

# 신뢰도 신호를 갖는 RC 회로 기반 PUF 설계.

## (A Physically Unclonable Function based on RC Circuit with a Confidence Signal)

최 지원<sup>1)</sup>, 김 범 중<sup>1)</sup>, 이 형 규<sup>2)\*</sup>, 이 중 회<sup>3)\*</sup>, 박 아 란<sup>4)</sup>, 이 규 호<sup>4)</sup>, 장 우 현<sup>4)</sup>  
(Jione Choi, Beomjoong Kim, Hyung Gyu Lee, Junghee Lee, Aran Park, Gyuhoo Lee, and Woo Hyun Jang)

**요 약** PUF(physically unclonable function)는 회로의 자연적인 변이를 이용하여 복제 불가능한 난수를 생성하는 회로이다. 통제가 어려운 변이를 활용하기 때문에 예측이 불가능하여 완전한 난수를 생성할 수 있지만 환경 변수에 의해 영향을 받는다는 문제가 있다. 본 논문에서는 이를 해결하기 위해 신뢰도 신호를 생성하는 PUF를 제안한다. 두 회로의 시간상수(time constant)의 차이를 이용한 PUF를 설계, 구현하여 서로 다른 PUF에서는 충분히 다른 출력이 나오고 같은 PUF에서는 온도가 변하여도 출력값의 큰 차이가 없음을 검증하였다. 오류정정코드를 사용하는 기존 기술 대비 700배 이상 작은 오버헤드로 동등한 수준의 신뢰도를 보장한다.

**핵심주제어:** RC회로, PUF, 신뢰도

**Abstract** A physically unclonable function (PUF) is a circuit that generates random numbers by exploiting natural variation. Since it utilizes variations, which cannot be fully controlled, it can be used to generate true random numbers, but environment change may distort the output. In this paper, we propose a PUF with a confidence signal. We designed a PUF that exploits the difference of the time constant of the circuit and verified that different PUFs generate distinct outputs and the same PUF keeps generating similar outputs regardless of the temperature change. Compared to the existing technique, which employs an error correction code, the proposed technique offers the same level of reliability at the 700 times smaller overhead.

**Keywords:** RC circuit, Physically Unclonable Function, Confidence

### 1. 서 론

PUF(physically unclonable function)는 자연적인 변이(variation)을 이용하여 난수를 발생시키는 회로이다. 논리적으로는 동일한 회로이지만 변이 때문에 전기적인 특성이 조금씩 달라지는 현상을 이용한다. 변이를 완벽히 통제할 수 없기 때문에 발생하는 현상이다. 따라서 회로를 복제하더라도 통제할 수 없는 변이 때문에 완벽히 동일한 출력을 얻을 수 없게 된다.

\* Corresponding Authors: j\_lee@korea.ac.kr, hglee@duksung.ac.kr  
Manuscript received May 03, 2022 / revised June 09, 2022 / accepted July 18, 2022

1) 고려대학교 정보보호대학원

2) 덕성여자대학교 소프트웨어전공, 공동교신저자

3) 고려대학교 정보보호대학원, 공동교신저자

4) LIG 넥스원

Table 1 Representative examples of PUF

Measurement	Examples	Representative Papers
Delay	Arbiter PUF	Daihyun Lim, J. et al. (2005)
	Ring Oscillator PUF	G. E. Suh and S. Devadas. (2007)
Memory	SRAM PUF	M. Kassem, et al. (2010)
	RRAM PUF	A. Chen (2015)
Optical	Optical PUF	X. Lu, et al. (2018)
Metastability	Butterfly PUF	S. S. Kumar, et al. (2008)

PUF의 복제 불가능한 성질 때문에 보안에 활용도가 높다. 완전 난수 생성기(true random number generator), 인증을 위한 식별자 생성, 암호키 생성 등에 활용된다.

PUF를 난수 생성에 활용할 때는 문제 없으나, 식별자, 암호키 생성에 활용하려면 같은 회로에서는 항상 같은 출력이 생성되어야 한다. 만약 한 비트라도 다른 값이 생성되면 식별자나 암호키가 달라져서 정상적인 회로임에도 인증에 실패하는 문제가 생긴다.

