

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
G06F 12/14 (2006.01)



# [12] 发明专利说明书

专利号 ZL 200410031646.2

[45] 授权公告日 2006 年 12 月 20 日

[11] 授权公告号 CN 1291329C

[22] 申请日 2004.3.31

[21] 申请号 200410031646.2

[30] 优先权

[32] 2003. 3. 31 [33] US [31] 10/404,881

[73] 专利权人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 罗伯特·J·沙弗拉内克  
德伯德拉·达斯·夏尔玛

审查员 吴紫璇

[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

代理人 王 怡

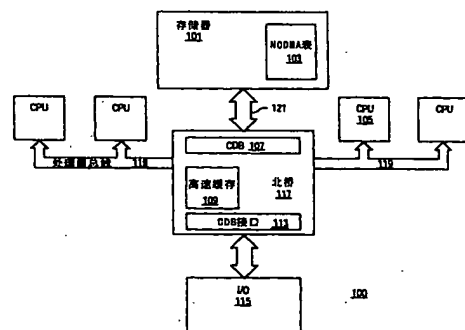
权利要求书 2 页 说明书 11 页 附图 4 页

## [54] 发明名称

用于访问存储器的装置和方法

## [57] 摘要

本发明提供了一种包括了超级页字段的 NoDMA 高速缓存。所述超级页字段指示何时一组页包含受保护信息。NoDMA 高速缓存被计算机系统用来拒绝 I/O 设备对系统存储器中受保护信息的访问。



1. 一种用于访问存储器的装置，包括：  
内容可寻址存储器；
- 5 耦合到所述内容可寻址存储器的第一存储设备，用来存储用于所述存储器第一区段的第一保密指示符，其中所述第一保密指示符指示所述第一区段是否包含受保护信息；和  
耦合到所述内容可寻址存储器的第二存储设备，用来存储用于所述存储器区段超集的第二保密指示符，所述区段超集包括所述第一区段，其中  
10 所述第二保密指示符指示所述区段超集是否包含受保护信息。
2. 如权利要求 1 所述的装置，还包括：  
高速缓存管理存储设备。
3. 如权利要求 1 所述的装置，还包括：  
用来确定所述第二保密指示符的值的电路。
- 15 4. 如权利要求 1 所述的装置，其中所述第一区段为一页。
5. 如权利要求 1 所述的装置，其中所述区段超集是超级页。
6. 如权利要求 1 所述的装置，还包括：  
用来改变存储在内容可寻址存储器中的数据的数据的电路。
7. 一种用于访问存储器的方法，包括：  
20 存储所述存储器中表条目的地址；  
存储用于所述存储器第一区段的第一保密指示符，其中所述第一保密指示符指示所述第一区段是否包含受保护信息；以及  
存储用于区段超集的第二保密指示符，所述区段超集包括所述第一区段，其中所述第二保密指示符指示所述区段超集是否包含受保护信息。
- 25 8. 如权利要求 7 所述的方法，还包括：  
接收存储器访问请求；  
将被请求的地址与所存储的地址比较；以及  
确定用于所述所存储地址的第二保密位是否被设置。
9. 如权利要求 8 所述的方法，还包括：

确定所述第一保密指示符是否被设置。

10. 如权利要求 8 所述的方法，还包括：

如果所述第二保密指示符被设置，产生侵犯指示符。

11. 如权利要求 10 所述的方法，还包括：

5 记录所述侵犯指示符。

12. 如权利要求 8 所述的方法，其中所述区段超集为超级页。

13. 一种用于访问存储器的装置，包括：

总线；

耦合到所述总线的存储器设备；

10 耦合到所述总线的处理器；

耦合到所述存储器设备的高速缓存，

用来存储用于所述存储器设备第一区段的第一保密指示符，其中所述第一保密指示符指示所述第一区段是否包含受保护信息，并

15 用来存储用于所述存储器设备所述第一区段的超集的第二保密指示符，其中所述第二保密指示符指示所述超集是否包含受保护信息；和  
耦合到所述高速缓存的网络接口设备。

14. 如权利要求 13 所述的装置，其中所述高速缓存包括高速缓存管理电路。

15. 如权利要求 13 所述的装置，还包括：

20 用来确定所述第二保密指示符的值的电路。

16. 如权利要求 13 所述的装置，还包括：

耦合到第二总线的外设；

其中所述第二总线被耦合到所述高速缓存。

## 用于访问存储器的装置和方法

## 5 技术领域

本发明一般地涉及用于保护敏感数据免受 I/O 设备不适当访问的安全设备。更具体而言，本发明涉及用于 NoDMA 表的高速缓存，所述 NoDMA 表跟踪包含敏感数据的存储器区段。

## 10 背景技术

越来越多的金融和个人交易在计算设备上进行。但是，这些金融交易数量上的持续增长也带来了对支持这些交易的计算机系统的更多的攻击，并导致了对安全性增强（SE）环境的相应需要以防止对敏感数据的未授权访问或者丢失敏感数据。敏感数据的丢失或者未授权访问（例如，社会保  
障号码、帐户号码、财务数据、帐户余额、密码、授权密钥等等）导致隐  
私的泄漏、私人财务数据的被盗以及类似的恶性行为。

