https://doi.org/10.33778/kcsa.2023.23.5.143

물리적 복제 불가능 회로 정량적 특성 평가 방법 연구

김 문 석*

요 약

하드웨어를 이용한 보안 프로토콜 구현 및 사용에 있어 물리적 복제 불가능 회로 연구가 증가하고 있다. 물리적 복제 불가능 회로는 집적 회로 및 보안 시스템의 인증, 복제 방지. 중요 정보 저장 등의 기능 수행이 가능하다. 물리적 복제 불가능 회로의 구현을 통해 기밀성, 무결성, 가용성 보안 기능 중 많은 보안 기능의 적용이 가능한 솔루션이다. 따라서, 물리적 복제 불가능 회로는 안전한 반도체 집적 회로 및 보안 시스템 구현에 중요한 기반 기술로 주목받고 있다. 하지만, 물리적 복제 불가능 회로가 보안 기능을 갖기 위해서는 예측 불가능성, 특이성, 견고성 특성을 가져야 한다, 이 연구에서는 물리적 복제 불가능 회로의 특성 방법에 관하여 자세히 설명하고 소개한다. 이 연구 결과를 적용하여 구현한 물리적 복제 불가능 회로의 정량적 특성 평가가 가능하고 보안 시스템의 적용 가능성을 평가할 수 있다.

A Study of Quantitative Characterization of Physically Uncloanble Functions

Moon-Seok Kim*

ABSTRACT

Applications on physically unclonable circuits (PUFs) for implementing and utilizing security protocols with hardware is on the rise. PUFs have the capability to perform functions such as authentication, prevention of replication, and secure storage of critical information in integrated circuits and security systems. Through the implementation of physically unclonable circuits, a wide range of security features, including confidentiality, integrity, and availability, can be applied. Therefore, PUFs are promising candidate to build secure integrated circuits and hardware systems. However, in order that PUFs possess security features, PUFs should possess characteristics such as unpredictability, uniqueness, and robustness characteristics. This study provides a detailed explanation and introduction of the methods to characterize the PUF properties. By applying the results, it becomes possible to quantitatively evaluate the characteristics of implemented PUFs and assess their availabilities for security system applications.

Key words : Physically Unclonable Functions(PUF), Unpredictability, Uniqueness, Robustness, Authentication, Random number generation

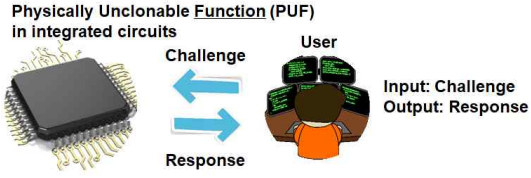
접수일(2023년 11월 17일), 수정일(2023년 12월 11일), 게재확정일(2023년 12월 22일)

* 국립한발대학교 반도체시스템공학과 조교수

1. 서 론

1.1 PUF 정의

PUF는 Physically Unclonable Functions의 약자로 한국어로 물리적 복제 불가능 회로라고도 하며 반도체 지문으로도 부른다[1]. PUF는 기기 식별 및 인증(device identification and authentication), 중요 정보의 안전한 저장 등을 가능하게 하여 보안 시스템 프로토콜 및 보안 아키텍처에서 중심적인 하드웨어 구성 요소로 제안 받고 있다[2][3]. 현재 하드웨어 보호, 위조 방지 및 RFID(Radio Freqency IDentification)의 응용 분야로 PUF를 활용한 보안 제품들이 시장에 판매하기도 한다[4][5]. PUF는 임베디드 시스템 혹은 반도체 칩 내 하드웨어 형태로 구현한다. 중요 정보의 안전한 저장 기능을 통해 보안 기밀성(Confidentiality)에 기여하고 기기 식별 및 인증 기능을 통해 보안 인증(Authentication) 및 무결성(Integrity) 기능에 기여한다. 즉, 보안 CIA(Confidentiality, Integrity, and Availability) 모델에도 적용되는 보안 소자(security primitive)이다[6]. PUF는 일종의 함수로 도전/응답(challenge/response) 형태로 사용자와 동작한다[7]. (그림 1)은 PUF 도전/응답 개념도를 보여준다. PUF는 사용자가 도전의 입력을 주면 응답의 출력을 주는 일종의 함수이다. 즉, PUF는 사용자가 도전 입력을 인가하였을 때 예측 불가능성, 특이성, 견고성 특성을 가지는 응답을 사용자에게 제공한다[8][9]. 이 세 가지 특성을 가질 때 PUF는 반도체 지문 역할을 가진다. 이 반도체 지문 역할을 바탕으로 반도체 칩의 보안 기능을 수행한다.



