



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0103747
(43) 공개일자 2011년09월21일

(51) Int. Cl.

H04L 9/14 (2006.01) G06F 21/00 (2006.01)

G06F 9/06 (2006.01) G06F 15/16 (2006.01)

(21) 출원번호 10-2010-0022959

(22) 출원일자 2010년03월15일

심사청구일자 없음

(71) 출원인

삼성전자주식회사

경기도 수원시 영통구 매탄동 416

(72) 발명자

김호정

경기도 수원시 영통구 망포동 늘푸른벽산아파트 109-701

유인경

경기도 용인시 수지구 신봉동 LG신봉자이1차아파트 113-802

신재광

경기 안양시 동안구 범계동 목련우성아파트 707-505

(74) 대리인

리엔특허법인

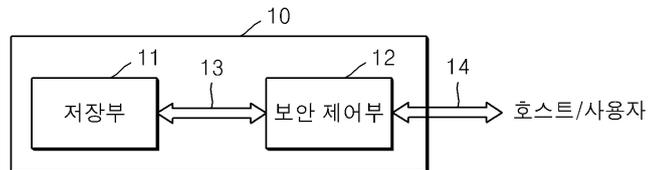
전체 청구항 수 : 총 25 항

(54) 보안 기능을 갖는 저장 장치 및 그 보안 방법

(57) 요약

본 발명은 저장 장치에 관한 것으로, 복수의 제1 배선들을 통해 전달되는 데이터를 저장하는 저장부; 및 암호화 키(key)에 따라 프로그램되는 복수의 비휘발성 메모리 소자들을 이용하여, 외부 장치에 연결된 복수의 제2 배선들의 각각과 상기 복수의 제1 배선들의 각각의 연결을 제어하는 보안 제어부를 포함한다.

대표도 - 도1



특허청구의 범위

청구항 1

복수의 제1 배선들을 통해 전달되는 데이터를 저장하는 저장부; 및

암호화 키(key)에 따라 프로그램되는 복수의 비휘발성 메모리 소자들을 이용하여, 외부 장치에 연결된 복수의 제2 배선들의 각각과 상기 복수의 제1 배선들의 각각의 연결을 제어하는 보안 제어부를 포함하는 저장 장치.

청구항 2

제1항에 있어서,

상기 보안 제어부는, 상기 암호화 키를 기초로 하여 상기 복수의 비휘발성 메모리 소자들을 프로그램하고, 프로그램된 상기 복수의 비휘발성 메모리 소자들에 의해 상기 복수의 제1 및 제2 배선들의 라우팅(routing)을 제어하여 상기 복수의 제1 배선들과 상기 복수의 제2 배선들을 일대일로 연결시키는 것을 특징으로 하는 저장 장치.

청구항 3

제1항에 있어서,

상기 보안 제어부는,

상기 암호화 키를 수신하여 키 수열(stream)을 생성하는 키 수열 생성부; 및

상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어하기 위하여, 상기 키 수열을 기초로 하여 상기 복수의 비휘발성 메모리 소자들에 대해 프로그램 동작을 수행하는 배선 연결 제어부를 더 포함하는 것을 특징으로 하는 저장 장치.

청구항 4

제3항에 있어서,

상기 보안 제어부는, 배선 연결부를 더 포함하고,

상기 배선 연결부는,

상기 복수의 제1 배선들;

상기 복수의 제2 배선들; 및

상기 복수의 제1 배선들과 상기 복수의 제2 배선들이 교차하는 영역들에 각각 배치되고, 상기 배선 연결 제어부에 의한 프로그램 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 스위칭하는 상기 복수의 비휘발성 메모리 소자들을 포함하는 것을 특징으로 하는 저장 장치.

청구항 5

제4항에 있어서,

상기 복수의 비휘발성 메모리 소자들은 저항형 메모리 소자 또는 플래시(Flash) 메모리 소자를 포함하는 것을 특징으로 하는 저장 장치.

청구항 6

제4항에 있어서,

상기 복수의 비휘발성 메모리 소자들은 '1'로 프로그램된 경우의 저항과 '0'으로 프로그램된 경우의 저항의 차이가 미리 설정된 값보다 큰 저항형 메모리 소자를 포함하는 것을 특징으로 하는 저장 장치.

청구항 7

제3항에 있어서,

상기 보안 제어부는, 배선 연결부를 더 포함하고,

상기 배선 연결부는,

상기 복수의 제1 배선들;

상기 복수의 제2 배선들; 및

상기 복수의 제1 배선들과 상기 복수의 제2 배선들이 교차하는 영역들에 각각 배치되는 복수의 스위칭부들을 포함하고,

상기 복수의 스위칭부들의 각각은,

스위치; 및

상기 배선 연결 제어부에 의해 프로그램되는 적어도 하나의 비휘발성 메모리 소자를 포함하고, 상기 스위치의 온/오프를 제어하는 스위치 제어부를 포함하는 것을 특징으로 하는 저장 장치.

청구항 8

제7항에 있어서,

상기 스위치 제어부는,

상기 적어도 하나의 비휘발성 메모리 소자에 프로그램된 논리 값을 읽어내서 저장하는 래치를 더 포함하는 것을 특징으로 하는 저장 장치.

청구항 9

제7항에 있어서,

상기 스위치 제어부는,

상기 암호화 키에 의해 상보적으로 프로그램되는 적어도 한 쌍의 비휘발성 메모리 소자에 프로그램된 논리 값을 읽어내서 저장하는 래치를 더 포함하는 것을 특징으로 하는 저장 장치.

청구항 10

제9항에 있어서,

상기 래치는,

전원 전압 단자에 연결되는 제1 풀업(pull up) 트랜지스터 및 상기 제1 풀업 트랜지스터와 직렬 연결된 제1 풀다운(pull down) 트랜지스터를 포함하는 제1 인버터;

상기 전원 전압 단자에 연결되는 제2 풀업 트랜지스터와 제2 풀다운 트랜지스터를 포함하고, 상기 제1 인버터에 교차 결합되는 제2 인버터; 및

등화 신호에 따라 상기 제1 풀다운 트랜지스터의 게이트와 상기 제2 풀다운 트랜지스터의 게이트의 사이를 연결시키는 등화부를 포함하는 것을 특징으로 하는 저장 장치.

청구항 11

제10항에 있어서,

상기 등화부는, 등화 신호가 활성화되면 턴온되어 상기 제1 풀다운 트랜지스터의 게이트와 상기 제2 풀다운 트랜지스터의 게이트를 연결시키는 트랜지스터를 포함하는 것을 특징으로 하는 저장 장치.

청구항 12

제10항에 있어서,

상기 적어도 한 쌍의 비휘발성 메모리 소자는,

상기 제1 풀다운 트랜지스터의 소스와 접지 전압 단자 사이에 연결되는 제1 비휘발성 메모리 소자; 및

상기 제2 풀다운 트랜지스터의 소스와 상기 접지 전압 단자 사이에 연결되는 제2 비휘발성 메모리 소자들을 포함하는 것을 특징으로 하는 저장 장치.

청구항 13

제7항에 있어서,

상기 적어도 하나의 비휘발성 메모리 소자는 저항형 메모리 소자, 자기 메모리 소자 및 플래시 메모리 소자 중 하나를 포함하는 것을 특징으로 하는 저장 장치.

청구항 14

제1항에 있어서,

상기 보안 제어부는, 상기 암호화 키에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어함으로써, 상기 외부 장치로부터 입력된 원본(original) 데이터를 보안 데이터로 변경하여 상기 저장부에 제공하고, 상기 저장부에 저장된 상기 보안 데이터를 상기 원본 데이터로 변경하여 상기 외부 장치에 제공하는 것을 특징으로 하는 저장 장치.

청구항 15

제1항에 있어서,

상기 보안 제어부는, 상기 암호화 키에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어함으로써, 상기 외부 장치로부터 입력된 보안 데이터를 원본 데이터로 변경하여 상기 저장부에 제공하고, 상기 저장부에 저장된 상기 원본 데이터를 상기 보안 데이터로 변경하여 상기 외부 장치에 제공하는 것을 특징으로 하는 저장 장치.

청구항 16

제1항에 있어서,

상기 복수의 제1 배선들과 상기 복수의 제2 배선들은 매트릭스 형태로 배열된 것을 특징으로 하는 저장 장치.

청구항 17

제1항 내지 제16항 중 어느 한 청구항의 저장 장치; 및

상기 저장 장치에 액세스 가능한 프로세서(processor)를 포함하는 전자 장치.

청구항 18

제17항에 있어서,

상기 저장 장치는, 자기 저장 매체, 광학 저장 매체 및 반도체 저장 매체 중 적어도 하나인 것을 특징으로 하는 전자 장치.

청구항 19

제1항 내지 제16항 중 어느 한 청구항의 저장 장치; 및

네트워크를 통해, 클라이언트(client)의 요청에 따라 상기 저장 장치로부터 데이터를 제공하거나 상기 저장 장치에 데이터를 저장하는 서버(server)를 포함하는 스토리지 서버.

