(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0014828
(43) 공개일자 2009년02월11일

(51) Int. Cl.
G06F 12/16 (2006.01) *G06F 11/08* (2006.01)
(21) 출원번호 10-2007-0079103
(22) 출원일자 2007년08월07일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
최성업
경기 화성시 병점동 신창비바훼밀리2차 201동 1206호
이윤태
서울 강남구 대치2동 미도아파트 103동 504호
황성만
경기도 용인시 수지읍 풍덕천리 진산마을 삼성5차 아파트 501동1304호
(74) 대리인
권혁수, 송윤호, 오세준

전체 청구항 수 : 총 11 항

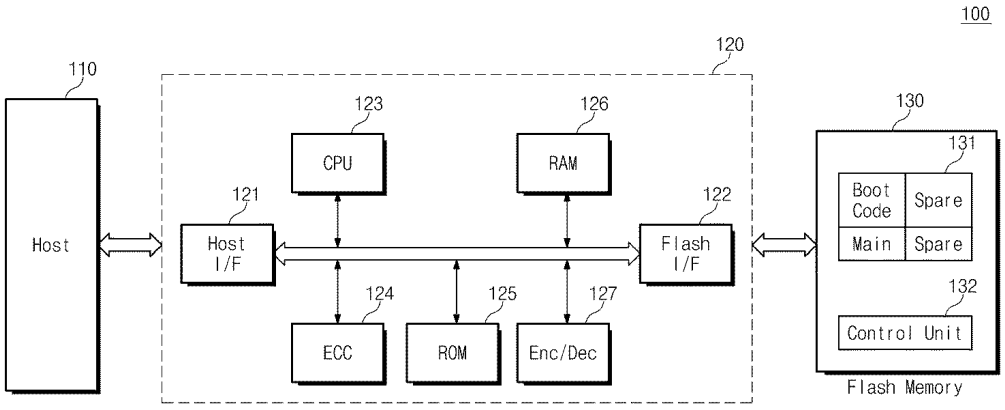
(54) 에러 정정 코드를 암호화하는 플래시 메모리 시스템 및플래시 메모리 시스템의 암호화 방법

(57) 요 약

본 발명은 멀티비트 데이터를 각각 저장하는 메모리 셀을 갖는 플래시 메모리 시스템의 암호화 방법에 관한 것이다.

본 발명에 따른 플래시 메모리 시스템은 플래시 메모리; 및 상기 플래시 메모리를 제어하는 메모리 컨트롤러를 포함하되, 상기 플래시 메모리는 메인 영역과 상기 메인 영역의 제1 에러 정정 코드를 저장하는 스페어 영역을 포함하고, 상기 메모리 컨트롤러는 상기 제1 에러 정정 코드를 암호화한다.

대 표 도



특허청구의 범위

청구항 1

플래시 메모리; 및

상기 플래시 메모리를 제어하는 메모리 컨트롤러를 포함하되,

상기 플래시 메모리는 메인 영역과 상기 메인 영역의 제1 에러 정정 코드를 저장하는 스페어 영역을 포함하고, 상기 메모리 컨트롤러는 상기 제1 에러 정정 코드를 암호화하는 플래시 메모리 시스템.

청구항 2

제 1 항에 있어서,

상기 메모리 컨트롤러는 상기 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드를 생성하는 플래시 메모리 시스템.

청구항 3

제 2 항에 있어서,

상기 제2 에러 정정 코드는 상기 스페어 영역에 저장되는 플래시 메모리 시스템.

청구항 4

제 2 항에 있어서,

상기 메모리 컨트롤러는,

상기 제1 에러 정정 코드를 암호화하고, 상기 암호화된 제1 에러 정정 코드를 복호화하는 암호화 및 복호화부; 그리고

상기 제1 에러 정정 코드와 상기 제2 에러 정정 코드를 생성하는 에러 정정 코드 생성부를 포함하는 플래시 메모리 시스템.

청구항 5

제 1 항에 있어서,

상기 메모리 컨트롤러는 외부로부터 전송된 키를 이용하여 상기 제1 에러 정정 코드를 암호화하는 플래시 메모리 시스템.

청구항 6

제 2 항에 있어서,

상기 스페어 영역은 상기 암호화된 제1 에러 정정 코드, 상기 제2 에러 정정 코드, 및 플래시 변환 레이어를 저장하는 플래시 메모리 시스템.

