Abstract

The current global business model of the semiconductor industry divulges the Intellectual Property (IP) of design to multiple third-party agents involved in different phases of IC development. Notably, the fabrication of the ICs is often outsourced to dedicated specialist fab houses. Many leading companies rely on several offshore fab labs for the fabrication of their chips. Not only that, recently, test, assembly, and packaging services are also carried out through outsourced assembly and test (OSAT) companies. However, this outsourcing reliant cost-effective global business model comes with a certain degree of security concerns. Since the entire layout of the design gets revealed to the third-party fab labs, it opens the backdoor of several security vulnerabilities such as IP piracy, overbuilding, counterfeiting, and insertion of hardware Trojans (HT). Not only the third-party fab labs are threats to the secrecy of the hardware designs, but also an end-user can extract the internal details of an IC using advanced reverse engineering set-ups.

Logic encryption is a popular countermeasure against these threats, which offers protection against the potential adversaries in the fab labs as well as the end-users. However, over the years, logic encryption has been a target of several attacks, especially Boolean satisfiability attacks. The state-of-the-art solutions against the SAT attack are not only vulnerable to numerous other attacks but also face the challenge to meet a fundamental criterion of logic encryption, i.e.- high output corruption for wrong keys. This thesis exploits the inability of the SAT attack to deobfuscate sequential circuits as a defense against it. Various strategies, proposed in this thesis, are capable of preventing the SAT attack by obfuscating the scan-based Design-for-Testability (DfT) infrastructure. Unlike the existing SAT-resilient schemes, the proposed scan-obfuscation guided SAT-preventive strategies do not suffer from poor output corruption for wrong keys. This thesis also proposes various probable solutions for inserting the key-gates into the circuit that ensures protection against numerous other attacks, which exploit weak key-gate locations. Besides proposing several gate-level obfuscation strategies, this research work also offers obfuscation at a higher abstraction level, that is, RTL-level. It introduces a Cellular Automata (CA) guided FSM obfuscation strategy that provides a key-based obfuscation to each state-transition of the FSM. For all the proposed obfuscation techniques, rigorous security analysis against various attacks evaluates their strengths and limitations. Testability analysis also ensures that none of the proposed schemes hamper the basic testing properties of the ICs. Apart from logic encryption, this research work also presents a CA-based FSM watermarking strategy that helps to detect potential theft of the designer's IP by any adversary. The proposed easily detectable watermarking technique can withstand various tampering and removal attacks.

Keywords: Hardware Security; IP Piracy & Counterfeiting; IP Protection; Design-for-Security; Logic Encryption; FSM Obfuscation; Secret Key; Key-gate Placement; SAT Attack; Design-for-Testability; Scan Obfuscation; FSM Watermarking; Cellular Automata; Particle-Swarm-Optimization.