Capstone Summer 2021

University of Windsor

Department of Electrical and Computer Engineering

FPGA Hardware Trojan Power Analysis

Brajan Ilievski
Khanh Hoa Huynh

University of Windsor
thinking forward

Abstract

FPGA hardware trojans pose a security threat due to the rising adoption of FPGAs across many key industries. Trojans are often triggered by rare events, and it is not possible to isolate and test specific components of modern-day ICs with all exhaustive input patterns. Further, the lack of Golden ICs prevents direct comparison of potentially infected ICs with known clean benchmarks. The current industry problem is the lack of mature strategies for detecting and protecting against trojan attacks in FPGAs. Our group set out to demonstrate that power analysis is unable to differentiate the changes in power consumption between a non-infected and infected ISCAS-85 benchmark circuit implemented on an FPGA. Our design is constrained to infecting a 16x16-bit multiplier with a half-adder trojan and measuring AC power consumption during active multiplication. We determined that power consumption of the infected circuit was negligibly impacted, and no significant differences could be measured.

Introduction

The primary objective of this capstone design project is to demonstrate that the power consumption in an infected ISCAS-85 benchmark circuit is unaffected by subtle and malicious hardware. The infected benchmark circuit must demonstrate nearly identical functionality of a clean circuit except for the altered 32-bit output when the circuit is in a trojan state.

In the realm of FPGAs, the current state of the art for the detection of hardware trojans includes several non-destructive methods:

1. Non-invasive logic testing techniques that aim to activate/detect HTs using input test vectors.
2. On-chip sensors to capture any unexpected differentiation in temperature, power, current etc.
3. Side-channel analysis methods to detect physical EM emissions, power, and timing to detect structural changes in the design and compare it to a “golden chip”.

Deliverables

This project required:

1. Develop the Verilog code implementing the infected ISCAS-85 benchmark circuit containing the chosen half-adder trojan.

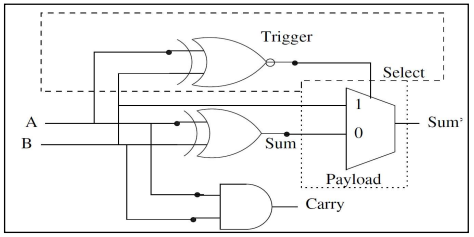


Figure 1: Half-adder trojan logic gates

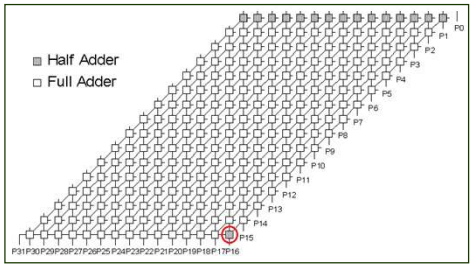


Figure 2: ISCAS-85 C6288 (16x16 Multiplier)

2. Develop methods (Verilog code, python scripts) to capture the power traces of the infected circuit on a target FPGA using ChipWhisperer CW1200 scope and CW308 capture board.

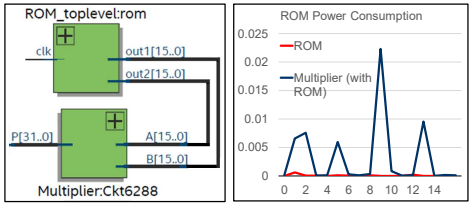


Figure 3: ISCAS-85 C6288 RTL model (with ROM)

3. Verifying operation and outputs of the infected circuit using ModelSim and comparing power traces to a non-infected circuit.

Experimental Results

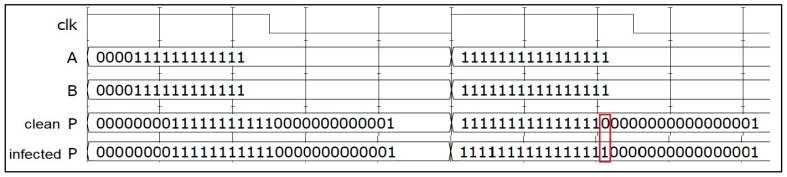
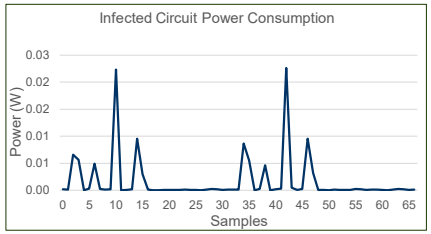


Figure 4: Bit flip (position 16) due to trojan activation



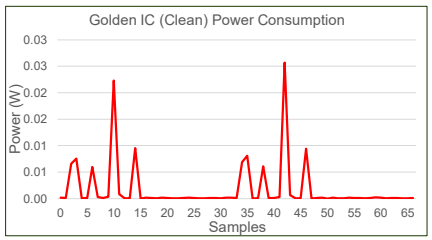


Figure 5: Power draw of clean and infected circuit

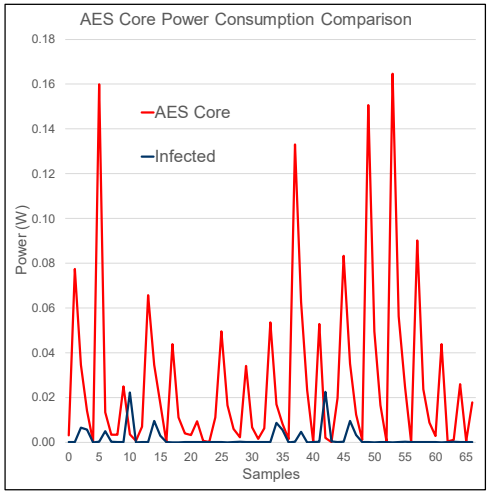


Figure 6: Power draw comparison of standard AES core with an infected circuit

Future Work

Future work can focus on in-depth analysis of captured power traces to elucidate subtle differences in power consumption between clean and infected circuits. This work may involve leveraging machine learning to provide a more powerful analysis of side-channel information. Further experimentation can be pursued with different ISCAS-85 benchmark circuits and trojan combinations to generate additional data for training ML models.

Other exploratory work includes modifying the available Simple Serial communication protocol. This would enable seamless communication between ChipWhisperer software and FPGA target board without relying on a ROM for inputs.

Conclusions

Hardware trojans pose a serious threat to the industry. By displaying the negligible differences between a clean and infected circuit, we have demonstrated the difficulty in isolating and detecting trojans in a simple ISCAS benchmark. The resulting power trace graphs displayed minimal differences that can be attributed to many factors, including but not limited to process variation effects and electrical noise.