FPGA 내 TDC 센서를 활용한 CPA 기반 AES-128 암호화 키 추출

노윤진, 양희훈, 엄유진, 유호영
충남대학교 전자공학과
e-mail : yjnoh.cas@gmail.com, hhyang.cas@gmail.com, yjeom.cas@gmail.com, hyyoo@cnu.ac.kr

AES-128 Encryption Key Extraction Based on CPA Using TDC Sensors in FPGA

Yunjin Noh, Heehun Yang, Yujin Eom, and Hoyoung Yoo
Dept.of Electronics Engineering,
Chungnam National University

Abstract

Implementing TDC (Time-to-Digital Converter) sensors in FPGAs allows monitoring voltage fluctuations caused by internal logic activities. TDC sensors are more sensitive to small voltage changes than RO (Ring Oscillator) sensors, making them effective for side-channel attacks. This study implements a TDC sensor-based side-channel attack circuit on an FPGA using the SAKURA-X board and AES-128 encryption. The effectiveness is demonstrated by successfully extracting the AES-128 secret key using CPA (Correlation Power Analysis).

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A5A8026986), and supported by Basic Science Research 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)

I. Introduction

현대 회로 산업에서는 ASIC(Application Specific Integrated Circuit)에 비해 낮은 개발비용과 활용도가 높은 이점으로 FPGA(Field-Programmable Gate Array)를 활용한 연구 및 개발이 활발히 이루어지고 있다. 특히 여러 사용자가 동시에 클라우드로 하나의 FPGA 칩을 사용하는 시나리오에 대한 관심이 증가하고 있다[1]. FPGA 플랫폼에 대한 원격 액세스는 새로운 종류의 보안 위협인 on-chip 부채널 공격 가능성을 제공한다. 부채널 공격은 SoC의 전력 소비 패턴과 실행 시간 등을 분석하여 SoC에 들어있는 암호화 키나 정보 등을 추출하는 것을 말한다. 기본적으로 FPGA 내의 PDN(Power Distribution Network)은 일정한 크기의 전압 공급을 하는 것을 목표로 설계되어 있다. 하지만 실제로는 내부 로직 활동에 의해 전압 공급에 변동이 발생하며, FPGA 내에 TDC 또는 RO 센서를 구현하면 PDN의 전압 변동을 모니터링할 수 있다. 이런 모니터링은 클라우드 기반의 다중 사용자 FPGA 환경에서 다른 사용자의 로직을 대상으로 부채널 공격을 시도할 수 있는 잠재적인 위험 요소로 활용될 수 있다. TDC 센서와 RO센서는 모두 소자의 전파 지연 특성을 기반으로 하는 전압 센서이다. 특히 TDC 센서는 RO 센서 보다 작은 전압 변동을 더 잘 감지하여 암호화 알고리즘의 비밀키를 찾는

부채널 공격에 적합하다. TDC 센서를 사용한 공격은 상대적으로 저비용에 높은 정밀도를 제공하여 효과적인 부채널 분석을 가능하게 한다. 또한 공격자가 간단한 장비와 기술만으로도 효과적인 공격을 수행할 수 있어 다양한 공격 시나리오에 적용될 수 있다. 이러한 이유들 때문에 FPGA 산업에서 TDC센서를 이용한 암호화 키 추출은 매우 심각한 보안 위협으로 간주된다. TDC를 활용한 공격 시도를 통해 시스템이 실제로 얼마나 취약한지 평가할 수 있으며, 이를 바탕으로 보안 개선 방안을 마련할 수 있다.

본 논문에서는 FPGA on-chip에서 부채널 공격 취약성을 확인하기 위해 TDC 센서 기반 부채널 공격 회로를 구현하였다. 성능 검증을 위해 SAKURA-X 보드 환경에서 실험을 진행하였으며, AES-128 암호화 알고리즘과 TDC 전압 센서를 사용하여 CPA를 수행했다. AES-128 암호화 알고리즘의 암호키를 추출함으로써 구현된 부채널 공격 회로의 성능을 평가하였다.

