

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

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



(10) 국제공개번호
WO 2012/133964 A1

(51) 국제특허분류:
G06F 7/58 (2006.01)

(21) 국제출원번호: PCT/KR2011/002219

(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: **김태욱**

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

(74) 대리인: 특허법인 무한 (**MUHANN PATENT & LAW FIRM**); 서울시 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).

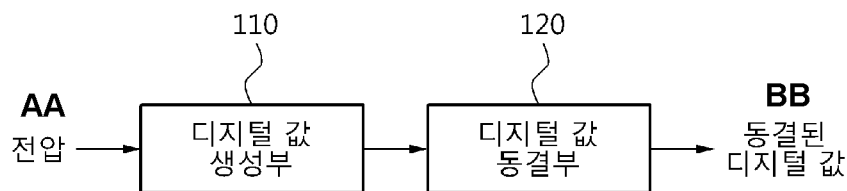
공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: APPARATUS AND METHOD FOR GENERATING DIGITAL VALUE

(54) 발명의 명칭 : 디지털 값 생성 장치 및 방법

[Fig. 1]



AA ... Voltage

BB ... Frozen digital value

110 ... Digital value generation unit

120 ... Digital value freezing unit

(57) Abstract: An apparatus and a method for generating a physically unclonable function (PUF) value are disclosed. An apparatus for generating a digital value comprises: a digital value generation unit for generating a random digital value by using a process variation of a semiconductor; and a digital value freezing unit, which is connected to the digital value generation unit and is fixed in either a first state or a second state in accordance with the generated digital value, for freezing the digital value, thereby freezing the digital value that is generated when the digital value generation unit is initially driven.

(57) 요약서: PUF(Physically Unclonable Function) 값 생성 장치 및 방법이 개시된다. 디지털 값 생성 장치는 반도체의 공정 편차를 이용하여 무작위의 디지털 값을 생성하는 디지털 값 생성부 및 상기 디지털 값 생성부에 연결되고 상기 생성된 디지털 값에 대응하여 제 1 상태 또는 제 2 상태 중 어느 한 상태로 고정되어 상기 디지털 값을 동결하는 디지털 값 동결부를 포함하여 상기 디지털 값 생성부의 초기 구동 시 생성된 디지털 값을 동결할 수 있다.



WO 2012/133964 A1

명세서

발명의 명칭: 디지털 값 생성 장치 및 방법

기술분야

- [1] 디지털 보안 분야에 연관되며, 보다 특정하게는 전자장치의 보안, 임베디드 시스템(Embedded system) 보안, SoC(System on Chip) 보안, 스마트 카드(Smart Card) 보안, USIM(Universal Subscriber Identity Module) 보안 등을 위하여 필요한 암호화 및 복호화 방법과 디지털 서명 등에 사용되는 식별키를 생성하는 장치 및 방법에 연관된다.

배경기술

- [2] 최근 전자태그 등의 기술이 발달하면서 대량으로 생산되는 칩에 고유의 아이디(이하에서는 식별 키라 함)를 삽입해야 할 필요성이 증가하였다. 따라서, 무작위의 디지털 값(이를테면, 식별 키 또는 고유 아이디 등)을 생성하는 장치 및 방법의 개발이 필요하게 되었다.
- [3] 하지만 식별 키를 장치 또는 칩의 고유 아이디로 활용하기 위해서는, 생성된 식별 키를 구성하는 디지털 비트들이 '1'일 확률과 '0'일 확률이 완전히 랜덤한 무작위성(Randomness)과 한 번 생성된 식별 키는 시간이 지나도 변하지 않는 시불변성(Time-invariance)이 높은 수준으로 보장되어야 한다.
- [4] 그러나, 종래의 디지털 값을 생성하는 장치로부터 생성되는 디지털 값은 무작위성은 만족하지만, 노이즈, 차동 노화(differential aging) 등으로 인하여 신뢰성 즉, 시불변성(time invariant)을 만족하기는 어렵다는 문제가 있었다.
- [5] 따라서, 노이즈에 강하고 외부 온도 등의 환경 변화에도 강한 시불변성이 보장되는 복제가 불가능한 디지털 값을 생성하는 장치 및 방법은 절실하게 요구되고 있다.

발명의 상세한 설명

기술적 과제

- [6] 반도체 칩의 제조 공정의 공정편차를 이용하여 물리적으로 복제가 불가능한 PUF를 구현함으로써, 구조가 간단하면서도 무작위적 디지털 값을 생성하고, 생성된 값은 시불변성이 보장되도록 동결(Freezing)하는 장치 및 방법을 제공한다.
- [7] 노이즈 및 환경 변화에도 강하고 시불변성이 보장되는 신뢰할 수 있는 무작위의 디지털 값을 생성할 수 있는 디지털 값 생성 장치 및 방법을 제공한다.

과제 해결 수단

- [8] 디지털 값 생성 장치는 반도체의 공정 편차를 이용하여 무작위의 디지털 값을 생성하는 디지털 값 생성부 및 상기 디지털 값 생성부에 연결되고 상기 생성된 디지털 값에 대응하여 제1 상태 또는 제2 상태 중 어느 한 상태로 고정되어 상기 디지털 값을 동결하는 디지털 값 동결부를 포함하여 생성된 디지털 값을 동결할

수 있다.

- [9] 일측에 따르면, 상기 디지털 값 생성부는 물리적으로 복제가 불가능한 PUF(Physically Unclonable Function)를 포함할 수 있다.
- [10] 다른 측면에 따르면, 상기 디지털 값 생성부는 제1 인버터의 출력 단자 및 제2 인버터의 입력 단자는 제1 노드에 연결되고 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자는 제2 노드에 연결되어, 상기 제1 노드 및 상기 제2 노드가 단락되는 경우 상기 제1 노드 및 상기 제2 노드 중 적어도 하나의 논리적 레벨을 이용하여 상기 디지털 값을 생성할 수 있다.
- [11] 또 다른 측면에 따르면, 상기 디지털 값 생성부는 두 개의 입력 노드 간의 전위차를 증폭시키는 차동 증폭기를 포함하고, 상기 두 개의 입력 노드가 단락되는 경우의 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성할 수 있다.
- [12] 또 다른 측면에 따르면, 상기 디지털 값 생성부는 두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR 래치(Set-Reset latch)를 포함하고, 상기 두 개의 입력 노드가 단락되는 경우 상기 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성할 수 있다.
- [13] 또 다른 측면에 따르면, 상기 디지털 값 동결부는 상기 디지털 값 생성부의 초기 구동 시 생성된 상기 디지털 값에 대응하여 과전류를 받아 끊어지거나 끊어지지 않음으로써 상기 디지털 값을 동결하는 퓨즈(fuse)일 수 있다.
- [14] 또 다른 측면에 따르면, 상기 제1 상태는 상기 퓨즈가 끊어진 상태이고, 상기 제2 상태는 상기 퓨즈가 끊어지지 않은 상태일 수 있다.
- [15] 또 다른 측면에 따르면, 상기 디지털 값 동결부는 상기 디지털 값 생성부의 초기 구동 시 생성된 상기 디지털 값을 저장하는 비휘발성 메모리 소자일 수 있다.
- [16] 또 다른 측면에 따르면, 상기 비휘발성 메모리 소자는 EEPROM(Electrically Erasable Programmable Read-Only Memory), 플래시 메모리(Flash Memory) 중 어느 하나 일 수 있다.
- [17] 또 다른 측면에 따르면, 상기 제1 상태는 상기 비휘발성 메모리 소자에 디지털 값 '0'이 저장된 상태이고, 상기 제2 상태는 상기 비휘발성 메모리 소자에 디지털 값 '1'이 저장된 상태일 수 있다.
- [18] 또 다른 측면에 따르면, 상기 디지털 값 동결부는 상기 디지털 값 생성부의 내부에 위치할 수 있다.
- [19] 한편, 디지털 값 생성 방법은 디지털 값 생성 장치가 반도체 공정 편차를 이용하여 디지털 값을 생성하는 방법에 있어서, 상기 장치의 디지털 값 생성부가 무작위의 상기 디지털 값을 생성하는 단계 및 상기 생성부에 연결되는 상기 장치의 디지털 값 동결부가 상기 생성된 무작위의 디지털 값을 동결하는 단계를 포함할 수 있다.
- [20] 다른 측면에 따르면, 상기 디지털 값 생성부는 물리적으로 복제가 불가능한 PUF(Physically Unclonable Function)를 포함할 수 있다.

