(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 104541281 B
(45)授权公告日 2018.07.17

(21)申请号 201380041796.9

(22)申请日 2013.06.13

(65)同一申请的已公布的文献号
申请公布号 CN 104541281 A

(43)申请公布日 2015.04.22

(30)优先权数据
13/571,671 2012.08.10 US

(85)PCT国际申请进入国家阶段日
2015.02.06

(86)PCT国际申请的申请数据
PCT/US2013/045681 2013.06.13

(87)PCT国际申请的公布数据
WO2014/025453 EN 2014.02.13

(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 P·J·波斯特莱三世
J·H·斯塔布斯 P·T·小米勒

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英

(51)Int.Cl.
G06F 21/79(2006.01)
G06F 21/62(2006.01)

(56)对比文件
US 2012/0131481 A1,2012.05.24,
US 2012/0159183 A1,2012.06.21,
CN 1647046 A,2005.07.27,
CN 101589398 A,2009.11.25,
US 2006/0048221 A1,2006.03.02,

审查员 张立丽

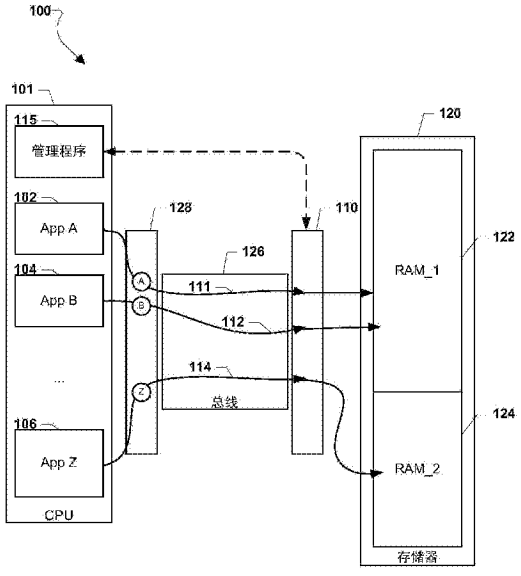
权利要求书4页 说明书12页 附图7页

(54)发明名称

用于选择性RAM加扰的方法和设备

(57)摘要

一种用于基于数据标记来选择性地对与计算设备相关联的存储器内的数据进行加扰的方法。计算设备可以定义受保护的安全域。由应用产生的数据可以被封装为具有描述应用和/或数据的标记信息的数据总线事务。可以在计算设备的总线上将数据总线事务发送给诸如内部存储器之类的存储器，其中，计算设备可以将标记信息与存储的描述安全域的信息进行比较。当基于标记信息确定数据是受保护的时，计算设备可以对数据执行加扰操作。在一方面，标记信息可以描述用于在处理器上执行各个应用的虚拟机。在另一方面，标记信息可以定义目的存储器地址或内容保护比特值。



CN 104541281 B

1.一种用于在计算设备内进行选择性存储器加扰的方法,包括:

由总线主控器将标记信息添加到在所述计算设备的总线上发送的数据中,其中所述标记信息标识所述数据的来源,以及进一步其中所述数据将被存储在存储器中;

基于所述标记信息来确定所述数据的所述来源;

基于所述数据的所述来源来确定所述数据是否包括受保护内容,其中所述存储器被分区成第一分区和第二分区;

当所述数据包括受保护内容时,作为将所述数据存储在所述第一分区中的一部分,对所述数据应用加扰例程;以及

当所述数据不包括受保护内容时,将所述数据存储在所述第二分区中,而不对所述数据应用所述加扰例程。

2.根据权利要求1所述的方法,其中,受保护内容是从以下的组中选择的:

数字版权管理(DRM)下的数据,

个人信息,

安全信息,

认证信息,

受保护的内容应用信息,和

医疗数据。

3.根据权利要求1所述的方法,其中:

基于所述标记信息来确定所述数据的所述来源包括:将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。

4.根据权利要求1所述的方法,其中,所述标记信息包括虚拟机标识(VMID)。

5.根据权利要求1所述的方法,其中,所述标记信息包括总线主控器标识。

6.根据权利要求1所述的方法,其中:

添加到所述数据的所述标记信息是目的存储器地址,以及

所述存储器将特定的存储器地址用于受保护的内容数据。

7.根据权利要求1所述的方法,其中,添加到所述数据的所述标记信息是内容保护比特。

8.根据权利要求1所述的方法,其中,所述方法是在以下各项中的至少一项上执行的:所述计算设备内的第一处理器、所述计算设备内的协处理器和所述计算设备内的对等处理器。

9.一种计算设备,包括:

存储器,其至少配置有安全域和非安全域,其中,所述安全域中的数据被加扰,其中,所述安全域包括所述存储器的第一分区,以及,所述非安全域包括所述存储器的第二分区;以及

处理器,其耦合到所述存储器,其中,所述处理器配置有处理器可执行指令以执行包括以下各项的操作:

由总线主控器将标记信息添加到在总线上发送的数据中,其中所述标记信息标识所述数据的来源,以及进一步其中所述数据将被存储在所述存储器中;以及

基于所述标记信息来确定所述数据的所述来源;

基于所述数据的所述来源来确定所述数据是否包括受保护内容；

当所述数据包括受保护内容时，作为将所述数据存储在所述安全域的所述第一分区中的一部分，对所述数据应用加扰例程；以及

当所述数据不包括受保护内容时，将所述数据存储在所述非安全域的所述第二分区中，而不对所述数据应用所述加扰例程。

10.根据权利要求9所述的计算设备，其中，受保护内容是从以下的组中选择的：

数字版权管理(DRM)下的数据，

个人信息，

安全信息，

认证信息，

受保护的内容应用信息，和

医疗数据。

11.根据权利要求9所述的计算设备，其中，所述处理器配置有处理器可执行指令以执行操作，使得：

基于所述标记信息来确定所述数据的所述来源包括：将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。

12.根据权利要求9所述的计算设备，其中，所述标记信息包括虚拟机标识(VMID)。

13.根据权利要求9所述的计算设备，其中，所述标记信息包括总线主控器标识。

14.根据权利要求9所述的计算设备，其中：

添加到所述数据的所述标记信息是目的存储地址，以及

所述存储器将特定的存储地址用于受保护的内容数据。

15.根据权利要求9所述的计算设备，其中，添加到所述数据的所述标记信息是内容保护比特。

16.根据权利要求9所述的计算设备，其中，所述处理器是以下各项中的一项：所述计算设备内的多个处理器中的第一处理器、所述计算设备内的协处理器和所述计算设备内的对等处理器。

17.一种用于在计算设备内进行选择性存储器加扰的装置，包括：

用于由总线主控器将标记信息添加到在计算设备的总线上发送的数据中的单元，其中所述标记信息标识所述数据的来源，以及进一步其中所述数据将被存储在存储器中；

用于基于所述标记信息来确定所述数据的所述来源的单元；

用于基于所述数据的所述来源来确定所述数据是否包括受保护内容的单元，其中所述存储器被分区成第一分区和第二分区；

用于当所述数据包括受保护内容时，作为将所述数据存储在所述第一分区中的一部分，对所述数据应用加扰例程的单元；以及

用于当所述数据不包括受保护内容时，将所述数据存储在所述第二分区中，而不对所述数据应用所述加扰例程的单元。

18.根据权利要求17所述的装置，其中，受保护内容是从以下的组中选择的：

数字版权管理(DRM)下的数据，

个人信息，

安全信息，

认证信息，

受保护的内容应用信息，和

医疗数据。

19.根据权利要求17所述的装置，其中：

用于基于所述标记信息来确定所述数据的所述来源的单元包括：用于将所述标记信息与存储的与经授权的安全域相关的标识符进行比较的单元。

20.根据权利要求17所述的装置，其中，所述标记信息包括虚拟机标识(VMID)。

21.根据权利要求17所述的装置，其中，所述标记信息包括总线主控器标识。

22.根据权利要求17所述的装置，其中：

添加到所述数据的所述标记信息是目的存储地址，以及

所述存储器将特定的存储地址用于受保护的内容数据。

23.根据权利要求17所述的装置，其中，添加到所述数据的所述标记信息是内容保护比特。

24.根据权利要求17所述的装置，还包括：

用于执行应用的单元，所述用于执行应用的单元包括以下各项中的至少一项：所述计算设备内的多个处理器中的第一处理器、所述计算设备内的协处理器和所述计算设备内的对等处理器。

25.一种非暂时性处理器可读存储介质，其具有存储在其上的处理器可执行指令，所述处理器可执行指令被配置为使处理器执行包括以下各项的操作：

由总线主控器将标记信息添加到在总线上发送的数据中，其中所述标记信息标识所述数据的来源，以及进一步其中所述数据将被存储在存储器中；

基于所述标记信息来确定所述数据的所述来源；

基于所述数据的所述来源来确定所述数据是否包括受保护内容，其中，所述存储器被分区成第一分区和第二分区；

当所述数据包括受保护内容时，作为将所述数据存储在所述第一分区中的一部分，对所述数据应用加扰例程；以及

当所述数据不包括受保护内容时，将所述数据存储在所述第二分区中，而不对所述数据应用所述加扰例程。

26.根据权利要求25所述的非暂时性处理器可读存储介质，其中，所存储的处理器可执行指令被配置为使处理器执行操作，使得受保护内容是从以下的组中选择的：

数字版权管理(DRM)下的数据，

个人信息，

安全信息，

认证信息，

受保护的内容应用信息，和

医疗数据。

27.根据权利要求25所述的非暂时性处理器可读存储介质，其中，所存储的处理器可执行指令被配置为使处理器执行操作，使得：

基于所述标记信息来确定所述数据的所述来源包括:将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。

28.根据权利要求25所述的非暂时性处理器可读存储介质,其中,所述标记信息包括虚拟机标识(VMID)。

29.根据权利要求25所述的非暂时性处理器可读存储介质,其中,所述标记信息包括总线主控器标识。

30.根据权利要求25所述的非暂时性处理器可读存储介质,其中,所存储的处理器可执行指令被配置为使处理器执行操作,使得:

