신뢰성 향상을 위한 듀얼 안티퓨즈 OTP 메모리 채택 D-PUF 회로★

김승열* · 이제훈**

요 약

기존 SRAM 기반 PUF (physical unclonable function)는 난수 생성 및 키교환에 사용된다. SRAM에서 생성된 출력값은 일정하게 유지되어야 하나, 외부 환경에 의해 변화하는 문제가 발생된다. 본 논문은 듀얼 안티퓨즈 OTP (one time programmable) 메모리를 SRAM 기반 PUF에 채택한 새로운 구조의 D-PUF (deterministic PUF) 회로를 제안한다. 제안된 PUF 회로는 SRAM에서 한 번 생성된 출력값을 일정하게 계속 유지시켜 PUF 회로의 신뢰성을 향상시킬 수 있다. 우선, 높은 보안 수준을 갖는 안티퓨즈를 이용하여 OTP 메모리를 구성하였다. SRAM은 크로스 커플 인버터쌍의 미스매치를 이용하여 전원이 들어온 후 초기값을 임의로 생성하고 이를 출력한다. 마스킹된 출력값은 안티퓨즈 OTP ROM (read-only memory)에 난수값으로 프로그램된다. 한번 프로그램된 ROM 값은 되돌려지지도 변화하지도 않는다. 따라서, 제안된 D-PUF 회로는 SRAM의 출력값을 OTP 메모리에 저장시켜 한 번 결정된 PUF 출력값을 계속 유지시킨다. 제안된 D-PUF의 출력은 동작 전압 및 온도 변화 등과 같은 외부 환경 변수에 영향을 받지 않아 신뢰성이 향상된다. 따라서, 제안된 D-PUF는 강력한 오류 정정 코드없이 사용하더라도 안정적인 동작을 수행할 수 있다.

PUF Logic Employing Dual Anti-fuse OTP Memory for High Reliability

Seung Youl Kim* · Je Hoon Lee**

ABSTRACT

A typical SRAM-based PUF is used in random number generation and key exchange process. The generated outputs should be preserved, but the values are changed owing to the external environment. This paper presents a new D-PUF logic employing a dual anti-fuse OTP memory to the SRAM-based PUF. The proposed PUF can enhance the reliability of the logic since it can preserve the output values. First, we construct the OTP memory using an anti-fuse. After power up, a SRAM generates the random values owing to the mismatch of cross coupled inverter pair. The generated random values are programed in the proposed anti-fuse ROM. The values that were programed in the ROM at once will not be changed and returned. Thus, the outputs of the proposed D-PUF are not affected by the environment variable such as the operation voltage and temperature variation, etc. Consequently, the reliability of the proposed PUF will be enhanced owing to the proposed dual anti-fuse ROM. Therefore, the proposed D-PUF can be stably operated, in particular, without the powerful ECC in the external environment that are changed.

Key words : Reproduction, Copy prevention, PUF, Anti-fuse, OTP

접수일(2015년 5월 4일), 수정일(1차: 2015년 5월 20일)
게재확정일(2015년 5월 30일)

★ 본 연구는 교육부와 한국연구재단의 지역혁신창의인력 양성사업으로 수행된 연구결과임 (No. NRF-2012H1B8A2026055).

* (주)씨엔로봇
** 강원대학교 삼척캠퍼스 전자정보통신공학부(교신저자)

1. 서 론

최근, 통신과 네트워크의 발전으로 RFID, 스마트 카드, 휴대 전화 등 개인정보를 포함하고 있는 IC의 사용이 급격히 증가하고 있다. 또한 정보의 무분별한 유통 및 해킹, 위협 등의 보안 문제가 발생하고 있다 [1]. 따라서 개인정보와 같은 민감한 데이터를 포함하고 있는 IC의 보호를 위하여 데이터 암호 및 인증, 복제 방지 등의 보안 기술을 필요로 하고 있다. 이를 위하여 제안된 물리적인 복제 방지 기술로 PUF (physical unclonable function)가 있다.

