

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 10 월 4 일 (04.10.2012)



(10) 국제공개번호
WO 2012/133965 A1

(51) 국제특허분류:
G06K 19/073 (2006.01)

(21) 국제출원번호: PCT/KR2011/002244

(22) 국제출원일: 2011 년 3 월 31 일 (31.03.2011)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **한양대학교 산학협력단 (IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY))** [KR/KR]; 서울시 성동구 행당동 17 번지, 133-791 Seoul (KR).

(72) 발명자: **김**

(75) 발명자/출원인 (US 에 한하여): **김동규 (KIM, Dong Kyue)** [KR/KR]; 서울 동대문구 장안 3 동 래미안 장안 1 차 아파트 105 동 2103 호, 130-718 Seoul (KR). **최병덕 (CHOI, Byong Deok)** [KR/KR]; 서울 강동구 성내 2 동 77-5 번지, 134-840 Seoul (KR). **김태욱 (KIM, Tae Wook)** [KR/KR]; 서울 성동구 행당동 한양대학교 ITBT 1217 호, 133-791 Seoul (KR).

(74) 대리인: **특허법인 무한 (MUHANN PATENT & LAW FIRM)**; 서울 강남구 논현동 51-8 명림빌딩 2,5,6 층, 135-814 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

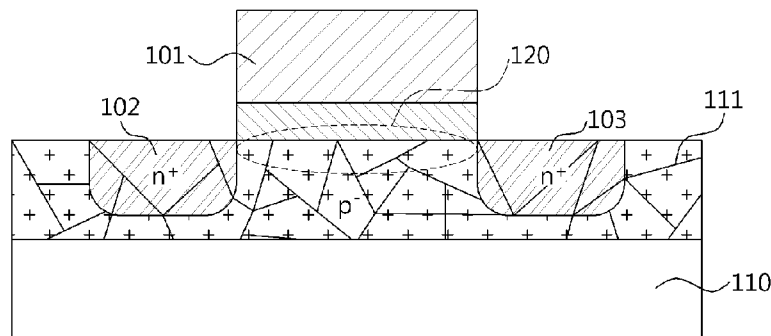
— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: APPARATUS AND METHOD FOR GENERATING IDENTIFICATION KEY USING PROCESS VARIATION

(54) 발명의 명칭 : 공정편차를 이용한 식별 키 생성 장치 및 방법

[Fig. 1]

100



(57) Abstract: An electronic apparatus for enabling a physically unclonable function (PUF) by means of a process variation in a process for manufacturing a semiconductor is provided. According to one embodiment of the present invention, the electronic apparatus comprises an N number of unit cells that are generated in the same process, on inorganic or organic material substrate, excluding a mono-crystalline silicon wafer, for example, on a display panel made from a glass material on which a TFT is integrated. In this case, each of the N number of unit cells comprise a plurality of elements further comprising an amorphous-Si, a poly-Si, a metal oxide, an organic substance, among others, wherein the a digital value having at least an N number of bits is generated by generating a digital value having least 1 bit from each of the N number of unit cells, using the characteristic differences, which is caused by the process variation from the process for manufacturing the semiconductor, between the plurality of elements that are included in each of the N number of unit cells.

(57) 요약서:

[다음 쪽 계속]



반도체 제조 공정의 공정 편차에 의해, 물리적으로 복제 불가능한 회로(Physically Unclonable Function; PUF)를 구현한 전자 장치가 제공된다. 본 발명의 일실시예에 따르면, 상기 전자 장치는, 동일한 공정에서 단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료 서브스트레이트, 이를테면 TFT가 집적되는 유리 재질의 디스플레이 패널 상에 생성되는 N개의 단위 셀을 포함한다. 이 경우, 상기 N개의 단위 셀의 각각은 비결정 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 등으로 구성된 복수 개의 소자를 포함하고, 반도체 제조 공정의 공정 편차에 의해 생기는 상기 N개의 단위 셀 각각에 포함된 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 생성하여, 상기 전자 장치는 적어도 N비트의 디지털 값을 생성한다.

명세서

발명의 명칭: 공정편차를 이용한 식별 키 생성 장치 및 방법

기술분야

- [1] 본 발명의 실시예들은 식별 키 생성을 위한 전자 장치 및 그를 이용한 보안 인증 방법에 관한 것이다.

배경기술

- [2] 최근 보안 기술의 중요성이 높아지면서, 전자 기기 또는 전자 기기를 구성하는 개별 장치(또는 모듈)에 고유의 아이디(이하에서는 식별 키라 함)를 삽입해야 할 필요성이 증가하였다.
- [3] 이러한 식별 키는 암호 키로서 사용되어 암호화 알고리즘에 이용될 수도 있으며, 경우에 따라서는 보안, 인증 이외에도 다양한 목적을 위해 상기 식별 키가 이용될 수도 있다.
- [4] 식별 키를 기기 또는 장치(또는 모듈)의 고유 아이디로 활용하기 위해서는, 생성된 식별 키를 구성하는 디지털 비트들이 1일 확률과 0일 확률이 완전히 랜덤한 무작위성(Randomness)과, 한 번 생성된 식별 키는 시간이 지나도 변하지 않는 시불변성(Time-invariance)이 높은 수준으로 보장되어야 한다.
- [5] 기존에는 무작위의 디지털 값을 생산하기 위한 방법의 일 예로 하드웨어 또는 소프트웨어를 통한 방법이 제시되었다.
- [6] 그러나, 하드웨어 또는 소프트웨어를 통한 디지털 값의 생성은 하드웨어 및 소프트웨어 개발 또는 제작에 소요되는 경비로 인하여 칩 단가가 증가하는 문제점과 생산 속도의 한계를 가지고 있다.
- [7] 따라서, 제작 비용이 낮고, 제작 과정이 간단하며, 복제가 불가능한 디지털 값을 생성하고 관리하는 시스템 및 방법은 절실하게 요구되고 있다.
- [8] 이러한 요구에 부응하기 위하여, 종래에 이러한 식별 키를 실리콘 웨이퍼 상에서 생성되는 소자들, 이를테면 CMOS(Complementary Metal?Oxide?Semiconductor)의 생산 공정에서의 공정 편차(Process variation)를 이용하여, PUF(Physically Un-clonable Function) 형태로 구현하고자 하는 몇몇 시도가 있었다. 이를테면, 동일한 공정에서 동일한 설계로 생성된 소자들 간의 특성 값(characteristic), 이를테면 threshold voltage의 차이를 이용하여 무작위적으로 0 또는 1의 디지털 값을 생성하는 방식이다.
- [9] 그런데, 실리콘 웨이퍼를 활용한 반도체 공정은 공정 편차가 비교적 작기 때문에, 그 위에 구현한 소자의 특성 값을 이용하여 생성한 PUF의 시불변성이 높은 수준으로 보장되지 않는 문제가 있었다. 즉, PUF에서 생성된 식별 키의 디지털 값이 노이즈나, 소자의 에이징(aging) 등의 원인에 의해 변경될 수 있는 여지가 있었다.

발명의 상세한 설명

기술적 과제

- [10] 공정 편차를 이용하여 무작위의 식별 키를 제공하며, 제조된 뒤에는 시불변성이 높은 수준으로 유지되는 식별 키 생성 장치가 제공된다.
- [11] 물리적으로 복제가 불가능하여 보안 공격을 방지할 수 있는 PUF를 구현함에 있어서, 생성된 식별 키의 무작위성과 시불변성을 동시에 만족시킬 수 있는 식별 키 생성 장치 및 방법이 제공된다.
- [12] 종래의 실리콘 웨이퍼 등에 비해, 에이징이나 노이즈에 매우 강한 식별 키 생성 장치 및 방법이 제공된다.

과제 해결 수단

- [13] 본 발명의 일측에 따르면, 전자 장치에 있어서, 동일한 공정에서, 비실리콘 서브스트레이트 상에 생성되는 N 개의 단위 셀을 포함하고 - 단, N은 자연수임 -, 상기 N 개의 단위 셀의 각각은, 비정질 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써 구성되는 복수 개의 소자를 포함하고, 상기 전자 장치는, 반도체 제조 공정의 공정 편차에 의해 생기는 상기 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N 개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 생성함으로써, 적어도 N 비트의 디지털 값을 생성하는, 전자 장치가 제공된다.
- [14] 이하에서 별다른 언급이 없더라도, 상기 전자 장치의 다양한 실시예는 상기 전자 장치가 반도체 장치인 예를 포함한다.
- [15] 본 발명의 일실시예에 따르면, 상기 비실리콘 서브스트레이트는 단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료이다.
- [16] 본 발명의 일부 실시예에 따르면, 상기 비실리콘 서브스트레이트는 플라스틱 패널일 수 있다. 다른 실시예에서는 상기 비실리콘 서브스트레이트가 유리 패널(glass panel)일 수도 있다. 또 다른 실시예에서는, 상기 비실리콘 서브스트레이트가 금속 박막 호일일 수도 있다. 나아가, 본 발명의 또 다른 일실시예에 따르면, 상기 비실리콘 서브스트레이트는 플렉서블(flexible) 패널로써 구성된다.
- [17] 본 발명의 일실시예에 따르면, 상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는, 제1 논리 임계치를 갖는 제1 인버터, 및 제2 논리 임계치를 갖는 제2 인버터를 포함하고, 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자는 제1 노드에 연결되고, 상기 제1 인버터의 출력 단자 및 상기 제2 인버터의 입력 단자는 제2 노드에 연결되어, 피드백 구조를 이루고, 상기 제1 논리 임계치와 상기 제2 논리 임계치는 반도체 제조 공정의 공정 편차에 기반하여 서로 상이하며, 상기 제1 노드의 논리 레벨과 상기 제2 노드의 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트 디지털 값이 결정된다.
- [18] 본 발명의 다른 일실시예에 따르면, 상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는, 제1 차동 증폭기를 구성하고, 상기 제1 차동 증폭기의

두 개의 입력 단자가 단락되는 경우, 상기 제1 차동 증폭기의 두 개의 출력 단자의 논리 레벨은 반도체 제조 공정의 공정 편차에 기반하여 서로 상이하며, 상기 두 개의 출력 단자의 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트 디지털 값이 결정된다.

