(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0105561
(43) 공개일자 2022년07월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/79 (2013.01) *G06F 21/60* (2013.01)
(52) CPC특허분류
G06F 21/79 (2013.01)
G06F 21/60 (2013.01)
(21) 출원번호 10-2021-0034739
(22) 출원일자 2021년03월17일
심사청구일자 2021년03월17일
(30) 우선권주장
1020210007982 2021년01월20일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
안나영
서울특별시 동대문구 약령시로3길 18-3 , 302호 (제기동, 덕산맨션)
(74) 대리인
김홍석

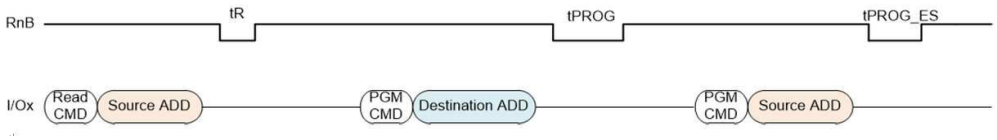
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 **NAND 플래시 메모리의 보안 카피-백 프로그램 방법**

(57) 요 약

NAND 플래시 메모리의 보안 카피-백 프로그램 방법은 소스 주소에 대응하는 물리적 페이지에 대한 읽기를 수행하고, 목적지 주소에 대응하는 물리적 페이지 및 상기 소스 주소에 대응하는 물리적 페이지에 대한 프로그램 동작을 수행하고, 및 상기 소스 주소에 대응하는 물리적 페이지에서 보안 프로그램 동작을 수행하는 것을 포함한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	1711083346
과제번호	2017R1A2B3009643
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	향상된 제어흐름 무결성 검증 기법이 통합된 컴파일러 설계 및 구현
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2017.03.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

NAND 플래시 메모리의 보안 카피-백 프로그램 방법에 있어서,

소스 주소에 대응하는 물리적 페이지에 대한 읽기를 수행하고;

목적지 주소에 대응하는 물리적 페이지에 대한 프로그램 동작을 수행하고; 및

상기 소스 주소에 대응하는 물리적 페이지에서 보안 프로그램 동작을 수행하는,

NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 2

제1항에 있어서,

상기 보안 프로그램 동작은 원본 데이터를 변경하는 덮어 쓰기를 수행하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 3

제2항에 있어서,

상기 덮어 쓰기를 이용하여 선택된 워드 라인에 인접한 워드 라인들에 대해, 읽기 조건을 변경하여 읽기 동작을 더 수행하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 4

제1항에 있어서,

상기 보안 프로그램 동작은 상기 소스 주소에 대응하는 물리적 페이지에 랜덤 데이터를 프로그램밍하는 것을 포함하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 5

제1항에 있어서,

상기 보안 프로그램 동작은 상기 소스 주소에 대응하는 물리적 페이지에 해당하는 워드 라인에 복수의 삭제 펄스를 인가하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 6

제1항에 있어서,

상기 보안 프로그램 동작으로 인해 발생된 프로그램 방해를 줄이기 위하여, 보안 카피-백 프로그램 동작을 수행하는 것을 더 포함하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

청구항 7

제6항에 있어서,

상기 보안 카피-백 프로그램 동작은,

상기 NAND 메모리의 채널에 전원공급전압을 사전 충전하는 것을 포함하는 NAND 플래시 메모리의 보안 카피-백 프로그램 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 NAND 플래시 메모리의 보안 카피-백 프로그램 방법에 관한 것이다.

배 경 기 술

[0002] 오늘날 우리는 디지털 정보의 홍수 속에서 살고 있다. 사물 인터넷을 통해 디지털 정보가 더 빠르게 공유되고 확산되고 있다. 동시에 디지털 정보 보안 문제가 대두되고 있다. 대부분의 정보 장치는 NAND 플래시 메모리를 사용한다. NAND 플래시 메모리는 비 휘발성 메모리로 기존 휘발성 메모리에 비해 전력 측면에서 유리하다. 또한, NAND 플래시 메모리는 통합을 우선시하기 때문에 기존 DRAM보다 적은 공간에 비교적 많은 양의 데이터를 저장할 수 있다.

[0003] NAND 플래시 메모리는 전자 장치/데이터 센터의 저장 장치로 널리 사용되며 일반적으로 덮어 쓸 수 없는 메모리 유형으로 알려져 있다. 데이터 블록의 고유한 구조로 인해 물리적 삭제(또는 삭제) 동작을 수행하는 것보다 매핑 관계를 논리적으로 파괴하는 삭제 동작을 사용하는 것이 좋다. 이러한 기능은 NAND 플래시 메모리가 포렌식 대상이 될 가능성을 높이다. NAND 플래시 메모리의 관리 데이터인 메타 데이터를 복원하여 디지털 포렌식을 수행하기 위한 많은 연구가 수행되었다

[0004] 이러한 메타 데이터 취약점을 보완하기 위해 연구에서는 파일 삭제 기술을 제안했다. 파일 삭제는 파일 삭제 시 파일 시스템의 메타 데이터가 수정되는 동안 데이터 영역에 남아있는 취약점을 해결하는 대신 파일을 완전히 삭제하는 기술이다. 완전 삭제를 위해 데이터와 동일한 논리 주소의 데이터 영역에서 0 또는 1, 특정 패턴 데이터 및 난수 데이터를 여러 번 덮어 쓰는 것이다.

