JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 24, No. 8: 1037~1043, Aug. 2020

스위칭 회로를 이용한 다수의 입출력 쌍을 갖는 SRAM 기반 물리적 복제 불가능 보안회로

백승범[1] · 홍종필[2*]

Switched SRAM-Based Physical Unclonable Function with Multiple Challenge to Response Pairs

Seungbum Baek[1] · Jong-Phil Hong[2*]

[1]Graduate Student, School of Electrical Engineering, Chungbuk National University, Cheongju, 28644 Korea
[2*]Associate Professor, School of Electrical Engineering, Chungbuk National University, Cheongju, 28644 Korea

요 약

본 논문에서는 IoT 기기를 위한 저가, 초소형, 저 전력의 반도체 공정 기반 물리적 복제 불가능 보안회로를 소개한다. 제안하는 보안회로는 SRAM 구조의 인버터 간 교차결합 경로에 스위칭 회로를 연결하여 챌린지 입력을 인가함으로써 다수개의 입출력 쌍을 갖도록 한다. 그 결과 제안된 구조는 기존 SRAM 기반 물리적 복제 불가능 보안회로의 빠른 동작 속도와 비트 당 소요면적이 작은 장점을 유지하면서도 다수개의 입출력 쌍을 갖는다. 제안된 스위칭 SRAM 기반의 물리적 복제 불가능 보안회로는 성능 검증을 위해 180nm CMOS 공정을 이용하여 총 면적 0.095mm^{2}의 칩으로 제작하였다. 측정 결과 4096-bit의 CRP, 0의 Intra-HD, 0.4052의 Inter-HD의 우수한 성능을 보였다.

ABSTRACT

This paper presents a new Physical Unclonable Function (PUF) security chip based on a low-cost, small-area, and low-power semiconductor process for IoT devices. The proposed security circuit has multiple challenge-to-response pairs (CRP) by adding the switching circuit to the cross-coupled path between two inverters of the SRAM structure and applying the challenge input. As a result, the proposed structure has multiple CRPs while maintaining the advantages of fast operating speed and small area per bit of the conventional SRAM based PUF security chip. In order to verify the performance, the proposed switched SRAM based PUF security chip with a core area of 0.095mm^2 was implemented in a 180nm CMOS process. The measurement results of the implemented PUF show 4096-bit number of CRPs, intra-chip Hamming Distance (HD) of 0, and inter-chip HD of 0.4052.

키워드 : 상보형 금속 산화물 반도체, 사물인터넷, 물리적 복제 불가능 함수, 보안, 정적 램

Keywords : CMOS, IoT, Physical Unclonable Function, Security, SRAM

Received 16 July 2020, **Revised** 21 July 2020, **Accepted** 22 July 2020

*** Corresponding Author** Jong-Phil Hong(E-mail:jphong@cbnu.ac.kr, Tel:+82-43-261-3536)
Associate Professor, School of Electrical Engineering, Chungbuk National University, Cheongju, 28644 Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.8.1037 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 4차 산업혁명 구현을 위한 관련 기술이 활발히 연구되고 관련 시장이 급성장하고 있으며, 특히 초연결 사회의 기반 기술이자 차세대 인터넷인 사물 간 인터넷(IoT)환경 구축이 가속화되고 있다[1-4]. 네트워크 레이어의 제일 말단에 위치한 IoT 기기의 경우 과거 서버로부터의 단방향 통신에서, 수집한 중요 데이터를 전달하고 다시 명령을 수행하는 양방향 통신으로의 전환이 필수적으로 요구되면서 해킹과 기기 복제의 문제점이 대두되고 있다[5].

