HARDWARE TROJAN DETECTION USING MACHINE LEARNING

Minor Project Synopsis

Bachelor of Technology

(Information Technology Engineering)

Submitted By:

Sehajbir Singh (2004984)

Gurmukh Singh (2004913)

Amay Avasthi (2004888)

Rajvir Singh (2004974)

(2020 - 2024)

GURU NANAK DEV ENGINEERING COLLEGE LUDHIANA

(An Autonomous College Under UGC ACT)

Contents

1. Introduction

Concerns regarding the security of manufactured ICs intended for use in sensitive applications have grown rapidly as a result of the use of untrusted parties throughout the IC supply chain network. The adversarial infestation of manufactured ICs with a Hardware Trojan (HT) is one of these security risks. A malicious alteration to a circuit intended to control, modify, disable, or observe its logic is known as a Trojan. There are more designers and design irms due to the expansion and globalization of IC design and development. IC design houses unable to manufacture their chips internally must use external foundries because building up a fabrication facility might easily cost more than $20 billion, and expenses for advanced nodes could be substantially higher. It can be difficult to build confidence with these external foundries, and they are often not trusted

Due to the unique and un-modelled nature of these malicious modifications, conventional manufacturing VLSI test and verification procedures are ineffective in identifying HTs. This has motivated other researchers to look at methods for HTs detection using statistical analysis of side-channel data gathered from ICs, including side-channel power analysis, power supply transient signal analysis, regional supply currents analysis, temperature analysis, wireless transmission power analysis, and side-channel delay analysis.

We develop and train a learning-assisted timing-adjustment model combined with the STA acts as a golden model The side-channel statistical power analysis approach for HT detection in proposed that the trusted region for the operation of a Trojan-free IC can be learned using a combination of measurements from the meticulously designed and distributed PCM structures, advanced statistical tail modelling techniques, and measurements from the trusted simulation model. However, this approach uses side-channel power analysis to find HTs. The size of the HT must be considered to see a significant change in leakage or dynamic power. As a result, this method cannot detect HTs constructed with a few gates. This is when the solution outlined in this project can detect even a single added logic gate in a tested timing path.

The side channel delay analysis solution in [60] utilizes the Clock Frequency Sweeping Test (CFST) to locate the HT. For a delay comparison, a Golden IC must be present, though. This work served as the basis for the development of the side-channel HT detection method (shown in this tutorial), which does not need a Golden IC but instead creates label data points for each feature set using CFST.

2. Objectives

- **Early Detection of Hardware Trojan** – The main objective of the project is to detect the Hardware Trojan in IOT devices and other hardware system using Machine learning as it can be used to identify hardware trojans at an early stage, before they have the chance to cause damage. This can help to prevent serious security breaches and minimize the impact of any detected trojans

- **Protection of Hardware Devices –** As the IOT industry is growing exponentially in the coming years, the other main objective of the project is to help secure and protected manufacturing and implementation of IOT devices into various sectors as help in secured data transfer in between devices.

- **Prevention of sensitive information leakage:** The other main essential objective of detecting hardware trojans are to verify the trustworthiness of manufactured ICs and to prevent disaster effects such as denial of service, sensitive information leakage from inside a chip (e.g. the key in a cryptographic chip) during the field operation.