(그림 1) PUF 및 사용자 도전/응답 입출력 개념도

예측 불가능성(unpredictability): 예측 불가능성은 공격자가 PUF의 도전/응답(입력/출력) 관계를 일부 알고 있더라도 나머지 미지 입력-출력 관계에 대해서 예측 불가능함을 뜻한다. 즉, PUF 도전/응답 관계를 측정하기 전에 시뮬레이션이나 기계 학습에 의해 예측이 불가능함을 뜻한다. 이것은 PUF를 인증수단으로 활용할 때 중요한 특징이다. 좀 더 구체적으로 설명하면 예측 불가능성은 통계적으로 0,1 논리 값 중 편향된 논리 값을 가지지 않아야 한다. 또한 물리적인 위치에도 독립적인 논리 값을 출력해야 한다. PUF의 예측 불가능성은 해밍 무게(hamming weight), 최소 엔트로피(min entropy) 2개의 지표로 확인한다[10].

특이성(uniqueness): 특이성이란 다른 칩에 PUF 출력이 상관관계가 없음을 보여주는 특성이다. PUF는 예측 불가능한 공정상의 편차로 인해 칩마다 다른 논리 값들을 만들어내는 반도체의 지문과 같은 역할을 한다. 칩들이 상관관계가 없이 독립적인 출력을 가지고 있는 것은 PUF를 반도체 지문을 활용하기에 중요한 평가 요소이다. 특이성은 다른 칩 PUF 출력에 해밍 거리를 계산하여 측정한다. 다른 칩 PUF 출력에 해밍 거리를 인터 칩(inter chip) 해밍 거리라고 하고 같은 칩 PUF 출력에 해밍 거리를 인트라 칩(intra chip) 해밍 거리라고 한다. 인터 칩과 인트라 칩 해밍 거리를 비교하여 특이성을 평가한다[11].

견고성(Robustness): PUF의 견고성이란 같은 칩, 같은 입력의 PUF 출력이 항상 동일한 출력을 가짐을 의미한다. 같은 칩 PUF 출력이 시간이 지나도 동일한 출력을 가져야 한다는 것을 의미한다. 이 때, 견고성은 온도 및 전압같은 환경 변화에도 동일한 출력을 가지는 것을 포함한다. 따라서, 온도 및 전압 환경시험을 통하여 PUF 출력의 견고성을 확인하는 것은 중요하다. 견고성은 인트라 칩 해밍 거리(bit error rate)을 계산하여 특성 평가를 수행한다[12].

(그림 2)는 PUF의 반도체 지문 기능인 예측 불가능성, 특이성, 견고성 특징을 비유적으로 설명해준다. 예측 불가능성은 모델이나 계산을 통하여 PUF 출력을 알 수 없다는 그림이고, 특이성은 사람마다 고유의 특성을 가진다는 그림이며, 견고성은 동일 칩은 노화 효과(aging effect)에도 동일 출력을 가진다는 그림이다.

(그림 2) PUF 주요 특성 비유 그림

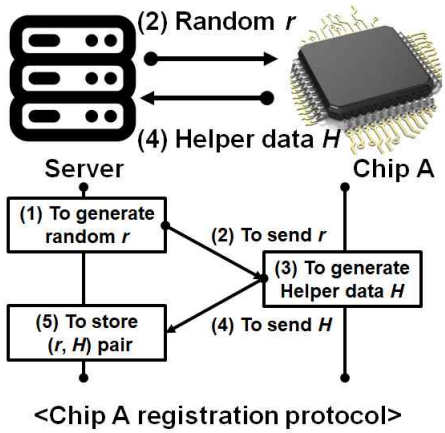
1.2 PUF 응용

PUF는 반도체 칩 혹은 임베디드 시스템 내 구현하는 하드웨어로 기기 식별 및 인증(device identification and authentication), 중요 정보의 안전한 저장 기능이 가능하다[13][14][15]. PUF의 반도체 지문 기능을 활용한 주요 보안 기능을 정리하면 아래와 같다.