添加到所述数据的所述标记信息是目的存储地址,以及

所述存储器将特定的存储地址用于受保护的内容数据。

31.根据权利要求25所述的非暂时性处理器可读存储介质,其中,所述标记信息包括内容保护比特。

32.根据权利要求25所述的非暂时性处理器可读存储介质,其中,所存储的处理器可执行指令被配置为由从以下各项的组中选择的处理器来执行:多个处理器中的一个处理器、协处理器和对等处理器。

用于选择性RAM加扰的方法和设备

技术领域

[0001] 本发明涉及数字版权管理内容领域，特别涉及用于选择性RAM加扰的方法和设备。

背景技术

[0002] 诸如数字版权管理(DRM)内容(例如，电影、音乐和游戏)之类的受保护数据的提供者，越来越需要额外的措施来确保他们的有价值内容的安全。这种受保护数据的提供者通常要求访问内容的计算设备(例如，个人计算机、移动设备和机顶盒显示单元)在它们的易失性存储器(例如，随机存取存储器(RAM))内采用加密或加扰保护策略。这被称为RAM加扰。目前提供者需要执行RAM(或存储器)加扰算法，在该算法中，存储控制器在将数据发送给内部存储器/将其存储在内部存储器中之前对数据进行加扰。对存储在RAM内的受保护数据进行模糊，而不是以明文方式对内容进行存储，保护了内容免受访问内部存储器内容的攻击。

[0003] 由于RAM加扰算法出于性能的原因使用了较简单的加密技术，所以RAM加扰通常没有与非易失性存储器和传输一起使用的更加复杂的加密技术安全。对于RAM加扰而言，更加复杂的加密技术(例如，AES加密)在访问受保护内容的许多计算设备中可能是不可行的，这是因为这些技术需要更多的时间来编码/解码，而且这些技术是资源密集型的。RAM加扰使用较简单的算法结构和较小的密钥以使对存储器性能的影响最小化。然而，加扰技术的较低复杂度可能允许攻击者通过重复地将已知数据插入存储有受保护内容的内部存储器中来确定存储器的什么地址与所插入的已知数据相关联，从而进行暴力攻击。通过根据这种模式匹配攻击来查明加扰结果，恶意应用可以对RAM加扰实现方式的密钥和算法进行反向工程，并且获得对受保护数据(例如，DRM内容)的不受限制的访问。

发明内容

[0004] 各个实施例提供了对用于存储在电子设备的存储器中的数据进行选择性加扰的方法和设备，这为包括受保护内容的数据提供了提高的安全性。用于在计算设备内进行选择性存储器加扰以有效地保护数据免受模式匹配攻击的实施例方法包括：确定要存储在存储器中的数据是否包括受保护内容；当所述数据包括受保护内容时，作为将所述数据存储在所述存储器中的一部分，对所述数据应用加扰例程；以及当所述数据不包括受保护内容时，将所述数据存储在所述存储器中，而不对所述数据应用所述加扰例程。所述受保护内容可以是数字版权管理(DRM)下的数据、个人信息、安全信息、银行信息、密码、认证信息、受保护的内容应用信息和医疗数据。所述存储器可以是高速缓冲存储器、易失性存储器、非易失性存储器和片外存储器。在一个实施例中，确定要被存储在存储器中的所述数据是否包括受保护内容可以包括：将用于标识所述数据的来源或内容的标记信息添加到在所述计算设备的总线上发送的数据中，以及基于所述标记信息来确定所述事务的来源或内容，以及当所述数据包括受保护内容时，作为将所述数据存储在所述存储器中的一部分，对所述数据应用加扰例程可以包括：基于所确定的来源或内容，来对所述数据进行加扰并且将所述数据存储在存储器中。在一个实施例中，利用标识所述数据的来源或内容的信息对在所述计

算设备的总线上发送的数据进行标记可以包括:将信息添加到与能够存储所述数据的安全域相关的数据中,以及基于所述标记信息来确定所述事务的来源或内容可以包括:将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。在各个实施例中,添加到所述数据中的标记信息可以是虚拟机标识(VMID)、总线主控器标识、目的存储地址、所述数据的来源或内容的标识符和/或内容保护(CP)比特。

[0005] 其它实施例包括计算设备,所述计算设备具有配置有至少安全域和非安全域的存储器、以及耦合到所述存储器的处理器,其中,所述安全域中的数据被加扰,所述处理器配置有处理器可执行指令以执行以上所描述的方法的操作。在一个实施例中,所述处理器可以是以下各项中的一个或多个:独立处理器、所述计算设备内的多个处理器中的一个处理器、所述计算设备内的协处理器和所述计算设备内的对等处理器。

[0006] 其它实施例包括计算设备,所述计算设备具有用于执行以上所述的方法的功能的单元。

[0007] 其它实施例包括其上存储有处理器可执行指令的非暂时性处理器可读存储介质,所述处理器可执行指令被配置为使处理器执行以上所描述的方法的操作。在一个实施例中,存储在所述非暂时性处理器可读存储介质上的处理器可执行指令被配置为由从以下各项的组中选择的处理器来执行:多个处理器中的一个处理器、协处理器和对等处理器。

[0008] 其它实施例包括计算设备,所述计算设备包括配置有至少安全域和非安全域的存储器、耦合到所述存储器的存储控制器和耦合到所述存储器和所述存储控制器的处理器,其中,所述安全域中的数据被加扰,所述处理器配置有处理器可执行指令以执行包括以下各项的操作:将标记信息添加到在所述计算设备的总线上发送的数据中,以及对所述存储控制器进行编程以执行包括以下各项的操作:基于所述标记信息来确定要被存储在所述存储器中的数据是否包括受保护内容;当所述数据包括受保护内容时,作为将所述数据存储在所述存储器中的所述安全域中的一部分,对所述数据应用加扰例程;以及当所述数据不包括受保护内容时,将所述数据存储在所述非安全域中,而不对所述数据应用所述加扰例程。所述受保护内容可以是数字版权管理(DRM)下的数据、个人信息、安全信息、银行信息、密码、认证信息、受保护的内容应用信息和医疗数据。所述存储器可以是高速缓冲存储器、易失性存储器、非易失性存储器和片外存储器。在一个实施例中,处理器可以配置有处理器可执行指令以执行操作,使得:将标记信息添加到在所述计算设备的总线上发送的数据中可以包括将信息添加到与能够存储所述数据的安全域相关的所述数据中,以及基于标记信息来确定要被存储在存储器中的数据是否包括受保护内容可以包括将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。添加到所述数据中的标记信息可以是虚拟机标识(VMID)、总线主控器标识、目的存储地址、所述数据的来源或内容的标识符和/或内容保护(CP)比特。其它实施例包括其上存储有处理器可执行指令的非暂时性存储介质,所述处理器可执行指令被配置为使这样的计算设备的处理器执行前述的操作。

[0009] 其它实施例包括计算设备,所述计算设备包括:用于将标记信息添加到在所述计算设备的总线上发送的数据中的单元,以及用于对存储控制器进行编程以执行包括以下各项的操作的单元:基于所述标记信息来确定要被存储在存储器中的数据是否包括受保护内容;当所述数据包括受保护内容时,作为将数据存储在所述存储器中的安全域中的一部分,对所述数据应用加扰例程;以及当所述数据不包括受保护内容时,将所述数据存储在非安

全域中，而不对所述数据应用加扰例程。在一个实施例中，用于将标记信息添加到在所述计算设备的总线上发送的数据的单元可以包括用于将信息添加到与能够存储所述数据的安全域相关的数据中的单元，以及基于标记信息来确定要被存储在所述存储器中的数据是否包括受保护内容可以包括将所述标记信息与存储的与经授权的安全域相关的标识符进行比较。

附图说明

[0010] 并入本文并且构成本说明书一部分的附图示出了本发明的示例性方面，并且与以上给出的概括描述和以下给出的详细描述一起，用于解释本发明的特征。

[0011] 图1A是适合于与各个方面一起使用的、传送受保护数据的各个计算设备部件的通信系统框图。

[0012] 图1B是描述安全域并且可由管理程序操作系统例程访问的示例数据表的组成部分框图。

[0013] 图2是示出了用于基于虚拟机标识信息来对存储器内的受保护内容进行加扰的一方面方法的过程流图。

[0014] 图3是示出了用于基于目的存储器地址来对存储器内的受保护内容进行加扰的一方面方法的过程流图。

[0015] 图4是示出了用于基于内容保护比特信息来对存储器内的受保护内容进行加扰的一方面方法的过程流图。

[0016] 图5是适合于与各个方面一起使用的示例无线移动计算设备的部件框图。

[0017] 图6是适合于与各个方面一起使用的示例膝上型计算设备的部件框图。

具体实施方式

[0018] 将参照附图对各个方面进行详细描述。在可能的情况下，将贯穿附图使用相同的附图标记来指代相同或类似的部分。对特定例子和实现方式的提及是为了说明的目的，而非旨在限制本发明或权利要求的范围。

[0019] 本文中使用“示例性的”一词意指“用作例子、实例或说明”。本文中被描述为“示例性的”任何实现方式不必需被解释为比其它实现方式更优选或更具优势。

[0020] 本文中使用术语“计算设备”以指代以下各项中的任一个或全部：蜂窝电话、智能电话、个人或移动多媒体播放器、个人数据助理(PDA的)、膝上型计算机、台式计算机、平板计算机、智能本、掌上计算机、无线电子邮件接收机、启用多媒体互联网的蜂窝电话、电视机、智能电视、智能电视机顶盒、集成智能电视机、流媒体播放器、智能电缆盒、机顶盒、数字视频录像机(DVR)、数字媒体播放器以及包括可编程处理器、存储器和至少能够发送和/或接收无线和/或有线数据传输、访问本地或远程数据库结构和执行各种计算的电路的类似的个人电子设备。

