

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/08 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200810178020.2

[43] 公开日 2009 年 6 月 10 日

[11] 公开号 CN 101452423A

[22] 申请日 2008.12.8

[21] 申请号 200810178020.2

[30] 优先权

[32] 2007.12.6 [33] US [31] 12/000005

[71] 申请人 ARM 有限公司

地址 英国剑桥郡

[72] 发明人 N·C·帕弗 S·D·比尔斯

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 张雪梅 魏军

权利要求书 4 页 说明书 11 页 附图 5 页

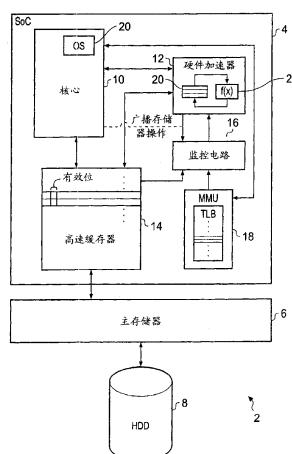
[54] 发明名称

控制硬件加速器内数据值的清除

[57] 摘要

本发明涉及控制硬件加速器内数据值的清除。

数据处理装置 2 包括耦合到硬件加速器 12 的可编程通用处理器 10。存储器系统 14、6、8 由处理器 10 和硬件加速器 12 共享。存储器系统监控电路 16 响应于由处理器 10 在存储器系统 14、6、8 上进行的一个或多个预定操作而生成到硬件加速器 12 的触发，该触发用于令硬件加速器 12 中断其操作并清除作为临时变量保持在硬件加速器的寄存器 20 内的任何数据值回到存储器系统 14、6、8。



1. 一种用于处理数据的设备，包括：

可编程通用处理器，其在程序指令控制下工作以进行数据处理操作；

耦合到所述处理器的存储器系统，所述存储器系统用于存储要由所述处理器处理的数据值；

耦合到所述处理器和所述存储器系统的硬件加速器，所述硬件加速器具有存储相应数据值的一个或多个寄存器，所述相应数据值是要由所述硬件加速器处理的临时变量，所述一个或多个寄存器内的所述数据值从所述存储器系统中读取并缓存在所述一个或多个寄存器内；和

耦合到所述硬件加速器的系统监控电路，所述存储器系统监控电路响应于在所述设备内正进行的一个或多个预定操作而生成触发信号；其中

所述硬件加速器响应于所述触发信号而中断由所述硬件加速器正进行的处理并进行清除操作，由此不同于所述存储器系统内的对应数据值的所述一个或多个寄存器内的任何数据值被回写到所述存储器系统。

2. 根据权利要求 1 所述的设备，其中所述系统监控电路包括耦合到所述存储器的存储器系统监控电路，所述存储器系统监控电路响应于所述处理器对所述存储器系统进行的一个或多个预定存储器操作而生成触发信号。

3. 根据权利要求 2 所述的设备，其中所述存储器系统包括旁路转换缓冲器且所述一个或多个预定存储器操作包括对应于所述硬件加速器正使用的数据值的在所述旁路转换缓冲器内的入口的无效。

4. 根据权利要求 2 所述的设备，其中所述存储器系统包括响应于页表数据的存储器管理单元，且所述一个或多个预定存储器操作包括对应于所述硬件加速器正使用的数据值的所述页表数据内的入口的修改。

5. 根据权利要求 2 所述的设备，其中所述存储器系统包括高速缓冲存储器，且所述一个或多个预定存储器操作包括在一个或多个高速缓冲线上进行的一个或多个清除操作，所述一个或多个高速缓冲线存储在所述高速缓冲存储器内且对应于经受所述硬件加速器处理的数据值。

6. 根据权利要求 2 所述的设备，其中所述存储器系统包括高速缓冲存储器，且所述一个或多个预定存储器操作包括在一个或多个高速缓

冲线上进行的一个或多个清除和无效操作，所述一个或多个高速缓冲线存储在所述高速缓冲存储器内且对应于经受所述硬件加速器处理的数据值。

7. 根据权利要求 2 所述的设备，其中所述处理器生成广播存储器管理命令且所述存储器系统监控电路通过接收一个或多个对应的广播存储器管理命令来检测所述一个或多个预定存储器操作。

8. 根据权利要求 2 所述的设备，其中所述一个或多个预定存储器操作包括所述处理器访问由所述硬件加速器正使用的所述存储器系统内的存储器地址空间区域内的数据值。

9. 根据权利要求 2 所述的设备，其中所述一个或多个预定存储器操作包括对在由所述硬件加速器使用的所述存储器系统内的存储器地址空间区域内的数据值的高速缓存窥探操作。

10. 根据权利要求 2 所述的设备，其中所述处理器在操作系统程序的控制下工作且所述操作系统程序独立于所述硬件加速器而管理所述存储器系统。

11. 根据权利要求 1 所述的设备，其中要由所述硬件加速器处理的所述数据值被存储在与所述处理器共享的所述存储器系统内的一个或多个区域内。

12. 根据权利要求 1 所述的设备，其中所述处理器和所述硬件加速器在共用的虚拟存储器地址空间内工作。

13. 根据权利要求 1 所述的设备，其中所述处理器和所述硬件加速器共享存储器管理单元和页表数据。

14. 根据权利要求 1 所述的设备，其中所述处理器和所述硬件加速器在不同上下文中工作。

15. 一种用于处理数据的设备，包括：

在程序指令控制下工作的用于进行数据处理操作的可编程通用处理器装置；

耦合到所述处理器装置的存储器系统装置，用于存储要由所述处理器装置处理的数据值；

耦合到所述处理器装置和所述存储器系统装置的硬件加速器装置，所述硬件加速器装置具有用于存储相应数据值的一个或多个寄存器装置，所述相应数据值是要由所述硬件加速器装置处理的临时变量，所述

