(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년07월25일
(11) 등록번호 10-1642651
(24) 등록일자 2016년07월19일

(51) 국제특허분류(Int. Cl.)
H01L 29/06 (2006.01) *H01L 29/41* (2006.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H01L 29/0665 (2013.01)
H01L 29/413 (2013.01)
(21) 출원번호 10-2015-0035206
(22) 출원일자 2015년03월13일
심사청구일자 2015년03월13일
(56) 선행기술조사문헌
KR1020090080653 A
US20090254981 A1
US20130119348 A1
KR101393806 B1

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
성균관대학교산학협력단
경기도 수원시 장안구 서부로 2066 (천천동, 성균관대학교내)
(72) 발명자
김선국
경기도 용인시 기흥구 덕영대로 1732, 전자정보대 516호(서천동)
양준성
경기도 수원시 장안구 서부로 2066, 반도체시스템공학과(천천동)
(뒷면에 계속)
(74) 대리인
김연권

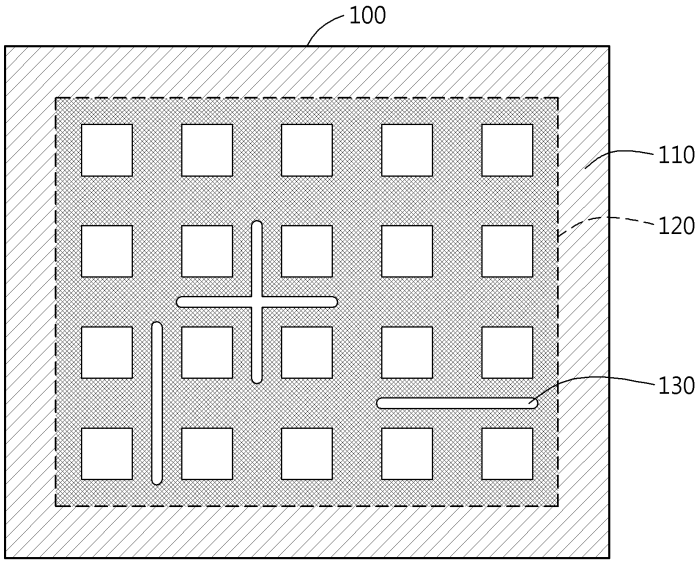
전체 청구항 수 : 총 8 항 심사관 : 고재현

(54) 발명의 명칭 **시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치**

(57) 요 약

본 발명은 분자 비대칭성(chirality)을 이용하여 기판에 분산된 나노넷 물질 및 상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝(electrical burning) 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 포함하는 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치를 개시한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/3278 (2013.01)
(72) 발명자
장익준
서울특별시 성동구 독서당로40길 25, 107동 1207호(옥수동, 현대아파트)
이형준
서울특별시 성동구 금호로 17, 209동 703호(금호동4가, 서울숲2차푸르지오)

이 발명을 지원한 국가연구개발사업
과제고유번호 2013M3C1A3059590
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 첨단융합기술개발
연구과제명 가변렌즈용 고유연 광전자 나노소자 연구
기 여 율 1/3
주관기관 경희대학교 산학협력단
연구기간 2013.09.17 ~ 2016.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 2014M3A9D7070732
부처명 미래과학창조부
연구관리전문기관 한국연구재단
연구사업명 헬스케어원천기술개발
연구과제명 생체신호 진단용 인공피부센서 개발
기 여 율 1/3
주관기관 경희대학교 산학협력단
연구기간 2014.12.11 ~ 2017.12.10
이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2013R1A1A1009854
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 기초연구사업(학술진흥)(2013)-일반연구자지원사업-신진연구
연구과제명 모바일 사용자의 무선네트워크 접속 기록으로부터 소셜 데이터마이닝을 통한 지능형 무선 애드혹 네트워크용 데이터 추천 및 라우팅 기법
기 여 율 1/3
주관기관 이화여자대학교 산학협력단
연구기간 2013.06.01 ~ 2016.05.31

명 세 서

청구범위

청구항 1

분자 비대칭성(chirality)을 이용하여 기판에 분산된 나노넷 물질; 및

상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝(electrical burning) 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이

를 포함하고,

상기 나노넷 물질은

상기 전극 어레이로부터 선택되는 임의의 전극 사이에 시그널 패스(signal path)를 제공하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 2

제1항에 있어서,

상기 나노넷 물질은

상기 전기적 버닝 방식에 의하여 상기 선정된 전극 주위에서의 금속성이 제거된 것을 특징으로 하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 3

제1항에 있어서,

상기 전기적 버닝 방식은

상기 나노넷 물질의 성장 밀도함수 파라미터, 금속성 파라미터 및 반도체성 파라미터 중 적어도 하나를 고려하여 상기 선정된 전극에 상기 전압을 스위핑하여 인가하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 4

제1항에 있어서,

상기 전기적 버닝 방식은

상기 선정된 도메인 크기 및 상기 복수의 전극 개수 중 적어도 하나를 고려하여 맵 규칙에 대응하는 상기 선정된 전극에 전압을 인가하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 5

제1항에 있어서,

상기 나노넷 물질은

무작위성 네트워크, 방향성 네트워크, 크로스바 네트워크 및, 상기 무작위성 네트워크, 상기 방향성 네트워크 및 상기 크로스바 네트워크를 조합한 네트워크 중 적어도 하나의 형상으로 상기 기판에 분산되는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 6

제1항에 있어서,

상기 나노넷 물질은

선정된 패턴의 에칭 공정에 의하여 생성되는 상기 시그널 패스의 랜덤성을 포함하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 7

제1항에 있어서,

상기 카오스 나노넷 소자는

입력 비트에 연관되어 선택되는 두 개의 전극 사이의 상기 시그널 패스의 형성 여부에 대응하여 출력 비트를 생성하는

시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자.

청구항 8

챌린지 비트를 입력 비트로 생성하는 제1 응답 생성기(response generator);

상기 생성된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택하는 디코더;

상기 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성하는 카오스 나노넷 소자;

상기 출력 비트를 리스폰스 비트로 생성하는 제2 응답 생성기; 및

주문형 반도체를 이용하여 상기 리스폰스 비트를 공개키 및 비밀키로 생성하는 보안키 생성기

를 포함하고,

상기 카오스 나노넷 소자는

분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질; 및

상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이

를 포함하는 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치에 관한 것으로, 보다 상세하게는 전기적 버닝 방식에 기초하여 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치에 관한 것이다.

배 경 기 술

[0002] 정보통신기술이 발달함에 따라 정보통신기술을 의료산업, 헬스케어, 원격검침, 스마트홈, 및 스마트카 등 다양한 분야에 접목하는 추세이고, 특히, 다양한 분야에서 사용되는 사물을 네트워크로 연결하여 정보를 공유하는 사물 인터넷(IoT, internet of things) 기술을 사용하고 있는 추세이다.

[0003] 예를 들어, 의료산업의 경우 사물기기를 이용하여 환자의 건강 유지에 필요한 건강 정보를 실시간으로 주치의와 공유할 수 있고, 실시간으로 처방 및 대처를 할 수 있다.

[0004] 그러나, 최근에는 각 소스 사물에서 수집된 정보를 목적지 사물로 전송하는 경우, 권한이 없는 사용자가 수집된 정보를 열람하는 보안 사고가 빈번히 발생되고 있으므로, 보안 사고를 해결하기 위한 보안 인증을 사물 인터넷에 적용하여 사용하고 있는 추세이다.

[0005] 예를 들어, 의료산업의 경우 환자의 생체 신호 정보 및 병명 내역 정보 등 데이터를 수집하는 소스 사물이 목적지 사물로 해당 데이터를 전송하는 경우, 권한이 있는 사용자가 보안 인증을 통해 목적지 사물에서 데이터를 열

람할 수 있다.

[0006] 보안 인증 방법으로는 비휘발성 메모리에 기반하여 인증에 필요한 키(예를 들어, 비밀키(private key), 공개키(public key) 등) 정보를 저장하고, 저장된 키 정보를 이용하여 보안 인증을 수행하는 하드웨어를 이용한 방법이 있다.