낮은 사양, 저 전력 시스템의 IoT 기기를 위한 보안 시스템의 요구사항은 다음과 같다. 첫째, IoT 기기 본연의 시장 경쟁력을 잃지 않기 위해서 보안 시스템 자체도 저가, 경량 및 저 전력으로 구현이 되어야 한다. 둘째, 보안 시스템 자체가 복제되는 것을 방지하기 위해 물리적 복제 불가능 함수의 특성을 가져야 한다. 복잡한 알고리즘을 사용하여 난수를 생성하는 기존의 소프트웨어 기반 보안기술은 PC와 메모리 등 고사양을 필요로 하고, 고성능 PC로 해킹이 가능한 문제가 있기 때문에 IoT 기기를 위한 보안 시스템으로는 적합하지 않다. 이에 반해 최근 연구되고 있는 반도체 기반 보안 기술은 반도체 공정 기술을 이용하여 저가, 초소형, 저 전력으로 구현이 가능하며 회로를 복제하더라도, 제조 공정의 편차에 의한 값이 다 달라 물리적 복제가 불가능한 특성을 가지고 있기 때문에 IoT 기기를 위한 최적의 보안기술로 떠오르고 있다.

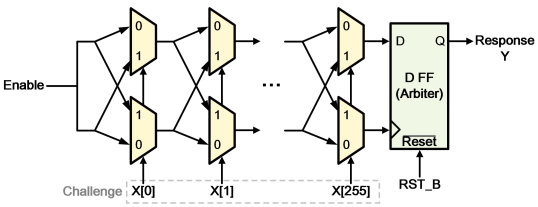

Fig. 1 Structure of a delay based PUF.

반도체 공정편차를 이용한 물리적 복제 불가능 보안회로는 동작원리에 따라 일반적으로 지연 기반과 메모리 기반 구조로 분류할 수 있다. 그림 1에서 나타내는 지연 기반의 물리적 복제 불가능 보안회로의 경우 공정편차에 따른 지연 및 발진주파수의 오차를 이용하는 방법으로서 챌린지 입력과 출력응답 쌍(Challenge-to-Response Pairs: CRP)의 개수가 많은 장점이 있는 반면에 비트 당 소요되는 면적이 크고 출력 값을 생성하는 속도가 느린 문제가 있다[6-7]. 반면에 메모리 소자의 랜덤 한 준안정 상태를 이용하는 메모리 기반 구조는 지연 기반 구조의 문제점을 해결하여 비트 당 소요되는 면적이 작고 출력 값을 생성하는 속도가 빠르나 CRP 개수 1개여서 난수 생성기 등의 제한적 사용만 가능한 문제가 있다[8-9].

본 논문에서는 SRAM 내부의 인버터 교차결합 경로에 스위치를 연결하고, 챌린지 입력으로 스위치를 제어함으로써 기존의 소형 및 빠른 동작속도의 장점을 보이면서 동시에 다수개의 CRP를 갖는 새로운 SRAM 구조 기반 물리적 복제 불가능 보안회로를 제안한다.

Ⅱ. 새롭게 제안하는 다수의 입출력 쌍을 갖는 스위칭 기반 SRAM 구조

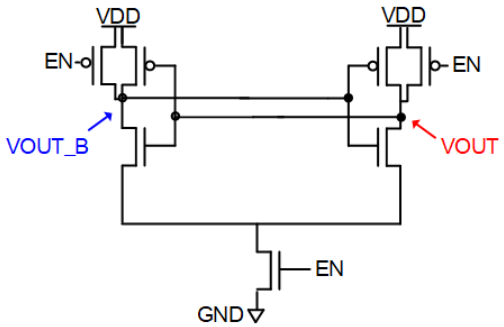

Fig. 2 Schematic of basic SRAM PUF.

