(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년01월17일
(11) 등록번호 10-2756992
(24) 등록일자 2025년01월15일

(51) 국제특허분류(Int. Cl.)
G06F 12/14 (2006.01) *G06F 21/60* (2013.01)
G06F 21/79 (2013.01) *G06F 9/30* (2018.01)
(52) CPC특허분류
G06F 12/14 (2013.01)
G06F 21/60 (2013.01)
(21) 출원번호 10-2018-7013380
(22) 출원일자(국제) 2016년09월06일
심사청구일자 2021년08월23일
(85) 번역문제출일자 2018년05월11일
(65) 공개번호 10-2018-0072723
(43) 공개일자 2018년06월29일
(86) 국제출원번호 PCT/GB2016/052736
(87) 국제공개번호 WO 2017/068317
국제공개일자 2017년04월27일
(30) 우선권주장
1518541.6 2015년10월20일 영국(GB)
(56) 선행기술조사문헌
JP62256040 A
(뒷면에 계속)
전체 청구항 수 : 총 19 항

(73) 특허권자
에이알엠 리미티드
영국 캠브리지 씨비1 9엔제이 체리힌톤 풀번로드 110
(72) 발명자
파커 제이슨
영국 셰필드 에스1 4이비 로킹엄 스트리트 152, 로킹엄 코트, 에이알엠 리미티드
그리센드와이트 리차드 로이
영국 캠브리지 씨비1 9엔제이 체리힌톤 풀번로드 110 에이알엠 리미티드
(74) 대리인
이화익

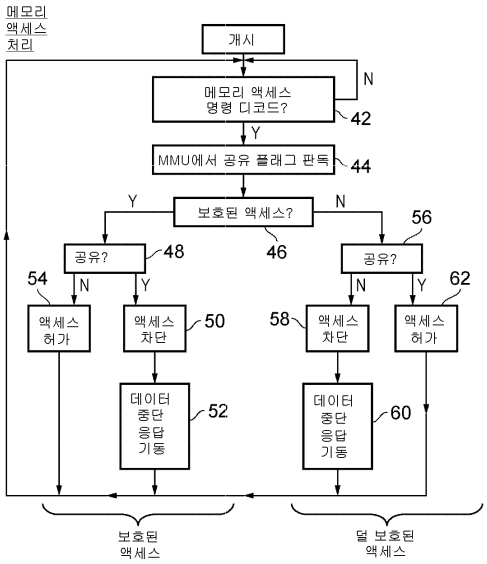
심사관 : 장호근

(54) 발명의 명칭 **메모리 액세스 명령**

(57) 요 약

데이터 처리 시스템(2)은 보호된 메모리 액세스 명령(LDR/STR) 및 덜 보호된 메모리 액세스 명령(LDNPR/STNPR)을 디코드하여 로드 스토어 유닛(120을 제어하기 위한 제어신호를 발생하는 명령 디코더(10)를 구비한다. 덜 보호된 메모리 액세스 명령은 보호된 메모리 액세스 명령보다 덜 제한적인 메모리 액세스 조건과 관련된다. 일례로서, 덜 보호된 메모리 액세스 명령은 공유 메모리 영역(26, 28)을 액세스하기 위해 사용되는 한편, 보호된 메모리 액세스 명령은 이와 같은 공유 영역을 액세스하기 위해 사용되지 않는다. 역으로, 덜 보호된 메모리 액세스 명령은 전용 메모리 영역(30, 32, 34)을 액세스하는데 사용되지 않는다.

대 표 도 - 도5



(52) CPC특허분류
G06F 21/79 (2013.01)
G06F 9/30043 (2013.01)

(56) 선행기술조사문헌
KR1020060002843 A*
US06895508 B1*
US20090172713 A1
US20140108719 A1*
US20150100791 A1*
US20160188337 A1
KR1020060028403 A*
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

프로그램 명령에 의해 지정된 처리 동작을 행하는 처리회로와,

메모리 액세스를 위한 명령을 디코드하여 상기 처리회로가 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 디코더를 구비하고,

상기 메모리 액세스를 위한 명령은,

보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

덜 보호된(less-protected) 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각각의 인코딩을 갖고,

상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리회로는 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리장치.

청구항 2

제 1항에 있어서,

상기 덜 보호된 메모리 액세스를 위한 명령은 상기 보호된 메모리 액세스를 위한 명령과 다른 수의 변종(variant)들을 허용하는 인코딩을 갖는 데이터 처리장치.

청구항 3

제 2항에 있어서,

상기 덜 보호된 메모리 액세스를 위한 명령은 상기 보호된 메모리 액세스를 위한 명령보다 적은 수의 변종들을 허용하는 인코딩을 갖는 데이터 처리장치.

청구항 4

제 1항, 제 2항 또는 제 3항 중 어느 한 항에 있어서,

메모리 보호 데이터에 따라 메모리 어드레스 공간의 영역들에 대한 액세스를 제어하는 메모리 액세스 제어회로를 구비하고, 상기 메모리 보호 데이터는, 상기 보호된 메모리 액세스를 위한 명령보다 상기 덜 보호된 메모리 액세스를 위한 명령에 대해 메모리 액세스를 위한 덜 제한적인 조건을 실행하기 위해 상기 메모리 액세스 제어회로에 의해 주어진 적어도 한 개의 속성을 포함하는 데이터 처리장치.

청구항 5

제 4항에 있어서,

상기 적어도 한 개의 속성은 메모리 어드레스가 공유 메모리 어드레스인 시기를 나타내고,

상기 메모리 액세스 제어회로는 상기 보호된 메모리 액세스를 위한 명령에 의해 상기 공유 메모리 어드레스에 대한 메모리 액세스를 차단하고,

상기 메모리 액세스 제어회로는, 상기 덜 보호된 메모리 액세스를 위한 명령에 의한 상기 공유 메모리 어드레스에 대한 메모리 액세스를 허가하는 데이터 처리장치.

청구항 6

제 5항에 있어서,

상기 적어도 한 개의 속성은 메모리 어드레스가 전용 메모리 어드레스인 시기를 나타내고,

상기 메모리 액세스 제어회로는 상기 보호된 메모리 액세스를 위한 명령에 의해 상기 전용 메모리 어드레스에 대한 메모리 액세스를 허가하고,

상기 메모리 액세스 제어회로는, 상기 덜 보호된 메모리 액세스를 위한 명령에 의한 상기 전용 메모리 어드레스에 대한 메모리 액세스를 차단하는 데이터 처리장치.

청구항 7

제 5항에 있어서,

상기 메모리 액세스 제어회로는 보호된 메모리 액세스를 위한 명령에 의한 상기 공유 메모리 어드레스에 대한 시도된 메모리 액세스에 응답하여 데이터 중단 응답을 기동하는 데이터 처리장치.

청구항 8

제 5항에 있어서,

상기 메모리 액세스 제어회로는 덜 보호된 메모리 액세스를 위한 명령에 의한 공유 메모리 어드레스 이외에 대한 시도된 메모리 액세스에 응답하여 데이터 중단 응답을 기동하는 데이터 처리장치.

청구항 9

제 4항에 있어서,

상기 메모리 액세스 제어회로는 메모리 관리 유닛이고, 상기 메모리 보호 데이터는 메모리 페이지 테이블 데이터인 데이터 처리장치.

청구항 10

제 4항에 있어서,

상기 메모리 액세스 제어회로는 메모리 보호 유닛이고, 상기 메모리 보호 데이터는 상기 메모리 보호 유닛을 제어하기 위한 허가 데이터인 데이터 처리장치.

