(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년05월21일
(11) 등록번호 10-0831468
(24) 등록일자 2008년05월15일

(51) Int. Cl.
G06F 12/08 (2006.01)
(21) 출원번호 10-2005-7018689
(22) 출원일자 2005년09월30일
심사청구일자 2005년09월30일
번역문제출일자 2005년09월30일
(65) 공개번호 10-2006-0006791
(43) 공개일자 2006년01월19일
(86) 국제출원번호 PCT/US2004/003387
국제출원일자 2004년02월06일
(87) 국제공개번호 WO 2004/095205
국제공개일자 2004년11월04일
(30) 우선권주장
10/404,881 2003년03월31일 미국(US)
(56) 선행기술조사문헌
US05930826A1*
US 5432950 A
US2002/156962 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코오퍼레이션
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
샤르마, 데벤드라 다스
미국 95050 캘리포니아주 산타 클라라 아카시아 코트 2043
사프라네크, 로버트
미국 97229 오레곤주 포트랜드 노스웨스트 네카니컴 와 5816
(74) 대리인
백만기, 이중희, 주성민

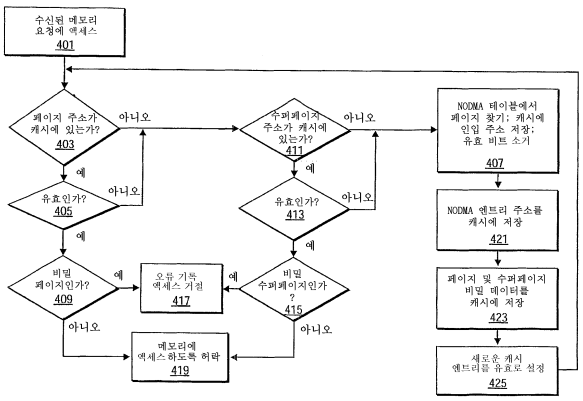
전체 청구항 수 : 총 24 항 심사관 : 이종익

(54) NODMA 캐시

(57) 요 약

수퍼페이지(superpage) 필드를 포함하는 NoDMA 캐시(no direct memory access cache)가 기술된다. 수퍼페이지 필드는 페이지들의 세트가 보호된 정보를 포함하는 때를 표시한다. NoDMA 캐시는 시스템 메모리의 보호된 정보에 대한 I/O 장치의 액세스를 거절하기 위해 컴퓨터 시스템에 의해 사용된다.

대표도 - 도4



특허청구의 범위

청구항 1

메모리에 액세스하기 위한 장치로서,

CAM(content addressable memory);

상기 CAM에 결합되어, 상기 메모리의 제1 세그먼트(segment)에 대한 제1 비밀 표시자(secrecy indicator)를 저장하는 제1 저장 디바이스 -상기 제1 비밀 표시자는 상기 제1 세그먼트가 보호되는 정보를 포함하고 있는지 여부를 표시함-; 및

상기 CAM에 결합되어, 상기 제1 세그먼트를 포함하는 상기 메모리의 세그먼트 수퍼세트(superset)에 대한 제2 비밀 표시자를 저장하는 제2 캐시 저장 디바이스 -상기 제2 비밀 표시자는 세그먼트 수퍼세트가 보호되는 정보를 포함하는지 여부를 표시함-

를 포함하는 메모리에 액세스하기 위한 장치.

청구항 2

제1항에 있어서,

캐시 관리 저장 디바이스를 더 포함하는 메모리에 액세스하기 위한 장치.

청구항 3

제1항에 있어서,

상기 제2 비밀 표시자의 값을 결정하기 위한 회로를 더 포함하는 메모리에 액세스하기 위한 장치.

청구항 4

제1항에 있어서,

상기 제1 세그먼트는 상기 메모리의 한 페이지(page)이고, 상기 메모리는 상기 CAM을 포함하지 않는 메모리에 액세스하기 위한 장치.

청구항 5

제1항에 있어서,

상기 세그먼트 수퍼세트(superset)는 상기 메모리의 한 수퍼페이지(superpage)이고, 상기 메모리는 상기 CAM을 포함하지 않는 메모리에 액세스하기 위한 장치.

청구항 6

제1항에 있어서,

상기 CAM 안에 저장된 데이터를 변경하기 위한 회로를 더 포함하는 메모리에 액세스하기 위한 장치.

청구항 7

메모리에 액세스하기 위한 방법으로서,

상기 메모리에 테이블 엔트리(table entry)에 대한 주소를 저장하는 단계;

상기 메모리의 제1 세그먼트에 대한 제1 비밀 표시자를 저장하는 단계 -상기 제1 비밀 표시자는 상기 제1 세그먼트가 보호되는 정보를 포함하는지 여부를 표시함-; 및

상기 제1 세그먼트를 포함하는 세그먼트 수퍼세트에 대한 제2 비밀 표시자를 캐시에 저장하는 단계 -상기 제2 비밀 표시자는 상기 세그먼트 수퍼세트가 보호되는 정보를 포함하고 있는지 여부를 표시함-

를 포함하는 메모리에 액세스하기 위한 방법.

청구항 8

제7항에 있어서,

메모리 액세스 요청을 수신하는 단계;

저장된 주소와 요청된 주소를 비교하는 단계; 및

제2 비밀 비트가 상기 저장된 주소에 대해 설정되는지 판정하는 단계

를 더 포함하는 메모리에 액세스하기 위한 방법.

청구항 9

제8항에 있어서,

제1 비밀 표시자가 설정되는지를 판정하는 단계를 더 포함하는 메모리에 액세스하기 위한 방법.

청구항 10

제8항에 있어서,

상기 제2 비밀 표시자가 설정된 경우 위반 표시자(violation indicator)를 생성하는 단계를 더 포함하는 메모리에 액세스하기 위한 방법.

청구항 11

제10항에 있어서,

상기 위반 표시자를 기록(logging)하는 단계를 더 포함하는 메모리에 액세스하기 위한 방법.

청구항 12

제8항에 있어서,

상기 세그먼트 수퍼세트는 수퍼페이지인 메모리에 액세스하기 위한 방법.

청구항 13

메모리에 액세스하기 위한 장치로서,

버스;

상기 버스에 결합된 메모리 디바이스;

상기 버스에 결합된 프로세서;

상기 메모리 디바이스에 결합되어, 상기 메모리 디바이스의 제1 세그먼트에 대한 제1 비밀 표시자를 저장하고, 상기 메모리 디바이스의 상기 제1 세그먼트의 수퍼세트에 대한 제2 비밀 표시자를 저장하는 캐시; 및

상기 캐시에 결합된 네트워크 인터페이스 디바이스

를 포함하며, 상기 제1 비밀 표시자는 상기 제1 세그먼트가 보호되는 정보를 포함하는지 여부를 표시하고, 상기 제2 비밀 표시자는 상기 수퍼세트가 보호되는 정보를 포함하는지 여부를 표시하는 메모리에 액세스하기 위한 장치.

청구항 14

제13항에 있어서,

상기 캐시는 캐시 관리 회로를 포함하는 장치.

