IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

# Detecting Trojans and Enhancing Security of Safety Critical IP Cores

**Srinivas Mallimoggala[1], Ravi Tej Nulu[2]**

Assistant Professor (C), School Of Avionics JNTUK Kakinada[1]

PG Student, JNTUK Kakinada[2]

**Abstract:** The Intellectual Property (IP) blocks are designed by hundreds of IP vendors distributed across the world. Such IPs cannot be assumed trusted as Trojans can be maliciously inserted into them and could be used in military, financial and other critical applications. It is extremely difficult to detect Trojans in third-party IPs simply with conventional verification methods as well as methods developed for detecting Trojans in fabricated ICs. The transfer of provably trustworthy modules between hardware IP producers and consumers, and discuss what it might mean for a device to be considered "secure". We outline a semantic model representing the constructs permissible in a Verilog Hardware Description Language (HDL) and show how this model can be used to reason about the trustworthiness of circuits represented at the Register-Transfer Level (RTL). Identifying Suspicious Signals (SS) with formal verification, coverage analysis and Structural tests is area of focus.

**Keywords:** HDL, RTL, IP, Trojans, secure, formal verification, coverage analysis, Structural tests.

## 1. INTRODUCTION

The problem of hardware security has grown more important and more difficult with the emergence of an increasingly globalized design process. The tight control manufacturers once exerted over their devices is no longer possible when more complicated systems now employ hardware components from a variety of different suppliers whose trustworthiness is unknown. Researchers have, accordingly, devised techniques to diffuse the threat of malicious circuitry (Trojans) being inserted into the supply chain, relying variously on physical, behavioural, and formal methods .Our scheme is different from previous approaches to the problem of hardware Trojans in that it does not concentrate on the physical level of chip layout, but focuses instead on the security of third-party Intellectual Property (IP) modules commonly used in contemporary designs. Moreover, it differs even from all other pre-silicon security methods, because it makes guarantees that are more expressive than simple equivalence testing. We imagine an attacker who makes malicious modifications to a module's HDL code in order to introduce the potential for undesired behaviour. This module may then be sold for use in a larger system which, with the inclusion of tampered IP, becomes itself vulnerable to attack.

If, however, we can guarantee that certain carefully specified properties hold across the outputs of components from un-trusted IP vendors, then we may be able to guard against certain types of undesirable or insecure behaviour. These can include disruption of operation, manipulation of signals, or misuse of sensitive data. Each case requires different kinds of properties, but a strong specification can render many modes of attack significantly more difficult to implement. If these safeguards become integrated into the design process, then when an IP consumer asks for some module to be constructed, he will provide the vendor with not only a functional specification, but also a list of specific security-related properties (Test bench) that the desired module must obey.

The ultimate goal of developing security-critical systems is to provide evidence that, in addition to the functionality and quality of service requirements, the specific security requirements are met. To Implement and Simulate Functional Test Bench for an IP-Core following methodology is followed ,Soft IP-cores which generally include register transfer level (RTL) descriptions in languages such as Verilog or VHDL is taken for analysis . Software tool used for this purpose is Xilinx ISE and the Simulator is Questa Verification IP which is a model used to verify a protocol or interface. These models bridge the gap between RTL, TLM, and system-level verification by using a hierarchy of transactions to create a link between different TLM and RTL abstraction levels. Questa Verification IP's include stimulus generation, reference checking and coverage measurements. Functional verification is done by writing the test bench and compared with Structural tests the final outcome of this verification process is to find the Trojans

## 2. DESCRIPTION OF IP CORE

Soft IP-cores are the category of IP-core that comes to the user with the most life-cycle data. This data generally include

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

register transfer level (RTL) descriptions in languages such as Verilog or VHDL. This allows a detailed analysis and optimization (and eventually customization) of the soft IP-cores for the intended application. Soft IP-cores still need to be synthesized placed and routed (P & R) in the target. Firm IP-cores are next in the decreasing level of design description, specified in technology-independent netlist level format. This allows the IP provider to hide the critical IP details and yet allow the IP user to perform some limited amount of analysis and optimization during placement, routing, and technology-dependent mapping of the IP block. Firm IP-cores still need to be placed and routed in the device. Hard IP-cores have the least design description and life-cycle data, specified in technology-dependent physical layout format using industry standard languages such as stream, polygon, or GDSII format. Hard IP-cores can be thought of as a "black box" that, due to the lack of knowledge about the internal detailed design, they cannot be fully analyzed and/or co-optimized. Hard IP-cores come with a detailed specification of integration requirements in terms of clock, testing, power consumption, interfaces and a host of other parameters. Hard IP-cores are embedded in the PLD/ASIC at the silicon level.