[0005] 그러나 운영 체제에서 파일 삭제를 수행하더라도 기존 NAND 플래시 메모리 장치만으로는 물리적으로 덮어 쓰기가 수행되지 않는다. 파일 삭제는 원본 데이터와 그 하위 데이터만 NAND 플래시 메모리에 광범위하게 남긴다. 이는 운영 체제에서 파일을 변경해도 NAND 플래시 메모리를 덮어 쓰지 않고 기본적으로 새 덮어 쓰기 파일이 NAND 플래시 메모리에 생성된다는 것을 의미하기 때문이다. 호스트가 파일을 덮어 쓰지만 데이터는 남아 있다. 이 문제를 해결하기 위해 완전한 데이터 삭제 기법을 도입하고 가비지 수집(garbage collection)으로 인한 데이터 보존 문제를 제기하고 원본 데이터를 처리하는 방법을 제안했다. 가비지 수집과 마찬가지로 카피-백 프로그램은 NAND 플래시 메모리를 처리하기 위한 중요한 관리 동작이다. 이러한 카피-백 프로그램은 일반적으로 백그라운드에서 수행되며 이 경우 원본 데이터는 그대로 남아있는 경우가 많다. 이것은 포렌식 방지 대상이 될 수 있다.

발명의 내용

해결하려는 과제

[0006] 본원 발명이 해결하고자 하는 과제는 보안성이 향상된 NAND 플래시 메모리의 보안 카피-백 프로그램 방법에 관한 것이다.

과제의 해결 수단

[0007] 해결하고자 하는 과제를 달성하기 위하여 본 발명의 실시예들에 따른 NAND 플래시 메모리의 보안 카피-백 프로그램 방법은, 소스 주소에 대응하는 물리적 페이지에 대한 읽기를 수행하고, 목적지 주소에 대응하는 물리적 페이지 및 상기 소스 주소에 대응하는 물리적 페이지에 대한 프로그램 동작을 수행하고 및 상기 소스 주소에 대응하는 물리적 페이지에서 보안 프로그램 동작을 수행하는 것을 포함한다.

발명의 효과

[0008] 본 발명의 실시예들에 따르면, NAND 플래시 메모리의 보안 카피-백 프로그램의 보안성이 향상될 수 있다.

도면의 간단한 설명

[0009] 도 1은 일반적인 카피-백 프로그램 동작을 설명하기 위한 블록도이다.

도 2는 NAND 플래시 메모리에서 카피-백 프로그램을 나타내는 블록도이다.

도 3은 본 발명의 일 실시예에 따른 NAND 플래시 메모리의 카피-백 프로그램 동작의 타이밍도이다.

도 4a 및 도 4b는 본 발명의 실시예들에 따른 NAND 플래시 메모리의 보안 카피-백 프로그램 방법을 설명하는 도면들이다.

도 5는 일반적인 3D NAND 플래시 메모리의 구조를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0010] 본 발명의 구성 및 효과를 충분히 이해하기 위하여, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예들을 설명한다. 그러나 본 발명은, 이하에서 개시되는 실시예들에 한정되는 것이 아니라, 여러 가지 형태로 구현될 수 있고 다양한 변경을 가할 수 있다.

[0011] 메모리 시스템은 메모리 장치 및 메모리 컨트롤러를 포함한다. 메모리 장치는 메모리 컨트롤러의 제어에 따라 동작한다. 보다 구체적으로, 메모리 장치는 메모리 컨트롤러로부터의 쓰기 요청에 응답하여 메모리 셀 어레이에 데이터를 기입한다. 메모리 컨트롤러로부터 쓰기 요청으로서 프로그램 커맨드, 어드레스 및 데이터가 수신되면, 메모리 장치는 어드레스가 가리키는 메모리 셀들에 데이터를 기입한다. 메모리 컨트롤러로부터의 읽기 요청에 응답하여, 메모리 장치는 읽기 동작을 수행한다. 메모리 컨트롤러로부터 읽기 요청으로서 읽기 커맨드 및 어드레스가 수신되면, 메모리 장치는 어드레스가 가리키는 메모리 셀들의 데이터를 읽고, 읽혀진 데이터를 메모리 컨트롤러로 출력한다.

