(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년06월12일
(11) 등록번호 10-1155697
(24) 등록일자 2012년06월05일

(51) 국제특허분류(Int. Cl.)
G06F 13/16 (2006.01) *G06F 12/06* (2006.01)
G06F 12/08 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2010-0019023
(22) 출원일자 2010년03월03일
심사청구일자 2010년03월03일
(65) 공개번호 10-2010-0100649
(43) 공개일자 2010년09월15일
(30) 우선권주장
12/398,090 2009년03월04일 미국(US)
(56) 선행기술조사문헌
KR1020040101342 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
애플 인크.
미합중국 95014 캘리포니아 쿠퍼티노 인피니트 루프 1
(72) 발명자
헤르만, 케네스
미국 캘리포니아주 산 호세
비옴, 매튜
미국 캘리포니아주 캠프벨
(뒷면에 계속)
(74) 대리인
백만기, 양영준

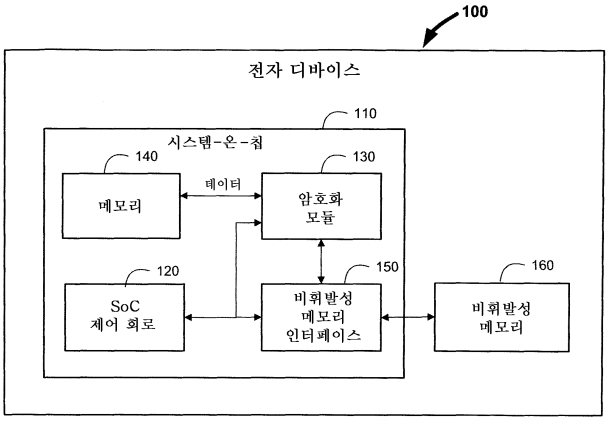
전체 청구항 수 : 총 20 항 심사관 : 엄인권

(54) 발명의 명칭 **비휘발성 메모리에 데이터를 기록하고 이로부터 데이터를 판독하기 위한 데이터 화이트닝**

(57) 요 약

플래시 메모리와 같은 비휘발성 메모리로의 저장을 위해 데이터를 화이트닝하고 관리하기 위한 시스템들, 장치들 및 방법들이 제공된다. 일부 실시예들에서, 시스템-온-칩(SoC) 및 비휘발성 메모리를 포함하는 미디어 플레이어와 같은 전자 디바이스가 제공된다. SoC는 SoC 제어 회로, 및 SoC 제어 회로와 비휘발성 메모리간의 인터페이스로서 동작하는 메모리 인터페이스를 포함한다. SoC는 또한 고급 암호 표준(AES)에 기초한 블록 암호와 같은 암호화 모듈을 포함할 수 있다. 메모리 인터페이스는 비휘발성 메모리로의 저장에 앞서서 민감한 데이터, 비-민감한 데이터 및 메모리 관리 데이터를 포함하는 모든 타입들의 데이터를 화이트닝하도록 암호화 모듈에게 지시할 수 있다. 이것은 예를 들면 프로그램-디스터브 문제들 또는 다른 판독/기록/삭제 신뢰성 이슈들을 방지하거나 감소시킬 수 있다.

대 표 도 - 도1



(72) 발명자
스미스, 마이클 제이.
미국 캘리포니아주 샌 프란시스코

토엘케스, 타호마 엠.
미국 캘리포니아주 산 호세

특허청구의 범위

청구항 1

시스템으로서,

비휘발성 메모리와 시스템 온 칩(system-on-a-chip; SoC)을 포함하고,

상기 시스템 온 칩은,

암호화 키 또는 화이트닝(whitening) 키에 따라 데이터를 암호화하도록 구성된 암호화 모듈 - 상기 데이터는 민감한 데이터(sensitive data), 비-민감한 데이터(non-sensitive data) 및 메모리 관리 데이터 중 적어도 하나를 포함함 -; 및

상기 암호화 모듈에 결합되고, 상기 암호화 데이터를 상기 비휘발성 메모리에 저장하도록 구성된 메모리 인터페이스를 포함하고,

상기 암호화 모듈은 상기 메모리 인터페이스에 의해,

상기 암호화 키를 이용해 상기 민감한 데이터를 암호화하고,

상기 화이트닝 키를 이용해 적어도 상기 비-민감한 데이터를 암호화하도록 지시되어, 적어도 상기 비-민감한 데이터가 상기 비휘발성 메모리에 저장되기 이전에 화이트닝 되는 것이 보장되는, 시스템.

청구항 2

제1항에 있어서,

상기 암호화 모듈은 AES(Advanced Encryption Standard) 엔진을 포함하는 시스템.

청구항 3

제1항에 있어서,

상기 SoC는 상기 비휘발성 메모리와 상기 민감한 데이터 및 비-민감한 데이터를 교환하기 위해 상기 메모리 인터페이스에 명령들을 발행하도록 구성된 파일 시스템을 더 포함하며,

상기 메모리 인터페이스는 상기 민감한 데이터 또는 비-민감한 데이터의 상기 비휘발성 메모리로의 저장을 관리하기 위한 메모리 관리 데이터를 생성하도록 구성된 메모리 트랜슬레이션(translation) 층을 포함하는 시스템.

청구항 4

제3항에 있어서,

상기 파일 시스템은 상기 민감한 데이터와 함께 암호화 키를 제공하도록 또한 구성되고, 상기 파일 시스템은 상기 비-민감한 데이터와 함께 어떠한 암호화 키도 제공하지 않도록 또한 구성되는 시스템.

청구항 5

사용자 데이터의 비휘발성 메모리로의 저장을 관리하기 위한 장치로서,

상기 사용자 데이터에 대한 메모리 관리 데이터를 생성하고, 상기 메모리 관리 데이터를 저장할 상기 비휘발성 메모리의 제1 물리적 어드레스를 선택하며, 상기 선택된 제1 물리적 어드레스에 기초하여 제1 암호화 시드(seed)를 계산하도록 구성된 메모리 인터페이스와,

상기 선택된 제1 물리적 어드레스에서의 저장을 위해 상기 제1 암호화 시드를 이용하여 상기 메모리 관리 데이터를 랜덤화(randomize)하도록 구성되는 암호화 모듈

을 포함하는 장치.

청구항 6

제5항에 있어서,

상기 암호화 모듈은 AES 엔진을 포함하고, 상기 제1 암호화 시드는 초기화 벡터를 포함하며,

상기 메모리 인터페이스는 상기 AES 엔진에 대한 비밀 키로서 미리 정해진 키를 선택하도록 더 구성되고, 상기 미리 정해진 키는 상기 선택된 제1 물리적 어드레스의 값과 독립되어 있는 장치.

청구항 7

제5항에 있어서,

상기 메모리 인터페이스는,

상기 암호화 모듈이 상기 제1 암호화 시드를 이용하여 상기 메모리 관리 데이터를 암호해제(decrypt)하도록 지도(direct)하고,

상기 메모리 관리 데이터를 저장할 상기 비휘발성 메모리의 제2 물리적 어드레스를 선택하며,

상기 선택된 제2 물리적 어드레스에 기초하여 제2 암호화 시드를 계산하고,

상기 암호화 모듈이 상기 선택된 제2 물리적 어드레스에서 상기 비휘발성 메모리로의 저장을 위해 상기 제2 암호화 시드를 이용하여 상기 메모리 관리 데이터를 랜덤화하게 지도하도록 또한 구성되는 장치.

청구항 8

암호화 모듈과,

비휘발성 메모리를 관리하고 암호화 모듈과 통신하도록 동작가능한 메모리 인터페이스를 포함하고,

상기 메모리 인터페이스는,

논리적 어드레스에 정보 - 이 정보는 비-민감한 데이터를 포함함 - 를 저장하라는 명령을 수신하고,

상기 논리적 어드레스에 기초하여 암호화 시드를 생성하며,

상기 암호화 모듈이 상기 비휘발성 메모리의 제1 물리적 어드레스로의 저장을 위해 상기 암호화 시드를 이용하여 상기 정보를 암호화하도록 지도하고,

상기 암호화된 정보를 상기 비휘발성 메모리의 상기 제1 물리적 어드레스로부터 제2 물리적 어드레스로 이동시킬 때 상기 정보의 암호해제를 바이패싱하도록 구성되는 시스템.

청구항 9

제1항 또는 제8항에 있어서,

상기 비휘발성 메모리는 NAND 플래시를 포함하는 시스템.

청구항 10

제8항에 있어서,

상기 메모리 인터페이스는,

적어도 하나의 암호화 시드가 결여된 명령에 기초하여 상기 정보가 비-민감한 데이터를 포함하고 있는 것을 검출하도록 또한 구성되는 시스템.

청구항 11

제8항에 있어서,

상기 메모리 인터페이스는,

상기 비휘발성 메모리에 대한 가비지 콜렉션(garbage collection)을 개시하도록 구성되고, 상기 암호화된 정보는 상기 가비지 콜렉션 동안에 상기 제1 물리적 어드레스로부터 제2 물리적 어드레스로 이동되는 시스템.

청구항 12

제8항에 있어서,

상기 메모리 인터페이스는,

상기 논리적 어드레스를 상기 제2 물리적 어드레스와 연관시키도록 메모리 관리 데이터를 업데이트하고,

상기 논리적 어드레스로부터 상기 정보를 검색하라는 판독 명령을 수신하며,

상기 메모리 관리 데이터를 이용하여 상기 제2 물리적 로케이션을 결정하고,

상기 논리적 어드레스에 기초하여 상기 암호화 시드를 재생성하며,

상기 암호화 모듈이 상기 재생성된 암호화 시드를 이용하여 상기 정보를 암호해제하게 지도하도록 또한 구성되는 시스템.

