Published on *CPS-VO* (https://cps-vo.org)

Grey Zone in Pre-Silicon Hardware Trojan Detection

Submitted by grigby1 on Fri, 03/15/2019 - 11:58am

Title	Grey Zone in Pre-Silicon Hardware Trojan Detection
Publication Type	Conference Paper
Year of Publication	2018
Authors	Ye, J., Yang, Y., Gong, Y., Hu, Y., Li, X.
Conference Name	2018 IEEE International Test Conference in Asia (ITC-Asia)
ISBN Number	978-1-5386-5180-3
Keywords	activation probability, Behaviour Simulation, behaviour simulations, benchmark, electronic engineering computing, elemental semiconductors, functional test, grey zone, Hardware, hardware Trojan benchmark circuits, integrated circuit design, integrated circuit testing, invasive software, learning (artificial intelligence), low signal probability, machine learning, Pre-Silicon Hardware Trojan Detection, pre-silicon hardware trojan detection method, probability, pubcrawl, Si, Silicon, trojan horse detection, Trojan horses, Trust-Hub

Abstract

Pre-Silicon hardware Trojan detection has been studied for years. The most popular benchmark circuits are from the Trust-Hub. Their common feature is that the probability of activating hardware Trojans is very low. This leads to a series of machine learning based hardware Trojan detection methods which try to find the nets with low signal probability of 0 or 1. On the other hand, it is considered that, if the probability of activating hardware Trojans is high, these hardware Trojans can be easily found through behaviour simulations or during functional test. This paper explores the "grey zone" between these two opposite scenarios: if the activation probability of a hardware Trojan is not low enough for machine learning to detect it and is not high enough for behaviour simulation or functional test to find it, it can escape from detection. Experiments show the existence of such hardware Trojans, and this paper suggests a new set of hardware Trojan benchmark circuits for future study.

URL	https://ieeexplore.ieee.org/document/8462952
DOI	10.1109/ITC-Asia.2018.00024
Citation Key	ye_grey_2018

activation probability Behaviour Simulation behaviour simulations benchmark electronic engineering computing elemental semiconductors

functional test grey zone Hardware hardware Trojan benchmark circuits integrated circuit design integrated circuit testing invasive software learning (artificial intelligence) low signal probability machine learning Pre-Silicon Hardware Trojan Detection pre-silicon hardware trojan detection method probability pubcrawl Si Silicon trojan horse detection Trojan horses Trust-Hub