청구항 7

멀티레벨 셀을 포함하는 플래시 메모리 시스템의 암호화 방법에 있어서:

입력 데이터에 대한 제1 에러 정정 코드를 생성하고; 그리고

상기 제1 에러 정정 코드를 암호화하는 것을 포함하는 암호화 방법.

청구항 8

제 7 항에 있어서,

상기 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드를 생성하는 것을 더 포함하는 암호화 방법.

청구항 9

제 7 항에 있어서,

상기 입력 데이터는 외부의 호스트로부터 전송되는 암호화 방법.

청구항 10

제 7 항에 있어서,

상기 암호화된 제1 에러 정정 코드는 외부로부터 전송된 키를 이용하여 생성되는 암호화 방법.

청구항 11

제 8 항에 있어서,

상기 입력 데이터, 상기 암호화된 제1 에러 정정 코드, 및 상기 제2 에러 정정 코드를 독출하고,

상기 제2 에러 정정 코드에 근거해서 상기 암호화된 제1 에러 정정 코드에 에러를 검출하고,

상기 암호화된 제1 에러 정정 코드에 에러가 검출될 때 상기 암호화된 제1 에러 정정 코드를 정정하고,

상기 제2 에러 정정 코드를 디코딩하고,

상기 암호화된 제1 에러 정정 코드를 복호화하고,

상기 복호화된 제1 에러 정정 코드에 근거해서 상기 입력 데이터에 에러를 검출하고, 그리고

상기 입력 데이터에 에러가 검출될 때 상기 복호화된 제1 에러 정정 코드를 디코딩하는 암호화 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 플래시 메모리 시스템에 관한 것으로, 좀 더 구체적으로는 멀티비트 데이터를 각각 저장하는 메모리 셀을 갖는 플래시 메모리 시스템의 암호화 방법에 관한 것이다.

배 경 기 술

<2> 일반적인 플래시 메모리의 어레이(Array)는 데이터를 저장하는 메인 영역(Main Area)과 스페어 영역(Spare Area)을 포함한다. 스페어 영역은 데이터에 대한 에러 정정 코드(ECC;Error Correction Code), 및 플래시 변환 레이어(FTL:Flash Translation Layer) 등을 포함한다. 예를 들면, 플래시 메모리의 한 페이지(page)에 대한 메인 영역이 512 Byte인 경우 스페어 영역은 16 Byte이다.

<3> 플래시 변환 레이어는 쓰기 연산(Write operation) 시에 파일시스템이 생성한 논리주소를 플래시 메모리 상의 이미 삭제연산을 수행한 영역에 대한 물리주소로 변환하는 역할을 수행한다.

<4> 에러 검출 및 정정 기술들은 다양한 원인들로 인해 손상되는 데이터의 효율적인 복구를 제공한다. 예를 들면, 메모리에 데이터를 저장하는 과정에서 다양한 원인들로 인해서 데이터가 손상될 수 있고, 소오스에서 목적지로 데이터가 전송되는 데이터 전송 채널의 불안(perturbations)에 의해서 데이터가 손상될 수 있다.

<5> 손상된 데이터를 검출하고 정정하기 위한 다양한 방법들이 제안되고 있다. 잘 알려진 에러 검출 기술들에는 RS 코드(Reed-Solomon code), 헤밍 코드(Hamming code), BCH(Bose-Chaudhuri-Hocquenghem) 코드, CRC(Cyclic Redundancy Code) 코드 등이 있다. 이러한 코드들을 이용하여 손상된 데이터를 검출하고 정정하는 것이 가능하다.

<6> 불휘발성 메모리 장치가 사용되는 대부분의 응용 분야에 있어서, 데이터는 에러 정정 코드(error correcting code: ECC)라 불리는 값 (이하, ECC 라 칭함)과 함께 플래시 메모리 장치에 저장된다. ECC 데이터는 플래시 메모리 장치의 읽기 동작시 발생하는 에러를 정정하기 위한 것이다. ECC 데이터를 이용하여 정정 가능한 비트 에러 수는 제한되어 있다. 읽기 동작시 생기는 비트 에러는 잘 알려진 블록 대체(block replacement)와 같은 별도

의 구제 과정없이 에러 검출 및 정정 기술을 통해 정정될 수 있다.

<7> 멀티 비트 데이터를 각각 저장하는 메모리 셀들을 갖는 플래시 메모리는 멀티 레벨 셀(Multi-level Cell;MLC)의 고유한 특성으로 인하여 데이터 내부에 비트 에러를 포함한다. 따라서, 비트 에러를 정정하기 위하여 플래시 메모리는 스페어 영역에 에러 정정 코드를 포함한다. 만약 비트 에러가 발생되면 플래시 메모리 시스템은 에러 정정 코드에 근거하여 비트 에러를 정정한다.