II. Proposed Design

2.1 TDC 전압 센서

TDC(Time-to-Digital Converter)는 소자의 전파 지연을 이용하여 시간을 디지털 데이터로 변환하는 장치이다. CMOS 소자에서 전압이 증가하면 MOSFET의 채널이 더 넓게 열리면서 전류가 더 쉽게 흐를 수 있다. 이로 인해 노드의 용량 충전 속도가 빨라지고, 결과적으로 신호 전파 지연 시간이 짧아진다. 반대로, 전압이 감소하면 MOSFET의 채널이 좁아지고 전류가 줄어들어 노드의 용량 충전 속도가 느려져 신호 전파 지연 시간이 길어진다[3]. 전파 지연 시간과 전압 사이의 관계를 이용하여, TDC는 지연 라인을 통해 신호의 전파 지연 시간을 측정하고 전압 변동을 감지할 수 있다. TDC의 지연 라인은 논리 게이트 또는 버퍼로 구성된 일련의 지연 요소들로 구성된다. TDC의 지연 라인에 입력 신호를 주면, 신호는 각 지연 요소를 순차적으로 통과하게 된다. 이때 특정 시점에서 지연 라인의 상태를 캡처하면 신호가 얼마나 많은 지연 요소를 통과했는지 알 수 있다. 전파 지연 시간이 짧을수록 신호가 더 많은 지연 요소를 통과하므로 지연 라인에서 "1"의 개수를 세는 방식으로 회로의 전압 변동을 유추할 수 있다. TDC 전압 센서는 초기 지연 라인, 관측 지연

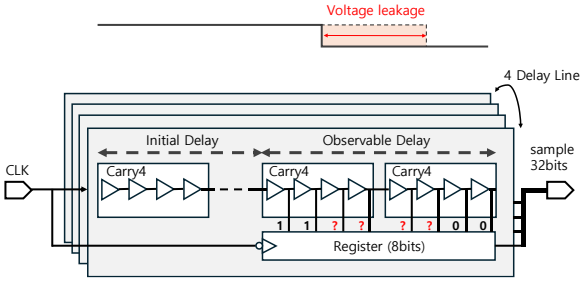

그림1. TDC 센서 구조

라인, 레지스터로 구성된다. 지연 라인에서 전압변동에 의한 상태 변화가 나타나는 부분을 관측 지연 라인으로 설정한다. 레지스터는 관측 지연 라인의 상태를 샘플링하고 저장한다. 지연 라인에서 전압 변동에 의한 상태 변화가 나타나지 않는 부분은 초기 지연라인이다. 초기 지연 라인의 조정을 통해 TDC 전압 센서의 정확도를 높일 수 있다[4].

본 논문에서는 그림 1과 같이 CARRY4 로직을 사용하여 4개의 딜레이 라인으로 구성된 TDC 전압 센서를 구현하였다. 각 딜레이 라인은 8개의 CARRY4 로직을 직렬로 연결하여 구성되었다. CARRY4는 Xilinx FPGA에서 제공하는 빠르게 캐리를 연산하기 위한 논리 요소로, 신호 전파 지연 시간이 매우 짧아 TDC의 지연 라인에 사용하기 적합하다. 각 딜레이 라인에서 전압 변동을 8비트씩 캡처하며, 4개의 딜레이 라인을 통해 총 32비트의 TDC 데이터가 레지스터에 저장된다. TDC 전압 센서는 100MHz의 클럭으로 샘플링 된다.

2.2 AES-128 암호화 알고리즘

AES(Advanced Encryption Standard)는 2001년 미국 국립표준기술연구소(NIST)에 의해 발표된 대칭 블록 암호이다. 대칭 블록 암호는 동일한 키가 암호화와 복호화에 모두 사용되는 데이터 암호화 알고리즘의 한 유형이다[5]. 따라서 대칭 블록 암호의 비밀키를 알아내면 복호화 과정을 통해 암호로부터 원문을 알아낼 수 있다. AES는 기본적으로 128bit의 평문을 암호화하며, 암호화 과정에 사용되는 암호키의 길에 따라 AES-128, AES-192, AES-256로 종류가 나뉜다. AES-128 암호화 과정은 초기 변환과 10개의 라운드로 구성된다. AES의 각 라운드는 해당 라운드의 라운드키를 사용하여 암호화를 진행한다. AES-128의 키 확장 알고리즘은 입력으로 초기 암호키를 받아 10개의 확장된 키들을 생성하며 확장된 키는 각 라운드에 사용되는 라운드 키로