[0007] 그러나, 종래의 하드웨어를 이용한 인증 방법은 해커들이 다양한 메모리 읽기 방법을 통해 비휘발성 메모리에 저장되어 있는 키 정보를 유출하는 문제점이 존재하였다.

[0008] 하드웨어를 이용한 인증 방법의 문제점을 해결하기 위해 최근에 나노넷 물질 기반의 물리적 복제 방지(PUF, physical unclonable function) 회로를 이용하여 물리적으로 복제가 불가능하도록 구현하는 기술이 급부상하고 있다.

[0009] 나노넷 물질은 나노선(nanowire) 및 카본나노튜브(CNT, carbon nano tube) 중 적어도 하나를 포함할 수 있다.

[0010] 나노선은 나노미터 단위의 크기를 갖는 와이어 구조이고, 카본나노튜브는 탄소 6개로 이루어진 육각형들이 서로 연결되어 관 모양을 이루는 구조이다.

[0011] 나노선 및 카본나노튜브 등 나노넷 물질은 금속성 또는 반도체성을 갖는 소재이고, 반도체, 평판 디스플레이, 배터리, 초강력 섬유, 생체 센서 및 브라운관 등 다양한 장치에 사용되는 소재이다.

[0012] 그러나, 나노넷 물질은 성장 과정에서 분자 비대칭성(chirality)을 통제하기 어려워 대면적 집적회로 구현이 어려운 결점이 존재하였다. 이러한 결점을 해결하기 위해 나노넷 물질의 성장 상에서 발생되는 결점을 제거 또는 완화시키는 기술에 대한 연구가 활발히 진행되고 있다.

[0013] 그러나, 나노넷 물질의 성장 상에서 발생되는 결점을 활용하고자 하는 연구는 이루어지지 못하고 있는 실정이다.

선행기술문헌

특허문헌

[0014] (특허문헌 0001) 대한민국 등록특허 제101393806호(2014.05.02). "다단계 물리적 복제 불가 함수 시스템"

비특허문헌

[0015] (비특허문헌 0001) N. Pimparkar, Q. Cao, J. A. Rogers, and M. A. Alam, "Theory and Practice of "Striping" for Improved ON/OFF Ratio in Carbon Nanonet Thin Film Transistors," Nano Research, pages 167-175, 2009.

(비특허문헌 0002) G. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation,"In ACM Design Automation Conference(DAC), pages 9??14, 2007.

발명의 내용

해결하려는 과제

[0016] 본 발명은 나노넷 물질의 성장 상에서 발생되는 분자 비대칭성을 이용하여 물리적 복제 방지의 고유 특성을 향상시키는 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치를 제공한다.

[0017] 본 발명은 전기적 버닝 방식을 이용하여 나노넷 물질에 대한 시그널 패스의 랜덤성을 극대화하는 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치를 제공한다.

[0018] 본 발명은 시그널 패스의 랜덤성을 제공하여 보안 인증의 안정성을 향상 시키는 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자 및 PUF 보안 장치를 제공한다.

[0019] 본 발명은 카오스 나노넷 소자의 입출력 단에 응답 생성기를 사용하여 챌린지 비트와 리스폰스 비트간의 대응 관계 경우의 수를 증가시킴으로써, 보안 인증의 안정성을 향상시키는 시그널 패스의 랜덤성을 보장하는 카오스

나노넷 소자 및 PUF 보안 장치를 제공한다.

과제의 해결 수단

[0020] 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자는 분자 비대칭성(chirality)을 이용하여 기판에 분산된 나노넷 물질 및 상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝(electrical burning) 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 포함하고, 상기 나노넷 물질은 상기 전극 어레이로부터 선택되는 임의의 전극 사이에 시그널 패스(signal path)를 제공한다.

[0021] 상기 나노넷 물질은 상기 전기적 버닝 방식에 의하여 상기 선정된 전극 주위에서의 금속성이 제거된 것을 특징으로 할 수 있다.

[0022] 상기 전기적 버닝 방식은 상기 나노넷 물질의 성장 밀도함수 파라미터, 금속성 파라미터 및 반도체성 파라미터 중 적어도 하나를 고려하여 상기 선정된 전극에 상기 전압을 스위핑하여 인가할 수 있다.

[0023] 또한, 상기 전기적 버닝 방식은 상기 선정된 도메인 크기 및 상기 복수의 전극 개수 중 적어도 하나를 고려하여 맵 규칙에 대응하는 상기 선정된 전극에 전압을 인가할 수 있다.

[0024] 본 발명의 일측에 따르면, 상기 나노넷 물질은 무작위성 네트워크, 방향성 네트워크, 크로스바 네트워크 및, 상기 무작위성 네트워크, 상기 방향성 네트워크 및 상기 크로스바 네트워크를 조합한 네트워크 중 적어도 하나의 형상으로 상기 기판에 분산될 수 있다.

[0025] 또한, 상기 나노넷 물질은 선정된 패턴의 에칭 공정에 의하여 생성되는 상기 시그널 패스의 랜덤성을 포함할 수 있다.

[0026] 상기 카오스 나노넷 소자는 입력 비트에 연관되어 선택되는 두 개의 전극 사이의 상기 시그널 패스의 형성 여부에 대응하여 출력 비트를 생성할 수 있다.

[0027] 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 보안 장치는 챌린지 비트를 입력 비트로 생성하는 제1 응답 생성기(Response generator), 상기 생성된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택하는 디코더, 상기 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성하는 카오스 나노넷 소자, 상기 출력 비트를 리스폰스 비트로 생성하는 제2 응답 생성기 및 주문형 반도체를 이용하여 상기 리스폰스 비트를 공개키 및 비밀키로 생성하는 보안키 생성기를 포함하고, 상기 카오스 나노넷 소자는 분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질 및 상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 포함한다.

[0028] 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자를 제조하는 방법은 분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질을 형성하는 단계 및 상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 형성하는 단계를 포함하고, 상기 나노넷 물질을 형성하는 단계는 상기 전극 어레이로부터 선택되는 임의의 전극 사이에 시그널 패스(signal path)를 제공한다.

[0029] 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치의 동작 방법은 제1 응답 생성기를 통하여 챌린지 비트를 입력 비트로 생성하는 단계, 디코더를 통하여 상기 생성된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택하는 단계, 카오스 나노넷 소자를 통하여 상기 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성하는 단계, 제2 응답 생성기를 통하여 상기 출력 비트를 리스폰스 비트로 생성하는 단계 및 주문형 반도체를 이용하여 상기 리스폰스 비트를 공개키 및 비밀키로 생성하는 단계를 포함하고, 상기 카오스 나노넷 소자는 분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질 및 상기 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 포함한다.

발명의 효과

[0030] 본 발명은 나노넷 물질의 성장 상에서 발생되는 분자 비대칭성을 이용하여 물리적 복제 방지의 고유 특성을 향상시킬 수 있다.

[0031] 본 발명은 전기적 버닝 방식을 이용하여 나노넷 물질에 대한 시그널 패스의 랜덤성을 극대화할 수 있다.

[0032] 본 발명은 시그널 패스의 랜덤성을 제공하여 보안 인증의 안정성을 향상 시킬 수 있다.

[0033] 본 발명은 카오스 나노넷 소자의 입출력 단에 응답 생성기를 사용하여 챌린지 비트와 리스폰스 비트간의 대응 관계 경우의 수를 증가시킴으로써, 보안 인증의 안정성을 향상시킬 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자를 도시한 것이다.

도 2는 전기적 버닝 방식에 따른 전류와 전압 간의 관계를 예시한 도면이다.

도 3a 내지 도 3c는 나노넷 물질의 네트워크 형상에 대한 예를 도시한 것이다.

도 4a 내지 도 4f는 나노넷 물질의 네트워크 형상을 변형한 예를 도시한 것이다.

도 5a는 본 발명의 실시예에 따른 분산된 나노넷 물질의 금속성과 반도체성에 의해 시그널 패스가 생성되는 예를 도시한 것이다.

도 5b는 본 발명의 실시예에 따른 에칭 패턴을 통하여 시그널 패스가 생성되는 예를 도시한 것이다.

도 5c는 본 발명의 실시예에 따른 분산된 나노넷 물질에 선정된 전극의 전압 인가를 통하여 시그널 패스가 생성되는 예를 도시한 것이다.

도 6은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치를 도시한 블록도이다.

