



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년10월07일
(11) 등록번호 10-1663544
(24) 등록일자 2016년09월30일

(51) 국제특허분류(Int. Cl.)
G06F 21/72 (2013.01) G06F 21/85 (2013.01)

(52) CPC특허분류
G06F 21/72 (2013.01)
G06F 21/85 (2013.01)

(21) 출원번호 10-2015-0061196

(22) 출원일자 2015년04월30일

심사청구일자 2015년04월30일

(56) 선행기술조사문헌

KR1020070024680 A

KR1020100021446 A

김태용 외 1인, '복제 방지용 PUF의 전자계 해석 방안', 한국정보통신종합학술대회 논문집, 2012

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

김현민

서울특별시 성북구 길음로 118, 414동 1801호 (길음동, 길음뉴타운)

홍석희

서울특별시 도봉구 마들로 859-19, 103동 107호 (도봉동, 도봉한신아파트)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 7 항

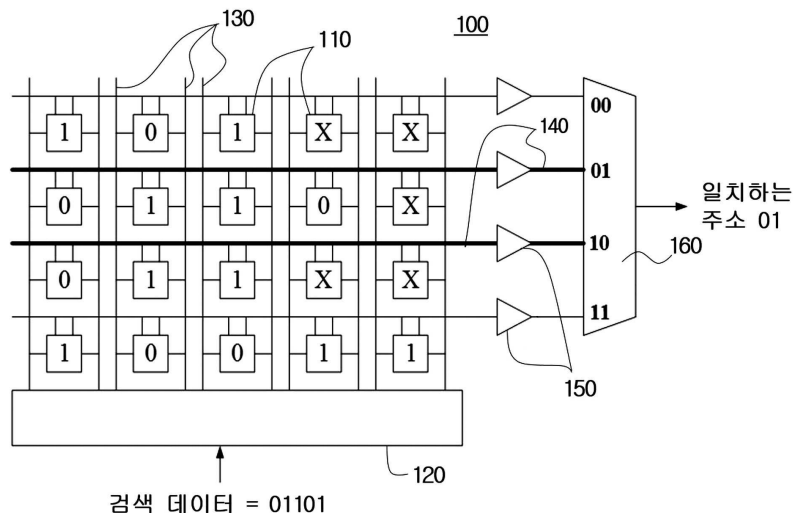
심사관 : 구대성

(54) 발명의 명칭 내용 주소화 메모리 기반의 암호화 장치

(57) 요약

본 발명은 내용 주소화 메모리 기반의 암호화 장치에 관한 것으로, 메모리에 저장된 데이터 접근 시 상기 데이터 자체를 검색하는 내용 주소화 메모리(content addressable memory, CAM)를 포함하되, 상기 내용 주소화 메모리는, 복수행으로 이루어져 데이터를 저장하는 내용 주소화 메모리 셀과, 상기 내용 주소화 메모리 셀에 저장된 데이터를 검색하기 위해 검색 데이터를 입력 받는 서치라인 드라이버(search line driver) 및 상기 검색 데이터와 상기 내용 주소화 메모리 셀에 저장된 데이터의 각 행을 비교하여 일치하는 행의 주소를 출력하는 인코더를 포함하며, 상기 내용 주소화 메모리 단독으로 물리적 복제 방지 기능(physically unclonable functions, PUFs)을 구현하는 것을 특징으로 한다.

대표도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호 IITP-2015-H8501-15-1003

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 ITRC

연구과제명 제어시스템 보안 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.01.01 ~ 2015.12.31

명세서

청구범위

청구항 1

메모리에 저장된 데이터 접근 시 상기 데이터 자체를 검색하는 내용 주소화 메모리(content addressable memory, CAM)를 포함하되,

상기 내용 주소화 메모리는,

복수행으로 이루어져 데이터를 저장하는 내용 주소화 메모리 셀;

