A041 ENGR

Strategic Hardware Trojan Testing with Hierarchical Trojan Types

Abstract

In this paper, we consider the problem of detecting hardware Trojans in an Integrated Circuit (IC) from a game theoretic standpoint. The paper considers the presence of multiple classes of Trojans, with each class containing multiple Trojan types, and characterizes the Nash Equilibrium (NE) strategy for inserting a Trojan (from the perspective of a malicious entity) and detecting a Trojan (from the perspective of a defender) under consideration of the impact that an undetected Trojan has on the defender's system. The paper also models a sequential hardware Trojan testing game, where the defender tests for the presence of Trojans over time and characterizes the NE strategy of such a game. Numerous simulation results are presented to gain insights into the game theoretic hardware Trojan testing techniques presented in the paper.