

Programmable Ring Oscillator 기반 전력 부채널 은닉 효과 분석

김윤소, 노윤진, 라승환, 유호영*

충남대학교 전자공학과

e-mail: yskim.cas@gmail.com, yjnoh.cas@gmail.com, shla.cas@gmail.com, hyyoo@cnu.ac.kr

Evaluation of Power Side-Channel Hiding Using Programmable Ring Oscillators

Yoonso Kim, Yunjin Noh, and Hoyoung Yoo*

Department of Electronics Engineering

Chungnam National University

Abstract

This paper analyzes the effect of the number of PRO-based Power Waster instances on power signature obfuscation in an FPGA-based AES environment. Using the CW305 FPGA target board and the CW-Husky measurement platform, power traces were collected while varying the total number of PRO instances from 0 to 256. The collected traces were evaluated in terms of SNR, CPA-based MTD, FPGA resource utilization, and power consumption.

Experimental results show that the SNR decreased from 21.1 dB to -5.5 dB, while the MTD increased from 990 traces to 1,037,000 traces. These results indicate that the PRO-based Power Waster effectively obfuscates the data-dependent power components of AES, thereby improving resistance against side-channel analysis. However, since FPGA resource utilization and power consumption also increase, the trade-off between security enhancement and hardware overhead must be carefully considered.

I. 서론

보안 시스템에서는 암호 연산의 고속화와 구현 유연성으로 인해 FPGA가 AES, SHA 등 암호 모듈 구현 플랫폼으로 활용되고 있다.[1][2] 그러나 FPGA 보안 시스템은 알고리즘 자체가 안전하더라도, 동작 중 발생하는 전력 소비나 전자파 등 물리적 정보가 부채널로 활용될 수 있다.[3] 이에 대응하기 위해 FPGA에서 암호 연산과 무관한 스위칭을 발생시키고, 측정 전력 신호에 노이즈를 삽입하여 암호 연산 관련 전력 패턴을 은닉할 수 있다.

그러나 Power Waster 인스턴스 수가 AES 전력 파형과 키 복구 난이도에 미치는 영향을 정량적으로 분석한 연구는 제한적이며, 자원 사용량과 전력 소모 증가에 따른 하드웨어 오버헤드도 함께 고려해야 한다. 이에 본 논문에서는 FPGA 기반 AES 환경에서 Programmable Ring Oscillator(PRO)[4] 구조를 Power Waster로 적용하고, 인스턴스 수를 0개부터 256개까지 변화시키며 전력 특성 은닉 효과를 분석한다. 측정 전력 파형을 기반으로 SNR, CPA[3] 기반 MTD, FPGA 자원 사용량을 비교하여 노이즈 삽입 효과, 키 복구 난이도, 하드웨어 복잡도 간 설계 trade-off를 평가한다.

II. 배경

2.1 FPGA 전력 소비 특성

FPGA의 전력 소비는 스위칭 여부와 무관하게 발생하는 정적 전력과, 클럭 동작에 따른 내부 노드·레지스터·배선 자원의 충·방전으로 발생하는 동적 전력으로 구분된다. 이 중 동적 전력은 신호의 스위칭 활동에 직접적으로 영향을 받기 때문에, 연산 중 처리되는 데이터와 상관관계를 가질 수 있다.

부채널 분석에서는 이러한 데이터 의존적 전력 소비를 설명하기 위해 Hamming Weight(HW) 모델과 Hamming Distance(HD) 모델이 주로 사용된다. HW 모델은 특정 시점 데이터의 '1'의 개수, HD 모델은 이전 상태와 현재 상태 사이에서 변화한 비트 수가 전력 소비와 관련된다고 가정한다.

FPGA 기반 AES에서는 S-box 출력, 라운드 키 결합 결과, 레지스터 갱신 값 등의 중간 데이터가 반복적으로 저장되거나 전이된다. 따라서 공격자는 측정 전력 파형과 키 가설 기반 중간값 사이의 통계적 상관관계를 분석하여 AES 내부 연산 정보를 추정할 수 있다.