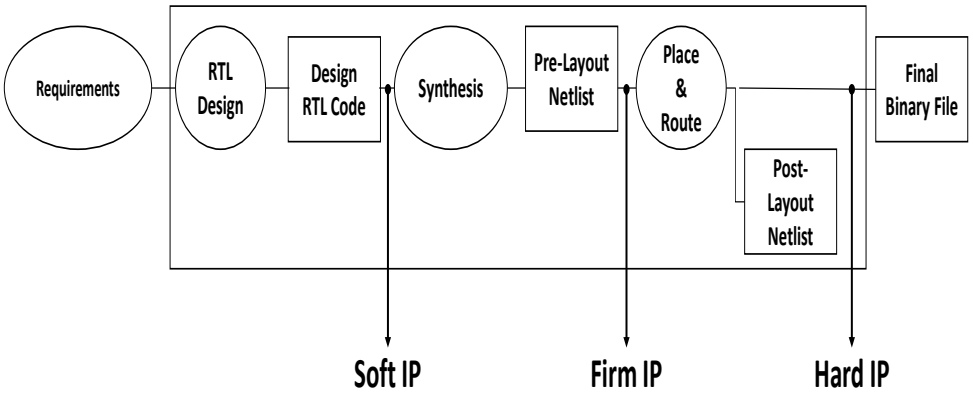


Fig: 1 Soft, Firm & Hard IP in FPGA IP-core Development

## 3. METHODOLOGY

Soft IP-cores which generally include Register Transfer Level (RTL) descriptions in languages such as Verilog or VHDL is taken for analysis. Software tool used for this purpose is Xilinx ISE and the Simulator is Questa Verification IP which is a model used to verify a protocol or interface. Software tool used for this purpose is Xilinx ISE and the Simulator is Questa Verification IP which is a model used to verify a protocol or interface