청구항 13

메모리 인터페이스를 이용하여 비휘발성 메모리를 관리하는 방법으로서,

상기 비휘발성 메모리로의 저장을 위해 정보를 수신하는 단계와,

상기 정보가 민감한 정보인지 또는 비-민감한 정보인지 여부를 검출하는 단계와,

상기 검출 단계에 기초하여 개인(privacy) 키와 화이트닝 키 사이에서 선택하는 단계와,

상기 비휘발성 메모리로의 저장을 위해 상기 정보를 암호화하도록 상기 선택된 키를 이용하여 상기 정보의 암호화를 인에이블하는 단계

를 포함하는 비휘발성 메모리 관리 방법.

청구항 14

제13항에 있어서,

상기 검출 단계는 상기 개인 키가 상기 정보를 상기 비휘발성 메모리에 기록하라는 명령과 함께 수신되었는지 여부를 결정하는 단계를 포함하는 비휘발성 메모리 관리 방법.

청구항 15

제13항에 있어서,

상기 화이트닝 키의 값은 상기 정보, 및 상기 정보와 연관된 어드레스와 독립적인 비휘발성 메모리 관리 방법.

청구항 16

제13항에 있어서,

상기 검출된 정보가 민감한 정보인 경우에 제1 초기화 벡터를 수신하는 단계와,

상기 검출된 정보가 비-민감한 정보인 경우에 제2 초기화 벡터를 생성하는 단계와,

상기 정보가 민감한 정보인지 또는 비-민감한 정보인지 여부에 기초하여 상기 제1 및 제2 초기화 벡터들 사이에서 선택하는 단계

를 더 포함하는 비휘발성 메모리 관리 방법.

청구항 17

제13항에 있어서,

상기 수신된 정보에 대해 메모리 관리 데이터를 생성하는 단계와,

상기 비휘발성 메모리로의 저장을 위해 상기 화이트닝 키를 이용하여 상기 메모리 관리 데이터의 암호화를 인에이블하는 단계

를 더 포함하는 비휘발성 메모리 관리 방법.

청구항 18

메모리 인터페이스를 이용하여 비휘발성 메모리로의 저장을 위해 정보를 준비하는 방법 - 상기 정보는 논리적 어드레스와 연관됨 - 으로서,

상기 논리적 어드레스에 기초하여 상기 정보를 암호화하는 단계와,

상기 논리적 어드레스를 상기 비휘발성 메모리의 제1 물리적 어드레스에 매핑하는 메모리 관리 데이터를 생성하는 단계와,

상기 비휘발성 메모리의 제2 물리적 어드레스에 기초하여 상기 메모리 관리 데이터를 암호화하는 단계와,

상기 암호화된 정보를 상기 제1 물리적 어드레스에 저장하는 단계와,

상기 암호화된 메모리 관리 데이터를 상기 비휘발성 메모리의 제2 물리적 어드레스에 저장하는 단계

를 포함하는 정보 준비 방법.

청구항 19

제18항에 있어서,

상기 암호화된 정보를 상기 제1 물리적 어드레스로부터 상기 비휘발성 메모리의 제3 물리적 어드레스로 이동시키는 단계를 더 포함하고, 상기 암호화된 정보는 상기 이동 단계 전체에 걸쳐 암호화된 상태로 유지되는 정보 준비 방법.

청구항 20

제13항 또는 제18항에 있어서,

상기 비휘발성 메모리는 NAND 플래시 메모리를 포함하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 NAND 플래시 메모리와 같은 비휘발성 메모리로의 저장을 위해 데이터를 화이트닝(whitening)하고 관리하기 위한 시스템들, 방법들 및 장치들에 관한 것이다.

배 경 기 술

[0002] 다른 타입들의 비휘발성 메모리들뿐만 아니라 NAND 플래시 메모리는 대용량 저장을 위해 전자 디바이스들에 일반적으로 이용되고 있다. 예를 들면, 휴대용 미디어 플레이어들은 음악, 비디오들 및 다른 미디어를 저장하는 플래시 메모리를 종종 포함한다.

[0003] 메모리 용량들을 유지하거나 증가시키면서도 이들 전자 디바이스들의 크기를 감소시키기 위해, 플래시 및 다른 타입들의 메모리 셀들은 계속적으로 크기가 축소되고 있고 더욱 더 밀집하여 팩킹되고(packed) 있다. 이것은 비휘발성 메모리에 기록하고 이로부터 판독할 때 신뢰성을 감소시키는 프로그램-교란 및 다른 문제들을 야기시킬 수 있다. 특히, 하나 이상의 페이지들(즉, 비휘발성 메모리에 한번에 기록될 수 있는 데이터의 단위)의 프로그래밍 동안에, 메모리 셀들에 저장되어 있는 데이터 비트들이 거의 모두 동일한 값(예를 들면, 거의 모두 1 또는 모두 제로)인 경우, 이들 메모리 셀들에 인가된 프로그래밍 전압들은 근처의 메모리 셀들에 대해 강한 전계 효과를 끼칠 수 있다. 이것은 영향을 받은 메모리 셀들이 부정확하게 또는 부분적으로 프로그래밍되도록 유발할 수 있고, 이는 데이터가 후속 판독 동작 동안에 부정확하게 해석될 가능성을 증가시킬 수 있다.

발명의 내용

해결하려는 과제

[0004] NAND 플래시 메모리와 같은 비휘발성 메모리 상의 저장을 위해 데이터를 화이트닝하거나 관리하기 위한 시스템들, 장치들 및 방법들이 제공된다. "화이트닝"은 일반적으로 데이터의 시퀀스의 랜덤성을 증가시키는 것을

지칭하는 것으로, 이는 데이터 시퀀스들이 고도로 불균형한 개수의 1들 내지 0들을 가질 가능성을 감소시킬 수 있다. 데이터 화이트닝은 고급 암호 표준(Advanced Encryption Standard; AES)에 기초한 블록 암호(block cipher)와 같은 암호화 모듈을 이용하여 수행될 수 있다. 암호화 모듈은 민감한 정보(예를 들면, 개인 정보)에 대한 보안을 제공하는 데에도 이용될 수 있으므로, 개시된 실시예들은 이러한 목적에 전용된 하드웨어를 요구하지 않고서도 데이터 화이트닝을 제공할 수 있다.

[0005] 일부 실시예들에서, 미디어 플레이어와 같은 전자 디바이스가 제공된다. 전자 디바이스는 시스템-온-칩(system-on-a-chip; SoC) 및 플래시 메모리와 같은 비휘발성 메모리를 포함할 수 있다. SoC는 암호화 모듈 및 메모리 인터페이스를 포함할 수 있다. 메모리 인터페이스는 비휘발성 메모리와 통신하여 판독 및 기록 명령들 각각에 응답하여 비휘발성 메모리로부터 데이터를 판독하거나 이것에 데이터를 프로그래밍할 수 있다. 일부 실시예들에서, 메모리 인터페이스는 비휘발성 메모리와, 판독 및 기록 명령들을 발행할 수 있는 SoC의 파일 시스템 사이의 인터페이스로서 기능할 수 있는 트랜슬레이션층(translation layer)을 포함할 수 있다.

[0006] 프로그램-교란 또는 다른 신뢰성 이슈들을 방지하기 위해, 메모리 인터페이스는 파일 시스템이 암호화되도록 요구하는 단지 민감한 데이터만이 아니라, 비휘발성 메모리에 기록되는 모든 데이터를 암호화하도록 암호화 모듈에게 지시할 수 있다. 메모리 인터페이스는 비휘발성 메모리에 저장되는 임의의 메모리 관리 데이터뿐만 아니라 암호화가 요구되지 않는 비-민감한 데이터를 암호화할 수 있다. 종종 메타데이터로도 지칭되는 메모리 관리 데이터는 민감하거나 비-민감한 데이터의 저장을 관리할 때 이용하기 위해 메모리 인터페이스에 의해 생성되는 임의의 데이터를 포함할 수 있다. 일부 실시예들에서, 메타데이터는 데이터에 대해 파일 시스템에 의해 제공되는 어드레스(또는 "논리적 어드레스") 및 이 데이터가 저장될 것이거나 저장되었던 비휘발성 메모리의 어드레스(또는 "물리적 어드레스") 사이의 매핑을 추적할 수 있는 메모리 맵 정보를 포함할 수 있다.

[0007] SoC의 암호화 모듈은 종종 "암호화 시드들(seeds)"로 지칭될 수 있는 하나 이상의 초기 값들을 이용하여 데이터를 암호화하고 암호해제할 수 있다. AES 엔진들에 있어서, 암호화 시드들은 키 및 초기화 벡터("IV")를 포함할 수 있다. 메모리 인터페이스는 판독되거나 프로그래밍되고 있는 데이터의 타입(예를 들면, 민감한 데이터, 비-민감한 데이터, 또는 메타데이터)에 기초하여 암호화 시드들을 생성하거나 선택할 수 있다. 일부 실시예들에서, 메모리 인터페이스는 파일 시스템으로부터 데이터를 판독하거나 기록하는 명령을 수신할 수 있고, 메모리 인터페이스는 정보가 민감한 지 또는 비-민감한 지 여부를 검출할 수 있다. 데이터가 민감한 경우, 메모리 모듈은 파일 시스템에 의해 제공되는 안전한 개인 키 및 초기화 벡터를 이용하여 데이터를 암호화할 수 있다. 그렇지 않으면, 비-민감한 데이터에 대해, 메모리 인터페이스는 데이터의 논리적 어드레스에 기초하여 생성될 수 있는 소정의 화이트닝 키 및 IV를 이용할 수 있다.

[0008] 이러한 기술을 이용함으로써, 메모리 인터페이스는 데이터의 물리적 어드레스에 종속될 수 있는 암호화 시드를 이용하지 않고 민감한 및 비-민감한 데이터를 화이트닝할 수 있다. 그러므로, 민감한 및 비-민감한 데이터는 이전 물리적 어드레스에 기초하여 데이터를 암호해제하고 새로운 물리적 어드레스에 기초하여 데이터를 재-암호화할 필요없이 비휘발성 메모리의 상이한 물리적 로케이션들 사이에서 이동될 수 있다(예를 들면, 가비지 콜렉션(garbage collection) 또는 웨어 레벨링 동안에, 데이터는 유효 정보 및 자유로운 블록들을 통합하도록 이동되는 경우).