그림 2는 일반적인 인버터 교차결합 기반의 SRAM 메모리 구조이다. 그림에서 두 차동출력 신호(VOUT_B와 VOUT)는 두 인버터 간의 초기 조건에 의해 하나는 1로 다른 하나는 0으로 결정되는데 초기 조건은 공정편차에 의해 무작위로 설정된다. 예를 들어 교차결합 되는 두 인버터 노드의 초기 전압이 공정 편차에 의해 준안정 지점(Meta-stable point)을 기점으로 왼쪽에 형성되면 VOUT은 1, VOUT_B는 0이 되고, 반대로 오른쪽에 형성이 되면 VOUT이 0, VOUT_B가 1이 된다. 그림 2의 기존 SRAM 구조는 회로를 복제하더라도 공정편차를 알 수 없기 때문에 출력에 대한 물리적 복제가 불가능하고, 지연기반 구조와 비교하면 초기 조건에 의해 출력 값이 바로 결정되어 동작속도가 빠르며, 적은 개수의 트

랜지스터로 구성된 하나의 SRAM 회로에서 하나의 출력비트를 얻을 수 있어 작은 면적으로 구현이 가능한 장점이 있다. 그러나 기존 SRAM 구조는 동일한 칩에서 챌린지 입력 없이 하나의 출력 값만을 갖기 때문에 제한적인 분야에만 사용이 가능한 단점이 있다.

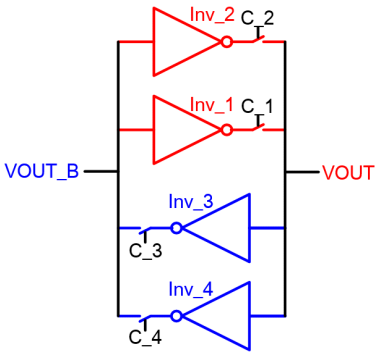

Fig. 3 Block diagram of the proposed switched SRAM based CRP PUF.

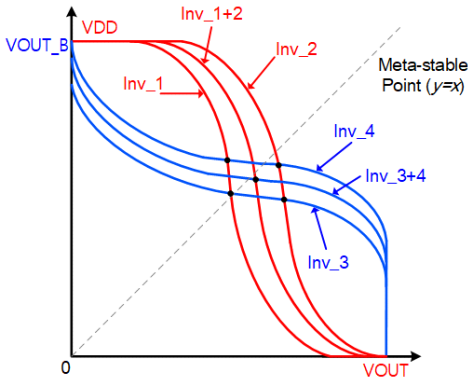

Fig. 4 Voltage transfer curve of the proposed switched SRAM based CRP PUF.

그림 3은 새롭게 제안하는 스위칭 SRAM 기반의 물리적 복제 불가능 회로도 예를 보여주고 있다. 제안하는 구조는 그림 2에서 기존 두 인버터 간의 교차결합 경로 각각에 Pass 트랜지스터 형태의 스위칭 회로를 연결하고, 챌린지 입력으로 스위칭 회로를 제어하도록 함으로써 챌린지 입력에 따라 교차결합을 재구성하여 다수개의 출력 값을 가질 수 있다. 그림 3의 구성은 두 개의 SRAM 인버터 각각에 스위칭 회로를 연결하여 4-bit 챌린지 입력을 갖는다. 그림 4는 그림 3의 회로에서 챌린지 입력 대비 가능한 모든 출력 값을 보여준다. 그림 4에서 인버터의 차동 출력 전압은 두 곡선(빨간 실선과 파란 실선)이 만나는 지점에서 결정되고, 공정편차에 의해 복수 개의 값을 가질 수 있다. 공정편차가 무작위하다고 가정할 때, 그림 3의 인버터 INV_1과 INV_2 곡선은 준안정 상태를 기점으로 좌우, INV_3과 INV_4의 곡선은 상하에 위치할 수 있다. 인버터의 차동 출력 전압이 만나는 지점이 준안정 상태를 기점으로 위에 있으면 VOUT 출력은 1이 되고 아래에 있으면 0이 된다. 이때, 출력 값은 예측이 불가능한 공정편차에만 결정이 되어야 무작위한 값을 얻을 수 있기 때문에 위의 빨간색 인버터와 아래의 파란색 인버터의 수는 반드시 동일해야 한다. 그렇지 않고 교차결합 인버터의 수가 다를 경우, 공정편차와 상관없이 한 쪽으로 값이 정해지므로 복제가 가능하다. 위의 조건을 고려하면 제안된 스위칭 기반 SRAM 구조에서 4-bit 챌린지 입력을 사용할 경우 그림 4와 같이 5개의 출력 값을 얻을 수 있으며 표 1은 그림 4일 예에서 챌린지 입력과 그 때의 출력 값을 정리한 결과이다.