2.2 Power Waster

Power Waster는 FPGA의 동적 전력이 내부 신호의 스위칭 활동에 의해 발생한다는 점을 이용하여, 암호 연산과 무관한 추가 스위칭을 인위적으로 발생시키는 회로이다. AES 모듈과 병렬로 동작할 경우 데이터 비의존적 전력 소비가 증가하고, AES 연산에 따른 데이터 의존적 전력 변화는 전체 측정 신호에서 상대적으로 약화된다. 이에 따라 전력 파형과 AES

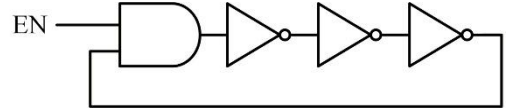


그림 1. Ring-Oscillator 구조

중간값 사이의 상관관계가 감소하며, 부채널 분석에 필요한 SNR이 저하된다.

대표적인 Power Waster 구조로는 Ring Oscillator(RO)가 사용된다. RO의 구조는 그림 1과 같다. RO는 홀수 개의 인버터를 순환 연결하여 출력이 지속적으로 토글되도록 구성한 발진 회로이며, 동작 중 반복적인 스위칭을 통해 FPGA 내부에 지속적인 동적 전력 소비를 발생시킨다.

2.3 Programmable Ring-Oscillator

Programmable Ring Oscillator(PRO)는 RO 구조를 기반으로 하되, 선택 신호에 따라 루프 내부의 지연 경로를 변경할 수 있도록 구성한 회로이다. PRO는 서로 다른 지연 시간을 갖는 delay cell들로 구성되며, 각 delay cell은 인버터 경로와 bypass 경로를 포함한다. 선택 신호에 따라 특정 delay cell이 루프에 포함되거나 우회되면서 전체 루프 지연 시간이 변화하고, 이에 따라 발진 주파수가 조절된다.

기존 RO 기반 Power Waster는 구현 후 발진 주파수가 비교적 고정되어 반복적이고 예측 가능한 노이즈를 발생시킬 수 있다. 반면 PRO 기반 Power Waster는 선택 신호를 통해 발진 주파수를 변화시킬 수 있으므로, 시간에 따라 변화하는 스위칭 노이즈를 삽입할 수 있다. 따라서 본 논문에서는 PRO를 전력 특성 은닉을 위한 Power Waster 구조로 적용하였다.