一个或多个寄存器装置内的所述数据值从所述存储器系统装置中读取并缓存在所述一个或多个寄存器装置内；和

耦合到所述硬件加速器的系统监控电路，所述存储器系统监控电路响应于在所述设备内正进行的一个或多个预定操作而生成触发信号；其中

所述硬件加速器装置响应于所述触发信号而中断正由所述硬件加速器装置进行的处理并进行清除操作，由此不同于所述存储器系统装置内的对应数据值的所述一个或多个寄存器装置内的任何数据值被回写到所述存储器系统装置。

16. 一种处理数据的方法，包括以下步骤：

用在程序指令控制下工作的可编程通用处理器进行数据处理操作；

在耦合到所述处理器的存储器系统中存储要由所述处理器处理的数据值；

在硬件加速器的一个或多个寄存器内存储相应数据值，所述相应数据值是要由所述硬件加速器处理的临时变量，所述硬件加速器耦合到所述处理器和所述存储器系统，且所述一个或多个寄存器内的所述数据值从所述存储器系统中读取并缓存在所述一个或多个寄存器内；以及

使用耦合到所述硬件加速器的系统监控电路，响应于在所述设备内正进行的一个或多个预定操作而生成触发信号；和

响应于所述触发信号，中断由所述硬件加速器正进行的处理并进行清除操作，由此不同于所述存储器系统内的对应数据值的所述一个或多个寄存器内的任何数据值被回写到所述存储器系统。

17. 根据权利要求 16 所述的方法，其中所述系统监控电路包括耦合到所述存储器的存储器系统监控电路，且所述生成步骤响应于由所述处理器在所述存储器系统上正进行的一个或多个预定存储器操作而生成触发信号。

18. 根据权利要求 17 所述的方法，其中所述存储器系统包括旁路转换缓冲器且所述一个或多个预定存储器操作包括对应于所述硬件加速器正使用的数据值的在所述旁路转换缓冲器内的入口的无效。

19. 根据权利要求 17 所述的方法，其中所述存储器系统包括响应于页表数据的存储器管理单元，且所述一个或多个预定存储器操作包括对应于所述硬件加速器正使用的数据值的所述页表数据内的入口的修

改。

20. 根据权利要求 17 所述的方法，其中所述存储器系统包括高速缓冲存储器，且所述一个或多个预定存储器操作包括在一个或多个高速缓冲线上进行的一个或多个清除操作，所述一个或多个高速缓冲线存储在所述高速缓冲存储器内且对应于经受所述硬件加速器处理的数据值。

21. 根据权利要求 17 所述的方法，其中所述存储器系统包括高速缓冲存储器，且所述一个或多个预定存储器操作包括在一个或多个高速缓冲线上进行的一个或多个清除和无效操作，所述一个或多个高速缓冲线存储在所述高速缓冲存储器内且对应于经受所述硬件加速器处理的数据值。

22. 根据权利要求 17 所述的方法，还包括用所述处理器生成广播存储器管理命令且通过接收一个或多个对应的广播存储器管理命令而检测所述一个或多个预定存储器操作。

23. 根据权利要求 17 所述的方法，其中所述一个或多个预定存储器操作包括所述处理器访问由所述硬件加速器正使用的所述存储器系统内的存储器地址空间区域内的数据值。

24. 根据权利要求 17 所述的方法，其中所述一个或多个预定存储器操作包括对在所述硬件加速器正使用的所述存储器系统内的存储器地址空间区域内的数据值的高速缓存窥探操作。

25. 根据权利要求 17 所述的方法，其中所述处理器在操作系统程序的控制下工作且所述操作系统程序独立于所述硬件加速器来管理所述存储器系统。

26. 根据权利要求 16 所述的方法，其中要由所述硬件加速器处理的所述数据值被存储在与所述处理器共享的所述存储器系统内的一个或多个区域内。

27. 根据权利要求 16 所述的方法，其中所述处理器和所述硬件加速器在共用的虚拟存储器地址空间内工作。

28. 根据权利要求 16 所述的方法，其中所述处理器和所述硬件加速器共享存储器管理单元和页表数据。

29. 根据权利要求 16 所述的方法，其中所述处理器和所述硬件加速器在不同上下文中工作。

控制硬件加速器内数据值的清除

技术领域

本发明涉及数据处理系统领域。更具体地，本发明涉及具有可编程通用处理器和硬件加速器的数据处理系统。

背景技术

提供将可编程通用处理器与硬件加速器结合的系统是已知的。这样的系统可以共享存储器系统以便共享数据值。使用这样的布置，需要协调对存储在存储器系统内的数据值的操纵和管理。例如，由可编程通用处理器所进行的处理可能需要页调入 (page in) 及页调出 (page out) 同样正在被硬件加速器访问的存储器区域。如果在没有考虑硬件加速器的需求的情况下进行了这样的页面调度 (paging) 操作，那么硬件加速器所需要的数据就可能被不适当当地页调出，并且或许更严重的是：已被硬件加速器更改但尚未回到存储器系统的数据可能具有被页调出的该数据的过期的存储器系统副本，导致那些数据值持有不正确的值。

为了解决这些问题，已知的是提供一种在可编程通用计算机上执行的操作系统，其能够控制并协调存储器管理以便考虑处理器及硬件加速器二者的需求和状态。以此方式使用该操作系统需要对其进行修改，以使其能够适当地处理硬件加速器的需求以及硬件加速器产生的数据。有很多种不同形式的硬件加速器，该硬件加速器可以被设置成针对系统的不同潜在用途的这些不同形式。例如，可以在一个系统中提供针对加密的硬件加速器，可以在另一系统中提供形式明显不同且针对另一用途（诸如视频处理）的硬件加速器。具有每个均能处理这些不同硬件加速器的若干独立的操作系统或版本或甚至具有能够处理多种不同硬件加速器的单个操作系统是个重大的实际困难。当为了一个新目的开发一种新的硬件加速器时，那么将需要对操作系统代码进行修改并使其重新生效，以便支持这种新的硬件加速器。这不但耗时而且昂贵，并且在小批量产品情况下可能是不切实际的。

