进位标志C和溢出标志V),该条件标志可取决于处理操作的结果来设置并且可由条件指令测试,该条件指令可然后取决于条件状态标志的状态而有条件地触发操作(诸如分支操作或算术/逻辑操作)。因此,可能有用的是,基于RCW指令所请求的写入的任何部分是否不成功来更新条件状态标志,以允许后续指令取决于写入的结果来采取动作,而不需要重新读取存储器系统位置以检查写入是否成功。

[0182] 图12、图13和图14示出了受保护条目检查RCW指令的多个变体的处理。图12示出了指令的存储变体或交换变体的处理的示例(除了取决于变体的最终步骤726或728之外,大多数处理步骤对于两个指令是相同的)。存储变体和交换变体都指定提供用于生成待更新的给定存储器系统位置的地址的地址操作数的寄存器Xd,以及提供要写入到给定存储器系统位置的新数据的源寄存器Xs。至少交换变体还指定从给定存储器系统位置读取的旧数据将被写入到的目的地寄存器Xt。存储变体不需要指定任何目的地寄存器,因为存储变体与交换变体的不同之处在于旧数据不被写入到任何目的地寄存器。然而,在一个示例中,存储变体和交换变体可使用相同的编码来编码,不同之处在于当用于指定目的地寄存器Xt的字段具有预定值时,指令可被视为存储变体。例如,一些指令集架构可将特定寄存器指定符(例如,寄存器31)定义为对应于“零”寄存器,该“零”寄存器在被指定为指令的操作数时致使操作数被视为如同其具有值零,而不需要实际上从硬件中提供的寄存器读取操作数。因此,在一些示例中,当目的地寄存器Xt被指定为“零”寄存器X31时,可将指令视为存储变体。在其他示例中,存储指令可被编码为与交换指令完全不同的指令类型。

[0183] 在图12的步骤700处,从分别由寄存器指定符Xd和Xs标识的寄存器读取要写入的地址操作数和新数据(“NewData”)。在步骤702处,基于地址操作数来确定用于存储器访问的目标地址。例如,地址操作数可被视为直接指定目标地址的绝对地址,或可定义相对于参考地址(诸如另一基寄存器中的值或标识RCW指令自身的地址的程序计数器值)的偏移。基于地址操作数计算的目标地址是虚拟地址并且可由MMU 28转换成物理地址。在步骤704处,

假定传递了用于目标地址是否对于当前指令可访问的任何MMU检查(除了受保护条目检查),则向存储器系统发出读取请求以获得从对应于(经转换)目标地址的存储器系统位置读取的数据(“ReadData”)。这对应于RCW指令的“读取”。

[0184] 在步骤706处,受保护条目检查电路54确定ReadData是否具有与受保护阶段1(S1)转换表条目的编码一致的值。这对应于RCW指令的“检查”部分。如果ReadData不具有与作为受保护的阶段1转换表条目一致的值,则在步骤708处,受保护条目检查电路检查NewData是否被编码为受保护的阶段1转换表条目。如果是,则在步骤710处,拒绝由RCW指令请求的写入,或另选地可将由RCW指令指定为NewData的阶段1转换表条目的非更新受限位写入到存储器系统位置的对应位,其中至少用于对条目是否被保护进行编码的位被视为未写入的更新受限位。无论哪种方式,在步骤712处,将条件状态标志设置为报告未能完全执行由RCW指令请求的写入。

[0185] 如果在步骤706处,确定ReadData被编码为受保护的阶段1转换表条目,则在步骤716处,受保护条目检查电路54确定所读取的数据是否具有与作为有效或无效的阶段1转换表条目一致的值。如果所读取的数据具有与作为无效的受保护的阶段1转换表条目一致的值,则在步骤718处,受保护条目检查电路54确定NewData是否尝试改变阶段1转换表条目的任何无效条目更新受限位(至少包括用于编码条目是否被保护的任何位),并且如果是,则方法再次行进到步骤710和712以抑制至少无效条目更新受限位的更新并且设置条件状态标志(再次,这可通过完全拒绝写入或者通过仅向非更新受限位进行写入来完成)。

[0186] 另一方面,如果在步骤716处,确定ReadData具有与作为被编码为受保护条目的有效的阶段1转换表条目一致的值,则在步骤720处,受保护条目检查电路54确定NewData是否尝试改变从对应于目标地址的存储器系统位置读取的阶段1转换表条目的任何有效条目更新受限位(至少包括用于编码条目是否被保护的任何位)。如果是,则再次在步骤710处拒绝或仅允许写入非更新受限位,并且在步骤712处设置条件状态标志以报告写入的失败。

[0187] 在不支持将无效转换表条目编码为受保护条目的具体实施中,可省略步骤716和718,并且在将ReadData编码为受保护条目的情况下,方法可直接从步骤706行进到步骤720。

[0188] 如果在步骤708处,在ReadData不是受保护条目的情况下将写入NewData,或在步骤718或720处,NewData(在ReadData是受保护条目的情况下将写入)不尝试改变任何更新受限位,则在步骤714处,允许RCW指令的写入,并且因此将NewData写入到对应于目标地址的存储器系统位置。

[0189] 不管写入是成功还是被拒绝(至少部分地),在步骤724处,操作取决于正在执行的当前RCW指令是存储变体还是交换变体而变化。如果指令是存储变体,则在步骤726处不需要进一步动作,并且不将ReadData写入到任何目的地寄存器。如果指令是交换变体,则在步骤728处,将ReadData写入到目的地寄存器Xt。一些具体实施可能不支持存储变体和停止变体两者,在该情况下,可省略步骤724,并且方法可直接从步骤714行进到步骤726和728中的相关步骤。

[0190] 在步骤704处的读取、在步骤714处的写入以及在步骤704和714之间执行的各种检查操作以原子方式来执行,作为不可分的操作集合,对于该操作集合,对存储器系统位置的介入写入不可能在步骤704处的读取与步骤710或714处的写入之间发生,或者另一执行线

程不可能看到执行操作集合的部分结果。

[0191] 以下示出了用于表示RCW指令的存储/交换变体的功能性的一些示例性伪代码。应当理解,这仅是一个示例并且比图12中示出的更一般的表示更具体。例如,伪代码假设针对有效和无效受保护条目的更新受限位的选择被定义在对应掩码寄存器中,但是如以上所讨论的,这不是必要的,并且其他示例可硬连线哪些位是更新受限的选择,或者考虑受保护条目的所有位是更新受限。在该示例中,通过将条件状态标志的“零”标志Z设置为1来报告写入失败。其他示例可选择不同的条件状态来编码写入失败。应当理解,可使用上文所描述的受保护条目检查电路54中的硬件电路逻辑来实现下文以伪代码示出的功能性,因此伪代码旨在示出电路逻辑的逻辑功能性,而非暗示软件执行这些功能。

[0192]
```
bits(4) pstate_bits = "0000";
NewData = X[s];
Address = X[d];

ReadData<63:0> = Mem[Address];
protected = ReadData<0> == '1' ? ReadData<Valid_Protected_Bitpos>:
ReadData<Invalid_Protected_Bitpos>;
if protected == '0' then
    new_protected = NewData<0> == '1' ? NewData<Valid_Protected_Bitpos>:
    NewData<Invalid_Protected_Bitpos>;
    if new_protected == '0' then // can't change the protected field
        Mem[Address] = NewData;
    else
        pstate_bits="0100"; // Z bit set on failure to write
else
    if ReadData<0> == '0' then // invalid entry
    if NewData<Invalid_Protected_Bitpos> == '0' && NewData<0> == '0'
       then // can't change valid or protected
            Mem[Address] = NewData;
        else
            pstate_bits="0100"; // Z bit set on failure to write
    else
        if (NewData^ReadData) & ~RCWMask_EL2 == Zeros(64) then
            Mem[Address] = NewData;
        else
            pstate_bits = "0100" ; // Z bit set on failure to write
PSTATE.NZCV = pstate_bits;
X[t] = ReadData; // return the old value
```

[0193] 图13是示出受保护条目检查RCW指令的比较和交换(CAS)变体的处理的流程图。通过与图12中相同的附图标记示出的图13的步骤与以上讨论的步骤相同。应当注意,与图12相比,用于存储ReadData且提供NewData的寄存器的符号已在图13中交换—Xt现在为提供NewData的寄存器并且Xs是在写入之前用ReadData的旧值写入的目的地寄存器。图13与图12的不同之处在于步骤700通过步骤750来替换,因为CAS变体指定了被称为比较数据(“CompareData”)的附加源操作数。在该示例中,为了减小指令编码中所需的寄存器字段的数量,在步骤728处,在用作写入ReadData的目的地寄存器的相同寄存器X中指定CompareData,但这并非必要,并且其他示例可在与X分开的另一寄存器中指定比较数据。

[0194] 步骤702和704与图12中的步骤相同。在步骤704之后,执行附加步骤752以将从对应于目标地址的给定存储器系统位置读取的ReadData与寄存器Xs中的RCW指令所指定的CompareData进行比较。受保护条目检查电路54基于比较来确定是否满足比较条件。例如,比较条件可为CompareData与ReadData是否相等,或可基于另一比较条件,诸如小于、大于、不相等等。一些具体实施可将比较条件固定为相等条件,而其他实施方案可允许指令的参

数选择要执行哪种类型的比较。如果不满足比较条件,则在步骤754处,拒绝RCW指令所请求的写入并且设置条件状态标志以报告由比较条件失败引起的写入失败(例如,在比较条件失败上设置否定标志N)。如果满足比较条件,则以与图12中相同的方式执行步骤706、708、710、714、716、718、720以检查从对应于目标地址的存储器系统位置读取的数据的受保护条目状态,并且基于检查的结果来控制是否许可写入。如果许可写入,则步骤714与先前讨论的步骤相同以允许写入继续进行,从而将NewData写入到存储器系统位置。如果在步骤710处拒绝写入或仅部分地执行写入,则图12的后续步骤712被图13的步骤762替换,这是相同的,因为它设置条件状态标志以报告写入失败,但是在比较和交换变体的情况下,这可区分该失败是由受保护条目检查失败引起的,从而将条件状态标志设置为与在比较条件失败的情况下在步骤754处使用的值不同的值。

[0195] 不管是否满足比较条件或者受保护条目检查是否成功,步骤724、726和728都与图12中相同以任选地将ReadData写入到目的地寄存器Xs(当目的地寄存器指定符指定预定值(例如31)时,再次可以抑制目的地寄存器Xs的更新)。

[0196] 示出用于RCW指令的CAS变体的功能性的一种可能具体实施的伪代码示例在下面示出:

[0197]
```
bits(4) pstate_bits = "0000";
NewData = X[t];
CompData =X[s];
Address = X[d];

ReadData<63:0>  = Mem[Address];
if ReadData == CompData then
    protected = ReadData<0> == '1' ? ReadData<Valid_Protected_Bitpos>:
      ReadData<Invalid_Protected_Bitpos>;
    if protected == '0' then
      new_protected = NewData<0> == '1' ? NewData<Valid_Protected_Bitpos>:
        NewData<Invalid_Protected_Bitpos>;
        if new_protected == '1' then // can't change the protected field
            pstate_bits="0100"; // Z bit set on failure to write
    else
        if ReadData<0> == '0' then // invalid entry
            if NewData<Invalid_Protected_Bitpos> == '1' ||
               NewData<0> == '1' then  // can't change valid or protected
                pstate_bits="0100"; // Z bit set on failure to write
            else
                if (NewData^ReadData) & ~RCWMask_EL2 == Zeros(64) then
                    Mem[Address] = NewData;
                else
                    pstate_bits = "0100" ; // Z bit set on failure to write
else
    pstate_bits = "1000";  // new return value on N bit of a CAS failure
PSTATE.NZCV = pstate_bits;
X[s] = ReadData;   // return the old value
```

[0198] 该伪代码示例示出了其中比较条件评估优先于受保护条目检查的情况,因此如果比较条件失败但条目也被保护并且步骤708、718、720处的检查失败,则条件状态代码将使用N位来指示CAS失败。受保护条目检查也可能优先,使得如果条目被保护并且步骤708、718或720处的检查失败,则即使比较条件已失败,则条件状态代码也将使用Z位来指示由于受保护条目检查引起的写入失败。例如,图13可被修改为在步骤714之后而不是在步骤706之前实现步骤752和754。

[0199] 图14是示出受保护条目检查RCW指令的位设置/清除变体的处理的流程图。在图14

中,步骤700-728与图12中相同,不同之处在于在图14中,NewData不是直接在源寄存器中指定,而是基于源寄存器Xs中提供的位掩码(“BitMask”)来计算,该位掩码对所寻址的存储器系统位置内的待设定或清除的位的位置进行编码。因此,相对于图12的唯一差异在于,在步骤700处,寄存器Xs定义BitMask而不是直接指定NewData,并且在步骤704与706之间执行附加步骤770、772、774。在步骤770处,方法取决于正在执行位设置指令还是位清除指令而不同(不必支持两种类型的指令,因此如果仅支持这些指令中的一者,则可省略步骤770并且在步骤704之后执行步骤772、774中的相关一者)。如果正在执行位设置指令,则在步骤774处,将NewData设置为对从所寻址的存储器系统位置读取的ReadData和由RCW指令指定的BitMask执行逐位或运算的结果(因此,对于位设置指令,请求BitMask中用“1”标记的位的位置在所寻址的存储器系统位置内被设置为1)。相比之下,在步骤772处,如果正执行位清除指令,则将NewData设置为对ReadData和BitMask的逆执行逐位与运算的结果(因此,对于位清除指令,请求BitMask中用“1”标记的位的位置在所寻址的存储器系统位置内被清除为0)。对于位设置变体和位清除变体两者,对应于BitMask的“0”位的ReadData的位在NewData中保持其原始值,因此不被RCW指令改变。在步骤772或774处计算了NewData之后,图14的后续步骤全部与图12中相同。

