Security and Trust in Integrated Circuits

Vasisht Duddu

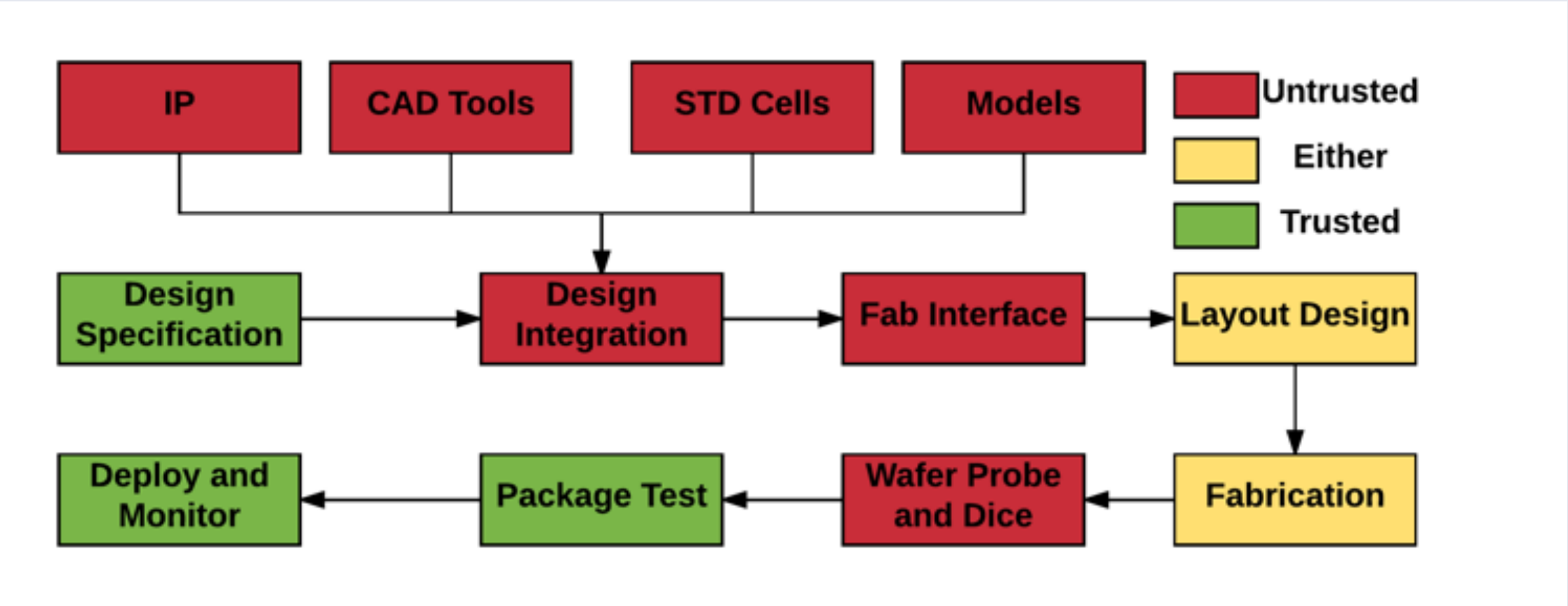
Advisors: Dr. Mohammad Hashmi, Dr. Donghoon Chang

Abstract

The increasing globalisation of Integrated Circuits(ICs) supply chain has reduced the control of the vendor over the design and fabrication process which increases the possible threats by adversaries to exploit vulnerabilities and compromise the hardware. The fabrication of ICs is a multi-step process spread across various parts of the world for commercial reasons. In such situation, hardware root of trust, i.e, the assumption that the hardware is secure against all possible attacks is violated. Design and study of trusted integrated circuit design and reliable circuits are therefore crucial, especially, when the circuits are being used for critical applications like military and critical national infrastructure. This work studies the threat model of Integrated circuits supply chain and study various attacks and then explores topics like Hardware Trojans and physically unclonable functions by implementing a counter based asynchronous trojan and an analog unclonable function.

Threat Modelling

IC Supply Chain



Specification Phase: The designers decide on the high level description of the building blocks and define the system's characteristics including power consumption, area, delay and functionality.

Design Phase: This is the most vulnerable phase where designers consider functional, logical, timing and physical constraints and they map the schematic to the hardware. This includes using multiple 3rd party IP cores, standard cells and EDA tools which might be vulnerable and contain trojans.