Table. 1 Operational truth table of the proposed switched SRAM based CRP PUF

C1	C2	C3	C4	VOUT
1	0	1	0	1
1	0	0	1	1
0	1	1	0	0
0	1	0	1	0
1	1	1	1	0

Ⅲ. 스위칭 기반 SRAM을 적용한 물리적 복제 불가능 보안회로 설계 및 측정결과

그림 5는 2장에서 제안한 구조를 적용하여 설계한 스위칭 SRAM 기반 물리적 복제 불가능 보안회로 시스템을 나타낸다. 제안하는 SRAM 셀은 16*16 어레이 형태로 제어 회로(Controller)와 함께 구성되어 있다. SRAM 어레이는 교차 결합된 양측 인버터들이 균일한 기생성분을 가져 공정편차에 의해 신뢰할 수 있는 난수가 생성될 수 있도록 설계하였다. 셀 어레이는 칩 입력 신호에 따라 행(WL, 워드라인) 단위로 동작하고, 열들의 병렬 출력(BL, 비트라인)을 Readout 회로를 통해 출력한다.

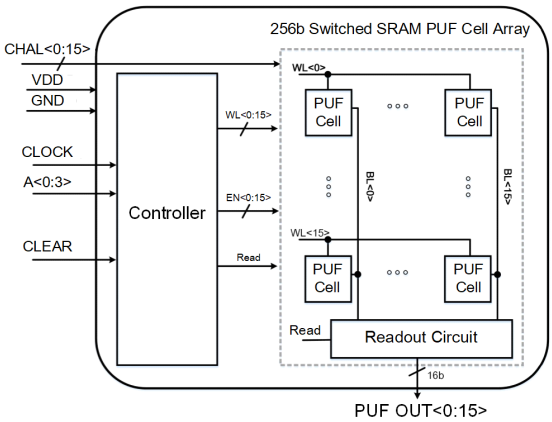

Fig. 5 Top block diagram of the proposed switched SRAM based CRP PUF.

제어 회로는 행 디코더, 워드라인 드라이버, 그리고 동작 모드 선택 회로로 구성되어 있다. 주소 선택 신호 A<0:3>를 통해 동작시킬 행을 선택하면, 디코더와 워드라인 드라이버를 통해 워드라인 선택 신호(WL, 워드라인)를 생성하여 어레이에 전달한다. CLOCK과 CLEAR 신호를 통해 동작 모드를 선택할 수 있고, 이에 따라 셀 활성화 신호인 EN 신호 그리고 Readout 동작 신호인 Read 신호를 생성하여 전달한다. Readout 회로와 PUF 셀 간에는 tri-state 버퍼로 연결되어, 셀들의 동작이 끝나기 전에는 외부 부하의 영향을 받지 않도록 완충 역할을 수행하여 공정 편차에 의해서만 난수가 생성될 수 있도록 하였다. 난수 생성 동작이 끝나면 비트라인과 연결되어 노이즈를 제거하고, 충분한 출력 전류와 함께 출력을 칩 외부로 전달하는 역할을 수행한다.