청구항 11

제 1항 내지 제 3항 중 어느 한 항에 있어서,

상기 보호된 메모리 액세스를 위한 동작에 의해 메모리에 기억된 데이터를 암호화하고 상기 보호된 메모리 액세스를 위한 동작에 의해 상기 메모리에서 판독된 데이터를 복호화하는 암호화 회로를 구비한 데이터 처리장치.

청구항 12

제 1항 내지 제 3항 중 어느 한 항에 있어서,

메모리에 기억된 데이터를 암호화하고 상기 메모리에서 판독된 데이터를 복호화하는 암호화 회로를 구비하고, 상기 암호화 회로는 상기 보호된 메모리 액세스를 위한 동작에 대해서는 활성이고, 상기 암호화 회로는 상기 덜 보호된 메모리 액세스를 위한 동작에 대해서는 비활성인 데이터 처리장치.

청구항 13

삭제

청구항 14

제 1항 내지 제 3항 중 어느 한 항에 있어서,

상기 처리 동작은,

복수의 프로그램을 실행하는 것과,

상기 복수의 프로그램 중에서 상기 다른 프로그램 내부의 보호된 메모리 액세스를 위한 명령을 실행하여 상기 다른 프로그램에 대해 전용인 메모리 어드레스를 액세스하는 것과,

상기 복수의 프로그램 중에서 상기 다른 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령을 실행하여 상기 복수의 프로그램 사이에서 공유된 메모리 어드레스를 액세스하는 것을 포함하는 데이터 처리장치.

청구항 15

제 14항에 있어서,

상기 복수의 프로그램은 특권 프로그램과 상기 특권 프로그램에 의해 제공된 실행 환경을 이용하여 실행되는 적어도 한 개의 또 다른 프로그램을 포함하고, 상기 적어도 한 개의 또 다른 프로그램은 보호된 메모리 액세스를 위한 명령을 이용하여 상기 특권 프로그램으로부터 전용의 메모리 어드레스를 액세스하는 데이터 처리장치.

청구항 16

제 15항에 있어서,

상기 특권 프로그램은 하이퍼바이저 프로그램이고, 상기 적어도 한 개의 또 다른 프로그램은 운영체계 프로그램인 데이터 처리장치.

청구항 17

제 15항에 있어서,

상기 특권 프로그램은 운영체계 프로그램이고, 상기 적어도 한 개의 또 다른 프로그램은 어플리케이션 프로그램인 데이터 처리장치.

청구항 18

프로그램 명령에 의해 지정된 처리 동작을 행하는 처리수단과,

메모리 액세스를 위한 명령을 디코드하여 상기 처리수단이 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 디코더수단을 구비하고,

상기 메모리 액세스를 위한 명령은,

보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

덜 보호된 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각각의 인코딩을 갖고,

상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리수단은 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리장치.

청구항 19

메모리 액세스를 위한 명령을 디코드하여 처리회로가 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 단계를 포함하고,

상기 메모리 액세스를 위한 명령은,

보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

덜 보호된 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각각의 인코딩을 갖고,

상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리회로는 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리방법.

청구항 20

청구항 1 내지 3 중 어느 한 항에 기재된 장치에 대응하는 가상머신 실행 환경을 제공하도록 컴퓨터를 제어하기

위해 비일시적인 기억매체에 기억된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 데이터 처리 시스템 분야에 관한 것이다. 특히, 본 발명은 데이터 처리 시스템 내부의 메모리 액세스 명령들과 이들 메모리 액세스 명령들과 관련된 액세스 조건에 관한 것이다.

배 경 기 술

[0002] 디코드되었을 때 메모리와 프로세서 코어 사이에서 데이터 로드 또는 데이터 스토어 등의 메모리 액세스 동작을 행하는 역할을 하는 메모리 액세스 명령을 데이터 처리 시스템에 설치하는 것이 알려져 있다. 이와 같은 시스템 내부에서 메모리 액세스 조건을 관리하기 위해, 메모리 액세스를 제어하는데 사용되는 허가 데이터를 사용하여 프로그래밍되는 메모리 관리 유닛 또는 메모리 보호 유닛 등의 하드웨어를 설치하는 것이 알려져 있으며, 예를 들어, 특정한 메모리 어드레스 또는 메모리 어드레스들의 범위가 판독 전용, 판독/기록, 특권 액세스 전용 등으로 표기된다.

발명의 내용

과제의 해결 수단

[0003] 본 발명의 적어도 일부 실시예는,

[0004] 프로그램 명령에 의해 지정된 처리 동작을 행하는 처리회로와,

[0005] 메모리 액세스를 위한 명령을 디코드하여 상기 처리회로가 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 디코더를 구비하고,

[0006] 상기 메모리 액세스를 위한 명령은,

[0007] 보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

[0008] 덜 보호된(less-protected) 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각각의 인코딩을 갖고,

[0009] 상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리회로는 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리장치를 제공한다.

[0010] 본 발명의 적어도 일부 실시예는,

[0011] 프로그램 명령에 의해 지정된 처리 동작을 행하는 처리수단과,

[0012] 메모리 액세스를 위한 명령을 디코드하여 상기 처리수단이 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 디코더수단을 구비하고,

[0013] 상기 메모리 액세스를 위한 명령은,

[0014] 보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

[0015] 덜 보호된 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각

각의 인코딩을 갖고,

[0016] 상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리수단은 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리장치를 제공한다.

[0017] 본 발명의 적어도 일부 실시예는,

[0018] 메모리 액세스를 위한 명령을 디코드하여 처리회로가 메모리 액세스를 위한 동작을 행하도록 제어하는 제어신호를 발생하는 단계를 포함하고,

[0019] 상기 메모리 액세스를 위한 명령은,

[0020] 보호된 메모리 액세스를 위한 동작에 대응하는 보호된 메모리 액세스를 위한 명령과,

[0021] 덜 보호된 메모리 액세스를 위한 동작에 대응하는 덜 보호된 메모리 액세스를 위한 명령을 지정하는 각각의 인코딩을 갖고,

[0022] 상기 덜 보호된 메모리 액세스를 위한 동작은 상기 보호된 메모리 액세스를 위한 동작보다 메모리 액세스를 위한 덜 제한적인 조건과 관련되고,

상기 처리회로는 더 낮은 예외 레벨 상태들과 더 높은 예외 레벨 상태들을 포함하는 복수의 예외 레벨 상태들을 갖고,

상기 복수의 예외 레벨 상태들 내부의 예외 레벨 상태에서 실행되는 프로그램 내부의 덜 보호된 메모리 액세스를 위한 명령으로 액세스되는 메모리 어드레스는 상기 복수의 예외 레벨 상태들 내부의 상기 더 높은 예외 레벨 상태들에서 실행되는 프로그램들과 공유되고,

상기 복수의 예외 레벨 상태들 내부의 다른 예외 레벨 상태에서 실행되는 다른 프로그램 내부의 보호된 메모리 액세스를 위한 다른 명령으로 액세스되는 다른 메모리 어드레스는 다른 프로그램에 대해 전용이 되는 데이터 처리방법을 제공한다.

도면의 간단한 설명

[0023] 이하, 다음의 첨부도면을 참조하여 실시예를 설명한다.

도 1은 데이터 처리 시스템을 개략적으로 나타낸 것이다.