[0200] 示出用于RCW指令的位设置/清除变体的功能性的一种可能具体实施的伪代码示例在下面示出:

```
bits(4) pstate_bits = "0000";
NewData = X[s];
Address = X[d];

ReadData<63:0>  = Mem[Address];
protected = ReadData<0> == '1' ? ReadData<Valid_Protected_Bitpos>:
ReadData<Invalid_Protected_Bitpos>;

NewData = ReadData & ~NewData;//CLR or NewData = ReadData | NewData;//SET

if protected == '0' then
    new_protected = NewData<0> == '1' ? NewData<Valid_Protected_Bitpos>:
    NewData<Invalid_Protected_Bitpos>;
[0201]    if new_protected == '0' then // can't change the protected field
            Mem[Address] = NewData;
        else
            pstate_bits="0100"; // Z bit set on failure to write
else
    if ReadData<0> == '0' then // invalid entry
       if NewData<Invalid_Protected_Bitpos> == '0' && NewData<0> == '0'
       then  // can't change valid or protected
            Mem[Address] = NewData;
        else
            pstate_bits="0100"; // Z bit set on failure to write
   else
        if (NewData^ReadData) & ~RCWMask_EL2 == Zeros(64) then
            Mem[Address] = NewData;

        else
[0202]          pstate_bits = "0100" ; // Z bit set on failure to write
PSTATE.NZCV = pstate_bits;
X[t] = ReadData;   // return the old value
```

[0203] 对于本申请中的所有流程图来说,应当理解,相同的功能也可以以不同的顺序来实现,使得虽然流程图示出了步骤的顺序序列,但是对于彼此不依赖的任何步骤来说,可以重新排序这些步骤或者至少部分并行地执行这些步骤。

[0204] 因此,如图6中所示,用于遍历转换表树结构以到达对应于敏感存储器页(例如,预期用于敏感数据或指令的页)的中间地址映射的各种阶段1转换表条目可被设置为具有受保护条目编码。即使这些条目中的一者被临时设置为无效以禁止访问该页(例如,作为分页操作的结果),情况也可能如此。同时,与受保护条目相同的页表中的其他条目可以是更新受到较少限制的非受保护条目。通过支持受保护条目编码,这使得存储在存储器的PRO区域中的给定页表能够包含受保护和非受保护条目的混合,其中非受保护条目能够由在EL1下执行的操作系统代码更新而无需系统管理程序干预,通过根据上文讨论的变型中的任一者执行RCW指令,同时受保护条目可以具有对其施加的更严格的限制。由于专用类型的指令(例如,上述RCW指令的变体中的一者或多者)被提供用于触发受保护条目检查,并且PRO许可防止其他类型的指令(诸如大多数存储指令)能够更新存储器的PRO区域,这避免了在对存储器的每次写入时执行受保护条目检查的需要,这在性能方面将是非常昂贵的。

[0205] 抗混叠检查

[0206] 上文讨论的机制对于保护特定的阶段1转换条目不被破坏(或者被恶意方黑客攻击的代码故意破坏或者被写得很差的代码偶然破坏)是有用的。然而,如图15中所示,通过定义指定相同中间地址映射62的阶段1转换表条目,若干不同虚拟地址有可能混叠到相同中间地址。为了防止攻击者能够通过定义将不同虚拟地址VA2映射到相同中间地址IPA的混叠阶段1条目来规避上文针对第一组阶段1转换条目映射VA1到IPA所论述的PRO许可和受保护条目编码所提供的保护,如图8中所示,阶段2转换表条目可具有指定存储器的对应区域是否具有抗混叠性质的位字段79。如果该区域被指示为具有抗混叠性质,则对于针对该区域的访问执行附加的抗混叠检查,以检查所有遍历的阶段1转换表条目(其将在转换表遍历中被访问以定位指定从该区域的虚拟地址到物理地址的阶段1地址映射的对应阶段1转换表条目)是否是:(a)存储在存储器的PRO区域中并且被编码为受保护条目,或者(b)存储在存储器的只读区域中。需注意,这不一定要求在对与具有抗混叠性质的阶段2转换表条目相关联的存储器区域的每次访问时实际执行对那些遍历的阶段1转换表条目的页表遍历。有可能将信息高速缓存在TLB 29中以指示是否通过抗混叠检查(或针对某些遍历的阶段1转换表条目指示其是否已被确定为存储在PRO区域中和/或是受保护条目),以避免每次需要执行完整的转换表遍历。

[0207] 图16是示出执行抗混叠检查的方法的流程图。在步骤800处,发出指定特定目标虚拟地址VAx的存储器访问请求。在步骤802处,MMU 28根据从VAx到中间地址IPAy的阶段1映射和从中间地址IPAy到目标物理地址PAz的阶段2映射来发起从目标虚拟地址VAx到目标物理地址PAz的地址转换(对于阶段1和阶段2转换执行两个单独动作不是必要的,虽然这是一个选项,但其他示例可具有组合的阶段1与阶段2TLB,其可针对已高速缓存的转换直接从VAx映射到PAz,但在TLB中未命中时,通过执行如图6所示的阶段1和阶段2遍历来识别新的VA到PA映射)。

[0208] 在步骤804处,MMU 28检查对应于IPAy的阶段2转换表条目(块或页描述符)是否指示抗混叠性质。如果是,则在步骤806处,MMU检查是否所有遍历的阶段1转换表条目都满足抗混叠条件。如果执行了对应于虚拟地址VAx的完整转换表遍历,则遍历的阶段1转换表条目是将在转换表遍历中被访问以定位指定从VAx到IPAy的S1地址映射的对应S1转换表条目的条目(取决于已经在TLB 29中高速缓存的内容,当前存储器访问可能实际上不需要遍

历)。例如,在图6中,遍历的阶段1转换表条目将是L0、L1和L2阶段1页表中的标记为D_Table的条目,以及L3阶段1页表中的标记为D_Page的条目。当满足以下条件中的任一项时,对于给定的遍历的阶段1转换表条目,满足抗混叠条件:

[0209] (a)给定的遍历的阶段1转换表条目被指定为受保护条目,并且给定的遍历的阶段1转换表条目被存储在物理地址PAj处,对于该物理地址,PRO许可由提供用于导出PAj的阶段2地址映射的相关阶段2转换表条目指定;或者

[0210] (b)只读许可由相关阶段2转换表条目指定,该相关阶段2转换表条目提供用于导出给定的遍历的阶段1转换表条目的物理地址PAj的阶段2地址映射。

[0211] 对于图6的特定示例,用于导出所访问页的PA的L1阶段1条目的相关阶段2转换表条目将是在图6中被指示为"D_Page"的阶段2L3条目。对于图6中所示的其他遍历的阶段1条目,将类似地存在相关阶段2L3条目(或阶段2L1或L2条目,如果发现阶段2块描述符对应于IPAy的话),其应当用PRO或只读许可来标记,以便满足抗混叠条件(这些是为了获得每个遍历的阶段1转换表的物理地址而示出的各个阶段2转换遍历的结束处的条目)。

[0212] 如果在图16的步骤806处,MMU 28确定遍历的阶段1转换表条目中的任一者或多者不满足抗混叠条件,则在步骤808处拒绝存储器访问。可以发信号通知故障,其可触发异常处置器(例如,在EL2处执行)以执行错误处置动作。

[0213] 如果所有遍历的阶段1转换表条目满足抗混叠条件,则省略步骤808。在这种情况下,在步骤810处,MMU 28还检查是否满足任何其他检查(例如基于针对对存储器区域的访问设置的PRO许可的任何检查,受保护条目检查是否响应于RCW指令而发出存储器访问请求,或用于防止其他不适当访问的任何其他特定检查,例如基于支持这一点的实施方案中的安全/非安全状态的检查)。如果不满足任何其他检查,则再次在步骤808处拒绝存储器访问(所生成的故障类型可以取决于访问检查失败的原因)。否则在步骤812处允许存储器访问请求继续进行。

[0214] 因此,如图6中所示,可在提供正被访问的存储器区域的物理地址映射(此可为页描述符或块描述符)的阶段2转换表条目中设置抗混叠性质。如果设置了抗混叠性质,则对于针对对应存储器位置的有效访问,这将要求到为该存储器区域提供中间地址映射的条目的路径上的所有被遍历的阶段1转换表条目(a)被标记为受保护,并且对于提供存储那些被遍历的阶段1转换表条目的区域的物理地址映射的阶段2条目指定PRO许可,或者(b)被存储在由为该PA提供PA映射的阶段2条目指定只读许可的PA处。这意味着攻击者不能容易地建立新的混叠阶段1地址映射来规避应用于预期用于访问存储器的对应区域的可信地址映射的保护。能够影响EL1下的操作系统代码的行为的攻击者将不能控制用于控制存储器访问的阶段2条目,因为这将基于VTTBR_EL2寄存器中的基地址,该基地址不能由在EL1下执行的代码更新(因此不能使PRO或只读许可变为针对存储攻击者的新创建的混叠阶段1地址映射的区域而设置)。此外,由于在EL1下执行的用于更新阶段1转换表条目的代码的机制可以是执行上文讨论的受保护条目检查类型的RCW指令(其他指令被禁止写入存储器的PRO区域),并且该指令不能改变任何转换表条目的受保护状态,所以攻击者不能使阶段1条目变得受保护。此外,只读区域不能被任何写入指令写入。因此,攻击者能够创建的任何新条目应当未通过用于获得VA-IPA映射的阶段1条目是否被保护以及那些条目是否被存储在存储器的PRO或只读区域中的抗混叠检查中的至少一者。

[0215] 防止对阶段1顶层基地址的不适当更新

[0216] 能够影响在EL1下执行的操作系统代码的行为的攻击者可能尝试的另一攻击可以是修改由基地址寄存器TTBR_EL1指示的阶段1顶层基地址(标识L0阶段1页表的存储器中的位置)。例如,攻击者可以替换由攻击者定义的一组新的阶段1表的地址,以替换经授权的页表结构的地址,该地址被正确地形成并且如由管理程序所验证的那样正确地表现。而且,攻击者可能试图迫使MMU 28以非预期方式使用现有经授权的阶段1页表,例如通过替换L1、2或3页表中的一者的基地址以替换正确的L0基地址,使得用于不同存储器区域的下一级表指针或地址映射可不正确地用于正被访问的存储器区域,这是由于所访问的表在树的不同于预期层级的错误层级处使用,使得虚拟地址的不同位用于从表选择相关条目。

[0217] 图17示出了阶段1顶层基地址检查,其可以被执行以防止这些类型的攻击。在步骤1000处,对于指定特定目标虚拟地址的存储器访问请求需要页表遍历(对于不需要页表遍历的存储器访问请求,因为所需要的地址映射已经可从TLB获得,那么当那些地址映射在较早页表遍历之后被分配到高速缓存时,将已经完成任何所需要的阶段1顶层基地址检查,并且因此不必实施另一检查)。在步骤1002处,基于阶段1转换表基地址寄存器TTBR_EL1中的值来确定阶段1顶层基地址。基地址被指定为中间地址IPA_base。在步骤1004处,MMU 28获得由相关联阶段2转换表条目指定的提供从IPA_base到PA_base的映射的信息。例如,如果已经高速缓存在TLB中,则可以从TLB 29获得该信息,或者可以通过使用在阶段2转换表基地址寄存器VTTBR_EL2中指定的阶段2基地址执行阶段2转换表遍历来获得该信息。

[0218] 在步骤1006处,MMU 28确定是否启用阶段1顶层表部分只读检查。例如,这可以基于存储在控制寄存器(例如,阶段2转换控制寄存器VTCR_EL2,其更新被限制为在异常层级EL2或更高层级执行的代码)中的阶段1顶层表部分只读检查启用控制值来确定。另选地,其他具体实施可以认为阶段1顶层表部分只读检查被永久地启用。如果阶段1顶层表部分只读检查被启用,则在步骤1008处,MMU 28检查相关联的阶段2转换表条目是否指定PRO许可,并且如果不指定,则在步骤1010处,拒绝存储器访问并且发信号通知故障。这意味着如果攻击者试图修改阶段1转换表基地址寄存器TTBR_EL1以指向由攻击者创建的新的L0页表,则基于经修改的基地址的访问将失败,因为攻击者将不能修改存储器的PRO区域并且因此必须写入非PRO区域,因此阶段1顶层表PRO检查将失败。

[0219] 如果阶段1顶层表PRO检查在步骤1006处被禁用,或者被启用但在步骤1008处通过,则在步骤1012处MMU 28确定阶段1顶层表存在检查是否被启用。再次,这可以基于存储在控制寄存器(例如,阶段2转换控制寄存器VTCR_EL2)中的阶段1顶层表存在检查启用控制值来确定。用于确定是否在步骤1012处启用检查的启用控制值可与上文针对步骤1006所提及的启用控制值相同(例如,在一些实施方案中,步骤1008和1014处的检查可被视为作为整体启用或作为整体停用的单个检查的两个步骤)。如果阶段1顶层表存在检查被启用,则在步骤1014处,MMU 28确定相关联的阶段2转换表条目是否指定阶段1顶层条目存在许可80。如上文关于图8所提及,阶段1顶层条目存在许可可以被编码为PRO许可的另选变体(使得具有阶段1顶层条目存在许可的存储器区域也被假定为具有PRO许可),或另选地被编码为与是否提供PRO许可的指示分离的独立属性。如果相关联的阶段2转换表条目没有指定阶段1顶层条目存在许可,则再次在步骤1010处拒绝存储器访问并且发信号通知故障。这可用于通过将阶段1顶层基地址修改为指向L1、L2或L3表的地址来防止有效且可信的L1、L2或L3表

替代L0表,因为对应于用于保存L1、L2或L3表的存储器区域的阶段2条目可被定义为不具有阶段1顶层条目存在许可。仅用于保持任何有效且可信的阶段1L0表的存储器区域可在对应的阶段2条目中被标记为具有阶段1顶层条目存在许可,以限制哪些地址可用作用于有效存储器访问的阶段1L0基地址。

[0220] 如果阶段1顶层表存在检查在步骤1012处被禁用,或者被启用但在步骤1014处通过,则在步骤1016处MMU执行访问由PA_base标识的存储器区域所需的任何其他检查,并且如果这些检查失败,则在步骤1010处再次拒绝存储器访问。如果任何其他检查通过,则在步骤1018处,阶段1顶层基地址IPA_base可以有效地用于执行页表搜索。因此,通过将索引偏移应用于所确定的PA_base来获得阶段1顶层转换表条目的地址,其中基于待转换的目标VA的位子集来确定索引偏移。然后如前面所讨论的继续页表遍历。

