USC Viterbi
School of Engineering

Attacks to Security of Logic Locking

Muqing (Michael) Zhao, muqingzhao526@gmail.com
Yorba Linda High School, Class of 2022
USC Viterbi Department of Electrical Engineering, SHINE 2021

SHINE
Summer High School Intensive
in Next-Generation Engineering

Introduction

Globalization of the modern integrated circuit (IC) design flow has ushered in many security concerns like IP piracy, design overproduction, and counterfeiting.

Hardware security protects Intellectual properties (IPs) from attackers through various defense mechanisms like logic locking, gate camouflaging, and split manufacturing.

Logic locking adds “keys” to the IPs such that the IP behaves as intended only when the correct key combination is provided.

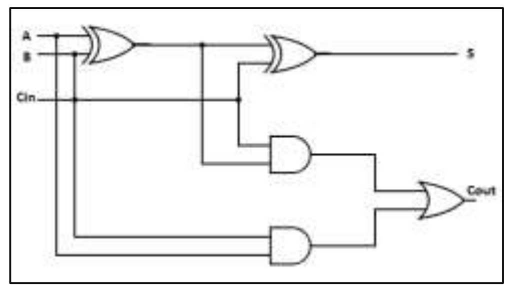
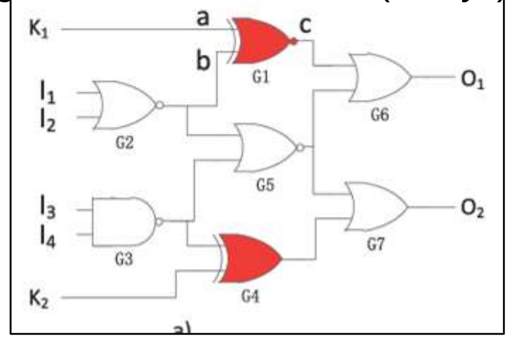


Figure 1.1 Unlocked Circuit.
PC:WatElectronics.com

Figure 1.2Locked Circuit (2 keys)



PC: WatElectronics.com

However, there exists many attacks which try to circumvent logic locking:

- ❑ Boolean Satisfiability (SAT) Attack
- ❑ Removal Attack
- ❑ Machine Learning based Attack

Objective & Impact of Professor’s Research

Professor Nuzzo’s research group focuses on analyzing different attacks on hardware to understand the can's and cannot's of these attacks, bring out the limitation of current defense techniques to offer directions for future research on mitigating the attacks on hardware.

Machine Learning Based Attack on Logic Locking

The overall flow of the Machine learning based attack on logic locking is:

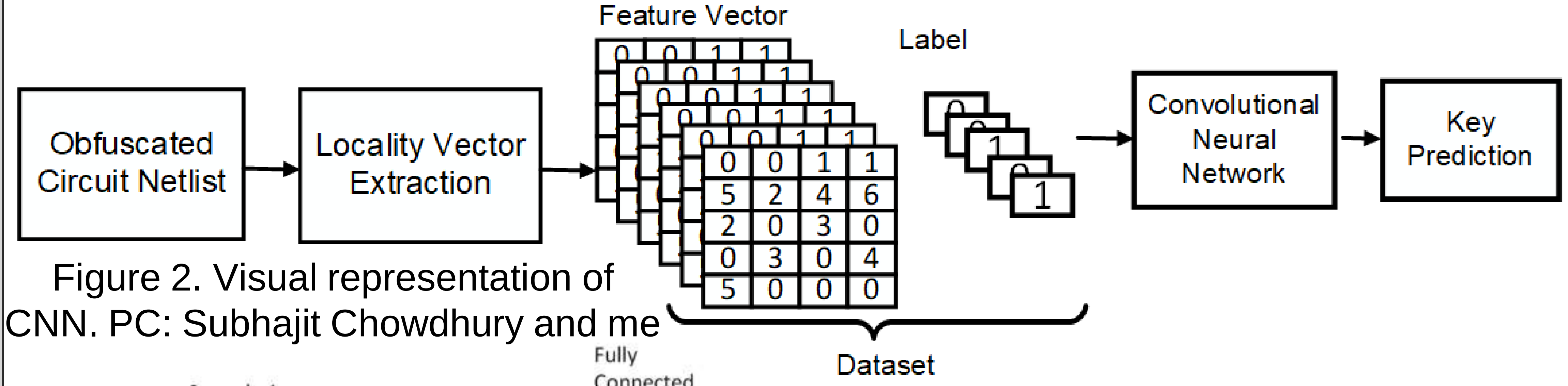
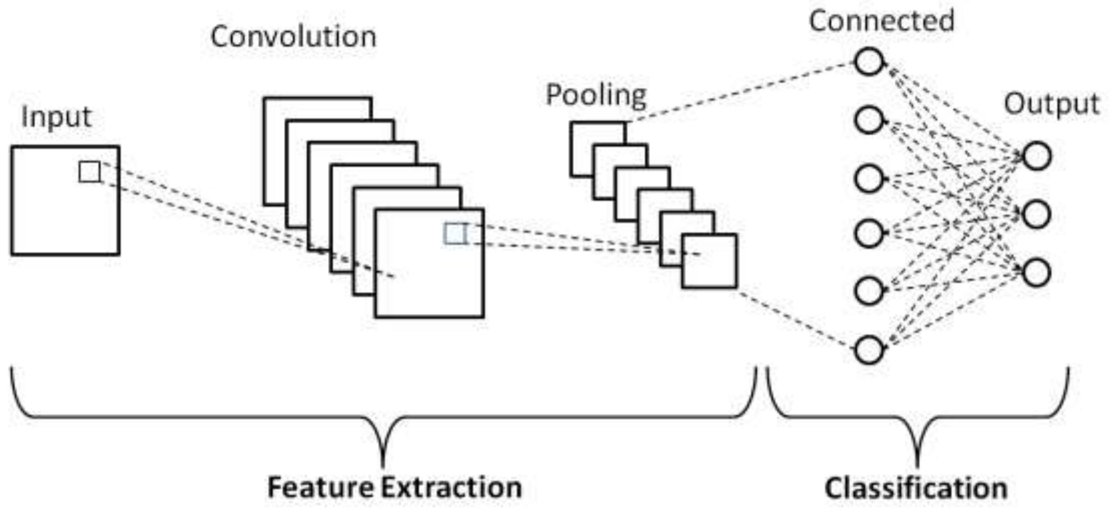

