(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G11C 8/00

(45) 공고일자 2004년07월30일
(11) 등록번호 10-0442216
(24) 등록일자 2004년07월20일

(21) 출원번호 10-2001-0030069
(22) 출원일자 2001년05월30일

(65) 공개번호 10-2002-0025650
(43) 공개일자 2002년04월04일

(30) 우선권주장 2000-299012 2000년09월29일 일본(JP)

(73) 특허권자 미쓰비시덴키 가부시키가이샤
일본국 도쿄도 지요다쿠 마루노우치 2쵸메 2반 3고

(72) 발명자 야마우치다다아키
일본도쿄도지요다쿠마루노우치2쵸메2반3고미쓰비시덴키가부시키가이샤내

고자루구니히코
일본도쿄도지요다쿠마루노우치2쵸메2반3고미쓰비시덴키가부시키가이샤내

(74) 대리인 김창세

심사관 : 김용웅

(54) 반도체 기억 장치

요약

인터페이스부(2)는 어드레스 신호 ADD.에 의해 지정되는 영역이 논리 제어 영역인 경우에는 DRAM(4)과 데이터를 송수신하는 대신에, 레지스터(6)와 데이터 송수신을 실행한다. 그 때의 데이터 신호 DATA는 레지스터(6)에 유지되는 논리 회로(8)에 대한 제어 명령이나 논리 회로에서의 처리를 위한 입력 데이터이다. 레지스터(6)의 유지 내용에 따라서 논리 회로(8)는 예컨대 암호 처리나 화상 처리 등의, 마이크로 컴퓨터에서는 시간을 요하는 처리를 실행한다. 처리 결과는 레지스터(6)에 보존되고 DRAM에 대한 판독과 마찬가지 순서로 판독된다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예 1의 반도체 기억 장치(1)의 구성을 도시한 블럭도,
도 2는 실시예 1의 논리 내장 반도체 기억 장치의 메모리 맵의 예를 도시한 도면,
도 3은 외부로부터 입력되는 신호가 논리 회로로 전달되는 상태를 설명하기 위한 도면,
도 4는 실시예 1의 반도체 기억 장치의 표준적인 타이밍을 설명하기 위한 파형도,
도 5는 실시예 1의 변형예인 논리 내장 DRAM(10)의 구성을 도시한 블럭도,
도 6은 도 5에 도시한 논리 내장 DRAM(10)의 메모리 맵을 도시한 도면,
도 7은 실시예 2의 논리 내장 DRAM(30)의 구성을 도시한 블럭도,

도 8은 실시예 2의 논리 내장 DRAM에 적용되는 시스템의 메모리 맵을 도시한 도면,
도 9는 도 7의 암호 연산 논리(74)가 지원하는 암호 방식을 도시한 도면,
도 10 내지 도 18은 레지스터에 할당되는 데이터 예를 도시한 제 1 도 내지 제 9 도,
도 19는 본 발명의 논리 내장 DRAM(92)과 마이크로 컴퓨터(90)가 접속되는 상태를 도시한 도면,
도 20은 논리 내장 DRAM의 제어를 설명하기 위한 흐름도,
도 21은 실시예 4에 있어서 할당한 메모리 맵을 도시한 도면,
도 22는 실시예 5의 논리 내장 DRAM(l11)의 구성을 도시한 도면,
도 23은 실시예 5에 있어서의 마이크로 컴퓨터 시스템의 메모리 맵을 도시한 도면,
도 24는 실시예 5의 논리 내장 DRAM의 제어를 설명하기 위한 동작 파형도,
도 25는 실시예 5의 변형예를 설명하기 위한 도면,
도 26은 실시예 5의 변형예의 동작을 설명하기 위한 동작 파형도,
도 27은 ScRAM(200)의 구성을 도시한 블럭도,
도 28은 제어 레지스터의 설정에 따른 메모리 맵의 상태 변화를 설명하기 위한 도면,
도 29는 도 27에 도시한 모드 레지스터(208)를 설명하기 위한 제 1 도,
도 30은 도 27에 도시한 모드 레지스터(208)를 설명하기 위한 제 2 도,
도 31은 도 27에 도시한 모드 레지스터(208)를 설명하기 위한 제 3 도,
도 32는 ScRAM의 암호 제어 입구/출구에 관련된 상태 천이도,
도 33은 제어 레지스터 액세스의 일예를 도시한 동작 파형도,
도 34 내지 도 37은 제어 레지스터의 어드레스 맵을 도시한 제 1 도 내지 제 4 도,
도 38은 신호 CRYP를 인가하는 단자를 제어할 수 있는 시스템을 설명하기 위한 도면,
도 39는 CRYP 단자를 제어할 수 없는 시스템에 대해 설명하기 위한 제 1 도,
도 40은 CRYP 단자를 제어할 수 없는 시스템에 대해 설명하기 위한 제 2 도,
도 41은 제어 레지스터로의 설정을 설명하기 위한 동작 파형도,
도 42 내지 도 44는 암호화 처리의 기본 단위에 대해 도시한 제 1 내지 제 3 개략도,
도 45 내지 도 47은 복호화 처리의 단위에 대해 도시한 제 1 내지 제 3 개략도,
도 48은 ECB 모드에 대해 설명하기 위한 제 1 도,
도 49는 ECB 모드에 대해 설명하기 위한 제 2 도,
도 50은 CBC 모드의 연산을 설명하기 위한 도면,
도 51은 CBC 모드에 있어서의 암호화의 개요를 도시한 개념도,
도 52는 CBC 모드에 있어서의 복호화의 개요를 도시한 개념도,
도 53은 종래의 동기형 다이나믹 랜덤 액세스 메모리(SDRAM)의 핀 배치를 도시한 도면,
도 54는 SDRAM의 단자명과 기능을 도시한 도면,
도 55는 종래의 논리 내장 DRAM의 구성을 도시한 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 반도체 기억 장치에 관한 것으로서, 더욱 특정적으로는 논리 회로를 내장한 반도체 기억 장치 및 그 제어 방법에 관한 것이다.
도 53은 종래의 64Mbit의 용량을 갖고 워드 구성이 ×16bit인 동기형 다이나믹 랜덤 액세스 메모리(SDRAM)의 핀 배치를 도시한 도면이다.
도 54는 SDRAM의 단자명과 기능을 도시한 도면이다.
도 53 및 도 54를 참조하면, 종래의 SDRAM은 54핀의 단자를 갖는 패키지에 수납되어 있고, 마스터 클럭이 입력되는 단자 CLK, 클럭 인에이블 신호가 입력되는 단자 CKE, 칩 선택 신호가 입력되는 단자 /CS, 행어드레스 스트로브 신호가 입력되는 단자 /RAS, 열어드레스 스트로브 신호가 입력되는 단자 /CAS, 라이트 인에이블 신호가 입력되는 단자 /WE를 갖고 있다.
종래의 SDRAM은 또 데이터 입출력 신호를 송수신하는 단자 DQ0 DQ15, 출력 디스에이블 신호/라이트 마스크 신호가 입출력되는 단자 DQM(U/L), 어드레스가 입력되는 단자 A0 A11, 뱅크 어드레스가 입력되는 단자 BA0, BA1, 전원이 인가되는 단자 VDD, 출력용 전원이 인가되는 단자 VDDQ, 접지 전위가 인가되는 단자 VSS, 출력용 접지 전위가 인가되는 단자 VSSQ를 갖고 있다.
이들 단자는, 도 53에 도시하는 바와 같이, 1번 핀부터 13번 핀 및 42번 핀부터 54번 핀 사이에 데이터 입출력 단자 및 전원이 배치되고, 15번 핀부터 19번 핀 및 37번 핀부터 39번 핀 사이에 제어 신호 및 클럭 신호가 배치되어 있고, 20번 핀부터 35번 핀 사이에 어드레스 입력 핀이 배치되어 있다. 이러한 단자 배치는 어느 정도 범용성을 갖고 있어 메모리를 탑재하는 시스템에 이용되는 기판에도 자주 사용되고 있다.

도 55는 종래의 논리 내장 DRAM의 구성을 도시한 도면이다.
도 55를 참조하면, 칩(501)에는 DRAM(504)과 논리(508)가 탑재되어 있고, DRAM으로의 액세스용의 제어 신호 /RAS, /CAS, … , /CS나 어드레스 신호 ADD. 및 데이터 신호 DATA를 입력하거나 또는 출력하는 단자가 마련되어 있다.
칩(501)에는 또 논리 특유의 제어 핀 CTR0, CTR1이나 논리에 액세스 요구를 하는 요구(request) 신호 REQ를 입력하는 단자 및 논리가 처리 완료를 외부에 알리기 위한 스트로브 신호 STRB를 출력하기 위한 단자를 포함하고 있다.

발명이 이루고자 하는 기술적 과제

종래는 논리(508)를 제어하기 위해서 논리(508)를 위한 특유한 핀을 마련하고 있었기 때문에, 도 53에 도시한 바와 같은 범용적인 DRAM에 대해서 핀 수가 증가하거나 또 보드 상에서 시스템을 조립하기 때문에 논리 혼재 DRAM을 제어하기 위해서 전용의 컨트롤러를 준비할 필요가 있었다. 따라서, 통상의 마이크로 컴퓨터에 접속하는 바와 같은 범용성이 손실되거나 또는 시스템을 제어하기 위해 마이크로 컴퓨터에 특수한 명령을 사용할 필요가 있었다.
본 발명의 목적은 범용적인 DRAM과 마찬가지 제어 방법으로 논리부를 제어하 는 것이 가능한 논리 회로가 혼재된 반도체 기억 장치를 제공하는 것이다.

발명의 구성 및 작용

본 발명은 요약하면 반도체 기억 장치로서, 단자군, 메모리 셀 어레이 및 논리 회로를 구비한다.
단자군은 외부로부터 인가되는 제어 신호, 어드레스 및 데이터를 받는다. 메모리 셀 어레이는 어드레스에 의해서 지정되는 영역에 대해서 제어 신호에 따라 데이터의 송수신을 실행한다. 논리 회로는 메모리 셀 어레이에 대해서 제어 신호, 어드레스 및 데이터가 인가되는 순서(시퀀스)와 동일한 순서로 단자군에 제어 신호, 어드레스 및 데이터가 인가된 경우, 어드레스가 소정의 제 1 영역을 지정했을 때에 제어 신호, 어드레스 및 데이터 중의 적어도 어느 1개에 따라 데이터 처리를 실행한다.
본 발명의 다른 국면에 따르면, 반도체 기억 장치의 제어 방법으로서, 지정하는 단계와 명령을 인가하는 단계를 구비한다.
반도체 기억 장치는 단자군, 메모리 셀 어레이 및 논리 회로를 포함한다. 단자군은 외부로부터 인가되는 제어 신호, 어드레스 및 데이터를 받는다. 메모리 셀 어레이는 어드레스에 의해서 지정되는 영역에 대해서 제어 신호에 따라 데이터의 송수신을 실행한다. 논리 회로는 메모리 셀 어레이에 대해서 제어 신호, 어드레스 및 데이터가 인가되는 순서와 동일한 순서로 단자군에 제어 신호, 어드레스 및 데이터가 인가된 경우, 어드레스가 소정의 제 1 영역을 지정했을 때에 제어 신 호, 어드레스 및 데이터 중의 적어도 어느 1개에 따라 데이터 처리를 실행한다.
지정하는 단계는 제 1 영역을 예약 영역으로 지정한다. 명령을 인가하는 단계는 메모리 셀 어레이로의 기록 순서와 동일한 순서로 어드레스에 의해서 제 1 영역을 지정하여 논리 회로로의 명령을 인가한다.
본 발명의 또 다른 국면에 따르면, 반도체 기억 장치로서, 제 1 단자군, 제 2 단자, 메모리 및 논리 회로를 구비한다.
제 1 단자군은 외부로부터 인가되는 제어 신호, 어드레스 및 데이터를 받는다. 제 2 단자는 외부로부터 인가되는 선택 신호를 받는다. 메모리는 행렬 형상으로 배치되는 복수의 메모리셀을 포함하고, 선택 신호에 따라 활성화되며, 어드레스에 의해서 지정되는 영역에 대해서 제어 신호에 따라 데이터의 송수신을 실행한다. 논리 회로는 선택 신호에 따라 메모리와 상보적으로 활성화되고, 어드레스 및 데이터 중 적어도 어느 1개에 따라 데이터 처리를 실행한다.
따라서, 본 발명의 주된 이점은 범용적인 메모리에 대해서 데이터, 어드레스 및 제어 신호를 인가하는 것과 마찬가지 순서로 신호를 인가하는 것에 의해 내장하는 논리 회로를 제어할 수 있고, 기존의 시스템에 큰 변경을 가할 필요가 없어 용이하게 제어할 수 있는 것이다.
본 발명의 다른 이점은 마이크로 컴퓨터 시스템에 있어서, 논리 내장의 반도체 기억 장치를 용이하게 제어할 수 있는 것이다.
본 발명의 또 다른 이점은 최소한의 제어 단자의 추가에 의해 내장 메모리에 어드레스나 데이터를 인가하는 경로를 유효하게 사용하여 내장하는 논리 회로의 제 어를 실행할 수 있는 것이다.
(바람직한 실시예의 설명)
이하에 있어서, 본 발명의 실시예에 대해 도면을 참조하여 상세하게 설명한다. 또한, 도면 중 동일 부호는 동일 또는 상당 부분을 나타낸다.
(실시예 1)
도 1은 본 발명의 실시예 1의 반도체 기억 장치(1)의 구성을 도시한 블럭도이다.
도 1을 참조하면, 반도체 기억 장치(1)는 제어 신호 /RAS, /CAS, …, /CS, /WE 등의 제어 신호를 받는 단자와 어드레스 신호 ADD를 받는 단자와 데이터 신호 DATA를 받는 단자, 제어 신호 /RAS, /CAS, …, /CS, /WE, 어드레스 신호 ADD. 및 데이터 신호 DATA에 따라 내부로 제어 신호를 출력하는 인터페이스부(2), 인터페이스부(2)의 출력을 받아 동작하는 DRAM(4), 인터페이스부(2)로부터 인가되는 데이터나 명령을 유지하는 레지스터(6), 레지스터(6) 및 인터페이스부(2)로부터의 출력에 따라 신호 처리 등의 동작을 실행하는 논리 회로(8)를 포함한다.
칩(1)의 단자는 범용 DRAM에서 이용되고 있는 단자뿐이다. 따라서, 범용 DRAM 칩을 수납하고 있는 것과 동일한 패키지를 이용할 수 있다. 예컨대, 도 53에 도시한 바와 같은 핀 배치를 갖는 패키지이다.
그 때문에, 본 발명의 반도체 기억 장치(1)를 기존의 애플리케이션에서 이용 하는 경우, 기존의 범용 DRAM과 교체할 뿐이므로, 보드의 재설계나 전용의 제어 LSI를 개발할 필요가 없다. 즉, 범용 DRAM과 핀 겸용이기 때문에, 소프트웨

어의 변경만으로 새로운 기능을 추가할 수 있다. 예컨대 새로운 기능으로는 화상의 고속 처리용의 회로나 암호 처리 등의 마이크로 컴퓨터에서는 시간이 걸리는 처리를 실행하는 논리 회로의 추가가 고려된다. 또, 범용 DRAM을 수납하고 있는 패키지에 수 개의 미사용 단자, 예컨대 도 53에 있어서의 36번 핀이나 40번 핀과 같은 NC(비접속) 핀을 이용하여 제어 신호를 입력하도록 해도 좋다.

다음에, 구체적인 제어 방법을 설명한다. 탑재되는 논리 회로의 제어에는 소위 메모리 매핑된(memory mapped) IO 방식을 적용한다.

도 2는 실시예 1의 논리 내장 반도체 기억 장치의 메모리 맵의 예를 도시한 도면이다.

도 2를 참조하면, 칩에 탑재되는 DRAM의 용량을 64Mbit로 하고, 워드 구성을 ×16으로 한다. DRAM의 어드레스는 X어드레스가 X0 X13, Y어드레스가 Y0 Y7이다. 따라서, 8MByte를 제어하는 메모리 어드레스는 0h 3FFFFFh이다.

범용의 DRAM에서는 이 어드레스 공간 전부에 데이터를 기록하여 판독할 수 있다. 이러한 데이터를 기록하여 판독할 수 있는 공간을 DRAM 공간이라고 부르기로 한다. 본 발명에서는 임의의 특정 영역을 탑재하는 논리 회로를 위한 논리 제어 영역으로 할당한다. 예컨대, 어드레스의 0h 1Fh의 공간을 논리 제어 영역으로 할당한다. 논리 제어 영역의 용량은 예컨대 256×2Byte의 512Byte이다. 이 어드레스 공간에 기록하는 데이터에 의해서 논리를 제어하는 명령이나 모드를 선택할 수 있다.

도 2에서는 최하위 어드레스에 영역을 확보했지만, 최상위 측(3FFFFFh 3 FFFE0h)에 논리 제어 영역을 할당해도 좋다. 탑재하는 DRAM으로서 SDRAM을 상정한 경우에는 모드 레지스터 세트 시에 어드레스를 할당하는 영역을 선택할 수 있도록 해도 좋다. 또, 모드 레지스터 세트 시에 논리 제어 영역을 할당하지 않으면, 통상의 64Mbit의 SDRAM으로서 사용할 수도 있다.

