(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년03월19일
(11) 등록번호 10-1959738
(24) 등록일자 2019년03월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 21/30* (2013.01)
(21) 출원번호 10-2012-0055527
(22) 출원일자 2012년05월24일
심사청구일자 2017년04월25일
(65) 공개번호 10-2013-0140968
(43) 공개일자 2013년12월26일
(56) 선행기술조사문헌
JP2004201038 A
(뒷면에 계속)

(73) 특허권자
삼성전자 주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
왕, 웨이싱
경기 수원시 영통구 영통1동 수원우편집중국 120
조희창
서울 서초구 강남대로16길 33, 201호 (양재동, 강남파크빌)
(뒷면에 계속)
(74) 대리인
특허법인가산

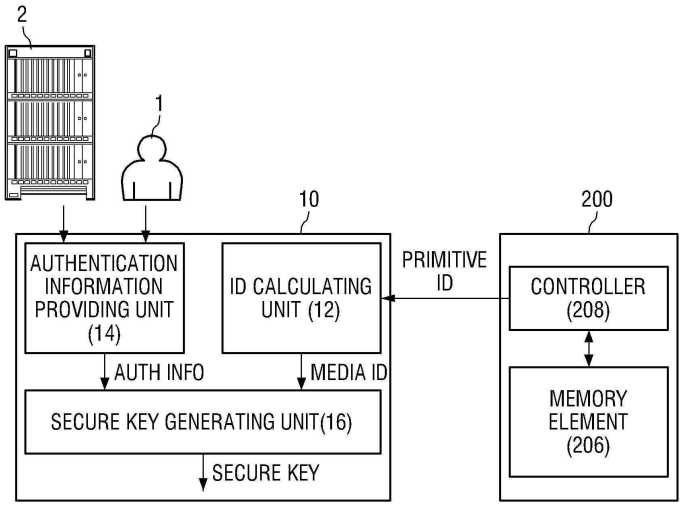
전체 청구항 수 : 총 17 항 심사관 : 남기영

(54) 발명의 명칭 **장치 식별자와 사용자 인증 정보에 기반한 보안 키 생성 장치**

(57) 요 약

장치 식별자와 사용자 암호를 모두 사용하여 보안 키를 생성함으로써, 특정 장치 및 특정 사용자에 동시에 결부되는 보안 키를 생성하는 장치 및 방법이 제공 된다. 본 발명에 따른 보안 키 생성 장치는 저장 장치에 저장 된 원시 ID를 제공 받아 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하는 ID 연산부, 사용자를 인증하기 위한 인증 정보를 보안 키 생성부에 제공하는 인증 정보 제공부; 및 상기 미디어 ID 및 상기 인증 정보를 모두 이용하여 보안 키를 생성하는 보안 키 생성부를 포함한다.

대 표 도 - 도1



(72) 발명자

이원석

경기 수원시 영통구 봉영로 1526, 715동 1302호 (영통동, 살구골7단지아파트)

김민욱

서울 관악구 솔밭로7길 16, 301동 404호 (봉천동, 낙성대현대홈타운)

장형석

경기 수원시 영통구 영통로290번길 25, 514동 303호 (영통동, 신나무실5단지아파트)

(56) 선행기술조사문헌

JP2005174388 A*

KR1020110102165 A*

US20040210707 A1*

US20050235143 A1*

*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

저장 장치에 저장된 원시 ID를 제공받아, 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하는 ID 연산부;

사용자를 인증하기 위한 인증 정보를 보안 키 생성부에 제공하는 인증 정보 제공부; 및

상기 미디어 ID 및 상기 인증 정보를 모두 이용하여 보안 키를 생성하는 보안 키 생성부를 포함하되,

상기 원시 ID는 상기 저장 장치에 구비된 메모리 소자의 고유 식별자인 메모리 ID가 암호화된 암호화 메모리 ID 및 상기 저장 장치에 구비된 컨트롤러의 고유 식별자인 컨트롤러 ID를 포함하고,

상기 ID 연산부는 상기 암호화 메모리 ID를 상기 메모리 ID로 복호화하고, 상기 메모리 ID로부터 메모리 파생 ID를 연산하며, 상기 컨트롤러 ID 및 상기 메모리 파생 ID를 모두 이용하여 상기 미디어 ID를 연산하는 보안 키 생성 장치.

청구항 2

제 1항에 있어서,

상기 원시 ID는 상기 미디어 ID 연산에 이용 되는 하나 이상의 식별용 데이터로, 상기 미디어 ID와는 다른 데이터인 보안 키 생성 장치.

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 ID 연산부는 상기 메모리 소자의 인증 프로세스를 수행하며, 상기 인증 프로세스의 수행 결과 메모리 소자의 인증을 성공한 경우에 한하여 상기 메모리 ID로부터 상기 메모리 파생 ID를 연산하는 보안 키 생성 장치.

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 ID 연산부는 상기 컨트롤러와 상호인증을 수행하며, 상기 상호인증 과정에서 상기 컨트롤러 ID를 제공받는 보안 키 생성 장치.

청구항 7

삭제

청구항 8

제 1항에 있어서,

상기 인증 정보 제공부는 상기 사용자로부터 상기 인증 정보를 입력 받는 보안 키 생성 장치.

청구항 9

저장 장치에 저장된 원시 ID를 제공받아, 프로세서에 제공하는 저장 장치 인터페이스; 및

상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하고, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성하는 프로세서를 포함하되,

상기 원시 ID는 상기 저장 장치에 구비된 메모리 소자의 고유 식별자인 메모리 ID가 암호화된 암호화 메모리 ID 및 상기 저장 장치에 구비된 컨트롤러의 고유 식별자인 컨트롤러 ID를 포함하고,

상기 프로세서는 상기 암호화 메모리 ID를 상기 메모리 ID로 복호화하고, 상기 메모리 ID로부터 메모리 파생 ID를 연산하며, 상기 컨트롤러 ID 및 상기 메모리 파생 ID를 모두 이용하여 상기 미디어 ID를 연산하는 보안 키 생성 장치.

청구항 10

제9 항에 있어서,

상기 프로세서는 일반 실행 모드 및 보안 실행 모드 중 하나로 동작하는 것이고,

상기 인증 정보는 상기 프로세서가 일반 실행 모드에서 보안 실행 모드로 동작 상태를 전환하기 위한 모드 전환 인증에 사용 되는 보안 키 생성 장치.

청구항 11

제 10항에 있어서,

상기 프로세서는 상기 일반 실행 모드에서의 명령어 실행을 담당하는 일반 가상 코어 및 상기 보안 실행 모드에서의 명령어 실행을 담당하는 보안 가상 코어를 포함하고,

상기 일반 가상 코어는 상기 인증 정보를 검증하여, 상기 검증의 성공 시 인터럽트 신호를 생성하고,

상기 프로세서는 상기 인터럽트 신호에 응답하여 동작 모드를 일반 실행 모드에서 보안 실행 모드로 전환하며,

상기 보안 가상 코어는 상기 보안 키를 생성하는 보안 키 생성 장치.

청구항 12

제 11항에 있어서,

상기 보안 키 생성 장치는 RAM을 더 포함하고,

상기 RAM은 상기 일반 가상 코어에서 실행되는 명령어에 의하여 접근될 수 있는 제1 영역 및 상기 보안 가상 코어에서 실행되는 명령어에 의하여 접근될 수 있는 상기 제1 영역과 겹치지 않는 제2 영역을 포함하며,

상기 일반 가상 코어에서 실행되는 명령어는 상기 제2 영역에 접근할 수 없는 보안 키 생성 장치.

청구항 13

제 9항에 있어서,

상기 인증 정보를 입력 받아 상기 프로세서에 제공 하는 입력부를 더 포함하고,

상기 프로세서는 일반 실행 모드 및 보안 실행 모드 중 하나로 동작하는 것이고, 상기 보안 실행 모드에서 상기 인증 정보를 상기 입력부로부터 제공 받는 것과 상기 보안 키를 생성하는 것을 실행하는 보안 키 생성 장치.

청구항 14

제 13항에 있어서,

상기 보안 키 생성 장치는 RAM을 더 포함하고,

상기 RAM은 상기 프로세서가 보안 실행 모드로 동작할 때에만 접근 가능한 보안 영역을 포함하고, 상기 인증 정보, 원시 ID, 미디어 ID 및 보안 키는 상기 보안 영역에 저장되는 보안 키 생성 장치.

청구항 15

저장 장치와 연결되어 원시 ID를 상기 저장 장치로부터 제공받아 시스템 온 칩에 제공하는 저장 장치 인터페이스; 및

상기 저장 장치 인터페이스와 연결된 시스템 온 칩(System-on-Chip; SoC)을 포함하되,

상기 시스템 온 칩은,

상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하며, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성하는 보조 로직(peripheral logic)을 포함하되,

상기 원시 ID는 상기 저장 장치에 구비된 메모리 소자의 고유 식별자인 메모리 ID가 암호화된 암호화 메모리 ID 및 상기 저장 장치에 구비된 컨트롤러의 고유 식별자인 컨트롤러 ID를 포함하고,

상기 보조 로직은 상기 암호화 메모리 ID를 상기 메모리 ID로 복호화하고, 상기 메모리 ID로부터 메모리 파생 ID를 연산하며, 상기 컨트롤러 ID 및 상기 메모리 파생 ID를 모두 이용하여 상기 미디어 ID를 연산하는 호스트 장치.

청구항 16

제15 항에 있어서,

상기 시스템 온 칩은,

상기 인증 정보를 제공 받아 상기 보조 로직에 제공 하는 코어(Core)를 더 포함하는 호스트 장치.

청구항 17

삭제

청구항 18

15 항에 있어서,

상기 시스템 온 칩에 의하여 제어 되고, 사용자로부터 상기 인증 정보를 입력 받아 상기 시스템 온 칩에 제공하는 입력부를 더 포함하는 호스트 장치.

청구항 19

제15 항에 있어서,

상기 시스템 온 칩은 상기 보안 키를 저장하는 레지스터를 더 포함하는 호스트 장치.

청구항 20

제15 항에 있어서,

상기 보조 로직은 상기 보안 키를 이용하여 컨텐츠를 암호화 한 후 상기 저장 장치 인터페이스를 통하여 상기 저장 장치에 제공하는 호스트 장치.

청구항 21

제15 항에 있어서,

상기 저장 장치 인터페이스는 상기 저장 장치로부터 암호화 컨텐츠를 제공받아 상기 시스템 온 칩에 제공하고,

상기 보조 로직은 상기 보안 키를 생성하여 상기 암호화 컨텐츠를 복호화하는 호스트 장치.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 키 생성 장치에 관한 것이다. 보다 자세하게는 장치 식별자와 사용자 암호 등 사용자 인증 정보를 모두 사용하여 보안 키를 생성함으로써, 특정 장치 및 특정 사용자에 동시에 종속 되는 보안 키를 생성하는 장치, 상기 보안 키를 활용하는 저장 장치 및 보안 키 생성 방법에 관한 것이다.

배 경 기 술

[0002] 최근 여러 형태의 이동식 저장 장치가 소개 되고 있다. 최근 소개 되는 이동식 저장 장치는 저장 용량이 늘어나면서도, 차지하는 부피는 점점 줄어들고 있으며, 이동식 저장 장치의 인터페이스는 호스트 장치로의 착탈이 가능한 방식으로 구현 되어 있다. 이에 따라, 이동식 저장 장치의 이동성이 점점 더 강화되고 있다. 예를 들어, 플래시 메모리를 저장 수단으로 사용한 메모리 카드 또는 USB(Universal Serial Bus) 포트에 연결 가능한 USB 메모리가 소개 되고 있고, 최근 SSD(Solid State Drive)도 소개되어 점점 널리 사용 되고 있다. 또한, 저렴한 저장 장치 중 하나로 평가 받고 있는 하드디스크 역시 외장형 하드 디스크가 등장하여, 기존의 PC에 고정 된 하드디스크와는 달리 이동성을 제공한다.

[0003] 상기 이동식 저장 장치뿐만 아니라, 상기 이동식 저장 장치에 연결될 수 있는 호스트 장치 역시 소형화 되었다. 이와 같이, 언제 어디서나 이동식 저장 장치에 저장 된 디지털 컨텐츠를 이동식 호스트 장치를 통해 즐길 수 있는 환경이 조성되었고, 컨텐츠의 유통 방식은 디지털 데이터의 형태로 유통 되는 것으로 변화하고 있다. 이에 따라, 디지털 컨텐츠의 불법 복제를 방지하는 기술이 점점 더 중요해지고 있다.

[0004] 디지털 컨텐츠의 불법 복제를 방지하기 위하여, 상기 디지털 컨텐츠는 원본 그대로가 아닌 암호화 된 상태로 이동식 저장 장치에 저장 되는 것이 바람직하다. 상기 암호화는 특정 암호화 키를 사용하여 수행 된다.

[0005] 한편, 특정 장치에 대하여만 결부 되는 보안 키를 이용한 암호화 및 복호화 기술은, 상기 특정 장치를 사용하기만 하면 데이터에 대한 보안이 해제 된다. 그런데, 예를 들어 사생활을 보호 받기 위하여 특정인 만이 재생이 가능하도록 컨텐츠를 암호화 하고자 하는 경우가 존재할 수 있다. 따라서, 특정 장치에 대하여 종속 될 뿐만 아니라, 특정 사용자에게도 종속 되는 보안 키 생성 기술 및 그 활용 기술의 제공이 필요하다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 기술적 과제는 특정 장치 및 특정 사용자에 동시에 종속 되는 보안 키를 생성하는 장치, 상기 보안 키를 활용하여 컨텐츠를 자체 암호화 저장 하는 저장 장치 및 보안 키 생성 방법을 제공하는 것이다.

[0007] 본 발명이 해결하고자 하는 다른 기술적 과제는 특정 장치의 식별자 및 사용자에 의해 입력 된 사용자 인증 정보를 모두 이용하여 연산 된 보안 키를 생성하는 장치, 상기 보안 키를 활용하여 컨텐츠를 자체 암호화 저장 하는 저장 장치 및 보안 키 생성 방법을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 또 다른 기술적 과제는 신뢰 컴퓨팅(Trusted Computing)을 지원하는 호스트 장치에서 상기 보안 키를 안전하게 생성하는 장치를 제공하는 것이다.

[0009] 본 발명이 해결하고자 하는 또 다른 기술적 과제는 보안 키를 생성함에 있어서 장치 식별자 및 사용자 인증 정

보 및 생성 된 보안 키가 유출 되지 않도록 신뢰 된 실행 환경에서 보안 키를 생성하는 호스트 장치를 제공하는 것이다.

[0010] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해 될 수 있을 것이다.

과제의 해결 수단

[0011] 상기 기술적 과제를 달성하기 위한 본 발명의 일 실시예에 따른 보안 키 생성 장치는 저장 장치에 저장 된 원시 ID를 제공 받아, 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하는 ID 연산부; 사용자를 인증하기 위한 인증 정보를 보안 키 생성부에 제공하는 인증 정보 제공부; 및 상기 미디어 ID 및 상기 인증 정보를 모두 이용하여 보안 키를 생성하는 보안 키 생성부를 포함한다. 상기 원시 ID는 상기 미디어 ID 연산에 이용 되는 하나 이상의 식별용 데이터로, 상기 미디어 ID와는 다른 데이터이다. 상기 인증 정보 정보 제공부는 상기 사용자로부터 상기 인증 정보를 입력 받을 수 있다.

[0012] 일부 실시예에 따르면 상기 원시 ID는 상기 저장 장치에 구비 된 메모리 소자의 고유 식별자인 메모리 ID가 암호화 된 암호화 메모리 ID이고, 상기 ID 연산부는 상기 암호화 메모리 ID를 상기 메모리 ID로 복호화 하고, 상기 메모리 ID로부터 메모리 파생 ID를 연산하며, 상기 메모리 파생 ID를 상기 미디어 ID로 사용할 수 있다. 또한, 상기 ID 연산부는 상기 메모리 소자의 인증 프로세스를 수행하며, 상기 인증 프로세스의 수행 결과 메모리 소자의 인증을 성공한 경우에 한하여 상기 메모리 ID로부터 상기 메모리 파생 ID를 연산할 수 있다.

[0013] 일부 실시예에 따르면 상기 원시 ID는 상기 저장 장치에 구비 된 메모리 소자의 고유 식별자인 메모리 ID일 수도 있다. 또한, 상기 미디어 ID는 상기 메모리 ID와 동일할 수 있다. 따라서, 본 실시예에 따르면 ID 연산부는 상기 저장 장치로부터 상기 메모리 ID를 제공 받아, 상기 메모리 ID를 상기 미디어 ID로써 상기 보안 키 생성부에 제공할 수 있다.

[0014] 일부 실시예에 따르면 상기 원시 ID는 상기 저장 장치에 구비 된 컨트롤러의 고유 식별자인 컨트롤러 ID를 포함하고, 상기 ID 연산부는 상기 컨트롤러 ID를 이용하여 상기 미디어 ID를 연산할 수도 있다. 상기 ID 연산부는 상기 컨트롤러와 상호인증을 수행하며, 상기 상호인증 과정에서 상기 컨트롤러 ID를 제공 받을 수 있다.