- [19] 본 발명의 또 다른 일실시예에 따르면, 상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는, 제1 SR 래치를 구성하고, 상기 제1 SR 래치의 두 개의 입력 단자가 단락되는 경우, 상기 제1 SR 래치의 두 개의 출력 단자의 논리 레벨은 반도체 제조 공정의 공정 편차에 기반하여 서로 상이하며, 상기 두 개의 출력 단자의 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트 디지털 값이 결정된다.
- [20] 본 발명의 다른 일측에 따르면, 전자 장치를 포함하는 보안 시스템에 있어서, 상기 전자 장치는, 동일한 공정에서, 비실리콘 서브스트레이트 상에 생성되는 N 개의 단위 셀을 포함하고 - 단, N은 자연수임 -, 상기 N 개의 단위 셀의 각각은, 비결정 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써 구성되는 복수 개의 소자를 포함하고, 상기 전자 장치는, 반도체 제조 공정의 공정 편차에 의해 생기는 상기 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N 개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 생성함으로써, 적어도 N 비트의 디지털 값을 생성하고, 상기 보안 시스템은, 상기 적어도 N 비트의 디지털 값을 암호 키로 이용하여 보안을 위한 암호화 알고리즘을 수행하는, 보안 시스템이 제공된다.
- [21] 여기서, 상기 비실리콘 서브스트레이트는 플라스틱 패널일 수 있으며, 다른 실시예에서는 상기 비실리콘 서브스트레이트가 유리 패널(glass panel)일 수도 있고, 또 다른 실시예에서는, 상기 비실리콘 서브스트레이트가 금속박막 호일일 수도 있다.
- [22] 한편, 상기 복수 개의 소자는 비정질 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써 구성될 수 있다.
- [23] 본 발명의 일실시예에 따르면, 상기 보안 시스템에서, 상기 서브스트레이트는 비결정질 또는 다결정질의 박막필름트랜지스터 (TFT)가 집적되는 디스플레이 패널이고, 상기 보안 시스템은, 디스플레이 장치에 포함되어, 상기 적어도 N 비트의 디지털 값을 이용하여 상기 디스플레이 장치에서 디스플레이 되는 콘텐츠의 보안 인증이 수행된다.
- [24] 한편, 상기 보안 시스템에 포함되는 상기 서브스트레이트는 ISO/IEC (International Organization for Standardization/IEC) 7810 표준에 따른 ID-1 규격의 풀사이즈(Full-Size) 카드, ISO/IEC 표준에 따른 ID-000의 규격의 미니심(Mini-SIM) 카드, 및 ETSI TS 102 221 V9.0.0, Mini-UICC 표준에 따른 마이크로심(Micro-SIM) 카드 중 어느 하나의 카드의 플라스틱 부분일 수 있으며, 이 경우에 상기 보안 시스템은, 상기 적어도 N 비트의 디지털 값을 암호 키로 이용하여 상기 어느 하나의 카드의 보안을 위한 암호화 알고리즘을 수행할 수

있다.

[25] 또한, 본 명세서에서 상기 보안 시스템은, 반도체 장치로서 구현된 상기 보안 장치를 포함하는 임의의 시스템으로 이해될 수 있다.

[26] 본 발명의 또 다른 일측에 따르면, 전자 장치를 이용하여 보안 인증을 수행하는 방법에 있어서, 상기 전자 장치는, 동일한 공정에서, 비결정질 또는 다결정질의 서브스트레이트 상에 생성되는 N 개의 단위 셀을 포함하고 - 단, N은 자연수임 -, 상기 N 개의 단위 셀의 각각은, 비정질 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써 구성되는 복수 개의 소자를 포함하고, 상기 방법은, 반도체 제조 공정의 공정 편차에 의해 생기는, 상기 N 개의 단위 셀 각각에 포함된 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N 개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 식별하여 적어도 N 비트의 디지털 값을 생성하는 단계, 및 상기 적어도 N 비트의 디지털 값을 암호 키로 이용하여 보안을 위한 암호화 알고리즘을 수행하는 단계를 포함하는, 방법이 제공된다.

발명의 효과

[27] 비실리콘(단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료) 서브스트레이트 상에서 하드웨어적으로 PUF를 구성하므로, 생성된 식별 키 값의 무작위성뿐만 아니라 시불변성이 높은 수준으로 보장된다.

[28] 소자의 에이징(aging), 온도나 습도 등의 외부 환경 변화, 및 노이즈에 강하여 신뢰도가 높은 PUF가 제공된다.

[29] 디스플레이 장치의 콘텐츠 보안 인증이나, 스마트 카드의 보안 인증 등에 다양하게 활용될 수 있는 신뢰할 수 있고 물리적인 복제가 불가능한 전자 장치가 제공된다.

도면의 간단한 설명

[30] 도 1은 본 발명의 일실시예에 따른 전자 장치를 구현하는 원리를 설명하기 위한 개념적 소자 단면도이다.

[31] 도 2는 본 발명의 일실시예에 따라 공정 편차를 이용하여 1 비트의 디지털 암호 키를 생성하는 하나의 단위 셀의 예시적 회로도이다.

[32] 도 3은 본 발명의 실시예들을 이해하기 위한 참고 그래프이다.

[33] 도 4는 본 발명의 일실시예에 따라 전자 장치 위에 구현된, 식별 키 생성을 위한 예시적 구현을 도시하는 회로도이다.

[34] 도 5는 본 발명의 일실시예에 따라, 차동 증폭기에 의해 구현되는 단위 셀을 도시한다.

[35] 도 6은 본 발명의 일실시예에 따라 식별 키 생성을 위한 전자 장치가 구현된 예시적 회로도를 도시한다.

[36] 도 7은 본 발명의 일실시예에 따라 NOR 타입 SR 래치로 구현되는 단위 셀을 도시한다.

도 8은 본 발명의 다른 일실시예에 따라 NAND 타입 SR 래치로 구현되는 단위 셀을 도시한다.

도 9는 본 발명의 일실시예에 따른 전자 장치를 포함하는 보안 시스템이 디스플레이 장치의 적어도 일부에 포함되는 예를 도시한 조감도이다.

도 10은 본 발명의 또 다른 하나의 예시적 응용을 도시한다.

【발명을 실시하기 위한 구체적인 내용】

이하에서, 본 발명의 일부 실시예를, 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

도 1은 본 발명의 일실시예에 따른 전자 장치를 구현하는 원리를 설명하기 위한 개념적 소자 단면도(100) 이다.

반도체 공정에서 공정편차는 다양한 이유에 의해 기인한다. 이를테면, 트랜지스터를 제조하는 경우, 유효 게이트 길이, 도핑 농도 관련 지수, 산화물 두께 관련 지수 또는 문턱전압 등의 파라미터가 공정편차의 원인이 될 수 있다. 이러한 공정 편차는 자연현상에 기인하는 것이므로, 공정편차를 작게 할 수는 있어도 완전히 제거하는 것은 불가능하다.

일반적으로 공정편차가 작은 반도체 제조 공정이 우수한 것으로 인식되어 반도체 공정의 기술분야에서는 공정 편차를 줄이기 위한 다양한 시도를 하고

있었다.

그러나, 본 발명의 실시예들에서는, 오히려 이러한 반도체 공정의 공정 편차를 이용하여, 임의로 결정되며 한 번 결정되면 쉽게 변경되지 않는 디지털 값을 생성하는 식별 키 생성 방법에 이용한다.

예를 들어, 도 1에서는 NMOS 타입 트랜지스터를 생성하기 위한 서브스트레이트(substrate)(110)로서, 종래의 실리콘 웨이퍼 대신 유리(glass) 또는 금속막(호일)을 사용하였다.

다만, 본 발명의 실시예에서는 서브스트레이트(110)에 무기 물질뿐만 아니라, 유기 물질도 사용될 수 있다.

이러한 본 발명의 실시예에서, 서브스트레이트(110) 위에 구현된 poly-Si TFT의 channel 내에는 결정들 간의 불규칙한 결정 단면(111)이 존재하고, 이러한 단면들은 시불변성 및 무작위성을 가지고 그 편차 또한 크기 때문에, 소스 및 드레인 (102 또는 103)의 도핑 농도와 그 영역이 확산(diffusion)에 의해 변하는 것에 비하여 소자 특성에 훨씬 결정적인 영향을 준다.

통상적인 실리콘 웨이퍼를 사용하여 제작하는 전자 장치의 경우, 반도체 소자의 동작에 따른 열 또는 시간에 따른 자연적인 확산에 의해 소스 또는 드레인(102 및 103)의 도핑 농도와 그 영역이 변하기도 하고, 또한 자연적으로

에이징(aging)에 의한 소자 열화로 인해 소자 특성이 변하기도 한다.

