FPGA 기반의 그룹화된 링 오실레이터 PUF 성능 분석

이은채, 최소연, 양희훈, 유호영*
충남대학교 전자공학과
e-mail : *eclee.cas@gmail.com, sychoi.cas@gmail.com, hhyang.cas@gmail.com, hyyoo@cnu.ac.kr*

Performance Analysis of Grouped Ring-Oscillator PUF Based on FPGA

Eunchae Lee, Soyeon Choi, Heehun Yang, and Hoyoung Yoo*
Department of Electronics Engineering
Chungnam National University

Abstract

In this paper, the performance of conventional Ring-Oscillator PUF and grouped Ring-Oscillator PUFs is compared. Each Ring-Oscillator PUF is implemented using Xilinx's Artix-7 chip. The grouped Ring-Oscillator PUF with N oscillators showed improved uniformity as the number of Ring-Oscillators increased, but they also occupied larger area. The grouped Ring-Oscillator PUF with $N/2$ oscillators used the same number of Ring-Oscillators as the conventional Ring-Oscillator PUF, resulting in similar area occupation, but improved uniformity. The grouped Ring-Oscillator PUF with $N/4$ oscillators performed the best in terms of uniformity and area utilization. However, as the number of Ring-Oscillators decreased, the number of CRP significantly decreased, resulting in low reliability of the PUF performance metrics. The uniqueness was low for all four structures.

I. 서론

Field Programmable Gate Array (FPGA)의 사용이 증가함에 따라 FPGA에서의 보안 회로 구현에 대한 중요성 또한 높아졌다. FPGA 암호화 알고리즘에 사용되는 비밀 키는 battery-backed SRAM과 같은 휘발성 메모리 또는 플래시 메모리와 EEPROM과 같은 비휘발성 메모리에 저장된다. 하지만 해당 방식은 FPGA가 공격받는 경우, 비밀 키가 노출될 가능성이 존재한다 [1].

Physical Unclonable Function (PUF)은 이러한 문제를 해결하기 위해 도입된 새로운 형태의 보안 회로이다. 트랜지스터의 threshold voltage, 회로 요소 간 지연, 메모리 초기 상태와 같은 반도체 칩의 특성은 제조 공정에 따라 각 칩마다 차이가 존재한다. PUF는 칩의 제조 변동성을 활용하여 그림 1과 같이 각 칩에서만 유지되는 고유한 입출력 쌍인 Challenge-Response Pair (CRP)를 생성할 수 있다 [2]. Net delay, gate delay와 같이 회로에서 발생하는 지연 차이를 이용한 지연 기반 PUF에는 대표적으로 링 오실레이터 PUF가 존재한다 [3].

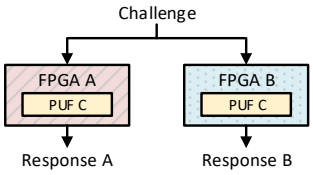

그림 1. PUF 동작

홀수 개의 인버터로 이루어진 링 오실레이터는 출력이 다시 입력으로 인가되며 비동기적으로 진동하는 루프를 생성한다. 이때 제조 변동성으로 인해, 각 링 오실레이터 출력의 주파수마다 차이가 발생한다. 이를 이용한 링 오실레이터 PUF는 각 링 오실레이터 출력의 주파수를 비교하여 CRP를 생성한다. 기존의 링 오실레이터 PUF [4]는 상관관계로 인해 PUF의 균일성이 저하된다. 따라서 본 논문에서는 기존의 링 오실레이터 PUF와 그룹화된 링 오실레이터 PUF [5]의 성능을 비교하여 그룹화된 링 오실레이터 PUF가 비밀 키 생성 및 인증에 더 적합하다는 것을 보이고자 한다.

II. 링 오실레이터 기반의 PUF

그림 3과 그림 4에 나타난 링 오실레이터 PUF는 입력 신호인 challenge를 통해 비교할 링 오실레이터 한 쌍을 선택하고, 카운터를 통해 일정 시간 동안 각 주파수의 상승 에지 수를 감지한다. 비교기는 두 카운터의 출력을 비교하여 0 또는 1의 단일 비트 response를 출력한다.

그림 3에 나타난 기존의 링 오실레이터 PUF [4]는 한 그룹 내에서 링 오실레이터 쌍을 선택하므로 출력이 상관관계를 갖는다. 예를 들어, 링 오실레이터 A가 B보다 빠르고, B가 C보다 빠르다면, A는 C보다 빠르다는 것을 알 수 있다. 따라서 기존의 링 오실레이터 PUF는 편향된 response를 출력한다. 하지만 그림 4의 그룹화된 링 오실레이터 PUF [5]는 각 그룹의 링 오실레이터를 하나씩 선택하여 비교하므로 상관관계를 갖지 않는 독립적인 response를 출력한다.

III. 구현 및 실험 결과

각 링 오실레이터 PUF는 최대 동작 주파수가 1.2GHz인 Xilinx 사의 Artix-7 칩을 이용하여 구현되었으며, 동작 주파수는 100MHz로 설정되었다. 본 논문에서 각 PUF의 성능 평가는 고유성, 균일성의 두 가지 지표로 이루어진다 [6].