PUF는 미세한 환경 변화에도 영향을 받기 때문에 같은 회로라도 항상 같은 값을 보장하기 어렵다. 기존의 연구에서는 ECC(error correction code)를 사용하여 달라진 값을 복구하는 방식을 사용하였다. 이 방식은 복구 가능한 비트의 수를 늘리려면 복잡한 ECC를 사용해야하므로 후처리에 큰 성능과 하드웨어 비용을 지불해야하는 문제가 있다.

본 논문에서는 이 문제를 해결하기 위해 신뢰도(confidence)를 측정하는 방식을 제안한다. 본 논문에서 제안하는 PUF는 두 회로의 시간상수(time constant)의 차이를 이용하는 방식으로 시간상수의 차이가 충분히 큰지 여부를 알려주는 신뢰도 신호를 함께 생성한다. 식별자나 암호키 생성을 할 때 여러 비트를 생성하여 그 중에서 신뢰도가 큰 비트만 사용하면 잡음으로 인해 출력값이 달라질 가능성을 크게 낮출 수 있다. 신뢰도를 이용한 방식은 기존 ECC에 비해 성능과 하드웨어 비용이 매우 작다는 장점이 있다.

2장에서 기존 PUF와 관련된 연구를 살펴보고 3장에서 제안하는 PUF를 설명한다. 4장에서 실험을 통해 검증한 내용을 설명한 후 5장에서 결론을 맺는다.

## 2. 관련연구

기존 대표적 PUF는 Table 1에 요약되어 있다. PUF는 지금까지 워낙 많은 연구가 진행되어 왔기 때문에 여기서 모든 논문을 포괄적으로 다루는 것은 불가능하다. Table 1는 대표적인 PUF의 예시만 보여준다.

PUF를 구현하기 위해 다양한 물리적 현상을 이용할 수 있다. 가장 대표적인 방식이 지연시간(delay)의 차이를 이용하는 방식이다. 이 방식은 특정 경로의 신호 전달 속도가 미세하게 다른 현상을 이용한다. 대표적인 예로 arbiter PUF(Daihyun Lim, J. et al. (2005)), ring oscillator PUF(G. E. Suh and S. Devadas. (2007)) 등이 있다. 메모리의 초기 값이나 저장물질의 미세한 차이를 이용한 방식도 연구가 많이 되어 왔다(M. Kassem, et al. (2010), A. Chen (2015)). 이 외에도 광학적 성질을 이용하거나(X. Lu, et al. (2018)), metastability를 이용하는 방법(S. S. Kumar, et al. (2008))과 같이 다양한 물리적 현상을 이용하여 PUF를 구현하는 연구들이 있었다.

PUF 출력이 항상 같을 필요가 있는 응용들을 위해 ECC를 활용하는 방식이 많이 사용된다(S. Satpathy et al.(2017)). 평소와 다른 출력을 예러로 취급하여 ECC를 통해 교정하는 방식이다. ECC도 여러 가지 방식이 있기 때문에 사용하는 ECC의 종류에 따라 세분할 수 있지만 PUF에서 얼마나 많은 예러가 발생할지 예측이 어려워 복잡한 ECC가 필요하게 된다.

SRAM의 경우에는 안정적인 값이 생성되는 셀인지 여부를 미리 판단하는 방법이 연구되기

도 하였다(A. Alheyasat, et. al (2020)). 이 방법은 통계적으로 예측하는 간접적인 방법으로 안정적인 출력을 보장하지는 않는다.

### 3. RC PUF 설계

#### 3.1 신뢰도

본 논문에서 사용하는 PUF는 물리적 현상의 측정값 두 개를 비교하여 둘의 차이에 따라 출력을 다르게 만드는 방식을 사용한다. 절대값을 사용하는 방식에 비해 차이를 사용하는 방식은 환경적 요인에 영향을 덜 받는다는 장점이 있다. 환경적 요인은 두 측정값에 유사한 영향을 주기 때문이다.