청구항 20

제1항 내지 제16항 중 어느 한 청구항의 저장 장치; 및

네트워크를 통해 상기 저장 장치를 적어도 하나의 사용자와 연결시킬 수 있는 네트워크 인터페이스를 포함하는 네트워크 스토리지.

청구항 21

데이터를 저장하는 저장부 및 상기 데이터에 대해 보안 기능을 제공하는 보안 제어부를 포함하는 저장 장치의 보안 방법으로서,

상기 저장 장치에 제공되는 암호화 키에 따라 상기 보안 제어부에 포함된 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계; 및

상기 복수의 비휘발성 메모리 소자들 각각의 프로그램 결과에 따라, 상기 저장부에 연결되는 복수의 제1 배선들의 각각과 외부 장치에 연결되는 복수의 제2 배선들의 각각의 사이의 연결을 제어하는 단계를 포함하는 저장 장치의 보안 방법.

청구항 22

제21항에 있어서,

상기 암호화 키를 수신하여 키 수열을 생성하는 단계를 더 포함하고,

상기 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계는,

상기 키 수열을 기초로 하여 상기 복수의 비휘발성 메모리 소자들의 각각에 대해 프로그램 동작을 수행하는 것을 특징으로 하는 저장 장치의 보안 방법.

청구항 23

제21항에 있어서,

상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어하는 단계는,

상기 복수의 비휘발성 메모리 소자들 각각의 프로그램 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각을 일대일로 연결시키는 것을 특징으로 하는 저장 장치의 보안 방법.

청구항 24

제21항에 있어서,

상기 암호화 키가 변경되는 경우 변경된 암호화 키에 따라 상기 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계를 더 포함하고,

상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 연결을 제어하는 단계는,

상기 변경된 암호화 키에 따라 상기 복수의 비휘발성 메모리 소자들이 프로그래밍된 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 변경하는 것을 특징으로 하는 저장 장치의 보안 방법.

청구항 25

제21항에 있어서,

상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결에 따라 상기 데이터를 상기 저장부 또는 외부 장치에 전달하는 단계를 더 포함하는 것을 특징으로 하는 저장 장치의 보안 방법.

명세서

기술분야

[0001] 본 발명은 저장 장치에 관한 것으로서, 더욱 상세하게는 보안 기능을 갖는 저장 장치 및 그 보안 방법에 관한 것이다.

배경기술

[0002] 데이터를 저장하는 저장 장치로는 자기 디스크(magnetic disk), 광 디스크(optical disk), 반도체 메모리 등이 있다. 이러한 저장 장치에 저장된 데이터를 보호하기 위해서 다양한 보안 프로그램들이 개발되고 있으나, 이러한 보안 프로그램들을 적용하는 경우에 많은 비용이 들고, 구성이 복잡해짐에 따라 저장 장치의 성능이 저하될

수 있다.

발명의 내용

해결하려는 과제

[0003] 본 발명이 해결하고자 하는 과제는 비휘발성 메모리 소자를 이용하여 적은 비용 및 적은 면적으로, 메모리나 스토리지와 같은 저장부에 저장된 데이터에 대하여 고성능의 보안 기능을 제공할 수 있는 저장 장치, 상기 저장 장치를 포함하는 전자 장치, 상기 저장 장치를 포함하는 스토리지 서버, 상기 저장 장치를 포함하는 네트워크 스토리지 및 상기 저장 장치의 보안 방법을 제공하는데 있다.

과제의 해결 수단

[0004] 상기 과제를 해결하기 위한 본 발명의 일 실시예에 따른 저장 장치는, 복수의 제1 배선들을 통해 전달되는 데이터를 저장하는 저장부; 및 암호화 키(key)에 따라 프로그램되는 복수의 비휘발성 메모리 소자들을 이용하여, 외부 장치에 연결된 복수의 제2 배선들의 각각과 상기 복수의 제1 배선들의 각각의 연결을 제어하는 보안 제어부를 포함한다.

[0005] 일부 실시예에 있어서, 상기 보안 제어부는, 상기 암호화 키를 기초로 하여 상기 복수의 비휘발성 메모리 소자들을 프로그램하고, 프로그램된 상기 복수의 비휘발성 메모리 소자들에 의해 상기 복수의 제1 및 제2 배선들의 라우팅(routing)을 제어하여 상기 복수의 제1 배선들과 상기 복수의 제2 배선들을 일대일로 연결시킬 수 있다.

[0006] 일부 실시예에 있어서, 상기 보안 제어부는, 상기 암호화 키를 수신하여 키 수열(stream)을 생성하는 키 수열 생성부; 및 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어하기 위하여, 상기 키 수열을 기초로 하여 상기 복수의 비휘발성 메모리 소자들에 대해 프로그램 동작을 수행하는 배선 연결 제어부를 더 포함할 수 있다.

[0007] 일부 실시예에 있어서, 상기 보안 제어부는, 배선 연결부를 더 포함하고, 상기 배선 연결부는, 상기 복수의 제1 배선들; 상기 복수의 제2 배선들; 및 상기 복수의 제1 배선들과 상기 복수의 제2 배선들이 교차하는 영역들에 각각 배치되고, 상기 배선 연결 제어부에 의한 프로그램 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 스위칭하는 상기 복수의 비휘발성 메모리 소자들을 포함할 수 있다. 상기 복수의 비휘발성 메모리 소자들은 저항형 메모리 소자 또는 플래시(Flash) 메모리 소자를 포함할 수 있다. 일부 실시예에 있어서, 상기 복수의 비휘발성 메모리 소자들은 '1'로 프로그램된 경우의 저항과 '0'으로 프로그램된 경우의 저항의 차이가 미리 설정된 값보다 큰 저항형 메모리 소자를 포함할 수 있다.

[0008] 일부 실시예에 있어서, 상기 보안 제어부는, 배선 연결부를 더 포함하고, 상기 배선 연결부는, 상기 복수의 제1 배선들; 상기 복수의 제2 배선들; 및 상기 복수의 제1 배선들과 상기 복수의 제2 배선들이 교차하는 영역들에 각각 배치되는 복수의 스위칭부들을 포함하고, 상기 복수의 스위칭부들의 각각은, 스위치; 및 상기 배선 연결 제어부에 의해 프로그램되는 적어도 하나의 비휘발성 메모리 소자를 포함하고, 상기 스위치의 온/오프를 제어하는 스위치 제어부를 포함할 수 있다. 일부 실시예에 있어서, 상기 스위치 제어부는, 상기 적어도 하나의 비휘발성 메모리 소자에 프로그램된 논리 값을 읽어내서 저장하는 래치를 더 포함할 수 있다. 일부 실시예에 있어서, 상기 스위치 제어부는, 상기 암호화 키에 의해 상보적으로 프로그램되는 적어도 한 쌍의 비휘발성 메모리 소자에 프로그램된 논리 값을 읽어내서 저장하는 래치를 더 포함할 수 있다.

[0009] 상기 래치는, 전원 전압 단자에 연결되는 제1 풀업(pull up) 트랜지스터 및 상기 제1 풀업 트랜지스터와 직렬 연결된 제1 풀다운(pull down) 트랜지스터를 포함하는 제1 인버터; 상기 전원 전압 단자에 연결되는 제2 풀업 트랜지스터와 제2 풀다운 트랜지스터를 포함하고, 상기 제1 인버터에 교차 결합되는 제2 인버터; 및 등화 신호에 따라 상기 제1 풀다운 트랜지스터의 게이트와 상기 제2 풀다운 트랜지스터의 게이트의 사이를 연결시키는 등화부를 포함할 수 있다. 상기 등화부는, 등화 신호가 활성화되면 턴온되어 상기 제1 풀다운 트랜지스터의 게이트와 상기 제2 풀다운 트랜지스터의 게이트를 연결시키는 트랜지스터를 포함할 수 있다. 상기 적어도 한 쌍의 비휘발성 메모리 소자는, 상기 제1 풀다운 트랜지스터의 소스와 접지 전압 단자 사이에 연결되는 제1 비휘발성 메모리 소자; 및 상기 제2 풀다운 트랜지스터의 소스와 상기 접지 전압 단자 사이에 연결되는 제2 비휘발성 메모리 소자들을 포함할 수 있다. 상기 적어도 하나의 비휘발성 메모리 소자는 저항형 메모리 소자, 자기 메모리 소자 및 플래시 메모리 소자 중 하나를 포함할 수 있다.

[0010] 일부 실시예에 있어서, 상기 보안 제어부는, 상기 암호화 키에 따라 상기 복수의 제1 배선들의 각각과 상기 복

수의 제2 배선들의 각각의 사이의 연결을 제어함으로써, 상기 외부 장치로부터 입력된 원본(original) 데이터를 보안 데이터로 변경하여 상기 저장부에 제공하고, 상기 저장부에 저장된 상기 보안 데이터를 상기 원본 데이터로 변경하여 상기 외부 장치에 제공할 수 있다.

