IEEE.org IEEE *Xplore* IEEE SA IEEE Spectrum More Sites Subscribe Donate Cart Create Account Personal Sign In

Institutional Sign In

Institutional Sign In

All

ADVANCED SEARCH

Conferences > 2024 IEEE International Confe...

Exploring the PSO-Driven Test Pattern Generation Approach for Hardware Trojan Detection

Publisher: IEEE Cite This PDF

Sandip Chakraborty ; Mudumba Sri Varenya ; Anindan Mondal ; Bibhash Sen **All Authors**

49
Full
Text Views

Alerts

Manage Content Alerts
Add to Citation Alerts

Abstract

Document Sections

Show Full Outline

Authors

Figures

References

Keywords

Metrics

More Like This

Downl
PDF

Abstract:
Hardware Trojans (HT) refer to tiny circuits that adversaries implant for malicious purposes. These circuits operate stealthily and, once triggered, can lead to severe di... **View more**

Metadata

Abstract:
Hardware Trojans (HT) refer to tiny circuits that adversaries implant for malicious purposes. These circuits operate stealthily and, once triggered, can lead to severe disruptions. Detecting their presence requires the application of suitable test vectors. However, a huge search space often complicates the test generation task. In this regard, evolutionary algorithms are promising candidates due to their ability to explore such search space with effective test vectors. This paper introduces a test generation methodology that effectively utilizes the capabilities inherent in particle swarm optimization (PSO) to successfully attain its intended objectives. The validity of the proposed approach is confirmed by applying it to multiple ISCAS '85 benchmark circuits. The results show a significant reduction in test generation time, exceeding 50%, alongside an enhancement in test set quality compared to the current state-of-the-art techniques.

Published in: 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)

Date of Conference: 14-16 March 2024 **DOI:** 10.1109/IATMSI60426.2024.10502952

Date Added to IEEE *Xplore*: 24 April 2024

Publisher: IEEE

Conference Location: Gwalior, India

ISBN Information:

Electronic ISBN:979-8-3503-6052-3

Print on Demand(PoD) ISBN:979-8-3503-6053-0

Sandip Chakraborty
Dept of CSE, NIT Durgapur, BCREC Durgapur

Mudumba Sri Varenya
Dept of CSE, NIT Durgapur

Anindan Mondal
Dept of CSE, NIT Durgapur

Bibhash Sen
Dept of CSE, NIT Durgapur

Contents

I. Introduction

The rapid advancement of integrated circuits (ICs) and electronic systems has led to an increased risk of hardware security threats comprising IP piracy and Hardware Trojans (HTs). HTs are tiny malicious modifications inserted during the design or manufacturing phase of ICs, posing significant risks to system functionality and security. Many different techniques for Hardware Trojan detection have been presented in the literature that can be broadly categorized into two categories:(i) side-channel analysis and (ii) simulation-based validation (logic testing) [1] [2].

Authors

Sandip Chakraborty
Dept of CSE, NIT Durgapur, BCREC Durgapur

Mudumba Sri Varenya
Dept of CSE, NIT Durgapur

Anindan Mondal
Dept of CSE, NIT Durgapur

Bibhash Sen
Dept of CSE, NIT Durgapur

Figures

References

Keywords

Metrics

2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) | 979-8-3503-6052-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IATMSI60426.2024.10502930

Preface

This volume contains the papers presented at IEEE IATMSI-2024: 2nd IEEE International conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) held on March 14-16, 2024 in ABV-IIITM Gwalior.

The **2nd IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI-2024)** is a globally recognized event organized by the Department of Electrical and Electronics Engineering at **ABV-IIITM Gwalior**, India, in collaboration with the **IEEE MP Section**. Serving as a prestigious platform, this flagship conference facilitate the dissemination of cutting-edge advancements across a spectrum of disciplines, including communication, IT-enabled management, and industrial electronics applications such as health, energy, VLSI, smart transportation, biomedical science, agriculture, AI applications, robotics, defense, technology policies, and allied domains. As a recurring annual event with nationwide participation, IATMSI-2024 converge experts, researchers, scholars, and industry professionals from around the world to share and deliberate on their work, offering profound insights into emerging technological trends. The picturesque city of Gwalior, renowned for its natural splendor and cultural heritage,serve as the host for IATMSI-2024. With the theme **”Enabling the Change! Social Innovation for Sustainable Societies,”** this flagship conference is set to encompass a comprehensive and high-quality interdisciplinary exploration of technology and management. The event feature various research themes, including paper presentations, poster sessions, industry exhibitions, expert talks, tutorials by distinguished speakers, and an exhibition. Since its inception in 2022, IATMSI has rapidly evolved into a distinguished flagship conference jointly hosted by ABV-IIITM Gwalior and the IEEE MP Section. The conference has successfully encompassed a wide spectrum of cutting-edge research domains, solidifying its reputation as a premier academic event.

