(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0034783
(43) 공개일자 2025년03월11일

(51) 국제특허분류(Int. Cl.)
G11C 11/24 (2006.01) *G11C 7/24* (2006.01)
(52) CPC특허분류
G11C 11/24 (2013.01)
G11C 7/24 (2013.01)
(21) 출원번호 10-2023-0117171
(22) 출원일자 2023년09월04일
심사청구일자 2023년09월04일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
김형진
서울특별시 금천구 시흥대로47길 43, 9동 1205호(시흥동, 럭키아파트)
안수현
경기도 안양시 동안구 경수대로884번길 12, 109동 402호(비산동, 평촌래미안푸르지오)
송민석
경기도 성남시 수정구 대왕판교로 1187, 공군아파트 36동 305호(심곡동)
(74) 대리인
양성보

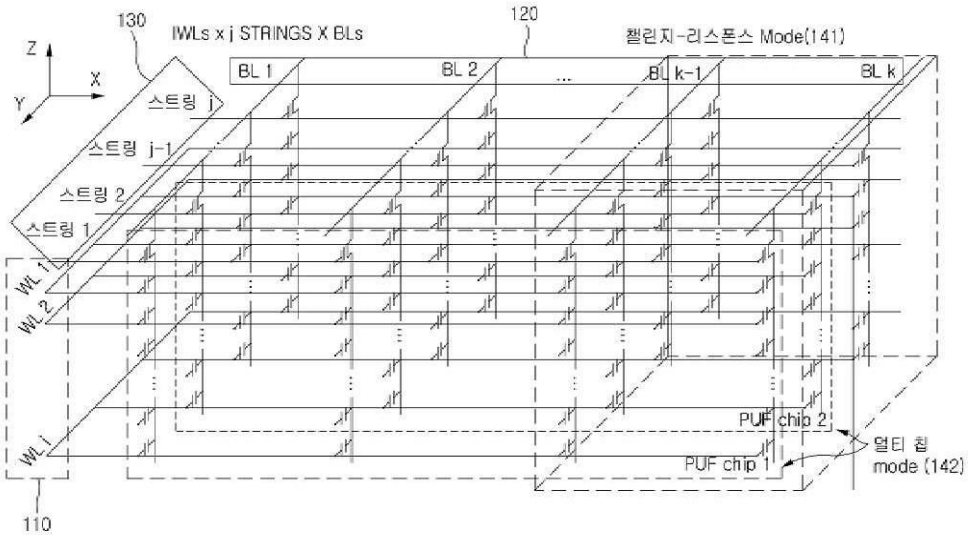
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 스트링 구조 및 그 동작 방법**

(57) 요 약

물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 구조 및 그 동작 방법이 제시된다. 본 발명에서 제안하는 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 구조는 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 챌린지가 인가되는 워드라인(Wordline), 상기 인가되는 챌린지에 따른 리스폰스가 추출되는 비트라인(Bitline) 및 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조를 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 스트링을 포함한다.

대 표 도



이 발명을 지원한 국가연구개발사업
과제고유번호 1711186719
과제번호 2022M3I7A1078544
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 원천기술개발사업
연구과제명 [Ezbaro] 전하저장형 실리콘 MOS 커패시터 기반 물리적 복제불가 함수 개발
기 여 율 5/10
과제수행기관명 서울대학교
연구기간 2023.01.01 ~ 2023.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711183638
과제번호 2021R1C1C1014530
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 우수신진연구
연구과제명 [Ezbaro] 3차원 적층형 멤리스터 크로스바 어레이 구조를 이용한 물리적 복제 불가 함수 및 하드웨어 보안 시스템 개발
기 여 율 3/10
과제수행기관명 인하대학교
연구기간 2023.03.01 ~ 2024.02.29
이 발명을 지원한 국가연구개발사업
과제고유번호 1345362086
과제번호 2022R1A6A1A03051705
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 중점연구소
연구과제명 [Ezbaro] 3D 나노융합소자 연구 센터
기 여 율 2/10
과제수행기관명 인하대학교
연구기간 2023.03.01 ~ 2024.02.29

명 세 서

청구범위

청구항 1

물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 챌린지가 인가되는 워드라인(Wordline);

상기 인가되는 챌린지에 따른 리스폰스가 추출되는 비트라인(Bitline); 및

PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조를 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 스트링

을 포함하는 커패시터 어레이 구조.

청구항 2

제1항에 있어서,

상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 챌린지-리스폰스 모드 또는 멀티 칩 모드의 동작을 위한 3차원 적층형 커패시터 어레이 구조의 평면을 선택하는

커패시터 어레이 구조.

청구항 3

제2항에 있어서,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xyz 평면을 모두 활용하여 PUF를 이용한 보안키의 수를 최대화하기 위해 모든 워드 라인과 스트링 선택을 랜덤으로 설정하여 챌린지-리스폰스 모드의 동작원리를 나타내는

커패시터 어레이 구조.

청구항 4

제2항에 있어서,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xz 평면을 하나의 PUF 칩으로 활용하여 z 방향으로의 독립적인 개별 PUF 칩 활용을 통한 멀티 칩 모드의 동작원리를 나타내는

커패시터 어레이 구조.

청구항 5

물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 워드라인(Wordline)으로 챌린지가 인가되는 단계;

상기 인가되는 챌린지에 따른 리스폰스가 비트라인(Bitline)으로부터 추출되는 단계; 및

PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계

를 포함하는 커패시터 어레이의 동작 방법.

청구항 6

제5항에 있어서,

상기 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계는,

상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 챌린지-리스폰스 모드 또는 멀티 칩 모드의 동작을 위한 3차원 적층형 커패시터 어레이 구조의 평면을 선택하는

커패시터 어레이의 동작 방법.