도 2는 보호된 메모리 액세스 명령과 덜 보호된 메모리 액세스 명령을 개략적으로 나타낸 것이다.

도 3은 도 2의 메모리 액세스 명령에 대한 명령 인코딩을 개략적으로 나타낸 것이다.

도 4는 공유/전용 플래그를 포함하는 메모리 관리 유닛 페이지 엔트리를 개략적으로 나타낸 것이다.

도 5는 메모리 액세스 처리를 개략적으로 나타낸 흐름도이다.

도 6은 메모리의 영역들로 데이터를 암호화하는 암호화 회로를 포함하는 또 다른 실시예를 개략적으로 나타낸 것이다.

도 7은 서로 다른 예외 레벨에서 실행되는 특권화된 프로그램과 덜 특권화된 프로그램의 계층구조를 개략적으로 나타낸 것이다.

도 8은 메모리 시스템 계층 내의 복수의 층과 암호화 회로를 포함하는 데이터 처리 시스템의 또 다른

실시예를 개략적으로 나타낸 것이다.

발명을 실시하기 위한 구체적인 내용

[0024] 도 1은 프로세서(4)와 메모리(6)를 포함하는 데이터 처리 시스템(2)을 개략적으로 나타낸 것이다. 프로세서 코어(4)는 명령 페치 유닛(8), 디코더(10), 로드 스토어 유닛(12), 메모리 관리 유닛(14), 레지스터 뱅크(16)와, 승산기(18), 시프터(20) 및 가산기(22)를 포함하는 산술 처리회로를 구비한다. 동작시에, 명령 페치 유닛(8)은 메모리(6)에서 프로그램 명령을 페치하여 이것을 디코더(10)에 전달한다. 디코더(10)는 프로그램 명령을 디코드하여 제어신호를 발생하며, 이 제어신호는 그후에 로드 스토어 유닛(12) 및 산술 처리회로들(18, 20, 22) 등의 처리회로의 다른 구성요소에 의해 행해지는 처리 연산을 제어한다.

[0025] 레지스터 뱅크(16) 내부의 레지스터와 메모리(6) 내부의 메모리 어드레스 사이에서의 로드 명령 및 스토어 명령으로부터 발생된 메모리 액세스 동작은 로드 스토어 유닛(12)에 의해 행해진다. 디코더(10)에 의해 발생된 제어신호는 로드 스토어 유닛(12)을 제어하여 디코드된 메모리 액세스 명령에 의해 지정된 메모리 액세스 동작을 행한다. 메모리 관리 유닛(14)은 메모리(6) 내부에 기억된 페이지 테이블 데이터(24)를 사용하여 메모리 내부의 메모리 어드레스(또는 메모리 페이지 등의 메모리 어드레스들의 영역)와 관련된 액세스 조건을 실시한다. 이들 메모리 액세스 조건은, 특정한 메모리 어드레스가 판독하기 위해 액세스 가능하거나, 기록하기 위해 액세스 불가능하거나, 캐시에 기억가능하거나, 특정한 특권 레벨(특정한 예외 레벨)에게만 액세스 가능하거나, 또는 다른 속성인 것을 포함한다.

[0026] 메모리(6)는 본 실시예에서 나타낸 것과 같이 복수의 영역 내부에 데이터를 기억한다. 이들 영역은 공유 영역 26, 28과 전용 영역 30, 32, 34를 포함한다. 공유 영역 26, 28은 프로그램들 사이에서 공유되므로, 프로그램들 사이에서 데이터의 공유/교환을 용이하게 한다. 전용 영역 30, 32, 34는 특정한 프로그램 전용이다. 전용 영역 30, 32, 34에 대한 전용 액세스를 갖는 프로그램보다 더 높은 특권 레벨을 갖는 프로그램들에 대해 이와 같은 프라이버시가 실시된다. 따라서, 어플리케이션 프로그램은, 이 어플리케이션 프로그램이 액세스 가능하지만, 위에 놓이는 운용체계 또는 더 낮은 특권 레벨(예외 레벨)에 있는 프로그램에 대해 실행 환경을 제공하고 있는 하이퍼바이저 프로그램 등과 같이, 더 높은 특권 레벨(예외 레벨)에서 동작하고 있는 프로그램이 액세스 불가능한 전용 메모리 영역 30, 32, 34를 갖는다.

[0027] 도 1에 도시된 예는 메모리 관리 유닛(14)과 페이지 테이블 데이터(24)를 이용한다. 이때, 다른 실시예는, 메모리 액세스 공간 내부의 메모리 보호 영역들과 관련된 액세스 조건을 적용하는 메모리 보호 유닛 등의 다른 메모리 액세스 제어회로를 이용할 수도 있다는 것은 본 기술분야의 당업자에게 있어서 자명할 것이다.

[0028] 메모리 관리 유닛(및 메모리 보호 유닛)의 사용과 관련된 잠재적인 보안 취약성은, 페이지 테이블 데이터(24)(또는 메모리 영역과 메모리 보호 유닛의 보호를 정의하는 데이터)에 대한 잘못되거나 악의적인 변경이 공유로서 처리되는 것 대신에 전용으로 처리되고 액세스가 다른 어플리케이션 프로그램에 부적절하게 주어지는 메모리 영역 30, 32, 34를 제공할 수도 있다는 것이다. 이와 같은 전용 영역 30, 32, 34는 암호 키, 금융 데이터 등의 민감한 데이터를 포함해도 된다.

[0029] 본 실시예에 따라 제공된 메모리 액세스 명령은 보호된 로드 명령 LDR, 또는 보호된 스토어 명령 STR 등의 보호된 메모리 액세스 명령의 형태를 취한다. 메모리 액세스 명령은 덜 보호된 로드 명령 LDNPR 또는 덜 보호된 스토어 명령 STNPR 등의 덜 보호된 메모리 액세스 명령을 더 포함한다. 이들은 그 자신의 명령 인코딩을 갖는 별개의 종류의 명령이다. 한가지 종류의 인코딩의 모든 변종(variant)이 다른 종류의 인코딩을 위해 제공될 필요는 없다. 본 실시예에서, 보호된 메모리 액세스 명령은 덜 보호된 메모리 액세스 명령보다 인코딩에서 더 많은 변종을 갖는데, 예를 들어, 보호된 메모리 액세스 명령은, 데이터 값 크기, 부호를 갖는/부호를 갖지 않는 데이터, 메모리 어드레스에 적용할 색인(indexing) 및 기타 옵션의 지정을 허용하는 옵션을 갖는다. 이에 비해, 덜 보호된 메모리 액세스 명령은 데이터 크기 및 부호를 갖는/부호를 갖지 않는 데이터 등과 같이 더 적은 옵션을 갖는다.