- [0011] 일부 실시예에 있어서, 상기 보안 제어부는, 상기 암호화 키에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어함으로써, 상기 외부 장치로부터 입력된 보안 데이터를 원본 데이터로 변경하여 상기 저장부에 제공하고, 상기 저장부에 저장된 상기 원본 데이터를 상기 보안 데이터로 변경하여 상기 외부 장치에 제공할 수 있다.
- [0012] 일부 실시예에 있어서, 상기 복수의 제1 배선들과 상기 복수의 제2 배선들은 매트릭스 형태로 배열될 수 있다.
- [0013] 또한, 상기 과제를 해결하기 위한 본 발명의 일 실시예에 따른 전자 장치는, 상술한 저장 장치; 및 상기 저장 장치에 액세스 가능한 프로세서(processor)를 포함한다. 일부 실시예에 있어서, 상기 전자 장치는 자기 저장 매체, 광학 저장 매체 및 반도체 저장 매체 중 적어도 하나일 수 있다.
- [0014] 또한, 상기 과제를 해결하기 위한 본 발명의 일 실시예에 따른 스토리지 서버는, 상술한 저장 장치; 및 네트워크를 통해, 클라이언트(client)의 요청에 따라 상기 저장 장치로부터 데이터를 제공하거나 상기 저장 장치에 데이터를 저장하는 서버(server)를 포함한다.
- [0015] 또한, 상기 과제를 해결하기 위한 본 발명의 일 실시예에 따른 네트워크 스토리지는, 상술한 저장 장치; 및 네트워크를 통해 상기 저장 장치를 적어도 하나의 사용자와 연결시킬 수 있는 네트워크 인터페이스를 포함한다.
- [0016] 또한, 상기 과제를 해결하기 위한 본 발명의 일 실시예에 따른 저장 장치의 보안 방법은, 데이터를 저장하는 저장부 및 상기 데이터에 대해 보안 기능을 제공하는 보안 제어부를 포함하는 저장 장치의 보안 방법으로서, 상기 저장 장치에 제공되는 암호화 키에 따라 상기 보안 제어부에 포함된 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계; 및 상기 복수의 비휘발성 메모리 소자들 각각의 프로그램 결과에 따라, 상기 저장부에 연결되는 복수의 제1 배선들의 각각과 외부 장치에 연결되는 복수의 제2 배선들의 각각의 사이의 연결을 제어하는 단계를 포함한다.
- [0017] 일부 실시예에 있어서, 상기 보안 방법은 상기 암호화 키를 수신하여 키 수열을 생성하는 단계를 더 포함하고, 상기 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계는, 상기 키 수열을 기초로 하여 상기 복수의 비휘발성 메모리 소자들의 각각에 대해 프로그램 동작을 수행할 수 있다.
- [0018] 일부 실시예에 있어서, 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 제어하는 단계는, 상기 복수의 비휘발성 메모리 소자들 각각의 프로그램 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각을 일대일로 연결시킬 수 있다.
- [0019] 일부 실시예에 있어서, 상기 보안 방법은 상기 암호화 키가 변경되는 경우 변경된 암호화 키에 따라 상기 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계를 더 포함하고, 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 연결을 제어하는 단계는, 상기 변경된 암호화 키에 따라 상기 복수의 비휘발성 메모리 소자들이 프로그램된 결과에 따라 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결을 변경할 수 있다.
- [0020] 일부 실시예에 있어서, 상기 보안 방법은 상기 복수의 제1 배선들의 각각과 상기 복수의 제2 배선들의 각각의 사이의 연결에 따라 상기 데이터를 상기 저장부 또는 외부 장치에 전달하는 단계를 더 포함할 수 있다.

발명의 효과

- [0021] 본 발명에 따르면, 저장 장치는 암호화 키에 따라 프로그램되는 비휘발성 메모리 소자들을 이용하여 저장부에 연결되는 내부 배선들의 각각과 외부 장치에 연결되는 외부 배선들의 각각의 연결을 제어하는 보안 제어부를 포함함으로써, 저장부에 저장된 데이터에 대하여 보안 기능을 제공할 수 있다. 구체적으로, 보안 제어부는 암호화 키에 따라 내부 배선들과 외부 배선들의 라우팅을 변경하여 내부 배선들과 외부 배선들을 일대일로 연결시킴으로써, 저장 장치는 외부 장치에서 입력되는 원본 데이터를 보안 데이터로 변경하여 저장할 수 있고, 적절한 암호화 키가 제공되면 보안 데이터를 원본 데이터로 변경하여 제공할 수 있다.
- [0022] 또한, 본 발명에 따르면, 내부 배선들과 외부 배선들이 교차하는 영역들에 각각 비휘발성 메모리 소자를 배치함으로써, 면적 증가를 최소화하면서 내부 배선들과 외부 배선들 사이의 연결을 효과적으로 제어할 수 있다.
- [0023] 또한, 본 발명에 따르면, 내부 배선들과 외부 배선들이 교차하는 영역들에 각각 스위치 및 스위치 제어부를 배

치하고, 스위치 제어부는 비휘발성 메모리 소자를 포함함으로써, 배선들 간의 연결을 원하지 않는 경우에는 스위치를 오픈시켜서 배선들 사이의 누설 전류를 제거할 수 있다.

[0024] 또한, 본 발명에 따르면, 별도의 암호화 프로그램을 적용하지 않고서도 외부 장치와 저장 장치 사이의 배선들 간의 라우팅을 변경함으로써 데이터에 대한 보안을 제공하므로, 실시간으로 데이터에 대해 암호화 또는 복호화를 수행할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 저장 장치를 개략적으로 나타내는 블록도이다.

도 2는 도 1의 저장 장치에 포함된 보안 제어부를 상세히 나타내는 블록도이다.

도 3은 도 2의 보안 제어부에 포함된 배선 연결부를 상세히 나타내는 회로도이다.

도 4는 도 3의 배선 연결부에 포함된 스위칭부의 일 예를 나타내는 회로도이다.

도 5는 도 3의 배선 연결부에 포함된 스위칭부의 다른 예를 나타내는 회로도이다.

도 6은 본 발명의 일 실시예에 따른 전자 장치를 개략적으로 나타내는 블록도이다.

도 7은 도 6의 전자 장치에 포함된 RAM의 일 예를 나타내는 블록도이다.

도 8은 도 6의 전자 장치에 포함된 스토리지의 일 예를 나타내는 블록도이다.

도 9는 본 발명의 일 실시예에 따른 서버-클라이언트 시스템을 개략적으로 나타내는 블록도이다.

도 10은 본 발명의 일 실시예에 따른 네트워크 스토리지를 개략적으로 나타내는 블록도이다.

도 11은 본 발명의 일 실시예에 따른 저장 장치의 보안 방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 첨부한 도면을 참조하여 본 발명에 따른 바람직한 실시예를 설명함으로써 본 발명을 상세하게 설명한다. 그러나 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예는 본 발명의 개시가 완전하도록 하며, 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려 주기 위해 제공되는 것이다. 도면에서 구성 요소들은 설명의 편의를 위하여 그 크기가 과장될 수 있다.

[0027] 도 1은 본 발명의 일 실시예에 따른 저장 장치를 개략적으로 나타내는 블록도이다.

[0028] 도 1을 참조하면, 저장 장치(10)는 저장부(11) 및 보안 제어부(12)를 포함할 수 있고, 저장부(11)와 보안 제어부(12)는 내부 데이터 버스(13)를 통해 연결될 수 있다. 또한, 저장 장치(10)는 외부 데이터 인터페이스(14)를 통해 호스트(host) 또는 사용자와 같은 외부 장치에 연결됨으로써, 저장부(11)에 저장된 데이터를 사용자에게 제공하거나, 사용자로부터 제공된 데이터를 저장부(11)에 저장할 수 있다. 여기서, 호스트는 개인용 컴퓨터(PC), 워크 스테이션(work station), 데스크톱 컴퓨터, 랩탑 컴퓨터 또는 개인용 디지털 단말기(PDA) 등 저장 장치(10)에 저장된 데이터에 접근할 수 있는 일체의 단말기를 포함할 수 있다.

[0029] 본 발명의 일 실시예에서 저장 장치(10)는 메인 메모리, USB 플래시 드라이브(USB flash drive), 외장 하드 드라이브, SSD(solid state drive), 스마트 미디어(smart media, SM) 카드, 메모리 스틱, SD(secure digital) 카드, 멀티 미디어 카드(multi media card, MMC), CF(compact flash) 카드, MS 카드, xD 픽처(xD-Picture) 카드 또는 스토리지(storage) 등일 수 있으나, 이에 제한되지 않는다.