도 3은 외부로부터 입력되는 신호가 논리 회로로 전달되는 상태를 설명하기 위한 도면이다.

도 3을 참조하면, 인터페이스부(2)는 제어 신호 /RAS, /CAS,…, /CS, /WE, 어드레스 신호 ADD. 및 데이터 신호 DATA를 받는 버퍼(3), 버퍼(3)의 출력을 받아 디코드하는 디코드 회로(5)를 포함하고 있고, 디코드 회로(5)의 출력에 따라 레지스터(6)는 모드나 명령 등의 정보를 유지하고 이들 유지한 정보에 따라 논리 회로(8)가 제어된다.

디코드 회로(5)는 어드레스 신호 ADD와 데이터 신호 DATA를 디코드하지만, 어드레스 신호에 의해서 지정되는 논리 제어 영역에 기록된 데이터를 그대로 레지스터(6)에 보존하는 경우도 있다. 레지스터가 SRAM(Static Random Access Memory) 등으로 구성되어 있는 경우에는 어드레스 신호 ADD에 따라 지정되는 SRAM의 영역에 데이터가 유지되는 경우도 있다. 또, 레지스터(6) 대신에 유지 회로로서 DRAM 일부의 영역을 이용하고, 그 영역에 논리 회로 제어용의 데이터를 유지시켜도 좋다.

도 4는 실시예 1의 반도체 기억 장치의 표준적인 타이밍을 설명하기 위한 파 형도이다.

도 4에 있어서는 데이터 입출력 단자로부터 입력 및 출력이 가능한 SDRAM에 있어서, 연속해서 8개의 데이터를 기록 또는 판독하는 동작을 설명한다. 연속해서 판독되는 데이터의 비트 수는 버스트 길이라고 불리고, SDRAM에서는 통상 모드 레지스터에 의해서 변경할 수 있다.

도 4를 참조하면, 시각 t1에 있어서, 외부로부터의 클럭신호 ext. CLK(예컨대, 시스템 클럭)의 상승 에지에서 외부로부터의 제어 신호(행어드레스 스트로브 신호 /RAS, 열어드레스 스트로브 신호 /CAS, 어드레스 신호 ADD 등)가 페치된다. 행어드레스 스트로브 신호 /RAS가 활성 상태의 L레벨에 있고, 열어드레스 스트로브 신호 /CAS 및 라이트 인에이블 신호 /WE는 H레벨에 있기 때문에, 로우 액티브 명령 ACT가 입력된 것으로 된다. 이 때의 어드레스 신호 ADD는 행어드레스 Xa로서 페치된다.

시각 t2에 있어서, 열어드레스 스트로브 신호 /CAS가 활성 상태의 L레벨로 되고, 클럭 ext.CLK의 상승과 동기해서 내부로 페치된다. 열어드레스 스트로브 신호 /CAS가 L레벨이고 행어드레스 스트로브 신호 /RAS 및 라이트 인에이블 신호 /WE가 H레벨이라고 하는 제어 신호의 조합은 판독 명령 READ이다. 이 때의 어드레스 신호 ADD는 열어드레스 Y로서 페치된다.

어드레스에 의해 지정된 영역이 도 2의 DRAM 공간인 경우에는 이 페치된 행어드레스 Xa 및 열어드레스 Yb에 따라서, 도 1의 DRAM(4) 내에 있어서, 행 및 열의 선택 동작이 실시된다.

행어드레스 Xa 및 열어드레스 Yb가 도 2의 논리 지정 영역의 어드레스인 경우에는 선택되는 것은 도 1의 DRAM(4)의 행 및 열이 아니라, 레지스터(6)의 소정의 영역이다. 예컨대, 이 소정의 영역에는 논리(8)의 동작 상태를 나타내는 플래그나 논리(8)의 연산 결과가 저장되어 있다.

D/Q는 데이터 입출력 단자에서 입출력되는 데이터 신호 DATA를 나타낸다. 행어드레스 스트로브 신호 /RAS가 L레벨로 하강하고 나서 소정의 클럭 주기(도 4에 있어서는 6클럭 사이클)가 경과한 후, 시각 t3에 있어서, 최초의 데이터 q0이 출력되고, 데이터 q0에 후속해서 데이터 q1 q7이 연속해서 출력된다. 이 데이터의 출력은 클럭 신호 ext.CLK의 하강에 응답해서 출력된다.

이 출력된 데이터는 DRAM(4)에 유지되어 있던 데이터 또는 레지스터(6)의 내용이다. 레지스터(6)의 내용은, 예컨대 논리(8)의 동작 상태를 나타내는 플래그나 논리(8)의 연산 결과이다.

시각 t4 이후는 기록 동작을 나타낸다. 시각 t4에 있어서, 로우 액티브 명령 ACT가 입력되고, 행어드레스 Xc가 페치된다. 시각 t5에 있어서, 열어드레스 스트로브 신호 /CAS 및 라이트 인에이블 신호 /WE가 모두 활성 상태의 L레벨이고, 또한 행어드레스 스트로브 신호 /RAS가 H레벨인 조합 즉, 기록 명령 WRITE가 인가되면, 그 때의 클럭 신호 ext.CLK의 상승 에지에서 열어드레스 Yd가 페치됨과 동시에 그 때에 인가되고 있던 데이터 d0이 최초의 기록 데이터로서 페치된다.

어드레스에 의해 지정된 영역이 도 2의 DRAM 공간인 경우에는 행어드레스 스트로브 신호 /RAS 및 열어드레스 스트로브 신호 /CAS의 하강에 응답해서 SDRAM 내 부에 있어서는 행 및 열 선택 동작이 실시된다. 이후 클럭 신호 ext.C

LK와 동기해서 순차 입력 데이터 d1 d7이 페치되고, 대응하는 메모리셀에 기록된다.
행어드레스 Xc 및 열어드레스 Yd에 의해 지정되는 영역이 도 2의 논리 지정 영역인 경우에는 선택되는 것은 도 1의 DRAM(4)의 행 및 열이 아니라 레지스터(6)의 소정 영역이다. 이 경우는 입력 데이터 d1 d7은 레지스터(6)의 소정 영역에 기록하는 데이터이다. 예컨대, 인가하는 데이터는 논리(8)가 처리하는 화상 데이터, 암호 데이터 등의 처리 데이터나 리셋, 처리 개시 등의 동작을 지정하는 명령 데이터이다.
(실시예 1의 변형예)
도 5는 실시예 1의 변형예인 논리 내장 DRAM(10)의 구성을 도시한 블럭도이다.
도 5를 참조하면, 논리 내장 DRAM(10)은 제어 신호 /RAS, /CAS, …, /CS, 어드레스 신호 ADD, 데이터 신호 DATA를 받는 인터페이스부(12), 인터페이스부(12)의 출력에 따라 동작하는 DRAM(4), 인터페이스부(12)의 출력에 따라 제어용 데이터를 유지하는 레지스터(14),(16), 레지스터(14),(16)에 각각 유지되는 제어용 데이터에 따라 동작하는 논리 회로(18),(20)를 갖는다.
도 6은 도 5에 도시한 논리 내장 DRAM(10)의 메모리 맵을 도시한 도면이다.
도 6을 참조하면, 64Mbit의 어드레스 공간 0h 3FFFFFh 중 어드레스 0h 1Fh는 논리 회로(18)에 대한 제어 명령이나 데이터를 기록하는 논리 제어 영역이고, 어드레스 20h 2Fh는 논리 회로(20)에 대한 명령이나 데이터를 기록하는 논리 제어 영역이다.
이와 같이, 메모리 맵된 IO 공간을 복수개로 분할하여 탑재하는 복수개의 논리 회로를 제어하는 것이 가능해진다.
(실시예 2)
도 7은 실시예 2의 논리 내장 DRAM(30)의 구성을 도시한 블럭도이다.
도 7을 참조하면, 논리 내장 DRAM(30)은 SDRAM부(32)와 논리부(34)를 포함한다.
SDRAM부(32)는 외부로부터의 신호를 받아 그것에 따른 제어 신호를 출력하는 인터페이스부(36) 및 인터페이스부(36)로부터의 출력에 따라 데이터의 유지를 실행하는 DRAM 코어(38)를 포함한다. 인터페이스부(36)는 제어 신호 /CS, /RAS, /CAS, /WE 및 DQM을 받는 제어 신호 입력 회로(40), 클럭 신호 CLK 및 클럭 인에이블 신호 CKE를 받아 내부 클럭을 발생하는 클럭 버퍼(44), 클럭 버퍼(44)의 출력과 동기해서 어드레스 신호 A0 An을 페치하는 어드레스 버퍼(46), 내부 클럭과 동기하여 데이터 신호 DQ0 DQn의 입출력을 실행하는 입출력 회로(52)를 포함한다.
인터페이스부(36)는, 또한 제어 신호 입력 회로(40)의 출력에 따라 명령 신호 ACT, PRE 등을 출력하는 제어 회로(42), 제어 회로(42)의 출력에 따라 어드레스 버퍼(46)의 출력을 X어드레스, Y어드레스로서 다중하는 멀티플렉서(48)를 포함한다.
멀티플렉서(48)는 모드 레지스터 세트(MRS) 명령에 따라 어드레스 신호 A0 Am 중 어느 하나의 신호 비트에 따라 설정할 수 있는 모드 레지스터(50)를 포함하고 있다.
DRAM 코어(38)는 행렬 형상으로 메모리셀이 배치되는 메모리셀 어레이(54), 멀티플렉서(48)로부터 인가되는 행어드레스에 따라 메모리셀 어레이(54)의 행 선택을 실행하는 로우 디코더(56), 멀티플렉서(48)로부터 인가되는 열어드레스에 따라 메모리셀 어레이(54)의 열 선택을 실행하는 행디코더(56), 선택된 메모리셀로부터 데이터를 판독하고 또한 선택된 메모리셀에 대해서 데이터의 기록을 실행하는 센스 앰프 드라이버 및 라이트 드라이버(60)를 포함한다.
논리부(34)는 암호 연산 논리(74), 인터페이스부(36)의 출력에 따라 암호 연산 논리(74)를 제어하기 위한 모드 정보나 암호 연산 논리에 입력할 데이터 및 암호 연산 논리의 연산 결과를 유지하는 레지스터부(72)를 포함한다.
레지스터부(72)는 어드레스 신호 A0 Am에 의해서 지정되는 영역이 소정값인 경우에 활성화되고, 입출력 회로(52)를 거쳐서 외부로부터 입력되는 데이터 신호를 페치하기 위한 셀렉터(선택기)(76), 셀렉터(76)를 거쳐서 외부로부터 인가된 데이터를 기록하는 제어 레지스터(78), 모드 레지스터(80) 및 데이터 레지스터(84), 암호 연산 논리에서 출력되는 데이터를 유지하고 그 유지 데이터를 셀렉터(76)와 입출력 회로(52)를 거쳐서 외부로 데이터 신호 DQ0 DQn으로서 판독하기 위한 상태 레지스터(82), 데이터 레지스터(86)를 포함한다.
도 8은 실시예 2의 논리 내장 DRAM에 적용되는 시스템의 메모리 맵을 도시한 도면이다.
도 8을 참조하면, 시스템 메모리 맵 중의 외부 RAM 영역이 논리 내장 DRAM에 대응한다. 논리 내장 DRAM은 그 영역이 논리 제어 영역과 DRAM 영역으로 분할되어 있고, 논리 제어 영역으로의 액세스에 의해서 내장하는 암호 논리를 제어한다. 이 논리 제어 영역에 대응하는 시스템 메모리 맵 상의 영역은 시스템 예약 영역으로 하고, CPU의 캐시 및 MMU(메모리 관리 유닛)를 사용하는 경우에는 캐시 불가능 영역으로 해 둔다. 또, 오퍼레이팅 시스템(운영체제)이 이 영역으로 로드되지 않도록 미리 시스템의 펌웨어에 의해 제어한다. 또, 애플리케이션 프로그램도 이 영역을 사용 금지로 한다.
이 논리 제어 영역은, 예컨대 DRAM의 행어드레스 X=3FFFh, 열어드레스 Y= 0H FFh에 할당한다.
도 7의 제어 레지스터(78)는 X=3FFFh, Y=00h에 할당된다. 모드 레지스터(80)는 H=3FFFh, Y=01h에 할당된다. 상태 레지스터(82)는 어드레스 X=3FFFh, Y=02h에 할당된다. 제 1 데이터 레지스터(84)는 어드레스 X=3FFFh, Y=03h에 할당되고, 제 2 데이터 레지스터(86)는 어드레스 X=3FFFh, Y=04h에 할당된다.
이 예에서는 X=3FFFh의 페이지(Y=00h FFh)를 제어 명령 영역에 할당하고 있다. 따라서, 도 7의 구성에 있어서 ACT 명령 입력 시에 X=3FFFh가 입력된 시점에서 레지스터부(72)로 액세스할 수 있도록 멀티플렉서를 제어해 둔다. 또, 레지스터의 인에이블 신호나 레지스터를 제어하고 있는 클럭도 동작시켜 둔다. 이와 같 이 하면, 제어 명령의 입력 기간 중, 이외에서 레지스터부(72)에 의해 소비되는 전력을 억제할 수 있다. 또, X=3FFFh의 페이지에 판독, 기록 명령이 입력되더라도 이미 레지스터부(72)가 활성화되어 있으므로, 레지스터로의 액세스가 지연되는 일은 없다.
도 7의 암호 연산 논리(74)는 네트워크 상의 안전(security) 확보를 위해 사용되고 있는 주요한 암호 방식의 가속 장치(액셀러레이터)를 내장하고 있다. 이 암호 연산 논리(74)는 전자 인증에서 이용되는 공개키 방식과 인증 후의 데이터 송수신에서 이용되는 비밀키 암호 방식의 기능을 지원하고 있다. 암호 전용의 논리 회로에 의해 처리하므로, 처리

를 범용의 CPU로 처리하는 것보다 저소비 전력으로 고속 처리를 실행할 수 있고, 예컨대 전지 구동의 시스템 등에 적합하다.

도 9는 도 7의 암호 연산 논리(74)가 지원하는 암호 방식을 도시한 도면이다.

도 9를 참조하면, 암호 연산 논리(74)는 공개키 암호 방식으로서 RSA를 지원하고, 비밀키 암호 방식으로서 DES 방식과 트리플(Triple) DES 방식을 지원한다. 또, 비밀키 암호 방식에서는 주요한 블럭 암호화 모드인 ECB(Electric Code Book), CBC(Cipher Block Chaining), OFB(Output Feed Back), CFB(Cipher Feed Back)의 각 모드를 지원하고 있다. 암호 연산 논리(74)는 애플리케이션의 적합성을 높이기 위해서, 암호화에 있어서, 정밀한(critical) 처리가 할당되고 있고, 그 밖에는 논리 내장 DRAM(30)을 제어하는 마이크로 컴퓨터 측에서 소프트웨어 처리하게 된다. 그리고, 최대의 특징은 범용의 SDRAM과 핀 겸용으로 암호 제어를 실현할 수 있는 것 이다.

다음에, 도 8에 도시한 논리 제어 영역의 각 레지스터에 어떠한 할당이 되어 있는가를 설명한다.

도 10 내지 도 18은 레지스터에 할당되는 데이터를 설명하기 위한 도면이다.

도 7 및 도 10을 참조하면, 제어 레지스터(78)는 Y어드레스가 0h인 D0 D15의 16비트가 할당되고 있다. 그리고, 비트 D0에 1을 기록하는 것에 의해 암호 기능이 리셋된다. 즉, 암호 연산 논리(74)에 소정 시간의 리셋 펄스를 인가하는 처리가 실행된다. 또, 비트 D1이 1인 경우에는 암호 연산 논리(74)가 암호 처리 중인 것을 나타낸다. 따라서, 외부로부터 암호 연산 논리로 액세스하는 경우에는 비트 D1에 표시되는 플래그가 0인 것을 확인하고 나서 액세스하지 않으면 안된다.

이 제어 레지스터(78)는 공개키와 비밀키의 양 방식 공통으로 이용된다.

다음에, 비밀키 방식의 제어에 이용되는 몇 개의 레지스터의 예에 대해 설명한다.

도 7 및 도 11을 참조하면, Y=1h인 어드레스에 대해서는 모드 레지스터(80)가 할당되어 있고, 이 16비트 중 비트 D1, D0은 암호 방식 선택에 사용된다. 이 2개의 비트가 '01'이면 암호 방식은 DES이다. '10'이면 암호 방식은 트리플 DES이다. '00'이면 암호 방식은 홀드된다.

비트 D5 D2는 블럭 암호화 모드 선택에 사용된다. 이 비트가 '0001'이면 블럭 암호화 모드는 ECB가 지정된다. 또, '0010' 인 경우에는 블럭 암호화 모드는 CBC가 지정된다. '0100'인 경우에는 암호 모드는 OFB가 지정된다. 이들 비트가 '1000'인 경우에는 블럭 암호화 모드는 CFB64로 지정된다. 또, 이들 비트가 '0000'인 경우에는 블럭 암호화 모드는 홀드된다.

