Optimizing Obfuscation For Hardware Security

Luis Parra, luisparra12276@gmail.com
Bell Gardens High School, Class of 2019
USC Viterbi Department of Electrical Engineering, SHINE 2018

Introduction

Hardware Security is a big concern nowadays due to the vulnerabilities of ICs. Many attacks threaten IP holders, these attacks are mainly aimed at two purposes:

- IP Piracy
- Information Leakage

Scenario:

A designer has developed and validated an IC and is about to send off to a foundry for production. However, he/she wants the IC to be protected from any spot in the supply chain, such that attacks to the IC will not be successful.

Attacks:

Attackers must perform certain attacks to be able to gain access to whatever they are trying to seek information from. Some types of attacks include:

- Sensitization
- Removal
- SAT

Defenses:

However, those attacks above can be prevented using certain obfuscation techniques such as logic locking. Some obfuscation techniques that are available are:

- Random Logic Locking
- Fault Logic Locking
- Strong Logic Encryption
- SARLock
- ANTISat

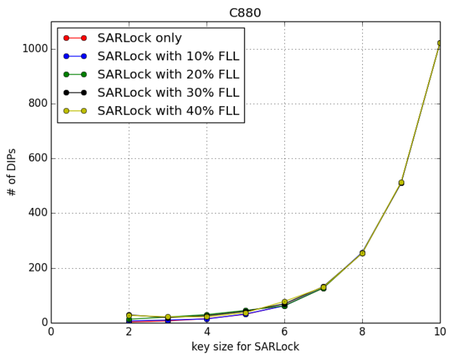


Fig.3 SARlock + FLL Implementation

The number of DIPs is a good parameter to see the SAT resilience of the circuit. It is exponentially proportional to the key size of SARLock.

Attack Techniques & Obfuscation Protection

Breakdown:

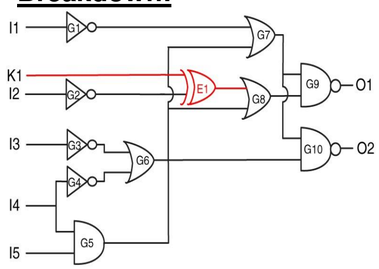


Fig.1 Circuit Encrypted with a key gate Inserted

Fig.1 shows a circuit encrypted with an XOR gate (E1), the XOR gate is what's known as a key gate. The key gate is responsible for giving correct outputs only if the correct key is given. In contrast, a wrong key will give a wrong output, and vice-versa. However, this defense is very vulnerable to an attack known as sensitization.

Sensitization:

The goal of sensitization is to determine the secret key used for the logic encryption. The attacker is assumed to have access to a locked netlist and also have access to a functional IC, which embeds the logic locking key. The functional IC is used as an oracle from which the attacker can get correct I/O pattern pairs. When it tries to know the value of one chosen key bit, the attacker tries to find an input pattern which can mute the propagation of all the unknown key bits to the output, such that the correctness of the output is solely determined by the key bit he/she is concerned about.

Strong Logic Encryption:

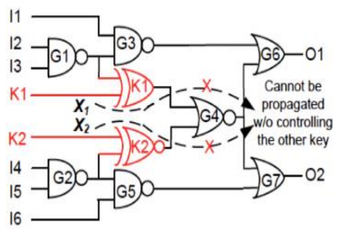


Fig.2 Circuit with two parallel Key-Gates

Fig.2 exhibits a Strong Logic Encrypted circuit. This technique prevents sensitization as both Key-Gates,(K1 & K2), are parallel to each other. This brings difficulty to the attacker because they need to find the value of one key gate(K1), however, they need the value of the other key gate(K2) in order to find the first key gate(K1). But, they can't have the value of (K2) unless they have the value of (K1), and vice-versa. This technique is vulnerable to an attack, known as SAT-Attack.

SAT-Attack:

Boolean satisfiability based attack (SAT Attack), is an attack that can decode most Logic Locking techniques within a reasonable amount of time, and also for a large key size. This attacks works by repeatedly solving formulas that will continuously get rid of incorrect keys until the correct keys are given. However, this can be prevented by a couple of obfuscation techniques known as SARLock and ANTISat.