상기 내용 주소화 메모리 셀에 저장된 데이터를 검색하기 위해 검색 데이터를 입력 받는 서치라인 드라이버(search line driver); 및

상기 검색 데이터와 상기 내용 주소화 메모리 셀에 저장된 데이터의 각 행을 비교하여 일치하는 행의 주소를 출력하는 인코더를 포함하며,

상기 내용 주소화 메모리 단독으로 물리적 복제 방지 기능(physically unclonable functions, PUFs)을 구현하되,

상기 물리적 복제 방지 기능은 칩으로 처음 제작 시 각각의 상기 물리적 복제 방지 기능 칩의 같은 메모리 주소들간의 엔트로피를 체크하여 상기 엔트로피가 최고인 부분을 실행코드로 사용하는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 2

제 1항에 있어서,

상기 내용 주소화 메모리는,

노어(NOR) 메모리 형태로 바이너리(binary) 내용 주소화 메모리 또는 터너리(ternary) 내용 주소화 메모리로 구성되는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 3

제 2항에 있어서,

상기 바이너리 내용 주소화 메모리는,

4개의 수평 워드라인(horizontal wordline)을 포함하고, 상기 워드라인 각각의 비트가 상기 내용 주소화 메모리 셀에 저장되며, 실행코드와 일치되는 메모리 주소의 코드를 출력으로 추출하는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 4

제 2항에 있어서,

상기 터너리 내용 주소화 메모리는,

추가적인 주소를 포함하고, 다른 주소 공간에 엔트로피가 확보되지 않을 경우 상기 추가적인 주소를 이용하는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 5

제 1항에 있어서,

상기 물리적 복제 방지 기능은,

정적 메모리(static random access memory, SRAM)를 더 포함하며,

상기 정적 메모리를 상기 내용 주소화 메모리의 입력에 연결한 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능 또는 상기 정적 메모리를 상기 내용 주소화 메모리 뒤의 출력에 연결한 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능을 포함하는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 6

제 5항에 있어서,

상기 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능은,

상기 내용 주소화 메모리 셀에 상기 정적 메모리의 랜덤한 초기값이 저장되고, 상기 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능의 출력값은 상기 내용 주소화 메모리 단독으로 구성된 물리적 복제 방지 기능과 동일하게 동작하는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 7

제 5항에 있어서,

상기 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능은,

상기 내용 주소화 메모리 셀에 저장되는 비트들은 상기 내용 주소화 메모리 단독으로 구성된 물리적 복제 방지 기능과 동일하게 생성 및 저장되고, 상기 정적 메모리의 초기 셋팅값이 상기 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능의 출력값으로 생성되는 것을 특징으로 하는 내용 주소화 메모리 기반의 암호화 장치.

청구항 8

삭제

발명의 설명

기술 분야

[0001] 본 발명은 내용 주소화 메모리 기반의 암호화 장치에 관한 것으로, 특히 내용 주소화 메모리를 물리적 복제 방지 기능에 적용하여 디지털 장비를 암호화할 수 있는 내용 주소화 메모리 기반의 암호화 장치에 관한 것이다.

배경 기술

[0002] 최근 들어, 각종 전자 기기들이 고급화되어 널리 보급됨에 따라, 이러한 전자기기에 대한 인증 방법의 여러 연구가 이루어지고 있다. 특히 이러한 인증 방법 중 하나로써, 물리적 복제 방지 기능에 대한 사용이 점차 증가하고 있다. 이와 같이 사용되는 물리적 복제 방지 기능(Physically Unclonable Function, PUF)이란, 모든 반도체 제품에 존재하는 고유의 지문을 이용하여 암호키를 생성하거나 보호함으로써, 개별 반도체 칩의 데이터 도난 및 설계 유출을 방지하는 기술을 말한다.