청구항 15

제13항에 있어서,

상기 제2 비밀 표시자의 값을 결정하기 위한 회로를 더 포함하는 메모리에 액세스하기 위한 장치.

청구항 16

제13항에 있어서,

제2 버스에 결합된 주변 디바이스를 더 포함하고, 상기 제2 버스는 상기 캐시에 결합된 메모리에 액세스하기 위한 장치.

청구항 17

콘텐츠 어드레스가능 저장(content addressable storage)용 수단;

저장 디바이스의 제1 세그먼트에 대한 제1 비밀 표시자를 저장하기 위한 수단 -상기 제1 비밀 표시자를 저장하기 위한 수단은 상기 콘텐츠 어드레스가능 저장용 수단에 결합되며, 상기 제1 비밀 표시자는 상기 제1 세그먼트가 보호되는 정보를 포함하는지 여부를 표시함-; 및

상기 저장 디바이스의 제2 세그먼트에 대한 제2 비밀 표시자를 저장하기 위한 제2 캐시 수단 - 상기 제2 세그먼트는 상기 제1 세그먼트의 수퍼세트이고, 상기 제2 비밀 표시자는 상기 수퍼세트가 보호되는 정보를 포함하는지 여부를 표시함-

을 포함하는 장치.

청구항 18

제17항에 있어서,

캐시 관리를 위한 수단을 더 포함하는 장치.

청구항 19

제17항에 있어서,

상기 제2 비밀 표시자 값을 결정하기 위한 수단을 더 포함하는 장치.

청구항 20

기계에 의해 실행될 때 상기 기계가,

메모리에 테이블 엔트리에 대한 주소를 저장하는 단계;

상기 메모리의 제1 세그먼트에 대한 제1 비밀 표시자를 저장하는 단계 -상기 제1 비밀 표시자는 상기 제1 세그먼트가 보호되는 정보를 포함하는지 여부를 표시함-; 및

상기 제1 세그먼트의 세그먼트 수퍼세트에 대한 제2 비밀 표시자를 캐시에 저장하는 단계 -상기 제2 비밀 표시자는 상기 세그먼트 수퍼세트가 보호되는 정보를 포함하는지 여부를 표시함-

를 포함하는, 메모리에 액세스하기 위한 동작들을 수행하게 하는 명령어들을 제공하는 기계 판독 가능 매체(machine-readable medium).

청구항 21

제20항에 있어서,

상기 제2 비밀 표시자의 값을 결정하는 단계를 더 포함하는 기계 판독 가능 매체.

청구항 22

제20항에 있어서,

상기 제2 비밀 표시자가 설정된 경우 위반 표시자를 생성하는 단계를 더 포함하는 기계 판독 가능 매체.

청구항 23

제1항에 있어서, 상기 제1 저장 디바이스는 랜덤 액세스 메모리(RAM)인 메모리에 액세스하기 위한 장치.

청구항 24

제1항에 있어서, 상기 제1 저장 디바이스는 제2 캐시 저장 디바이스인 메모리에 액세스하기 위한 장치.

명 세 서

기 술 분 야

<1> 본 발명은 I/O 장치들에 의한 부적절한 액세스로부터 민감한 데이터(sensitive data)를 보호하기 위한 보안 장치들에 관련된다, 더 상세하게는, 민감한 데이터를 포함하는 메모리 세그먼트들을 추적(track)하는 NoDMA 테이블을 위한 캐시에 관련된다.

배 경 기 술

<2> 금융 트랜잭션들 및 개인적인 트랜잭션들은 컴퓨팅 장치들에서 증가하는 속도로 수행되고 있다. 그러나, 그러한 금융 트랜잭션들의 수에 있어서 계속되는 성장으로 인해 그러한 트랜잭션들을 지원하는 컴퓨터 시스템들에 대한 증가된 공격들 및 그에 대응하는, 민감한 데이터에 대한 승인되지 않은 액세스 또는 손실을 막기 위한 SE(security enhanced) 환경들에 대한 필요성이 존재한다. 민감한 데이터(예를 들면, 사회 보장 번호들, 계좌 번호들, 금융 데이터, 계정 잔액들, 암호들, 인증키 등)의 손실 또는 승인되지 않은 액세스는 사생활 손실, 개인 금융 데이터 절도 및 유사한 비행들을 초래한다.

<3> 보호된 데이터에 액세스하려고 하는데 사용되는 하나의 기술은 DMA(direct memory access) 컨트롤러를 통한 주변장치들로부터의 메모리 액세스 요청들의 사용이다. DMA 컨트롤러는 네트워크 카드들과 같은 주변 장치들이 CPU(central processing unit)의 최소한의 사용으로 시스템 메모리를 판독하고 기록하게 한다. I/O 장치들로부터의 메모리 액세스 요청들의 사용은 운영 체제에 의해 제공되는 보안 수단들을 회피할 수 있다. 이는, 주변장치에 의해 사용되도록 지정된 시스템 메모리의 세그먼트 바깥에 있는 민감한 정보를 포함하는 메모리 세그먼트들로의 메모리 액세스를 요청함으로써 달성될 수 있다.

발명의 상세한 설명

<9> 도 1은 칩셋("노스 브리지")(117), CPU(105)들의 세트 및 시스템 메모리(101)를 포함하는 컴퓨터 시스템(100)의 일 실시예를 예시한다. 일 실시예에서, CPU들(105)의 세트는 프로세서 버스(119)를 경유하여 노스 브리지(117)에 접속된다. 일 실시예에서, 컴퓨터 시스템(100)은 서버 환경에서 멀티프로세싱(multiprocessing)을 지원하는 다수의 프로세서들(105)을 포함한다. 또 다른 실시예에서, 컴퓨터 시스템(100)은 단일 CPU를 포함할 수 있다. 시스템 메모리(101)는 메모리 버스(121)를 경유해 노스 브리지(117)에 접속된다. 시스템 메모리(101)는 NoDMA 테이블(103)을 포함한다.

<10> 일 실시예에서, 시스템 메모리(101)는 SDRAM(synchronous dynamic random access memory), DDR RAM(double data rate random access memory), 또는 유사한 장치들과 같은 랜덤 액세스 메모리 장치들의 세트이다. 메모리 시스템(101)은 레지스터들 및 유사한 저장 장치들도 포함할 수 있다. NoDMA 테이블(103)은 시스템 메모리(101)에 저장되고, 민감한 데이터를 포함하는 시스템 메모리(101)의 세그먼트를 추적한다. 민감한 데이터는 사회 보장 번호들, 금융 계좌 번호들, 암호들 및 유사한 데이터를 포함할 수 있다.

<11> NoDMA 테이블(103) 데이터는, 민감한 데이터를 포함하는 메모리 세그먼트에 대응하는 NoDMA 테이블(103)의 엔트리(entry)를 플래깅(flagging)하고 비밀 정보에 액세스하도록 인가된 프로그램들만이 메모리(101)의 보호된 구역들에 액세스할 수 있게 함으로써 민감한 정보를 포함하는 메모리 세그먼트들로의 액세스를 제한하도록 OS(operating system)에 의해 사용될 수 있다. 일 실시예에서, 시스템 메모리(101)는 페이지들로 분할된다. 페이지들은 운영 체제에 의해 정해진 것과 같이 크기가 변할 수 있다. 일 실시예에서, 페이지들은 4kbyte 크기이다.