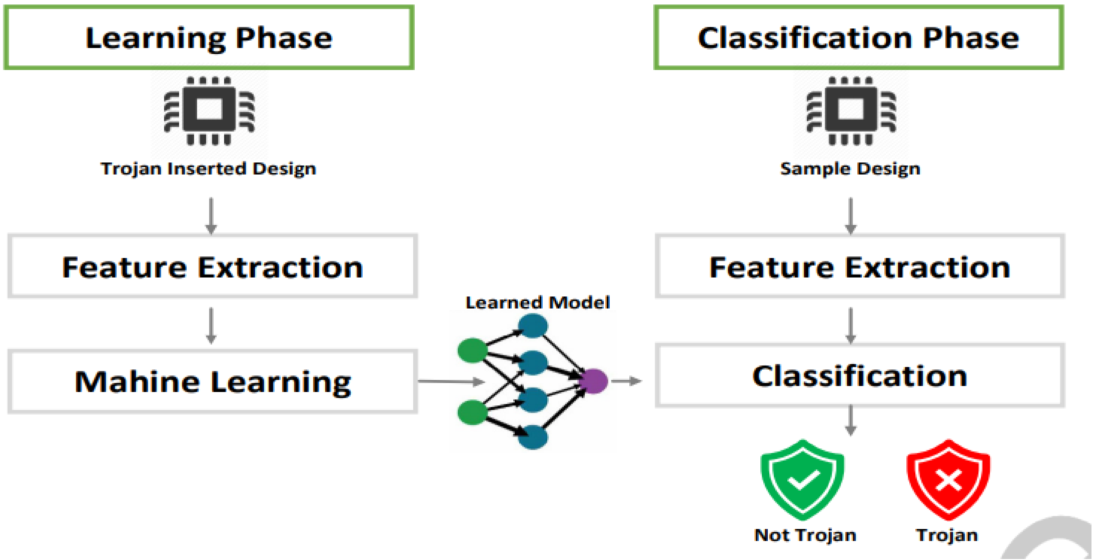


Figure 1 Objective of Hardware Trojan detection

3. Feasibility Study

- **Technical Feasibility:**
  The proposed project is technically feasible as there are existing methods and techniques for Hardware Trojan detection. The use of scan chains, fault injection, and side-channel analysis are some of the common methods used in the industry. The project will require expertise in hardware design, computer engineering, and machine learning, and the necessary hardware and software tools for implementation are readily available.
- **Market Feasibility:**
  Hardware Trojan detection is an emerging field, and the demand for such systems is expected to increase in the coming years as more organizations become aware of the potential risks associated with hardware Trojans. The project has the potential to be used by various industries such as defence, finance, and telecommunications, which require high levels of security.
- **Financial Feasibility:**
  The project may require a significant investment in hardware and software tools, but the cost of implementation will depend on the level of complexity and the size of the ICs that the system will be designed for. The revenue potential of the project will depend on the target market and the pricing strategy that is adopted. The project may require a significant initial investment, but the potential return on investment is expected to be high.
- **Operational Feasibility:**
  The study should evaluate the operational requirements of the hardware Trojan detection system, including the staffing needs, training requirements, and potential risks associated with the system.
- **Legal and Ethical Feasibility:**
  The development of a hardware Trojan detection system raises legal and ethical concerns such as intellectual property rights and privacy. The project team will need to ensure that they comply with relevant laws and regulations and that they take appropriate measures to protect the privacy of users.

Conclusion:

Overall, the feasibility study suggests that the proposed project is technically, market, financially, and legally feasible. With the increasing demand for hardware Trojan detection systems, the project has the potential to be successful and provide a valuable solution to the industry. However, it is important to consider and address the ethical and legal concerns associated with the project.

5. Methodology

Hardware Trojan detection using Python can be done through various methods, and the exact methodology used will depend on the specific requirements and characteristics of the hardware system being analysed. However, here are some general steps that can be taken:

- **Define the System:** Identify the hardware system that will be analyzed for the presence of hardware Trojans, including the type of integrated circuit (IC) and its functionality.

- **Identify Trojan Models:** Gather information on known hardware Trojan models that are likely to affect the type of IC being analyzed. This can be done through research on existing literature and other resources.

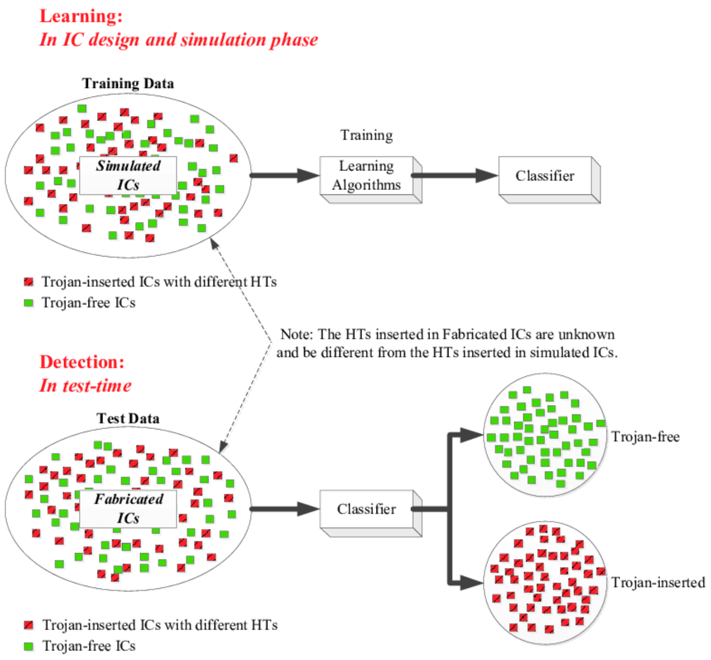
- **Analyse the Circuit Design:** Use Python tools and libraries to analyze the circuit design of the IC, identifying any deviations from the expected behaviour. This can be done using techniques such as reverse engineering or side-channel analysis.

