LUT-Based SAT Attack-Resilient Hardware Encryption Scheme
Rayan Singh r8y8ns@gmail.com
DesCyPhy Lab
Mountain View High School, Class of 2021
USC Viterbi Department of Engineering, SHINE 2019

Introduction
IP piracy and reverse engineering of Integrated Circuits (IC) has led to substantial losses for IC providers. Various countermeasures such as logic encryption have been proposed over the past decade. This project studies a recent logic encryption scheme, the Universal Circuit (UC), which is a Look-Up Table (LUT)-based logic structure used to replace the original circuit component so that the structural and functional traces of the circuit do not leak information to attackers. We find that UC is also robust against SAT attacks, a powerful logic decryption attack based on SAT solvers.

Objective and Impact of Professor’s Research
Nowadays, hardware security has become as much of an important research topic as software security. In the supply chain of IC manufacturing, several untrusted third parties, such as foundry, testing, and end users, may put reverse engineering efforts to steal the design secret for illegal reproduction or insert Hardware Trojans to disturb the normal functionality of the chip. To prevent those attacks, many countermeasures have been proposed, such as EPIC, SARLock, and Universal Circuit, but the security guarantees of those countermeasures are not verified due to lack of common security metrics. Prof. Nuzzo’s lab is trying to build a unifying methodology for evaluating different logic encryption and obfuscation techniques. The goal is to provide optimal strategies for obfuscating a circuit which satisfy the user’s security specifications.

Relation to STEM Coursework
My work in this program has built upon my previous work in school. For example, in AP Computer Science, we used Java with classes. Without that knowledge, I wouldn’t know how to write object-oriented python code. Also, I am sure that learning Boolean algebra will help me a lot next year in Advanced Computer Science.

Skills Learned
In this program, I have learned many things that I am sure will be used in my future work, such as:

• Class-oriented Python programming.
• Organizing code with GitHub.
• Fundamentals of Boolean Algebra and Digital Circuits.
• Working with Linux (Ubuntu) systems.
• Collaboration in a research-oriented environment.
• Annotated bibliography writing.

Advice for Future SHINE Students and Next Steps
I hope to continue doing research work next year and in college. For future SHINE students, I encourage you to take advantage of all the resources that you have here at USC. Initially, you may feel uneasy with all the new tools and information thrown at you, but after a while, you will feel comfortable and supported. Also, when reading academic papers, do not be scared when you see the amount of pages or words you don’t understand. Take it one step at a time and you will be alright.

Acknowledgements
I would like to thank Professor Nuzzo for allowing me to be part of his lab. I am also very grateful to Yinghua Hu, for being so organized and answering every question I had (a lot). Thank you to my parents for taking so much time off work to bring me here and to Dr. Mills, Dr. Herrold, and the SHINE program for this amazing opportunity.