<12> 일 실시예에서, NoDMA 테이블(103)은 각각 메모리(101)의 페이지에 대응하는 비트들의 연속적인 세트로 구성될 수 있다. 만약 어떤 페이지가 민감한 데이터를 포함한다면 운영 체제는 NoDMA 테이블(103)의 그 페이지와 대응하는 비트를 '설정'할 것이다. NoDMA 테이블(103)의 개시 또는 베이스(base)는 시스템 메모리(101)내에 재배치가 가능하다. 일 실시예에서, 운영 체제, BIOS(basic input output system) 또는 유사한 시스템이 NoDMA 테이

블(103)을, 예를 들면 시스템(100)의 부트(boot) 이후에 재배치할 수 있다. NoDMA 테이블(103)은 베이스 레지스터에 저장된 개시 주소에 기초하여 시스템 메모리에 위치된다. NoDMA 테이블(103)은 크기 레지스터에 저장된 데이터에 따라 크기가 정해진다. NoDMA 테이블(103)이 인에이블될 때, I/O 장치에 의한 모든 액세스들은 테이블(103)에 대해 검사되어야 한다.

<13> 일 실시예에서, NoDMA 테이블(103)은 페이지 경계에서 개시하고 페이지 경계에서 종료하도록 정렬된다. 이 정렬은 NoDMA 테이블(103)의 사용을 단순화한다. 또 다른 실시예에서, NoDMA 테이블(103)은 테이블(103)에 대해 충분한 연속 공간을 허용하는 메모리(101)의 임의의 주소에서 개시할 수 있다. NoDMA 테이블(103)의 개시점에서부터 종료점까지의 각 비트는, 보호될 필요가 있는 전체 메모리 주소 공간(address space)을 커버하기 위해 주소 0으로 시작하는 메모리(101)의 각 페이지의 비-CPU 액세스들에 대한 액세스 특권을 나타낸다. 노스 브리지(117)가 특정한 주소에 대한 액세스 권한 특권을 검사할 필요가 있는 경우, 노스 브리지(117)는 NoDMA 테이블(103)의 개시 주소 및 액세스될 페이지의 페이지 주소를 액세스하기 때문에 해당 페이지에 대한 액세스 특권을 쉽게 판정할 수 있다. 그래서, 대응하는 NoDMA 테이블(103) 엔트리는 쉽게 계산되고 액세스될 수 있다.

<14> 일 실시예에서, 노스 브리지(117)는 시스템 메모리(101), CPU들(105) 및 I/O 장치들(115) 사이의 통신을 다룬다. 노스 브리지(117)는 CPU들(105), I/O 장치들 및 소스들(115)로부터의 인입 메모리 액세스 요청들을 처리하는 CDB(central data buffer)를 포함한다. 중앙 제어 블록(CDB 인터페이스)(113)은 인입 메모리 액세스 요청들의 초기 처리 및 인출 요청들의 최종 처리를 다룬다. CDB(107) 또는 CDB 인터페이스(113)에 의해 처리되기를 기다리는 메모리 액세스 요청들은 대기열들에 저장된다. CDB(107) 및 CDB 인터페이스(113)는 I/O 장치들(115)로부터의 메모리 요청들을 처리하고 요청된 데이터를 시스템 메모리(101)로부터 I/O 장치들(115)로 보낸다.

<15> 노스 브리지(117)는 인입 및 인출 메모리 액세스 요청들(예를 들면, 판독 및 기록 요청들)을 저장하는 대기열들의 세트를 포함한다. 일 실시예에서, 대기열들은 FIFOs(first in first out) 대기열들이거나 또는 유사한 대기열 관리 방식을 사용할 수 있다. 노스 브리지(117)는 최근에 요청된 NoDMA 테이블 엔트리들을 저장하는 NoDMA 캐시(109)도 포함할 수 있다. 이 캐시(109)는 메모리(101)에 액세스하기 전에 CDB 인터페이스(113)에 의해 유지되고 사용된다. CDB 인터페이스(113)는 각자의 대기열 내의 인입 및 인출 메시지들도 관리한다. 일 실시예에서, 노스 브리지(117)는 NoDMA 테이블(103) 및 NoDMA 캐시(109)의 기능에 관련된 레지스터들의 세트도 포함한다. 이들 레지스터들은 상태 레지스터들, NoDMA 테이블(103)이 개시하는 메모리(101)의 주소를 나타내는 베이스 주소 레지스터, 및 시스템 메모리(101)의 NoDMA 테이블(103)의 크기를 나타내는 크기 레지스터를 포함한다.

<16> 일 실시예에서, 노스 브리지(117)는 비-CPU 장치들에 의한 액세스로부터 메모리(101)를 보호한다. 보호된 데이터를 포함하는 메모리 세그먼트들은 비-CPU 장치에 의해 판독되거나 기록될 수 없다. 보호된 페이지들은 정적이지 않고 페이지들은 보호된 상태 안팎으로 이동될 수 있다. 일 실시예에서, 이 시스템을 실행하기 위해 노스 브리지(117)는 NoDMA 테이블(103) 및 NoDMA 캐시(109)를 사용한다. NoDMA 캐시(109)는 I/O 성능에서 도움이 된다. 일 실시예에서, NoDMA 테이블(103)이 디스에이블일 때 조차도 메모리(101)의 NoDMA 테이블(103) 영역에 대한 I/O 액세스는 언제나 거절된다. 시스템 메모리(101)의 이러한 영역에 액세스하려는 임의의 시도는 오류를 일으키고, 노스 브리지(117) 칩셋에 의해 기록되고 시스템은 재설정된다.

<17> I/O 소스(115)는 주변장치들(예를 들면, 저장 드라이버들, 모뎀들, 네트워크 카드들 및 유사한 장치들)과 다른 주변장치들 또는 노스 브리지(117) 사이의 통신을 다루는 통신 컨트롤 장치("사우스 브리지")일 수 있다. 사우스 브리지(115) 또는 노스 브리지(117)는 다양한 폭의 포트들을 가지도록 구성될 수 있는 다수의 I/O 유닛들을 가질 수 있다. I/O 유닛들은 PCI-익스프레스(PCI-Express), HL(Hublink), PCI(Peripheral Component Interconnect) 및 유사한 시스템들을 포함하는 통신 프로토콜들을 지원할 수 있다. 독립된 NoDMA 캐시(109)는 NoDMA 검증 성능을 개선시키기 위해 각 I/O 유닛 또는 전체 유닛들의 서브세트에 대해 전용일 수 있다. 또 다른 실시예에서, I/O 소스(115)는 노스 브리지(117)에 직접 접속된 주변 장치들의 세트일 수 있다.