Skills Learned

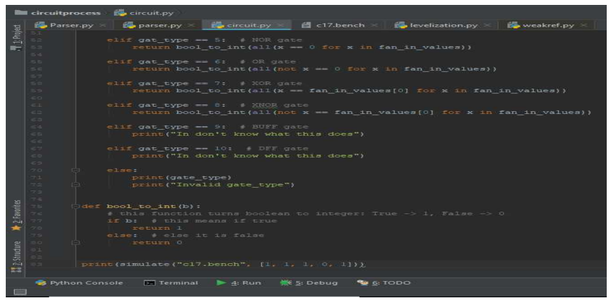
Throughout my seven weeks here at SHINE, I have learned many concepts including the basics of:

- Boolean Logic
- Digital Circuits

Principles of:

- Circuit/Logic Obfuscation

Coding was key to my research as I was responsible for creating a simulation function for citcuits. Therefore, **Python** was the programming language that I learned to be able to create the simulation function.



Code created for the simulation function

- Communication skills was another skill learned as it was key to my research as I was able to express my concerns and share some ideas with the team.

Impact of Professor's Research

Hardware security is as important as software and network security. Many people nowadays are concerned about their privacy and security. Circuits are stored with lots of confidential information that attackers are trying to reveal. Also, attackers can steal the design of a, non-obfuscated, circuit and can illegally reproduce and sell it for profit, which is what is trying to be prevented by hardware obfuscation.

In Professor Pierluigi Nuzzo's lab, we are trying to model and optimize multiple hardware obfuscation techniques for hardware Security. A tool for finding the best obfuscation solution to any IC is their ultimate goal in this research.

Advice for Future SHINE Students

To all future SHINE students:

- Do not be afraid of the material that will be given to you in your labs, there is a range of profound vocabulary that may seem frightening at first, but with constant effort in it, you will get the hang of it and it will become understandable.
- Do not be discouraged if you do not know the material or the subject at all, talk with your mentors as they are there to fully guide you and they will not let you down.
- Do a thorough background survey of your research as it will give you a better understanding of what you will be working with.
- Make connections and ask questions with the SHINE team, they will be there for you and will also help you to strengthen your academics.
- Make the seven weeks at SHINE last!!! Get to know your fellow SHINE peers, go out and have fun, it will definitely brighten up your experience.

References

- Kirov, D., Nuzzo, P., Passerone, R., & Sangiovanni-Vincentelli, A. (2017, June). ArchEx: An extensible framework for the exploration of cyber-physical system architectures. In *Design Automation Conference (DAC), 2017 54th ACM/EDAC/IEEE*(pp. 1-6). IEEE.
- Bajaj, N., Nuzzo, P., Masin, M., & Sangiovanni-Vincentelli, A. (2015, March). Optimized selection of reliable and cost-effective cyber-physical system architectures. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition* (pp. 561-566). EDA Consortium.
- Rajendran, J., Zhang, H., Zhang, C., Rose, G. S., Pino, Y., Sinanoglu, O., & Karri, R. (2015). Fault analysis-based logic encryption. *IEEE Transactions on computers*, *64*(2), 410-400240.
- Rajendran, J., Pino, Y., Sinanoglu, O., & Karri, R. (2012, June). Security analysis of logic obfuscation. In *Proceedings of the 49th Annual Design Automation Conference* (pp. 83-89). ACM.
- Yasin, M., Mazumdar, B., Rajendran, J. J., & Sinanoglu, O. (2016, May). Sarlock: Sat attack resistant logic locking. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on* (pp. 236-241). IEEE.

Acknowledgements

I would like to thank Professor Pierluigi Nuzzo, my Ph.D. mentors, Yinghua Hu, and Subhajit Dutta Chowdhury, my lab mate, Tristan Brankovic; Dr. Katie Mills, Dr. Megan Herrold, Patrick Valadez and the SHINE team; my teachers, Mrs. Karin Ching and Ms. Rosa Garcia; Cynthia Gonzalez, Lauren Lizarrga, and all my TELACU family; and lastly I would like to thank my parents and my siblings, Luis, Maria, Evelinda, Sam, and Sophia, for supporting and pushing me to achieve my best, it will all pay off soon.