一种试图用于访问受保护数据的技术是使用来自外设的通过直接存储器访问（DMA）控制器的存储器访问请求。DMA 控制器允许例如网卡的外设读取系统存储器和向其写入而最少地使用中央处理单元。使用来自  
I/O 设备的存储器访问请求可以避开操作系统所提供的安全措施。这可以  
通过请求对分配给外设使用的系统存储器区段以外包含敏感信息的存储器  
区段的存储器访问来实现。

## 发明内容

25 根据本发明的第一个方面，提供了一种装置，该装置包括内容可寻址存储器（CAM）、第一存储设备和第二存储设备；其中第一存储设备用来存储用于第一存储器区段的第一保密指示符，所述第一保密指示符指示所述第一存储器区段是否包含受保护信息，第二存储设备用来存储用于存储器超集的第二保密指示符，所述存储器超集包括所述第一存储器区段，所

述第二保密指示符指示所述存储器超集是否包含受保护信息。

根据本发明的第二个方面，提供了一种方法，该方法包括：存储表条目的地址；存储用于第一存储器区段的第一保密指示符，其中所述第一保密指示符指示所述第一存储器区段是否包含受保护信息；以及存储用于超集的第二保密指示符，所述超集包括所述第一存储器区段，其中所述第二保密指示符指示所述超集是否包含受保护信息。

根据本发明的第三个方面，提供了一种装置，该装置包括总线、耦合到所述总线的存储器设备、耦合到所述总线的处理器、耦合到所述存储器设备的高速缓存和耦合到所述高速缓存的网络接口设备。所述高速缓存用来存储用于所述存储设备的第一区段的第一保密指示符，并存储用于所述存储设备的所述第一区段的超集的第二保密指示符，其中所述第一保密指示符指示所述第一区段是否包含受保护信息，所述第二保密指示符指示所述超集是否包含受保护信息。

根据本发明的第四个方面，提供了一种装置，该装置包括用于内容可寻址存储的装置、用于存储用于存储设备的第一区段的第一保密指示符的装置和用于存储用于所述存储设备的第二区段的第二保密指示符的第二装置，所述第二区段是所述第一区段的超集，其中所述第一保密指示符指示所述第一区段是否包含受保护信息，所述第二保密指示符指示所述超集是否包含受保护信息。

20

### 附图说明

本发明的实施例通过举例而非限制的方式被图示于附图的图形中，其中相似的标号指示类似的元件。应该认识到在公开说明中对“实施例”或者“一个实施例”的引用未必指同一实施例，而这样的引用表示至少一个实施例。

25

图 1 是包括 NoDMA 高速缓存的计算机系统的框图；

图 2 是通过实现 NoDMA 的芯片组的输入、输出数据流的框图；

图 3 是 NoDMA 高速缓存结构的示图；

图 4 是 NoDMA 高速缓存系统的流程图。

## 具体实施方式

图 1 图示了一个实施例的计算机系统 100，所述计算机系统 100 包括芯片组（“北桥”）117、一组中央处理单元（CPU）105 和系统存储器 101。在一个实施例中，该组 CPU 105 经由处理器总线 119 被连接到北桥 117。在一个实施例中，计算机系统 100 包含多个处理器 105 以支持在服务器环境中的多重处理。在另一个实施例中，计算机系统 100 可以包括单个 CPU。系统存储器 101 经由存储器总线 121 被连接到北桥 117。系统存储器 101 包括非直接存储器访问（NoDMA）表 103。

10 在一个实施例中，系统存储器 101 是一组随机访问存储器设备，例如同步动态随机访问存储器（SDRAM）、双倍数据速率随机访问存储器（DDR RAM）或者类似设备。存储器系统 101 还可以包括寄存器和类似存储设备。NoDMA 表 103 存储在系统存储器 101 中，该 NoDMA 表跟踪系统存储器 101 的包含敏感数据的区段。敏感数据可以包括社会保障号  
15 码、财务帐户号码、密码以及类似数据。

通过标记 NoDMA 表 103 中对应于包含敏感数据的存储器区段的条目并且只允许被授权访问保密信息的那些程序访问存储器 101 的受保护部分，NoDMA 表 103 数据可以被操作系统（OS）用来限制对包含敏感数据的存储器区段的访问。在一个实施例中，系统存储器 101 被划分成页。页  
20 在大小上可以变化，这由操作系统来决定。在一个实施例中，页的大小是 4k 字节。

在一个实施例中，NoDMA 表 103 被构造成一组连续的位，每一位对应存储器 101 的一页。如果一页包含有敏感数据，则操作系统会“设置”NoDMA 表 103 中对应该页的位。NoDMA 表 103 的基址或起始位置在系  
25 统存储器 101 中是可以重新定位的。在一个实施例中，操作系统、基本输入输出系统（BIOS）或类似系统可以对 NoDMA 表 103 重新定位，例如在启动系统 100 之后。NoDMA 表 103 根据存储在基址寄存器中的起始地址在系统存储器 101 内定位。NoDMA 表 103 的大小根据存储在尺寸寄存器（size register）中的数据而定。当 NoDMA 表 103 被使能时，I/O 设备的所