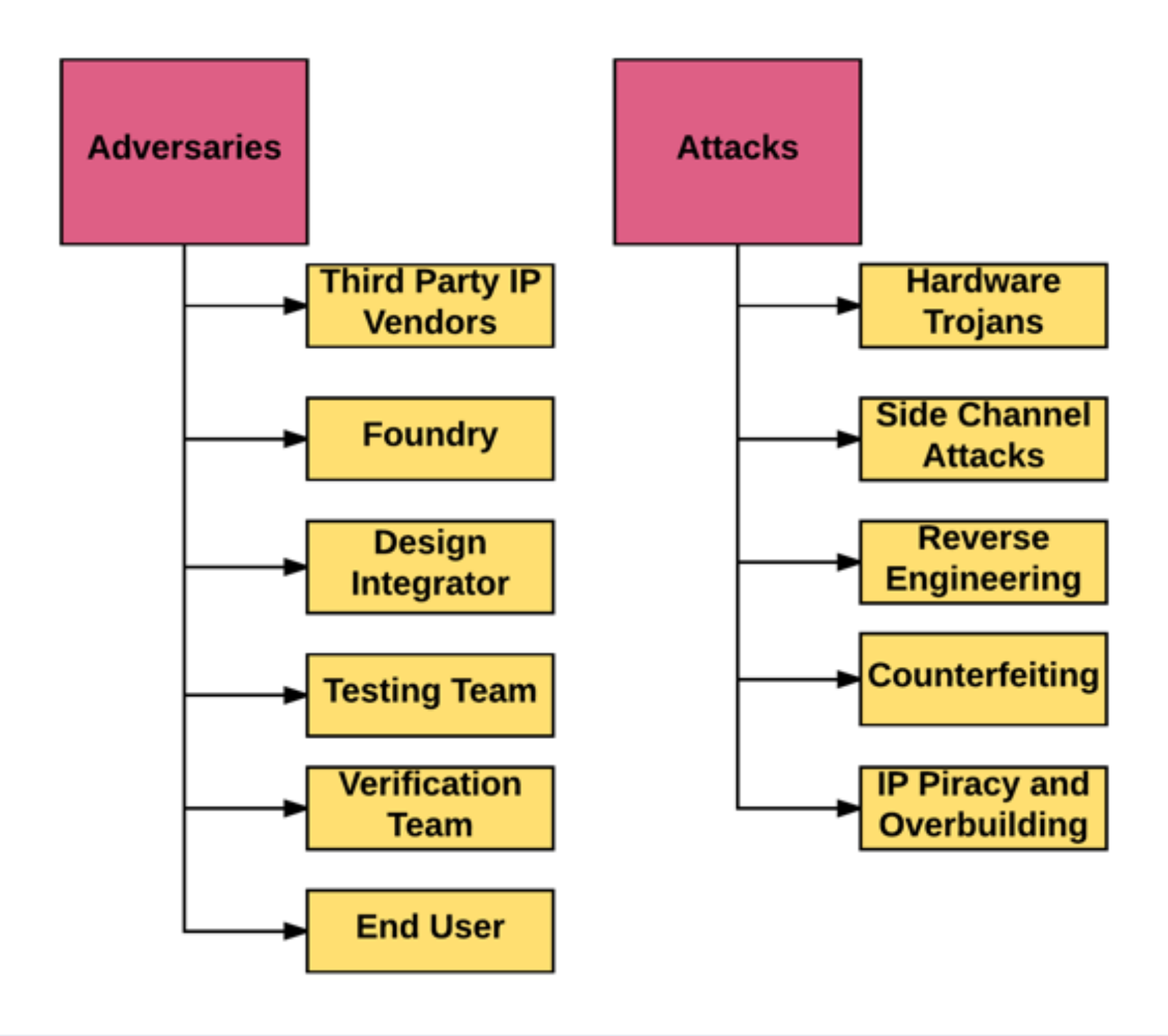
Fabrication Phase: Designers create the layout/mask and send it to the fab to create the chip. Attacker might make small modifications to the mask or change chemical composition to effect the current flow decreasing the reliability of the circuit.

Assembly: At this stage, different components are assembled on a PCB and every junction where two components are connected is a possible site for trojan insertion. Even if all individual chips are trustworthy, malicious assembly might create security issues in the circuit. The usage of unshielded wires to leak information via side channels.