[0015] 일부 실시예에 따르면, 상기 원시 ID는 상기 저장 장치에 구비 된 메모리 소자의 고유 식별자인 메모리 ID가 암호화 된 암호화 메모리 ID 및 상기 저장 장치에 구비 된 컨트롤러의 고유 식별자인 컨트롤러 ID를 포함하고, 상기 ID 연산부는 상기 암호화 메모리 ID를 상기 메모리 ID로 복호화 하고, 상기 메모리 ID로부터 메모리 파생 ID를 연산하며, 상기 컨트롤러 ID 및 상기메모리 파생 ID를 모두 이용하여 상기 미디어 ID를 연산할 수도 있다.

[0016] 상기 기술적 과제를 달성하기 위한 본 발명의 다른 실시예에 따른 보안 키 생성 장치는 저장 장치에 저장 된 원시 ID를 제공 받아, 프로세서에 제공 하는 저장 장치 인터페이스; 및 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하고, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성하는 프로세서를 포함한다.

[0017] 일부 실시예에 따르면, 상기 프로세서는 일반 실행 모드 및 보안 실행 모드 중 하나로 동작하는 것이고, 상기 인증 정보는 상기 프로세서가 일반 실행 모드에서 보안 실행 모드로 동작 상태를 전환하기 위한 모드 전환 인증에 사용 될 수 있다. 상기 프로세서는 상기 일반 실행 모드에서의 명령어 실행을 담당하는 일반 가상 코어 및 상기 보안 실행 모드에서의 명령어 실행을 담당하는 보안 가상 코어를 포함하고, 상기 일반 가상 코어는 상기 인증 정보를 검증하여, 상기 검증의 성공 시 인터럽트 신호를 생성하고, 상기 프로세서는 상기 인터럽트 신호에 응답하여 동작 모드를 일반 실행 모드에서 보안 실행 모드로 전환하며, 상기 보안 가상 코어는 상기 보안 키를 생성할 수 있다. 상기 보안 키 생성 장치는 RAM을 더 포함하고, 상기 RAM은 상기 일반 가상 코어에서 실행 되는 명령어에 의하여 억세스 될 수 있는 제1 영역 및 상기 보안 가상 코어에서 실행 되는 명령어에 의하여 억세스 될 수 있는 상기 제1 영역과 겹치지 않는 제2 영역을 포함할 수 있다. 상기 일반 가상 코어에서 실행 되는 명령어는 상기 제2 영역에 억세스할 수 없는 것이 바람직하다.

[0018] 일부 실시예에 따르면, 상기 보안 키 생성 장치는 상기 인증 정보를 입력 받아 상기 프로세서에 제공 하는 입력부를 더 포함하고, 상기 프로세서는 일반 실행 모드 및 보안 실행 모드 중 하나로 동작하는 것이고, 상기 보안 실행 모드에서 상기 인증 정보를 상기 입력부로부터 제공 받는 것과 상기 보안 키를 생성하는 것을 실행할 수 있다. 상기 보안 키 생성 장치는 RAM을 더 포함하고, 상기 RAM은 상기 프로세서가 보안 실행 모드로 동작할 때에만 억세스 가능한 보안 영역을 포함하고, 상기 인증 정보, 원시 ID, 미디어 ID 및 보안 키는 상기 보안 영역

에 저장 될 수 있다.

[0019] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시예에 따른 호스트 장치는 저장 장치와 연결 되어 상기 원시 ID를 상기 저장 장치로부터 제공 받아 시스템 온 칩에 제공하는 저장 장치 인터페이스; 및 상기 저장 장치 인터페이스와 연결 된 시스템 온 칩(System-on-Chip; SoC)을 포함한다. 상기 시스템 온 칩은, 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하며, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성하는 보조 로직(pheriperal logic)을 포함할 수 있다. 상기 시스템 온 칩은, 상기 인증 정보를 제공 받아 상기 보조 로직에 제공 하는 코어(Core)를 더 포함할 수 있다. 상기 보조 로직은 상기 저장 장치 인터페이스와 상기 코어 사이의 데이터 패스(data path) 상에 연결 된 것일 수 있다. 상기 호스트 장치는 상기 시스템 온 칩에 의하여 제어 되고, 사용자로부터 상기 인증 정보를 입력 받아 상기 시스템 온 칩에 제공하는 입력부를 더 포함할 수 있다. 상기 시스템-온-칩은 상기 보안 키를 저장하는 레지스터를 더 포함할 수 있다. 상기 보조 로직은 상기 보안 키를 이용하여 컨텐츠를 암호화 한 후 상기 저장 장치 인터페이스를 통하여 상기 저장 장치에 제공할 수 있다. 상기 저장 장치 인터페이스는 상기 저장 장치로부터 암호화 컨텐츠를 제공 받아 상기 시스템 온 칩에 제공하고, 상기 보조 로직은 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하며, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 상기 암호화 컨텐츠를 복호화 하기 위한 보안 키를 생성할 수 있다.

[0020] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시예에 따른 저장 장치는 메모리 ID 및 상기 메모리 ID가 암호화 된 암호화 메모리 ID를 저장하는 메모리 소자; 호스트 장치로부터 사용자를 인증하기 위한 인증 정보를 제공 받아 보안 키 생성부에 제공 하고, 상기 호스트 장치로부터 컨텐츠를 제공 받아 암호화부에 제공하는 호스트 인터페이스; 상기 메모리 소자로부터 상기 암호화 메모리 ID를 리드(read)하고, 상기 암호화 메모리 ID를 복호화하여 상기 메모리 ID를 얻고, 상기 메모리 ID를 이용하여 상기 메모리 소자의 다른 고유 식별자인 메모리 파생 ID를 생성하는 파생 ID 연산부; 상기 인증 정보 및 상기 상기 메모리 파생 ID를 모두 이용하여 보안 키를 생성하는 보안 키 생성부; 및 상기 보안 키를 이용하여 상기 컨텐츠를 암호화 하여 상기 메모리 소자에 저장 하는 암호화부를 포함한다. 상기 메모리 ID는 상기 메모리 소자의 고유 식별자일 수 있다. 상기 인증 정보는 SD 카드 규격(SD Card Standard) 커맨드의 파라미터로 포함 되어 상기 호스트 장치로부터 제공 될 수 있다.

[0021] 일부 실시예에 따르면 상기 저장 장치는 랜덤 넘버 생성기를 더 포함하고, 상기 보안 키 생성부는 상기 랜덤 넘버 생성기에 의하여 생성 된 랜덤 넘버를 더 이용하여 상기 보안 키를 생성할 수 있다. 상기 저장 장치는 TCG(Trusted Computing Group)의 OPAL SSC(Opal Security Subsystem) 규격에 따라 동작하는 것일 수 있다.

[0022] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시예에 따른 보안 키 생성 방법은 저장 장치를 보안 키 생성 장치에 전기적으로 연결하고; 상기 보안 키 생성 장치가 상기 저장 장치에 저장 된 원시 ID를 제공 받아, 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하고; 상기 보안 키 생성 장치가 사용자로부터 상기 사용자를 인증하기 위한 인증 정보를 직접 입력 받거나, 상기 인증 정보를 네트워크를 통해 연결 된 다른 장치로부터 제공 받고; 상기 보안 키 생성 장치가 상기 미디어 ID 및 상기 인증 정보를 모두 이용하여 보안 키를 생성하는 것을 포함한다.

발명의 효과

[0023] 상기와 같은 본 발명에 따르면, 장치 및 사용자 모두에 종속 되어 보안성이 뛰어난 보안 키를 생성할 수 있는 효과가 있다. 예를 들어, 본 발명에 따른 보안 키 생성 장치에 의하여 생성 된 보안 키로 암호화 된 컨텐츠는 상기 보안 키 생성과 관련 된 특정 사용자가 특정 장치를 사용하는 경우에만 복호화 될 수 있다.

[0024] 또한, 상기 보안 키를 생성하는 장치가 신뢰 컴퓨팅을 지원하는 장치인 경우, 신뢰 컴퓨팅 환경을 지원하는 보안 모드에서 상기 보안 키 생성 작업을 수행하여 사용자 인증 정보, 장치의 식별자 및 생성 된 보안 키와 같은 정보의 유출을 막을 수 있는 효과가 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 보안 키 생성 장치의 구성을 나타낸 블록도이다.

도 2 내지 3은 본 발명의 일 실시예에 따른 보안 키 생성 장치의 ID 연산부와 관련 된 구성을 나타낸 블록도이다.

도 4는 본 발명의 일 실시예에 따른 보안 키 생성 장치의 ID 연산부의 동작을 설명하기 위한 참고도이다.

도 5는 본 발명의 일 실시예에 따른 보안 키 생성 장치의 구성을 나타낸 블록도이다.

도 6 내지 7은 본 발명의 일 실시예에 따른 보안 키 생성 장치가 신뢰 컴퓨팅을 지원하는 장치인 경우의 구성을 나타낸 블록도이다.

도 8은 본 발명의 일 실시예에 따른 보안 키 생성 장치의 구성을 나타낸 블록도이다.

도 9는 도 8에 도시 된 보안 키 생성 장치의 보조 로직의 배치를 설명하기 위한 참고도이다.

도 10 내지 11은 도 8에 도시 된 보안 키 생성 장치가 암복호화를 수행하는 경우의 구성을 나타낸 블록도이다.

도 12 내지 13은 본 발명의 일 실시예에 따른 저장 장치의 구성을 나타낸 블록도이다.

도 14는 본 발명의 일 실시예에 따른 저장 장치의 구성을 나타낸 블록도이다.

도 15는 본 발명의 일 실시예에 따른 보안 키 생성 방법의 순서도이다.

도 16은 본 발명의 일 실시예에 따른 보안 키 생성 및 상기 보안 키를 이용한 컨텐츠 암호화 방법의 순서도이다.

도 17 내지 20은 본 발명의 일 실시예에 따라 미디어 ID를 생성하는 방법의 순서도이다.

도 21은 본 발명의 일 실시예에 따른 보안 키 생성 및 상기 보안 키를 이용한 컨텐츠 복호화 방법의 순서도이다.

도 22는 본 발명의 일 실시예에 따른 컨텐츠 무단 복제 시 컨텐츠 복호화 실패 과정을 나타낸 순서도이다.

도 23은 본 발명의 일 실시예에 따른 사용자 인증 정보 입력 오류 시 컨텐츠 복호화 실패 과정을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 도면에서 표시된 구성요소의 크기 및 상대적인 크기는 설명의 명료성을 위해 과장된 것일 수 있다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭하며, "및/또는"은 언급된 아이템들의 각각 및 하나 이상의 모든 조합을 포함한다.

[0027] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[0028] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.

[0029] 본 명세서에서 기술하는 실시예들은 본 발명의 이상적인 구성도를 참고하여 설명될 것이다. 따라서, 제조 기술 등에 의해 구성도의 형태나 구조가 변형될 수 있다. 따라서, 본 발명의 실시예들은 도시된 특정 형태로 제한되는 것이 아니라 그로부터 변형된 형태도 포함하는 것이다. 즉, 도시된 구성은 본 발명의 특정 형태를 예시하기 위한 것이고, 발명의 범주를 제한하기 위한 것은 아니다.

[0030] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0031] 도 1을 참조하여 본 발명의 일 실시예에 따른 보안 키 생성 장치(10)의 구성 및 동작을 설명한다. 본 실시예에

따른 보안 키 생성 장치(10)는 저장 장치(200)에 연결 되고, 저장 장치(200)의 고유 식별자인 미디어 ID와 사용자(1)를 인증하기 위한 인증 정보를 이용하여 보안 키를 생성한다.

[0032] 보안 키 생성 장치(10)는 저장 장치(200)에 연결 되고, 저장 장치(200)로부터 원시 ID를 제공 받는다. 상기 원시 ID는 저장 장치(200)의 고유 식별자인 미디어 ID 연산에 이용 되는 하나 이상의 식별용 데이터로, 상기 미디어 ID와는 다른 데이터이다. 보안 키 생성 장치(10)는 상기 원시 ID로부터 상기 미디어 ID를 생성한다. 즉, 보안 키 생성 장치(10)는 저장 장치(200)로부터 상기 미디어 ID를 직접 제공 받는 것이 아니라, 상기 미디어 ID를 생성할 수 있는 소스 데이터인 원시 ID를 제공 받는 것이다. 상기 미디어 ID가 노출 되는 것을 방지하기 위한 것으로, 보안 키 생성 장치(10)는 상기 원시 ID로부터 상기 미디어 ID를 생성하기 위하여 사용 되는 데이터를 저장할 수 있다.

[0033] 본 실시예에 따른 보안 키 생성 장치(10)는 ID 연산부(12), 인증 정보 제공부(14) 및 보안 키 생성부(16)를 포함할 수 있다. ID 연산부(12)는 저장 장치에 저장 된 원시 ID를 제공 받아, 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산한다.

[0034] 인증 정보 제공부(14)는 사용자(1)를 인증하기 위한 인증 정보를 보안 키 생성부(16)에 제공한다. 상기 인증 정보는 사용자(1)가 보안 키 생성 장치(10)에 직접 입력할 수 있다. 또한, 사용자 인증 서버(2)가 보안 키 생성 장치(10)에 사용자 인증 정보를 제공할 수도 있다. 즉, 인증 정보 제공부(14)는 사용자로부터 입력 받거나, 사용자 인증 서버(2)로부터 제공 받은 상기 인증 정보를 보안 키 생성부(16)에 제공할 수 있다. 상기 인증 정보는, 예를 들어 특정 회원제 서비스에 사용 되는 사용자 인증 정보, 사용자 식별정보 또는 개인 정보일 수 있다. 상기 개인 정보는 개인의 신상과 관련 된 정보로, 예를 들어 주소, 생일, 전화 번호, 메일 주소, 주민 등록 번호, 사용자(1)가 사용하는 금융 보안 카드의 특정 번호에 해당하는 코드일 수 있다.

[0035] 보안 키 생성부(16)는 상기 미디어 ID 및 상기 인증 정보를 모두 이용하여 보안 키를 생성한다. 보안 키의 생성에 상기 미디어 ID가 이용 된다는 것은, 보안 키 생성에 있어서, 상기 미디어 ID가 적어도 한번은 입력 되는 것을 의미한다. 또한, 보안 키의 생성에 상기 인증 정보가 이용 된다는 것은, 보안 키 생성에 있어서, 상기 인증 정보가 적어도 한번은 입력 되는 것을 의미한다.

[0036] 보안 키 생성부(16)는 상기 미디어 ID 및 상기 인증 정보를 이진 연산하여 상기 보안 키를 생성할 수 있다. 상기 이진 연산은, 예를 들어 AND, OR, NOR, XOR, NAND 등이 사용 될 수 있다. 보안 키 생성부(16)는 상기 미디어 ID 및 상기 인증 정보를 문자열 연결 연산(String Concatenation; STRCAT)하여 상기 보안 키를 생성 할 수도 있다. 상기 문자열 연결에 있어서 선후 관계는 한정 되지 않는다. 즉, 상기 미디어 ID 뒤에 상기 인증 정보가 연결 될 수도 있으며, 상기 인증 정보 뒤에 상기 미디어 ID가 연결 될 수도 있다.

[0037] 보안 키 생성부(16)는 상기 미디어 ID 및 상기 인증 정보 만을 이용하여 상기 보안 키를 생성할 수도 있고, 상기 미디어 ID 및 상기 인증 정보 외에 하나 이상의 가변 데이터 또는 고정 데이터를 더 이용하여 상기 보안 키를 생성할 수도 있다.

[0038] 상기 보안 키는 사용자 인증 정보, 미디어 ID 및 보안 키 연산 공식 세가지를 모두 알아야 생성 될 수 있다. 보안 키 자체가 유출 되지 않는다면, 상기 보안 키 연산 공식이 알려지더라도, 상기 사용자 인증 정보 및 상기 미디어 ID를 모두 알아내지 않는 한 상기 보안 키는 연산 될 수 없다. 그런데, 상기 미디어 ID는 외부로 유출 되지 않는 값이고 저장 장치(200)가 제공하는 원시 ID로부터 얻어낼 수 밖에 없는 값이다. 또한 상기 인증 정보 역시 특정 사용자가 외부로 유출 되지 않도록 관리할 것이므로 쉽게 외부로 유출 되지 않는 값이다. 따라서, 본 실시예에 따른 보안 키 생성 장치(10)는 저장 장치(200)에 종속 되고, 동시에 특정 사용자에 종속 되는 보안 키를 생성한다.

[0039] 이하, 도 2 내지 3을 참조하여 원시 ID로부터 미디어 ID를 연산하는 ID 연산부(12)의 동작을 보다 자세히 설명하기로 한다.