[0030] 저장부(11)는 명령어나 데이터를 저장하는데, 예를 들어, 서적 데이터, 영상 데이터 또는 오디오 데이터와 같은 미디어 콘텐츠를 저장할 수 있다. 여기서, 저장부(11)는 자기 저장 매체(예를 들어, 플로피 디스크 또는 하드 디스크 드라이브(HDD)), 광학 저장 매체(예를 들어, 레이저 디스크, 콤팩트 디스크, 광자기 디스크, MD, CD-ROM, DVD, 블루레이 디스크) 또는 반도체 저장 매체(예를 들어, DRAM(dynamic random access memory), SRAM(static RAM)과 같은 휘발성 메모리 또는 플래시(flash) 메모리, MRAM(magnetic RAM), RRAM(resistive RAM), PRAM(phase change RAM), NFGM(nano floating gate memory), PoRAM(polymer RAM), ReRAM(Ferroelectric RAM), EEPROM(electrically erasable programmable read only memory) 등과 같은 비휘발성 메모리)와 같은 대용량 저장부를 포함할 수 있다.

[0031] 보안 제어부(12)는 내부 데이터 버스(13)를 통해 저장부(11)에 연결되는 복수의 내부 배선들과 외부 데이터 인

터페이스(14)를 통해 호스트 또는 사용자와 같은 외부 장치에 연결되는 복수의 외부 배선들 사이의 라우팅(routing)을 제어함으로써, 저장부(11)에 저장된 데이터에 대하여 보안 기능을 제공할 수 있다. 구체적으로, 보안 제어부(12)는 암호화 키(key)에 따라 프로그램되는 복수의 비휘발성 메모리 소자들을 포함할 수 있다. 이때, 복수의 비휘발성 메모리 소자들은 프로그램 결과에 따라 각각 스위치로 동작할 수 있는데, 예를 들어, '1'로 프로그램된 비휘발성 메모리 소자는 '온' 상태가 되고, '0'으로 프로그램된 비휘발성 메모리 소자는 '오프' 상태가 될 수 있다.

[0032] 보다 상세하게는, 보안 제어부(12)는 복수의 비휘발성 메모리 소자들을 포함하고 복수의 비휘발성 메모리 소자들의 프로그램 결과에 따른 재설정 가능 논리 소자(reconfigurable logic device)로 구현될 수 있는데, 이로써 암호화 키에 따라 복수의 내부 배선들과 복수의 외부 배선들 사이의 라우팅이 변경될 수 있다. 구체적으로, 보안 제어부(12)는 암호화 키에 따라 복수의 내부 배선들과 복수의 외부 배선들의 라우팅을 변경할 수 있으므로, 외부 장치에서 입력되는 원본 데이터는 보안 데이터로 변경되어 저장부(11)에 저장될 수 있다. 정당한 권한을 가진 사용자, 즉, 암호화 키를 가진 사용자가 저장 장치(10)에 액세스하는 경우에, 해당 암호화 키에 따라 복수의 내부 배선들과 복수의 외부 배선들의 라우팅을 변경할 수 있으므로, 저장부(11)에 저장된 보안 데이터는 원본 데이터로 변경되어 사용자에게 제공될 수 있다. 이때, 저장 장치(10)의 저장부(11)에는 보안 데이터가 저장되어 있으므로, 정당한 권한이 없는 사용자, 즉, 암호화 키를 가지지 않은 사용자가 저장 장치(10)에 액세스 하는 경우에는 원본 데이터를 획득할 수 없다.

[0033] 도 2는 도 1의 저장 장치에 포함된 보안 제어부를 상세히 나타내는 블록도이다.

[0034] 도 2를 참조하면, 보안 제어부(12)는 키 수열(stream) 생성부(121), 배선 연결 제어부(122) 및 배선 연결부(123)를 포함할 수 있다. 이하에서는, 보안 제어부(12)에 포함된 각 구성 요소들에 대하여 구체적으로 상술하기로 한다.

[0035] 키 수열 생성부(121)는 저장 장치(10)에 제공되는 암호화 키를 수신하고, 수신된 암호화 키를 기초로 하여 키 수열을 생성할 수 있다. 저장 장치(10)에 제공되는 암호화 키가 변경되는 경우에는, 키 수열 생성부(121)는 다른 키 수열을 생성할 수 있다. 예를 들어, 키 수열 생성부(121)는 해쉬 함수(hash function)를 사용하여 키 수열을 생성할 수 있다. 그러나, 키 수열을 생성하는데 사용되는 함수는 반드시 이에 한정되는 것은 아니며, 다양한 암호화 함수가 적용될 수 있다. 한편, 생성된 키 수열은 고정적인 것이 아니라, 주기적으로 갱신됨으로써, 보다 높은 레벨의 보안 기능을 제공할 수 있다.

[0036] 배선 연결 제어부(122)는 키 수열 생성부(121)에서 생성된 키 수열을 기초로 하여 복수의 비휘발성 메모리 소자들 각각을 '1' 또는 '0'으로 프로그램할 수 있다. 저장 장치(10)에 제공되는 암호화 키가 변경되는 경우에는, 배선 연결 제어부(122)는 복수의 비휘발성 메모리 소자들 각각에 대해 다시 프로그램할 수 있다. 이에 따라, 복수의 사용자가 서로 다른 암호화 키를 가지고 저장 장치(10)에 액세스할 때, 저장부(11)에서 각 사용자들이 액세스할 수 있는 영역은 서로 다를 수 있고, 동일한 영역에 대해서 액세스하더라도 획득 가능한 데이터는 서로 다를 수 있다. 한편, 배선 연결 제어부(122)는 복수의 비휘발성 메모리 소자들 전부에 대해 주기적으로 '1' 또는 '0'으로 프로그램하거나, 복수의 비휘발성 메모리 소자들 전부에 저장된 데이터를 소거함으로써, 저장 장치(10)의 보안 기능을 강화할 수 있다.

[0037] 배선 연결부(123)는 복수의 비휘발성 메모리 소자들을 포함하고, 복수의 비휘발성 메모리 소자들이 배선 연결 제어부(122)에 의해 프로그램된 결과에 따라 복수의 내부 배선들과 복수의 외부 배선들을 일대일로 연결시킨다. 배선 연결부(123)의 구성에 대한 상세한 설명은 도 3을 참조하여 후술하기로 하다.

[0038] 본 발명의 다른 실시예에 따르면, 보안 제어부(12)는 암호화부(미도시)를 더 포함할 수도 있다. 이때, 암호화부는 배선 연결부(123)와 내부 데이터 버스(13)의 사이 또는 배선 연결부(123)와 외부 데이터 인터페이스(14)의 사이에 배치될 수 있다. 암호화부가 배선 연결부(123)와 내부 데이터 버스(13)의 사이에 배치되는 경우에는, 암호화부는 배선 연결부(123)에서 제공되는 데이터에 대하여 암호화 알고리즘을 적용하여 암호화된 데이터를 저장부(11)에 제공함으로써, 저장 장치(10)에 입력되는 데이터에 대한 보안을 더욱 강화할 수 있다. 한편, 암호화부가 배선 연결부(123)와 외부 데이터 인터페이스(14)의 사이에 배치되는 경우에는, 암호화부는 배선 연결부(123)에서 제공되는 데이터에 대하여 암호화 알고리즘을 적용하여 암호화된 데이터를 호스트 또는 사용자에게 제공함으로써, 저장 장치(10)로부터 출력되는 데이터에 대한 보안을 더욱 강화할 수 있다.

[0039] 도 3은 도 2의 보안 제어부에 포함된 배선 연결부를 상세히 나타내는 회로도이다.

[0040] 도 3을 참조하면, 배선 연결부(123)는 복수의 내부 배선들(W11 내지 W19), 복수의 외부 배선들(W21 내지 W29)

및 복수의 스위칭부들(SW11 내지 SW99)을 포함할 수 있다. 도 3에서는 편의상 9개의 내부 배선들과 9개의 외부 배선들을 도시하였으나, 내부 배선들과 외부 배선들의 개수는 실시예에 따라 자유롭게 변경될 수 있다.

[0041] 복수의 내부 배선들(W11 내지 W19)의 각각은 내부 데이터 패드들(P11 내지 P19)의 각각에 연결되고, 내부 데이터 패드들(P11 내지 P19)은 내부 데이터 버스(13)에 연결된다. 복수의 외부 배선들(W21 내지 W29)의 각각은 외부 데이터 패드들(P21 내지 P29)의 각각에 연결되고, 외부 데이터 패드들(P21 내지 P29)은 외부 데이터 인터페이스(14)에 연결된다. 본 실시예에서, 복수의 내부 배선들(W11 내지 W19)과 복수의 외부 배선들(W21 내지 W29)은 매트릭스(matrix) 형태로 배열될 수 있는데, 복수의 내부 배선들(W11 내지 W19)과 복수의 외부 배선들(W21 내지 W29)의 배치 관계는 이에 한정되지 않는다.