发明内容

从一方面看来，本发明提供了用于处理数据的设备，该设备包括：在程序指令控制下工作以进行数据处理操作的可编程通用处理器；耦合到所述处理器的存储器（memory）系统，所述存储器系统用于存储要由所述处理器处理的数据值；

耦合到所述处理器和所述存储器系统的硬件加速器，所述硬件加速器具有存储相应数据值的一个或多个寄存器，所述相应数据值是要由所述硬件加速器处理的临时变量，所述一个或多个寄存器内的所述数据值是从所述存储器系统读取并缓存（cache）在所述一个或多个寄存器内；和

耦合到所述硬件加速器的系统监控电路，所述存储器系统监控电路响应于在所述设备内进行的一个或多个预定操作而产生触发信号；其中

所述硬件加速器响应于所述触发信号以中断（halt）所述硬件加速器正进行的处理并进行清除操作，由此不同于所述存储器系统内的对应数据值的所述一个或多个寄存器内的任何数据值被回写到所述存储器系统。

本技术认识到起因于可编程通用处理器所执行的处理、并导致需要中断硬件加速器的处理且清除硬件加速器所持有的数据值的情形受到约束且可以被与硬件加速器相关联的系统监控电路可靠地识别。如果在系统内探测到一个或多个（指示此需求的）预定操作，硬件加速器通过这种方式本身可以负责确保其中断操作并清除其正存储回存储器系统的任何数据值。因而，例如，可编程通用处理器的操作系统不再需要负责中断硬件加速器所进行的处理和从硬件加速器清除数据值，从而避免了修改操作系统以考虑可能存在或不存在的不同硬件加速器的需要。相反，本技术认识到发生了特有的操作（由通用处理器驱动），该操作指示需要中断硬件加速器所进行的处理和清除存储在硬件加速器内的数据值。此外，这些预定操作被足够充分地限定为其可以用与硬件加速器相关联的专用硬件有效地检测到。

当意识到预定操作可以采用诸如由可编程通用计算机所进行的上下文（context）切换的多种不同形式时，本技术非常适合于这样的实施例：其中系统监控电路包括存储器系统监控电路并且响应于由处理器正在存储器系统上进行的一个或多个预定存储器操作生成触发信号。

该一个或多个正进行的预定存储器操作本身可以依据系统的特定

配置而采取多种不同形式。示例包括：在包括旁路转换缓冲器(translation lookaside buffer)的系统内的入口(entry)的无效，其中无效入口对应于硬件加速器正使用的数据值；在包括存储器管理单元的系统中与硬件加速器正使用的数据值所对应的页表数据入口的修改；在存储对于经受硬件加速器处理的数据值的数据的高速缓冲存储器的一个或多个高速缓存线(cache line)上进行的无效和清除操作；在存储对于经受硬件加速器处理的数据值的数据的高速缓冲存储器的一个或多个高速缓存线上进行的清除操作；在存储对于经受硬件加速器处理的数据值的数据的高速缓冲存储器的一个或多个高速缓存线上进行的高速缓存窥探操作(snoop operation)；以及另外的示例。

在某些示例系统中，作为其正常操作的一部分，处理器可生成广播存储器管理命令，且这些可以直接被存储器系统监控电路用来检测该一个或多个预定存储器操作，所述预定存储器操作指示需要停止由硬件加速器进行的处理并清除由硬件加速器存储回存储器系统的数据值。

指示需要触发由硬件加速器进行的上述类型的恢复动作的一个或多个预定存储器操作的另一示例是处理器访问硬件加速器正使用的存储器地址空间区域内的数据值。期望处理器同时访问由硬件加速器正对其进行处理的数据值的情况很少是合理的。

尽管处理器在进行其自己的存储器管理时可以许多不同方式工作，最常见的是其在操作系统的控制下工作，其中该操作系统管理存储器系统，且该操作系统进行的这种管理与硬件加速器的存在和状态无关。

尽管硬件加速器配备有特殊分区的存储器区域是可能的，但是当将硬件加速器处理的数据值存储在与处理器共享的（尽管不是同时使用的）存储器系统的一个或多个区域内时，可以更容易地实现至少用于输入和输出目的的数据共享。

处理器和硬件加速器可以方便地在共用的虚拟存储器地址空间内工作。该虚拟存储器地址空间可以由处理器上执行的操作系统来管理。处理器和硬件加速器可以共享存储器管理单元和页表数据或，在处理器和硬件加速器在不同上下文中工作的其它实施例中，给处理器和硬件加速器的每一个提供其自己的存储器管理单元和页表数据（至少在逻辑上）可能是适当的。

从又一方面看来，本发明提供了用于处理数据的设备，该设备包括：

在程序指令控制下工作的用于进行数据处理操作的可编程通用处理器装置；

耦合到所述处理器装置的存储器系统装置，用于存储要由所述处理器装置处理的数据值；

耦合到所述处理器装置和所述存储器系统装置的硬件加速器装置，所述硬件加速器装置具有用于存储相应数据值的一个或多个寄存器装置，所述相应数据值是要由所述硬件加速器装置处理的临时变量，所述一个或多个寄存器装置内的所述数据值是从所述存储器系统装置读取并缓存在所述一个或多个寄存器装置内； 和

耦合到所述硬件加速器的系统监控电路，所述存储器系统监控电路响应于在所述设备内正进行的一个或多个预定操作而生成触发信号； 其中

所述硬件加速器装置响应于所述触发信号以中断由所述硬件加速器装置正进行的处理并进行清除操作，由此不同于所述存储器系统装置内的对应数据值的所述一个或多个寄存器装置内的任何数据值被回写到所述存储器系统装置。

从又一方面看来，本发明提供了一种处理数据的方法，该方法包括以下步骤：

用在程序指令控制下工作的可编程通用处理器进行数据处理操作；

在耦合到所述处理器的存储器系统中存储将由所述处理器处理的数据值；

在硬件加速器的一个或多个寄存器内存储相应数据值，所述相应数据值是将由所述硬件加速器处理的临时变量，所述硬件加速器耦合到所述处理器和所述存储器系统，且所述一个或多个寄存器内的所述数据值从所述存储器系统读取并缓存在所述一个或多个寄存器内； 以及