- [50] 따라서, 실리콘 웨이퍼를 서브스트레이트로서 사용하는 종래의 전자 장치에 비해, 본 발명의 실시예에 따라 단결정 실리콘 웨이퍼가 아닌 무기 또는 유기 물질 서브스트레이트(110)를 사용하여 그 위에 비결정 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 등의 물질을 기반으로 게이트(101), 소스 또는 드레인(102 및 103)을 생성하여 트랜지스터를 구현하고 PUF 회로를 구성한 경우, 트랜지스터의 특성 값, 이를테면 임계전압(threshold voltage)의 우열이 변경될 확률이 더 작고, 실리콘 웨이퍼 서브스트레이트 공정에서 구현한 소자보다 큰 편차를 보인다.
- [51] 따라서, 시간의 변화에 따른 에이징(aging) 현상도 개선되고, 노이즈나 외부 온도 변화에 따른 소자 특성 값의 변화도 훨씬 작아진다.
- [52] 본 발명의 실시예들에서, 실리콘 웨이퍼 대신 무기 또는 유기 재료를 서브스트레이트로서 선택했기 때문에, 동일 공정에서 생성되는 소자들 간의 uniformity가 실리콘 웨이퍼를 사용하는 반도체 공정보다 낮으며, 또한 소자의 전기적 특성의 우열이 바뀌는 것도 방지하였다.
- [53] PUF를 구성하는 다양한 실시예들은 도 2 이하를 참조하여 보다 상세히 후술한다.
- [54] 도 2는 본 발명의 일실시예에 따라 공정 편차를 이용하여 1 비트의 디지털 암호 키를 생성하는 하나의 단위 셀의 예시적 회로도이다.
- [55] 도 2의 예에서 제1 인버터(210) 과 제2 인버터(220)가 도시되었다.
- [56] 본 실시예에서, 제1 인버터(210) 및 제2 인버터(220)는 공히, 도 1과 같이, 다결정 또는 비결정 서브스트레이트 위에 게이트, 소스 및 드레인 단자를 구현하여 생성된다.
- [57] 통상적인 반도체 제조 공정에서, 인버터(inverter)는 단결정 실리콘 웨이퍼(Silicon Wafer)인 서브스트레이트 위에, 포토리소그래피 방식 등에 의해 게이트, 소스 및 드레인 단자를 구현함으로써 생성된다.
- [58] 그러나, 본 실시예에서는 단결정 웨이퍼 대신 다결정 또는 비결정 서브스트레이트를 사용하여 인버터 소자를 구현한다.
- [59] 이 경우, 도 1을 참고하여 상기한 바와 같이, 단결정 실리콘 웨이퍼를 서브스트레이트로 사용할 때보다 공정편차는 더 커진다. 이러한 공정편차는 후술할 제1 인버터(210)와 제2 인버터(220) 간의 논리 임계치 차이로 이해될 수 있다.
- [60] 본 실시예에서, 제1 인버터(210)은 제1 논리 임계치를 갖고, 제2 인버터(220)은 제2 논리 임계치를 갖는다. 논리 임계치(logic threshold)는 인버터의 입력 전압과 출력 전압이 동일한 값을 가지는 경우의 전압 값이며, 도 3을 참조하여 보다 상세히 후술한다.
- [61] 인버터 소자의 논리 임계치는, 동작 중인 인버터의 출력 단자와 입력 단자를 단락(short)시키는 경우의 전압 값으로 측정될 수 있다.

- [62] 만약 공정편차가 없다면, 동일한 공정에서 제조되는 인버터들은 이론상 동일한 논리 임계치를 갖도록 디자인 되지만, 상기한 바와 같이 실제 제조 공정에서는 공정편차가 존재하기 때문에, 실제로는 어느 두 개의 인버터도 완벽히 동일한 논리 임계치를 가질 수 없다.
- [63] 더구나, 실리콘 웨이퍼 서브스트레이트 대신 금속, 유리, 플라스틱과 같은 무기 또는 유기 재료 서브스트레이트를 사용한 본 발명의 실시예들에서는 상기 논리 임계치의 차이는 더 커진다.
- [64] 따라서, 상기 제1 인버터(210)와 상기 제2 인버터(220)는 동일한 제조 공정에서 제조된 것으로서, 공정편차에 기인한 논리 임계치의 차이를 갖는다.
- [65] 상기 논리 임계치의 차이는, 공정에 따라 상이하지만, 이를테면 수 내지 수십 밀리볼트 정도의 크기 또는 그 이상일 수 있다. 이러한 논리 임계치의 차이가 측정에 의해 정확하게 측정되지 않을 수도 있기 때문에, 상기 제1 인버터(210)의 논리 임계치와 상기 제2 인버터(220)의 논리 임계치를 별도의 비교기 회로를 이용하여 측정하는 것은, 정확하지 않을 수 있다.
- [66] 따라서, 두 인버터의 논리 임계치를 상대적으로 비교할 수 있는(즉, 별도의 비교기 회로를 이용하지 않고 측정하는) 방법이 요구된다. 본 발명의 일부 실시예들에서는, 두 개의 인버터 사이의 논리 임계치를 상대적으로(별도의 비교기 회로를 이용하지 않고 자체적으로) 비교하여, 어느 쪽의 논리 임계치가 큰지 판단할 수 있다.
- [67] 만약 제2 인버터(220)가 존재하지 않는 경우라면, 제1 인버터(210)의 입력 단자와 출력 단자를 단락시키는 경우 제1 인버터(210)의 출력 전압은 상기 제1 인버터(210)의 논리 임계치와 같을 것이다.
- [68] 또한, 제1 인버터(210)가 존재하지 않는 경우라면, 제2 인버터(220)의 입력 단자와 출력 단자를 단락시키는 경우 제2 인버터(220)의 출력 전압은 상기 제2 인버터(220)의 논리 임계치와 같을 것이다.
- [69] 그러나, 도 2와 같이 제1 인버터(210)의 입력 단자와 제2 인버터(220)의 출력 단자가 단락되어 제1 노드에 연결되어 있고, 제1 인버터(210)의 출력 단자와 제2 인버터(220)의 입력 단자가 단락되어 제2 노드에 연결되는 경우는 위의 경우들과 다른 결과를 가져온다.
- [70] 스위치(230)를 이용하여 상기 제1 노드와 상기 제2 노드를 단락시키는 경우, 단락된 상기 두 노드의 전압 값은, 상기 제1 인버터(210)의 논리 임계치와 상기 제2 인버터(220)의 논리 임계치의 사이의 어떤 값(평균 값이 아닐 수 있음, 이하 같다)이 된다.
- [71] 상기 두 인버터의 논리 임계치 중 어느 쪽의 값이 높은지와 무관하게, 상기 스위치(230)가 닫혀있는 동안은, 출력 전압의 값이 상기 두 인버터의 논리 임계치들의 사이의 값이 된다.
- [72] 그리고, 그 후 스위치(230)를 열어서, 상기 제1 노드와 상기 제2 노드를 개방(open)시키는 경우, 상기 제1 노드와 상기 제2 노드 중 어느 하나의 전압 값의

- 논리적 레벨(logical level)은 "0"이 되고, 다른 하나의 논리적 레벨은 "1"이 된다.
- [73] 이를테면, 만약 제1 인버터(210)의 논리 임계치가 상기 제2 인버터(220)의 논리적 임계치 보다 낮다고 가정하는 경우, 상기 스위치(230)가 닫혀서 제1 노드(Out의 반대쪽 노드)와 제2 노드(Out 노드)가 단락된 동안의 제1 노드의 전압은 상기 제1 인버터(210)의 논리 임계치보다 높다.
- [74] 따라서, 상기 스위치(230)가 다시 열려서 상기 제1 노드와 상기 제2 노드가 개방된 후, 제1 인버터(210)는 (자신의 입력 단자인) 제1 노드의 전압을 논리적 레벨 하이(High)로 인식하고, 따라서, 제1 인버터(210)의 출력 단자인 제2 노드의 전압을 논리적 레벨 로우(Low)로 만든다.
- [75] 이 경우, 제2 인버터(220)는 (자신의 입력 단자인) 제2 노드의 전압을 논리적 레벨 로우로 인식하고, 따라서, 제2 인버터(220)의 출력 단자인 제1 노드의 전압을 논리적 레벨 하이로 만든다.
- [76] 결국, 도 2의 출력 단자("Out")인 제2 단자의 전압의 논리적 레벨은 하이(High)가 된다.
- [77] 반대로, 만약 제1 인버터(210)의 논리 임계치가 상기 제2 인버터(220)의 논리적 임계치 보다 높다고 가정하는 경우, 상기 스위치(230)가 닫혀서 제1 노드와 제2 노드가 단락된 동안의 제1 노드의 전압은 상기 제1 인버터(210)의 논리 임계치보다 낮다.
- [78] 따라서, 상기 스위치(230)가 다시 열려서 상기 제1 노드와 상기 제2 노드가 개방된 후, 제1 인버터(210)는 (자신의 입력 단자인) 제1 노드의 전압을 논리적 레벨 로우로 인식하고, 따라서, 제1 인버터(210)의 출력 단자인 제2 노드의 전압을 논리적 레벨 하이로 만든다.
- [79] 이 경우, 제2 인버터(220)는 (자신의 입력 단자인) 제2 노드의 전압을 논리적 레벨 하이로 인식하고, 따라서, 제2 인버터(220)의 출력 단자인 제1 노드의 전압을 논리적 레벨 로우로 만든다.
- [80] 결국, 도 2의 출력 단자("Out")인 제2 단자의 전압의 논리적 레벨은 로우가 된다.
- [81] 상기한 바와 같이, 제1 인버터(210)의 논리 임계치와 제2 인버터(220)의 논리 임계치 중 어느 쪽이 높은가에 따라, 스위치(230)의 단락-개방 이후의 출력 단자("Out")의 논리적 레벨은 하이(또는 "1")로 되거나, 또는 로우(또는 "0")으로 된다.
- [82] 그런데, 동일한 제조 공정에서 제조된 상기 제1 인버터(210)와 제2 인버터(220) 중, 어느 쪽의 논리 임계치가 높을지는 랜덤(random)하며, 확률적으로 두 개의 인버터 중 한 쪽의 논리 임계치가 다른 쪽의 논리 임계치보다 높을 확률은 50% 정도이다.
- [83] 그리고, 일단 제조되고 나서는, 상기 논리 임계치가 높은 쪽이 어느 쪽인지는 바뀌기 어렵다. 이는 종래의 실리콘 웨이퍼를 서브스트레이트 위에 소자를 구현한 경우도 그렇지만, 본 발명의 실시예들과 같이, 유리, 금속, 플라스틱과 같은 무기 또는 유기 재료 서브스트레이트 위에 비결정 실리콘(amorphous-Si),

다결정 실리콘(poly-Si), 산화 금속, 유기물 등으로 구성된 소자를 사용한 경우에는 더욱 그렇다.