[0012] 메모리 장치는 낸드 플래시 메모리(NAND flash memory), 수직형 낸드 플래시 메모리(Vertical NAND, 이하, 'VNAND'라고 함), 노아 플래시 메모리(NOR flash memory), 저항성 램(resistive random access memory: RRAM), 상변화 메모리(phase-change memory: PRAM), 자기저항 메모리(magnetoresistive random access memory: MRAM), 강유전체 메모리(ferroelectric random access memory: FRAM), 스핀주입 자화반전 메모리(spin transfer torque random access memory: STT-RAM) 등이 될 수 있다. 또한, 본 발명의 메모리 장치는 3차원 어레이 구조(three-dimensional array structure)로 구현될 수 있다. 본 발명은 전하 저장층이 전도성 부유 게이트로 구성된 플래시 메모리 장치는 물론, 전하 저장층이 절연막으로 구성된 차지 트랩형 플래시(charge trap flash; CTF)에도 적용될 수 있다. 메모리 컨트롤러는 메모리 장치 및 호스트 사이에 연결된다. 메모리 컨트롤러는 호스트와 메모리 장치를 인터페이싱하도록 구성된다. 메모리 컨트롤러는 호스트의 제어에 따라 메모리 장치에 쓰기 요청을 전송하거나 읽기 요청을 전송할 수 있다.

[0013] 메모리 장치는 메모리 셀 어레이, 어드레스 디코더, 읽기 및 쓰기 회로, 제어 로직 및 전압 생성부를 포함한다. 메모리 셀 어레이는 다수의 메모리 블록들을 포함한다. 다수의 메모리 블록들은 워드라인들을 통해 어드레스 디코더에 연결된다. 다수의 메모리 블록들은 비트 라인들을 통해 읽기 및 쓰기 회로에 연결된다. 다수의 메모리 블록들 각각은 다수의 메모리 셀들을 포함한다. 실시 예로서, 다수의 메모리 셀들은 불휘발성 메모리 셀들이며, 수직 채널 구조를 갖는 불휘발성 메모리 셀들로 구성될 수 있다. 상기 메모리 셀 어레이는 2차원 구조의 메모리 셀 어레이로 구성될 수 있다. 실시 예에 따라, 상기 메모리 셀 어레이는 3차원 구조의 메모리 셀 어레이로 구성될 수 있다. 한편, 메모리 셀 어레이에 포함되는 복수의 메모리 셀들은 복수의 메모리 셀들 각각은 적어도 1비트의 데이터를 저장할 수 있다. 일 실시 예에서, 메모리 셀 어레이에 포함되는 복수의 메모리 셀들 각각은 1비트의 데이 터를 저장하는 싱글-레벨 셀일 수 있다. 다른 실시 예에서, 메모리 셀 어레이에 포함되는 복수의 메모리 셀들 각각은 2비트의 데이터를 저장하는 멀티-레벨 셀일 수 있 다. 또다른 실시 예에서, 메모리 셀 어레이에 포함되는 복수의 메모리 셀들 각각은 3비트의 데이터를 저장 하는 트리플-레벨 셀일 수 있다. 또 다른 실시 예에서, 메모리 셀 어레이에 포함되는 복수의 메모리 셀들 각각은 4비트의 데이터를 저장하는 쿼드-레벨 셀일 수 있다. 실시 예에 따라, 메모리 셀 어레이는 5비트 이상의 데이터를 각각 저장하는 복수의 메모리 셀들을 포함할 수 있다.

[0014] 어드레스 디코더, 읽기 및 쓰기 회로, 제어 로직 및 전압 생성부는 메모리 셀 어레이를 구동하는 주변 회로로서 동작한다. 어드레스 디코더는 워드라인들을 통해 메모리 셀 어레이에 연결된다. 어드레스 디코더는 제어 로직의 제어에 응답하여 동작하도록 구성된다. 어드레스 디코더는 메모리 장치 내부의 입출력 버퍼를 통해 어드레스를 수신한다. 어드레스 디코더는 수신된 어드레스 중 블록 어드레스를 디코딩하도록 구성된다. 어드레스 디코더는 디코딩된 블록 어드레스에 따라 적어도 하나의 메모리 블록을 선택한다. 또한 어드레스 디코더는 읽기 동 작 중 읽기 전압 인가 동작 시 선택된 메모리 블록 중 선택된 워드라인에 전압 생성부에서 발생된 읽기 전압을 선택된 워드라인에 인가하고, 나머지 비 선택된 워드라인들에 패스 전압을 인가한다. 또 한 프로그램 검증 동작 시에는 선택된 메모리 블록 중 선택된 워드라인에 전압 생성부에서 발생된 검증 전 압을 선택된 워드라인에 인가하고, 나머지 비 선택된 워드라인들에는 패스 전압을 인가한다.

[0015] 어드레스 디코더는 수신된 어드레스 중 열 어드레스를 디코딩하도록 구성된다. 어드레스 디코더는 디 코딩된 열 어드레스를 읽기 및 쓰기 회로에 전송한다. 메모리 장치의 읽기 동작 및 프로그램 동작은 페이지 단위로 수행된다. 읽기 동작 및 프로그램 동작 요청 시에 수신되는 어드레스는 블록 어드레스, 행 어드레스 및 열 어드레스를 포함한다. 어드레스 디코더는 블록 어드레스 및 행 어드레스에 따라 하나의 메모리 블록 및 하나의 워드라인을 선택한다. 열 어드레스는 어드레스 디코더에 의해 디코딩되어 읽기 및 쓰기 회로에 제공된다. 어드레스 디코더는 블록 디코더, 행 디코더, 열 디코더 및 어드레스 버퍼 등을 포함할 수 있다.

