Securing the Digital Era

Tristan Brankovic, tristan.brankovic@lilalions.com
International School of Los Angeles, Class of 2019
USC Viterbi Department of Electrical Engineering, SHINE 2018

Introduction

- Security has been a major concern in any computer system. There exists various types of attacks on the hardware that raises major security concerns for the electronic industry.
- Hardware security deals with protecting circuits from these attackers by using different types defense mechanisms like Obfuscation, Split Manufacturing, Gate camouflaging to mention a few.
- But these existing defense mechanism are easily broken by the attacks like:
  - **Hardware Trojan attacks**
  - **Reverse Engineering attacks**
  - **Side channel attacks**
- In this Shine Program I have majorly worked on logic Encryption and its attacks. These attacks are majorly reverse engineering attacks.
- In logic encryption the circuit is secured by obfuscation i.e. hiding the functionality of the circuit by adding extra logic gates known as key gates.
- In order to make the circuit functional, correct key should be always entered. Although this technique sounds robust but currently there exists many strong attacks that can easily break it in seconds!

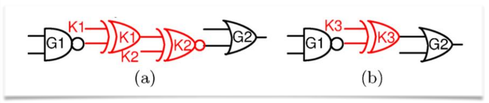
Objective & Impact of Professor's Research

- Professor Nuzzo's research group analyzes different types of hardware security attacks and defense techniques in order to model them with the final objective to design a tool and also formulate metrics that will enable designing of more Secure hardware.
- His research is fundamental to modern society because it aims to protect it.
- This research will enable a multitude of companies to continue developing their technologies and releasing them at a far more accelerated pace.

Evolution of Logic Encryption Attacks & Defenses

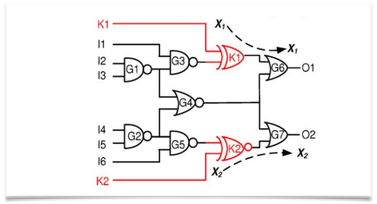
Different types of attacks on Logic Obfuscation:

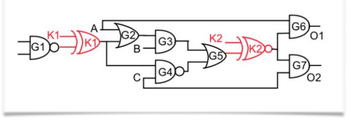
✦**Sensitization attack**: An attack where the attacker propagates a key's value to the primary outputs by muting the effect of the other keys and gates. Examples of Sensitization attacks are:



Runs of keys simplified into a single key

Isolated key gates easily sensitized



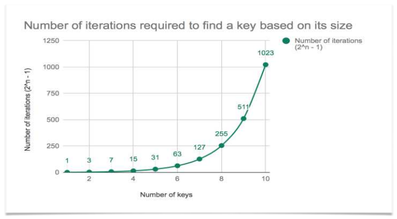


Dominating Key gates

✦ **Sat attack**: An attack where the attacker constantly finds input combinations that when fed to the 'golden chip' and the obfuscated chip will result in outputs that are different. In this way it decreases the search space of the all possible keys by the process of elimination of wrong keys.

✦**Key gate removal attack**: An attack where the attacker finds and removes the key gates thus leaving out only the original circuit.

✦ **Brute force attack**: An attack where the attacker attempts every single key combination until the correct one is found. It is the least optimal & least efficient attack mechanism.



Number of Brute Force attempts needed to recover the correct Key

Different types of Logic Obfuscation techniques and their vulnerabilities:

Random Key Implementation: Key gates are placed randomly in the circuit. This technique is vulnerable to:

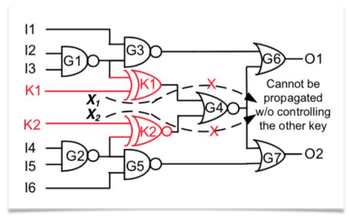
- ✦ **Sensitization attack**
- ✦**SAT attack**
- ✦**Brute force attack**

Fault Logic Locking: Key gates are placed in certain positions based on their fault impact values. This technique is vulnerable to:

- ✦ **Sensitization attack**
- ✦ **SAT attack**
- ✦**Brute force attack**

Security Logic Locking: Key gates are places in a certain position such that they are non mutable with respect to each others. This technique is vulnerable to:

- ✦ **SAT attack**
- ✦ **Brute force attack**



2 non-mutable key gates

Anti-SAT: An anti-SAT block is added to the circuit with keys included which prevents SAT attacks. This technique is still vulnerable to:

- ✦ **Key gate removal attack**

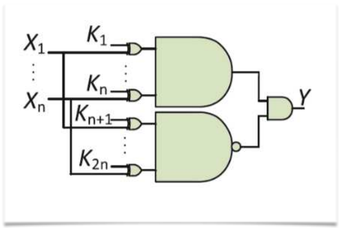


Diagram of the anti-SAT block

Skills Learned & Accomplishments

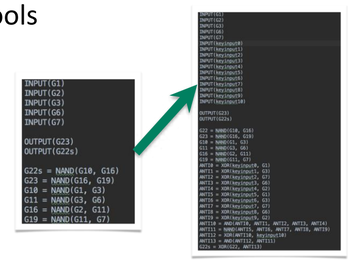
Skills learned

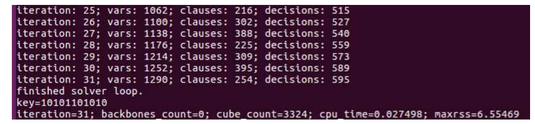
- ✦Digital Circuit basics
- ✦Circuit representation at gate level
- ✦Coding in Python
- ✦Netlist parsing
- ✦Concepts of VLSI Testing - Controllability and Observability measurement of a netlist
- ✦Concepts of Satisfiability
- ✦ SAT attacks on obfuscated netlist
- ✦ Use of de-obfuscation tool
- ✦MATLAB
- ✦Understanding & experiencing research

Accomplishments

- ✦ Creating a circuit simulator in python
- ✦Creating a tool for measuring controllability and observability of a netlist
- ✦ Implementing the Anti-SAT obfuscation technique
- ✦Testing and verifying the security of the implemented Anti-SAT technique using de-obfuscation tools

Complete implementation of Anti-SAT with 10 keys on ISCAS C17 benchmark in Python





Testing the implemented Anti-SAT technique using the De-obfuscation tool

Acknowledgements

I would like to thank Professor Pierluigi Nuzzo, my Ph.D. mentor Subhajit Dutta Chowdhury, Yinghua Hu, Luis Parra, Dr. Mills, Dr. Herrold for all of the help, support, time, and hospitality they've offered to me during my time here!