[0042] 복수의 스위칭부들(SW11 내지 SW99)은 복수의 내부 배선들(W11 내지 W19)과 복수의 외부 배선들(W21 내지 W29)이 교차하는 영역들에 각각 배치된다. 복수의 스위칭부들(SW11 내지 SW99)의 각각은 배선 연결 제어부(122)에 의해 '1' 또는 '0'으로 프로그램되는 적어도 하나의 비휘발성 메모리 소자를 포함하여 온/오프되고, 이에 따라, 복수의 내부 배선들(W11 내지 W19)의 각각과 복수의 외부 배선들(W21 내지 W29)의 각각을 일대일로 연결시킨다. 구체적으로, 제1 외부 배선(W21)에 연결되는 복수의 스위칭부들(SW11 내지 SW19) 중 하나는 '온'되고 나머지는 '오프'된다. 이로써, 제1 외부 배선(W21)은 '온'된 스위칭부에 연결된 내부 배선(W1)과 일대일로 연결된다.

[0043] 예를 들어, 복수의 스위칭부들(SW11 내지 SW99) 중 아홉 개의 스위칭부들(SW13, SW25, SW37, SW49, SW51, SW62, SW74, SW86, SW98)이 '온'되고, 나머지 스위칭부들은 '오프'된다고 하자. 이때, 제1 외부 배선(W21)에 연결된 복수의 스위칭부들 중 세 번째 스위칭부(SW13)가 '온'되었으므로, 제1 외부 배선(W21)은 제3 내부 배선(W13)에 연결된다. 또한, 제2 외부 배선(W22)에 연결된 복수의 스위칭부들 중 다섯 번째 스위칭부(SW25)가 '온'되었으므로, 제2 외부 배선(W22)은 제5 내부 배선(W15)에 연결된다. 또한, 제3 외부 배선(W23)에 연결되는 복수의 스위칭부들 중 일곱 번째 스위칭부(SW37)가 '온'되었으므로, 제3 외부 배선(W23)은 제7 내부 배선(W17)에 연결된다. 또한, 제4 외부 배선(W24)에 연결되는 복수의 스위칭부들 중 아홉 번째 스위칭부(SW49)가 '온'되었으므로, 제4 외부 배선(W24)은 제9 내부 배선(W19)에 연결된다. 또한, 제5 외부 배선(W25)에 연결되는 복수의 스위칭부들 중 첫 번째 스위칭부(SW51)가 '온'되었으므로, 제5 외부 배선(W25)은 제1 내부 배선(W11)에 연결된다. 또한, 제6 외부 배선(W26)에 연결되는 복수의 스위칭부들 중 두 번째 스위칭부(SW62)가 '온'되었으므로, 제6 외부 배선(W26)은 제2 내부 배선(W12)에 연결된다. 또한, 제7 외부 배선(W27)에 연결되는 복수의 스위칭부들 중 네 번째 스위칭부(SW74)가 '온'되었으므로, 제7 외부 배선(W27)은 제4 내부 배선(W14)에 연결된다. 또한, 제8 외부 배선(W28)에 연결되는 복수의 스위칭부들 중 여섯 번째 스위칭부(SW86)가 '온'되었으므로, 제8 외부 배선(W28)은 제6 내부 배선(W16)에 연결된다. 또한, 제9 외부 배선(W29)에 연결되는 복수의 스위칭부들 중 여덟 번째 스위칭부(SW98)가 '온'되었으므로, 제9 외부 배선(W29)은 제8 내부 배선(W18)에 연결된다. 따라서, 제1 내지 제9 외부 데이터 패드들(P21 내지 P29)에 순차적으로 a, b, c, d, e, f, g, h, i의 데이터가 입력되는 경우에, 제1 내지 제9 내부 데이터 패드들(P11 내지 P19)에는 순차적으로 e, f, a, g, b, h, c, i, d의 데이터가 출력된다.

[0044] 이와 같이, 본 실시예에 따르면, 호스트 또는 사용자로부터 원본 데이터(예를 들어, abcdefghi)가 입력될 때에, 보안 제어부(12)는 암호화 키에 따라 복수의 비휘발성 메모리 소자들을 프로그램하여 복수의 스위칭부들의 온/오프를 제어함으로써 저장부(11)에 보안 데이터(예를 들어, efagbhcid)를 제공할 수 있다. 따라서, 정당한 권한을 가지지 않은 사용자가 저장 장치(10)에 액세스하더라도 저장부(11)에는 원본 데이터가 아닌 보안 데이터가 저장되어 있으므로, 정당한 권한을 가지지 않은 사용자는 원하는 데이터를 획득할 수 없게 된다.

[0045] 또한, 본 실시예에 따르면, 별도의 암호화 프로그램을 적용하지 않고서도 외부 장치와 저장 장치(10) 사이의 배선들 간의 라우팅을 변경함으로써 데이터에 대한 보안을 제공하므로, 실시간으로 데이터에 대해 암호화 또는 복호화를 수행할 수 있다.

[0046] 한편, 사용자가 저장부(11)에 저장된 데이터를 독출하고자 하는 경우, 사용자는 저장부(11)에 데이터를 저장했을 때와 동일한 암호화 키를 이용하여 복수의 내부 배선들과 복수의 외부 배선들 사이의 라우팅을 제어함으로써, 저장부(11)에 저장된 보안 데이터를 다시 원본 데이터로 변경하여 독출할 수 있다.

[0047] 여러 명의 사용자들이 저장 장치(10)를 이용하는 경우 사용자들은 서로 다른 암호화 키를 가질 수 있으므로, 이때, 각 사용자는 해당 암호화 키를 이용하여 복수의 내부 배선들과 복수의 외부 배선들 사이의 라우팅을 제어할 수 있다. 따라서, 동일한 저장 장치(10)에 액세스 하더라도, 각 사용자가 저장부(11)로부터 획득하는 데이터는 서로 다를 수 있다.

- [0048] 도 4는 도 3의 배선 연결부에 포함된 스위칭부의 일 예를 나타내는 회로도이다.
- [0049] 도 4를 참조하면, 스위칭부(SW1)는 내부 배선(W1)과 외부 배선(W2)이 교차하는 영역에 배치되는 비휘발성 메모리 소자(NV)를 포함할 수 있다. 여기서, 내부 배선(W1)은 저장부(11)에 연결되는 배선들 중 하나이고, 외부 배선(W2)은 외부 장치에 연결되는 배선들 중 하나이다. 예를 들어, 비휘발성 메모리 소자(NV)는 저항형 메모리 소자 또는 플래시 메모리 소자일 수 있다. 이하에서는 비휘발성 메모리 소자(NV)가 저항형 메모리 소자인 경우에 대하여 상술하기로 한다. 그러나, 비휘발성 메모리 소자(NV)는 이에 한정되지 않고, 다양하게 변경될 수 있다.
- [0050] 먼저, 비휘발성 메모리 소자(NV)가 '1'로 프로그램되면 비휘발성 메모리 소자(NV)는 저저항 상태가 된다. 따라서, 내부 배선(W1)과 외부 배선(W2) 사이에는 전류가 잘 흐를 수 있으므로, 내부 배선(W1)과 외부 배선(W2)은 서로 연결된다. 한편, 비휘발성 메모리 소자(NV)가 '0'으로 프로그램되면 비휘발성 메모리 소자(NV)는 고저항 상태가 된다. 따라서, 내부 배선(W1)과 외부 배선(W2) 사이에는 전류가 잘 흐르지 못하므로, 내부 배선(W1)과 외부 배선(W2)은 연결되지 않는다.
- [0051] 이 경우, 비휘발성 메모리 소자(NV)에 의해 내부 배선(W1)과 외부 배선(W2)의 연결을 용이하게 제어하기 위해서는, 비휘발성 메모리 소자(NV)가 '1'로 프로그램된 경우, 즉 저저항 상태에서의 저항과 비휘발성 메모리 소자(NV)가 '0'으로 프로그램된 경우, 즉 고저항 상태에서의 저항의 차이가 큰 저항 물질을 이용하여 비휘발성 메모리 소자(NV)를 구현할 수 있다.
- [0052] 본 실시예에 따르면, 보안 제어부(12)는 내부 배선(W1)과 외부 배선(W2)이 교차하는 영역에 비휘발성 메모리 소자(NV)를 배치시키고, 비휘발성 메모리 소자(NV)를 '1' 또는 '0'으로 프로그램함으로써 내부 배선(W1)과 외부 배선(W2)의 연결을 제어할 수 있다. 이와 같이, 내부 배선(W1)과 외부 배선(W2)의 사이에 비휘발성 메모리 소자(NV)만을 배치하여 내부 배선(W1)과 외부 배선(W2)의 연결을 제어할 수 있으므로 구현이 매우 간단하고, 적은 면적을 차지하므로 효율성이 높다.
- [0053] 도 5는 도 3의 배선 연결부에 포함된 스위칭부의 다른 예를 나타내는 회로도이다.
- [0054] 도 5를 참조하면, 스위칭부(SW2)는 내부 배선(W1)과 외부 배선(W2)이 교차하는 영역에 배치되는 스위치(NM) 및 스위치 제어부(50)를 포함할 수 있다. 여기서, 내부 배선(W1)은 저장부(11)에 연결되는 배선들 중 하나이고, 외부 배선(W2)은 외부 장치에 연결되는 배선들 중 하나이다. 본 실시예에서, 스위치(NM)은 엔모스(NMOS) 트랜지스터로 구현될 수 있는데, 이때, 스위치(NM)의 소스 및 드레인은 각각 내부 배선(W1) 및 외부 배선(W2)에 연결될 수 있다. 그러나, 스위치(NM)의 구성은 이에 한정되지 않고, 다른 실시예에서 스위치(NM)는 다르게 구현될 수 있다.
- [0055] 스위치 제어부(50)는 스위치(NM)에 연결되어, 스위치(NM)의 온/오프를 제어할 수 있다. 구체적으로, 스위치 제어부(50)는 배선 연결 제어부(122)에 의해 프로그램되는 적어도 하나의 비휘발성 메모리 소자를 포함하고, 적어도 하나의 비휘발성 메모리 소자의 프로그램 결과를 기초로 하여 스위치(NM)의 온/오프를 제어할 수 있다. 본 실시예에서, 스위치 제어부(50)는 제1 및 제2 풀업 소자들(PU1, PU2), 제1 및 제2 풀다운 소자들(PD1, PD2), 등화부(51) 및 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)을 포함할 수 있다.
- [0056] 제1 풀업 소자(PU1)는 전원 전압 단자(VDD)에 연결된 소스, 제1 노드(N1)에 연결된 드레인 및 제2 노드(N2)에 연결된 게이트를 가지는 피모스 트랜지스터로 구현될 수 있다. 제1 풀다운 소자(PD1)는 제1 노드(N1)에 연결된 드레인 및 제2 노드(N2)에 연결된 게이트를 가지는 엔모스 트랜지스터로 구현될 수 있다. 제1 풀업 소자(PU1)와 제1 풀다운 소자(PD1)는 제1 인버터를 구성할 수 있다.
- [0057] 제2 풀업 소자(PU2)는 전원 전압 단자(VDD)에 연결된 소스, 제2 노드(N2)에 연결된 드레인 및 제1 노드(N1)에 연결된 게이트를 가지는 피모스 트랜지스터로 구현될 수 있다. 제2 풀다운 소자(PD2)는 제2 노드(N2)에 연결된 드레인 및 제1 노드(N1)에 연결된 게이트를 가지는 엔모스 트랜지스터로 구현될 수 있다. 제2 풀업 소자(PU2)와 제2 풀다운 소자(PD2)는 제2 인버터를 구성할 수 있다. 이와 같이, 제1 인버터와 제2 인버터는 교차 결합되어 래치(latch)를 구성할 수 있다.
- [0058] 등화부(51)는 제1 풀다운 소자(PD1)의 게이트와 제2 풀다운 소자(PD2)의 게이트 사이에 연결되어, 등화 신호(EQ)가 활성화되면 제1 풀다운 소자(PD1)의 게이트와 제2 풀다운 소자(PD2)의 게이트를 연결시킨다. 예를 들어, 등화부(51)는 제1 풀다운 소자(PD1)의 게이트에 연결되는 소스, 제2 풀다운 소자(PD2)의 게이트에 연결되는 드레인 및 등화 신호가 인가되는 게이트를 가지는 엔모스 트랜지스터로 구현될 수 있다. 이때, 등화 신호