청구항 7

제6항에 있어서,

상기 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계는,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xyz 평면을 모두 활용하여 PUF를 이용한 보안키의 수를 최대화하기 위해 모든 워드 라인과 스트링 선택을 랜덤으로 설정하여 챌린지-리스폰스 모드의 동작원리를 나타내는

커패시터 어레이의 동작 방법.

청구항 8

제6항에 있어서,

상기 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계는,

상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xz 평면을 하나의 PUF 칩으로 활용하여 z 방향으로의 독립적인 개별 PUF 칩 활용을 통한 멀티 칩 모드의 동작원리를 나타내는

커패시터 어레이의 동작 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 스트링 구조 및 그 동작 방법에 관한 것이다.

배 경 기 술

[0002] 모바일 장치의 확산과 스마트 통신 기술의 급속한 성장으로 보안 통신을 위한 신뢰할 수 있는 암호화 솔루션에 대한 수요가 증가하고 있다.

[0003] 기존 보안 및 인증 분야에서는 대부분 소프트웨어 보안 방식을 통해 암호화를 수행하였지만, 기존 소프트웨어 기반 암호화 솔루션의 경우 최근 개인 정보 유출 등과 같은 많은 보안 사고를 유발하게 되어 보다 더 강력한 보안 솔루션의 필요성이 극대화되고 있다.

[0004] 현대 사회에서 개인 정보 유출 등과 같은 보안 사고가 증가함에 따라 더욱 높은 보안성이 요구되고 있으며, 이를 위해 하드웨어 적으로 제조 공정 편차, 본질적 특성 등의 예측할 수 없는 특성을 기반으로 암호화에 활용하는 PUF의 연구가 활발하게 이루어지고 있다.

[0005] 따라서, 보안키 생성을 위해서는 매우 많은 챌린지-리스폰스 쌍이 필수적이며, 기본적으로 장치의 고유한 물리적 특성을 이용하여 암호화를 수행하는 물리적 복제 불가능 기능은 물리적 특성을 이용한다는 점에서 복제나 해

킹이 어렵기 때문에 높은 보안성에 적합하다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국등록특허 제10-2212513호(2021.01.29)

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적 과제는 3차원 적층형 커패시터 어레이 구조를 통해 두 가지 방안으로 활용될 수 있는 하드웨어 기반 보안기술인 물리적 복제 불가 함수(Physical Unclonable Function; PUF) 기술을 제안한다. PUF는 3차원 구조에서 스트링 선택 방식에 따라 두 가지 방식으로 활용될 수 있고, 랜덤하게 스트링을 선택하면 챌린지(입력)-리스폰스(출력) 모드로 이용이 가능하다. 한 개의 스트링만 선택하게 된다면 각 2차원 어레이를 각각 독립된 개별 물리적 복제 불가 함수로 이용하는 모드로, 하나의 어레이 내에서 다중 PUF칩 동작을 수행할 수 있다.

과제의 해결 수단

[0008] 일 측면에 있어서, 본 발명에서 제안하는 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 구조는 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 챌린지가 인가되는 워드라인(Wordline), 상기 인가되는 챌린지에 따른 리스폰스가 추출되는 비트라인(Bitline) 및 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조를 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 스트링을 포함한다.

[0009] 본 발명의 실시예에 따른 상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 챌린지-리스폰스 모드 또는 멀티 칩 모드의 동작을 위한 3차원 적층형 커패시터 어레이 구조의 평면을 선택한다.

[0010] 본 발명의 실시예에 따르면, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xyz 평면을 모두 활용하여 PUF를 이용한 보안키의 수를 최대화하기 위해 모든 워드 라인과 스트링 선택을 랜덤으로 설정하여 챌린지-리스폰스 모드의 동작원리를 나타낸다.

[0011] 본 발명의 실시예에 따르면, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xz 평면을 하나의 PUF 칩으로 활용하여 z 방향으로의 독립적인 개별 PUF 칩 활용을 통한 멀티 칩 모드의 동작원리를 나타낸다.

[0012] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 구조의 동작 방법은 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 워드라인(Wordline)으로 챌린지가 인가되는 단계, 상기 인가되는 챌린지에 따른 리스폰스가 비트라인(Bitline)으로부터 추출되는 단계 및 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계를 포함한다.

발명의 효과

[0013] 본 발명의 실시예들에 따르면 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 3차원 적층형 커패시터 어레이 스트링 구조 및 그 동작 방법을 통해 PUF는 3차원 구조에서 스트링 선택 방식에 따라 두 가지 방식으로 활용될 수 있고, 랜덤하게 스트링을 선택하면 챌린지(입력)-리스폰스(출력) 모드로 이용이 가능하다. 이는 3차원 구조를 이용하기 때문에 챌린지-리스폰스 쌍의 개수가 지수적으로 증가하여 매우 강한 물리적 복제 불가 함수로써 이용될 수 있다. 추가적으로 한 개의 스트링만 선택하게 된다면 각 2차원 어레이를 각각 독립된 개별 물리적 복제 불가 함수로 이용하는 모드로, 하나의 어레이 내에서 다중 PUF칩 동작을 수행할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 스트링 구조를 나타내는 도면이다.

도 2는 본 발명의 일 실시예에 따른 챌린지-리스폰스 모드를 설명하기 위한 도면이다.

도 3은 본 발명의 일 실시예에 따른 멀티 칩 모드를 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이의 동작 방법을 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 TANOS스택을 갖는 MOS 커패시터의 단면 TEM 이미지를 나타내는 도면이다.