[0021] 各个方面通过将受保护数据的差别(或选择性)加扰与基于事务标记的加扰一起使用，解决了较低复杂度随机存取存储器(RAM)加扰技术的安全性降低的问题。一般而言，可以在计算设备上执行的操作系统内加载并注册应用。操作系统或存储控制器可以建立安全域并且将已知应用与特定的域进行关联。操作系统、存储控制器或控制对存储器的访问

的其它单元可以利用定义应用可以如何访问(例如,存储)计算设备内的数据的许可集。例如,可以不允许应用访问与本地存储器(例如,双倍数据速率(DDR)存储器)内的某个区域相对应的某个安全域。在一方面,计算设备可以执行操作系统内的管理计算设备内的安全域的顶层例程,即“管理程序”。基于定义的注册应用的许可,管理程序可以指示或配置存储控制器以处理/存储与各个应用相关的数据,以为受保护数据而不是其它数据提供RAM加扰。作为进行该确定的一部分,管理程序可以访问描述针对所有安全域的内容、许可和注册应用的信息。例如,管理程序可以访问将针对各个应用的标识信息或代码与特定安全域相关联的数据表。

[0022] 在替代的方面,安全域可以由与管理程序不同的其它例程或客户端软件来管理。例如,独立于操作系统的管理程序的防火墙管理器例程可以管理安全域。在这种情况下,管理程序可以被锁定而不能访问安全域硬件并且可以不被认证为可信代码。此外,安全域管理可以由硬件来执行,例如,存储控制器或另一存储单元控制器。

[0023] 在由计算设备的处理器执行期间,应用可以在数据总线上执行信息事务。在各个方面,总线可以包括内部总线(例如,系统、数据等)和/或在计算设备的各个部件之间创建物理连接的外部总线(例如,串行总线)。总线控制器(或总线主控器)可以管理在总线上传送的信息事务。出于描述各个方面的目的,在数据总线上所执行的这样的信息事务被称为“数据总线事务”。总线主控器可以提供具有源应用的指示符(即,标记或标记信息)和/或所发送的信息的特征的数据总线事务。在一方面,总线主控器可以对包括受保护内容的数据总线事务(例如,由从通信链路或非易失性存储器接收DRM内容的应用进行的数据总线事务)进行标记。总线控制器可以应用指示被用来执行应用并产生在总线上进行传送的数据的虚拟机ID(VMID)的标记信息。或者,标记信息可以标识将标记信息应用到数据总线事务的总线主控器(即,总线ID)或使得计算设备能够区分应用之间的操作分区的其它识别码。在一方面,VMID可以表示总线主控器ID的集合。在一方面,总线控制器还可以将特定的标记应用到包含来自被授权以处理DRM内容数据的应用的DRM内容的数据总线事务。例如,总线控制器可以通过设置指示存在受保护内容的数据比特,来对来自DRM媒体阅读应用的数据总线事务进行标记。

[0024] 所标记的数据总线事务可以被送到计算设备内部的各个目的部件或与计算设备相关联的各个目的部件。首先,数据总线事务可以被发送给内部存储器单元(例如,RAM)或在内部存储器单元处进行接收。然而,在各个方面,数据总线事务可以被发送给内部存储器单元和/或任何片外存储器,并且在内部存储器单元和/或任何片外存储器内被加扰,其中,片外存储器包括通过PCI Express、PCI Express移动(PCI Express Mobile)或任何其它有线协议连接到计算设备的远程存储器或存储器单元。

[0025] 当所标记的数据总线事务到达目的部件(例如,内部存储器)时,管理程序软件可以使用数据总线事务的标记信息来确定针对发起该数据总线事务的应用的关联的安全域。例如,由与某个安全域相关联的应用产生的事务可以利用特定的VMID来标记。基于所确定的安全域关联,关联程序可以向各个部件控制器(例如,用于RAM单元的控制器)指示可以如何处理由部件控制器接收的数据。具体地,管理程序可以向存储控制器指示存储控制器是否应当执行RAM加扰算法以对由应用所产生的数据进行加密。例如,管理程序可以指示DDR存储控制器基于接收的数据的标记的VMID来对所接收的数据进行加扰和存储。在一方面,

安全域可以与多个VMID的集合、总线ID和/或存储器地址范围相关联。

[0026] 由于只有当数据涉及受保护的安全域(例如,由与受保护内容安全域相关联的VMID所产生)时,存储控制器才可以对数据进行加扰,所以计算设备可以使用标记信息来避免对存储在存储器单元中的所有数据(包括从不需要数据保护的应用发送给RAM的数据)进行加扰。这使得计算设备能够压制模式匹配攻击,使用用于RAM加扰的不太复杂的加密方案以及只将加密操作应用到受保护的内容数据。

[0027] 在一方面,计算设备可以基于目的存储器地址来执行选择性存储器加扰。由应用产生的数据总线事务可以针对存储器地址的特定范围(例如,存储器单元内的某些物理地址)内的存储。如果计算设备将数据总线事务的目的存储器地址识别为与存储器的预定义的"受保护"区域相关,那么,作为存储过程的一部分,计算设备可以指示存储控制器对数据进行加扰。

[0028] 在一方面,计算设备可以基于包括在数据总线事务内或与数据总线事务相关联的自定义比特的值,经由存储控制器来对总线事务数据进行加扰。例如,用于特定设备的总线主控器可以利用每个经发送的数据总线事务中的一个或多个比特来定义数据总线事务的质量、属性或内容,以便控制其是否经受RAM加扰。如果自定义比特或内容保护(CP)比特指示数据总线事务包括受保护内容,那么作为数据存储过程的一部分,计算设备(例如,存储控制器)可以对数据进行加扰。

[0029] 在一方面,存储控制器可以存储并直接访问定义安全域的数据。例如,DDR控制器可以将接收的数据总线事务内的标记信息与由DDR控制器维护(或编码到DDR控制器中)的数据表进行比较。因此,存储控制器可以在没有来自管理程序例程或者与计算设备的操作系统相关联的类似软件的指示或输入的情况下,确定数据总线事务是否包含受保护数据。

[0030] 在各个方面,计算设备可以可互换地使用数据表、数据库元素、硬编码定义、操作系统调用以及用于引用信息以定义数据总线事务特性(例如,事务标识、保护类别等)、标识关联的安全域和/或标识产生数据总线事务的应用的任何其它机制。将对计算设备使用数据表来对数据进行分类的描述提供作为,计算设备处理器或总线控制器出于选择性RAM加扰的目的,可以如何对数据进行分类、识别或引用的非限制性例子。例如,为了识别数据总线事务内的数据的属性,计算设备可以基于用于将数据总线事务发送给存储器的操作系统调用或计算设备元件,经由管理程序来确定数据总线事务的属性。

[0031] 在各个方面,配置硬件以及设置用于执行加扰操作的策略(例如,定义与各个安全域相关联的应用等)的软件或部件可以不对存储器内的数据进行加扰。例如,管理程序、防火墙管理器或与计算设备相关联的其它软件可以评估与数据总线事务相关联的标记信息,但是不对存储器中的所关联的数据进行加扰。另外,总线控制器可以不对存储器内的数据进行加扰,但是可以仅附加标记信息以及以其它方式将数据总线事务指引到计算设备内的各个部件(例如,存储控制器)。一般而言,加扰操作和算法可以专门由存储控制器来执行。

[0032] 在各个方面,计算设备还可以通过旋转加密(或加扰)密钥来提高RAM加扰的安全性。由计算设备执行的存储器加扰算法可以使用仅为计算设备的受保护的或受信任的元件已知的加密、秘密或编码密钥来执行。例如,存储控制器单元和管理程序可以共享秘密加密密钥,其中秘密加密密钥被用来对存储在存储器内的内容和从存储器取回的内容进行加扰和解扰。除了本文所描述的RAM加扰方法(例如,基于虚拟机标识、目的存储器地址和/或内

容保护比特信息的方法)之外,计算设备还可以按预定义的时间表或频率旋转(或修改)加密密钥。通过定期地旋转秘密加密密钥,计算设备还可以提防试图使用伪造的凭证来获得对存储在计算设备中的数据的不当访问的恶意应用。

[0033] 在一方面,受保护内容还可以包括用于访问、改变或以其它方式处理受保护的内容数据(即,受保护的内容应用信息)的应用的可操作指令或程序指令。例如,与DRM-内容渲染应用有关的信息(包括应用的代码或指令)可以作为受保护内容存储在存储器内。

[0034] 图1A示出了计算设备100内的数据总线事务的流。计算设备的处理器或中央处理单元(CPU)101可以执行多个软件应用并且可以将应用数据存储在应用存储器或高速缓冲存储器内。例如,CPU 101可以同时执行安装的应用App Z 106、App B 104、App A 102以及包括管理程序115例程的操作系统软件。应用102、104和106可以执行计算设备100内的各种功能,例如,实现互联网浏览、与远程数据服务器进行通信以及对本地存储在硬盘驱动器上的音频数据进行渲染。在CPU 101上的执行期间,应用102、104和106可以产生数据总线事务111、112、114。例如,App A可以是产生要被暂时存储在内部存储器120中的配置数据(例如,cookie信息)的互联网浏览器应用。CPU 101可以跨越总线126将数据总线事务111、112、114指引到内部存储器120。在一方面,也可以将数据总线事务111、112、114发送给各个片外存储器单元,例如,经由有线协议(例如,PCI Express、PCI Express Mobile)发送给远程DDR。