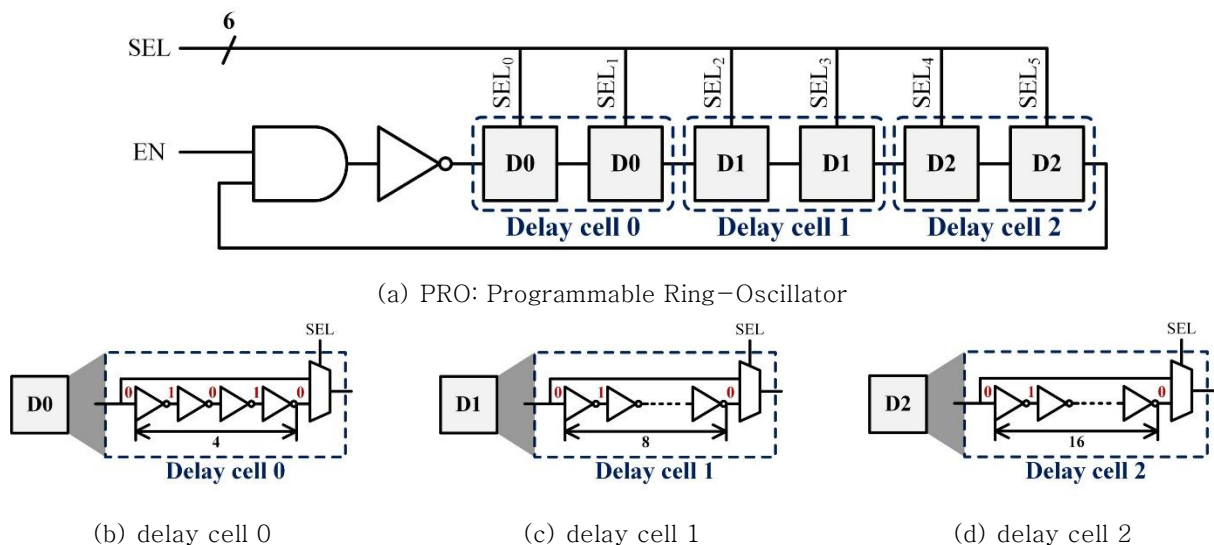


그림 2. Programmable Ring-Oscillator

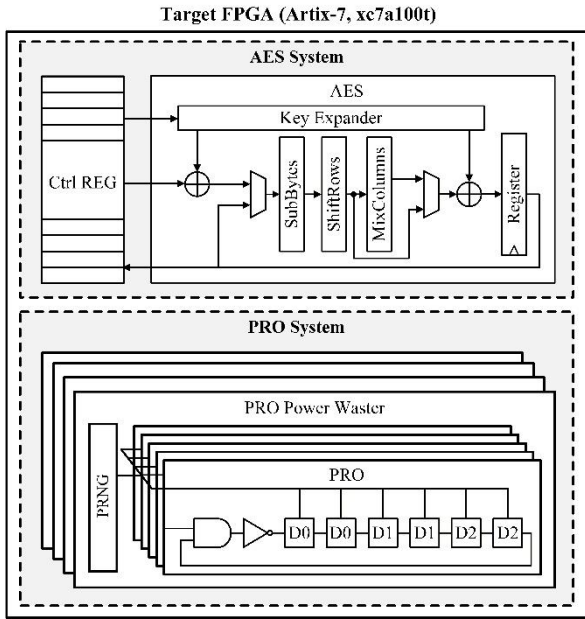


그림 3. PRO 기반 평가 시스템

III. PRO 기반 평가 시스템 구현

3.1 PRO Power Waster

랜덤 주파수 기반의 전력 노이즈를 생성하기 위해 본 논문에서는 PRO 기반 Power Waster를 구현하였다. 제한한 PRO Power Waster는 1개의 PRNG와 8개 단위로 구성된 PRO 인스턴스로 이루어진다.

각 PRO는 서로 다른 지연 특성을 갖는 delay cell을 조합하여 구성된다. 본 설계에서는 각각 4개, 8개, 16개의 인버터를 포함하는 delay cell 0, delay cell 1, delay cell 2를 사용하였다. 하나의 PRO Power Waster 내부에는 여러 개의 PRO가 병렬로 배치되며, 각 PRO는 공통의 SEL 신호에 의해 선택되는 delay cell 조합에 따라 서로 다른 발진 주파수를 생성한다.

랜덤 주파수 동작을 구현하기 위해서는 SEL 신호가 고정값이 아니라 시간에 따라 변화하는 무작위 값으로 입력되어야 한다. 이를 위해 본 논문에서는 6개의 delay cell 선택 신호에 대응하는 6비트 PRNG를 구현하였다. PRNG는 LFSR 기반으로 구성하였으며, 다항식은 $x^5 + x + 1$ 와 같다.

3.2 평가 시스템 구현

그림 3은 PRO 기반 Power Waster가 AES 암호 회로의 전력 특성에 미치는 영향을 평가하기 위해 구축한 전체 평가 시스템의 구조를 나타낸다. Target FPGA는 AES 시스템과 PRO 기반 Power Waster 시스템으로 구성된다.