[0009] 일부 실시예들에서, 메모리 인터페이스에 의해 생성된 메타데이터는 비휘발성 메모리에 유지될 수 있다. 이들 실시예들에서, 메모리 인터페이스는 메타데이터가 비휘발성 메모리에 저장되기 이전에 화이트닝을 위해 메타데이터를 암호화할 수 있다. AES 엔진에 대해, 메모리 인터페이스는 메타데이터가 저장되는 물리적 어드레스에 기초하여 생성될 수 있는 소정 화이트닝 키 및 IV로 AES 엔진을 시딩(seed)할 수 있다. IV는 물리적 어드레스에 기초하고 있기 때문에, 민감한 또는 비-민감한 정보와는 달리, 메모리 인터페이스는 메타데이터를 상이한 물리적 로케이션들 사이에서 이동시키고 있을 때(예를 들면, 가비지 콜렉션 동안에) 메타데이터의 각 페이지 상에서 암호해제(decryption) 및 재암호화를 수행할 수 있다.

도면의 간단한 설명

[0010] 본 발명의 상기 및 다른 양태들 및 장점들은 유사한 참조번호들이 전체에 걸쳐 유사한 부분들을 지칭하는 첨부된 도면들과 관련한 이하의 상세한 설명을 고려할 때 더욱 명백하게 될 것이다.

도 1은 본 발명의 실시예에 따라 구성된 전자 디바이스의 개략도이다.

도 2는 전자 디바이스 상에 구현되고 본 발명의 실시예에 따라 구성된 시스템-온-칩의 개략도이다.

도 3은 본 발명의 실시예에 따라 비휘발성 메모리에 데이터를 기록하기 위한 예시적 프로세스의 플로우차트이

다.

도 4는 본 발명의 실시예에 따라 비휘발성 메모리로부터 데이터를 판독하기 위한 예시적 프로세스의 플로우차트이다.

도 5는 본 발명의 실시예에 따라 비휘발성 메모리의 물리적 페이지들 사이에서 데이터를 이동시키기 위한 예시적 프로세스의 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0011] 도 1은 전자 디바이스(100)의 개략도이다. 일부 실시예들에서, 전자 디바이스(100)는 휴대용 미디어 플레이어(예를 들면, 캘리포니아주 쿠페르티노의 애플 인크에 의해 가용하게 된 iPod™), 셀룰러 전화기(예를 들면, 애플 인크에 의해 가용하게 되는 iPhone™), 포켓 크기의 퍼스널 컴퓨터들, 개인휴대단말기(PDA), 데스크탑 컴퓨터, 랩탑 컴퓨터, 및 임의의 다른 적합한 타입의 전자 디바이스이거나 이들을 포함할 수 있다.

[0012] 전자 디바이스(100)는 시스템-온-칩(SoC, 110) 및 비휘발성 메모리(160)를 포함할 수 있다. 비휘발성 메모리(160)는 플로팅 게이트 기술에 기반한 NAND 플래시 메모리일 수 있고, 각각이 한번에 삭제될 수 있는 "블록들"로 구성될 수 있고, 각각이 한번에 프로그램가능하고 판독가능할 수 있는 "페이지들"로 더 구성될 수 있다. 비휘발성 메모리(160)의 각 페이지는 물리적 페이지 어드레스를 이용하여 어드레싱될 수 있다. 도 1(나중 도면들도 포함) 및 다양한 개시된 실시예들이 플래시 기술를 이용하는 측면에서 기술되지만, 임의의 다른 타입의 비휘발성 메모리가 대신 구현될 수 있다. 예를 들면, 비휘발성 메모리(160)는 NAND 플래시, NOR 플래시, 임의의 장래 세대의 비휘발성 메모리, 또는 그 조합을 포함할 수 있다. 또한, 일부 실시예들에서, 비휘발성 메모리(160)는 오프-칩(off-chip) 대신에 시스템-온-칩(110) 상에 구현될 수 있고, 전자 디바이스(100)는 도면을 과도하게 복잡하게 하는 것을 방지하기 위해 도 1에 도시되지는 않은, 전력원 또는 임의의 사용자 입력 또는 출력 디바이스들과 같은 다른 컴포넌트들을 포함할 수 있다.

[0013] 시스템-온-칩(110)은 SoC 제어 회로(120), 암호화 모듈(130), 메모리(140), 및 비휘발성 메모리 인터페이스(150)를 포함할 수 있다. SoC 제어 회로(120)는 SoC(110) 및 그 다른 컴포넌트들의 일반적인 동작들 및 기능들을 제어할 수 있다. 예를 들면, 사용자 입력들 또는 애플리케이션의 명령들에 응답하여, SoC 제어 회로(120)는 비휘발성 메모리 인터페이스(150)에 판독 또는 기록 명령들을 발행하여 비휘발성 메모리(160)로부터 데이터를 얻거나 이것에 데이터를 저장할 수 있다. SoC 제어 회로(120)는 하드웨어, 소프트웨어, 및 펌웨어의 임의의 조합, 및 전자 디바이스(100)의 기능을 구동하도록 동작하는 임의의 컴포넌트들, 회로 또는 로직을 포함할 수 있다.

[0014] 메모리(140)는 다이나믹 랜덤 액세스 메모리(DRAM), 동기형 다이나믹 랜덤 액세스 메모리(SDRAM), 더블-데이터-레이트(DDR) RAM, 캐시 메모리, 또는 판독 전용 메모리(ROM)와 같은 임의의 적합한 타입의 휘발성 또는 비휘발성 메모리를 포함할 수 있다. 메모리(140)는 비휘발성 메모리(160)에 프로그래밍하거나 이로부터 판독하기 위한 데이터를 일시적으로 저장할 수 있는 데이터 소스를 포함할 수 있다. 일부 실시예들에서, 메모리(140)는 SoC 제어 회로(120) 또는 메모리 인터페이스(150)에 의해 실행될 수 있는 펌웨어 또는 소프트웨어 애플리케이션들을 저장할 수 있고, 펌웨어 또는 소프트웨어를 위한 일시 스토리지를 제공하거나, 또는 그 조합을 제공할 수 있다.

[0015] 비휘발성 메모리 인터페이스(150)는 SoC 제어 회로(120)와 비휘발성 메모리(160) 사이에서 드라이버 또는 인터페이스(예를 들면, 플래시 인터페이스)로서 동작할 수도 있는, 하드웨어 및 소프트웨어의 임의의 적합한 조합을 포함할 수 있다. 예를 들면, 메모리 인터페이스(150)는 SoC 제어 회로(120)로부터의 판독 또는 기록 명령들을 해석하여 비휘발성 메모리(160)의 버스 프로토콜과 양립할 수 있는 판독 및 프로그램 명령들을 생성할 수 있다. 메모리 인터페이스(150)는 이하에 설명되는 바와 같이 비휘발성 메모리(160)에 저장될 데이터를 화이트닝하도록 암호화 모듈(130)에게 지시하는 것 및 웨어 레벨링(wear leveling) 또는 가비지 콜렉션(garbage collection) 동안에 비휘발성 메모리(160)의 물리적 로케이션들 사이에서 데이터의 페이지들을 이동시키는 것을 포함하여, 비휘발성 메모리(160)의 페이지들 및 블록들을 관리하도록 이들 및 임의의 다른 적합한 기능들을 수행할 수 있다. 메모리 인터페이스(150)가 SoC 제어 회로(120)로부터 분리된 모듈로서 도시되어 있지만, 일부 실시예들에서, 이들 모듈들은 하드웨어 또는 소프트웨어 컴포넌트들(또는 양쪽 모두)을 공유할 수 있고, 일부 기능은 교환가능할 수 있다.

[0016] 암호화 모듈(130)은 적합한 암호에 기초하여 암호화 및 암호해제를 수행하도록 구성된 임의의 하드웨어 또는

소프트웨어, 또는 그 조합이거나 이들을 포함할 수 있다. 예를 들면, 암호화 모듈(130)은 고급 암호 표준(AES), 데이터 암호 표준(DES), 또는 RSA에 기초할 수 있다. 암호화 모듈(130)은 비휘발성 메모리(160)에 저장되거나 전자 디바이스(100)와 송/수신되는(예를 들면, 도 1에 도시되지 않은 Wi-Fi™와 같은 통신 회로를 이용함) 개인 정보 또는 빌링(billing) 정보와 같은 민감한 데이터에 대한 보안을 제공할 수 있다. 보안을 제공할 뿐만 아니라, 암호화 모듈(130)에 의해 이용되는 암호화 알고리즘은 그것이 암호화하는 데이터를 화이트닝하거나 랜덤화하는 추가 특징을 제공할 수 있다. 그러므로, 암호화 모듈(130)은 그 데이터가 민감하지 않더라도 데이터를 암호화하도록 지시될 수 있고, 따라서 이러한 데이터는 비휘발성 메모리(160)에 기록되기 이전에 화이트닝될 수 있다. 이런 방식으로, 프로그램-교란 및 다른 신뢰성 이슈들이 감소될 수 있다.

[0017] 암호화 모듈(130)은 암호화 알고리즘에 의해 암호화 또는 암호해제를 수행하도록 요구될 수 있는, SoC 제어 회로(120) 또는 비휘발성 메모리 인터페이스(150)에 의해 제공되는 하나 이상의 "암호화 시드들"을 이용하여 데이터를 암호화하고 암호해제할 수 있다. 일부 실시예들에서, 그리고 특히 AES-기반 암호화 모듈들에 대해, 암호화 시드들은 키 및 초기화 벡터("IV")를 포함할 수 있다. 암호화된 데이터로부터 원래의 암호화되지 않은 데이터를 복원하기 위해, 암호해제에 이용되는 암호화 시드들은 암호화에 원래 이용된 시드들과 동일할 필요가 있다. 그러므로, 전자 디바이스가 이들 암호화 시드들을 관리하고 생성하는데 이용될 수 있는 다양한 기술들을 예시하는 다양한 특징들이 도 2 내지 5와 관련하여 아래에 개시된다.