[0035] 总线控制器128可以利用标识信息对每个数据总线事务111、112、114进行标记。如上所述,这样的标记信息可以包括描述产生数据总线事务的应用的指示符(例如,VMID)、总线控制器128标识信息、数据总线事务内的内容的特性以及与目的存储器地址相关的信息。数据总线事务111、112、114可以跨越总线126来进行传输并且可以由存储控制器单元110来处理。例如,存储控制器单元110可以对数据总线事务114内的数据进行加扰。

[0036] 存储控制器110可以将数据总线事务标记信息传送给管理程序115例程并且从管理程序115例程接收响应指令。在接收到数据总线事务标记信息时,管理程序115可以评估每个数据总线事务111、112、114的标记信息(例如,VMID)。在一方面,管理程序例程115可以将每个数据总线事务的标记与以下参照图1B所描述的安全域数据表进行比较,并且根据从该表获取的适于每个标记的规则来指示存储控制器110处理数据总线事务111、112、114,以用于存储。例如,基于标记信息,管理程序115可以指示存储控制器110将来自不受保护的内容应用102、104的数据总线事务111、112送到存储器122的未被加扰的部分。然而,基于与标识App Z 106的标记信息相关联的安全域,可以将相关的数据总线事务114指引到内部存储器124的加扰部分。换言之,数据总线事务114可以被识别为来自受保护的内容应用106并且因此可以被加扰并被保存到RAM 124的安全部分。在一方面,RAM加扰(或被加扰的数据)可以受限于存储器的特定分段或分区。因此,基于标记信息将数据指引到存储器的过程,可以将不受保护的内容应用数据发送到未被加扰的分段/分区。以这种方式,不受保护的内容应用或不具有存储受保护内容的授权的应用(例如,恶意软件)仅可以访问存储器的未经受RAM加扰并且不受保护的部分。

[0037] 图1B示出了由在计算设备100内执行的管理程序115例程使用的简化的一方面安全域数据表150。如上所述,管理程序115可以基于与安全域数据表150的比较,来处理与数据总线事务相关联的标记信息。安全域数据表150可以描述由计算设备支持的各个安全域,其包含针对每个安全域的记录152、154。记录152、154可以存储用于与各个域相关联的应用

的应用标识信息。例如，针对某个安全域的记录154可以包括用于指示具有某个VMID的应用与该域相关联的信息。在一方面，安全域数据表150可以包含用于指示存储器单元内的地址、总线控制器标识和/或与各个安全域的应用相关联的专门的比特值(例如，CP比特)的记录。在另一方面，管理程序115可以配置存储控制器(例如，参照图1A所描述的)和/或存储安全域数据表150，使得存储控制器可以使用硬件(HW)查找操作来利用安全域数据表150。

[0038] 图2示出了用于基于虚拟机ID信息来对在数据总线事务内的受保护数据进行处理和加扰的一方面方法200。虚拟机是本领域所公知的并且通常被定义为被配置为建立某些执行环境(例如，仿真系统)的软件，其中，虚拟机可以利用这些执行环境来执行其它应用。计算设备可以经由其操作系统和/或管理程序例程，来将唯一的标识码或VMID分配给在计算设备上执行的虚拟机。如上所述，VMID可以被存储在系统数据中并且可以与安全域相关联。在一方面，计算设备可以存储并且使用用于在计算设备内的单个处理器上、计算设备内的协处理器(或对等处理器)上、或计算设备内的各个处理器的组合上运行的虚拟机的VMID。

[0039] 在框202处，运行在计算设备上的虚拟机可以执行应用。例如，虚拟机可以仿真特定的硬件配置以及执行音频数据编辑应用。作为另一个例子，虚拟机可以保留来自计算设备的资源并且可以使用所保留的资源来执行应用。虚拟机可以执行具有公共操作参数或功能特性的多个单独的应用。例如，虚拟机可以执行被设计用于在不同于计算设备的硬件上执行的一些应用(例如，移植的、以用于在非本地计算机架构上执行的应用)。在一方面，计算设备可以并发地执行多个虚拟机。

[0040] 在框204处，虚拟机可以基于对应用的执行来产生数据。例如，由虚拟机所执行的应用可以计算要被存储在系统数据结构内的值。作为另一个例子，视频播放器应用可以产生DRM视频数据。虚拟机可以处理所产生的数据并且跨越总线将要发送的数据指引到目的存储器。在框206处，总线主控器(或控制器)可以接收所产生的数据并且将所产生的数据封装成数据总线事务，使得该事务包括用于指示虚拟机的VMID的标记信息。例如，总线主控器可以利用用于表示执行视频播放器应用的虚拟机的代码来标记数据总线事务(例如通过向数据添加信息)。在另一方面，总线主控器可以利用所添加的信息(例如，总线主控器标识(ID)、时间戳、应用存储器信息、用户信息或任何其它描述数据)来标记数据总线事务。

[0041] 在框208处，基于由虚拟机提供的目的地信息，总线主控器可以在总线上将数据总线事务发送给与目的存储器相关联的控制器单元。例如，可以将数据总线事务指引到用于本地DDR存储器单元的控制器。

[0042] 在框210处，计算设备可以基于数据总线事务的标记信息内的VMID来确定数据总线事务的数据的属性或保护分类。在一方面，保护分类可以将数据总线事务定义为“受保护的”或“不受保护的”。例如，具有“受保护的”保护分类的数据可以包括DRM-内容，例如，有版权的媒体、安全信息(例如，银行信息)、个人信息、安全信息、银行信息、密码、认证信息和医疗数据，以及与受限的使用联系方式(contact)相关联的其它数据。在一方面，存储控制器可以将标记信息传送给管理程序例程以确定所发送的数据总线事务的保护分类。在替代的方面，管理程序可以直接从数据总线事务中提取标记信息。

[0043] 在一方面，管理程序可以识别标记信息内的虚拟机的VMID并且将该VMID与如上所述的描述安全域的数据表进行比较。换言之，数据表可以包含多个安全域条目，多个安全域

条目一起可以包括对在计算设备上执行的应用或虚拟机的引用。管理程序可以在数据表中查找到与VMID相关联的安全域条目(例如,该条目包含对VMID的引用),并且基于该安全域条目内的数据保护信息来确定数据总线事务的保护分类。例如,管理程序在查找到在“不受保护的”安全域条目中所引用的VMID时,可以确定“不受保护的”保护分类。作为另一个例子,与视频应用流DRM内容相关联的安全域的保护分类可以是“受保护的”。

[0044] 在替代的方面,管理程序可以对存储控制器110进行编程,以识别标记信息内的虚拟机的VMID并且将该VMID与如上所述的描述安全域的数据表进行比较。换言之,数据表可以包含多个安全域条目,多个安全域条目一起可以包括对在计算设备上执行的应用或虚拟机的引用。存储控制器110可以在数据表中查找到与VMID相关联的安全域条目(例如,该条目包含对VMID的引用),并且基于该安全域条目内的数据保护信息来确定数据总线事务的保护分类。例如,存储控制器110在查找到在“不受保护的”安全域条目中所引用的VMID时,可以确定“不受保护的”保护分类。作为另一个例子,与视频应用流DRM内容相关联的安全域的保护分类可以是“受保护的”。

[0045] 在一方面,如果VMID不在数据表(或访问计算设备的其它引用知识库)内,管理程序可以确定数据总线事务的保护分类为不受保护的内容。在一方面,数据表可以包括被硬编码为计算设备的操作系统的元素的、由内容提供者所供应的和/或在各个应用在计算设备上的执行期间更新的信息。例如,当计算设备确定与应用相关联的内容是DRM、来自特定的内容提供者或以任何方式与受保护数据相关联时,数据表可以包括用于修改的应用的默认数据保护信息。

[0046] 在替代的方面,如果VMID不在数据表(或访问计算设备的其它引用知识库)内,存储控制器110可以确定数据总线事务的保护分类为不受保护的内容。在一方面,数据表可以包括被硬编码为计算设备的操作系统的元素的、由内容提供者所供应的和/或在各个应用在计算设备上的执行期间更新的信息。例如,当计算设备确定与应用相关联的内容是DRM、来自特定的内容提供者或以任何方式与受保护的数据相关联时,数据表可以包括用于修改的应用的默认数据保护信息。

[0047] 在确定框212处,计算设备可以基于所确定的保护分类来确定总线事务数据是否是受保护的。如果数据是受保护的(即,确定框212=“是”),在框214中,存储控制器可以通过执行存储器加扰例程或算法来对在数据总线事务内所发送的数据进行加扰。可以在各个方面中使用的各种存储器或RAM加扰算法是本领域所公知的。在另一方面,如果数据是不受保护的(即,确定框212=“否”),在框216中,存储控制器可以将不受保护的总线事务数据作为未被加扰的数据存储在存储器内(即,不作为存储数据的一部分来执行存储器加扰算法)。

[0048] 在一方面,添加到数据总线事务中的数据中的标记信息可以包括VMID和管理程序可以用来指示RAM加扰算法的额外的代码(例如,应用ID或代码)。例如,管理程序可以确定VMID是与通常与受保护数据有关的安全域相关联的。然而,应用ID可以指示该应用不要求对数据进行加扰。基于该应用ID,管理程序可以指示存储控制器不对总线事务数据进行加扰。在一方面,定义安全域的数据表可以包括针对每个虚拟机(或VMID)的一般保护分类和针对由每个虚拟机所执行的应用的特殊保护分类。