비트 D8 D6은 암호 처리의 단위량을 지정하는 데이터 처리 모드의 선택에 사용된다. 이들의 비트가 '001'인 경우에는 처리를 8Byte 단위로 실행하는 노멀 모드가 지정되고, '010'인 경우에는 블록 길이를 지정한 블록 단위로 처리를 실행하는 블럭 모드가 지정되고, '100'인 경우에는 버퍼에 축적한 정보를 단위로 해서 일괄 처리하는 버퍼 모드가 지정되고, '000'인 경우에는 데이터 처리 모드는 홀드된다.

이와 같이, Y=1h인 1어드레스 2Byte의 데이터의 16비트를 복수의 모드 지정에 할당할 수 있으므로, 2의 16승의 조합을 유효하게 사용하면 지정할 모드가 복수 있는 경우라도 1회의 액세스에 의해 동작 모드의 지정을 완료할 수 있다.

도 7 및 도 12를 참조하면, 어드레스 Y=02h에는 상태 레지스터(82)가 할당되고 있다. 상태 레지스터의 비트 D1, D0이 '01'일 때는 암호화를 나타내고, '10'일 때는 복호화를 나타내고, '00'일 때는 홀드를 나타낸다. 비트 D5, D4가 '01'일 때는 평문 또는 암호문의 입력 개시를 나타내고 있고, '10'일 때에는 입력 정지를 나타내고, '00'일 때에는 홀드를 나타낸다.

비트 D9 D6은 OFB, CFB의 1블럭 중의 텍스트 길이를 나타낸다.

도 7 및 도 13을 참조하면, Y어드레스 3h 6h는 64비트의 DES의 키 등이 저장되는 영역이다.

도 7 및 도 14를 참조하면, 제 1 데이터 레지스터(86)는 트리플 DES에 사용 되는 키를 저장하는 영역이다. 어드레스 Y=7h Ah인 영역이 상당한다.

데이터 레지스터(84),(86)는 모두 외부로부터는 1개의 레지스터로 보이지만 실제로는 복수의 레지스터로 구성되어 있고, 일종의 FIFO 메모리이다.

기타는 도 7에는 도시되어 있지 않지만, 도 15에 도시한 바와 같은 초기 벡터를 설정하는 레지스터, 도 16에 도시한 바와 같은 블럭 길이를 지정하는 레지스터, 도 17에 도시한 바와 같은 버퍼 개수를 지정하는 레지스터, 도 18에 도시한 바와 같은 버퍼 ID를 나타내는 레지스터 등이 있다.

또한, 공개키 방식, 예컨대 RSA 암호 처리를 실행하기 위해서, Y=12h 1Fh인 영역은 예약 영역으로 되어 있다. 공개키 방식의 경우에는 암호 처리 결과가 내장 레지스터에 유지되기 때문에, 암호 처리 중이더라도 DRAM 영역으로 액세스할 수 있다.

SDRAM에 대한 ACT 명령에 의해 판독되는 행어드레스 X가 3FFFh인 경우, 멀티플렉서(48)가 이것을 검출하여 셀렉터(76)를 활성화시킨다. 그리고, 판독 명령 또는 기록 명령에 의해 열어드레스 Y가 입력되는 것에 의해서 어느 1개의 레지스터로 액세스할 것인지가 선택된다. 그리고, 입출력 회로(52)를 거쳐서 외부로부터 입력되는 데이터가 레지스터에 기록된다.

실시예 2의 경우에는 논리 제어 영역으로서 확보한 어드레스 영역은 3FFF00h 3FFFFFh이었지만, 모드 레지스터 세트 명령에 의해 세트할 수 있는 도 7에 있어서의 레지스터(50)의 유지 내용에 따라서 멀티플렉서에 있어서 할당하여 어드레스를 변경할 수 있도록 하는 것에 의해, 각종 마이크로 컴퓨터 시스템에 본 발명의 논리 내장 DRAM을 탑재하는 것이 가능해진다. 모드 레지스터 세트 명령에 의해 어드레스를 할당하지 않는 경우에는 본 발명의 논리 내장 DRAM은 통상의 64Mbit의 SDRAM으로서 사용 가능하다. 통상의 SDRAM으로서 사용하는 용도를 위해 모드 레지스터에 내부 탑재 논리를 사용할지 사용하지 않을지를 지정하는 비트를 마련해도 좋다.

(실시예 3)

도 19는 본 발명의 논리 내장 DRAM(92)과 마이크로 컴퓨터(90)가 접속되는 상태를 도시한 도면이다.

마이크로 컴퓨터(90)에는 CPU 코어(94), 캐시 메모리(96), 메모리 컨트롤러(98) 및 외부 버스 인터페이스 회로(100)가 포함되어 있고, 이들은 내부 버스(102)에 의해서 접속되어 있다. 외부 버스 인터페이스 회로(100)는 CPU 코어(94)로부터의 지령에 따라 논리 내장 DRAM에 대해서 제어 신호 및 어드레스 신호 및 데이터를 출력한다. 따라서, 외부 버스 인터페이스 회로(100)와 논리 내장 DRAM(92)은 제어 신호 /RAS, /CAS, …, /CS 등의 제어 신호를 전달하는 제어 신호 버스, 어드레스 신호 ADD.를 전달하는 어드레스 버스 및 데이터 DATA를 전달하는 데이터 버스에 의해서 접속되어 있다.

이러한 시스템에 있어서 논리 내장 DRAM(92)을 제어하기 위해서는 마이크로 컴퓨터(90) 상에서 작동하는 소프트웨어에 유의하지 않으면 안되는 사항이 있다.

도 20은 논리 내장 DRAM의 제어를 설명하기 위한 흐름도이다.

도 20을 참조하면, 우선 최초에 단계 S1에 있어서, 논리 제어 영역으로 되는 어드레스를 예약 영역으로 지정한다. 즉, 논리 회로에 대한 명령 제어용의 어드레스 공간 상에 프로그램이 할당되지 않도록 한다. 할당하지 않는 방법으로서는 예컨대, OS(오퍼레이션 시스템)의 기능을 이용하여 논리 제어 영역을 예약 영역으로 하는 방법이 있다.

메모리 관리, 인터럽트 관리, 프로세스간 통신과 같은 시스템의 기본적인 제어를 실행하는 OS에 있어서의 중핵 부분인 커넬(kernel) 자체가 논리 제어 영역에 할당되지 않도록 OS의 상승 시점에도 주의를 요한다. 따라서, 커넬 자체가 논리 제어 영역에 할당되지 않도록 주의해서 예약 영역을 OS측에서 지정해 둔다.

다음에, 단계 S2에 있어서, 데이터 캐시가 있는 시스템에 있어서는 논리 제어 영역을 캐시 불가능 영역으로 하고 있다.

즉, 도 19에 있어서의 CPU 코어(94)로부터 논리 내장 DRAM(92)에 대해서 소정의 어드레스 공간을 지정하여 명령에 상당하는 데이터를 내부 버스(102)로 보낸 경우라도, 캐시 메모리(96)가 동작하면 그 명령에 상당하는 데이터는 캐시 메모리(96)에 기록되어 논리 내장 DRAM(92)으로는 전달되지 않는 경우가 있을 수 있다. 그러면, 논리 내장 DRAM(92)에 탑재하고 있는 논리 회로는 그 명령에 따라 동작할 수 없게 된다. 따라서, 논리 제어 영역이 캐시되지 않도록 설정할 필요가 있다. 대개의 마이크로 컴퓨터에서는 일부의 어드레스 공간을 캐시 불가능(uncachable) 영역으로 지정하는 제어가 가능하다.

또, 메모리 관리 유닛 기능을 갖고 있는 경우에는 가상 어드레스 공간이 논 리 제어 영역에서 이용되지 않도록 설정한다.

이와 같이, 캐시 메모리가 있는 시스템에서는 시스템의 초기 설정에 있어서, 논리 내장 DRAM의 논리 제어 영역에 대해서는 캐시 메모리를 사용하지 않도록 하여 반드시 액세스되도록 한다.

다음에, 단계 S3에 있어서, 할당한 영역에 통상 기록하는 것에 의해서 논리 제어를 위한 명령을 입력하고, 단계 S4에 있어서, 통상 판독에 의해 논리의 처리 상황의 체크나 처리 결과의 판독을 실행할 수 있다. 또, 단계 S5에 있어서, 처리가 아직 종료하지 않았으면 단계 S3 및 S4를 반복하게 된다. 구체적으로는, 도 10에서 설명한 바와 같이, 어드레스 Y=0h의 비트 D1에 기록되어 있는 플래그를 체크하는 것에 의해서 처리 상황을 판단할 수 있다. 이 플래그를 체크하여 처리의 완료를 확인하고 나서, 마이크로 컴퓨터는 연산 결과를 액세스하는 등 다음의 동작을 시작할 수 있다.

따라서, 본 발명에 따르면 종래에는 처리의 종료를 전용의 핀에 의해 수신자 측에 전하고 있었던 데 비해, SDRAM에 통상의 통상 판독을 실행하는 것에 의해 플래그 상태를 체크하는 것이 가능해진다.

(실시예 4)

실시예 1 내지 실시예 3에서 설명한 예는 칩에 탑재하는 DRAM 메모리의 일부의 공간을 분할해서 명령 제어용의 공간으로서 할당하고 있었다. 따라서, 할당한 부분만은 마이크로 컴퓨터 시스템의 메인 메모리로서는 사용할 수 없었다. 실시예 4에서는 고스트 공간을 제어용으로 할당한다.

도 21은 실시예 4에 있어서 할당한 메모리 맵을 도시한 도면이다.

도 21을 참조하면, 탑재하는 DRAM을 64Mbit의 용량이고, 워드 구성이 ×16인 SDRAM이라고 하면, X어드레스는 X0 X13, Y어드레스는 Y0 Y7이었다. X어드레스를 1단자 추가하고 X14='0'인 영역을 실제(實) 메모리 공간으로 하고, X14='1'인 영역을 고스트 공간으로 한다. 메모리가 존재하지 않는 이 더미의 고스트 공간의 일부를 논리 제어 영역으로 할당한다. 이 공간에는 반드시 직접 액세스가 되도록 실시예 3에서 설명한 바와 같은 연구를 해 둔다.

X14를 인가하기 위한 단자가 1단자 증가하게 되지만, 패키지에서 미사용 단자가 있는 경우에는 그것을 할당하면 좋다. 예컨대, 도 53의 40번 핀이나 36번 핀 등의 NC 단자를 할당하면 좋다. 도 21에서는 X14의 어드레스를 추가한 경우를 설명했지만, Y어드레스를 1비트 추가해도 좋다. 즉, Y8=0인 영역을 DRAM 공간으로 하고, Y8=1인 영역을 고스트 공간으로 하는 것도 가능하다. DRAM에서는 X어드레스와 Y어드레스는 통상은 다중화되어 있고, X어드레스 쪽이 비트가 많으므로, Y어드레스를 추가하는 경우에는 사용하는 단자의 추가는 필요없다.

이상은 고스트 공간의 일부에 논리 제어 영역을 할당한 경우를 설명했지만, 고스트 공간에 대해서 판독하면 그것에 대응하는 실제 공간의 어드레스에 저장되어 있는 데이터에 연산이 가해져 출력되거나, 그 어드레스의 데이터가 재기록되는 경우도 고려된다. 즉, X14=1로서 액세스하면, 지정한 어드레스의 X14=0으로 한 실제공간의 어드레스에 유지되어 있는 데이터에 어떠한 처리를 가하도록 해도 좋다. 이 경우에 있어서도 X14의 어드레스를 확장하는 대신에 Y8의 어드레스를 확장해도 좋고, 또 X14가 1인 경우에 고스트 공간으로 했지만, X14=0인 경우를 고스트 공간으로 하고 X14=1인 경우를 실제 메모리 공간으로 해도 좋다. Y8의 어드레스를 확장하는 경우에도 Y8=0인 경우를 고스트 공간으로 하고, Y8=1인 경우를 실제 메모리 공간으로 해도 좋다.

(실시예 5)

도 22는 실시예 5의 논리 내장 DRAM(111)의 구성을 도시한 도면이다.

도 22를 참조하면, 논리 내장 DRAM(111)에는 통상의 DRAM(114)를 제어하기 위한 어드레스 ADD., 데이터 DQ 및 클럭 신호 CLK나 제어 신호 /RAS, /CAS, …, /CS, /WE를 제어하기 위한 단자에 부가해서, 신호 WE_L, ADD_L을 인

가하기 위한 단자가 마련되어 있다.
논리 내장 DRAM(111)은 또 통상의 DRAM(114), 소정의 제어 신호를 유지하기 위한 레지스터(116), 레지스터(116)의 유지 정보에 따라 동작하는 논리 회로(118)를 포함한다.
즉, 제어 전용의 단자를 최소한 첨가하는 것에 의해서 제어 공간을 자유롭게 설정할 수 있다. 도 22에서는 추가한 제어 단자는 제어 신호 WE_L, ADD_L이 입력되는 단자이다. 추가하는 단자는 도 53에 도시한 36번 핀이나 40번 핀과 같은 NC 핀에 할당하면 좋다.
제어 신호 ADD_L이 L레벨인 경우에 DRAM 액세스 모드로 되고, 제어 신호 ADD_L이 L레벨에서 H레벨로 되면 DRAM(114)은 비활성화되고 대신에 레지스터(116)에 신호가 입력 가능하게 되어 논리(118)가 동작하는 모드로 된다.
도 23은 실시예 5에 있어서의 마이크로 컴퓨터 시스템의 메모리 맵을 도시한 도면이다.
도 23을 참조하면, 0h 3FFFFFh가 DRAM 공간에 할당된다. X어드레스가 X0 X13의 14 비트, Y어드레스가 Y0 Y7의 8비트이며, 마이크로 컴퓨터 시스템에 있어서, DRAM 공간을 지정하는 어드레스 비트로는 모두 합쳐서 A0 A21까지가 이용된다.
그리고, 예컨대 제어 신호 ADD_L이 입력되는 단자를 마이크로 컴퓨터 시스템의 어드레스 비트 A23과 접속한 경우에는 논리 제어 영역은 800000h 803FFFh를 할당할 수 있다. 즉, 어드레스 비트 A23='1'로 하고, 어드레스 핀 멀티플렉스를 사용하지 않을 때에 어드레스를 입력하는 최대수의 단자부터 DRAM의 어드레스로서 지정할 수 있는 범위, 즉 X어드레스로서 지정 가능한 범위와 동일한 0h 3FFFh가 논리 제어 영역으로서 할당 가능한 범위이다. 실제로 사용할 때에는 논리 제어 영역의 상한은 필요에 따라서 설정하면 좋다.
단, 마이크로 컴퓨터가 어드레스 비트 A23='1'인 다른 어드레스 영역을 사용할 가능성이 있는 경우에는 논리 제어 영역(800000h 803FFFh)으로 액세스하는 경우에만 논리 내장 DRAM에 대해서 칩 선택 신호 /CS를 활성화시킬 필요가 있다.
도 24는 실시예 5의 논리 내장 DRAM의 제어를 설명하기 위한 동작 파형도이다.
도 24를 참조하면, 시각 t1까지는 클럭 신호 CLK와 동기한 통상의 DRAM에 대한 액세스가 실행된다.
시각 t1에 있어서, 제어 신호 ADD_L이 H레벨로 되면, 논리 회로에 대한 명령 제어 모드로 들어간다. 이후, 클럭 신호 CLK와 동기해서 어드레스 신호 ADD에 의해서 지정된 레지스터에 데이터의 송수신이 실행된다. 도 24의 경우에는 추가된 제어 신호 /WE_L이 L레벨이므로, 명령 제어용 레지스터에 명령 입력이 실행된다.
(실시예 5의 변형예)
도 25는 실시예 5의 변형예를 설명하기 위한 도면이다.
통상의 DRAM 어드레스 공간을 액세스할 때에는 마이크로 컴퓨터(132)는 CPU 코어(134)로부터 지정된 어드레스에 대해서 메모리 컨트롤러(136)가 멀티플렉스 회로(140)를 이용하여 X어드레스 및 Y어드레스를 어드레스 신호 A0 A13이 전달되는 어드레스 버스로 다중화하여 출력한다.
그러나, 도 23에 도시한 바와 같이, DRAM 공간과는 다른 영역에 논리 제어 영역이 할당되는 경우에는 메모리 컨트롤러(136)는 멀티플렉스 회로(140)를 이용하지 않고 그대로 어드레스를 외부 버스 인터페이스 회로(142)에서 출력하게 된다.
이 경우에는 어드레스 신호 A0 A20 중 다중화된 후 유효하게 되어 있는 핀 수에 대응하는 어드레스 신호 A0 A13을 이용해서 SRAM과 마찬가지 방법에 의해 어드레스의 지정이 실행된다. 이 경우, 신호 A14 A20은 어떤 것이라도 상관없는 상태 소위 「Don ' t Care」의 상태이다. 이러한 어드레스 신호 A0 A20이 /CS의 활 성화와 동시에 지정되면, 따라서 논리 내장 DRAM(121)이 처리를 실행한다.
단, 이 경우에도 마이크로 컴퓨터가 어드레스 비트 A23='1'인 다른 어드레스 영역을 사용할 가능성이 있는 경우에는 논리 제어 영역(800000h 803FFFh)으로 액세스하는 경우에만 논리 내장 DRAM에 대해서 칩 선택 신호 /CS를 활성화시킬 필요가 있다.
이러한 경우에는 논리 내장 DRAM(121)은 레지스터(126)의 일부에 어드레스의 변화를 검지하는 ATD(Address Transition Detect) 회로(130)를 마련한다.
도 26은 실시예 5의 변형예의 동작을 설명하기 위한 동작 파형도이다.
이 경우에는 시각 t1까지는 제어 신호 ADD_L은 L레벨로서 통상의 DRAM 액세스가 실행되지만, ADD_L이 H레벨로 되면 논리 회로에 대한 명령 제어 모드로 들어간다. 이 때, /WE_L이 L레벨인 경우에는 기록 모드가 지정되고, /WE_L이 H레벨인 경우에는 판독 모드가 지정된다.
그리고, 어드레스 신호 A0 A13에 의해서 지정되는 어드레스 ADD가 변화하면, ATD 회로(130)가 이것을 검지하여 클럭 신호 CLK에 관계없이 내부의 동작 클럭을 발생하고, DQ에 인가되는 신호를 내부의 명령 레지스터에 기록하거나 어드레스에 의해 지정되는 레지스터의 내용을 DQ 단자로부터 판독할 수 있다.
이상 설명한 바와 같이, 반도체 기억 장치(121)의 제어 신호 /WE_L을 받는 단자와 마이크로 컴퓨터(132) 측의 SRAM 제어용으로 출력되는 신호 A23이 출력되는 단자를 접속하는 것에 의해서, 반도체 기억 장치(121)를 SRAM과 같이 제어하면, 특수한 기능을 마이크로 컴퓨터 측에 마련할 필요가 없다. 마이크로 컴퓨터는 외부 확장한 SRAM 등의 메모리에 대해서 데이터의 기록 또는 판독을 실행하는 통상의 명령을 실행하면, 반도체 기억 장치(121)에 탑재한 논리 회로를 제어할 수 있다.
(실시예 6)
실시예 6에서는 보다 구체적인 암호 논리 내장 DRAM에 대해서 설명한다. 이후, 이 암호 논리 내장 DRAM을 안전 SDRAM(ScRAM)이라고 칭한다.
도 27은 ScRAM(200)의 구성을 도시한 블럭도이다.

