1.

Accession number: 14636191

Title: **Testing for Hardware Trojans: A Game-Theoretic Approach**

Authors: Kamhoua, C.A.1 Email author charles.kamhoua.1@us.af.mil; Rodriguez, M.1 Email author manuel.rodriguez-moreno.1.ctr@us.af.mil; Kwiat, K.A.1 Email author [kevin.kwiat@us.af.mil](mailto:kevin.kwiat@us.af.mil)

Source: Decision and Game Theory for Security. 5th International Conference, GameSec 2014. Proceedings: LNCS 8840

Publication date: 2014

ISBN-13: 978-3-319-12600-5

Document type: Conference article (CA)

Conference name: Decision and GameTheory for Security. 5th International Conference, GameSec 2014

Conference date: 6-7 Nov. 2014

Publisher: Springer International Publishing

Material Identity Number: YXB4-1901-839

Abstract: The microcircuit industry is witnessing a massive outsourcing of the fabrication of ICs (Integrated Circuit), as well as the use of third party IP (Intellectual Property) and COTS (Commercial Off-The-Shelf) tools during IC design. These issues raise new security challenges and threats. In particular, it brings up multiple opportunities for the insertion of malicious logic, commonly referred to as a hardware Trojan, in the IC. Testing is typically used along the IC development lifecycle to verify the functional correctness of a given chip. However, the complexity of modern ICs, together with resource and time limitations, makes exhaustive testing commonly unfeasible. In this paper, we propose a game-theoretic approach for testing digital circuits that takes into account the decision-making process of intelligent attackers responsible for the infection of ICs with hardware Trojans. Testing for hardware Trojans is modeled as a zero-sum game between malicious manufacturers or designers (i.e., the attacker) who want to insert Trojans, and testers (i.e., the defender) whose goal is to detect the Trojans. The game results in multiple possible mixed strategy Nash equilibria that allow to identify optimum test sets that increase the probability of detecting and defeating hardware Trojans in digital logic.

## Accession number: 16410066

## Title: Hardware Trojans classification for gate-level netlists based on machine learning

## Authors: Hasegawa, K.1 Email author Kento.hasgawa@togawa.cs.waseda.ac.jp; Oya, M.1; Yanagisawa, M.1; Togawa, N.1 Email author [togawa@togawa.cs.waseda.ac.jp](mailto:togawa@togawa.cs.waseda.ac.jp)

## Source: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)

## Publication date: 2016

## Language: English

## ISBN-13: 978-1-5090-1507-8

## Document type: Conference article (CA)

## Conference name: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)

## Conference date: 4-6 July 2016

## Conference location: Sant Feliu de Guixols, Spain

## Material Identity Number: YXB6-1902-553

## Abstract: Recently, we face a serious risk that malicious third-party vendors can very easily insert hardware Trojans into their IC products but it is very difficult to analyze huge and complex ICs. In this paper, we propose a hardware-Trojan classification method to identify hardware-Trojan infected nets (or Trojan nets) using a support vector machine (SVM). Firstly, we extract the five hardware-Trojan features in each net in a netlist. Secondly, since we cannot effectively give the simple and fixed threshold values to them to detect hardware Trojans, we represent them to be a five-dimensional vector and learn them by using SVM. Finally, we can successfully classify a set of all the nets in an unknown netlist into Trojan ones and normal ones based on the learned SVM classifier. We have applied our SVM-based hardware-Trojan classification method to Trust-HUB benchmarks and the results demonstrate that our method can much increase the true positive rate compared to the existing state-of-the-art results in most of the cases. In some cases, our method can achieve the true positive rate of 100%, which shows that all the Trojan nets in a netlist are completely detected by our method.

## Accession number: 16410066

## Title: Hardware Trojans classification for gate-level netlists based on machine learning

## Authors: Hasegawa, K.1 Email author Kento.hasgawa@togawa.cs.waseda.ac.jp; Oya, M.1; Yanagisawa, M.1; Togawa, N.1 Email author togawa@togawa.cs.waseda.ac.jp

## Author affiliation: 1 Dept. of Comput. Sci. & Commun. Eng., Waseda Univ., Tokoyo, Japan

## Source: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)

## Publication date: 2016

## Pages: 203-6

## Language: English

## ISBN-13: 978-1-5090-1507-8

## Document type: Conference article (CA)

## Conference name: 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)

## Conference date: 4-6 July 2016

## Conference location: Sant Feliu de Guixols, Spain

## Sponsor: IEEE Council on Electron. Design Autom.

## Publisher: IEEE

## Place of publication: Piscataway, NJ, USA

## Material Identity Number: YXB6-1902-553

## Abstract: Recently, we face a serious risk that malicious third-party vendors can very easily insert hardware Trojans into their IC products but it is very difficult to analyze huge and complex ICs. In this paper, we propose a hardware-Trojan classification method to identify hardware-Trojan infected nets (or Trojan nets) using a support vector machine (SVM). Firstly, we extract the five hardware-Trojan features in each net in a netlist. Secondly, since we cannot effectively give the simple and fixed threshold values to them to detect hardware Trojans, we represent them to be a five-dimensional vector and learn them by using SVM. Finally, we can successfully classify a set of all the nets in an unknown netlist into Trojan ones and normal ones based on the learned SVM classifier. We have applied our SVM-based hardware-Trojan classification method to Trust-HUB benchmarks and the results demonstrate that our method can much increase the true positive rate compared to the existing state-of-the-art results in most of the cases. In some cases, our method can achieve the true positive rate of 100%, which shows that all the Trojan nets in a netlist are completely detected by our method.

## Hardware Trojans classification for gate-level netlists based on machine learning

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=9&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Guided test generation for isolation and detection of embedded trojans in ICs

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=7&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Hardware Trojans: current challenges and approaches

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=6&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Tutorial T4: All You Need to Know about Hardware Trojans and Counterfeit ICs

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=5&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Hardware Trojans in wireless cryptographic ICs

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=4&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=3&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## A chip architecture for compressive sensing based detection of IC trojans

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=1&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Improving IC Security Against Trojan Attacks Through Integration of Security Monitors

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=76&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Power supply signal calibration techniques for improving detection resolution to hardware trojans

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=56&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

**Designing and implementing hardware Trojans in ARM9 IP**

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=44&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## A clock sweeping technique for detecting hardware trojans impacting circuits delay

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=42&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Side-channel analysis-based detection approach of hardware Trojans

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=19&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Detecting Hardware Trojans using On-chip Sensors in an ASIC Design

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=16&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## The problem of hardware Trojans detection in system-on-chip

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=15&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Hardware Trojans detection based on projection pursuit

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=14&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Hardware Enlightening: No Where to Hide Your Hardware Trojans!

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=13&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Interacting with Hardware Trojans over a network

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=12&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>

## Detecting hardware Trojans: A tale of two techniques

<https://www-engineeringvillage-com.ezproxy2.library.drexel.edu/search/doc/abstract.url?pageType=quickSearch&usageOrigin=searchresults&usageZone=resultslist&searchtype=Quick&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&DOCINDEX=11&database=8388611&format=quickSearchAbstractFormat&dedupResultCount=&SEARCHID=3164698fM7ee6M4d9aMacbcMcc087d2412ad&referer=%2Fsearch%2Fresults%2Fquick.url>