- [21] 또 다른 측면에 따르면, 상기 디지털 값을 생성하는 단계는 제1 인버터의 출력 단자 및 제2 인버터의 입력 단자를 제1 노드에 연결하고 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자를 제2 노드에 연결하여, 상기 제1 노드 및 상기 제2 노드가 단락되는 경우 상기 제1 노드 및 상기 제2 노드 중 적어도 하나의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 단계일 수 있다.
- [22] 또 다른 측면에 따르면, 상기 디지털 값을 생성하는 단계는 두 개의 입력 노드 간의 전위차를 증폭시키는 차동 증폭기를 기초로, 상기 두 개의 입력 노드가 단락되는 경우의 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 단계일 수 있다.
- [23] 또 다른 측면에 따르면, 상기 디지털 값을 생성하는 단계는 두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR 래치(Set-Reset latch)를 기초로, 상기 두 개의 입력 노드가 단락되는 경우 상기 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 일 수 있다.
- [24] 또 다른 측면에 따르면, 상기 디지털 값을 동결하는 단계는 상기 회로의 초기 구동 시 생성된 상기 디지털 값에 대응하여 퓨즈(fuse)에 과전류를 흘림으로써, 상기 퓨즈가 끊어지게 하여 상기 디지털 값을 동결하는 단계일 수 있다.
- [25] 또 다른 측면에 따르면, 상기 디지털 값을 동결하는 단계는 상기 회로의 초기 구동 시 생성된 상기 디지털 값을 비휘발성 메모리 소자에 저장하는 단계일 수 있다.
- [26] 또 다른 측면에 따르면, 상기 비휘발성 메모리 소자는 EEPROM(Electrically Erasable Programmable Read-Only Memory), Flash ROM 중 어느 하나 일 수 있다.

발명의 효과

- [27] 반도체 칩의 제조 공정의 공정편차를 이용하여 디지털 값을 생성하는 회로의 구조가 간단하면서도 시불변성이 만족됨에 따라 상기 디지털 값의 신뢰성이 높아지게 된다.
- [28] 또한, 동일한 설계 하에서 다른 회로를 만들더라도 동일한 식별 키가 생성되지 않음으로써 회로의 물리적인 복제가 불가능하므로, 높은 보안성을 보장한다.

도면의 간단한 설명

- [29] 도 1은 본 발명의 일실시예에 있어서, 디지털 값 생성 장치를 도시한 블록도이다.
- [30] 도 2는 본 발명의 일실시예에 있어서, 디지털 값 생성 장치의 구성을 나타내는 회로도이다.
- [31] 도 3은 본 발명의 일실시예에 있어서, 디지털 값 생성 장치에 전압이 인가됨에 따른 타이밍도이다.
- [32] 도 4 내지 도 9는 본 발명의 다양한 실시예에 있어서, 디지털 값 생성 장치의 구성을 설명하기 위한 회로도이다.
- [33] 도 10은 본 발명의 일실시예에 있어서, 디지털 값 생성 방법을 나타내는

순서도이다.

발명의 실시를 위한 형태

- [34] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [35] 도 1은 본 발명의 일실시예에 있어서, 디지털 값 생성 장치를 도시한 블록도이다. 본 발명의 일실시예에 따른 디지털 값 생성 장치는 디지털 값 생성부(110) 및 디지털 값 동결부(120)를 포함한다.
- [36] 상기 디지털 값 생성부(110)는 상기 디지털 값 생성부(110)에 인가되는 전압(vdd)을 기초로 무작위의 디지털 값을 생성한다.
- [37] 반도체 공정에서 공정편차는 다양한 이유에 의해 발생한다. 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.
- [38] 따라서 일반적으로는 공정편차가 작은 반도체 제조 공정이 우수한 것으로 인식되어 반도체 공정의 기술분야에서는 공정 편차를 줄이기 위한 다양한 시도를 하고 있다. 그러나, 본 발명에 따른 디지털 값 생성부(110)는 오히려 이러한 반도체 공정의 공정 편차를 이용하여, 무작위로 결정되며 한 번 결정되면 변경되지 않는 디지털 값을 생성한다.
- [39] 상기 디지털 값 동결부(120)는 상기 디지털 값 생성부(110)에 연결되어 상기 디지털 값 생성부(110)에서 생성된 디지털 값에 대응하여 제1 상태 또는 제2 상태 중 어느 한 상태로 고정되어 상기 디지털 값을 동결(freezing)한다.
- [40] 상기 디지털 값 생성부(110)에서 생성된 디지털 값은 상기 공정 편차에 의하여 무작위성이 보장되기는 하지만, 노이즈, 차동 노화(differential aging) 등으로 인하여 시간의 경과에 따라 상기 디지털 값이 변동될 수 있다. 따라서, 상기 디지털 값 동결부(120)는 노이즈, 환경 변화 등에도 상기 디지털 값이 변화되지 않도록 상기 디지털 값을 동결함으로써 시불변성이 보장되는 디지털 값이 생성되도록 한다.
- [41] 이하, 도 2를 참조하여 본 발명의 일실시예에 있어서 디지털 값 생성 장치의 구성을 보다 상세히 설명하도록 한다.
- [42] 도 2를 참조하면, 상술한 바와 같이, 디지털 값 생성부(210)는 물리적으로 복제가 불가능한 디지털 값을 생성하는 것으로서, 일 예로 PUF(Physically Unclonable Function)를 포함할 수 있다.
- [43] 도 2에는 일실시예로서, 디지털 값 생성부(210)가 SR 래치(Set-Reset latch)를 포함하는 PUF 회로를 포함함이 도시되어 있다. 그리고, 디지털 값 동결부(220)가 제1 퓨즈(fuse) 및 제2 퓨즈를 포함한 실시예가 예시적으로 도시되어 있다.
- [44] 디지털 값 생성 장치의 초기 구동 시 디지털 값 생성부(210)에 포함된 SR 래치에 전압(vdd)이 인가되면 상기 SR 래치의 공정 편차에 의해 무작위의 디지털

값이 생성된다. 이 때, 생성된 무작위 디지털 값에 의해 과전류를 상기 과전류가 디지털 값 동결부(220)로 흘리게 된다.

