

고성능 저비용의 내장형 TDC 전압 센서 기반 FPGA 부채널 분석 시스템

노윤진, 김윤소, 안지민, 유호영*

충남대학교 전자공학과

e-mail : yjnoh.cas@gmail.com, yskim.cas@gmail.com, jmahn.cas@gmail.com,
hyyoo.cnu@gmail.com

A High-Performance and Low-Cost FPGA Side-Channel Analysis System Based on an Embedded TDC Voltage Sensor

Yunjin Noh, Yoonso Kim, Jimin Ahn and Hoyoung Yoo*

Department of Electronics Engineering

Chungnam National University

Abstract

A high-performance and low-cost FPGA side-channel analysis system is proposed by embedding a time-to-digital converter (TDC) voltage sensor inside the FPGA. Implemented on a SAKURA-X Dual-FPGA platform, the system captures TDC traces corresponding to local voltage variations during AES-128 operations. Compared with a ChipWhisperer-based external power measurement setup under the same CPA conditions, the proposed system reaches the key recovery criterion with an average of 1914 traces and reduces the required trace count by 41.1%. These results show that embedded TDC voltage sensing is effective for high-performance and low-cost FPGA side-channel analysis.

I. Introduction

FPGA 기반 암호 구현은 재구성 가능성과 실험 유연성으로 인해 하드웨어 보안 연구에서 널리 활용되고 있다. 특히 AES와 같은 대칭키 암호 알고리즘은 FPGA 상에서 하드웨어로 구현되어 실제 암호 장치와 유사한 환경에서 부채널 누설 특성을 분석할 수 있다.

기존 부채널 계측에서는 ChipWhisperer 또는 Oscilloscope와 같은 외부 전력 계측 방식이 널리 사용되어 왔다. 그러나 외부 계측은 측정 환경의 영향을 받으며, 별도 장비가 필요해 비용과 수집 복잡도가 증가한다. 또한 FPGA 내부 암호 코어 인근의 국소 전압 변동을 직접 반영하기 어렵다.

반면 FPGA 내부에 배치된 TDC 기반 전압 센서는 암호 연산 중 발생하는 국소 전압 변동을 지연 변화로 관측할 수 있다. 이를 통해 외부 전력 측정 파형과 다른 형태의 부채널 정보를 획득할 수 있다. 또한 외부 계측 장비 없이 FPGA 내부에서 측정 파형을 수집할 수 있다. 계측 회로와 암호 코어를 동일한 FPGA에 배치할 수 있으므로 측정 경로를 단순화할 수 있다. 이는 장비 구성 비용과 측정 파형 수집 절차의 복잡도를 낮추는 데 유리하다. 나아가 암호 코어 주변에서 발생하는 전압 변동을 활용하므로 내장형 부채널 분석 시스템의 계측 수단으로 적합하다.

본 연구에서는 SAKURA-X 기반 Dual-FPGA 환경에 AES-128 하드웨어 코어와 TDC 전압 센서를 통합한 고성능 저비용 부채널 분석 시스템을 구현한다. 제안 시스템은 암호 연산 제어와 TDC 측정 파형 수집을 하나의 호스트 제어 흐름으로 수행하며, ChipWhisperer 기반 외부 전력 계측 방식과의 CPA 성능 비교를 통해 저비용 계측 구조에서도 높은 부채널 분석 성능을 제공할 수 있음을 보인다.