[0221] 因此,如图6所示,在由软件定义的预期使用中(因此不是作为硬件的要求而强制执行的),在页表遍历上访问的阶段1条目中,为了获得期望添加保护的存储器区域的PA映射64,提供标识阶段1L0页表的存储位置的PA映射64的阶段2页/块描述符指定PRO和阶段1顶层存在许可,并且提供标识阶段1L1、L2或L3页表的存储位置的PA映射64的阶段2页/块描述符指定PRO许可,但是不指定阶段1顶层存在许可。这防止了上述基地址替换攻击。避免需要实现基地址检查的另选方案可为将对阶段1基地址寄存器TTBR_EL1的任何访问捕获到在EL2下执行的管理程序,该管理程序随后可检查在EL1下执行的操作系统代码所请求的更新是否有效并且在必要时拒绝更新。然而,在实践中,操作系统可能频繁地需要在上下文切换时切换基地址寄存器TTBR_EL1中的地址,并且因此在性能方面捕获每个更新可能是昂贵的。通过实现图17中所示的阶段1顶层基地址检查,这可以避免对基地址寄存器更新到TTBR_EL1的此类捕获的需要,以改善性能。

[0222] 在一些示例中,可以支持阶段1顶层存在许可的单个变体,在这种情况下,图17的步骤1014处的检查可以简单地是对是否已经指定阶段1顶层存在许可的检查。

[0223] 其他示例可支持阶段1顶层存在许可的多个变体以允许对特定阶段1转换表基址寄存器可指定对应存储器区域中的地址的更精细控制。例如,一些具体实施可支持两个阶段1基地址寄存器:

[0224] ●TTBR0_EL1,当待转换的虚拟地址的最高有效位的可配置数量(N)全部被设置为0(N可以在控制寄存器中指定的控制值中定义)时,在EL0或EL1中被选择用于阶段1转换;和

[0225] ●TTBR1_EL1,当待转换的虚拟地址的N个最高有效位中的任一者不是0时,在EL0或EL1中被选择用于阶段1转换。

[0226] 然后可以定义阶段1顶层存在许可的若干变体,包括:

[0227] ●Toplevel0:指示被允许用于经由TTBR0_EL1访问的顶层转换表而不是经由TTBR1_EL1访问的顶层转换表的存储器区域;

[0228] ●Toplevel1:指示允许用于经由TTBR1_EL1访问的顶层转换表而不是经由TTBR0_EL1访问的顶层转换表的存储器区域;

[0229] ●Toplevel01:指示允许用于经由TTBR0_EL1或TTBR1_EL1访问的顶层转换表的存储器区域。

[0230] 在这种情况下,如果满足以下条件中的任一项,则步骤1014处的检查的一个具体实施可以使得在图17的步骤1010处发信号通知故障:

[0231] ●TTBR0_EL1用于提供对应存储器区域不具有Toplevel0或Toplevel01许可的基地址;或者

[0232] ●TTBR1_EL1用于提供对应存储器区域不具有Toplevel1或Toplevel01许可的基地址。

[0233] 在一些具体实施中,在由EL2下的软件控制的控制寄存器中设置的另外的控制可以控制是否禁止TTBR0_EL1给予对Toplevel1页的访问,以及是否禁止TTBR1_EL1给予对Toplevel0页的访问。在这种情况下,如果满足以下条件中的任一项,则步骤1014处的检查可以使得在步骤1010处发信号通知故障:

[0234] ●TTBR0_EL1用于提供基地址,对于该基地址,当TTBR0/Toplevel01故障启用控制被设置为使得故障能够在TTBR0_EL1用于访问Toplevel1页时被触发时,对应存储器区域不具有Toplevel1许可或者具有Toplevel1;或者

[0235] ●TTBR1_EL1用于提供基地址,对于该基地址,当TTBR1/Toplevel01故障启用控制被设置为使得故障能够在TTBR1_EL1用于访问Toplevel0页时被触发时,对应存储器区域不具有Toplevel0许可或者具有Toplevel0许可。

[0236] 这些特征允许对可用于提供顶层阶段1转换表的存储器地址区域的更细粒度的控制,但如果认为任何顶层页可用于提供TTBR0和TTBR1两者的基地址是可接受的,则启用控制允许这些更细粒度的检查被禁用。

[0237] 在一些具体实施中,各种顶层存在许可Toplevel0、Toplevel1、Toplevel01的编码可以与PR0许可的编码相组合,使得这些被视为Toplevel0 PR0许可、Toplevel1 PR0许可和Toplevel01 PR0许可。在此类具体实施中,将不可能将Toplevel0、Toplevel1或Toplevel01存储器区域定义为不具有PR0许可。然而,可以将PR0区域定义为不具有任何Toplevel0、Toplevel1或Toplevel01许可,因为存在不被视为具有任何阶段1顶层表存在许可的单独PR0许可编码。

[0238] 模拟器示例

[0239] 图18示出了可以使用的模拟器具体实施。虽然先前所述的实施方案在用于操作支持所涉及的技术的特定处理硬件的装置和方法方面实现了本发明,但也可以提供根据本文所述的实施方案的指令执行环境,该指令执行环境是通过使用计算机程序来实现的。此类计算机程序通常被称为模拟器,在一定程度上是因为此类计算机程序提供硬件架构的基于软件的具体实施。模拟器计算机程序的种类包括仿真器、虚拟机、模型和二进制转换器,其包括动态二进制转换器。通常,模拟器具体实施可在支持模拟器程序1210的主机处理器1230上运行,该主机处理器任选地运行主机操作系统1220。在一些布置中,在硬件和所提供的指令执行环境和/或在同一主机处理器上提供的多个不同指令执行环境之间可存在多个模拟层。在历史上,需要强大的处理器来提供以合理速度执行的模拟器具体实施,但这种方法在特定情况下可能是合理的,诸如当出于兼容性或重复使用原因而希望运行另一个处理器本地的代码时。例如,模拟器具体实施可向指令执行环境提供主机处理器硬件不支持的附加的功能性,或者提供通常与不同硬件架构相关联的指令执行环境。模拟概述在以下文献中给出:“Some Efficient Architecture Simulation Techniques”,Robert Bedichek,Winter 1990USENIX Conference,第53-63页。

[0240] 就先前已参考特定硬件构造或特征描述了实施方案而言,在模拟的实施方案中,

等效功能可由合适的软件构造或特征提供。例如,特定电路系统可在模拟的实施方案中被实现为计算机程序逻辑。类似地,存储器硬件诸如寄存器或高速缓存存储器可在模拟的实施方案中被实现为软件数据结构。在先前描述的实施方案中参考的硬件元件中的一个或多个硬件元件存在于主机硬件(例如,主机处理器1230)上的布置中,在合适的情况下,一些模拟的实施方案可利用主机硬件。

[0241] 模拟器程序1210可存储在计算机可读存储介质(其可以是非暂态介质)上,并且向目标代码1200(其可包括应用程序、操作系统和管理程序)提供程序接口(指令执行环境),该程序接口与由模拟器程序1210建模的硬件架构的接口相同。因此,目标代码1200的程序指令(包括上述受保护条目检查RCW指令)可使用模拟器程序1210从指令执行环境内执行,使得实际上不具有上述装置2的硬件特征的主机计算机1230可仿真这些特征。类似地,可以使用模拟器程序1210的存储器管理程序逻辑1218来模拟如上所述的各种存储器管理检查功能,包括对PRO区域类型的支持。

[0242] 因此,模拟器程序1210可以具有模拟上述处理电路4的状态的处理程序逻辑1212。例如,处理程序逻辑1212可以响应于在目标代码1200的模拟执行期间发生的事件来控制执行状态EL0-EL3的转变。指令解码程序逻辑1214对目标代码1200的指令进行解码并且将这些指令映射到主机装置1230的本地指令集中的对应指令集。寄存器仿真程序逻辑1216将目标代码所请求的寄存器访问映射到对在主机装置1230的主机硬件上维护的对应数据结构的访问,诸如通过访问主机装置1230的寄存器或存储器1232中的数据。存储器管理程序逻辑1218以与上述硬件实现的实施方案中描述的MMU 28相对应的方式实现地址转换、页表遍历和访问控制检查,但是还具有将基于为目标代码1200定义的页表通过地址转换中的阶段2映射获得的模拟物理地址映射到用于访问主机存储器1232的主机虚拟地址的附加功能。这些主机虚拟地址本身可以使用由主机支持的标准地址转换机制被转换成主机物理地址(主机虚拟地址到主机物理地址的转换在由模拟器程序1210控制的范围之外)。

[0243] 在本申请中,字词"被配置为..."用于意指装置的元件具有能够执行所限定的操作的配置。在该上下文中,"配置"意指硬件或软件的互连的布置或方式。例如,该装置可以具有提供所限定的操作的专用硬件,或者可以对处理器或其他处理装置进行编程以执行该功能。"被配置为"并不意味着装置元件需要以任何方式改变以便提供所限定的操作。

[0244] 虽然本文已结合附图详细描述了本发明的示例性实施方案,但应当理解,本发明并不限于那些精确的实施方案,并且在不脱离所附权利要求书所限定的本发明的范围的前提下,本领域的技术人员可在其中实现各种变化和修改。

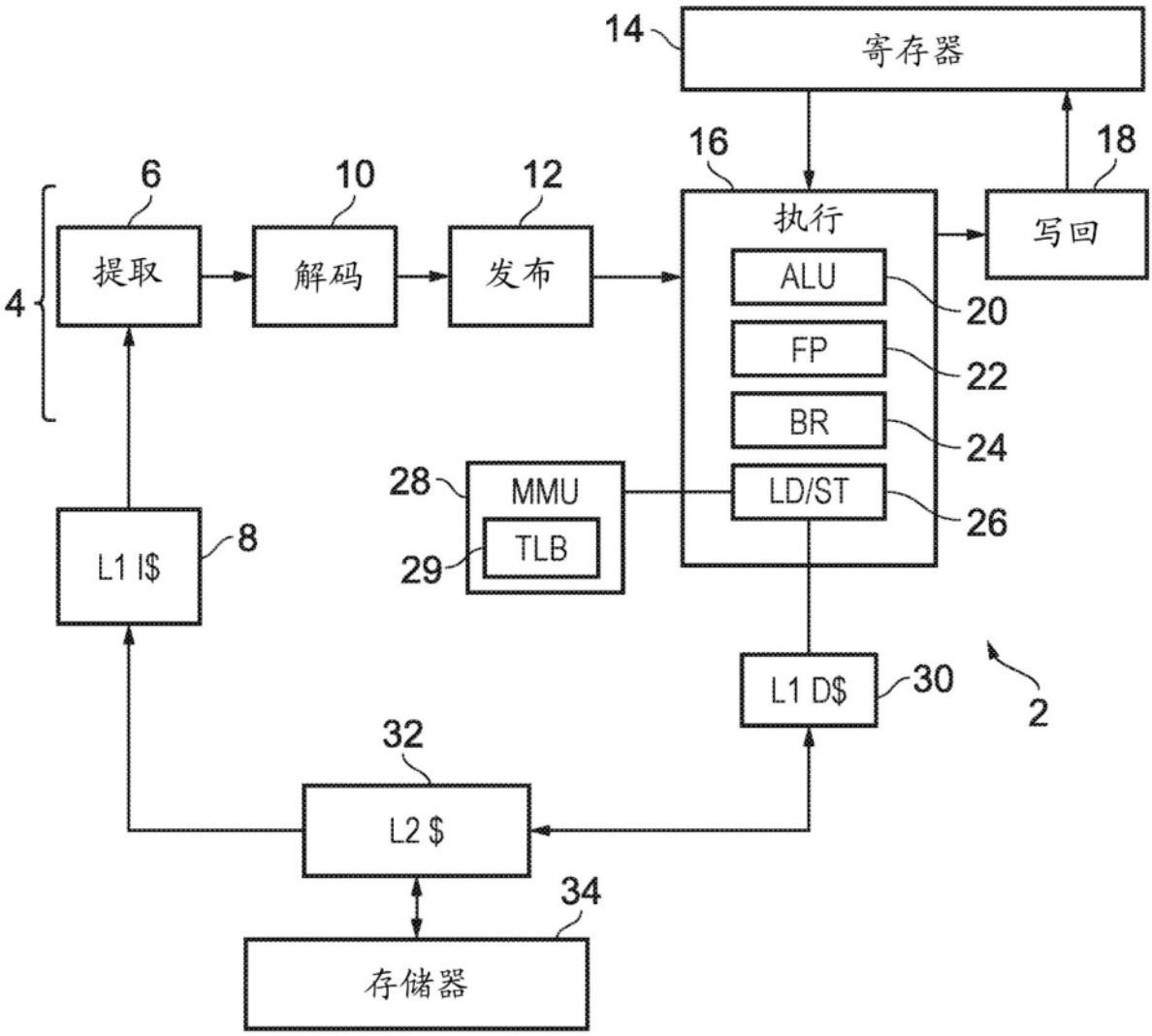

14
寄存器
16
18
6
10
12
执行
写回
提取
解码
发布
4
ALU
20
FP
22
BR
24
28
MMU
LD/ST
26
TLB
29
L1 I$
8
L1 D$
30
2
32
L2 $
34
存储器