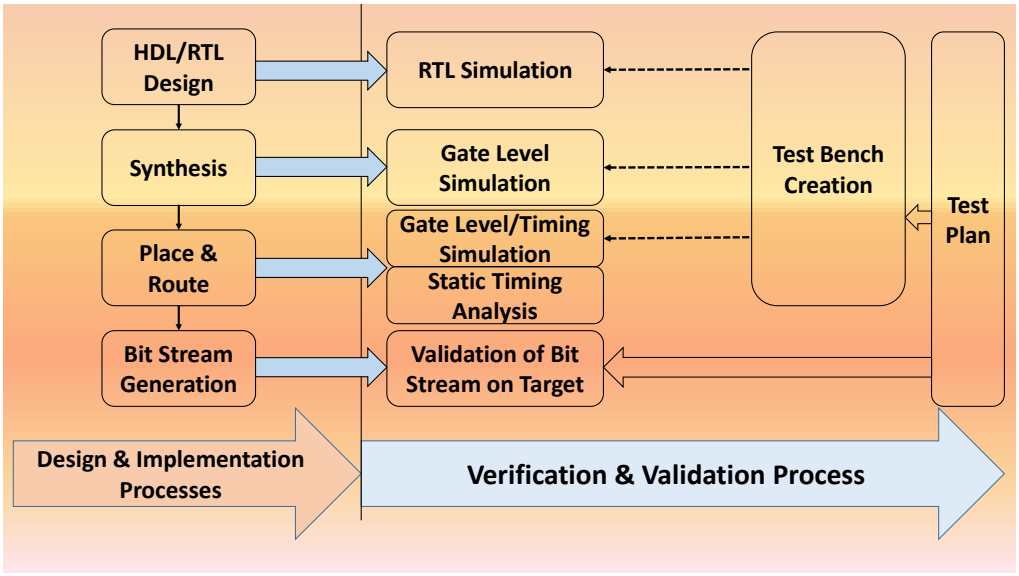


Fig: 2 Hardware Developments

The semiconductor industry verification flow for any hardware can be summarized as Assertions are used as a debug tool and also as coverage metric. Multiple coverage metrics are used, including: Statement coverage, Branch coverage, Expression coverage, Path coverage, Finite State Machine (FSM) coverage, Toggle coverage, and Functional coverage. Three primary structural coverage metrics:

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

- **Statement coverage**: Every statement in the program has been invoked or used at least once.
- **Decision coverage (DC):** Every entry and exit point in the program has been invoked at least once. In addition, each decision in the program has been taken on all possible outcomes (true/false) at least once.
- **Modified condition decision coverage (MCDC):** Every entry and exit point in the program has been invoked at least once. Every condition in a decision in the program has taken on all possible outcomes at least once

Verification plan should be written to address which device functions need to be tested and also under which conditions the functions are to be tested. Functional coverage metric is then used to measure how many of the identified device functions have been tested. Were all possible input stimuli variations injected? Was all possible output conditions achieved? Did all possible internal state transitions take place? Did all the interesting events occur?

## 3. TESTING PROCESS

The Mentor Graphics Questa Sim shall be used for following testing purpose.

1. RTL Behavioural Simulation 2. Post Synthesis Simulation 3. Place & Route Simulation

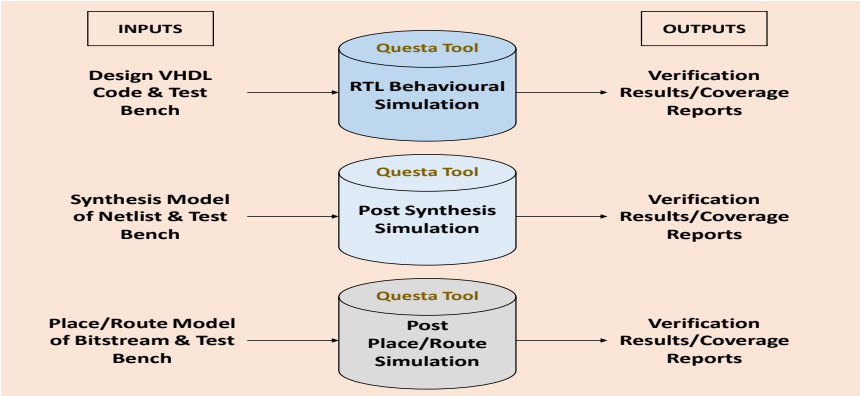


Fig: 3 Testing Tool Usage

A. **Simulation and On-Target Testing** Mentor Graphics Questa Sim shall be utilized for performing the simulation activities of the designed IP-core. On target the testing is limited for performing functionality test of the IP-core.

B. **Test Execution and Test Results Compilation** Test cases execution for Behavioral Simulation, Post Synthesis Simulation, Post Translate simulation and Post PNR (Place & Route) simulation will be performed and associated results will be generated.

C. **Elemental Analysis Resolution** Elemental Analysis (code coverage) will be performed on RTL code and on Post Synthesis verification model at integrated levels.

Table: 1 Method of Verification

| Design | Verification methods | Reports |
|---|---|---|
| RTL code | Behavioral simulation at unit level and integration level | Code coverage , behavioral simulation and traceability reports |
| Post translate verification model | Functional simulation at integration level | Functional simulation results |
| Post place & route verification model | Static timing analysis, functional &timing simulation at integration level | Static timing analysis, functional &timing simulation reports |

## 5. IC AUTHENTICATION AND TROJAN DETECTION

The objective is to ensure that the designed chip/system will carry out only our desired function and nothing more. Functional patterns could potentially detect a “functional” Trojan. For which a Exhaustive test would be effective and it is Not applicable for large circuits such as 64 input adder which has $2^{65}$ input combination including carry in, this is impractical. Generally only a few and effective patterns are used, resulting in escape of Trojans. The fault coverage is low for manufacturing test.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

In practice, structural tests are used. Structural tests cannot verify functionality of a circuit as Trojan is not a defect until is being activated.