그림 6은 그림 3의 제안된 스위칭 SRAM 구조를 확장하여 구현된 16비트 챌린지 입력 PUF 회로이며 그림 5의 단위 PUF 셀 내부 회로를 보여준다. 그림 7은 그림 6의 단위 PUF 셀 동작 모드를 나타낸다. 단위 셀은 16개의 인버터들이 pass 트랜지스터와 함께 교차 결합을 이루며, 동작 활성화와 어레이 구성 시 행 선택을 위한 EN 및 WL 트랜지스터가 추가된다. 동작 모드는 Pre-charging을 담당하는 Standby 모드와 고유 난수를 생성하는 Evaluation모드로 구분된다. 먼저 Standby 모드에서 EN 노드에 논리 0을 인가하여 출력 노드를 Pre-charging하여 양쪽 인버터 출력을 모두 논리 1로 만들고, 챌린지 입력을 통해 인버터들의 교차결합을 재구성한다. 그림 6에는 포함되어 있지 않지만, SRAM 셀 출력 노드들뿐만 아니라 비트라인도 Pre-charging이 필요한데, 이는 일반 SRAM의 Read 동작과 동일하게 수행한다. Evaluation 모드에서 EN 노드에 상승 신호를 인가하면 양쪽의 인버터가 공정 편차에 의해 난수 키를 생성하기 시작한다. 일정 시간 이후, SRAM 셀이 안정 상태에 도달하여 난수 키가 결정되면, WL 트랜지스터를 활성화하여 출력을 비트라인으로 전달한다. 이때, 워드라인을 EN보다 늦게 활성화하는 이유는 안정 상태에 도달하기 전에 워드라인을 활성화하면 비트라인에 존재하는 부하가 셀 동작에 악영향을 줄 수 있기 때문이다.

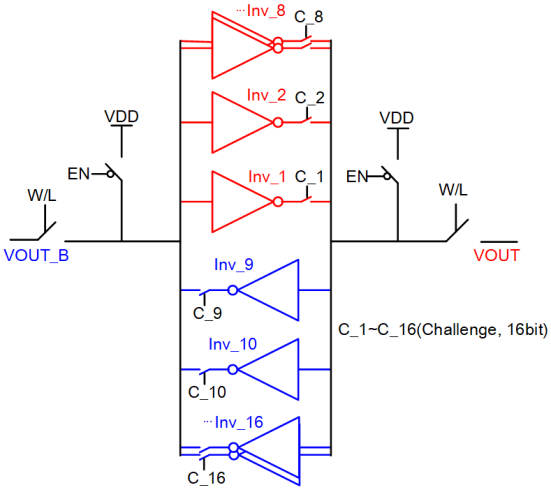

Fig. 6 Block diagram of the proposed switched SRAM based CRP PUF with 16-bit challenge input.

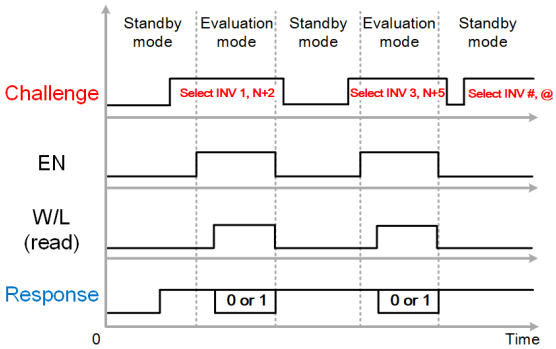

Fig. 7 Operational timing diagram of the proposed switched SRAM based CRP PUF.

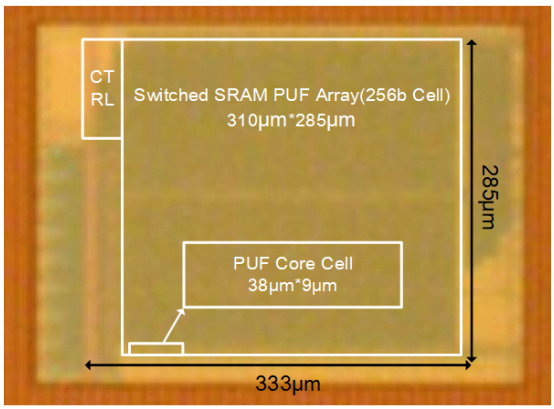

Fig. 8 Die micrograph of the proposed switched SRAM based CRP PUF.