대표적인 PUF인, 실리콘 PUF는 제조공정에서 제어할 수 없는 공정의 편차를 이용하여 임의의 값을 생성한다. 생성된 임의의 값은 비밀키 생성, 식별, 인증 등 보안 응용에 사용된다 [2-3]. 실리콘 PUF는 크게 지연 기반과 쌍-안정 (bi-stable) 기반의 PUF의 두 가지로 나뉜다. 지연 PUF는 중재기 (arbiter) PUF, RO (ring oscillator) PUF등이 있고 쌍-안정 기반 PUF로는 SRAM-PUF, SA (sense amplifier) PUF가 있다 [4-6].

PUF는 IC 제조 공정상에서 발생하는 공정 편차의 고유한 특징을 이용하여 설계되기 때문에 전압변화 또는 온도 변화 등에 따른 외부적인 환경조건에 민감하다. 따라서 PUF의 신뢰성을 높이기 위하여 오류 보정 능력이 높은 ECC (error correct code) 또는 퍼지 추출 회로 (fuzzy extractor)가 사용된다 [4].

기존 실리콘 PUF는 주로 제조 공정상의 편차만을 이용하여 만들어진다. 하지만 PUF는 제조 공정상의 편차를 제외하고 온도변화, 전압 램프-업 (voltage ramp up), 동작 전압 등 다양한 환경 변화에 영향을 받아 그 값이 변화된다 [4]. 따라서 기존의 PUF는 초기 생성된 PUF 값으로 입력 challenge에 대한 출력 응답 값을 그대로 사용할 수 없고 별도의 회로를 필요로 한다.

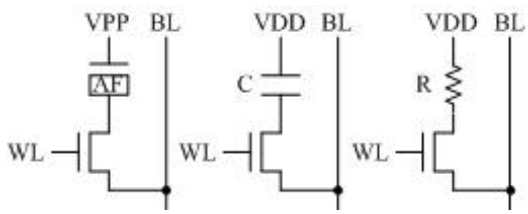
본 논문은 이중 안티퓨즈 (anti-fuse) OTP (one time programmable) 메모리를 이용하여 PUF가 환경적인 변화에 노출된 상황에서 영향을 받지 않도록 하였고 복잡한 ECC를 필요로 하지 않도록 하였다. 제안된 PUF는 SRAM PUF의 특성인 독특성과 다양성을 보장하고 환경 변화에 따라 출력값이 변하는 SRAM PUF의 출력 값을 안티퓨즈 ROM에 저장함으로써 출력값이 변화하지 않는 높은 신뢰성을 제공한다.

2. CMOS 안티퓨즈 셀

CMOS gate oxide를 이용한 안티퓨즈는 표준 CMOS 공정에서 추가적인 마스크 (mask) 없이 제작될 수 있다. 또한 임베디드 플래쉬 메모리, ROM, 전기 퓨즈 (electrical fuse), CMOS 플로팅 게이트 (floating gate)와 비교하여 높은 보안 수준을 가지고 있다 [7]. Gate oxide를 이용한 안티퓨즈 셀은 흔히 2개의 트랜지스터 혹은 3개의 트랜지스터로 구성된 구조를 갖는다 [8-9].

그림 1은 2개의 트랜지스터 구조를 갖는 안티퓨즈 셀과 그의 등가회로이다. 안티퓨즈 셀은 프로그램 되기 전과 프로그램 된 후로 각각 그림 1(b), 그림 1(c)와 같은 등가회로로 나타낼 수 있다 [8-9]. 프로그램 된 안티퓨즈는 그림 1(c)와 같이 저항으로 나타낼 수 있다. 한 번 프로그램 된 후, breakdown된 안티퓨즈의 저항 값은 수십Ω부터 수십 kΩ까지 나타나며 soft breakdown될 경우 수백 kΩ 이상의 저항 값을 갖고 있다 [10].

기존 안티퓨즈 셀 (cell)의 출력은 단일 출력으로 이루어져 있고 센스 앰프를 이용하여 감지한다. 안티퓨즈 셀이 soft breakdown 상태가 되면 출력이 약하다 [10]. 따라서 제안된 CMOS 듀얼 안티퓨즈 셀은 차동 (differential) 구조로 구성하고 차동 신호를 감지하여 soft breakdown 상태에서 강한 동작을 할 수 있도록 한다.