有访问必须对照该表 103 来检验。

在一个实施例中，NoDMA 表 103 被对齐以从页边界开始并且在页边界结束。这种对齐简化了对 NoDMA 表 103 的使用。在另一个实施例中，NoDMA 表 103 可以从存储器 101 中能够为表 103 提供足够的连续空间的任何地址开始。从 NoDMA 表 103 的起始点到结束点的每一位指示对存储器 101 从地址 0 开始到覆盖全部需要保护的存储器地址空间每一页的非 CPU 访问的访问权限。当北桥 117 需要检验对特定地址的访问权限时，它可以方便地确定该页的访问权限，因为北桥 117 能够获得 NoDMA 表 103 的起始地址和要访问页的页地址。这样，对应的 NoDMA 表 103 条目可以方便地被计算和访问。

在一个实施例中，北桥 117 控制系统存储器 101、CPU 105 以及 I/O 设备 115 之间的通信。北桥 117 包括中央数据缓冲器（CDB），其处理进入的来自 CPU 105、I/O 设备和源 115 的存储器访问请求。中央控制块（CDB 接口）113 控制对进入的存储器访问请求的最初处理和对出去的请求的最后处理。等待被 CDB 107 或者 CDB 接口 113 处理的存储器访问请求存储在队列中。CDB 107 和 CDB 接口 113 处理来自 I/O 设备 115 的存储器请求并从系统存储器 101 向 I/O 设备发送被请求的数据。

北桥 117 包括一组队列，所述队列存储了进入和出去的存储器请求（例如，读取和写入请求）。在一个实施例中，队列是先入先出队列（FIFO）或者采用类似的队列管理机制。北桥 117 还包括 NoDMA 高速缓存 109，所述高速缓存存储最近被请求的 NoDMA 表条目。CDB 接口 113 在访问存储器 101 之前来维护和使用高速缓存 109。CDB 接口 113 还管理各自队列中进入和出去的消息。在一个实施例中，北桥 117 还包括一组与 NoDMA 表 103 和 NoDMA 高速缓存 109 功能相关的寄存器。这些寄存器包括状态寄存器、基址寄存器和尺寸寄存器，所述基址寄存器指示存储器 101 中 NoDMA 表 103 起始的地址，尺寸寄存器指示系统存储器 101 中 NoDMA 表 103 的大小。

在一个实施例中，北桥 117 保护存储器 101 免受非 CPU 设备的访问。包含受保护数据的存储器区段不能被非 CPU 设备所读取或写入。受保护的

页不是静态的，并且页可以被移入或者脱离受保护状态。在一个实施例中，北桥 117 使用 NoDMA 表 103 和 NoDMA 高速缓存 109 来实施例该系统。NoDMA 高速缓存 109 有利于 I/O 性能。在一个实施例中，对存储器 101 的 NoDMA 表 103 区域的 I/O 访问总是被拒绝，即使当该 NoDMA 表 103 被禁用时。任何访问系统存储器 101 的这一区域的尝试都会引起错误，被北桥 117 芯片组记录并且系统重启。

I/O 源 115 可以是通信控制设备（“南桥”），其控制外设（例如，存储驱动器、调制解调器、网卡以及类似设备）和其它外设或者北桥 117 之间的通信。南桥 115 或者北桥 117 可以具有多个能够被配置成不同宽度的端口的 I/O 单元。I/O 单元能够支持包括 PCI-Express、Hublink (HL)、外围部件互连 (Peripheral Component Interconnect, PCI) 以及类似系统的通信协议。独立的 NoDMA 高速缓存 109 可以为每个 I/O 单元或者所有单元的一个子集所专用以提高 NoDMA 校验的性能。在另一个实施例中，I/O 源 115 可以是直接连接到北桥 117 的一组外设。

图 2 是北桥 117 的框图。该图所图示的结构支持从外设 217 到系统存储器 101 的存储器访问请求以及返回被请求的或者出去的数据。网络或者外围设备 217 通过物理层 215 和链路层 213 与 I/O 单元 250 的进站处理器或逻辑 209 以及出站处理器或逻辑 211 通信。进站处理器 209 从链路层 213 接收存储器访问请求和消息，并将这些消息放置在进站队列 201 中。在一个实施例中，进站队列 201 和出站队列 203 各由若干队列构成，所述若干队列的每一个控制特定类型的消息或请求或者定义的一组请求或消息类型。进站队列控制 207 管理通过队列 201 的数据的移动，队列 201 被 CDB 接口 113 所读取。CDB 接口 113 处理存储器访问请求，并可以生成被发送到出站队列 203 的响应消息（例如，当处理读取操作时）。通过出站队列 203 的数据流由出站队列控制器 205 所控制。

在一个实施例中，根据 PCI-Express、HL、PCI 或者其它类似系统所使用的消息或者存储器访问的类型，存在多个进站和出站队列 201 和 203。出站处理器 211 通过链路层 213 和物理层 215 发送响应数据给外设 217。在一个实施例中，出站逻辑 211 和进站处理器 209 控制来自以不同于北桥



117 的速度运行的 I/O 通信总线的数据传输。

在一个实施例中，CDB 接口 113 和 CDB 107 通过在进站队列 201 中先行而来执行对被请求的存储器的推测式预取。CDB 接口 113 负责向 CDB 做出请求并为这些请求服务。CDB 接口 113 实施对系统存储器 101 5 的访问权利，跟踪到 CDB 107 的未完成的请求，为未完成的 DMA 读取请求服务，执行 DMA 写入，跟踪进站完成情况，中断以及类似功能。