[0016] 읽기 및 쓰기 회로는 다수의 페이지 버퍼들을 포함한다. 읽기 및 쓰기 회로는 메모리 셀 어레이의 읽기 동작 시에는 "읽기 회로(read circuit)"로 동작하고, 기입 동작 시에는 "쓰기 회로(write circuit)"로 동작할 수 있다. 다수의 페이지 버퍼들은 비트 라인들을 통해 메모리 셀 어레이에 연결된다. 다수의 페이지 버퍼들은 읽기 동작 및 프로그램 검증 동작 시 메모리 셀들의 문턱 전압을 센싱하기 위하여 메모리 셀들과 연결된 비트라인들에 센싱 전류를 계속적으로 공급하면서 대응하는 메모 리 셀의 프로그램 상태에 따라 흐르는 전류량이 변화되는 것 센싱 노드를 통해 감지하여 센싱 데이터로 래치한다. 읽기 및 쓰기 회로는 제어 로직에서 출력되는 페이지 버퍼 제어 신호들에 응답하여 동작한다. 읽기 및 쓰기 회로는 읽기 동작시 메모리 셀의 데이터를 센싱하여 독출 데이터를 임시 저장한 후 메모리 장치의 입출력 버퍼로 데이터를 출력한다. 예시적인 실시 예로서, 읽기 및 쓰기 회로는 페이지 버퍼들(또는 페이지 레지스터들) 이외에도 열 선택 회로 등을 포함할 수 있다.

[0017] 제어 로직은 어드레스 디코더, 읽기 및 쓰기 회로, 및 전압 생성부에 연결된다. 제어 로직은 메모리 장치의 입출력 버퍼를 통해 명령어 및 제어 신호를 수신한다. 제어 로직은 제어 신호에 응답하여 메모리 장치의 제반 동작을 제어하도록 구성된다. 또한 제어 로직은 다수의 페이지 버퍼들의 센싱 노드 프리차지 전위 레벨을 조절하기 위한 제어신호를 출력한다. 제어 로직은 메모리 셀 어레이의 읽기 동작을 수행하도록 읽기 및 쓰기 회로를 제어할 수 있다.

[0018] 전압 생성부는 제어 로직에서 출력되는 제어 신호에 응답하여 읽기 동작시 리드 전압 및 패스 전압을 생성한다. 전압 생성부는 다양한 전압 레벨들을 갖는 복수의 전압들을 생성하기 위해서, 내 부 전원 전압을 수신하는 복수의 펌핑 커패시터들을 포함하고, 제어 로직의 제어에 응답하여 복수의 펌핑 커패시터들을 선택적으로 활성화하여 복수의 전압들을 생성할 것이다. 어드레스 디코더, 읽기 및 쓰기 회로 및 전압 생성부는 메모리 셀 어레이에 대한 읽기 동 작, 쓰기 동작 및 소거 동작을 수행하는 "주변 회로"로서 기능할 수 있다. 주변 회로는 제어 로직의 제어 에 기초하여, 메모리 셀 어레이에 대한 읽기 동작, 쓰기 동작 및 소거 동작을 수행한다.

[0019] 본 발명에 따른 NAND 플래시 메모리의 보안 카피-백 프로그램 방법을 설명하기 이전에 NAND 플래시 메모리에서 카피-백 프로그램에 대하여 살펴보도록 한다.

[0020] 도 1은 일반적인 카피-백 프로그램 동작을 설명하기 위한 블록도이다. 도 1을 참조하면, 첫 번째 블록의 소스 페이지 데이터는 프로그램 복사 명령에 따라 두 번째 블록의 대상 페이지로 전송된다. 프로그램 복사 동작 후 소스 페이지에 저장된 데이터는 관리되지 않는 데이터가 된다.

[0021] 도 2는 NAND 플래시 메모리에서 카피-백 프로그램을 나타내는 블록도이다. 특히, 도 2는 NAND 플래시 메모리에서 카피-백 프로그램 동작을 수행할 때 프로세스는 해커가 대상으로 하는 관리되지 않는 데이터와 해커가 이러한 관리되지 않는 데이터에 액세스할 수 있는 방법을 보여준다.

[0022] NAND 플래시 메모리의 경우 데이터는 전하 저장 계층에 저장된 전하량에 해당한다. 그러나 전하 저장 층의 전하는 환경(예: 온도, 시간 및 전압)의 변화에 민감하게 반응하므로 열화 특성이 있다. 일반적으로 이로 인해 전하가 손실되어 저장된 데이터가 손상된다. 이 문제를 방지하기 위해 NAND 플래시 메모리에서 카피-백 프로그램(copy-back program) 동작이 사용된다. 메모리 셀의 열화 정도를 모니터링하고 특정 조건이 충족되면 내부적으로 카피-백 프로그램 동작을 수행한다. 카피-백 프로그램 동작에서, 도 2에 도시된 바와 같이, 제 1 블록(BLK1)의 소스 페이지에 저장된 원본 데이터는 제 2 블록 (BLK2)의 목적지 페이지에 프로그래밍된다. 일반적으로 NAND 플래시 메모리는 카피-백 명령에 응답하여 이러한 카피-백 프로그램 동작을 수행한다.