Testing Phase: This is the phase for detection of any vulnerabilities introduced in the circuits which includes using trojan detection techniques and test vectors that have to kept secret to prevent attacker from effecting the testing phase. This phase is considered as trustworthy to detect any modification made by attacker to the circuit in the previous **stages.**

Attacker Motive

- **Leak information**
- **Steal Data**
- **Counterfeit/Duplicate circuit**
- **Reduce the reliability of the system**
- **Denial of Service**
- **Maintain and monitor system activities**



Threats

Hardware Trojan: An attacker either in the design house or foundry may add malicious circuitry or modify existing circuits to effect the reliability of circuit or run some malicious logic.

Intellectual Property(IP) Piracy or overbuilding: An IP user or rogue foundry may pirate the IP without the knowledge or consent of the designer leading to IP Theft. A malicious foundry may build more than required number of ICs and sell the excess components to the grey market.

Reverse Engineering: The attacker traces back the IC to some abstraction level in the IC supply chain. The attacker may use Reverse engineering to reach a desired abstraction level and then modify the IP or change it.

Side Channel Analysis: Circuits while executing some code or performing cryptographic operations radiates EM waves or information from other channels. An attacker can extract information from these side channels and process them to get secret information like cryptographic keys.

Counterfeit: Attacker forges original component by reverse engineering the IC to certain abstraction level and rebuild these circuits using other components. Systems using these circuits might effect the reliability and security.

Attacker Knowledge

Complete Knowledge: The attacker may have complete Knowledge of the system using which he may reverse engineer the circuit, counterfeit the circuit design, leak secret information like cryptographic keys and insert trojan to maintain backdoor access to the system.

Partial Knowledge: If the attacker has partial knowledge he is required to alleviate knowledge using side channel and Reverse Engineering and then perform other attacks like insert trojans for future access and control of system.