<18> 도 2는 노스 브리지(117)의 블록도이다. 이 도면은 주변 장치(217)로부터 시스템 메모리(101)로의 메모리 액세스 요청 및 요청된 또는 인출 데이터의 반환을 지원하는 구조를 예시한다. 네트워크 또는 주변 장치들(217)은 물리층(215) 및 링크 층(213)을 통해 I/O 유닛(250)의 인바운드 프로세서 또는 로직(209) 및 아웃바운드 프로세서 또는 로직(211)과 통신한다. 인바운드 프로세서(209)는 링크 층(213)으로부터의 메시지들 및 메모리 액세스 요청들을 수신하고 이들 메시지를 인바운드 대기열(201)에 놓는다. 일 실시예에서, 인바운드 대기열(201) 및 아웃바운드 대기열(203)은 각각 특정한 유형의 메시지 또는 요청 또는 메시지 유형들 또는 요청들의 정의된 세

트를 다루는 수많은 대기열들로 각각 이루어진다. 인바운드 대기열 제어(207)는 CDB 인터페이스(113)에 의해 판독되는 대기열(201)을 통한 데이터의 이동을 관리한다. CDB 인터페이스(113)는 메모리 액세스 요청들을 처리하고 아웃바운드 대기열(203)으로 보내지는 응답 메시지를 생성할 수 있다(예를 들면, 판독 작업들을 처리할 때). 아웃바운드 대기열(203)을 통한 데이터흐름은 아웃바운드 대기열 컨트롤러(205)에 의해 제어된다.

<19> 일 실시예에서, PCI-익스프레스, HL, PCI 또는 다른 유사한 시스템들에 의해 사용된 메모리 액세스 유형들 또는 메시지들에 대응하는 다수의 아웃바운드 및 인바운드 대기열(201 및 203)이 존재한다. 아웃바운드 프로세서(211)는 링크 층(213) 및 물리층(215)을 통해 주변 장치(217)로 응답 데이터를 보낸다. 일 실시예에서, 아웃바운드 로직(211) 및 인바운드 프로세서(209)는 노스 브리지(117)와 다른 속도로 동작하는 I/O 통신 버스로부터 오는 데이터의 전송을 다룬다.

<20> 일 실시예에서, CDB 인터페이스(113) 및 CDB(107)는 인바운드 대기열들(201)을 미리 봄으로써, 요청된 메모리의 예측 사전 인출(predictive prefetch)을 수행한다. CDB 인터페이스(113)는 CDB에 요청하는 것과, 그 요청들을 서비스하는 것을 담당한다. CDB 인터페이스(113)는 시스템 메모리에 대한 액세스 권한을 시행하고, CDB(107)에 대한 미해결 요청들을 추적하고, 미해결 DMA 판독 요청들을 서비스하고, DMA 기록들을 수행하고, 인바운드 완료, 인터럽트들 및 유사한 기능들을 추적한다.

<21> CDB 인터페이스(113)는 시스템의 보안을 보장하기 위해 I/O 장치들로부터의 메모리 액세스들에 대해 액세스 권한 검사를 수행한다. 만약 I/O 장치가 액세스 권한이 없는 메모리 영역에 액세스하려 한다면 CDB 인터페이스(113)는 그 요청에 대한 액세스를 거절할 것이다. 완료가 필요한 임의의 액세스에 대해, 액세스가 무효였다고 나타내는 마스터-강제종료(master-abort) 응답을 요청자에게 보낸다. 메모리 기록 및 응답을 필요로 하지 않는 다른 트랜잭션들에 대해, 기록은 CDB 인터페이스(113)의 제어 로직에 의해 드롭된다. 모든 경우에, 보안 위반은 노스 브리지(117)에 의해 기록된다.

<22> CDB(107)는 입력-출력 유닛(Input-Output unit)(250), 프로세서 버스(processor bus)(119), 및 메모리 버스(memory bus)(121) 사이에서 데이터를 라우팅하고 전달하기 위해 CDB 인터페이스(113), 메모리 버스 인터페이스(231), CPU 버스 인터페이스(227) 및 다른 인터페이스들(229)과 상호작용한다. 일 실시예에서, CDB(107)는 SMBus(System Management Bus), JTAG(Joint Test Action Group)(225) 또는 유사한 인터페이스에 대한 입출력도 다룬다.

<23> 일 실시예에서, SMBus, JTAG, 및 유사한 인터페이스 액세스들을 수신하는 경우, 노스 브리지(117)는 NoDMA 캐시(109) 및 NoDMA 테이블(103)을 검사한다. 이러한 인터페이스들은 시스템 관리자들 또는 서비스 요원이 시스템을 모니터하고 진단하게 한다. SMBus, JTAG, 또는 유사한 인터페이스들로부터의 메모리 액세스들은 주변 장치들의 메모리 액세스들과 유사하게 처리된다. SMBus, JTAG, 또는 유사한 인터페이스들로부터의 메모리 액세스들은 NoDMA 테이블(103) 및 NoDMA 캐시(109)에 대해 검사된다. 이는, 심지어 시스템 관리자들 또는 서비스 요원이 OS의 페이지 보호 메카니즘들을 회피하고 비밀 정보가 있는 페이지들에 액세스하는 것을 막는다. 또 다른 실시예에서, SMBus, JTAG 및 유사한 인터페이스 액세스들이 NoDMA 테이블에 대해 검사되지 않도록, 또는 보안 레벨 설정이 이러한 인터페이스들에 대한 NoDMA 검사를 인에이블 또는 디스에이블 할 수 있게 조정될 수 있도록 노스 브리지(117)가 구성될 수 있다.

<24> 도 3은 NoDMA 테이블 캐시(109)의 구조의 도면이다. 일 실시예에서, 캐시(109)는 시스템 메모리(101)의 NoDMA 테이블(103)에 액세스하는 것에 의해 발생되는 대역폭 손실을 감소시킨다. NoDMA 테이블(103) 및 캐시(109)는 비밀 내용이 있는 페이지들을 추적하기 위한 메모리의 블록맵(blockmap)이 필요하지 않다. 일 실시예에서, 컴퓨터 시스템(100)의 메모리 액세스들은 시스템 캐시 라인 크기들에 대해 최적화된다. 메모리에 대한 일반적인 캐시인 시스템 캐시는 시스템 메모리에 액세스한다. 일 실시예에서, 캐시 라인 크기는 512 비트이다.

<25> 일 실시예에서, NoDMA 캐시(109)는 CAM(content addressable memory) 구조(301) 및 비밀 저장 정보 구조(302)를 포함한다. CAM 구조(301)는 정보를 '행들(rows)'에 저장한다. 각 행은 시스템 메모리(101)에 저장된 NoDMA 테이블(103)의 엔트리(예를 들면, 페이지 비밀 표시자(indicator))에 대응한다. 일 실시예에서, CAM 구조(301)는 색인(303)을 저장하거나 원래부터 포함한다. 색인은 캐시 라인들을 식별하고 교체하기 위한 캐시 교체 방식과 연관되어 사용된다. 일 실시예에서, 하드웨어의 로직 회로는 어떤 엔트리가 인덱스에 대응하는지 알기 때문에 CAM 구조(301)는 인덱스(303)를 명시적으로 저장하지 않는다.