- [45] 이에 따라, 상기 과전류를 받은 상기 디지털 값 동결부(220)에 포함된 퓨즈는 끊어지게 되고, 따라서 상기 디지털 값 동결부(220)를 통하여 출력되는 디지털 값을 영구적으로 동결할 수 있다. 즉, 이러한 동결 후에는, 퓨즈가 끊어졌는지의 여부에 따라 회로의 구성이 영구히 변경되므로, 초기 구동에 의해 상기 회로가 변경된 후에는 디지털 값이 변경되지 않으며, 이러한 과정을 동결(freezing)이라 할 수 있다.
- [46] 한 번 끊어진 퓨즈가 다시 연결되지는 않기 때문에, 이러한 실시예에 의하면, 종래의 공정 편차를 이용한 PUF 회로에서 디지털 값을 생성하는 경우 문제되던, 시불변성의 보장이 되지 않던 문제점이 해결된다.
- [47] 이하 도 3을 참조하여 본 발명의 일실시예에 있어서 디지털 값 생성 장치에 전압이 인가됨에 따라 출력되는 디지털 값을 나타내는 타이밍도이다.
- [48] 도 3은 일 예로서 상기 과전류가 제2 퓨즈를 통하여 흐름에 따라 상기 제2 퓨즈가 끊어진 상태가 되었을 경우를 나타낸다.
- [49] 도 2 및 도 3을 참조하면, 디지털 값 생성 장치가 초기 구동을 수행하여 상기 디지털 값 생성부(210)에 전압이 인가되면, 상기 디지털 값 동결부(220)의 상기 제2 퓨즈가 끊어짐에 따라 제 1 출력 값은 언제나 0으로 생성되고, 제 2 출력 값은 언제나 1로 생성된다.
- [50] 따라서, 상기 디지털 값 동결부(220)는 상기 퓨즈의 상태 즉, 상기 퓨즈가 끊어진 제1 상태 및 상기 퓨즈가 끊어지지 않은 제2 상태에 따라 상기 디지털 값 생성부(210)에서 생성된 무작위의 디지털 값을 동결할 수 있다.
- [51] 도 4 내지 도 9는 본 발명의 다양한 실시예에 있어서, 디지털 값 생성 장치의 구성을 설명하기 위한 회로도이다. 이하에서는 본 발명의 다양한 실시예를 각각의 도면을 참조하여 상세히 설명하기로 한다.
- [52] 먼저 도 4를 참조하면 디지털 값 생성부는 도 4a에 도시된 바와 같이 두 개의 입력 노드 간의 전위차를 증폭시키는 차동 증폭기(differential amplifier)를 포함하도록 구현되어 상기 두개의 입력 노드가 단락(short)되는 경우 출력 노드의 논리적 레벨을 이용하여 디지털 값을 생성할 수 있다.
- [53] 디지털 값 동결부(400)는 두 개의 퓨즈를 포함하도록 구현될 수 있는데, 이 때 상기 퓨즈는 도 2에서와 같이 상기 디지털 값 생성부와 그라운드(ground) 사이에 연결될 수도 있지만, 도 4b 내지 도 4d와 같이 디지털 값 생성부 내에 연결될 수 있다.
- [54] 이 경우, 상기 디지털 값 결정부의 퓨즈는 각각의 입력 노드 중 상호 대응되는 위치에 연결될 수 있는데, 도 4b에 도시된 바와 같이 입력 단자와 출력 단자 사이에 연결될 수 있고, 도 4c에 도시된 바와 같이 전원과 출력 단자 사이에 병렬로 연결될 수도 있으며, 도 4d에 도시된 바와 같이 입력 단자와 출력 단자 사이에 병렬로 연결 될 수도 있다.

- [55] 이러한 도식된 예시적 퓨즈들의 구성에 따르면, 최초 동작시 발생하는 디지털 값에 의하여 선택적으로 어느 한 쪽의 퓨즈에 과전류가 흐르게 되어, 최초 이후의 동작부터는 출력값의 우위가 고정되게 된다.
- [56] 예를 들면 도 4(b)의 회로에서 최초 동작시 OUT이 OUTb(OUT의 부신호)보다 높은 전압을 출력할 경우, 이를 비교기를 통해 비교하여 디지털 값으로 변환하고 논리회로와 과전류 부하회로를 거쳐 오른쪽 퓨즈에만 과전류를 흘려서 끊는다.
- [57] 그러면 이후 동작부터는 OUT의 출력 전압은 항상 vdd이며, OUTb(OUT의 부신호)는 항상 vdd보다 낮은 출력 전압을 가지게 되므로, 이로서 출력 전압의 우열이 고정되어, 이를 변환한 디지털 값 또한 고정된다.
- [58] 다음으로 도 5를 참조하면 디지털 값 생성부는 도 5a에 도식된 바와 같이 듀얼 인버터(dual inverter)를 포함하여 구현될 수 있다.
- [59] 이 경우, 제1 인버터의 출력 단자 및 제2 인버터의 입력 단자는 제1 노드에 연결되고 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자는 제2 노드에 연결되어 상기 제1 노드 및 상기 제2 노드가 단락되는 경우 상기 제1 노드 및 상기 제2 노드 중 적어도 하나의 논리적 레벨을 이용하여 상기 디지털 값을 생성할 수 있다.
- [60] 이 때, 상기 디지털 값 동결부의 퓨즈도 도 5b에서와 같이 상기 디지털 값 생성부와 그라운드 사이에 연결될 수도 있지만, 도 5c에서와 같이 전원과 출력 단자 사이에 연결될 수 있고, 도 5d에서와 같이 출력 단자와 그라운드 사이에 병렬로 연결될 수 있으며, 도 5e에서와 같이 전원과 출력 단자 사이에 병렬로 연결될 수도 있다.
- [61] 다음으로 도 6를 참조하면 디지털 값 생성부는 도 6a에 도식된 바와 같이 두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR 래치를 포함하여 구현되어, 상기 두 개의 입력 노드가 단락되는 경우 상기 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성할 수 있다.
- [62] 이 때, 상기 디지털 값 동결부의 퓨즈도 도 6b 내지 도 6d에서와 같이 상기 디지털 값 생성부와 그라운드 사이에 연결될 수도 있다.
- [63] 한편, 도 7에 도식된 바와 같이, 본 발명의 디지털 값 동결부는 상기 디지털 값 생성부의 초기 구동 시 생성된 상기 디지털 값을 저장하는 EEPROM(Electrically Erasable Programmable Read-Only Memory), 플래시 메모리(Flash Memory) 등의 비휘발성 메모리 소자로 구현될 수 있다.
- [64] 이하의 실시예에서는 상기 디지털 값 동결부로서 비휘발성 메모리 소자를 이용하는 구성을 설명하고 있으나, 상기 디지털 값 동결부는 상기 비휘발성 메모리 소자를 포함하여 구성되는 것에 한정되는 것이 아니라 모든 부동 게이트(floating gate) 소자를 활용하여 구성될 수 있다.
- [65] 상기 디지털 값 동결부가 비휘발성 메모리 소자를 포함하도록 구현될 경우에도 상술한 바와 같은 퓨즈를 포함하도록 구현되는 경우와 마찬가지로, 상기 디지털 값 생성부에 인가된 전원에 의해 발생된 전하가 충전되는 상태 즉, 상기

비휘발성 메모리 소자에 디지털 값 '0'이 저장된 제1 상태 및 상기 비휘발성 메모리 소자에 디지털 값 '1'이 저장된 제2 상태에 따라 생성되는 디지털 값을 동결할 수 있다.