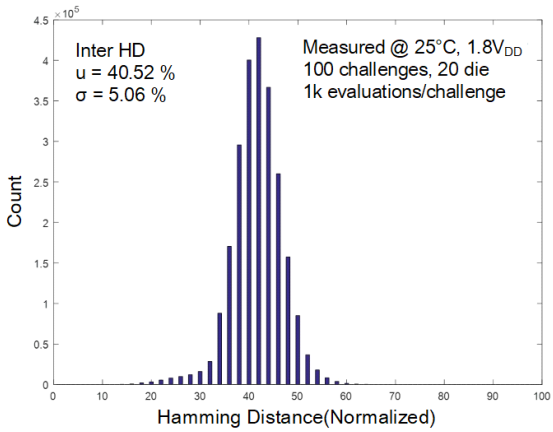

Fig. 9 Measured inter-chip hamming distance distribution.

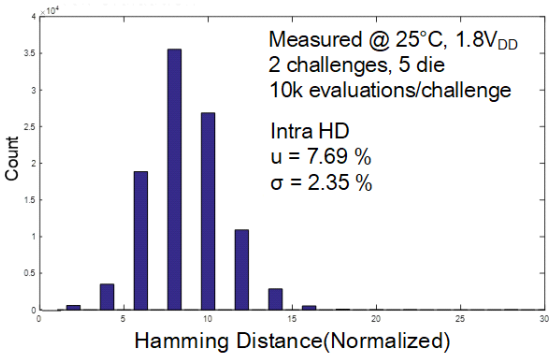

Fig. 10 Measured intra-chip hamming distance distribution.

그림 8은 제안하는 스위칭 SRAM 기반 물리적 복제 불가능 함수의 동작 및 성능을 분석하기 위해 180nm CMOS 공정으로 제작된 칩 사진을 나타낸다. 총 면적은 대략 0.095mm^{2}이고, 물리적 복제 불가능 단위 PUF 셀의 면적은 342um^{2}이다. 제작된 칩은 1.8V의 공급전원으로 동작시켰고 FPGA, 칩 소켓 그리고 메모리가 포함된 테스트보드를 활용하여 측정하였다. PC에서 터미널 프로그램과 UART 통신을 통해 테스트 벤치를 보드에 전송하면, 이를 메모리에 저장한 후, FPGA를 통해 구현된 Scan chain 테스트 회로를 통해 칩에 입력으로 순차적으로 인가하였다. 마찬가지로 칩의 출력을 Scan chain 회로, UART 통신을 통해 PC에서 수신하였다. 이 후, Matlab에서 칩의 출력을 불러와 성능을 계산할 수 있는 스크립트를 구현하여 가시화하였다.

물리적 복제 불가능 함수에서 대표적인 성능 지표는 난수 키의 인증식별성 및 인증재생산성인데, 두 지표 모두 해밍 거리를 통해 계산한다[6]. 해밍 거리는 동일한 길이를 갖는 두 비트열이 서로 다른 정도를 거리로 표현할 수 있는 단위이다. 인증식별성은 동일한 회로로 제작된 서로 다른 두 칩에 동일한 챌린지를 인가하였을 때 생성되는 두 출력이 서로 다른 정도를 해밍거리(Inter-chip hamming distance)를 통해 수치화할 수 있다. 이상적인 수치는 50%로써, 1 또는 0이 생성될 확률이 50%라는 의미를 갖는다. 인증재생산성은 한 칩에 동일한 챌린지를 두 번 인가하였을 때 생성되는 두 출력이 서로 다른 정도를 해밍거리(Intra-chip hamming distance)를 통해 수치화 할 수 있다. 이상적인 수치는 0%로써, 동일한 입력에는 100% 균일한 출력을 생성한다는 의미를 갖는다. 이를 많은 칩 개수, 챌린지 그리고 반복 측정을 통해 수행하면 가우시안 분포를 나타내어 통계적으로 유의미한 수치를 얻을 수 있다.