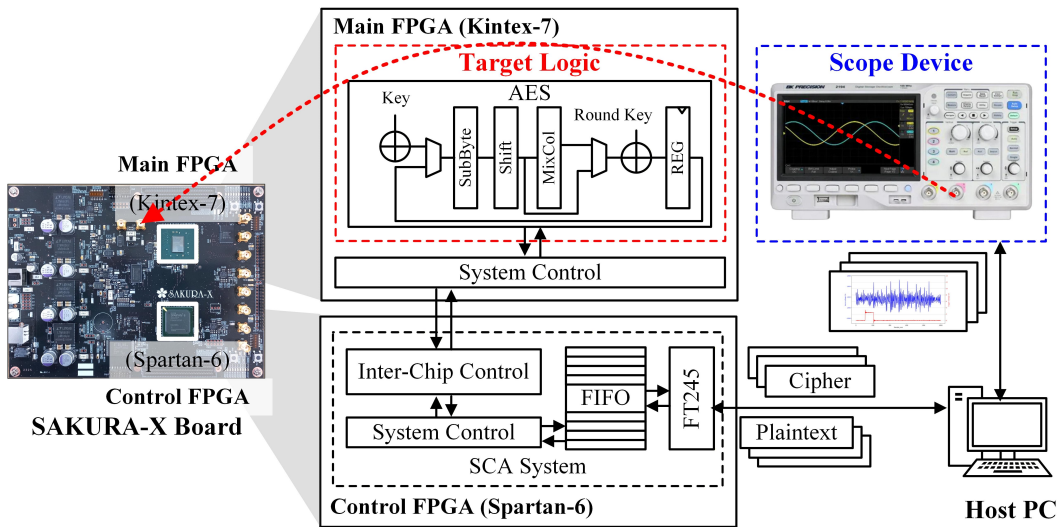


그림 1. 외부 계측 장비 기반 FPGA 부채널 측정 시스템

II. Backgrounds

2.1 FPGA 부채널 분석 시스템

그림 1은 외부 전력 계측 장비를 사용하는 기존 FPGA 부채널 분석 시스템을 나타낸다. SAKURA-X 보드는 암호 연산을 수행하는 Main FPGA와 시스템 제어를 담당하는 Control FPGA로 구성된 Dual-FPGA 환경을 제공한다[1]. 기존 방식에서는 Main FPGA에서 AES 연산을 수행하고, 보드 상의 measurement point에서 발생하는 전력 변화를 외부 계측 장비로 측정하여 부채널 측정 파형을 획득한다.

이 방식에서는 Oscilloscope 또는 ChipWhisperer와 같은 상용 계측 장비가 측정 파형 수집을 담당한다. 따라서 대상 보드와 별도의 계측 장비가 모두 필요하며, 암호 연산 실행 흐름과 계측 장비의 트리거 및 수집 흐름을 함께 관리해야 한다. 또한 측정 지점이 FPGA 외부 전력 경로에 위치하므로, 수집된 측정 파형은 보드 전원망과 주변 회로의 영향을 포함할 수 있다.

2.2 TDC 전압 센서

TDC 전압 센서는 FPGA 내부의 carry chain 또는 delay line을 이용하여 전압 변동에 따른 지연 변화를 디지털 코드로 변환한다[2]. FPGA 내부 전압이 변화하면 logic delay와 routing delay가 변하므로, TDC 출력은 전압 자체를 직접 측정한 값이 아니라 전압 변화에 의해 달라진 지연 응답으로 해석할 수 있다.

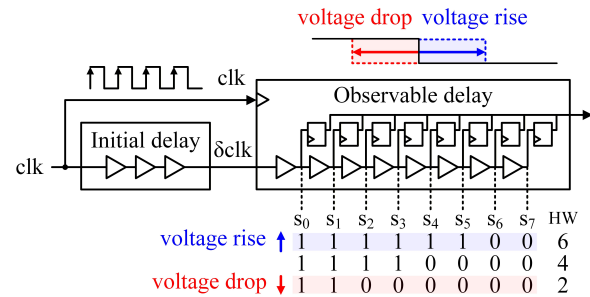
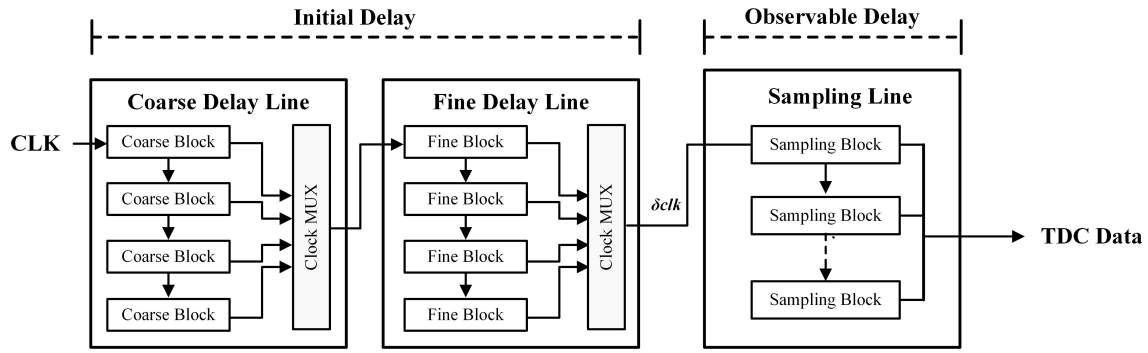