[0040] 이미 언급한 바와 같이, 상기 원시 ID는 상기 미디어 ID와는 다른 데이터이고, 상기 원시 ID 역시 저장 장치(200)의 적어도 1 파트를 식별하기 위한 데이터이다. 예를 들어, 저장 장치(200)가 제1, 2 파트를 구비하고, 상기 제1 파트의 식별자인 제1 원시 ID 및 상기 제2 파트의 식별자인 제2 원시 ID가 각각 저장 장치(200)로부터 ID 연산부(12)에 제공 될 수 있을 것이다. 이때, 상기 원시 ID는 상기 제1 원시 ID 및 상기 제2 원시 ID를 포함하는 것이다.

[0041] 도 2은 ID 연산부(12)가 상기 원시 ID 중 하나로써 암호화 메모리 ID(264)를 저장 장치(200)로부터 제공 받는 것을 도시한다. 암호화 메모리 ID(264)는 저장 장치(200)에 구비 된 메모리 소자(206)의 고유 식별자인 메모리

ID(262)가 암호화 된 데이터이다. 메모리 ID(262)는 메모리 소자(206)의 제조 시에 제조사에 의하여 프로그램 된 데이터일 수 있다. 메모리 ID(262)는 시스템 영역에 저장 되어, 사용자 영역에 대한 억세스와 동일한 방식으로 억세스 되지 않는 것이 바람직하다. 사용자 영역에 저장 되는 경우, 메모리 ID(262)가 삭제 되거나 변형 될 수 있고, 외부로 유출 될 수 있기 때문이다.

[0042] 또한, 도 3은 ID 연산부(12)가 상기 원시 ID 중 다른 하나로써 컨트롤러 인증 정보를 저장 장치(200)로부터 제공 받는 것을 도시한다. 상기 컨트롤러 인증 정보는 보안 키 생성 장치(10)와 저장 장치(200)에 구비 된 메모리 소자 컨트롤러(208)는 상호 인증을 수행할 수 있는데, 상기 컨트롤러 인증 정보는 상기 상호 인증을 위하여 컨트롤러(208)가 보안 키 생성 장치(10)에 제공 하는 정보이다.

[0043] 도 4는 ID 연산부(12)가 미디어 ID를 생성하는 것을 설명하기 위한 참고도이다.

[0044] ID 연산부(12)는 암호화 메모리 ID(264)를 복호화 하여 메모리 ID(264)를 얻고, 메모리 ID(264)로부터 메모리 파생 ID를 생성한다. 또한, ID 연산부(12)는 상기 컨트롤러 인증 정보로부터 컨트롤러(208)의 고유 식별자인 컨트롤러 ID를 얻는다.

[0045] 암호화 메모리 ID(264)를 복호화 하기 위하여 사용 되는 제1 복호화 키는 암호화 된 상태로 저장 장치(200)로부터 제공 받을 수 있다. 또한, 암호화 제1 복호화 키를 복호화 하기 위한 제2 복호화 키는 보안 키 생성 장치(10)에 구비 된 저장부(미도시)에 저장 될 수 있다.

[0046] 즉, ID 연산부(12)는 암호화 제1 복호화 키를 저장 장치(200)로부터 제공 받고, 상기 제2 복호화 키를 이용하여 상기 암호화 제1 복호화 키로부터 제1 복호화 키를 얻은 후, 상기 제1 복호화 키를 이용하여 암호화 메모리 ID(264)를 메모리 ID(264)로 복호화 할 수 있다.

[0047] 상기 메모리 파생 ID는 메모리 소자(206)의 다른 고유 식별자이다. 즉, 메모리 소자(206)는 제조사에 의하여 프로그램 된 고유 식별자인 메모리 ID(262) 및 메모리 ID(262)를 이용하여 생성 된 메모리 파생 ID 두개의 고유 식별자를 가질 수 있다. 메모리 ID(262)는 메모리 소자(206)에 저장 되나, 상기 메모리 파생 ID는 메모리 소자(206)에 저장 되는 값이 아니라, 저장 장치(200)에 연결 되는 보안 키 생성 장치(10)에 의하여 생성 되는 값이다.

[0048] ID 연산부(12)는 상기 컨트롤러 인증 정보를 이용하여 상기 컨트롤러 ID를 생성할 수 있다. 상기 컨트롤러 인증 정보에는 컨트롤러 인증서 ID 및 컨트롤러(208)의 고유 식별 코드가 포함 될 수 있는데, ID 연산부(12)는 상기 컨트롤러 인증서 ID 및 상기 고유 식별 코드를 이용하여 상기 컨트롤러 ID를 생성할 수 있다. 예를 들어, ID 연산부(12)는 상기 컨트롤러 인증서 ID와 상기 고유 식별 코드를 문자열 연결 연산(string concatenation operation)하여 상기 컨트롤러 ID를 생성할 수 있다.

[0049] ID 연산부(12)는 상기 메모리 파생 ID 및 상기 컨트롤러 ID를 이용하여 상기 미디어 ID를 생성한다. 예를 들어, ID 연산부(12)는 상기 메모리 파생 ID 및 상기 컨트롤러 ID를 이진 연산에 입력하거나, 문자열 연결 연산에 입력 하여 상기 미디어 ID를 생성할 수 있다.

[0050] 본 발명의 일 실시예에 따른 보안 키 생성 장치의 구성 및 동작을 도 5 내지 7을 참조하여 설명하기로 한다.

[0051] 본 실시예에 따른 보안 키 생성 장치(20)는, 도 5에 도시 된 바와 같이 프로세서(102) 및 저장 장치 인터페이스(104)를 포함할 수 있다. 보안 키 생성 장치(20)는 프로세서(102)가 실행하는 명령어를 임시 저장하는 RAM(106), 사용자 인증 정보를 입력 받는 입력부(108)를 더 포함할 수 있다. 프로세서(102), 저장 장치 인터페이스(104), RAM(106) 및 입력부(108)는 시스템 버스(110)에 연결 될 수 있다.

[0052] 도 5에 도시 된 바와 같이, 저장 장치 인터페이스(104)는 보안 키 생성 장치(20)와 저장 장치(200) 간의 데이터 송수신을 중계할 수 있다. 저장 장치 인터페이스(104)는 저장 장치(200)로부터 원시 ID를 제공 받아 시스템 버스(110)를 통하여 프로세서(102)에 제공할 수 있다.

[0053] 프로세서(102)는 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하고, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성할 수 있다. 입력부(108)는 상기 인증 정보는 사용자로부터 입력 받아 프로세서(102)에 제공할 수 있다. 프로세서(102)는 상기 보안 키를 여러 가지 용도로 사용할 수 있다. 예를 들어, 상기 보안 키를 높은 보안 등급에서의 사용자의 인증 정보로 사용하거나, 저장 장치(200)에 저장 될 컨텐츠의 암호화 키로 사용할 수 있다.

[0054] 본 발명의 일 실시예에 따른 보안 키 생성 장치(20)는 보안 실행 환경(Secure Execution Environment)을 지원

하는 것일 수 있다. 보안 실행 환경은 프로세서, 운영체제 등의 지원을 통해서 프로그램의 안전한 수행을 보장하는 환경을 의미한다. 안전한 수행을 보장하는 방법으로는 무결성, 기밀성 보장 등이 있다. 일반적으로 하드웨어 기반의 보안 실행 환경 접근 방법이 소프트웨어 기반의 보안 실행 환경 접근 방법 보다 안전한 것으로 알려져 있다. 본 실시예에 따른 보안 키 생성 장치(20) 역시 하드웨어 기반의 보안 실행 환경을 제공하는 것으로 가정한다.

[0055] 도 6 내지 7에 도시 된 바와 같이, 보안 키 생성 장치(20)는 프로세스 실행 환경을 분리하기 위하여 두 개의 코어를 가지는 프로세서(102)를 포함할 수 있다. 프로세서(102)는 물리적으로 별개인 두 개 이상의 코어를 구비하여 보안 실행 모드 및 일반 실행 모드로 각각 사용할 수도 있고, 하나의 코어를 가상으로 분할하여, 보안 실행 모드 및 일반 실행 모드 용도로 각각 사용할 수도 있다. 이하, 도 6 및 도 7에서는 프로세서(102)가 두개의 가상 코어(120, 124)를 가지는 것을 가정하여 설명한다.

[0056] 보안 키 생성 장치(20)는 상기 보안 실행 환경을 제공 하는 보안 실행 모드에서 실행 되는 프로세스에 의해 생성 되는 데이터를, 상기 보안 실행 환경을 제공 하지 않는 일반 실행 모드에서 실행 되는 프로세스가 억세스 할 수 없도록 하는 것이 바람직하다. 즉, 상기 보안 실행 모드와 상기 일반 실행 모드에서의 데이터 억세스는 서로 분리 되는 것이 바람직하다. 예를 들어, RAM(106)은 일반 가상 코어(120)에서 실행 되는 명령어에 의하여 억세스 될 수 있는 제1 영역 및 보안 가상 코어(124)에서 실행 되는 명령어에 의하여 억세스 될 수 있는 상기 제1 영역과 겹치지 않는 제2 영역을 포함할 수 있다.

[0057] 프로세서(120)의 코어가 보안 실행 모드에서의 프로세스 실행을 위한 보안 가상 코어(124) 및 일반 실행 모드에서의 프로세스 실행을 위한 일반 가상 코어(120)로 논리적으로 분할 되어 운영 되는 경우, 상기 보안 실행 모드와 상기 가상 실행 모드 간의 전환은 컨텍스트 스위칭(Context Switching) 방식으로 이뤄질 수 있다.

[0058] 이상 설명 된 보안 실행 환경 제공 관련 기술과 관련하여, 프로세서(102)는 ARM사의 TRUSTZONE 기술, INTEL사의 Wireless TPM 기술, Texas Instument사의 M-Shield 기술, Freescale사의 보안 기술, SafeNet사의 SafeXcel TPM 기술, SafeNet사의 SafeZone 기술, Discretix사의 Security platform 기술, Qualcomm사의 SecureMSM 기술 중 적어도 하나가 적용 된 것일 수 있다.

[0059] 한편, 특정 프로세스가 프로세서(102)의 보안 실행 모드에서 실행 되기 위하여는 소정의 인증 절차가 필요할 수 있다. 상기 인증 절차는 사용자 인증 정보를 입력 받고, 상기 인증 정보가 기 저장 된 것과 동일한지 검증하는 것일 수 있다. 상기 검증을 통과한 경우, 프로세서(102)의 동작 모드를 일반 실행 모드에서 가상 실행 모드로 전환하기 위한 인터럽트 신호가 생성되고, 프로세서(102)가 상기 인터럽트 신호에 응답하여 동작 모드를 보안 실행 모드로 전환할 수 있다. 도 6에는 일반 실행 모드에서 동작하던 프로세서(102)가 보안 실행 모드로의 전환을 위하여 사용자 인증을 수행하고, 상기사용자 인증을 위하여 사용자 인증 정보를 입력부(108)로부터 제공 받으며, 상기 사용자 인증 정보를 이용한 인증이 성공하는 경우, 일반 가상 코어(120)에서 모니터 프로시져(122)를 거쳐 보안 가상 코어(124)로 활성화 되는 가상 코어를 교체하는 것이 기재 되어 있다.

[0060] 즉, 본 실시예에 따른 보안 키 생성 장치(20)의 프로세서(102)는 일반 실행 모드인 상태에서 실행 모드 전환을 위한 사용자 인증 정보를 입력 받고, 그 결과 실행 모드를 보안 실행 모드로 전환하며, 상기 보안 실행 모드에서 보안 키를 생성한다. 본 실시예에 따른 보안 키 생성 장치(20)는 보안 실행 모드에서 보안 키를 생성하므로, 사용자 인증 정보, 원시 ID, 메모리 ID, 미디어 ID 등이 유출 되는 것을 방지할 수 있는 효과가 있다.

[0061] 본 발명의 일 실시예에 따른 보안 키 생성 장치(20)의 프로세서(102)는 보안 실행 모드로 전환 된 상태에서 사용자 인증 정보 및 원시 ID를 제공 받고, 상기 보안 키를 생성할 수도 있다. 도 7에는 본 실시예에 따른 보안 키 생성 장치(20)의 프로세서(102)가 보안 실행 모드로 전환 된 상태에서 사용자 인증 정보 및 원시 ID를 제공 받고 상기 보안 키를 생성하는 것이 도시 되어 있다. 본 실시예에 따른 보안 키 생성 장치(20)에 구비 되는 RAM(106)은 프로세서(102)가 보안 실행 모드로 동작할 때에만 억세스 가능한 보안 영역을 포함하고, 프로세서(102)는 상기 인증 정보, 원시 ID, 미디어 ID 및 상기 보안 키는 상기 보안 영역에 저장 할 수 있다.

[0062] 본 실시예에 따르면, 사용자 인증 정보를 입력 받는 시점에 이미 보안 키 생성 장치(20)가 보안 실행 모드로 동작하는 상태이므로, 사용자 인증 정보, 원시 ID, 메모리 ID, 미디어 ID 등이 유출 되는 것을 방지할 수 있는 효과가 있다.

[0063] 이하, 본 발명의 일 실시예에 따른 보안 키 생성 장치의 구성 및 동작에 대하여 도 8 내지 11을 참조하여 설명하기로 한다.

[0064] 도 8에는 본 실시예에 따른 보안 키 생성 장치의 구성이 도시 되어 있다. 도 8에 도시 된 바와 같이, 본 실시예

에 따른 보안 키 생성 장치(30)는 시스템 온 칩(System on Chip; SoC)(302) 및 시스템 온 칩(302)과 연결 된 저장 장치 인터페이스(104)를 포함할 수 있다. 본 실시예의 저장 장치 인터페이스(104)는 저장 장치(200)와 연결 되어 상기 원시 ID를 상기 저장 장치로부터 제공 받아 시스템 온 칩(302)에 제공한다.

[0065] 시스템 온 칩(302)은 여러 가지 기능을 가진 시스템을 하나의 칩으로 구현한 것으로, 본 실시예에 따른 시스템 온 칩(302)은 상기 원시 ID로부터 상기 저장 장치의 고유 식별자인 미디어 ID를 연산하며, 상기 미디어 ID 및 사용자를 인증하기 위한 인증 정보를 모두 이용하여 보안 키를 생성하는 보조 로직(pheriperal logic)(320)을 포함한다.

[0066] 시스템 온 칩(302)은 명령어 연산을 수행 하는 코어(322)를 더 포함할 수 있다. 코어(322)는 보안 키 생성 장치(30)에 포함 된 RAM(미도시)에 저장 된 명령어들을 읽어 들여 실행할 수 있다. 상기 RAM은 시스템 온 칩(302) 내부에 구비 될 수도 있고, 외부에 구비 될 수도 있다. 코어(322)는 보안 키 생성 장치(30)의 입출력 관련 동작을 제어한다. 예를 들어, 코어(322)는 입력부(108)를 통하여 입력 된 사용자 인증 정보를 입력부(108)로부터 제공 받는다. 코어(322)는 상기 사용자 인증 정보를 보조 로직(320)에 제공한다.

[0067] 보조 로직(320)은 상기 사용자 인증 정보는 코어(322)로부터 제공 받지만, 상기 원시 ID는 저장 장치 인터페이스(104)로부터 코어(322)를 경유하지 않고 직접 제공 받을 수 있다. 이를 위해, 도 9에 도시 된 바와 같이, 보조 로직(320)은 저장 장치 인터페이스(104)와 코어(322) 사이의 데이터 패스(data path)(324) 상에 연결 된 것일 수 있다. 보조 로직(320)은 저장 장치(200)로부터 제공 된 상기 원시 ID를 데이터 패스(324)를 통해 제공 받고, 코어(322)에 전달하지 않을 수 있다. 코어(322)는 해킹 시도에 취약하고, 코어(322)에서 상기 원시 ID를 이용한 연산을 수행하지 않기 때문에, 보조 로직(320)은 상기 원시 ID를 코어(322)에 전달하지 않는 것이 바람직하다.

[0068] 즉, 보조 로직(320)은 보안 키를 생성함에 있어서, 코어(322)와 독립적으로 동작한다. 코어(322)로부터 사용자 인증 정보를 제공 받는 것 이외에는 상기 보안 키의 생성과 관련 된 모든 연산을 보조 로직(320)이 담당한다. 또한, 보조 로직(320)은 상기 RAM에 저장 되어 있는 프로그램을 실행하지 않고, 보조 로직(320) 내에 구비 된 ROM 등의 비휘발성 메모리에 저장 되어 있는 보안 키 생성 전용 프로그램 만을 실행할 수 있다.

[0069] 보조 로직(320)은 상기 생성 된 보안 키를 시스템 온 칩(302) 내에 구비 된 레지스터(324)에 저장 할 수 있다.

[0070] 보안 키, 미디어 ID, 메모리 ID 등을 빼내는 것을 목적으로 하는 해킹 프로그램은 코어(322)에서 실행 되는 것이 일반적이다. 따라서, 코어(322)와 독립 된 보조 로직(320)이 보안 키 생성 관련 연산을 전담하는 본 실시예의 보안 키 생성 장치(30)는 보안 키 생성 관련 데이터가 외부로 유출 되는 것을 효과적으로 방지할 수 있다.