제안하는 물리적 복제 불가능 함수의 인증식별성 측정 결과를 히스토그램, 평균 그리고 표준편차로써 그림 9에서 나타낸다. 인증식별성 평균은 40.52% 그리고 표준편차는 5.06%로 도출되었다. 20개의 칩, 100개의 챌린지 입력 그리고 신뢰성을 위해 챌린지당 1천 번의 반복 측정을 통해 도출하였고, 공급전원 1.8V와 상온 환경에서 측정되었다. 그래프의 x축은 해밍거리를 제안하는 보안 칩의 출력 비트 길이인 256으로 나눈 것이다. 그림 10은 제안하는 회로의 인증재생산성 측정 결과를 나타낸다. 평균은 7.69% 그리고 표준편차는 2.35%로 도출되었다. 5개의 칩, 2개의 챌린지 입력 그리고 좀 더 엄격한 평가를 위해 챌린지당 1만 번의 반복 측정을 통해 도

출하였고, 동작 환경은 인증식별성 측정 환경과 동일하게 설정하였다.

Table. 2 Performance Comparison with State of the Art

	This Work	ISSCC' 15 [10]	VLSI'17 [11]	VLSI'17 [12]
Technology	180nm CMOS	40nm CMOS	130nm CMOS	28nm FDSOI
Architecture	Bi-Stable (SRAM)	Delay (RO)	Analog	Bi-Stable (SRAM)
Response Bit-width	256	1	1	64
Challenge Bit-width	16	96	65	-
Number of CRPs	~1.3*104	~5.5*1028	~3.7*1027	~1.17*1011
Core Area (um2)	342	845	39000	1140
Efficiency (pJ/bit)	0.9	17.75	11	0.097
Inter-Chip HD	0.4052	0.5007	0.499	0.483
Intra-Chip HD	0 (46% CRPs discard)	0 (34% CRPs discard)	0.001 (46% CRPs discard)	0.0317
Worst Settling Time (ns)	8	1100	-	-

표 2는 본 논문에서 제안하는 다수의 CRP를 생성하는 스위칭 SRAM 기반 물리적 복제 불가능 함수와 이전의 연구 결과들을 비교한 표이다. 이전 연구들과 비교했을 때 본 논문에서 제안하는 구조가 가장 작은 셀 면적을 나타내는데, 이는 SRAM 구조의 장점이다.[12] 구조도 같은 SRAM을 이용하지만 주소 순서를 단순 변경시켜 64 비트 CRP를 생성하는데 반해, 본 논문에서는 SRAM 구조 자체를 변경하므로 제안된 구조가 더 많은 4096 비트 CRP를 생성하는데도 불구하고 적은 면적으로 구현되었다. 0.9 pJ/bit의 에너지 효율 또한 SRAM 구조가 지연 기반이나 아날로그 기반 다른 구조들에 비해 빠른 동작속도를 갖기 때문에 우수한 성능을 보였고, [12]의 구조보다는 크지만 28nm와 180nm의 디지털 공정 속도를 고려하였을 때 제안하는 구조가 충분한 경쟁력을 보이는 것으로 생각된다. 인증재생산성 지표인 Intra-chip hamming distance의 경우, post-processing을 통해 46%의 불안정한 CRP를 제거하였을 때 이상적인 지표인 0이 도출되었고, 이전 연구들과 유사한 성능을 갖는다. 제안하는 구조가 이전 연구들에 비해 CRP의 개수가 더 적은데, 이 이유는 본 논문에서 제작된 제안하는 구조의 보안 칩이 16 비트 챌린지를 가지기 때문이다. 본 논문의 구조를 96비트의 챌린지로 확장하면, CRP의 개수는 ~$6.4*10^{27}$개로 늘어날 수 있다.