<8> 일반적인 플래시 메모리 시스템은 공격자(Attacker)로부터 플래시 메모리의 메인 영역의 해킹을 방지하기 위하여 플래시 메모리의 메인 영역의 데이터를 암호화(Encryption)한다. 그리고, 플래시 메모리 시스템은 암호화된 메인 영역의 데이터에 대한 에러 정정 코드를 스페어 영역에 저장한다.

발명의 내용

해결 하고자하는 과제

<9> 본 발명의 목적은 플래시 메모리의 데이터를 효율적으로 암호화하는 플래시 메모리 시스템 및 플래시 메모리 시스템의 암호화 방법을 제공하는 데 있다.

과제 해결수단

<10> 본 발명에 따른 플래시 메모리 시스템은 플래시 메모리; 및 상기 플래시 메모리를 제어하는 메모리 컨트롤러를 포함하되, 상기 플래시 메모리는 메인 영역과 상기 메인 영역의 제1 에러 정정 코드를 저장하는 스페어 영역을 포함하고, 상기 메모리 컨트롤러는 상기 제1 에러 정정 코드를 암호화한다.

<11> 실시 예로서, 상기 메모리 컨트롤러는 상기 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드를 생성한다.

<12> 실시 예로서, 상기 제2 에러 정정 코드는 상기 스페어 영역에 저장된다.

<13> 실시 예로서, 상기 메모리 컨트롤러는, 상기 제1 에러 정정 코드를 암호화하고, 상기 암호화된 제1 에러 정정 코드를 복호화하는 암호화 및 복호화부; 그리고 상기 제1 에러 정정 코드와 상기 제2 에러 정정 코드를 생성하는 에러 정정 코드 생성부를 포함한다.

<14> 실시 예로서, 상기 메모리 컨트롤러는 외부로부터 전송된 키를 이용하여 상기 제1 에러 정정 코드를 암호화한다.

<15> 실시 예로서, 상기 스페어 영역은 상기 암호화된 제1 에러 정정 코드, 상기 제2 에러 정정 코드, 및 플래시 변환 레이어를 저장한다.

<16> 본 발명에 따른 멀티레벨 셀을 포함하는 플래시 메모리 시스템의 암호화 방법은 입력 데이터에 대한 제1 에러 정정 코드를 생성하고; 그리고 상기 제1 에러 정정 코드를 암호화하는 것을 포함한다.

<17> 실시 예로서, 상기 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드를 생성하는 것을 더 포함한다.

<18> 실시 예로서, 상기 입력 데이터는 외부의 호스트로부터 전송된다.

<19> 실시 예로서, 상기 암호화된 제1 에러 정정 코드는 외부로부터 전송된 키를 이용하여 생성된다.

<20> 실시 예로서, 상기 입력 데이터, 상기 암호화된 제1 에러 정정 코드, 및 상기 제2 에러 정정 코드를 독출하고, 상기 제2 에러 정정 코드에 근거해서 상기 암호화된 제1 에러 정정 코드에 에러를 검출하고, 상기 암호화된 제1 에러 정정 코드에 에러가 검출될 때 상기 암호화된 제1 에러 정정 코드를 정정하고, 상기 제2 에러 정정 코드를 디코딩하고, 상기 암호화된 제1 에러 정정 코드를 복호화하고, 상기 복호화된 제1 에러 정정 코드에 근거해서 상기 입력 데이터에 에러를 검출하고, 그리고 상기 입력 데이터에 에러가 검출될 때 상기 복호화된 제1 에러 정정 코드를 디코딩한다.

효 과

<21> 본 발명은 일부의 데이터를 암호화함으로 메모리 시스템의 성능을 향상하고, 암호화/복호화를 위한 하드웨어 및 소프트웨어의 오버헤드(Overhead)를 감소시키고, 부트 코드의 노출을 차단하는 효과를 가진다.

발명의 실시를 위한 구체적인 내용

<22> 본 발명에 따른 멀티 레벨 셀을 포함하는 플래시 메모리의 어레이(Array)는 데이터를 저장하는 메인 영역과 데이터의 에러 정정 코드를 저장하는 스페어 영역을 포함한다.