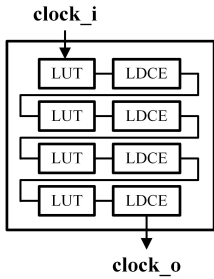
그림 2. TDC 전압 센서 동작 원리

그림 2는 전압 변동이 TDC 출력으로 반영되는 과정을 나타낸다. 암호 연산 중 로직 스위칭에 따른 전류 소모 변화는 암호 코어 주변의 국소 전압 변동으로 이어질 수 있다. 전압 강하가 발생하면 신호 전파 지연이 증가하여 샘플링 시점에 1로 관측되는 탭 수가 감소한다. 반대로 전압이 회복되면 신호 도달 시점이 앞당겨져 1의 개수가 증가한다. 따라서 TDC 비트 벡터의 해밍 가중치(Hamming Weight)는 전압 변동에 따른 지연 응답을 나타낸다. 본 논문에서는 이를 부채널 측정 파형으로 사용한다.

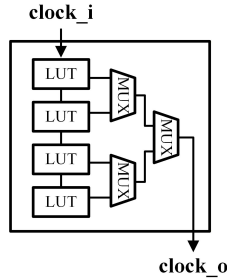
TDC 전압 센서는 FPGA 내부에 구현되므로 암호 코어 주변의 국소 전압 변동을 관측할 수 있다. 또한 센서 출력이 디지털 값이므로 내부 로직과 연계하여 저장하고 전송하기 쉽다. 이러한 특성은 별도 아날로그 계측 경로를 줄일 수 있어 저비용 부채널 분석 시스템 구성에 적합하다.



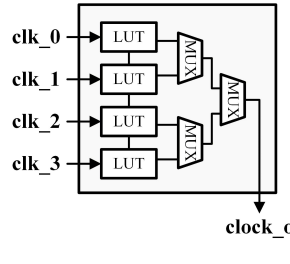
(a) TDC 센서 전체 구조



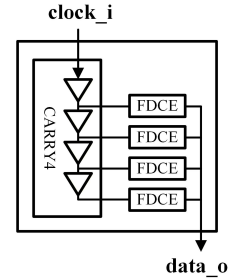
(b) Coarse block 구조



(c) Fine block 구조



(d) Clock MUX 구조



(e) Sampling block 구조

그림 3. TDC 전압 센서 구조

III. TDC 전압 센서 구현

3.1 TDC 전압 센서 구조

그림 3은 제안 시스템에 포함된 TDC 전압 센서의 내부 구조를 나타낸다. 전체 TDC는 coarse delay line, fine delay line, sampling line으로 구성되며, 입력 clock은 coarse block과 fine block을 거쳐 sampling line으로 전달된다. Coarse block은 LUT와 LDCE 기반 delay cell을 직렬로 연결하여 clock 지연을 누적하고, fine block은 LUT delay와 MUX tree를 통해 보다 세밀한 지연 경로를 제공한다. Clock MUX는 각 delay path의 출력을 선택하여 sampling line으로 전달하고, sampling line은 전달된 신호의 지연 변화를 관측한다.