도 27을 참조하면, ScRAM(200)은 외부로부터 클럭 신호 CLK를 받는 클럭 버퍼(202), 외부와 데이터 신호 DQ를 송수신하기 위한 입출력 버퍼(204), 외부로부터 어드레스 신호 ADD, 명령 신호 CMD 및 신호 CRYP를 받는 입력 버퍼(206)를 포함한다.
ScRAM(200)은 또 입력 버퍼(206)의 출력에 따라 동작 모드 정보를 유지하는 모드 레지스터(208), 입력 버퍼(206) 및 모드 레지스터(208)의 출력에 따라 ScRAM의 제어를 실행하는 DRAM 제어 어드레스 카운터(210), DRAM 제어 어드레스 카운터(210)의 제어 하에서 데이터 유지 동작을 실행하는 DRAM부(212)를 포함한다.
입출력 버퍼(204)와 DRAM부(212)는 내부 버스 mbus[15:0]에 의해 접속된다. DRAM부(212)는 복수의 뱅크를 구비하고 있고, 각 뱅크는 메모리 어레이, 행디코더, 열디코더 및 센스 앰프, 입출력 제어 회로를 포함하고 있다.
ScRAM(200)은 또 셀렉터(214), 레지스터 REG0, REG1, REG2, 카운터(220),(224), 제어 회로(222), 암호 논리(228)를 포함한다.
모드 레지스터(208)에는 SDRAM의 제어 명령인 모드 레지스터 세트(MRS) 시의 파라미터가 보존된다. 이 파라미터로서는 SDRAM의 모드 설정뿐만 아니라, 제어 레지스터 REG0 REG2의 액세스의 인에이블/디스에이블도 설정할 수 있다. 또, MRS가 입력되면 제어 레지스터 REG0 REG2 및 암호 논리(228)가 리셋된다.
ScRAM(200)에는 암호 논리 기능을 제어하기 위해서 3종류의 제어 레지스터 REG0 REG3이 마련되어 있다.
제어 레지스터 REG0은 암호 논리를 제어하는 명령이나 모드를 제어하기 위한 레지스터이다. 제어 레지스터 REG1은 암호 논리의 입력 데이터를 유지하는 레지스터이다. 제어 레지스터 REG1의 유지 용량은 최대 4kb이다.
제어 레지스터 REG2는 암호 논리의 출력 결과를 유지하는 레지스터이다. 제어 레지스터 REG2도 그 유지 용량은 최대4kb이다.
다음에, 제어 레지스터 REG0 REG2에 대한 액세스 방법을 설명한다.
외부로부터 제어 레지스터를 액세스하는 것에 의해 ScRAM(200)이 내장하는 암호 논리의 제어, 데이터의 입출력, 저소비 전력화 모드의 제어를 실행할 수 있다.
도 28은 제어 레지스터의 설정에 따른 메모리 맵의 상태 변화를 설명하기 위한 도면이다.
도 28을 참조하면, ScRAM이 내장하는 암호 기능을 제어하기 위해서는 2가지 방법이 있다.
우선, 첫 번째 방법은 제어 레지스터 액세스 인에이블 신호 CRYP로서 외부로 부터 1을 입력하는 것이다. 이것에 의해, X=#3FFF로 표시되는 페이지가 제어 레지스터 영역으로 된다.
두 번째 방법은 제어 레지스터 액세스 인에이블 신호 CRYP가 0인 경우에 SDRAM의 모드 설정을 위해 MRS 명령을 입력할 때, 어드레스 비트 A10으로서 1을 입력하는 것이다. 이 경우에는 어드레스 비트 A11이 0인 경우에는 X=#3FFF로 표시되는 페이지가 제어 레지스터 영역으로 된다. 또, 어드레스 비트 A11이 1인 경우에는 X=#0000으로 표시되는 페이지가 제어 레지스터 영역으로 된다.
ScRAM의 제어 레지스터를 사용하지 않는 경우에는 SDRAM의 모드를 설정하기 위한 통상의 MRS 명령을 A10=0으로 설정함으로써 입력한다. 이 경우, 제어 레지스터 액세스 인에이블 신호 CRYP=0으로 할 필요가 있다. 신호 CRYP나 MRS 명령 입력으로부터 tRSC 이후에는 ScRAM은 새로운 명령에 대해서 동작 가능하게 된다.
제어 레지스터 액세스가 인에이블인 기간, 특정 행어드레스(X=#3FFF 또는 X=#0)의 어드레스 공간에 대해서 정해진 데이터를 기록/판독하는 것에 의해서, 제어용 레지스터 REG0 REG2로 액세스할 수 있다. 이 기간에는 암호를 논리 제어용으로 할당된 4k비트의 어드레스 공간을 메모리로서 이용할 수는 없다. 그 이외의 공간에 대해서는 통상의 메모리 영역으로서 외부로부터 액세스하는 것이 가능하다.
여기서, 제어 레지스터 액세스에 대응하는 어드레스 공간에 외부로부터 액세스한 경우에는 DRAM부(212)에 대해서는 액세스가 실행되지 않는다. 따라서, 제어 레지스터 액세스의 인에이블 상태가 끝나면, 제어 레지스터 영역이던 특정 행어드레스에 대응하는 메모리 공간을 통상의 메모리 공간으로서 액세스할 수 있다. 제 어 레지스터 액세스의 인에이블 상태가 끝나기 전에 레지스터에 설정한 값은 신호 CRYP를 0으로 하여 동작 모드에서 빠져 나온 경우에는 유지된다. 그러나, MRS 명령을 이용하여 동작 모드에서 빠져 나온 경우에는 레지스터에 설정한 값은 리셋된다. 즉, MRS 명령을 입력하는 것에 의해, 레지스터를 리셋할 수 있다.
제어용 레지스터 REG0 REG2에 대한 액세스는 제어용 레지스터에 할당된 어드레스 공간 내에서 범용 SDRAM과 동일한 순서로 액세스하는 것에 의해 실행된다. 제어 레지스터로부터의 판독 데이터는 SDRAM의 모드 레지스터 세트 시에 설정된 동일한 CAS 대기 시간(latency)으로 출력되지만, 제어용의 레지스터로의 액세스 시의 버스트 길이는 1로 고정된다.
다음에, 도 27의 모드 레지스터(208)에 대해서 설명한다.
도 29, 도 30 및 도 31은 도 27에 도시한 모드 레지스트(208)를 설명하기 위한 도면이다.
도 29를 참조하면, 모드 레지스터 세트 명령은 클럭 신호 CLK의 상승 시에 명령 신호 CMD에 포함되는 신호 /CS, /RAS, /CAS, /WE를 모두 L레벨로 설정하는 것으로써 인가되고, 이 때에 어드레스 신호 ADD에 포함되는 어드레스 비트 BA0, BA1, A0 A11에 의해 설정되는 값이 도 30에 도시한 각 비트에 기록된다. 단, 어드레스 비트 A8, A7은 0으로 설정된다. 다른 비트는 도 31에 도시하는 바와 같이 각종 설정으로 할당되고 있다.
모드 레지스터 세트에서는 SDRAM의 모드 설정, SDRAM의 저파워 모드 설정 및 제어 레지스터의 액세스를 실행할 수 있다.
SDRAM의 모드 설정에서는 버스트 길이, 버스트 타입 및 /CAS 대기 시간을 프로그램할 수 있다.
SDRAM의 저파워 모드 설정에서는 비파워 다운모드 시의 프리차지 스탠바이 전류를 저감할 수 있다. 단, 이 모드를 사용하기 위해서는 입력 신호의 셋업 시간을 5ns 이상으로 할 필요가 있다.
제어 레지스터의 액세스에서는 모드 레지스터 세트 시에 비트 A10을 1로 하면, 암호 기능을 제어하기 위한 레지스터 공간이 나타난다. 이 방법은 신호 CRYP를 입력하는 단자의 제어를 실행할 수 없기 때문에, 이 단자를 0으로 고정시킨

시스템에 적합하다. 제어 레지스터로의 액세스는 SDRAM의 액세스 순서와 동일하고, 동일한 /CAS 대기 시간에서 데이터가 출력된다. 그러나, 제어 레지스터의 액세스는 항상 버스트 길이가 1로 고정되어 있다.
모드 레지스터 세트에 의해 세트된 데이터는 다음의 MRS 명령이 입력될 때까지 모드 레지스트에 저장된다. 다음의 MRS 명령은 양 뱅크가 비활성화 상태에 있으면 입력할 수 있다. MRS 명령으로부터 tRSC 후에는 SDRAM은 새로운 명령에 대해서 동작 가능하게 된다. 또, MRS 명령이 입력되면, 제어 레지스터가 리셋된다. 제어 레지스터의 내용을 유지한 채로 제어 레지스터 액세스의 디스에이블과 인에이블을 전환하는 동작은 SDRAM의 모드 레지스터 세트 시에 비트 A10을 0으로 하여 신호 CRYP의 제어를 실행하는 것에 의해서 실현할 수 있다.
도 32는 ScRAM의 암호 제어 입출력에 관련된 상태 천이도이다.
전원 투입이 되면, 초기 상태(340)로 ScRAM의 상태가 천이한다. 계속해서, 신호 CRYP를 1로 하면, 암호 제어가 인에이블인 상태(344)로 천이한다. 한편, 신호 CRYP가 0인 경우라도 모드 레지스터 세트 명령에 의해 비트 A10을 1로 설정하는 것에 의해서, 암호 제어 인에이블 상태(344)로 천이시킬 수 있다.
파워 온의 초기 상태(340)에 있어서, 신호 CRYP를 0으로 설정하고 모드 레지스터 명령에 의해서 비트 A10을 0으로 하면, 암호 제어가 디스에이블인 상태(342)로 천이한다.
상태(342)에서 상태(344)로 천이시키기 위해서는 신호 CRYP를 1로 하는 것에 의한 경우와, 신호 CRYP가 0인 상태이고 모드 레지스터 세트 명령에 의해 비트 A10을 1로 설정하는 것에 의한 경우가 있다.
한편, 암호 제어 인에이블 상태(344)에서 암호 제어 인에이블 상태(342)로 천이시키는 경우를 설명한다. 암호 제어 인에이블 상태(344)로 신호 CRYP를 1로 설정하는 것에 의해 들어간 경우에는 반대로 신호 CRYP를 0으로 설정하는 것에 의해 천이시킬 수 있다. 또, 신호 CRYP를 0으로 설정하고 모드 레지스터 세트 명령에 의해 비트 A10을 1로 설정하여 인에이블 상태(344)로 들어간 경우에는 모드 레지스터 세트 명령에 의해 비트 A10을 0으로 설정하는 것에 의해서 디스에이블 상태(342)로 천이시킬 수 있다.
도 33은 제어 레지스터 액세스의 일예를 도시한 동작 파형도이다.
도 33을 참조하면, 제어 레지스터 액세스 영역으로서 X=#3FFF로 표시되는 페이지가 할당된 경우를 나타낸다. SDRAM의 모드가 CAS 대기 시간 CL=3으로 설정되어 있으므로, 레지스터 출력도 CL=3인 타이밍으로 되어 있다.
여기서, 모드 레지스터 세트에 의해 설정된 버스트 길이 BL에 의존하지 않고, 레지스터 액세스에 관해서는 버스트 길이는 1로 고정된다. 따라서, 판독/기록 명령과 열어드레스를 매(每)사이클 입력할 필요가 있다.
도 34 내지 도 37은 제어 레지스터의 어드레스 맵을 도시한 도면이다.
도 34는 열어드레스가 h00, h01인 경우를 도시한 것이고, 도 35는 열어드레스가 h02인 경우를 도시한 것이고, 도 36은 열어드레스가 h03, h04, h05, h 06인 경우를 도시한 것이다. 도 37은 열어드레스가 h13 h20인 경우에 대해 도시한 것이다.
이들 X어드레스는 X=h3FFF 또는 X=h0 중 어느 하나로 초기 설정된 값이다.
다음에, ScRAM이 내장하는 암호 기능의 특징에 대해서 설명한다.
ScRAM은 네트워크 상의 안전 확보를 위해 사용되고 있는 주요한 암호 방식의 가속 장치를 내장하고 있다. 또, ScRAM은 전자 인증에서 이용되는 공개키 방식과 인증 후의 데이터 송수신에서 이용되는 비밀키 암호 방식의 기능을 지원하고 있다. 이들은 도 27에 도시한 전용의 암호 논리(228)에 의해 처리하므로, 저소비 전력으로서 고속 암호 처리가 필요한 시스템에 적합하다.
지원하는 암호 방식에 대해서는 도 9에 도시한 경우와 마찬가지이고, 공개키 암호 방식으로서 RSA를, 비밀키 암호 방식으로서 DES와 트리플 DES를 지원하고 있다. 또, 비밀키 암호 방식에서는 주요 블럭 암호 모드인 ECB, CBC, OFB, CFB-64를 지원하고 있다.
일반적인 네트워크뿐만 아니라, 인터넷에서도 이들 암호 방식은 주요한 암호 방식으로서 이용되고 있다. ScRAM은 주요한 브라우저인 넷스케이프 커뮤니케이터(Netscape Communicator)나 인터넷 익스플로러(Explorer) 등이나 암호화 전자 메일 방식인 S/MIME에도 대응할 수 있다. 금후의 확대가 기대되는 전자 상거래 시장에서는 이들 암호 방식을 이용한 안전의 확립이 중요하게 될 것으로 고려된다. 또, 휴대 전화에의 운용이 예상되는 무선 애플리케이션 프로토콜(WAP)에서도 상술한 암호화 방식이 지원되기 때문에, ScRAM은 각종 시스템에 폭넓은 적합성이 있다.
ScRAM은 애플리케이션의 적합성을 높이기 위해서, 내부 암호 논리에 의해 암호화로 정밀한 처리만을 담당한다. 즉, 해쉬(hash), 데이터 인코딩, 패딩(padding) 등의 처리는 종래와 같이 소프트웨어 측에서 담당하게 되어 애플리케이션 측의 자유도를 높이도록 고려되고 있다. 또, RSA에서는 소프트웨어 처리 시에 필요로 하는 처리 시간의 대부분을 차지하고 있던 다음의 a) 및 b)의 연산만을 처리한다.
a) RSA에 의한 전자 인증을 고속화하기 위해서
누승 잉여 연산 $M^{e} \bmod N$,
몽고메리 승산 잉여 연산 $X*Y*R^{-1} \bmod N$,
잉여 연산 Y mod N을 실시한다.
b) 암호화 통신의 고속화를 하기 위해서, 트리플 DES, DES(CBC, ECB, OFB, CFB-64)의 연산을 실행한다. 단, 최종 텍스트 블럭부의 패딩 처리는 규격에 따라서 다양하므로, 적절하게 소프트웨어로 처리할 필요가 있다.
계속해서, 암호 처리 속도에 대해서 설명한다.
어드레스 처리 전용 논리와 DRAM의 원칩(One-chip)화에 의해서 고속화와 저소비 전력화를 실현하고 있다. 그 결과, 휴대 단말에 적합한 저전원 전압(2.5V계)에서 1024bit의 RSA 암호 서명 처리 시간이 100 200ms 정도로 된다. 즉, 트리플 DES인 경우에 약 60Mbps, DES이면 약 180Mbps의 성능을 실현할 수 있다.
또, ScRAM은 특정 어드레스 공간을 액세스하는 것에 의해 암호 논리 부분을 제어하고 있으므로, 범용 SDRAM과 핀 교환을 실현할 수 있다. 또, 암호 기능을 디스에이블로 하면, SDRAM으로서의 기능만을 사용할 수도 있다.