[0030] 다양한 종류의 메모리 액세스 명령의 설치는 프로그래머(또는 컴파일러)가 디폴트로 보호된 메모리 액세스 명령을 사용하고, 그후 프로그래머가 알기에는 덜 제한된 메모리 액세스 조건을 안전하게 겪는 특정한 메모리 액세스 동작에 대해서는 덜 보호된 메모리 액세스 명령의 사용을 선택할 수 있도록 한다. 예를 들어, 보호된 메모리 액세스 명령은, 프로그래머에 의해 메모리(6) 내부의 공유 영역 26, 28에 대해 행해지도록 정의된 것으로 알려진 것 이외의 모든 메모리 액세스에 대해 디폴트로 사용된다. 공유 영역에 대한 이들 메모리 액세스는 덜 보호된 메모리 액세스 명령을 사용해도 된다. 프로그래머는 프로그램 코드의 작성시에 특정한 데이터가 다른 어플리

케이션 프로그램과 공유되어야 하며 공유 영역 26, 28에 기록되어야 하므로, 이와 같은 메모리 액세스가 덜 보호된 메모리 액세스 명령을 이용하여 행해지는 것이 적절하다는 것을 알게 된다. 이에 따라, 메모리 관리 유닛(14)(또는 메모리 보호 유닛)을 제어하는 데이터가 틀리더라도, 더 제한된 메모리 액세스 조건을 갖는 보호된 메모리 명령의 사용은 프로그래머가 공유 영역 26, 28에 부주의하게 데이터를 기억하는 것을 방지하고 공유 영역 26, 28로부터 부주의하게 (변경된) 데이터를 로드하는 것을 방지하는 역할을 한다.

[0031] 도 3은 보호된 메모리 액세스 명령 LDR/STR 및 덜 보호된 메모리 액세스 명령 LDNPR/STNPR 모두에 대한 인코딩의 예를 개략적으로 나타낸 것이다. 이들 명령은 다른 인코딩(옵코드)을 가지므로, 디코더(10)에 의해 다른 종류의 명령으로 인식되어, 로드 스토어 유닛(120을 제어하여 후술하는 것과 같이 이들 서로 다른 종류의 명령에 대해 서로 다르게 거동하도록 하기 위해 서로 다른 제어신호를 발생한다. 보호된 메모리 액세스 명령 LDR, STR은 도시된 것과 같이 덜 보호된 메모리 명령 LDNPR/STNPR보다 명령과 관련된 크기, 부호를 갖는/부호를 갖지 않는, 색인 등의 더 많은 관련된 옵션을 갖는다. 프로그램 명령은, 메모리 액세스 명령이 관련되고, 예를 들어, 메모리(6) 내부에 대상 메모리 어드레스를 포함하는 레지스터 뱅크(16) 내부의 레지스터들과 같은 파라미터를 더 지정한다. 덜 보호된 메모리 액세스 명령에 대한 더 적은 수의 옵션의 설치는 이들 명령이 더 적은 명령 세트 비트 공간을 소모하도록 한다. 이것은 프로세스 또는 아키텍처 내부의 유한한 자원으로 다른 곳에서는 가치있게 사용될 수도 있다. 실제로는, 공유가 비교적 드문 경향이 있고 이에 따라 더 적은 수의 옵션의 설치를 필요로 하는 것으로 프로그래머가 알고 있는 데이터에 대한 메모리 액세스 동작은, 이와 같은 덜 보호된 메모리 액세스에 대해서는, 코드 크기의 과도한 증가를 일으키지 않으므로, 명령 세트 비트 공간의 절감보다 더 중요하다.

[0032] 도 4는 메모리 관리 유닛 페이지 테이블 엔트리(36)를 개략적으로 나타낸 것이다. 이와 같은 페이지 테이블 엔트리는 다양한 범위의 다른 형태를 가질 수 있다. 일반적으로 이와 같은 메모리 관리 유닛 페이지 테이블 엔트리(36)는 가상 어드레스 TAG(38)와 이에 대응하는 물리 어드레스 변환 데이터(40)를 이용하여 가상 어드레스와 물리 어드레스 사이의 어드레스 변환을 지원한다. 또한, 페이지 엔트리와 관련된 메모리 어드레스 공간 내부의 각각의 페이지(영역)와, 판독가능성, 기록가능성, 특권 레벨 액세스 제한, 캐시 기억가능성 등의 특성을 정의하는 메모리 페이지 속성이 관련된다. 또한, 메모리 페이지 속성 데이터 내부에는, 이 영역 내부의 메모리 어드레스가 공유인지 전용인지를 표시하는 공유/전용 플래그가 포함된다. 공유 어드레스는 복수의 프로그램 내에서 공유되는 한편, 전용 어드레스는 한 개의 프로그램만 액세스 가능하다. 다른 형태의 메모리 페이지 속성은, 특정한 영역이 암호화되었는지 암호화되지 않았는지를 표시하는 플래그를 포함한다. 암호화된 영역은 암호화 키를 사용하여 암호화된 후, 적절한 복호화 키를 소유하고 있는 적절한 권한을 갖는 프로그램에 의해 복호화된다.

[0033] 공유/전용 플래그의 경우에, 공유로 표기된 메모리 영역은 덜 보호된 메모리 액세스 명령에 의해서만 액세스되어야 하며, 마찬가지로, 전용으로 표기된 메모리 영역은 보호된 메모리 액세스 명령에 의해서만 액세스되어야 한다. 틀린 종류(인코딩)의 메모리 액세스 명령이 특정한 영역의 메모리에 대한 메모리 액세스를 시도하면, 이것이 검출되어 데이터 중단을 일으킨다(메모리 액세스 예외처리를 기동한다).

[0034] 도 5는 한가지 형태의 메모리 액세스 처리를 개략적으로 나타낸 흐름도이다. 스텝 S52에서 메모리 액세스 명령이 디코드될 때까지 처리가 대기한다. 메모리 액세스 명령이 디코드되면, 디코더(10)에 의해 제어신호가 발생되어 로드 스토어 유닛(120을 제어하여 메모리 관리 유닛(18)과 협력하여 지정된 메모리 액세스 동작을 행한다. 스텝 44에서는, 스텝 42에서 디코드된 메모리 액세스 명령에 대한 공유 플래그 데이터(기타 데이터도)가 판독된다. 그후, 스텝 46은 스텝 42에서 디코드된 메모리 액세스 명령이 보호된 메모리 액세스 명령이었는지 여부를 판정한다. 스텝 42에서 디코드된 명령이 보호된 메모리 액세스 명령이었으면, 스텝 48로 처리가 진행하여 스텝 44에서 판독된 공유 플래그가 액세스할 메모리 어드레스를 포함하는 메모리 영역이 공유된 것을 표시하는지 아닌지에 대한 판정이 행해진다. 스텝 48에서의 판정 결과 메모리 영역이 공유이면, 이것은 보호된 메모리 액세스 명령이 적절히 사용되고 있다는 것을 나타내므로, 스텝 50으로 처리가 진행하여 액세스가 차단된 후 스텝 42로 처리를 되돌리기 전에 스텝 52에서 데이터 중단 응답이 기동된다. 스텝 48에서의 판정 결과 메모리 액세스가 공유 영역에 대한 것이 아닌 경우에는, 보호된 메모리 액세스 명령의 사용이 적절하지 않으므로(즉, 메모리 영역이 전용이므로) 스텝 54에서 액세스가 허가되어 수행된다. 스텝 46의 판정 결과 스텝 42에서 디코드된 메모리 액세스 명령이 덜 보호된 메모리 액세스 명령인 경우에는, 스텝 56으로 처리를 진행하여, 스텝 44에서 판독된 공유 플래그가 덜 보호된 메모리 액세스 명령과 관련된 메모리 어드레스가 공유된 것으로 나타내는지 아닌지에 대한 판정이 행해진다. 메모리 영역이 공유되지 않으면, 이것은 덜 보호된 메모리 액세스 명령의 사용이 부적절하다는 것을 나타내므로, 스텝 58로 처리를 진행하여, 메모리 액세스가 차단되고, 스텝 60에서 데이터 중단 응

답이 기동된다. 스텝 56에서의 판정 결과 메모리 영역이 공유이면, 스텝 42에서 디코드된 덜 보호된 메모리 액세스 명령의 사용이 부적절하므로, 스텝 62로 처리를 진행하여 액세스가 허가된다.