[0003] 이러한 물리적 복제 방지 기능은 물리적으로 랜덤한 특성과 복제 불가능한 특성을 이용하여 현재 주로 안전한

키 스토리지(key storage)와 객체 인증(ID authentication)에 주로 사용되고 있다. 특히, 소프트웨어적으로 생성된 함수를 이용하여 랜덤한 시드(seed)를 추출해 내는 것이 아니라, 물리적으로 칩이나 장비가 제작(manufacturing)될 때 각각의 칩과 장비가 동일하게 제작될 수 밖에 없는 물리적인 특성을 이용하여 진성 랜덤(true random)한 시드값을 추출한다. 이와 같이 추출한 시드값은 사용자 고유의 값으로 이용하여 객체 인증에 사용할 수 있을 뿐만 아니라, 진성 랜덤한 값이기 때문에 복제 불가능한 칩이나 장비에 적용할 수 있는 코드를 생성하는데 이용할 수 있다.

[0004] 한편, 물리적 복제 방지 기능이 계속 발전하면서 임베디드 물리적 복제 방지 기능이 소개되었으며, 임베디드 물리적 복제 방지 기능은 크게 메모리 기반의 물리적 복제 방지 기능과 딜레이 기반의 물리적 복제 방지 기능으로 나누어진다. 메모리 기반의 물리적 복제 방지 기능은 현재 개발되어 사용되고 있는 메모리에서 물리적 복제 방지 기능의 주요 특성을 만족하는 부분만을 추출하여 이용하는 것이고, 딜레이 기반의 물리적 복제 방지 기능은 하드웨어의 물리적 특성을 통해서 발생할 수 있는 딜레이 특성을 이용하는 것이다.

[0005] 이러한 메모리 기반의 물리적 복제 방지 기능은 대표적으로 정적 메모리(static memory, SRAM) 기반의 물리적 복제 방지 기능이 있다. 이 정적 메모리 기반의 물리적 복제 방지 기능은 초기 상태에서의 불안정한 초기값을 이용하며, 제작 시 추가적인 작업 없이 기존의 메모리 프리미티브(primitive)를 그대로 사용하여 만든다는 점에서 다른 물리적 복제 방지 기능들보다 생성하기 쉽고, 현실적으로 사용 가능한 장점이 있다.

[0006] 또한, 정적 메모리의 랜덤한 초기값은 메모리 제조단계에서 제작 시 모든 메모리들을 동일한 제작 조건하에서 동일한 제작 방식으로 이루어질 수 없으므로 물리적 복제 방지 기능의 특성을 충분히 만족하는 정적 메모리 기반의 물리적 복제 방지 기능을 쉽게 만들어 낼 수 있는 장점이 있다.

[0007] 다만, 정적 메모리를 비롯한 메모리 기반의 물리적 복제 방지 기능은 회로의 에이징(aging) 문제나 시간이 지남에 따라 메모리 회로의 특성이 변하는 문제가 발생하고, 이러한 문제를 해결하기 위하여 추가적으로 오류 정정 함수(error correction function)나 보조 정보(helper data)가 필요하다.

[0008] 이러한 후처리는 물리적 복제 방지 기능 시스템 설계 시 추가적인 면적이 많이 필요하게 되어 소형 전자장비에 적용하기가 큰 부담으로 여겨지며, 보안성 측면에서 심각한 엔트로피 손실을 초래하는 문제점이 발생한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) KR 10-1488433 (PUF를 이용한 저장장치 및 저장장치의 인증 및 암호화 방법, 숭실대학교 산학협력단) 2015.01.26.

발명의 내용

해결하려는 과제

[0010] 본 발명은 상술한 종래기술의 문제점을 극복하기 위한 것으로서, 내용 주소화 메모리를 이용하여 단독 또는 정적 메모리와 함께 결합하여 후처리 과정 없이 다양한 형태의 안정적인 물리적 복제 방지 기능을 수행할 수 있는 내용 주소화 메모리 기반의 암호화 장치를 제공하는 데에 그 목적이 있다.