- [66] 이 경우, 도 7a에서와 같이 디지털 값 생성부가 입력 노드 간의 전위차를 증폭시키는 차동 증폭기를 포함하도록 구현하고, 상기 퓨즈가 연결되는 위치에 대응되는 위치에 상기 디지털 값 동결부(700)를 연결함으로써 상기 비휘발성 메모리 소자에 디지털 값이 저장되는 상태를 이용하여 생성된 디지털 값을 동결할 수 있다.
- [67] 구체적으로 보면 회로가 동작할 때 ON 전압을 flash memory 소자의 gate에 인가하게 되는데, 최초 동작에서 출력 전압의 우열에 따라 flash memory 소자의 floating gate를 음전하로 충전시켜준다.
- [68] 도 7b의 회로를 예로 들면 OUT 전압이 높다면 오른쪽의 flash memory 소자를, OUTb 전압이 높다면 왼쪽의 flash memory 소자의 floating gate를 음전하로 충전한다. 만약 OUT의 전압이 높아 오른쪽 flash memory 소자의 floating gate를 음전하로 충전했다면, 이후 동작에서 flash memory 소자의 gate에 ON 전압을 입력해도, 오른쪽 flash memory 소자는 켜지지 않기 때문에, OUT 출력 전압은 vdd가 되고 OUTb 출력 전압은 그보다 낮은 값이 되어 최초 동작의 전압 우열이 그대로 고정되는 효과가 있다.
- [69] 이 때, 도 7b와 마찬가지로 상기 비휘발성 메모리 소자는 입력 단자와 출력 단자 사이에 연결될 수 있고, 도 7c에 도시된 바와 같이 전원과 출력 단자 사이에 병렬로 연결될 수도 있으며, 도 7d에 도시된 바와 같이 입력 단자와 출력 단자 사이에 병렬로 연결될 수도 있다.
- [70] 다음으로 도 8를 참조하면 디지털 값 생성부는 도 8a에 도시된 바와 같이 듀얼 인버터(dual inverter)를 포함하여 구현되고, 디지털 값 동결부는 비휘발성 메모리 소자를 포함하여 구현될 수 있다.
- [71] 이 경우, 상기 디지털 값 동결부의 비휘발성 메모리 소자는 도 8b에서와 같이 상기 디지털 값 생성부와 그라운드 사이에 연결될 수도 있지만, 도 8c에서와 같이 전원과 출력 단자 사이에 연결될 수 있고, 도 8d에서와 같이 출력 단자와 그라운드 사이에 병렬로 연결될 수 있으며, 도 8e에서와 같이 전원과 출력 단자 사이에 병렬로 연결될 수도 있다.
- [72] 다음으로 도 9를 참조하면 디지털 값 생성부는 도 9a에 도시된 바와 같이 두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR 래치를 포함하여 구현되고, 상기 디지털 값 생성부는 비휘발성 메모리 소자를 포함하여 구현될 수 있다.
- [73] 이 경우에도, 상기 디지털 값 동결부의 비휘발성 메모리 소자는 도 9b 내지 도 9d에서와 같이 상기 디지털 값 생성부와 그라운드 사이에 다양한 형태로 연결될 수 있다.
- [74] 이와 같은 구성으로 인하여 본 발명에 따른 디지털 값 생성 장치는 동일한 설계 하에서 다른 회로를 만들더라도 동일한 식별 키가 생성되지 않음으로써 회로의

물리적인 복제가 불가능하므로, 식별 키의 무작위성과 시불변성이 만족되는 한편, 듀얼 인버터, 차동 증폭기, SR 래치, EEPROM, 플래시 메모리 등의 동일한 소자를 복수개 이용하여 식별 키를 생성하기 때문에 물리적으로 복사가 불가능하므로 높은 보안성이 보장된다.

- [75] 이하 도 10을 참조하여 본 발명의 일실시예에 있어서 디지털 값 생성 장치를 이용하여 디지털 값을 생성하는 방법을 설명한다.
- [76] 먼저 디지털 값 생성 장치의 초기 동작 시 디지털 값 생성부에 전압이 인가되면(S1010), 상기 디지털 값 생성부에 포함된 PUF에서 상기 PUF의 공정 편차로 인한 무작위의 디지털 값이 생성된다(S1020).
- [77] 그러면, 상기 디지털 값 생성 장치의 디지털 값 동결부는 상기 전압에 의한 전류를 이용하여 상기 디지털 값 동결부에 포함된 퓨즈가 끊어지게 하거나, 상기 디지털 값 동결부에 포함된 비휘발성 메모리 소자에 디지털 값을 저장함으로써 상기 디지털 값 생성 장치에서 생성되는 디지털 값이 영구적으로 동결되게 한다(S1030).
- [78] 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.
- [79] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

청구범위

- [청구항 1] 반도체의 공정 편차를 이용하여 무작위의 디지털 값을 생성하는 디지털 값 생성부; 및
상기 디지털 값 생성부에 연결되고 상기 생성된 디지털 값에 대응하여 제1 상태 또는 제2 상태 중 어느 한 상태로 고정되어 상기 디지털 값을 동결하는 디지털 값 동결부를 포함하는 디지털 값 생성 장치.
- [청구항 2] 제1항에 있어서,
상기 디지털 값 생성부는
PUF(Physically Unclonable Function)를 포함하는, 디지털 값 생성 장치.
- [청구항 3] 제2항에 있어서,
상기 디지털 값 생성부는
제1 인버터의 출력 단자 및 제2 인버터의 입력 단자는 제1 노드에 연결되고 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력 단자는 제2 노드에 연결되어, 상기 제1 노드 및 상기 제2 노드가 단락되는 경우 상기 제1 노드 및 상기 제2 노드 중 적어도 하나의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는, 디지털 값 생성 장치.
- [청구항 4] 제2항에 있어서,
상기 디지털 값 생성부는
두 개의 입력 노드 간의 전위차를 증폭시키는 차동 증폭기를 포함하고, 상기 두 개의 입력 노드가 단락되는 경우의 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는, 디지털 값 생성 장치.
- [청구항 5] 제2항에 있어서,
상기 디지털 값 생성부는
두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR 래치(Set-Reset latch)를 포함하고, 상기 두 개의 입력 노드가 단락되는 경우 상기 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는, 디지털 값 생성 장치.
- [청구항 6] 제1항에 있어서,
상기 디지털 값 동결부는
상기 디지털 값 생성부의 초기 구동 시 생성된 상기 디지털 값에 대응하여 과전류를 받아 끊어지거나 끊어지지 않음으로써 상기 디지털 값을 동결하는 퓨즈(fuse)인, 디지털 값 생성 장치.
- [청구항 7] 제6항에 있어서,

- 상기 제1 상태는
상기 퓨즈가 끊어진 상태이고,
상기 제2 상태는
상기 퓨즈가 끊어지지 않은 상태인, 디지털 값 생성 장치.
- [청구항 8] 제1항에 있어서,
상기 디지털 값 동결부는
상기 디지털 값 생성부의 초기 구동 시 생성된 상기 디지털 값을
저장하는 비휘발성 메모리 소자인, 디지털 값 생성 장치.
- [청구항 9] 제8항에 있어서,
상기 비휘발성 메모리 소자는
EEPROM(Electrically Erasable Programmable Read-Only Memory),
플래시 메모리(Flash Memory) 중 어느 하나 인, 디지털 값 생성
장치.
- [청구항 10] 제8항에 있어서,
상기 제1 상태는
상기 비휘발성 메모리 소자에 디지털 값 '0'이 저장된 상태이고,
상기 제2 상태는
상기 비휘발성 메모리 소자에 디지털 값 '1'이 저장된 상태인,
디지털 값 생성 장치.
- [청구항 11] 제1항에 있어서,
상기 디지털 값 동결부는
상기 디지털 값 생성부의 내부에 위치하는, 디지털 값 생성 장치.
- [청구항 12] 디지털 값 생성 장치가 반도체 공정 편차를 이용하여 디지털 값을
생성하는 방법에 있어서,
상기 장치의 디지털 값 생성부가 무작위의 상기 디지털 값을
생성하는 단계; 및
상기 생성부에 연결되는 상기 장치의 디지털 값 동결부가 상기
생성된 무작위의 디지털 값을 동결하는 단계
를 포함하는 디지털 값 생성 방법.
- [청구항 13] 제12항에 있어서,
상기 디지털 값 생성부는
PUF(Physically Unclonable Function)를 포함하는, 디지털 값 생성
방법.
- [청구항 14] 제13항에 있어서,
상기 디지털 값을 생성하는 단계는
제1 인버터의 출력 단자 및 제2 인버터의 입력 단자를 제1 노드에
연결하고 상기 제1 인버터의 입력 단자 및 상기 제2 인버터의 출력
단자를 제2 노드에 연결하여, 상기 제1 노드 및 상기 제2 노드가

단락되는 경우 상기 제1 노드 및 상기 제2 노드 중 적어도 하나의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 단계인, 디지털 값 생성 방법.