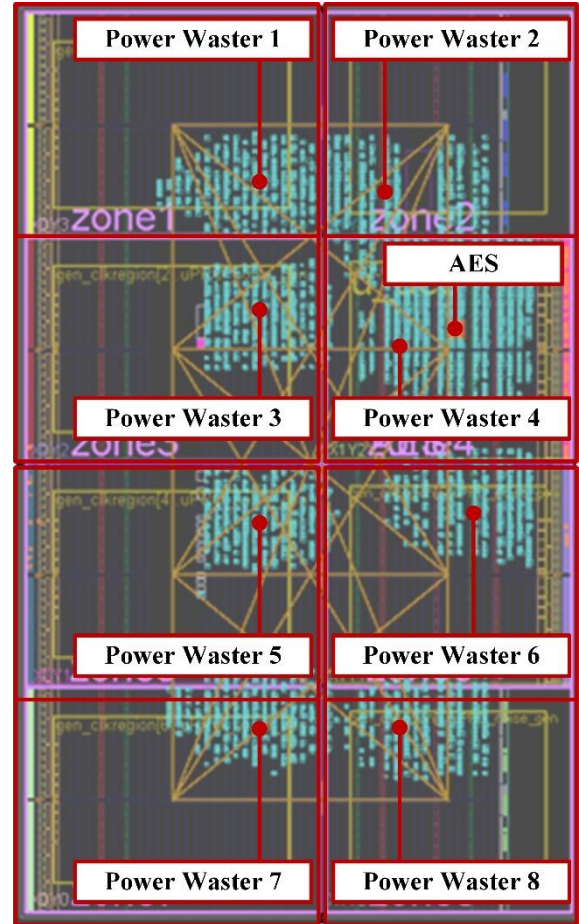


그림 4. PRO 인스턴스 256개 분산 배치도

AES 시스템은 AES-128 암호화 모듈과 제어 레지스터로 구성된다. 제어 레지스터는 PC와 USB 인터페이스를 통해 평문과 키를 수신하고, 이를 AES-128 모듈에 전달하여 암호화를 수행한다. 생성된 암호문은 다시 PC로 송신된다. PRO 기반 Power Waster 시스템은 총 8개의 Power Waster 인스턴스로 구성된다. 각 인스턴스는 파라미터를 통해 내부 PRO 개수를 조절할 수 있으며, 본 논문에서는 인스턴스당 PRO 개수를 1, 2, 4, 8, 16, 32개로 설정하였다. 이에 따라 전체 PRO 인스턴스 수는 각각 8, 16, 32, 64, 128, 256개가 된다. PRO Power Waster가 특정 영역에 집중될 경우 AES 회로와의 물리적 거리 및 배치 위치에 따라 노이즈 영향이 편향될 수 있다. 이를 방지하기 위해 8개의 Power Waster 인스턴스를 FPGA의 8개 Clock Region에 균등 배치하여, PRO 기반 노이즈가 FPGA 전반에 분산되도록 하였다. 그림 4는 전체 PRO 인스턴스 수가 256개인 조건에서의 분산 배치 결과를 나타낸다.

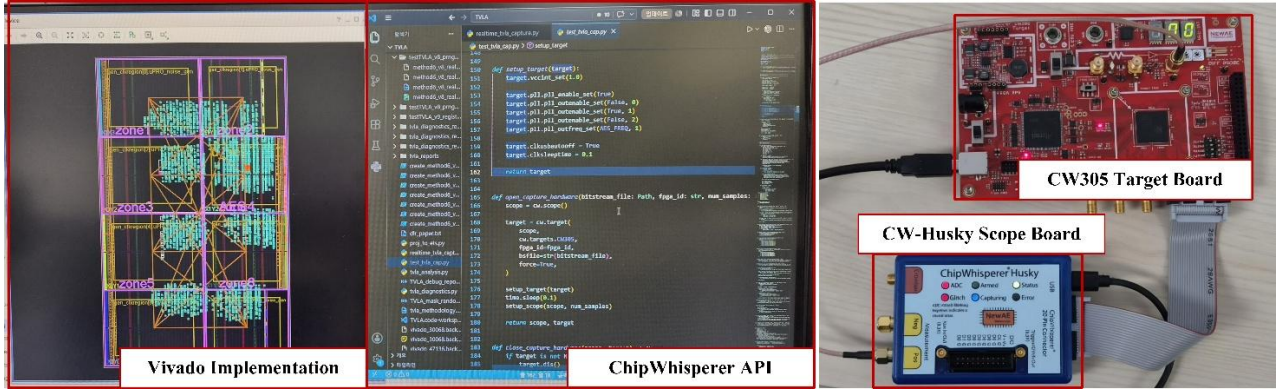


그림 5. 실험 환경

IV. 실험 방법

4.1 실험 환경

본 연구는 NewAE사의 CW305 FPGA Target Board와 CW-Husky 계측 보드를 이용하여 수행하였다. 그림 5는 본 연구에서 사용한 실제 전력 측정 실험 환경을 나타낸다. CW305 보드는 AES 암호 모듈과 PRO 기반 Power Waster를 구현하기 위한 FPGA 타겟 보드로 사용하였으며, 탑재 FPGA는 Xilinx Artix-7 XC7A100T이다. CW-Husky는 AES 암호 연산 중 발생하는 전력 파형 수집 장비로 사용하였다. AES 시스템 및 PRO 기반 Power Waster 시스템 설계에는 Xilinx Vivado 2021.2를 사용하였다.