Table 2: Classification of Hardware Trojans

| **Insertion Phase** | **Abstraction Level** | **Activation Mechanism** | **Effects** | **Location** |
|---|---|---|---|---|
| Specification | System level | Always on | Change the functionality | Processor |
| Design | Development environment | Triggered Internally | Downgrade performance | Memory |
| Fabrication | Register-transfer level | Triggered Externally | Leak information | I/O |
| Testing | Gate level | ---- | Deny service | Power supply |
| Assembly and package | Transistor level | ---- | ---- | Clock grid |
| ---- | Physical level | ---- | ---- | ---- |

According the Classification, there are many types of Trojans that are not functional and cannot be activated using test patterns. Full Activation: The process in which a triggered Trojan launches its malicious function. Partial Activation: The process in which some gates, often at the earlier stages, switch. Activity will refer to partial activation in this case.

**Detection Schemes:** following are the different Trojans detection techniques from literature

1. Activation Techniques

An attempt to fully activate Trojans will be made or else Improve the likelihood of partial activity of Trojans this Techniques are Use in conjunction with side-channel techniques.

2. Side Channel Techniques

In this Technique Monitoring circuit's side-channel parameters to determine abnormalities will be made.

3. Design for Trust

Any technique that alters the design process to make Trojan-insertion more difficult, but it does not aim to detect Trojans that have already been inserted. Fill unused standard cells. Unused spaces are often filled with decoupling capacitors which Reduce noise but Consume power. Even some may be removed without any noticeable change to the circuit. Modify design process to make Trojan-insertion difficult

4. Reverse Engineering

Here thorough examination of the physical manifestation of the circuit is done Destructive reverse-engineering is used to build golden models. Alone, destructively testing a subset of all ICs cannot guarantee that the rest of the ICs are actually Trojan Free. MARVEL: Malicious Alteration Recognition and Verification by Emission of Light i.e. Active devices emit infrared light when turned on; High sensitivity photon sensors capture the weak emission while the circuit is supplied with test patterns.

Present paper focuses on Side Channel Techniques; Side Channel Signal Analysis consists of Transient Power (Current) Analysis for which Full activation is not necessary. Switching at the inputs of a Trojan and inside the Trojan can increase transient power .Circuit Delay Analysis is one in which Trojan does not need to be targeted Trojan itself will impact circuit path delay , focus is on Target paths rather than Trojans.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

Table 3: Methods to find Hardware Trojans

| Hardware Trojans | Logic Test | Power SCA | Delay SCA | Run Time |
|---|---|---|---|---|
| Parametric | No | Yes | Yes | No |
| Big | Can't say | Yes | Can't say | Yes |
| Small | Yes | No | Yes | Can't say |
| Tight | Yes | Yes | Yes | Can't say |
| Loose | Yes | Can't say | Yes | Can't say |
| Always ON | No | No | Yes | No |
| Leak info | No | Yes | No | Yes |

Hardware Trojans inserted in chip can change the power consumption characteristics. Tight or loose distribution of Trojans can significantly impact detection through power analysis and isolation. Partial activation of Trojan can be extremely valuable for power analysis .The current drawn is dependent on the number of gates which are partially activated.

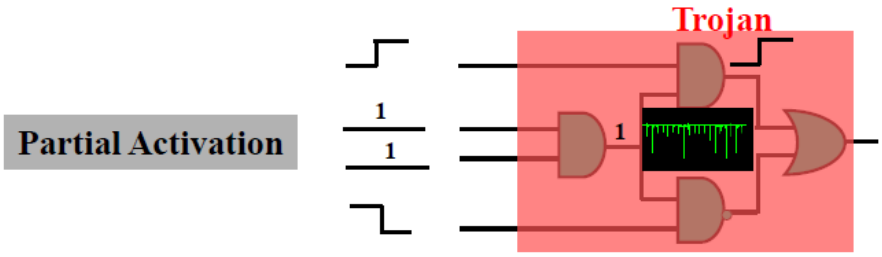


Fig: 4 Partial activation of Trojan (example)