물리적 현상의 측정값은 온도와 같은 환경적 요인에 따라 일시적으로 잡음이 포함될 수 있다. 잡음은 일시적인 현상이지만 PUF에서 활용하는 변이는 영구적인 현상이다. 이를 개념적으로 표현하면 Fig. 1과 같이 표현할 수 있다.

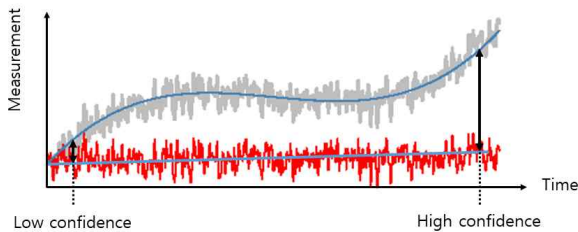


Fig. 1 Noise versus variance

본 논문에서는 일시적인 잡음(noise)과 영구적인 변이(variance)를 구분한다. Fig. 1의 오른쪽 high confidence로 표시된 부분처럼 변이가 충분히 크면 잡음이 섞여도 두 값의 우위가 뒤바뀌는 경우가 매우 드물다. 그러나 왼쪽의 low confidence로 표시된 부분처럼 변이가 충분히 크지 않다면 잡음에 의해 측정값의 우위가 자주 바뀔 수 있다. 따라서 두 측정값의 차이가 충분히 크면 신뢰도가 높다고 판단할 수 있다.

본 논문에서 제안하는 PUF는 변이가 충분히 큰 PUF의 출력만 활용하여 PUF 출력의 안정

성을 보장한다는 것이 다른 PUF와 차별되는 가장 큰 특징이다.

#### 3.2 설계

본 논문에서 제안하는 PUF는 시간상수(time constant)의 차이를 이용한 PUF이다. PUF에 사용될 수 있는 소자는 생산할 때 통제 불가능한 요인이 있어야 한다. 또한, 이 통제 불가능한 요인이 시간상수값에 영향을 줘야 하며, 환경적 요인에 의한 영향을 받지 않을수록 좋다. 두 RC(resistor capacitor)회로의 시간상수의 차이를 이용하면 환경 변화가 두 회로에 비슷한 영향을 주기 때문에 환경적 요인으로 출력이 변하는 것을 최소화 할 수 있다.

제안하는 PUF는 같은 용량 두 개의 축전기(C)와 같은 저항 값인 두 개의 저항(R)을 사용하여 두 개의 RC 회로에서 축전기 방전 속도 차이를 PUF로 활용한다. 실제로는 회로의 여러 소자들에 크고 작은 RC 성분이 있기 때문에 이 모든 성분들의 변이가 PUF 출력에 영향을 주게 된다.

Fig. 2에 두 RC 회로의 추상화된 회로도도 나와 있다. 전원과 연결된 트랜지스터는 축전기에 충전기를 위한 스위치이다. 축전기를 완전히 충전시킨 후 스위치를 열면 방전이 시작된다. 두 RC회로의 시간상수값(R과 C의 곱)에 따라 방전 속도가 달라진다. 제안하는 PUF는 이 방전 속도의 차이를 이용한다.

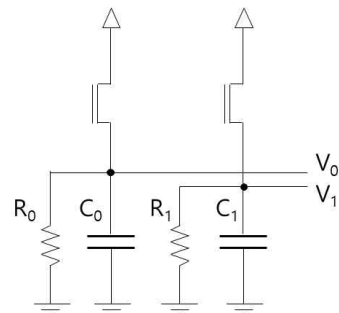
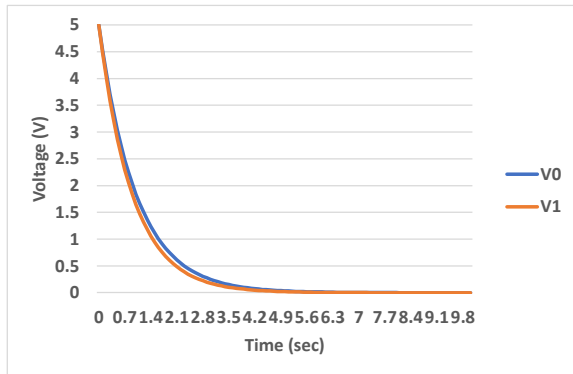