<26> CAM 구조(301)는 주소 태그 저장 필드들(305)에 저장된 주소들에 의해 어드레스된다. '유효' 저장 비트 필드(307)는 행에 대한 엔트리가 유효한지 아닌지를 나타낸다. 캐시 행에 대응하는 페이지가 기록되거나 바뀌면 그

후 페이지의 내용들이 더 이상 알려지지 않고 따라서 보호된 정보가 해당 페이지에 저장되는지가 알려지지 않기 때문에 유효 비트가 소거된다.

<27> 일 실시예에서, CAM 구조(301)는 LRU(least recently used)비트(309)와 같은 캐시 관리 정보도 저장한다. CAM(301)의 이 필드(309)는 더 오래되거나 가끔 사용되는 엔트리들이 최근의 또는 더 자주 사용되는 엔트리들로 교체될 수 있도록 엔트리의 상대적인 나이를 추적하는데 사용된다. NoDMA 캐시(109)에 대해 임의의 캐시 관리 및 교체 방식이 사용될 수 있다. 비밀 정보 저장 장치(302)는 NoDMA 테이블(103)의 각 엔트리에 대해 두 개의 개별적인 비밀 표시자들을 저장한다. 페이지 비밀 필드(311)는 메모리(101)의 페이지가 보호된 정보를 포함하는지 여부를 가리킨다. 페이지 비밀 표시자는 캐시(109)의 동일한 행의 NoDMA 테이블 주소에 대응하는 페이지의 상태(예를 들면, '보호된 정보를 포함함')를 인코딩하는 비트 또는 비트들의 세트일 수 있다.

<28> 수퍼페이지 비밀 필드(313)는 엔트리에 의해 어드레스된 페이지가 속하는 페이지들의 세트가 보호된 정보를 포함하는지 여부를 나타낸다. 일 실시예에서, 수퍼페이지는 인접한 페이지들의 세트이다. 수퍼페이지의 크기는 운영 체제, BIOS, 또는 유사한 소프트웨어에 의해 설정될 수 있다. 일 실시예에서, 각 수퍼페이지에는 512 페이지가 있다. 일 실시예에서, NoDMA 테이블(103)의 비트들은 시스템 캐시 라인의 크기 및 메모리 액세스 크기들에 대응하는 수퍼페이지들로 그룹화된다. 수퍼페이지 비밀 표시자(313)는 단일 비트 또는 비트들의 그룹일 수 있다. 일 실시예에서, 새로운 엔트리가 NoDMA 캐시(109)에 만들어질 때 수퍼페이지는 계산된다. 수퍼페이지에 대응하는 모든 비트들은, 캐시(109) 내의 새로운 엔트리에 대응하는 특정한 페이지 비트와 함께 검색된다. 이러한 비트들은 단일 수퍼페이지 비트의 값을 결정하기 위해 논리적으로 "OR" 처리된다. 일 실시예에서, 수퍼페이지는 다수의 비트들로 표현된다. 수퍼페이지는 그 후 각 비트에 대응하는 수퍼페이지의 각 부분구간들을 결정하기 위해 논리적 'OR'을 사용하여 계산된다. 예를 들면 512 연속적인 페이지들은, 각각이 128 페이지들의 세트에 대응하는 NoDMA 캐시(109)의 4개의 수퍼페이지 비트들로 표현될 수 있다. 수퍼페이지 크기들은 액세스들의 크기에 대응하도록 조정될 수 있다. 단일 수퍼페이지 또는 다수의 수퍼페이지들은 캐시 라인 액세스의 크기에 대응할 수 있다. 일 실시예에서, 페이지들의 세트의 크기는 메모리 컨트롤러의 원래의 액세스 크기와 동등하다.

<29> 일 실시예에서, CAM의 주소 태그(305)는 두 부분: 수퍼페이지 및 해당 수퍼페이지 내의 페이지 오프셋으로 구성된다. I/O 유닛(250)이 액세스를 수신할 때, 인입 주소는 CAM 구조를 통해 전달된다. 유효 비트가 설정되면 각 행은 이러한 인입 주소와 주소 태그(305)를 비교한다. 각 행에 대한 3가지 가능한 결과들이 있다. 첫째로, 수퍼페이지 및 페이지 오프셋들이 매치하는 경우(그리고 유효로 설정된 경우), 둘째로, 수퍼페이지 오프셋만 인입 주소와 매치하는 경우(그리고 유효로 설정된 경우), 및, 셋째로, 매치하지 않거나 유효 비트가 설정되지 않은 경우이다. 많아도 하나의 행이 제1 결과를 가질 것이다. 그 경우, 대응하는 페이지 비밀 표시자(311)는 메모리 액세스 요청에 대해 인입 주소에 대한 액세스 권한을 결정하는데 사용된다. 만약 인입 주소가 주소 태그(305)의 수퍼페이지 및 페이지 오프셋들과 매치될 수 없다면, 그 후 수퍼페이지 오프셋과 매치하는 캐시 행이 사용된다. 수퍼페이지 비밀 표시자(313)가 수퍼페이지에 속한 임의의 페이지에 비밀들이 없다는 것을 나타낸다면, 그 후 액세스 권한이 주어진다. NoDMA(103) 테이블을 찾는 것은 더 이상 필요하지 않다. 그러나, 수퍼페이지 비밀 표시자(313)가 수퍼페이지의 적어도 한 페이지가 비밀들을 가진다고 나타낸다면, 그 후 노스 브리지(117)는 요청된 메모리 액세스 페이지가 비밀들을 포함하는지 판정하기 위해 NoDMA 테이블(103)에 액세스한다. 캐시(109)의 다수의 엔트리들이 매치하는 수퍼페이지 주소 태그들(305)를 가질 수 있다. 그러한 상황에서는, 행들과 매치하는 임의의 수퍼페이지가 사용될 수 있다. 캐시(109)의 행들이 매치하는 수퍼페이지 주소를 가지지 않으면, 그 후 NoDMA 테이블(103)이 액세스될 필요가 있다.

<30> 일 실시예에서, NoDMA 테이블(103)의 사용을 통해 컴퓨터 시스템(100)은 (예를 들면, 4GB를 초과하는) 큰 시스템 메모리(101) 및 메모리의 동적 리사이징(resizing)(예를 들면, 메모리가 시스템에 핫 플러깅(hot plugged)되었을 때)에 대해 스케일링 될 수 있다. 메모리의 동적 리사이징에 대한 지원 및 페이지뿐만 아니라 수퍼 페이지의 사용은 시스템 재설정을 요구하지 않고 메모리 액세스들을 검증하는데 있어 다양한 레벨의 세밀도(granularity)를 제공한다. 수퍼페이지는 수퍼페이지가 표현하는 세그먼트 크기의 세밀도 레벨을 제어하기 위한 다수의 비트들로 이루어질 수 있다. 부가적인 비트들은 수퍼페이지들이 더 작은 메모리 세그먼트들을 표현하고 보호된 정보가 위치된 곳의 보다 정확한 표시를 만족시킬 수 있게 한다. 특히 수퍼페이지 표시자의 생성에 있어 더 적은 비트들로 표현된 수퍼페이지는 NoDMA 캐시 시스템의 복잡성을 감소시킨다. 논리적 'OR'의 구현은 더 적은 비트들이 사용될 때 단순해진다. 수퍼페이지를 표현하는 비트들을 변화시킴에 의한 세밀도 레벨의 변화는, 시스템의 니즈에 의존적인 감소된 공간 요구조건들 또는 속도를 위한 보다 큰 맞춤화(customization)를 제공한다.