CDB 接口 113 对来自 I/O 设备的存储器访问的访问权利进行检验以确保系统的安全。如果 I/O 设备试图访问存储器中它没有访问权利的区域，则 CDB 接口 113 拒绝该请求的访问。对于存储器读取以及任何需要完成的访问，它发送一个主异常终止（master-abort）响应，向请求者表明该访问 10 无效。对于存储器写入和其它不需要响应的事务，该写入被 CDB 接口 113 的控制逻辑所丢弃。任何一种情况中，此次安全侵犯都会被北桥 117 所记录。

CDB 107 与 CDB 接口 113、存储器总线接口 231、CPU 总线接口 227 15 以及其它接口 229 相互作用以在输入-输出单元 250、处理器总线 119 和存储器总线 121 之间路由和转发数据。在一个实施例中，CDB 107 还控制到系统管理总线（SMBus）、联合测试行动组（JTAG）225 或类似接口的输入和输出。

在一个实施例中，当接收到 SMBus、JTAG 以及类似接口访问时，北 20 桥 117 检验 NoDMA 高速缓存 109 和 NoDMA 表 103。这些接口允许系统管理者或服务人员对系统进行监视和诊断。对来自 SMBus、JTAG 或类似接口的存储器访问的处理类似于外设的存储器访问。来自 SMBus、JTAG 或类似接口的存储器访问被对照 NoDMA 表 103 和 NoDMA 高速缓存 109 来检验。这甚至防止了系统管理者或服务人员避开 OS 的页保护机制而访问具有保密信息的页。在另一个实施例中，北桥 117 可以被配置成使得 25 SMBus、JTAG 以及类似接口访问不被对照 NoDMA 表检验，或者使得可以调节安全级别设置以使能或者禁用对这些接口的 NoDAM 检验。

图 3 是 NoDMA 表高速缓存 109 结构的示图。在一个实施例中，高速缓存 109 减小由于访问系统存储器 101 中的 NoDMA 表 103 而引起的带宽

损失。NoDMA 表 103 和高速缓存 109 使得不再需要存储器映射块来跟踪保密页。在一个实施例中，计算机系统 100 中的存储器访问根据系统高速缓存线大小而被优化。该系统高速缓存是用于对系统存储器的存储器访问的通用高速缓存（general cache）。在一个实施例中，高速缓存线大小为 512 位。

在一个实施例中，NoDMA 高速缓存 109 包括内容可寻址存储器（CAM）结构 301 和保密存储信息结构 302。CAM 结构 301 按“行”存储信息。每一行对应于存储于系统存储器 101 中的 NoDMA 表 103 中的一个条目。在一个实施例中，CAM 结构 301 存储或者固有包括索引 303。该索引通过与高速缓存替代机制结合而被用来识别和替代高速缓存线。在一个实施例中，CAM 结构 301 并不显式地存储索引 303，因为硬件中的逻辑电路知道哪个条目对应于索引。

CAM 结构 301 通过存储在地址标识存储字段 305 中的地址来寻址。

“有效”存储位字段 307 指示该行的条目是否是有效的。如果对应于高速缓存行的页被写入或者被改变，则该有效位将被清除，因为该页的内容已经不再已知并且因此不知道该页中是否存储受保护的信息。

在一个实施例中，CAM 结构 301 还存储高速缓存管理信息，例如最近最少使用位 309（LRU）。CAM301 的这个字段 309 用来跟踪条目的相对时间，使得更早或者不经常使用的条目能够被新近的或者更经常使用的条目所替代。任何高速缓存管理和替代机制可以被用于 NoDMA 高速缓存 109。保密信息存储设备 302 为 NoDMA 表 103 中的每个条目存储两个单独的保密指示符。页保密字段 311 指示存储器 101 的页是否包含受保护信息。页的保密指示符可以是将对应于高速缓存 109 的同一行中 NoDMA 表地址的页的状态（例如，包含受保护的信息）编码的一位或者一组位。

超级页（superpage）保密字段 313 指示被该条目寻址的页所属的一组页是否包括受保护的信息。在一个实施例中，超级页是一组连续的页。超级页的大小可以由操作系统、BIOS 或者类似软件来设置。在一个实施例中，在每个超级页中有 512 页。在一个实施例中，NoDMA 表 103 的位被分组到对应于系统高速缓存线的大小和存储器访问大小的超级页中。超级

页保密指示符 313 可以是单个位或者一组位。在一个实施例中，当在 NoDMA 高速缓存 109 中加入新的条目时计算超级页。与对应于进入高速缓存 109 的新条目的特定页的位一起，检索所有对应于该超级页的位。对这些位进行逻辑“或”以确定单个超级页位的值。在一个实施例中，超级  
5 页用多个位来表示。因此可以通过使用逻辑“或”来计算该超级页以确定对应于各位的超级页的每一个子部。例如 512 连续的页可以由 NoDMA 高速缓存 109 中的四个超级页位来表示，每一个对应一个 128 页的组。可以调节超级页的大小以对应访问的大小。单个超级页或者多个超级页可以对应于高速缓存线访问的大小。在一个实施例中，一组页的大小等于存储器  
10 控制器的内在访问大小。

