초기 지연 가변 TDC 전압 센서를 활용한 FPGA 부채널 분석 시스템 구현

노윤진, 김은세, 유호영
충남대학교 공과대학 전자공학과

Side Channel Analysis System based on FPGA Using Delay Controllable TDC Voltage Sensor

Yunjin Noh, Eunse Kim, Hoyoung Yoo
Electronics Engineering Department
Chungnam National University
E-mail : yjnoh.cas@gmail.com, ddongse55@gmail.com, hyyoo.cnu@gmail.com

Abstract

This paper presents a side-channel analysis system using delay Controllable TDC(Time-to-Digital Converter). The proposed system performs encryption, samples power traces, and transmits data to a PC for analysis. Proposed system successfully extracted one byte of an AES(Advanced Encryption Standard) key with 8,900 traces, demonstrating its effectiveness for cryptographic security evaluation and its potential for designing more secure hardware.

I. 서론

FPGA(Field-Programmable Gate Array)는 높은 유연성과 낮은 개발 비용으로 인해 다양한 분야에서 활용되고 있으며, 특히 암호화 하드웨어 연구에 중요한 역할을 하고 있다. 부채널 공격은 하드웨어가 동작하는 동안 발생하는 물리적 특성을 이용해 민감한 정보를 추출하는 공격 기법으로, 암호화 시스템에 심각한 위협이 된다. 그 중 전력 분석 공격은 칩의 전력 소비 패턴을 측정하고 이를 바탕으로 암호화 알고리즘의 내부 동작을 역추적하여 암호키를 추출하는 방식이다[1]. 이 방법은 상대적으로 간단한 측정 장비와 알고리즘으로도 실행 가능하기 때문에 암호화 하드웨어 설계에서 매우 중요한 보안 문제로 여겨진다.

암호화 하드웨어 개발 시에는 전력 기반의 부채널 공격에 대한 취약성을 파악할 필요성이 있다. 따라서 본 연구에서는 FPGA 내부에서 작동하는 초기 지연 가변 TDC(Time-to-Digital Converter) 전압 센서를 활용하여 부채널 분석 시스템을 구현하였다.

This research was supported by National Research Foundation of Korea(NRF) funded by the Korea government(MSIT) (IITP-2024-RS-2024-00436406 (50%), 2020M3H2A1078119) and by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2022R1A5A8026986)

II. FPGA 부채널 분석 시스템 구현

개발한 부채널 분석 시스템은 그림 1과 같다. SAKURA-X Main FPGA 내에 부채널 분석 대상인 암호화 모듈과 함께 초기 지연 가변 TDC 전압 센서를 사용하여 구현된다. GPIO(General-Perpose I/O), BRAM(Black Random Access Memory), UART(Universal Asynchronous Receiver Transmitter), Microblaze와 같은 모듈은 Xilinx에서 제공하는 IP를 활용하였다. TDC 전압 센서는 시간을 측정하는 TDC(Time-to-Digital Converter) 회로를 기반으로 만들어졌으며 소자의 입력 전압에 따른 전파 지연 시간의 변화를 이용하여 전압을 측정한다[2].