Fig. 2 Abstract RC circuit

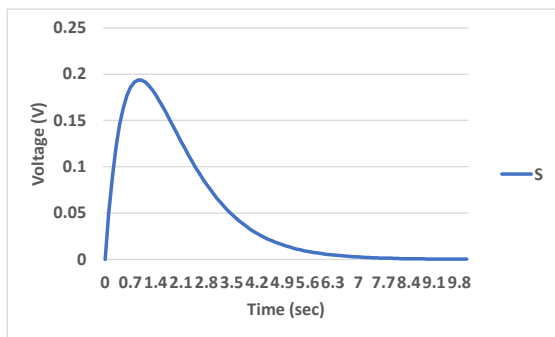
각 회로에서 나오는 출력 전압을 각각  $V_0$ ,  $V_1$  이라고 하면 Fig. 3(a)와 같은 그래프를 관측할

수 있고 그 두 값의 차이는 Fig. 3(b)와 같다.

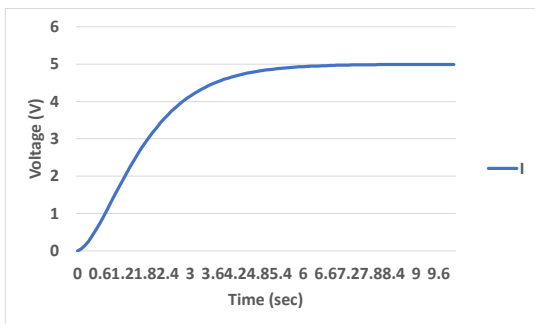
Fig. 3의 예에서는  $V_0$ 가 더 느리게 방전되어  $V_0 - V_1$ 이 양수이다. 만약  $V_0$ 이 더 빠르게 방전된다면  $V_0 - V_1$ 은 음수가 된다. 제안하는 PUF는  $V_0 - V_1$ 가 음수인지 양수인지에 따라 출력값을 결정한다.



(a) Out of the RC circuit ( $V_0, V_1$ )



(b) Difference of  $V_0$  and  $V_1$  ( $S = V_0 - V_1$ )



(c) Output of the integrator ( $I = \int V_0 - V_1$ )

Fig. 3 Simulated outputs

음수인지 양수인지 안정적으로 판별하기 위해 차이값을 적분하는 방식을 사용한다. 적분된 결과가 음수인지 양수인지에 따라 출력값을 결정한다. 적분기 출력값의 예가 Fig. 3(c)에 나와 있다.

적분기 출력값은 두 회로 방전 속도의 차이에 비례하여 커진다. 따라서 적분기 출력값의 절대값이 커지면 두 회로의 방전 속도의 차이가 충분히 크다는 뜻이다. 제안하는 PUF는 적분기의 출력값을 임계치와 비교하여 그보다 크면 신뢰도 신호를 1로 생성하고 그렇지 않으면 0으로 생성한다.

### 3.3 분석

이번 절에서는 3.2절의 설계의 배경이 되는 분석 모델(analytical model)을 설명한다. 먼저,  $V_0$ 와  $V_1$ 은 각각 아래의 수식으로 표현할 수 있다.

$$V_0(t) = Ve^{-\frac{t}{\tau_0}} \quad (1)$$

$$V_1(t) = Ve^{-\frac{t}{\tau_1}} \quad (2)$$

여기서  $V$ 는 입력 전원,  $t$ 는 시간,  $\tau_0$ 는 첫 RC 회로의 저항값과 축전기값을 곱한 시간상수를 의미한다.  $\tau_1$ 는 두 번째 회로의 시간상수이다.