The main tracks of the conference are listed below:

Track 1: Technology Solutions for Healthcare
Track 2: Power, Control, Energy and Intelligent Transportation Technologies
Track 3: Artificial Intelligence (AI), IOT and Computer Vision Enabled Technologies
Track 4: Green Electronics, VLSI, Communication and Sensor Based Technologies
Track 5: IT enabled Management for Social Change

There were 1305 submissions. Each submission was reviewed by at least 3, and on the average 3, program committee members. The committee decided to accept 376 papers. The program also includes 9 invited talks. This conference is sponsored by Scientech, IJGSAR, Cadre Design, and IEEE MP Section.

14-16 March 2024

Dr Somesh Kumar
Dr. Pinku Ranjan
Dr. Sandesh Jain
Dr. Alok Kumar Kamal

2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) | 979-8-3503-6052-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IATMSI60426.2024.10502952

Exploring the PSO-Driven Test Pattern Generation Approach for Hardware Trojan Detection

Sandip Chakraborty
Dept of CSE
NIT Durgapur, BCREC Durgapur
sandipch240@gmail.com

Mudumba Sri Varenya
Dept of CSE
NIT Durgapur
srivarenya123@gmail.com

Anindan Mondal
Dept of CSE
NIT Durgapur
anindanmondal14@gmail.com

Bibhash Sen
Dept of CSE
NIT Durgapur
bibhash.sen@cse.nitdgp.ac.in

***Abstract*—Hardware Trojans (HT) refer to tiny circuits that adversaries implant for malicious purposes. These circuits operate stealthily and, once triggered, can lead to severe disruptions. Detecting their presence requires the application of suitable test vectors. However, a huge search space often complicates the test generation task. In this regard, evolutionary algorithms are promising candidates due to their ability to explore such search space with effective test vectors. This paper introduces a test generation methodology that effectively utilizes the capabilities inherent in particle swarm optimization (PSO) to successfully attain its intended objectives. The validity of the proposed approach is confirmed by applying it to multiple ISCAS ’85 benchmark circuits. The results show a significant reduction in test generation time, exceeding 50%, alongside an enhancement in test set quality compared to the current state-of-the-art techniques.**

***Index Terms*—Hardware Trojan, Test Generation, Particle Swarm Optimization, VLSI.**

I. Introduction

The rapid advancement of integrated circuits (ICs) and electronic systems has led to an increased risk of hardware security threats comprising IP piracy and Hardware Trojans (HTs). HTs are tiny malicious modifications inserted during the design or manufacturing phase of ICs, posing significant risks to system functionality and security. Many different techniques for Hardware Trojan detection have been presented in the literature that can be broadly categorized into two categories:(i) side-channel analysis and (ii) simulation-based validation (logic testing) [1] [2].

Particle Swarm Optimization (PSO) represents a bio-inspired technique capable of finding optimal solutions in the search space. It emerges as the top choice for generating test patterns in HT detection, surpassing other evolutionary techniques. Its balanced exploration-exploitation strategy efficiently reveals concealed Trojans, supported by global search abilities and adaptability to dynamic scenarios. PSO’s parallel processing and simplicity amplify its suitability, establishing it as a robust option for effective HT detection. To address the challenge of detecting these elusive HTs, we introduce an innovative test pattern generation approach via PSO, conducting a thorough comparative analysis with the current Genetic Algorithm (GA) based HT detection method.

A comprehensive comparative analysis with two state-of-the-art test pattern generation: TRIAGE (Hardware Trojan Detection using an advanced genetic algorithm-based logic testing) [3] and MERO (Multiple Excitation of Rare logic conditions at internal nodes) [4] is reported here. TRIAGE is a prominent GA-based test pattern generation technique used for Hardware Trojan detection. Our comparative analysis evaluates the fault coverage, detection accuracy, and test pattern diversity between PSO and TRIAGE. The diversity achieved by PSO enables it to identify HTs hidden in uncommon gate conditions that might evade TRIAGE. On the other hand, MERO is an advanced technique focusing on multiple excitations of rare logic conditions at internal nodes for detecting Hardware Trojans. Our comparison examines the efficiency and effectiveness of PSO against MERO. The non-identical pattern selection in PSO plays a crucial role in its improved performance compared to MERO.

The proposed work emphasizes rare gate coverage, aiming to activate specific gates where HTs are likely to be hidden. In light of the above discussion, the key contributions of our research are -

- *PSO-based Test Pattern Generation*: The power of PSO is used in our approach to generate high-quality test patterns that are capable of detecting Hardware Trojans efficiently. PSO is capable of balancing exploration and exploitation of the solution space. It is capable of identifying test patterns that effectively target rare gate conditions where HTs are likely to be hidden.
- *Rare Gate Coverage Emphasis*: The fitness function in our PSO algorithm is designed to evaluate rare gate coverage, focusing on activating specific gates that are susceptible to hosting Hardware Trojans.
- *Non-Identical Pattern Selection*: To enhance diversity, we implement a strategy to select non-identical test patterns within each generation. By using this feature, our PSO algorithm can explore different regions of the solution space, leading to a more comprehensive detection capability.
- The effectiveness of the suggested approach is assessed in eight distinct ISCAS ’85 benchmark circuits.
- The performance is in contrast to conventional logical testing techniques, affirming the validity of the proposed

979-8-3503-6052-3/24/$31.00 ©2024 IEEE