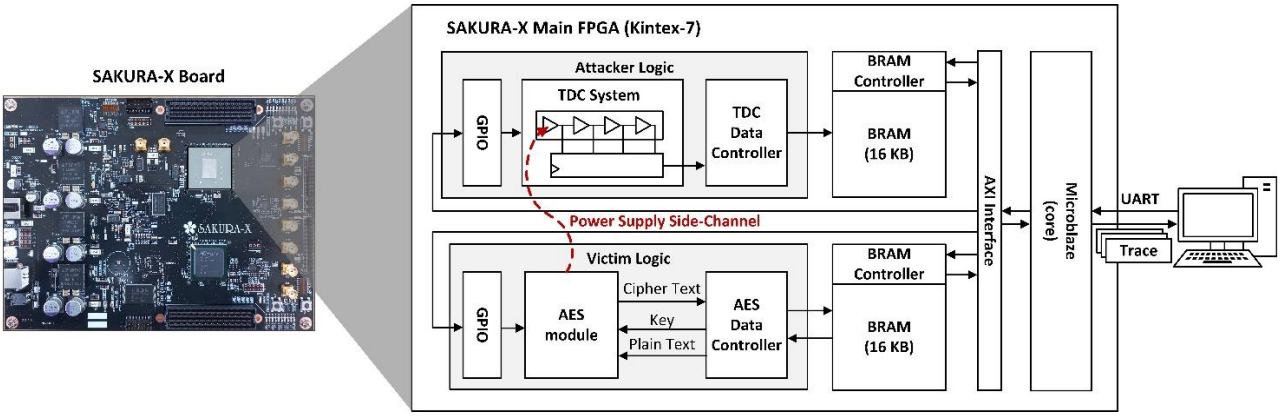

그림 1. SAKURA-X 부채널 분석 시스템 블록 다이어그램

기존 TDC 전압 센서는 초기 지연이 고정되어 있어 실험 환경에 따라 초기 지연 라인의 길이를 조정해야 하는 어려움이 있다. 하지만 제안한 시스템에 사용된 초기 지연 가변 TDC 전압 센서는 초기 지연 정도를 코어에서 조절할 수 있어 효율적으로 전압을 측정할 수 있다.

본 연구에서는 개발한 시스템을 활용하여 AES 암호화 모듈에 대해 부채널 분석을 수행하였다. 시스템의 동작 과정은 다음과 같다. 먼저 사용자 PC 에서 UART 통신을 사용하여 수행할 암호화 횟수를 전송한다. 이후 부채널 분석 시스템은 AES 암호화를 수행하는 동시에 TDC 전압 센서를 샘플링하고 샘플 값을 BRAM 에 저장한다. AES 가 수행되는 동안 측정된 전력 파형은 그림 2 와 같다. 측정된 전력 파형과 암호화된 데이터는 UART 통신을 통해 사용자의 PC 로 전송된다. 사용자는 수집된 전력 데이터를 통해 전력 분석 공격인 CPA(Correlation Power Analysis)를 사용하여 암호화 모듈의 암호키를 추출해 낼 수 있다.

III. 결론

본 연구에서는 SAKURA-X 의 Main FPGA 에 가변 지연 TDC 전압 센서를 활용한 부채널 분석 시스템을 활용하여 AES 암호화 모듈을 대상으로 전력 분석 공격을 수행하였다. 공격은 AES 의 마지막 라운드에서 이루어졌으며 암호키 한 바이트를 알아내는데 평균 8900 트레이스가 사용되었다.

제안한 FPGA 부채널 분석 시스템을 활용하면 암호화 모듈에 대한 부채널 공격을 직접 수행하여 부채널 취약성을 평가할 수 있다.

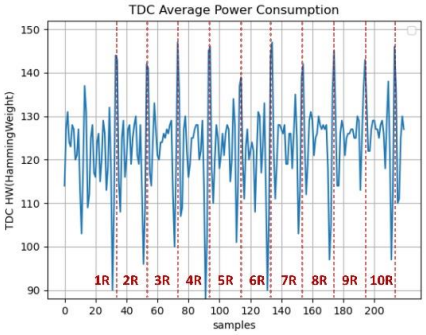

그림 2. AES 암호화 모듈 전력 소비 패턴

참고문헌

[1] Khawaja, A., Landgraf, J., Prakash, R., Wei, M., Schkufza, E., & Rossbach, C. J. (2018, October). Sharing, Protection, and Compatibility for Reconfigurable Fabric with AmorphOS. 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI 18), 107–127

[2] Moini, S., Deric, A., Li, X., Provelengios, G., Burleson, W., Tessier, R., & Holcomb, D. (2022, December). Voltage Sensor Implementations for Remote Power Attacks on FPGAs. ACM Transactions on Reconfigurable Technology and Systems, 16(1), Article 11, 1-21.