도 7은 도 6의 나노넷 물질을 이용한 카오스 나노넷 기반의 물리적 복제 방지 보안 장치를 단일 칩으로 구현한 예를 도시한 것이다.

도 8은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자의 제조 방법을 도시한 흐름도이다.

도 9는 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치의 동작 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0035] 소자(elements) 또는 층이 다른 소자 또는 층의 "위(on)" 또는 "상(on)"으로 지칭되는 것은 다른 소자 또는 층의 바로 위뿐만 아니라 중간에 다른 층 또는 다른 소자를 개재한 경우를 모두 포함한다. 반면, 소자가 ""직접 위(directly on)" 또는 "바로 위"로 지칭되는 것은 중간에 다른 소자 또는 층을 개재하지 않은 것을 나타낸다.

[0036] 공간적으로 상대적인 용어인 "아래(below)", "아래(beneath)", "하부(lower)", "위(above)", "상부(upper)" 등은 도면에 도시되어 있는 바와 같이 하나의 소자 또는 구성 요소들과 다른 소자 또는 구성 요소들과의 상관관계를 용이하게 기술하기 위해 사용될 수 있다. 공간적으로 상대적인 용어는 도면에 도시되어 있는 방향에 더하여 사용시 또는 동작시 소자의 서로 다른 방향을 포함하는 용어로 이해되어야 한다. 예를 들면, 도면에 도시되어 있는 소자를 뒤집을 경우, 다른 소자의 "아래(below 또는 beneath)"로 기술된 소자는 다른 소자의 "위(above)"에 놓여질 수 있다. 따라서, 예시적인 용어인 "아래"는 아래와 위의 방향을 모두 포함할 수 있다. 소자는 다른 방향으로도 배향될 수 있으며, 이 경우 공간적으로 상대적인 용어들은 배향에 따라 해석될 수 있다.

[0037] 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, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

[0038] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 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.

[0039] 한편, 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0040] 도 1은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자를 도시한 것이다.

[0041] 도 1을 참조하면, 카오스 나노넷 소자(100)는 기판(미도시), 나노넷 물질(110) 및 전극 어레이(120)를 포함한다.

[0042] 나노넷 물질(110)은 분자 비대칭성(chirality)을 이용하여 기판에 분산된다. 여기서, 나노넷 물질(110)은 나노선(nanowire) 및 카본나노튜브(CNT, carbon nano tube) 중 적어도 하나를 포함할 수 있다. 또한, 나노넷 물질(110)은 복수의 나노선 및 복수의 카본나노튜브 중 적어도 하나를 포함할 수 있다.

[0043] 나노선은 나노미터 단위의 크기를 갖는 와이어 구조이고, 카본나노튜브는 탄소 6개로 이루어진 육각형들이 서로 연결되어 관 모양을 이루는 구조이다.

[0044] 나노선 및 카본나노튜브 등 나노넷 물질은 금속성 또는 반도체성을 갖는 소재이고, 반도체, 평판 디스플레이, 배터리, 초강력 섬유, 생체 센서 및 브라운관 등 다양한 장치에 사용되는 소재이다.

[0045] 나노넷 물질(110)은 선정된 밀도 및 두께를 고려하여 기판에 분산될 수 있다. 선정된 밀도 및 두께는 나노넷 물질의 직경(diameter) 및 분자 비대칭성에 의해 선정될 수 있고, 나노넷 물질이 사용되는 하드웨어의 환경조건, 예를 들어, 온도 변이 및 열화 등의 조건에 따라 다양하게 선정될 수 있다.

[0046] 또한, 나노넷 물질(110)은 나노 크기의 양자적인 효과를 기반으로 산란(scattering)이 없는 초고속 이동도의 장점을 가지는 반면, 대면적 성장 물질들이 균일한 전기 특성을 제공하지 못하는 분자 비대칭성이 존재하는데, 나노넷 물질(110)은 성장 상에 성장 밀도함수, 금속성 및 반도체성이 무작위적으로 나타내는 결점이 존재한다.

[0047] 실시예에 따르면, 카오스 나노넷 소자(100)는 나노넷 물질(110)의 분자 비대칭성을 이용하여 보안 인증의 안정성을 향상시킬 수 물리적 복제 방지(PUF, physical unclonable function) 보안 장치에 사용될 수 있다.

[0048] 보다 상세하게는, 나노넷 소자(100)는 나노넷 물질(110)의 시그널 패스(signal path)의 랜덤성을 이용하여 보안 인증의 안정성을 향상시킬 수 PUF 보안 장치에 사용될 수 있다.

[0049] 전극 어레이(120)는 나노넷 물질(110) 상에 선정된 도메인 크기를 갖고, 전기적 버닝(electrical burning) 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성된다.

[0050] 선정된 도메인 크기는 PUF 보안 장치(또는 보안 칩)의 입력 비트에 대한 입력 영역 및 입력 비트에 대응하는 PUF 보안 장치의 출력 비트에 대한 출력 영역을 고려한 크기일 수 있다.

[0051] 이하, 도 2를 참조하여 전기적 버닝 방식을 상세히 설명하기로 한다.

[0052] 도 2는 전기적 버닝 방식에 따른 전류와 전압 간의 관계를 예시한 도면이다.

[0053] 도 2를 참조하면, 나노넷 물질은 전기적 버닝 방식에 의하여 선정된 전극 주위에서의 금속성이 제거될 수 있다. 여기서, 각각의 전극은 소스(source) 전극, 드레인(drain) 전극 및 게이트(gate) 전극을 포함할 수 있다.

[0054] 예를 들어, 나노넷 물질은 전압을 인가받는 드레인 전극 주위에서의 금속성이 제거될 수 있다. 이 때, 게이트 전극은 플로팅(floating)의 상태일 수 있다.

[0055] 본 발명의 일측에 따르면, 전기적 버닝 방식은 나노넷 물질의 성장 밀도함수 파라미터, 금속성 파라미터 및 반도체성 파라미터 중 적어도 하나를 고려하여 선정된 전극에 전압을 스위핑(sweeping)하여 인가할 수 있다.

[0056] 예를 들어, 각각의 파라미터는 파라미터 계측기(HP 4156A)를 통하여 계측될 수 있다.

[0057] 또한, 전기적 버닝 방식은 도 2에 도시된 바와 같이, 선정된 전극에 4단계의 전압(5V, 10V, 15V 및 20V 등)을 스위핑하여 인가할 수 있다.

[0058] 본 발명의 다른 일측에 따르면, 전기적 버닝 방식은 선정된 도메인 크기 및 복수의 전극 개수 중 적어도 하나를 고려하여 맵 규칙에 대응하는 선정된 전극에 전압을 인가할 수 있다.

[0059] 맵 규칙은 선정된 도메인 크기 별 및 복수의 전극 개수 별 중 적어도 하나에 대응하는 선정된 전극의 개수에 대한 정보와 선정된 전극의 위치에 대한 정보가 포함될 수 있다.

[0060] 실시예에 따르면, 나노넷 물질은 선정된 전극의 전압 인가에 의하여 선정된 전극 주위에서의 금속성이 제거되고, 인위적인 '0' 시그널을 발생할 수 있다.

[0061] 따라서, 카오스 나노넷 소자는 전기적 버닝 방식에 의하여 나노넷 물질에 대한 시그널 패스의 랜덤성을 제공할 수 있다.

[0062] 실시예에 따르면, 나노넷 물질은 무작위성 네트워크, 방향성 네트워크, 크로스바 네트워크 및, 무작위성 네트워크, 방향성 네트워크 및 크로스바 네트워크를 조합한 네트워크 중 적어도 하나의 형상으로 기판에 분산될 수 있다.

[0063] 이하에서는 도 3a 내지 도 3c 및 도 4a 내지 4f 를 참고하여 나노넷 물질(110)의 네트워크 형상을 상세히 설명하기로 한다.

[0064] 도 3a 내지 도 3c는 나노넷 물질의 네트워크 형상에 대한 예를 도시한 것이다.

[0065] 도 3a는 나노넷 물질의 무작위성 네트워크 형상을 도시한 것으로서, 도 3a를 참조하면, 나노넷 물질(110)은 특정 패턴 및 규칙이 없는 무작위성 네트워크 형상으로 기판에 분산될 수 있다.