- [84] 왜냐하면 도 1을 참고하여 상술한 바와 같이, 단결정 실리콘 웨이퍼에 집적한 트랜지스터에 비해 무기 또는 유기 재료 서브스트레이트 위에 집적한 다결정 실리콘 박막트랜지스터(poly-Si TFT)에서는 결정간의 경계(도 1의 111)에 의한 소자 편차가 확산(diffusion)에 의한 소자의 특성변화 보다 매우 크기 때문이다.
- [85] 즉, 제1 인버터(210)나 제2 인버터(220)의 논리적 임계치의 차이는 더욱 커지면서, 둘 중에서 논리적 임계치가 작은 쪽이 논리적 임계치가 큰 쪽으로 바뀔 확률은 매우 작아진다.
- [86] 이러한 특징은 통상의 반도체 소자로서는 열등한 특징이지만, 랜덤한 식별 키를 생성한 다음, 한 번 생성된 식별 키가 바뀌지 않으므로, 하드웨어 펌프프린트나 암호 키 생성을 위한 PUF로서는 우수한 특징이다.
- [87] 결국, 도 2의 실시예를 통해, 단위 셀에 1 비트의 디지털 값("1"이 되거나 "0"이 될 확률은 동일하지만, 한 번 결정되고 나면 바뀌기 어려운 값)이 생성된다.
- [88] 그리고, 도 2에 도시된 단위 셀이 N 개(N은 자연수) 있다면, N 비트의 디지털 값인 식별 키가 생성될 수 있다.
- [89] 상기 과정은, 도 3의 그래프를 참조하는 경우, 보다 명확히 이해될 수 있다.
- [90] 도 3은 본 발명의 실시예들을 이해하기 위한 참고 그래프이다.
- [91] 그래프 (a)는 종래의 단결정 실리콘 웨이퍼 위에 트랜지스터 소자 들을 구현하는 경우의 셀들의 Threshold voltage의 분포 (좌측 점선 부분) 및 본 발명의 일실시예에 따라 무기 또는 유기 재료 서브스트레이트 상에 구현된 폴리실리콘 박막트랜지스터 소자 들을 구현하는 경우의 셀들의 Threshold voltage의 분포 (우측 실선 부분)을 도시한다.
- [92] 무기 또는 유기 재료 서브스트레이트를 사용하는 경우에는 실리콘 웨이퍼를 이용하는 경우에 비해, 셀들의 평균적 Threshold voltage가 높고, 셀 간의 Threshold voltage 차이가 크다. 즉, 공정 편차가 크다. 이러한 점이 원래 반도체 소자에서는 단점으로 인식되지만, 본 발명의 실시예들과 같은 식별 키 생성을 위한 PUF에서는 장점이 된다.
- [93] 그래프 (b)는 구현되는 반도체 소자 도핑 후 이동도(mobility) 분포를 비교한 것이다. 도시된 바와 같이, 무기 또는 유기 재료 패널 위에 폴리실리콘 박막트랜지스터 소자 들을 구현하는 경우의 셀들의 평균적 이동도는 낮고 분포는 넓으나 (좌측 실선 부분), 종래의 단결정 실리콘 웨이퍼 위에 트랜지스터 소자 들을 구현하는 경우에는 평균적 이동도는 높고 분포는 좁은 것을 확인할 수 있다. (좌측 점선 부분)
- [94] 따라서, 단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료 패널들, 유리, 플라스틱, 알루미늄 호일 등을 사용하는 경우, 식별 키 생성에 있어서 무작위성과 시불변성이 커지리라는 것을 쉽게 이해할 수 있다.
- [95] 도 4는 본 발명의 일실시예에 따라 전자 장치 위에 구현된, 식별 키 생성을 위한

예시적 구현을 도시하는 회로도이다.

- [96] 본 실시예에서, 식별 키 생성을 위한 반도체 장치(400)은, 인버터(411) 내지 인버터(415)의 5 개의 인버터, 선택부(420) 및 비교기(430)을 포함한다.
- [97] 선택부(420)는 도 4에 도시된 5 개의 인버터 중, 어느 두 개를 선택한다. 이를테면, 인버터(412)와 인버터(413)가 선택될 수 있다.
- [98] 이 경우, 비교기(430)는, 인버터(412)의 논리 임계치와 인버터(413)의 논리 임계치를 비교하고, 상기 비교 결과에 따라 Out 단자로 출력 전압을 제공한다. 그리고 상기 Out 단자의 출력 전압의 논리적 레벨에 따라 1 비트의 디지털 값이 생성될 수 있다.
- [99] 그리고, 선택부(420)가 다른 두 개의 인버터를 선택하는 경우, 상기 비교기(430)은 다시 1 비트의 디지털 값을 생성할 수 있다.
- [100] 상기한 바와 같이, 선택부(420)가 5 개의 인버터(411 내지 415) 중 두 개를 선택하고, 비교기(430)가 선택된 두 개의 인버터의 논리 임계치를 비교함으로써 디지털 값을 생성하는 경우, 최대 10 비트의 디지털 값이 생성될 수 있다.
- [101] 본 실시예에서는 인버터가 5 개 포함되었으나, 본 발명은 이에 한정되지 않으며, 생성하고자 하는 디지털 값의 비트 수, 회로의 면적 등을 고려하여 다양한 변경이 가능하다.
- [102] 그리고, 전자 장치 내에 집적될 수 있는 비교기(430)의 면적이 인버터들(431 내지 435)의 면적에 비해 상당히 큰 것을 고려했기 때문에, 본 실시예에서는 선택부(420)를 통해 복수 개의 인버터와 하나의 비교기(430)가 연결되었다. 그러나, 다른 응용 예에서는 인버터 두 개 당 비교기 하나가 짝을 이루어, N 비트의 디지털 값을 생성할 수도 있다.
- [103] 한편, 본 발명의 다른 실시예에서는, 반도체 공정 편차를 이용한 인버터 소자의 논리 임계치 차이를 이용하여 디지털 값 형태의 식별 키를 생성하는 전자 장치의 단위 셀은 아래 도 5와 같은 구성도 가능하다.
- [104] 도 5는 본 발명의 일실시예에 따라, 차동 증폭기에 의해 구현되는 단위 셀(500)을 도시한다.
- [105] 단위 셀(500)은 차동 증폭기 회로이다. 트랜지스터 및 저항 중 적어도 하나의 소자로 구성되는 차동 증폭기 회로인 단위 셀(500)은 제1 입력 단자(511)와 제2 입력 단자(512)의 전압의 차이를 증폭하여, 제1 출력 단자(521)와 제2 출력 단자(522) 사이의 전압 차이로서 제공한다.
- [106] 따라서, 상기 제1 입력 단자(511)과 제2 입력 단자(522)를 단락시키는 경우, 이론적으로는, 출력 전압 값인 제1 출력 단자(521)와 제2 출력 단자(522) 사이의 전압 차이가 0이어야 한다.
- [107] 그러나, 반도체 공정편차에 의한 소자간의 전기적 특성 차이 때문에, 제1 출력 단자(521)의 전압과 제2 출력 단자(522)의 전압은 완전히 같지 않다.
- [108] 따라서, 도 4의 실시예에서 인버터의 논리 임계치를 비교한 것과 같은 방법으로, 두 출력 단자 중 어느 출력 단자의 전압이 높은 지를 비교한다면, 1

비트의 디지털 값을 생성할 수 있다.