[0023] 도 1에 도시된 바와 같이, 이 카피-백 프로그램 동작은 소스 페이지로부터 판독된 데이터의 신뢰성을 향상시키기 위해 오류 정정을 수행한다. 이러한 오류 수정은 NAND 플래시 메모리(오프 칩 ECC) 외부의 컨트롤러 또는 자체적으로 NAND 플래시 메모리(온칩 ECC)에 의해 수행된다.

[0024] 카피-백 프로그램 동작이 완료되면, 제 1 블록(BLK1)의 소스 페이지로부터의 원본 데이터는 관리되지 않는 데이터가 되고, 제 2 블록(BLK2)의 목적지로부터의 데이터는 관리 가능하여 검증 데이터가 된다. 이 때, 관리되지 않는 데이터가 개인 정보인 경우 관리되는 데이터 형식뿐만 아니라 관리되지 않는 데이터 형식으로도 NAND 플래

시 메모리에 개인 정보가 존재할 수 있으며, 이는 관리되지 않는 데이터가 불법 사용자에 의해 해킹될 수 있음을 의미한다. 즉, 이러한 종류의 관리되지 않는 데이터를 통해 개인 정보가 노출될 가능성이 높다.

[0025] 일련의 극단적인 가정 하에서 데이터 노출 가능성이 높다는 것을 확인할 수 있다. 카피-백 프로그램 동작은 내부적으로 수행되는 것으로 가정하고 원본 데이터도 개인 정보라고 가정한다. 호스트는 필요에 따라 개인 정보에 대한 삭제 요청을 저장 장치(SSD/USB/카드)로 전송한다. 호스트 요청에 따라, 스토리지 장치의 컨트롤러는 제 2 블록(BLK2)에 소거 명령을 NAND 플래시 메모리로 전송할 수 있다. NAND 플래시 메모리는 명령에 따라 제 2 블록(BLK2)에 대해 소거 동작을 수행한다. 이에 따라 제 2 블록(BLK2)의 목적지 페이지에 저장된 개인 정보가 삭제된다. 지우기 동작이 완료되면 NAND 플래시 메모리는 지우기 동작 완료 정보를 컨트롤러에 출력한다. 컨트롤러는 삭제 완료 정보에 대한 응답으로 삭제 완료를 호스트에 출력하고 이후 호스트는 개인 정보가 더 이상 저장 장치에 저장되지 않음을 인식한다. 그러나, 도 1에 설명된 바와 같이. 관리되지 않는 데이터로 저장된 개인 정보는 NAND 플래시 메모리에 남아 있다.

[0026] 도 2를 참조하면, 잠재적인 해커가 이러한 캐시-백(cache-back) 프로그램 동작의 약점을 악용할 수 있다. 해커가 강력한 능력을 가지고 있고, 컨트롤러의 관리 정보에 접근할 수 있고, 컨트롤러의 블록 관리 정보에 충분히 접근할 수 있으며, 관리되지 않는 블록을 관리 가능한 블록으로 변경하여 NAND 플래시 메모리에 접근할 수 있다고 가정한다. 이 시점에서 해커는 다른 일반 사용자와 마찬가지로 관리되지 않는 데이터에 대한 주소에 액세스하기 위해 관리되지 않는 데이터에 액세스하고 저장 장치에 읽기 요청을 보낼 수 있다. 이러한 유형의 읽기 요청에 응답하여 컨트롤러는 읽기 명령을 전송하고 NAND 플래시 메모리의 관리되지 않는 데이터에 대한 액세스를 허용할 수 있다. 읽기 명령에 응답하여, NAND 플래시 메모리는 관리되지 않는 데이터가 저장된 제 1 블록(BLK1)의 소스 페이지로부터 읽기 동작을 수행하고 그 결과를 컨트롤러로 전송할 수 있다. 결과적으로 컨트롤러는 읽기 동작에 따라 읽기 데이터를 해커에게 전송할 수 있다. 이런 식으로 NAND 플래시 메모리의 프라이버시는 단순한 용어로만 침해된다.

[0027] 이하에서는, 본 발명에 따른 NAND 플래시 메모리의 카피-백 프로그램을 설명하기로 한다.

[0028] 도 3은 본 발명의 일 실시예에 따른 NAND 플래시 메모리의 카피-백 프로그램 동작의 타이밍도이다. 도 3을 참조하면, 하나의 읽기 명령과 두 개의 프로그램 명령으로 구성된다.

[0029] 도 3에 도시된 바와 같이, 보안 카피-백 프로그램 동작은 소스 주소에 대응하는 물리적 페이지(소스 페이지)에 대한 읽기 동작, 목적지 주소에 대응하는 물리적 페이지(목적지 페이지)에 및 소스 페이지에 대응하는 물리적 페이지에 대한 프로그램 동작을 포함한다. 또한 향상된 보안 프로그램 동작이 포함될 수 있다.