[0066] 본 발명의 일측에 따르면, 나노넷 물질(110)은 선정된 밀도 및 두께를 고려하여 무작위성 네트워크 형상으로 기판에 분산될 수 있다. 선정된 밀도 및 두께는 나노넷 물질(110)의 직경(diameter) 및 분자 비대칭성에 의해 선정될 수 있고, 나노넷 물질(110)이 사용되는 하드웨어의 환경조건, 예를 들어, 온도 변이 및 열화 등의 조건에 따라 다양하게 선정될 수 있다.

[0067] 도 3b는 나노넷 물질의 방향성 네트워크 형상을 도시한 것으로서, 도 3b를 참조하면, 나노넷 물질(110)은 수직접합 기반의 방향성 네트워크 형상으로 기판에 분산될 수 있다.

[0068] 본 발명의 일측에 따르면, 나노넷 물질(110)은 수직접합 기반의 방향성 네트워크 형상으로 기판에 분산됨으로써, 초소형 사물기기의 보안 장치에 사용될 수 있으며, 뛰어난 전계 효과를 나타낼 수 있다.

[0069] 도 3c는 나노넷 물질의 크로스바 네트워크 형상을 도시한 것으로서, 도 3c를 참조하면, 나노넷 물질(110)은 가로로 크로싱하는 패턴의 크로스바(crossbar) 네트워크 형상으로 기판에 분산될 수 있다.

[0070] 도 4a 내지 도 4f는 나노넷 물질의 네트워크 형상을 변형한 예를 도시한 것이다.

[0071] 도 4a 및 도 4b는 나노넷 물질의 무작위성 네트워크와 방향성 네트워크를 조합한 형상을 도시한 것으로서, 도 4a 및 도 4b를 참조하면, 나노넷 물질(110)은 무작위성 네트워크와 방향성 네트워크를 조합한 형상으로 기판에 분산될 수 있다.

[0072] 본 발명의 일측에 따르면, 나노넷 물질(110)은 무작위성 네트워크와 방향성 네트워크를 조합하여 이방성 평면의 이중층 형상으로 기판에 분산될 수 있다.

[0073] 도 4c 및 도 4d는 나노넷 물질의 방향성 네트워크와 크로스바 네트워크를 조합한 형상을 도시한 것으로서, 도 4c 및 도 4d를 참조하면, 나노넷 물질(110)은 방향성 네트워크와 크로스바 네트워크를 조합한 형상으로 기판에 분산될 수 있다.

[0074] 본 발명의 일측에 따르면, 나노넷 물질(110)은 방향성 네트워크와 크로스바 네트워크를 조합하여 상부구조 기반의 다수층 형상으로 기판에 분산될 수 있다.

[0075] 도 4e 및 도 4f는 기하학적 구조를 이용한 나노넷 물질의 방향성 네트워크 형상을 도시한 것으로서, 도 4e 및 도 4f를 참조하면, 나노넷 물질(110)은 기하학적 구조의 방향성 네트워크 형상으로 기판에 분산될 수 있다.

[0076] 본 발명의 일측에 따르면, 나노넷 물질(110)은 삼중층 또는 삼각 그물구조를 포함하는 기하학적 구조의 방향성

네트워크 형상으로 기판에 분산될 수 있다.

[0077] 다시 도 1을 참조하면, 나노넷 물질은(110)는 전극 어레이(120)로부터 선택되는 임의의 전극 사이에 시그널 패스를 제공한다. 이 때, 디코더(decoder)가 전극 어레이(120)로부터 임의의 전극을 선택할 수 있다. 상기 디코더는 후술되는 도 6를 참조하여 상세히 설명하기로 한다.

[0078] 또한, 시그널 패스는 나노넷 물질(110)의 분자 비대칭성에 의해 생성될 수 있다. 이하에서는, 도 5a 내지 도 5c를 참조하여 시그널 패스가 생성되는 과정을 설명하기로 한다.

[0079] 도 5a는 본 발명의 실시예에 따른 분산된 나노넷 물질의 금속성과 반도체성에 의해 시그널 패스가 생성되는 예를 도시한 것이다.

[0080] 도 5a를 참조하면 시그널 패스는 나노넷 물질의 분자 비대칭성에 의해 생성될 수 있고, 상세하게는 시그널 패스는 나노넷 물질의 금속성(510)과 반도체성(520)을 기반으로 생성될 수 있다.

[0081] 도 5a에 도시된 바와 같이, 시그널 패스는 임의로 선택된 두 전극을 기반으로, 금속성(510) 및 반도체성(520)을 기반으로 생성될 수 있다.

[0082] 즉, 금속성(510) 및 반도체성(520)을 갖는 분산된 나노넷 물질의 랜덤성에 기초하여 임의로 선택된 두 전극 사이에 시그널 패스가 형성될 수 있다.

[0083] 도 5b는 본 발명의 실시예에 따른 에칭 패턴을 통하여 시그널 패스가 생성되는 예를 도시한 것이다.

[0084] 도 5b를 참조하면, 나노넷 물질은 에칭 공정에 의해 시그널 패스의 랜덤성이 극대화될 수 있고, 시그널 패스는 선정된 에칭 패턴(530)에 의해 생성될 수 있다. 예를 들어, 분산된 나노넷 물질은 선정된 에칭 패턴(530)의 에칭 공정에 의하여 생성되는 시그널 패스의 랜덤성을 포함할 수 있다.

[0085] 선정된 에칭 패턴(530)은 카오스 나노넷 소자에서 복수의 전극의 위치를 고려하여 선정될 수 있고, 선정된 에칭 패턴은 일자 패턴, 교차 패턴, 지그재그 패턴 및 이를 조합한 패턴과 같은 다양한 패턴을 포함할 수 있다.

[0086] 본 발명의 카오스 나노넷 소자는 에칭 패턴(530)을 통하여 금속성과 반도체성을 갖는 분산된 나노넷 물질에 분자 비대칭성을 증가시킬 수 있고, 증가된 분자 비대칭성으로부터 시그널 패스의 랜덤성을 제공할 수 있다.

[0087] 도 5c는 본 발명의 실시예에 따른 분산된 나노넷 물질에 선정된 전극의 전압 인가를 통하여 시그널 패스가 생성되는 예를 도시한 것이다.

[0088] 도 5c를 참조하면, 나노넷 물질은 선정된 전극에 전압 인가(전술한 전기적 버닝)에 의하여 선정된 전극 주위에서의 금속성이 제거된 것을 특징으로 할 수 있고, 이에 따라 시그널 패스는 선정된 전극에 전압 인가에 의해 생성될 수 있다. 예를 들어, 분산된 나노넷 물질은 선정된 전극에 전압 인가에 의하여 선정된 전극 주위에서의 금속성이 제거된 영역(540)을 포함할 수 있다.

[0089] 본 발명의 카오스 나노넷 소자는 전극 어레이에 포함되는 복수의 전극 중에 선정된 전극에 전압의 인가를 통하여, 상기 선정된 전극 주위에 위치하는 나노넷 물질의 금속성이 제거된 영역(540)을 포함하도록 하여 시그널 패스의 랜덤성을 제공할 수 있다.

[0090] 다시 도 1을 참조하면, 카오스 나노넷 소자(100)는 PUF 보안 장치의 입력 비트에 연관되어 선택되는 두 개의 전극 사이의 시그널 패스의 형성 여부에 대응하여 PUF 보안 장치의 출력 비트를 생성할 수 있다. 입력 비트에 연관된 두 개의 전극은 디코더를 통하여 선택될 수 있다.

[0091] 보다 상세하게는, 카오스 나노넷 소자(100)는 입력 비트에 연관되어 선택되는 두 개 전극 사이의 금속성과 반도체성에 기반하여 다양한 시그널 패스를 형성할 수 있고, 형성된 시그널 패스에 대응하여 출력 비트를 생성할 수 있다.

[0092] 예를 들어, 선택된 두 개의 전극 사이에 시그널 패스가 형성된 경우, 카오스 나노넷 소자(100)는 출력 비트 '1'을 생성할 수 있고, 시그널 패스가 형성되지 않은 경우, 카오스 나노넷 소자(100)는 출력 비트 '0'을 생성할 수 있다.