① 칩 ID 및 데이터의 인증
② 무단 복제 방지
③ 중요 정보 생성 및 안전한 저장
④ 의사난수발생기 시드 생성

이 중에서 PUF를 이용한 핵심 응용인 IC 인증 및 의사 난수 발생기(Pseudo Random Number Generator: PRNG) 시드 생성 기능을 소개하려고 한다[16].

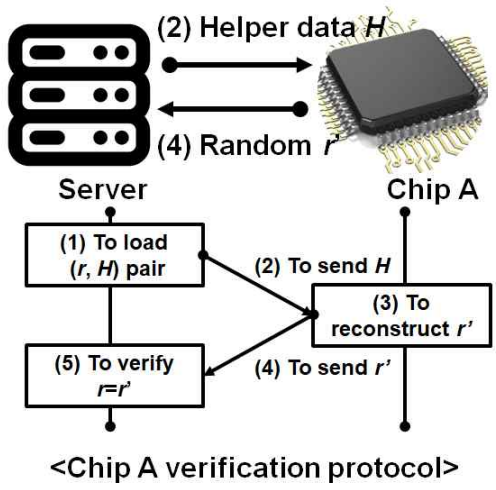
(그림 3)과 (그림 4)는 PUF를 이용한 IC(Integrated Circuit) 인증 기능 프로토콜 개념도를 보여준다. IC 인증 기능 프로토콜이란 서버와 칩 간의 통신을 통해 IC 인증 기능을 제공하는 프로세스를 뜻한다. IC 인증 프로토콜은 IC 등록(registration)과 IC 검증(verification) 프로세스로 나눌 수 있다. IC 등록은 반도체 ID 정보를 서버에 등록하는 절차를 말하며, 서버로부터 난수 값을 수신하여 보조 데이터(helper data)를 서버에 제공하는 절차이다. IC 검증은 IC 등록을 통해 서버에 등록한 정보와 반도체 IC 정보가 일치하는지 확인하는 절차로, 서버로부터 보조 데이터를 입력받아 난수 값을 제공하는 절차이다. (그림 3)은 PUF를 이용한 IC 등록 절차를 그림으로 보여준다.



(그림 3) PUF를 이용한 IC 등록 절차

IC 등록은 아래와 같은 절차로 수행한다.

① 서버가 칩 A에게 난수 데이터를 전송한다.
② 칩 A는 수신한 난수 데이터와 PUF 응답으로부터 보조 데이터를 생성한다.
③ 칩 A는 생성한 보조 데이터를 서버에 전송하고, 칩은 난수 데이터와 보조 데이터 쌍을 저장한다.



(그림 4) PUF를 이용한 IC 인증 절차

IC 등록을 수행한 칩들은 IC 검증 절차를 통하여 IC 인증 보안 기능 수행이 가능하다. 즉, IC 검증 절차는 IC 등록 절차를 마친 후 수행이 가능하다. (그림 4)는 IC 검증 프로토콜을 보여준다. IC 인증은 아래와 같은 절차로 수행한다.

① 서버는 IC 등록에서 저장한 칩 A의 보조 데이터를 전송한다.
② 칩 A는 수신한 보조 데이터로부터 서버에서 IC 등록 때 제공한 난수 데이터를 복원한다.
③ 칩 A는 복원한 난수 데이터를 서버에 전송한다.
④ 서버는 난수 데이터 무결성을 검증하여 IC 인증 성공/실패 여부를 결정한다.

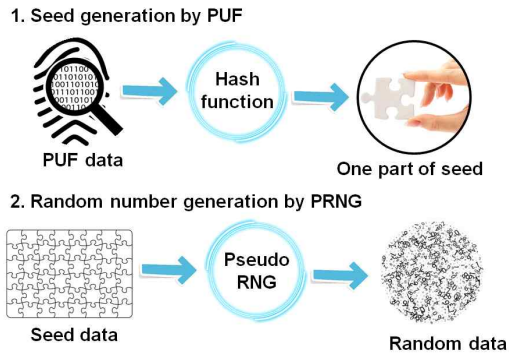
IC 인증 절차 결과 성공하면 IC 등록의 칩과 같은 칩이라는 것을 확인할 수 있다.