(EQ)가 '1'로 활성화되면 등화부(51)는 턴온되어 제1 풀다운 소자(PD1)의 게이트와 제2 풀다운 소자(PD2)의 게이트를 연결시키고, 이에 따라 제1 풀다운 소자(PD1)의 게이트와 제2 풀다운 소자(PD2)의 게이트의 전압 레벨은 동일해진다.

- [0059] 제1 비휘발성 메모리 소자(NV1)는 제1 풀다운 소자(PD1)의 소스와 접지 전압 단자(VSS) 사이에 연결되고, 제2 비휘발성 메모리 소자(NV2)는 제2 풀다운 소자(PD2)의 소스와 접지 전압 단자(VSS) 사이에 연결된다. 이때, 제1 비휘발성 메모리 소자(NV1)와 제2 비휘발성 메모리 소자(NV2)는 상보적으로 프로그램될 수 있다.
- [0060] 본 실시예에서, 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)은 저항형 메모리 소자, 자기 메모리 소자 또는 플래시 메모리 소자일 수 있다. 이하에서는 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)이 저항형 메모리 소자인 경우, 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)에 대한 프로그램 결과에 따른 스위치(SW)의 동작에 대하여 상술하기로 한다. 그러나, 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)는 이에 한정되지 않고, 다양하게 변경될 수 있다.
- [0061] 먼저 제1 비휘발성 메모리 소자(NV1)가 '1'로 프로그램되고, 제2 비휘발성 메모리 소자(NV2)가 '0'으로 프로그램된 경우, 제1 비휘발성 메모리 소자(NV1)는 저저항 상태이고, 제2 비휘발성 메모리 소자(NV2)는 고저항 상태가 된다. 이때, 등화 신호(EQ)가 '1'이 되면 등화부(51)가 턴온되고, 동일한 접지 전압 단자(VSS)에 연결된 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2) 중 제1 비휘발성 메모리 소자(NV1)의 저항이 낮으므로, 제1 노드(N1)가 전원 전압 단자(VSS)에 연결된다. 따라서, 제1 노드(N1)의 전압 레벨은 '0'이 되고, 제2 노드(N2)의 전압 레벨은 '1'이 되며, 이에 따라, 스위치(NM)가 턴온되어 내부 배선(W1)과 외부 배선(W2)이 연결된다.
- [0062] 다음으로 제1 비휘발성 메모리 소자(NV1)가 '0'으로 프로그램되고, 제2 비휘발성 메모리 소자(NV2)가 '1'로 프로그램된 경우, 제1 비휘발성 메모리 소자(NV1)는 고저항 상태이고, 제2 비휘발성 메모리 소자(NV2)는 저저항 상태가 된다. 이때, 등화 신호(EQ)가 '1'이 되면 등화부(51)가 턴온되고, 동일한 접지 전압 단자(VSS)에 연결된 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2) 중 제2 비휘발성 메모리 소자(NV2)의 저항이 낮으므로, 제2 노드(N2)가 전원 전압 단자(VSS)에 연결된다. 따라서, 제2 노드(N2)의 전압 레벨은 '0'이 되고, 이에 따라, 스위치(NM)가 턴오프되어 내부 배선(W1)과 외부 배선(W2)은 연결되지 않는다.
- [0063] 본 실시예에 따르면, 보안 제어부(12)는 내부 배선(W1)과 외부 배선(W2)이 교차하는 영역에 스위치(NM) 및 스위치 제어부(50)를 배치시키고, 스위치 제어부(50)에 포함된 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)을 상보적으로 프로그램함으로써 내부 배선(W1)과 외부 배선(W2)의 연결을 제어할 수 있다. 이때, 내부 배선(W1)과 외부 배선(W2)이 연결되지 않도록 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2)을 프로그램한 경우에 스위치(NM)는 오프되므로 내부 배선(W1)과 외부 배선(W2)의 사이에는 누설 전류가 흐르지 않는다.
- [0064] 한편, 다른 실시예에 따르면, 스위치 제어부(50)는 제1 및 제2 비휘발성 메모리 소자들(NV1, NV2) 대신에 하나의 비휘발성 메모리 소자와 저항 소자를 포함할 수도 있다. 이때, 상기 저항 소자의 저항 값이 상기 비휘발성 메모리 소자가 고저항 상태일 때의 저항 값과 저저항 상태일 때의 저항 값의 중간 정도가 되도록, 상기 저항 소자를 선택할 수 있다. 구체적으로, 상기 비휘발성 메모리 소자의 프로그램 결과에 따라 변경되는 저항 값과 상기 저항 소자의 저항 값의 비교를 통해 내부 배선(W1)과 외부 배선(W2)의 연결을 제어할 수 있다.
- [0065] 보다 상세하게는, 상기 비휘발성 메모리 소자가 '1'로 프로그램된 경우 상기 비휘발성 메모리 소자는 저저항 상태가 되고 이는 상기 저항 소자의 저항 값보다 낮을 수 있다. 따라서, 제1 노드(N1)의 전압 레벨은 '0'이 되고, 제2 노드(N2)의 전압 레벨은 '1'이 되며, 이에 따라 스위치(NM)가 턴온되어 내부 배선(W1)과 외부 배선(W2)은 연결될 수 있다. 한편, 상기 비휘발성 메모리 소자가 '0'으로 프로그램된 경우 상기 비휘발성 메모리 소자는 고저항 상태가 되고 이는 상기 저항 소자의 저항 값보다 높을 수 있다. 따라서, 제2 노드(N2)의 전압 레벨은 '0'이 되고, 이에 따라 스위치(NM)가 턴오프되어 내부 배선(W1)과 외부 배선(W2)은 연결되지 않을 수 있다.
- [0066] 도 6은 본 발명의 일 실시예에 따른 전자 장치를 개략적으로 나타내는 블록도이다.
- [0067] 도 6을 참조하면, 전자 장치(60)는 프로세서(61), RAM(62), ROM(63), 인터페이스(64) 및 스토리지(65)를 포함할 수 있다. 여기서, RAM(62), ROM(63) 또는 스토리지(65)는 도 1 내지 도 5에 도시된 저장 장치로 구현될 수 있다.
- [0068] 프로세서(61)는 프로그램을 실행하여 전자 장치(60)를 제어하는 역할을 할 수 있는데, 예를 들어, 프로세서(61)는 마이크로프로세서일 수 있다. 이때, 프로세서(61)는 RAM(62), ROM(63) 및 스토리지(65)에 액세스할 수 있다. RAM(62)은 프로세서(61)가 신속하게 이용할 수 있는 명령어와 데이터, 예를 들어, 운영 체제의 주요 부분

과 응용 프로그램의 일부(또는 전부), 그리고 현재 사용 중인 데이터가 저장될 수 있다. ROM(63)은 전자 장치(60)에 항상 필요한 바이오스(BIOS) 등과 같은 특별한 프로그램이나 데이터를 유지하기 위해 사용된다. 스토리지(65)는 인터페이스(64)를 통해 시스템 버스(66)에 연결될 수 있고, OS, 소프트웨어 또는 데이터를 저장하는데 이용되고, 하드 디스크 드라이브, 광 디스크 드라이브, SSD 등을 포함할 수 있다.