Sampling line을 구성하는 sampling block은 CARRY4 기반 delay tap과 FDCE flip-flop으로 구성된다. 지연된 신호는 sampling clock 기준으로 각 tap의 상태가 동시에 저장되며, 그 결과는 비트 벡터 형태의 TDC 상태값으로 출력된다. 본 시스템은 이 상태값의 해밍 가중치를 이용하여 AES 연산 중 발생하는 지연 응답을 측정 파형으로 변환한다.

3.2 하드웨어 구현 결과

제안한 TDC 전압 센서는 Main FPGA 내부에 8개를 병렬로 배치하여 구현하였다. 각 센서는 AES 연산 중 발생 하는 지연 응답을 관측할 수 있도록 암호 코어와 함께 구성된다. 병렬 센서 구조는 단일 측정 구간에서 여러 TDC 출력을 수집할 수 있게 한다. 수집된 센서 출력은 데이터 처리 로직을 거쳐 측정 파형으로 저장된다.

표 1은 구현된 TDC 관련 로직의 하드웨어 복잡도를 나타낸다. TDC Sensor (N=1)는 단일 센서의 지연 관측 로직에 해당한다. Data Processor는 센서 출력 저장과 측정 파형 전달을 위한 주변 로직을 포함한다. Total은 8개의 TDC 센서와 데이터 처리 로직을 합산한 결과이다.

표 1. TDC 전압 센서 구현 결과

Logic	FF	LUT	MUX	CARRY4
TDC Sensor (N=1)	48	40	18	8
Data Processor	1133	938	32	15
Total	1517	1258	176	79

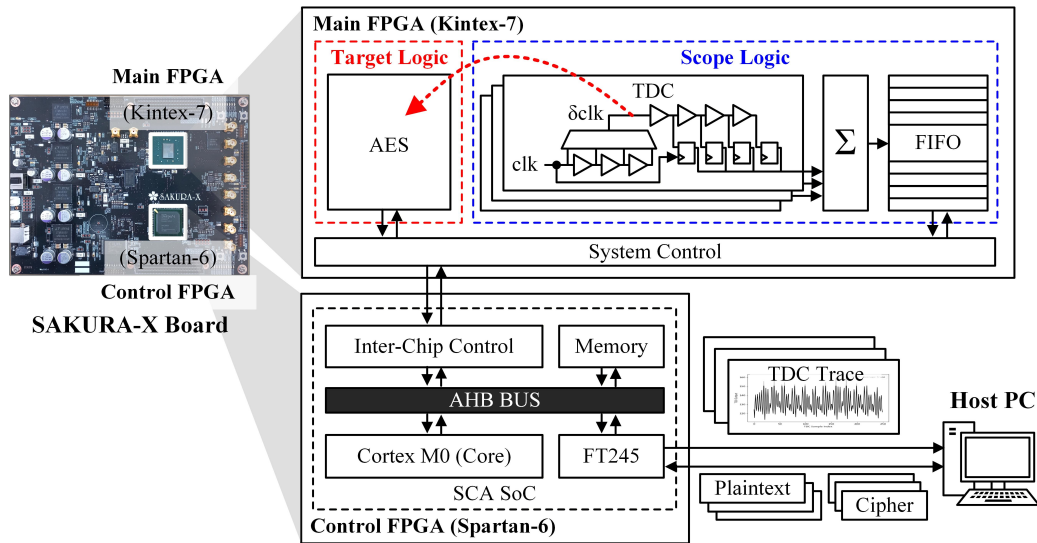


그림 4. 제안하는 TDC 기반 부채널 분석 시스템

IV. TDC 기반 부채널 계측 시스템

4.1 시스템 하드웨어 구조

그림 4는 제안하는 TDC 기반 Dual-FPGA 부채널 분석 시스템의 전체 구조를 나타낸다. 시스템은 SAKURA-X 보드의 Main FPGA와 Control FPGA를 이용하여 구성된다. Main FPGA에는 AES 암호 모듈과 TDC 기반 측정 로직을 배치하고, Control FPGA에는 호스트 통신과 시스템 제어를 위한 SCA SoC를 배치한다. 호스트 PC는 Control FPGA를 통해 AES 입력 설정, 암호 연산 실행, 암호문 읽기, TDC 측정 파형 수집을 수행한다.