$V_0$ 와  $V_1$ 의 차이를 적분한 최종값  $I$ 는 아래 수식으로 표현된다. 두 값의 차  $S$ 는 Fig. 3(b)에서 볼 수 있듯이 시간이 지나면 0으로 수렴하고 절대값은 변하여도 양수인지 음수인지가 변하지는 않는다.  $S$ 를 적분하게 되면 단조 증가를 하거나 단조 감소를 하고 시간이 지나면서 특정값으로 수렴한다. 수렴된 값을 구하기 위해 0에서 무한대까지 적분한 값을 구하였다.

본 수식을 통해 적분기의 출력값은 두 RC 회로의 시간상수의 차이에 비례한다는 것을 확인할 수 있다.

$$\begin{aligned} I &= \int_0^{\infty} (Ve^{-\frac{t}{\tau_0}} - Ve^{-\frac{t}{\tau_1}}) dt \quad (3) \\ &= \left[ -\tau_0 Ve^{-\frac{t}{\tau_0}} + \tau_1 Ve^{-\frac{t}{\tau_1}} \right]_0^{\infty} \\ &= (\tau_1 - \tau_0) V \end{aligned}$$

### 3.4 구현

제안하는 PUF는 Fig. 4에 도식화된 회로를 이용하여 구현되었다.  $V_0$ 와  $V_1$ 의 차이를 구하기 위한 감산기(subtractor)를 거쳐 적분기(integrator)를 통해 출력이 생성되고 적분기의 출력과 역치(threshold)를 비교하여 신뢰도 신호가 생성된다. 적분기 출력은 음수 또는 양수가 나올 수 있는데 음수와 양수를 하나의 비교기(comparator)에서 처리할 수 없어 두 개의 비교기를 사용하였다. 실제 구현에 사용된 회로도도 Fig. 5에 나와 있다.

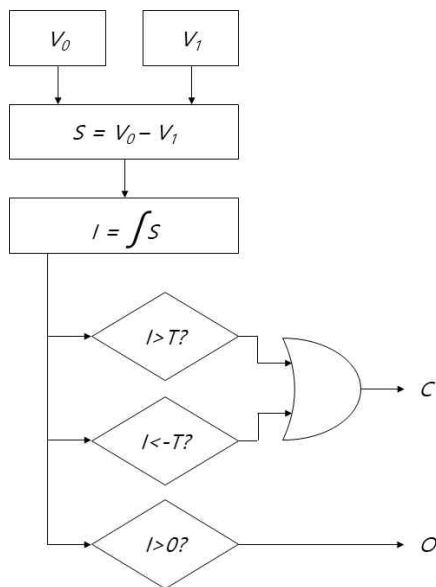


Fig. 4 Conceptual block diagram of the proposed PUF

### 4. 실험

Fig. 5의 회로를 실제 PCB(printed circuit board)에 구현하여 결과를 확인하였다. 감산기와 적분기 구현을 위해 사용한 op-amp (operational amplifier)는 Analog Devices사의 OP07이고 수동 소자들은 Fig. 5 회로도에 나와 있는 값을 사용하였다. 실제 제작하여 조립한 PCB의 사진이 Fig. 6에 나와 있다.

실험을 위해 하나의 보드에 하나의 PUF를 구현하였지만 실제 사용 환경에서는 여러 비트의 출력이 필요하므로 하나의 보드에 여러 PUF를 구현하게 된다.

본 논문을 위한 실험에서는 총 4개의 PUF를 구현하였다. 각 PUF에서 발생하는 값이 랜덤한지 확인하기 위해 적분기의 출력값을 측정하였다. 그 결과가 Fig. 7이다. 측정 오차 및 환경 변화에 의해 출력값이 미세하게 변화하기 때문에 최소값과 최대값을 막대로 표시하였다.

실험 결과를 보면 4개 PUF의 값이 모두 오차 범위 밖으로 큰 차이를 보임을 알 수 있다. 즉, PUF의 출력이 충분히 랜덤한 것을 확인할 수 있다.