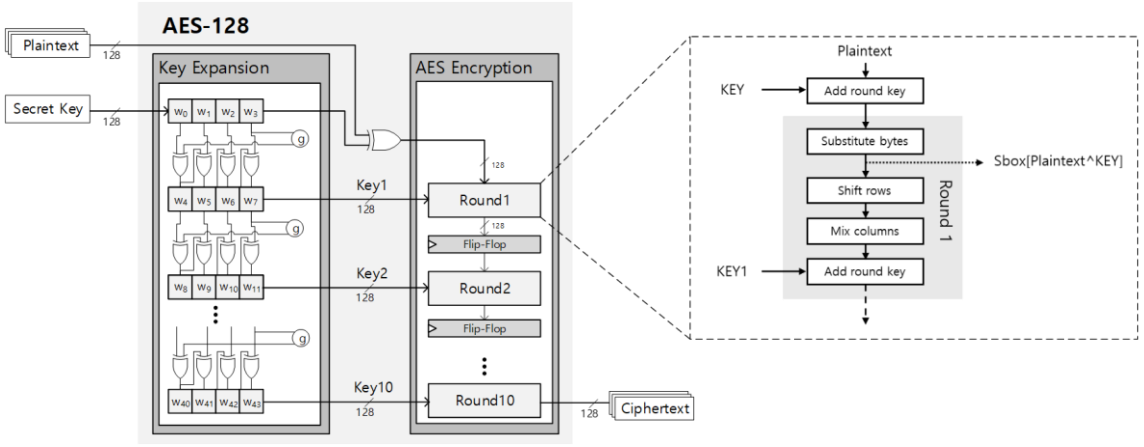

그림 2. AES 알고리즘 블록 다이어그램

사용된다. 초기 변환은 암호키와 평문의 XOR 연산으로 이루어진다. AES의 각 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundkey의 단계로 이루어진다. SubBytes 단계는 S-box라는 look-up table에 따라 각 바이트가 다른 바이트로 대체되는 단계이다. ShiftRows는 행 이동 변환으로, 데이터의 각 행이 일정 수의 스텝만큼 순환적으로 밀리는 단계이다. MixColumns는 열 혼합 변환으로, 상태 행렬의 각 열이 새로운 값으로 변환된다. 마지막으로 AddRoundkey 단계는 라운드 키를 데이터에 XOR 연산을 수행하는 단계이다.

본 논문에서 구현한 AES-128 암호화 알고리즘은 각 라운드의 연산 결과를 레지스터에 저장 후 다음 라운드로 넘어가도록 설계하였다. 한 라운드의 연산에 1클럭이 소요되고, 전체 암호화 과정에는 10클럭이 소요된다.

2.3 CPA(Correlation Power Analysis) 공격

CPA는 전력 분석 공격의 한 형태로, 암호화 기기에서 수행되는 연산 중 발생하는 전력 소비 변동을 분석하여 암호키를 추출하는 기법이다[6]. CPA 공격은 전력 소비 패턴과 키의 후보들 간의 통계적 상관관계를 계산하여 올바른 키를 찾아낸다. CPA 수행 시 공격자는 특정 연산에 대한 전력 소비 모델을 설정한다. AES의 경우, 가장 일반적으로 사용되는 모델은 S-box의 입력 데이터와 출력 데이터 사이의 HD(Hamming Distance)이다. n비트 길이의 두 데이터 x, y 사이의 HD는 아래와 같이 계산한다(1).