使用耦合到所述硬件加速器的系统监控电路， 响应于在所述设备内进行的一个或多个预定操作而生成触发信号； 和

响应于所述触发信号而中断由所述硬件加速器进行的处理并进行清除操作，由此不同于所述存储器系统内的对应数据值的所述一个或多个寄存器内的任何数据值被回写到所述存储器系统。

根据结合附图阅读的说明性实施例的下列详细描述，本发明的上述及其它目的、特征和优点将变得显而易见。

附图说明

图 1 示意性地示出了包括可编程通用处理器、硬件加速器和存储器系统的数据处理系统；

图 2 示意性示出了可编程通用处理器可以与硬件加速器共享存储器系统的两种不同方式；

图 3 是示意性示出可编程通用处理器如何调用硬件加速器上的处理的流程图；

图 4 是示意性示出控制硬件加速器以便响应于从存储器监控电路接收到的触发信号的流程图；和

图 5 是示意性示出存储器监控电路如何响应于可编程通用处理器进行的确定的存储器操作以生成提供给硬件加速器的触发信号的流程图。

具体实施方式

图 1 示意性地示出了用于处理数据 2 的设备，其包括连接到主存储器 6 的集成电路片上系统 (system-on-chip) 4，主存储器 6 又连接到形式为硬盘驱动器 8 的非易失性存储器。在集成电路 4 内提供有诸如 ARM 处理器核心的可编程通用处理器 10，硬件加速器 12 和高速缓冲存储器 14。同样在集成电路 4 内存在有存储器系统监控电路 16 和存储器管理单元 18。

除了硬件加速器 14 和存储器系统监控电路 16 的动作以外，在图 1 中示出的用于处理数据 2 的设备的正常操作对于本领域技术人员是熟悉的。特别地，高速缓冲存储器 14、主存储器 6 和硬盘驱动器 8 一起提供分级存储器系统。存储器管理单元 18 合并了存储页表入口的旁路转换缓冲器，所述页表入口定义了虚拟到物理地址映射。在可编程通用处理器 10 上执行的操作系统 20 控制存储器系统 14、6、8 以便依据由可编程通用处理器 10 执行的一个（或多个）应用程序的当前需求而进行存储器操作，诸如在主存储器 6 与硬盘驱动器 8 之间的存储器区域的页调入和页调出。操作系统 20 可通过使用存储器管理单元 18 及其存储页表入口数据的旁路转换缓冲器而支持虚拟存储器。主页表数据可以存储在主存储器 6 内。

耦合到可编程通用处理器 10 和存储器系统 14、6、8 的硬件加速器

用于进行由可编程通用处理器 10 指派给它的处理操作。因而，可以由硬件加速器 12 在可编程通用处理器 10 所使用的相同存储器系统 14、6、8 内存储的数据上执行处理功能，诸如计算密集的加密或解密处理，媒体处理或其它这种处理活动。硬件加速器 12 合并了寄存器 20，寄存器 20 在任何给定时间点存储由硬件加速器 12 正处理或正使用的临时变量。硬件加速器 12 内的处理逻辑 22 在该临时变量上进行所需的操纵/处理。在硬件加速器 12 的操作期间从存储器系统 14、6、8 读取临时变量并将其有效地缓存在寄存器 20 内。临时变量的例子可以是要操纵的输入数据值、代表所产生的结果且需要回写到存储器系统 14、16、8 的输出数据值、随着硬件加速器 12 中处理的进行而被更新的用于输入数据和输出数据的指针、及其它形式的临时变量。保持在硬件加速器 12 内的临时变量的缓存性质的特性是，如果硬件加速器 12 停止其操作，则重要的是已被硬件加速器 12 改变但尚未回写到存储器系统 14、6、8 的任何这些临时变量应被写回，使得从硬件加速器中清除该数据值并维持数据完整性/一致性。

存储器系统监控电路 16 响应于 MMU 18 和高速缓存 14 内的信号而检测存储器系统操作，所述存储器系统操作指示可编程通用处理器 10 进行处理操作且结果是硬件加速器 12 不再合适或不再可能继续其当前操作。这种预定存储器系统操作的例子包括：存储器管理单元 18 的旁路转换缓冲器内入口的无效、页表内入口的修改、和在高速缓冲存储器 14 内对存储硬件加速器 12 正使用的数据值的高速缓冲线进行的清除和无效操作。上述预定存储器系统操作都指示在操作系统 20 的控制下进行的准备从存储器系统 14、6 的低位部分页调出数据以便仅将其存储在硬盘驱动器 8 上的操作。为了确保合适的存储器系统操作和一致性，仔 细设计和约束操作系统，从而使得它们在页调出数据之前进行一连串精确受控的无效和清除操作。这些精确限定的预定存储器系统操作由存储器系统监控电路 16 检测并导致生成提供给硬件加速器 12 的触发信号，该触发信号用于触发硬件加速器 12 中断处理并进行清除操作，由此清除（即，写出（write out）到存储器系统 14、6、8）不同于存储器系统 14、6、8 内的对应数据值的寄存器 20 内所保持的任何数据值。

可以使用存储器系统配置的多种不同布置。在某些实施例中，可编程通用处理器 10 和硬件加速器 12 可以在相同的上下文中工作，其中硬

件加速器 12 协助在当前在可编程通用处理器 10 上活动 (active) 的上下文中执行计算密集任务。在其它实施例中，可编程通用处理器 10 和硬件加速器 12 也有可能在不同上下文中用它们自己的页表和虚拟到物理地址映射进行工作。

同样在图 1 中示出的是可编程通用处理器 10 生成指示正进行的存储器操作的广播信号的可能性。用于这种可编程通用处理器 10 的某些处理器架构生成广播存储器操作信号以便促进在多重处理环境 (multiprocessing environment) 中协调存储器控制。如果可用的话，除了前述的对高速缓存 14 和存储器管理单元 18 进行“窥探”或替代这种窥探操作，存储器系统监控电路 16 可响应于这种广播存储器操作信号。