[0069] 프로세서(61), RAM(62), ROM(63) 및 인터페이스(64)는 시스템 버스(66)를 통해 통신할 수 있다. 시스템 버스(66)는 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스 및 각종 버스 아키텍처 중 임의의 것을 이용하는 로컬 버스를 비롯한 몇몇 유형의 버스 구조 중 어느 것이라도 될 수 있다. 예를 들어, 이러한 아키텍처는 ISA(industry standard architecture) 버스, MCA(micro channel architecture) 버스, EISA(enhanced ISA) 버스, VESA(video electronics standard association) 로컬 버스, 및 PCI(peripheral component interconnect) 버스, FSB(front side bus), QPI(Quick Path InterConnect), 하이퍼 트랜스포트(HyperTransport, HT) 등을 포함하지만 이에 제한되는 것은 아니다. 한편, 인터페이스(64)는 USB, IEEE 1394, PCMCIA(personal computer memory card international association), ExpressCard, e-SATA(serial ATA), SCSI(small computer system interface) 등일 수 있다.

[0070] 도 7은 도 6의 전자 장치에 포함된 RAM의 일 예를 나타내는 블록도이다.

[0071] 도 7을 참조하면, RAM(62)은 DRAM(621) 및 보안 제어부(622)를 포함할 수 있다. 여기서, 보안 제어부(622)는 도 1에 도시된 보안 제어부(12)와 실질적으로 동일하게 구현될 수 있으므로, 이에 대한 상세한 설명은 생략하기로 한다. 이와 같이, RAM(62)에 포함된 DRAM(621)의 앞 단에 보안 제어부(622)를 포함시킴으로써, DRAM(621)에 저장된 데이터에 대한 보안 기능을 제공할 수 있다. 이때, RAM(62)은 DRAM(621)을 포함하는 것으로 도시되었으나, 이는 일 예에 불과하고, RAM(62)은 다른 메모리 장치를 포함할 수도 있다.

[0072] 도 8은 도 6의 전자 장치에 포함된 스토리지의 일 예를 나타내는 블록도이다.

[0073] 도 8을 참조하면, 스토리지(65)는 비휘발성 메모리(651) 및 보안 제어부(652)를 포함할 수 있다. 여기서, 보안 제어부(652)는 도 1에 도시된 보안 제어부(12)와 실질적으로 동일하게 구현될 수 있으므로, 이에 대한 상세한 설명은 생략하기로 한다. 비휘발성 메모리(651)는 플래시 메모리 소자, RRAM, MRAM, PRAM, EEPROM 등과 같은 다양한 메모리 소자들로 구현될 수 있다.

[0074] 도 9는 본 발명의 일 실시예에 따른 서버(server)-클라이언트(client) 시스템을 개략적으로 나타내는 블록도이다.

[0075] 도 9를 참조하면, 서버-클라이언트 시스템(90)은 서버(91) 및 네트워크(93)를 통해 서버(91)와 연결 가능한 복수의 클라이언트들(94, 95, 96)을 포함할 수 있다. 서버(91)는 네트워크(93)를 통해 복수의 클라이언트들(94, 95, 96)의 요청에 따라 스토리지(92)로부터 데이터를 제공하거나, 스토리지(92)에 데이터를 저장할 수 있다. 이때, 서버(91)와 스토리지(92)를 스토리지 서버라고 할 수 있다. 여기서, 스토리지(92)는 도 1 내지 도 5에 도시된 저장 장치일 수 있다.

[0076] 예를 들어, 서버(91)는 음악 파일을 제공하는 서비스 사업자일 수 있고, 복수의 클라이언트들(94, 95, 96)은 상기 서비스에 가입한 사용자들일 수 있다. 스토리지(92)에는 음악 파일 A, 음악 파일 B, 음악 파일 C이 보안 데이터의 형태로 저장될 수 있다. 이때, 제1 클라이언트(94)는 음악 파일 A에 대한 정당한 권한을 가진 사용자이고, 제2 및 제3 클라이언트들(95, 96)은 음악 파일 A에 대하여는 권한이 없고, 음악 파일 B와 음악 파일 C에 대한 정당한 권한을 가진 사용자일 수 있다. 따라서, 제1 클라이언트(94)는 적법한 암호화 키를 이용하여 스토리지(92)에 액세스할 수 있으며, 스토리지(92)로부터 음악 파일 A의 원본 데이터를 획득할 수 있다. 그러나, 제2 및 제3 클라이언트들(95, 96)은 음악 파일 A에 대해서는 암호화 키가 없거나 암호화 키가 적법하지 않기 때문에, 스토리지(92)에 액세스하더라도 음악 파일 A에 대한 원본 데이터를 획득할 수 없다.

[0077] 도 10은 본 발명의 일 실시예에 따른 네트워크 스토리지를 개략적으로 나타내는 블록도이다.

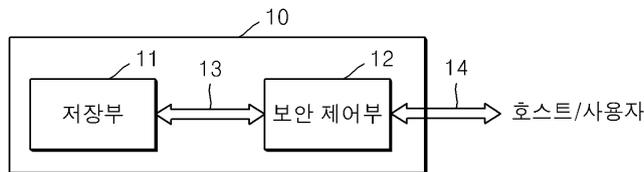
[0078] 도 10을 참조하면, 네트워크 스토리지(100)는 스토리지(101) 및 네트워크 인터페이스(102)를 포함하여, 네트워크 인터페이스(102)를 통해 네트워크(103)에 연결될 수 있다. 복수의 사용자들(104, 105, 106)은 네트워크(103)를 통해 네트워크 스토리지(100)에 접속하여, 스토리지(101)에 데이터를 저장하거나 스토리지(101)로부터 데이터를 읽어낼 수 있다. 여기서, 스토리지(101)는 도 1 내지 도 5에 도시된 저장 장치일 수 있다. 복수의 사용자들(104, 105, 106)은 각자 암호화 키를 이용하여 자신의 파일을 실시간으로 암호화하여 저장하고 독출할 수 있으며, 다른 사용자의 파일에 대해서는 액세스 하더라도 암호화 키가 없거나 암호화 키가 적법하지 않기 때

문에 원본 데이터를 입수할 수 없다.

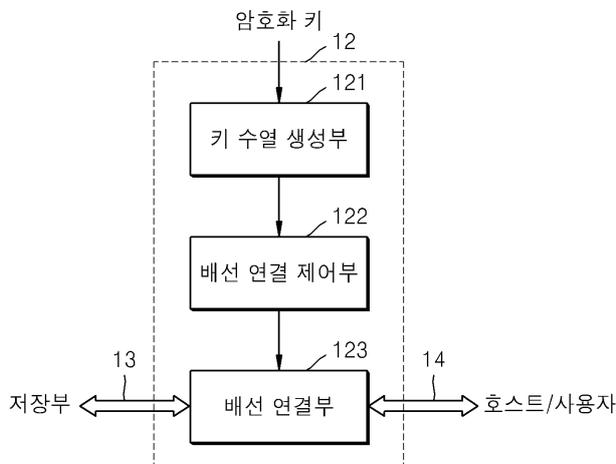
- [0079] 도 11은 본 발명의 일 실시예에 따른 저장 장치의 보안 방법을 개략적으로 나타내는 흐름도이다.
- [0080] 도 11을 참조하면, 저장 장치의 보안 방법은 도 1 내지 도 5에 도시된 저장 장치(10)에서의 보안 방법을 나타낸다. 따라서, 도 1 내지 도 5에서 상술된 내용은 본 실시예에도 적용될 수 있다.
- [0081] 1110 단계에서, 암호화 키를 수신하여 키 수열을 생성한다.
- [0082] 1120 단계에서, 키 수열을 기초로 복수의 비휘발성 메모리 소자들 각각에 대해 프로그램 동작을 수행한다.
- [0083] 1130 단계에서, 복수의 비휘발성 메모리 소자들 각각의 프로그램 결과에 따라, 복수의 내부 배선들과 복수의 외부 배선들의 연결을 제어한다.
- [0084] 1140 단계에서, 복수의 내부 배선들과 복수의 외부 배선들의 연결에 따라 데이터를 저장부 또는 외부 장치에 전달한다.
- [0085] 본 발명의 다른 실시예에서, 보안 방법은 암호화 키가 변경되는 경우 변경된 암호화 키에 따라 상기 복수의 비휘발성 메모리 소자들을 각각 프로그램하는 단계를 더 포함할 수 있다. 이때, 1130 단계는, 변경된 암호화 키에 따라 복수의 비휘발성 메모리 소자들이 프로그래밍된 결과에 따라 복수의 제1 배선들의 각각과 복수의 제2 배선들의 각각의 사이의 연결을 변경할 수 있다.
- [0086] 이상에서 설명한 본 발명이 전술한 실시예 및 첨부된 도면에 한정되지 않으며, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