- [109] 이를테면, 제1 입력 단자(511)와 제2 입력 단자(512)를 단락시킨 경우에, 제1 출력 단자(521)의 전압 값이 제2 출력 단자(522)의 전압 값보다 높은 경우, 디지털 값 "1"로 인식하고, 반대의 경우에는 디지털 값 "0"으로 인식할 수 있다.
- [110] 따라서, 이러한 차동 증폭기 단위 셀(500)이 N 개 집적되면 N 비트의 디지털 값 형태로 식별 키를 제공할 수 있으며, 이러한 구현이 아래 도 6에서 도시된다.
- [111] 도 6은 본 발명의 일실시예에 따라 식별 키 생성을 위한 반도체 장치(600)가 구현된 예시적 회로도를 도시한다.
- [112] 도시된 실시예에서 전자 장치(600)는 6 개의 차동 증폭기(611 내지 616), 상기 6 개의 차동 증폭기 중 어느 하나를 선택하는 선택부(620), 및 상기 선택부(620)에 의해 선택된 차동 증폭기의 두 개의 출력 전압을 비교하여 1 비트의 디지털 값을 생성하는 비교부(630)를 포함한다.
- [113] 이 경우, 상기 6 개의 차동 증폭기(611 내지 616)의 전체 입력 단자는 단락되며, 동일한 전압을 갖는다.
- [114] 본 발명의 일 실시예에 따르면, 선택부(620)는 6:1 MUX 소자일 수 있다. 다만, 이는 본 발명의 구현을 위한 일 실시예에 불과하며, 본 발명은 특정한 실시예에 한정되지 않는다.
- [115] 따라서, MUX 소자의 입력/출력 포트의 수는 변경될 수 있으며, 나아가 선택부(620)는 MUX 소자가 아닌 다른 소자일 수도 있다. 상기 6:1 MUX 소자는 12 개의 입력 단자를 통해 입력 되는 6 개의 차동 증폭기의 출력 전압을 두 개의 출력 단자로 출력한다. 그리고, 이 두 개의 출력 단자는 비교부(630)의 두 개의 입력 단자에 연결된다.
- [116] 도 6의 실시예에서는 적어도 6 비트의 디지털 값인 식별 키가 생성될 수 있다.
- [117] 한편, 본 발명의 다른 실시예들에서는, 도 2 내지 도 4의 인버터를 이용한 실시예, 또는 도 5 내지 도 6의 차동 증폭기를 이용한 실시예 외에도 다양한 응용이 가능하다.
- [118] 이를 테면, 상기 단위 셀은 SR 래치(Latch)를 이용하여 구현될 수도 있다.
- [119] 도 7은 본 발명의 일실시예에 따라 NOR 타입 SR 래치로 구현되는 단위 셀(700)을 도시한다.
- [120] 그리고 도 8은 본 발명의 다른 일실시예에 따라 NAND 타입 SR 래치로 구현되는 단위 셀(800)을 도시한다.
- [121] 도 7의 실시예에서, 입력 단자들(711 및 712)을 단락(short)시킴으로써 출력 단자 OUT의 논리적 레벨은 두 개의 NOR 소자들의 논리적 임계치에 따라 임의로 결정되며, 한 번 결정된 값은 변경되기 어렵다.
- [122] 도 8의 경우도 입력 단자들(811 및 812)을 단락(short)시킴으로써 출력 단자 OUT의 논리적 레벨은 두 개의 NAND 소자들의 논리적 임계치에 따라 임의로 결정되며, 한 번 결정된 값은 변경되기 어렵다.
- [123] 도 9 및 도 10은 본 발명의 다양한 실시예들이 이용된 예시적 응용예들을

도시한다.

- [124] 도 9는 본 발명의 일실시예에 따른 전자 장치를 포함하는 보안 시스템이 디스플레이 장치(910)의 적어도 일부에 포함되는 예를 도시한 조감도(900)이다.
- [125] 본 예에서, 디스플레이 장치(910)는 빌딩의 옥상에 위치하여 영상을 디스플레이 한다.
- [126] 이 경우, 상기 디스플레이 장치(910)의 적어도 일부분에 포함되는 실리콘 웨이퍼를 제외한 무기 또는 유기 재료 패널 상에, 도 1 내지 도 9를 참조하여 설명한 본 발명의 실시예에 따른 식별 키 생성을 위한 단위 셀들이 집적된다.
- [127] 그러면 이러한 단위 셀들이 집적된 전자 장치(920)은 디스플레이 장치(910)에 고유한 식별 키를 제공할 수 있으며, 이 식별 키는 인증 처리부(930)에 제공되어, 디스플레이 장치(910)를 통해 디스플레이 되는 영상 콘텐츠의 인증 작업을 수행한다.
- [128] 이를 테면, 공상과학 영화에서, 해커가 네트워크 해킹을 통해, 옥외 광고 디스플레이 장치에 자신이 원하는 영상을 디스플레이 시키는 불법적 행위들이 등장한다. 테러리스트가 자신들의 협박 영상을, 허가 없이 뉴욕 타임 스퀘어의 옥외 광고 디스플레이장치에서 플레이 시키는 경우를 상상할 수 있다.
- [129] 그러나, 본 발명의 실시예들에 따른 전자 장치(920)가 N 비트의 디지털 값을 생성하고, 이를 암호화 키 또는 하드웨어 펌거프린트 값으로 하여 인증 처리부(930)가 콘텐츠의 인증을 수행한다.
- [130] 이 과정에서, 디스플레이 장치(910)에 디스플레이 될 허가 받은 콘텐츠는 인증 처리부(930)가 생성된 식별 키를 이용하여 플레이를 승인하고, 허가 받지 않은 콘텐츠는 플레이를 승인하지 않을 수 있다.
- [131] 그러면 디스플레이 장치(910) 자체적으로, 그것이 디스플레이 할 콘텐츠를 최종적으로 확인하여 잘못된 영상이 디스플레이 되는 것을 방지할 수 있다.
- [132] 도 9의 응용에는 어디까지나 본 발명의 실시예들이 활용될 수 있는 다양한 예시적 응용에 중 하나일 뿐이다.
- [133] 따라서, 비슷한 원리에 의해, 오디오 플레이 장치에 본 발명의 실시예들에 따른 전자 장치를 포함시켜, 영상이 아닌 음성 신호를 인증시키는 것도 가능하다.
- [134] 이러한 응용들은, 해커에 의한 네트워크 해킹 및 허가 받지 않은 콘텐츠의 임의적 플레이를 방지하기 위한 것이다.
- [135] 그러나, 본 발명의 실시예들의 다른 응용에서는, 이를 미디어 콘텐츠의 디지털 권리 관리(Digital Right Management; DRM)에 활용할 수도 있다.
- [136] 또한, 본 발명의 실시예들의 또 다른 응용에서는, 이러한 식별 키를 동영상 시청 등급(Under 17, Under 13 등급 등) 제한에 이용할 수도 있다.
- [137] 도 10은 본 발명의 또 다른 하나의 예시적 응용을 도시한다.
- [138] 신용 카드(1000)는, 이를테면 ISO/IEC (International Organization for Standardization/IEC) 7810 표준에 따른 ID-1 규격의 풀사이즈(Full-Size) 카드일 수 있다.

- [139] 신용 카드(1000)는 IC 칩(1010)이 내장된 스마트 카드일 수도 있다.
- [140] 스마트 카드(1000)에서 IC 칩(1010)은, 전자 결제나 신분 확인을 위한 데이터를 저장하거나 및/또는 몇 가지 컴퓨팅을 수행할 수도 있다.
- [141] 이 경우에, IC 칩(1010) 자체적으로 암호 키를 이용하여 보안 인증 작업을 수행할 수도 있으나, 본 발명의 일 실시예에 따르면, 도 1 내지 도 8을 참조하여 상술한 실시예들에서, 단위 셀이 신용 카드(1000)의 플라스틱 부분 위에 집적될 수도 있다.
- [142] 여기서, 상기 실시예들에 사용된 단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료 서브스트레이트는 신용 카드(1000)의 플라스틱 부분일 수 있다.
- [143] 그러면, 전자 장치(1020)는 IC 칩(1010)의 보안 인증 작업과 병행하여, 또는 이를 보조하거나 대신하여 보안 인증 작업에 활용될 수 있다.
- [144] 또는, IC 칩(1010)에 대한 물리적 공격(Physical attack), 이를테면 카드를 분해하여 IC 칩의 보안 모듈을 공격하거나 암호 키를 알아내는 등의 행위를 방지할 수 있다.
- [145] 물리적 공격을 위해 신용 카드(1000)의 플라스틱 부분을 파손하는 경우, IC 칩(1010)과 함께 또는 이에 대신하여 보안 인증을 위한 식별 키를 제공하는 본 발명의 실시예들에 의한 전자 장치(1020)도 함께 파괴되기 때문이다.
- [146] 이러한 실시예에 의해, 신용 카드(1000)의 보안 수준은 한번 더 높아질 수 있다.
- [147] 한편, 도 10의 신용 카드(1000) 또한 하나의 실시예에 불과하며, 카드 크기나 종류는 다양하게 변경될 수도 있다. 이를테면, ISO/IEC 표준에 따른 ID-000의 규격의 미니심(Mini-SIM) 카드, 및 ETSI TS 102 221 V9.0.0, Mini-UICC 표준에 따른 마이크로심(Micro-SIM) 카드 중 어느 하나의 카드의 플라스틱 부분도, 본 발명의 실시예들에 의한 전자 장치를 집적하는 서브스트레이트가 될 수 있다.
- [148] 본 발명의 일 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 본 발명을 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 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

- [149] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.
- [150] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

청구범위

- [청구항 1] 전자 장치에 있어서,
동일한 공정에서, 비실리콘 서브스트레이트 상에 생성되는 N 개의 단위 셀을 포함하고 - 단, N은 자연수임 -,
상기 N 개의 단위 셀의 각각은, 비정질 실리콘(amorphous-Si), 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써 구성되는 복수 개의 소자를 포함하고,
상기 전자 장치는, 반도체 제조 공정의 공정 편차에 의해 생기는 상기 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N 개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 생성함으로써, 적어도 N 비트의 디지털 값을 생성하는, 전자 장치.
- [청구항 2] 제1항에 있어서,
상기 비실리콘 서브스트레이트는 단결정 실리콘 웨이퍼를 제외한 무기 또는 유기 재료인, 전자 장치.
- [청구항 3] 제1항에 있어서,
상기 비실리콘 서브스트레이트는 플라스틱 패널인, 전자 장치.
- [청구항 4] 제1항에 있어서,
상기 비실리콘 서브스트레이트는 유리 패널(glass panel)인, 전자 장치.
- [청구항 5] 제1항에 있어서,
상기 비실리콘 서브스트레이트는 금속 박막 호일인, 전자 장치.
- [청구항 6] 제1항에 있어서,
상기 비실리콘 서브스트레이트는 플렉서블 패널로써 구성되는, 전자 장치.
- [청구항 7] 제1항에 있어서,
상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는,
제1 논리 임계치를 갖는 제1 인버터; 및
제2 논리 임계치를 갖는 제2 인버터
를 포함하고,
상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자는 제1 노드에 연결되고, 상기 제1 인버터의 출력 단자 및 상기 제2 인버터의 입력 단자는 제2 노드에 연결되어, 피드백 구조를 이루고,
상기 제1 논리 임계치와 상기 제2 논리 임계치는 반도체 제조 공정의 공정 편차에 기반하여 서로 상이하며, 상기 제1 노드의 논리 레벨과 상기 제2 노드의 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트 디지털 값이 결정되는, 전자 장치.