$$\mathrm{HD}(x,\ y) = \sum_{i=0}^{n}(x \oplus y)_i \qquad (1)$$

위 수식에서 $(x \oplus y)_i$는 $x \oplus y$의 i번째 비트이다. 입력과 출력 사이의 HD의 값이 클수록 데이터 값의 변동이 크므로 전력 소비가 클 가능성이 높다. 이러한 전력 소비 모델로 특정 연산 수행 시 전력 소비가 얼마나 발생하는 지 예측할 수 있다. 설정한 전력 소비 모델을 실제 측정된 전력 소비와 비교하여 회로에서 수행된 연산을 예측할 수 있다. 각 키 후보에 대해 예측된 전력 소비와 실제 측정된 전력 소비 사이의 피어슨 상관계수ρ를 계산하고, 상관계수 점수가 가장 높은 키가 올바른 키로 간주된다. 예측된 전력 소비를 P_p, 측정된 전력 소비 P_m 사이의 상관계수ρ는 아래와 같이 계산한다(2).

$$\rho(\mathrm{P_p}, \mathrm{P_m}) = \frac{cov(\mathrm{P_p}, \mathrm{P_m})}{\sigma_x \sigma_y} \qquad (2)$$

본 논문에서는 AES의 첫번째 라운드에 대해 CPA를 수행하여 암호키를 알아내는 것을 목표로 한다. AES의 첫번째 라운드는 그림 2와 같이 진행되므로 전력 소비 모델을 Plaintext와 첫번째 Substitute bytes 결과 사이의 HD로 선정하였다.

Ⅲ. Experimental results

3.1 전체 시스템

본 논문에서 구현한 시스템은 SAKURA-X의 main FPGA(Kintex-7)에 소프트 코어인 Microblaze를 이용하여 그림 3과 같이 구성하였다. 회로의 동작은 다음과 같다. 코어에서 AXI BUS를 통해 BRAM에 암호화될 평문을 저장하고, AES-128 모듈은 BRAM에서 해당 데이터들을 읽어와 암호화 연산을 수행하고 코어에 전달한다.

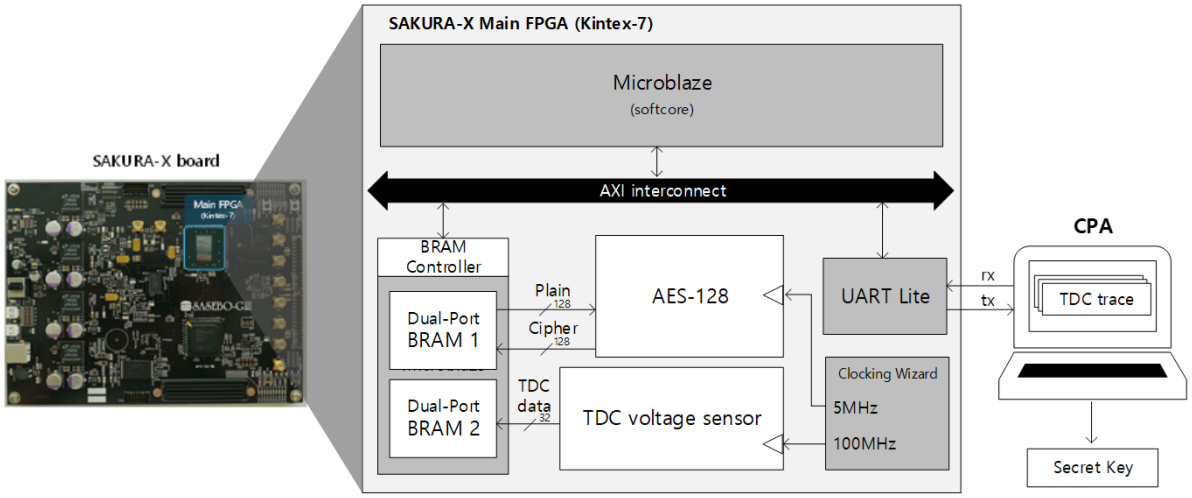

그림 3. 전체 시스템의 블록 다이어그램

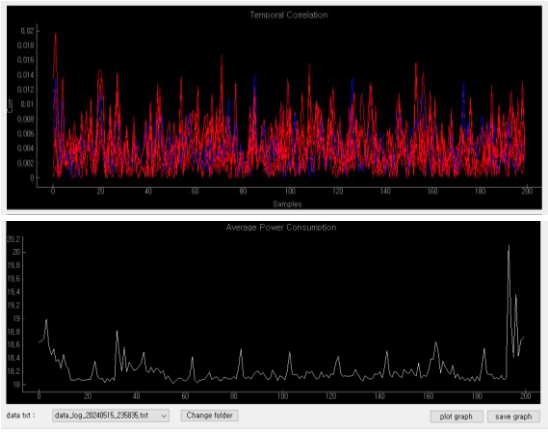

그림 4. CPA GUI 인터페이스 (Python)