Main FPGA(Kintex-7)의 Target Logic에는 AES-128 하드웨어 코어가 구현된다. Scope Logic에는 TDC 전압 센서와 FIFO가 배치되며, AES 연산 중 발생하는 국소 전압 변동을 TDC 측정 파형으로 변환하여 저장한다. AES 코어는 호스트에서 전달된 키와 평문을 이용해 암호 연산을 수행하고, TDC 전압 센서는 연산 구간의 지연 응답을 관측한다. 생성된 측정 파형은 FIFO에 저장된 뒤 Control FPGA를 통해 호스트 PC로 전달된다.

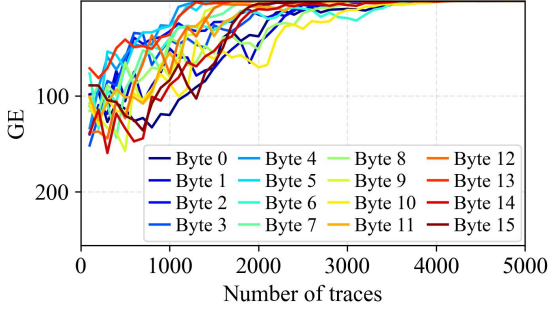
Control FPGA(Spartan-6)는 호스트와 Main FPGA 사이의 제어 및 데이터 전달 경로를 담당한다. 내부 SCA SoC는 Cortex-M0 기반 제어 코어, FT245 통신 경로, AHB 버스, Inter-Chip Control을 포함한다. 호스트 PC에서 전달된 명령은 Control FPGA에서 처리되어 Main FPGA 내부 레지스터 접근, AES 실행 제어, 데이터 읽기 요청으로 변환된다.

두 FPGA 사이의 제어는 Inter-Chip Control 경로를 통해 수행된다. Control FPGA 내부의 AHB 버스는 호스트 요청과 시스템 제어 블록을 연결하는 공통 접근 경로로 동작하며, Main FPGA 내부 AES 제어 레지스터와 측정 데이터 경로에 대한 접근을 일관된 구조로 제공한다.

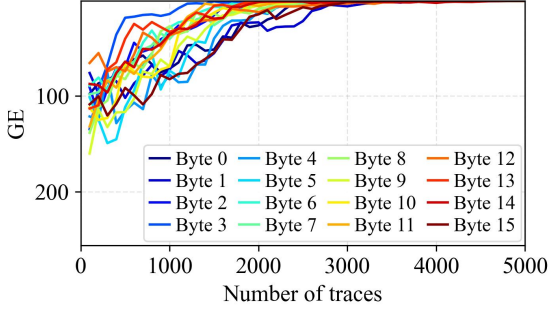
4.2 시스템 동작

제안 시스템의 측정 파형 수집은 호스트 소프트웨어가 Control FPGA를 통해 Main FPGA 내부 레지스터에 접근하는 방식으로 수행된다. 먼저 호스트는 AES 키와 평문, TDC 동작 조건을 설정한 뒤 AES 연산을 실행한다. 연산이 완료되면 암호문을 읽어 하드웨어 AES 결과를 검증하고, AES 동작 중 FIFO에 저장된 TDC 측정 파형을 호스트 PC로 전송한다. 수집된 측정 파형은 평문, 암호문, 키 정보와 함께 저장되어 이후 CPA 분석에 사용된다.

기존 외부 전력 계측 방식은 FPGA 보드 제어와 계측 장비 제어를 동시에 수행해야 한다. 반면 제안 시스템은 TDC 전압 센서를 FPGA 내부에 포함하므로 별도의 외부 측정 장비가 필요하지 않다. 암호 연산 제어와 측정 파형 수집이 동일한 호스트 제어 흐름에서 수행되므로 수집 절차가 단순해지고, 상용 계측 장비를 추가하지 않아도 부채널 분석 시스템을 구성할 수 있다. 따라서 제안 시스템은 구현 비용과 수집 난이도를 낮추는 동시에 내부 계측 기반의 부채널 분석을 가능하게 한다.