도 6은 본 발명의 일 실시예에 따른 MOS 커패시터의 서로 다른 임계 전압에 대한 충전 전류를 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 CRP 모드의 해밍 가중치 분포, 인터 해밍 거리 분포, 멀티 칩 모드에 대한 인트라 해밍 거리 분포를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명은 3차원 적층형 커패시터 어레이 구조를 통해 두 가지 방안으로 활용될 수 있는 하드웨어 기반 보안기술인 물리적 복제 불가 함수(Physical Unclonable Function; PUF) 기술을 제안한다. PUF는 3차원 구조에서 스트링 선택 방식에 따라 두 가지 방식으로 활용될 수 있고, 랜덤하게 스트링을 선택하면 챌린지(입력)-리스폰스(출력) 모드로 이용이 가능하다. 이는 3차원 구조를 이용하기 때문에 챌린지-리스폰스 쌍의 개수가 지수적으로 증가하여 매우 강한 물리적 복제 불가 함수로써 이용될 수 있다. 추가적으로 한 개의 스트링만 선택하게 된다면 각 2차원 어레이를 각각 독립된 개별 물리적 복제 불가 함수로 이용하는 모드로, 하나의 어레이 내에서 다중 PUF칩 동작을 수행할 수 있다. 본 발명은 소프트웨어 기반의 방식들과는 달리 메모리 반도체의 3차원 구조로 예측할 수 없는 하드웨어 물리적 복제 방지 기능을 제안하는 발명이다. 메모리 기능을 갖는 커패시터 소자의 3차원 적층형 어레이 구조를 활용하여 스트링 선택 방식 변경을 통해 각각 챌린지-리스폰스 쌍이 지수적으로 증가할 수 있는 매우 강한 물리적 복제 불가 함수, 각 칩끼리의 산포가 추가된 더욱 랜덤성 있는 물리적 복제 불가 함수로 동작할 수 있다. 하드웨어 보안 기술은 암호화 키 생성 또는 보안인증 과정 등에서 응용될 수 있으며 각종 IoT 기기에서 활용가능 하다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0017] 도 1은 본 발명의 일 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 스트링 구조를 나타내는 도면이다.

[0018] 메모리 소자로 구성된 어레이에서 PUF는 일반적으로 워드라인(wordline; WL)방향으로 챌린지를 인가할 때 비트라인(bitline; BL)에서 추출되는 리스폰스를 통해 보안 및 인증에 사용되도록 구현된다. 이때 챌린지의 인가 방식과 리스폰스 추출 방식은 다양하게 활용되며, 주로 전압 인가를 통해 행렬곱 연산의 결과로 얻을 수 있는 랜덤한 전류 비교를 통해 리스폰스를 추출하게 된다.

[0019] 이때 제조 상의 공정 편차 및 소자 간의 편차, 프로그램 이레이즈 동작에 의한 편차 등을 활용하여 PUF 기능을 구현하기 때문에 랜덤성 있는 PUF 칩을 위한 랜덤한 소스를 얻는 것이 중요하다. 또한, 한 번 보안과 인증에 사용된 챌린지-리스폰스 쌍은 재사용할 수 없기 때문에 최대한 많은 챌린지-리스폰스 쌍을 얻는 것이 중요한 요소가 된다.

[0020] 본 발명에서는 3차원 적층형 커패시터 어레이의 구조적인 특징을 통해 스트링 선택 방식의 차이를 이용하여 두 가지 모드로 이용할 수 있는 PUF 기술을 제안한다. 이는 지수적으로 챌린지-리스폰스가 증가하는 매우 강한 PUF 모드와 2차원 PUF끼리의 편차를 추가적인 랜덤 소스로 이용하여 더욱 랜덤성 있는 PUF 모드로 활용할 수 있음을 보장한다.

[0021] 본 발명의 일 실시예에 따른 3차원 적층형 커패시터 어레이의 구조(WL i개, 스트링 j개, BL k개)와 각 모드를 이용하기 위한 평면 선택 방법을 나타낸다. 해당 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고, 이를 통해 스트링 선택의 방식을 다르게 함으로써 두 가지 모드의 동작이 가능

하다.

[0022] 본 발명의 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이 스트링 구조는 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 챌린지가 인가되는 워드라인(Wordline)(110), 상기 인가되는 챌린지에 따른 리스폰스가 추출되는 비트라인(Bitline)(120) 및 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조를 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 스트링(130)을 포함한다.

[0023] 본 발명의 실시예에 따르면, 상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고, 이를 통해 스트링 선택의 방식을 다르게 함으로써 두 가지 모드의 동작이 가능하다.

[0024] 본 발명의 실시예에 따르면, 상기 워드라인(110), 상기 비트라인(120) 및 상기 스트링(130)의 선택 방식에 따라 챌린지-리스폰스 모드(141) 또는 멀티 칩 모드(142)의 동작을 위한 3차원 적층형 커패시터 어레이 구조의 평면을 선택할 수 있다.

[0025] 3차원 구조의 메모리 어레이를 이용하게 되면 PUF칩의 챌린지-리스폰스 쌍의 개수를 지수적으로 증가할 수 있으며, 이를 통해 매우 강한 PUF로써 동작할 수 있어 보안성을 높일 수 있다. 또한, 스트링 선택을 하나씩만 하게 된다면 개별적으로 독립된 2차원 PUF칩 여러 개로 이용할 수 있기 때문에 단일 메모리 칩 내에서의 멀티 PUF칩 구동이 가능해진다. 기본적인 PUF칩의 랜덤한 특성에 PUF칩끼리의 편차를 추가적으로 이용할 수 있기 때문에 보다 더 큰 랜덤성을 보장할 수 있다.

[0026] 본 발명의 일 실시예에 따르면, 상기 워드라인(110), 상기 비트라인(120) 및 상기 스트링(130)의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xyz 평면을 모두 활용하여 PUF를 이용한 보안키의 수를 최대화하기 위해 모든 워드 라인과 스트링 선택을 랜덤으로 설정하여 챌린지-리스폰스 모드(141)의 동작원리를 나타낼 수 있다.