<31> 일 실시예에서, NoDMA 캐시(109) 및 노스 브리지(117)는 NoDMA 캐시(109)의 기능과 관련된 명령들의 세트를 처리한다. 캐시(109)는 독립된 명령들에 의해 인에이블되거나 디스에이블될 수 있다. 인에이블(enable) 명령은 NoDMA 캐시의 사용을 인에이블시키고, 캐시(109)에 저장된 엔트리들에 대해 모든 유효 비트들을 소거하고, NoDMA 캐시(109)의 인에이블을 나타내는 캐시 레지스터들 및 노스 브리지(117)에 상태 비트들을 설정한다. 디스에이블(disable) 명령은 NoDMA 캐시(109)를 디스에이블시키고 캐시(109)의 인에이블을 나타내는 캐시(109) 및 노스 브리지(117) 레지스터들의 상태 비트들을 소거한다. NoDMA 테이블(103)이 인에이블되는 동안, NoDMA 캐시(109)는 디스에이블될 수 있다. 무효화(invalidate) 명령은 캐시의 모든 엔트리들에 대한 유효 비트들을 소거한다.

<32> 일 실시예에서, 예를 들면, 수퍼페이지 비트, 페이지 비트, LRU 비트 또는 유사한 저장된 값과 같은 비트 또는 저장된 값은 논리 '1' 또는 논리 '1'들의 세트를 적절한 필드에 저장함으로써 '설정'된다. 비트 또는 저장된 값은 논리 '0'을 포함하는 임의의 값을 저장함으로써 논리적으로 '설정'될 수 있다. 지정된 값은 '설정' 작업과 관련하여 정의된다. 마찬가지로, 비트 또는 저장된 값에 대한 '소거(clear)' 작업은 '설정' 표시자 값 이외의 임의의 지정된 값을 사용할 수 있다.

<33> 일 실시예에서, NoDMA 캐시(109)는 운영 체제와 같은 소프트웨어에 의해 유지된다. 기록 작업들이 허용될 때, 운영 체제는 NoDMA 캐시(109)의 기록된 구역들에 대한 참조들을 적절하게 무효화시키는 것을 담당한다. 일 실시예에서, 비밀 페이지들을 식별하기 위해 OS는 NoDMA 테이블(103)을 갱신한다. NoDMA 테이블(103) 또는 NoDMA 캐시(109)가 검사되고 있을 때 OS는 진행 중인 다른 메모리 액세스들이 있는지도 판정한다.

<34> 도 4는 NoDMA 캐시(109)의 작업의 순서도이다. 일 실시예에서, 메모리 액세스 요청들은 CDB(107) 및 CDB 인터페이스(113)에 의해 처리된다(블록 401). 액세스가 요청된 주소가 캐시(109)에 저장되어 있는지 판정하기 위해 CDB 인터페이스(113)는 NoDMA 캐시(109)를 검사한다. 요청된 주소는 CAM 구조(301)의 사용에 의해 캐시(109)에 저장된 주소 태그들(305)과 비교된다(블록 403). 만약 요청된 페이지 주소와 매치하는 태그(305)가 캐시(109)에서 발견되면, 그 후 캐시 엔트리가 여전히 유효한지 판정하기 위해 대응하는 유효 비트가 검사된다(블록 405). 만약 유효 비트가 설정되면, 그 후 페이지 비밀 표시자(311)가 검사된다(블록 409). 만약 비밀 표시자가 설정되면 그 후 액세스가 거절되고 오류가 기록될 수 있다(블록 417). 만약 비밀 표시자가 설정되지 않으면 액세스는 허락된다(블록 419).

<35> 일 실시예에서, 요청된 페이지에 대한 캐시(109)의 엔트리가 발견되지 않을 때, 그 후 보호된 정보가 수퍼페이지에 저장되어 있는지를 판정하기 위해 캐시(109)가 검사된다. 먼저, 대응하는 수퍼페이지 엔트리를 찾기 위해 주소 태그들(305)이 검사된다(블록 411). 만약 엔트리가 발견되면, 그것의 유효성이 검사된다(블록 413). 만약 수퍼페이지 엔트리가 발견되고 보호된 데이터가 수퍼페이지에 저장되어 있지 않으면, 그 후 메모리 액세스 요청이 진행되도록 허락된다(블록 419). 만약 수퍼페이지 비밀 표시자(313)가 설정되어 있으면 그 후 액세스가 거절되고 오류가 기록될 수 있다(블록 417).

<36> 일 실시예에서, 요청된 수퍼페이지 주소가 캐시(109)에서 발견되지 않거나 엔트리가 유효하지 않으면, 그 후 시스템 메모리(101)에 저장된 NoDMA 테이블(103)로부터 페이지 비밀 정보가 검색된다(블록 407). 주소 태그는 가용한 캐시 행에 저장되고 그 행에 대한 유효 비트는 소거된다. 그 후 NoDMA 테이블(103)으로부터 액세스된 데이터는 NoDMA 캐시(109)에 저장된다(블록 421).

<37> 캐시(109)에 만들어진 엔트리는 페이지 비밀 표시자(311) 및 수퍼페이지 비밀 표시자(313)를 포함한다. 수퍼페이지 비밀 표시자(313)는 수퍼페이지 안의 페이지들의 논리적 'OR'에 기초하여 계산되고 저장된다(블록 423). 일 실시예에서, 특정한 페이지 비밀 정보는 엔트리로서 검색되고 저장될 것이다. 또 다른 실시예에서, 엔트리는 수퍼페이지의 제1 페이지에 대응할 것이다. 또 다른 실시예에서, 엔트리는 수퍼페이지의 임의의 페이지에 대응할 수 있다. 엔트리가 만들어질 때 그 엔트리에 대한 유효 비트가 설정된다(블록 425).