(a) ChipWhisperer 계측



(b) TDC 계측

그림 5. 측정 파형 수에 따른 GE 변화

V. 실험 결과

5.1 실험 환경

실험은 SAKURA-X 기반 Dual-FPGA 환경에서 수행하였다. 대상 암호는 FPGA 하드웨어 AES-128 코어이며, AES 코어는 5 MHz 클럭으로 동작한다. 제안 시스템에서는 Main FPGA 내부에 배치된 8개의 TDC 전압 센서를 사용하였고, TDC 샘플링 클럭은 200 MHz로 설정하였다.

성능 비교를 위해 ChipWhisperer 기반 외부 전력 계측 방식으로도 동일한 AES 구현의 측정 파형을 수집하였다. ChipWhisperer의 샘플링 주파수는 200 MHz, 아날로그 이득은 55 dB로 설정하였다.

두 계측 방식은 동일한 AES 키와 난수 평문 입력을 사용하여 파형을 수집하였다. 키 추정값에 따른 누설 모델과 측정 파형 사이의 상관관계를 이용하는 부채널 분석 기법인 CPA(Correlation Power Analysis)[3]를 사용하여 두 계측 방식을 평가하였다.

표 2. 키 바이트별 평균 키 복구 측정 파형 수

KeyBytes	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CW Trace	4300	4100	4700	2900	2100	1900	4200	2500	4000	2100	4400	3300	2500	2000	4200	2800
TDC Trace	2420	2530	1850	1130	2320	1870	1720	2090	1750	1960	1700	1730	1990	1250	1950	2370
Diff. (%)	43.7	38.3	60.6	61.0	-10.5	1.6	59.0	16.4	56.2	6.7	61.4	47.6	20.4	37.5	53.6	15.4

5.2 CPA 수행 결과

본 실험에서는 AES 마지막 라운드 CPA 결과에서 각 키 바이트의 Guessing Entropy(GE)가 1에 도달하는 측정 파형 수를 키 복구 기준으로 사용하였다. GE=1은 실제 키 후보가 상관계수 순위 1위에 도달했음을 의미한다. 그림 5는 측정 파형 수에 따른 GE 변화를 나타내며, 표 2는 10회 반복 실험의 키 바이트별 평균 결과를 정리한다.

ChipWhisperer 기반 외부 전력 측정 파형은 키 바이트별 평균 3250개의 측정 파형이 필요하였다. 반면 제안 시스템의 TDC 측정 파형은 평균 1914개의 측정 파형에서 키 복구 기준에 도달하였다. 이는 평균 41.1%의 측정 파형 감소에 해당한다.

VI. 결론

FPGA 내부에 TDC 전압 센서를 내장한 저비용 부채널 분석 시스템을 구현하였다. 제안 시스템은 외부 계측 장비 없이 AES 연산의 측정 파형을 수집하며, ChipWhisperer 기반 외부 전력 계측보다 적은 측정 파형으로 키 복구 기준에 도달하였다. 이는 내장형 TDC 센서가 국소 전압 변동을 활용한 부채널 계측에 유효함을 보인다.

Acknowledgments

This work was supported by the NRF (No. 2022R1A5A8026986) and the MSIT/IITP under ITRC program (IITP-2025-RS-2024-00436406).

참고문헌

- [1] T. Katashita et al., "Development of Side-Channel Attack Standard Evaluation Environment," in Proc. ECCTD, 2009, pp. 403-408.
- [2] S. Moini et al., "Voltage Sensor Implementations for Remote Power Attacks on FPGAs," ACM TRETs, vol. 16, no. 1, Art. no. 11, 2022.
- [3] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in Proc. CHES, 2004, pp. 16-29.