[0027] 본 발명의 또 다른 실시예에 따르면, 상기 워드라인(110), 상기 비트라인(120) 및 상기 스트링(130)의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xz 평면을 하나의 PUF 칩으로 활용하여 z 방향으로의 독립적인 개별 PUF 칩 활용을 통한 멀티 칩 모드(141)의 동작원리를 나타낼 수 있다.

[0029] 도 2는 본 발명의 일 실시예에 따른 챌린지-리스폰스 모드를 설명하기 위한 도면이다.

[0030] 도 2는 3차원 xyz 평면을 모두 활용하여 보안키의 수를 극대화할 수 있는 챌린지-리스폰스 모드의 동작원리를 나타낸다. 이때 모든 워드 라인과 스트링 선택을 랜덤으로 설정할 때 설정 할 수 있는 입력 수가 지수적으로 증가될 수 있기 때문에 챌린지-리스폰스 쌍의 개수가 지수적으로 증가하게 되어 보안 수준이 높은 매우 강한 PUF로 동작할 수 있게 된다.

[0031] 본 발명의 일 실시예에서, 만약 BL을 2개 랜덤하게 선택하여 비교하는 형태로 리스폰스를 생성하는 방법을 선택할 경우 WL 선택 방법 2^i개, 스트링 선택 방법 2^j개, BL 선택 방법 ${}_kC_2$개를 곱한 전체 CRP(Challenge-Response Pair) 개수($2^i \times 2^j \times {}_kC_2$)를 확보할 수 있다. 하지만, 이는 일 실시예일뿐, 이외에도 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 다양한 CRP을 생성하여 평면 선택에 따른 동작 모드를 나타낼 수 있다.

[0033] 도 3은 본 발명의 일 실시예에 따른 멀티 칩 모드를 설명하기 위한 도면이다.

[0034] 도 3은 3차원 구조에서 xz 평면을 하나의 PUF칩으로 활용하여 z 방향으로의 독립적인 개별 PUF칩 활용을 통한 멀티 칩 모드의 동작원리를 나타낸다. 하나의 스트링을 선택할 경우 각 스트링에 해당하는 2차원 어레이를 하나의 PUF칩으로 독립적으로 이용할 수 있게 되며, 하나의 메모리 칩에서 멀티 PUF칩을 활용할 수 있는 멀티 칩 모드 동작이 가능하다. 위와 마찬가지로 만약 BL을 2개 랜덤하게 선택하여 비교하는 형태로 리스폰스를 생성하는 방법을 선택할 경우 WL 선택 방법 2^i개, BL 선택 방법 ${}_kC_2$개를 곱한 전체 CRP 개수($2^i \times {}_kC_2$) 확보가 가능하다. 이는 일 실시예일뿐, 이외에도 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 다양한 CRP을

생성하여 평면 선택에 따른 동작 모드를 나타낼 수 있다.

[0036] 도 4는 본 발명의 일 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이의 동작 방법을 설명하기 위한 흐름도이다.

[0037] 본 발명의 일 실시예에 따른 물리적 복제불가 함수를 위한 3차원 적층형 커패시터 어레이의 동작 방법은 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 워드라인(Wordline)으로 챌린지가 인가되는 단계(410), 상기 인가되는 챌린지에 따른 리스폰스가 비트라인(Bitline)으로부터 추출되는 단계(420) 및 PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출하는 단계(430)를 포함한다.

[0038] 단계(410)에서, 물리적 복제 불가 함수(Physical Unclonable Function; PUF)를 위한 메모리 소자로 구성된 어레이에서 워드라인(Wordline)으로 챌린지가 인가된다.

[0039] 단계(420)에서, 상기 인가되는 챌린지에 따른 리스폰스가 비트라인(Bitline)으로부터 추출되나.

[0040] 단계(430)에서, PUF를 위한 암호화를 수행하기 위해 3차원 적층형 커패시터 어레이 구조의 스트링을 이용하여 선택 방식의 차이에 따라 복수의 챌린지-리스폰스 쌍을 추출한다.

[0041] 본 발명의 실시예에 따르면, 상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고, 이를 통해 스트링 선택의 방식을 다르게 함으로써 두 가지 모드의 동작이 가능하다.

[0042] 단계(430)에서, 상기 3차원 적층형 커패시터 어레이 구조에서 커패시터 소자들은 병렬 연결되어 있기 때문에 병렬 연산 동작이 가능하고, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 챌린지-리스폰스 모드(431) 또는 멀티 칩 모드(432)의 동작을 위한 3차원 적층형 커패시터 어레이 구조의 평면을 선택한다.

[0043] 단계(431)에서, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xyz 평면을 모두 활용하여 PUF를 이용한 보안키의 수를 최대화하기 위해 모든 워드 라인과 스트링 선택을 랜덤으로 설정하여 챌린지-리스폰스 모드에서 동작할 수 있다.

[0044] 단계(432)에서, 상기 워드라인, 상기 비트라인 및 상기 스트링의 선택 방식에 따라 3차원 적층형 커패시터 어레이 구조의 xz 평면을 하나의 PUF 칩으로 활용하여 z 방향으로의 독립적인 개별 PUF 칩 활용을 통한 멀티 칩 모드에서 동작할 수 있다.

[0046] 도 5는 본 발명의 일 실시예에 따른 TANOS스택을 갖는 MOS 커패시터의 단면 TEM 이미지를 나타내는 도면이다.

[0047] 본 발명의 구체적인 실시예는 TANOS($TiN/Al_2O_3/Si_3N_4/SiO_2/Si$) 스택을 갖는 MOS 커패시터 어레이를 활용한다. 해당 구조는 전하트랩 레이어에 전하를 저장하는 정도에 따라 문턱 전압이 바뀌어 메모리 기능을 갖는 커패시터로 동작할 수 있다. 본 발명은 해당 구조에 국한되지 않으며 메모리 기능을 갖는 커패시터(ferroelectric capacitor 등) 어레이에 적용될 수 있다.

[0049] 도 6은 본 발명의 일 실시예에 따른 MOS 커패시터의 서로 다른 임계 전압에 대한 충전 전류를 나타내는 도면이다.

[0050] 커패시터를 읽는 동작 메커니즘은, 먼저 게이트 전극에 충전 전압(Vc)을 인가하여 커패시터를 충전한다. 그런 다음 게이트 바이어스를 방전 전압(Vd)으로 변경하여 BL 방향을 통해 커패시터 양단에 축적된 전하를 감지한다. MOS 커패시터의 문턱전압(Vth)은 전하 트랩층 덕분에 프로그램 및 소거 동작에 의해 조절될 수 있으므로 그에 따라 축적된 전하가 변조될 수 있다. Vc에서 Vd로의 천이 기간 동안 방전 전류는 BL 방향으로 흐르며, 이 기간 동안 방전되는 전하량(Q)은 커패시터의 Vth에 의해 결정된다.

[0052] 도 7은 본 발명의 일 실시예에 따른 CRP 모드의 해밍 가중치 분포, 인터 해밍 거리 분포, 멀티 칩 모드에 대한 인트라 해밍 거리 분포를 나타내는 도면이다.

[0053] 본 발명의 일 실시예에 따른 MOS 커패시터의 동작 특성을 바탕으로 3차원 적층형 커패시터 어레이를 구성하고 각 모드로 동작시켰을 때 PUF의 동작 특성을 도 7과 같이 확인하였으며 50%에 가까운 균일성, 확산성, 고유성을 두 두 가지 모드 모두에서 확보 가능하다.

[0054] 본 발명의 실시예에 따른 두 가지 작동 모드에 대해 가능한 BL 선택 사례($_{16}C_2$= 120비트 키)의 수를 그룹화하여 주요 PUF 메트릭이 분석된다. 1k 챌린지는 멀티 칩 모드에서 1k 무작위 WL 선택으로 테스트되지만 CRP 모드에서는 1k 무작위 문자열 선택이 추가되어 1M 챌린지가 테스트된다. 추출된 해밍 가중치 분포는 도 7(a)에 도시된 바와 같이, 두 모드에서 추출된 균일성이 ~50%임을 확인할 수 있다. 도 7(b)에 도시된 바와 같이, 멀티 칩 모드와 CRP 모드에 대해 각각 총 해밍 거리 $_{1k}C_2$ = ~500k 및 $_{1M}C_2$ = ~0.5T를 사용하여 ~50%의 확산도가 검증되었다. 하나의 3D 배열 구조에서 다중 PUF 칩의 고유성은 도 7(c)와 같이 문자열(z) 축(총 해밍 거리 1,000×$_{16}C_2$ = 120k)을 따라 16개의 PUF 인스턴스에서 ~50%로 평가됩니다.

[0056] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0057] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

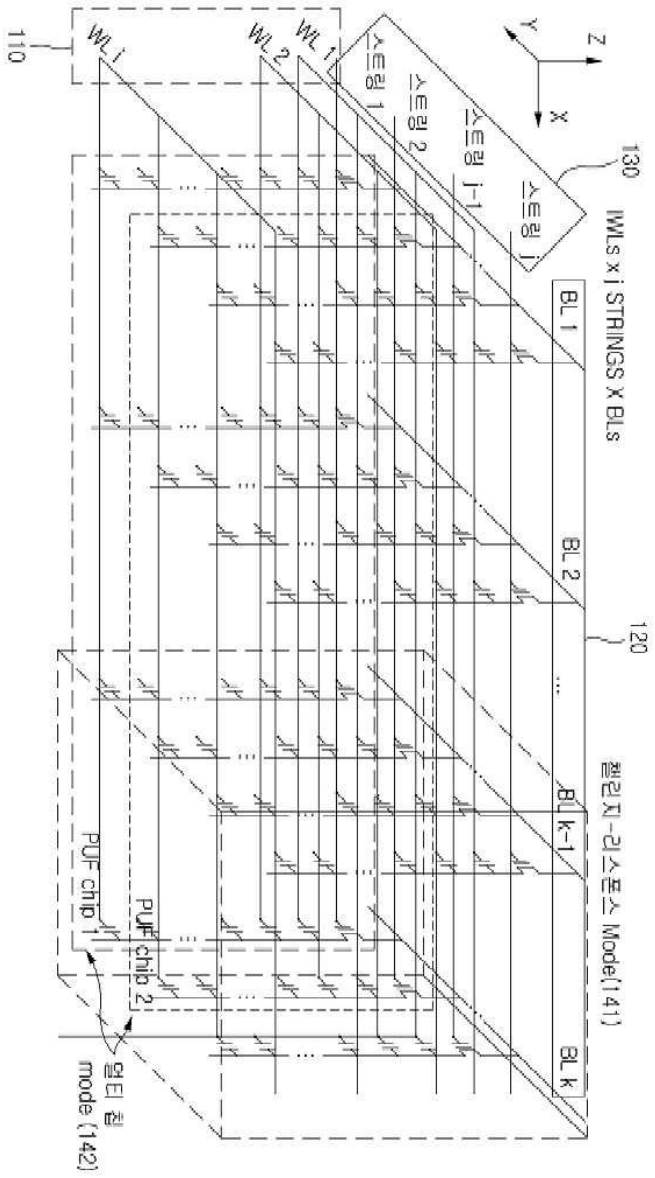
[0058] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0059] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

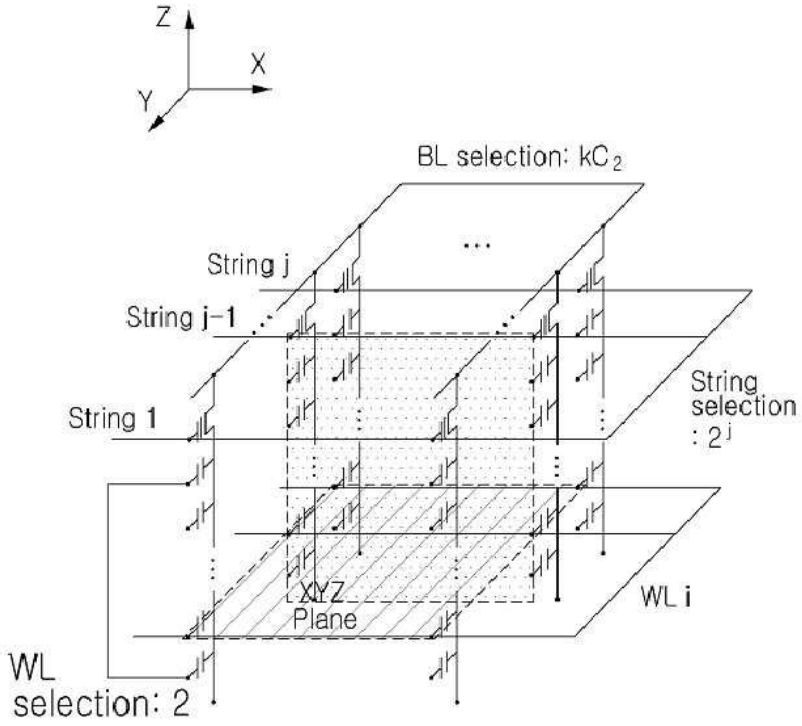
[0060] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

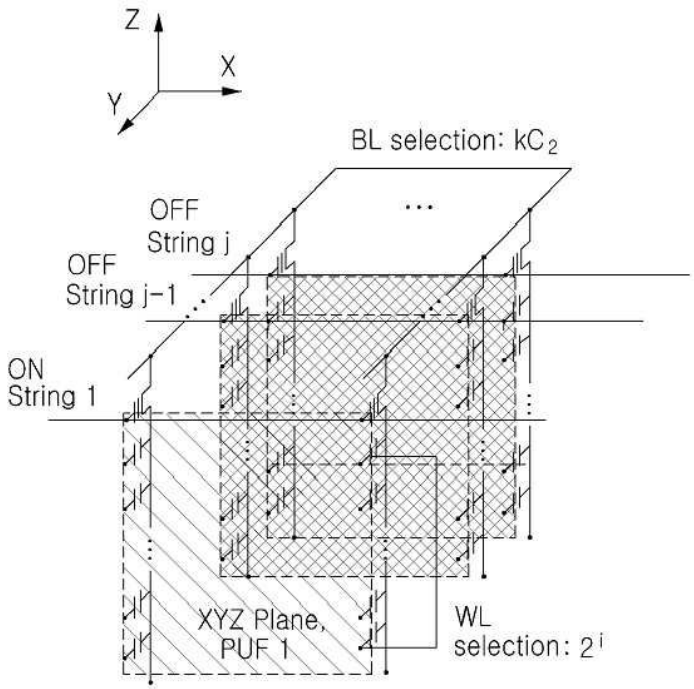
도면1


110
WL i
WL 2
WL 1
스트링 1
스트링 2
스트링 j-1
스트링 j
130
IWLs x j STRINGS X BLs
BL 1
BL 2
BL k-1
BL k
120
챌린지-리스폰스 Mode(141)
PUF chip 1
PUF chip 2
멀티 칩 mode (142)
Z
Y
X

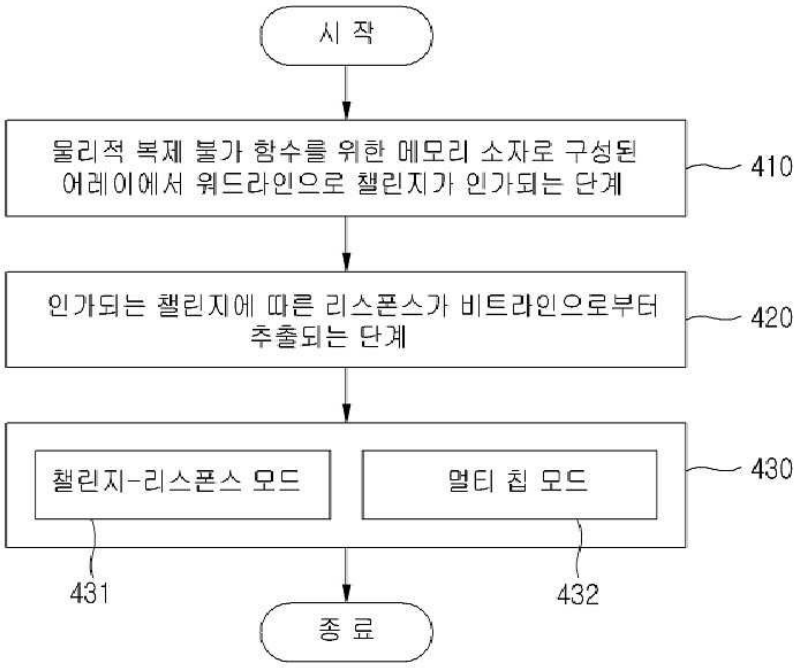
도면2


Z
X
Y
BL selection: kC2
String j
String j-1
String 1
String selection : 2j
XYZ Plane
WL i
WL selection: 2