Ⅳ. 결 론

본 논문에서는 저가, 경량, 저 전력 IoT 기기를 위한 새로운 반도체 공정 기반의 물리적 복제 불가능 보안회로 구조를 제안하였다. 제안하는 보안회로는 SRAM 구조에서 인버터 간의 교차결합 경로에 스위칭 회로를 연결하고 스위칭 동작을 챌린지 입력으로 제어함으로써 다수개의 입출력 쌍을 생성하였다. 그 결과 기존 SRAM 기반 물리적 복제 불가능 회로의 빠른 동작 속도와 소형화의 장점과 더불어 다수개의 입출력 쌍으로 동작시킬 수가 있었다. 제안된 스위칭 SRAM 기반의 물리적 복제 불가능 보안회로는 난수생성 구조로써 뿐만 아니라, 기존 SRAM 기반 구조로는 적용이 불가능한 메시지 인증, 객체 인증 등 다양한 분야에 사용이 가능할 것으로 생각된다.

ACKNOWLEDGEMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1 B07042607). This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program(IITP-2020-0-01462) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). The chip fabrication and EDA Tool were supported by the IC Design Education Center.

REFERENCES

[1] T. Idriss, H. Idriss, and M. Bayoumi, “A PUF-based paradigm for IoT security,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston: VA, pp. 700-705, Dec. 2016.

[2] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, and M. M. Prabhu, “Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifi er Database,” *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424 – 437, Jun. 2019.

[3] Y. Zheng, S. S. Dhabu and C. Chang, "Securing IoT Monitoring Device using PUF and Physical Layer Authentication," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, pp. 1-5, May 2018.

[4] J. Y. Lee and L. Kolasani, “Security Based Network for Health Care System,” *Asia-pacific Journal of Convergent Research Interchange*, vol. 1, no. 1, pp. 1-6, Mar. 2015.

[5] H.-J. Han and D.-W. Park, “Cybersecurity of The Defense Information System network connected IoT Sensors,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 24, no. 6, pp. 802-808, Jun. 2020.

[6] R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions,” in *Towards Hardware-Intrinsic Security*, Berlin: Springer, pp. 3-37, Oct. 2010.

[7] Y. Gao, S. F. Al-Sarawi, and D. Abbott, “Physical unclonable functions,” *Nature Electronics*, vol. 3, no. 2, pp. 81-91, Feb. 2020.

[8] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “FPGA Intrinsic PUFs and Their Use for IP Protection,” in *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Berlin: Springer, pp. 63-80, 2007.

[9] K.-U. Choi, S. Baek, J. Heo, and J.-P. Hong, “A 100% Stable Sense- Amplifier-Based Physically Unclonable Function With Individually Embedded Non-Volatile Memory,” *IEEE Access*, vol. 8, pp. 21857-21865, Feb. 2020.

[10] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, “14.2 A physically unclonable function with BER $<10^{-8}$ for robust chip authentication using oscillator collapse in 40nm CMOS,” in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, San Francisco: CA, pp. 1-3, Feb. 2015.

[11] X. Xi, H. Zhuang, N. Sun, and M. Orshansky, “Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS,” in *2017 Symposium on VLSI Circuits*, Kyoto, pp. C268-C269, Jun. 2017.

[12] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, “A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell,” in *2017 Symposium on VLSI Circuits*, Kyoto, pp. C270-C271, Jun. 2017.

백승범(Seungbum Baek)

2015년 충북대학교 정보통신공학부 학사 졸업
2017년 충북대학교 정보통신공학부 석사 졸업
2017년 3월~현재 충북대학교 전기공학부 박사과정
※관심분야 : 물리적 복제 불가능 정보보안 인증 SoC, 웨어러블 생체 신호 습득 시스템, 임베디드 시스템

홍종필(Jong-Phil Hong)

2005년 한국항공대학교 항공전자공학과 학사 졸업
2007년 KAIST 정보통신공학과 석사 졸업
2010년 KAIST 정보통신공학과 박사 졸업
2010년 3월~2012년 8월 삼성전자 시스템 LSI 사업부 책임 연구원
2012년 9월~현재 충북대학교 전자정보대학 부교수
※관심분야 : 서브테라헤르츠 집적회로, 하드웨어 기반 경량 보안인증 시스템, 경량 웨어러블 생체 신호 습득 시스템