Following equations represent Current consumption of Trojan-free and Trojan-inserted circuits

$$Q_{trojan\text{-}free}(t) = \int I_{trojan\_free}(t) \; . \; dt$$

$$Q_{trojan\text{-}inserted}(t) = \int I_{trojan\_inserted}(t) \; . \; dt = \int (I_{trojan\_free}(t) + I_{trojan}(t)) \; . \; dt$$

Hardware Trojans can also change the circuit delay characteristics. Some Trojans cannot be detected using power analysis methods. A change in physical dimension of the wires and transistors can also inject delay to the paths in the circuit.

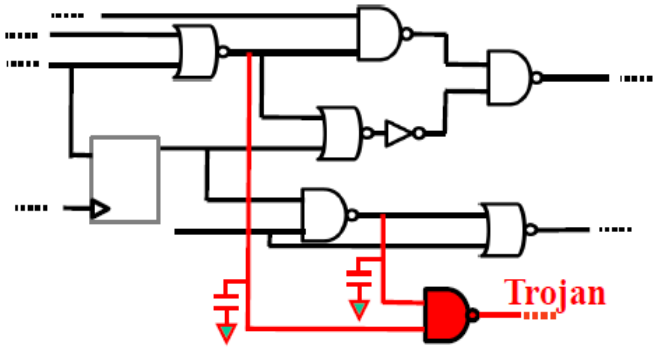


Fig: 5 Side Channel Analysis – Delay

Path Slack: difference between operating period and the period where a particular path is likely to fail and cause a timing error.
Critical Path: The longest path in the circuit. The critical path is used to determine the operating frequency.
Path slack decreases with path length. A Trojan is more likely to cause a timing error on a longer path. A Trojan will consume more power on a shorter path. Adversaries must find a balance while also achieving the desired malicious effect.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

## 6. PROOF OF CONCEPT

The ISCAS '85 benchmark circuits are ten combinational networks provided to authors at the 1985 International Symposium on Circuits and Systems. They subsequently have been used by many researchers as a basis for comparing results in the area of test generation. As an example, a small, six-NAND-gate circuit, known as “c17”, will be used. Listed below is the netlist for c17:

1 1gat inpt 1 0 >sa1
2 2gat inpt 1 0 >sa1
3 3gat inpt 2 0 >sa0 >sa1
8 8fan from 3gat >sa1
9 9fan from 3gat >sa1
6 6gat inpt 1 0 >sa1
7 7gat inpt 1 0 >sa1
10 10gat nand 1 2 >sa1
1 8
11 11gat nand 2 2 >sa0 >sa1
9 6
14 14fan from 11gat >sa1
15 15fan from 11gat >sa1
16 16gat nand 2 2 >sa0 >sa1
2 14
20 20fan from 16gat >sa1
21 21fan from 16gat >sa1
19 19gat nand 1 2 >sa1
15 7
22 22gat nand 0 2 >sa0 >sa1
10 20
23 23gat nand 0 2 >sa0 >sa1
21 19

