상관 전력 분석을 통한 FPGA 레지스터의 비트 전이 패턴의 실험적 검증

전재호, 김영식
전기전자컴퓨터공학과, 대구경북과학기술원

dgwogh@dgist.ac.kr, ysk@dgist.ac.kr

Experimental Validation of Bit-Flipping Patterns in FPGA Registers through Correlation Power Analysis

Jae Ho Jeon, Young-Sik Kim
Department of Electrical Engineering and Computer Science, DGIST

요 약

본 논문은 FPGA 레지스터의 비트 플리핑(bit-flipping)이 전력 소모에 미치는 영향을 분석하고, 이를 상관 전력 분석(CPA)을 통해 실험적으로 검증한다. 기존 부채널 공격이 주로 알고리즘 수준의 데이터 종속성을 활용한 데 비해, 본 연구는 하드웨어 내부의 레지스터 전이에 따른 전력 차이를 활용한다. 해밍 거리(Hamming Distance)와 전력 소모 간의 상관관계를 가정하고, 이를 다양한 비트 전이 입력을 통해 측정한 전력 트레이스를 기반으로 분석하였다. 그 결과, 전력 소비는 비트 전이 수에 비례하며, 레지스터 전이 구간에서 높은 CPA 상관값이 관측되었다. 본 연구는 FPGA 와 같은 범용 하드웨어에서도 비트 플리핑이 부채널 누설의 원인이 될 수 있음을 보여주며, 향후 하드웨어 보안 분석에 새로운 시사점을 제공한다.

Ⅰ. 서 론

임베디드 시스템은 부채널 분석(Side-Channel Analysis, SCA)에 취약하며, 특히 ARM Cortex-M4 와 같은 MCU (Microcontroller Unit)를 대상으로 한 공격은 활발히 연구되어 왔다. 이러한 공격은 주로 암호 연산 중의 전력 소모나 전자기 방출을 분석하여 민감 정보를 유출하는 방식이다.

FPGA (Field-Programmable Gate Array) 또한 물리적 구현을 기반으로 동작하는 만큼 SCA 에 노출될 수 있으나, 구조적 특성상 MCU 보다 분석이 더 어렵다. 명령어 기반의 MCU 와 달리, FPGA 는 병렬적으로 동작하는 사용자 정의 회로로 구성되어 있어 공격자가 누설 지점을 명확히 지정하거나 동기화하기 어렵기 때문이다.

그러나 FPGA 내부에서도 레지스터 갱신 시 비트 플리핑(bit-flipping)이 전력 차이를 유발하며, 이로 인해 정보가 누설될 수 있다는 가능성이 널리 알려져 있다. 본 연구에서는 이러한 가설을 세우고, 비트 전이 수에 따라 전력 소비가 어떻게 달라지는지를 실험적으로 검증하였다.

FPGA 에 비트 플리핑 패턴을 갖는 입력을 주입하고 고해상도 전력 트레이스를 수집한 결과, 상관 전력 분석(CPA, correlation power analysis)을 통해 해밍 거리와 전력 소비 간의 명확한 상관관계가 관찰되었다. 본 연구는 FPGA 회로 설계 시 bit-flipping 자체가 공격 대상이 될 수 있음을 보여주며, FPGA 기반 시스템에 대한 부채널 보안 분석의 기초를 제시한다.

Ⅱ. 본론

하드웨어 회로, 특히 레지스터와 같은 순차 논리 소자에서는 이전 상태에서 새로운 상태로의 전이가 발생할 때, 내부 전압 변화에 따라 물리적인 전력 소모가 발생한다. 이때 전력이 실제로 소비되는 주요 원인은 비트 플리핑(bit-flipping), 즉 논리값이 0 에서 1 로 또는 1 에서 0 으로 바뀌는 전이이다.

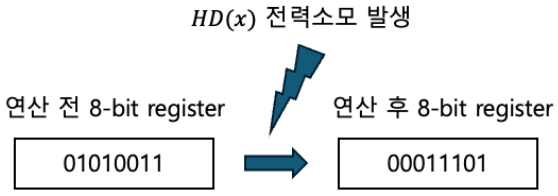

그림 1. 레지스터 상태가 01010011 에서 00011101 로 전이되며, 해밍 거리 HD = HW(01010011 ⊕ 00011101) = 4 가 발생하여 전력 소모가 유도된다.

이를 보다 명확하게 설명하기 위해, 8 비트 크기의 레지스터를 예로 들 수 있다. 그림 1 은 초기 상태가 01010011 인 레지스터가 다음 클럭 사이클에서 00011101 로 갱신되는 상황을 보여준다. 이 두 이진 값 간의 해밍 거리는 4 이며, 이는 총 4 개의 비트 위치에서 값이 바뀌었음을 의미한다.

이러한 비트 전이는 각각의 플립마다 전력 공급망에서 충전 혹은 방전이 발생하기 때문에, 전력 트레이스 상에서 명확한 전력 소비 차이를 유발할 것이라고 널리

알려져 있다. 특히, FPGA 내부의 레지스터는 복수의 병렬 플립플롭으로 구성되어 있어, 비트 플리핑 수가 많을 수록 소모 전력이 증가하는 경향이 존재한다.