<23> 멀티 레벨 셀을 포함하는 플래시 메모리의 데이터는 비트 에러를 포함하고 있으므로 공격자의 해킹으로부터 보호된다. 즉, 본 발명에 따른 플래시 메모리 시스템은 플래시 메모리의 스페어 영역을 암호화(Encryption)한다. 구체적으로, 본 발명은 스페어 영역 내의 메인 영역의 데이터에 대한 에러 정정 코드를 암호화한다.

<24> 따라서, 공격자는 비트 에러를 포함하는 데이터와 암호화된 에러 정정 코드를 해킹하고, 암호화된 에러 정정 코드를 복호화해야 정확한 정보를 구할 수 있다.

<25> 본 발명에 따른 플래시 메모리 시스템은 스페어 영역의 일부 데이터(즉, 에러 정정 코드)를 암호화함으로 플래시 메모리 시스템의 성능을 향상하고, 플래시 메모리 시스템의 암호화/복호화를 위한 하드웨어 및 소프트웨어의 오버헤드(Overhead)를 감소시킨다.

<26> 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있도록 본 발명의 실시예를 첨부된 도면을 참조하여 설명한다.

<27> 도 1은 본 발명에 따른 메모리 시스템을 보여주는 블록도이다. 도 1을 참조하면, 본 발명에 따른 메모리 시스템(100)은 호스트(110), 메모리 컨트롤러(120), 그리고 플래시 메모리(130)를 포함한다.

<28> 도 1에서, 메모리 컨트롤러(120) 및 플래시 메모리(130)는 하나의 저장 장치 내에 포함될 수 있다. 이러한 저장 장치에는 USB 메모리 및 메모리 카드(M MC(Multi_Media Card), SD 카드, xD 카드, CF 카드, SIM 카드 등) 등과 같은 이동식 저장 장치도 포함된다. 또한, 이러한 저장 장치는 컴퓨터, 노트북, 디지털 카메라, 휴대폰, MP3 플레이어, PMP(Portable Multimedia Player), 게임기 등과 같은 호스트(110)에 접속되어 사용된다.

<29> 본 발명에 따른 멀티레벨 셀을 포함하는 플래시 메모리(130)의 어레이(131)에는 다수의 비트 에러(Bit Error)가 존재한다. 따라서, 공격자는 어레이(131)의 메인 영역만을 해킹해서는 온전한 정보를 얻을 수 없다.

<30> 본 발명에 따른 멀티레벨 셀을 포함하는 플래시 메모리(130)는 스페어 영역 내에 메인 영역에 대한 에러 정정 코드를 암호화한다. 즉, 공격자는 메인 영역과 스페어 영역을 모두를 해킹하여도 정확한 정보를 얻을 수 없다.

<31> 도 1을 참조하면, 본 발명에 따른 플래시 메모리 시스템(100)은 호스트(110), 메모리 컨트롤러(120), 그리고 플래시 메모리(130)를 포함한다.

<32> 메모리 컨트롤러(120)는 호스트 인터페이스(121), 플래시 인터페이스(Flash Interface;122), 중앙처리장치(CPU;123), ECC(Error Correction Code) 회로(124), ROM(125), RAM(126), 및 Enc/Dec 회로(127)을 포함한다.

<33> 호스트 인터페이스(121)는 호스트(110)와 인터페이스 하도록 구성되고, 플래시 인터페이스(122)는 플래시 메모리(130)와 인터페이스 하도록 구성된다. 중앙처리장치(123)는 호스트(110)의 요청에 응답하여 플래시 메모리(130)의 읽기 또는 쓰기 동작 등을 제어하도록 구성된다.

<34> ECC 회로(124)는 플래시 메모리(130)로 전송되는 데이터(메인 데이터)를 이용하여 메인 영역에 저장된 데이터에 대한 제1 에러 정정 코드 그리고 제1 에러 정정 코드를 암호화한 후에 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드를 생성한다. 암호화된 제1 에러 정정 코드와 제2 에러 정정 코드는 플래시 메모리(130)의 스페어 영역(spare area)에 저장된다. ECC 회로(124)는 플래시 메모리(130)로부터 읽혀진 데이터의 에러를 검출한다. 만약 검출된 에러가 정정 범위 내이면, ECC 회로(124)는 검출된 에러를 정정한다. 한편, ECC 회로(124)는 플래시 메모리 시스템(100)에 따라, 플래시 메모리(130) 내에 위치할 수도 있고, 메모리 컨트롤러(120) 밖에 위치할 수도 있다.