[0018] 이제, 도 2를 참조하면, 시스템-온-칩(SoC, 210)의 개략도가 도시되어 있다. SoC(210)는 SoC(110)의 더 상세한 도면이거나, 시스템-온-칩의 완전히 상이한 구현일 수 있다. SoC(210)는 SoC 제어 회로(220), 암호화 모듈(230) 및 비휘발성 메모리 인터페이스(250)를 포함할 수 있고, 이들 각각은 도 1의 유사하게 명명된 컴포넌트들과 관련하여 상기 설명된 특징들 및 기능들의 임의의 하나를 가질 수 있으며 그 역으로도 마찬가지다. 예를 들면, 일부 실시예들에서, 암호화 모듈(230)은 암호화 시드들을 획득하는 키 및 IV 입력, 및 데이터 입력(도시되지 않음)으로부터 수신된 데이터의 암호화를 인에이블시키거나 디스에이블시키는 인에이블 입력을 가지는 고급 암호 표준(AES) 엔진이거나 이를 포함할 수 있다.

[0019] 도 2에는 어떠한 메모리 모듈들도 도시되지 않았지만, 도 2에 도시된 임의의 다양한 컴포넌트들 사이에 하나 이상의 적합한 버퍼들 또는 다른 일시 저장 모듈들이 제공될 수 있다는 것은 자명하다. 이들 메모리 모듈들은 SoC 제어 회로(220)의 내부에, SoC 제어 회로(220)의 외부에(예를 들면, 도 1의 메모리(140)), 또는 비휘발성 메모리 인터페이스(250)의 내부 또는 외부와 같이, SoC(210) 상의 임의의 적합한 위치에 배치될 수 있다.

[0020] SoC 제어 회로(220)는 전자 디바이스(예를 들면, 도 1의 전자 디바이스(100))의 일반적인 기능들을 제공할 수 있다. 예를 들면, SoC 제어 회로(220)는 사용자에 의해 개시되는 임의의 애플리케이션들(예를 들면, 음악 또는 다른 미디어 애플리케이션들)을 실행할 수 있고, 전자 디바이스의 오퍼레이팅 시스템을 포함할 수 있다. 동작 동안에, 애플리케이션들 및 다른 프로그램들 또는 펌웨어는 대량 스토리지(예를 들면, 도 1의 비휘발성 메모리(160))로부터 데이터를 저장하거나 검색할 필요가 있을 수 있다. SoC 제어 회로(220)는 애플리케이션이 실행되고 있는 정보 타입, 또는 전자 디바이스를 동작시키는 특정 사용자와 같은 다양한 인자들에 기초하여 "민감한" 또는 "비-민감한"정보로서 이러한 데이터를 할당할 수 있다. "민감한 데이터"는 일반적으로 데이터를 암호화하는 명령과 함께 저장을 위해 제공되는(예를 들면, 이하에 설명되는 바와 같이 파일 시스템(222)으로부터) 임의의 정보를 지칭한다. 민감한 데이터는 예를 들면 개인 정보 및 신용카드 정보를 포함할 수 있다.

[0021] SoC 제어 회로(220)는 애플리케이션 또는 오퍼레이팅 시스템에 의해 명령되는 판독 및 기록 명령들을 발행하는 파일 시스템(222)을 포함할 수 있다. 파일 시스템(222)은 파일 할당 테이블(FAT) 파일 시스템과 같은 임의의 적합한 타입의 파일 시스템을 포함할 수 있다. 각각의 판독 또는 기록 명령과 함께, 파일 시스템(222)은 데이터가 판독되거나 기록되어야 하는 장소를 나타내는 논리적 어드레스를 제공할 수 있다. 파일 시스템(222)은 오퍼레이팅 시스템 또는 애플리케이션이 데이터가 민감한 것으로 결정했는지 여부에 관한 정보를 제공할 수 있다. 민감한 데이터에 대해, 파일 시스템(222)은 판독 또는 기록 명령과 함께 개인 키 및 초기화 벡터를 제공할 수 있다. 데이터가 비-민감한 경우, 파일 시스템(222)은 유효한 암호화 시드들을 제공하지 않을 수 있다. 예를 들면, 파일 시스템(222)은 유효한 암호화 시드들 대신에 NULL 값들을 제공할 수 있다.

[0022] 파일 시스템(222)은 전자 디바이스(예를 들면, NAND 플래시) 상에서 구현되는 비휘발성 메모리와 직접적으로는 양립가능하지 않은 프로토콜을 이용하여 논리적 어드레스 및 암호화 시드들과 함께 판독 및 기록 요구들을 제공할 수 있다. 예를 들면, 파일 시스템(222)에 의해 제공되는 논리적 어드레스들은 하드드라이브 기반 시

스템에 전형적인 규약들(conventions) 또는 프로토콜들을 이용할 수 있다. 플래시 메모리와는 달리, 하드드라이브 기반 시스템은 처음에 블록 삭제를 수행하지 않고서도 메모리 로케이션을 중복기록할 수 있고, 디바이스의 수명을 증가시키기 위해 웨어 레벨링을 수행할 필요가 없다. 그러므로, SoC(210)는 비휘발성 메모리에 적합한 방식으로 파일 시스템 요구들을 다루는 임의의 메모리-특정(예를 들면, 플래시-특정) 또는 벤더-특정(또는 양쪽 모두) 기능들을 수행할 수 있는 비휘발성 메모리 인터페이스(250)를 포함할 수 있다.

[0023] 비휘발성 메모리 인터페이스(250)는 트랜슬레이션 층(252), 멀티플렉서들(254, 256), 및 버스 컨트롤러(258)를 포함할 수 있다. 일부 실시예들에서, 트랜슬레이션 층(252)은 플래시 트랜슬레이션 층일 수 있다. 트랜슬레이션 층(252)은 파일 시스템(222)으로부터 판독 및 기록 명령들을 해석하고 판독 및 기록 명령들을 비휘발성 메모리에 적합한 명령들로 번역할 수 있다. 특히, 기록/프로그램 동작 시에, 논리적 어드레스가 비휘발성 메모리 상의 자유롭고(free) 삭제된 물리적 로케이션에 대응하지 않을 수 있기 때문에, 트랜슬레이션 층(252)은 파일 시스템(222)으로부터 수신된 논리적 어드레스에 데이터를 직접 기록하지 않을 수 있다. 대신에, 트랜슬레이션 층(252)은 파일 시스템(222)으로부터 수신된 논리적 어드레스를, 비휘발성 메모리 상의 자유로운 물리적 어드레스로 변환할 수 있다. 판독 동작 시에, 트랜슬레이션 층(252)은 수신된 논리적 어드레스에 대응하는 저장된 데이터의 실제적인 물리적 어드레스를 결정할 수 있다.

[0024] 트랜슬레이션 층(252)은 논리적 및 물리적 어드레스들 간의 이러한 매핑을 유지하는 메모리 관리 데이터(또는 "메타데이터")를 생성할 수 있다. 메모리 "관리 데이터" 또는 "메타데이터"는 파일 시스템에 의해 제공되지 않은 임의의 데이터를 포함할 수 있고, 대신에 이는 인터페이스(250)의 컴포넌트들(예를 들면, 트랜슬레이션 층(252))에 의해 생성될 수 있다. 트랜슬레이션 층(252)은 또한 이하에 설명된 가비지 콜렉션 또는 웨어 레벨링을 수행하는 것을 포함하여, 비휘발성 메모리 상의 저장을 관리하기 위한 임의의 다른 적합한 태스크들을 수행할 수 있다.

[0025] 메모리 관리 데이터(예를 들면, 결정된 물리적 어드레스들)를 이용하는 경우, 트랜슬레이션 층(252)은 버스 컨트롤러(258)에게 판독 및 기록 요청들을 제공할 수 있고, 삭제 요청들을 버스 컨트롤러(258)에게 발행하여 비휘발성 메모리 상의 저장 공간을 자유롭게 할 수 있다. 버스 컨트롤러(258)는 비휘발성 메모리에 의해 채용된 버스 프로토콜을 이용하여 비휘발성 메모리와 통신함으로써 요구된 판독, 기록 및 삭제 동작들을 실행한다. 일부 실시예들에서, 버스 컨트롤러(258)는 벤더-특정 비휘발성 메모리와 통신할 수 있는 "메모리 기술 드라이버(memory technology driver)"를 포함할 수 있다.

[0026] 버스 컨트롤러(258)가 비휘발성 메모리에 데이터를 기록하도록 하기 이전에, 비휘발성 메모리 인터페이스(250)는 암호화 모듈(230)이 데이터를 화이트닝할 수 있게 한다. 일부 실시예들에서, 트랜슬레이션 층(252)은 저장 이전에, 암호화 모듈(230)이 임의의 및 모든 타입들의 데이터 또는 메타데이터(예를 들면, 민감한 데이터, 비-민감한 데이터, 또는 메모리 관리 데이터)를 암호화할 수 있도록 함으로써, 결과적으로 화이트닝된 데이터가 프로그램/판독/삭제-교란들의 발생을 감소시키거나 최소화시킬 수 있다. 데이터를 화이트닝하기 위해, 트랜슬레이션 층(252)은 암호화 모듈(230)에게 어느 암호화 시드들(여기에서는, 키 및 초기화 벡터)을 제공해야 할 지를 결정할 수 있다. 암호화 시드들은 암호해제가 수행되는 경우에 복원될 수 있고 파일 시스템(222)에 의해 제공된 안전한 암호화 키들이 가용한 경우에 이용되도록 선택될 수 있고 또한 종종 그렇게 선택되어야 한다.