[0071] 도 11에 도시 된 바와 같이, 본 실시예에 따른 보안 키 생성 장치(30)는 상기 보안 키를 이용하여 컨텐츠를 암호화 한 후, 보안 키 생성 장치(30)에 연결 되고, 상기 보안 키를 생성하는 데 사용 되는 미디어 ID를 생성하기 위하여 원시 ID를 제공 한 저장 장치(200)에 암호화 된 컨텐츠를 저장 할 수 있다. 보안성을 강화하기 위하여, 상기 암호화 또한 보조 로직(320)이 담당할 수 있다. 이를 위해, 보조 로직(320)은 암복호화 엔진(321)을 포함할 수 있다. 암복호화 엔진(321)은 레지스터(324)에 저장 된 보안 키를 암복호화 키로 사용할 수 있다.

[0072] 본 실시예에 따른 보안 키 생성 장치(30)는 저장 장치(200)와 연결 되어, 저장 장치(200)에 저장 된 암호화 컨텐츠를 복호화 할 수도 있다. 보안 키 생성 장치(30)는 상기 암호화 컨텐츠의 복호화 키를 자체 생성 해야 하는데, 상기 복호화 키는 저장 장치(200)로부터 원시 ID를 제공 받고, 보안 키 생성 장치(30)의 사용자로부터 인증 정보를 입력 받은 후, 상기 원시 ID로부터 저장 장치(200)의 미디어 ID를 생성하고, 상기 미디어 ID 및 상기 인증 정보를 이용하여 상기 컨텐츠의 복호화 키를 생성할 수 있다.

[0073] 이상, 보안 키 생성 장치(10, 20, 30)는 컴퓨터, UMPC (Ultra Mobile PC), 워크스테이션, 넷북(net-book), PDA (Personal Digital Assistants), 포터블(portable) 컴퓨터, 웹 타블렛(web tablet), 모바일 폰(mobile phone), 스마트폰(smart phone), e-북(e-book), PMP(portable multimedia player), 휴대용 게임기, 네비게이션(navigation) 장치, 블랙박스(black box), 디지털 카메라(digital camera), 3차원 수상기(3-dimensional television), 디지털 음성 녹음기(digital audio recorder), 디지털 음성 재생기(digital audio player), 디지털 영상 녹화기(digital picture recorder), 디지털 영상 재생기(digital picture player), 디지털 동영상 녹화기(digital video recorder), 디지털 동영상 재생기(digital video player), 정보를 무선 환경에서 송수신할 수 있는 장치, 홈 네트워크를 구성하는 다양한 전자 장치들 중 하나, 컴퓨터 네트워크를 구성하는 다양한 전자 장치들 중 하나, 텔레매틱스 네트워크를 구성하는 다양한 전자 장치들 중 하나, 컴퓨팅 시스템을 구성하는 다양한 구성 요소들 중 하나 등과 같은 전자 장치의 다양한 구성 요소들 중 하나로 제공 될 수 있다.

[0074] 이하, 본 발명의 일 실시예에 따른 저장 장치에 대하여 도 12 내지 도 14를 참고하여 설명하기로 한다. 본 실시예에 따른 저장 장치(40)는 자체 암호화 기능을 구비한 것이다. 즉, 저장 장치(40)가 호스트 장치에 연결 되어 호스트 장치로부터 저장할 데이터를 제공 받더라도 상기 데이터를 그대로 저장 하지 않고 자체 암호화 한 후 저장한다.

[0075] 본 실시예에 따른 저장 장치(40)는 상기 자체 암호화에 사용 되는 암호화 키를 상기 호스트 장치로부터 제공 받은 사용자 인증 정보 및 저장 장치(40)에 구비 된 메모리 소자(206)의 메모리 파생 ID를 이용하여 생성한다.

[0076] 도 12를 참조하여, 본 실시예에 따른 저장 장치(40)의 구성 및 동작을 설명한다. 도 12에 도시 된 바와 같이, 본 실시예에 따른 저장 장치(40)는 메모리 소자(206), 호스트 인터페이스(210), 파생 ID 연산부(212), 보안 키 생성부(214) 및 암호화부(216)를 포함할 수 있다.

[0077] 호스트 인터페이스(210)는 호스트 장치로부터 사용자를 인증하기 위한 인증 정보를 제공 받아 보안 키 생성부(214)에 제공 하고, 상기 호스트 장치로부터 컨텐츠를 제공 받아 암호화부(216)에 제공한다.

[0078] 메모리 소자(206)는 메모리 ID(262) 및 메모리 ID(264)가 암호화 된 암호화 메모리 ID(264)를 저장한다. 메모리 소자(206)는 사용자 영역 및 시스템 영역으로 저장 영역이 구분 되어 있을 수 있으며, 상기 사용자 영역에 대한 억세스 방법으로는 상기 시스템 영역으로 억세스하는 것이 불가능한 것이 바람직하다. 메모리 ID(262) 및 암호화 메모리 ID(264)는 상기 시스템 영역에 저장 되는 것이 바람직 하다.

[0079] 메모리 소자(262)는 불휘발성 메모리로서, NAND-FLASH 메모리, NOR-FLASH 메모리, 상변화 메모리 (PRAM: Phase change Random Access Memory), 고체 자기 메모리(MRAM: Magnetic Random Access Memory), 저항 메모리(RRAM, Resistive Random Access Memory)를 저장 수단으로 사용 한 칩 또는 패키지 일 수 있다. 또한, 상기 패키지 방식과 관련하여, 상기 메모리 소자는 PoP(Package on Package), Ball grid arrays(BGAs), Chip scale packages(CSPs), Plastic Leaded Chip Carrier(PLCC), Plastic Dual In Line Package(PDIP), Die in Waffle Pack, Die in Wafer Form, Chip On Board(COB), Ceramic Dual In Line Package(CERDIP), Plastic Metric Quad Flat Pack(MQFP), Thin Quad Flatpack(TQFP), Small Outline(SOIC), Shrink Small Outline Package(SSOP), Thin Small Outline(TSOP), Thin Quad Flatpack(TQFP), System In Package(SIP), Multi Chip Package(MCP), Wafer-level Fabricated Package(WFP), Wafer-Level Processed Stack Package(WSP) 등과 같은 방식으로 패키지화되어 실장 될 수 있다.

[0080] 파생 ID 연산부(212)는 메모리 소자(206)로부터 암호화 메모리 ID(264)를 리드(read)하고, 암호화 메모리 ID(264)를 복호화하여 메모리 ID(262)를 얻고, 메모리 ID(262)를 이용하여 메모리 소자(206)의 다른 고유 식별자인 메모리 파생 ID를 생성한다.

[0081] 보안 키 생성부(214)는 상기 인증 정보 및 상기 상기 메모리 파생 ID를 모두 이용하여 보안 키를 생성한다. 보안 키 생성부(214)가 상기 보안 키를 생성하는 방법은 보안 키 생성 장치(10)의 보안 키 생성부(16)가 보안 키를 생성하는 방법과 동일하다.

[0082] 암호화부(216)는 상기 보안 키를 이용하여 상기 컨텐츠를 암호화 하여 메모리 소자(206)에 저장 한다.

[0083] 본 실시예에 따른 저장 장치(40)는 호스트 장치로부터 제공 된 컨텐츠를 암호화 하여 저장 함에 있어서, 저장 장치(40)에 구비 된 메모리 소자(206)의 고유 식별자를 반영하여 생성 된 암호화 키를 이용하므로, 저장 된 암호화 컨텐츠가 무단 복제 되더라도 복호화 되는 것을 방지할 수 있는 효과가 있다. 복제 된 후에 암호화 컨텐츠가 저장 된 저장 장치에서는 원래 암호화 컨텐츠가 저장 되어 있던 저장 장치(40)의 미디어 ID와 동일한 미디어 ID를 얻을 수 없기 때문이다.

[0084] 본 실시예에 따른 저장 장치(40)는 사용자를 인증할 수 있는 사용자 인증 정보를 더 반영하여 생성 된 암호화 키를 이용하므로, 사용자의 인증 정보를 알지 못하면 저장 장치(40)에 저장 된 컨텐츠를 복호화 할 수 없게 된다.

[0085] 본 실시예에 따른 저장 장치(40)는 클라우드 컴퓨팅 서비스의 클라우드 서버에 구비 되는 저장 장치로 사용 될 수 있다. 즉, 클라우드 컴퓨팅 서비스의 사용자가 업로드 하는 컨텐츠 또는 데이터는 상기 사용자의 인증 정보 및 저장 장치(40)의 미디어 ID를 모두 이용하여 암호화 된 후 저장 된다. 이 경우, 사용자가 업로드 하는 컨텐츠 또는 데이터가 서버단에서 해킹 되어 암호화 된 상태로 유출 되더라도, 유출 된 컨텐츠 또는 데이터가 동일한 저장 장치에 저장 되어 있지 않고, 사용자의 인증 정보가 입력 되지 않으면 복호화가 불가능하다. 따라서, 본 실시예에 따른 저장 장치가 클라우드 컴퓨팅 서비스의 클라우드 서버에 구비 되어, 업로드 되는 컨텐츠 또는

데이터의 저장 수단으로 사용 되는 경우, 사용자가 업로드 하는 컨텐츠 또는 데이터의 유출 위험을 줄일 수 있는 효과가 있다.

[0086] 본 실시예에 따른 저장 장치(40)는 SD 협회(Secure Digital Association)의 SD 카드 규격을 만족하는 것일 수 있다. 이 경우, 호스트 인터페이스(210)는 SD 카드 규격에 따른 커맨드의 파라미터로써 수신 된 상기 인증 정보를 보안 키 생성부(214)에 제공할 수 있다.

[0087] 본 실시예에 따른 저장 장치(40)는 SSD(Solid State Drive), 또는 플래시 메모리를 내부에 포함하고 있는 HDD(Hard Disk Drive) 규격일 수있다. 이 경우, 호스트 인터페이스(210)는 대용량 저장장치를 위한 통신 커맨드를 지원하는 ATA, SATA, SCSI, PCIe, USB 등의 물리적 인터페이스일 수 있다.

[0088] 본 실시예에 따른 저장 장치(40)는, 도 13에 도시 된 바와 같이 랜덤 넘버(Random Number; RN)를 더 이용하여 보안 키를 생성할 수도 있다. 즉, 보안 키 생성부(214)는 랜덤 넘버, 상기 인증 정보 및 상기 미디어 ID를 모두 이용하여 보안 키를 생성할 수 있다. 본 실시예에 따른 저장 장치(40)는 상기 랜덤 넘버를 생성하여 보안 키 생성부(214)에 제공하는 랜덤 넘버 생성기(217)를 더 포함할 수 있다. 본 실시예에 따른 저장 장치(40)는 TCG(Trusted Computing Group)의 OPAL SSC(Opal Security Subsystem) 규격에 따라 동작하는 것일 수 있다.

[0089] 도 14를 참조하여, 본 발명의 일 실시예에 따른 메모리 시스템에 대하여 설명한다.

[0090] 도 14를 참조하면, 메모리 시스템(1000)은 비휘발성 메모리 장치(1100) 및 컨트롤러(1200)를 포함한다. 앞서 설명한 저장 장치(200)는 도 14에 도시 된 메모리 시스템(1000) 형태로 구성 될 수 있다.

[0091] 여기서 비휘발성 메모리 장치(1100)는 앞서 설명한 적어도 하나의 메모리 소자(206)를 포함할 수 있다.

[0092] 컨트롤러(1200)는 호스트 장치 및 비휘발성 메모리 장치(1100)에 연결된다. 호스트 장치(100)로부터의 요청에 응답하여, 컨트롤러(1200)는 비휘발성 메모리 장치(1100)를 억세스하도록 구성된다. 예를 들면, 컨트롤러(1200)는 비휘발성 메모리 장치(1100)의 읽기, 쓰기, 소거, 그리고 배경(background) 동작을 제어하도록 구성된다. 컨트롤러(1200)는 비휘발성 메모리 장치(1100) 및 호스트 장치(100) 사이에 인터페이스를 제공하도록 구성된다. 컨트롤러(1200)는 비휘발성 메모리 장치(1100)를 제어하기 위한 펌웨어(firmware)를 구동하도록 구성된다.

[0093] 예시적으로, 컨트롤러(1200)는 램(RAM, Random Access Memory), 프로세싱 유닛(processing unit), 호스트 인터페이스(host interface), 그리고 메모리 인터페이스(memory interface)와 같은 잘 알려진 구성 요소들을 더 포함한다. 램(RAM)은 프로세싱 유닛의 동작 메모리, 비휘발성 메모리 장치(1100) 및 호스트 장치(100) 사이의 캐시 메모리, 그리고 비휘발성 메모리 장치(1100) 및 호스트 장치(100) 사이의 버퍼 메모리 중 적어도 하나로서 이용된다. 프로세싱 유닛은 컨트롤러(1200)의 제반 동작을 제어한다.

[0094] 호스트 인터페이스는 호스트 장치 및 컨트롤러(1200) 사이의 데이터 교환을 수행하기 위한 프로토콜을 포함한다. 예시적으로, 컨트롤러(1200)는 USB (Universal Serial Bus) 프로토콜, MMC (multimedia card) 프로토콜, PCI (peripheral component interconnection) 프로토콜, PCI-E (PCI-express) 프로토콜, ATA (Advanced Technology Attachment) 프로토콜, Serial-ATA 프로토콜, Parallel-ATA 프로토콜, SCSI (small computer small interface) 프로토콜, ESDI (enhanced small disk interface) 프로토콜, 그리고 IDE (Integrated Drive Electronics) 프로토콜 등과 같은 다양한 인터페이스 프로토콜들 중 적어도 하나를 통해 외부(호스트)와 통신하도록 구성된다. 메모리 인터페이스는 비휘발성 메모리 장치(1100)와 인터페이싱한다. 예를 들면, 메모리 인터페이스는 낸드 인터페이스 또는 노어 인터페이스를 포함한다.

[0095] 메모리 시스템(1000)은 오류 정정 블록을 추가적으로 포함하도록 구성될 수 있다. 오류 정정 블록은 오류 정정 코드(ECC)를 이용하여 비휘발성 메모리 장치(1100)로부터 읽어진 데이터의 오류를 검출하고, 정정하도록 구성된다. 예시적으로, 오류 정정 블록은 컨트롤러(1200)의 구성 요소로서 제공된다. 오류 정정 블록은 비휘발성 메모리 장치(1100)의 구성 요소로서 제공될 수 있다.

[0096] 컨트롤러(1200) 및 비휘발성 메모리 장치(1100)는 하나의 반도체 장치로 집적될 수 있다. 예시적으로, 컨트롤러(1200) 및 비휘발성 메모리 장치(1100)는 하나의 반도체 장치로 집적되어, 메모리 카드를 구성할 수 있다. 예를 들면, 컨트롤러(1200) 및 비휘발성 메모리 장치(1100)는 하나의 반도체 장치로 집적되어 PC 카드(PCMCIA, personal computer memory card international association), 컴팩트 플래시 카드(CF), 스마트 미디어 카드(SM, SMC), 메모리 스틱, 멀티미디어 카드(MMC, RS-MMC, MMCmicro), SD 카드(SD, miniSD, microSD, SDHC), 유니버설 플래시 기억장치(UFS) 등과 같은 메모리 카드를 구성할 것이다.

[0097] 컨트롤러(1200) 및 비휘발성 메모리 장치(1100)는 하나의 반도체 장치로 집적되어 반도체 드라이브(SSD, Solid

State Drive)를 구성할 수 있다. 반도체 드라이브(SSD)는 반도체 메모리에 데이터를 저장하도록 구성되는 메모리 소자를 포함한다. 메모리 시스템(1000)이 반도체 드라이브(SSD)로 이용되는 경우, 메모리 시스템(1000)에 연결된 호스트 장치의 동작 속도는 획기적으로 개선된다.

[0098] 지금까지 도 1 내지 도 14의 각 구성요소는 소프트웨어(software) 또는, FPGA(field-programmable gate array)나 ASIC(application-specific integrated circuit)과 같은 하드웨어(hardware)를 의미할 수 있다. 그렇지만 상기 구성요소들은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 어드레싱(addressing)할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 상기 구성요소들 안에서 제공되는 기능은 더 세분화된 구성요소에 의하여 구현될 수 있으며, 복수의 구성요소들을 합하여 특정한 기능을 수행하는 하나의 구성요소로 구현할 수도 있다.

[0099] 도 15를 참조하여 본 발명의 일 실시예에 따른 보안 키 생성 방법을 설명한다.

[0100] 본 실시예에 따른 보안 키 생성 방법은 호스트 장치가 저장 장치의 미디어 ID를 얻고, 상기 미디어 ID 및 사용자 인증 정보를 모두 이용하여 보안 키를 생성하는 것으로 요약 된다.