Obfuscated Circuit Netlist
Locality Vector Extraction
Feature Vector
0 0 1 1
5 2 4 6
2 0 3 0
0 3 0 4
5 0 0 0
Label
0
0
1
0
1
Dataset
Convolutional Neural Network
Key Prediction

Figure 2. Visual representation of CNN. PC: Subhajit Chowdhury and me



Convolutional Neural Network Architecture:
4 - 2dConv Layer
1 - MaxPool Layer
2 - Fully Connected Layer

Locality Vector Extraction:

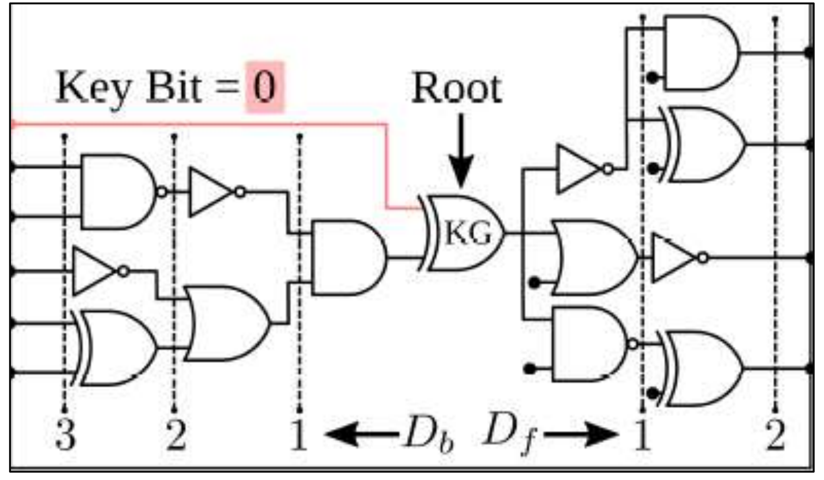
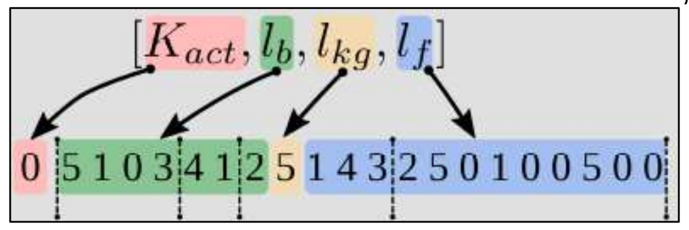


Figure 3.1, 3.2: Extracted LV for KG,
PC: DOMINIK SISEJKOVIC,



Locality Vector contains information about the neighborhood of a key gate

Results: Key Prediction Accuracy for different Benchmark Circuit

Benchmark	c432	c499	c880	c1908	c3540	c7552
Accuracy	61%	63%	57%	58%	58%	60%

Skills Learned

- Understanding Boolean Logic and designing digital circuits
- Basics of Neural Networks (MLP and CNN) and their implementation in pytorch
- Coding in Python and usage of different python packages
- Utilization of online library and strategy for reading science report papers
- Communication skills developed as researching with other students, mentor, and professor

How This Relates to Your STEM Coursework

In this SHINE program, I have gained coding skills which is going to help me further my STEM knowledge throughout my high school learning.

The ability to assimilate research papers is going to help me understand STEM concepts much easily in the future

Next Steps

The topic I have researched on in the SHINE program this summer has been very interesting and it has reinforced my interest in STEM. I want to continue following up on this topic in the future. Presently, the training dataset is small, and my next step is to add more data points to improve the training of the CNN. We expect that the key prediction accuracy will further go up as we add more data points to the dataset.

Acknowledgements

I would like to formally thank Professor Pierluigi Nuzzo, my Ph.D. Mentor Subhajit Dutta Chowdhury, my lab partner Nicholas Hornung, Center Mentor Emily Yamanaka, and Dr. Mills for all of this great time and all the help they have offered!