FPGA 활용 Ring Oscillator 기반 전압 센서 구현

구교덕, 유호영
충남대학교 전자공학과 소속
e-mail : gdku.cas@gmail.com, hyyoo@cnu.ac.kr

Implementation of a Ring Oscillator-based voltage sensor in FPGA

Kyoduk Ku and Hoyoung Yoo
Chungnam National University

Abstract

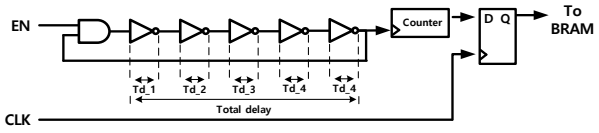
This paper aims to mitigate side-channel attacks by measuring leakage power. To achieve this, we implemented a ring oscillator-based voltage sensor within an FPGA. The circuit used to measure the leakage power is an overclocking waster circuit, which enables us to assess the leakage power both under load and no-load conditions. Our approach provides a detailed analysis of the power consumption patterns, which can be critical for enhancing the security of cryptographic devices against side-channel attacks. Experimental results demonstrate the effectiveness of our method in detecting variations in leakage power, thereby contributing to the development of more secure hardware designs.

I. 서론

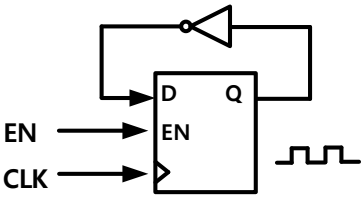
부채널 공격은 최근에 많은 관심을 받는 보안 위협 방법 중 하나이다. 이러한 공격은 비밀 정보를 유출하거나 전체적인 시스템을 훼손할 수 있는 위험성을 내포하고 있다. 전력 측정은 부채널 공격을 탐지하기 위한 주요 방법 중 하나로 인정받고 있다. 이를 위해 RO(Ring Oscillator)와 같은 전력을 측정할 수 있는 전압 센서가 사용되어 왔다.[1] RO는 간단한 구조와 낮은 복잡도로 회로를 구현하고 사용하기 쉽다는 특징이 있다. 따라서, 본 논문에서는 RO를 이용한 전압 센서를 구현하여 보드의 누설 전력을 측정한다. 이때, 측정하는 대상 회로는 Waster 회로를 사용한다. 해당 회로를 사용하여 보드에 부하를 가해 주며 부하가 걸릴 때와 안 걸릴 때 RO의 Count 값을 비교하여 전력 소비 및 시스템 성능을 분석한다.

II. 배경지식

RO는 다수의 inverter가 묶인 inverter chain을 활용하여 inversion된 출력 신호를 다시 입력으로 넣어 발진시키는 회로이다. 본 논문에서는 RO의 inverter 개수를 5개로 설정하여 구현한다. Waster 회로는 일반적으로 필요하지 않은 리소스를 소모하거나 성능을 저하시키는 회로를 의미한다. 이러한 회로는 설계 과정에서 실수로 남아있거나, 최적화되지 않은 코드로 인



(a) RO



(b) Waster Circuit

그림 1. Waster 회로 및 RO

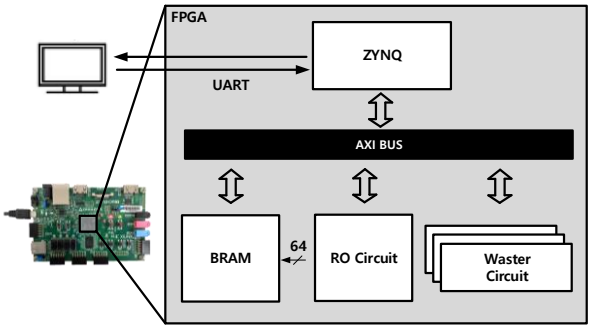
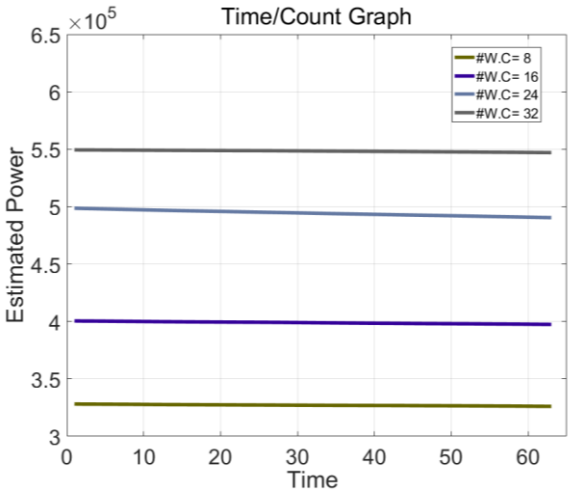


그림 2. 전체 Block Diagram

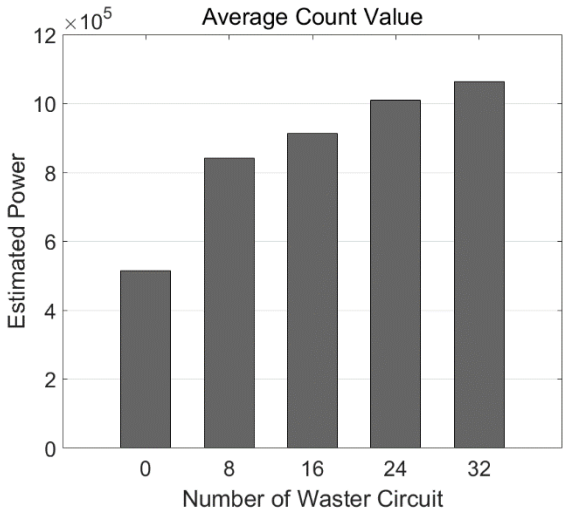
해 발생할 수 있다. Waster 회로는 FPGA의 효율성을 떨어뜨리고, 전력 소비를 증가시키며, 전체 시스템 성능을 저해할 수 있다. 이러한 Waster 회로를 특수한 목적을 갖고 구현할 수도 있는데, 그 방식에는 Gated Waster, Dynamic Waster, Clock Gating Waster, Overclocking Waster 등 다양한 종류가 있다. 본 논문에서는 특정 기간에만 clock 신호를 추가적으로 유발하여 전력 소모를 발생시키는 Overclocking Waster 회로를 구현한다.