[0030] 읽기 동작은 읽기 시간(tR) 동안 NAND 플래시 메모리의 읽기 명령 및 소스 주소를 통해 해당 소스 페이지에서 수행될 수 있다. 프로그램 동작(제1 프로그램 동작)은 제1 프로그램 시간이라 명명될 수 있는 프로그램 시간(tPROG) 동안 NAND 플래시 메모리의 프로그램 명령 및 대상 주소에 해당하는 대상 페이지에서 수행될 수 있다.

[0031] 그 후, 제2 프로그램 시간이라 명명될 수 있는 강화 보안 프로그램 동작 시간(tPROG_ES) 동안 프로그램 명령 및 소스 주소에 따라 NAND 플래시 메모리에서 강화된 보안 프로그램 동작(제2 프로그램 동작)이 수행될 수 있다. 기존의 카피-백 프로그램 동작 후, 소스 페이지에서 제안한 프로그램 동작을 더 수행할 수 있다. 예컨대, 덮어쓰기 동작을 통해 원본 페이지(소스 페이지)에 저장된 원본 데이터가 변경될 수 있다.

[0032] 전술한 바와 같이, 본 발명의 일 실시예에 따른 보안 카피-백 프로그램 동작은 기존의 카피-백 프로그램 동작 이후에 강화된 보안 프로그램 동작을 더 수행한다. 강화된 보안 프로그램 운영은 두 가지 주요 형태로 구현될 수 있다.

[0033] 도 4a 및 도 4b는 본 발명의 실시예들에 따른 NAND 플래시 메모리의 보안 카피-백 프로그램 방법을 설명하는 도면들이다.

[0034] 첫 번째, 강화된 보안 프로그램 동작은 소스 페이지에 랜덤 데이터를 프로그래밍하는 동작을 의미하지만, 도 4a를 참조하면, 랜덤 데이터는 소스 페이지에 저장된 데이터를 파괴하는 것이 목적이므로 소스 페이지에 완전히 프로그래밍할 필요는 없다. 두 번째, 강화 보안 프로그램 동작은, 도 4b를 참조하면, 소스 페이지에 복수의 삭제 펄스를 인가하는 동작을 의미한다. 소스 페이지에 저장된 데이터는 삭제 펄스 인가와 함께 알려지지 않은 형태로 변경된다. 여기서, 소거 펄스의 인가는 소스 페이지에 해당하는 워드 라인에 인가하는 것을 의미한다.

[0036] 프로그램 방해 문제

[0037] 한편, 강화된 보안 프로그램 동작을 수행할 때 다른 워드 라인에 연결된 데이터의 손상을 최소화하기 위해, 보안 카피-백 프로그램 동작을 수행해야 한다. 이는 강화된 보안 프로그램 운영으로 인해 프로그램 방해가 발생하기 쉽기 때문이다.

[0038] 도 5는 일반적인 3D NAND 플래시 메모리의 구조를 도시한 도면이다. 도 5를 참조하면, 판 모양의 워드 라인이 적층된 구조를 가질 수 있다. 워드 라인(WLi)에 연결된 메모리 셀에 소거 기법을 적용하면, 인접한 워드 라인에 연결된 메모리 셀에 프로그램 방해가 발생할 수 있다.

[0039] 강화된 보안 프로그램 동작으로 인한 프로그램 방해를 줄이기 위해, 일 예로 채널 부스팅 동작이 미리 수행될 수 있다. 특히, 프로그램 방해를 줄이기 위해 채널이 처음 충전될 때 강화된 보안 프로그램 동작을 수행할 수 있다. 향상된 보안 프로그램 동작을 수행하기 전에 채널에 전원 공급 장치 전압 (VDD)이 사전 충전된다. 채널은 워드 라인에 저장된 데이터에 따라 모두 사전 충전되거나 부분적으로 사전 충전된다. 도 5를 참조하면, 선택되지 않은 워드 라인(WLi-2, WLi-1, WLi+1, WLi+2)에는 패스 전압(Vpass)이 인가되고, 선택된 워드 라인에는 삭제 펄스 또는 프로그램 펄스가 인가될 수 있다. 따라서, 선택된 워드 라인(WLi)에 연결된 메모리 셀의 소스 데이터는 무효 데이터가 된다.

[0040] 덮어 쓰기 기술은 인접한 워드 라인에 연결된 메모리 셀의 열화에 필연적으로 영향을 미친다. 워드 라인 커플링의 영향을 최소화하기 위해 부스팅 동작이 수행되지만 여전히 충분하지 않다. 운영자가 불필요한 데이터를 삭제하려고 할 수 있지만 실제로 이 동작은 필요한 데이터의 신뢰성을 떨어뜨린다. 따라서, 덮어 쓰기 기법을 이용하여 워드 라인에 인접한 워드 라인에 대해 데이터 복구 읽기 동작이 수행될 수 있다.