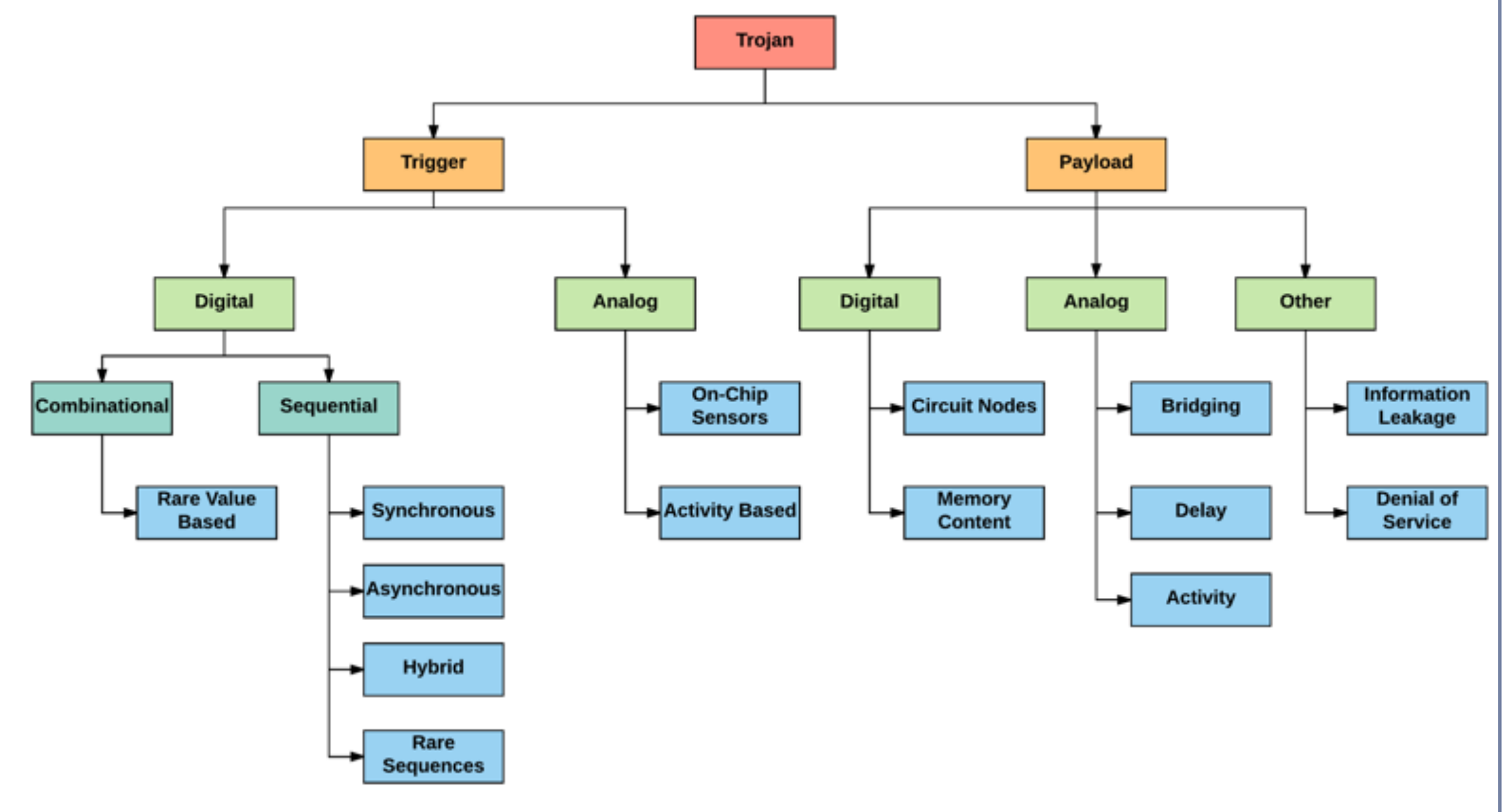
Hardware Trojans

Hardware trojans are any malicious addition or modification to a circuit or system. There are two main characteristics of hardware trojans:

- **Malicious Goals:** This includes change or control functionality, leak sensitive information and reduce circuit reliability.
- **Intentional addition or modification**

Hardware Trojans are very hard to detect as the opaqueness of circuit internals reduces observability, preventing use of some common types of detection methods. Secondly, the technology scaling in semiconductor makes it difficult to differentiate between variation and hardware trojan behaviour. Thirdly, there is a large uncharacteristic space for the possible Trojan insertion making it difficult to detect the trojans.

Taxonomy



IC Supply Chain: This is based on where the HT is inserted in the supply chain which has been discussed in Chapter 1.

Abstraction level: This classification is based on where the HT is embedded in the design phase abstraction. Following are the possible phases and corresponding trojans that can be inserted:

- **Architectural or RTL Level**: Attacker can make changes in the Verilog or VHDL code to modify the functionality.
- **Functional level**: Attacker can make modification to gate level schematics or sum equation or product function.
- **Logic synthesis/gate level**: Attacker can include a kill switch to disable a circuit using a control signal and modifying the gate to include a control signal.
- **Circuit or Transistor level**: This includes changing the threshold voltage or transistor to effect delay or power consumption
- **Physical design or Layout Level**: Dimensions or location of components can be changed to include HT.

Activation or Trigger Mechanism: This classification is on how the trojan will be activated and can be further broken into combinational trojan where the activation depends on certain rare condition in circuit and sequential trojan where activation depends on sequence of rare values in circuit. It is more difficult to trigger sequential as a particular sequence of rare values are required and test vectors may not cover them during the testing phase. The trojans can also be classified as synchronous which uses clock to count cycles(time bombs) and trigger at some instant or asynchronous trojan which uses output of some other logic to count the cycles.

Effects or Payload: This is on the basis of the result or payload of the trojan after being activated which includes DoS, changing memory content, effecting the parameters of circuit like performance, power and noise margin.