다음으로 신뢰도 신호의 임계값을 결정하기 위해 각 PUF의 값의 변화를 측정하였다. 여러 환경 변수가 출력값에 영향을 줄 수 있지만, 온도 변화가 가장 큰 영향을 준다는 것이 일반적으로 알려진 사실이다(M. Kaur(2018)). 따라서, 본 논문에서는 온도 변화에 대한 영향을 분석하

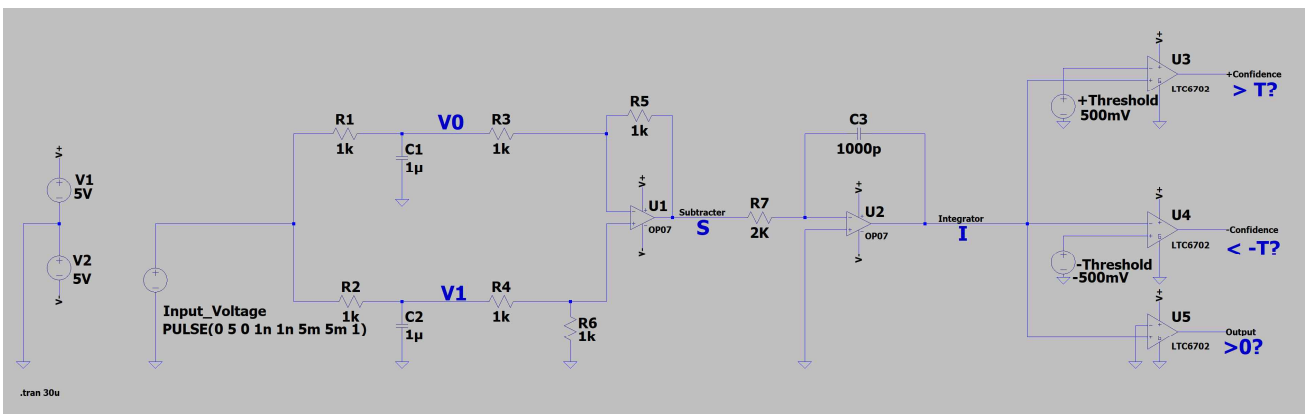


Fig. 5 Circuit implementation of the proposed PUF

었다. PUF의 온도 변화를 측정하기 위해 Fig. 8 과 같이 적외선 온도계를 사용하였다.



Fig. 6 PUF implementation on PCB.

나의 op-amp는 최소 3개의 트랜지스터와 1개의 다이오드, 많게는 20개의 트랜지스터로 구현된



Fig. 8 Temperature measurement.

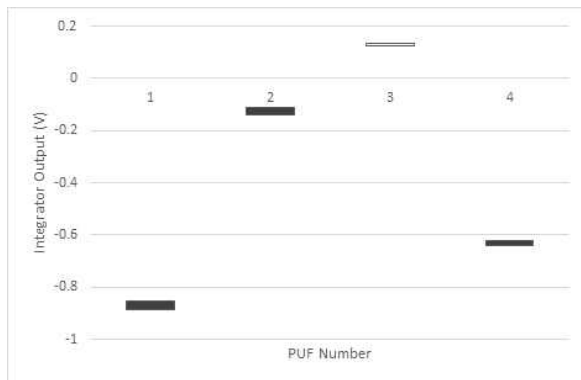


Fig. 7 The output from the integrator of each PUF.

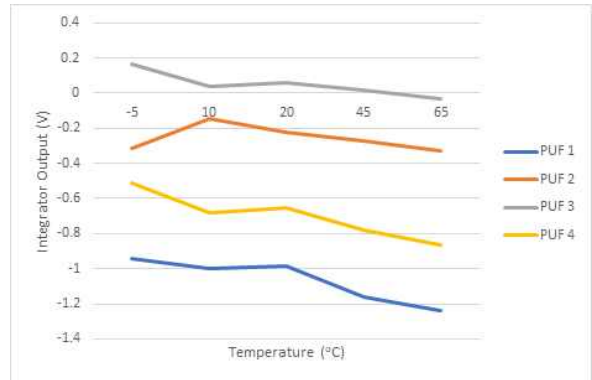


Fig. 9 Variation of the integrator output with temperature change.