在一个实施例中，CAM 的地址标识 305 由两部分构成：超级页和超级页中的页偏移量。当 I/O 单元 250 接收到一个访问时，进入的地址要经过 CAM 结构。如果有效位被设置了，则每一行都将该进入的地址与地址标识 305 比较。对于每一行有三种可能的结果。第一种，超级页和页的偏  
15 移量都匹配（并且设置了有效），第二种，只有超级页偏移量匹配进入的地址（并且设置了有效），以及第三种，都不匹配或者有效位没有被设置。最多一行会有第一种结果。在这种情况下，对应的页保密指示符 311 被用来指示存储器访问请求的进入的地址的访问权利。如果进入的地址不能与地址标识 305 的超级页以及页偏移量匹配，则使用超级页偏移量匹配  
20 的高速缓存行。如果超级页保密指示符 313 指示属于该超级页的任何页中都没有秘密，则赋予访问权利。就不需要进一步查询 NoDMA 表 103。但是，如果超级页保密指示符 313 指示超级页中至少一页具有秘密，则北桥 117 访问 NoDMA 表 103 以确定被请求的存储器访问页是否包含秘密。有可能高速缓存 109 中的多个条目会具有匹配的超级页地址标识 305。在这  
25 种情况下，任何超级页匹配的行都能被使用。如果高速缓存 109 中没有行具有匹配的超级页地址，则需要访问 NoDMA 表 103。

在一个实施例中，对 NoDMA 表 103 的使用允许计算机系统 100 扩展而用于大的系统存储器 101（例如大于 4GB）以及动态调整存储器大小（例如，如果存储器是带电插入系统的）。对动态调整存储器大小的支持

和使用超级页以及页，允许改变校验存储器访问中的粒度水平，而不需要系统重启。超级页可以由多个位组成以控制超级页所表示的区段大小的粒度水平。附加的位允许超级页表示存储器的更小的区段，而用于更精确地指示受保护信息的位置。用较少的位来表示的超级页降低了 NoDMA 高速缓存系统的复杂性，特别是超级页指示符的产生。当使用较少的位时逻辑“或”的实现被简化了。这种通过改变表示超级页的位来改变粒度水平允许更大程度的设计定制以满足依赖于系统需要对速度和减少空间的需求。

在一个实施例中，NoDMA 高速缓存 109 和北桥 117 处理一组与 NoDMA 高速缓存 109 功能相关的指令。高速缓存 109 可以被不同的指令所使能或者禁用。使能指令使能对 NoDMA 高速缓存的使用，清除高速缓存 109 中存储条目的所有有效位，并设置北桥 117 和高速缓存寄存器中指示对 NoDMA 高速缓存 109 的使能的状态位。禁用指令将 NoDMA 高速缓存 109 禁用，并清除北桥 117 和高速缓存 109 的寄存器中指示对高速缓存 109 的使能的状态位。当 NoDMA 表 103 被使能时，NoDMA 高速缓存 109 可以被禁用。使无效指令清除高速缓存中所有条目的有效位。

在一个实施例中，一个位或者存储值，例如，超级页位、页位、LRU 位或者类似的存储值通过在合适的字段中存储一个逻辑“1”或者一组逻辑“1”而被“设置”。一个位或者存储值可以通过存储包括逻辑“0”的任何值而在逻辑上被“设置”。所赋的值是结合“设置”操作来定义的。类似地，对一个位或者存储值的“清除”操作可以使用除了“设置”指示符值以外的任何所赋的值。

在一个实施例中，NoDMA 高速缓存 109 由软件来维护，例如操作系统。当允许写操作时，操作系统负责正确地使对 NoDMA 高速缓存 109 中被写入区域的引用无效。在一个实施例中，OS 更新 NoDMA 表 103 以标识保密页。该 OS 还确定当 NoDMA 表 103 或者 NoDMA 高速缓存 109 正在被检验时是否有其它存储器访问正在进行。

图 4 是 NoDMA 高速缓存 109 操作的流程图。在一个实施例中，存储器访问请求由 CDB 107 和 CDB 接口 113 处理（框 401）。CDB 接口 113 检验 NoDMA 高速缓存 109 以确定被请求访问的地址是否存储在高速缓存

109 中。通过使用 CAM 结构 301，被请求的地址与存储在高速缓存 109 中的地址标识 305 比较（框 403）。如果在高速缓存 109 中找到了匹配该被请求的页地址的标识 305，则对应的有效位被检验以确定高速缓存条目是否仍然有效（框 405）。如果有效位被设置，则检验页保密指示符 311（框 409）。如果保密指示符被设置，则拒绝该访问并可记录一次错误（框 417）。如果保密指示符没有被设置，则允许该访问（框 419）。

在一个实施例中，当在高速缓存 109 中没有找到用于被请求页的条目时，则高速缓存 109 被检验以确定受保护的信息是否存储在该超级页中。首先，地址标识 305 被检验以查找对应的超级页条目（框 411）。如果找到条目，则检验其有效性（框 413）。如果找到超级页条目并且在该超级页中没有存储受保护的数据（框 415），则该存储器访问请求被允许继续（框 419）。如果超级页保密指示符 313 被设置，则拒绝该访问并可记录一次错误（框 417）。