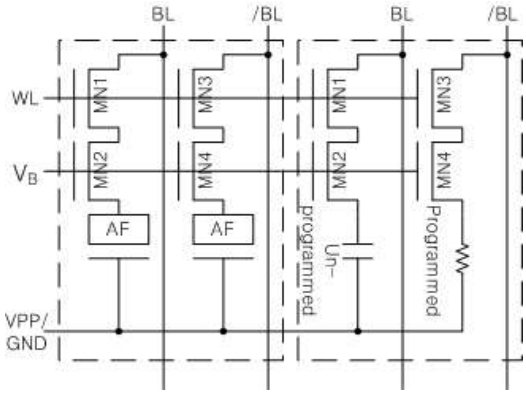


(그림 1) (a) 2-T 안티퓨즈 셀, (b) 프로그램 전 안티퓨즈 셀, (c) 프로그램 후 안티퓨즈 셀.

3. 제안된 CMOS Dual Anti-fuse OTP 메모리

제안된 듀얼 안티퓨즈 OTP 메모리는 표준 CMOS 0.18-um 공정에서 gate oxide 기반의 안티퓨즈로 구현된다. 그림 2는 제안된 듀얼 안티퓨즈 OTP 메모리의 듀얼 안티퓨즈 셀과 그의 등가회로를 나타낸다. 이 회로는 3개의 트랜지스터를 갖는 안티퓨즈 셀을 기반으로 구성되어 있다 [8]. 이 셀은 워드라인, WL (word line), 비트라인, BL (bit line), /BL, V_B, VPP/GND에 연결되어 있다. VPP/GND는 각각 프로그램 동작과 읽기 동작에서 사용된다. VPP는 프로그램 전압으로 안티퓨즈가 충분히 breakdown 될 수 있는 높은 고전압을 갖는다. V_B는 고전압의 VPP로부터 회로를 보호하기 위한 블록킹 nMOS의 게이트 입력 전압으로 VPP/2의 크기를 갖는다. 프로그램 모드가 끝난 후 V_B는 VDD전압을 갖는다. 그림 2(a)와 같이 듀얼 안티퓨즈 셀은 얇은 게이트 옥사이드 (thin gate oxide)로 구성된 2개의 안티퓨즈 nMOS와 4개의 nMOS로 구성된다. 그림 2(b)는 그림 2(a)의 등가회로를 나타낸다. 그림 2(a)에서 안티퓨즈는 그림 2(b)와 같이 프로그램 전과 프로그램 후에 각각 캐패시터와 저항으로 나타낼 수 있다 [6-7]. 프로그램 전 안티퓨즈는 nMOS 커패시터 (capacitor)와 같은 형태이고 저항값은 수 GΩ으로 나타낼 수 있다. 프로그램 후 안티퓨즈는 저항으로 나타나며 저항값은 oxide의 breakdown에 의해 수십 Ω에서 수백 Ω으로 나타나며 soft-breakdown이 될 경우 저항 값은 수 MΩ까지 나타날 수 있다 [10]. 제안된 회로는 두 개의 안티퓨즈 셀을 사용하여 soft-breakdown이 되는 경우에도 그 값을 감지하여 높은 신뢰성을 갖는다.