图1

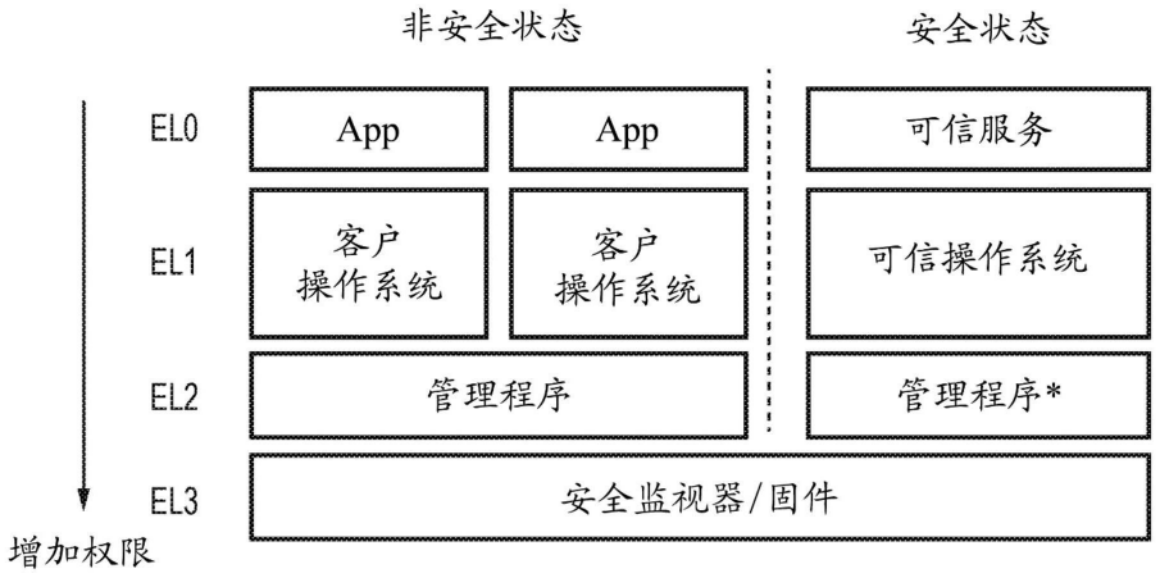

非安全状态
安全状态
EL0
App
App
可信服务
EL1
客户
操作系统
客户
操作系统
可信操作系统
EL2
管理程序
管理程序*
EL3
安全监视器/固件
增加权限

图2

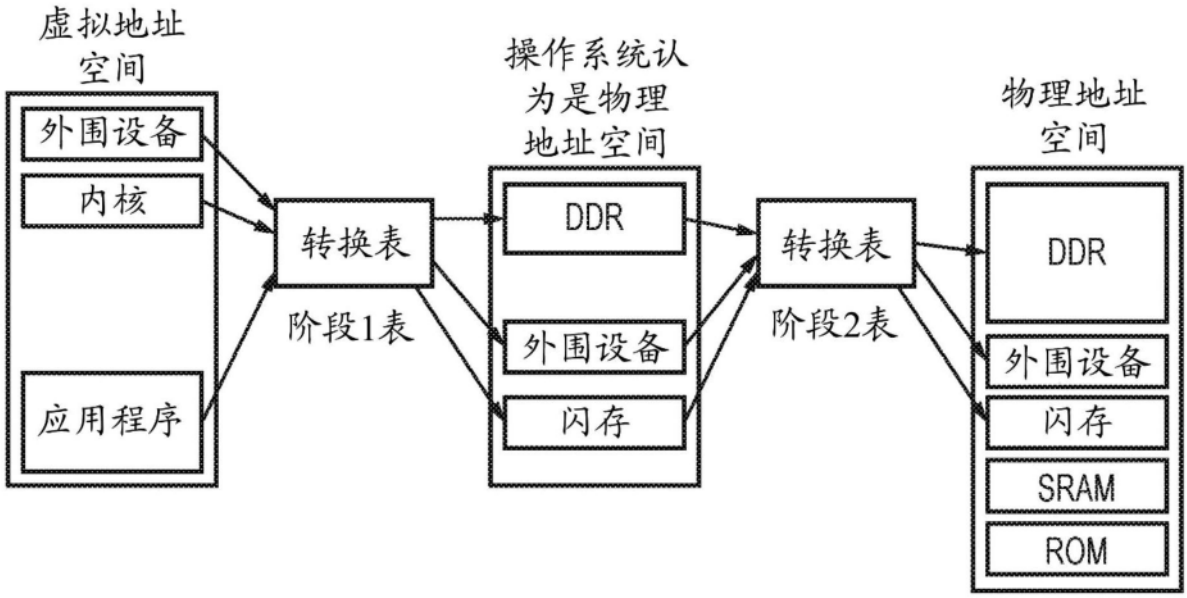

虚拟地址
空间
外围设备
内核
应用程序
转换表
阶段1表
操作系统认
为是物理
地址空间
DDR
外围设备
闪存
转换表
阶段2表
物理地址
空间
DDR
外围设备
闪存
SRAM
ROM

图3

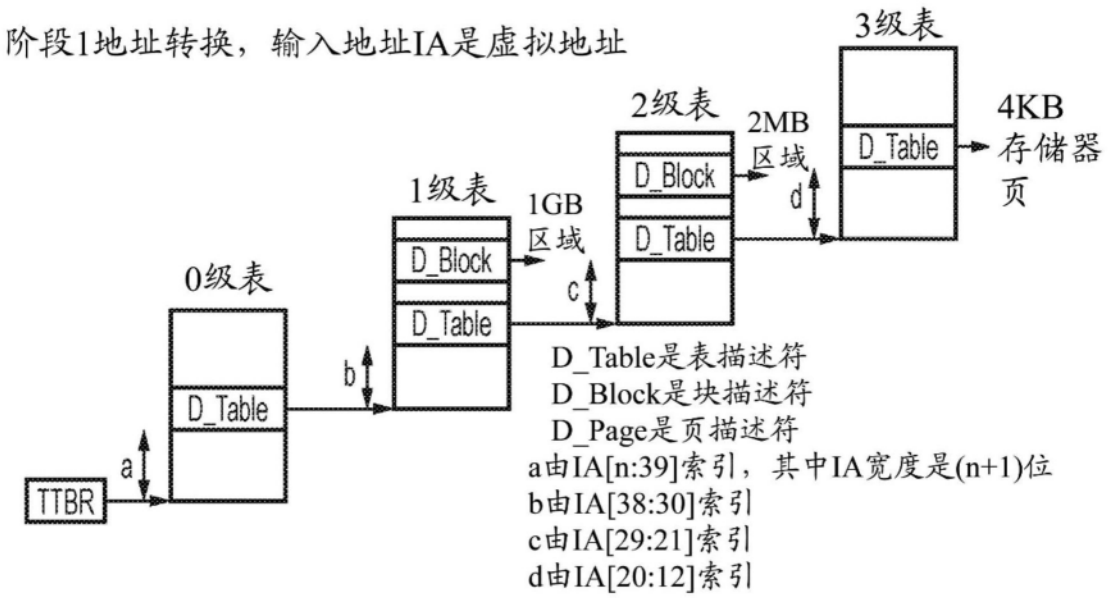

阶段1地址转换，输入地址IA是虚拟地址
3级表
2级表
2MB
区域
4KB
存储器
页
D_Table
D_Block
D_Table
d
1级表
1GB
区域
D_Block
D_Table
c
0级表
b
D_Table
a
TTBR
D_Table是表描述符
D_Block是块描述符
D_Page是页描述符
a由IA[n:39]索引，其中IA宽度是(n+1)位
b由IA[38:30]索引
c由IA[29:21]索引
d由IA[20:12]索引

图4

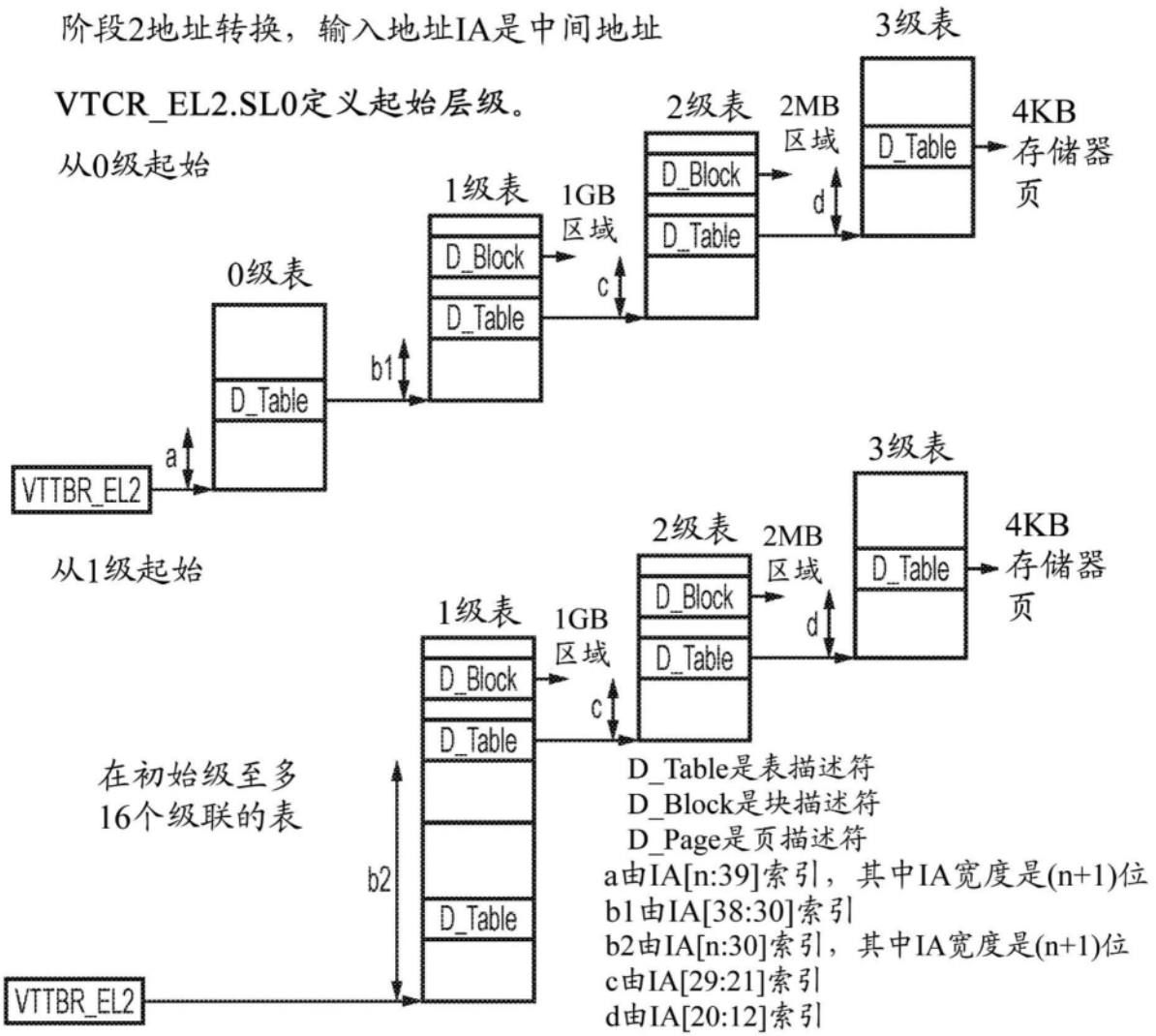

阶段2地址转换，输入地址IA是中间地址
VTCR_EL2.SL0定义起始层级。
从0级起始
从1级起始
0级表
1级表
2级表
3级表
D_Table
D_Block
1GB
区域
2MB
区域
4KB
存储器
页
VTTBR_EL2
a
b1
b2
c
d
在初始级至多
16个级联的表
D_Table是表描述符
D_Block是块描述符
D_Page是页描述符
a由IA[n:39]索引，其中IA宽度是(n+1)位
b1由IA[38:30]索引
b2由IA[n:30]索引，其中IA宽度是(n+1)位
c由IA[29:21]索引
d由IA[20:12]索引

图5

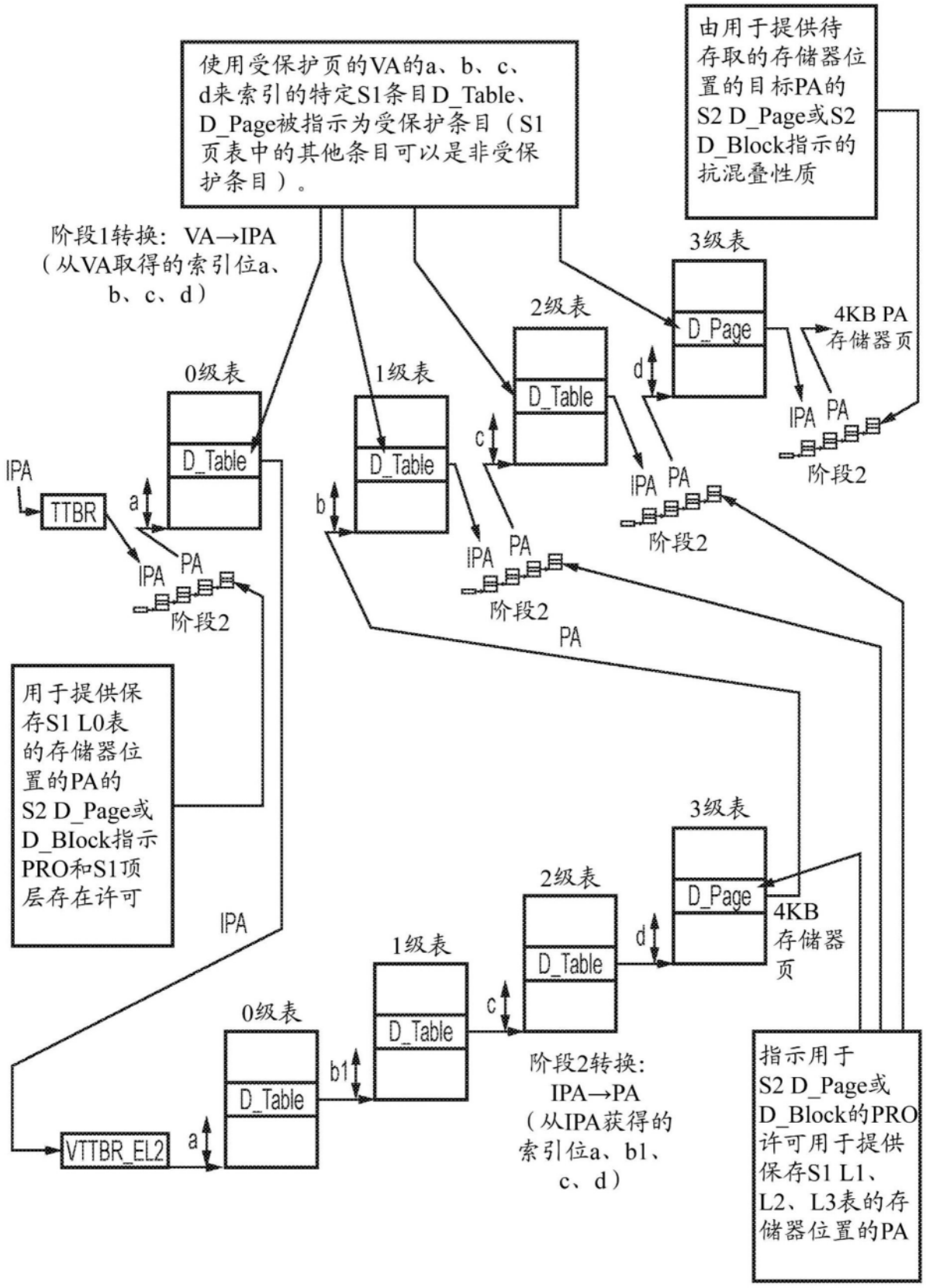

使用受保护页的VA的a、b、c、d来索引的特定S1条目D_Table、D_Page被指示为受保护条目（S1页表中的其他条目可以是非受保护条目）。
由用于提供待存取的存储器位置的目标PA的S2 D_Page或S2 D_Block指示的抗混叠性质
阶段1转换：VA→IPA（从VA取得的索引位a、b、c、d）
3级表
2级表
1级表
0级表
D_Page
D_Table
4KB PA存储器页
IPA
PA
阶段2
TTBR
a
b
c
d
用于提供保存S1 L0表的存储器位置的PA的S2 D_Page或D_Block指示PRO和S1顶层存在许可
VTTBR_EL2
b1
4KB存储器页
阶段2转换：IPA→PA（从IPA获得的索引位a、b1、c、d）
指示用于S2 D_Page或D_Block的PRO许可用于提供保存S1 L1、L2、L3表的存储器位置的PA