[0093] 도 6은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치를 도시한 블록도이다.

[0094] 도 6을 참조하면, PUF 보안 장치(600)는 제1 응답 생성기(response generator)(610), 디코더(620), 카오스 나노넷 소자(630), 제2 응답 생성기(640) 및 보안키 생성기(650)를 포함한다.

[0095] 제1 응답 생성기(610)는 챌린지(challenge) 비트를 입력 비트로 생성한다. 예를 들어, 제1 응답 생성기(610)는 다수의 플립플롭(flip-flop) 및 카운터(counter)를 사용하여 챌린지 비트를 좌측 또는 우측으로 이동하여 입력 비트로 생성할 수 있다.

[0096] 디코더(620)는 변환된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택한다. 예를 들어, 디코더(620)는 전극 어레이에 포함된 복수의 전극의 어드레스를 참조하여 변환된 입력 비트에 대응하는 두 개의 전극을 선택할 수 있다.

[0097] 실시예에 따라서는 디코더(620)는 선정된 도메인 크기를 고려하여 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택할 수 있다. 상기 선정된 도메인 크기는 입력 비트에 대한 입력 영역 및 입력 비트에 대응하는 출력 비트에 대한 출력 영역을 고려한 크기일 수 있다.

[0098] 카오스 나노넷 소자(630)는 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성한다.

[0099] 카오스 나노넷 소자(630)는 분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질 및 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 포함할 수 있다.

[0100] 여기서, 카오스 나노넷 소자(630)에 대한 상세한 설명은 전술한 도 1 및 도 5를 참조하기로 한다.

[0101] 제2 응답 생성기(640)는 출력 비트를 리스폰스(response) 비트로 생성한다.

[0102] PUF 보안 장치(600)는 제1 응답 생성기(610) 및 제2 응답 생성기(640)를 사용하여 챌린지 비트와 리스폰스 비트 간의 대응 관계 경우의 수를 기반으로 보안 장치로서 동작할 수 있다.

[0103] 보안키 생성기(650)는 주문형 반도체(ASIC, application specific intergrated circuit)를 이용하여 리스폰스 비트를 공개키 및 비밀키로 생성한다. 주문형 반도체는 공개키 및 비밀키를 포함하는 비대칭키를 연산하는 모듈을 포함할 수 있다.

[0104] 예를 들어, 보안키 생성기(650)는 타원곡선 암호(ECC, elliptic curve cryptosystem) 알고리즘이 포함된 주문형 반도체를 이용하여 리스폰스 비트를 공개키 및 비밀키로 생성할 수 있다.

[0105] 타원곡선 암호는 식으로 정의되고, 1985년 워싱턴대학교의 수학교수인 닐 코블리츠(Neal Koblitz)와 IBM연구소의 빅터 밀러(Victor Miller)에 의해 에 의해 고안된 암호화 방식이다.

[0106] 도 7은 도 6의 나노넷 물질을 이용한 카오스 나노넷 기반의 물리적 복제 방지 보안 장치를 단일 칩(SOC, system on chip)으로 구현한 예를 도시한 것이다.

[0107] 도 7을 참조하면, PUF 보안 칩은 제1 응답 생성기(610), 디코더(620-a, 620-b), 카오스 나노넷 소자(630), 제2 응답 생성기(640) 및 보안키 생성기(650)를 포함할 수 있다.

[0108] 제1 응답 생성기(610)는 챌린지 비트를 입력 비트로 생성한다. 제1 응답 생성기(610)는 다수의 플립플롭 및 카운터를 사용하여 챌린지 비트를 좌측 또는 우측으로 이동하여 입력 비트로 생성할 수 있다.

[0109] 디코더(620-a, 620-b)는 변환된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택한다. 예를 들어, 디코더(620-a, 620-b)는 전극 어레이에 포함된 복수의 전극의 어드레스를 참조하여 변환된 입력 비트에 대응하는 두 개의 전극을 선택할 수 있다.

[0110] 본 발명의 일측에 따르면, 카오스 나노넷 기반의 물리적 복제 방지 보안 칩은 입력 비트에 대응하는 두 개의 전극을 선택하기 위하여 행과 열로 구분된 두 개의 디코더(620-a, 620-b)가 포함될 수 있다.

[0111] 카오스 나노넷 소자(630)는 선택된 전극 사이의 시그널 패스의 형성 여부에 대응하여 출력 비트를 생성할 수 있

다.

[0112] 또한, 카오스 나노넷 소자(630)는 기판, 상기 기판 상에 분산된 나노넷 물질 및 전극 어레이를 포함할 수 있다.

[0113] 나노넷 물질은 분자 비대칭성을 이용하여 기판에 분산될 수 있고, 선정된 밀도 및 두께를 고려하여 무작위성 네트워크 형상으로 기판에 분산될 수 있다.

[0114] 본 발명의 일측에 따르면, 나노넷 물질은 무작위성 네트워크, 방향성 네트워크, 크로스바 네트워크 및, 무작위성 네트워크, 방향성 네트워크 및 크로스바 네트워크를 조합한 네트워크 중 적어도 하나의 형상으로 기판에 분산될 수 있다.

[0115] 전극 어레이는 나노넷 물질 상에 형성되고, 선정된 도메인 크기를 갖는 복수의 전극을 포함할 수 있다. 선정된 도메인 크기는 보안 칩의 입력 비트에 대한 입력 영역 및 입력 비트에 대응하는 보안 칩의 출력 비트에 대한 출력 영역을 고려한 크기일 수 있다.

[0116] 이 때, 카오스 나노넷 소자(530)는 디코더(520)를 통해 선택된 전극 사이에 분자 비대칭성에 대응하는 시그널 패스를 제공할 수 있고, 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성할 수 있다.

[0117] 제2 응답 생성기(640)는 출력 비트를 리스폰스 비트로 생성한다. 따라서, PUF 보안 장치(500)는 제1 응답 생성기(610) 및 제2 응답 생성기(640)를 사용하여 챌린지 비트와 리스폰스 비트간의 대응 관계 경우의 수를 기반으로 보안 장치로서 동작할 수 있다.

[0118] 보안키 생성기(650)는 주문형 반도체를 이용하여 리스폰스 비트를 공개키 및 비밀키로 생성한다. 주문형 반도체는 공개키 및 비밀키를 포함하는 비대칭키를 연산하는 모듈을 포함할 수 있다.

[0119] 도 8은 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 소자의 제조 방법을 도시한 흐름도이다.

[0120] 도 8을 참조하면, 카오스 나노넷 소자의 제조 방법은 단계 810에서, 분자 비대칭성을 이용하여 기판에 분산된 나노넷 물질을 형성한다.

[0121] 여기서, 나노넷 물질은 나노선 및 카본나노튜브 중 적어도 하나를 포함할 수 있다. 또한, 나노넷 물질은 복수의 나노선 및 복수의 카본나노튜브 중 적어도 하나를 포함할 수 있다.

[0122] 카오스 나노넷 소자의 제조 방법은 단계 820에서, 나노넷 물질 상에 선정된 도메인 크기를 갖고, 전기적 버닝 방식에 기초하여 전압을 인가받는 선정된 전극이 포함된 복수의 전극으로 구성되는 전극 어레이를 형성한다.

[0123] 선정된 도메인 크기는 PUF 보안 장치(또는 보안 칩)의 입력 비트에 대한 입력 영역 및 입력 비트에 대응하는 PUF 보안 장치의 출력 비트에 대한 출력 영역을 고려한 크기일 수 있다.

[0124] 또한, 나노넷 물질은 전압을 인가받는 드레인 전극 주위에서의 금속성이 제거될 수 있다. 이 때, 게이트 전극은 플로팅(floating)의 상태일 수 있다.

[0125] 본 발명의 일측에 따르면, 전기적 버닝 방식은 나노넷 물질의 성장 밀도함수 파라미터, 금속성 파라미터 및 반도체성 파라미터 중 적어도 하나를 고려하여 선정된 전극에 전압을 스위핑하여 인가할 수 있다.

[0126] 본 발명의 다른 일측에 따르면, 전기적 버닝 방식은 선정된 도메인 크기 및 복수의 전극 개수 중 적어도 하나를 고려하여 맵 규칙에 대응하는 선정된 전극에 전압을 인가할 수 있다.