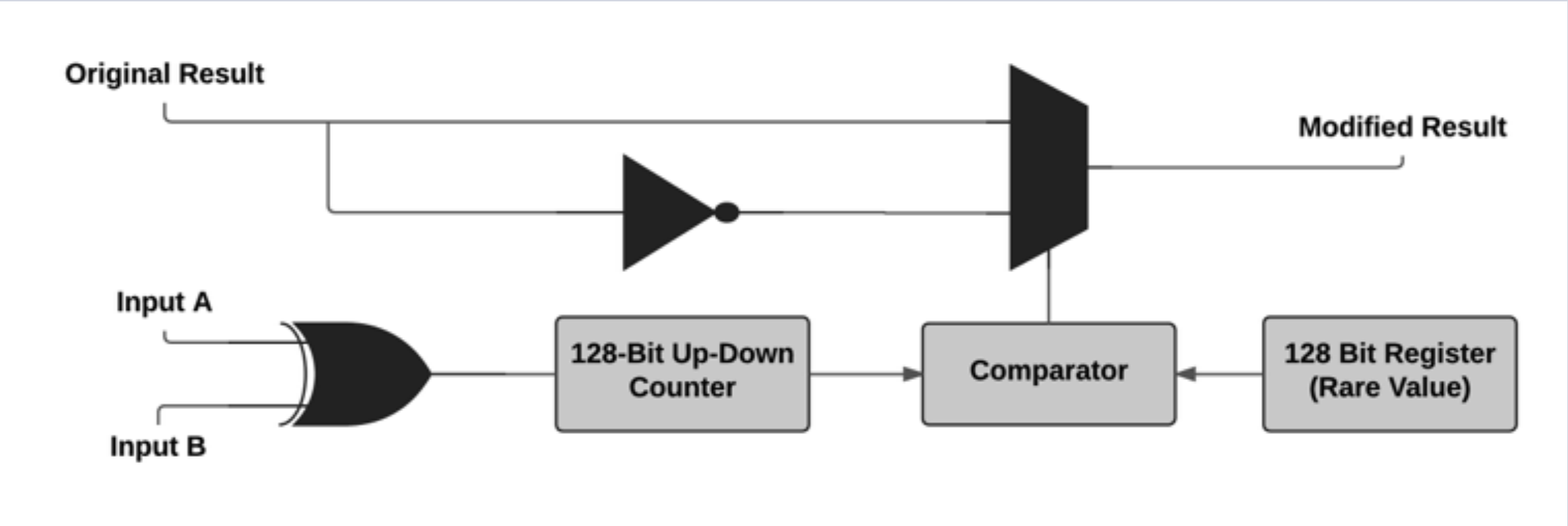
Location: This is based on where on-chip is HT located. The trojan may be located in the processor(change execution and functionality), memory(alter memory contents), IO devices(control/modify/modify data communication), power supply units(change power/current to reduce the reliability) and clock grid(change freq. to cause fault or failure)

Type: Trojans can be further classified into parametric or functional where parametric trojans aim to reduce the reliability of the system to increase the chance of performance failure. This includes thinning wires, weakening logic gates, modifying the power supply or changing the transistor size and properties. On the other hand, functional trojans includes addition/deletion of gates to effect the system's functionality.

Trojan Design

The trojan design mechanism has two aspects: trigger and output payload. The trojan should be triggered under rare events or conditions and should not be easily detected by testing.

In this work, we work on a Trojan design based on Asynchronous Counter. The design uses a 128 bit up down counter where the payload is to modify the output bit. The design schematic is given below.



Hardware Trojan Detection and Prevention

Destructive: This method uses one sample or set of sample ICs and reverse engineer each IC to reveal inner working and structure and find malicious modifications. It is not a practical approach as it requires tools, equipment, knowledge and time.

Also, a sample may not have a trojan however, me other IC may have the trojan.

Non-Destructive: Non-Destructive detection techniques can be broken as:

- **Test Time Techniques:** These techniques are used for trojan detection after the circuits have been designed and fabricated and during the testing phase by a trusted verification team.
- **Logic Test based HT detection**: This includes running different test vectors and monitoring the circuit's output behaviour. If HT is triggered, its malicious behaviour will be observed which can be detected. However, for big circuits the input size is huge and full coverage test is impractical. Random test will fail as HT are triggered by rare test vectors which may not be selected in random test.
- **Side Channel Analysis Based HT Detection**: This method monitors the side channel information during execution at test time. The presence of HT on chip will show on some physical parameters and can be observed through certain side channels. However, this method may give high false positives.

Run Time Techniques: These techniques monitor the execution at real time and observe malicious behaviour. The stop execution once HT is detected to protect system. It is a good complementary approach to test time approach which may not be 100\% effective. It however takes extra resources and more performance overhead.

Future Work

As part of future work, I would explore and design an analog physically unclonable function(PUF) as a hardware security primitive to improve the security and authenticate circuits. The study would explore various PUF architectures and study the recent trend in PUF design and implement an analog PUF using cadence(virtuoso)/spice and perform simulations.

