Preventing Piracy of Integrated Circuits via a Provable Security Mechanism

Al Ghannam, Fatimeh (School: Al-Anjal Private School)

Due to the rising cost of fabrication in the semiconductor industry, leading-edge integrated circuit design firms outsource fabrication to offshore foundries. However, third-party foundries may produce unauthorized clones of integrated circuits, committing intellectual property (IP) piracy. To prevent IP piracy, in this project a security mechanism was constructed that guarantees the unclonability of application-specific integrated circuits (ASICs). The implementation takes as input any ASIC function and combines it with a Trivium pseudorandom function (PRF). This done under a binary decision diagram (BDD) as an indistinguishability obfuscator, producing an implementation of the ASIC that reveals nothing about the function, along with an activation key which the designer keeps secret and programs into ASIC memory after fabrication. To verify the security of the mechanism, it was used to secure five benchmarks and tried several attacks from literature, including the SAT attack, on each benchmark. None of the attacks managed to deduce a valid key for cloning any of the locked benchmarks, despite being able to compromise prior mechanisms. Also, the overhead applying the mechanism incurs on chip speed, size, and power consumption was measured. Although applying the mechanism incurs comparatively higher overhead, it has the advantage of guaranteeing concrete and robust security. It was found that a high security level can be achieved for functions of input size as large as 26 bits; therefore, an ASIC can attain unclonabality, preventing IP piracy.

Awards Won: