



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2021년04월30일

(11) 등록번호 10-2246513

(24) 등록일자 2021년04월26일

(51) 국제특허분류(Int. Cl.)

G06F 7/58 (2006.01)

(52) CPC특허분류

G06F 7/588 (2013.01)

(21) 출원번호 10-2020-0016520

(22) 출원일자 2020년02월11일

심사청구일자 2020년02월11일

(56) 선행기술조사문헌

KR101610625 B1

KR1020150026737 A

KR1020190016800 A

JP2017010530 A

(73) 특허권자

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

신형순

서울특별시 서초구 반포대로5길 65, 102동 301호 (서초동, 아이파크빌)

김다영

서울특별시 중랑구 사가정로42길 90, 502동 301호 (면목동, 면목두산아파트)

(뒷면에 계속)

(74) 대리인

특허법인엠에이피에스

전체 청구항 수 : 총 12 항

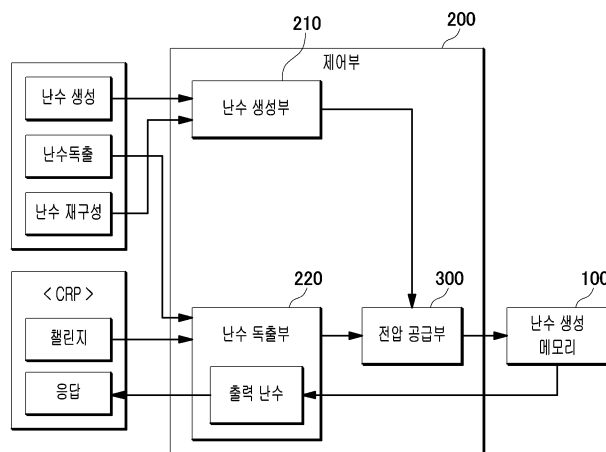
심사관 : 지정훈

(54) 발명의 명칭 물리적 복제 방지 기능을 가진 난수 발생 장치

(57) 요약

본 발명의 일측면에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치는 저항성 메모리로 이루어진 난수 생성 메모리; 난수 생성 모드에 따라, 상기 난수 생성 메모리에 난수를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하고, 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하고, 난수 독출 모드에 따라, 상기 난수 생성 메모리에 기록된 데이터를 독출하여, 난수로서 출력하는 제어부; 및 상기 난수 생성 모드시에 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리의 워드라인 및 비트라인에 전압을 공급하거나, 상기 난수 독출 모드시에 상기 난수 생성 메모리의 워드라인 및 비트라인에 독출 전압을 공급하는 전압 공급부를 포함한다.

대표도 - 도1



(72) 발명자

선우경

서울특별시 서대문구 북아현로4마길 18-6, 2층 (북아현동)

이정원

서울특별시 광진구 용마산로1길 78, 1동 603호 (중곡동, 대영아파트)

최서연

경기도 수원시 영통구 에듀타운로 65, 5203동 1304호 (이의동, 자연엔자이)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711098989

부처명 과학기술정보통신부

과제관리(전문)기관명 한국연구재단

연구사업명 개인기초연구(과기정통부)(R&D)

연구과제명 CRP(Challenge-Response Pair) 극대화를 위한 멀티비트 맴리스터 기반 PUF(Physical Unclonable Function) 아키텍처 개발

기 여 율 1/1

과제수행기관명 이화여자대학교

연구기간 2019.09.01 ~ 2020.02.29

명세서

청구범위

청구항 1

물리적 복제 방지 기능을 가진 난수 발생 장치에 있어서,

저항성 메모리로 이루어진 난수 생성 메모리;

난수 생성 모드에 따라, 상기 난수 생성 메모리에 난수를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하고, 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하고, 난수 독출 모드에 따라, 상기 난수 생성 메모리에 기록된 데이터를 독출하여, 난수로서 출력 하는 제어부;

상기 난수 생성 모드시에 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리의 워드라인 및 비트라인에 전압을 공급하거나, 상기 난수 독출 모드시에 상기 난수 생성 메모리의 워드라인 및 비트라인에 독출 전압을 공급하는 전압 공급부를 포함하는 난수 발생 장치.

청구항 2

제 1 항에 있어서,

상기 제어부는 난수 생성 모드에서,

상기 비트라인에 미리 설정된 레벨의 고정 전압이 인가되도록 하고, 각 워드라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 데이터가 기록되도록 하거나,

상기 워드라인에 미리 설정된 레벨의 고정 전압이 인가되도록 하고, 각 비트라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 데이터가 기록되도록 하고,

상기 각 교류파는 구형파, 삼각파 또는 사인파 중 어느 하나로 결정되고, 그 주기 및 진폭이 상이하게 설정될 수 있는 것인 난수 발생 장치.

청구항 3

제 1 항에 있어서,

상기 제어부는 난수 생성 모드에서,

상기 각 워드라인과 비트라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 데이터가 기록되도록 하되,

상기 각 교류파는 구형파, 삼각파 또는 사인파 중 어느 하나로 결정되고, 그 주기 및 진폭이 상이하게 설정될 수 있는 것인 난수 발생 장치.

청구항 4

제 1 항에 있어서,

상기 제어부는 난수 독출 모드에서,

랜덤하게 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 난수가 출력되도록 하는 것인 난수 발생 장치.

청구항 5

제 1 항에 있어서,

상기 제어부는 난수 독출 모드에서,

입력되는 쉘런지 값에 따라 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라

인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 챌린지 값에 대응하는 응답 난수가 출력되도록 하는 것인 난수 발생 장치.

청구항 6

제 5 항에 있어서,

상기 응답 난수는 외부 컴퓨팅 장치로 전송되어, 상기 챌린지 값과 응답 난수가 매칭되어 CRP 테이블에 저장되거나, 상기 챌린지 값과 응답 난수가 매칭된 CRP 테이블과 비교되어 인증 절차에 사용되는 것인 난수 발생 장치.

청구항 7

제 5 항에 있어서,

상기 제어부는 난수 생성 모드에서,

미리 설정된 복수개의 교류파의 조합 중 어느 하나의 교류파 조합을 선택하고, 선택된 교류파 조합에 의하여 데이터가 기록되도록 하고,

해당 교류파 조합에 대한 정보를 외부 컴퓨팅 장치로 전송하여, 상기 챌린지 값과 응답 난수가 매칭되어 생성된 CRP 테이블과 교류파 조합의 정보가 매칭되어 저장되도록 하는 것인 난수 발생 장치.

청구항 8

제 1 항에 있어서,

상기 제어부는

상기 난수 생성 메모리를 초기화한 후 상기 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 재선택하고, 상기 재선택된 교류파의 조합에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하는 것인 난수 발생 장치.

청구항 9

제 8 항에 있어서,

상기 제어부는 외부 컴퓨팅 장치로부터 수신한 교류파 조합의 식별 정보에 기초하여, 상기 교류파의 조합을 재선택하는 것인 난수 발생 장치.

청구항 10

물리적 복제 방지 기능을 갖는 난수 발생 장치의 동작 방법에 있어서,

상기 난수 발생 장치에 포함된 난수 생성 메모리에 데이터를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하는 단계;

상기 교류파의 조합 정보에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하는 단계; 및

상기 난수 생성 메모리에 기록된 데이터를 독출하여, 난수로서 출력하는 단계를 포함하되,

상기 교류파의 조합 정보는 각 워드라인 또는 비트라인별로 인가될 교류파의 종류와 각 교류파의 주기, 교류파의 지속시간 또는 진폭 설정에 대한 정보를 포함하는 것인 난수 발생 장치의 동작 방법.

청구항 11

제 10 항에 있어서,

입력되는 챌린지 값에 따라 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 챌린지 값에 대응하는 응답 난수가 출력되도록 하는 단계를 더 포함하되,

상기 응답 난수는 외부 컴퓨팅 장치로 전송되어, 상기 챌린지 값과 응답 난수가 매칭되어 CRP 테이블에 저장되거나, 상기 챌린지 값과 응답 난수가 매칭된 CRP 테이블과 비교되어 인증 절차에 사용되는 것인 난수 발생 장치

의 동작 방법.

청구항 12

제 10항에 있어서,

외부 컴퓨팅 장치로부터 교류파 조합의 식별 정보와 챌린지를 수신하는 단계;

상기 교류파 조합의 식별 정보에 기초하여, 상기 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 재선택하고, 상기 재선택된 교류파의 조합에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하는 난수 재구성을 수행하는 단계; 및

상기 난수 재구성이 완료된 난수 생성 메모리에 대하여, 상기 수신한 챌린지 값에 따라 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 챌린지 값에 대응하는 응답 난수가 출력되도록 하는 단계를 더 포함하되,

상기 응답 난수는 상기 챌린지 값과 응답 난수가 매칭된 CRP 테이블과 비교되어 인증 절차에 사용되는 것인 난수 발생 장치의 동작 방법.

발명의 설명

기술 분야

[0001] 본 발명은 물리적 복제 방지 기능을 가진 난수 발생 장치에 대한 것이다.

배경 기술

[0002] 본 발명은 하드웨어 보안 솔루션의 일종으로 하드웨어 장비에서 나타나는 공정 편차를 보안 키 생성에 활용하는 PUF 기술의 칩 구현에 필요한 난수 발생 회로에 관한 것이다

[0003] 기존의 하드웨어 기반 보안은 키(key)를 비휘발성 메모리에 저장해 두는 방식으로 진행되지만, 물리적 공격을 이용한 알고리즘 해킹 속도가 가속화됨에 따라 비휘발성 메모리에 저장된 디지털 키가 보안에 취약하다는 문제가 발생하게 되었다. 이를 극복하기 위해 유일한 휘발성 디지털 키를 생성하는 하드웨어 기반 보안 방식의 일종인 물리적 복제 방지 기술 (Physical Unclonable Function, PUF)이 연구 개발되고 있다.

[0004] PUF 기술은 하드웨어 장비에서 나타나는 예측 불가능하고 조절 불가능한 공정 편차를 디지털 키 생성에 활용하여, 간단한 하드웨어 칩으로 소프트웨어 보안 방식의 단점을 보완하므로, 보다 강력한 키 관리가 가능하다는 장점이 있다.

[0005] 기존의 PUF 기술은 주로 CMOS를 포함한 회로 기반 방식으로 제작되며, 대표적으로 아비터(Arbiter) PUF 나 링 오실레이터(Ring Oscillator)PUF 가 알려져 있다. 이러한 CMOS 회로 기반 PUF 의 경우, 상대적으로 전력과 면적 소모가 크다는 단점과 함께, 최근에는 이들을 시뮬레이션 하여 공격하는 방식이 고안되기 시작하는 등의 단점이 존재한다.

[0006] CMOS 회로 기반 PUF 대신 보안 성능이 더 뛰어나고, 전력과 면적 측면에서 유리한 나노전자 소자, 예를 들면, 멤리스터(Memristor), 탄소나노튜브 FET(CNFET), 상변화 메모리(PCM) 또는 STT-MRAM 등, 저항성 메모리 기반의 PUF 가 고안되기 시작하였다. 멤리스터 PUF 는 그 중에서도 공정 과정에서의 민감도가 높아 PUF 로서 사용하기 유리하고, CMOS 공정과 호환되어 제작 비용이 절감된다는 장점이 있다.

[0007] 기존의 멤리스터 PUF 는 주로 2D 배열 형태로 여러 개의 멤리스터가 배열되었을 때 각 멤리스터 별로 서로 다른 전기 저항을 갖는다는 편차를 이용하여 난수, 즉 무작위의 출력 비트를 생성하였다. 그러나, 이러한 방식의 경우 챌린지 응답 쌍(Challenge - Response Pair, CRP) 개수가 적어 보안 성능이 낮다는 단점이 있으며, 이를 극복하기 위해 2D 배열의 크기를 늘릴 경우 PUF 칩의 면적이 커져 하드웨어 보안으로 사용하기에 부적절하다는 단점이 있다. 또한, 제품 출시 단계에서 CRP 가 특정되면, 하나의 PUF 칩으로서 기능하게 되며, 이를 변경할 수 없게 된다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국등록특허 제 10-1566949 호(발명의 명칭: 가변구조형 PUF 장치 및 그의 동작 방법)

발명의 내용

해결하려는 과제

[0009] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 저항성 메모리 소자의 전기 저항 편차를 변경시키는 동작을 통해 다양한 전기 저항 편차를 갖는 PUF 칩을 생성할 수 있는 난수 발생 장치를 제공하고자 한다.

[0010] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0011] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 일측면에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치는 저항성 메모리로 이루어진 난수 생성 메모리; 난수 생성 모드에 따라, 상기 난수 생성 메모리에 난수를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하고, 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하고, 난수 독출 모드에 따라, 상기 난수 생성 메모리에 기록된 데이터를 독출하여, 난수로서 출력 하는 제어부; 및 상기 난수 생성 모드시에 상기 선택된 교류파의 조합에 따라 상기 난수 생성 메모리의 워드라인 및 비트라인에 전압을 공급하거나, 상기 난수 독출 모드시에 상기 난수 생성 메모리의 워드라인 및 비트라인에 독출 전압을 공급하는 전압 공급부를 포함한다.

[0012] 또한, 본 발명의 다른 측면에 따른 물리적 복제 방지 기능을 갖는 난수 발생 장치의 동작 방법은 상기 난수 발생 장치에 포함된 난수 생성 메모리에 데이터를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하는 단계; 상기 교류파의 조합 정보에 따라 상기 난수 생성 메모리에 데이터가 기록되도록 하는 단계; 및 상기 난수 생성 메모리에 기록된 데이터를 독출하여, 난수로서 출력하는 단계를 포함한다. 이때, 교류파의 조합 정보는 각 워드라인 또는 비트라인별로 인가될 교류파의 종류와 각 교류파의 주기, 교류파의 지속 시간 또는 진폭 설정에 대한 정보를 포함한다.

발명의 효과

[0013] 전술한 본 발명의 과제 해결 수단에 의하면, 교류파 조합에 따라 하나의 저항성 메모리로부터 다수의 CRP 데이터를 생성할 수 있으며, 이에 따라 하나의 난수 발생 장치가 복수의 PUF 칩으로 기능할 수 있도록 한다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치를 도시한 블록도이다.

도 2 는 본 발명의 일 실시예에 따른 난수 발생 장치의 교류파 선택 과정을 설명하기 위한 도면이다.

도 3은 본 발명의 본 발명의 일 실시예에 따른 난수 발생 장치가 선택된 교류파를 이용하여 난수 생성 메모리에 데이터를 기록하는 과정을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 난수 발생 장치의 전기 저항 변화를 도시한 그래프이다.

도 5는 본 발명의 일 실시예에 따른 난수 발생 장치의 저항 분포를 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 독출 과정을 도시한 도면이다.

도 7은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치의 동작 방법을 도시한 순서도이다.

도 8은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할

수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

- [0016] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0017] 도 1은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치를 도시한 블록도이다.
- [0018] 도시된 바와 같이, 난수 발생 장치(10)는 난수 생성 메모리(100), 제어부(200) 및 전압 공급부(300)를 포함한다.
- [0019] 난수 생성 메모리(100)는 저항성 메모리로 이루어지며, 예를 들면, 램리스터, 탄소나노튜브 FET(CNFET), 상변화 메모리(PCM) 또는 STT-MRAM 등으로 이루어질 수 있다. 저항성 메모리는 DRAM 등의 메모리에 비하여, 데이터 기록에 따라는 상태값들의 산포가 넓은 편이다. 따라서, DRAM 등에 비하여 랜덤성을 갖기 유리한 특성을 가지며, 본 발명에서는 이러한 저항성 메모리 소자의 특성을 활용하고자 한다.
- [0020] 제어부(200)는 난수 생성 메모리(100)에 대하여, 난수를 생성하여 기록하는 난수 생성 모드, 기록된 난수를 출력하는 난수 독출 모드, 새로운 PUF 칩으로 설정하는 난수 재구성 모드를 각각 수행한다.
- [0021] 제어부(200)는 난수 생성 모드에 따라, 난수 생성 메모리(100)에 난수를 기록하는 과정에서 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 선택하고, 선택된 교류파의 조합 정보에 따라 난수 생성 메모리(100)에 난수가 기록되도록 한다. 또한, 제어부(200)는 난수 독출 모드에 따라, 난수 생성 메모리(100)에 기록된 난수 데이터를 독출하도록 한다. 또한, 제어부(200)는 난수 재구성 모드에 따라, 난수 생성 메모리(100)를 초기화한 후 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 재선택하고, 재선택된 교류파의 조합 정보에 따라 난수 생성 메모리(100)에 난수가 기록되도록 한다. 이때, 교류파의 조합 정보는 각 워드라인 또는 비트라인별로 인가될 교류파의 종류와 각 교류파의 주기, 교류파의 지속시간 또는 진폭 설정에 대한 정보를 포함한다.
- [0022] 도 2 는 본 발명의 일 실시예에 따른 난수 발생 장치의 교류파 선택 과정을 설명하기 위한 도면이고, 도 3은 본 발명의 본 발명의 일 실시예에 따른 난수 발생 장치가 선택된 교류파를 이용하여 난수 생성 메모리에 데이터를 기록하는 과정을 설명하기 위한 도면이다.
- [0023] 도 2에서 도시된 바와 같이, 본 발명에서는 구형파, 삼각파 또는 사인파와 같은 다양한 종류의 교류파에 대하여, 각각의 주기 또는 진폭을 상이하게 설정하고, 이를 각각 워드라인 또는 비트라인에 인가하는 과정을 통해, 난수 생성 메모리(100)에 대하여 난수가 기록되도록 할 수 있다. 그리고, 도 3에 도시된 바와 같이, 워드라인별로 이와 같이 선택된 교류파를 서로 상이하게 인가할 수 있다. 도 3의 경우 각 워드라인에 구형파가 인가되는데, 구형파의 진폭은 동일하되, 주기(또는 펄스 폭)가 상이함을 확인할 수 있다.
- [0024] 도 4는 본 발명의 일 실시예에 따른 난수 발생 장치의 전기 저항 변화를 도시한 그래프이고, 도 5는 본 발명의 일 실시예에 따른 난수 발생 장치의 저항 분포를 설명하기 위한 도면이다.
- [0025] 도 4에 도시된 바와 같이, 각 메모리 셀에 문턱전압 이상의 전압이 인가되는 시간에 따라, 각 셀의 저항 값이 감소하는 성향을 확인할 수 있다. 또한, 같은 주기를 갖는 교류파의 경우, 펄스가 인가되는 횟수에 따라서 저항 값이 감소하는 속도가 상이함을 확인할 수 있다. 또한, 각 셀에 인가되는 교류파의 주기가 상이한 경우, 주기가 느린 교류파(또는 펄스 폭이 긴 교류파)가 인가될 수록 셀의 저항 값이 감소하는 속도도 더 빨라짐을 확인할 수 있다. 이는 곧, 교류파의 주기 또는 교류파가 인가되는 횟수, 교류파의 진폭 등에 따라 각 셀의 저항 값이 서로 상이하게 설정될 수 있음을 의미한다. 이러한 저항성 메모리의 특성을 이용하여, 각 워드라인 또는 비트라인에 상이한 종류의 교류파를 인가할 경우, 각 셀의 저항 값의 편차 또는 데이터 기록 상태의 분포는 상당히 커질 수 있다.
- [0026] 도 5는 워드라인(row)에 일정 전압(1.5V)을 인가하여 각 워드라인 별로 기록 동작을 수행할 뿐만 아니라 추가적으로 비트라인(col)에도 전압을 인가하여 기록 동작을 수행할 때 64x64배열의 저항성 메모리에서 약 3500개의 소자들이 어떤 저항 값을 갖는지를 나타낸 그래프이다. 그림 7을 보면, 검정색으로 도시된 그래프는 기존의 방법에 따라 데이터를 기록하여 저항 편차가 최소화 상태를 도시하고 있다. 적색으로 표시한 것은 워드라인에 대하여 교류파의 주기를 서로 다르게 설정한 결과를 도시한 것이고, 청색으로 표시한 것은 워드라인과 비트라인에

대하여 교류파의 주기를 서로 다르게 설정한 결과를 도시한 것이다. 적색 보다는 청색의 경우가 각 셀의 저항 편차가 넓어진 것을 확인할 수 있으며, 이러한 특성에 따라 저항성 메모리의 셀에 기록된 데이터의 랜덤성이 더욱 향상될 수 있다.

[0027] 이러한 실험 결과를 토대로, 본 발명의 제어부(200)는 비트라인에 미리 설정된 레벨의 고정 전압이 인가되도록 하고, 각 워드라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 난수가 기록되도록 할 수 있다. 또는, 제어부(200)는 각 워드라인에 미리 설정된 레벨의 고정 전압이 인가되도록 하고, 각 비트라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 난수가 기록되도록 할 수 있다. 또는, 제어부(200)는 각 비트라인과 각 워드라인별로 인가될 교류파를 선택하고, 선택된 교류파의 조합에 따라 난수가 기록되도록 할 수 있다. 이와 같은 구성에 따라, 각 워드라인 또는 비트라인에 인가될 교류파는 서로 상이한 주기를 갖거나, 동일한 주기를 가지면서도 그 지속 시간이 상이하거나, 진폭이 상이하도록 설정될 수 있다.

[0028] 이를 위해, 제어부(200)는 난수 생성부(210)와 난수 독출부(220)를 각각 포함할 수 있다. 난수 생성부(210)는 다양한 종류의 교류파 중 각 워드라인 또는 비트라인별로 인가될 교류파를 선택하고, 선택된 교류파의 주기, 교류파의 지속 시간 또는 교류파의 진폭등을 설정한다. 이와 같이 설정된 교류파의 조합에 대한 정보는 전압 공급부(300)에 전달되어, 선택된 교류파에 의하여 난수 생성 메모리(100)에 데이터가 기록되도록 한다.

[0029] 이와 같은 교류파의 조합은 실시간으로 랜덤하게 설정될 수 있으나, 실시예에 따라서는 난수 생성 메모리의 특성에 맞게 조합 상태가 미리 결정된 것일 수 있다. 즉, 각 난수 생성 메모리의 저항 편차 분포가 상이해 지도록, 여러 종류의 교류파 조합이 미리 마련될 수 있으며, 각각의 교류파 조합 정보에 따라 제어부(200)가 난수 생성 동작을 수행할 수 있다. 이러한 구성에 따르면, 각각의 교류파 조합 정보가 제어부(200)에 미리 저장되어 있을 수 있다. 또한, 교류파 조합 정보에 따라 하나의 난수 생성 메모리(10)에 대하여 서로 상이한 복수의 CRP 테이블을 제공할 수 있어, 보안성을 더욱 향상시킬 수 있다.

[0030] 한편, 제어부(200)는 소정의 프로그램이 저장된 메모리 및 이를 수행하는 프로세서로 이루어진 것으로서, 이때 프로세서는 데이터를 처리할 수 있는 모든 종류의 장치를 포함할 수 있다. 예를 들어 프로그램 내에 포함된 코드 또는 명령으로 표현된 기능을 수행하기 위해 물리적으로 구조화된 회로를 갖는, 하드웨어에 내장된 데이터 처리 장치를 의미할 수 있다. 이와 같이 제어부(200) 및 그 내부에 포함된 난수 생성부(210)와 난수 독출부(220)는 프로세서 등에 의하여 구현될 수 있고, 이 프로세서는 마이 크로프로세서(microprocessor), 중앙처리장치(central processing unit: CPU), 프로세서 코어(processor core), 멀티프로세서(multiprocessor), ASIC(application-specific integrated circuit), FPGA(field programmable gate array) 등의 처리 장치를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0031] 한편, 제어부(200)는 난수 독출 모드에 따라 난수 생성 메모리(100)에 기록된 난수 데이터를 독출한다.

[0032] 도 6은 본 발명의 일 실시예에 따른 독출 과정을 도시한 도면이다.

[0033] 도면에서와 같이, 난수 생성 메모리(100)는 복수의 저항성 메모리 셀이 2차원 어레이 형태로 배치된 것일 수 있다. 이때, 각 메모리 셀의 독출을 위해, 제어부(200)는 랜덤하게 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 난수가 출력되도록 한다. 도 6에 도시된 바와 같이, 전체 워드 라인 중 일부의 워드라인 만을 랜덤하게 선택하고, 선택된 워드라인에 읽기 전압($1/2 VDD$)을 인가하고, 비선택된 워드라인은 플로팅 상태를 유지시킨다. 그리고, 각 비트라인들은 플로팅 상태를 유지시켜, 각 메모리 셀이 갖는 전기 저항 값에 따른 전류가 각 비트라인 별로 접지 단자까지 흐르도록 하며, 이러한 전류를 감지한 후 센스 증폭기 등의 구성을 통해 증폭하여, 각 비트라인별로 0 또는 1의 출력 값이 출력되도록 한다. 이와 같이 출력된 값을 랜덤하게 선택된 워드라인에 대한 응답으로서, 임의의 난수로 출력한다.

[0034] 또한, 제어부(200)는 난수 독출 모드에서, 입력되는 챌린지(challenge) 값에 따라 워드라인을 선택한 후 선택된 워드라인에 독출 전압이 인가되도록 하고, 각 비트라인 별로 각 저항성 메모리 소자의 값이 독출되도록 하여 챌린지 값에 대응하는 응답(response) 난수가 출력되도록 할 수 있다. 제어부(200)는 챌린지 값을 서로 다르게 설정하므로, 이에 따라 선택되는 워드라인도 모두 달라진다. 그리고, 챌린지 값에 따라 독출되는 응답 난수를 각 챌린지 값과 매칭되도록 하고, 이것들이 CRP(challenge response pair) 테이블로 형성되도록, 외부 컴퓨팅 장치에 제공할 수 있다. 이와 같은, CRP 정보는 긴밀한 보안이 필요한 것으로서, 외부 서버등에 저장되어 관리될 수 있다. 이후, 본 발명에 따른 난수 발생 장치를 사용하여 인증을 수행할 때, 챌린지 값이 난수 발생 장치(10)에 입력되어 난수 생성 메모리(100)에서 직접 출력된 값과, 외부 서버 등에 저장된 CRP에서 독출된 값을 비교하여

동일한 경우에 정상적으로 인증을 완료할 수 있다.

- [0035] 한편, 본 발명에서는 교류파의 조합에 따라 서로 난수 생성 메모리(100)에 기록되는 난수의 상태를 서로 다르게 조절할 수 있다. 이에 따라, 교류파의 조합에 따라 서로 다른 CRP 테이블이 생성되는 것이다. 이를 이용하면, 난수 발생 장치(10)에 대하여 예를 들어, 서로 다른 교류파가 조합된 10개의 교류파 조합을 생성하고, 각 교류파 조합 별로 각각 CRP 테이블을 생성하는 과정을 거칠 수 있다. 이후, 각 교류파 조합에 대한 식별 정보와 각 교류파 조합에 근거하여 생성된 CRP 테이블을 외부 서버(예를 들면, 메모리 제조사의 내부 서버)등에 저장하여, 난수 발생 장치(10)에서 생성되는 복수의 CRP 테이블을 관리하도록 한다. 이 때 저장된 테이블의 CRP 정보는 각 PUF칩으로부터 분리되어 보관되므로 칩을 가진 사용자에게 해당 정보가 전송되지는 않는다. 따라서 외부에서는 한 예시의 인증이 발생할 때 마다 한 예시의 CRP에만 접근하므로 전체 테이블의 챌린지 투 리스폰즈 매카니즘은 알 수 없다는 장점이 있다.
- [0036] 이후 인증 과정에서는, 교류파 조합에 대한 식별 정보를 외부 서버 등에 전달하고, 교류파 조합의 식별 정보와 매칭되어 저장된 CRP 테이블을 기초로 인증 절차를 수행하도록 한다. 그리고, 난수 발생 장치(10)는 해당하는 교류파 조합에 대한 식별 정보를 이용하여 해당 교류파 조합에 따라 난수가 출력되도록, 난수 생성 메모리(100)의 재구성 절차를 진행한다.
- [0037] 제어부(200)는 난수 재구성 모드에 따라, 난수 생성 메모리(100)를 초기화한 후 각 워드라인 또는 비트라인에 인가될 교류파의 조합을 재선택하고, 재선택된 교류파의 조합 정보를 기록하며, 재선택된 교류파의 조합에 따라 난수 생성 메모리(100)에 난수가 기록되도록 한다. 이때, 교류파의 조합 정보는 실시간으로 랜덤하게 설정될 수 있으나, 앞서 설명한 실시예에서와 같이, 미리 설정되어 있는 복수의 교류파 조합 중 어느 하나가 선택될 수도 있다.
- [0038] 전압 공급부(300)는 제어부(200)의 지시에 따라 난수 생성 메모리(100)의 워드라인 또는 비트라인에 각각 쓰기 전압 또는 독출 전압을 인가하되, 독출 전압 인가시에는 앞서 설정된 교류파의 조합에 따라 각 워드라인 또는 비트라인에 각각 설정된 교류파가 인가되도록 한다.
- [0039] 도 7은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치의 동작 방법을 도시한 순서도이다.
- [0040] 특히, 난수 생성 메모리에 난수를 생성하는 과정과, 이를 기반으로 난수를 독출하는 과정을 도시한 것이다.
- [0041] 먼저, 앞서 설명한 내용에 따라 제어부(200)는 난수 생성모드에 따라 교류파 조합을 선택한다(S710). 이와 같은, 교류파 조합은 실시간으로 랜덤하게 설정될 수 도 있고, 미리 설정된 복수의 교류파 조합 중 어느 하나의 교류파 조합이 선택될 수 있다.
- [0042] 다음으로, 선택된 교류파 조합에 따라 난수 생성 메모리(100)에 난수가 생성되도록 한다(S720). 교류파 조합에 따라 전압 공급부(300)에 의하여 각 워드라인 또는 비트라인에 인가되는 전압이 결정되고, 그에 따라 난수 생성 메모리(100)에 데이터가 기록된다.
- [0043] 다음으로, 제어부(200)는 난수 생성 메모리(100)의 워드라인들 중 일부의 워드라인들을 선택하여, 난수가 출력되도록 한다. 난수가 출력되는 모드는 크게 2가지로 실시될 수 있다. 일 실시예로는 임의의 워드라인 복수개가 선택되도록 하여 임의의 난수가 출력되도록 할 수 있다.
- [0044] 다른 실시예로는, 미리 설정된 개수만큼의 워드라인 선택 조합을 각각의 챌린지로서 결정하고, 각 챌린지에 의하여 출력되는 값을 응답으로서 설정하는 과정을 통해, CRP 테이블이 생성되도록 할 수 있다. 이와 같은 CRP 테이블은 외부에서 접근이 어려운 제조사 측의 내부 컴퓨팅 장치에 의해 관리되어 해당 난수 발생 장치의 사용시에 활용될 수 있다. 또한, 도 7의 과정을 각각의 교류파 조합에 순차적으로 수행하는 과정을 통해, 각 교류파 조합별로 서로 상이한 CRP 테이블이 생성되도록 할 수 있다. 이에, 각 교류파 조합의 식별 정보와 이에 매칭되는 CRP 테이블의 정보가 서로 연결되어 관리될 수 있다.
- [0045] 도 8은 본 발명의 일 실시예에 따른 물리적 복제 방지 기능을 가진 난수 발생 장치의 동작 방법을 도시한 순서도이다.
- [0046] 도 8은 복수의 교류파 조합이 미리 결정된 경우의 실시예에서, 본 난수 발생 장치를 이용한 인증 방법을 도시한 것이다.
- [0047] 먼저, 난수 발생 장치(10)는 외부 장치로부터 교류파 조합의 식별 정보와 챌린지를 수신한다(S810). 외부 장

치에서 챌린지 정보가 전송될 때, 해당 챌린지가 복수의 CRP 테이블 중 어느 CRP 테이블에 저장되었던 것인지에 대한 정보와 해당 CRP 테이블에 매칭되는 교류과 조합의 식별 정보가 함께 전송될 수 있다. 이러한 교류과 조합의 식별 정보는 이후 난수 재구성 단계(S820)에서 활용될 수 있다. 한편, 챌린지에 의하여 독출할 메모리 셀의 워드라인 선택 조합이 결정되므로, 난수 생성 메모리(100)에서 독출할 메모리 셀의 주소가 특정될 수 있다.

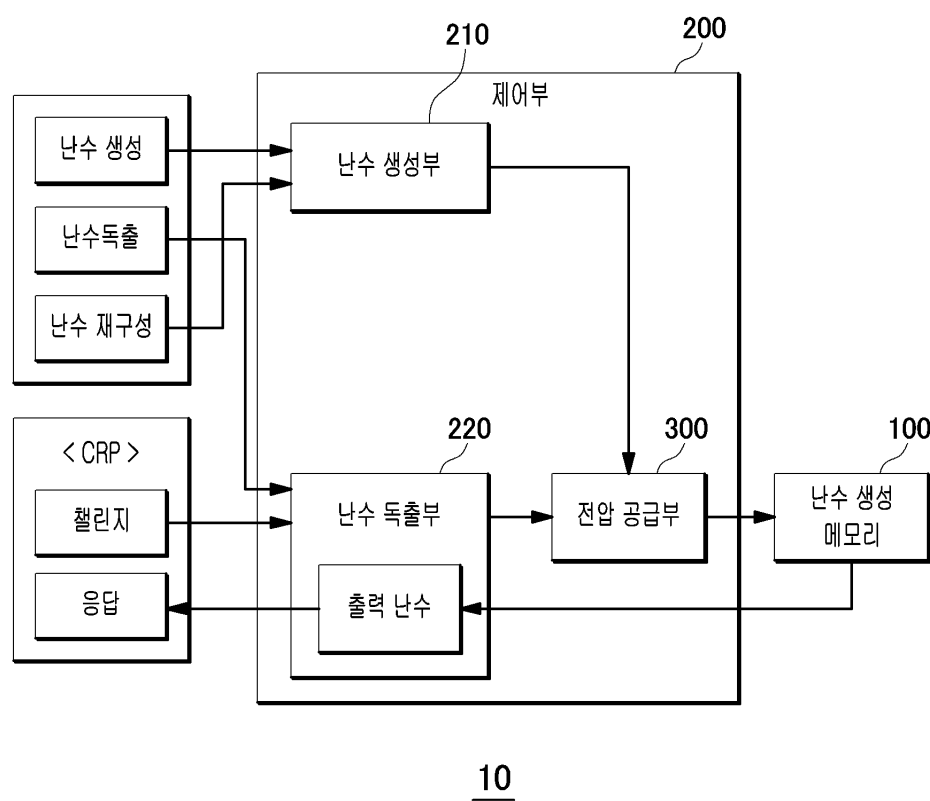
- [0048] 다음으로, 교류과 조합의 식별 정보를 이용하여 난수 재구성 단계를 수행할 수 있다(S820).
- [0049] 앞선 단계에서 수신한 교류과 조합의 식별 정보에 해당하는 난수 생성 메모리(100)가 설정되도록, 난수 생성 메모리(100)를 초기화하고, 교류과 조합의 식별 정보에 의해 지정된 교류과 조합에 의하여 난수가 생성되도록 한다. 만약, 교류과 조합의 식별 정보와 현재 난수 발생 장치(10)의 난수 생성 메모리(100)에 적용된 교류과 조합이 동일한 경우에는 본 단계(S820)가 생략될 수 있다.
- [0050] 다음으로, 챌린지에 대한 응답을 난수 생성 메모리(100)에서 독출한다(S830). 각 챌린지에 매칭되는 워드라인을 선택하고, 이에 해당하는 응답을 난수 생성 메모리(100)에서 독출한다. 독출된 값은 챌린지에 매칭되는 응답으로서 출력된다.
- [0051] 다음으로, 단계(S830)에서 독출된 응답 값이 CRP 테이블을 관리하는 외부 컴퓨팅 장치로 전송되어, 인증 절차가 수행되도록 한다(S840). 독출된 응답값이 CRP 테이블에 저장된 응답과 동일한 경우에 한하여, 인증 절차가 완료될 수 있다.
- [0052] 이와 같은 구성을 통해, 하나의 난수 발생 장치(10)에 설정되는 교류과 조합에 따라, 복수의 CRP 테이블이 생성될 수 있고, 이는 곧 하나의 난수 발생 장치(10)가 복수의 PUF 칩으로 기능할 수 있도록 한다.
- [0053] 이상에서 설명한 본 발명의 일 실시예에 다른 난수 발생 장치의 동작 방법은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.
- [0054] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0055] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

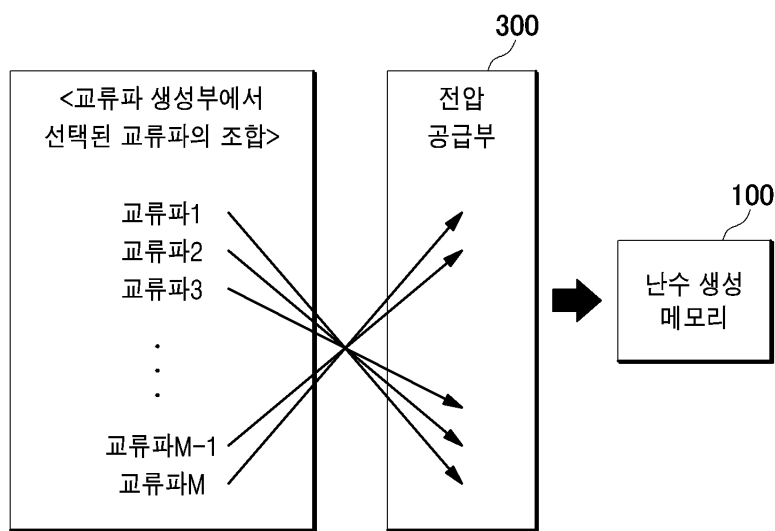
- [0056] 10: 난수 발생 장치
- 100: 난수 생성 메모리
- 200: 제어부
- 300: 전압 공급부