[0027] 트랜슬레이션 층(252)은 암호화 모듈(230)에 의한 이용을 위해 키를 선택하도록 멀티플렉서(254)를 제어할 수 있다. 일부 실시예들에서, 트랜슬레이션 층(252)는 암호화되고/화이트닝되는 데이터의 타입에 기초하여 개인 키 및 소정 화이트닝 키 사이에서 선택할 수 있다. 트랜슬레이션 층(252)은 민감한 데이터에 대한 판독 또는 기록 명령이 수신되었다는 것을 검출한 것에 응답하여, 파일 시스템(222)에 의해 제공될 수 있는 개인 키를 선택할 수 있다. 다른 타입들의 데이터(예를 들면, 비-민감한 데이터 또는 비-메타데이터)에 대해, 트랜슬레이션 층(252)은 유효한 개인 키가 제공되지 않으므로 소정 화이트닝 키를 선택할 수 있다. 화이트닝 키는 다양한 값들 중 임의의 하나를 취할 수 있고, 일부 실시예들에서 인터페이스(250)에 하드-코딩(hard-coded)되거나 하드-와이어링(hard-wired)될 수 있다. 화이트닝 키는 단지 보안을 위한 것 대신에 화이트닝에 적합한 값을 가질 수 있다. 예를 들면, 디바이스 시뮬레이션들 또는 수학적 모델들을 이용하여, 화이트닝 키의 값은 데이터의 다양한 가능한 값들에 대한 더 높은 수준의 화이트닝(다른 잠재적인 화이트닝 키들에 비교할 때)을 제공하도록 미리 결정될 수 있다. 그러므로, 일부 실시예들에서, 화이트닝 키의 값은 판독되거나 기록되는 데이터와 독립될 수 있다. 화이트닝 키의 값은 또한 로케이션-독립적일 수 있다(예를 들면, 데이터의 대응하는 논리적 또는 물리적 어드레스들에 독립적임).

[0028] 트랜슬레이션 층(252)은 암호화 모듈(230)에 의해 이용하기 위한 초기화 벡터를 선택하도록 멀티플렉서(256)

를 제어할 수 있다. 개인 키에서와 같이, 파일 시스템(222)은 민감한 정보에 대응하는 판독 또는 기록 명령과 함께 초기화 벡터를 제공할 수 있다. 이러한 초기화 벡터는 판독 또는 기록 명령으로 수신되는 논리적 어드레스에 기초할 수 있다. 파일 시스템(222)은 추가된 보안을 위해 논리적 어드레스에 기초하여 IV를 제공할 수 있다. 특히, 파일 시스템(222)이 복수의 논리적 어드레스들에서 동일한 데이터를 저장하는 기록 명령들을 발행하는 경우, 결과적으로 암호화된 데이터는 동일하지 않을 것이다.

[0029] 다른 타입들의 데이터(예를 들면, 비-민감한 데이터 또는 메타데이터)에 대해, 트랜슬레이션 층(252)은 논리적 또는 물리적 어드레스에 기초한 IV를 이용하는 사이에서 선택할 수 있다. 특히, 인터페이스(250)는 저장되거나 검색되는 정보의 물리적 어드레스 또는 논리적 어드레스에 기초하여 초기화 벡터를 계산할 수 있고, 트랜슬레이션 층(252)은 이들 벡터들 사이에서 선택하도록 멀티플렉서(256)를 제어할 수 있다. 상기 설명된 바와 같이, 어드레스(논리적 또는 물리적인지 여부에 관계없이)에 기초하여 초기화 벡터를 이용하는 것은 추가된 보안을 제공할 수 있다. 또한, 트랜슬레이션 층(252)은 유효한 논리적 및 물리적 어드레스들로 메타데이터를 유지할 수 있기 때문에, 논리적 또는 물리적 어드레스에 기초하여 데이터를 암호화하는 것은 나중의 암호해제를 위해 인터페이스(250)가 IV를 재구성할 수 있게 할 수 있다.

[0030] 트랜슬레이션 층(252)은 메타데이터가 논리적 어드레스와 연관되지 않으므로 메타데이터를 암호화하거나 암호해제하는데 물리적 어드레스에 기초하여 IV를 선택할 수 있다. 즉, 메타데이터는 파일 시스템(222)에 의해 제공되는 대신에 인터페이스(250)에 의해 생성될 수 있으므로, 유효한 IV가 논리적 어드레스로부터 생성될 수 없다. 일부 실시예들에서, 비휘발성 메모리에 저장되거나 저장되었던 임의의 정보에 대해, 트랜슬레이션 층(252)은 논리적 어드레스가 가용하지 않은 경우에(예를 들면, 메타데이터 또는 임의의 다른 적합한 정보) 물리적 어드레스에 기초하여 IV를 선택할 수 있다.

[0031] 트랜슬레이션 층(252)은 논리적 어드레스에 기초한 IV를 이용함으로써 비-민감한 데이터의 암호화 또는 암호해제를 가능하게 할 수 있다. 일부 실시예들에서, 비휘발성 메모리에 저장되거나 저장되었던 임의의 정보에 대해, 트랜슬레이션 층(252)은 예를 들면 비-민감한 또는 민감한 데이터에 대해, 가능한 경우에는 언제나 논리적 어드레스를 이용하여 정보의 암호화를 가능하게 할 수 있다. 이것은 특히 가비지 콜렉션 또는 웨어 레벨링 동안에 효율적인 메모리 관리를 가능하게 할 수 있다. 트랜슬레이션 층(252)은 프로그램 및 삭제 동작들이 비휘발성 메모리에 고르게 분산되는 것을 보장하고 삭제를 위해 블록들을 해제(free up)시키도록 웨어 레벨링 및 가비지 콜렉션을 수행할 수 있다. 웨어 레벨링 및 가비지 콜렉션은 하나의 물리적 어드레스로부터 새로운 물리적 어드레스로 페이지들을 이동시키는 것과 관련된다. 물리적 어드레스의 변경에 의해 영향을 받지 않는, 논리적 어드레스에 기초한 IV를 이용함으로써, 트랜슬레이션 층(252)은 데이터를 암호해제하거나 재암호화할 필요없이 민감한 및 비-민감한 데이터를 이동시킬 수 있다. 즉, 트랜슬레이션 층(252)은 메타데이터(물리적 어드레스에 기초하여 암호화됨)를 이동시키는 것에 대해 필요한 것과 같이, 이전 물리적 어드레스에 기초하여 저장된 데이터를 암호해제하고 새로운 물리적 어드레스를 이용하여 데이터를 재암호화할 필요는 없다. 비휘발성 메모리 상의 물리적 로케이션들 사이에서 데이터를 이동시키는 것은 도 5와 관련하여 아래에 더 상세하게 설명될 것이다.

[0032] 이제 도 3 - 5를 참조하면, 플래시 메모리와 같은 비휘발성 메모리 상의 저장을 위해 데이터를 화이트닝하기 위한 예시적 프로세스들의 플로우차트들이 도시되어 있다. 이들 프로세스들의 단계들은 도 2의 인터페이스(250)와 같은 메모리 인터페이스, 또는 전자 디바이스의 임의의 컴포넌트 또는 컴포넌트들의 조합에 의해 실행될 수 있다. 그러나, 제한이 아니라 명료성을 위해, 프로세스들은 메모리 인터페이스에 의해 수행되는 것으로 설명될 것이다.

[0033] 우선, 도 3을 참조하면, 기록 명령에 응답하여 비휘발성 메모리(예를 들면, NAND 플래시 메모리)에 저장을 위해 데이터를 화이트닝하기 위한 프로세스(300)의 플로우차트가 도시되어 있다. 프로세스(300)는 단계 302에서 시작될 수 있다. 단계 304에서, 메모리 인터페이스는 논리적 어드레스에 데이터를 기록하라는 명령을 수신할 수 있다. 일부 실시예들에서, 기록 명령은 파일 시스템(예를 들면, FAT 파일 시스템)으로부터 수신될 수 있고, 데이터는 온-칩 메모리(예를 들면, 도 1의 메모리(140))상에 저장될 수 있다. 데이터를 화이트닝할 때 어느 암호화 시드들을 이용할지를 결정하기 위해, 단계 306에서 메모리 인터페이스는 데이터가 민감한 정보인지 또는 비-민감한 정보인지 여부를 결정할 수 있다. 메모리 인터페이스는 유효한 암호화 시드들(예를 들면, 개인 키 및 IV)이 기록 명령의 일부로서 수신되었다면 데이터가 민감한 것으로 검출할 수 있다. 메모리 인터페이스는 데이터가 민감한 것으로 결정하는 경우, 메모리 인터페이스는 단계 308에서 수신된 개인 키 및 IV를 선택할 수 있다. 그렇지 않으면, 이들 암호화 시드들에 대한 값들이 파일 시스템에 의해 제공되지 않을 수 있고, 프로세스(300)는 대신에 단계 310으로 이동할 수 있다. 단계 310에서, 메모리 인터페이스는

소정 화이트닝 키를 선택할 수 있고, 단계 312에서, 데이터의 논리적 어드레스에 기초하여 초기화 벡터를 생성할 수 있다.

[0034] 단계 308 또는 312로부터, 프로세스(300)는 단계 314로 계속될 수 있다. 단계 314에서, 메모리 인터페이스는 선택된 키 및 선택되거나 생성된 초기화 벡터를 이용하여 데이터를 암호화할 수 있다. 이것은 선택되고/생성된 키 및 IV를 암호화 모듈에 제공하는 동안에, 도 2의 암호화 모듈(230)과 같은 암호화 모듈의 인에이블 신호를 어서팅하는(asserting) 것을 수반할 수 있다. 이와 같이, 민감한 데이터에 대해, 데이터는 파일 시스템에 의해 지정된 방식으로 안전하게 될 수 있고, 또한 화이트닝될 수 있다. 암호화될 필요가 없는 비-민감한 데이터는 프로그램 교란 또는 다른 판독/기록/삭제 문제들을 방지하기 위해 그럼에도 불구하고 화이트닝을 위해 설계된 키를 이용하여 암호화될 수 있다.