[0035] 도 6은 본 발명을 이용하는 데이터 처리 시스템(64)의 또 다른 실시예를 개략적으로 나타낸 것이다. 본 실시예에서는, 메모리(66) 내부의 메모리 영역이 암호화된 영역 68, 70, 72이거나 암호화되지 않은 영역 74, 76이다. 프로세서 코어(82)와 메모리(66) 사이에 배치된 암호화 회로(80)는, 암호화된 영역 68, 70, 72에 기록되고 있는 데이터에 대해 암호화를 제공하고 암호화 영역 68, 70, 72로부터 판독되고 있는 데이터에 대해 복호화를 제공하는 역할을 한다. 암호화 및 복호화는 각각의 암호화된 영역 68, 70, 72를 액세스하는 프로그램에 대해 전용의 암호화 키(84)를 사용한다.

[0036] 본 실시예에서, 메모리 액세스 제어회로는 암호화되거나 암호화되지 않는 것으로 표기되는 메모리(66)의 메모리 어드레스 공간 내부의 서로 다른 영역을 갖는 메모리 보호 유닛(86)의 형태를 갖는다. 메모리 영역이 암호화되면, 멀티플렉서 88, 90을 사용하여 전환되어 암호화 회로(80)를 거쳐 데이터의 경로를 지정한다. 액세스되고 있는 메모리 어드레스가 암호화되지 않은 영역 내부에 있을 때에는, 멀티플렉서 88, 90에 의해 암호화 회로(8)가 우회된다. 암호화 회로(80)는 보호된 메모리 액세스 명령에 대해 사용되고 활성이 되며 덜 보호된 메모리 액세스 명령에 대해서는 우회된다. 암호화되지 않은 영역 74, 76은 프로그램들 사이에서 공유되는 반면에, 암호화된 영역 68, 70, 72는 개별 프로그램 또는 암호화 키를 공유하는 다수의 프로그램에 대해 전용이 될 수 있다. 덜 보호된 메모리 액세스 명령이 메모리 보호 유닛(86)에 의해 암호화된 것으로 표기된 메모리 액세스와 대해 사용되면, 데이터 중단이 기동된다. 마찬가지로, 보호된 메모리 액세스 명령이 암호화되지 않은 영역 내부의 메모리 어드레스에 대해 사용되면, 데이터 중단이 마찬가지로 기동된다.

[0037] 도 7은 다양한 특권/예외 레벨에서 동작하는 프로그램들의 계층구조를 개략적으로 나타낸 것이다. 프로그램들은 최상의 특권 레벨에 더 낮은 특권 레벨(더 낮은 예외 레벨)에서 동작하고 있는 게스트 운영체계 프로그램들 94, 96에 대한 실행환경을 제공하는 하이퍼바이저 프로그램(92)을 포함한다. 각각의 운영체계 프로그램들 94, 96은 각각 어플리케이션 프로그램들 98, 100 또는 어플리케이션 프로그램들 102, 104에 대한 실행 환경을 제공한다. 운영체계 프로그램들 94, 96은 어플리케이션 프로그램들 98, 100, 102, 104보다 더 높은 특권 레벨(예외 레벨)에서 동작한다.

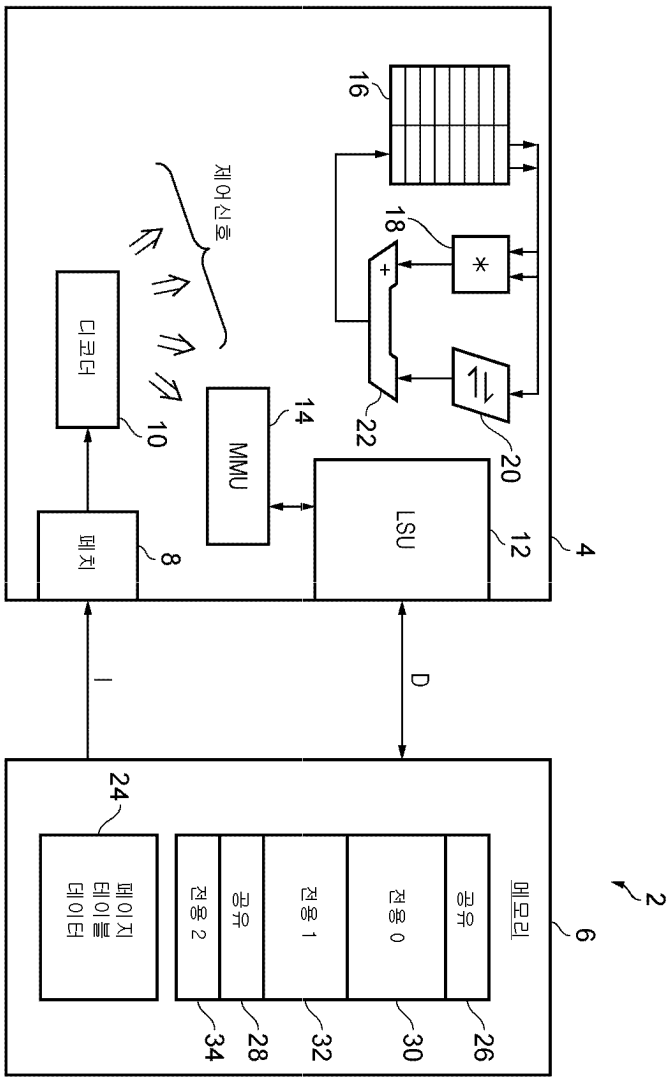
[0038] 전술한 실시예는 보호된 메모리 액세스 명령과 덜 보호된 메모리 액세스 명령과 관련하여 공유/전용 플래그 또는 암호화된/암호화되지 않은 플래그를 이용하여 액세스를 제어하였다. 또 다른 실시예는 프로그램이 실행되고 있는 특권 레벨(예외 레벨)과 관련된 메모리 액세스 조건을 부과하는 역할을 한다. 프로그래머는 다른 레벨(특권 레벨)에서 동작하는 한 개 이상의 다른 프로그램과 데이터를 공유하는 것이 적절하다고 결정할 수도 있다. 일례로서, 어플리케이션 프로그램들 98, 100, 102, 104는 위에 놓이는 운영체계 프로그램 94, 96과 데이터를 공유할 수 있지만, 다른 어플리케이션 프로그램이나 하이퍼바이저 프로그램(92)과는 공유할 수 없도록 제어된다. 덜 보호된 메모리 액세스 명령은 다른 예외 레벨과 공유하는 것이 바람직한 데이터와 관련되는 한편, 다른 예외 레벨과 공유하는 것이 바람직하지 않은 데이터는 보호된 메모리 액세스 명령을 사용하여 액세스된다.