[0127] 맵 규칙은 선정된 도메인 크기 별 및 복수의 전극 개수 별 중 적어도 하나에 대응하는 선정된 전극의 개수에 대한 정보와 선정된 전극의 위치에 대한 정보가 포함될 수 있다.

[0128] 실시예에 따르면, 카오스 나노넷 소자의 제조 방법은 단계 810에서, 전극 어레이로부터 선택되는 임의의 전극 사이에 대응하는 시그널 패스를 제공한다.

[0129] 도 9는 본 발명의 실시예에 따른 시그널 패스의 랜덤성을 보장하는 카오스 나노넷 기반의 물리적 복제 방지 보안 장치의 동작 방법을 도시한 흐름도이다.

[0130] 도 9를 참조하면, PUF 보안 장치는 단계 910에서, 챌린지 비트를 입력 비트로 생성한다. 예를 들어, PUF 보안

장치는 단계 910에서, 다수의 플립플롭 및 카운터를 사용하여 챌린지 비트를 좌측 또는 우측으로 이동하여 입력 비트로 생성할 수 있다.

[0131] PUF 보안 장치는 단계 920에서, 생성된 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택한다. 예를 들어, PUF 보안 장치는 단계 920에서, 전극 어레이에 포함된 복수의 전극의 어디레스를 참조하여 변환된 입력 비트에 대응하는 두 개의 전극을 선택할 수 있다.

[0132] 또한, PUF 보안 장치는 단계 920에서, 선정된 도메인 크기를 고려하여 입력 비트에 연관된 어드레스에 대응하는 두 개의 전극을 선택할 수 있다. 선정된 도메인 크기는 입력 비트에 대한 입력 영역 및 입력 비트에 대응하는 출력 비트에 대한 출력 영역을 고려한 크기일 수 있다.

[0133] PUF 보안 장치는 단계 930에서, 선택된 전극 사이의 시그널 패스의 형성 여부에 대한 출력 비트를 생성한다.

[0134] 이를 위해, PUF 보안 장치는 기판, 상기 기판 상에 분산된 나노넷 물질 및 전극 어레이를 포함할 수 있다.

[0135] PUF 보안 장치는 단계 940에서, 출력 비트를 리스폰스 비트로 생성하고, 단계 950에서, 주문형 반도체를 이용하여 리스폰스 비트를 공개키 및 비밀키로 생성한다. 주문형 반도체는 공개키 및 비밀키를 포함하는 비대칭키를 연산하는 모듈을 포함할 수 있다.

[0136] 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0137]

[0138] 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.

[0139]

[0140] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0141] 100, 630: 카오스 나노넷 소자