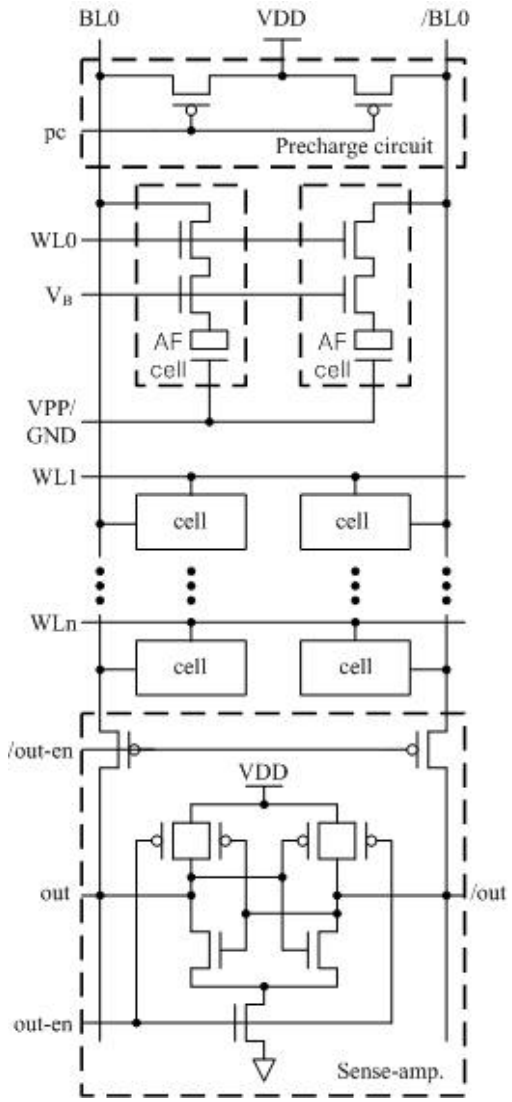
제안된 듀얼 안티퓨즈 OTP 메모리는 그림 3과 같이 precharge회로, 듀얼 안티퓨즈 셀과 센스 앰프로 구성되어 있다. 이 회로의 동작은 프로그램 모드와 읽기 모드가 있다. 첫째, 프로그램 모드는 OTP ROM이기 때문에 1회 사용된다. VPP는 프로그램 모드에서만 사용되며 anti-fuse nMOS를 breakdown 시키기 위해 고 전압으로 약 6.5V를 사용한다. 표준 CMOS 0.18um 공정에서 thin gate oxide nMOS는 주어진 전압에서 충분히 breakdown 된다 [8]. 이 고 전압 VPP



(그림 2) (a) 듀얼 안티퓨즈 셀, (b) 등가회로

는 프로그램 모드에서만 사용된다. 제안된 회로는 differential 구조로 BL과 /BL에 서로 반대의 입력 신호가 인가되고 WL 신호가 nMOS를 on하면 BL 또는 /BL 중 하나가 '0'이 입력되어 프로그램 되고 다른 하나는 프로그램 되지 않은 상태가 된다. 따라서 그림 2(b)와 같이 캐패시터와 저항의 모델로 나타낼 수 있다.

두 번째, 읽기 모드는 모든 신호의 입력 전압으로 1.8V VDD 전압을 이용한다. 그리고 안티퓨즈의 게이트에 연결되어 있는 VPP/GND 중 gorund인 GND가 사용된다. 읽기 동작을 위해 precharge 회로는 pMOS를 on하여 VDD 전압을 BL과 /BL에 인가한다. Precharge가 완료된 회로는 WL을 선택하여 안티퓨즈 셀의 nMOS를 on 시킨다. 선택된 WL의 안티퓨즈는 프로그램되지 않았을 경우 캐패시터이므로 nMOS를 통해 전류가 흐르지 않기 때문에 BL은 VDD를 유지한다. 반면에 프로그램 된 안티퓨즈는 저항이므로 nMOS를 통해 전류가 흐르게 되므로 BL 전압이 방전된다. 따라서 프로그램 된 BL의 전압은 방전되지 않은 /BL과 비교하여 충분히 큰 전위차를 갖는다. 센스 앰프는 충분히 큰 전위차를 갖는 BL과 /BL를 비교하여 신뢰성 높은 출력을 제공한다.



(그림 3) Dual antifuse cell OTP 메모리

4. 제안된 Deterministic PUF

제안된 결정적 (deterministic) PUF는 듀얼 안티퓨즈 OTP 메모리와 SRAM으로 구성된다. SRAM은 PUF 값을 생성하고 OTP 메모리는 SRAM의 출력을 저장한다. 이 동작은 단 한번 이루어지기 때문에 OTP 메모리에는 최초 SRAM의 출력 값만을 저장하고 있다. 따라서 OTP 메모리의 값은 변화하지 않기 때문에 challenge 값에 대하여 response 값이 일관성 있게 유지된다.

PUF는 입력 challenge와 출력 응답 (response)을 하나의 쌍으로 갖는다. 그리고 CRP (challenge response pair)는 독특성 (uniqueness)과 다양성을 만족해야 한다. 또한 한번 생성된 CRP의 값은 변하지 않아야 한다. CRP 생성회로는 동일한 회로와 구조를 갖고 있지만 제조 공정상의 편차로 서로 다른 CRP가 만들어진다.