- [청구항 8] 제1항에 있어서,
 상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는,
 제1 차동 증폭기를 구성하고,
 상기 제1 차동 증폭기의 두 개의 입력 단자가 단락되는 경우, 상기
 제1 차동 증폭기의 두 개의 출력 단자의 논리 레벨은 반도체 제조
 공정의 공정 편차에 기반하여 서로 상이하며, 상기 두 개의 출력
 단자의 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트
 디지털 값이 결정되는, 전자 장치.
- [청구항 9] 제1항에 있어서,
 상기 N 개의 단위 셀 중 제1 단위 셀에 포함된 복수 개의 소자는,
 제1 SR 래치를 구성하고,
 상기 제1 SR 래치의 두 개의 입력 단자가 단락되는 경우, 상기 제1
 SR 래치의 두 개의 출력 단자의 논리 레벨은 반도체 제조 공정의
 공정 편차에 기반하여 서로 상이하며, 상기 두 개의 출력 단자의
 논리 레벨에 따라 상기 제1 단위 셀에 대응하는 1 비트 디지털 값이
 결정되는, 전자 장치.
- [청구항 10] 전자 장치를 포함하는 보안 시스템에 있어서,
 상기 전자 장치는,
 동일한 공정에서, 비실리콘 서브스트레이트 상에 생성되는 N 개의
 단위 셀을 포함하고 - 단, N은 자연수임 -,
 상기 N 개의 단위 셀의 각각은, 비결정 실리콘(amorphous-Si),
 다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써
 구성되는 복수 개의 소자를 포함하고,
 상기 전자 장치는, 반도체 제조 공정의 공정 편차에 의해 생기는
 상기 복수 개의 소자들 간의 특성 차이를 이용하여, 상기 N 개의
 단위 셀 각각으로부터 적어도 1비트의 디지털 값을 생성함으로써,
 적어도 N 비트의 디지털 값을 생성하고,
 상기 보안 시스템은, 상기 적어도 N 비트의 디지털 값을 암호 키로
 이용하여 보안을 위한 암호화 알고리즘을 수행하는, 보안 시스템.
- [청구항 11] 제10항에 있어서,
 상기 비실리콘 서브스트레이트는 플라스틱 패널인, 보안 시스템.
- [청구항 12] 제10항에 있어서,
 상기 비실리콘 서브스트레이트는 유리 패널(glass panel)인, 보안
 시스템.
- [청구항 13] 제10항에 있어서,
 상기 비실리콘 서브스트레이트는 금속박막 호일인, 보안 시스템.
- [청구항 14] 제10항에 있어서,
 상기 서브스트레이트는 비결정질 또는 다결정질의

[청구항 15]

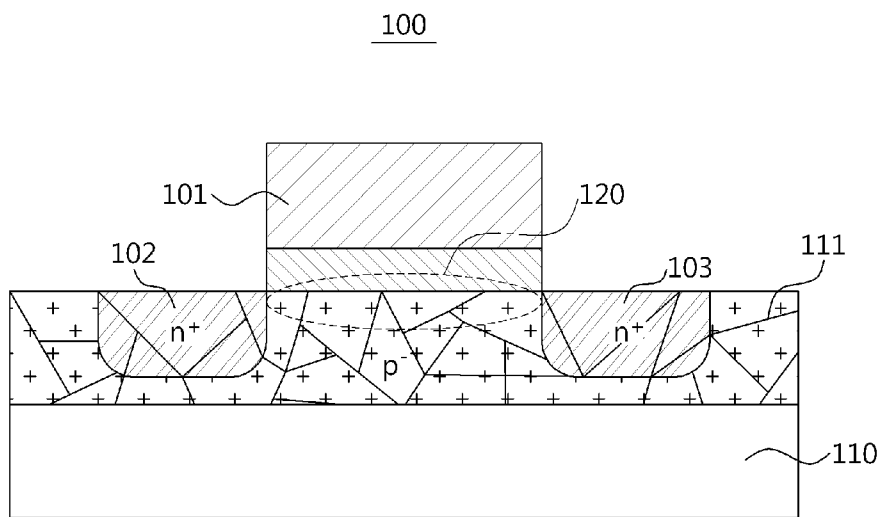
박막필름트랜지스터 (TFT)가 집적되는 디스플레이 패널이고,
상기 보안 시스템은, 디스플레이 장치에 포함되어, 상기 적어도 N
비트의 디지털 값을 이용하여 상기 디스플레이 장치에서
디스플레이 되는 콘텐츠의 보안 인증을 수행하는, 보안 시스템.
제10항에 있어서,

상기 서브스트레이트는 ISO/IEC (International Organization for
Standardization/IEC) 7810 표준에 따른 ID-1 규격의
풀사이즈(Full-Size) 카드, ISO/IEC 표준에 따른 ID-000의 규격의
미니심(Mini-SIM) 카드, 및 ETSI TS 102 221 V9.0.0, Mini-UICC
표준에 따른 마이크로심(Micro-SIM) 카드 중 어느 하나의 카드의
플라스틱 부분이고,
상기 보안 시스템은, 상기 적어도 N 비트의 디지털 값을 암호 키로
이용하여 상기 어느 하나의 카드의 보안을 위한 암호화
알고리즘을 수행하는, 보안 시스템.

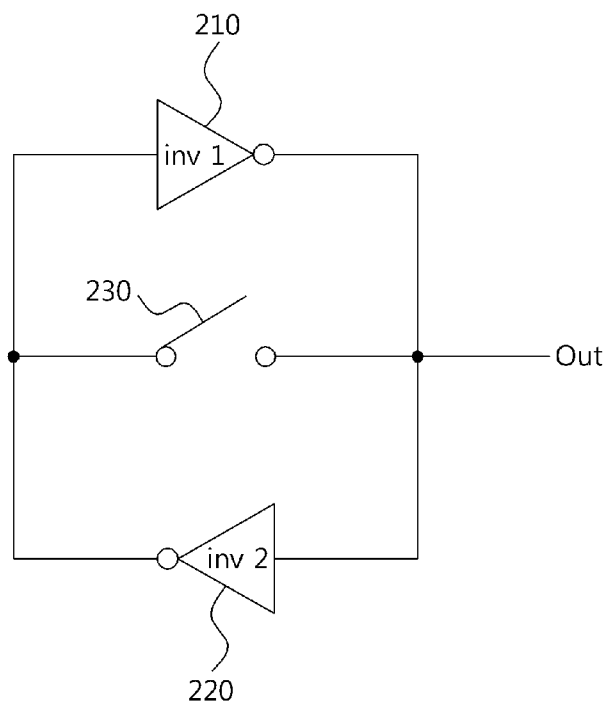
[청구항 16]

전자 장치를 이용하여 보안 인증을 수행하는 방법에 있어서,
상기 전자 장치는,
동일한 공정에서, 비결정질 또는 다결정질의 서브스트레이트 상에
생성되는 N 개의 단위 셀을 포함하고 - 단, N은 자연수임 -,
상기 N 개의 단위 셀의 각각은, 비정질 실리콘(amorphous-Si),
다결정 실리콘(poly-Si), 산화 금속, 유기물 중 적어도 하나로써
구성되는 복수 개의 소자를 포함하고,
상기 방법은,
반도체 제조 공정의 공정 편차에 의해 생기는, 상기 N 개의 단위 셀
각각에 포함된 복수 개의 소자들 간의 특성 차이를 이용하여, 상기
N 개의 단위 셀 각각으로부터 적어도 1비트의 디지털 값을
식별하여 적어도 N 비트의 디지털 값을 생성하는 단계; 및
상기 적어도 N 비트의 디지털 값을 암호 키로 이용하여 보안을
위한 암호화 알고리즘을 수행하는 단계
를 포함하는, 방법.