계속해서, 암호 기능 제어 방법에 대해서 설명한다.
앞서 설명한 바와 같이, ScRAM에 내장하고 있는 암호 기능의 제어는 제어 레지스터에 대해서 액세스를 실행하는 것에 의해 실행할 수 있다. 제어 레지스터로 액세스하기 위해서는 모드 레지스터 세트 시에 소정의 어드레스를 입력하거나, 신호 CRYP가 인가되는 단자를 1로 설정하여 특정 어드레스로 액세스하는 것에 의해 제어 레지스터로 액세스할 수 있다. 여기서, 제어 레지스터에 할당된 불량(default)의 어드레스 공간은 X=h3FFF로 표시되는 페이지이다. 또, MRS 명령 입력 시에 비트 A10, A11을 모두 1로 설정하면, X=h0으로 표시되는 페이지에 제어 레지스터를 할당할 수도 있다.
그러나, 펌웨어 설계에서는 제어 레지스터 액세스를 위해 예약된 공간을 그 이외의 용도로 사용하지 않는 것이 요구된다. 예컨대, 애플리케이션이나 커넬에 이 공간을 할당하는 것을 금지하지 않으면 안된다. 커넬에 대해서는 부트 시에 할당되지 않도록 주의할 필요가 있다.
계속해서, 시스템 설계의 예를 설명한다.
도 38은 신호 CRYP를 인가하는 단자를 제어할 수 있는 시스템을 설명하기 위한 도면이다.
도 38을 참조하면, 일반 마이크로 컴퓨터(MCU)가 구비하고 있는 I/O포트를 CRYP 신호를 받는 단자에 접속할 수 있는 시스템에 대해서 예시하고 있다. 이 구성에서는 시스템의 부트 전에 CRYP 단자를 0으로 할 수 있으면, 제어 레지스터에 할당된 어드레스 공간이 나타나 있지 않기 때문에, 프로그램을 초기 로드하는 공간에는 제약이 없다. 프로그램이 로드된 영역이 X=h3FFF를 포함하고 있는 경우에는 그 후에 CRYP 단자를 1로 설정하여, 제어 레지스터에 할당된 어드레스 공간을 X=h0으로 표시되는 페이지로 변경할 필요가 있다.
도 39 및 도 40은 CRYP 단자를 제어할 수 없는 시스템에 대해서 설명하기 위한 도면이다.
도 39를 참조하면, CRYP 단자에 인가하는 값을 0으로 고정시킨 경우에는 ScRAM의 모드 레지스터 세트(MRS) 입력 시에 비트 A10을 1로 하여 제어 레지스터로의 액세스를 인에이블로 한다. 이 때, 비트 A11에 의해 프로그램이 로드되어 있지 않은 공간을 선택한다.
도 40을 참조하면, CRYP 단자에 인가하는 값을 1로 고정시킨 경우에는 X=h3FFF로 표시되는 페이지에 제어 레지스터로의 액세스 공간이 할당되므로, 이 공간을 피해서 프로그램의 로드를 실행할 필요가 있다.
도 41은 제어 레지스터로의 설정을 설명하기 위한 동작 파형도이다.
도 41을 참조하면, 제어 레지스터의 설정에 대해서 신호 입력의 일예가 도시된다. 제어 레지스터로의 액세스에서 DRAM과 유일하게 다른 점은 MRS의 설정에 의존하지 않고 버스트 길이가 1로 되는 점이다. 그 이외에 대해서는 DRAM과 동일한 타이밍에서 또한 동일한 순서로 제어 레지스터에 대해서 액세스를 실행한다.
도 41에서는 제어 레지스터로 액세스하기 위한 어드레스 공간이 X=h3FFF인 경우를 예로서 도시하고 있다.
우선, 시각 t1에 있어서, 제어 레지스터로 액세스하기 위한 어드레스 X=h3FFF가 입력된다.
계속해서, 시각 t2에 있어서, 소프트 리셋이 된다.
시각 t3에서는 모드 설정 (1)이 실행된다. 모드 설정 (1)은 비밀키 암호 방식으로서 DES-56을 선택하고, CBC 모드에서 처리를 실행하는 모드 설정이다.
계속해서, 시각 t4에서는 모드 설정(2)이 실행된다. 모드 설정(2)은 암호화, REG1과 REG2의 어드레스 카운터를 리셋하고 초기값으로서 IV를 사용한다는 모드가 설정된다.
시각 t5 t6에서는 비밀키가 입력된다.
시각 t6 t7에서는 초기 벡터 IV가 입력된다.
시각 t7 t8에서는 8바이트 단위의 평문을 입력하고, 평문 입력 후 시각 t8 에 있어서 EOF(End of File)의 입력이 실행된다.
그리고, 시각 t9에서는 플래그 영역에 대한 판독을 실행하고, 암호 논리가 처리 중인지 여부를 체크한다.
이 체크 결과는 CAS 대기 시간에 의해 데이터 신호 DQ로서 판독된다.
계속해서, ScRAM이 지원하는 비밀키 암호 방식에 대해서 설명한다.
도 42 도 44는 암호화 처리의 기본 단위에 대해서 도시한 개략도이다.
도 42는 키의 길이가 56bit인 DES를 도시한 것이고, 도 43은 키의 길이가 112bit인 트리플 DES 방식을 도시한 것이고, 도 44는 키의 길이가 168bit인 트리플 DES 방식에 대해서 도시한 것이다. ScRAM에서는 비밀키 암호화 방식으로서 DES와 트리플 DES를 지원하고 있다. 인터넷의 안전 소켓 레이어, S/MIME의 전자 메일, 무선 애플리케이션 프로토콜에서 이들 암호화 방식이 이용되고 있다. 또한, 트리플 DES는 DES를 암호화-복호화-암호화의 3회 처리를 실행한 것이다.
도 45 내지 도 47은 복호화 처리의 단위에 대해서 도시한 개략도이다.
도 45는 도 42의 암호화에 대응하는 복호화를 도시한 것이고, 도 46은 도 43의 암호화에 대응하는 복호화를 도시한 것이고, 도 47은 도 44의 암호화에 대응하는 복호화를 도시한 것이다.
계속해서, ScRAM이 지원하는 비밀키 암호의 암호 이용 모드에 대해서 설명한다. 예로서 ECB, CBC의 2개의 모드에 대해서 설명한다.
도 48 및 도 49는 ECB 모드에 대해서 설명하기 위한 도면이다.
도 48 및 도 49를 참조하면, ECB 모드는 기본 모드이고, 암호/복호 처리 기 본 단위에 해당한다. 암호화에서는 통상의 데이터(평문) M을, 도 48에 도시한 바와 같이, 64비트마다 분해한 블럭 Mi(M=M1, M2, M3…)를 송신자와 수신자만이 공통으로 갖는 비밀의 키라고 불리는 데이터 K를 이용하여 각 블럭마다 암호화 처리를 실행한다. 그리고, 64 비트의 암호문 Ci(C=C1, C2, C3…)가 생성된다. 복호화에서는, 도 49에 도시한 바와 같이, 65비트의 암호문 Ci를 수취하여, 암호화에 이용한 것과 동일한 키 데이터 K를 이용하여 평문 Mi(M=M1, M2, M3…)를 생성한다.
다음에, CBC 모드에 대해서 설명한다.

도 50은 CBC 모드의 연산을 설명하기 위한 도면이다.
도 50을 참조하면, CBC 모드에서는 우선 암호화는 평문 M을 64비트마다 분해한 블럭 Mi를 ECB 모드와 마찬가지로 암호화를 실행한다. 그리고, 또 이 암호문 블럭 Ci와 다음의 블럭 Mi+1과의 배타적 논리합을 다음의 암호화 입력으로 한다. 이것을 반복해서 차례차례 연쇄시키는 것이다.
한편, 복호화는 암호 블럭문 Ci를 ECB 모드와 마찬가지로 복호화한 결과를 Mi로 하고, Ci와 다음의 암호문 블럭 Ci+1의 복호 결과와의 배타적 논리합을 취해 출력 평문 블럭 Mi+1로 한다. 이것을 반복해서 차례차례 연쇄시키는 것이다. 또한, 도 50에 있어서, 평문은 Mi, 암호문은 Ci(i=1, 2, …), 암호키 K를 이용한 암호화를 Ek, 복호화를 Dk로 한다. 또, IV(초기 벡터)는 초기값으로서, 최초의 암호화와 복호화 시에 이용된다. IV는 암호 측과 복호 측에서 동일한 값을 이용한다. IV의 값은 제 3 자에게 알려져도 좋으므로, IV는 송신자와 수신자 사이에서 비밀로 보낼 필요가 없다. IV의 값을 변경하면, 동일한 메세지로부터 다른 암호문이 생성된다.
도 51은 CBC 모드에 있어서의 암호화의 개요를 도시한 개념도이다.
도 52는 CBC 모드에 있어서의 복호화의 개요를 도시한 개념도이다.
도 51 및 도 52를 참조하면, ScRAM에 한번에 입력 가능한 평문 길이는 레지스터 REG1의 사이즈인 4k비트이다. 따라서, 4k비트보다 긴 평문을 처리하는 경우에는 직전의 암호문 블럭 Ci가 초기값으로 되도록 제어 레지스터에 대해서 설정을 실행한다.
본 명세서의 실시예에서는 SDRAM에 본 발명을 적용한 경우를 예로 들어 설명했지만 SDRAM에 제한되는 것은 아니며, 비동기형의 DRAM, 예컨대 EDO(Extended Data 0ut) DRAM 등에도 본 발명을 적용할 수도 있다. 또, 동기형의 다른 DRAM, 예컨대 DDR(Double Data Rate)형의 인터페이스를 갖는 DRAM 등이더라도 본 발명을 적용하는 것이 가능하다.

발명의 효과

본 발명에 따르면, 범용적인 메모리에 대해서 데이터, 어드레스 및 제어 신호를 인가하는 것과 마찬가지 순서로 신호를 인가하는 것에 의해 내장하는 논리 회로를 제어할 수 있고, 기존의 시스템에 큰 변경을 가할 필요가 없어 용이하게 제어할 수 있다. 또한, 마이크로 컴퓨터 시스템에 있어서, 논리 내장의 반도체 기억 장치를 용이하게 제어할 수 있다. 그리고, 최소한의 제어 단자의 추가에 의해 내장 메모리에 어드레스나 데이터를 인가하는 경로를 유효하게 사용하여 내장하는 논 리 회로의 제어를 실행할 수 있는 것이다.

(57) 청구의 범위

청구항 1.
외부로부터 인가되는 제어 신호, 어드레스 신호 및 데이터를 수신하는 단자군과,
행렬 형상으로 배치되는 복수의 메모리셀을 포함하는 메모리셀 어레이와,
상기 단자군에 인가되는 상기 어드레스 신호가 소정의 제 1 영역을 지정했을 때에 상기 제어 신호, 상기 어드레스 신호 및 상기 데이터 중 적어도 어느 하나에 따라 데이터 처리를 행하는 논리 회로와,
상기 단자군에 인가되는 상기 어드레스 신호가 상기 제 1 영역 이외를 지정했을 때에 상기 제어 신호, 상기 어드레스 신호에 따라 상기 메모리셀 어레이의 대응하는 어드레스의 메모리셀에 데이터의 송수신을 행하는 메모리 회로
를 구비하는 반도체 기억 장치.

청구항 2.
제 1 항에 있어서,
상기 단자군으로부터 상기 제어 신호, 상기 어드레스 신호 및 상기 데이터를 수신하고, 상기 어드레스 신호에 따라 상기 메모리셀 어레이와 상기 논리 회로 중 어느 일방에 대해, 상기 제어 신호, 상기 어드레스 신호 및 상기 데이터 중 적어도 어느 하나에 따른 동작을 지시하는 인터페이스부를 더 구비하되,
상기 논리 회로는,
상기 인터페이스부로부터의 지시 내용을 유지하는 데이터 유지부와,
상기 데이터 유지부의 유지 내용에 따라 데이터 처리를 행하는 데이터 처리 회로
를 포함하는 반도체 기억 장치.

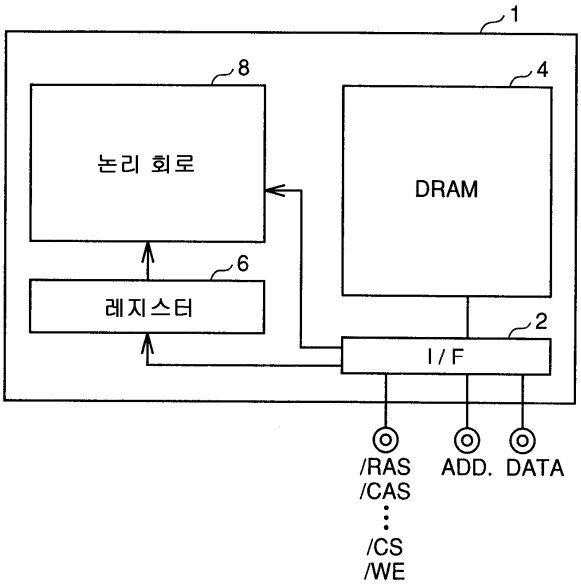
청구항 3.
외부로부터 인가되는 제어 신호, 어드레스 신호 및 데이터를 수신하는 제 1 단자군과,
행렬 형상으로 배치되는 복수의 메모리셀을 포함하고, 외부로부터 인가되는 선택 신호에 따라 활성화되며, 상기 어드레스 신호에 의해 지정되는 영역의 메모리셀에 대해 상기 제어 신호에 따라 상기 데이터의 송수신을 행하는 메모리와,
상기 선택 신호에 따라 상기 메모리와 상보적으로 활성화되고, 상기 어드레스 신호 및 상기 데이터 중 적어도 어느 하나에 따라 데이터 처리를 행하는 논리 회로와,
상기 선택 신호를 수신하는 제 2 단자
를 구비하는 반도체 기억 장치.

청구항 4.
제 3 항에 있어서,
상기 메모리는, 상기 제 1 단자군에 시분할적으로 인가되는 행 어드레스 신호와 열 어드레스 신호를 포함하는 상기

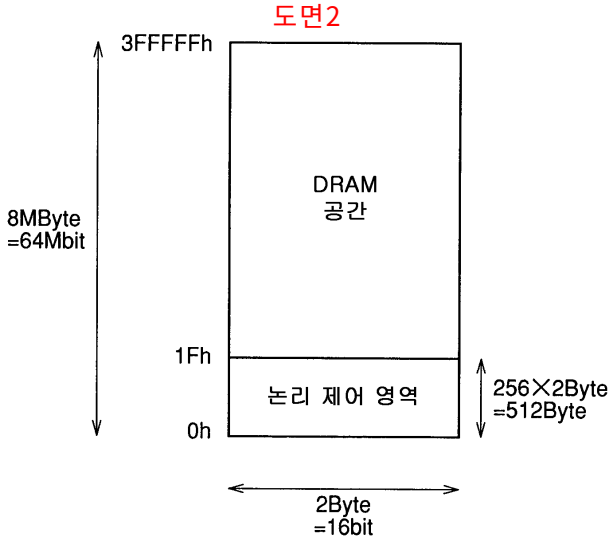
어드레스 신호에 따라 상기 메모리셀의 선택 동작을 행하고,
상기 논리 회로는, 상기 제 1 단자군에 일괄하여 인가되는 상기 어드레스 신호에 따라 동작을 행하는 반도체 기억 장치.

