International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

Trojan Detection & Implementation

Deepa, Richa Srivastava

***Abstract*— Trojan Detection is the current affair for the safety of VLSI circuits. It is the process to identify the malicious modification in the schematic design, logic equations, secret data, information pattern etc. Trojan categorization is very deep study here we are emphasizing on implementation as well as detection. We proposed detection approaches to observe a realistic terrifying modification implemented in the 9 stages ring oscillator (RO) to protect schematic design from treacherous variations. Our aim is to explore the impact of various stages of ring oscillator for identifying different classes of Trojan Horses. I am highly obliged to Asst. Professor Richa Srivastava as a project guide for her proper Guidance & support.**

***Index Terms*— Ring Oscillator, Length Optimization, Trojan Detection, Trigger and Payload Trojan, Trojan Implementation, Hardware Trojan (HT), FPGA Simulation.**

I. INTRODUCTION

As per the current scenario involvement and importance of VLSI (Very Large Scale Integration) designs is increasing day by day. VLSI is becoming latest trend in electronics, in which billion of transistors are placed on a single chip. Accuracy, sensitivity, power consumption, length optimization, propagation delay are such important parameters for Trojan detection of VLSI circuit designs. Trojan is a malicious or undesirable change in the actual design.

According to safety concern of VLSI industry, protection from Trojan Horses is most critical and very desirable task. Trojan is categorized in many types and can be applied during chip designing in foundries, manufacturing, verifying the design, implementing the design. Therefore Trojan Detection process is taken as a fault identification of schematic design for the safety & security of VLSI Industries. An intruder may alter the actual design which can destroy, damage or leak critical & secure information. Many authors proposed various Trojan detection approaches but those techniques are very expensive, consumes more time. In this paper Multisim 13.0, Ultiboard 13.0, ISE 10.1 Simulator, Adept interfacing tool with Basys 2 FPGA Kit is used for Trojan Detection. This will save many resources, energy, determine system accuracy with sensitivity and more over check the efficiency through virtual implementation and detection. Therefore this work is very helpful before final manufacturing at foundries and to make system Trojan free. IC (Integrated Circuit) Logic and within die and side channel variation determines non destructive Trojan detection. To understand the concept of Trojan detection, ring oscillator is taken as basic experimental design because RO is very common circuit which is applicable in electronic industries. In the way we are detecting Trojan in 9 stages ring oscillator shown in Figure 1, designer can test any VLSI schematic design by following the same procedure. VLSI technology is very popular in the current scenario for providing miniaturization with best results. It provides large scale integration of components in the era of fast growing technology. Trojan detection is a must case according to protection purpose, industrial security concern, testing equipments before fabrication & correct functional requirements. For VLSI circuits Trojan identification is very important concern to make VLSI industry reliable, efficient, less expensive, less time consuming, more accurate and secure.

Manuscript received June19, 2015.
***Deepa**, VLSI Design, UPTU Lucknow, India*
***Richa Srivastava**, VLSI Design, Asst. Professor, AKGEC, India*

II. RING OSCILLATOR & LENGTH OPTIMIZATION

Ring oscillator is a circuit design used to produce oscillations for various applications. For Trojan detection 9 stages ring oscillator is taken as a fundamental design. Ring oscillator (RO) consist odd number of inverters connected back to back in a loop, two voltage supplies are connected at enable 1 pin of NAND gate and other one is on enable 2 signal of AND gate. To produce high oscillations in ring oscillator, firstly enhance the input voltage causes increase in frequency then more will be consumption of current. Secondly reduce the stages of RO to speed up the functionality increases frequency of oscillations.

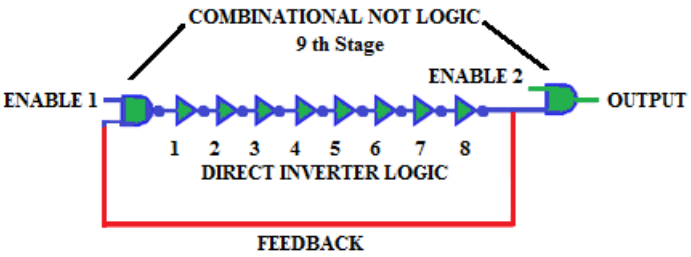

Figure 1: Trojan Free 9 Stages Ring Oscillator

Length optimization means modification in the length of RO by increasing or decreasing number of stages, used to achieve the important results about what happens when intruder or attacker reduces and increases number of stages or add some unwanted components while keeping the same functionality.