在一个实施例中，如果在高速缓存 109 中没有找到被请求的超级页地址或者条目无效，则从存储在系统存储器 101 中的 NoDMA 表 103 检索页保密信息（框 407）。地址标识被存储在一个可用的高速缓存行中，并且清除该行的有效位。从 NoDMA 表 103 被访问的数据然后被存储在 NoDMA 高速缓存 109 中（框 421）。

在高速缓存 109 中创建的条目包括页保密指示符 31 和超级页保密指示符 313。基于对该超级页中的页的逻辑“或”来计算并存储超级页保密指示符 313（框 423）。在一个实施例中，特定的页保密信息将被作为一个条目来检索和存储。在另一个实施例中，条目将对应于超级页中的第一页。在另一个实施例中，条目可以对应于超级页中的任何一页。当条目被创建时，该条目的有效位被设置（框 425）。

当在页中有受保护信息时，存储器访问不被允许（框 417）。根据存储器访问的类型（例如读取或者写入），可以返回错误响应消息（例如，如果读取操作被拒绝，则正常响应消息会被错误响应消息所替代）。错误和被拒绝的访问被记录以被后续分析来确定错误的起因或者确定是否作出了恶意请求或者攻击。在一个实施例中，可以定义产生错误或安全记录的

请求的类型（例如，由操作系统设置）。在一个实施例中，北桥 117 通过记录严重错误并重启来响应来自 NoDMA 高速缓存 109 的访问侵犯。错误包括在不被允许的时候访问具有秘密的页，或者访问 NoDMA 表 103。错误被记录在错误寄存器中。错误寄存器可以为检测到的给定错误映射合适的信号通知方法。错误寄存器不可以被可能请求存储器访问的 I/O 设备所访问。

在一个实施例中 NoDMA 高速缓存 109 以软件来实现（例如，微代码或者更高层次的计算机语言）。软件实现还可以被用来进行对 NoDMA 高速缓存 109 的模拟（simulation）或者仿真（emulation）。软件实现可以被存储 10 在机器可读介质中。“机器可读”介质可以包括能够存储或者传送信息的任何介质。机器可读介质的实例包括 ROM、软盘、CD-ROM、光盘、硬盘、射频（RF）链路或者类似介质。

在以上说明书中，已经参考本发明的具体实施例对其进行了描述。但是，显然可以对其作出各种修改和改变，而不背离所附权利要求中所陈述 15 的本发明的更广泛的精神和范围。因此说明书和附图被视为是说明性的，而不是限制性的。