[청구항 15]

제13항에 있어서,

상기 디지털 값을 생성하는 단계는

두 개의 입력 노드 간의 전위차를 증폭시키는 차동 증폭기를 기초로, 상기 두 개의 입력 노드가 단락되는 경우의 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 단계인, 디지털 값 생성 방법.

[청구항 16]

제13항에 있어서,

상기 디지털 값을 생성하는 단계는

두 개의 입력 노드 및 두 개의 출력 노드를 가지는 SR

래치(Set-Reset latch)를 기초로, 상기 두 개의 입력 노드가 단락되는 경우 상기 출력 노드의 논리적 레벨을 이용하여 상기 디지털 값을 생성하는 인, 디지털 값 생성 방법.

[청구항 17]

제12항에 있어서,

상기 디지털 값을 동결하는 단계는

상기 회로의 초기 구동 시 생성된 상기 디지털 값에 대응하여 퓨즈(fuse)에 과전류를 흘림으로써, 상기 퓨즈가 끊어지게 하여 상기 디지털 값을 동결하는 단계인, 디지털 값 생성 방법.

[청구항 18]

제12항에 있어서,

상기 디지털 값을 동결하는 단계는

상기 회로의 초기 구동 시 생성된 상기 디지털 값을 비휘발성 메모리 소자에 저장하는 단계인, 디지털 값 생성 방법.

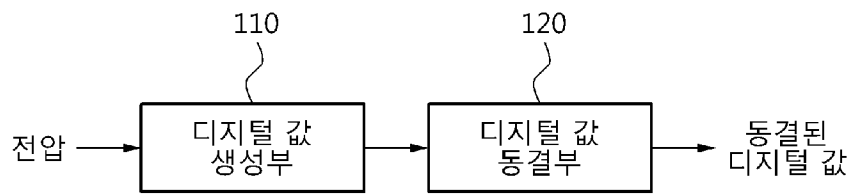
[청구항 19]

제18항에 있어서,

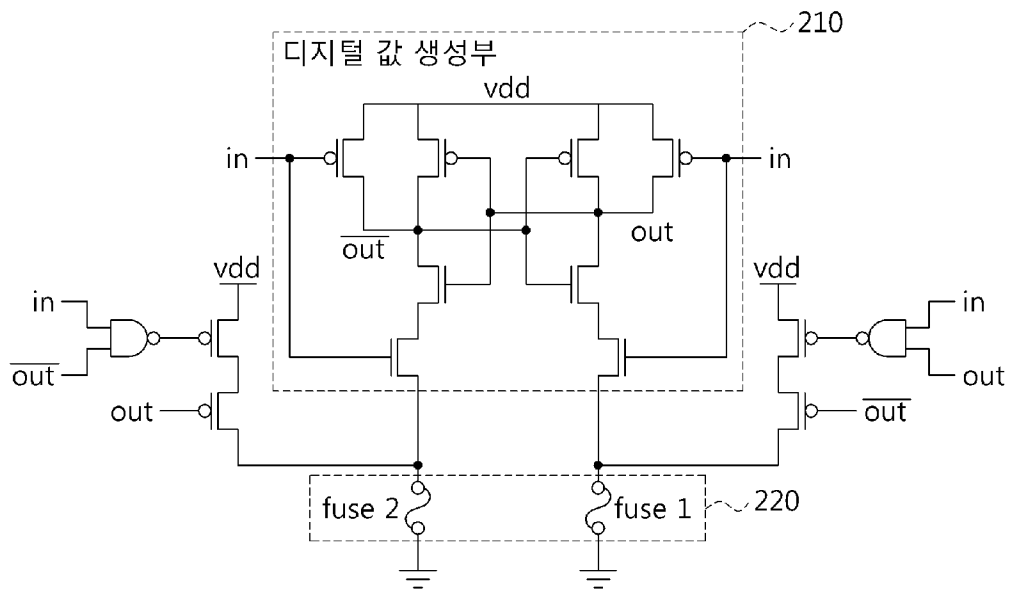
상기 비휘발성 메모리 소자는

EEPROM(Electrically Erasable Programmable Read-Only Memory), Flash ROM 중 어느 하나 인, 디지털 값 생성 방법.

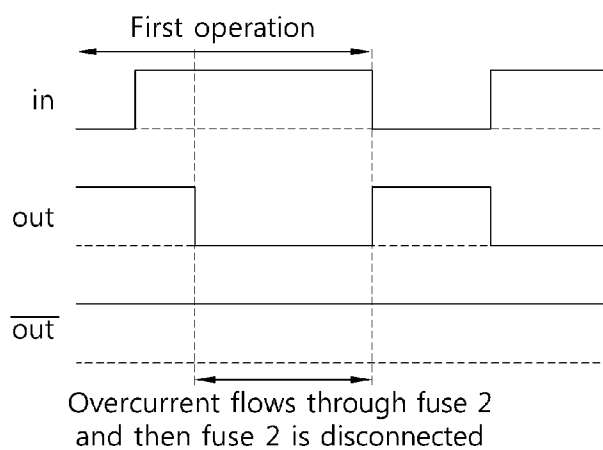
[Fig. 1]



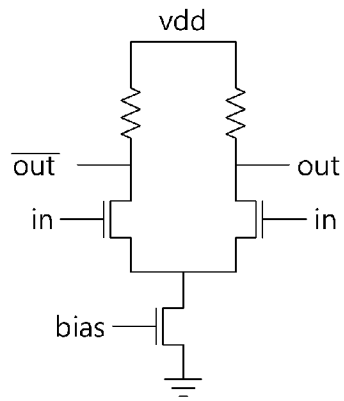
[Fig. 2]



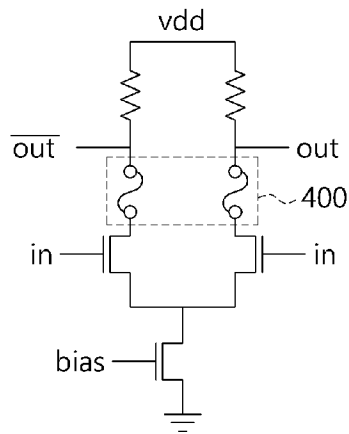
[Fig. 3]



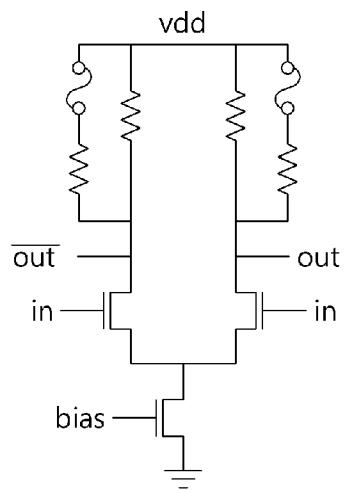
[Fig. 4]



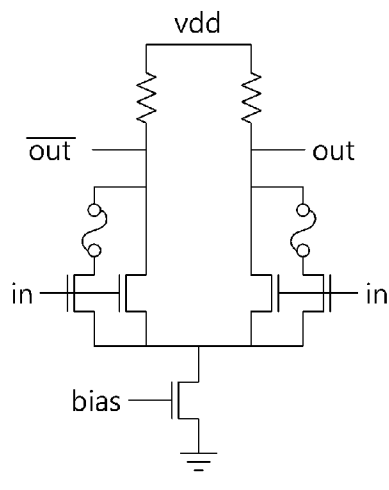
(a)



(b)