<38> 보호된 정보가 페이지에 있을 때 메모리 액세스는 허락되지 않는다(블록 417). 메모리 액세스의 유형(예를 들면, 판독 또는 기록)에 따라 오류 응답 메시지가 반환될 수 있다(예를 들면, 판독 작업이 거절되었다면, 정상 응답 메시지는 오류 응답 메시지로 교체될 것이다). 오류의 원인을 판정하기 위해 또는 악의적인 요청 또는 공격이 있었는지를 판정하기 위해 오류 및 거절된 액세스는 계속해서 분석되도록 기록된다. 일 실시예에서, 오류 또는 보안 기록을 생성하는 요청들의 유형들이 정의될 수 있다(예를 들면, 운영 체제에 의해서 설정된다). 일 실시예에서, 노스 브리지(117)는 치명적인 오류를 기록하고 재설정함으로써 NoDMA 캐시(109)로부터의 액세스 위반에 응답할 수 있다. 오류들은 허용되지 않을 때 비밀들이 있는 페이지에 액세스하는 것, 또는 NoDMA 테이블(103)에 액세스하는 것을 포함한다. 오류들은 오류 레지스터들에 기록된다. 오류 레지스터들은 소정의 검출된

오류에 대해 적절한 신호 방법을 매핑할 수 있다. 오류 레지스터들은 메모리 액세스를 요청하고 있을 수 있는 I/O 장치에 의해 액세스될 수 없다.

<39> 일 실시예에서, NoDMA 캐시(109)는 소프트웨어(예를 들면, 마이크로코드 또는 더 높은 레벨의 컴퓨터 언어들)로 구현된다. 소프트웨어 구현은 NoDMA 캐시(109)의 시뮬레이션들(simulations) 또는 에뮬레이션들(emulations)을 실행하는데도 쓰일 수 있다. 소프트웨어 구현은 기계 판독 가능 매체에 저장될 수 있다. "기계 판독 가능(machine readable)" 매체는 정보를 저장 또는 옮길 수 있는 임의의 매체를 포함할 수 있다. 기계 판독 가능 매체의 예들은 ROM, 플로피 디스켓(floppy diskette), CD-ROM, 광학 디스크, 하드 디스크, RF(radio frequency) 링크, 또는 유사한 매체를 포함한다.

<40> 전술한 명세서에서, 본 발명은 특정한 실시예들과 관련하여 기술되었다. 그러나, 첨부된 청구항들에서 제공되는 본 발명의 보다 넓은 사상 및 범위로부터 벗어나지 않고 다양한 수정들 및 변화들이 만들어질 수 있다는 것이 명백하다. 따라서, 본 명세서 및 도면들은 한정하는 의미라기보다 예시적인 의미로 여겨져야 한다.

도면의 간단한 설명

<4> 본 발명의 실시예들은, 비슷한 참조번호들이 유사한 요소들을 나타내는 첨부 도면들에서 한정이 아닌 예로서 예시된다. 주의할 점은, 본 명세서에서 "한" 또는 "일(one)" 실시예라는 언급들은 반드시 동일한 실시예에 대한 것은 아니며, 그러한 언급들은 적어도 하나를 의미한다는 것이다.

<5> 도 1은 NoDMA(no direct memory access) 캐시를 포함하는 컴퓨터 시스템의 블록도이다.

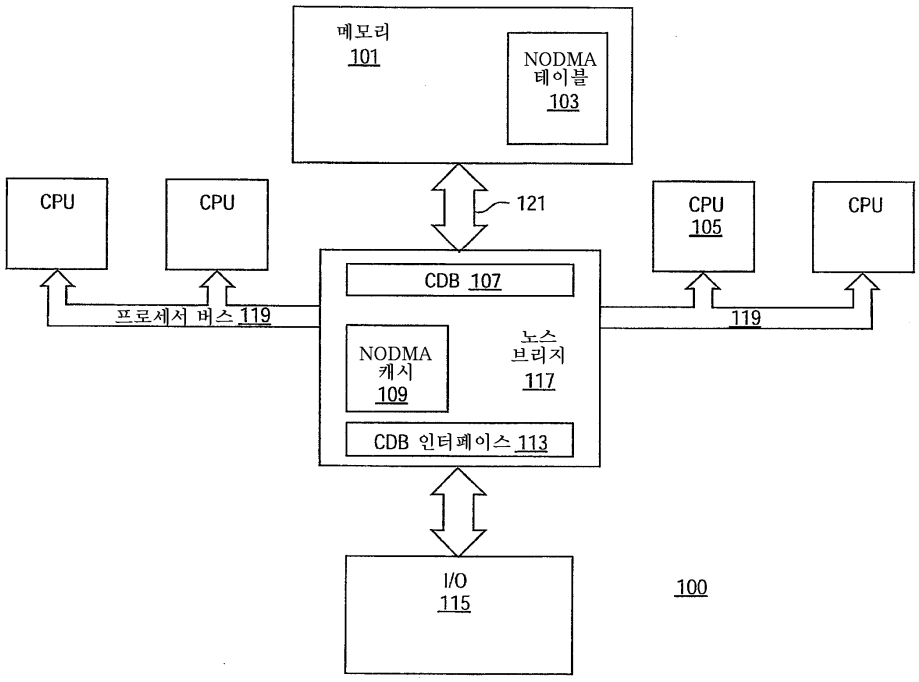
<6> 도 2는 NoDMA를 구현하는 칩셋(chipset)을 통한 입출력 데이터흐름(dataflow)의 블록도이다.

<7> 도 3은 NoDMA 캐시 구조의 도면이다.

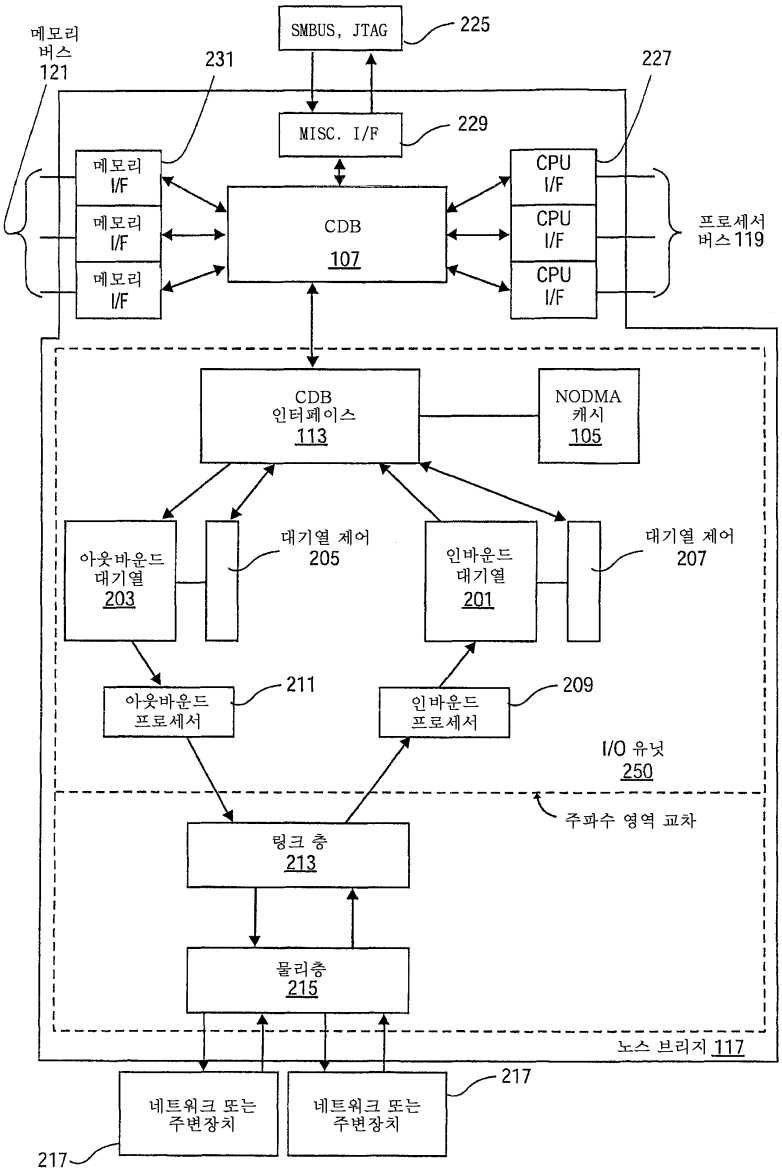
<8> 도 4는 NoDMA 캐시 시스템의 순서도이다.