<35> ROM(125)은 플래시 메모리(130)으로부터 부트 코드(Boot code) 등을 로딩하기 위한 기본적인 OS(Operating System) 데이터 등을 저장하며, RAM(126)은 메인 메모리 또는 버퍼 메모리로 사용된다. RAM(126)은 플래시 메모리(130)로부터 읽혀진 데이터 또는 호스트(110)로부터 제공되는 데이터를 임시 저장한다. RAM(126)은 DRAM, SRAM 등으로 구현될 수 있다.

<36> 한편, RAM(126)은 읽기 에러 정보를 관리하는 데 필요한 테이블 정보를 저장할 수 있다. 이 테이블 정보는 메타(meta) 데이터로, 중앙처리장치(123) 제어 하에 플래시 메모리(130)의 메타 영역에 저장된다. 이 테이블 정보는 파워 온(Power On) 시에 메타 영역으로부터 RAM(126)으로 복사된다.

<37> Enc/Dec 회로(127)는 제1 에러 정정 코드를 암호화(Encryption)하거나 복호화(Decryption)한다.

<38> 계속해서 도 1을 참조하면, 플래시 메모리(130)는 셀 어레이(131) 및 제어 유닛(132)을 포함한다. 셀 어레이(131)는 부트 코드를 저장하는 메인 영역과 그에 관한 스페어 영역 그리고 호스트(110)로부터 전송된 데이터를 저장하는 메인 영역과 그에 관한 스페어 영역을 포함한다. 제어 유닛(132)은 당업자에게 잘 알려진 바와 같이, 로우 디코더, 칼럼 디코더, 페이지 버퍼, 비트 라인 선택 회로, 그리고 데이터 버퍼 등을 포함한다.

<39> 본 발명에 따른 플래시 메모리 시스템(100)은 파워 온(Power-on) 시에 중앙 처리 장치(123)의 제어에 응답하여 플래시 메모리(130) 내에 저장된 부트 코드 및 부트 코드에 대응하는 스페어 영역의 데이터를 램(126)에 로딩한다.

<40> 스페어 영역에는 부트 코드, 부트 코드에 대한 암호화된 제1 에러 정정 코드, 암호화된 제1 에러 정정 코드에 대한 제2 에러 정정 코드, 및 플래시 변환 레이어 등이 저장된다.

<41> 따라서, 공격자는 램(126)에 로딩된 부트 코드를 해킹한다 하더라도 부트 코드는 비트 에러를 포함하고 있으므로 완전한 부트 코드를 알아낼 수 없다.

<42> 즉, 본 발명에 따른 플래시 메모리 시스템은 파워-온 시에 비트 에러가 포함된 부트 코드와 암호화된 에러 정정 코드를 램에 로딩함으로 공격자로부터 부트 코드의 노출을 차단한다. 따라서, 본 발명에 따른 플래시 메모리 시스템을 포함하는 집적회로 카드의 보안 레벨을 높이는 효과가 있다.

<43> 도 2는 도 1에 도시된 플래시 메모리의 어레이를 도시한 블록도이다.

<44> 도 1 및 도 2를 참조하면, 본 발명에 따른 플래시 메모리(130)은 어레이(131) 내에 메인 영역과 스페어 영역을 포함한다.

<45> 도 2에 도시된 하나의 페이지는 호스트로부터 전송된 데이터를 저장하는 메인 영역과 메인 영역에 대한 제1 에러 정정 코드(ECC_FM)과 제2 에러 정정 코드(ECC_FS), 및 플래시 변환 레이어 등을 저장하는 스페어 영역을 포함한다.

<46> 도 2에서, 플래시 메모리의 어레이(131)에는 한 페이지만이 도시되었으나, 플래시 메모리의 어레이(131)에는 복수의 페이지와 상기 복수의 페이지를 포함하는 복수의 블록이 있음은 당업자에 있어서 자명하다.

<47> 계속해서 도 1 및 도 2를 참조하면, 본 발명에 따른 플래시 메모리의 메인 영역은 256 word로 구성되고, 스페어 영역은 8 word로 구성된다. 스페어 영역 내의 제1 워드부터 제7 워드는 제1 에러 정정 코드(ECC_FM) 및 플래시 변환 레이어 등을 포함하고, 스페어 영역 내의 제8 워드는 제1 에러 정정 코드(ECC_FM)에 대한 제2 에러 정정 코드(ECC_FS)를 포함한다.