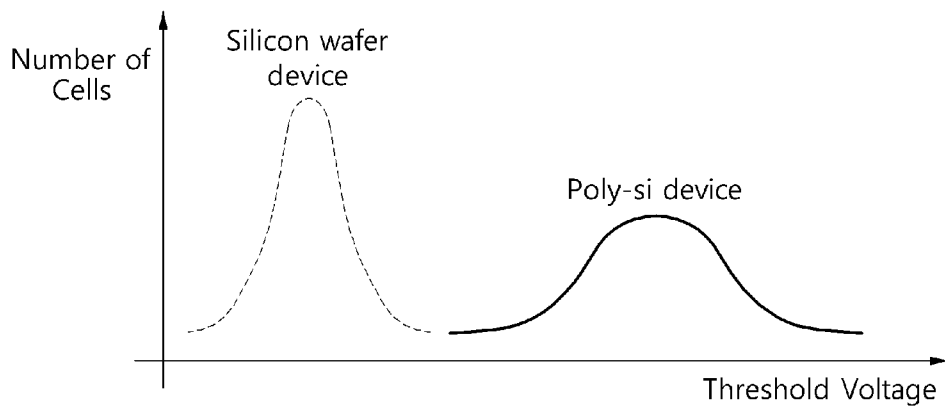
[Fig. 1]



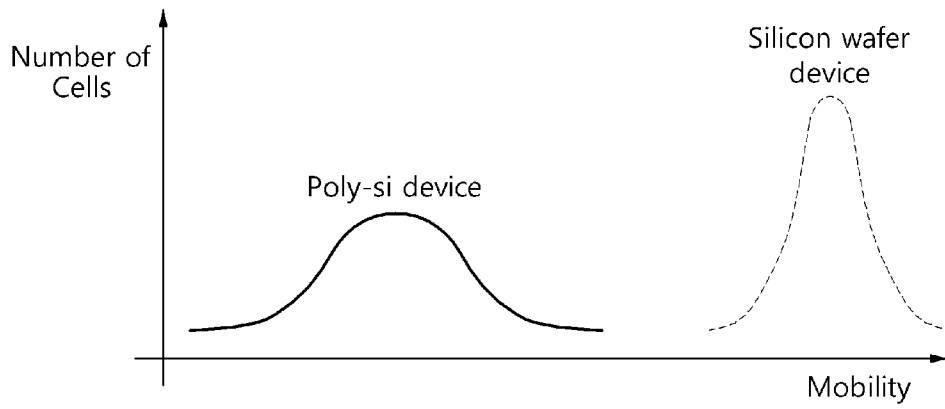
[Fig. 2]



[Fig. 3]

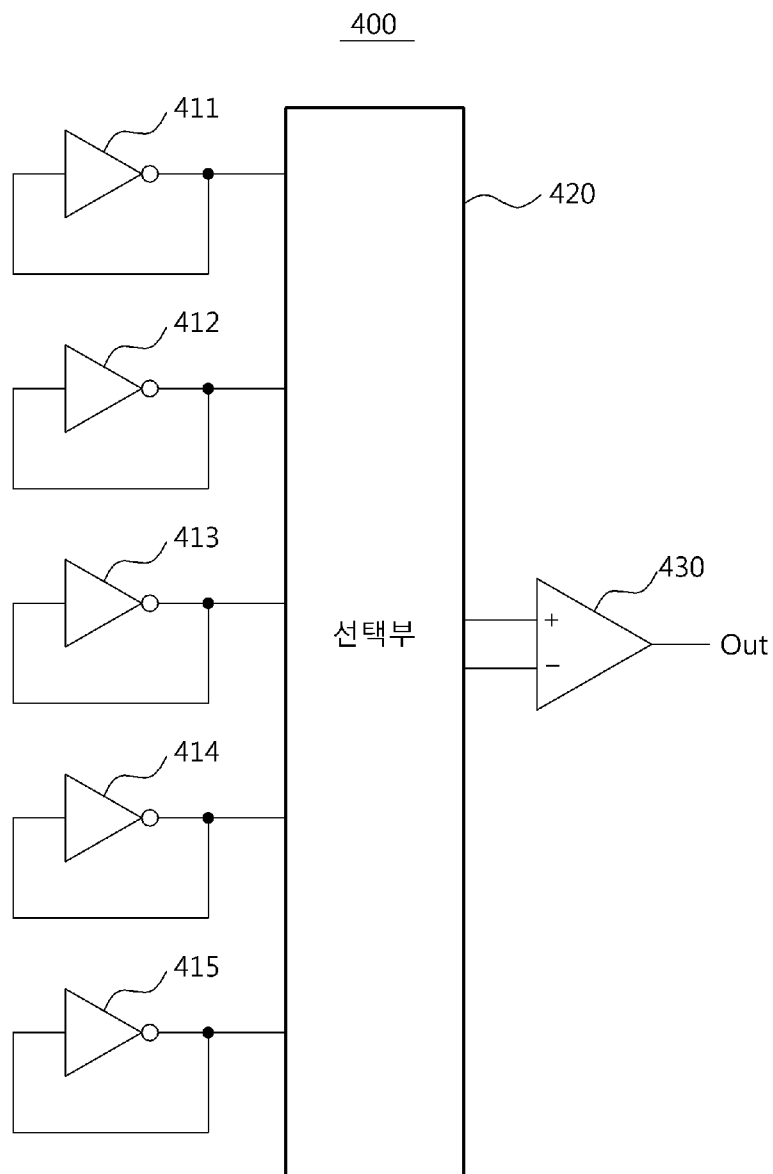


(a)

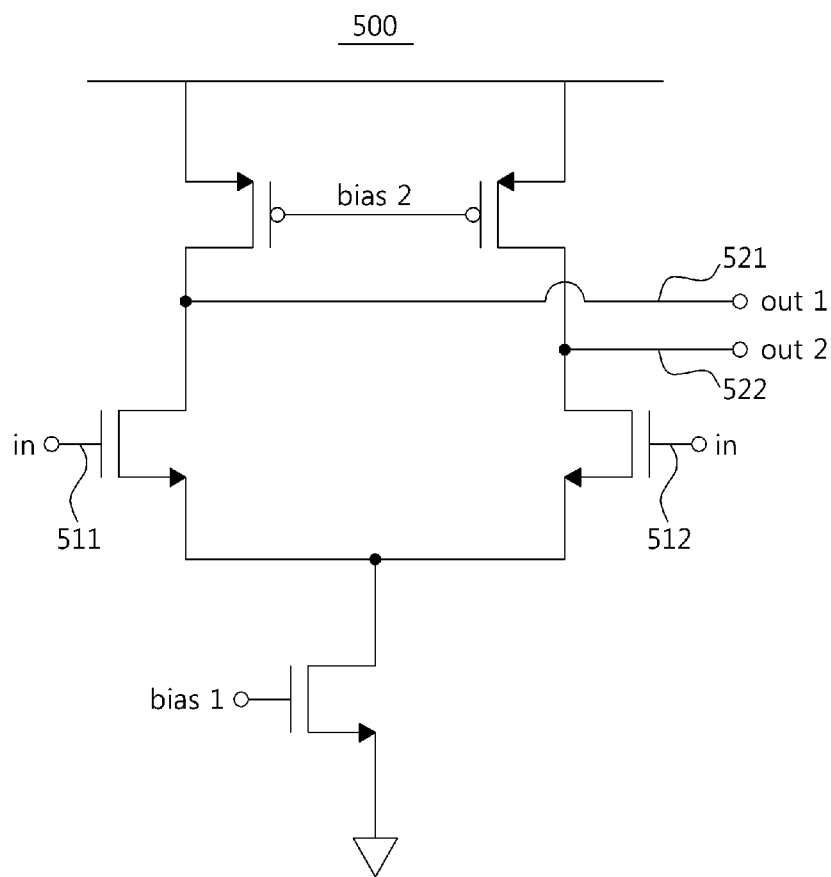


(b)

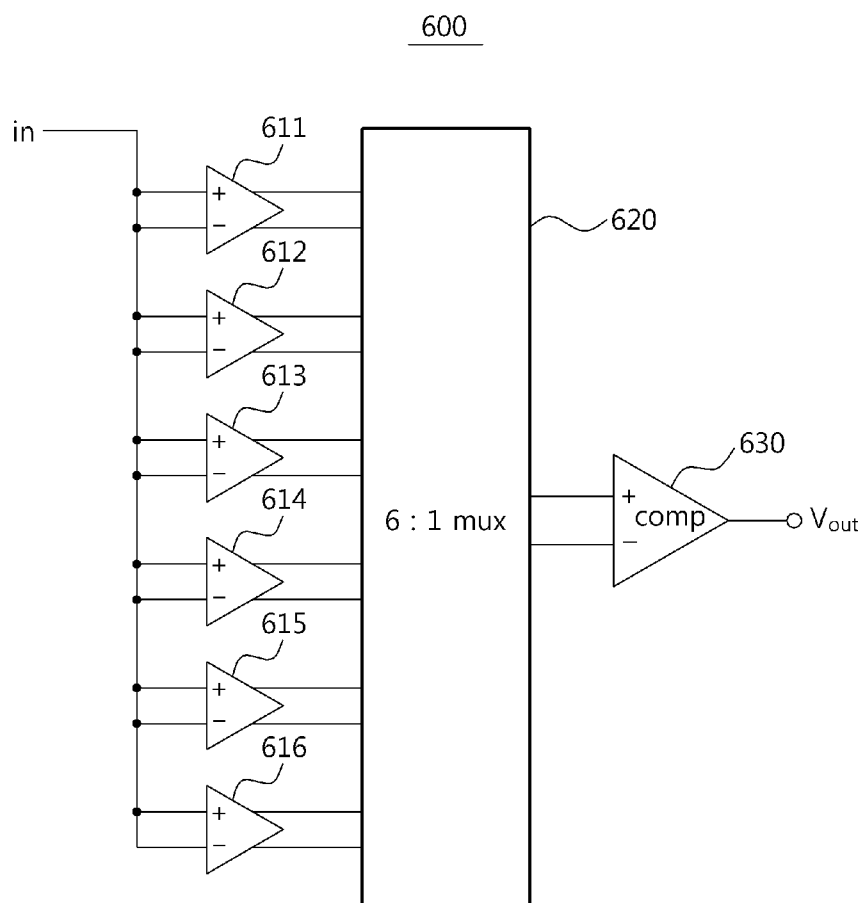
[Fig. 4]