도면

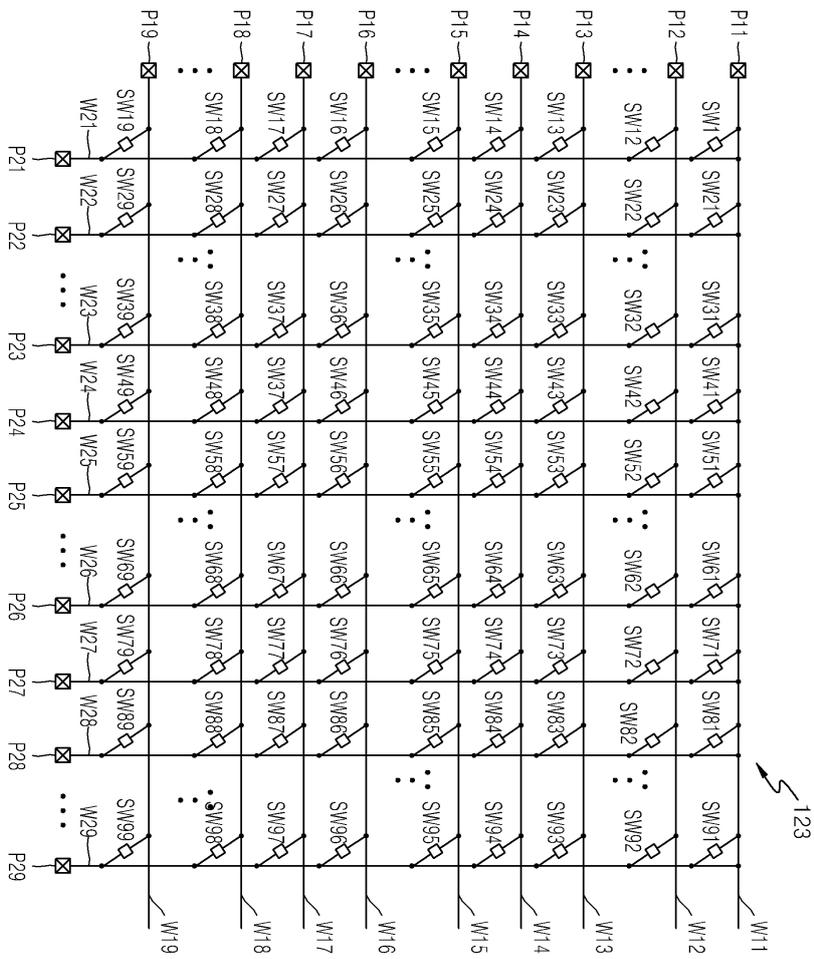
도면1



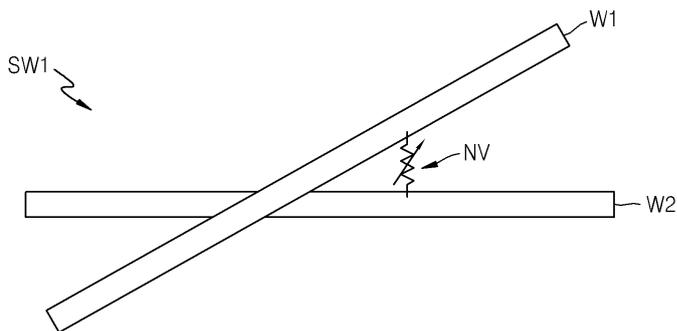
도면2



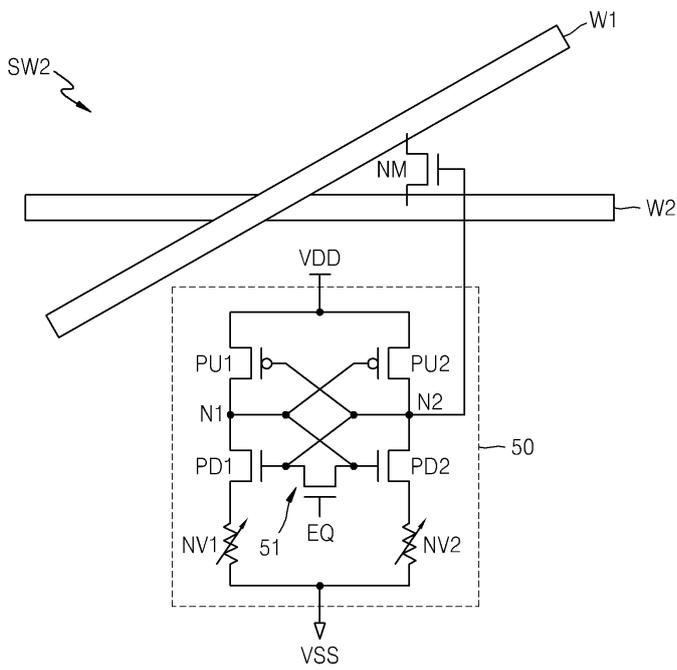
도면3



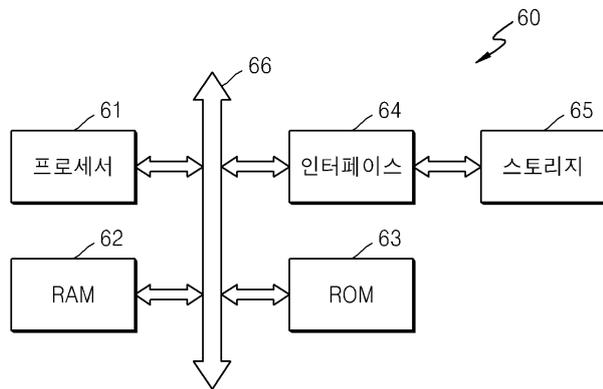
도면4



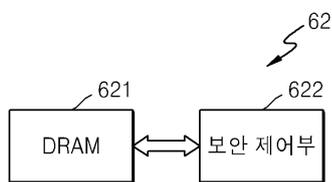
도면5



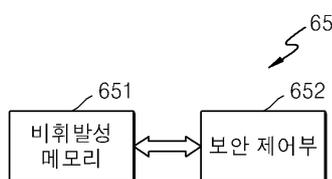
도면6



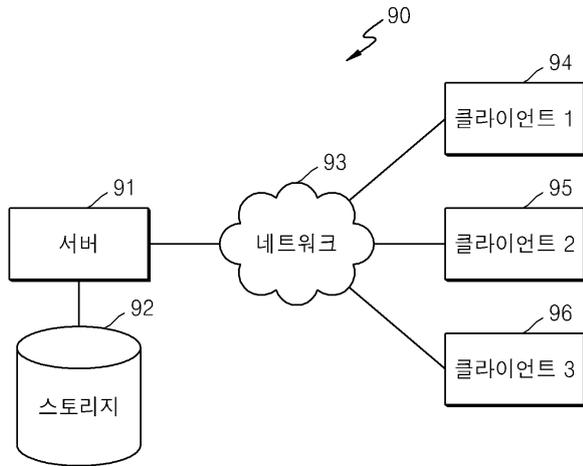
도면7



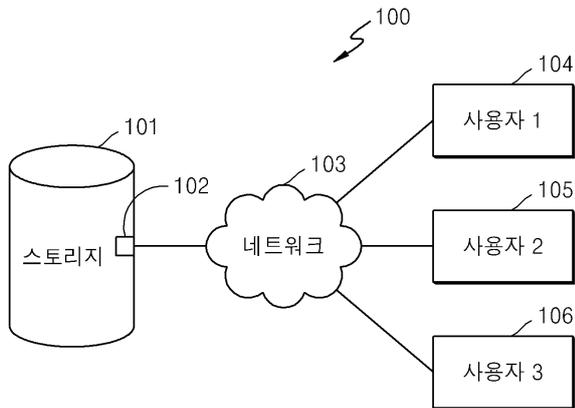
도면8



도면9



도면10



도면11