图6

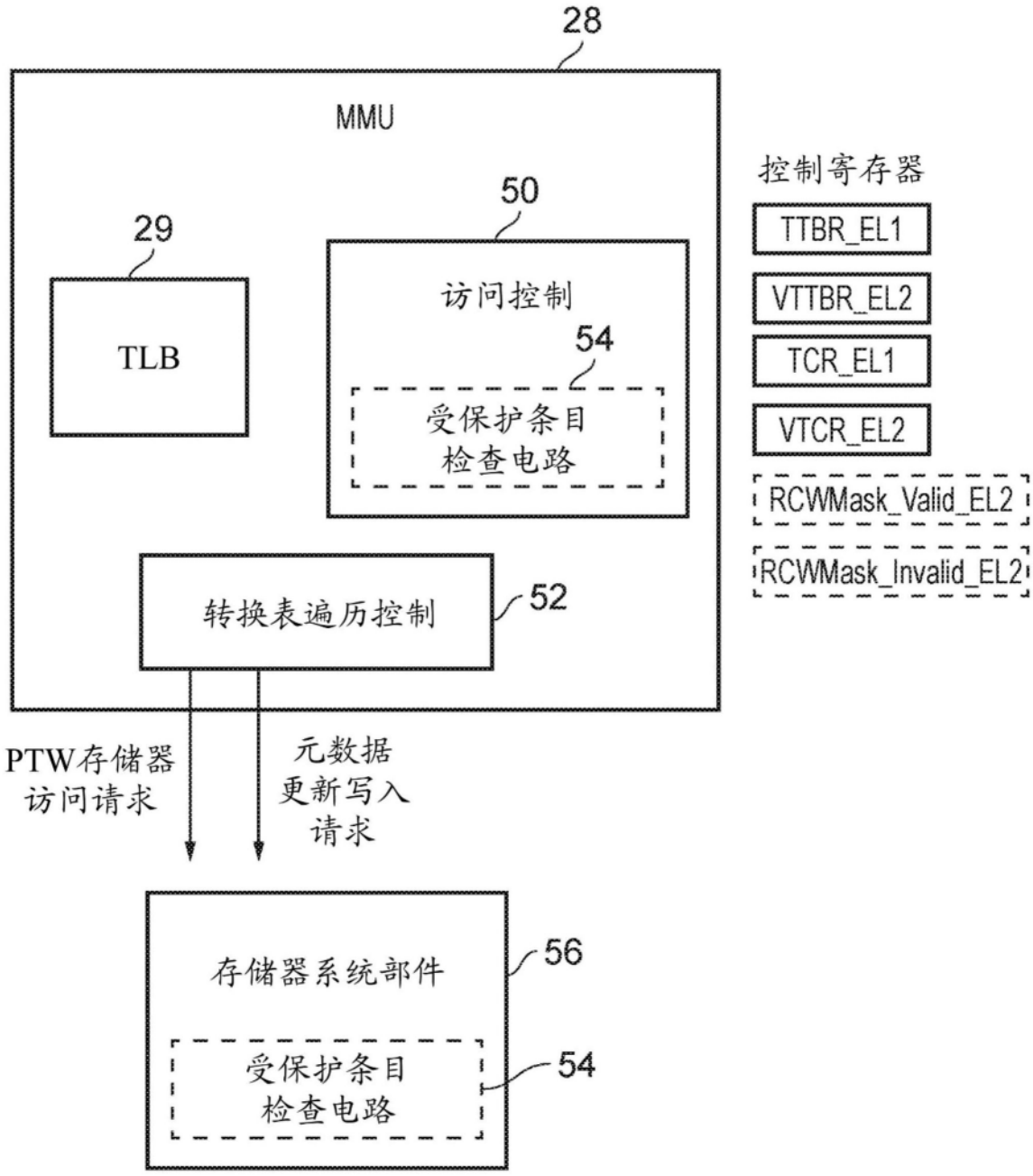

28
MMU
控制寄存器
TTBR_EL1
VTTBR_EL2
TCR_EL1
VTCR_EL2
RCWMask_Valid_EL2
RCWMask_Invalid_EL2
50
29
TLB
访问控制
54
受保护条目
检查电路
转换表遍历控制
52
PTW存储器
访问请求
元数据
更新写入
请求
存储器系统部件
56
受保护条目
检查电路
54

图7

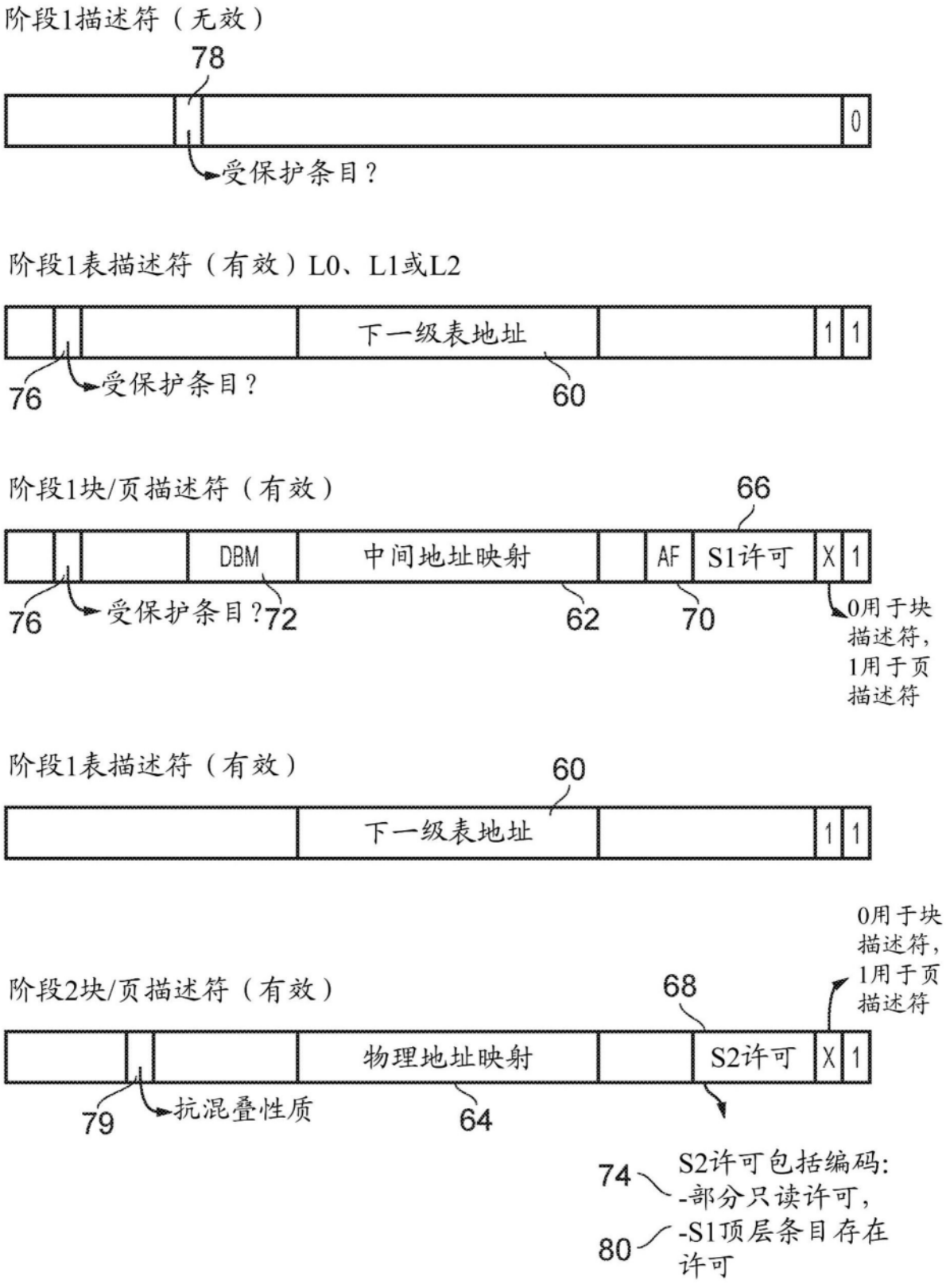

阶段1描述符（无效）
78
0
受保护条目？
阶段1表描述符（有效）L0、L1或L2
下一级表地址
1
1
76
受保护条目？
60
阶段1块/页描述符（有效）
66
DBM
中间地址映射
AF
S1许可
X
1
76
受保护条目？72
62
70
0用于块描述符，1用于页描述符
阶段1表描述符（有效）
60
下一级表地址
1
1
0用于块描述符，1用于页描述符
阶段2块/页描述符（有效）
68
物理地址映射
S2许可
X
1
79
抗混叠性质
64
74
S2许可包括编码:
-部分只读许可，
80
-S1顶层条目存在许可

图8

响应于不同的写入请求类型，对由S2许可标记为部分只读的存储器区域的写入访问控制：

允许写入到部分只读区域的写入请求类型	禁止写入部分只读区域的写入请求类型
（可选）响应于在EL2或EL3处执行的存储指令而发出的写入请求（包括如果在ELO或EL1处执行则禁止写入部分只读区域的至少一种类型的存储）	响应于在ELO或EL1处执行的至少一种类型的存储指令（例如，ISA的大多数存储指令）而发出的写入请求
在EL1处执行的预定类型的转换表条目更新指令，例如： •当通过受保护条目检查时，在EL1处执行的RCW指令的受保护条目检查类型。	
由MMU生成的用于更新转换表条目中的访问跟踪元数据的元数据更新写入请求（例如，AF、当DBM被设置时的写入许可）	

当在EL1处发出写入时被允许写入到部分只读区域的写入请求类型的受限子集

图9

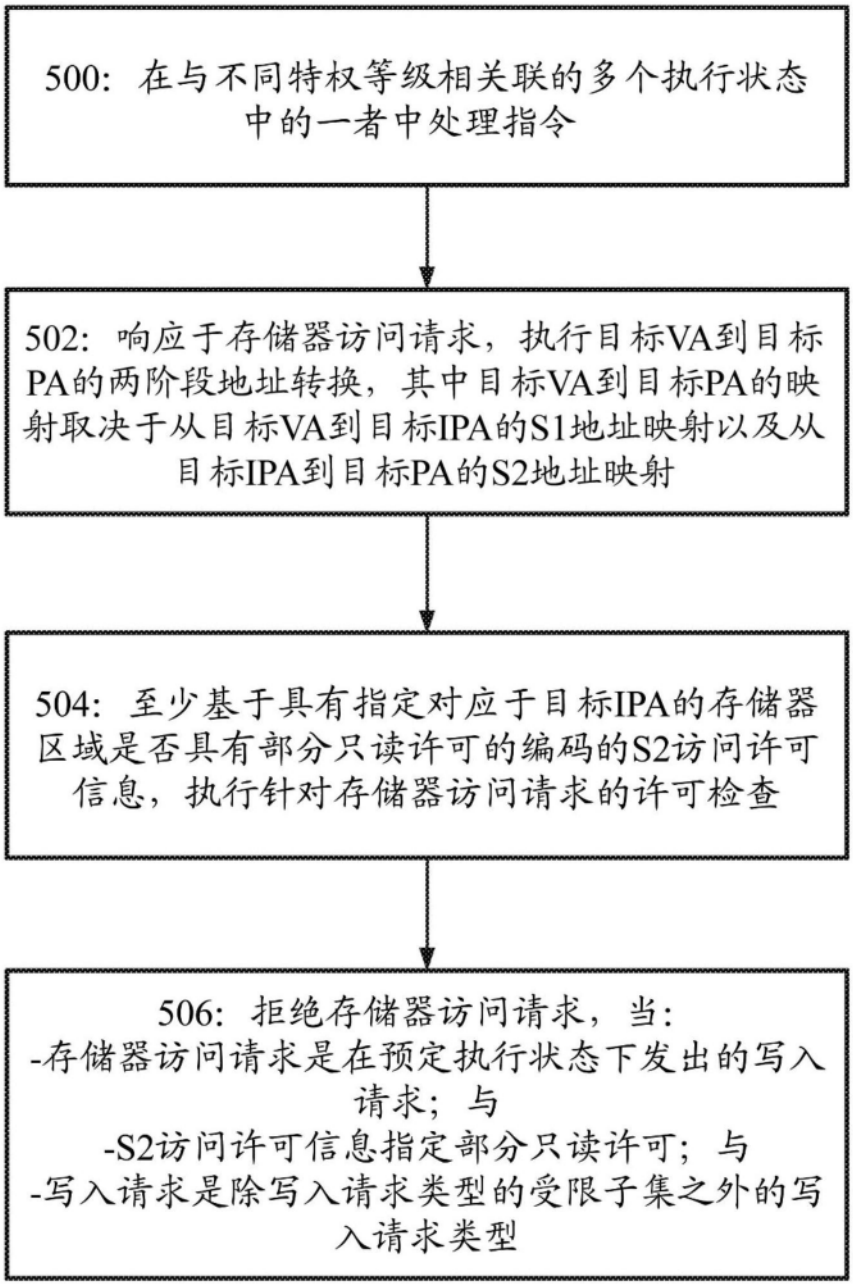

500：在与不同特权等级相关联的多个执行状态中的一者中处理指令
502：响应于存储器访问请求，执行目标VA到目标PA的两阶段地址转换，其中目标VA到目标PA的映射取决于从目标VA到目标IPA的S1地址映射以及从目标IPA到目标PA的S2地址映射
504：至少基于具有指定对应于目标IPA的存储器区域是否具有部分只读许可的编码的S2访问许可信息，执行针对存储器访问请求的许可检查
506：拒绝存储器访问请求，当：
-存储器访问请求是在预定执行状态下发出的写入请求；与
-S2访问许可信息指定部分只读许可；与
-写入请求是除写入请求类型的受限子集之外的写入请求类型