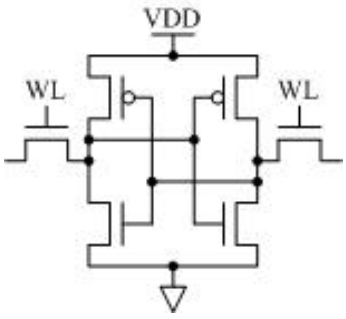
SRAM PUF는 그림 4와 같이 SRAM 셀로 구성된다. SRAM은 크로스 커플된 인버터 쌍으로 구성되어 있다. SRAM PUF는 SRAM의 크로스 커플된 인버터 쌍의 공정상의 미스매치 (mismatch)를 이용하여 SRAM에 전원이 입력되면 임의의 값으로 SRAM 셀의 출력 값이 결정된다. 하지만 공정의 미세한 차이는 동작 전압 또는 온도 변화 등과 같은 환경 변수가 발생하면 출력 값이 변화한다. 따라서 최초의 CRP들의 값과 이 후의 CRP들의 값이 일정 비율로 서로 다른 출력 값을 갖는다. 이를 보정하기 위해 ECC 또는 fuzzy extractor를 사용한다. 하지만 SRAM-PUF는 동작전압 또는 온도변화에 따른 환경 변수의 변화에 따라 20% 이상 CRP 매칭 오류가 발생한다. 오류의 발생률이 높기 때문에 오류 보정을 위한 ECC 또는 fuzzy extractor의 구성은 복잡해진다.

제안된 D-PUF는 SRAM PUF의 특성을 그대로 사용한다[4]. 하지만 SRAM PUF는 동작전압과 온도변화와 같은 환경 변수의 변화에 따라 CRP 값이 일정하지 못하고 변화하는 단점이 있다. 이 단 점을 해결하기 위하여 제안된 회로는 ROM을 사용한다. 그리고 제안된 회로에서 사용한 듀얼 안티퓨즈 OTP ROM은 보안 수준이 높은 안티퓨즈를 이용하였다.

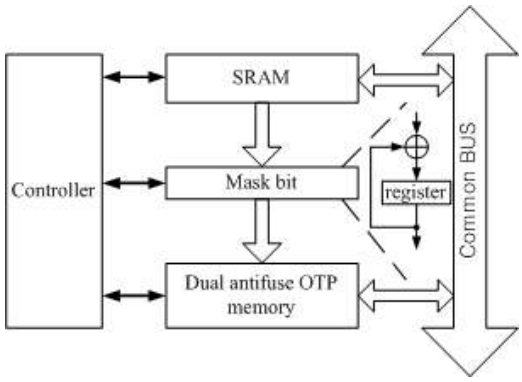
그림 5는 제안된 D-PUF의 블록도이다. D-PUF는 dual anti-fuse OTP 메모리와 SRAM, 제어기, 마스크 비트 그리고 공통버스로 구성된다. OTP 메모리는 단 한번 프로그램이 가능하고 프로그램 후에는 되돌릴 수 없다. SRAM은 OTP 메모리에 프로그램 될 PUF의 초기 값을 생성한다. 마스크 비트는 SRAM과 프로그램 된 OTP 메모리와의 상관관계를 숨기기 위해 사용된다. 프로그램 후 SRAM은 PUF에 사용되지 않고 SRAM 고유의 메모리로 사용된다. SRAM은 SoC(Sy

stem on a Chip)를 기반으로 하는 대부분의 회로에서 사용되고 있다. 따라서 OTP 메모리 추가에 따른 PUF회로의 중복을 방지함으로써 면적을 유지한다. 그리고 ROM을 사용하여 출력 값을 고정함으로써 SRAM PUF에서 발생하는 CRP 매칭 오류를 제거하였다.

