Abstract

In the era of escalating Integrated Circuit (IC) fabrication costs, a shift to fabless operations by most IC vendors has become prominent. Adopting a "horizontal" business model, emphasizing outsourcing in different phases of IC manufacturing, is widespread. While this model reduces costs and time-to-market, it has also attracted adversaries engaging in malicious activities within the IC supply chain. These activities include IP infringement, design piracy, IC overproduction, and the introduction of hardware Trojans (HTs), resulting in billions of dollars in losses. Among proposed countermeasures, *Logic Locking* has emerged as a proactive defense strategy against such threats, capable of mitigating adversarial attacks at any point in the supply chain. The fundamental concept of logic locking involves obscuring the actual design from adversaries by integrating key-based logic into the original design. The design behaves correctly only when the secret key is applied. However, logic locking faced setbacks with the emergence of SAT-based attacks, which could compromise existing locking techniques. Consequently, the community shifted focus towards designing SAT-based attack-resilient locking schemes.

This thesis contributes to logic locking in three key ways. First, it identifies serious vulnerabilities in state-of-the-art logic locking techniques and devises novel attack algorithms to mitigate them. Secondly, it contributes to the development of sound countermeasures capable of preventing existing vulnerabilities and thwarting proposed attacks. Lastly, this thesis presents an automation of logic locking techniques, which has been greatly limited in the community. The generic end-to-end combinational logic locking Computer-Aided Design (CAD) framework bridges the gap and integrates diverse combinational logic locking techniques.

The first contribution of the thesis evaluates the security of cellular automata (CA)-based obfuscation of Finite State Machines (FSM). This obfuscation scheme utilizes a class of non-group additive CA, known as $D1{*}CA$ and $D1{*}CA_{dual}$, to obfuscate each state-transition of an FSM, providing high testability in the absence of scan-based Design-for-Testability techniques, thwarting several existing scan-chain attacks. The thesis introduces a novel attack to extract the secret key used in obfuscating each state transition of the FSM, utilizing information leaked by the CA cell values obtained during the test mode execution of the obfuscated FSM. The secret key, which locks the combinational portion of the CA-based obfuscation, is also extracted through SAT-based attacks by constructing oracles from the leaked information.

Furthermore, the thesis discusses an attack against Cascaded Locking (CAS-Lock), an advanced logic locking technique leveraging the concept of a single-point function for SAT-based attack resilience. The proposed attack not only reveals the correct key but also exposes the exact chain configuration of the implemented CAS-Lock design, along with all the key gates used in both blocks of CAS-Lock. This attack relies on externally observable information like failing input patterns related to a carefully chosen key simulation of the locked design, eliminating the need for structural analysis of any kind on the locked netlist.

In the next contribution, the thesis investigates the root cause of the attack's success on a CA-based obfuscation strategy. Utilizing these findings, it proposes a couple of mitigation techniques

by appending non-linearity to the existing CA structure and slightly modifying the $D1{*}CA$ rule vector without affecting the inherent properties of the underlying CA.

Finally, the proposed logic locking CAD framework automates five combinational logic locking techniques, belonging to different genres of pre-SAT and post-SAT schemes, including one against which no known attacks exist. It further offers flexibility for integrating potential future techniques. It utilizes a graph-based representation of the desired circuit to thoroughly analyze and extract influential portions for locking, maximizing the security robustness of the locked circuits while minimizing the incurred hardware overheads.

Keywords. Hardware Security, Logic Locking, Cellular Automata, ORACALL, CAS-Lock, DIP Learning, Automation, Countermeasures, MIDAS