지금부터 PUF를 이용한 PRNG 시드 생성 기능을 설명하려고 한다. (그림 5)는 PUF를 이용한 PRNG 시드 생성 절차 개념도를 보여준다. PUF는 반도체 지문 기능을 가지므로 반도체 칩마다 PUF의 특이성을 가진다. 즉, PUF는 반도체 칩마다 다른 출력을 가지고 있다. 이런 다른 출력을 가지는 특성을 활용하여 의사

난수발생기의 시드로 활용이 가능하다. 의사난수발생기는 시드라는 입력을 받아 난수를 생성하는 장치이다. 의사난수발생기의 난수 발생의 핵심은 시드를 다른 값으로 인가하여 항상 다른 난수를 생성해야 한다는 것이다. PUF의 특이성 특성은 칩마다 다른 시드를 발생할 수 있도록 만들어준다. 즉, PUF를 통하여 생성한 시드를 통하여 보안 시스템 내 지속적인 난수 생성이 가능하다.

아래 절차들은 PUF를 이용한 PRNG 시드 생성 절차이다.

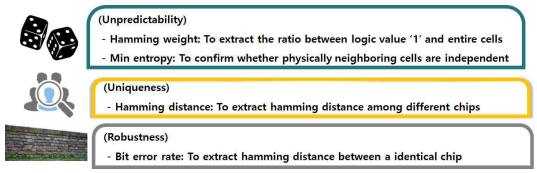
① PUF 응답 데이터를 해시 암호에 입력으로 사용
② 해시 출력을 의사난수발생기의 시드로 활용
③ 시드 데이터를 의사난수발생기의 입력으로 사용
④ 의사난수발생기의 출력을 난수로 활용



(그림 5) PUF를 이용한 PRNG 시드 생성 기능

2. PUF 특성평가 지표 목록

PUF는 반도체 지문 기능을 하는 보안 소자이다. 구현한 PUF가 반도체 지문의 보안 기능을 하기 위해서는 예측 불가능성, 특이성, 견고성 특성이 필요하다. 특성평가 지표 선정은 다양한 PUF 특성 평가 방식을 인용 및 참고하여 특성 평가 지표들을 마련하였다[1][8][17][18][19]. (그림 6)은 PUF 특성평가 지표 목록들을 보여준다. 예측 불가능성 특성 평가는 해밍 웨이트와 최소 엔트로피 정량적 지표를 통해 수행한다. 특이성 특성 평가는 인트라 칩 인터 칩 해밍 거리 비교를 통하여 정량적 평가를 수행한다. 견고성 특성 평가는 인트라 칩 해밍 거리(bit error rate) 정량적 계산을 통하여 수행한다.



(그림 6) PUF 특성평가 지표 목록

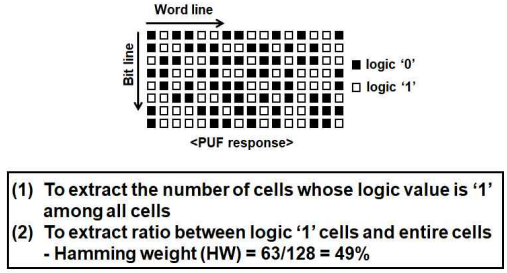
3. 예측 불가능성 특성 평가

예측 불가능성은 PUF 입력/출력(도전/응답)을 측정하기 전에 외부에서 시뮬레이션 혹은 기계 학습을 통해서 PUF 도전/응답을 예측할 수 없는 특성을 뜻한다. 예측 불가능성은 통계적으로 논리 0/1 중 편향된 논리 값을 가지지 않아야 한다. 또한 물리적 위치에 관계없이 높은 복잡성(entropy)를 가져야 한다. 예측 불가능성 특성 평가를 위해 해밍 웨이트와 최소 엔트로프 지표들을 활용한다.

3.1 해밍 웨이트

해밍 웨이트는 단일 칩 내 PUF 전체 비트 중 논리 1의 출력 비율을 보여준다. 즉, 인트라 칩 해밍 웨이트를 측정한다. 해밍 웨이트의 이상 결과(Ideal value)는 0.5(50%)이다. (그림 7)은 해밍 웨이트 특성평가 절차를 보여준다.