각 PUF를 냉장고와 헤어드라이기를 이용하여 온도를 변화시키고 적분기의 출력값을 측정하였다. Fig. 9가 그 결과이다. Fig. 9의 결과는 최소값만 표시하였으나 최대값도 본 결과와 크게 다르지 않았다. 변화량의 최대 크기는 1번 PUF가 65도일 때 0.259V이다. 이를 바탕으로 임계값을 0.3V로 설정할 수 있고, 이 경우 PUF 2와 3의 값은 신뢰도가 낮아 활용이 어렵다고 판단할 수 있다.

본 실험에서는 PUF를 상온(20 °C)에서 주로 사용하고 가능한 온도의 범위가 -5 °C에서 65 °C라고 가정하고 임계값을 결정하였다. 임계값을 결정하는 방법은 실제 사용 환경에 따라 달라질 수 있다.

제안하는 PUF는 출력의 신뢰도 판단을 위해 2개의 비교기와 1개의 OR 게이트가 필요하다. 각 비교기는 op-amp를 이용하여 구현하는데 하

다 (Learning About Electronics(2018)). 따라서 제안하는 PUF는 신뢰도 판단을 위해 op-amp 2개에 해당하는 40개의 트랜지스터와 OR 게이트 하나 구현을 위한 6개의 트랜지스터, 총 46개 정도의 트랜지스터가 필요하다.

반면, ECC를 사용하는 S. Satpathy et al. (2017) 경우에는 BCH code를 사용하였는데 H. Yoo et. al.(2013) 논문의 결과에 따르면 하드웨어 구현에 9,067 게이트가 필요한 것으로 보고 되었으며 이를 트랜지스터의 개수로 환산하면 36,268개로 제안하는 PUF와 700배이상 차이가 난다.

## 5. 결론

본 논문에서는 출력값이 안정적인지를 판단할

수 있는 신뢰도 신호를 생성하는 PUF를 제안하였다. 제안하는 PUF는 두 RC 회로의 시간상수의 차이를 이용한다. 두 RC 회로를 충전해 놓고 동시에 방전시키면 시간상수의 차이로 인해 방전되는 속도가 달라진다. 두 값의 차이를 감산기를 이용하여 계산하고 적분기를 통해 누적된 값을 측정한다. 적분기의 출력은 시간상수의 차이에 비례하기 때문에 이 값이 충분히 크면 출력값이 안정적이라고 판단하고 신뢰도 신호를 생성한다. 제안하는 방법은 오류정정코드를 사용하는 기존 기술에 비해 700 이상 작은 오버헤드로 동일한 수준의 안정성을 보장한다.

신뢰도 신호의 임계값을 결정하기 위해 온도 밖에 실험을 해 보지 않았는데 다른 변수들(습도, 노화)에 의한 영향도 검증해 볼 필요가 있다. 또한 신뢰도 신호를 활용하는 방법도 단순히 신뢰도가 낮은 PUF의 출력값을 버리는 방법 외에 다른 방법은 없을지 추가적인 연구가 필요하다.