[0039] 도 8은 본 발명을 이용하는 데이터 처리 시스템(106)의 또 다른 실시예를 개략적으로 나타낸 것이다. 이 데이터 처리 시스템(106)은 메인 메모리(114) 내부의 암호화된 메모리 영역 108, 110과 공유 메모리 영역(112)을 이용한다. 도 6의 실시예와 비교하면, 도 8의 실시예는 다양한 레벨의 계층을 사용하는 메모리 시스템을 이용한다. 4개의 프로세서 코어 116, 118, 120, 122는 각각 로컬 전용 캐시 메모리 124, 126, 128, 130을 갖는다. 메모리 계층에서 이들 로컬 캐시 124, 126, 128, 130 위에 있는 것은 공유 캐시 메모리(132)이다. 캐시 메모리들 124, 126, 128, 130, 132의 각각의 내부의 데이터는 그것이 암호화/공유된 것으로 표기된 것에 무관하게 암호화되지 않은 형태로 기억된다. 데이터를 암호화/공유하려면, 이 데이터가 캐시 메모리들 124, 126, 128, 130, 132 내부에서 플래그가 붙여지고, 이와 같은 플래그의 제어하에서 멀티플렉서 136, 138을 사용하여 암호화 회로(134)를 거쳐 또는 암호화 회로를 돌아서(우회하여) 경로가 지정된다. 따라서, 암호화 회로(134)보다 프로세서 코어들 116, 118, 120, 122에 더 가까운 데이터는 암호화되지 않은 형태로 기억되므로 암호화/복호화와 관련된 에너지/시간 불이익을 일으키지 않는 한편, 암호화 회로(134)보다 메모리 계층 구조 내에서 더 멀리 떨어진, 즉 인터커넥트(140)를 거쳐 전달되고 메인 메모리(114) 내부에 기억되는 데이터는 암호화된다. 그래픽 처리 유닛(142)과 직접 메모리 액세스 유닛(144)도 인터커넥트(140)를 거쳐 접속된다.

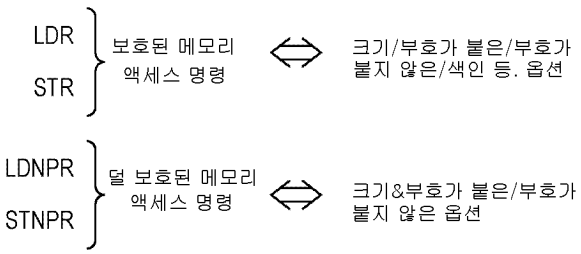
[0040] 첨부도면을 참조하여 본 발명의 예시적인 실시예들을 상세히 설명하였지만, 본 발명은 이들 실시예에 한정되지 않으며, 첨부된 청구범위의 보호범위 및 사상을 벗어나지 않으면서 본 발명이 속한 기술분야의 당업자에 의해 다양한 변경, 부가 및 변화가 행해질 수 있다는 것은 자명하다.

도면

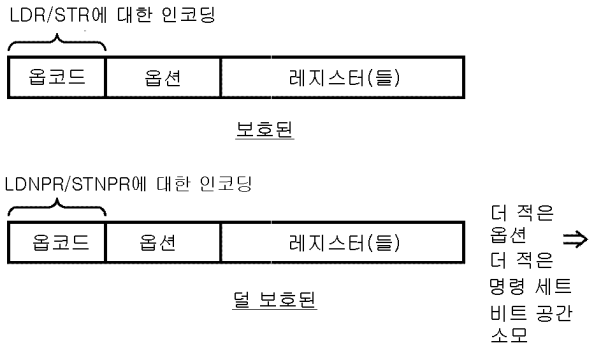
도면1


16
제어신호
18
디코더
10
14
MMU
22
20
LSU
12
4
페치
8
I
D
24
페이지 테이블 데이터
전용 2
공유
전용 1
전용 0
공유
메모리
6
2
34
28
32
30
26

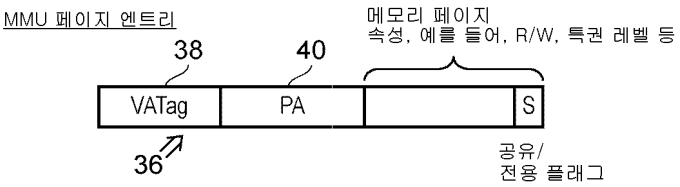
도면2


LDR
STR
보호된 메모리 액세스 명령
크기/부호가 붙은/부호가 붙지 않은/색인 등. 옵션
LDNPR
STNPR
덜 보호된 메모리 액세스 명령
크기&부호가 붙은/부호가 붙지 않은 옵션

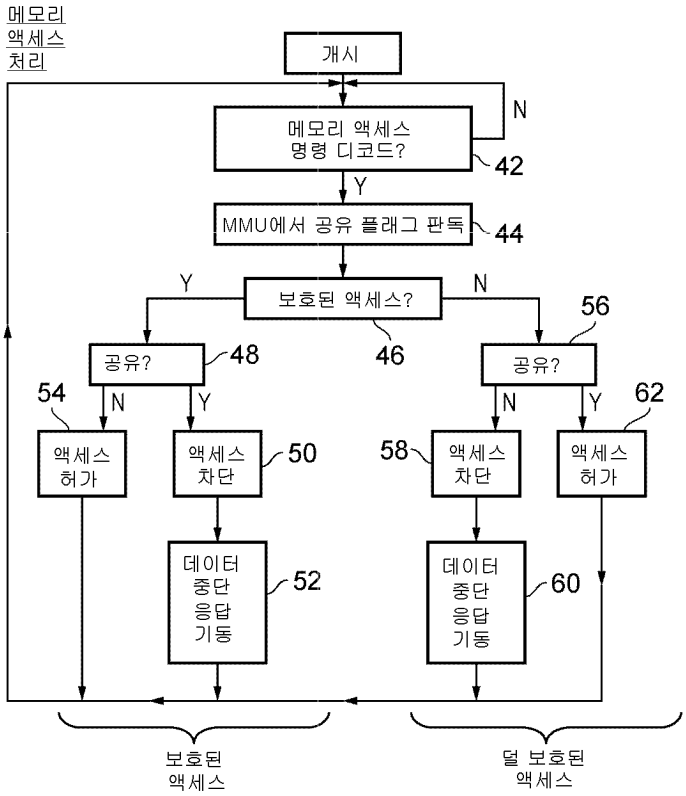
도면3


LDR/STR에 대한 인코딩
옵코드
옵션
레지스터(들)
보호된
LDNPR/STNPR에 대한 인코딩
옵코드
옵션
레지스터(들)
덜 보호된
더 적은
옵션
더 적은
명령 세트
비트 공간
소모