110: 나노넷 물질

120: 전극 어레이

130: 에칭

600: PUF 보안 장치

610: 제1 응답 생성기

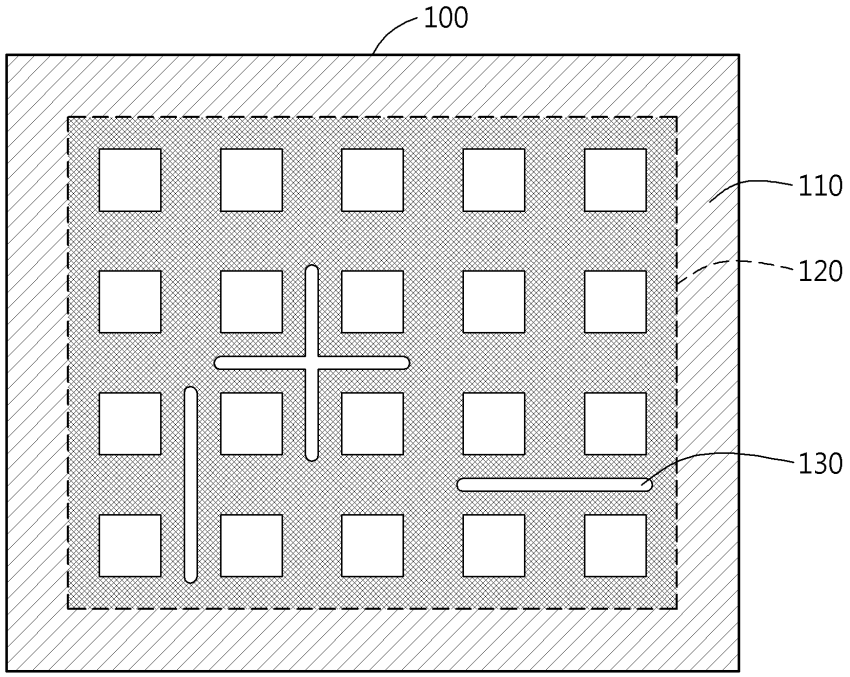
620, 620-a, 620-b: 디코더

640: 제2 응답 생성기

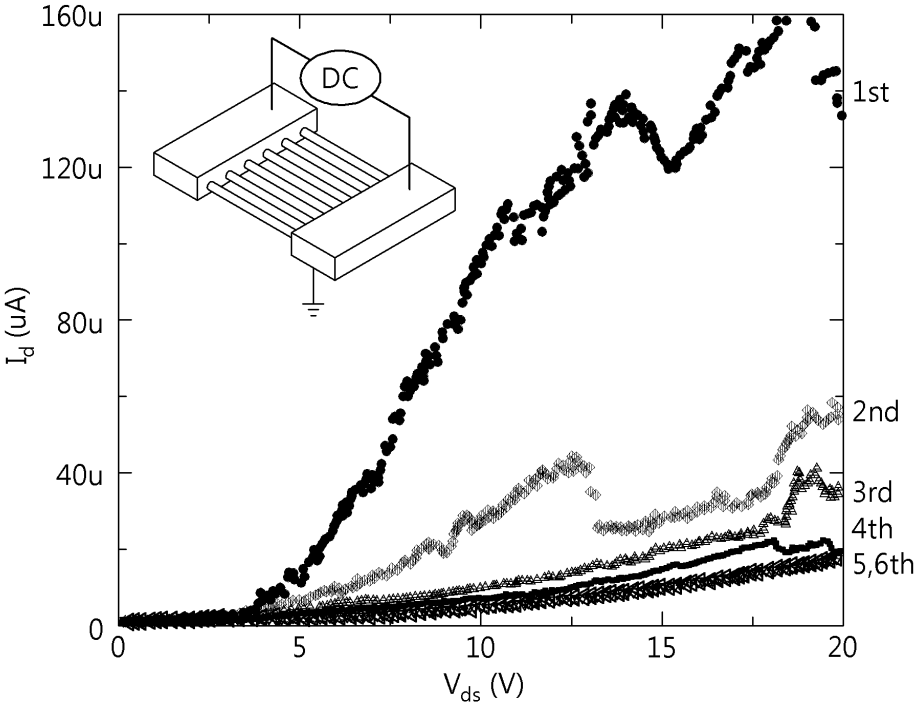
650: 보안키 생성기

도면

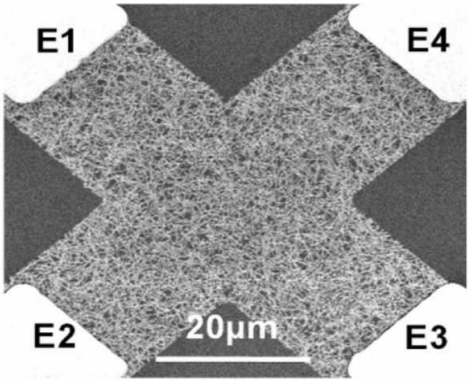
도면1



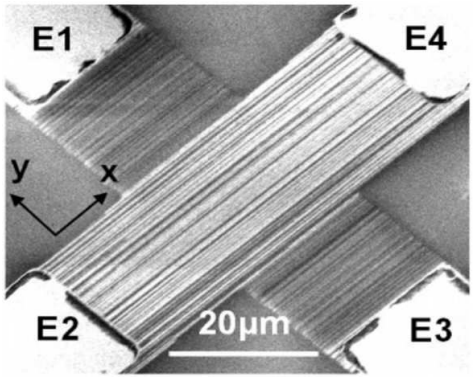
도면2



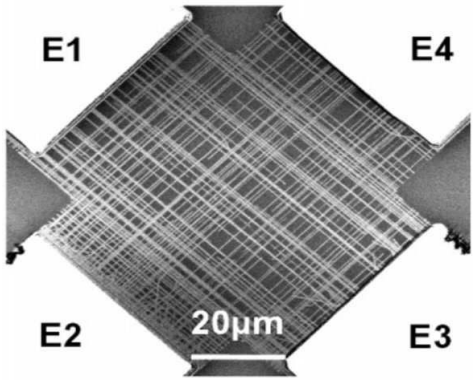
도면3a



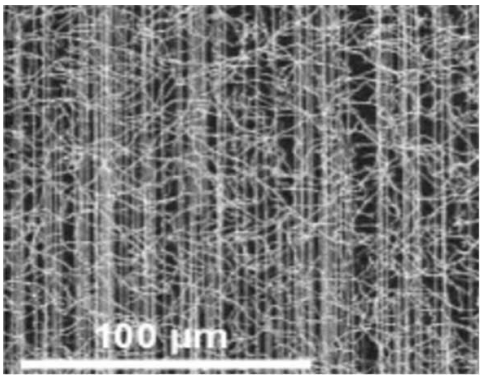
도면3b



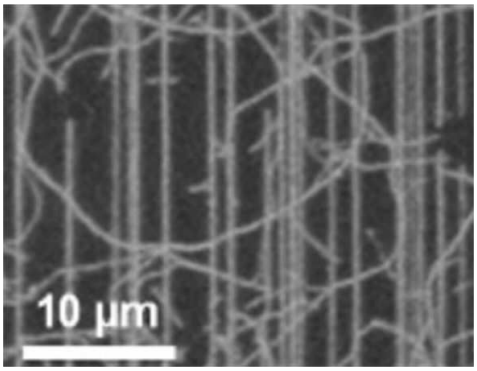
도면3c



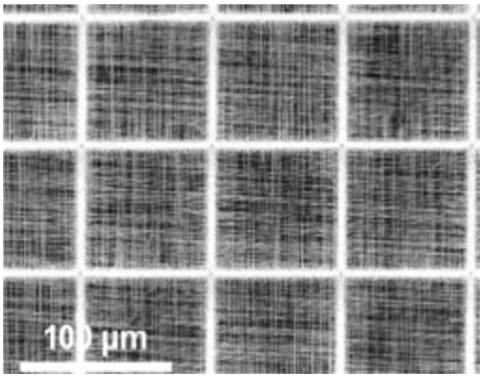
도면4a



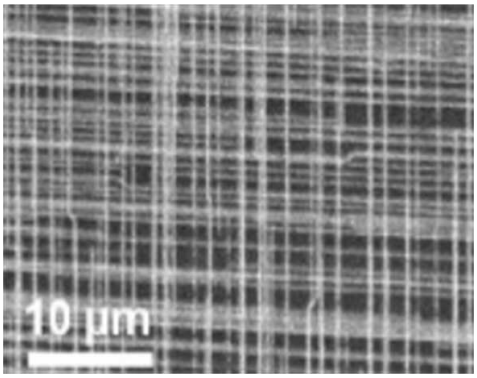
도면4b



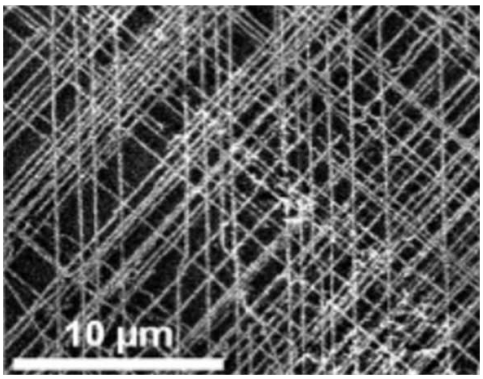
도면4c



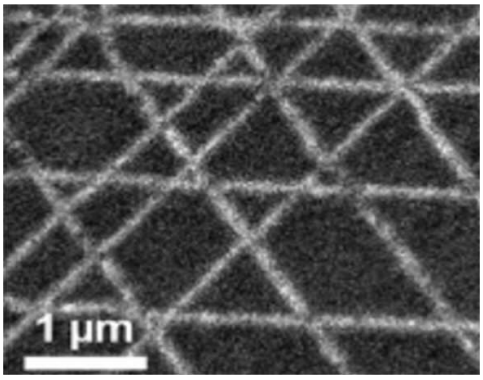
도면4d



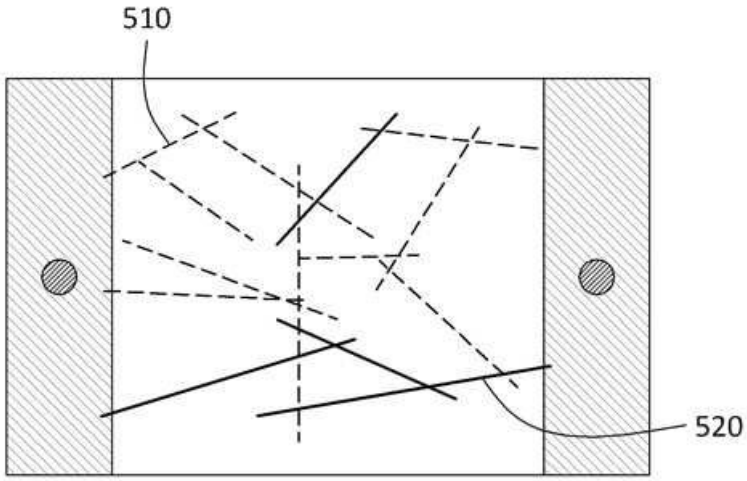
도면4e