제안된 회로의 동작은 다음과 같다. 첫 째, 전원이 인가되면 SRAM은 공정 편차에 의해 임의의 값을 갖는다. 그리고 그 값 중 20% 이상은 전원이 on/off 되었을 때 환경 변수에 따라 변화한다. 둘 째, SRAM의 초기 값이 변화하는 특징을 이용하여 마스크 비트를 생성한다. 최초 생성된 마스크 비트와 전원이 on/off 된 후 생성된 마스크 비트는 SRAM의 값이 변화하였기 때문에 서로 다르게 생성된다. 따라서 PUF의 값을 생성하기 위해 사용된 마스크 비트를 예측할 수 없다. 최초 마스크 비트는 SRAM의 주소 값을 마지막 까지 증가 시키며 초기 값과 exclusive-OR 연산을 함으로써 생성된다. 최초 마스크 비트는 레지스터에 저장되어 있고 그 값은 SRAM의 첫 번째 주소의 초기 값과 exclusive-OR 연산하여 첫 번째 PUF 출력 값을 생성한다. 그리고 두 번째 PUF 출력 값은 SRAM의 두 번째 초기 값과 첫 번째 PUF 출력 값을 exclusive-OR 연산을 통하여 생성된다. 이와 같이 처음 출력이 다음 출력에 영향을 주는 exclusive-OR 체인을 형성하여 PUF 값을 생성한다. 셋 째, 생성된 PUF 값은 OTP 메모리에 프로그램된다.



(그림 4) 기존의 6-T SRAM cell

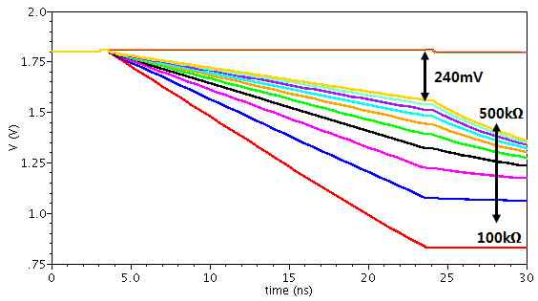


(그림 5) D-PUF 블록 다이어그램

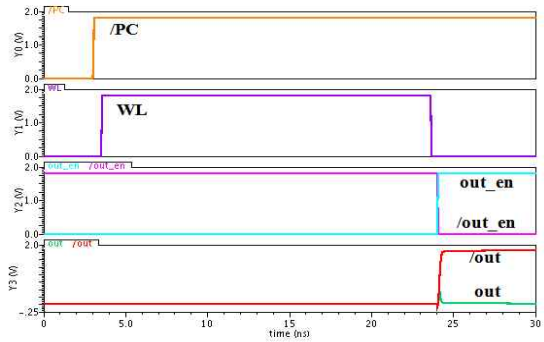
5. 시뮬레이션 결과

그림 6은 그림 2의 듀얼 안티퓨즈 셀과 그의 등가회로를 이용하여 프로그램 되지 않은 안티퓨즈와 프로그램 된 후 soft-breakdown된 안티퓨즈의 동작을 나타낸다. 등가 회로의 soft-breakdown된 안티퓨즈의 저항 값은 100kΩ 부터 500kΩ 까지 순차적으로 증가시켜 시뮬레이션 하였다. 시뮬레이션 조건으로 비트라인, BL에 연결되어 있는 안티퓨즈 셀의 수는 256 개이고, BL의 캐패시터 C_{BL}은 167fF이다. C_{BL}은 BL에 연결된 256개 cell의 nMOS 드레인 캐패시터와 precharge 회로, 센스 앰프회로에 연결된 pMOS의 캐패시터를 포함하고 있다. 그 결과, 저항 값이 500kΩ 일 때 24ns 후 BL과 /BL의 전압 차이는 240mV로 센스 앰프가 감지하기에 충분히 크다.

그림 7은 그림 3의 듀얼 안티퓨즈 OTP 메모리의 시뮬레이션 결과를 나타낸다. 프로그램된 안티퓨즈는 등가회로와 같이 저항으로 구성하였다. 프로그램된 안티퓨즈의 등가 저항의 값은 500kΩ으로 가정하여 실험하였다. 표 1에 나타낸 것처럼, 읽기 동작은 25ns 이하의 고속 동작을 수행한다. 프로그램된 저항값이 작을수록 25ns 보다 더 빠른 고속 동작이 가능하다.