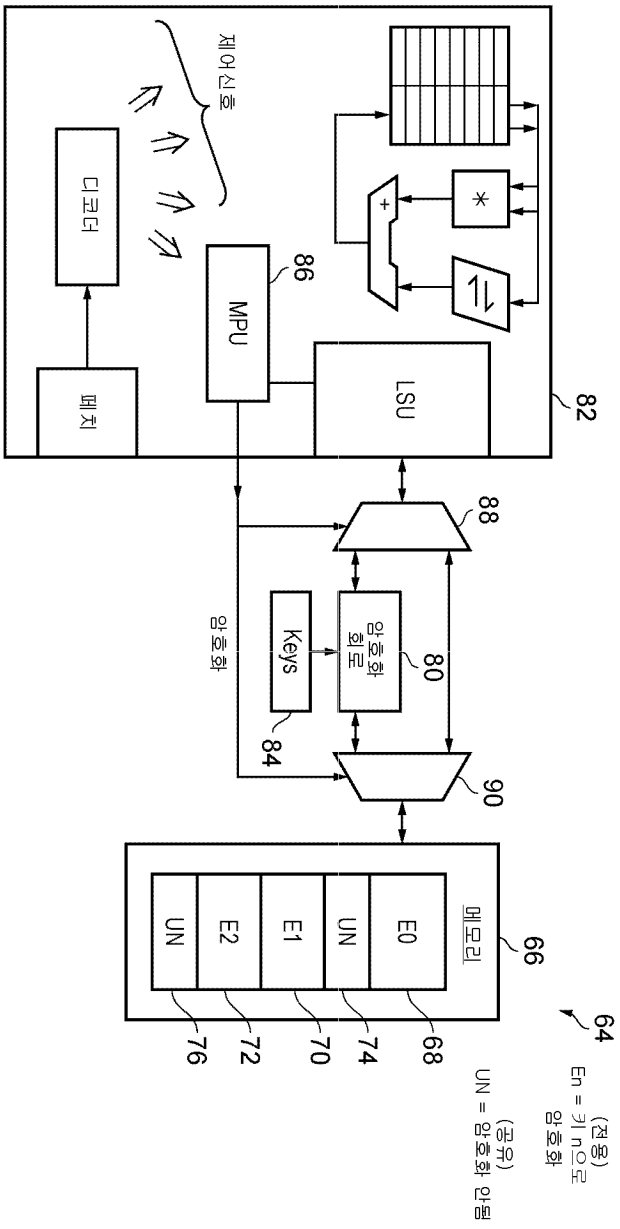
도면4


MMU 페이지 엔트리
메모리 페이지
속성, 예를 들어, R/W, 특권 레벨 등
38
40
VATag
PA
S
36
공유/
전용 플래그

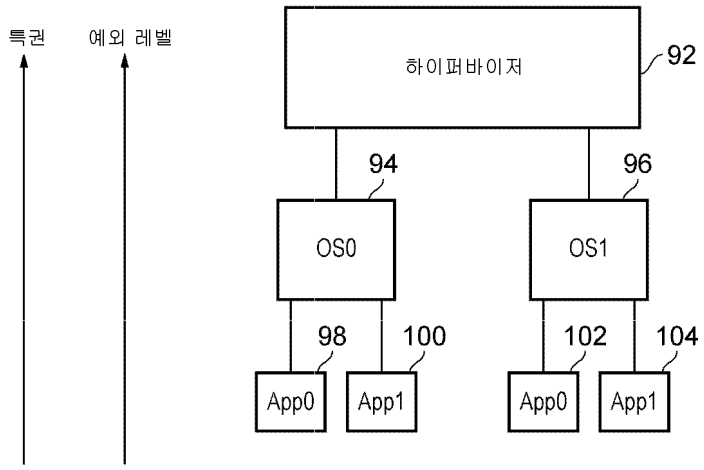
도면5


메모리
액세스
처리
개시
메모리 액세스
명령 디코드?
N
42
Y
MMU에서 공유 플래그 판독
44
Y
보호된 액세스?
N
46
56
공유?
48
공유?
54
N
Y
N
Y
62
액세스
허가
액세스
차단
50
58
액세스
차단
액세스
허가
데이터
중단
응답
기동
52
데이터
중단
응답
기동
60
보호된
액세스
덜 보호된
액세스

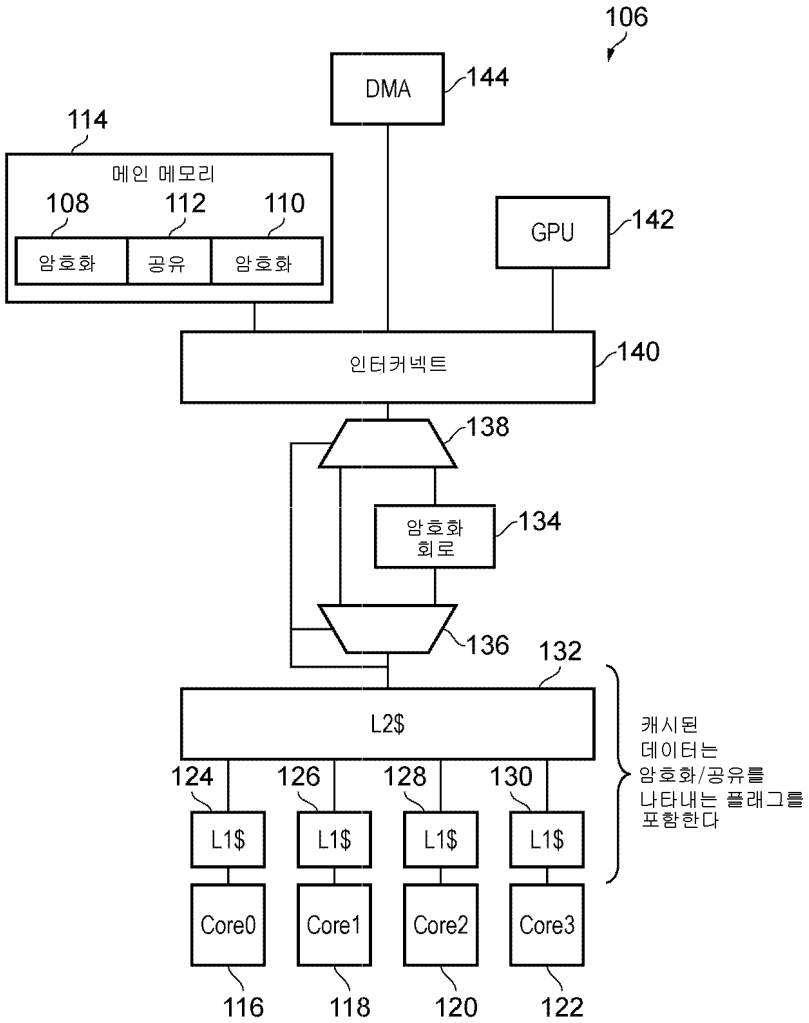
도면6


제어신호
디코더
MPU
86
페치
LSU
82
88
암호화
Keys
84
암호화 회로
80
90
메모리
66
UN
E2
E1
UN
E0
76
72
70
74
68
64
(점유) En = 키 n으로 암호화
(공유) UN = 암호화 안됨

도면7



도면8



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 발명(고안)의 설명

【보정세부항목】 식별번호 0030

【변경전】

다양한 종류의 메모리 액세스 명령의 설치는 프로그래머(또는 컴파일러)가 디폴트로 보호된 메모리 액세스 명령을 사용하고, 그후 프로그래머가 알기에는 덜 제한된 메모리 액세스 조건을 안전하게 겪는 특정한 메모리 액세스 동작에 대해서는 덜 보호된 메모리 액세스 명령의 사용을 선택할 수 있도록 한다. 예를 들어, 보호된 메모리 액세스 명령은, 프로그래머에 의해 메모리(6) 내부의 공유 영역 26, 28에 대해 행해지도록 의된 것으로 알려진 것 이외의 모든 메모리 액세스에 대해 디폴트로 사용된다. 공유 영역에 대한 이들 메모리 액세스는 덜 보호된 메모리 액세스 명령을 사용해도 된다. 프로그래머는 프로그램 코드의 작성시에 특정한 데이터가 다른 어플리케이션 프로그램과 공유되어야 하며 공유 영역 26, 28에 기록되어야 하므로, 이와 같은 메모리 액세스가 덜 보호된 메모리 액세스 명령을 이용하여 행해지는 것이 적절하다는 것을 알게 된다. 이에 따라, 메모리 관리 유닛(14)(또는 메모리 보호 유닛)을 제어하는 데이터가 틀리더라도, 더 제한된 메모리 액세스 조건을 갖는 보호된 메모리 명령의 사용은 프로그래머가 공유 영역 26, 28에 부주의하게 데이터를 기억하는 것을 방지하고 공유 영역 26, 28로부터 부주의하게 (변경된) 데이터를 로드하는 것을 방지하는 역할을 한다.