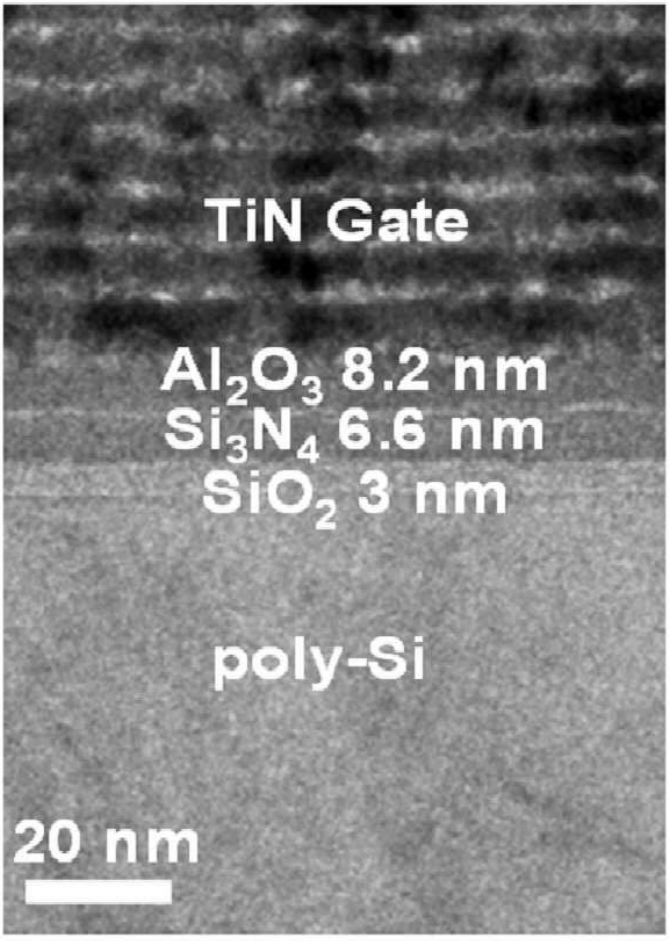
도면3


Z
X
Y
BL selection: kC2
OFF String j
OFF String j-1
ON String 1
XYZ Plane, PUF 1
WL selection: 2i

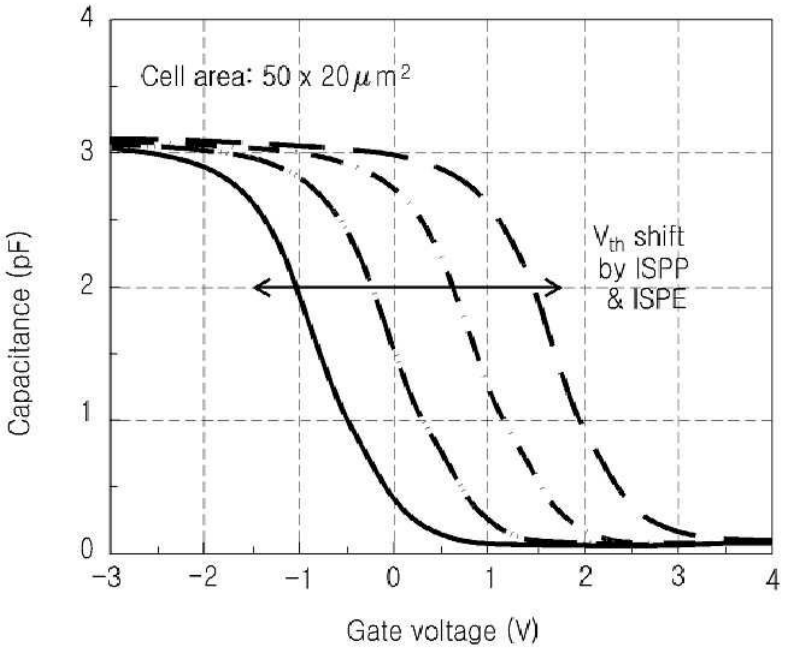
도면4


시 작
물리적 복제 불가 함수를 위한 메모리 소자로 구성된 어레이에서 워드라인으로 챌린지가 인가되는 단계
410
인가되는 챌린지에 따른 리스폰스가 비트라인으로부터 추출되는 단계
420
챌린지-리스폰스 모드
멀티 칩 모드
430
431
432
종 료

