Special Session: Countering IP Security Threats in Supply Chain

Submitted by grigby1 on Thu, 03/12/2020 - 12:09pm

Title Special Session: Countering IP Security Threats in Supply Chain
Publication Type Conference Paper
Year of Publication 2019
Authors Salmani, Hassan, Hoque, Tamzidul, Bhunia, Swarup, Yasin, Muhammad, Rajendran, Jeyavijayan JV, Karimi, Naghmeh
Conference Name 2019 IEEE 37th VLSI Test Symposium (VTS)
Published apr

Keywords Data models, electronic engineering computing, Human Behavior, integrated circuit design, integrated circuit fabrication, integrated circuit manufacture, integrated circuit technology, integrated circuits, Internet, invasive software, IP security threats, learning (artificial intelligence), learning-based trust verification, logic design, logic locking schemes, machine learning, Monitoring, production engineering computing, Protocols, pubcrawl, resilience, Resiliency, reverse engineering, Scalability, supply chain, supply chain management, supply chain security, tagging, telecommunication security, Training, Trojan insertion, Valves

Abstract The continuing decrease in feature size of integrated circuits, and the increase of the complexity and cost of design and fabrication has led to outsourcing the design and fabrication of integrated circuits to third parties across the globe, and in turn has introduced several security vulnerabilities. The adversaries in the supply chain can pirate integrated circuits, overproduce these circuits, perform reverse engineering, and/or insert hardware Trojans in these circuits. Developing countermeasures against such security threats is highly crucial. Accordingly, this paper first develops a learning-based trust verification framework to detect hardware Trojans. To tackle Trojan insertion, IP piracy and overproduction, logic locking schemes and in particular stripped functionality logic locking is discussed and its resiliency against the state-of-the-art attacks is investigated.

DOI 10.1109/VTS.2019.8758633
Citation Key salmani_special_2019
Data models electronic engineering computing Human behavior integrated circuit design integrated circuit fabrication integrated circuit manufacture integrated circuit technology integrated circuits internet invasive software IP security threats learning (artificial intelligence) learning-based trust verification logic design logic locking schemes machine learning Monitoring production engineering computing Protocols pubcrawl resilience Resiliency reverse engineering Scalability Supply Chain supply chain management supply chain security tagging telecommunication security Training Trojan insertion Valves