도면

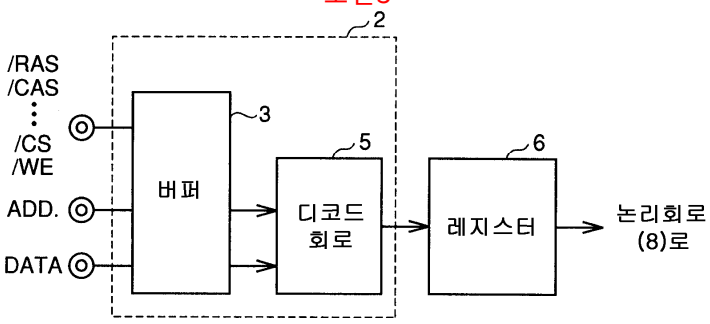
도면1



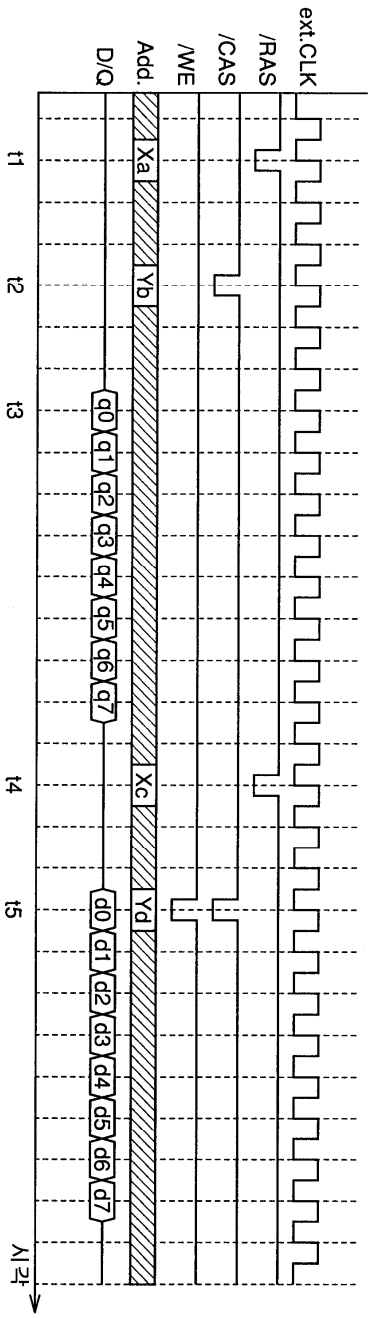
도면2



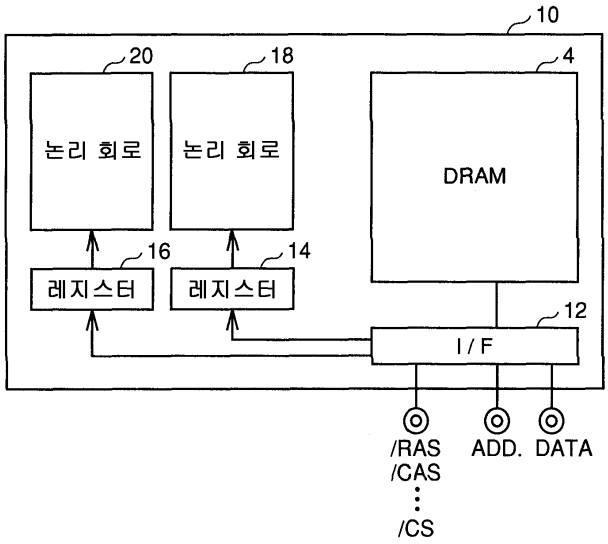
도면3



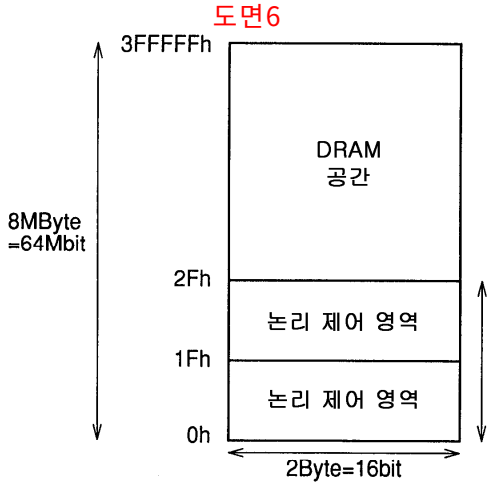
도면4


ext.CLK
/RAS
/CAS
/WE
Add.
D/Q
t1
t2
t3
t4
t5
시각
Xa
Yb
Xc
Yd
q0
q1
q2
q3
q4
q5
q6
q7
d0
d1
d2
d3
d4
d5
d6
d7

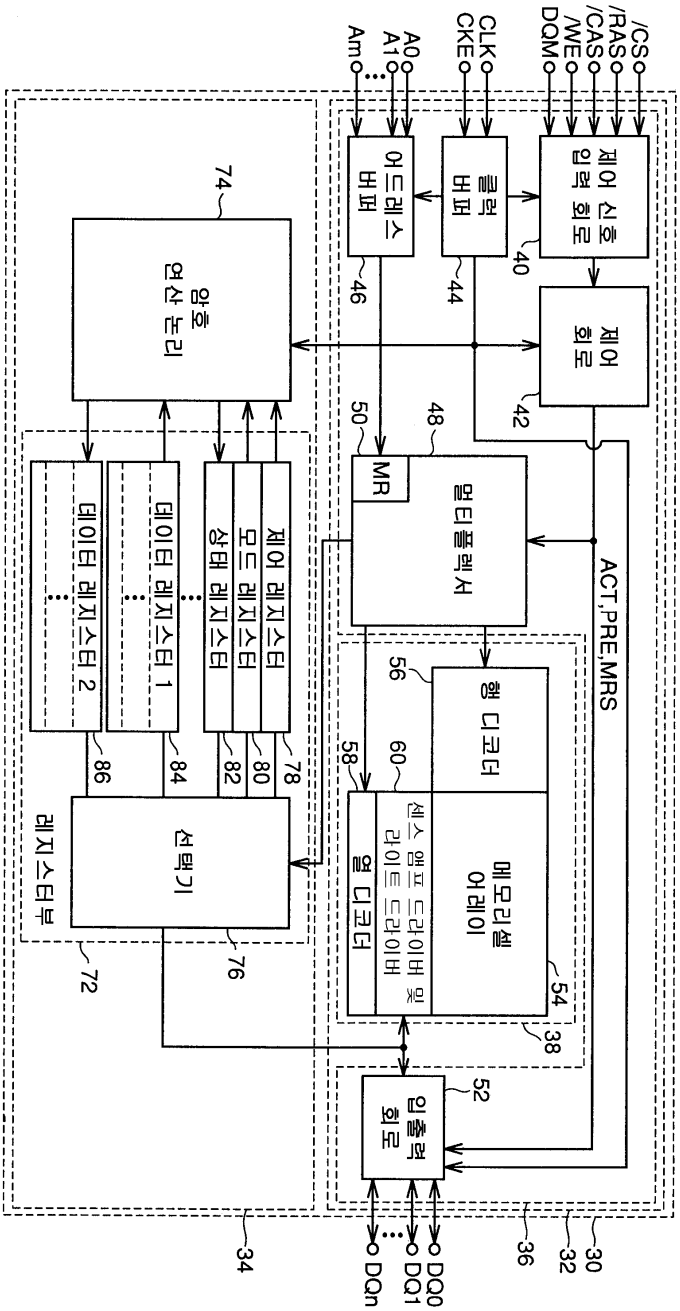
도면5


10
20
18
4
논리 회로
논리 회로
DRAM
16
14
레지스터
레지스터
12
I / F
/RAS
/CAS
/CS
ADD.
DATA

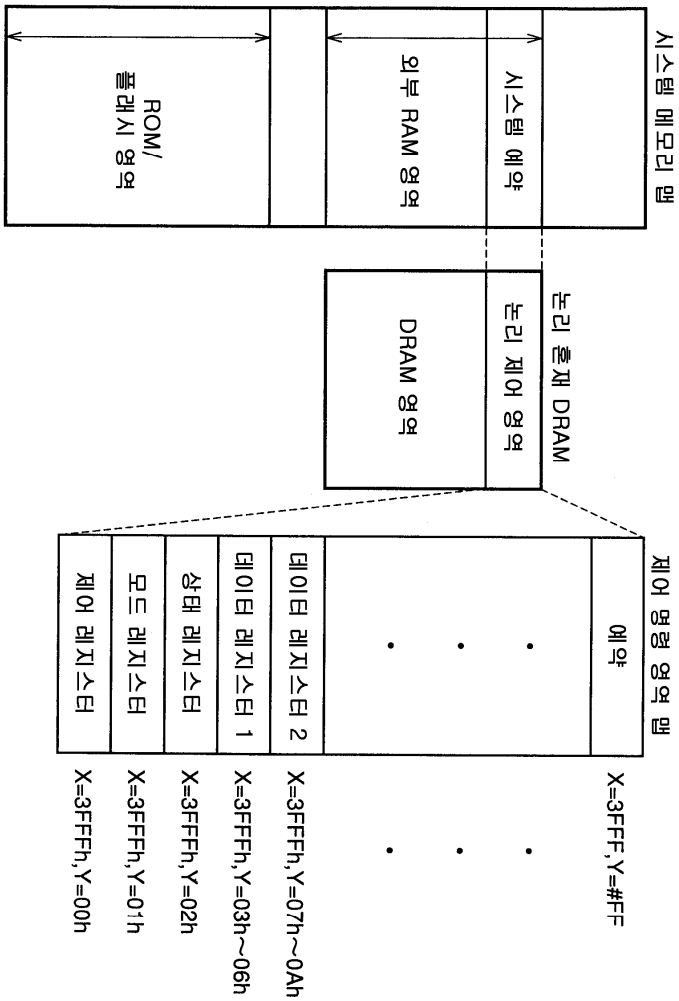
도면6


3FFFFFh
DRAM
공간
8MByte
=64Mbit
2Fh
논리 제어 영역
1Fh
논리 제어 영역
0h
2Byte=16bit

도면7


A0
A1
Am
CLK
CKE
/CS
/RAS
/CAS
/WE
DQM
어드레스 버퍼
클럭 버퍼
제어 신호 입력 회로
제어 회로
연산 논리
MR
멀티플렉서
ACT,PRE,MRS
행 디코더
열 디코더
센스 앰프 드라이버 및 라이트 드라이버
메모리셀 어레이
입출력 회로
데이터 레지스터 2
데이터 레지스터 1
제어 레지스터
모드 레지스터
상태 레지스터
선택기
레지스터부
DQn
DQ1
DQ0
74
46
44
40
42
50
48
56
58
60
54
38
52
86
84
82
80
78
72
76
34
36
32
30

도면8



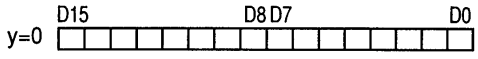
도면9

공개키 암호 방식	비밀키 암호 방식	
		블럭 암호화 모드
RSA	DES Triple DES	ECB:Electric Code Book CBC:Cipher Block Chaining OFB:Output Feed Back CFB:Cipher Feed Back

지원하는 암호 방식

도면10

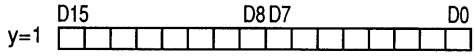
·공개키와 비밀키 방식 공통



D0 =1: 암호 기능 리셋
D1 =1: 암호 처리 중을 나타내는 플래그
(0을 확인하고나서 액세스 함)

도면11

·비밀키 방식의 제어

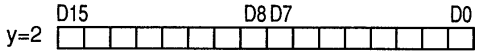


D1,0=01/10/00: DES/Triple DES/ 홀드
(암호 방식 선택, 그 외는 금지)

D5-2=0001/0010/0100/1000/0000: ECB/CBC/OFB/CFB64/ 홀드
(블럭 암호화 모드 선택, 그 외 조합은 금지)

D8-6=001/010/100/000: 통상/블럭/버퍼/홀드
(데이터 처리 모드, 그 외 조합은 금지)

도면12

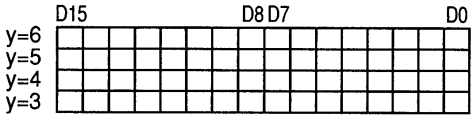


D1,0=01/10/00: 암호화/복호화/홀드(11은 금지)

D5,4=01/10/00: 평문 또는 암호문의 입력 개시/
정지/홀드 (11은 금지)

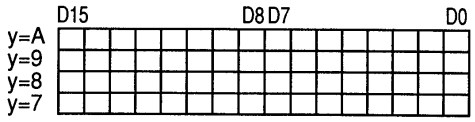
D9-6=1000-0001/0000:OFB, CFB의 1블럭 중의 텍스트 길이
(바이트 단위)/홀드 (그 외 조합은 금지)

도면13



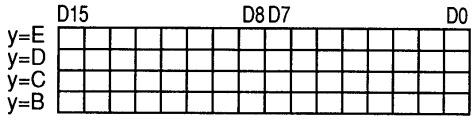
키1(최장 64비트):DES의 키,
Triple DES의 EDE의 E에 대한 키

도면14



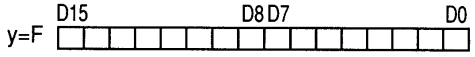
키2(최장 64비트):Triple DES의
EDE의 D에 대한 키

도면15



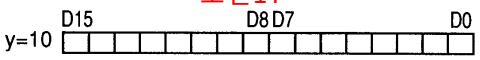
IV(Initial Vector): 초기 벡터

도면16



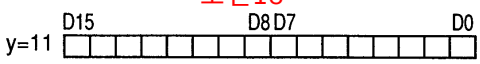
블럭 길이:바이트 단위로 설정
Max=2kByte(D=#FF) Min=1Byte(D=#0)

도면17



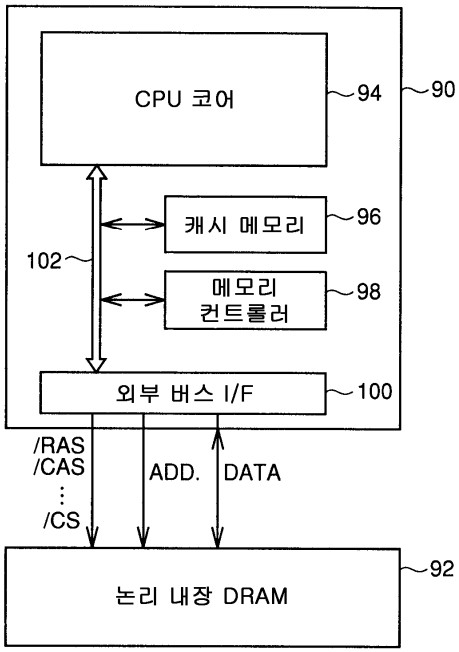
버퍼 개수:버퍼 모드에서 유효
Max=64k(D=#FFFF) Min=1(D=#0)

도면18

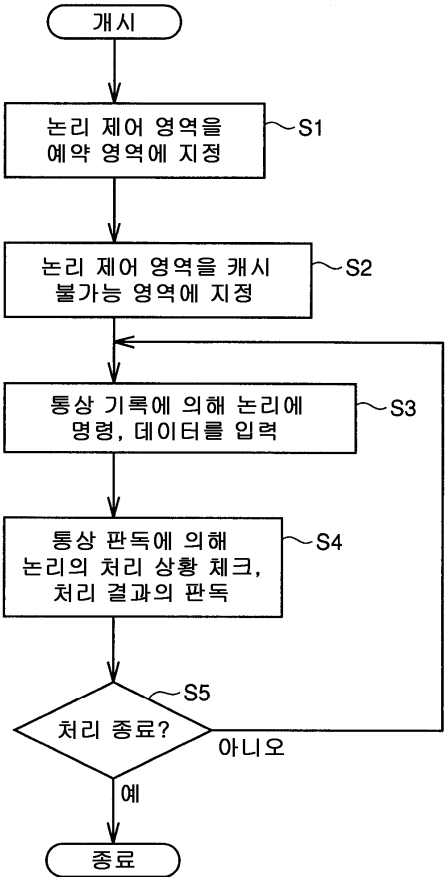


버퍼 ID

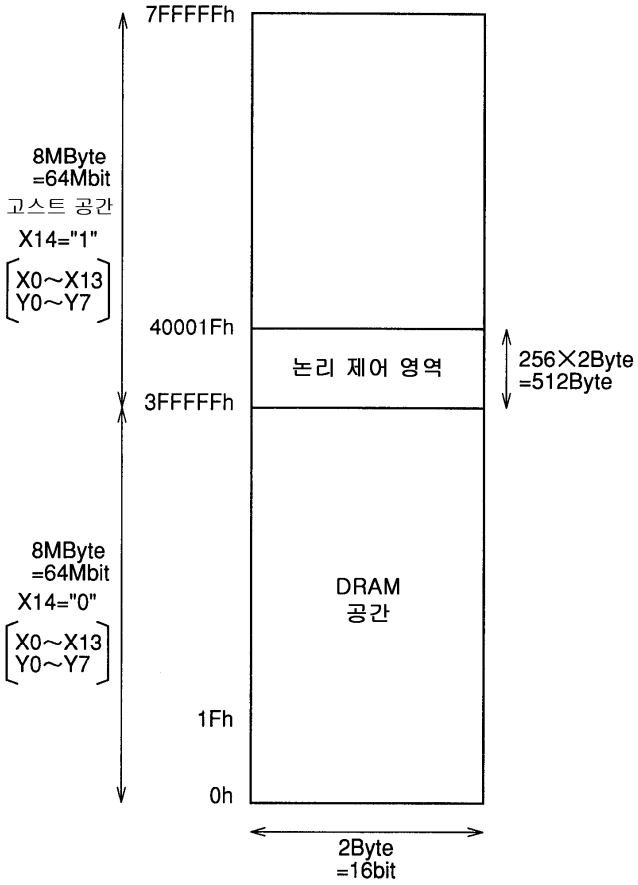
도면19


CPU 코어
94
90
캐시 메모리
96
102
메모리
컨트롤러
98
외부 버스 I/F
100
/RAS
/CAS
/CS
ADD.
DATA
논리 내장 DRAM
92