图10

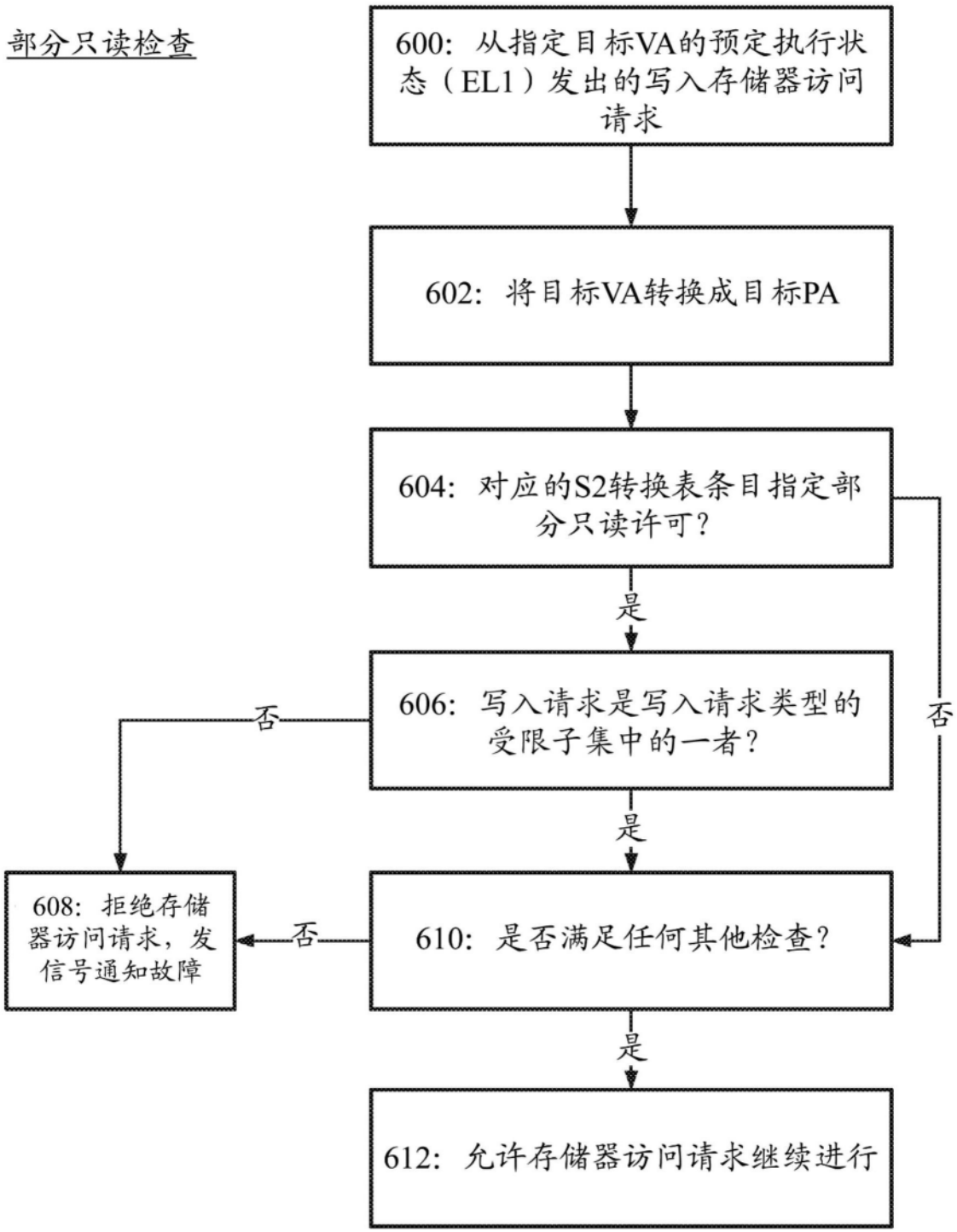

部分只读检查
600：从指定目标VA的预定执行状态（EL1）发出的写入存储器访问请求
602：将目标VA转换成目标PA
604：对应的S2转换表条目指定部分只读许可？
是
否
606：写入请求是写入请求类型的受限子集中的一者？
是
否
608：拒绝存储器访问请求，发信号通知故障
否
610：是否满足任何其他检查？
是
612：允许存储器访问请求继续进行

图11

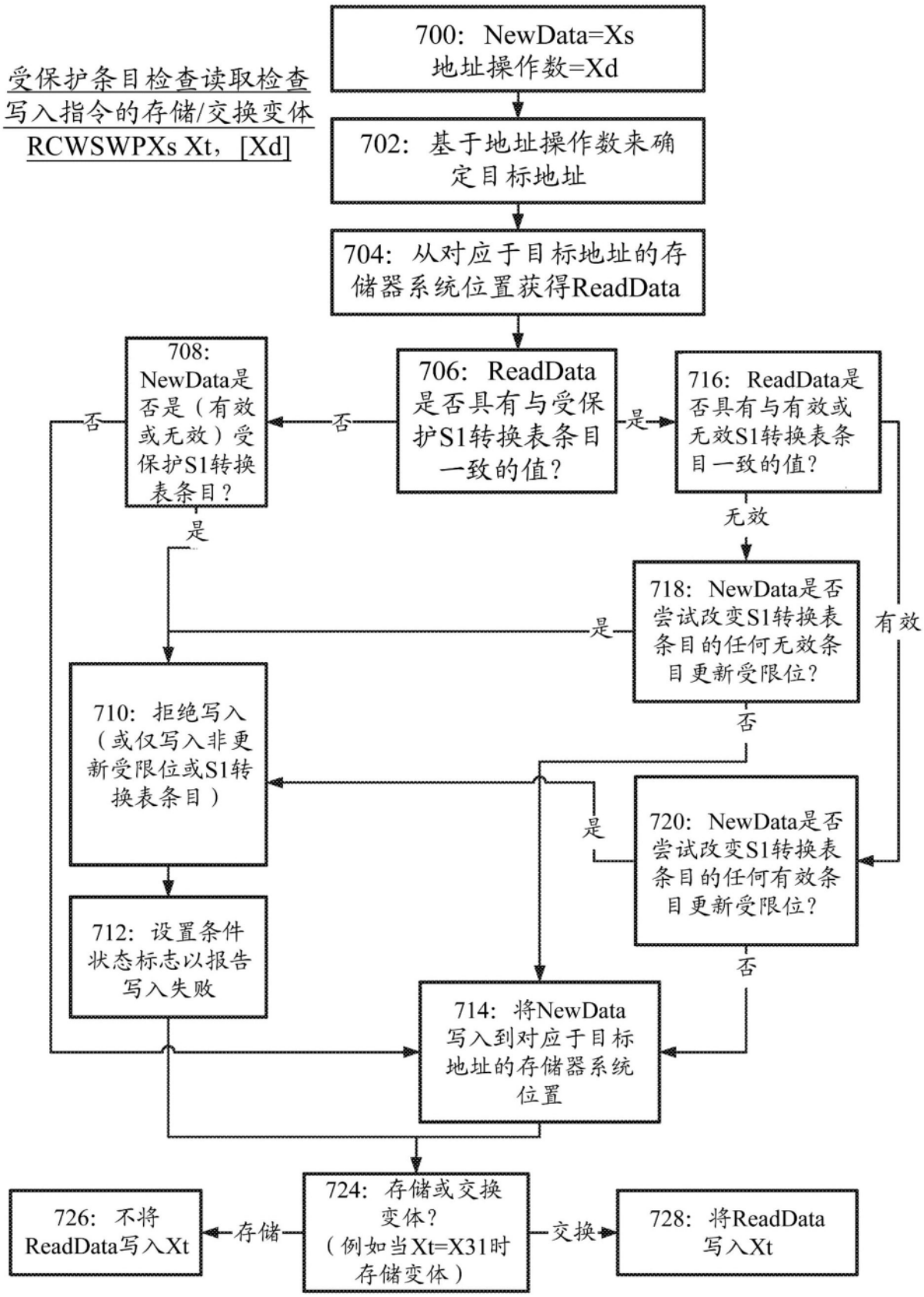

受保护条目检查读取检查写入指令的存储/交换变体
RCWSWPXs Xt，[Xd]
700：NewData=Xs
地址操作数=Xd
702：基于地址操作数来确定目标地址
704：从对应于目标地址的存储器系统位置获得ReadData
706：ReadData是否具有与受保护S1转换表条目一致的值？
否
是
708：NewData是否是（有效或无效）受保护S1转换表条目？
否
是
716：ReadData是否具有与有效或无效S1转换表条目一致的值？
无效
有效
718：NewData是否尝试改变S1转换表条目的任何无效条目更新受限位？
是
否
710：拒绝写入（或仅写入非更新受限位或S1转换表条目）
712：设置条件状态标志以报告写入失败
720：NewData是否尝试改变S1转换表条目的任何有效条目更新受限位？
是
否
714：将NewData写入到对应于目标地址的存储器系统位置
724：存储或交换变体？（例如当Xt=X31时存储变体）
存储
交换
726：不将ReadData写入Xt
728：将ReadData写入Xt

图12

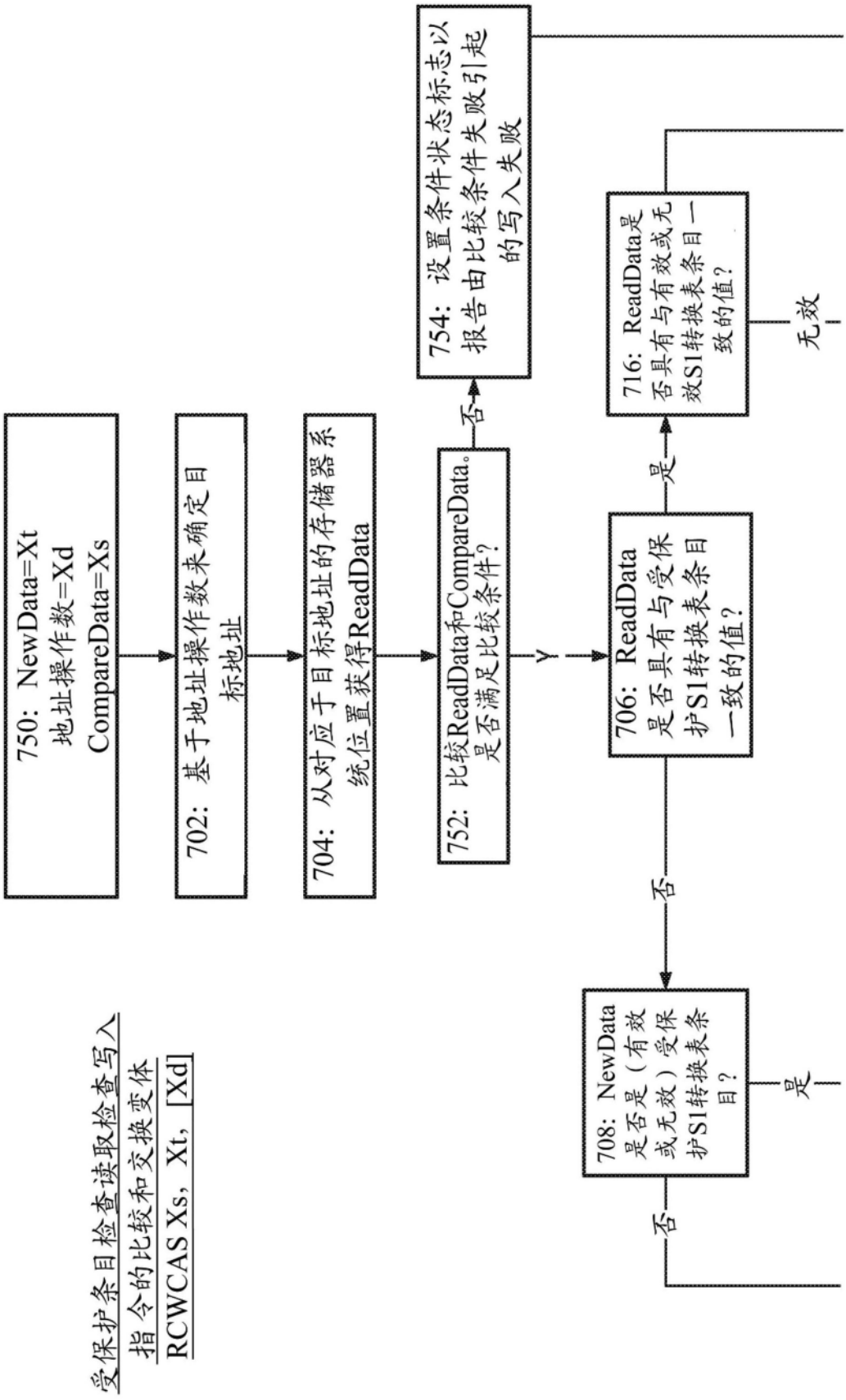

受保护条目检查读取检查写入
指令的比较和交换变体
RCWCAS Xs，Xt，[Xd]
750：NewData=Xt
地址操作数=Xd
CompareData=Xs
702：基于地址操作数来确定目标地址
704：从对应于目标地址的存储器系统位置获得ReadData
752：比较ReadData和CompareData。是否满足比较条件？
否
754：设置条件状态标志以报告由比较条件失败引起的写入失败
Y
706：ReadData是否具有与受保护S1转换表条目一致的值？
是
716：ReadData是否具有与有效或无效S1转换表条目一致的值？
无效
否
708：NewData是否是（有效或无效）受保护S1转换表条目？
是