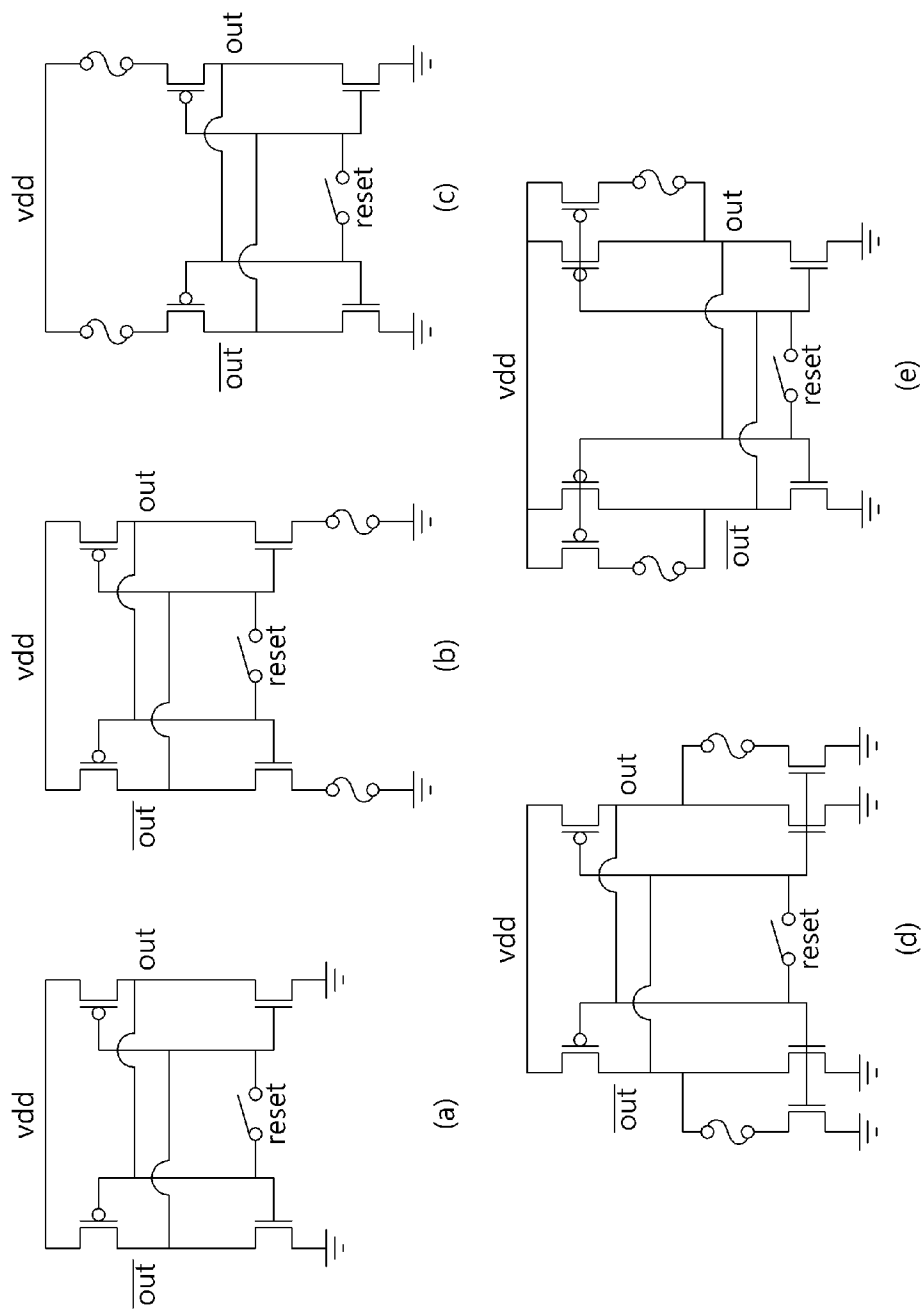


(c)

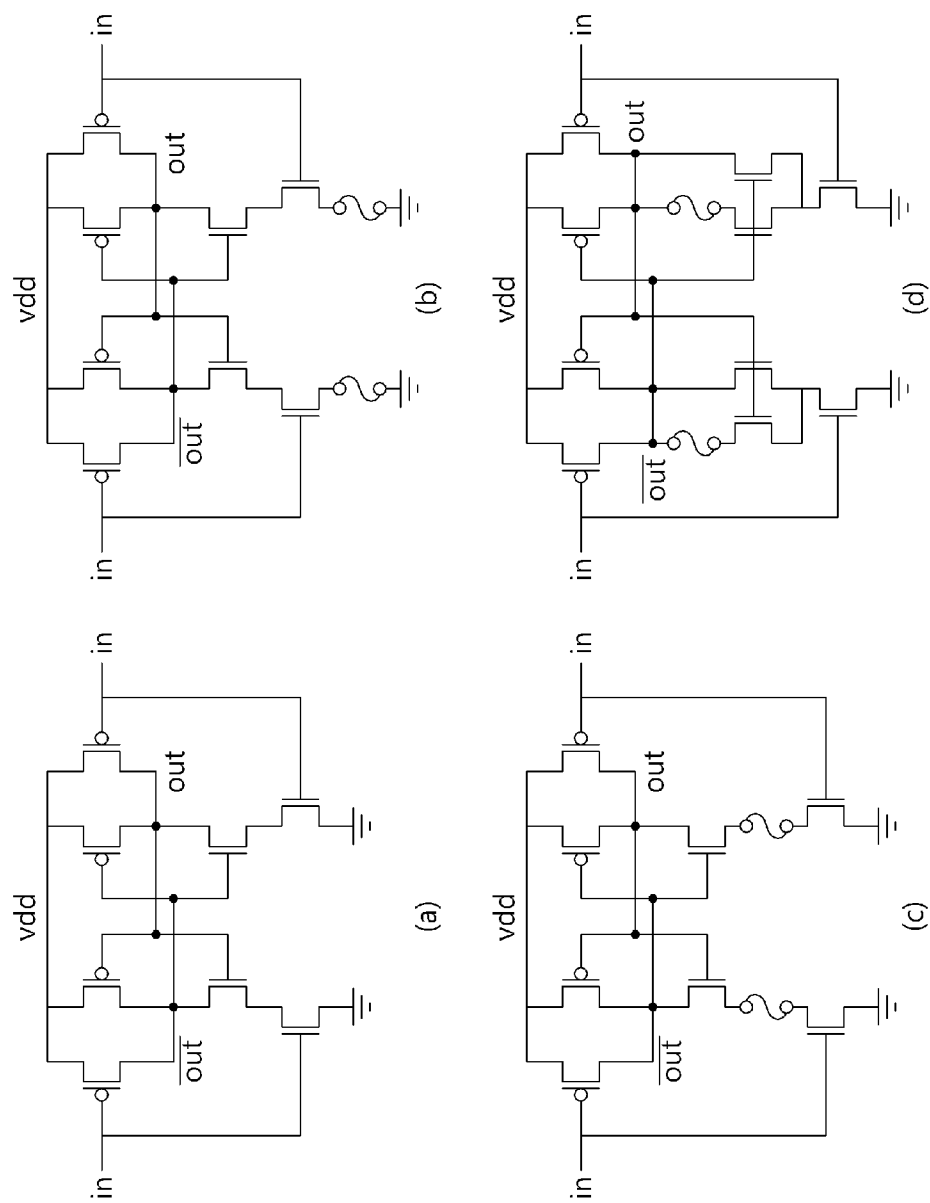


(d)

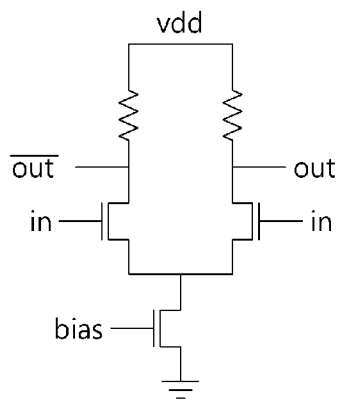
[Fig. 5]