【변경후】

다양한 종류의 메모리 액세스 명령의 설치는 프로그래머(또는 컴파일러)가 디폴트로 보호된 메모리 액세스 명령을 사용하고, 그후 프로그래머가 알기에는 덜 제한된 메모리 액세스 조건을 안전하게 겪는 특정한 메모리 액세스 동작에 대해서는 덜 보호된 메모리 액세스 명령의 사용을 선택할 수 있도록 한다. 예를 들어, 보호된 메모리 액세스 명령은, 프로그래머에 의해 메모리(6) 내부의 공유 영역 26, 28에 대해 행해지도록 정의된 것으로 알려진 것 이외의 모든 메모리 액세스에 대해 디폴트로 사용된다. 공유 영역에 대한 이들 메모리 액세스는 덜 보호된 메모리 액세스 명령을 사용해도 된다. 프로그래머는 프로그램 코드의 작성시에 특정한 데이터가 다른 어플리케이션 프로그램과 공유되어야 하며 공유 영역 26, 28에 기록되어야 하므로, 이와 같은 메모리 액세스가 덜 보호된 메모리 액세스 명령을 이용하여 행해지는 것이 적절하다는 것을 알게 된다. 이에 따라, 메모리 관리 유닛(14)(또는 메모리 보호 유닛)을 제어하는 데이터가 틀리더라도, 더 제한된 메모리 액세스 조건을 갖는 보호된 메모리 명령의 사용은 프로그래머가 공유 영역 26, 28에 부주의하게 데이터를 기억하는 것을 방지하고 공유 영역 26, 28로부터 부주의하게 (변경된) 데이터를 로드하는 것을 방지하는 역할을 한다.

【직권보정 2】

【보정항목】 발명(고안)의 설명

【보정세부항목】 식별번호 0034

【변경전】

도 5는 한가지 형태의 메모리 액세스 처리를 개략적으로 나타낸 흐름도이다. 스텝 S52에서 메모리 액세스 명령이 디코드될 때까지 처리가 대기한다. 메모리 액세스 명령이 디코드되면, 디코더(10)에 의해 제어신호가 발생되어 로드 스토어 유닛(120을 제어하여 메모리 관리 유닛(18)과 협력하여 지정된 메모리 액세스 동작을 행한다. 스텝 44에서는, 스텝 42에서 디코드된 메모리 액세스 명령에 대한 공유 플래그 데이터(기타 데이터도)가 판독된다. 그후, 스텝 46은 스텝 42에서 디코드된 메모리 액세스 명령이 보호된 메모리 액세스 명령이었는지 여부를 판정한다. 스텝 42에서 디코드된 명령이 보호된 메모리 액세스 명령이었으면, 스텝 48로 처리가 진행하여 스텝 44에서 판독된 공유 플래그가 액세스할 메모리 어드레스를 포함하는 메모리 영역이 공유된 것을 표시하는지 아닌지에 대한 판정이 행해진다. 스텝 48에서의 판정 결과 메모리 영역이 공유이면, 이것은 보호된 메모리 액세스 명령이 적절히 사용되고 있다는 것을 나타내므로, 스텝 50으로 처리가 진행하여 액세스가 차단된 후 스텝 42로 처리를 되돌리기 전에 스텝 52에서 데이터 중단 응답이 기동된다. 스텝 48에서의 판정 결과 메모리 액세스가 공유 영역에 대한 것이 아인 경우에는, 보호된 메모리 액세스 명령의 사용이 적절하지 않으므로(즉, 메모리 영역이 전용이므로) 스텝 54에서 액세스가 허가되어 수행된다. 스텝 46의 판정 결과 스텝 42에서 디코드된 메모리 액세스 명령이 덜 보호된 메모리 액세스 명령인 경우에는, 스텝 56으로 처리를 진행하여, 스텝 44에서 판독된 공유 플래그가 덜 보호된 메모리 액세스 명령과 관련된 메모리 어드레스가 공유된 것으로 나타내는지 아닌지에 대한 판정이 행해진다. 메모리 영역이 공유되지 않으면, 이것은 덜 보호된 메모리 액세스 명령의 사용이 부적절하다는 것을 나타내므로, 스텝 58로 처리를 진행하여, 메모리 액세스가 차단되고, 스텝 60에서 데이터 중단 응답이 기동된다. 스텝 56에서의 판정 결과 메모리 영역이 공유이면, 스텝 42에서 디코드된 덜 보호된 메모리 액세스 명령의 사용이 부적절하므로, 스텝 62로 처리를 진행하여 액세스가 허가된다.

【변경후】

도 5는 한가지 형태의 메모리 액세스 처리를 개략적으로 나타낸 흐름도이다. 스텝 S52에서 메모리 액세스 명령이 디코드될 때까지 처리가 대기한다. 메모리 액세스 명령이 디코드되면, 디코더(10)에 의해 제어신호가 발생되어 로드 스토어 유닛(120을 제어하여 메모리 관리 유닛(18)과 협력하여 지정된 메모리 액세스 동작을 행한다. 스텝 44에서는, 스텝 42에서 디코드된 메모리 액세스 명령에 대한 공유 플래그 데이터(기타 데이터도)가 판독된다. 그후, 스텝 46은 스텝 42에서 디코드된 메모리 액세스 명령이 보호된 메모리 액세스 명령이었는지 여부를 판정한다. 스텝 42에서 디코드된 명령이 보호된 메모리 액세스 명령이었으면, 스텝 48로 처리가 진행하여 스텝 44에서 판독된 공유 플래그가 액세스할 메모리 어드레스를 포함하는 메모리 영역이 공유된 것을 표시하는지 아닌지에 대한 판정이 행해진다. 스텝 48에서의 판정 결과 메모리 영역이 공유이면, 이것은 보호된 메모리 액세스 명령이 적절히 사용되고 있다는 것을 나타내므로, 스텝 50으로 처리가 진행하여 액세스가 차단된 후 스텝 42로 처리를 되돌리기 전에 스텝 52에서 데이터 중단 응답이 기동

된다. 스텝 48에서의 판정 결과 메모리 액세스가 공유 영역에 대한 것이 아닌 경우에는, 보호된 메모리 액세스 명령의 사용이 적절하지 않으므로(즉, 메모리 영역이 전용이므로) 스텝 54에서 액세스가 허가되어 수행된다. 스텝 46의 판정 결과 스텝 42에서 디코드된 메모리 액세스 명령이 덜 보호된 메모리 액세스 명령인 경우에는, 스텝 56으로 처리를 진행하여, 스텝 44에서 판독된 공유 플래그가 덜 보호된 메모리 액세스 명령과 관련된 메모리 어드레스가 공유된 것으로 나타내는지 아닌지에 대한 판정이 행해진다. 메모리 영역이 공유되지 않으면, 이것은 덜 보호된 메모리 액세스 명령의 사용이 부적절하다는 것을 나타내므로, 스텝 58로 처리를 진행하여, 메모리 액세스가 차단되고, 스텝 60에서 데이터 중단 응답이 기동된다. 스텝 56에서의 판정 결과 메모리 영역이 공유이면, 스텝 42에서 디코드된 덜 보호된 메모리 액세스 명령의 사용이 부적절하므로, 스텝 62로 처리를 진행하여 액세스가 허가된다.