AES-128 연산에는 5MHz의 클럭이 사용되며 각 라운드마다 한 클럭을 소요하여 암호화가 수행된다. 암호화가 진행되는 동안 TDC는 100MHz로 샘플링 되며 한 번의 암호화가 진행되는 동안 200번 샘플링 된다. 샘플링된 TDC 데이터와 암호문은 최종 BRAM에 저장되며 UART를 통해 BRAM에서 PC로 데이터가 전송된다.

3.2 CPA 수행 알고리즘

CPA 수행 알고리즘은 데이터 수집, 전력 소비 모델 설정, 상관관계 계산 순서로 수행된다. 데이터 수집 단계에서는 UART 인터페이스를 통해 SAKURA-X 보드로부터 TDC 전압 센서의 데이터와 AES-128 암호화 모듈의 입력 데이터인 평문을 전달받는다. 앞서 서술하였던 것처럼 전력 소비 모델은 AES Plaintext와 첫번째 Substitute bytes 결과 사이의 HD로 설정하였다. 모든 예측키에 대해 예측 소비 전력과 TDC 센서를 사용하여 측정된 소비 전력에 대해 상관 계수를 계산하고, 상관 계수의 값이 가장 큰 키를 예측키로 선택한다. 상관 계수 계산과 키 예측은 바이트 단위로 연산 된다. 실제 암호키를 알아내는 데에는 19,800개의 TDC 트레이스가 CPA에 사용되었다. 그림 4의 상단에 있는 그래프는 예측한 키의 상관 계수(빨간색)과 실제 키의 상관 계수(파란색)를 나타내고, 하단의 그래프는 전체 암호화 과정 동안 수집된 TDC 데이터의 평균 값을 나타낸다.

Ⅳ. Conclusion

본 논문에서는 TDC 전압센서와 AES-128 암호화 알고리즘이 구현된 시스템을 FPGA 내부에 구현하고, TDC 데이터를 통해 AES의 암호화 키를 알아내는 CPA 부채널 공격을 성공적으로 수행하였다. 이 결과는 CARRY4 로직을 사용하는 TDC 전압 센서가 부채널 공격에 효과적으로 활용이 가능함을 나타낸다. 제안한 TDC 전압 센서를 사용하여 IoT 분야에 제안되는 암호화 알고리즘인 DSEL, LBlock, TWINE 등에 대해서 부채널 취약성을 분석할 예정이다.

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] Shayan Moini, Aleksa Deric, Xiang Li, George Provelengios, Wayne Burleson, Russell Tessier, and Daniel Holcomb. 2022. Voltage Sensor Implementations for Remote Power Attacks on FPGAs. ACM Trans. Reconfigurable Technol. Syst. 16, 1, Article 11 (March 2023)

[3] A. Mantyniemi, T. Rahkonen and J. Kostamovaara, "A CMOS Time-to-Digital Converter (TDC) Based On a Cyclic Time Domain Successive Approximation Interpolation Method," in IEEE Journal of Solid-State Circuits, vol. 44, no. 11, pp. 3067-3078, Nov. 2009

[4] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, Philippe Loubet-Moundi, Olivier Francis. Remote Side-Channel Attacks on Heterogeneous SoC. Smart Card Research and Advanced Applications, 18th International Conference, CARDIS 2019, Nov 2019, Prague, Czech Republic.

[5] H. S. Deshpande, K. J. Karande and A. O. Mulani, "Efficient implementation of AES algorithm on FPGA," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, India, 2014, pp. 1895-1899

[6] Brier, Eric & Clavier, Christophe & Olivier, Francis. (2004). Correlation Power Analysis with a Leakage Model. Proc of Cryptographic Hardware and Embedded Systems. 3156. 16-29. 10.1007/978-3-540-28632-5_2.