[0011] 또한, 본 발명은 내용 주소화 메모리가 셀들로 구성되어 고속으로 물리적 복제 방지 기능의 출력값을 추출할 수 있는 내용 주소화 메모리 기반의 암호화 장치를 제공하는 데에 그 목적이 있다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위해 본 발명은 메모리에 저장된 데이터 접근 시 상기 데이터 자체를 검색하는 내용 주소화 메모리(content addressable memory, CAM)를 포함하되, 상기 내용 주소화 메모리는 복수행으로 이루어져 데이터를 저장하는 내용 주소화 메모리 셀과, 상기 내용 주소화 메모리 셀에 저장된 데이터를 검색하기 위해 검색 데이터를 입력 받는 서치라인 드라이버(search line driver) 및 상기 검색 데이터와 상기 내용 주소화 메모리

셀에 저장된 데이터의 각 행을 비교하여 일치하는 행의 주소를 출력하는 인코더를 포함하며, 상기 내용 주소화 메모리 단독으로 물리적 복제 방지 기능(physically unclonable functions, PUFs)을 구현한다.

- [0013] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 내용 주소화 메모리는, 노어(NOR) 메모리 형태로 바이너리(binary) 내용 주소화 메모리 또는 터너리(ternary) 내용 주소화 메모리로 구성되는 것을 특징으로 한다.
- [0014] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 바이너리 내용 주소화 메모리는 4개의 수평 워드라인을 포함하고, 상기 워드라인 각각의 비트가 상기 내용 주소화 메모리 셀에 저장되며, 실행코드와 일치되는 메모리 주소의 코드를 출력으로 추출하는 것을 특징으로 한다.
- [0015] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 터너리 내용 주소화 메모리는, 추가적인 주소를 포함하고, 다른 주소 공간에 엔트로피가 확보되지 않을 경우 상기 추가적인 주소를 이용하는 것을 특징으로 한다.
- [0016] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 물리적 복제 방지 기능은 정적 메모리(static random access memory, SRAM)를 더 포함하며, 상기 정적 메모리를 상기 내용 주소화 메모리의 입력에 연결한 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능 또는 상기 정적 메모리를 상기 내용 주소화 메모리 뒤의 출력에 연결한 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능을 포함하는 것을 특징으로 한다.
- [0017] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능은 상기 내용 주소화 메모리 셀에 상기 정적 메모리의 랜덤한 초기값이 저장되고, 상기 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능의 출력값은 상기 내용 주소화 메모리 단독으로 구성된 물리적 복제 방지 기능과 동일하게 동작하는 것을 특징으로 한다.
- [0018] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능은 상기 내용 주소화 메모리 셀에 저장되는 비트들은 상기 내용 주소화 메모리 단독으로 구성된 물리적 복제 방지 기능과 동일하게 생성 및 저장되고, 상기 정적 메모리의 초기 셋팅값이 상기 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능의 출력값으로 생성되는 것을 특징으로 한다.
- [0019] 본 발명에 따른 내용 주소화 메모리 기반의 암호화 장치에 있어서, 상기 물리적 복제 방지 기능은 칩으로 처음 제작 시 각각의 상기 물리적 복제 방지 기능 칩의 같은 메모리 주소들간의 엔트로피를 체크하여 상기 엔트로피가 최고인 부분을 실행코드로 사용하는 것을 특징으로 한다.

발명의 효과

- [0020] 본 발명의 내용 주소화 메모리 기반의 암호화 장치는 내용 주소화 메모리를 이용하여 단독 또는 정적 메모리와 함께 결합하여 후처리 과정 없이 다양한 형태의 안정적인 물리적 복제 방지 기능을 수행하는 효과가 있다.
- [0021] 또한, 본 발명의 내용 주소화 메모리 기반의 암호화 장치는 내용 주소화 메모리가 셀들로 구성되어 고속으로 물리적 복제 방지 기능의 출력값을 추출하는 효과가 있다.