도면

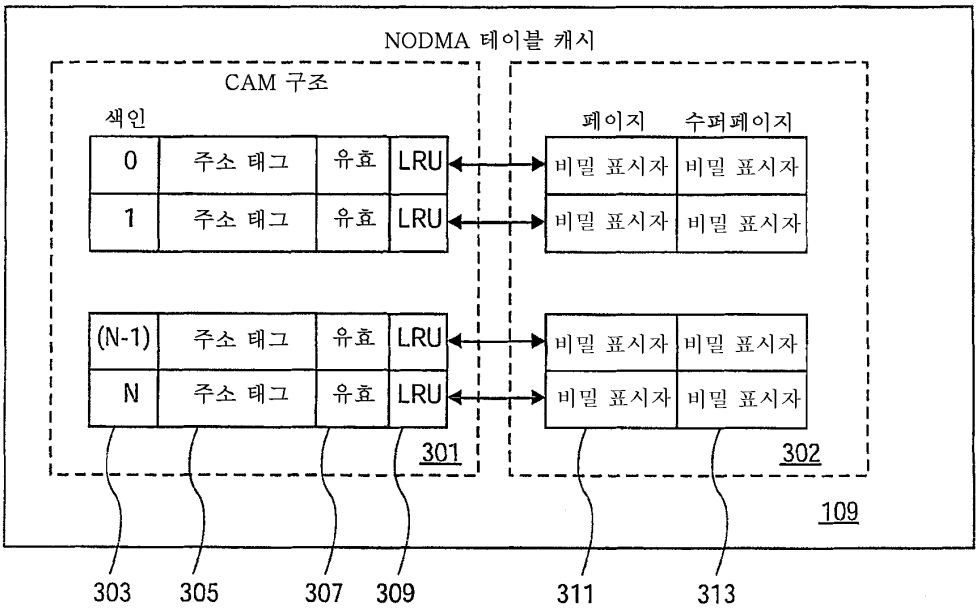
도면1



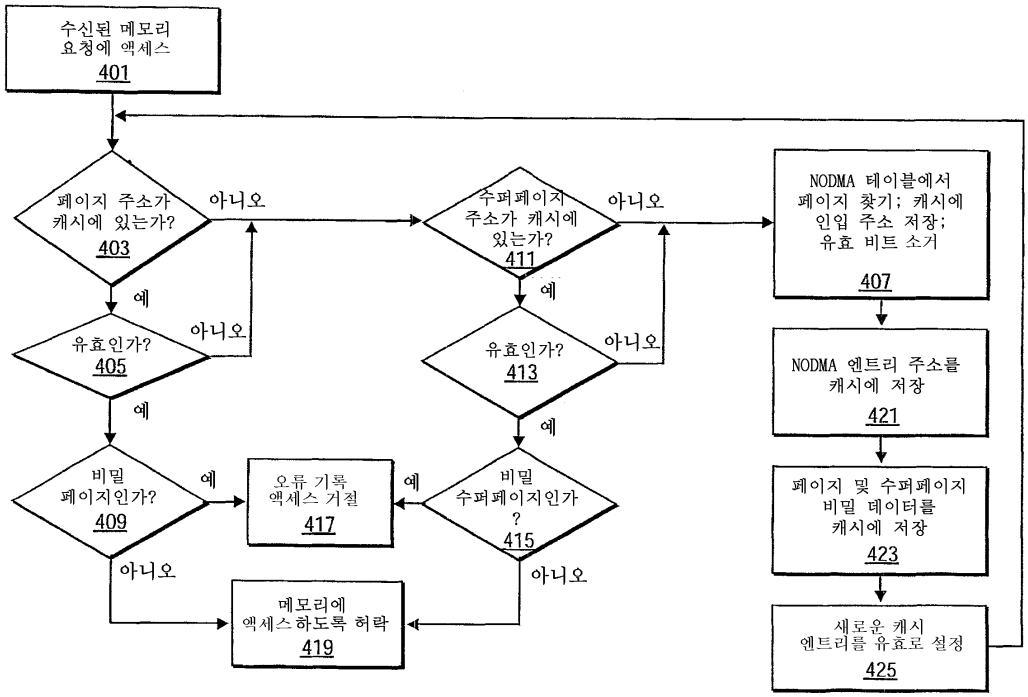
도면2


SMBUS, JTAG
225
메모리 버스 121
231
227
MISC. I/F
229
메모리 I/F
메모리 I/F
메모리 I/F
CDB 107
CPU I/F
CPU I/F
CPU I/F
프로세서 버스 119
CDB 인터페이스 113
NODMA 캐시 105
아웃바운드 대기열 203
대기열 제어 205
인바운드 대기열 201
대기열 제어 207
아웃바운드 프로세서
211
인바운드 프로세서
209
I/O 유닛 250
주파수 영역 교차
링크 층 213
물리층 215
노스 브리지 117
네트워크 또는 주변장치
네트워크 또는 주변장치
217
217

도면3


NODMA 테이블 캐시
CAM 구조
색인
페이지
수퍼페이지
0
주소 태그
유효
LRU
비밀 표시자
비밀 표시자
1
주소 태그
유효
LRU
비밀 표시자
비밀 표시자
(N-1)
주소 태그
유효
LRU
비밀 표시자
비밀 표시자
N
주소 태그
유효
LRU
비밀 표시자
비밀 표시자
301
302
109
303
305
307
309
311
313

도면4


수신된 메모리 요청에 액세스
401
페이지 주소가 캐시에 있는가?
403
아니오
예
유효인가?
405
아니오
예
비밀 페이지인가?
409
예
아니오
오류 기록 액세스 거절
417
메모리에 액세스하도록 허락
419
수퍼페이지 주소가 캐시에 있는가?
411
아니오
예
유효인가?
413
아니오
예
비밀 수퍼페이지인가?
415
예
아니오
NODMA 테이블에서 페이지 찾기; 캐시에 인입 주소 저장; 유효 비트 소거
407
NODMA 엔트리 주소를 캐시에 저장
421
페이지 및 수퍼페이지 비밀 데이터를 캐시에 저장
423
새로운 캐시 엔트리를 유효로 설정
425