[0041] 데이터 복구 읽기 동작은 선택된 워드 라인에 연결된 메모리 셀의 데이터를 읽을 때 인접한 워드 라인에 연결된 메모리 셀의 프로그램 상태를 반영하여 읽기 레벨을 변경하는 것을 의미한다. 데이터 복구 읽기 동작은 주로 인접한 선택되지 않은 워드 라인에 연결된 공격 셀에서 데이터를 읽는 것과, 변경된 읽기 조건 및 공격 셀의 읽기 데이터를 기반으로 선택된 워드 라인에 연결된 메모리 셀의 읽기 조건을 변경하는 것을 포함한다. 또한, 읽기 조건에 따라 선택된 워드 라인에 연결된 메모리 셀의 읽기 데이터를 읽는다. 여기서, 변경된 읽기 조건은 읽기 레벨, 개발 시간 또는 프리차지(precharge) 시간을 포함할 수 있다.

[0043] 희생 셀 정보를 이용한 덮어 쓰기

[0044] 인접한 워드 라인에 연결된 메모리 셀 중에는 영향을 많이 받는 셀과 그렇지 않은 셀이 있다. 예를 들어, 하위 상태로 프로그래밍된 셀은 희생 셀일 가능성이 높다. 반면, 더 높은 상태로 프로그래밍된 셀은 덮어 쓰기의 영향을 덜 받다. 따라서, 덮어 쓰기 기법에 따른 삭제 동작을 수행하기 전에 먼저 인접 워드 라인의 희생 셀 그룹 정보를 읽고, 읽은 희생 셀 그룹 정보를 이용하여 랜덤 데이터를 프로그래밍할지 여부를 결정할 수 있다.

[0046] 성능 비교

[0047] 비교예 1은 ECC-온칩이고, 비교예 2는 ECC-오프칩이며, 이는 도 1에 도시된 것을 참조한다. 실시예 1은 보안 ECC-온칩이고, 실시예 2는 보안 ECC-오프칩이다. 실시예 3은 프로그램 방해가 감소된 보안 ECC-온칩이고, 실시예 4는 프로그램 방해가 감소된 보안 ECC-오프칩이다. 설명의 편의를 위해, 무결성(integrity) 및 보안 카피 백 프로그램 동작은, 희생 셀 정보를 획득하기 위해 선택된 워드 라인에 인접한 워드 라인에 대해 적어도 두 번의 읽기 동작을 수행한다고 가정한다.

[0048] 표 1은 비교예 및 실시예에 따른 카피-백 프로그램 작동 성능 비교를 나타내는 표이다.

[0049] [표 1]

	총 동작 시간	인접 희생 셀 방지	포렌식 방지
비교예 1	$T_R+ T_{PGM}$	X	X
비교예 2	$T_R+ T_{ECC}+ T_{PGM}$	X	X
실시예 1	$T_R+ 2T_{PGM}$	X	O
실시예 2	$T_R+ T_{ECC}+ 2T_{PGM}$	X	O
실시예 3	$3T_R + 2T_{PGM}$	O	O
실시예 4	$3T_R+ T_{ECC}+ 2T_{PGM}$	O	O

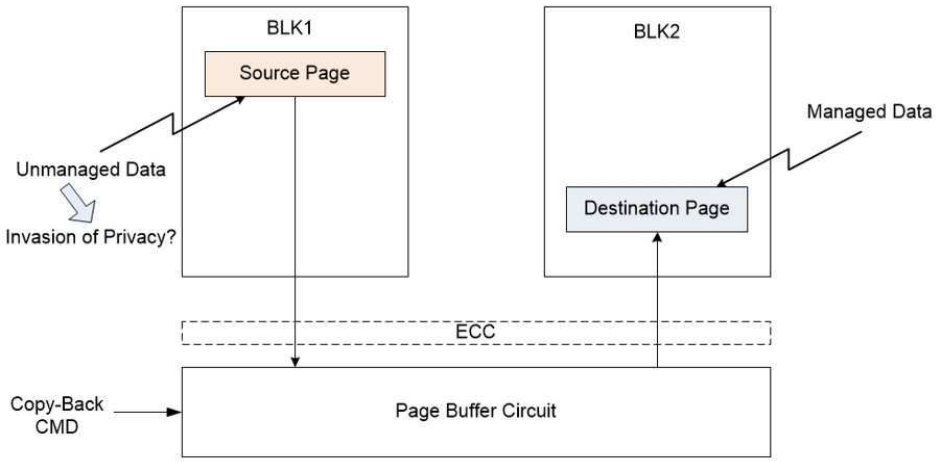
[0050]

[0051] 여기서 T_R은 읽기 동작 시간, T_{PGM}은 프로그램 동작 시간, T_{ECC}는 ECC 동작 시간이다. 비교예 1은 정상적인 카피 백 프로그램 작동에서 ECC 작동 시간을 숨길 수 있다. 따라서 비교예 2에서만 T_{ECC}가 존재한다. 예를 들어, 페이지 프로그램 T_{PGM}은 약 600 μs, 페이지 읽기 시간 T_R은 약 25 μs, 내부 ECC 시간 T_{ECC}는 약 100 μs이다. T_{ECC}와 T_R은 T_{PGM}에 비해 작기 때문에 전체 시간이 덜 영향을 받는다. 실시예들에서는 프로그래밍만큼 많은 시간을 소비하지만 포렌식을 방지할 수 있다는 추가 이점이 있다. 또한, 기존의 카피 백 프로그램 방식은 인접 셀 희생을 방지하지 못하지만, 본 발명에 따른 실시예들은 무결성 및 보안 카피 백 프로그램 방식이 이를 달성할 수 있다.