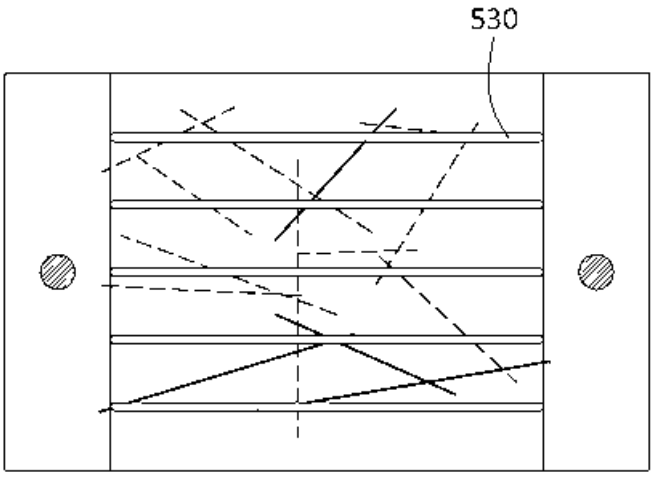
도면4f



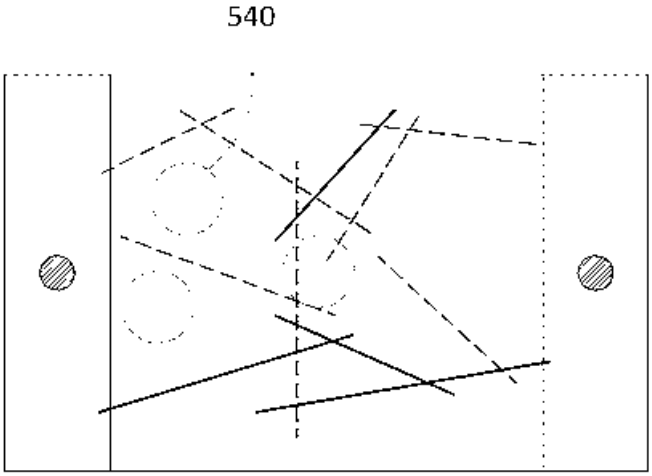
도면5a



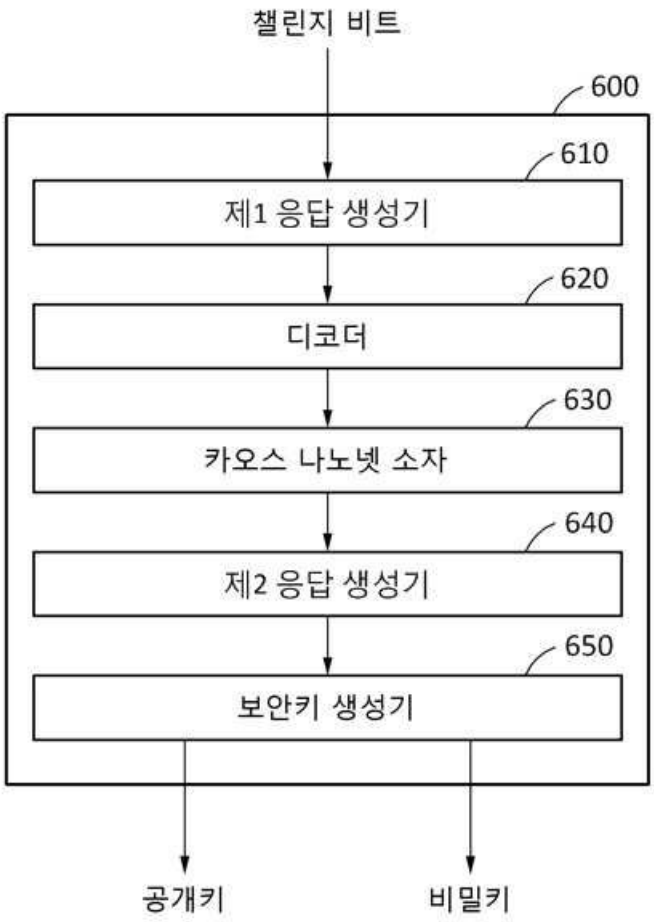
도면5b



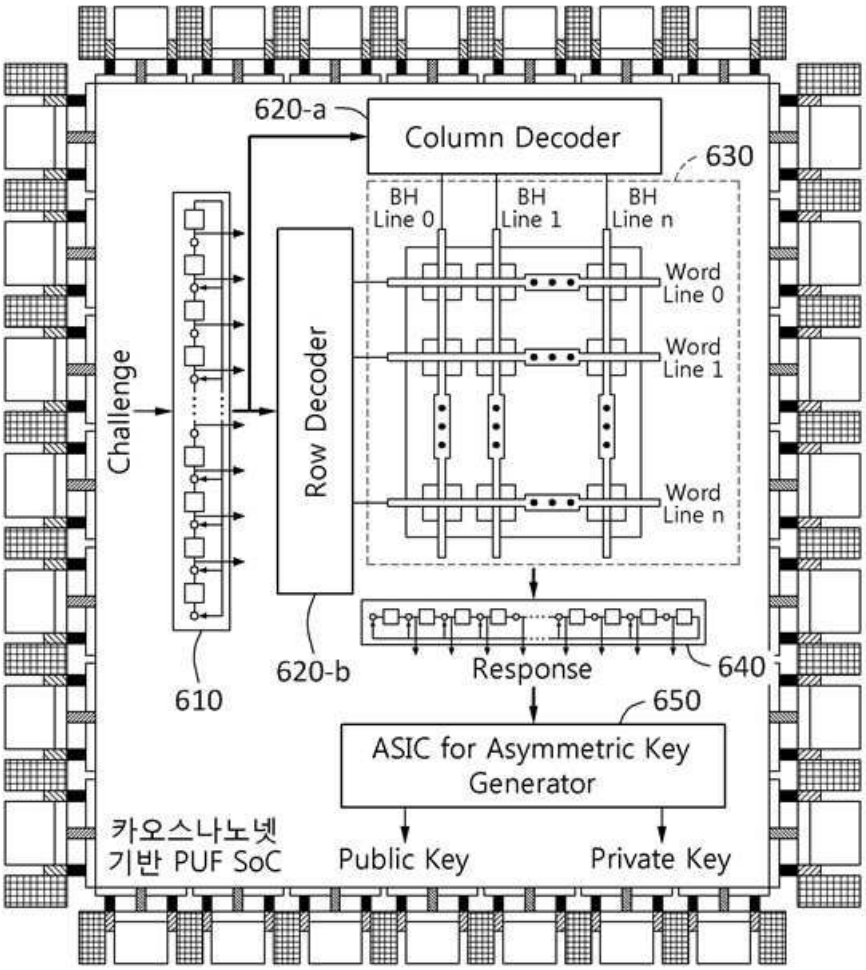
도면5c



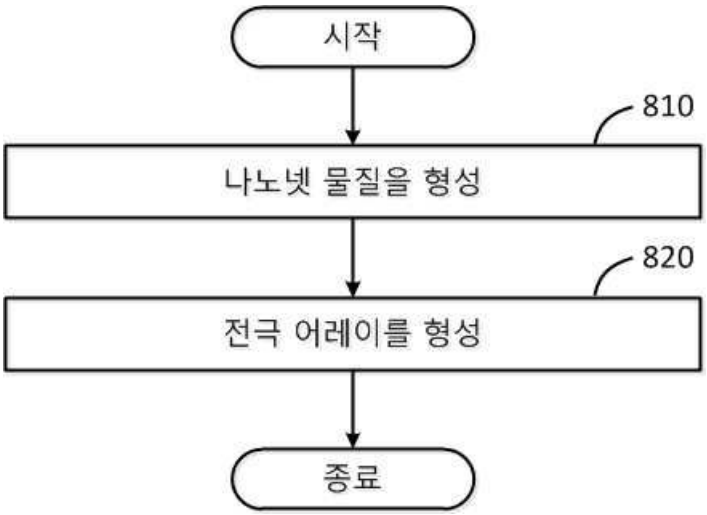
도면6


챌린지 비트
600
610
제1 응답 생성기
620
디코더
630
카오스 나노넷 소자
640
제2 응답 생성기
650
보안키 생성기
공개키
비밀키

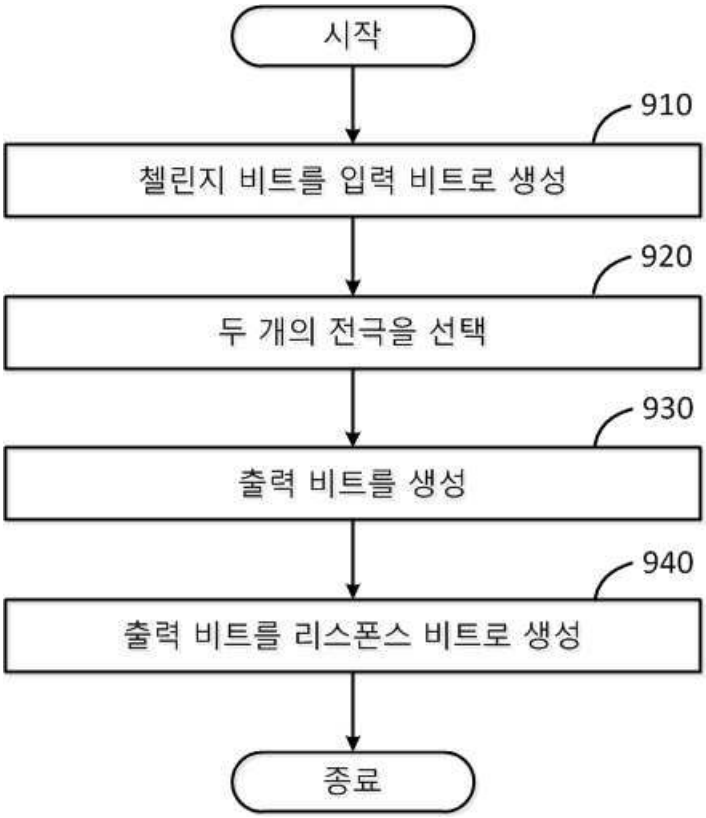
도면7


620-a
Column Decoder
630
BH Line 0
BH Line 1
BH Line n
Word Line 0
Word Line 1
Word Line n
Challenge
Row Decoder
620-b
610
Response
640
650
ASIC for Asymmetric Key Generator
카오스나노넷 기반 PUF SoC
Public Key
Private Key

도면8


시작
810
나노넷 물질을 형성
820
전극 어레이를 형성
종료

도면9


시작
910
첼린지 비트를 입력 비트로 생성
920
두 개의 전극을 선택
930
출력 비트를 생성
940
출력 비트를 리스폰스 비트로 생성
종료