[0049] 图3示出了用于基于目的存储器地址来对数据总线事务内的数据进行处理和加扰

的一方面方法300。存储器的某些存储器地址可以是受保护的并且仅可由经授权的应用来访问。例如，由计算设备授权的(例如，在受保护的内容安全域条目中引用的)应用可以将数据写入受保护的存储器地址范围内。作为另一个例子，计算设备可以禁止恶意的或未被识别的应用发送要被存储在受保护的存储器位置内的数据。存储在存储器地址的受保护范围内的数据可以由与存储器相关联的存储控制器来加扰。在各个方面，目的存储器地址可以是存储器的特定区域并且可以由物理存储器地址或虚拟存储器地址来定义。在一方面，计算设备可以对存储器或存储器单元进行分区并且可以指示某些分区、块或区域将被用于受保护的数据存储。

[0050] 在一方面，计算设备可以基于存储在定义每个应用被授权访问的安全区域的数据表中的信息，来确定应用是否被授权以访问受保护存储地址或位置中的数据和/或将数据存储在受保护存储地址或位置中。这样的数据表可以包括使在计算设备上安装的应用、数据标记和应用被授权以访问和存储数据的安全域相关的信息。使应用、数据标识符和安全域相关的这种数据表可以通过将数据中的信息(即，数据标记)用作查表例程中的查找值来识别与数据标记相对应的来源或内容，从而促进确定数据的来源或内容。以类似的方式，可以通过将应用名称或标识符用作查表例程中的查找值来识别对应的数据标记，来确定用于识别由应用所产生的数据的来源或内容的数据标记。此外，计算设备可以通过将数据中的信息(即，数据标记)用作查表例程中的查找值来识别与数据标记相对应的安全域，来识别用于存储数据的经授权的安全域。

[0051] 应用可能与不与受保护数据相关的安全域相关联，并且因此可能不被授权访问受保护的存储器位置。如果计算设备确定未经授权的应用正在请求在受保护的存储器位置内存储数据，则计算设备可以将该数据存储在不受保护的存储器内。或者，计算设备可以通过提示应用以信号方式发送用于标识信息或重新发送数据总线事务，来执行应用标识确认操作。在一方面，计算设备可以忽略未经授权而请求受保护的存储器的数据总线事务。

[0052] 在框302中，计算设备可以执行应用，例如DRM-内容渲染程序。应用可以由虚拟机执行或者可以不由虚拟机执行。在框304中，应用可以产生用于在系统总线上传送的数据。应用可以向总线控制器指示所产生的数据应当被存储在存储器中的特定目的存储地址内。例如，应用可以向总线控制器指示所产生的数据应当被指引到存储器的特定物理地址范围。在框306中，总线控制器可以将数据封装为数据总线事务，该数据总线事务包括至少指示目的存储器地址的标记信息。在框208中，总线控制器可以将数据总线事务发送给存储器，在该存储器处，该事务由存储控制器接收。

[0053] 在框310中，类似于以上参照框210的操作所描述的，计算设备可以基于目的存储器地址来确定数据总线事务内的信息的保护分类。存储控制器可以识别数据总线事务信息内的目的存储器地址，并且可以分析地址以确定数据总线事务是否涉及受保护内容。在一方面，可以利用存储器的受保护地址来对存储控制器(例如，DDR控制器)进行编程。在另一方面，存储控制器可以访问数据表，该数据表定义涉及受保护数据和不受保护数据的存储器地址。例如，数据表可以包括用于指示与受保护数据分类相对应的所有存储器地址的条目。或者，数据表可以包括针对系统的所有安全域的条目，并且计算设备可以定位各个安全域条目内的数据总线事务目的存储器地址。基于与目的存储器地址相关联的安全域的特性，计算设备可以确定数据总线事务的保护分类。

[0054] 在确定框212中，计算设备可以确定数据总线事务的保护分类是否指示数据应当被加扰。如果总线事务数据是受保护的(即，确定框212＝“是”)，则在框214中，计算设备可以经由存储控制器来对数据进行加扰，并且将其存储在预定为受保护位置的目的存储器地址内。然而，如果总线事务数据是不受保护的(即，确定框212＝“否”)，则在框216中，计算设备可以将总线事务数据存储在目的存储器地址内，而不执行任何加扰操作。换言之，当数据总线事务包含用于存储在不受保护的目的存储器地址内的数据时，可以以明文方式来对数据进行存储。

[0055] 图4示出了用于基于内容保护(或CP)比特值来对存储器内的受保护数据进行加扰的一方面方法400。方法400类似于以上所描述的方法，除了使用方法400的计算设备可以通过设置CP比特值而不是指示受保护的VMID或目的存储器地址来促使数据总线事务内的数据被加扰之外。在一方面，计算设备可以包括总线上的专用引脚或连接，以能够实现针对各个组件(例如，处理器、调制解调器等)的保护指示符。例如，调制解调器部件可以包括使得来自调制解调器的数据总线事务能够包括受保护的CP比特的专用引脚。在另一方面，具有专用引脚的部件可以被配置为选择性地设置用于存储器加扰的CP比特值。例如，具有用于设置受保护的CP比特值的专用引脚的部件可以发送数据总线事务，使得存储控制器可以不对事务数据进行加扰。

[0056] 在框304中，计算设备可以产生用于存储在存储器或存储器单元中的数据。数据可以由运行在处理器上的应用(例如，互联网协议上的语音程序)产生。在一方面，数据可以由计算设备内的部件(例如，图形处理器、外围设备或调制解调器)产生。在框402中，计算设备处理器可以利用标记信息来对数据进行封装，以在总线(例如，系统总线、串行总线等)上进行传输。可以通过将CP比特值添加到数据中，来将数据封装为具有指示数据是否受保护的CP比特的数据总线事务。在框208中，计算设备可以将数据总线事务发送给存储控制器(例如，DDR控制器)。在框404中，存储控制器可以评估数据总线事务(例如，识别数据的保护分类)，并且在确定框212中，可以基于CP比特值标记信息来确定数据是否是受保护的。例如，如果CP比特具有值“1”，则计算设备可以确定数据是受保护的，反之亦然。如数据是受保护的(即，确定框212＝“是”)，则计算设备可以经由存储控制器来对存储器中的数据进行加扰。或者，如果数据如CP比特值所指示的是不受保护的(即，确定框212＝“否”)，则计算设备可以不对数据加扰，而是可以以明文方式对数据总线事务的数据进行存储。

[0057] 各个方面可以用各种移动计算设备(例如，智能电话、功能手机等)的任意一种来实现，在图5中示出了移动计算设备的一个例子。例如，移动计算设备180可以包括耦合到内部存储器502的处理器501。内部存储器502可以是易失性存储器或非易失性存储器，并且还可以是安全的和/或加密的存储器、或者不安全的和/或未经加密的存储器或其任意组合。处理器501还可以耦合到触摸屏显示器506，例如，电阻传感触摸屏、电容传感触摸屏、红外传感触摸屏等。然而，移动计算设备180的显示器不必具有触摸屏能力。移动计算设备180可以具有用于发送和接收如本文所描述的无线信号的一个或多个短距离无线信号收发机518(例如，Peanut、蓝牙®、紫蜂(Zigbee)®、RF无线电设备)和天线508。收发机518和天线508可以与上述的电路一起用来实现各种无线传输协议栈/接口。移动计算设备180可以包括能够经由蜂窝网络实现通信的蜂窝网络无线调制解调器芯片520。移动计算设备180还可以包括用于接收用户输入的物理按钮512a和512b。

[0058] 计算设备的其它形式(包括个人计算机和膝上型计算机),可以被用来实现各个方面。这样的计算设备通常包括图6中所示的部件,图6示出了示例膝上型计算机设备110。许多膝上型计算机包括用作计算机的定点设备的触摸板触摸表面614,并且因此可以接收类似于在配备有触摸屏显示器的移动计算设备和以上所描述的移动计算设备上所实现的拖动、滚动和轻弹手势。这样的膝上型计算机110通常包括耦合到易失性内部存储器602和大容量非易失性存储器(例如,硬盘驱动器660)的处理器601。膝上型计算机110还可以包括耦合到处理器601的压缩光盘(CD)和/或DVD驱动器608。膝上型计算设备110还可以包括耦合到处理器601的、用于建立数据连接或接收外部存储器设备的多个连接器端口610,例如用于将处理器601耦合到网络的网络连接电路。膝上型计算设备110可以具有用于发送和接收如本文所描述的无线信号的一个或多个短距离无线信号收发机618(例如,Peanut、蓝牙®、Zigbee®、RF无线电设备)和天线620。收发机618和天线620可以与上述的电路一起用来实现各种无线传输协议栈/接口。在膝上型计算机或笔记本配置中,计算机外壳包括均耦合到处理器601的触摸板614、键盘612和显示器616。计算设备的其它配置可以包括如公知的、耦合到处理器(例如,经由USB输入)的计算机鼠标或轨迹球,其也可以结合各个方面来使用。

[0059] 处理器501和601可以是能够由软件指令(应用)配置以执行多种功能(包括以上所描述的各个方面的功能)的任何可编程微处理器、微计算机或多个处理芯片或芯片组。在各个设备中,可以提供多个处理器,例如专用于无线通信功能的一个处理器和专用于运行其它应用的一个处理器。通常,软件应用在其被访问并加载到处理器501和601中之前可以被存储在内部存储器502和602中。处理器501和601可以包括足以存储应用软件指令的内部存储器。在许多设备中,内部存储器可以是易失性存储器或非易失性存储器(例如,闪存)、或者二者的混合。出于此描述的目的,对存储器的一般提及是指可由处理器501和601访问的存储器,其包括内部存储器或在各种设备中插入的可移动存储器以及处理器501和601内的存储器。

[0060] 前述方法描述和过程流图仅作为说明性示例来提供,并不旨在要求或暗示必须以所呈现的次序来执行各个方面的步骤。正如本领域技术人员所明白的,可以以任何次序来执行前述方面的步骤的次序。诸如“此后”、“然后”、“接下来”等的词语并不旨在限制步骤的次序;这些词语仅被用来引导读者浏览对方法的描述。此外,对单数形式的权利要求元素的任何提及(例如,使用冠词“一(a)”、“一个(an)”或“所述”)不应当被解释为将元素限制为单数形式。