① 단일 칩의 PUF 출력 중 논리 값 1 셀 수를 계산
② 전체 셀 수 중 논리 값 1인 셀 수의 비율을 계산



(그림 7) 해밍 웨이트 계산 절차

3.2 최소 엔트로피

최소 엔트로피는 PUF 응답이 물리적 위치에 관계없이 예측 불가능한 응답을 가지는지 측정하는 특성 평가 항목이다. 해밍 웨이트와 같이 단일 칩 내 인트라

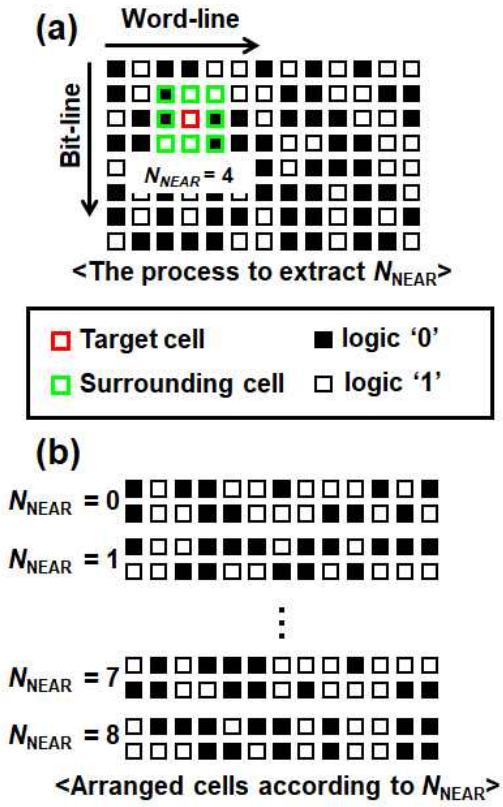
칩에서 특성을 추출하는 방법이다. 물리적으로 가까운 SRAM 셀들 사이에 충분한 복잡성(entropy)을 보유하고 있는지 확인하는 지표이다. (그림 8)은 최소 엔트로피 계산 절차를 보여준다.

① 단위 셀의 근접한 8개의 셀 중 논리 값 1의 개수(N_{NEAR}) 추출 ($0 \le N_{NEAR} \le 8$)

② N_{NEAR} 추출 후, 단위 셀의 논리 값이 1인지 0인지 확인

③ ①-②의 과정을 모든 셀의 반복하여 같은 N_{NEAR} 값을 가지는 셀들의 엔트로피를 추출

④ 추출된 엔트로피 값 중 최소 값을 추출

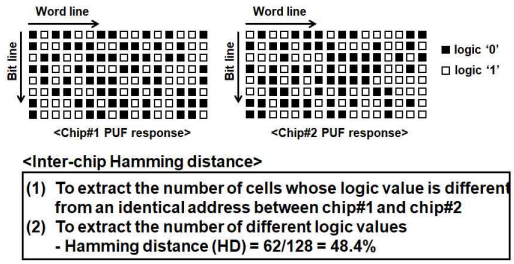


(그림 8) 최소 엔트로피 계산 절차

4. 특이성 특성 평가

4.1 해밍 거리

특이성이란 서로 다른 칩 PUF 응답이 상관관계가 없음을 보여주는 특성이다. 사람의 지문을 예로 들면 사람마다 특이성(uniqueness)을 갖는 지문 모양을 가지는 특성을 뜻한다. PUF는 예측 불가능한 공정상의 편차로 인해 칩마다 다른 논리 값들을 만들어내는 반도체 지문 역할을 한다. 칩들이 상관관계가 없이 독립적인 출력을 가지고 있는 것은 PUF를 반도체 지문을 활용하기에 중요한 평가 요소이다. 특이성은 인터 칩 해밍 거리와 인트라 칩 해밍거리를 계산하여 판정한다. 다른 칩 PUF 출력에 해밍 거리를 인터 칩 해밍 거리라고 하고, 같은 칩 PUF 출력에 해밍 거리를 인트라 칩 해밍 거리라고 한다. (그림 9)는 인터 칩 해밍거리 계산 절차를 보여준다. (그림 10)은 인트라 칩 해밍거리 계산 절차를 보여준다.



(그림 9) 인터 칩 해밍거리 계산 절차

아래 절차는 인터 칩 해밍 거리 계산 절차를 보여준다.

① 다른 칩 Chip#1과 Chip #2의 PUF 응답 추출

② Chip#1과 Chip #2의 같은 주소 PUF 응답 사이의 해밍 거리를 계산

③ 전체 셀 수 와 해밍 거리의 비율을 계산

④ ①-③의 과정을 실험군 칩에 대하여 반복

아래 절차는 인트라 칩 해밍 거리 계산 방법 및 절차를 보여준다.