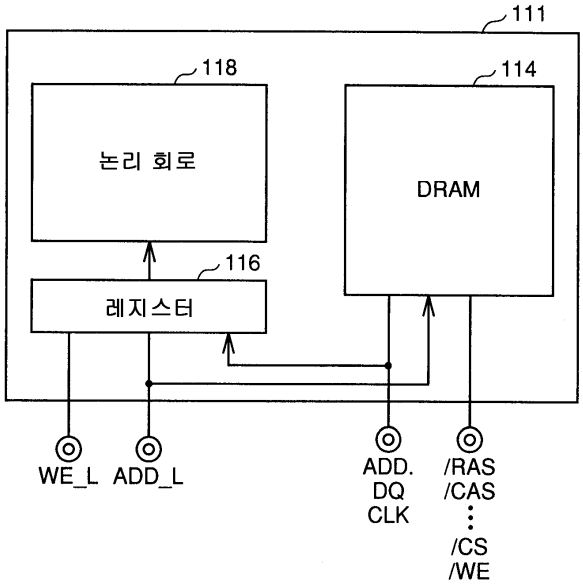
도면20


개시
논리 제어 영역을
예약 영역에 지정
S1
논리 제어 영역을 캐시
불가능 영역에 지정
S2
통상 기록에 의해 논리에
명령, 데이터를 입력
S3
통상 판독에 의해
논리의 처리 상황 체크,
처리 결과의 판독
S4
S5
처리 종료?
아니오
예
종료

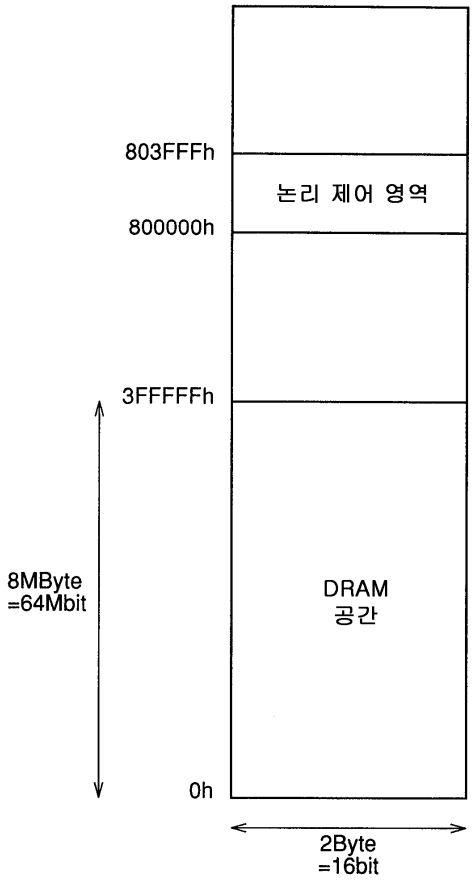
도면21


7FFFFFh
8MByte
=64Mbit
고스트 공간
X14="1"
X0~X13
Y0~Y7
40001Fh
논리 제어 영역
256×2Byte
=512Byte
3FFFFFh
8MByte
=64Mbit
X14="0"
X0~X13
Y0~Y7
DRAM
공간
1Fh
0h
2Byte
=16bit

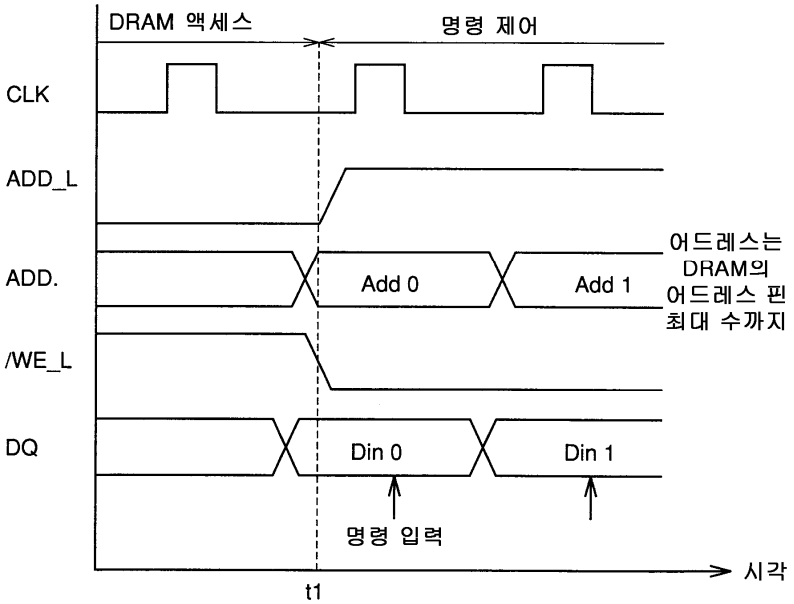
도면22


111
118
논리 회로
114
DRAM
116
레지스터
WE_L
ADD_L
ADD.
DQ
CLK
/RAS
/CAS
/CS
/WE

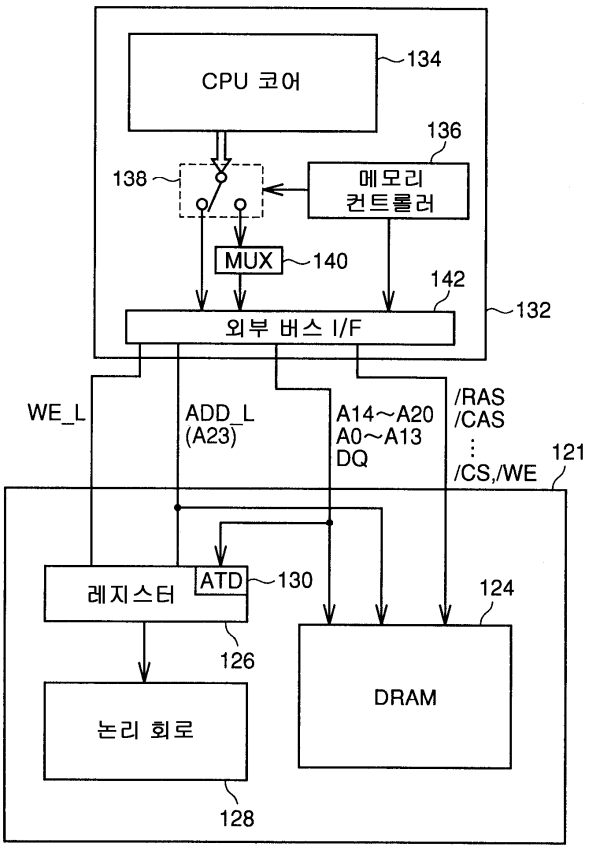
도면23


803FFFh
논리 제어 영역
800000h
3FFFFFh
8MByte
=64Mbit
DRAM
공간
0h
2Byte
=16bit

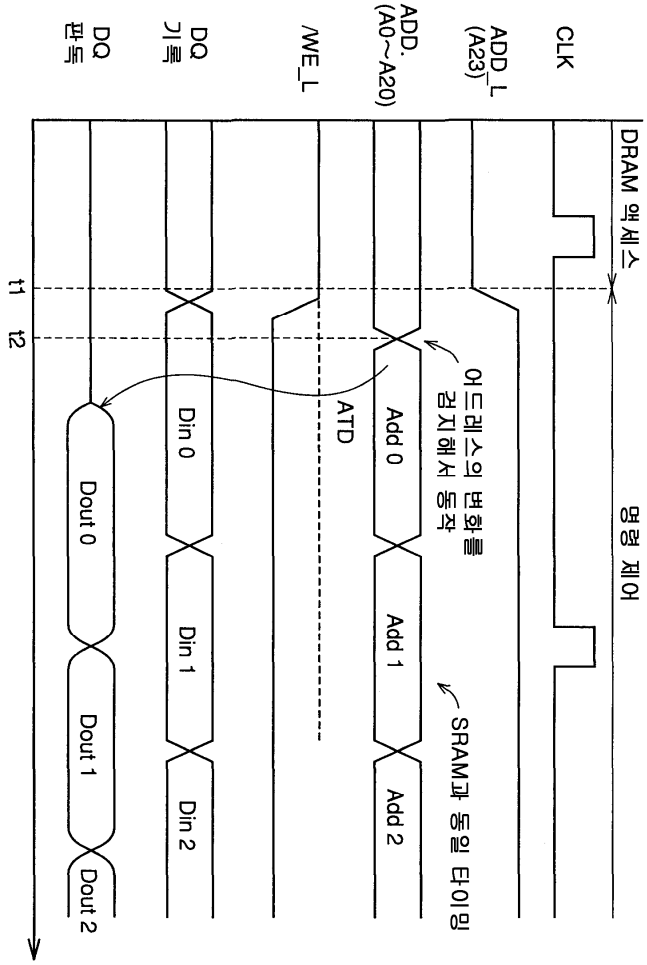
도면24


DRAM 액세스
명령 제어
CLK
ADD_L
ADD.
Add 0
Add 1
어드레스는
DRAM의
어드레스 핀
최대 수까지
/WE_L
DQ
Din 0
Din 1
명령 입력
시각
t1

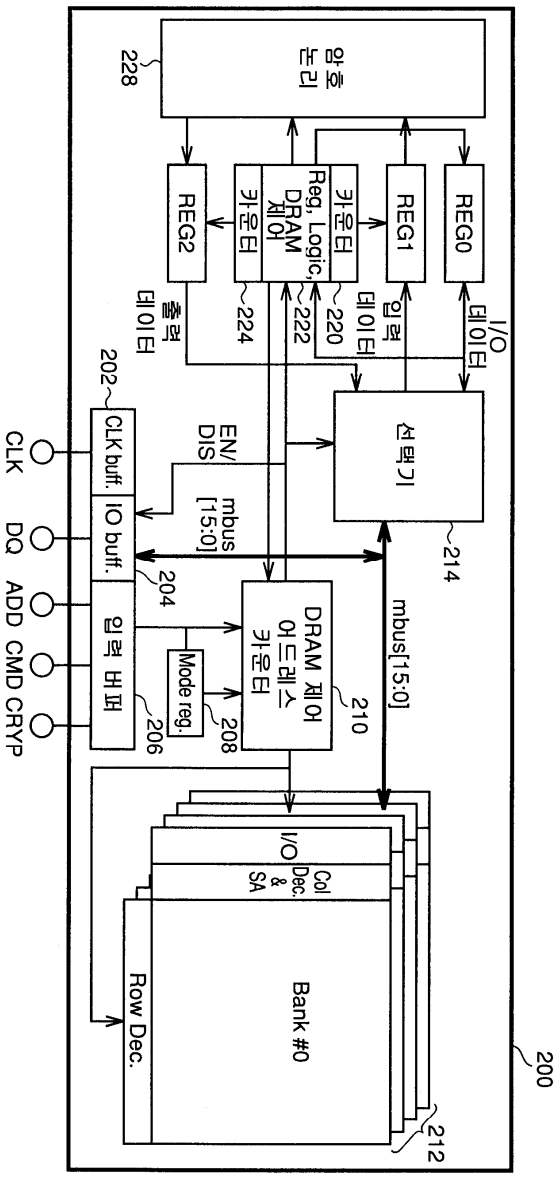
도면25


CPU 코어
134
136
138
메모리
컨트롤러
MUX
140
142
132
외부 버스 I/F
WE_L
ADD_L
(A23)
A14~A20
A0~A13
DQ
/RAS
/CAS
/CS,/WE
121
레지스터
ATD
130
124
126
DRAM
논리 회로
128

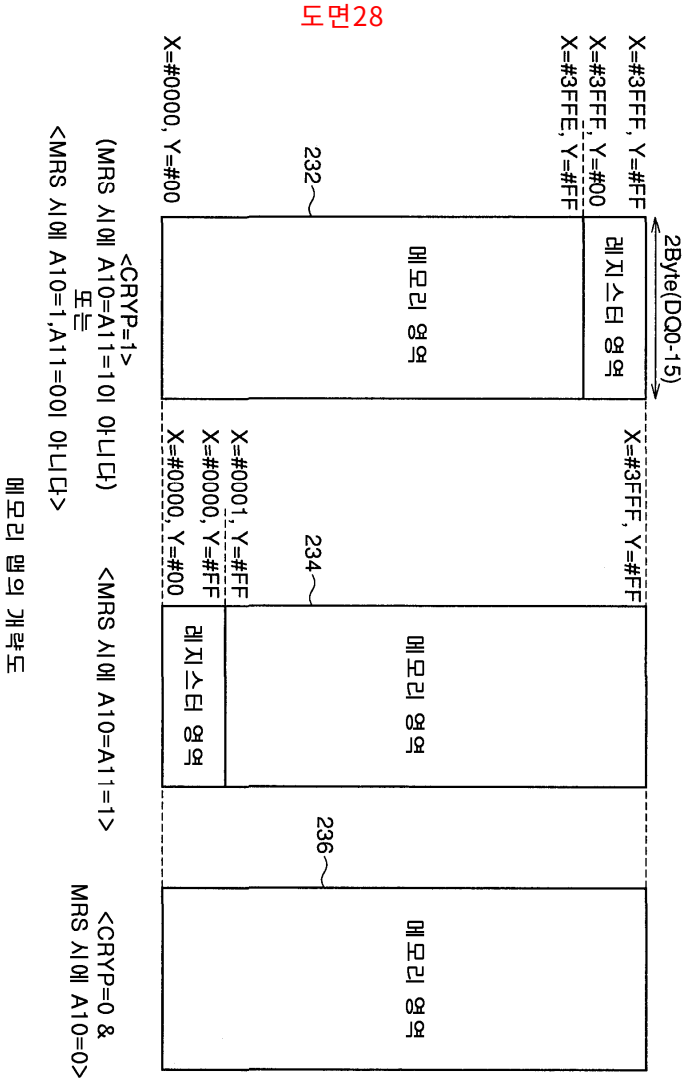
도면26


DQ 판독
DQ 기록
/WE_L
ADD. (A0~A20)
ADD_L (A23)
CLK
DRAM 액세스
t1
t2
Dout 0
Din 0
ATD
Add 0
어드레스의 변화를 검지해서 동작
Dout 1
Din 1
Add 1
SRAM과 동일 타이밍
Dout 2
Din 2
Add 2
명령 제어

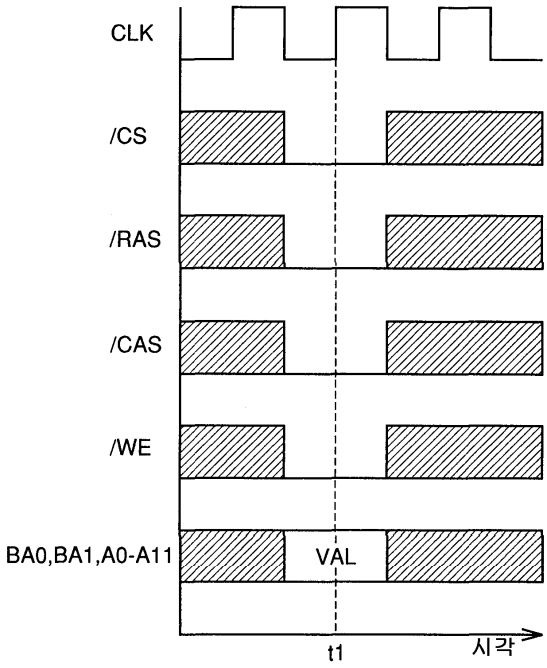
도면27


228
암호 논리
REG2
REG1
REG0
Reg, Logic, DRAM 제어
카운터
카운터
224
222
220
출력 데이터
입력 데이터
I/O 데이터
202
CLK buff.
IO buff.
입력 버퍼
206
204
EN/DIS
mbus [15:0]
선택기
214
Mode reg.
208
DRAM 제어 어드레스 카운터
210
mbus[15:0]
CLK
DQ
ADD
CMD
CRYP
I/O
Col Dec. & SA
Row Dec.
Bank #0
212
200