[0035] 단계 316으로 이동하여, 메모리 인터페이스는 비휘발성 메모리 상에 프로그래밍될 데이터에 대한 메타데이터를 계산할 수 있다. 예를 들면, 플래시 메모리에 대해, 메모리 인터페이스는 플래시 메모리의 논리적 어드레스(단계 304에서 수신됨)와 물리적 어드레스 사이의 매핑의 형태로 메타데이터를 생성할 수 있는 플래시 트랜슬레이션 층을 포함할 수 있다. 매핑 및 임의의 다른 적합한 메타데이터를 이용하는 경우, 메모리 인터페이스(예를 들면, 버스 컨트롤러를 통함)는 계산된 물리적 어드레스에서 암호화되고/화이트닝된 데이터를 비휘발성 메모리에 프로그래밍할 수 있다. 그러므로, 단계 306 내지 318(도 3에서 점선으로 윤곽지어져 있고 서브-프로세스(305)로 라벨링됨)은 파일 시스템에 의해 명령된 대로 데이터를 저장하기 위해 메모리 인터페이스에 의해 취해지는 단계들을 나타낼 수 있다.

[0036] 메모리 인터페이스는, 예를 들면 데이터를 판독하라는 후속 명령이 수신되는 경우에 저장된 데이터의 물리적 어드레스를 리콜(recall)할 수 있도록 단계 316에서 계산된 메타데이터를 유지할 필요가 있을 수 있다. 그러므로, 프로세스(300)는 메타데이터를 비휘발성 메모리에 저장하기 위한 후속 프로세스(319)의 단계들로 계속될 수 있다. 처음에, 단계 320에서, 메모리 인터페이스는 비-민감한 데이터에 대해 선택된(예를 들면, 단계 310에서) 화이트닝 키와 동일할 수도 그렇지 않을 수도 있는 화이트닝 키를 선택할 수 있다. 그리고나서, 단계 322에서, 메모리 인터페이스는 비휘발성 메모리의 물리적 어드레스에 기초하여 초기화 벡터를 생성할 수 있다. 이러한 단계는 메모리 인터페이스가 메타데이터를 비휘발성 메모리에 저장할 장소를 결정하고, 그리고나서 결정된 물리적 어드레스를 이용하여 초기화 벡터를 계산하는 단계와 관련된다. 일부 실시예들에서, 메모리 인터페이스는 나중 검색을 위해 메타 데이터가 저장된 장소를 나타내도록 비휘발성 메모리에 포인터를 유지하거나(예를 들면, 메모리 인터페이스 내부에 있는 메모리에), 메모리 인터페이스는 메타데이터 저장을 위해 각 블록 내의 특정 페이지들을 전담시킬 수 있다.

[0037] 단계 324에 계속되어, 메모리 모듈은 선택된 키 및 생성된 초기화 벡터를 이용하여 메타데이터를 암호화할 수 있다. 이러한 방식으로, 단계 326에서의 비휘발성 메모리로의 저장 이전에, 메타데이터는 또한 잠재적인 프로그램-교란 또는 다른 판독/기록/삭제 문제들을 회피하도록 암호화 모듈에 의해 화이트닝될 수 있다. 그리고나서, 프로세스(300)는 단계 328에서 종료할 수 있고, 화이트닝된 민감한 또는 비-민감한 데이터(파일 시스템에 의해 명령받음) 및 저장된 데이터와 연관된 화이트닝된 메모리 관리 데이터를 비휘발성 메모리에 저장했다.

[0038] 도 4는 메모리 인터페이스가 예를 들면 파일 시스템으로부터 수신된 판독 명령들을 처리하기 위해 실행할 수 있는 예시적 프로세스(400)의 플로우차트이다. 프로세스(400)는 프로세스(300)의 역 동작으로 보일 수 있다. 따라서, 도 3의 단계들의 상기 설명들이 단계 4의 대응하는 단계들에 적용될 수 있다는 것을 이해하고 있으므로, 도 4의 설명은 간단하게 이뤄질 것이다.

[0039] 프로세스(400)는 단계 402에서 시작할 수 있다. 그리고나서, 단계 404에서, 메모리 인터페이스는 논리적 어드레스로부터 데이터를 판독하라는 명령을 수신할 수 있다. 요청된 데이터가 저장되는 비휘발성 메모리의 물리적 어드레스를 식별하기 위해, 메모리 인터페이스는 서브-프로세스(405)의 단계들을 실행할 수 있다. 서브-프로세스(405)는 저장된 메타데이터를 획득하고 처리하기 위한 단계들을 포함할 수 있다. 특히, 메모리 인터페이스는 단계 406에서 비휘발성 메모리의 특정 물리적 로케이션으로부터 저장된 메타데이터를 판독하고, 단계 408에서 화이트닝 키를 선택하며, 단계 410에서 특정 물리적 로케이션에 기초하여 초기화 벡터를 생성하고, 화이트닝 키 및 생성된 초기화 벡터를 이용하여 메타데이터를 암호해제할 수 있다. 그리고나서, 메타데이터를 암호해제한 경우, 메모리 인터페이스는 단계 412에서 메타데이터를 해석하여 판독 명령에 의해 요청되는 데이터의 물리적 어드레스를 결정한다.

[0040] 프로세스(400)는 요청된 데이터를 판독하고, 처리하며, 이를 파일 시스템에 제공하는 단계들을 포함하는 서브

-프로세스(413)로 계속될 수 있다. 단계 414로 시작하여, 메모리 인터페이스는 메타데이터로부터 이전에 결정된 물리적 어드레스로부터 저장된 데이터를 판독할 수 있다. 그리고나서, 메모리 인터페이스는 단계 418에서 (민감한 데이터에 대해) 파일 시스템으로부터 수신된 개인 키 및 IV를 선택하거나, 단계 420 및 422에서 (비-민감한 데이터에 대해) 논리적 어드레스에 기초하여 화이트닝 키를 선택하고 IV를 생성할 수 있다. 단계 418 또는 422에 이어서, 메모리 인터페이스는 선택되고/생성된 키 및 초기화 벡터를 이용하여 민감한 또는 비-민감한 데이터를 암호해제할 수 있다. 이것은 파일 시스템에 의해 요청되는 원래의 미-화이트닝된(un-whitened) 데이터를 생성할 수 있고, 메모리 인터페이스는 단계 426에서 이러한 데이터를 파일 시스템에게 제공할 수 있다. 프로세스(400)는 단계 428에서 종료할 수 있다.

[0041] 이제, 도 5를 참조하면, 메모리 인터페이스에 의해 비휘발성 메모리(예를 들면, 플래시 메모리)의 물리적 페이지들 및/또는 블록들 사이에서 데이터를 이동하도록 실행될 수 있는 예시적 프로세스(500)의 플로우차트가 도시되어 있다. 데이터는 다양한 상이한 이유들로 인해 하나의 물리적 로케이션으로부터 다른 하나로 이동될 수 있다. 예를 들면, 메모리 인터페이스는 비휘발성 메모리 상의 삭제들 및 재기록들의 분포를 고르게 하기 위해 웨어 레벨링을 수행하는 경우에 데이터 또는 메타데이터를 이동시킬 수 있다. 다르게는, 메모리 인터페이스는 메모리 셀들의 블록으로부터 데이터 또는 메타데이터를 이동시켜, 삭제를 위해 블록을 해제시키거나 그 신뢰성이 실질적으로 감소하는 경우에 블록의 이용을 중지시킬 수 있다. 메모리 인터페이스(그리고, 특히 트랜슬레이션 층)는 다양한 상이한 이유들로 인해 페이지 재매핑을 개시할 수 있으므로, 프로세스(500)의 단계들은 수행되는 특정 관리 동작들에 대한 것이 아니라, 이동되는 경우에 데이터가 암호화/암호해제되는(또는 되지 않는) 방식에 주로 초점을 맞추고 있다. 이것은 단지 도면을 과도하게 복잡하도록 하는 것을 방지하기 위한 것이고 프로세스(500)의 일반적인 특징들은 비휘발성 메모리의 상이한 물리적 어드레스들 사이에서 데이터를 이동시키는 것과 관련된 임의의 메모리 관리 동작들에 포함되거나 이들에 적응될 수 있다는 것은 자명하다.

[0042] 프로세스(500)는 단계 502에서 시작할 수 있다. 그리고나서, 단계 504에서, 메모리 인터페이스는 비휘발성 메모리의 물리적 어드레스로부터 하나의 페이지를 판독할 수 있다. 단계 506에서, 메모리 인터페이스는 페이지가 어떤 타입의 데이터를 포함하는 지를 결정할 수 있다. 예를 들면, 메모리 인터페이스는 페이지가 하나의 블록 내에서 로케이팅된 장소에 기초하여 또는 임의의 다른 적합한 접근법을 이용하여 페이지가 데이터(예를 들면, 민감한 또는 비-민감한 데이터) 또는 메타데이터를 포함하고 있는지 여부를 결정할 수 있다. 페이지가 데이터를 포함하는 경우, 메모리 인터페이스는 단계 508에서 데이터를 새로운 물리적 어드레스에 저장할 수 있다. 메모리 인터페이스는 데이터를 암호해제하고 재암호화하는데 암호화모듈을 이용할 필요없이 새로운 물리적 페이지 어드레스에 데이터를 저장할 수 있다. 즉, 메모리 인터페이스는 데이터를 이동시키는 동안에 암호화 모듈을 디스에이블시키거나 바이패싱할 수 있다. 이것은 데이터가, 민감한 지 여부에 관계없이, 데이터의 물리적 어드레스와 독립되어 암호화 시드들을 이용하여 원래 암호화되었기 때문이다. 그러므로, 데이터의 물리적 어드레스의 변경들은 데이터가 암호화되고/화이트닝되어야 하는 방법에 영향을 미치지 않을 수 있다.

[0043] 단계 508에 이어서, 메모리 인터페이스는 단계 510에서 저장된 데이터에 대응하는 메타데이터를 업데이트할 수 있다. 이것은 메모리 인터페이스가 데이터(변경되지 않고 유지됨)의 논리적 어드레스와 데이터가 실제로 기록된 장소 사이의 적절한 매핑을 유지할 수 있게 허용한다. 단계 510은 메타데이터 자신이 비휘발성 메모리에 저장될 수 있으므로, 데이터에 대응하는 메타데이터를 판독하고, 업데이트하며 기록하는 것을 포함할 수 있다. 이들 단계들은 도면을 과도하게 복잡하게 하는 것을 방지하기 위해 도 5에 도시되어 있지 않고, 도 3 및 4와 관련하여 상기 설명된 메타데이터를 기록하고 판독하는 것들과 유사한 단계들을 포함할 수 있다.