① 단일 실험 칩에 대하여 PUF의 최초 응답을 추출

② 실험 칩에 전원을 10초 이상 차단

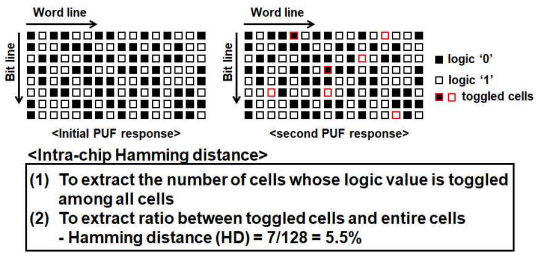
③ 실험 칩에 전원을 재인가하여 PUF 응답 재추출

④ ①과 ③ 과정에서 추출한 PUF 응답의 해밍 거리 계산

⑤ 전체 셀 수와 해밍 거리의 비율을 계산한다.

⑥ ①-⑤의 과정을 실험군 칩에 대하여 반복한다.

특이성은 합격 판정은 인트라 칩 해밍 거리의 최대 값과 인터 칩 해밍 거리의 최소 값을 비교하여 인트라 칩 해밍 거리의 최대 값이 인터 칩 해밍 거리의 최소 값보다 작으면 합격으로 판정할 수 있다.



(그림 10) 인트라 칩(비트 오류율) 계산 절차

5. 견고성 특성 평가

견고성은 같은 칩, 같은 입력의 PUF 출력이 항상 동일한 출력을 가짐을 의미하며 온도 및 전압과 같은 환경 변화에도 동일한 출력을 가지는 것을 포함한다. 특히, PUF의 견고성 특성은 중요 정보의 안전한 저장 및 IC 인증 기능에서 보안 기능 가용성(availability)에 있어서 가장 중요한 특성이다[1][8][17]. 견고성은 인트라 칩 해밍 거리(bit error rate)을 계산하여 특성 평가를 수행한다. 원칙적으로, PUF 보안 기능 적용을 위해 0%의 비트 오류율을 가져야 한다. 하지만, 실질적으로는 오류정정부호를 설계하여 오류정정 범위 내 비트 오류율를 허용한다. 즉, 비트 오류율 합격 기준은 시스템 내 구현한 오류정정부호 규격에 따라 달라진다.

5.1 비트 오류율

특이성 시험 절차에서 수행한 인트라 칩 해밍거리와 같은 시험 절차로 비트 오류율을 계산한다. (그림 10)은 PUF 견고성 시험 항목인 비트 오류율 시험 절차를 보여준다. 아래 절차는 비트 오류율 계산 절차를 보여준다.

① 단일 칩에 대하여 PUF의 최초 응답을 추출한다.
② ① 과정에 단일 칩에 전원을 10초 이상 차단한다.
③ ①, ② 과정에 단일 칩에 전원을 재인가하여 PUF의 응답을 다시 추출한다.
④ ①과 ③ 과정에서 같은 주소에서 추출한 PUF 응답의 해밍 거리를 계산한다.
⑤ 전체 셀 수와 해밍 거리의 비율을 계산한다.
⑥ ①-⑤의 과정을 실험군 칩에 대하여 반복한다.

6. 결론

물리적 복제 불가능 회로(PUF)가 보안 기능 실현을 하기 위해서는 예측 불가능성, 특이성, 견고성 특성이 필요하다. 이는 PUF가 인체에 지문과 같이, 반도체 칩에서 지문 기능을 수행하기 위해 필요한 특성들이다. 이 연구에서는 예측 불가능성, 특이성,. 견고성 특성 평가를 위한 평가 항목을 도출하고 정량적 계산 방법을 정리하였다. 예측 불가능성은 해밍 웨이트, 최소 엔트로피 평가 항목을 통하여 PUF 출력이 시뮬레이션이나 예측 알고리즘에 의해 예측 가능성을 없는지 정량적으로 확인할 수 있게 해준다. 특이성은 인터 칩 해밍 거리와 인트라 칩 해밍 거리 정량 지표를 통하여 집적 회로마다 독특성을 가지는지 정량적으로 확인할 수 있게 해준다. 견고성은 비트 오류율 지표를 통하여 PUF의 가용성을 정량적으로 확인할 수 있게 해준다. 이 연구 결과를 적용하여 구현한 PUF가 반도체 지문의 기능을 갖추고 있는지 정량적으로 평가하고 비교할 수 있도록 도와준다.