将理解，如果硬件加速器 12 将清除其数据值到存储器系统 14、6、8，那么应当在操作系统 20 产生的任何存储器系统变化生效之前完成此任务。这可以通过使存储器系统监控电路 16 检测正进行的适当的预定存储器系统操作并拖延 (hold off) (停止) 这些存储器系统操作，同时硬件加速器 12 进行其清除操作而实现。在操作系统 12 的级别上，这种活动看起来与慢速存储器存取是一样的，且与清除硬件加速器 12 相关联的额外延迟不会导致任何特定问题。

举例来说，可以考虑在 ARM 架构下与禁用存储器页面相关联的预定存储器系统操作。操作系统可以决定禁用页面，作为其最近使用的检测例程（以找出用于交换的候选物理存储器）的一部分，或作为与后备存储（硬盘驱动器 8）交换页面的先导 (precursor)。倘若操作系统禁用了硬件加速器 12 正使用的页面，硬件加速器 12 应停止使用该页面(中断其处理)且可取地硬件加速器应清除在其寄存器 20 内具有的属于被禁用页面的任何数据值，从而使得如果交换该页面则将不会丧失数据一致性。硬件加速器 12 相应地对来自存储器系统监控电路 16 的触发信号作出响应以中断其处理，且任选地可以用信号通知可编程通用处理器 10 它实际上使用的是该页面，因为这可能导致操作系统 20 不交换该页面。这等效于 CPU 线程“触及 (touching)”被禁用页面并引起终止 (abort)。

为了禁用页面操作系统一般经历的步骤是 (以伪代码形式)：

写新页表入口

DMB; 确保已完成对存储器的写入

TLB 无效 (Invalidate); 确保从存储器重新读取所缓存的页面

DMB; 确保 TLB 无效完成

IMB; 确保没有使用旧映射的指令

在此情况下该技术认识到，通过观察“TLB 无效”命令，存储器系统监控电路 16 可以得到硬件加速器 12 需要的页面不再有效的指示。该“TLB 无效”命令可引用单一页面，一组页面，或“所有”缓存的入口。存储器系统监控电路 16 可响应于任何“TLB 无效”命令，或可选地仅响应于与硬件加速器 12 的当前工作页面相冲突的这种命令。

预定存储器系统操作的另一示例涉及到重新使用存储器中的物理页面。如果操作系统 20 希望重新使用存储器中的这种物理页面，则其将进行下列步骤：

Disable Page(); 如前部分，可能在一段时间前执行

Cache Clean and Invalidate (高速缓冲存储器清除和无效)；确保任何先前缓存的副本是无效的，及确保脏线 (dirty line) 回写到物理存储器

DMB; 高速缓存 C&I 完成

DMA/Copy to Store; 复制输出数据到后备存储

Wait For Completion(); 隐式 (implicit) DMB

DMA/Copy from Store; 复制输入数据到物理存储器(使用维护映射 (maintenance mapping))

Waite For Completion;

Write New Page(); 类似于 Disable Page() - 启用使用新的物理页面

在此情况下该技术利用如下认识：存储器系统监控电路 16 可观察到“高速缓冲存储器清除和无效”操作（特别是与先前禁用的页面结合）作为操作系统 20 可能将所讨论的存储器页面调回 (paging back) 后备存储（例如硬盘 8）的指示。操作系统 20 将在重写物理存储器之前等待高速缓存维护操作 (cache maintenance operation) 完成且相应地硬件加速器 12 可以利用这来拖延这种高速缓存维护操作，同时其将硬件加速器 12 内保持的任何数据值回写到存储器系统 14、6、8。

该系统可区分出作为高速缓存一致性系统的一部分而发生的一致动作与显式的 (explicit) 维护操作之间的差异。例如，如果处理器读取由加速器缓存的块，则其可清除此块到存储器并随后重新读取该块从而

使得其继续处理。相反地，如果处理器导致显式的页面禁用/高速缓存清除和无效，则加速器可清除所涉及的块并使其无效，然后暂停(suspend)其本身发出适当信号(或状态位)，该信号提供其暂停返回处理器10的指示。

该系统也可能窥探对包含页表的存储器的写入且相应地确定是否已修改其中一个页表入口并将其作为导致中断和清除硬件加速器12的动作的指示。该系统也可能窥探对存储器14、6、8内的数据值的访问，硬件加速器12本身需要这些数据值进行处理。又一示例是该系统可以放弃或清除和无效在显式的高速缓存/TLB维护和预取操作(prefetched operation)时所有缓存的副本—如果已禁用所需页面，则加速器12的随后取出(fetch)将中断且加速器12将暂停并用信号将该暂停通知给处理器10。

指示需要清除和转储清除(flush)加速器的预定操作的另外示例是在存储对应于经受硬件加速器处理的数据值的数据的高速缓冲存储器的一个或多个高速缓冲线上进行的清除操作、和在存储对应于经受硬件加速器处理的数据值的数据的高速缓冲存储器的一个或多个高速缓冲线上进行的高速缓存窥探操作。监控电路16可配置成响应于这些形式的操作。

图2示意性地示出了其中可以看到可编程通用处理器10和硬件加速器12共享以存储器管理单元18和主存储器6为形式的存储器系统的布置。以虚线形式示出了可选布置，其中硬件加速器12可具有其自己的独立的存储器管理单元，该存储器管理单元存储其自己的页表数据，从而使得硬件加速器12可在不同上下文中用不同于可编程通用处理器10正使用的那些映射的虚拟到物理映射进行工作。

图3是示意性地示出处理器10如何调用由硬件加速器12进行的处理的流程图。在步骤24处，处理器10开始执行程序指令。在步骤26处，处理器10执行硬件加速器调用指令且这使得处理器10发送适当信号到硬件加速器12以触发其处理活动。硬件加速器12可能已被预配置(设置)以便能在接收到简单启动命令后开始其处理。所涉及的预配置类型可以是提供到待处理数据结构的适当指针，提供要在加密/解密中使用的密钥值(key value)等等。在步骤28处，调用硬件加速器的执行。在步骤30处，确定进行的调用是否是期望处理器10在其本身继续进一