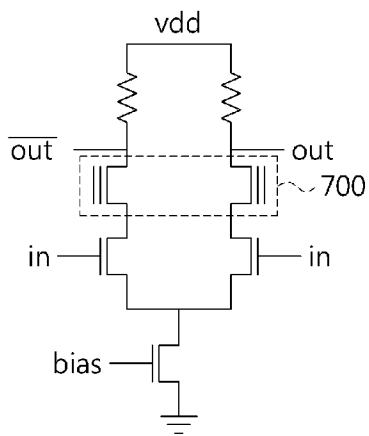
[Fig. 6]



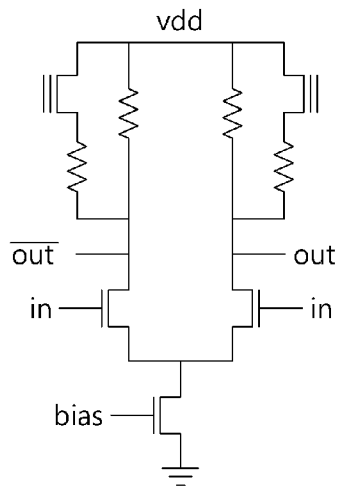
[Fig. 7]



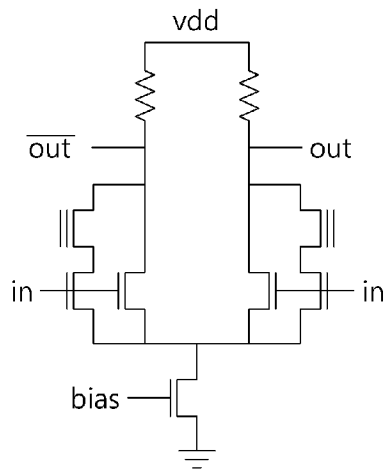
(a)



(b)

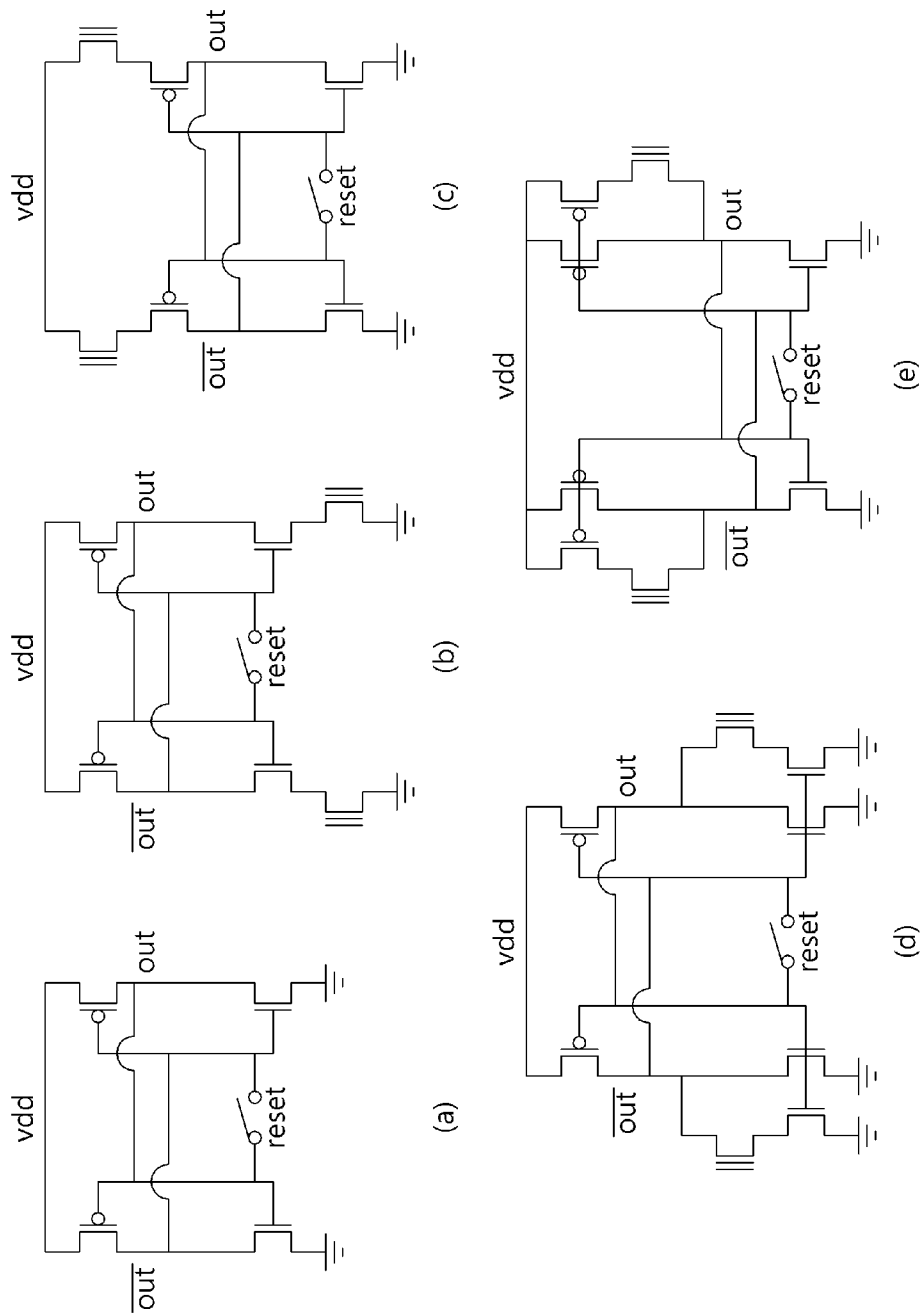


(c)