[0061] 结合本文公开的方面所描述的各种说明性的逻辑框、模块、电路和算法步骤可以实现为电子硬件、计算机软件或者二者的组合。为了清楚地说明硬件和软件的这种可交换性,上面对各种说明性的部件、框、模块、电路和步骤均围绕其功能进行了总体描述。至于这些功能是实现为硬件还是软件,取决于特定的应用和对整个系统所施加的设计约束。本领域技术人员可以针对每个特定的应用,以变通的方式实现所描述的功能,但是这样的实现决策不应当被解释为脱离本发明的范围。

[0062] 被设计为执行本文所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编辑门阵列(FPGA)或其它可编辑逻辑器件、分立门或晶体管逻辑器件、分立硬件组件或其任意组合,可以实现或执行用于实现结合本文公开的方面所描述的各种

说明性的逻辑、逻辑框、模块和电路的硬件。通用处理器可以是微处理器，或者，该处理器也可以是任何常规处理器、控制器、微控制器或状态机。处理器还可以实现为计算设备的组合，例如，DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合、或任何其它这样的配置。或者，一些步骤或方法可以由专用于给定功能的电路来执行。

[0063] 在一个或多个示例性方面，所描述的功能可以用硬件、软件、固件或其任意组合来实现。如果用软件实现，则可以将这些功能存储在计算机可读介质上或者作为计算机可读介质上的一个或多个指令或代码进行传输。本文所公开的方法或算法的步骤可以体现在可以位于有形的、非暂时性计算机可读存储介质上的处理器可执行软件模块中。有形的、非暂时性计算机可读存储介质可以是可由计算机存取的任何可用介质。通过举例而非限制的方式，这样的非暂时性计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储、磁盘存储或其它磁性存储设备、或者能够用于存储具有指令或数据结构形式的期望的程序代码并且能够由计算机存取的任何其它介质。如本文所使用的，磁盘和光盘，包括压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软盘和蓝光光盘，其中磁盘通常磁性地复制数据，而光盘利用激光来光学地复制数据。上文的组合也应当包括在非暂时性计算机可读介质的范围内。此外，方法或算法的操作可以作为代码和/或指令中的一个或任意组合或集合，位于有形的、非暂时性机器可读介质和/或计算机可读介质上，其可以被并入计算机程序产品内。

[0064] 提供所公开的方面的先前描述以使得本领域的任何技术人员都能够实现或使用本发明。对于本领域技术人员而言，对这些方面的各种修改都是显而易见的，并且在不脱离本发明的精神或范围的情况下，本文定义的总体原理可以应用于其它方面。因此，本发明并非旨在受限于本文所示出的方面，而是符合与以下权利要求和本文所公开的原理和新颖性特征相一致的最广范围。

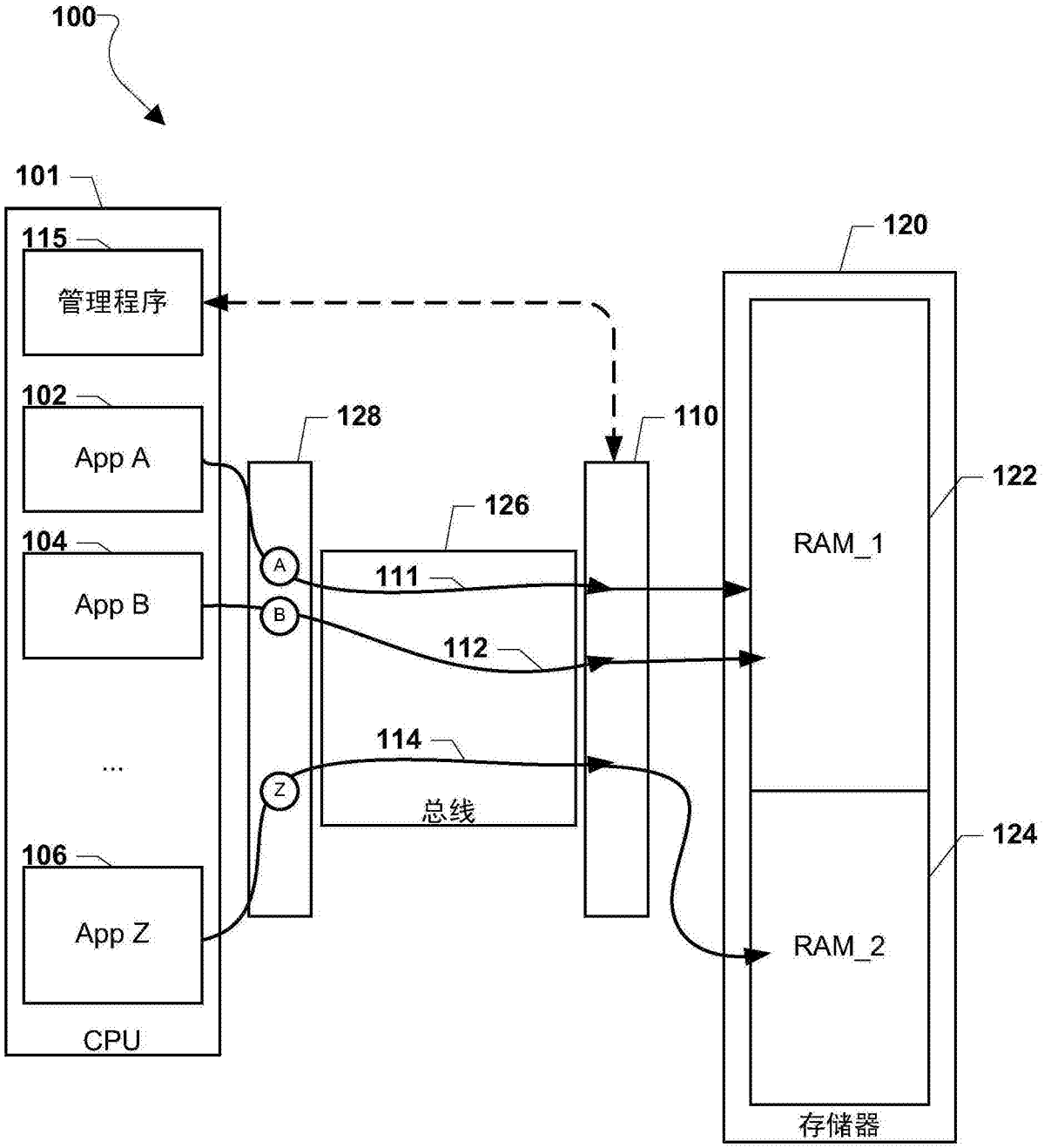

100
101
115
管理程序
102
App A
104
App B
...
106
App Z
CPU
128
126
A
B
Z
111
112
114
总线
110
120
122
RAM_1
124
RAM_2
存储器

