Journal of Electronic Testing
https://doi.org/10.1007/s10836-024-06122-w

Towards the Detection of Hardware Trojans with Cost Effective Test Vectors using Genetic Algorithm

Sandip Chakraborty[1,2] · Archisman Ghosh[1] · Anindan Mondal[1,3] · Bibhash Sen[1]

Received: 9 January 2024 / Accepted: 3 June 2024

Abstract
Hardware Trojans (HT) are tiny circuits designed to exploit electronic devices, posing risks such as device malfunction or leakage of sensitive information. The adversary aims to implant these HTs specifically targeting nets with minimal signal transition (rare gates) within a circuit, evading detection during functional tests. Some Trojan variants are activated by adversaries under specific periodic conditions. Logic testing, a well-established method for test generation in HT detection, faces challenges due to the impractical scale of the search space, whereas Genetic Algorithms (GA) excel in efficiently navigating extensive solution spaces. This paper presents a GA-based technique that integrates information on effective inputs, along with an adequate fitness function defined based on combinational controllability and structural features, for detecting conditionally triggered ultrasmall HTs. Upon assessing the ITC 99 and ISCAS 85 and 89 benchmarks, we note significant enhancements in trigger coverage and reduced run-time requirements in comparison to state-of-the-art methods like MERO and TRIAGE.

Keywords Hardware trojan · Transition probability · SCOAP measurements · Genetic algorithm

1 Introduction

IC design houses often outsource the manufacturing process to reduce cost and speed up development time [26]. However, these offshore facilities introduce risks such as Counterfeit parts, Intellectual property theft, and hardware Trojans (HTs) [7]. While piracy is one of the biggest challenges from a financial point of view, the presence of an HT circuit inside a design remains the biggest security threat. HTs pose a significant threat to device security due to their stealthy nature and destructive capabilities [4]. Based on the activation criteria, HTs can be broadly classified into two types, always on and conditionally activated [12]. While the former type is mainly used for information leakage, the latter one remains inactive most of the time and can be used for various malicious activities. These HT circuits are a huge security challenge due to the extreme difficulty of activating and detecting them during testing.

The difficulty with conditionally triggered HTs lies in their ability to elude detection during functional tests. To build such circuits, the adversary targets specific nets inside the netlist that do not exhibit many activities during regular operation. This ensures the HT avoids accidental activation during the test period. Traditional test methods have been found to be insufficient against such stealthy and extremely tiny HTs. As a result, several alternative countermeasures have been proposed in the literature [15]. Among them, logic testing has gained significant attraction due to its effectiveness against small HTs. This approach involves probing the input–output behaviour of a circuit and identifying inconsistencies between its expected and

Responsible Editor: U. Guin

✉ Bibhash Sen
bibhash.sen@cse.nitdgp.ac.in

Sandip Chakraborty
sandipch240@gmail.com

Archisman Ghosh
archiribhu@gmail.com

Anindan Mondal
anindanmondal14@gmail.com

[1] Department of Computer Science and Engineering, National Institute of Technology, Durgapur, India

[2] Department of Information Technology, Dr. B. C. Roy Enginering College, Durgapur, India

[3] Department of Computer Science and Engineering, Asansol Engineering College, Asansol, India

Published online: 25 June 2024