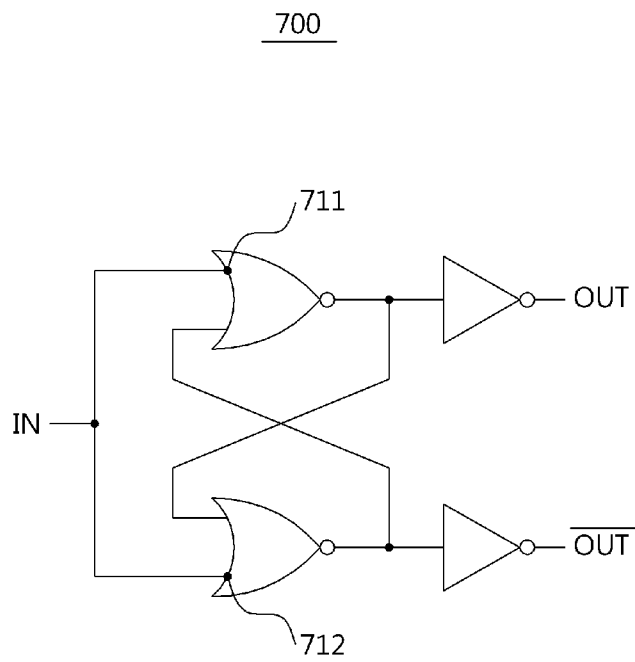
[Fig. 5]



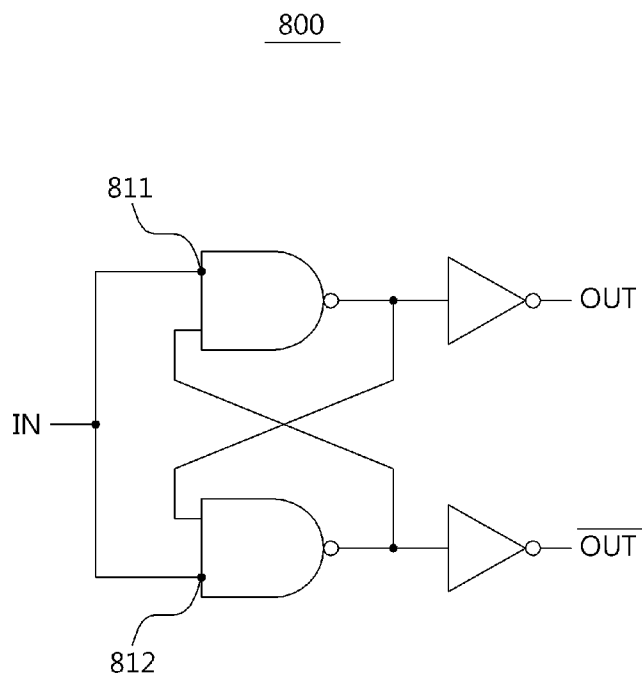
[Fig. 6]



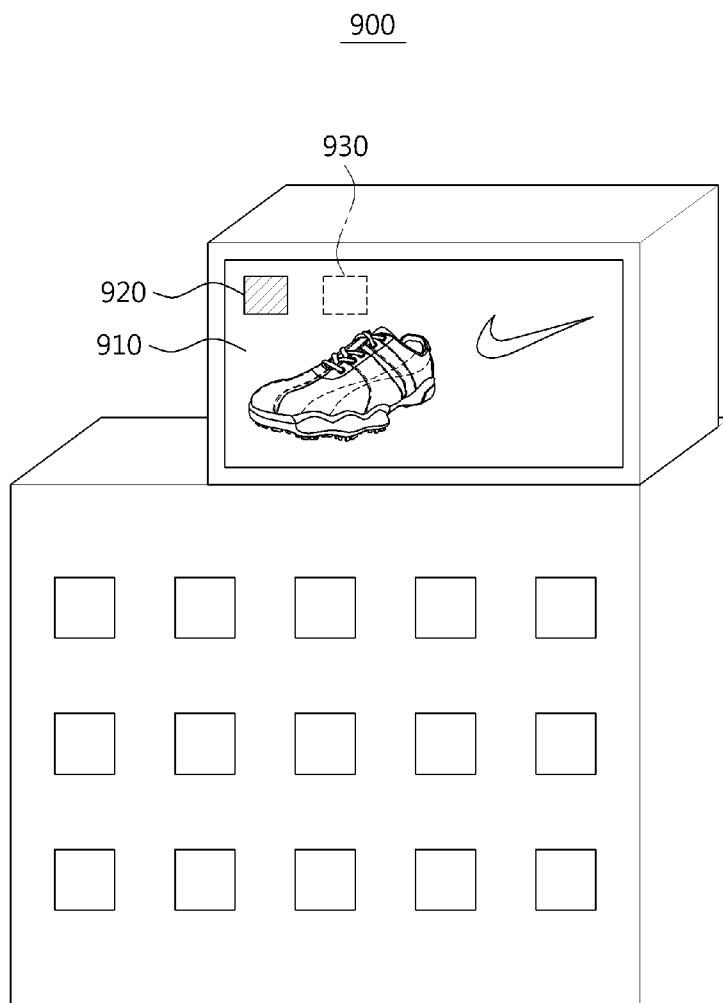
[Fig. 7]



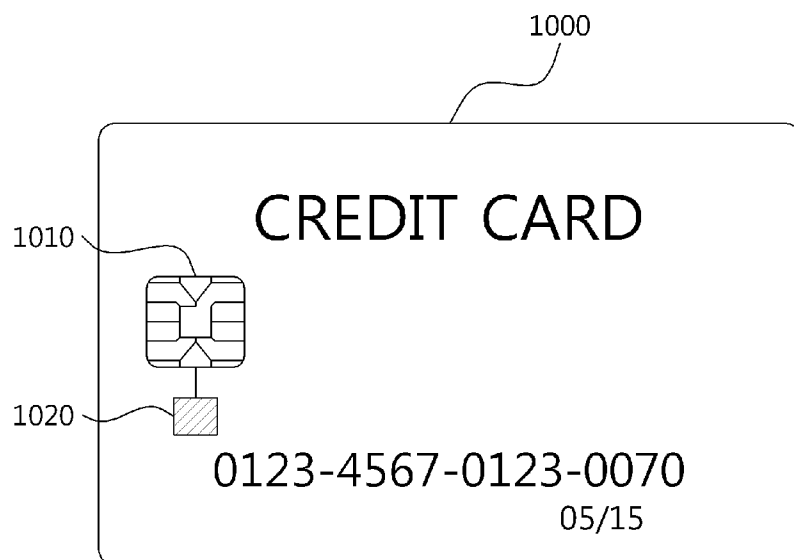
[Fig. 8]



[Fig. 9]



[Fig. 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2011/002244**A. CLASSIFICATION OF SUBJECT MATTER****G06K 19/073(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06K 19/073; G06F 17/50; G06K 17/00; H04B 5/02; G01R 31/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: semiconductor, element, characteristic, difference, bit, generation, non-silicon, amorphous silicone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0068987 A (CQTRON, INC.) 29 June 2009 See abstract and page 2.	1-16
A	US 2005-0183047 A1 (STEPHEN SAPIRO) 18 August 2005 See abstract and figures 1-8.	1-16
A	US 6161213 B1 (KEITH LOFSTROM) 12 December 2000 See abstract and figure 1.	1-16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

31 OCTOBER 2011 (31.10.2011)

Date of mailing of the international search report

01 NOVEMBER 2011 (01.11.2011)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2011/002244

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0068987 A	29.06.2009	NONE	
US 2005-0183047 A1	18.08.2005	US 7210634 B2	01.05.2007
US 6161213 B1	12.12.2000	CA 2362962 A1	24.08.200
		CN 1346473 A	24.04.2002
		EP 1203329 A1	08.05.2002
		JP 03787070 B2	21.06.2006
		JP 2002-537646 A	05.11.2002
		KR 10-0698560 B1	21.03.2007
		TW 449846 A	11.08.2001
		US RE040188 E1	25.03.2008
		WO 2000-049538 A1	24.08.2000

A. 발명이 속하는 기술분류(국제특허분류(IPC)) G06K 19/073(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) G06K 19/073; G06F 17/50; G06K 17/00; H04B 5/02; G01R 31/02 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 반도체, 소자, 특성, 차이, 비트, 생성, 비실리콘, 비정질 실리콘		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0068987 A (CQTRON, INC.) 2009.06.29 요약 및 페이지 2 참조.	1-16
A	US 2005-0183047 A1 (STEPHEN SAPIRO) 2005.08.18 요약 및 도면 1-8 참조.	1-16
A	US 6161213 B1 (KEITH LOFSTROM) 2000.12.12 요약 및 도면 1 참조.	1-16
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2011년 10월 31일 (31.10.2011)	국제조사보고서 발송일 2011년 11월 01일 (01.11.2011)	
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (302-701) 대전광역시 서구 청사로 189, 정부대전청사 팩스 번호 82-42-472-7140	심사관 박장환 전화번호 82-42-481-8463 	

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0068987 A	2009.06.29	없음	
US 2005-0183047 A1	2005.08.18	US 7210634 B2	2007.05.01
US 6161213 B1	2000.12.12	CA 2362962 A1	2000.08.24
		CN 1346473 A	2002.04.24
		EP 1203329 A1	2002.05.08
		JP 03787070 B2	2006.06.21
		JP 2002-537646 A	2002.11.05
		KR 10-0698560 B1	2007.03.21
		TW 449846 A	2001.08.11
		US RE040188 E1	2008.03.25
		WO 2000-049538 A1	2000.08.24