AES-128 암호 연산은 5MHz 클럭에서 수행하였고, CW-Husky의 ADC 샘플링 주파수는 100MHz로 설정하였다. AES 시작 신호를 기준으로 트리거를 발생시켜 암호 연산 구간의 전력 파형을 수집하였으며, 모든 조건에서 동일한 클럭, 샘플링 주파수, 트리거 조건을 유지하였다. Host PC는 Python 3.13 환경에서 ChipWhisperer API를 이용해 트리거 설정, ADC 샘플링, 파형 저장을 제어하였다.

4.2 평가 지표

PRO Power Waster 수에 따른 전력 특성 및 부채널 분석 저항성 변화를 평가하기 위해 SNR, MTD, 하드웨어 자원 사용량, 전력 소모를 지표로 사용하였다. SNR은 기준 신호 대비 노이즈 성분의 크기를 나타내며, 본 논문에서는 고정 평균 반복 측정으로 얻은 평균 파형을 기준 신호로 정의하였다. MTD는 CPA 수행 시 AES 128-bit 키 전체를 안정적으로 복구하는 데 필요한 최소 trace 수이다. 또한 하드웨어 오버헤드 평가를 위해 LUT, FF, Slice 사용량과 전력 소모를 함께 분석하여 보안성 향상과

하드웨어 비용 간 trade-off를 평가하였다.

4.3 평가 방법

본 논문에서는 baseline AES와 PRO Power Waster가 삽입된 시스템을 비교하였다. PRO 시스템은 전체 PRO 인스턴스 수를 기준으로 8, 16, 32, 64, 128, 256개 조건으로 설정하였다. 모든 조건에서 SNR 분석에는 고정 평균 반복 측정 데이터를, MTD 분석에는 동일한 가변 평균 시퀀스를 사용하였다.

SNR은 각 조건에서 수집한 전력 파형을 기반으로 계산하였다. Power Waster 인스턴스 수가 N일 때의 SNR은 식 (1)과 같이 정의된다.

$$SNR(N) = 10 \log \frac{\sum_{t=1}^T (\mu_N[t])^2}{\frac{1}{M} \sum_{i=1}^M \sum_{t=1}^T (x_{N,i}[t] - \mu_N[t])^2} \quad (1)$$

여기서 $x_{N,i}[t]$ 는 Power Waster가 N개 삽입된 조건에서 i번째로 측정한 전력 파형, $\mu_N[t]$ 는 M개의 파형을 평균한 기준 파형을 의미한다. M은 수집 파형 수, T는 AES 연산 구간의 샘플 수이다. 식 (1)의 분자는 평균 파형의 신호 에너지, 분모는 개별 파형이 평균 파형에서 벗어나는 노이즈 에너지를 나타낸다. 본 논문에서는 AES 연산 구간 내 250개 샘플을 분석 구간으로 설정하고, 각 조건에서 M=10,000개의 전력 파형을 사용하여 SNR을 계산하였다.

MTD는 CPA를 통해 산출하였다. CPA에는 AES 마지막 라운드의 HD 누설 모델을 사용하였으며, 16바이트 전체에서 정답 키가 모두 correlation rank 1로 안정적으로 유지되기 시작한 최초 trace 수를 MTD로 정의하였다. 각 조건별 실험은 동일한 가변 평균 시퀀스로 3회 반복하였고, 반복 실험에서 얻은 MTD 평균값을 최종 MTD로 사용하였다. 하드웨어 복잡도와 전력 소모는 Xilinx Vivado 구현 결과 보고서를 기반으로 평가하였다.