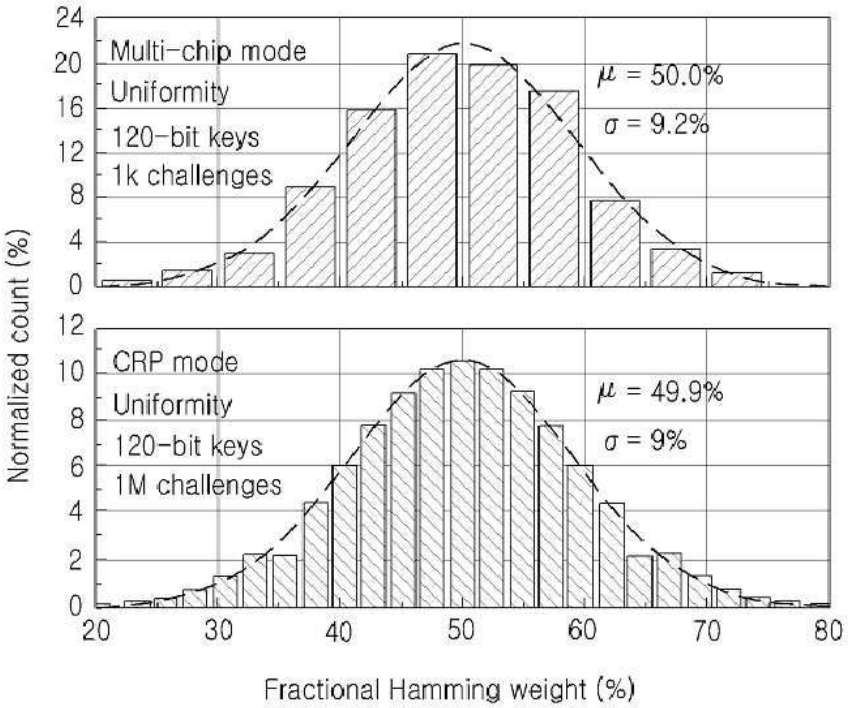
도면5


TiN Gate
Al_2O_3 8.2 nm
Si_3N_4 6.6 nm
SiO_2 3 nm
poly-Si
20 nm

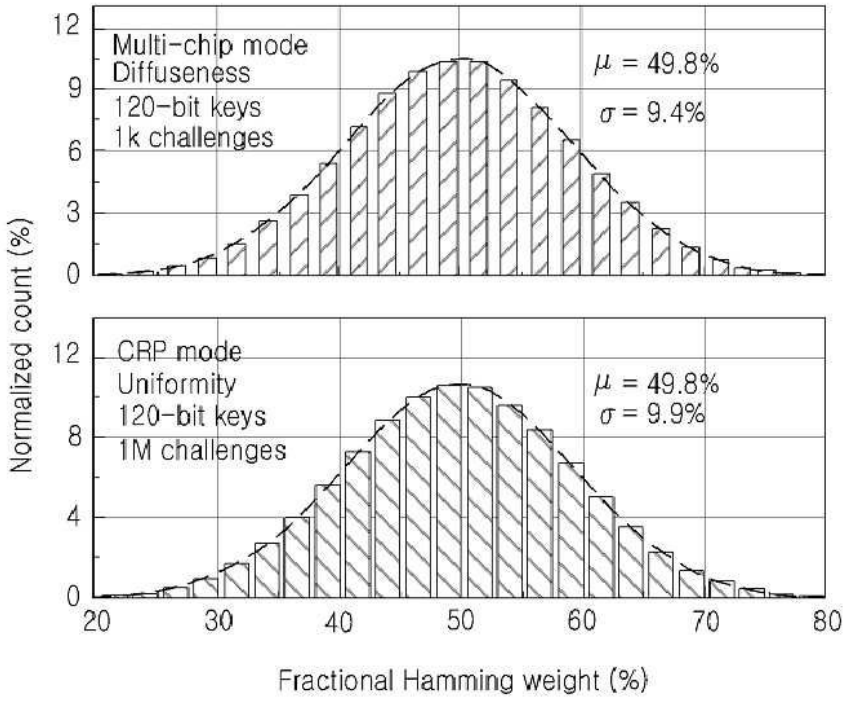
도면6


Cell area: 50 x 20 μm²
Vth shift
by ISPP
& ISPE
Capacitance (pF)
Gate voltage (V)
4
3
2
1
0
−3
−2
−1
0
1
2
3
4

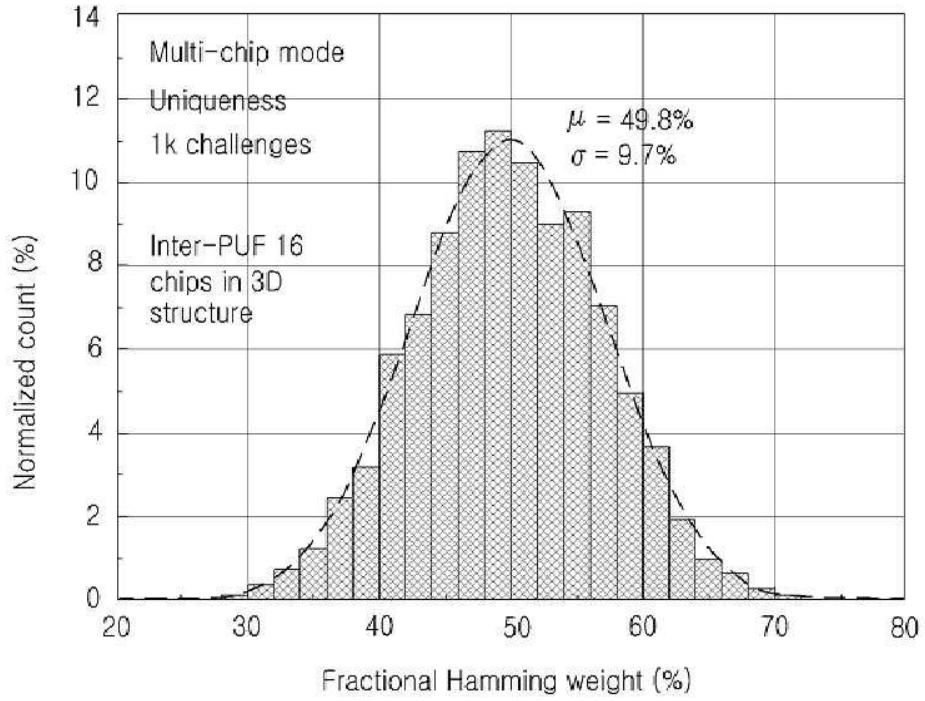
도면7a


Multi-chip mode
Uniformity
120-bit keys
1k challenges
μ = 50.0%
σ = 9.2%
CRP mode
Uniformity
120-bit keys
1M challenges
μ = 49.9%
σ = 9%
Normalized count (%)
Fractional Hamming weight (%)
20
30
40
50
60
70
80

도면7b


Multi-chip mode
Diffuseness
120-bit keys
1k challenges
μ = 49.8%
σ = 9.4%
CRP mode
Uniformity
120-bit keys
1M challenges
μ = 49.8%
σ = 9.9%
Normalized count (%)
Fractional Hamming weight (%)

도면7c


Multi-chip mode
Uniqueness
1k challenges
Inter-PUF 16
chips in 3D
structure
μ = 49.8%
σ = 9.7%
Normalized count (%)
Fractional Hamming weight (%)