이 특성은 통계적 분석 기법인 CPA 와 결합될 때, 비트 플리핑 패턴 자체가 유의미한 누설 정보로 작용할 수 있음을 시사한다. 본 연구에서는 이러한 전제를 기반하여 다음과 같이 실험을 설계하였다.

1. 32 비트 레지스터 활용
2. 가능한 해밍 거리 경우의 수를 [0, 8, 16, 24] 총 4 가지로 고정
3. FPGA 보드에서 하나의 해밍거리를 128 번 반복해서 전력 소모를 유도

이 실험 과정은 그림 2 처럼 두가지 상태를 반복해서 출력해서 특정 해밍 거리에 따른 전력 소모가 발생하도록 실험을 진행하였다.

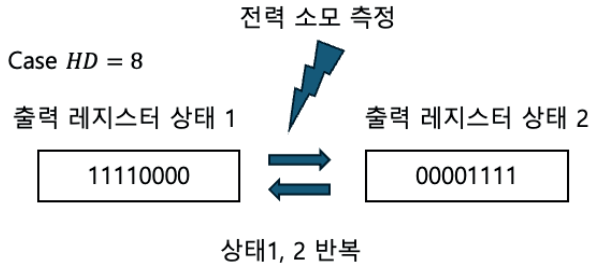

그림 2. 출력 레지스터에 두가지 상태를 반복해서 출력하도록 설계하여 전력 패턴을 유도한다. (해밍 거리가 8 인 경우)

해밍 거리가 0, 8, 16, 24 일때를 반복해서 측정하여, CPA 기법으로 임의의 해밍거리를 입력했을 때, 올바르게 값을 예측하는지 확인해보았다. 실험 측정환경은 chipwhisperer CW305 FPGA 보드에 실험 모델을 코딩하였고 picoscope3403D 오실로스코프로 전력을 측정하였다.

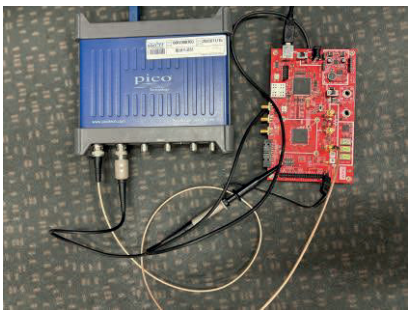

그림 3. CW305 보드와 picoscope 3403D 를 연결한 실험 세팅 사진

또한 각 해밍 거리마다 40 개씩 전력 소모를 측정하였고, 이를 CPA 기법으로 분석하여, [0, 8, 16, 24] 중에서 임의의 해밍 거리 전력 분석과 대조하여 올바르게 예측하는지 비교하였다. 그 결과는 다음 표 1 와 같았다.

표 1. 각 HD 값 별로 예측 횟수와 성공 횟수 결과값

HD값	총 예측 횟수	성공횟수
0	100	92
8	100	95
16	100	94
24	100	96

표 1 에서 알 수 있는 것처럼 FGPA 레지스터의 비트 플리핑 수와 전력 소모 사이의 관계를 실험적으로 분석하였으며, CPA 결과 90%이상의 높은 적중률을 보여주었다. 본 시뮬레이션은 NIST PQC 표준 후보였던 BIKE 알고리즘에서 성공적인 전력 분석 공격에 사용된 것과 유사하며, NIST PQC 표준으로 선정된 HQC 알고리즘의 Sparse polynomial 곱셈에 적용이 가능하다.

Ⅲ. 결론

본 연구는 FPGA 레지스터의 비트 플리핑 수와 전력 소모 사이의 관계를 실험적으로 분석하였으며, CPA 기반 예측에서 전반적으로 90% 이상의 높은 적중률을 확인하였다. 이를 통해 해밍 거리에 비례한 전력 차이가 실제로 존재함을 입증하였으며, 해당 특성이 다른 부채널 분석 기법에서도 유의미한 정보로 활용될 수 있음을 보여주었다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2024-00442085, 자율주행 차량 서비스 보호를 위한 V2X 무선통신 인프라 보안 핵심기술 개발).

참 고 문 헌

[1] Zhao, M., & Suh, G. E. (2018, May). FPGA-based remote power side-channel attacks. In *2018 IEEE symposium on security and privacy (SP)* (pp. 229-244). IEEE.

[2] Dewar, A., Thibault, J. P., & O'Flynn, C. (2020). NAEAN0010: Power Analysis on FPGA Implementation of AES Using CW305 & ChipWhisperer R O.

[3] Beckwith, L., Zhou, H., Kaps, J. P., & Gaj, K. (2024, December). Power Side-Channel Key Recovery Attack on a Hardware Implementation of BIKE. In *2024 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)* (pp. 1-6). IEEE.

[4] 최기훈, 오충연, 김주환, 박혜진, 한동국. (2025). HW 구현 대칭키 암호에 대한 범용적 딥러닝 기반 프로파일링 부채널 분석 방안. 정보보호학회논문지, 35(1), 37-46.