<48> 일반적인 플래시 메모리 시스템이 메인 영역의 데이터를 암호화하는데 반하여, 본 발명의 실시예에 따른 플래시 메모리 시스템은 스페어 영역 내의 제1 워드부터 제7 워드 내에 저장된 데이터(Enc Area)를 암호화한다.

<49> 따라서, 본 발명에 따른 플래시 메모리 시스템은 스페어 영역의 일부 데이터(즉, 에러 정정 코드)를 암호화함으로 플래시 메모리 시스템의 성능을 향상하고, 플래시 메모리 시스템의 암호화/복호화를 위한 하드웨어 및 소프트웨어의 오버헤드(Overhead)를 감소시킨다.

<50> 도 3은 본 발명에 따른 플래시 메모리 시스템의 암호화 방법을 도시한 순서도이다.

<51> 도 1 내지 도 3을 참조하면, 중앙 처리 장치(123)는 호스트(110)로부터 전송된 데이터를 램(126)에 저장한다(31). ECC 회로(124)는 상기 호스트(110)로부터 전송된 데이터에 대한 제1 에러 정정 코드(ECC_FM)을 생성한다(32). Enc/Dec 회로(127)는 생성된 제1 에러 정정 코드(ECC_FM)를 암호화한다(33). ECC 회로(124)는 암호화된 제1 에러 정정 코드(ECC_FM)에 대한 제2 에러 정정 코드(ECC_FS)를 생성한다(34). 중앙 처리 장치(123)는 호스트(110)로부터 전송된 데이터, 암호화된 제1 에러 정정 코드(ECC_FM), 및 제2 에러 정정 코드(ECC_FS)를 플래시 메모리(130)에 저장한다(35).

<52> 도 4는 도 1에 도시된 암호화된 플래시 메모리 시스템으로부터 데이터를 독출하는 방법을 도시한 순서도이다.

<53> 도 1 내지 도 4를 참조하면, 중앙 처리 장치(123)는 플래시 메모리(130)로부터 데이터(메인 영역의 데이터, 암호화된 제1 에러 정정 코드(ECC_FM), 및 제2 에러 정정 코드(ECC_FS))를 독출한다(41).

<54> 중앙 처리 장치(123)는 암호화된 제1 에러 정정 코드(ECC_FM)에 에러가 검출되는지를 판단한다(42).

<55> 만약 암호화된 제1 에러 정정 코드(ECC_FM)에 에러가 검출된다면, ECC 회로(124)는 제2 에러 정정 코드(ECC_FS)를 디코딩(Decoding)한다(43). 즉, 중앙 처리 장치(123)는 제2 에러 정정 코드(ECC_FS)에 근거하여 암호화된 제1 에러 정정 코드(ECC_FM)의 에러를 정정한다.

<56> Enc/Dec 회로(127)는 암호화된 제1 에러 정정 코드(ECC_FM)를 복호화한다(44). 중앙 처리 장치(123)는 메인 영역의 데이터에 에러가 검출되는지를 판단한다(45).

<57> 만약 메인 영역의 데이터에 에러가 검출된다면, ECC 회로(124)는 제1 에러 정정 코드(ECC_FM)를 디코딩(Decoding)한다(46). 즉, 중앙 처리 장치(123)는 제1 에러 정정 코드(ECC_FM)에 근거하여 메인 영역 데이터의 에러를 정정한다.

<58> 중앙 처리 장치(123)는 메인 영역의 데이터를 램(126)에 로딩한다(47).

<59> 본 발명에 따른 플래시 메모리 시스템은 스페어 영역의 일부 데이터(즉, 에러 정정 코드)를 암호화함으로 플래시 메모리 시스템의 성능을 향상하고, 플래시 메모리 시스템의 암호화/복호화를 위한 하드웨어 및 소프트웨어의 오버헤드(Overhead)를 감소시킨다.

<60> 또한, 본 발명에 따른 플래시 메모리 시스템은 파워-온 시에 비트 에러가 포함된 부트 코드와 암호화된 에러 정정 코드를 램에 로딩함으로 공격자로부터 부트 코드의 노출을 차단한다. 그리고, 본 발명에 따른 플래시 메모리 시스템을 포함하는 집적회로 카드의 보안 레벨을 높이는 효과가 있다.

<61> 이상에서와 같이 도면과 명세서에서 최적 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면의 간단한 설명

<62> 도 1은 본 발명에 따른 메모리 시스템을 보여주는 블록도.

<63> 도 2는 도 1에 도시된 플래시 메모리의 어레이를 도시한 블록도.

<64> 도 3은 본 발명에 따른 플래시 메모리 시스템의 암호화 방법을 도시한 순서도.