- **Simulation:** Simulate the IC and its behaviour under different conditions using Python to identify any anomalies that could be indicative of hardware Trojans.

- **Feature Extraction:** Extract relevant features from the simulation data using Python, such as power consumption, frequency, or timing measurements.

- **Machine Learning:** Use Python libraries for machine learning to train a model on the extracted features, distinguishing between normal and abnormal behaviour.

- **Trojan Detection:** Use the trained model to detect hardware Trojans in the IC under analysis. This can be done in real-time or through post-processing of captured data.


Learning:
In IC design and simulation phase
Training Data
Simulated ICs
Training
Learning Algorithms
Classifier
🟥 Trojan-inserted ICs with different HTs
🟩 Trojan-free ICs
Note: The HTs inserted in Fabricated ICs are unknown and be different from the HTs inserted in simulated ICs.
Detection:
In test-time
Test Data
Fabricated ICs
Classifier
Trojan-free
Trojan-inserted
🟥 Trojan-inserted ICs with different HTs
🟩 Trojan-free ICs

6. Facilities required for proposed work

- **Software required:**

- o Jupyter Notebook
- o Front End: With the aid of PYTHON, a programming language and its libraries.
- o Back End: With the aid of Database Management System.

- **Hardware required:**

- o 64-bit CPU (Intel / AMD architecture) (At least Dual core processor)
- o 4 GB RAM
- o At least 5 GB free disk space.
- o Defected and non-defective Integrated Circuits.

7. References

[1] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. 2007. Trojan detection using IC ingerprinting. In

2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 296ś310.

[2] Naveed Akhtar and Ajmal Mian. 2018. Threat of adversarial attacks on deep learning in computer vision: A survey. Ieee Access 6 (2018),

14410ś14430.

[3] Christoph Albrecht. 2005. IWLS 2005 benchmarks. In International Workshop for Logic Synthesis (IWLS): http://www. iwls. org.

[4] Karim Arabi, Resve Saleh, and Xiongfei Meng. 2007. Power supply noise in SoCs: Metrics, management, and measurement. IEEE Design

& Test of Computers 24, 3 (2007), 236ś244.

[5] Maitreyi Ashok, Matthew J Turner, Ronald L Walsworth, Edlyn V Levine, and Anantha P Chandrakasan. 2022. Hardware Trojan

Detection Using Unsupervised Deep Learning on Quantum Diamond Microscope Magnetic Field Images. ACM Journal on Emerging

Technologies in Computing Systems (JETC) (2022).

[6] Chongxi Bao, Domenic Forte, and Ankur Srivastava. 2014. On application of one-class SVM to reverse engineering-based hardware

Trojan detection. In Fifteenth International Symposium on Quality Electronic Design. 47ś54. https://doi.org/10.1109/ISQED.2014.6783305

[7] Chongxi Bao, Domenic Forte, and Ankur Srivastava. 2016. On Reverse Engineering-Based Hardware Trojan Detection. IEEE Transactions

on Computer-Aided Design of Integrated Circuits and Systems 35, 1 (2016), 49ś57. https://doi.org/10.1109/TCAD.2015.2488495

[8] Mariana Belgiu and Lucian Drăguţ. 2016. Random forest in remote sensing: A review of applications and future directions. ISPRS journal

of photogrammetry and remote sensing 114 (2016), 24ś31