도면의 간단한 설명

- [0022] 도 1은 본 발명의 바이너리 내용 주소화 메모리 셀을 나타내는 도면이다.
- 도 2는 본 발명의 터너리 내용 주소화 메모리 셀을 나타내는 도면이다.
- 도 3은 본 발명의 노어 메모리 형태에 내용 주소화 메모리의 구조를 나타내는 도면이다.
- 도 4(a)는 본 발명의 바람직한 실시 예에 따른 단독으로 구성된 내용 주소화 메모리의 구성을 나타내는 도면이다.
- 도 4(b)는 본 발명의 다른 실시 예에 따른 정적 메모리/내용 주소화 메모리의 구성을 나타내는 도면이다.
- 도 4(c)는 본 발명의 다른 실시 예에 따른 내용 주소화 메모리/정적 메모리의 구성을 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.
- [0024] 먼저 본 발명에 대하여 자세히 설명하기에 앞서, 본 발명에서 이용하는 내용 주소화 메모리에 대하여 자세히 설명하도록 한다.
- [0025] 내용 주소화 메모리(Content Addressable Memory, CAM)는 메모리에 저장된 데이터에 접근할 때에 주소를 이용하여 데이터에 접근하는 램과는 달리 저장된 내용 자체를 검색하는 방법으로 데이터에 접근하고 처리한다. 내용 주소화 메모리는 모든 워드를 대상으로 검색 과정이 동시에 진행되므로 한 번의 검색으로 저장된 데이터의 개수에 무관하게 검색할 수 있다. 그러므로, 메모리와 CPU사이에서 발생하는 병목현상에 대해 내용 주소화 메모리는 효과적인 개선책이 될 수 있으며, 이러한 이점으로 다양한 연구 분야에서 활용되고 있다.
- [0026] 한편, 기존의 정적 메모리를 이용한 물리적 복제 방지 기능은 상기에서 설명한 바와 같이 문제점이 있으며, 이를 해결하기 위한 방법으로는 추가 구성 등의 공간 및 비용적인 단점이 있어 본 발명에서는 이러한 물리적 복제 방지 기능 설계시 단점을 해결하기 위해 내용 주소화 메모리를 사용한다.
- [0027] 내용 주소화 메모리를 이용하여 물리적 복제 방지 기능을 구현하는 기술은 아직 개발되지 않았으며, 본 발명은 메모리를 이용하는 종래의 물리적 복제 방지 기능의 문제점을 내용 주소화 메모리의 룩업 함수를 이용하여 추가 구성 없이 해결할 수 있다.
- [0028] 이하에서는, 본 발명의 내용 주소화 메모리 기반의 암호화 장치에 대해서 도면을 참조하여 상세히 설명하도록 한다.
- [0029] 도 1과 도 2를 참조하면 내용 주소화 메모리는 바이너리(binary) 내용 주소화 메모리 셀과 터너리(ternary) 내용 주소화 메모리 셀로 구성된다.
- [0030] 도 1은 본 발명의 바이너리 내용 주소화 메모리 셀을 나타내는 도면이며, 도 2는 본 발명의 터너리 내용 주소화 메모리 셀을 나타내는 도면이다.