[0101] 저장 장치는 원시 ID(primitive ID)를 저장한다(S100). 상기 원시 ID는 저장 장치(200)에 구비 된 메모리 소자에 저장 될 수 있다.

[0102] 호스트 장치는 상기 원시 ID를 제공 받아(S102), 상기 원시 ID로부터 저장 장치(200)의 고유 식별자인 미디어 ID를 연산할 수 있다(S104). 상기 원시 ID는 제1 원시 ID 및 제2 원시 ID를 포함하고, 상기 제2 원시 ID가 변환된 제2 식별자와 제1 원시 ID가 결합 되어 상기 미디어 ID가 연산 될 수도 있으나, 상기 원시 ID 자체가 상기 미디어 ID일 수도 있다. 상기 미디어 ID를 연산하는 방법에 대하여는 이후 도 19 내지 22를 참조하여 보다 자세히 설명하기로 한다.

[0103] 호스트 장치는 사용자 인증 정보를 제공 받는다. 상기 사용자 인증 정보는 호스트 장치에 구비 된 입력 수단(미도시)을 통하여 사용자가 입력한 것일 수도 있고, 호스트 장치 이외의 단말(미도시)을 통하여 사용자가 입력한 것을 호스트 장치가 제공 받은 것일 수도 있다.

[0104] 도 16은 본 발명의 일 실시예에 따른 보안 키 생성 및 상기 보안 키를 이용한 컨텐츠 암호화 방법을 나타낸 순서도이다. 도 18에서 보안 키를 생성하는 동작(S100, S102, S104, S105, S106)까지는 도 17과 동일하다.

[0105] 본 실시예에 따른 호스트 장치는 상기 보안 키를 이용하여 컨텐츠를 암호화 하여, 암호화 컨텐츠를 생성하거나, 상기 컨텐츠를 암호화 컨텐츠로 변환한다(S108). 상기 암호화에 사용 되는 암호화 알고리즘 및 사용 되는 암호화 키는 특정한 것으로 제한 되지 않으나, 암호화 키와 복호화 키가 동일하도록 대칭키 암호화 방식에 의한 알고리즘, 예를 들어 AES(Advanced Encryption Standard) 표준에 따르는 암호화 알고리즘이 사용 될 수 있다.

[0106] 암호화 컨텐츠는 저장 장치에 제공 되고(S110), 저장 장치는 암호화 컨텐츠를 저장한다(S112). 도 16에 도시 된 바와 같이, 호스트 장치는 상기 원시 ID를 제공한 저장 장치에 상기 암호화 컨텐츠를 저장하는 것이 바람직하다. 즉, 원시 ID를 제공한 저장 장치와 암호화 컨텐츠를 저장하는 저장 장치가 서로 달라서는 안 된다.

[0107] 도 16에 도시 된 것과 같이, 호스트 장치는 상기 보안 키를 저장 장치에 제공하지 않고, 상기 암호화 컨텐츠에 포함시키지도 않는다. 따라서, 상기 암호화 컨텐츠의 복호화 키를 얻기 위하여는 상기 암호화 컨텐츠가 저장 된 저장 장치의 미디어 ID를 얻고, 상기 미디어 ID로부터 복호화 키를 생성해야 하며, 상기 암호화 컨텐츠의 복호화 키를 저장 장치로부터 직접 얻을 수는 없다. 따라서, 도 15에 도시 된 컨텐츠 암호화 방법에 따르면, 암호화 컨텐츠가 다른 저장 장치로 무단 복제 되더라도 복호화를 할 수 없는 효과가 있다.

[0108] 호스트 장치가 상기 미디어 ID를 연산하는 방법에 대하여 도 17 내지 20을 참조하여 보다 자세히 설명한다.

[0109] 도 17은 저장 장치가 제1 파트 및 제2 파트를 포함하고, 저장 장치에 제1 파트를 식별하기 위한 제1 원시 ID 및 제2 파트를 식별하기 위한 제2 원시 ID가 저장 되는 경우의 미디어 ID를 연산하는 방법에 대하여 도시한다. 제1 파트 및 제2 파트는 각각 저장 장치에 구비 되는 소자 또는 모듈을 뜻하는 것으로, 각각 특정 기능을 수행하는 소자 그룹 또는 모듈 그룹일 수도 있다. 예를 들어, 제2 파트는 데이터 저장 기능을 수행하는 소자, 모듈, 소자 그룹 또는 모듈 그룹일 수 있고, 제1 파트는 제어 기능을 수행하는 소자, 모듈, 소자 그룹 또는 모듈 그룹일 수 있다.

[0110] 도 17에 도시 된 바와 같이, 호스트 장치는 상기 제1 원시 ID 및 상기 제2 원시 ID를 제공 받는다(S114).

[0111] 호스트 장치는 상기 제1 원시 ID 및 상기 제2 원시 ID 중 적어도 하나를 이용하여 상기 미디어 ID를 연산한다

(S116). 상기 제1 원시 ID만을 이용하여 상기 미디어 ID를 연산하는 경우 상기 미디어 ID는 제1 파트에 의하여 특정 될 것이고, 상기 제2 원시 ID만을 이용하여 상기 미디어 ID를 연산하는 경우 상기 미디어 ID는 제2 파트에 의하여 특정 될 것이며, 상기 제1 원시 ID 및 상기 제2 원시 ID를 모두 이용하여 상기 미디어 ID를 연산하는 경우 상기 미디어 ID는 제1 파트 및 제2 파트 모두에 의하여 특정 될 것이다.

[0112] 도 18에 도시 된 바와 같이, 상기 제2 원시 ID는 제2 식별자로 변환 될 수 있으며(S118), 상기 미디어 ID는 상기 제1 원시 ID 및 상기 제2 식별자 중 적어도 하나를 이용하여 상기 미디어 ID를 연산할 수도 있다(S120). 예를 들어, 상기 미디어 ID는 상기 제1 원시 ID 및 상기 제2 식별자 모두를 이용하여 상기 미디어 ID를 연산할 수 있다.

[0113] 제2 파트의 고유 식별자가 외부에 유출 되어서는 아니 되는 경우, 상기 제2 파트의 고유 식별자 대신, 상기 제2 파트의 고유 식별자가 암호화 된 데이터가 상기 제2 원시 ID로써 호스트 장치에 제공 될 수 있으며, 호스트 장치는 상기 제2 원시 ID를 이용하여 제2 파트의 또 다른 식별자로 사용 될 수 있는 상기 제2 식별자를 생성할 수 있다.

[0114] 도 19 내지 20을 참조하여 상기 미디어 ID를 연산하는 방법을 설명한다.

[0115] 도 19에 도시 된 바와 같이, 상기 제2 파트는 메모리 소자일 수 있고, 제1 파트는 메모리 소자 컨트롤러 일 수 있다. 메모리 소자는 자신의 고유 식별자를 저장한다. 상기 메모리 소자 컨트롤러의 고유 식별자 역시 메모리 소자에 저장 될 수 있다.

[0116] 먼저, 메모리 소자의 다른 식별자로 사용 될 수 있는 메모리 파생 ID를 생성하는 방법(S10)을 설명한다. 상기 메모리 파생 ID는 도 18을 참조하여 설명 된 제2 식별자와 동일한 것으로 이해 될 수 있다.

[0117] 호스트 장치는 메모리 소자에 저장 된 상기 메모리 소자의 고유 식별자가 암호화 된 암호화 메모리 ID를 저장 장치로부터 제공 받는다. 상기 암호화 메모리 ID 역시 메모리 소자에 저장 된 것일 수 있다. 상기 암호화 메모리 ID는 도 20을 참조하여 설명 된 제2 원시 ID와 동일한 것으로 이해 될 수 있다.

[0118] 호스트 장치는 상기 암호화 메모리 ID를 복호화 하여 상기 메모리 소자의 고유 식별자인 메모리 ID를 생성한다(S124).

[0119] 호스트 장치는 상기 메모리 ID를 이용하여 제2 인증 정보를 생성한다(S126). 호스트 장치는 랜덤 넘버를 생성하고, 상기 랜덤 넘버를 암호화 하여 세션 키를 생성하며, 상기 메모리 소자의 고유 식별자와 상기 세션 키를 소정의 일방 함수(one-way function)에 입력하여 상기 제2 인증 정보를 생성할 수 있다. 상기 일방 함수는 비트 연산은 출력 값으로부터 입력 값을 각각 찾아내는 것이 계산상 불가능한 것으로서, 예를 들어 2개의 연산자(operand)를 입력 받는 비트 연산 중 배타적 논리합(XOR)일 수 있다.

[0120] 한편, 저장 장치도 상기 메모리 ID를 이용하여 제1 인증 정보를 생성한다(S128). 메모리 소자에는 메모리 ID 이외에도 복수의 보조키로 구성 된 보조키 셋이 더 저장 되어 있을 수 있는데, 저장 장치는 상기 보조키 셋의 보조키 중 하나의 보조키를 암호화 하고, 상기 암호화 된 보조키를, 상기 호스트 장치에 의하여 생성 된 랜덤 넘버를 암호화 키로 하여 재암호화 하여 세션키를 생성할 수 있다. 저장 장치는 상기 세션키 및 상기 메모리 ID를 소정의 일방 함수에 입력하여 상기 제1 인증 정보를 생성할 수 있다.

[0121] 호스트 장치는 상기 제1 인증 정보를 저장 장치로부터 제공 받아(S130) 상기 제2 인증 정보와 일치하는지 검증한다(S132). 검증(S132)의 결과 제1, 2 인증 정보가 불일치 하는 경우, 인증 실패로 처리한다(S134).

[0122] 검증(S132)의 결과 제1, 2 인증 정보가 일치 하는 경우, 상기 메모리 소자의 고유 식별자를 이용하여 메모리 파생 ID를 생성한다. 상기 메모리 파생 ID는 상기 메모리 소자의 고유 식별자와 애플리케이션 고유 키(Application Specific Secret Value; ASSV)를 소정의 일방 함수에 입력하여 생성 될 수 있다.

[0123] 상기 애플리케이션 고유 키는 호스트 장치에서 수행 되는 각 애플리케이션에 대하여 고유한 키가 부여 되는 것일 수 있다. 예를 들어 음악 기록 애플리케이션, 영상 기록 애플리케이션, 소프트웨어 기록 애플리케이션 별로 서로 다른 고유의 키가 부여 될 수 있다. 상기 애플리케이션 고유 키는 암호화 되는 상기 컨텐츠의 타입에 따라 고유한 값을 가지거나, 암호화 되는 상기 컨텐츠의 제공자 식별 정보에 따라 고유한 값을 가질 수 있다. 바람직하게는, 상기 애플리케이션 고유 키는 암호화 되는 상기 컨텐츠의 타입에 따라 고유한 값을 가질 수 있다. 상기 컨텐츠의 타입은, 예를 들어 동영상, 음악, 문서, 소프트웨어 등에서 하나가 선택 될 수 있다.

[0124] 다음으로, 메모리 소자 컨트롤러의 고유 식별자를 제공 받는 것(S20)을 설명한다.

[0125] 도 20을 참조하여 호스트 장치가 저장 장치로부터 컨트롤러의 식별자를 제공 받는 것(S20)을 설명한다.

[0126] 먼저, 컨텐츠 기록 장치가 저장 장치로부터 제3 인증 정보를 제공 받는다(S140). 상기 제3 인증 정보에는 이미 언급 된 바와 같이, 저장 장치(200)의 인증서 및 저장 장치(200)에 구비 된 컨트롤러의 식별 코드가 포함 될 수 있다.

[0127] 다음으로, 컨텐츠 기록 장치와 저장 장치 간에 상호 인증이 수행 된다(S141). 상기 상호 인증은 공개키 기반의 인증일 수 있다. 상호 인증(S141)의 실패 시, 컨텐츠 기록 장치는 인증 실패로 처리한다(S144). 컨텐츠 기록 장치는 상기 제3 인증 정보로부터 상기 컨트롤러 ID(CONTROLLER ID)를 얻을 수 있다(S148).

[0128] 호스트 장치는 상기 메모리 파생 ID 및 상기 컨트롤러 고유 식별자 중 적어도 하나를 이용하여 미디어 ID를 연산한다. 바람직하게는, 호스트 장치는 상기 메모리 파생 ID 및 상기 컨트롤러 고유 식별자 모두를 이용하여 미디어 ID를 연산한다.

[0129] 상기 미디어 ID는 상기 메모리 파생 ID 및 상기 컨트롤러 고유 식별자를 이진 연산한 결과일 수 있다. 예를 들어, 상기 메모리 파생 ID 및 상기 컨트롤러 고유 식별자를 AND, OR, XOR 등 2개의 피연산자를 요하는 이진 연산한 결과가 상기 미디어 ID일 수 있다.

[0130] 상기 미디어 ID는 상기 메모리 파생 ID 뒤에 상기 컨트롤러 고유 식별자를 문자열 연결 연산(string concatenation)한 결과일 수 있다. 상기 미디어 ID는 상기 컨트롤러 고유 식별자 뒤에 상기 메모리 파생 ID를 문자열 연결 연산한 결과일 수도 있다.

[0131] 이하, 본 발명의 일 실시예에 따른 보안 키 생성 및 상기 보안 키를 이용한 컨텐츠 복호화 방법에 대하여 도 21을 참조하여 설명한다.

[0132] 저장 장치에는 원시 ID 및 암호화 컨텐츠가 각각 저장 되어 있다(S200, S202). 상기 암호화 컨텐츠는 저장 장치의 미디어 ID 및 사용자 인증 정보(A)를 이용하여 생성 된 암호화 키를 이용하여 암호화 된 것으로 가정한다.

[0133] 호스트 장치는 상기 원시 ID를 저장 장치로부터 제공 받는다(S202). 도 8에는 도시 되어 있지 않지만, 호스트 장치는 상기 원시 ID의 제공을 저장 장치에 요청하고, 상기 요청에 대한 응답으로 상기 원시 ID를 제공 받을 수 있다. 호스트 장치는 상기 암호화 컨텐츠에 대한 재생 명령이 사용자로부터 입력 되는 경우, 상기 원시 ID 제공의 요청을 수행할 수 있다.

[0134] 호스트 장치는 상기 원시 ID를 이용하여 미디어 ID를 연산한다(S203). 호스트 장치가 미디어 ID를 연산하는 동작은 도 17 내지 도 20을 참조하여 설명 된 호스트 장치의 미디어 ID 연산 동작과 동일할 수 있으므로, 중복 된 설명을 생략한다.

[0135] 호스트 장치는 사용자로부터 입력 된 인증 정보를 제공 받는다(S204). 이때, 입력 된 인증 정보는 상기 암호화 컨텐츠의 암호화 키 생성에 사용 된 것과 같을 수도 있고 다를 수도 있으나, 설명의 편의를 위하여 같은 것으로 가정한다.

[0136] 호스트 장치는 상기 미디어 ID 및 상기 인증 정보를 이용하여 복호화 키를 생성한다(S205).

[0137] 복호화 키의 생성(S205)은 상기 미디어 ID 및 상기 사용자 인증 정보 만을 이용할 수도 있고, 상기 미디어 ID 및 상기 사용자 인증 정보 외에 하나 이상의 가변 데이터 또는 고정 데이터를 더 이용할 수도 있다.

[0138] 예를 들어, 상기 복호화 키는 상기 미디어 ID 및 상기 인증 정보를 이진 연산한 결과 산출 되는 데이터일 수 있다. 상기 복호화 키는 상기 이진 연산 중에서도 XOR(eXclusive OR) 연산의 결과 산출 되는 데이터일 수 있다. 즉, 상기 복호화 키는 상기 미디어 ID 및 상기 인증 정보를 XOR 연산한 결과 데이터일 수 있다.

[0139] 예를 들어, 상기 복호화 키는 상기 미디어 ID 및 상기 인증 정보를 문자열 연결 연산(String Concatenation; STRCAT)한 결과 산출 되는 데이터일 수도 있다. 상기 문자열 연결에 있어서 선후 관계는 한정 되지 않는다. 즉, 상기 미디어 ID 뒤에 상기 인증 정보가 연결 될 수도 있으며, 상기 인증 정보 뒤에 상기 미디어 ID가 연결 될 수도 있다.

[0140] 호스트 장치는 저장 장치에 저장 된 암호화 컨텐츠를 읽어온 후(S206), 상기 복호화 키를 이용하여 복호화 하여(S207), 재생한다(S208).

[0141] 도 22를 참조하여 컨텐츠 저장 장치 X(200)에 저장 되어 있던 암호화 컨텐츠가 컨텐츠 저장 장치 Y(201)로 무단 복제 되는 경우, 호스트 장치가 컨텐츠 저장 장치 Y(201)에 저장 된 암호화 컨텐츠의 복호화를 실패하는 동작을

설명한다.

[0142] 컨텐츠 저장 장치 Y(201)에는 컨텐츠 저장 장치 X(200)와는 다른 원시 ID Y가 저장 되어 있다(S210).