Ⅲ. RO를 활용한 전력 측정 회로

그림 2에는 RO 및 Waster 회로들이 Core인 ZYNQ에 연결되는 전체적인 흐름을 Block Diagram으로 나타내



(a) 시간 축



(b) 평균값

그림 3. 실험 결과

었다. RO 회로에서 BRAM에 count 값을 해당 주소에 맞춰 전달해 준다. ZYNQ에서는 BRAM에 저장된 값과 그 때의 주소 값을 UART 통신을 통해 PC로 전달해 주는 구조를 갖고 있다. RO 회로는 inverter 5개로 구성된 일반적인 형태로 구현하였다. RO 기반 전압 센서에서 누설 전력을 측정하는 방법은 다음과 같다. Waster 회로에서 발진이 발생하였을 때 발생하는 누설 전력 때문에 RO의 각 inverter들을 통과할 때 생기는 딜레이 값(Td)에 변화가 생기게 되고, 최종적으로 전체 딜레이 값(Total delay)이 달라져 RO의 출력

주파수가 달라지게 된다. 이 주파수의 차이를 확인하여 보드 내부의 누설 전력을 측정할 수 있다. Waster 회로 모듈은 외부에서 들어오는 EN_OC 신호가 Active High 일 때 모듈 내부에서 발진이 발생하도록 구현하였다. 본 논몬에서는 Waster 회로의 수를 증가시켜가며 결과를 분석하였다.

Ⅳ. 실험환경 및 실험결과

본 논문에서는, Xilinx Zybo Z7-10 보드를 사용하였고, Vivado Tool 2021.2 버전과 vitis Tool 2021.2 버전을 활용하여 Waster 회로 및 RO 전압 센서의 IP(Intellectual Property)를 구현하였고, BRAM의 주소에 담긴 값을 확인하였다. 구현된 IP를 보드에 올려 동작 주파수 125 MHz로 합성하였다. 본 논문에서 진행한 실험은 그림 1(b)의 EN_OC 신호가 Active High 일 때 Waster 회로의 수를 늘려가며 보드에 부하를 점점많이 주면서 센싱되는 값을 비교하여 측정하였다. BRAM의 각 주소에는 동일한 시간동안 측정된 Power 값을 Count 하여 넣었고, 해당 주소에 Counting된 Power 값을 넣은 뒤 다음 주소에 값을 넣을때 마다 초기화하여 넣었다. 결과는 그림 3에 그래프로 나타내었다. 그림 3(a)에는 시간에 따라 달라지는 Power 값을 나타내었고, 그림 3(b)는 Waster 회로의 갯수에 따른 Power 평균 값을 나타내었다. 두 그래프를 보면 Waster 회로 수가 많을수록 Counting 되는 Power 값이 많아지는 것을 확인할 수 있다.

Ⅴ. 결론

본 논문에서는 Xilinx 사의 Zybo Z7-10 보드를 사용하여 RO기반 전압 센서를 FPGA 내에 구현하여 FPGA 내부에 부하가 걸릴 때와 걸리지 않을때의 누설 전력을 RO 전압 센서에서 측정하였다. 부하를 걸어주는 방법으로는 Overclocking Waster 회로를 활용하였다. 실험 결과는 그림 3와 같이 Waster 회로의 수가 많아질수록 즉, 부하가 보드에 많이 걸릴수록 RO에서 측정된 Power 값이 많아지는 것으로 해석할 수 있다. 이로써, 본 논문에서 구현한 RO기반의 전압 센서로 보드에 부하가 점점 많이 걸릴 때의 Power 값의 변화를 감지하였다. 더불어, 이 연구는 앞으로의 부채널 공격에 대한 이해를 높이고, 회로 설계에 적용할 수 있는 보안 기술을 개발하는 데 기여할 수 있을 것이라 기대된다.

Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A5A8026986), Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2021R1I1A3055806), and National R&D Program through the National Research Foundation of Korea(NRF) funded by Ministry of Science and ICT(2020M3H2A1078119)

참고문헌

[1] SHAYAN MOIBI,ALEKSA DERIC, XIANG LI, GEORGE PROVELENGIOS, WAYNE BURLESON, RUSSELL TESSIER, and DANIEL HOLCOMB “Voltage Sensor Implementations for Remote Power Attacks on FPGAs”, ACM Transactions on Reconfigurable Technology and Systems, Vol. 16, No. 1, Article 11. Pub. December. 2022,

[2] 양희훈, 박지호, 이상원, 유호영 “Programmable Delay Logic을 이용한 링 오실레이터 기반의 실난수 생성기 구현”, 대한전자공학회 2023년도 하계종합학술대회, Jun. 2023,

[3] 정상남, 백상현 “Ring Oscillator를 이용한 신호의 동시 스위칭 밀도 분석”, 2008년 9월 전자공학회 논문지 제 45권 SD편 제 9호