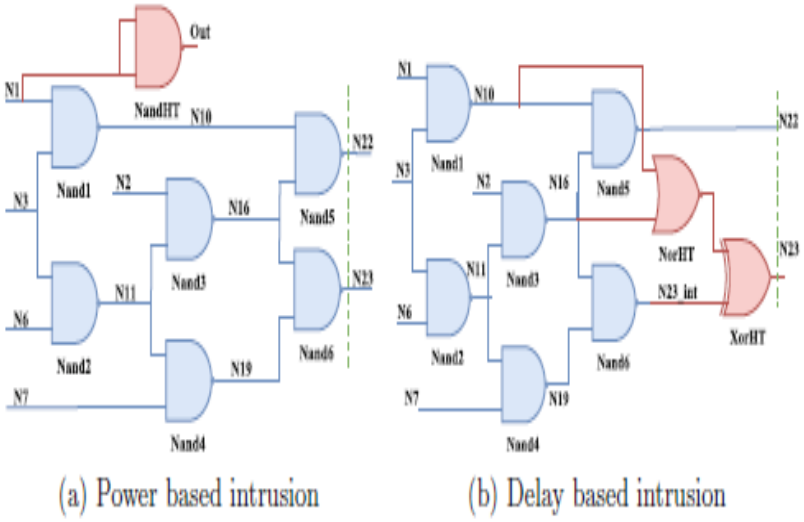


Fig: 6 Intruded ISCAS-85 C17 benchmark circuit

## 7. RESULTS AND ANALYSIS

**Functional verification**: Quantitative analysis for those coverage metrics for the case study is as follows:

- Statement coverage achieved 94.44%
- Branch coverage achieved 96.57%
- Expression coverage achieved 86.36%
- FEC condition coverage achieved 85.71%
- Functional coverage achieved 84.41%
- Coverage metrics achieved 68.67%

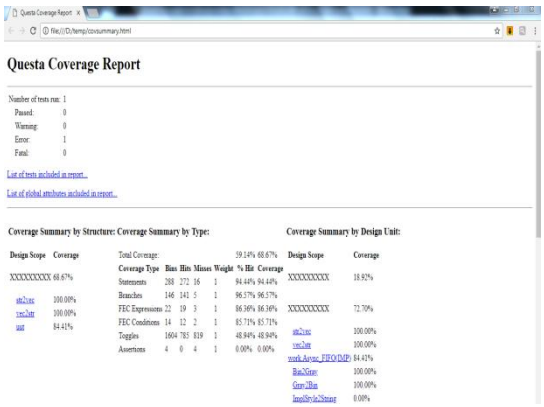


Fig: 6 representative coverage report

Above functional report doesn’t indicate the presence of any Trojan in the IP-cores

**Structural tests:** The intruded variant of C17 has 7 NAND gates, and it has one additional gate due to which the dynamic power check fails. The power consumption at a particular node depends upon the sum of gate and diffusion capacitances. Whenever there is an activity at the input of intruded gate, switching power is consumed by delivering energy to charge capacitance at the output node, and then dumping this energy to ground. The Hardware Trojan in modifies the output at node N23 on rare input vectors. The total load capacitance at the output nodes N23_int and N16 increases due to the addition of gate capacitances of XOR and NOR gates. Added capacitances contribute towards incrementing the propagation delays of the effected paths from input to output node N23.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 6, Issue 9, September 2018

## 8. CONCLUSION

This paper provides a reference for hardware security research and, hopefully, serves as a clear guide for researchers. Through this paper, we hope to develop more innovative and fundamental solutions to solve hardware level threats and, as the final goal, to ensure the trustworthiness. As proof of concept a traditional functional verification was done on an example circuit and shown, how Trojan can be missed, at the same time through a Structural test how they can be weeded out.

## REFERENCES

[1]. Piziali, A., Functional Verification Coverage Measurement and Analysis, Kluwer Academic Publishers, Chapter 4, 2004
[2]. Wei, S., Meguerdichian, S., Potkonjak, M.: Malicious circuitry detection using thermal conditioning. IEEE Trans. Inf. Forensics Secur. 6(3), 1136–1145 (2011)
[3]. Mukhopadhyay, D., Chakraborty, R.S.: Hardware Security: Design, Threats, and Safeguards. CRC (2014)
[4]. Y. Jin and Y. Makris, "Hardware Trojans in wireless cryptographic ICs," IEEE Design and Test of Computers, vol. 27, pp.26–35, 2010.
[5]. M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," Design Test of Computers,IEEE, vol. 27, pp. 10–25, 2010.
[6]. Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in IEEE International Workshop on Hardware-Oriented Security and Trust, 2008, pp. 51–57.
[7]. M, Banga and M, Hsiao, "Trusted RTL: Trojan detection methodology in pre-silicion designs," in Proc. IEEE Int Symposium on Hardware-Oriented Security and Trust (HOST 10), pp. 56-59 2010.