<65> 도 4는 도 3에 따라 암호화된 플래시 메모리 시스템을 독출하는 방법을 도시한 순서도.

<66> * 도면의 주요 부분에 대한 부호 설명 *

<67> 100; 플래시 메모리 시스템 110; 호스트

<68> 120; 메모리 컨트롤러 121; 호스트 인터페이스

<69> 122; 플래시 인터페이스 123; 중앙처리장치

<70> 124; ECC 회로 125; ROM

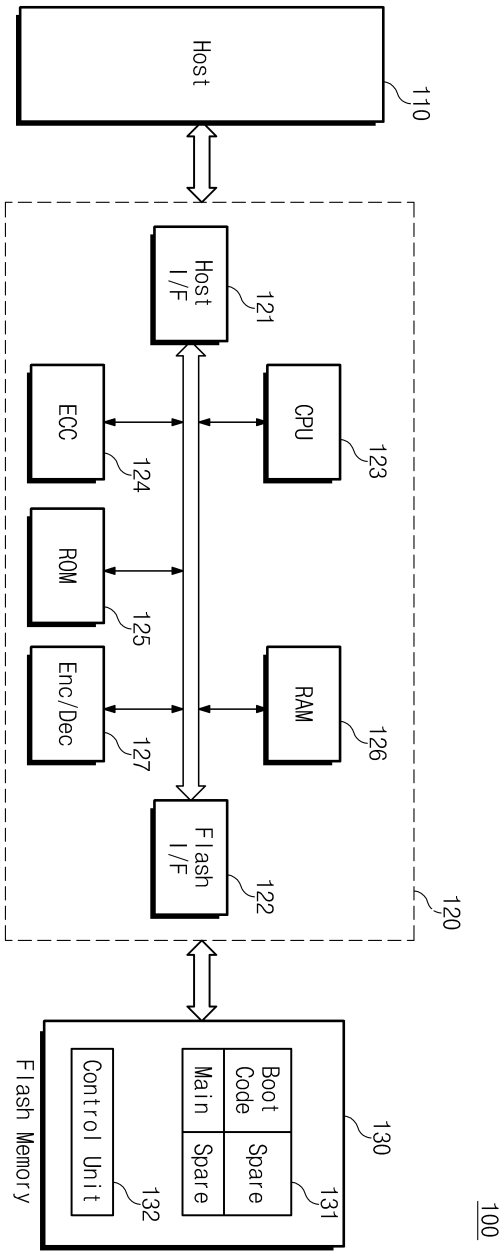
<71> 126; RAM 127; Enc/Dec 회로

<72> 130; 플래시 메모리 131; 어레이

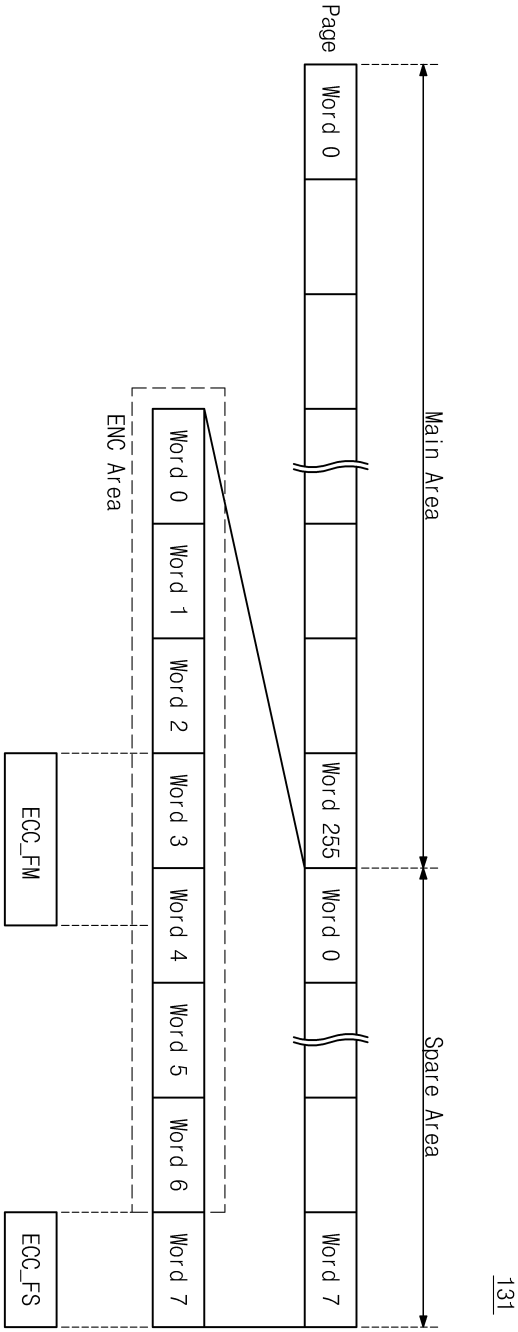
<73> 132; 제어 유닛

도면

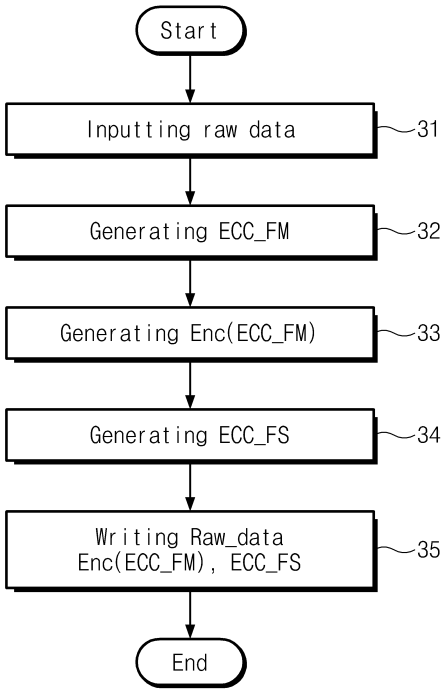
도면1


Host
110
Host I/F
121
ECC
124
CPU
123
ROM
125
Enc/Dec
127
RAM
126
Flash I/F
122
120
Flash Memory
Control Unit
132
Boot Code