N	LUT[#]	FF[#]	Slices[#]	Power[mW]	SNR[dB]	MTD[#]
0	2,000	260	500	45	21.1	990
8	2,528(+26.4%)	308(+18%)	632(+26.4%)	60(+33%)	6.5	19,290
16	3,040(+52%)	308(+18%)	760(+52%)	73(+62%)	4.2	32,300
32	4,064(+103%)	308(+18%)	1,016(+103%)	103(+128%)	-0.3	92,100
64	6,112(+206%)	308(+18%)	1,528(+206%)	156(+247%)	-1.9	203,600
128	10,208(+410%)	308(+18%)	2,552(+410%)	262(+482%)	-4.1	461,700
256	18,400(+820%)	308(+18%)	4,600(+820%)	472(+949%)	-5.5	1,037,000

표 1. PRO 인스턴스 수 별 오버헤드 및 보안성 평가 결과

V. 실험 결과

본 논문에서는 FPGA 환경에서 PRO 기반 Power Waster 인스턴스 수가 AES 전력 특성에 미치는 영향을 SNR, MTD, 하드웨어 자원 사용량 및 전력 소모를 통해 분석하였다. 표 1은 Power Waster 인스턴스 수에 따른 LUT, FF, Slice 사용량, 전력 소모, SNR 및 MTD 측정 결과를 나타낸다. 실험 결과, baseline 조건에서는 SNR이 21.1 dB, CPA 기반 MTD가 990개로 측정되었다. 반면 Power Waster 8개 삽입 시 SNR은 6.5 dB로 감소하고 MTD는 19,290개로 증가하였다. 이는 적은 수의 Power Waster만으로도 AES 전력 파형의 데이터 의존성이 약화되고, 키 복구에 필요한 trace 수가 증가함을 의미한다.

Power Waster 수가 증가함에 따라 SNR은 감소하고 MTD는 증가하는 경향을 보였다. N=8, 16, 32, 64, 128, 256 조건에서 SNR은 각각 6.5, 4.2, -0.3, -1.9, -4.1, -5.5 dB로 감소하였고, MTD는 N=32에서 92,100개, N=64에서 203,600개, N=128에서 461,700개, N=256에서 1,037,000개로 증가하였다. 그러나 Slice 사용량은 baseline 500개에서 N=256 조건의 4,600개로, 전력 소모는 45 mW에서 472 mW로 증가하였다. 이는 PRO 기반 Power Waster가 전력 특성 은닉에는 효과적이거나, 자원 사용량과 전력 소모 측면의 trade-off를 동반함을 보여준다.

VI. 결론

본 논문에서는 FPGA 기반 AES 환경에서 PRO의 인스턴스 수가 전력 특성 은닉 효과에 미치는 영향을 정량적으로 분석하였다. RO 인스턴스 수가 증가할수록 SNR은 감소하고 MTD는 증가하여 AES의 데이터 의존적 전력 성분이 효과적으로 은닉됨을 확인하였다.

특히 N=8 조건에서도 SNR이 21.1 dB에서 6.5 dB로 감소하고 MTD가 990개에서 19,290개로 증가하여, 적은 수의 Power Waster 삽입만으로도 부채널 분석 저항성이 향상됨을 보였다. 다만 N=32 이후부터 SNR 감소 폭은 완만해지는 반면, MTD는 지속적으로 증가하였고, LUT, Slice 사용량 및 전력 소모 역시 함께 증가하였다. 따라서 PRO 기반 Power Waster 적용 시에는 단순히 인스턴스 수를 늘리기보다, 목표 보안 수준과 허용 가능한 하드웨어 오버헤드를 함께 고려한 설계가 필요하다.

Acknowledgments

This research was supported by the National Research Foundation of Korea (NRF) (No. 2022R1A5A8026986), and by the IC Design Education Center (IDEC), Korea.

참고문헌

- [1] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS PUB 197-upd1, 2023.
- [2] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer, 2007.
- [3] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, LNCS 3156, pp. 16–29, 2004.
- [4] Y. Yao, P. Kiaei, R. Singh, S. Tajik, and P. Schaumont, "Programmable RO (PRO): A Multipurpose Countermeasure against Side-channel and Fault Injection Attacks," Cryptology ePrint Archive, Paper 2021/878, 2021.