图1A

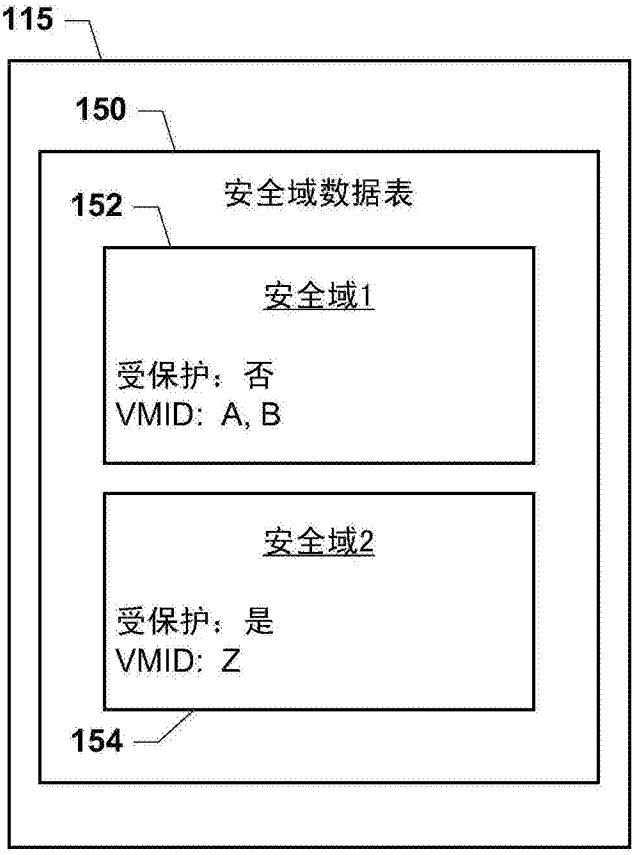


图1B

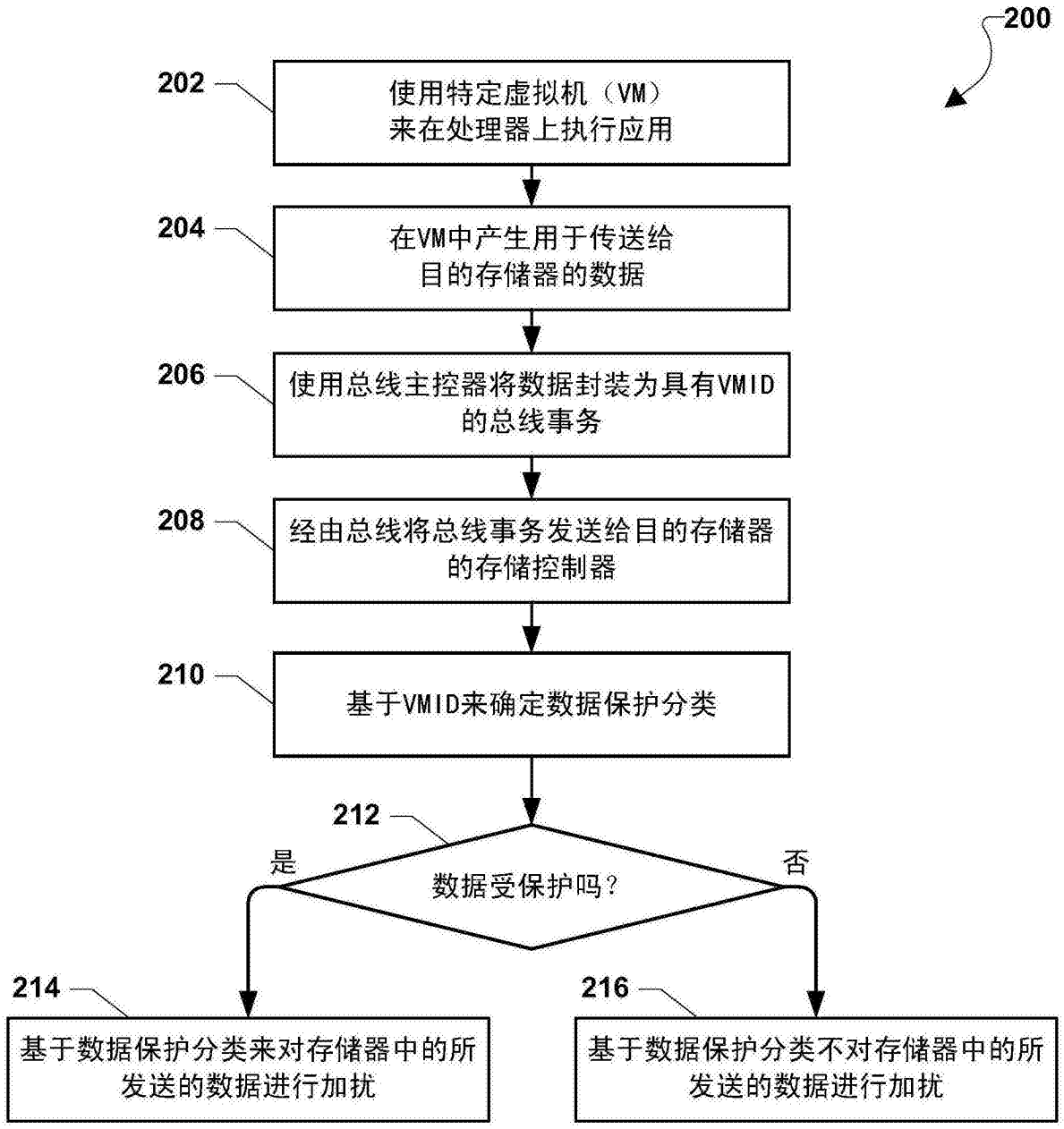

200
202
使用特定虚拟机（VM）
来在处理器上执行应用
204
在VM中产生用于传送给
目的存储器的数据
206
使用总线主控器将数据封装为具有VMID
的总线事务
208
经由总线将总线事务发送给目的存储器
的存储控制器
210
基于VMID来确定数据保护分类
212
数据受保护吗？
是
否
214
基于数据保护分类来对存储器中的所
发送的数据进行加扰
216
基于数据保护分类不对存储器中的所
发送的数据进行加扰

图2

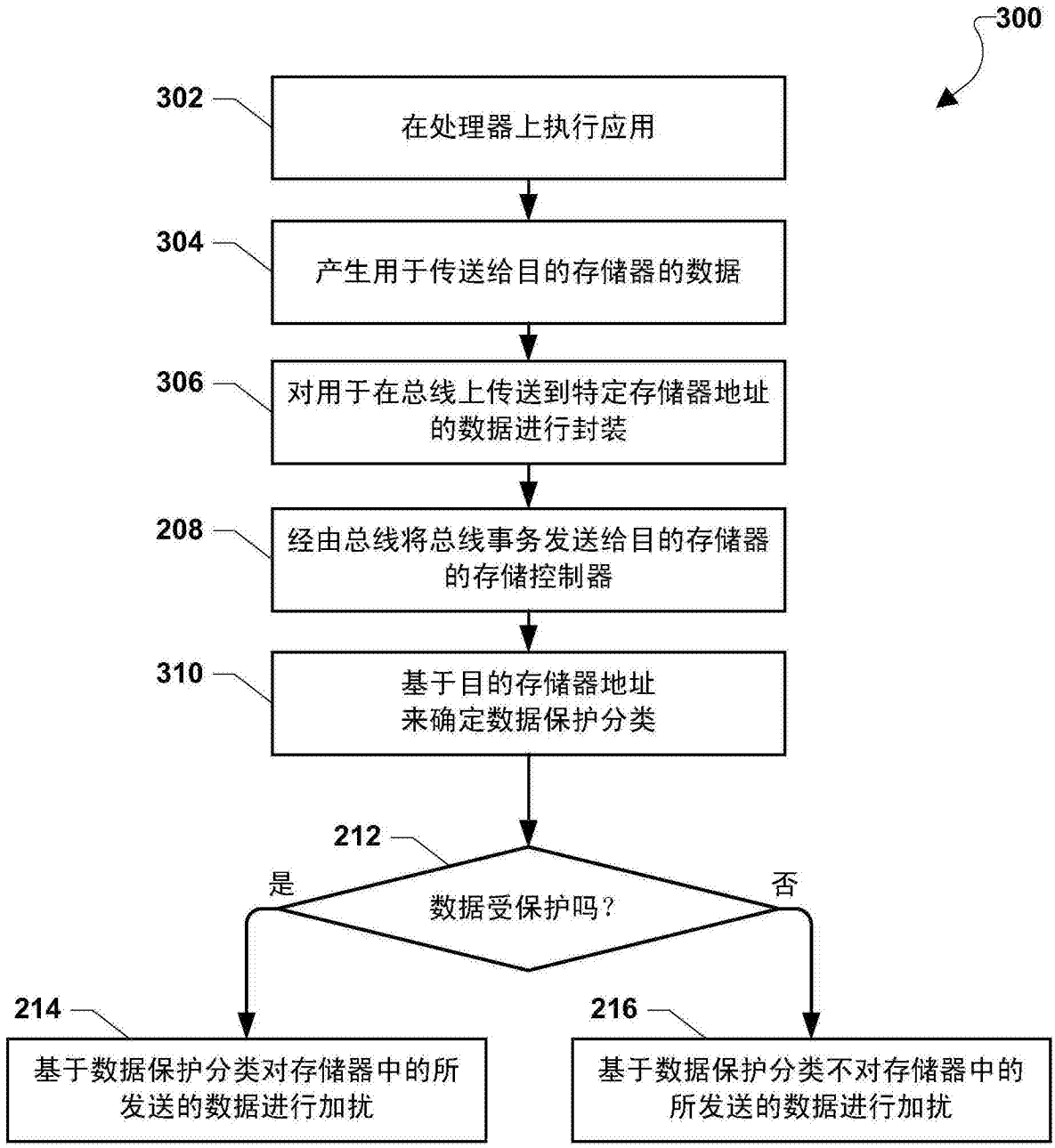

300
302
在处理器上执行应用
304
产生用于传送给目的存储器的数据
306
对用于在总线上传送到特定存储器地址的数据进行封装
208
经由总线将总线事务发送给目的存储器的存储控制器
310
基于目的存储器地址来确定数据保护分类
212
数据受保护吗？
是
否
214
基于数据保护分类对存储器中的所发送的数据进行加扰
216
基于数据保护分类不对存储器中的所发送的数据进行加扰