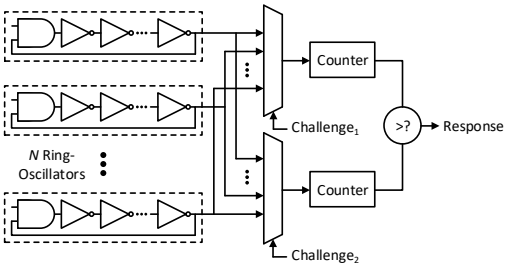

그림 3. N 개로 구성된 기존의 링 오실레이터 PUF [4]

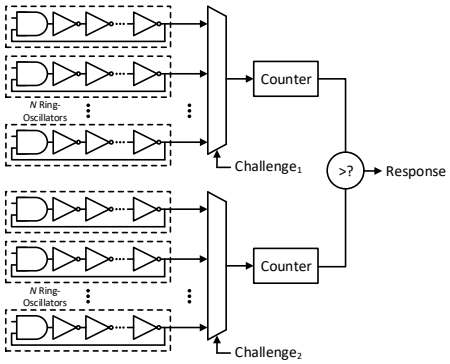

그림 4. N 개씩 그룹화된 링 오실레이터 PUF [5]

3.1 고유성 (Uniqueness)

고유성은 특정 칩을 고유하게 식별하는 능력을 나타낸다. k 개의 칩 중 i 번째 칩과 j 번째 칩 ($i \neq j$)이 동일한 challenge에 대해 각각 n 비트의 response R_i와 R_j 를 생성했을 때, R_i 와 R_j 사이의 hamming distance로 계산하며, 50%에 근접할수록 이상적이다.

$$Uniquness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\%, \quad (1)$$

3.2 균일성 (Uniformity)

균일성은 response에서 0과 1의 비율이 균일한 정도를 나타낸다. 칩 i 가 n 비트의 response를 생성했을 때, response의 hamming weight로 계산하며, 50%에 근접할수록 이상적이다.

$$(Uniformity)_i = \frac{1}{n} \sum_{i=1}^{k-1} r_{i,l} \times 100\%, \quad (2)$$

3.3 성능 비교 및 분석

N 개씩 그룹화된 링 오실레이터 PUF는 총 $2N$ 개의 링 오실레이터가 사용된다. 그림 5를 통해 해당 PUF는 기존의 링 오실레이터 PUF에 비해 균일성이 약 5% 향상되었음을 알 수 있다. 하지만 표 1을 보면 사용된 링 오실레이터의 수가 2배로 늘어났기 때문에 면적 또한 증가했음을 알 수 있다. $N/2$ 개씩 그룹화된

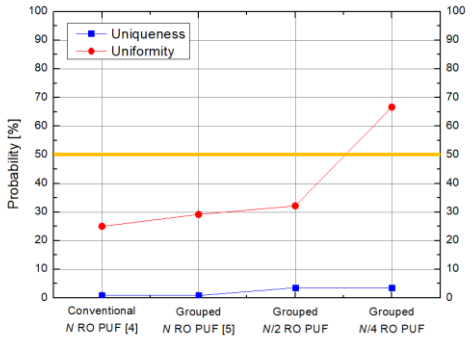

그림 5. PUF 간 성능 비교

링 오실레이터 PUF의 경우, 기존의 링 오실레이터 PUF와 동일한 수의 링 오실레이터를 사용하므로 비슷한 면적을 차지하지만 균일성은 향상되었음을 알 수 있다. *N*/4 개씩 그룹화된 링 오실레이터 PUF의 경우, 균일성 및 면적 사용량 측면에서 가장 우수했다. 하지만 링 오실레이터의 수가 감소함에 따라 CRP의 수가 크게 감소했기 때문에 PUF 성능 지표의 신뢰도가 낮다는 문제점이 존재한다. 고유성은 링 오실레이터의 수와 관계없이 네 가지 구조 모두 낮게 나타났다. 이는 칩 간 제조 변동성이 지배적으로 작용하지 않았기 때문이라고 예상된다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 Xilinx 사의 Artix-7 칩을 이용하여, 기존의 링 오실레이터 PUF와 *N* 개, *N*/2 개, *N*/4 개씩 그룹화된 링 오실레이터 PUF의 성능을 비교하였다. 그 결과, 링 오실레이터의 수가 감소할 수록 균일성이 향상되었으나, 링 오실레이터의 수가 크게 감소한 경우에는 PUF 성능 지표의 신뢰도가 낮아지는 문제가 발생했다. 또한 네 가지 구조는 모두 고유성이 낮게 나타났으며, 이는 공격자가 PUF의 출력을 예측 또는 추출할 가능성이 높인다. 따라서 고유성을 개선하기 위한 추가적인 연구가 필요하다.

Acknowledgments

This research was supported by Basic Science Reserarch Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2021R1I1A3055806), and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (2022-0-01170). The EDA tool was supported by the IC Design Education Center(IDEC), Korea.

표 1. PUF 간 면적 비교

	# of LUT	# of FF
Conventional *N* RO PUF [4]	102	73
Grouped *N* RO PUF [5]	166	73
Grouped *N*/2 RO PUF	98	73
Grouped *N*/4 RO PUF	64	73

참고문헌

[1] S. S. Mirzargar and M. Stojilovic, "Physical side-channel attacks and covert communication on FPGAs: A survey," in *Proc. 29th Int. Conf. Field Program. Log. Appl. (FPL)*, Barcelona, Spain, Sep. 2019, pp. 202–210.

[2] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," in *Proc. IEEE*, vol. 102, no. 8, Aug. 2014, pp. 1126–1141.

[3] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," in *Appl. Phys. Rev.*, vol. 6, Feb. 2019, Art. no. 011303.

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. ACM/IEEE Design Autom. Conf.*, San Diego, CA, USA, Jun. 2007, pp. 9–14.

[5] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Dopingless transistor based hybrid oscillator arbiter physical unclonable function," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, 2017, pp. 609–614.

[6] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design with FPGAs*. New York, NY, USA: Springer, Nov. 2012, pp. 245–267.