[0044] 단계 506으로 돌아가면, 메모리 인터페이스가 단계 504에서 판독된 페이지가 메타데이터를 포함하는 것으로 판정하는 경우, 프로세스(500)는 단계 512로 진행할 수 있다. 민감한 또는 비-민감한 데이터에서와는 달리, 메타데이터는 하나의 물리적 로케이션에서 다른 하나로 이동되는 경우에 암호해제되고 재암호화될 필요가 있다. 상기 설명된 바와 같이, 이것은 메타데이터의 암호해제는 메타데이터가 저장된 물리적 어드레스(논리적 어드레스는 아님)를 이용하는 것을 수반하고, 따라서 물리적 어드레스의 변경들은 메타데이터의 관리를 최신으로 유지하기 위해 암호화의 변경들을 필요로 할 수 있기 때문이다. 그러므로, 단계 512에서, 메모리 인터페이스는 메타데이터가 저장되었던 물리적 어드레스에 기초하여 초기화 벡터를 생성할 수 있다. 그리고나서, 단계 514에서, 메타데이터가 생성된 초기화 벡터 및 화이트닝 키를 이용하여 암호해제될 수 있다. 그리고나서, 단계 516에서, 메모리 인터페이스는 메타데이터가 저장될 새로운 물리적 어드레스에 기초하여 새로운 초기화 벡터를 생성할 수 있고, 단계 518에서, 새로운 초기화 벡터 및 화이트닝 키를 이용하여 메타데이터를 재암호화할 수 있다. 그리고나서, 재암호화된 메타데이터는 단계 520에서 새로운 물리적 어드레스에 저장될 수

있다.

[0045] 단계 510 또는 단계 520에 이어서, 프로세스(500)는 단계 522로 계속될 수 있다. 단계 522에서, 메모리 인터페이스는 추가 페이지들을 이동시킬 지 여부를 결정할 수 있다. 그렇다면, 프로세스(500)는 단계 504로 리턴할 수 있고, 메모리 인터페이스는 다른 하나의 물리적 어드레스로부터 데이터를 판독할 수 있다. 그렇지 않으면, 프로세스(500)는 단계 524로 이동하여 종료할 수 있다.

[0046] 도 3 - 5의 프로세스들이 단지 예시적이라는 것은 자명하다. 본 발명의 범주에서 벗어나지 않고서 임의의 단계들이 추가, 변형, 조합 또는 재배열될 수 있고, 임의의 추가적인 단계들이 추가될 수 있다. 예를 들면, 암호화 모듈이 키 및 IV와는 다른 암호화 시드들을 이용하는 경우, 상이한 암호화 시드들을 생성하도록 도 3-5의 단계들을 변형시킬 수 있고, 여기에서 메타데이터에 대한 암호화 시드들은 물리적 어드레스들에 기초할 수 있으며 민감한 및 비-민감한 데이터에 대한 시드들은 논리적 어드레스들에 기초할 수 있다.

[0047] 또한, 비휘발성 메모리에 정보를 저장하기 위한 본 개시의 다양한 실시예들은 민감한 데이터, 비-민감한 데이터 및 메모리 관리 데이터(또는 "메타데이터")를 저장하는데 초점을 맞추었다. 이것은 단지 예시에 불과하고 본 개시의 특징들은 저장된 정보가 이들 3가지 카테고리들에 들지 않는 디바이스 구현들에 이용될 수 있다는 것은 자명하다. 특히, 다른 디바이스 구현들에 대해, 디바이스는 가능한 경우에는 언제나 논리적 어드레스에 기초하여 암호화 시드들을 이용할 수 있고(데이터를 이동시키는 것이 더 효율적이다), 어떠한 논리적 어드레스도 제공되지 않은 경우에 디바이스는 물리적 어드레스를 이용할 수 있다. 어드레스에 기초하지 않은 암호화 시드들에 대해, 디바이스는 개인 키가 제공되지 않는 경우에 화이트닝 키 또는 다른 소정키를 이용할 수 있고, 여기에서 화이트닝 키는 높은 수준의 화이트닝을 제공함에 있어서 그 성능을 위해 선택될 수 있다.

[0048] 본 발명의 기재된 실시예들은 제한을 위해서가 아니라 예시의 목적으로 제공되고, 본 발명은 이하의 청구항들에 의해서만 제한된다.