- [0031] 바이너리 내용 주소화 메모리 셀은 도 1과 같이 구성되며 기본적인 내용 주소화 메모리 형태로 4개의 수평 워드라인(horizontal wordline)을 갖는다. 각 워드라인의 각 비트가 셀에 저장되며, 셀은 물리적 복제 방지 기능으로써 사용하기 위하여 랜덤하게 생성되는 초기값이 저장된다. 이 저장값은 룩업 함수(lookup function) 형태로 계속 셀에 저장된다. 다만, 외부에서는 저장값을 예측하기 어렵다. 여기서 룩업 함수는 룩업 테이블(lookup table)을 형성하기 위한 함수로 해당 내용을 사전 계산하여 미리 저장하기 위한 함수를 의미한다.
- [0032] 한편, 물리적 복제 방지 기능 칩을 제작 후 한 웨이퍼에서의 각각의 칩들 간에 같은 셀에 저장된 값들의 엔트로피를 확인하여 엔트로피가 충분한 것에 대한 내용 주소화 메모리에 주소의 값을 실행코드(activation code)로 사용자에게 제공하여 물리적 복제 방지 기능으로 사용시 동일한 실행코드를 전체 시스템에 입력으로 준다.
- [0033] 즉, 바이너리 내용 주소화 메모리는 실행코드와 일치(match)되는 메모리 주소의 코드를 출력으로 2비트 추출해 낸다. 예를 들어, 8비트의 출력을 얻고자 한다면 4개의 동일한 바이너리 내용 주소화 메모리를 연결하고, 순차적으로 실행코드를 "10010 00010 00000 11111"같이 주면, "00 10 11 11"과 같이 출력값을 얻을 수 있다. 단, 이값은 전체 물리적 복제 방지 기능 시스템을 비롯하여 물리적 복제 방지 기능을 이용하는 시스템에 전원이 공급되었을 때만 on-the-fly 형태로 출력이 되어 사용자는 볼 수 없고, 이 값을 사용하는 시스템의 다른 모듈만 실시간으로 값을 입력으로 받게 된다.
- [0034] 예를 들면 암호알고리즘의 마스터 키(master key) 값으로 이용시 이 8비트의 출력비트는 램 등의 다른 내부 메모리에 저장되지 않으므로 외부로 키 값이 유출될 염려가 없다. 또한, 프로빙 공격(probing attack)을 이용하여 실시간으로 전원을 흘리며 물리적 복제 방지 기능 출력핀에 프로브를 찍어서 값을 알아낼 수 있을 것이라고 생각할 수도 있지만, 이렇게 회로를 디캡(decap)하여 내부 회로의 출력핀 및 하나의 출력선에 프로브를 찍어서 값을 추출하기란 디캡시 내부 전원부에 손상이 일어나 실제 회로를 동작시킬 수 없으므로, 회로가 동작하지 않는다.
- [0035] 따라서, 내용 주소화 메모리 기반의 물리적 복제 방지 기능으로 생성되는 값을 암호알고리즘의 비밀키로 사용시 생성된 값이 유출될 염려는 거의 없다고 할 수 있다.