도면

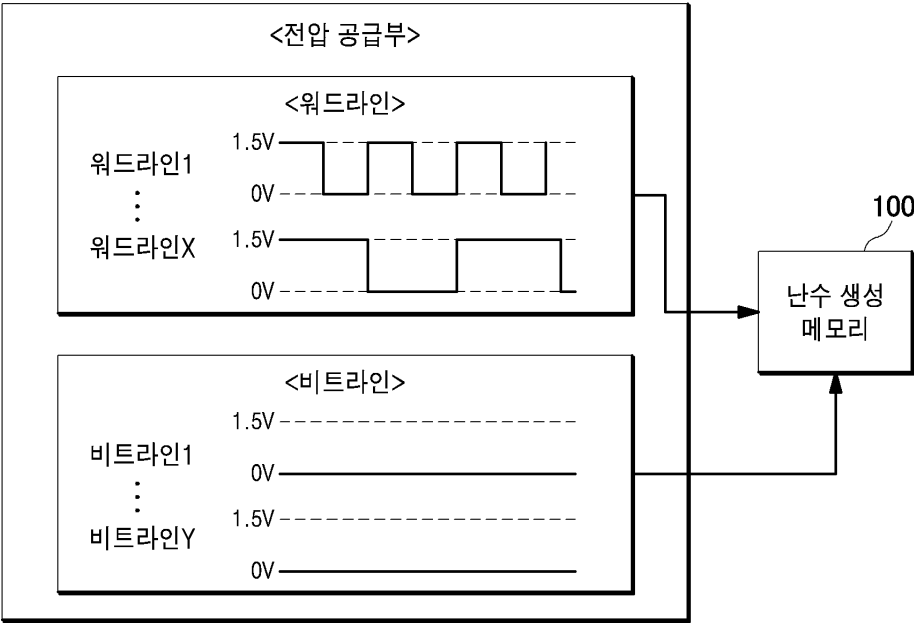
도면1



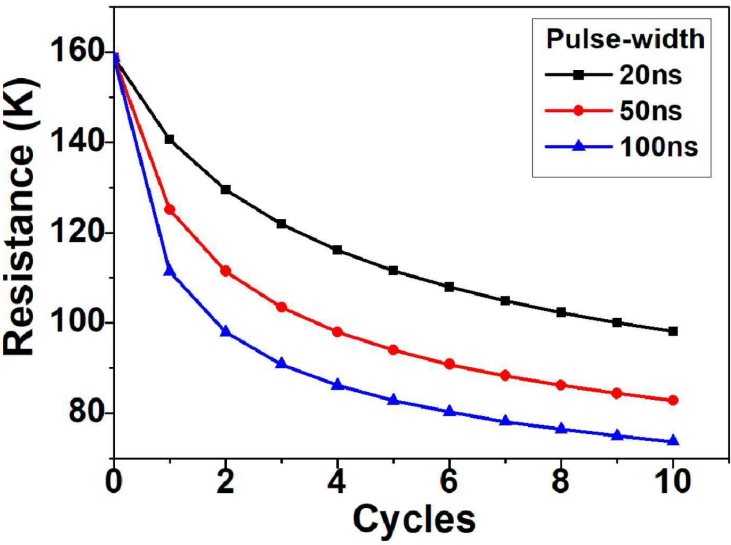
도면2



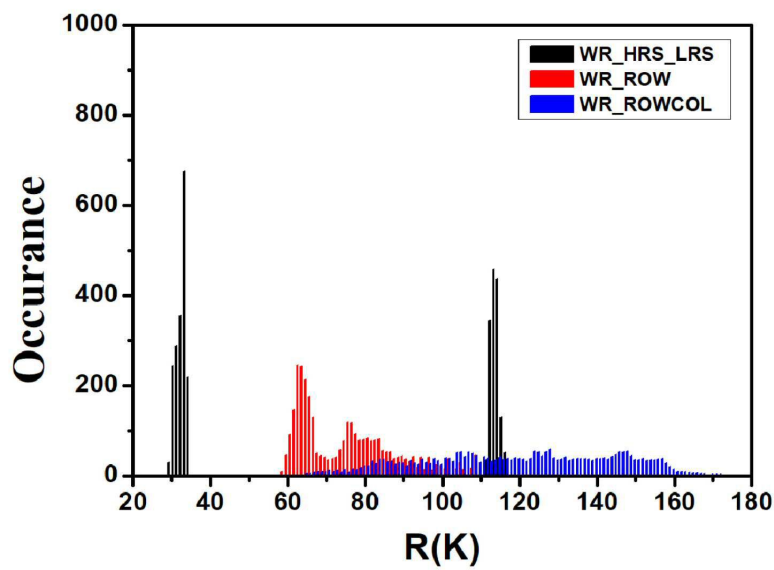
도면3



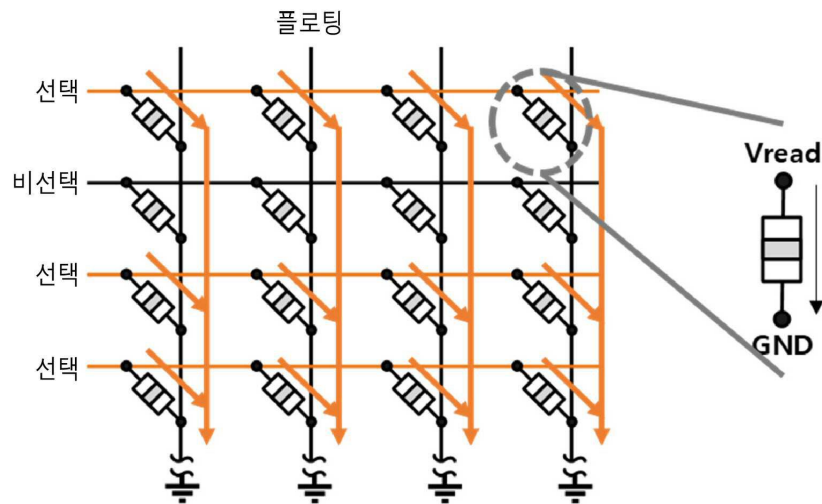
도면4



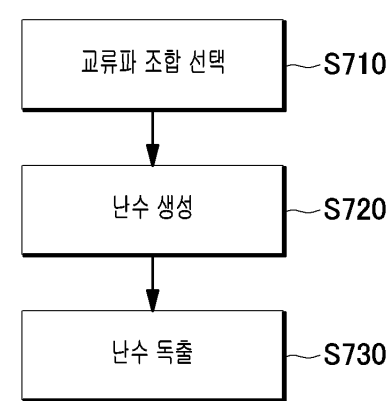
도면5



도면6



도면7



도면8