步处理之前应等待完成的调用。如果这不是需要“等待完成”的调用，则处理回到步骤 26。如果需要“等待完成”，则在处理回到步骤 26 之前，处理转入检测处理完成的步骤 32。

图 4 是示意性示出硬件加速器 12 的控制的流程图。在步骤 34 处硬件加速器 12 等待接收启动其处理的触发。当接收到这种触发时，处理前进到步骤 36，其中硬件加速器 12 从存储器系统载入其临时变量并对其进行处理，包括视情况回写结果。在步骤 38 处，确定所有待处理的值是否已被硬件加速器 12 处理。如果已处理了所有值，则控制回到步骤 34 以等待来自处理器 10 的下一触发以启动由硬件加速器 12 进行的另外的处理操作。如果在步骤 38 处确定仍然还有其它值待处理，则检查是否已从存储器系统监控电路 16 接收到触发信号，该信号指示由于处理器 10 的其它活动应中断处理并进行清除操作。如果尚未从监控电路 16 的存储器系统接收到这种触发，则处理回到步骤 36。然而，如果已经从存储器系统监控电路 16 接收到这种触发信号，则处理前进到步骤 42，在步骤 42 处中断由硬件加速器 12 进行的处理。然后步骤 44 通过将硬件加速器寄存器 20 内的任何“脏值 (dirty value)”回写到存储器系统 14、6、8 而清除了它们。处理然后回到步骤 34。

图 5 是示意性示出存储器系统监控电路 16 的动作的流程图。在步骤 46 处，该电路等待直到硬件加速器 12 为活动状态 (active)。当硬件加速器 12 处于活动状态时，处理前进到步骤 48，其中硬件加速器 12 使用的存储器区域被读取，从而在此示例中，存储器系统监控电路 16 可以响应于关于那些特定区域的操作，而不是潜在有冲突的一般存储器操作。步骤 50 然后确定是否已检测到指示硬件加速器 12 需要中断其处理并清除自身的任何预定存储器操作。如果已检测到这样的存储器操作，则步骤 52 生成适当的触发信号，该触发信号被发送到硬件加速器以触发其进行这种“中断及清除” (halt-and-clean) 操作。如果尚未检测到这样的预定存储器操作，处理从步骤 50 前进到步骤 54，在步骤 54 处检查硬件加速器是否仍处于活动状态。如果硬件加速器仍处于活动状态，则处理回到步骤 50。如果硬件加速器不再处于活动状态，则处理回到步骤 46。

上述技术与在题为“Providing Secure Services to A Non-Secure Application” 和 “Protecting the security of secure data sent from a central

processor for processing by a further processing device”、且具有代理人案号~~~~~的共同未决的美国专利申请中所描述的技术有关。这两个共同未决的申请的公开内容在此全部引入。

尽管已经参考附图详细描述了本发明的说明性实施例，应理解本发明不局限于那些精确的实施例，且本领域技术人员可以实施各种改变和修改而不脱离由所附权利要求书限定的本发明的范围和宗旨。