图3

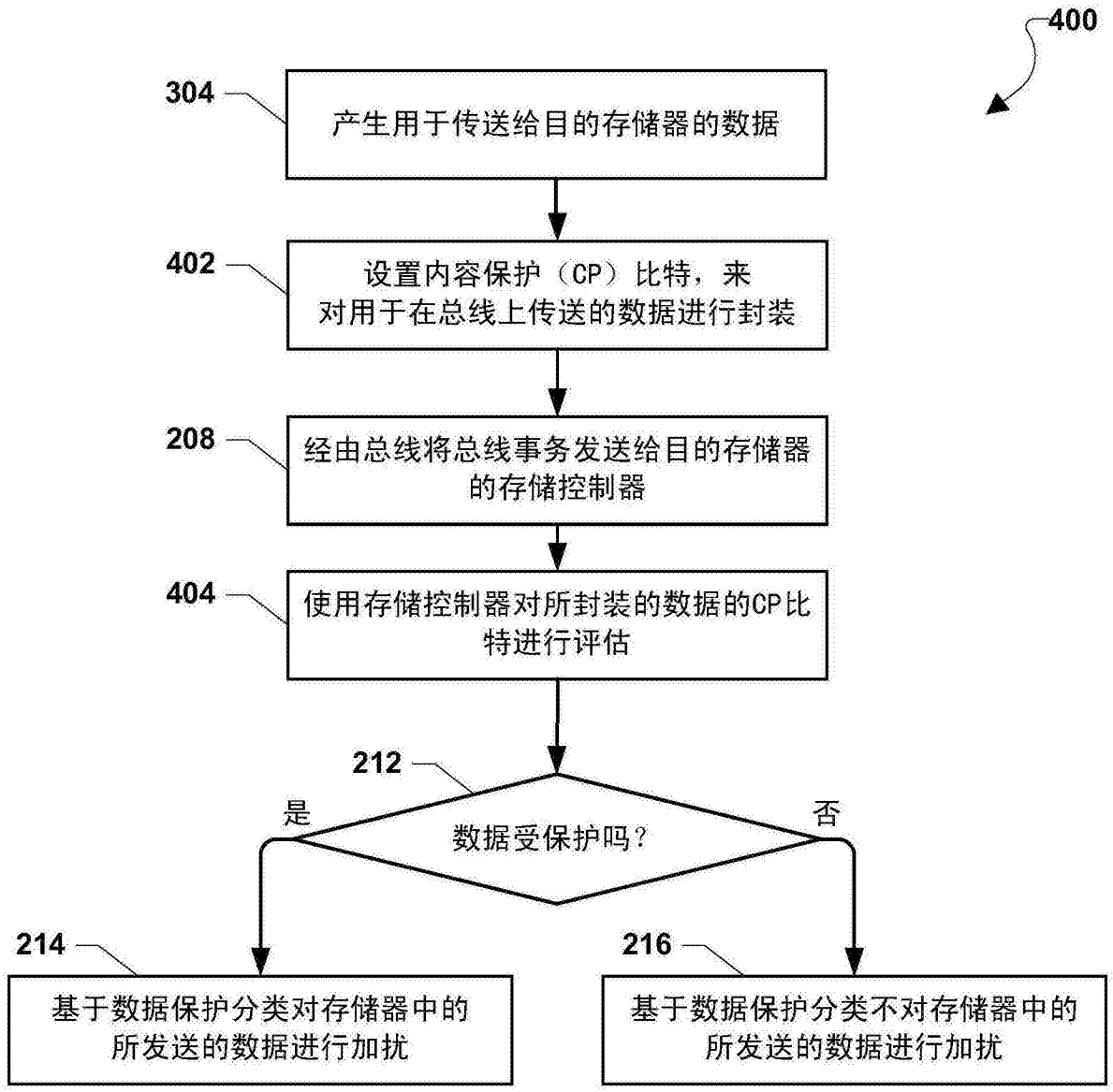

400
304
产生用于传送给目的存储器的数据
402
设置内容保护（CP）比特，来对用于在总线上传送的数据进行封装
208
经由总线将总线事务发送给目的存储器的存储控制器
404
使用存储控制器对所封装的数据的CP比特进行评估
212
数据受保护吗？
是
否
214
基于数据保护分类对存储器中的所发送的数据进行加扰
216
基于数据保护分类不对存储器中的所发送的数据进行加扰

图4

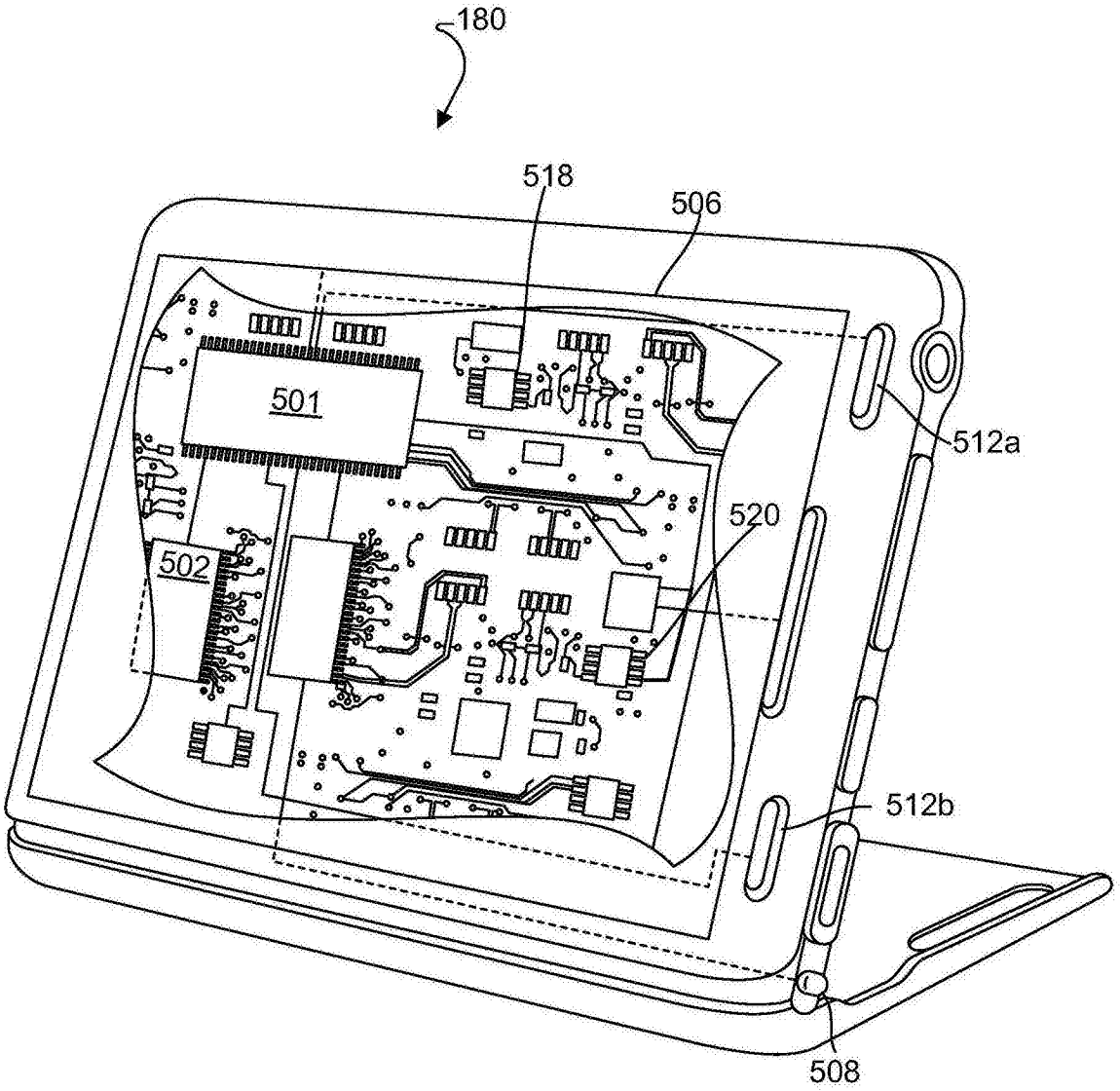


图5

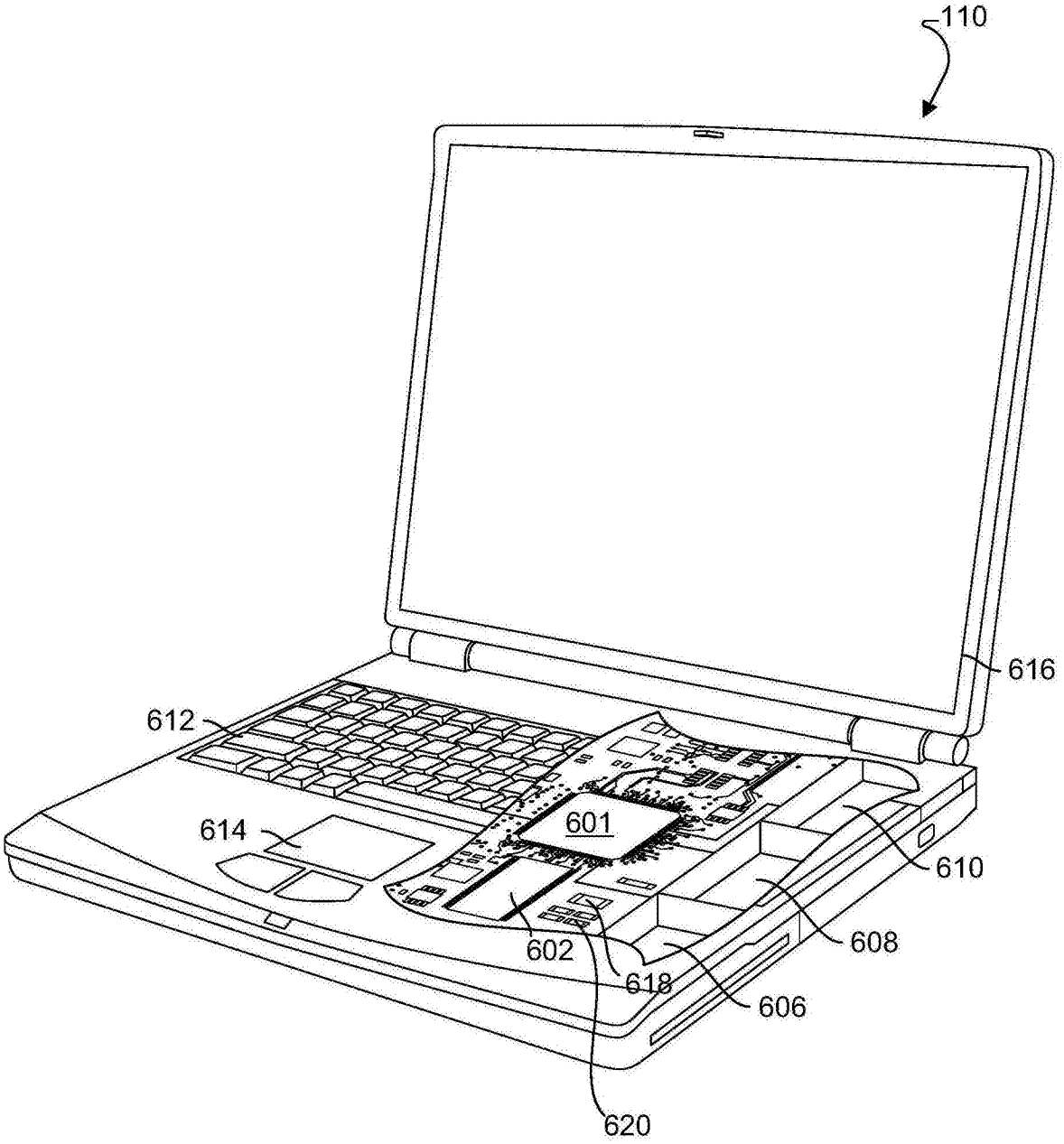


图6