부호의 설명

[0049] 100: 전자 디바이스

110: 시스템-온-칩

140: 메모리

130: 암호화 모듈

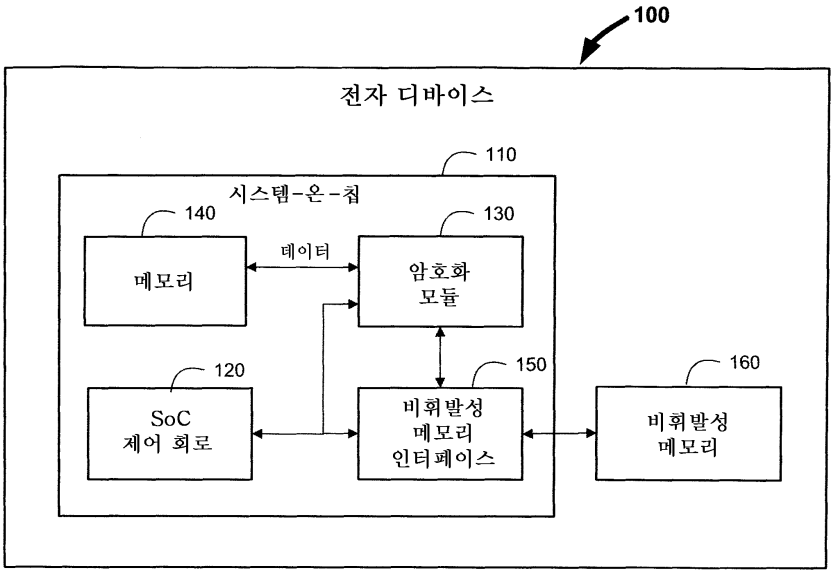
120: SoC 제어 회로

150: 비휘발성 메모리 인터페이스

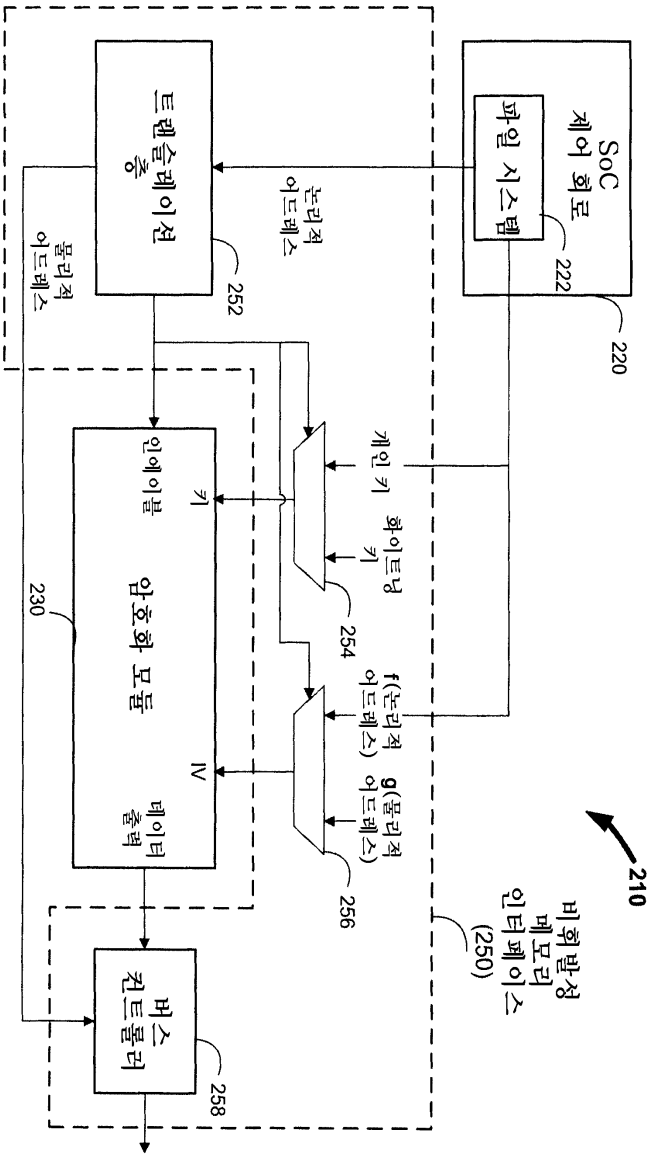
160: 비휘발성 메모리

도면

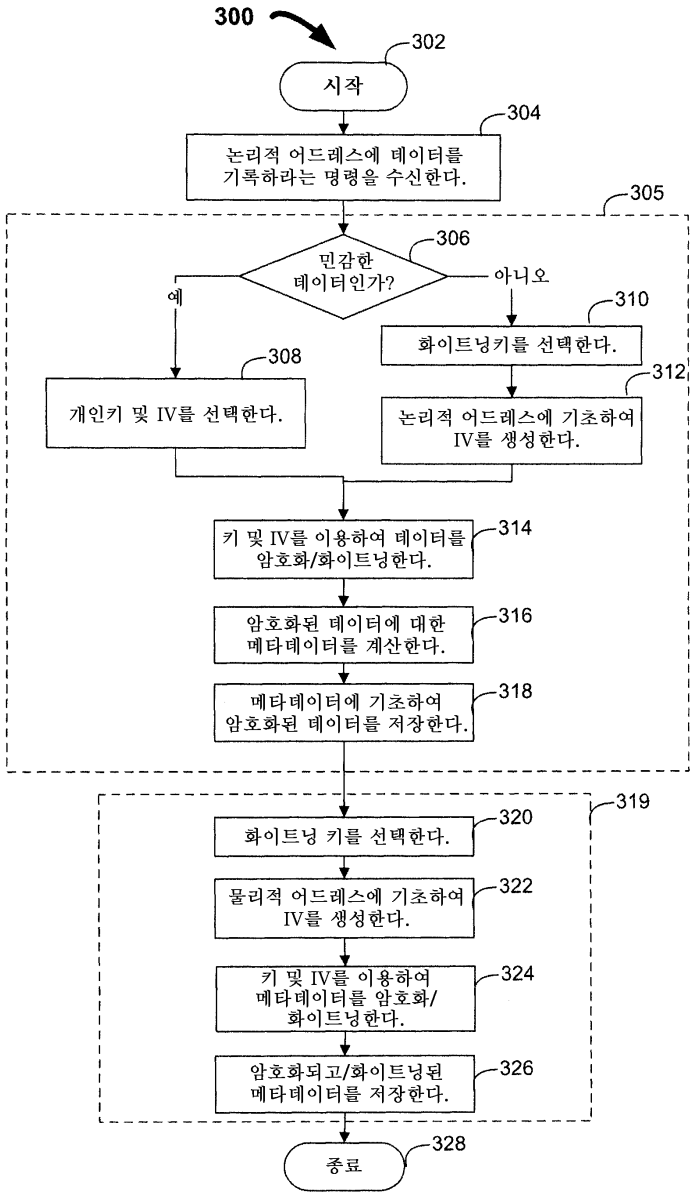
도면1


100
전자 디바이스
110
시스템-온-칩
140
메모리
데이터
130
암호화
모듈
120
SoC
제어 회로
150
비휘발성
메모리
인터페이스
160
비휘발성
메모리

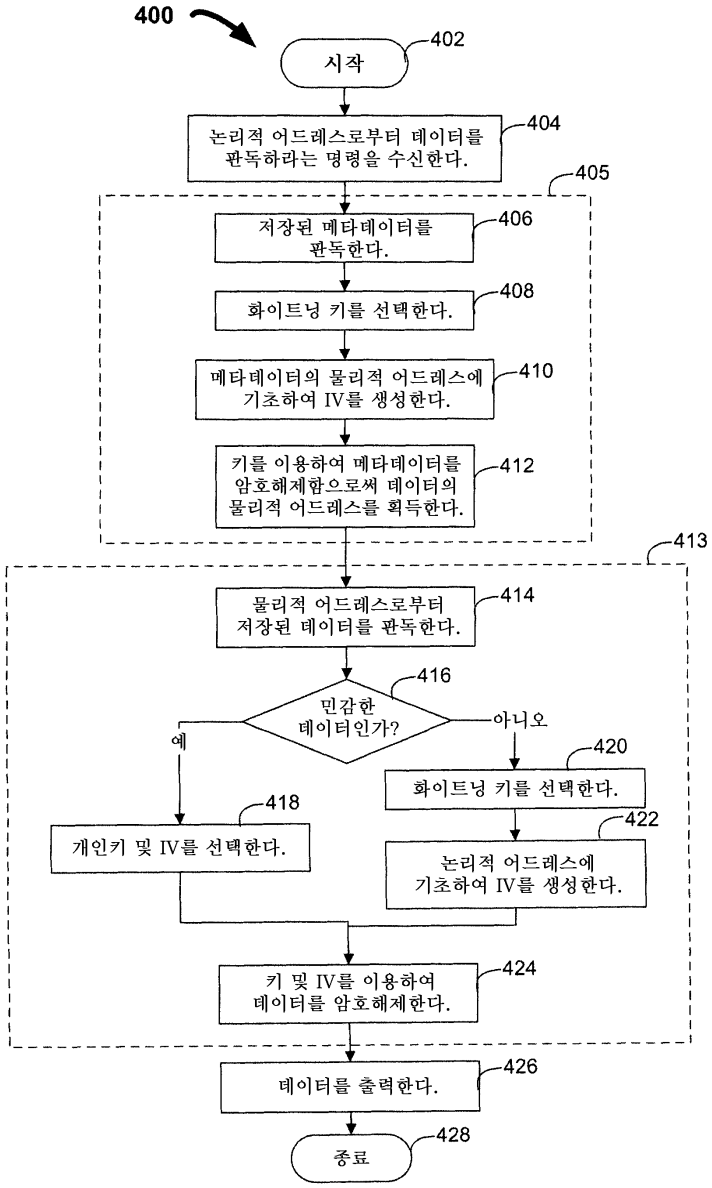
도면2


SoC
제어 회로
파일 시스템
222
220
트랜슬레이션
층
252
논리적
어드레스
물리적
어드레스
개인 키
화이트닝
키
254
f(논리적
어드레스)
g(물리적
어드레스)
256
인에이블
키
암호화 모듈
IV
데이터
출력
230
버스
컨트롤러
258
비휘발성
메모리
인터페이스
(250)
210

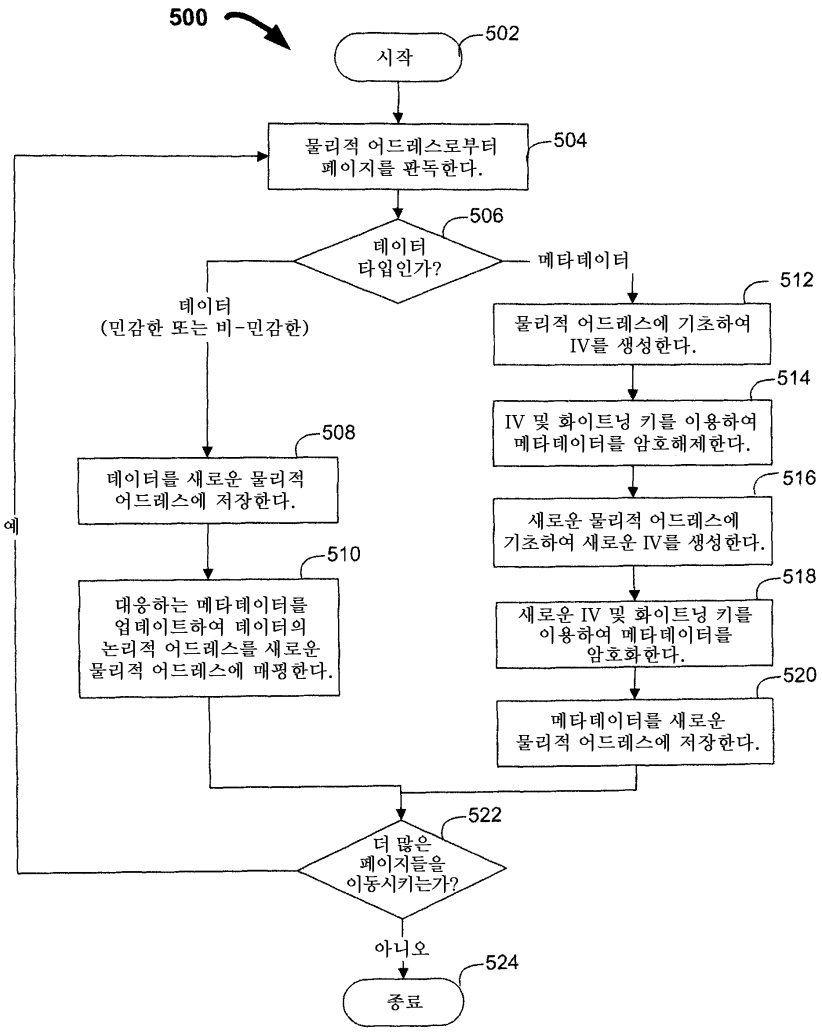
도면3


300
302
시작
304
논리적 어드레스에 데이터를 기록하라는 명령을 수신한다.
305
306
민감한 데이터인가?
예
아니오
308
개인키 및 IV를 선택한다.
310
화이트닝키를 선택한다.
312
논리적 어드레스에 기초하여 IV를 생성한다.
314
키 및 IV를 이용하여 데이터를 암호화/화이트닝한다.
316
암호화된 데이터에 대한 메타데이터를 계산한다.
318
메타데이터에 기초하여 암호화된 데이터를 저장한다.
319
320
화이트닝 키를 선택한다.
322
물리적 어드레스에 기초하여 IV를 생성한다.
324
키 및 IV를 이용하여 메타데이터를 암호화/화이트닝한다.
326
암호화되고/화이트닝된 메타데이터를 저장한다.
328
종료

도면4


400
시작
402
논리적 어드레스로부터 데이터를 판독하라는 명령을 수신한다.
404
405
저장된 메타데이터를 판독한다.
406
화이트닝 키를 선택한다.
408
메타데이터의 물리적 어드레스에 기초하여 IV를 생성한다.
410
키를 이용하여 메타데이터를 암호해제함으로써 데이터의 물리적 어드레스를 획득한다.
412
413
물리적 어드레스로부터 저장된 데이터를 판독한다.
414
민감한 데이터인가?
416
예
아니오
개인키 및 IV를 선택한다.
418
화이트닝 키를 선택한다.
420
논리적 어드레스에 기초하여 IV를 생성한다.
422
키 및 IV를 이용하여 데이터를 암호해제한다.
424
데이터를 출력한다.
426
종료
428

도면5


500
시작
502
물리적 어드레스로부터 페이지를 판독한다.
504
데이터 타입인가?
506
메타데이터
데이터 (민감한 또는 비-민감한)
512
물리적 어드레스에 기초하여 IV를 생성한다.
514
IV 및 화이트닝 키를 이용하여 메타데이터를 암호해제한다.
516
새로운 물리적 어드레스에 기초하여 새로운 IV를 생성한다.
518
새로운 IV 및 화이트닝 키를 이용하여 메타데이터를 암호화한다.
520
메타데이터를 새로운 물리적 어드레스에 저장한다.
508
데이터를 새로운 물리적 어드레스에 저장한다.
510
대응하는 메타데이터를 업데이트하여 데이터의 논리적 어드레스를 새로운 물리적 어드레스에 매핑한다.
예
522
더 많은 페이지들을 이동시키는가?
아니오
524
종료