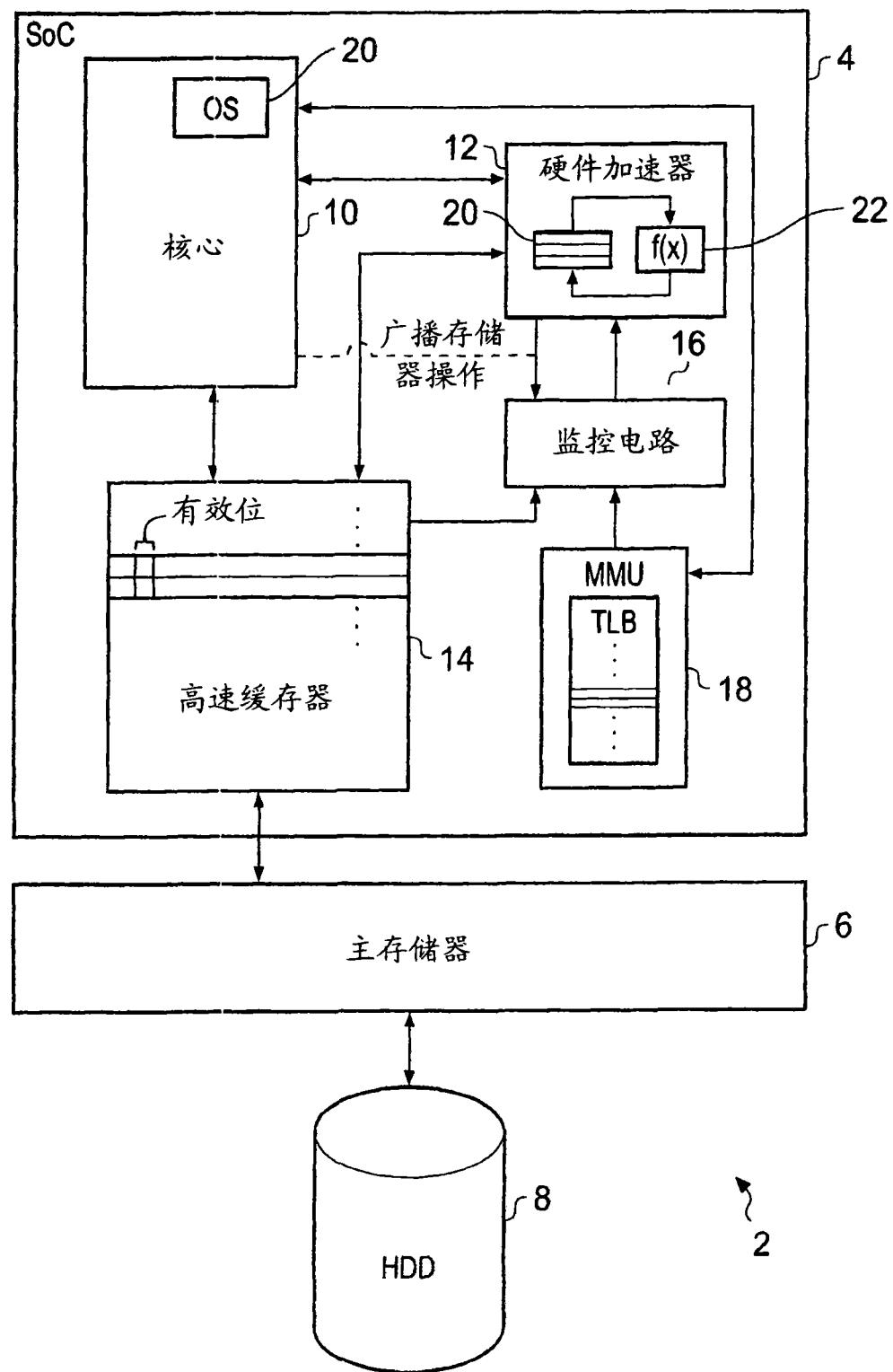


图 1

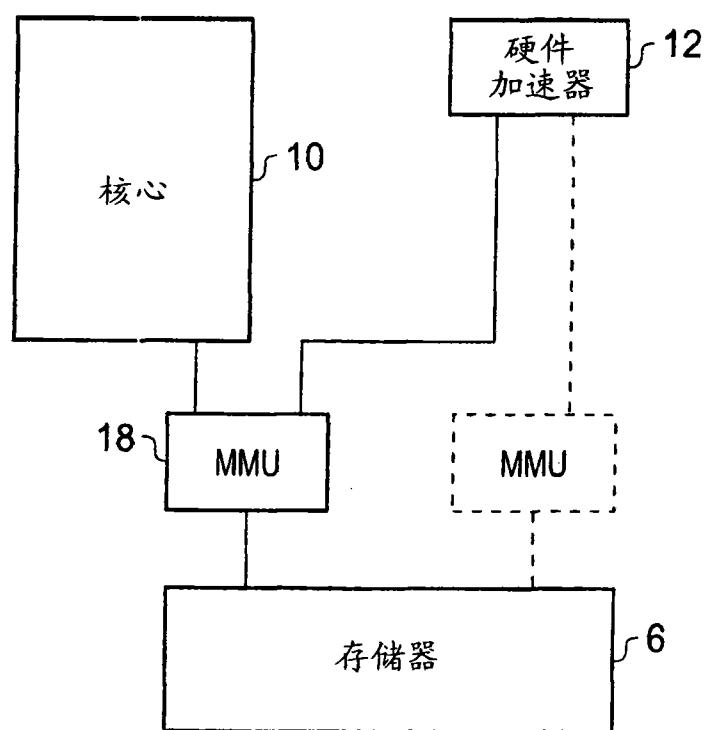


图 2

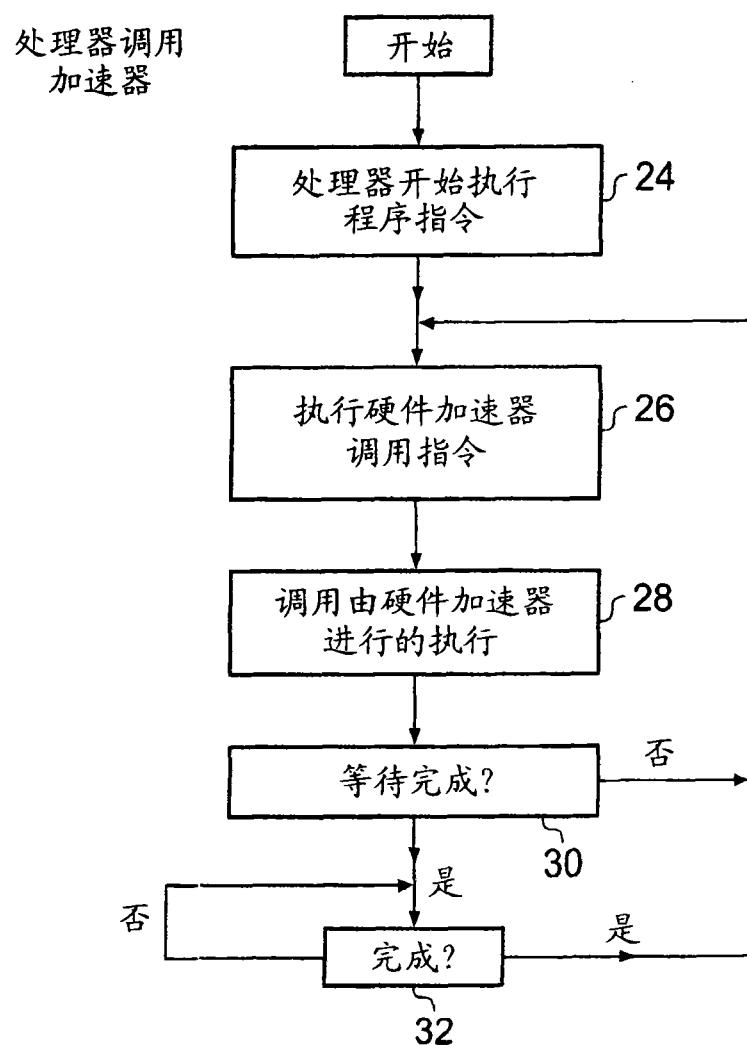