도면28



도면29

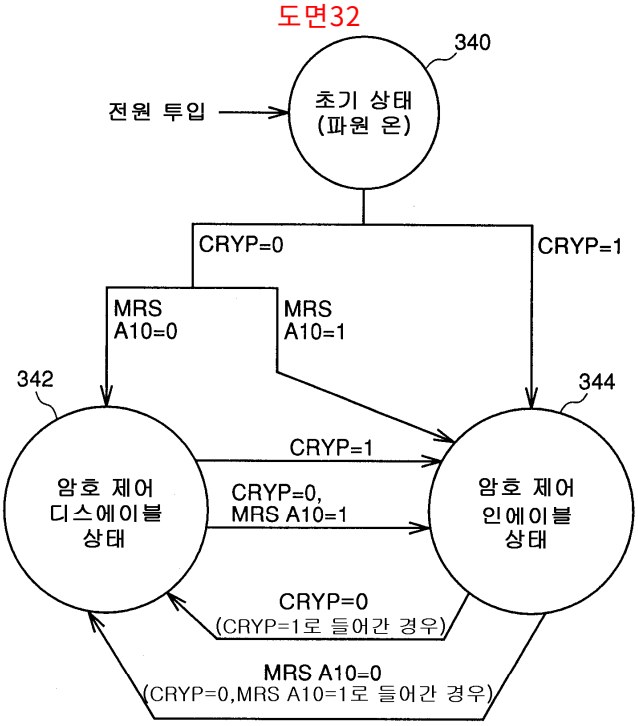


도면30

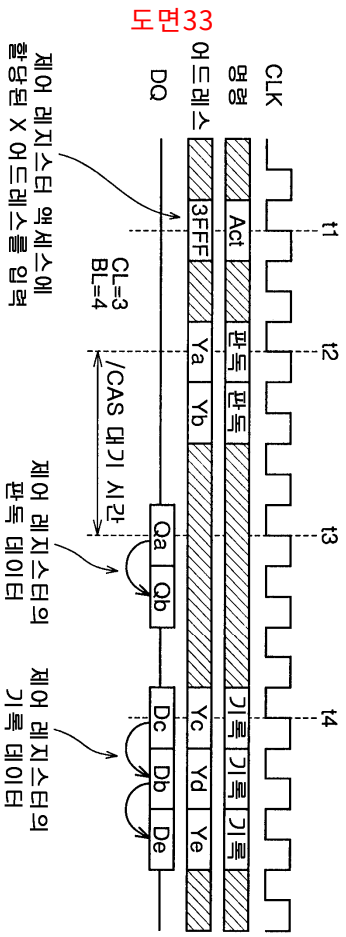
도면31

비트	이름	설명	
A2..0	버스트 길이	000 001 010 011 100 101 110 111	1 2 4 8 R R R 모든 페이지
A3	버스트 타입	0 1	시퀀셜 인터리브
A6..4	CAS 대기 시간	000 001 010 011 1XX	R R 2 3 R
A9	기록 모드	0 1	버스트 단일 비트
A10	제어 레지스터 액세스	0 1	디스에이블 인에이블
A11	제어 레지스터 어드레스	0 1	X=3FFF X=0
BA1	저파워 모드	0 1	디스에이블 인에이블
BA0	저 클럭 주파수	0 1	디스에이블 인에이블

도면32



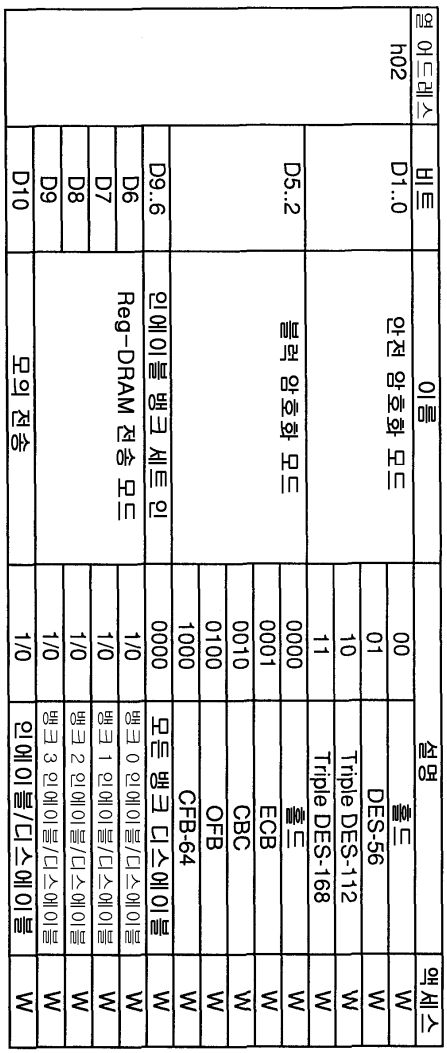
도면33


CLK
명령
어드레스
DQ
t1
t2
t3
t4
Act
판독
판독
기록
기록
기록
3FFF
Ya
Yb
Yc
Yd
Ye
Qa
Qb
Dc
Db
De
CL=3
BL=4
/CAS 대기 시간
제어 레지스터 액세스에
할당된 X 어드레스를 입력
제어 레지스터의
판독 데이터
제어 레지스터의
기록 데이터

도면34

열 어드레스	비트	이름	설명		액세스
h00	D0	소프트웨어 리셋	1	리셋	W
	D1	폴래그	0	완료	R
			1	프로세싱	R
	D2	레지스터 제어용 어드레스로 전환	1	X=h3FFF	W
	D3	레지스터 제어용 어드레스로 전환	1	X=h0	W
	D4	EOF(End of File)	1		W
h01	D1	부분 리프레시	1/0	뱅크 0 인에이블/디스에이블	W
	D2		1/0	뱅크 1 인에이블/디스에이블	W
	D3		1/0	뱅크 2 인에이블/디스에이블	W
	D4		1/0	뱅크 3 인에이블/디스에이블	W
	D5	LP 모드	1/0	인에이블/디스에이블	W
	D6	저클럭 주파수	1/0	인에이블/디스에이블	W

도면35



워드 어드레스	비트	이름	설명	액세스
h02	D1..0	안전 암호화 모드	00 홀드	W
			01 DES-56	W
			10 Triple DES-112	W
			11 Triple DES-168	W
	D5..2	블럭 암호화 모드	0000 홀드	W
			0001 ECB	W
			0010 CBC	W
			0100 OFB	W
			1000 CFB-64	W
	D9..6	인에이블 뱅크 세트 인	0000 모든 뱅크 디스에이블	W
	D6	Reg-DRAM 전송 모드	1/0 뱅크 0 인에이블/디스에이블	W
	D7		1/0 뱅크 1 인에이블/디스에이블	W
	D8		1/0 뱅크 2 인에이블/디스에이블	W
	D9		1/0 뱅크 3 인에이블/디스에이블	W
	D10	모의 전송	1/0 인에이블/디스에이블	W

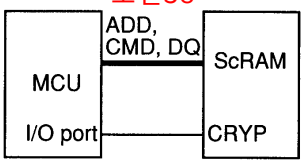
도면36

열 어드레스	비트	이름	설명		액세스
h03	D1..0	ENC/DEC	00	홀드	W
			01	암호화	W
			10	해독화	W
			11	RFU	W
	D2	레지스터1의 카운터	1	리셋	W
	D3	레지스터2의 카운터	1	리셋	W
	D4	IV 로드	0	이전 출력	W
			1	IV 로드	W
	D8..5	블럭당 문서 길이	0000	홀드	W
			Else	(D8..5)X1바이트	W
h04	D15..0	레지스터1 액세스	-	기록 데이터:D15..0	W
h05	D15..0	레지스터2 액세스	-	판독 데이터:D15..0	R
h06	D0	Reg-DRAM 전송	1	모드 입력	W
	D1		1	모드 출력	W
	D2		1	레지스터1의 카운터 리셋	W
	D3		1	레지스터1의 카운터 리셋	W

도면37

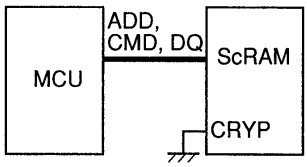
워드 어드레스	비트	이름	설명	액세스
h13-h10	D15..0	DES, Triple DES용 키1	LSB: h10[D0] USB: h13[D15]	키1 입력	W
h17-h14	D15..0	Triple DES용 키2	LSB: h14[D0] USB: h17[D15]	키2 입력	W
h1B-h18	D15..0	Triple DES-168용 키3	LSB: h18[D0] USB: h17B[D15]	키3 입력	W
h1F-h1C	D15..0	초기 벡터(IV)	LSB: h1C[D0] USB: h1F[D15]	IV 입력	W
hFF-h20	D15..0	예비용			

도면38



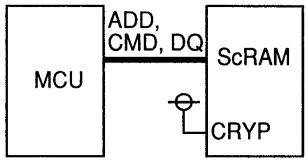
CRYP 단자를 I/O 포트에 의해 제어

도면39



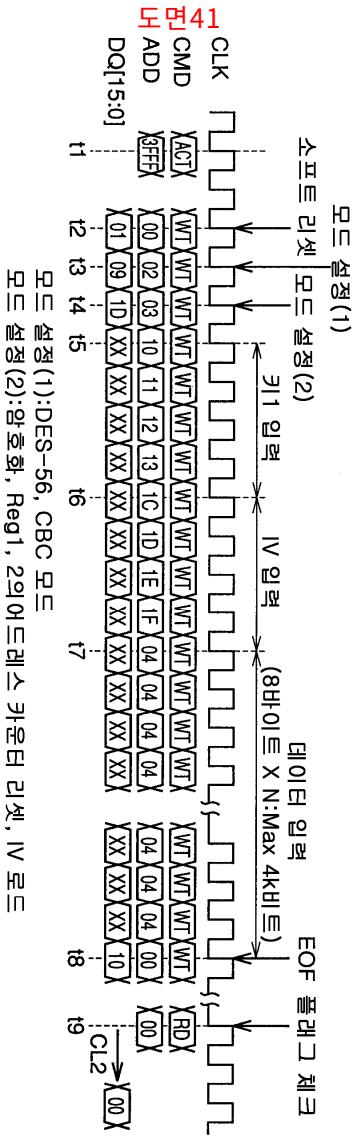
CRYP 단자를 L로 고정

도면40

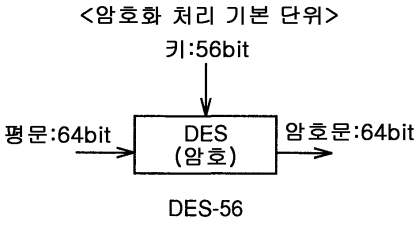


CRYP 단자를 H로 고정

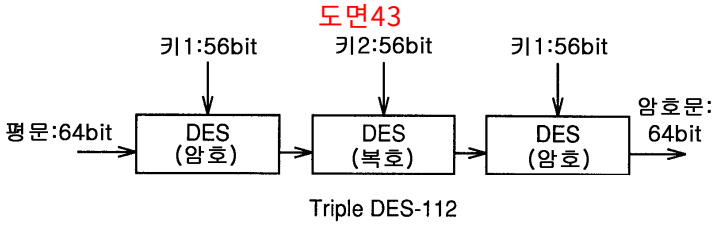
도면41



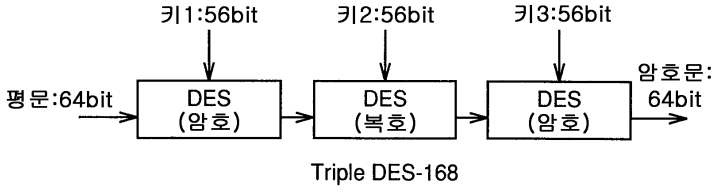
도면42



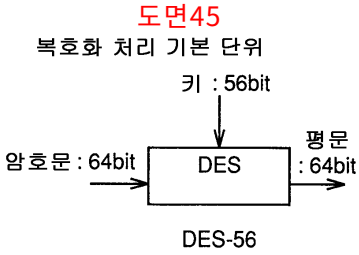
도면43



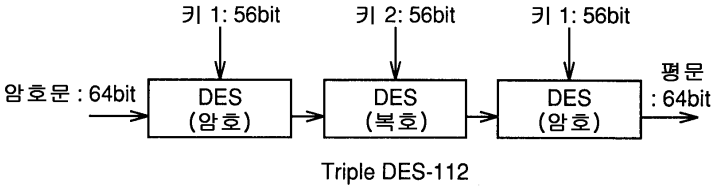
도면44



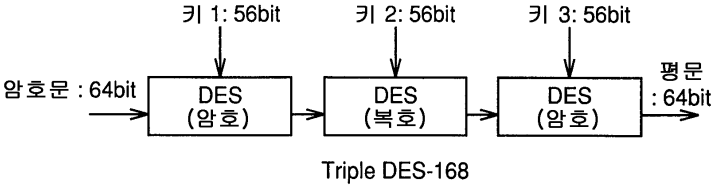
도면45



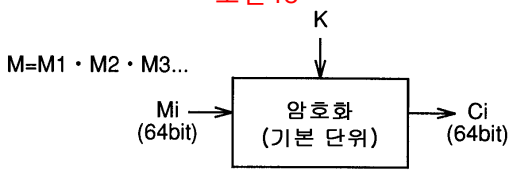
도면46



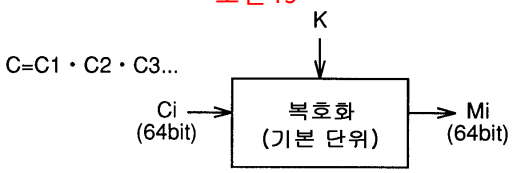
도면47



도면48



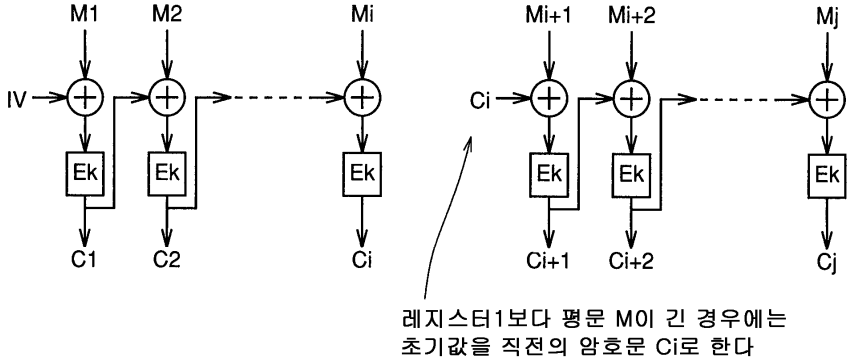
도면49



도면50

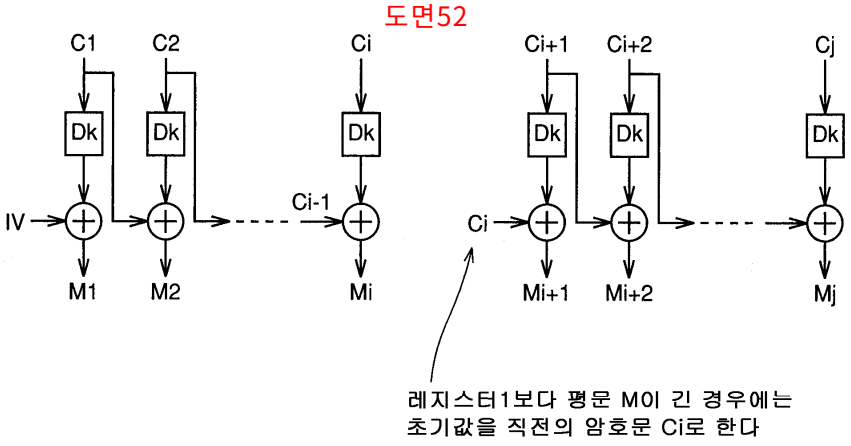
C1=Ek (M1 ⊕ IV)
Ci=Ek (Mi ⊕ Ci-1) (i=2,3,.....)
M1=Dk (C1) ⊕ M1
Mi=Dk (Ci) ⊕ Ci-1 (i=2,3,.....)

도면51



<CBC 모드에 있어서의 암호화의 개요>

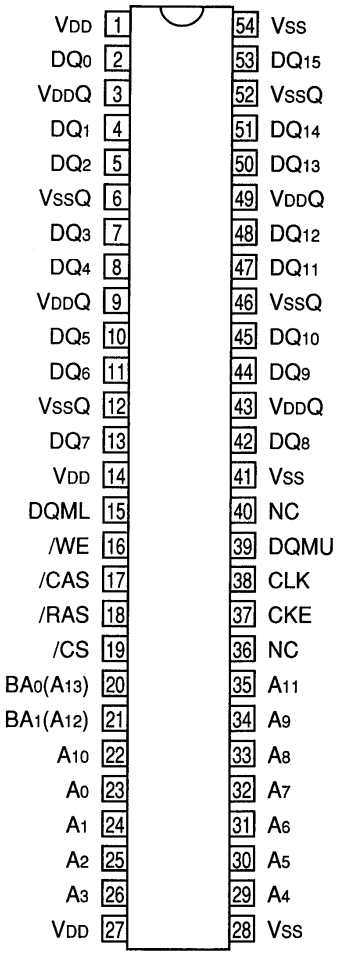
도면52



<CBC 모드에 있어서의 복호화의 개요>

도면53

(종래기술)



도면54

(종래기술)

단자명	기능
CLK	마스터 클럭
CKE	클럭 인에이블
/CS	칩 선택
/RAS	행 어드레스 스트로브
/CAS	열 어드레스 스트로브
/WE	기록 인에이블
$DQ_{0\sim15}$	데이터 입출력
DQM(U/L)	출력 디스에이블/기록 마스크
$A_{0\sim11}$	어드레스 입력
$BA_{0,1}(A_{12,13})$	뱅크 어드레스
V_{DD}	전원
$V_{DD}Q$	출력용 전원
V_{SS}	접지
$V_{SS}Q$	출력용 접지

도면55

(종래기술)