- [0036] 한편 터너리 내용 주소화 메모리는 도 2와 같이 구성되며, 돈 케어(don't care) 주소가 있어서, 다른 주소 공간이 충분한 엔트로피가 확보가 되지 않는다면 돈 케어 주소를 물리적 복제 방지 기능의 주소로 이용할 수 있다.
- [0037] 도 3은 본 발명의 노어 메모리 형태에 내용 주소화 메모리의 구조를 나타내는 도면이다.
- [0038] 도 3을 참조하면, 내용 주소화 메모리(100)는 내용 주소화 메모리 셀(110), 서치라인 드라이버(search line driver)(120), 서치라인(search line)(130), 매치라인(match line)(140), 매치라인 센스 앰프(match line sense amplifier)(150), 인코더(encoder)(160)을 포함하여 구성된다.
- [0039] 내용 주소화 메모리 셀(110)은 복수행으로 이루어져 각 행마다 각 워드라인의 각 비트가 저장되며, 서치라인 드라이버(120)는 검색 데이터를 입력받아 각 행별로 데이터를 검색한다.
- [0040] 서치라인(130)은 서치라인 드라이버(120)와 내용 주소화 메모리 셀(110) 각각을 서로 연결하며, 매치라인(140)은 검색 데이터와 내용 주소화 메모리 셀(110)에 저장된 데이터의 비교 결과를 매치라인 앰프(150)를 지나 인코더(160)에 출력한다.
- [0041] 인코더(160)는 매치라인(140)의 출력에 따라 검색 데이터와 내용 주소화 메모리 셀(110)에 저장된 데이터를 비교하여 일치하는 행의 주소를 최종적으로 출력한다.
- [0042] 따라서, 내용 주소화 메모리(100)의 데이터 검색 과정은 서치라인 드라이버(120)로 검색 데이터가 입력되면 내용 주소화 메모리 셀(110)의 각 행을 검색 데이터와 비교하여 비교 결과를 매치라인(140)과 매치라인 센스 앰프(150)를 통해 인코더(160)로 출력한다. 인코더(160)는 출력에 따라 검색 데이터와 내용 주소화 메모리 셀(110)에 저장된 데이터의 비교 결과 일치하는 행의 주소를 최종적으로 출력하게 된다.
- [0043] 본 발명은 다양한 실시 예로 구성될 수 있다. 도 4a와 도 4b 및 도 4c를 참조하면 내용 주소화 메모리 기반의 암호화 장치는 단독 또는 정적 메모리와 결합하여 구성될 수 있다.
- [0044] 먼저, 도 4a는 본 발명의 바람직한 실시 예에 따른 단독으로 구성된 내용 주소화 메모리의 구성을 나타내는 도면으로, 도 4a를 참조하면 내용 주소화 메모리에 검색 데이터가 입력되면 도 3에서 설명한 바와 같이 최종적으로 주소를 출력한다.
- [0045] 도 4b는 본 발명의 다른 실시 예에 따른 정적 메모리/내용 주소화 메모리의 구성을 나타내는 도면으로, 도 4b를 참조하면 정적 메모리의 랜덤한 초기값이 내용 주소화 메모리 셀에 저장되고, 데이터 검색 과정은 전압의 온/오프에 따라 정적 메모리에 랜덤값이 출력되고, 랜덤값을 입력 받은 내용 주소화 메모리는 도 3에서 설명한 바와 같이 랜덤값과 일치하는 행의 주소를 최종적으로 출력한다. 따라서 정적 메모리/내용 주소화 메모리 구조의 물리적 복제 방지 기능은 내용 주소화 메모리 단독으로 구성된 물리적 복제 방지 기능과 동일하게 강한 유의성(reliability)를 갖는다.
- [0046] 도 4c는 본 발명의 다른 실시 예에 따른 내용 주소화 메모리/정적 메모리의 구성을 나타내는 도면으로, 도 4c를 참조하면 내용 주소화 메모리 셀에 저장되는 비트들은 도 4a의 단독으로 구성된 내용 주소화 메모리와 동일하게 생성한 후 저장된다. 그리고, 출력된 주소가 정적 메모리에 입력되어 정적 메모리의 초기 셋팅값을 최종적으로 출력한다. 따라서 내용 주소화 메모리/정적 메모리 구조의 물리적 복제 방지 기능은 높은 엔트로피 특성이 필요한 경우에 사용할 수 있다.
- [0047] 본 명세서에 기재된 본 발명의 실시 예와 도면에 도시된 구성은 본 발명의 가장 바람직한 실시 예에 관한 것이고, 발명의 기술적 사상을 모두 포괄하는 것은 아니므로, 출원시점에 있어서 이들을 대체할 수 있는 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다. 따라서 본 발명은 상술한 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 권리범위 내에 있게 된다.