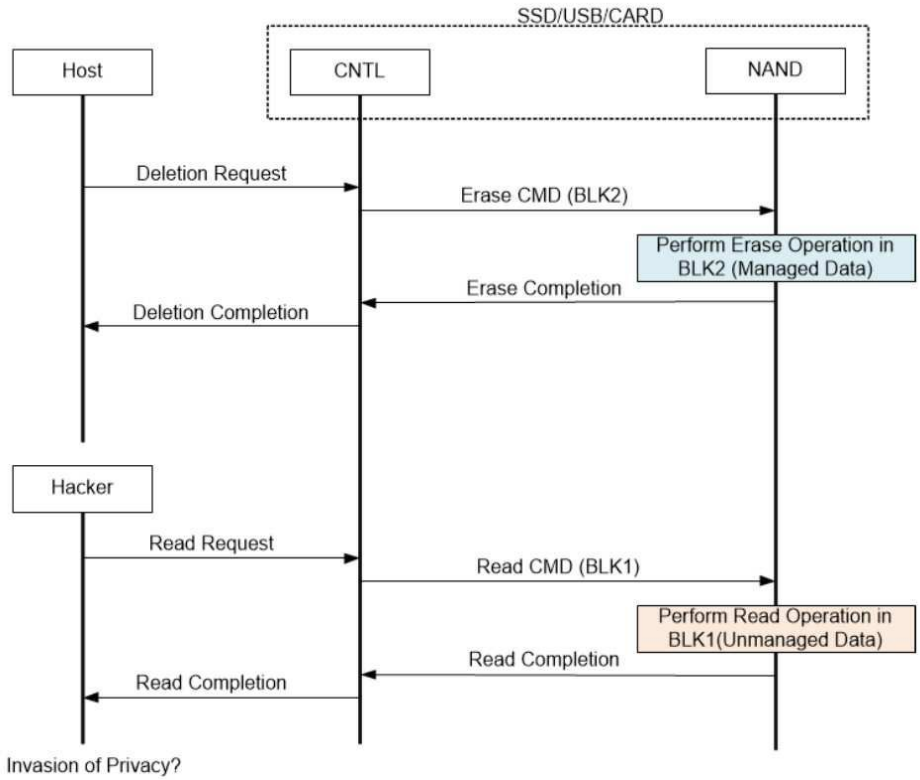
[0052] 이상, 첨부된 도면을 참조하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예에는 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

도면

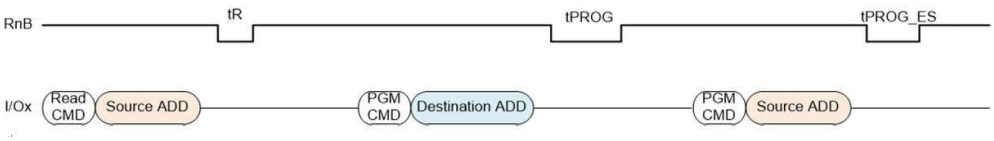
도면1



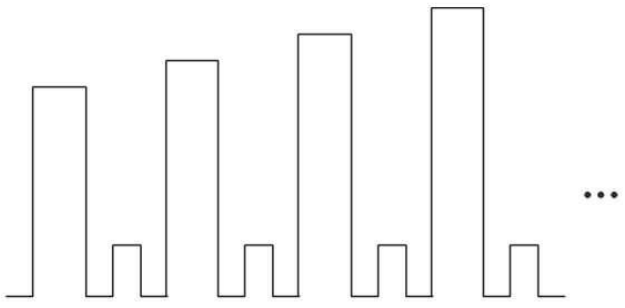
도면2



도면3

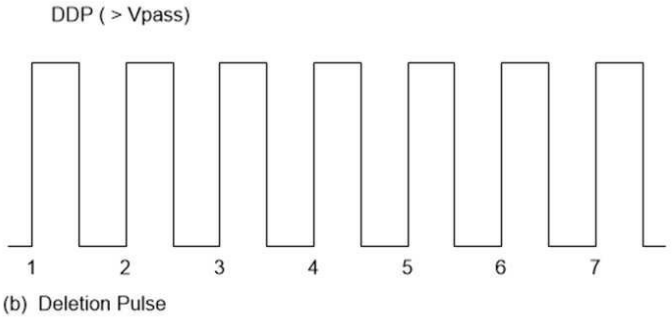


도면4a



(a) Overwriting Pulse with Random Data

도면4b



(b) Deletion Pulse

도면5