图13

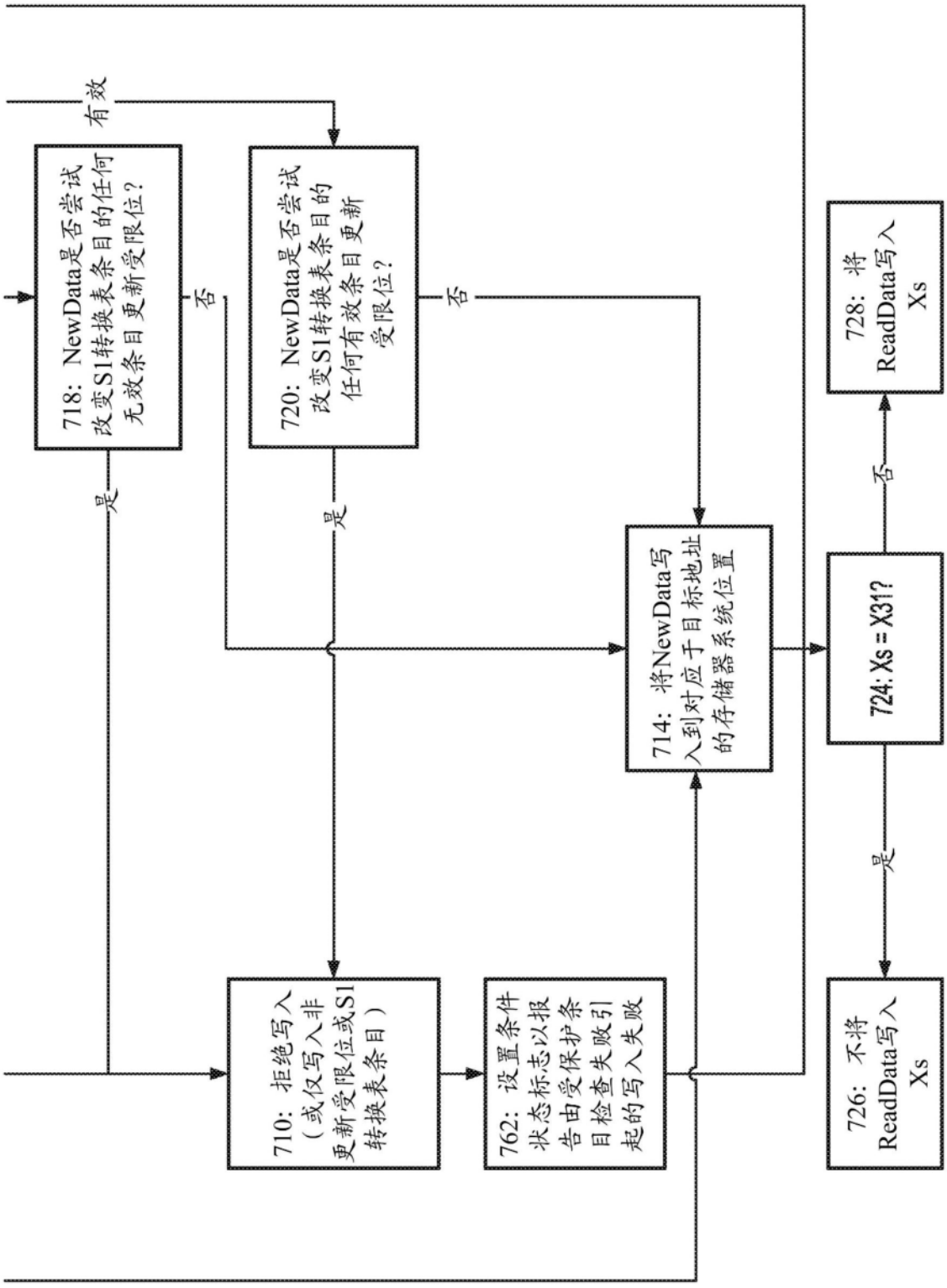

有效
718: NewData是否尝试改变S1转换表条目的任何无效条目更新受限位?
否
720: NewData是否尝试改变S1转换表条目的任何有效条目更新受限位?
否
是
是
714: 将NewData写入到对应于目标地址的存储器系统位置
724: Xs = X31?
否
是
728: 将ReadData写入Xs
710: 拒绝写入(或仅写入非更新受限位或S1转换表条目)
762: 设置条件状态标志以报告由受保护条目检查失败引起的写入失败
726: 不将ReadData写入Xs

图13(续)

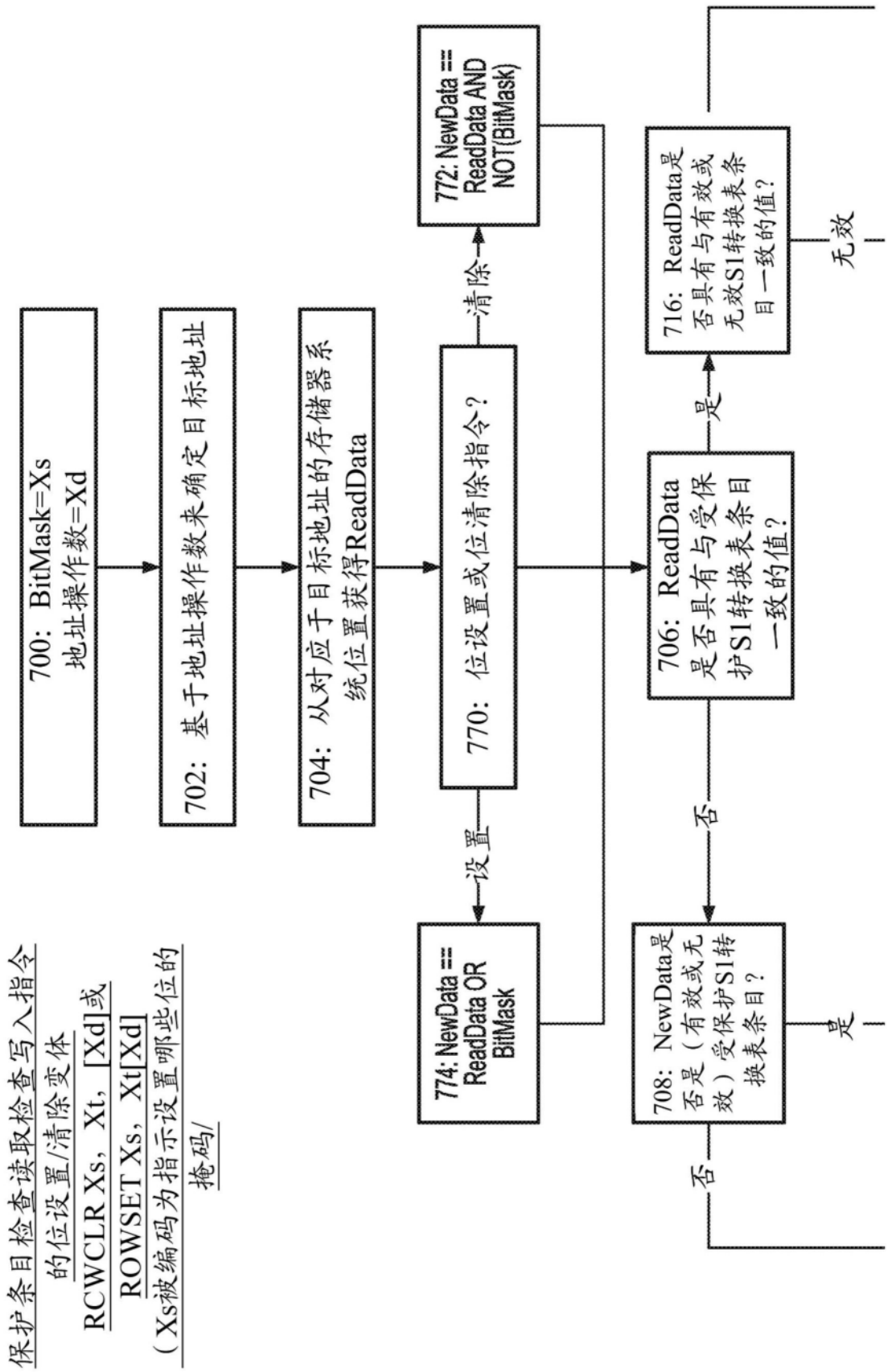

保护条目检查读取检查写入指令
的位设置/清除变体
RCWCLR Xs，Xt，[Xd]或
ROWSET Xs，Xt[Xd]
（Xs被编码为指示设置哪些位的
掩码/
700：BitMask=Xs
地址操作数=Xd
702：基于地址操作数来确定目标地址
704：从对应于目标地址的存储器系
统位置获得ReadData
770：位设置或位清除指令？
设置
清除
774: NewData ==
ReadData OR
BitMask
772: NewData ==
ReadData AND
NOT(BitMask)
706：ReadData
是否具有与受保
护S1转换表条目
一致的值？
是
否
716：ReadData是
否具有与有效或
无效S1转换表条
目一致的值？
无效
708：NewData是
否是（有效或无
效）受保护S1转
换表条目？
否
是

图14

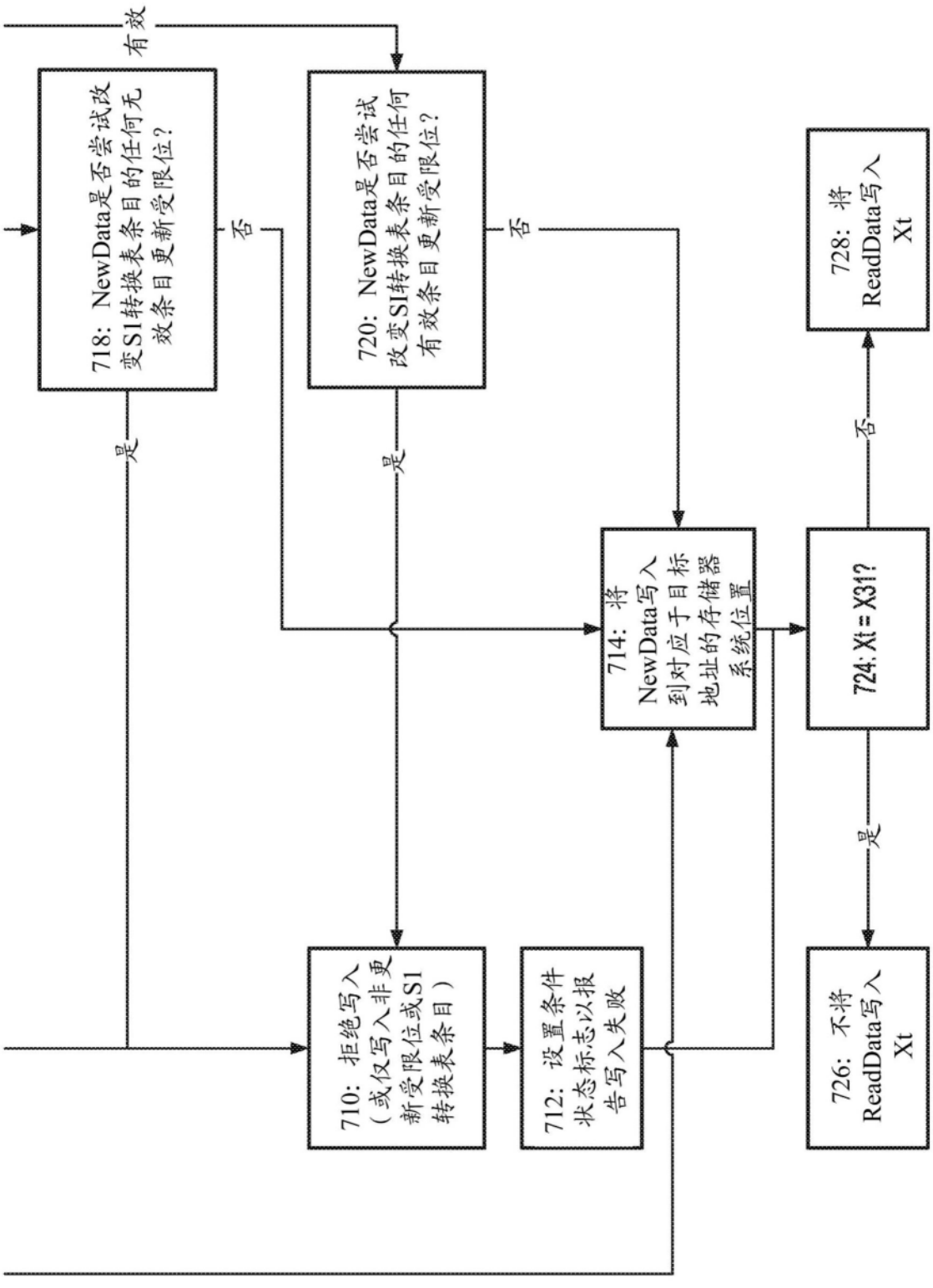

有效
718: NewData是否尝试改变S1转换表条目的任何无效条目更新受限位?
否
720: NewData是否尝试改变SI转换表条目的任何有效条目更新受限位?
否
是
是
714: 将NewData写入到对应于目标地址的存储器系统位置
724: Xt = X31?
否
728: 将ReadData写入Xt
是
710: 拒绝写入(或仅写入非更新受限位或S1转换表条目)
712: 设置条件状态标志以报告写入失败
726: 不将ReadData写入Xt

图14(续)