(그림 6) Dual antifuse cell 시뮬레이션 결과



(그림 7) 듀얼 안티퓨즈 OTP 메모리 시뮬레이션 결과

6. 결 론

제안된 D-PUF 회로는 SRAM 기반 PUF에 듀얼 안티퓨즈 OTP 메모리를 적용한 새로운 구조의 PUF이다. SRAM-PUF는 공정의 편차를 이용하여 SRAM의 출력값을 난수로 사용한다. 그러나, SRAM 기반 PUF는 환경 변화에 따라 출력값이 일정하지 않다는 문제가 있다. 제안된 회로는 듀얼 안티퓨즈 OTP 메모리를 이용하여 SRAM 기반 PUF에서 생성한 출력을 메모리에 저장하여 출력값이 일정하게 유지되도록 하였다. 이는 표준 CMOS 공정에서 추가적인 마스크 없이 구현이 가능하다. 또한, 차동 구조로 안티퓨즈 셀을 구성함으로써 25ns이하의 고속 읽기 동작이 가능하다. 제안된 회로는 별로의 SRAM을 사용하지 않고 일반적으로 SoC에 채택된 SRAM을 이용하여 면적 증가를 방지한다. 결론적으로, 제안된 회로는 PUF 회로의 CRP를 안티퓨즈 ROM에 저장하기 때문에 동작 전압 및 온도 변화와 같은 환경 변화에 따라 출력값이 변화하지 않는다. 또한, CRP 오류가 발생되지 않기 때문에 제안된 회로는 복잡한 ECC 혹은 Fuzzy extractor 대신 단순한 ECC 회로를 이용하여 신뢰성 높은 보안 어플리케이션 개발에 활용될 수 있다.

참고문헌

[1] 김영희, 국광호, “개인정보의 안전성 확보조치 기준에서의 우선순위 정립에 관한 연구”, 융합보안 논문지, 제14권, 제4호, pp.9-17, 2014.

[2] G. Gassend, D. Clarke, M. van Dijk and S. Devadas, “Silicon Physical Random Function”, In Proceedings of th eComputerand Communication Security Conference, November 18-22, 2002.

[3] G. E. Suh and S. Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation”, In Proceedings of the44th Design Automation Conference, IEEE, June 4-8, pp.9-14, 2007.

[4] M. Bhargava, C. Cakir and K. Mai, “Reliability Enhancement of Bi-Stable PUFs in 65nm Bulk CMOS”, In Proceedings of HOST, IEEE, pp.25-30, 2012.

[5] D. E. Hocomb, W. P. Burleson and K. Fu, “Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Number”, IEEE Trans. Computers, Vol. 58, pp.1198-1210, Sept. 2009.

[6] G.-J. Schrijen and V. van der Leest, “Comparative Analysis of SRAM Memories used as PUF Primitives”, In Proceedings of DATE , IEEE, pp.1319-1324, 2012.

[7] http://www.kilopass.com/wp-content/upload/2010/04/comparision_of_embedded_nvm.pdf

[8] H. K. Cha, I. Yun, J. Kim, B. C. So, K. Chun, I. Nam, and K. Lee,“A 32-KB standard CMOS antifuse one-time programmable ROM embedded in a 16-bit microcontroller,” IEEE J. Solid-State Circuits, vol.41, no. 9, pp. 2115-2124, Sep. 2006.

[9] N. D. Phan, I. J. Chang, J.-W. Lee, “A 2-Kb One-Time Programmable Memory for UHF Passive RFID Tag IC in a Standard 0.18um CMOS Process”, IEEE Trans. Circuits and Systems, Vol. 60, pp.1810-1822, 2013.

[10] M. Depas, T. Nigam, M. M. Heyns, “Soft Breakdown of Ultra-Thin Gate Oxide Layers”, IEEE Trans. Electron Devices, Vol. 43, pp.1499-1504, 1996.

[저 자 소 개]

김 승 열 (Seung-Youl Kim)

2002년 2월 충북대학교
정보통신공학과 학사
2004년 8월 충북대학교
정보통신공학과 석사

email : kimsy@hbt.cbnu.ac.kr

이 제 훈 (Je-Hoon Lee)

1998년 8월 충북대학교
정보통신공학과 공학사
2001년 2월 충북대학교
통신회로및시스템공학
공학석사
2005년 2월 충북대학교
통신회로및시스템공학
공학박사
2005년 4월-2006년 4월 : Univ. of Southern California
박사후연구원
2006년 8월-2009년 8월: 충북대학교
BK21 충북정보기술사업단
초빙조교수
2009년 8월-현재 : 강원대학교 공학대학
전자정보통신공학부 부교수

email : jehoon.lee@kangwon.ac.kr