## References

- A. Alheyasat, G. Torrens, S. Bota and B. Alorda, "Bit-Cell Selection Analysis for Embedded SRAM-Based PUF," 2020 IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1-4, doi: 10.1109/ISCAS45731.2020.9180780.
- A. Chen, "Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions," in IEEE Electron Device Letters, vol. 36, no. 2, pp. 138-140, Feb. 2015, doi: 10.1109/LED.2014.2385870.
- Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, pp. 1200-1205, Oct. 2005, doi: 10.1109/TVLSI.2005.859470.
- G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9-14.
- H. Yoo, J. Jung, J. Jo and I. -C. Park, "Area-Efficient Multimode Encoding Architecture for Long BCH Codes," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 60, no. 12, pp. 872-876, Dec. 2013, doi: 10.1109/TCSII.2013.2281941.
- Learning About Electronics, "Why Does an Op Amp Need a Power Supply?," Online: <http://www.learningaboutelectronics.com/Articles/Why-does-an-op-amp-need-a-power-supply.php>
- M. Geis, K. Gettings and M. Vai, "Optical physical unclonable function," 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), 2017, pp. 1248-1251, doi: 10.1109/MWSCAS.2017.8053156.
- M. Kassem, M. Mansour, A. Chehab and A. Kayssi, "A sub-threshold SRAM based PUF," 2010 International Conference on Energy Aware Computing, 2010, pp. 1-4, doi: 10.1109/ICEAC.2010.5702285.
- M. Kaur, R. Rashidzadeh and R. Muscedere, "Reliability of Physical Unclonable Function under Temperature and Supply Voltage Variations," 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018, pp. 1008-1011, doi: 10.1109/MWSCAS.2018.8623849.
- P. Choi and D. K. Kim, "Design of security enhanced TPM chip against invasive physical attacks," 2012 IEEE International Symposium on Circuits and Systems (ISCAS), 2012, pp. 1787-1790, doi: 10.1109/ISCAS.2012.6271612.
- S. S. Kumar, J. Guajardo, R. Maes, G. Schrijen and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," 2008 IEEE International Workshop on

Hardware-Oriented Security and Trust, 2008, pp. 67-70, doi: 10.1109/HST.2008.4559053.

S. Satpathy et al., "A 4-fJ/b Delay-Hardened Physically Unclonable Function Circuit With Selective Bit Destabilization in 14-nm Trigate CMOS", IEEE JSSC, vol. 52, no. 4, pp. 940-949, 2017.

X. Lu, L. Hong and K. Sengupta, "CMOS Optical PUFs Using Noise-Immune Process-Sensitive Photonic Crystals Incorporating Passive Variations for Robustness," in IEEE Journal of Solid-State Circuits, vol. 53, no. 9, pp. 2709-2721, Sept. 2018, doi: 10.1109/JSSC.2018.2850941.



**최 지원 (Jione Choi)**

- 동덕여자대학교 컴퓨터학과 공학학사
- (현재) 고려대학교 정보보호대학원 정보보호학과 석사 박사 통합과정
- 관심분야: 파일시스템 보안, 하드웨어 보안

하드웨어 보안



**김 범 중 (Beomjoong Kim)**

- 고려대학교 물리학과 이학학사
- (현재) 고려대학교 정보보호대학원 정보보호학과 석사 박사 통합과정
- 관심분야: 사이버보안, 하드웨어보안



**이 형 규 (Hyung Gyu Lee)**

- 정회원
- 서울대학교 전기컴퓨터공학부 공학석사
- 서울대학교 전기컴퓨터공학부 공학박사
- (현재) 덕성여자대학교 소프트웨어전공 부교수
- 관심분야: 저전력 시스템 설계, 에너지 하베스팅, 저전력 메모리, 엣지 컴퓨팅



**이 중 희 (Junghee Lee)**

- 정회원
- 서울대학교 컴퓨터공학과 공학 학사
- 서울대학교 컴퓨터공학과 공학 석사
- 조지아공과대학교 전자공학과 공학박사
- (현재) 고려대학교 정보보호대학원 부교수
- 관심분야: 하드웨어 보안



**박 아 란 (Aran Park)**

- 고려대학교 정보보호학과 공학 석사
- (현재) LIG넥스원 C4I연구소, 사이버전연구팀 선임연구원
- 관심분야: 디지털포렌식, 사이버보안



**이 규 호 (Gyuhoo Lee)**

- 인하대학교 컴퓨터공학과 공학 학사
- 인하대학교 정보통신공학과 공학석사
- (현재) LIG넥스원 C4I연구소, 사이버전연구팀 수석연구원
- 관심분야: 무기체계 사이버보안, 하드웨어 보안, 안티템퍼링



**장 우 현 (Woo Hyun Jang)**

- 서강대학교 컴퓨터학과 공학 학사
- 서강대학교 컴퓨터공학과 공학 석사
- LIG넥스원 C4I연구소, 사이버전연구팀 선임연구원
- 관심분야: 무기체계 사이버 보안, 사이버 훈련