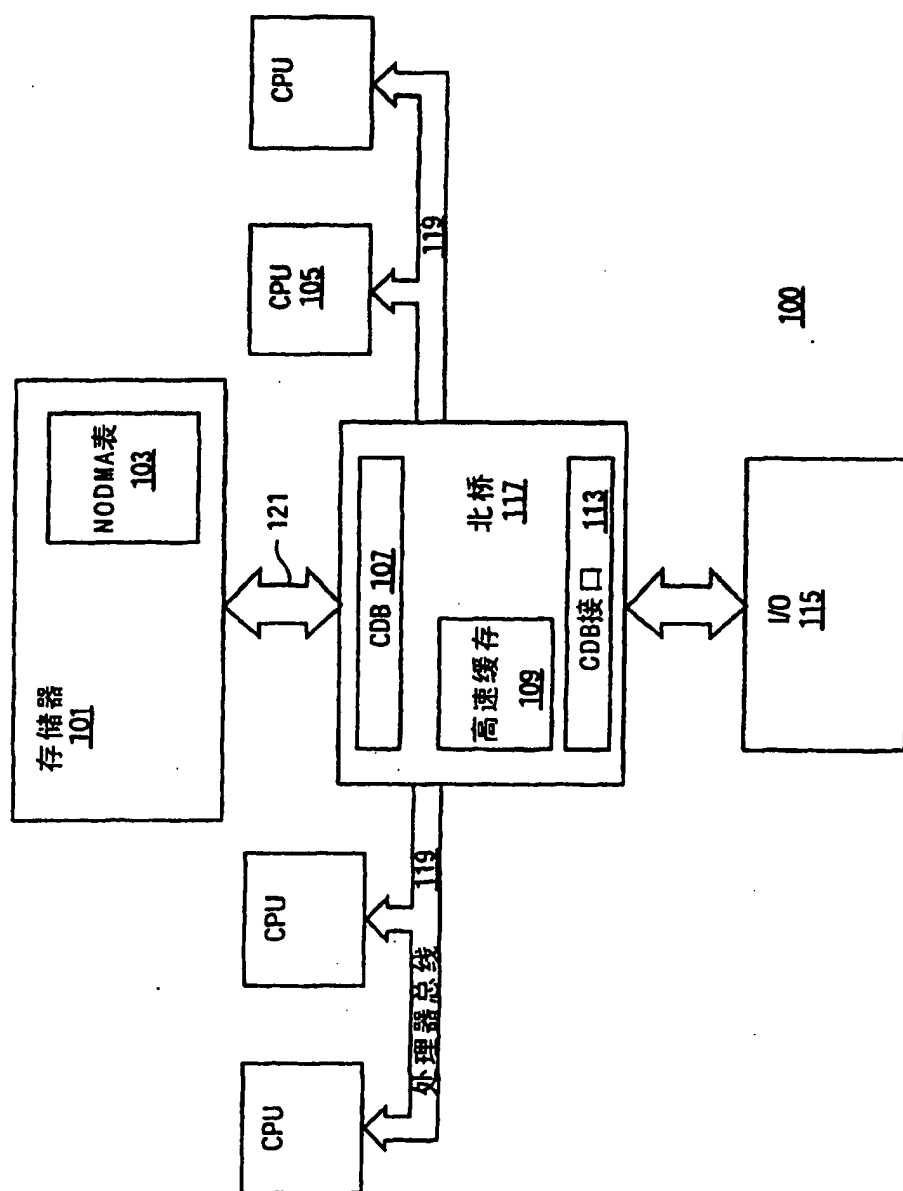


图1

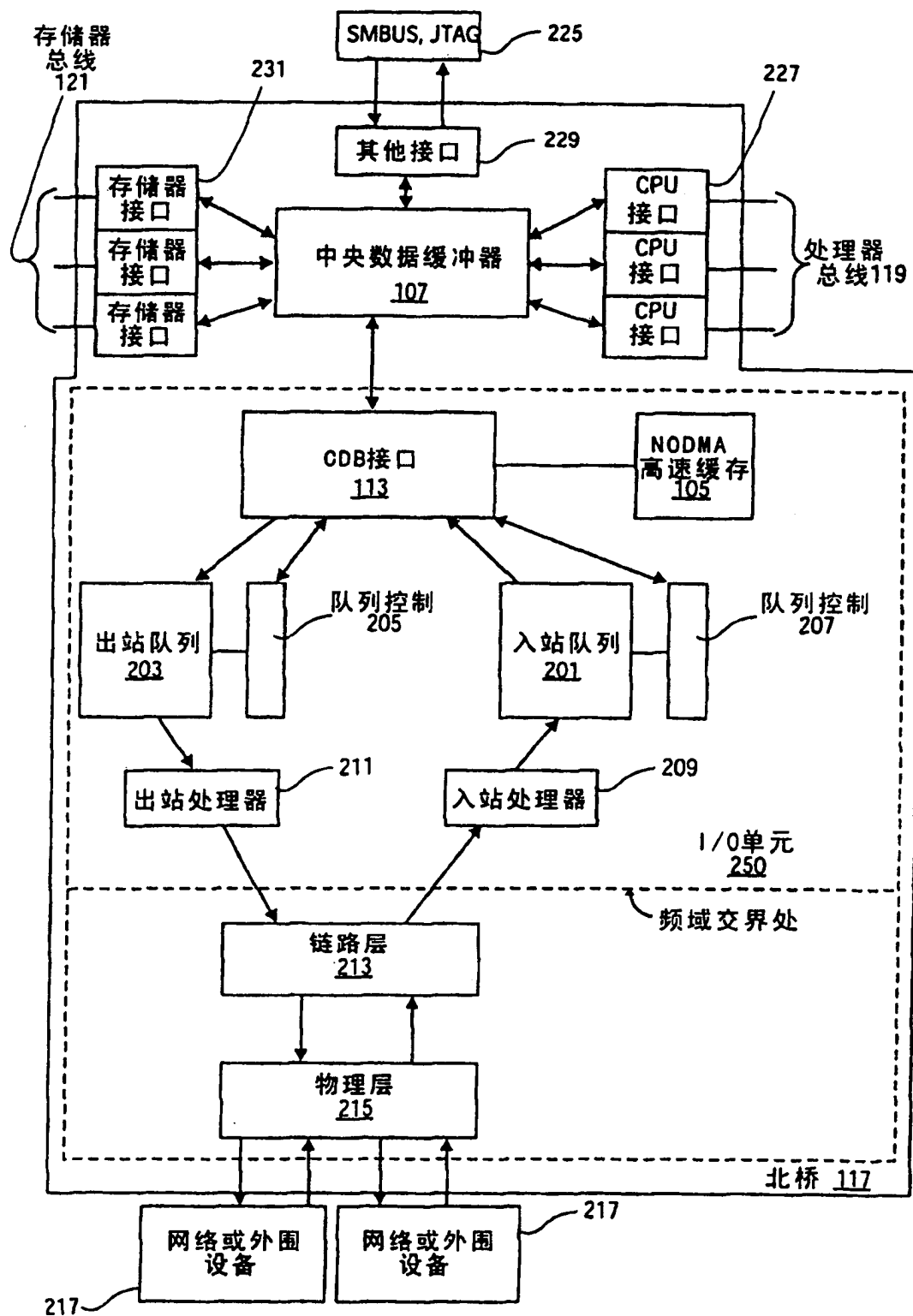


图2