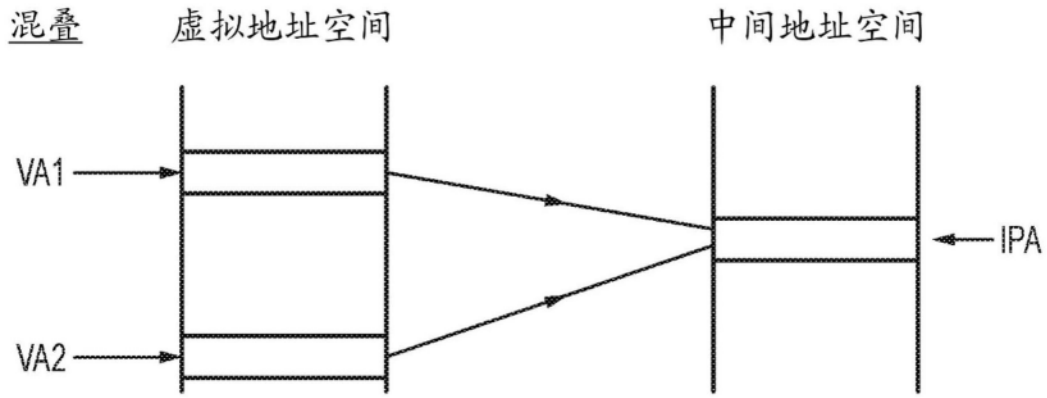


图15

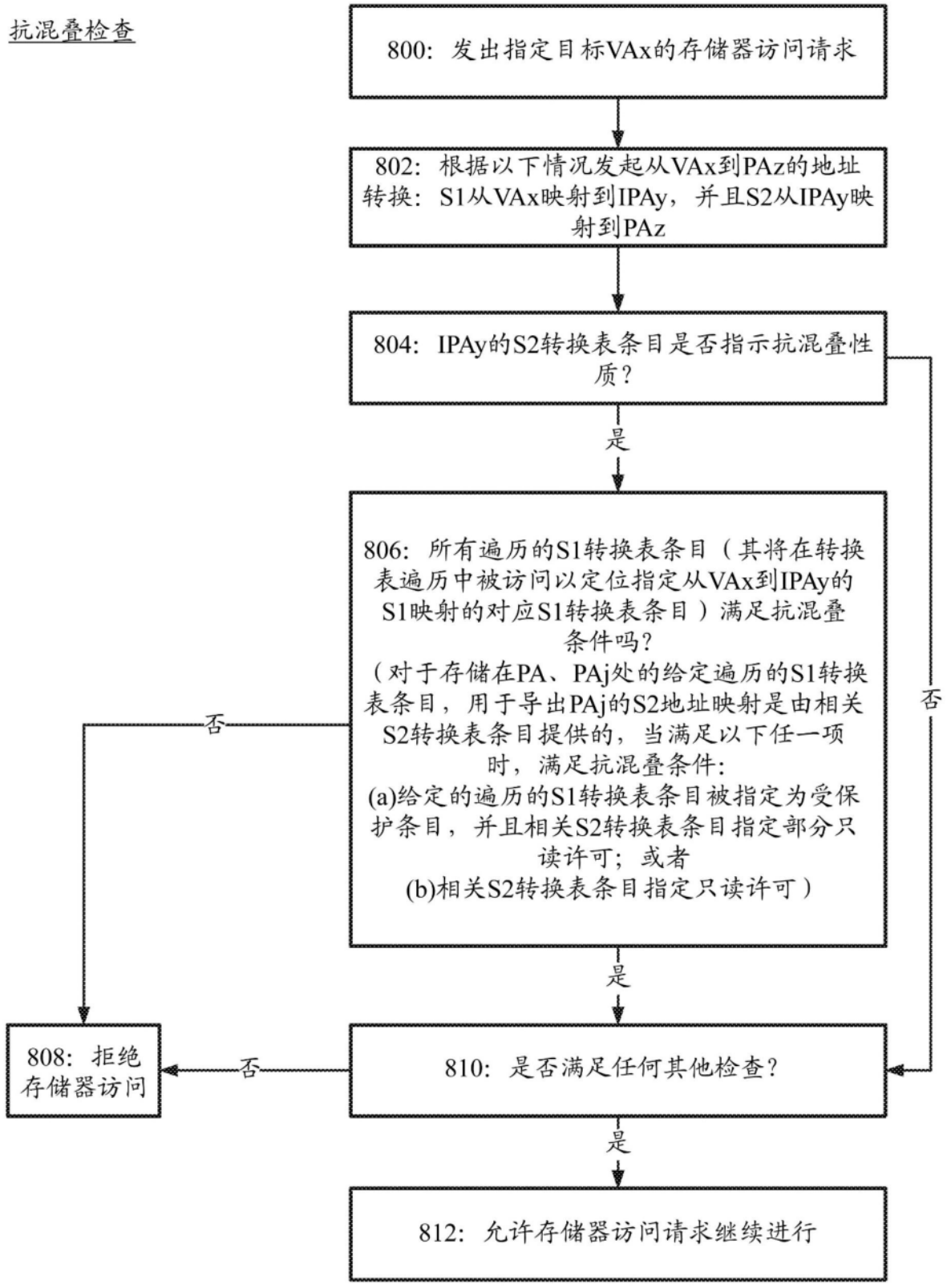

抗混叠检查
800: 发出指定目标VAx的存储器访问请求
802: 根据以下情况发起从VAx到PAz的地址转换: S1从VAx映射到IPAy，并且S2从IPAy映射到PAz
804: IPAy的S2转换表条目是否指示抗混叠性质?
是
否
806: 所有遍历的S1转换表条目（其将在转换表遍历中被访问以定位指定从VAx到IPAy的S1映射的对应S1转换表条目）满足抗混叠条件吗?
（对于存储在PA、PAj处的给定遍历的S1转换表条目，用于导出PAj的S2地址映射是由相关S2转换表条目提供的，当满足以下任一项时，满足抗混叠条件:
(a)给定的遍历的S1转换表条目被指定为受保护条目，并且相关S2转换表条目指定部分只读许可；或者
(b)相关S2转换表条目指定只读许可）
否
是
808: 拒绝存储器访问
否
810: 是否满足任何其他检查?
是
812: 允许存储器访问请求继续进行

图16

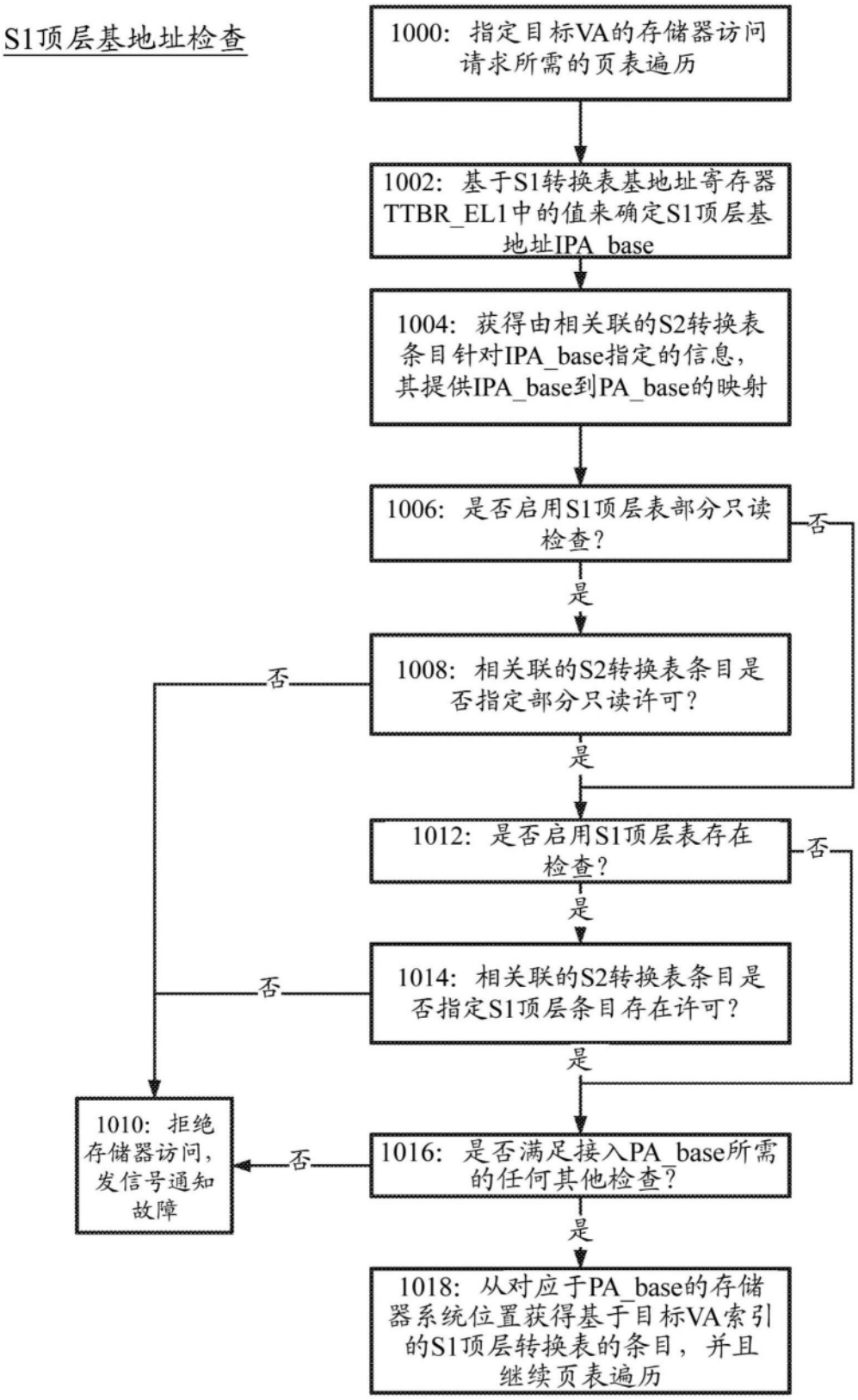

S1顶层基地址检查
1000: 指定目标VA的存储器访问请求所需的页表遍历
1002: 基于S1转换表基地址寄存器TTBR_EL1中的值来确定S1顶层基地址IPA_base
1004: 获得由相关联的S2转换表条目针对IPA_base指定的信息，其提供IPA_base到PA_base的映射
1006: 是否启用S1顶层表部分只读检查?
否
是
1008: 相关联的S2转换表条目是否指定部分只读许可?
否
是
1012: 是否启用S1顶层表存在检查?
否
是
1014: 相关联的S2转换表条目是否指定S1顶层条目存在许可?
否
是
1010: 拒绝存储器访问，发信号通知故障
否
1016: 是否满足接入PA_base所需的任何其他检查?
是
1018: 从对应于PA_base的存储器系统位置获得基于目标VA索引的S1顶层转换表的条目，并且继续页表遍历

图17

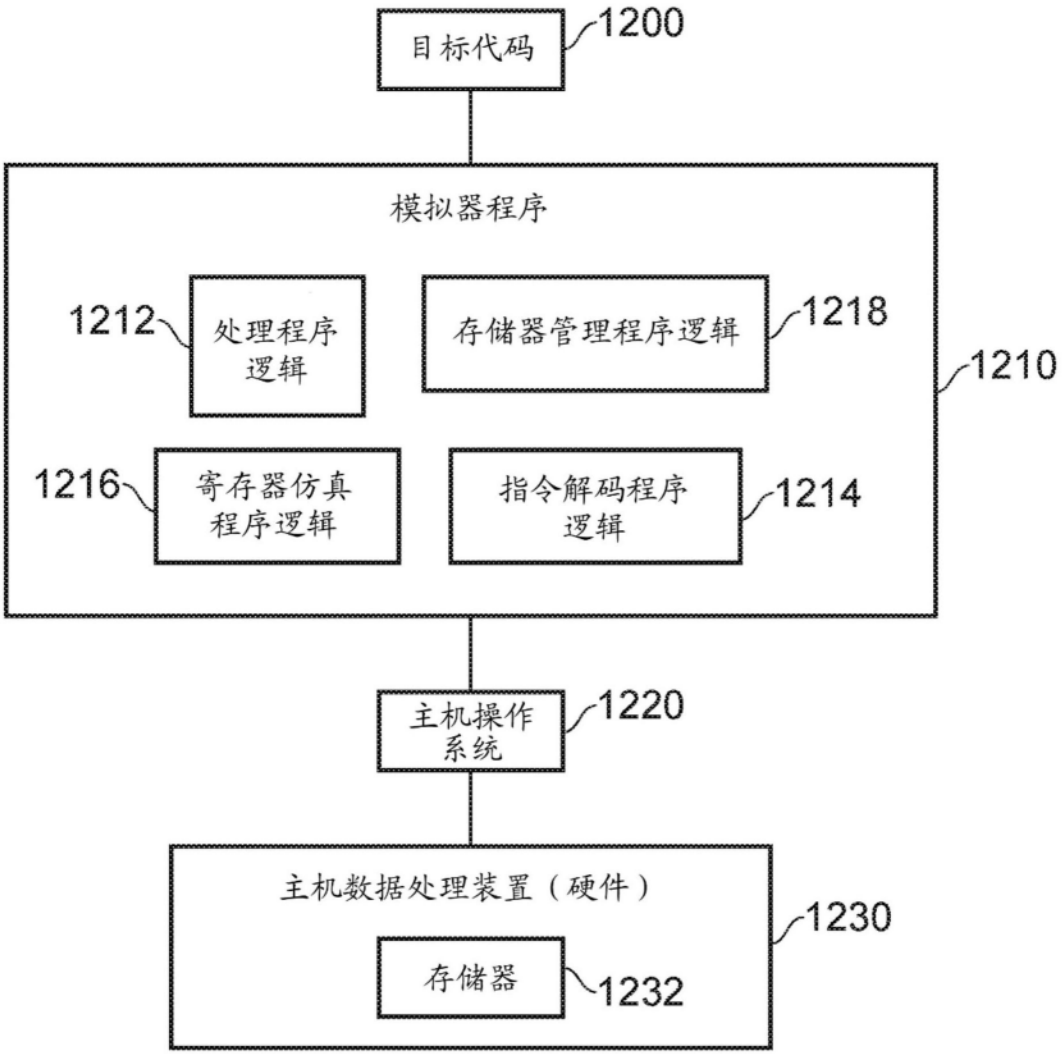

目标代码
1200
模拟器程序
1212
处理程序逻辑
存储器管理程序逻辑
1218
1210
1216
寄存器仿真程序逻辑
指令解码程序逻辑
1214
主机操作系统
1220
主机数据处理装置（硬件）
1230
存储器
1232

图18