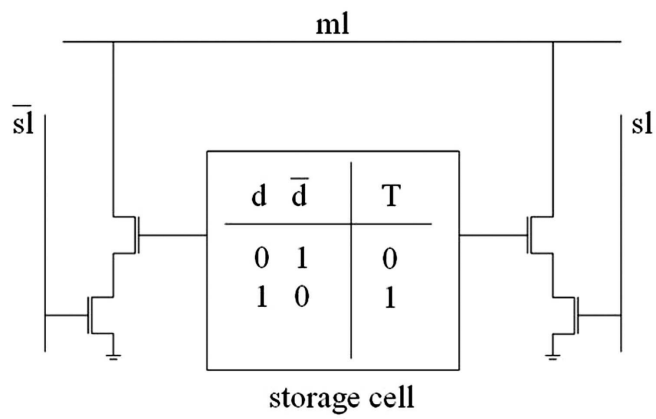
부호의 설명

- [0048] 100 : 내용 주소화 메모리
- 110 : 내용 주소화 메모리 셀

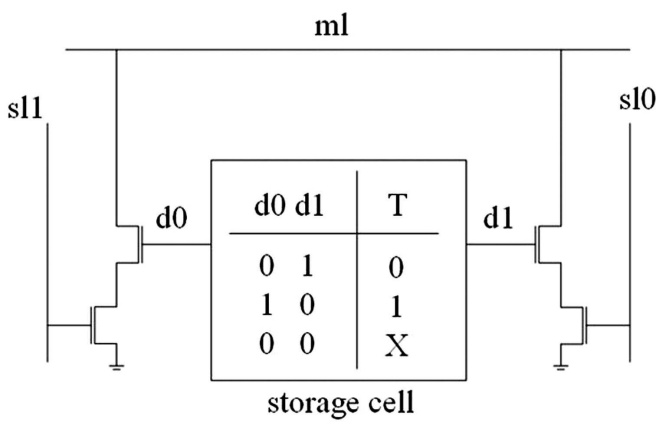
- 120 : 서치라인 드라이버
- 130 : 서치라인
- 140 : 매치라인
- 150 : 매치라인 센스 앰프
- 160 : 인코더

도면

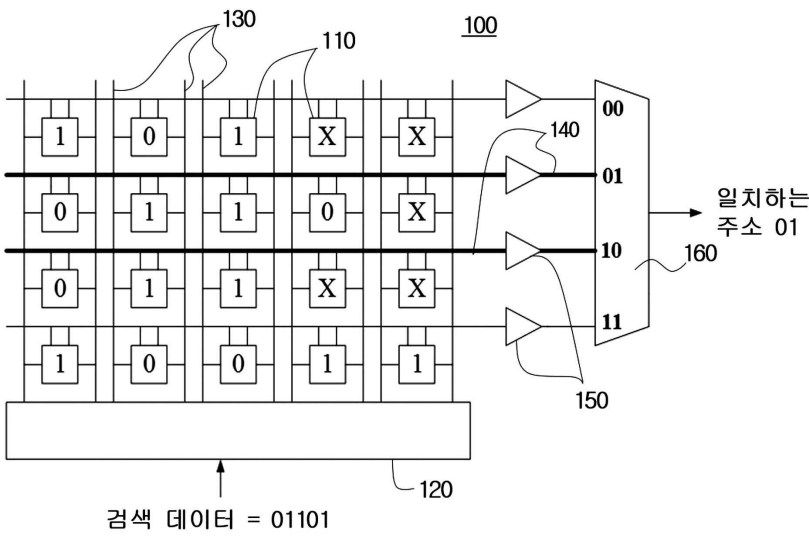
도면1



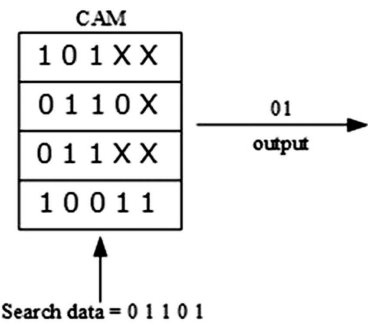
도면2



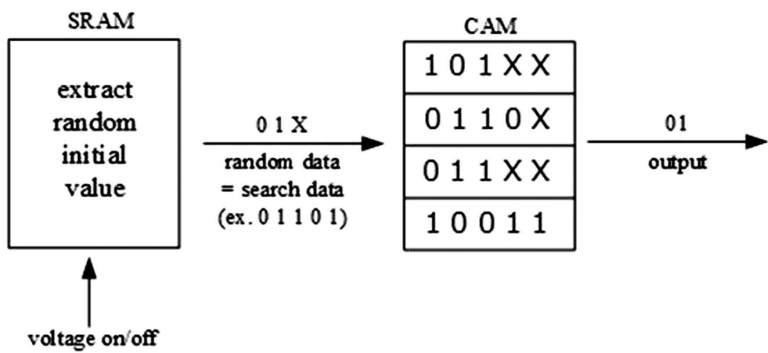
도면3



도면4a



도면4b



도면4c