[0143] 또한, 컨텐츠 저장 장치 X(200)는 도 18에 도시 된 컨텐츠 암호화 방법에 의하여 암호화 된 암호화 컨텐츠가 저장 되어 있다(S209). 상기 암호화 키("XA")를 생성하는 데 사용 된 인증 정보는 "A"인 것으로 가정한다. 사용자가 저장 장치 X(200)에서 컨텐츠 저장 장치 Y(201)로 상기 암호화 컨텐츠를 무단 복제한 상황(S211)을 가정한다.

[0144] 사용자가 호스트 장치에 컨텐츠 저장 장치 Y(201)를 연결하고, 상기 호스트 장치에 상기 암호화 컨텐츠의 재생 명령을 입력하는 경우, 호스트 장치는 컨텐츠 저장 장치 Y(201)에 저장 된 원시 ID Y를 제공 받는다(S213).

[0145] 호스트 장치는 상기 원시 ID Y를 이용하여 컨텐츠 저장 장치 Y(201)의 미디어 ID를 생성한다(S214).

[0146] 호스트 장치는 사용자 인증 정보를 입력 받는다(S215). 상기 사용자 인증 정보는 상기 암호화 컨텐츠의 암호화 키를 생성하는 데 사용 된 인증 정보와 같은 "A"인 것으로 가정한다.

[0147] 호스트 장치는 상기 미디어 ID 및 상기 사용자 인증 정보("A")를 이용하여 복호화 키("YA")를 생성한다(S216).

[0148] 호스트 장치는 생성 된 복호화 키를 이용하여 컨텐츠 저장 장치 Y(201)로부터 제공(S217) 받은 암호화 컨텐츠를 복호화 시도 한다(S218). 그러나, 생성(S216) 된 복호화 키가 상기 암호화 컨텐츠의 복호화 키와 다르기 때문에, 호스트 장치는 상기 암호화 컨텐츠를 복호화할 수 없다.

[0149] 따라서, 호스트 장치는 무단 복제 되어 저장 장치(201)에 저장 된 암호화 컨텐츠를 재생 할 수 없다(S219).

[0150] 도 22에는 호스트 장치의 사용자가 올바른 인증 정보, 즉 암호화 키의 생성에 사용 된 사용자 인증 정보와 동일한 것을 입력한 경우를 가정하였으나, 틀린 인증 정보, 즉 암호화 키의 생성에 사용 된 사용자 인증 정보와 다른 것을 입력하는 경우에도, 호스트 장치는 무단 복제 되어 저장 장치(201)에 저장 된 암호화 컨텐츠를 재생 할 수 없다(S219).

[0151] 즉, 무단 복제 되어 저장 장치(201)에 저장 된 암호화 컨텐츠는, 사용자 인증 정보를 올바르게 입력했는지와 무관하게 재생 될 수 없다.

[0152] 도 23은 암호화 컨텐츠의 암호화 키를 생성하는데 사용 된 사용자 인증 정보가 올바르지 않은 경우, 컨텐츠 재생을 실패하는 실시예를 도시 한다.

[0153] 컨텐츠 저장 장치 X(200)에는 저장 장치의 미디어 ID 및 사용자 인증 정보("A")를 이용하여 생성 된 암호화 키("XA")를 이용하여 암호화 된 암호화 컨텐츠가 저장 되어 있다(S209).

[0154] 사용자가 호스트 장치에 컨텐츠 저장 장치 X(200)를 연결하고, 호스트 장치에 상기 암호화 컨텐츠의 재생 명령을 입력하는 경우, 호스트 장치는 컨텐츠 저장 장치 X(200)에 저장 된 원시 ID X를 제공 받는다(S220).

[0155] 호스트 장치는 상기 원시 ID X를 이용하여 컨텐츠 저장 장치 X(200)의 미디어 ID를 생성한다(S211).

[0156] 호스트 장치는 사용자 인증 정보를 입력 받는다(S222). 상기 사용자 인증 정보는 상기 암호화 컨텐츠의 암호화 키를 생성하는 데 사용 된 인증 정보와 다른 "B"인 것으로 가정한다.

[0157] 호스트 장치는 상기 미디어 ID 및 상기 사용자 인증 정보("B")를 이용하여 복호화 키("XB")를 생성한다(S223).

[0158] 호스트 장치는 생성 된 복호화 키를 이용하여 저장 장치 Y(201)로부터 제공(S224) 받은 암호화 컨텐츠를 복호화 시도 한다(S225). 그러나, 생성 된 복호화 키("XB")가 상기 암호화 컨텐츠의 복호화 키("XA")와 다르기 때문에, 호스트 장치는 상기 암호화 컨텐츠를 복호화할 수 없다.

[0159] 따라서, 호스트 장치는 컨텐츠 저장 장치에 저장 된 암호화 컨텐츠를 재생 할 수 없다(S226).

[0160] 도 23에는 호스트 장치의 사용자가 올바르지 않은 인증 정보, 즉 암호화 키의 생성에 사용 된 사용자 인증 정보와 다른 것을 입력한 경우를 가정하였으나, 올바른 인증 정보, 즉 암호화 키의 생성에 사용 된 사용자 인증 정보와 동일한 것을 입력하는 경우에는 저장 장치에 저장 된 암호화 컨텐츠를 재생 할 수 있다.

[0161] 이상 첨부된 도면을 참조하여 본 발명의 실시예들을 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 실시예들은 모든 면에서 예시적인 것이며 한정

적이 아닌 것으로 이해해야만 한다.

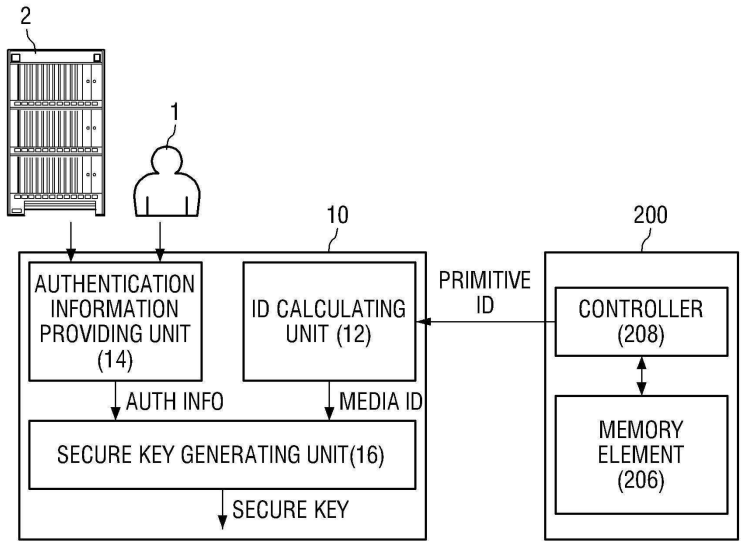
부호의 설명

[0162]

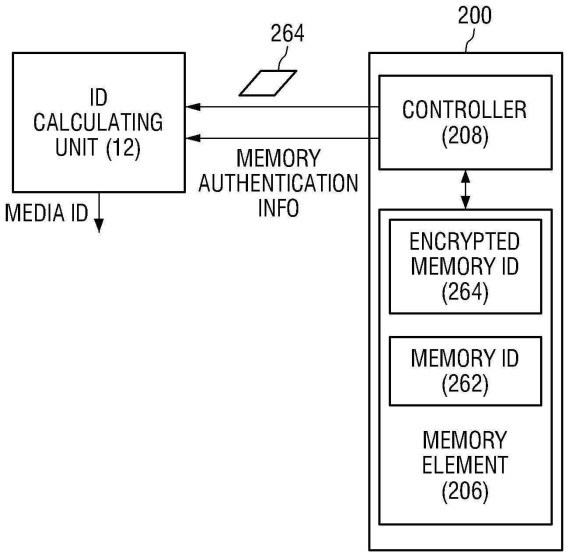
사용자 인증 서버	2
보안 키 생성 장치	10
저장 장치	200

도면

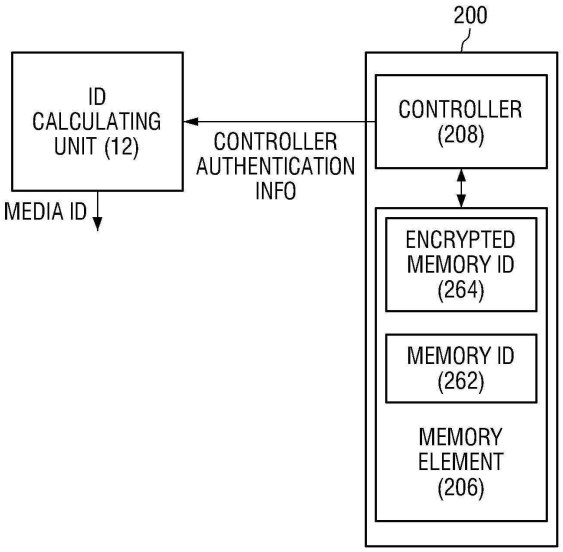
도면1



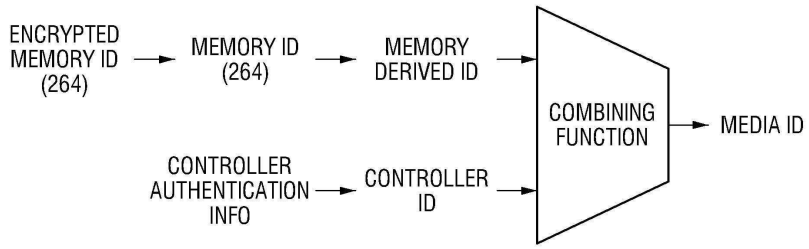
도면2



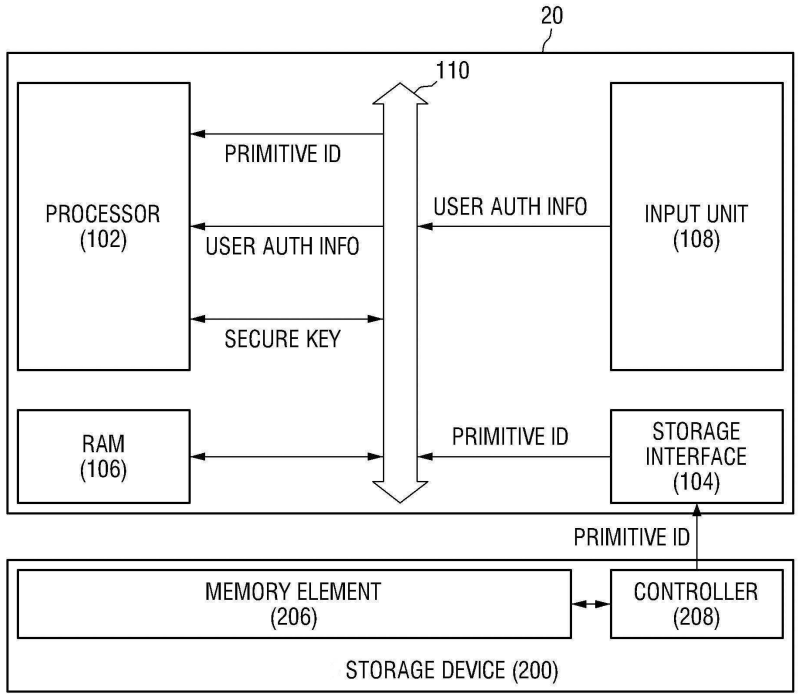
도면3


200
ID CALCULATING UNIT (12)
CONTROLLER AUTHENTICATION INFO
MEDIA ID
CONTROLLER (208)
ENCRYPTED MEMORY ID (264)
MEMORY ID (262)
MEMORY ELEMENT (206)

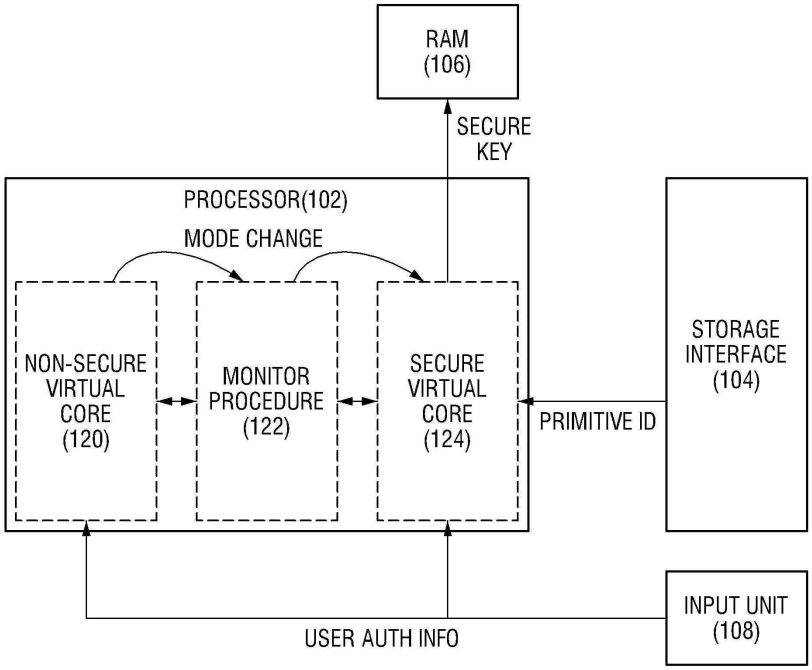
도면4


ENCRYPTED MEMORY ID (264)
MEMORY ID (264)
MEMORY DERIVED ID
CONTROLLER AUTHENTICATION INFO
CONTROLLER ID
COMBINING FUNCTION
MEDIA ID

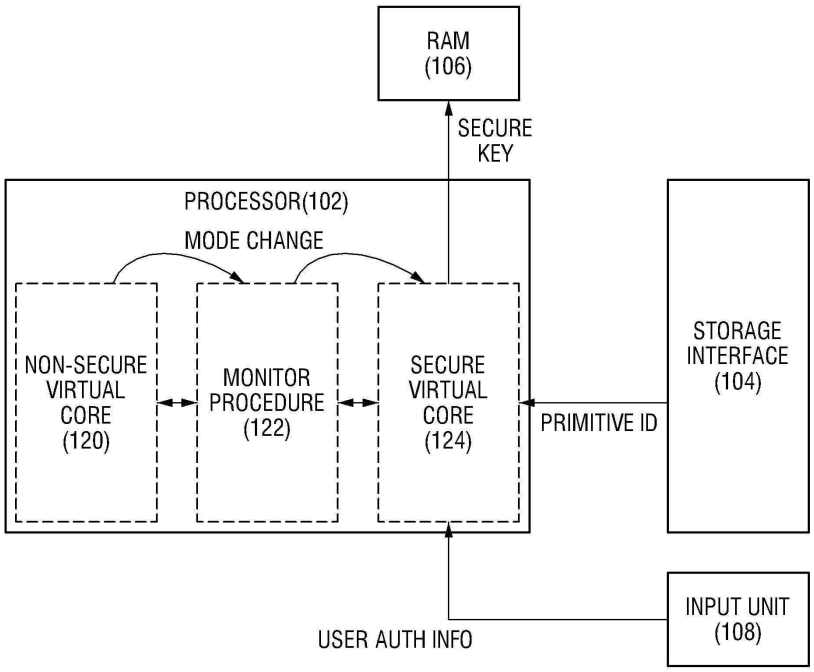
도면5


20
110
PROCESSOR (102)
PRIMITIVE ID
USER AUTH INFO
SECURE KEY
USER AUTH INFO
INPUT UNIT (108)
RAM (106)
PRIMITIVE ID
STORAGE INTERFACE (104)
PRIMITIVE ID
MEMORY ELEMENT (206)
CONTROLLER (208)
STORAGE DEVICE (200)

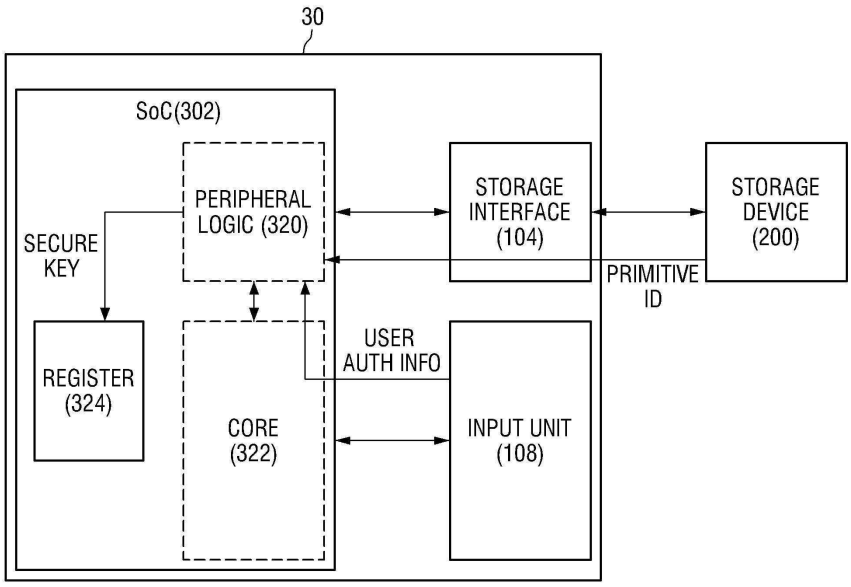
도면6


RAM
(106)
SECURE
KEY
PROCESSOR(102)
MODE CHANGE
NON-SECURE
VIRTUAL
CORE
(120)
MONITOR
PROCEDURE
(122)
SECURE
VIRTUAL
CORE
(124)
PRIMITIVE ID
STORAGE
INTERFACE
(104)
INPUT UNIT
(108)
USER AUTH INFO