图 3

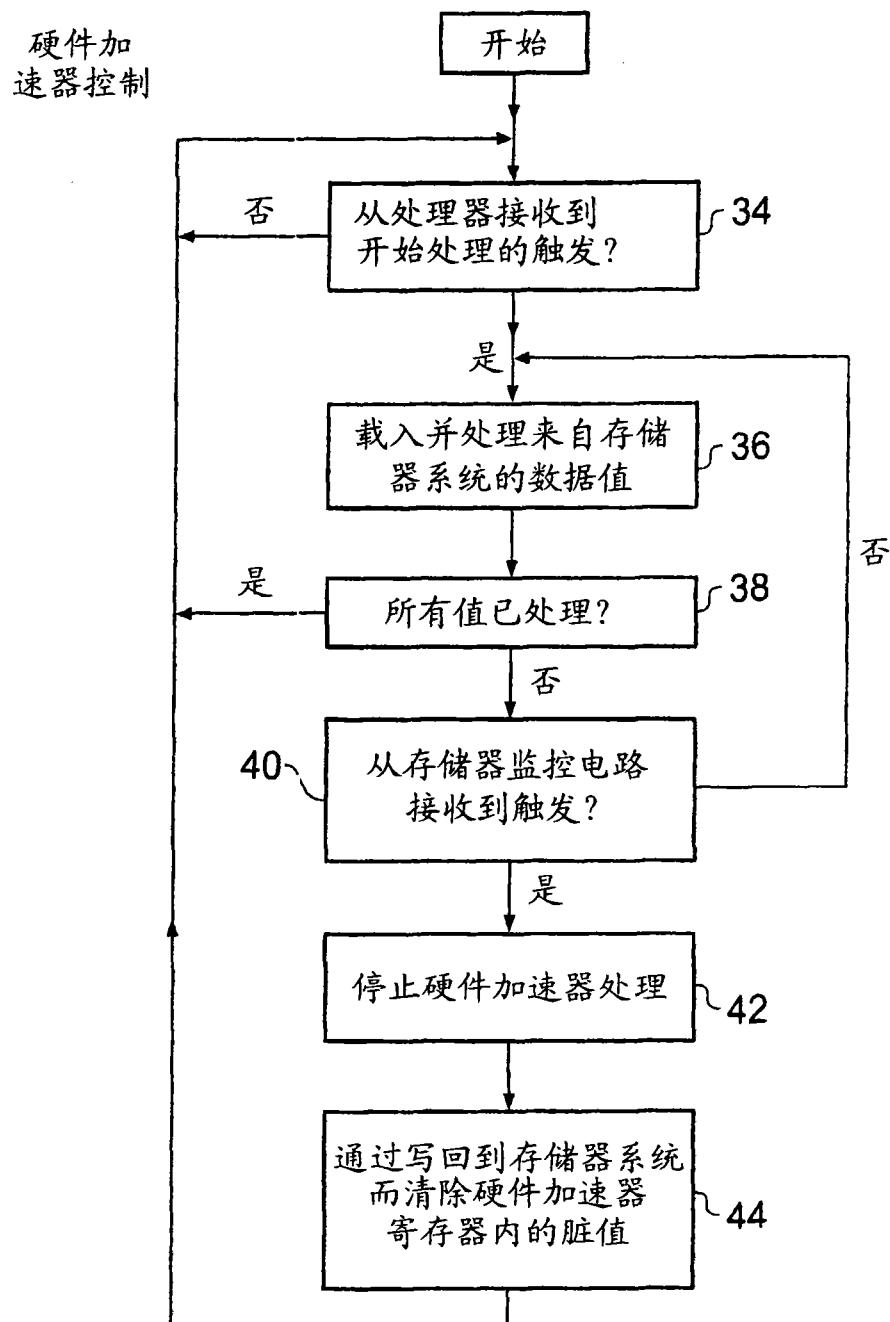


图 4

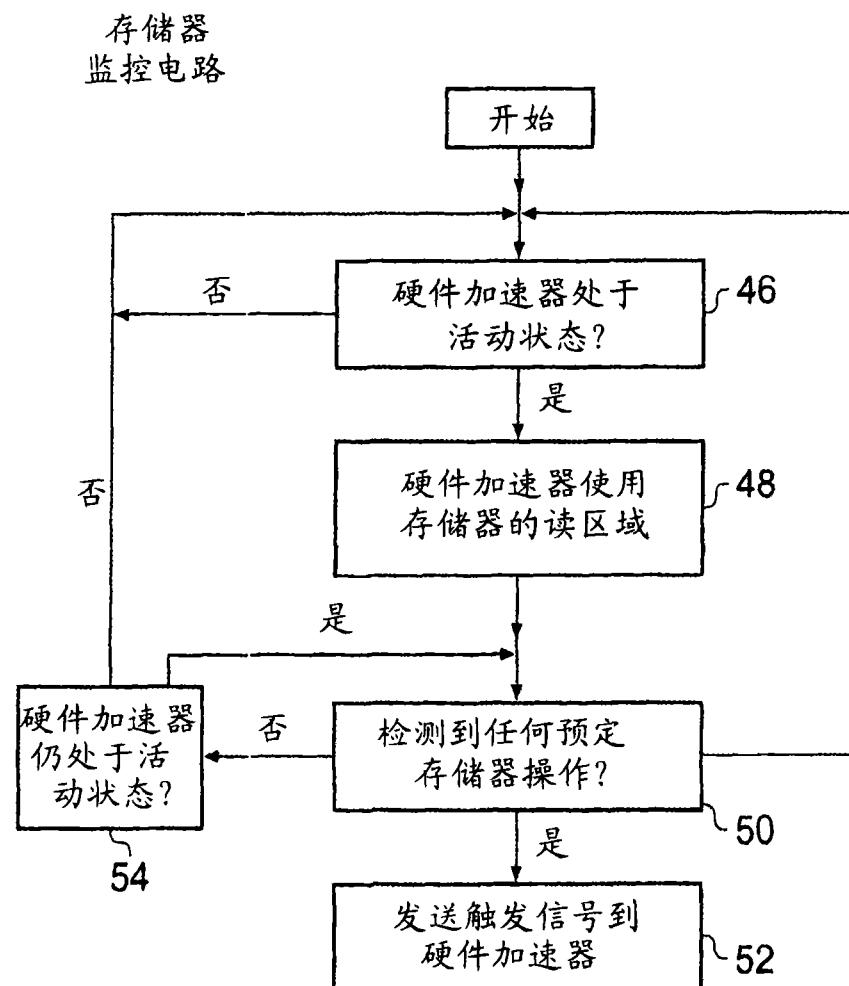


图 5