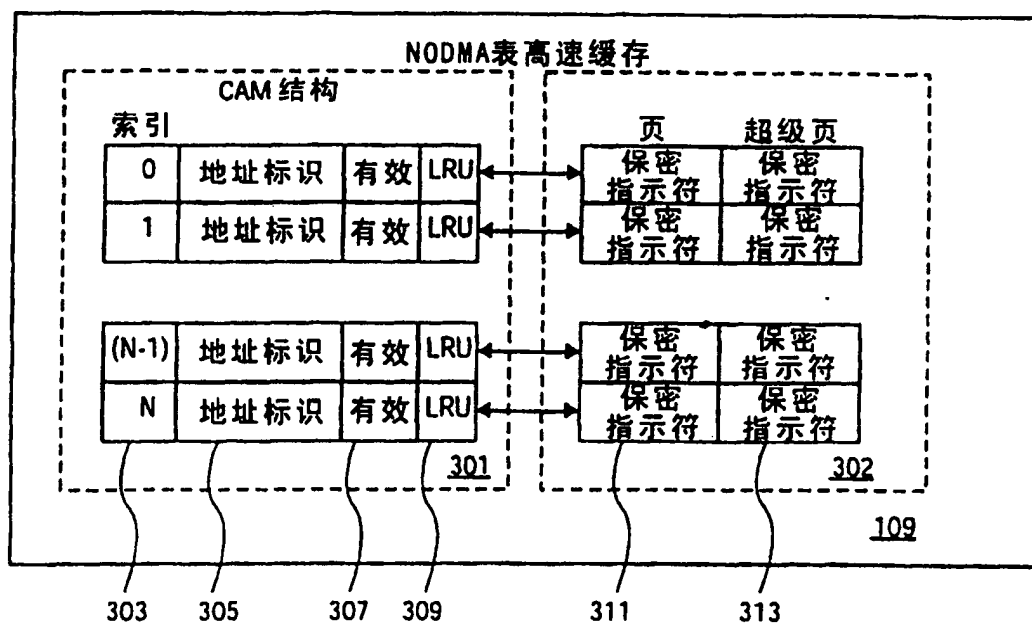


图3

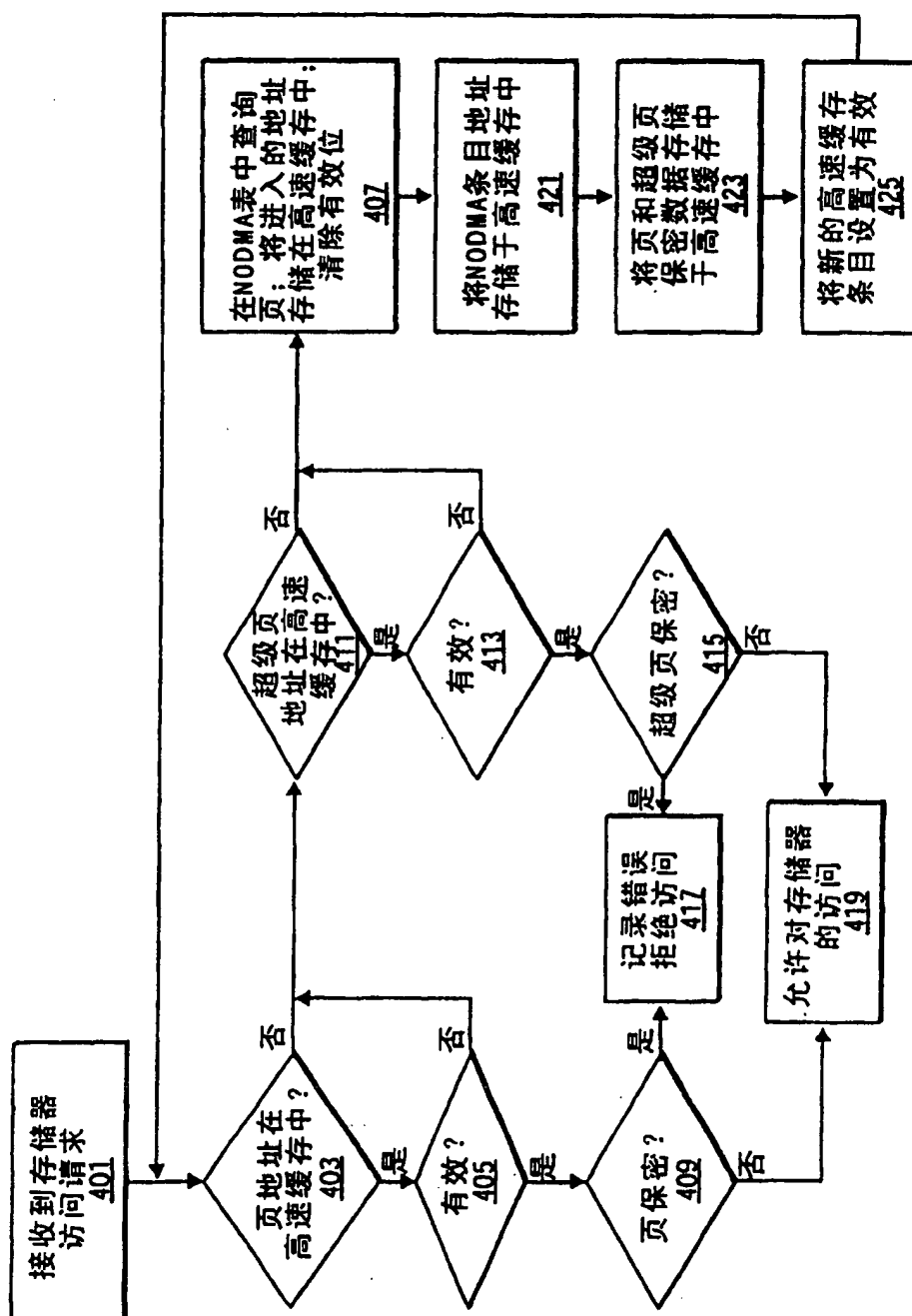


图4