References

[1] Ramesh Karri and Jeyavijayan Rajendran, Kurt Rosenfeld, Mohammad Tehranipoor, Trustworthy Hardware: Identifying And Classifying Hardware Trojans, IEEE Design \& Test of Computers, 2010

[2] Masoud Rostami, Farinaz Koushanfar, and Ramesh Karri, A Primer on Hardware Security: Models, Methods, and Metrics, Vol. 102, No. 8, August 2014 | Proceedings of the IEEE

[3] Swarup Bhunia, Michael S. Hsiao, Mainak Banga, and Seetharam Narasimhan, Hardware Trojan Attacks: Threat Analysis and Countermeasures, Vol. 102, No. 8, August 2014 | Proceedings of the IEEE

[4] Mohammad Tehranipoor, Farinaz Koushanfar, A Survey of Hardware Trojan Taxonomy and Detection, IEEE Design \& Test of Computers

[5] Seetharam Narasimhan, Xinmu Wang, and Swarup Bhunia, Wen Yueh and Saibal Mukhopadhyay, Improving IC Security Against Trojan Attacks Through Integration of Security Monitors

[6] Miodrag Potkonjak, Ani Nahapetian, Michael Nelson, Tammara Massey, Hardware Trojan Horse Detection Using Gate-Level Characterization, DAC'09, July 26-31, 2009, San Francisco, California, USA

[7] Rajat Subhra Chakraborty, Seetharam Narasimhan and Swarup Bhunia, Hardware Trojan: Threats and Emerging Solutions, IEEE 2009

[8] Mainak Banga and Michael S. Hsiao, Trusted RTL: Trojan Detection Methodology in Pre-Silicon Designs, IEEE 2010

[9] Huafeng Liu, Hongwei Luo, Liwei Wang, Design of Hardware Trojan Horse Based on Counter, IEEE 2011

[10] Jie Zhang and Qiang Xu, On Hardware Trojan Design and Implementation at Register-Transfer Level, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

[11] Yier Jin and Yiorgos Makris, Hardware Trojans in Wireless Cryptographic ICs, IEEE Design \& Test of Computers

[12] Swarup Bhunia, Michael S. Hsiao, Virginia Tech, Jim Plusquellic, Mohammad Tehranipoor, Miron Abramovici, Dakshi Agrawal, Paul Bradley, Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution, IEEE Design \& Test 2012

[13] K. XIAO, D. FORTE, Y. JIN, R. KARRI, S. BHUNIA and M. TEHRANIPOOR, Hardware Trojans: Lessons Learned after One Decade of Research, ACM Transactions on Design Automation of Electronic Systems, 2016

[14] Samantha Pham, Jennifer L. Dworak§, and Theodore W. Manikas, An Analysis of Differences between Trojans inserted at RTL and at Manufacturing with Implications for their Detectability

[15] Dakshi Agrawal Selcuk Baktır, Deniz Karakoyunlu, Pankaj Rohatgi, Berk Sunar, Trojan Detection using IC Fingerprinting

[16] Nicole Fern, Shrikant Kulkarni and Kwang-Ting (Tim) Cheng, Hardware Trojans Hidden in RTL Don't Cares - Automated Insertion and Prevention Methodologies, INTERNATIONAL TEST CONFERENCE, 2015

[17] H. Salmani, M. Tehranipoor, J. Plusquellic, New Design for Imroving hardware trojan detection and reducing Trojan activation time, HOST 2009

[18] J.Li and J. Lach, At speed delay characterization for IC authentication and hardware trojan Horse detection, HOST 2008

[19] M. Banga, M. Hsiao, VITAMIN: voltage inversion technique to ascertain malicious insertions in ICs, HOST 2009

[20] J. Gu, G. Qu and Q. Zhou, Information Hiding for trusted system design, DAC 2009

[21] RS Chakraborty and S. Bhunia, Security against hardware trojan through a novel application of design obfuscation, ICCADD 2009

[22] E. Love, Y. Jin, Y. Makris, Enhancing security via provably trustworthy hardware intellectual property, HOST 2011

[23] C. Dunbar, G. Qu, Designing trusted embedded system fro finite state machine, TECS 2014

[24] Nicole Fern, Shrikant Kulkarni, Kwang-Ting TIm Cheng, Hardware Trojans Hidden in RTL Don't Cares-Automated Insertion and Prevention Methodologies, International Test Conference, 2015

[25] Jie Zhang, Qiang Xu, On Hardware Trojan Design and Implementation at Register-Transfer Level