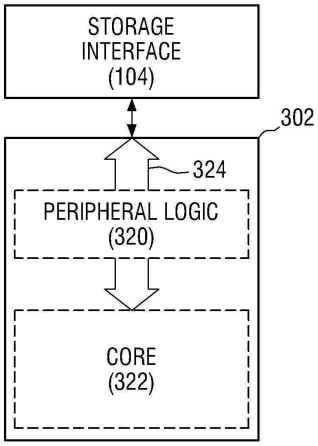
도면7


RAM
(106)
SECURE
KEY
PROCESSOR(102)
MODE CHANGE
NON-SECURE
VIRTUAL
CORE
(120)
MONITOR
PROCEDURE
(122)
SECURE
VIRTUAL
CORE
(124)
PRIMITIVE ID
STORAGE
INTERFACE
(104)
INPUT UNIT
(108)
USER AUTH INFO

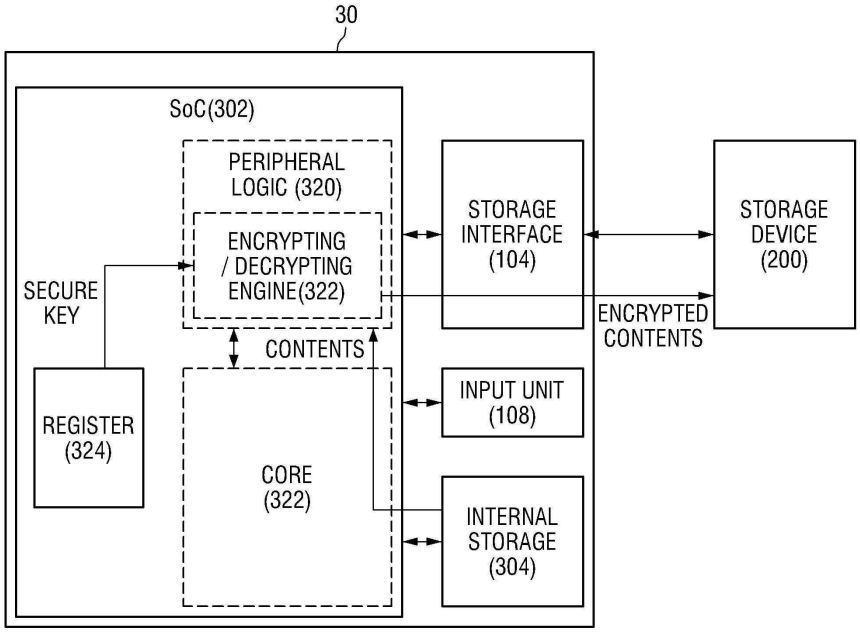
도면8


30
SoC(302)
PERIPHERAL LOGIC (320)
SECURE KEY
REGISTER (324)
CORE (322)
STORAGE INTERFACE (104)
STORAGE DEVICE (200)
PRIMITIVE ID
USER AUTH INFO
INPUT UNIT (108)

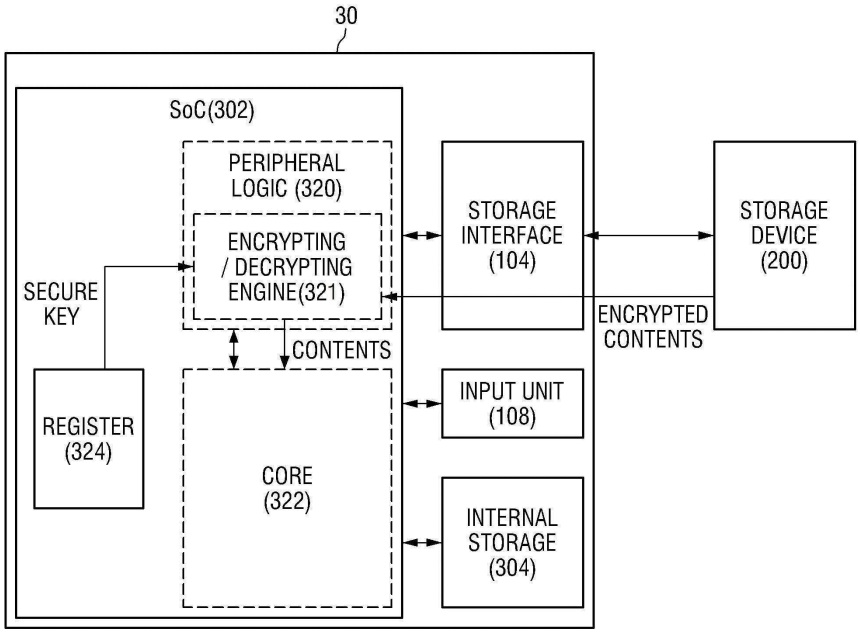
도면9


STORAGE INTERFACE (104)
302
324
PERIPHERAL LOGIC (320)
CORE (322)

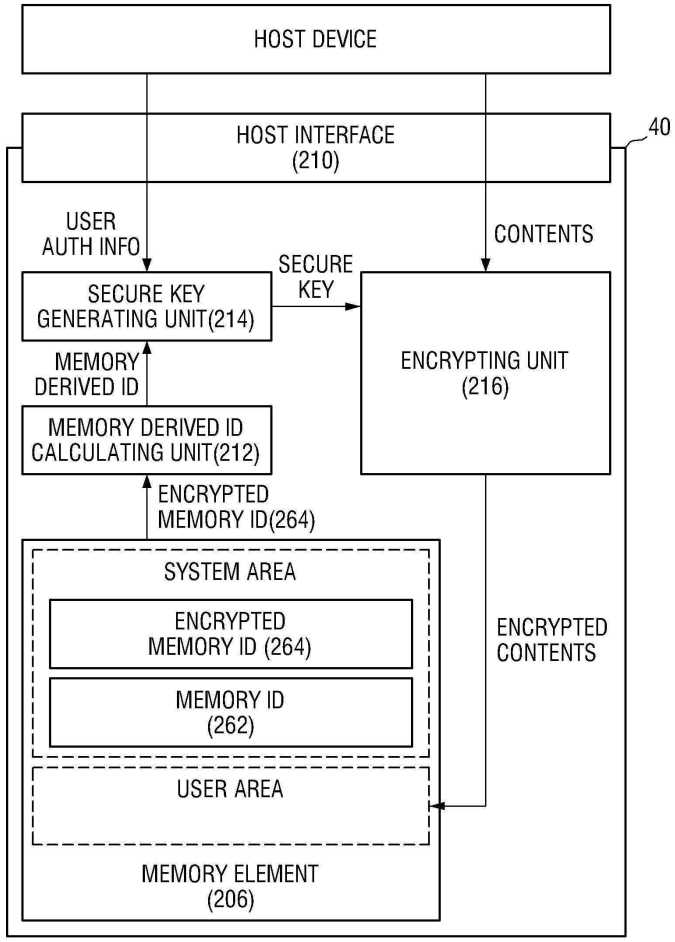
도면10


30
SoC(302)
PERIPHERAL LOGIC (320)
ENCRYPTING / DECRYPTING ENGINE(322)
SECURE KEY
CONTENTS
REGISTER (324)
CORE (322)
STORAGE INTERFACE (104)
INPUT UNIT (108)
INTERNAL STORAGE (304)
STORAGE DEVICE (200)
ENCRYPTED CONTENTS

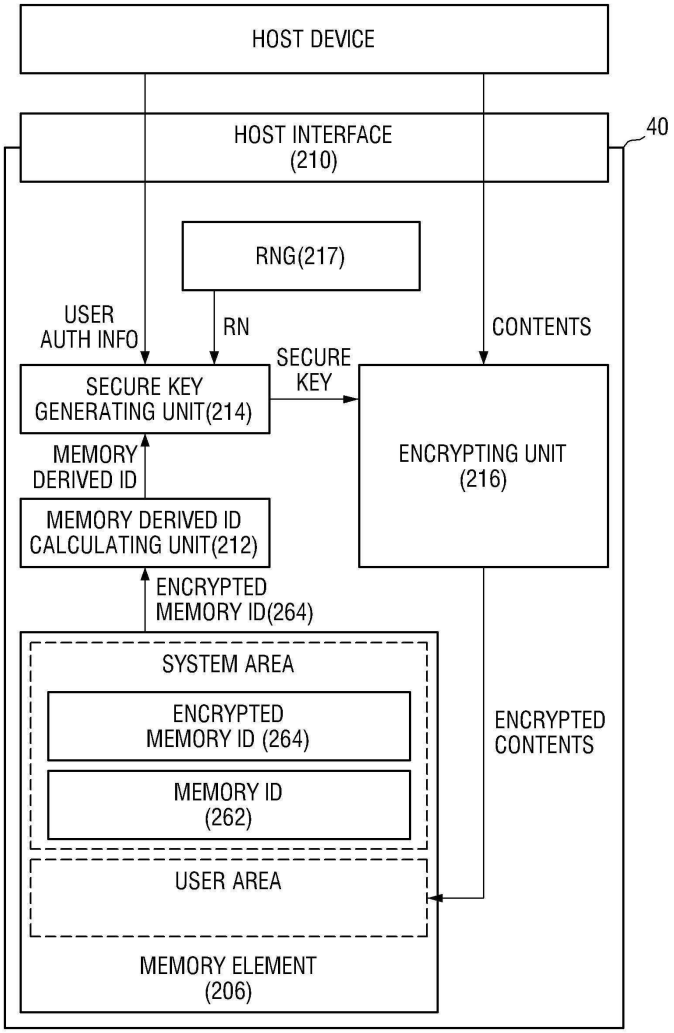
도면11


30
SoC(302)
PERIPHERAL LOGIC (320)
ENCRYPTING / DECRYPTING ENGINE(321)
SECURE KEY
CONTENTS
REGISTER (324)
CORE (322)
STORAGE INTERFACE (104)
INPUT UNIT (108)
INTERNAL STORAGE (304)
STORAGE DEVICE (200)
ENCRYPTED CONTENTS

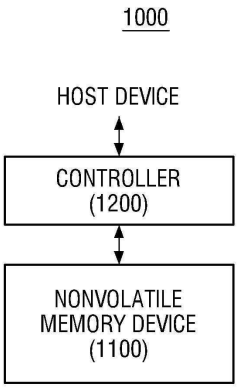
도면12


HOST DEVICE
HOST INTERFACE
(210)
40
USER
AUTH INFO
CONTENTS
SECURE
KEY
SECURE KEY
GENERATING UNIT(214)
ENCRYPTING UNIT
(216)
MEMORY
DERIVED ID
MEMORY DERIVED ID
CALCULATING UNIT(212)
ENCRYPTED
MEMORY ID(264)
SYSTEM AREA
ENCRYPTED
MEMORY ID (264)
MEMORY ID
(262)
ENCRYPTED
CONTENTS
USER AREA
MEMORY ELEMENT
(206)

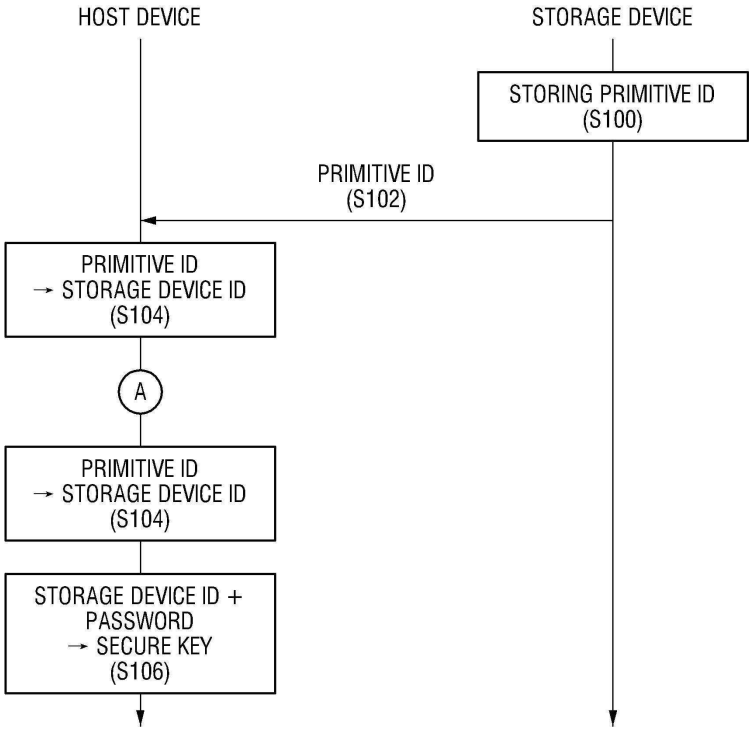
도면13


HOST DEVICE
HOST INTERFACE
(210)
40
RNG(217)
USER
AUTH INFO
RN
CONTENTS
SECURE
KEY
SECURE KEY
GENERATING UNIT(214)
ENCRYPTING UNIT
(216)
MEMORY
DERIVED ID
MEMORY DERIVED ID
CALCULATING UNIT(212)
ENCRYPTED
MEMORY ID(264)
SYSTEM AREA
ENCRYPTED
MEMORY ID (264)
MEMORY ID
(262)
ENCRYPTED
CONTENTS
USER AREA
MEMORY ELEMENT
(206)

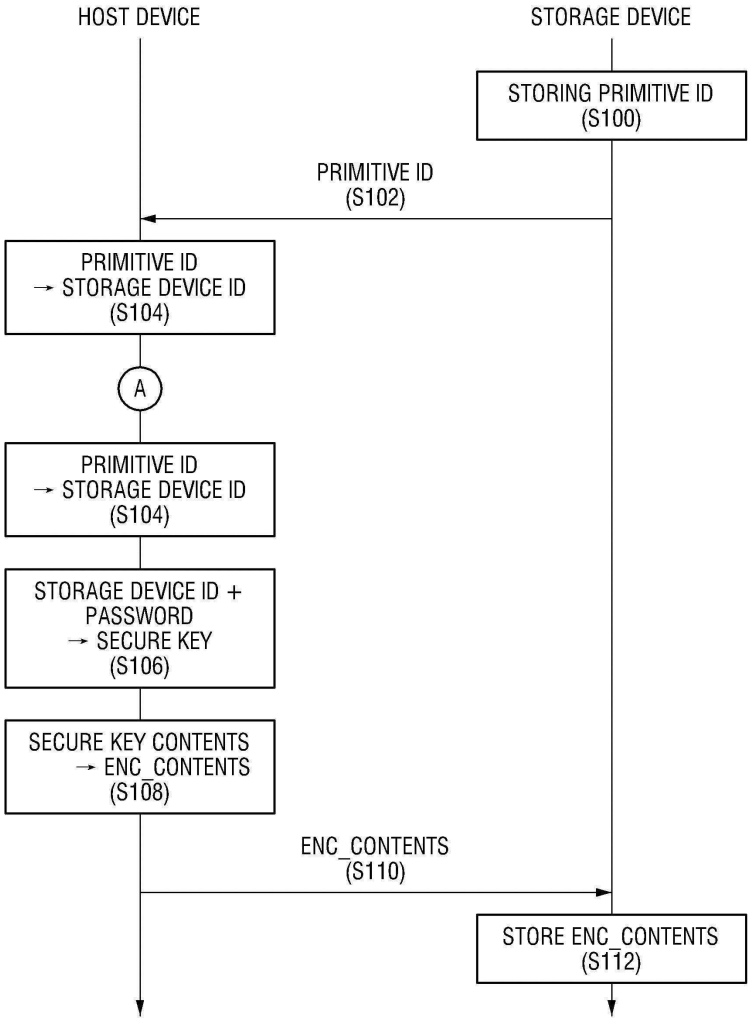
도면14


1000
HOST DEVICE
CONTROLLER
(1200)
NONVOLATILE
MEMORY DEVICE
(1100)

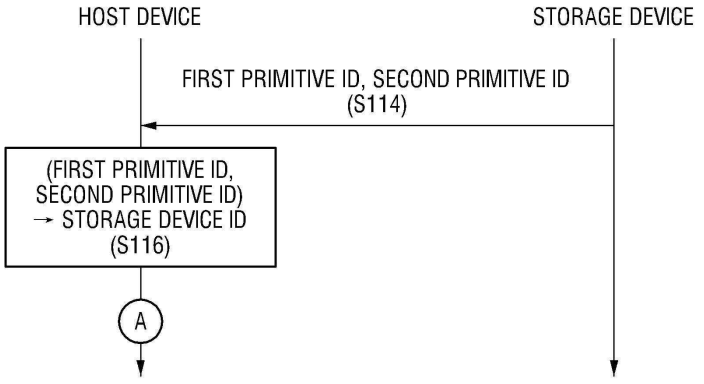
도면15


HOST DEVICE
STORAGE DEVICE
STORING PRIMITIVE ID
(S100)
PRIMITIVE ID
(S102)
PRIMITIVE ID
→ STORAGE DEVICE ID
(S104)
A
PRIMITIVE ID
→ STORAGE DEVICE ID
(S104)
STORAGE DEVICE ID +
PASSWORD
→ SECURE KEY
(S106)