Main
Spare
Spare
131
130
100

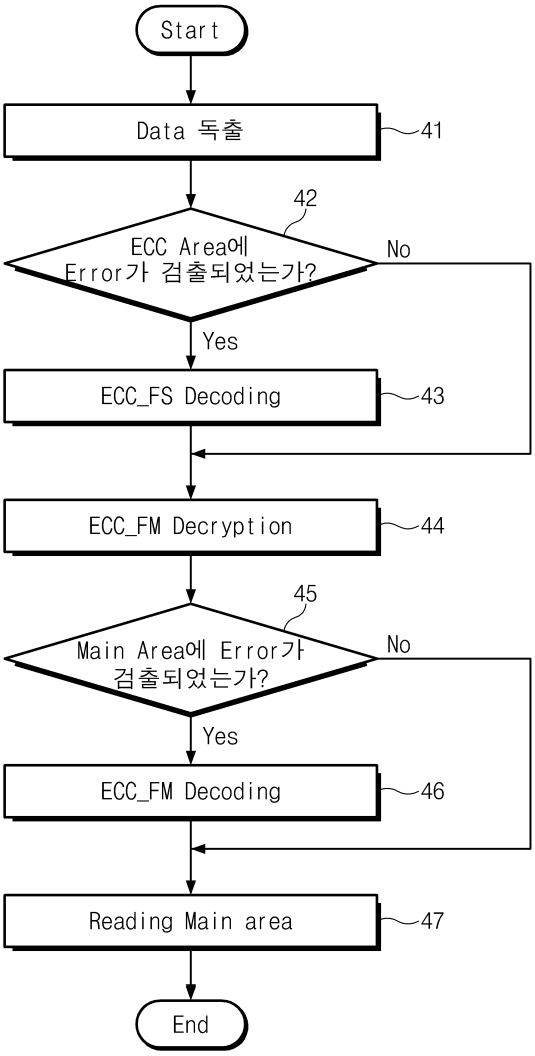
도면2


Page
Word 0
Word 255
Word 0
Word 7
Main Area
Spare Area
131
ENC Area
Word 0
Word 1
Word 2
Word 3
Word 4
Word 5
Word 6
Word 7
ECC_FM
ECC_FS

도면3


Start
Inputting raw data
31
Generating ECC_FM
32
Generating Enc(ECC_FM)
33
Generating ECC_FS
34
Writing Raw_data
Enc(ECC_FM), ECC_FS
35
End

도면4


Start
Data 독출
41
42
ECC Area에 Error가 검출되었는가?
No
Yes
ECC_FS Decoding
43
ECC_FM Decryption
44
45
Main Area에 Error가 검출되었는가?
No
Yes
ECC_FM Decoding
46
Reading Main area
47
End