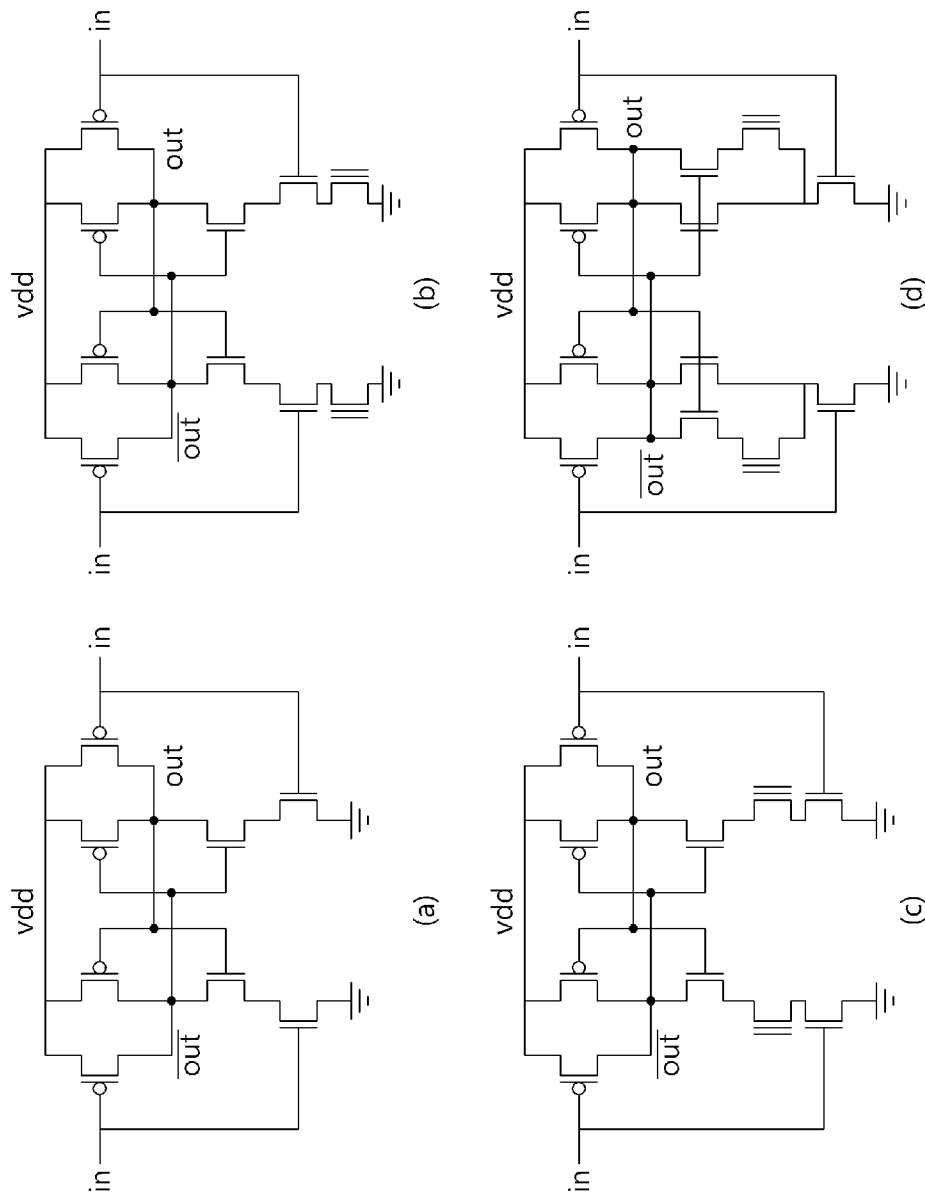


(d)

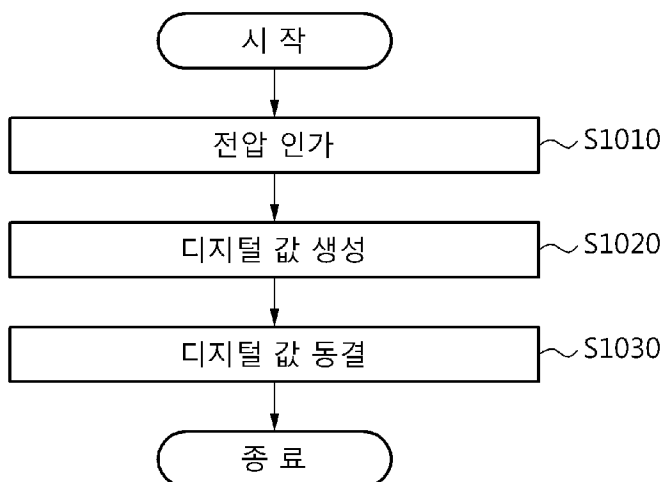
[Fig. 8]



[Fig. 9]



[Fig. 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2011/002219**A. CLASSIFICATION OF SUBJECT MATTER****G06F 7/58(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)

G06F 7/58; H01L 23/544; G06K 17/00; H04B 5/02; H01L 21/66; H01L 21/00

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: process variation, PUF

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, paragraphs [0019]-[0092] and figures 1-6	1-19
A	WO 2010-123185 A1 (IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY) et al.) 28 October 2010 See abstract, paragraphs [0063]-[0195] and figures 1-14	1-19
A	WO 2003-090259 A2 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY et al.) 30 October 2003 See abstract, page 9, line 3 - page 10, line 25, page 55, line 4 - page 56, line 19 and figures 1, 50A-50B	1-19
A	US 2006-0063286 A1 (WILLIAM BIDERMANN et al.) 23 March 2006 See abstract, paragraphs [0014]-[0048] and figures 1-5	1-19

☐ 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

28 NOVEMBER 2011 (28.11.2011)

Date of mailing of the international search report

28 NOVEMBER 2011 (28.11.2011)

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/KR2011/002219

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0068987 A	29.06.2009	NONE	
WO 2010-123185 A1	28.10.2010	KR 10-0926214 B1 KR 10-2010-0117006 A	09.11.2009 02.11.2010
WO 03-090259 A2	30.10.2003	AU 2003-221927 A1 AU 2003-221927 A8 CA 2482635 A1 EP 1497863 A2 EP 2302555 A2 EP 2302555 A3 EP 2320344 A2 EP 2320344 A3 JP 04-733924 B2 JP 2005-523481 A JP 2005-523481 T JP 2011-123909 A KR 10-2004-0102110 A US 2003-0204743 A1 US 2006-0221686 A1 US 2006-0271792 A1 US 2006-0271793 A1 US 2007-0183194 A1 US 2009-0222672 A1 US 7681103 B2 US 7757083 B2 US 7818569 B2 US 7840803 B2 US 7904731 B2 WO 03-090259 A2 WO 03-090259 A3	03.11.2003 03.11.2003 30.10.2003 19.01.2005 30.03.2011 10.08.2011 11.05.2011 06.07.2011 28.04.2011 04.08.2005 04.08.2005 23.06.2011 03.12.2004 30.10.2003 05.10.2006 30.11.2006 30.11.2006 09.08.2007 03.09.2009 16.03.2010 13.07.2010 19.10.2010 23.11.2010 08.03.2011 30.10.2003 30.10.2003
US 2006-0063286 A1	23.03.2006	US 7291507 B2	06.11.2007

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 7/58(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 7/58; H01L 23/544; G06K 17/00; H04B 5/02; H01L 21/66; H01L 21/00

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: 공정편차, PUF

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0068987 A (주식회사 시큐트론) 2009.06.29 요약, 단락 [0019]-[0092] 및 도면 1-6 참조	1-19
A	WO 2010-123185 A1 (IUCF-HYU (INDUSTRY-UNIVERSITY COOPERATION FOUNDATION HANYANG UNIVERSITY) 외 3명) 2010.10.28 요약, 단락 [63]-[195] 및 도면 1-14 참조	1-19
A	WO 2003-090259 A2 (MASSACHUSETTS INSTITUTE OF TECHNOLOGY 외 4명) 2003.10.30 요약, 페이지 9, 라인 3 - 페이지 10, 라인 25, 페이지 55, 라인 4 - 페이지 56, 라인 19 및 도면 1, 50A-50B 참조	1-19
A	US 2006-0063286 A1 (WILLIAM BIDERMAN 외 1명) 2006.03.23 요약, 단락 [0014]-[0048] 및 도면 1-5 참조	1-19

☐ 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

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2011년 11월 28일 (28.11.2011)

국제조사보고서 발송일

2011년 11월 28일 (28.11.2011)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
정부대전청사
팩스 번호 82-42-472-7140

심사관

최정권

전화번호 82-42-481-8507



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0068987 A	2009.06.29	없음	
WO 2010-123185 A1	2010.10.28	KR 10-0926214 B1 KR 10-2010-0117006 A	2009.11.09 2010.11.02
WO 03-090259 A2	2003.10.30	AU 2003-221927 A1 AU 2003-221927 A8 CA 2482635 A1 EP 1497863 A2 EP 2302555 A2 EP 2302555 A3 EP 2320344 A2 EP 2320344 A3 JP 04-733924 B2 JP 2005-523481 A JP 2005-523481 T JP 2011-123909 A KR 10-2004-0102110 A US 2003-0204743 A1 US 2006-0221686 A1 US 2006-0271792 A1 US 2006-0271793 A1 US 2007-0183194 A1 US 2009-0222672 A1 US 7681103 B2 US 7757083 B2 US 7818569 B2 US 7840803 B2 US 7904731 B2 WO 03-090259 A2 WO 03-090259 A3	2003.11.03 2003.11.03 2003.10.30 2005.01.19 2011.03.30 2011.08.10 2011.05.11 2011.07.06 2011.04.28 2005.08.04 2005.08.04 2011.06.23 2004.12.03 2003.10.30 2006.10.05 2006.11.30 2006.11.30 2007.08.09 2009.09.03 2010.03.16 2010.07.13 2010.10.19 2010.11.23 2011.03.08 2003.10.30 2003.10.30
US 2006-0063286 A1	2006.03.23	US 7291507 B2	2007.11.06