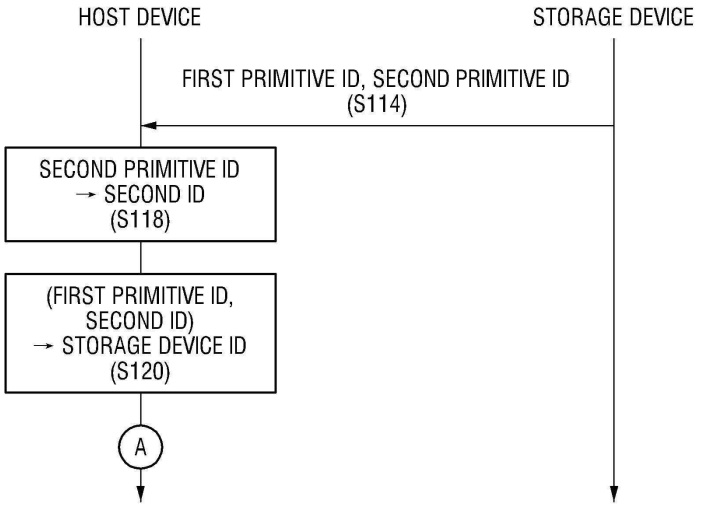
도면16


HOST DEVICE
STORAGE DEVICE
STORING PRIMITIVE ID
(S100)
PRIMITIVE ID
(S102)
PRIMITIVE ID
→ STORAGE DEVICE ID
(S104)
A
PRIMITIVE ID
→ STORAGE DEVICE ID
(S104)
STORAGE DEVICE ID +
PASSWORD
→ SECURE KEY
(S106)
SECURE KEY CONTENTS
→ ENC_CONTENTS
(S108)
ENC_CONTENTS
(S110)
STORE ENC_CONTENTS
(S112)

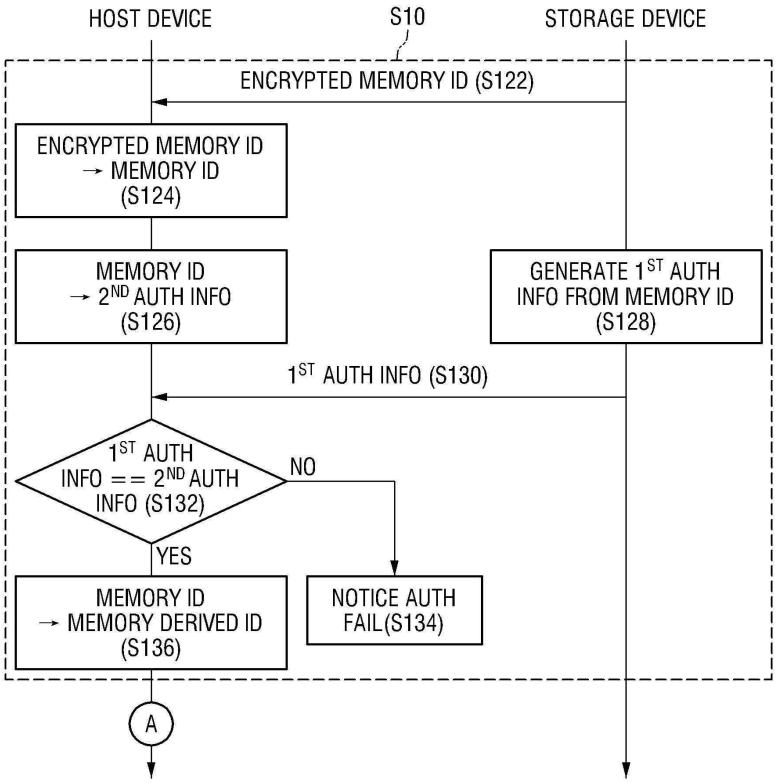
도면17


HOST DEVICE
STORAGE DEVICE
FIRST PRIMITIVE ID, SECOND PRIMITIVE ID
(S114)
(FIRST PRIMITIVE ID,
SECOND PRIMITIVE ID)
→ STORAGE DEVICE ID
(S116)
A

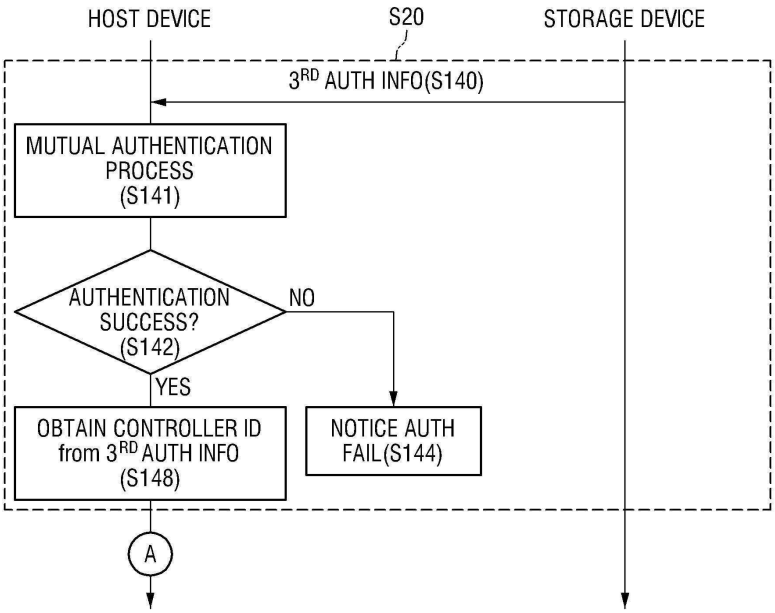
도면18


HOST DEVICE
STORAGE DEVICE
FIRST PRIMITIVE ID, SECOND PRIMITIVE ID
(S114)
SECOND PRIMITIVE ID
→ SECOND ID
(S118)
(FIRST PRIMITIVE ID,
SECOND ID)
→ STORAGE DEVICE ID
(S120)
A

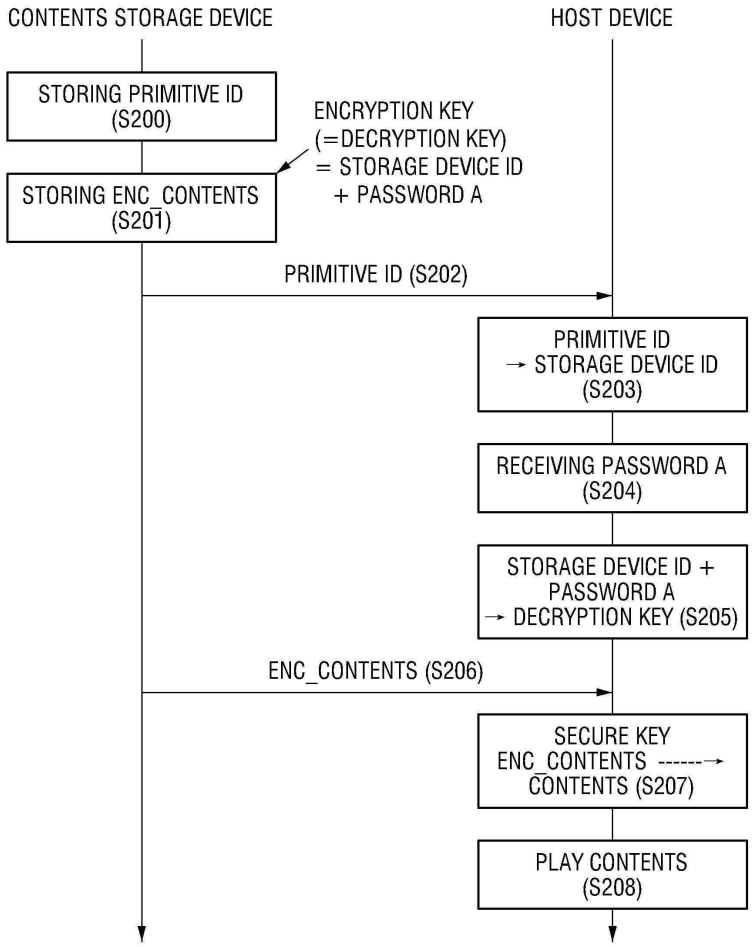
도면19


HOST DEVICE
S10
STORAGE DEVICE
ENCRYPTED MEMORY ID (S122)
ENCRYPTED MEMORY ID
→ MEMORY ID
(S124)
MEMORY ID
→ 2ND AUTH INFO
(S126)
GENERATE 1ST AUTH
INFO FROM MEMORY ID
(S128)
1ST AUTH INFO (S130)
1ST AUTH
INFO == 2ND AUTH
INFO (S132)
NO
YES
MEMORY ID
→ MEMORY DERIVED ID
(S136)
NOTICE AUTH
FAIL(S134)
A

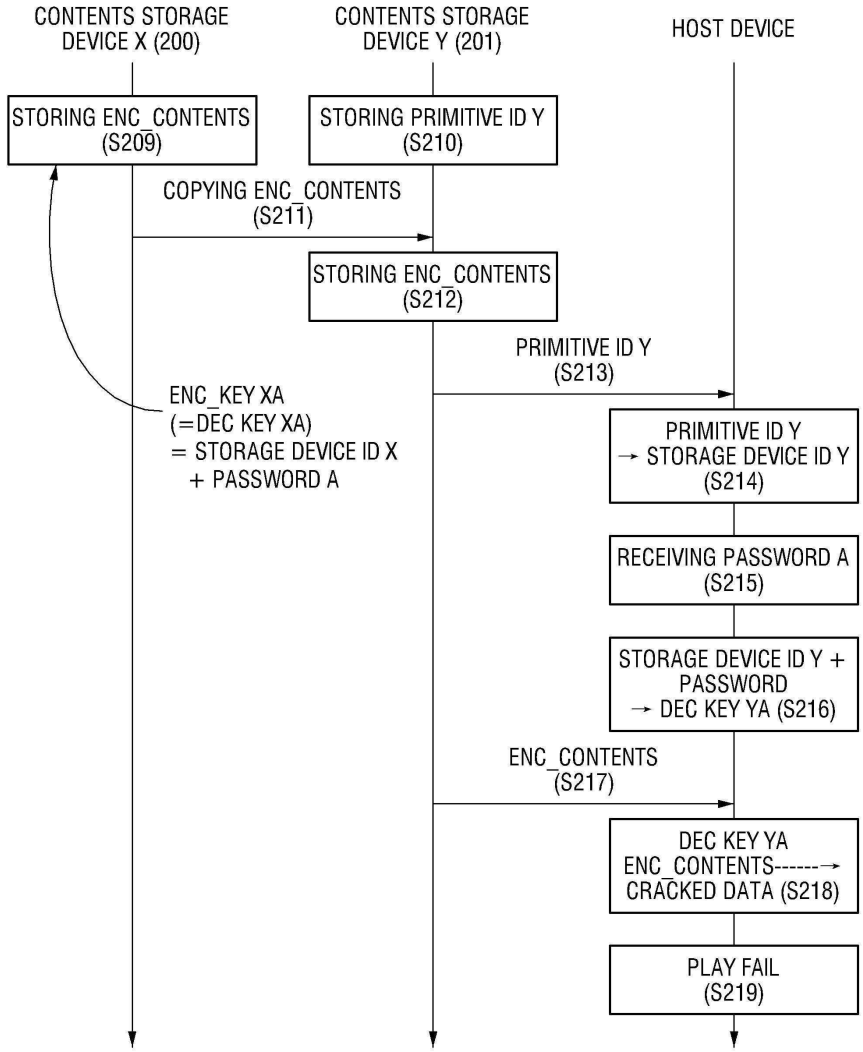
도면20


HOST DEVICE
S20
STORAGE DEVICE
3RD AUTH INFO(S140)
MUTUAL AUTHENTICATION PROCESS (S141)
AUTHENTICATION SUCCESS? (S142)
NO
YES
OBTAIN CONTROLLER ID from 3RD AUTH INFO (S148)
NOTICE AUTH FAIL(S144)
A

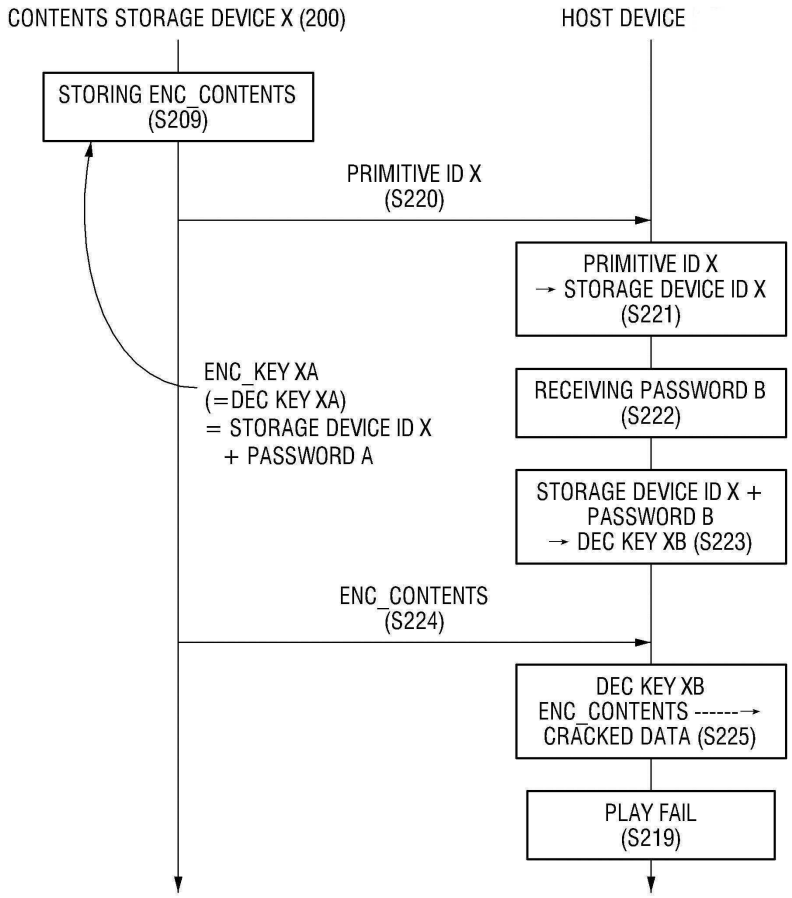
도면21


CONTENTS STORAGE DEVICE
HOST DEVICE
STORING PRIMITIVE ID (S200)
ENCRYPTION KEY (=DECRYPTION KEY) = STORAGE DEVICE ID + PASSWORD A
STORING ENC_CONTENTS (S201)
PRIMITIVE ID (S202)
PRIMITIVE ID → STORAGE DEVICE ID (S203)
RECEIVING PASSWORD A (S204)
STORAGE DEVICE ID + PASSWORD A → DECRYPTION KEY (S205)
ENC_CONTENTS (S206)
SECURE KEY ENC_CONTENTS ------→ CONTENTS (S207)
PLAY CONTENTS (S208)

도면22


CONTENTS STORAGE DEVICE X (200)
CONTENTS STORAGE DEVICE Y (201)
HOST DEVICE
STORING ENC_CONTENTS (S209)
STORING PRIMITIVE ID Y (S210)
COPYING ENC_CONTENTS (S211)
STORING ENC_CONTENTS (S212)
PRIMITIVE ID Y (S213)
ENC_KEY XA (=DEC KEY XA) = STORAGE DEVICE ID X + PASSWORD A
PRIMITIVE ID Y → STORAGE DEVICE ID Y (S214)
RECEIVING PASSWORD A (S215)
STORAGE DEVICE ID Y + PASSWORD → DEC KEY YA (S216)
ENC_CONTENTS (S217)
DEC KEY YA ENC_CONTENTS------→ CRACKED DATA (S218)
PLAY FAIL (S219)

도면23


CONTENTS STORAGE DEVICE X (200)
HOST DEVICE
STORING ENC_CONTENTS (S209)
PRIMITIVE ID X (S220)
PRIMITIVE ID X → STORAGE DEVICE ID X (S221)
ENC_KEY XA (=DEC KEY XA) = STORAGE DEVICE ID X + PASSWORD A
RECEIVING PASSWORD B (S222)
STORAGE DEVICE ID X + PASSWORD B → DEC KEY XB (S223)
ENC_CONTENTS (S224)
DEC KEY XB ENC_CONTENTS ------→ CRACKED DATA (S225)
PLAY FAIL (S219)