참고문헌

[1] M. S. Kim, S. Kim, S. K. Yoo, B. S. Lee, J. M. Yu, I. W. Tcho, and Y. K. Choi, "Error reduction of SRAM-based physically unclonable function for chip authentication," International Journal of Information Security, 1-12, 2023.

[2] U. Rührmair, and M. V. Dijk. "PUFs in security protocols: Attack models and security evaluations," 2013 IEEE symposium on security and privacy, 2013.

[3] K. Lounis, and Z. Mohammad. "T2T-MAP: A PUF-based thing-to-thing mutual authentication protocol for IoT," IEEE Access Vol. 9, 137384-137405, 2021.

[4] W. Liang, S. Xie, D. Zhang, X. Li, K. -C. Li, "A mutual security authentication method for RFID-PUF circuit based on deep learning," ACM Transactions on Internet Technology (TOIT), Vol. 22, No. 2, 1-20, 2021.

[5] R. Arppe, and T. J. Sørensen. "Physical unclonable functions generated through chemical

methods for anti-counterfeiting," Nature Reviews Chemistry, Vol. 1, No. 4, 0031, 2017.

[6] A. Kumar, R. Soha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," Journal of Network and Computer Applications, Vol. 204 pp. 103414, 2022.

[7] S. Shruti, and D. Sakhare. "A review—hardware security using puf (physical unclonable function)," ICCCE 2019: Proceedings of the 2nd International Conference on Communications and Cyber Physical Engineering. 2020.

[8] M. -S. Kim, D. -I. Moon, S. -K. Yoo, S. -H. Lee, and Y. -K. Choi, "Investigation of physically unclonable functions using flash memory for integrate dcircuit authentication," IEEE Transactions on nanotechnology, Vol. 14, No. 2, pp.384-389, 2015.

[9] S. U. Hussain, S. Yellapantula, M. Majzoobi, F. Koushanfar, "BIST-PUF: Online, hardware-based evaluation of physically unclonable circuit identifiers," 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2014.

[10] R. Wang, G. Selimis, R. Maes, and S. Goossens, "Long-term continuous assessment of SRAM PUF and source of random numbers," 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2020.

[11] R. L. Sembiring, R. R. Pahlevi, and P. Sukarno. "Randomness, uniqueness, and steadiness evaluation of physical Unclonable functions," 2021 9th International Conference on Information and Communication Technology (ICoICT), 2021.

[12] J. Li, T. Yang, and M. Seok. "A technique to transform 6T-SRAM arrays into robust analog PUF with minimal overhead," 2017 IEEE International Symposium on Circuits and Systems (ISCAS), 2017.

[13] J. Delvaux, D. Gu, D. Schellekens, I. Verbauwhede, "Helper data algorithms for PUF-based key generation: Overview and analysis," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 34, No. 6, pp.889-902, 2014.

[14] M. Taniguchi, M. Shiozaki, H. Kubo, and T. Fujino, "A stable key generation from PUF responses with a Fuzzy Extractor for cryptographic authentications," 2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE). 2013.

[15] W. Liang, S. Xie, J Long, K. -C. Li, D. Zhang, and K. Li,. "A double PUF-based RFID identity authentication protocol in service-centric internet of things environments," Information Sciences, Vol. 503, pp.129-147, 2019.

[16] S. Kalanadhabhatta, D. Kumar, K. K. Anumandla, S. A. Reddy, and A. Acharyya, "PUF-based secure chaotic random number generator design methodology," IEEE transactions on very large scale integration (VLSI) systems, Vol. 28, No. 7, pp. 1740-1744, 2020.

[17] S. Katzenbeisser, U. Kocabas, V. Rozic, A. -R. Sadeghi, I. Verbauwhede and C. Wachsmann, "PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," Cryptographic Hardware and Embedded Systems - CHES 2012: 14th International Workshop, 2012.

[18] P. Koeberl, J. Li, A. Rajan, C. Vishik, and W. Wu, "A practical device authentication scheme using SRAM PUFs," Trust and Trustworthy Computing: 4th International Conference, TRUST, 2011.

[19] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. V. D. Sluis, and V. V. D. Leest, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," Proceedings of the ESSCIRC (ESSCIRC). 2012.

〔저자소개〕

김 문 석 (Moon-Seok Kim)
2011년 2월 중앙대학교 학사
2013년 2월 한국과학기술원 석사
2022년 2월 한국과학기술원 박사
2023년 9월~현재 국립한밭대학교
반도체시스템공학과 조교수
email : mskim@hanbat.ac.kr