For this kind of observation we have observed 9 stages RO with 5 stages RO (reduced stages ring oscillator) and 11 stages RO (Increased stages of ring oscillator). Length

ISSN: 2278 – 909X

optimization of RO can be obtained through increasing & decreasing number of logical components in the actual schematic design. Detection approaches are described under the heading of Trojan detection with proper side channel analysis.

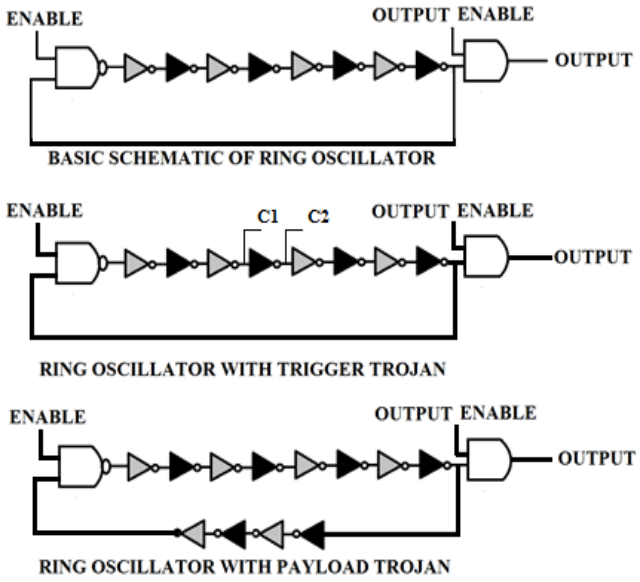

Figure 2: Nine stages Ring Oscillator with Trigger and Payload Trojan

III. TROJAN DETECTION

Trojan detection is accomplished using statistical comparative analysis of different parameters involved in various techniques. Side channel analysis of non destructive kind of Trojan is studied using Logic testing, LRAM & process variations. Deployed 9 stages ring oscillator in Digilent's Basys 2 FPGA board to perform functional simulation & testing.

1. LOGIC TESTING

Logic testing described Trojan implementation and detection. Figure 2 describes classification of Trojan is of two kinds: Trigger Trojan and Payload Trojans in RO. Trigger Trojan is implemented to perform all the unwanted activations of the signals in the circuit design & observed changes met with the experimental design. We calculated power consumption, rise/fall Time increases as compare to Trojan free schematic design parameters. Trigger Trojan activated by triggering the circuit through adding unwanted capacitive load in the actual circuit design. Payload Trojan works to destroy the circuit functionality through inserting extra unwanted logics. Trojans are used to harm, leak secure data or insecurity may causes damage in system therefore Trojan detection is necessary to prevent system design.

Figure 3 illustrate types of Trojan and our aim is to work on non destructive kind of Trojan. Trojan detection is done by establishing standards values of testable parameters of Trojan free & then compared with infected RO parameters. Figure 4 shows 9 stages ring oscillator schematic design with & without Trojan using NI Multisim. Our goal is to focus on the changes caused by Trojans insertion in the circuit and it can be detected using comparative statistical analysis to reduce undesirable variations.

This Trojan detection is simple and very useful which prevent from damage or loss of information and utilizes all resources efficiently. Length optimization of RO is implemented on nine, five and eleven stages. We are considering ring oscillator circuit as experimental design because this circuit is made up of series connection of inverter logic gates and maintain simplicity with ease in design, commonly found as a part of many hardware designs & give fastest switching while detecting Trojans. Further we summarized impact of length optimization & Trojan implementation on ring oscillator. Then some techniques are introduced for Trojan detection by observing functional check, layout level comparison and side channel analysis.

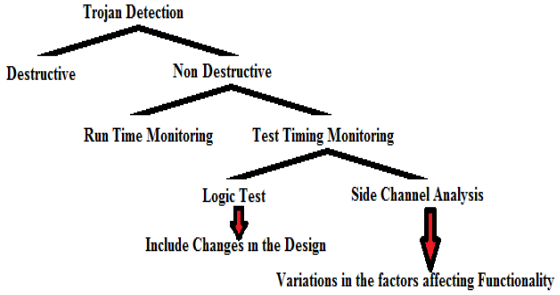

Figure 3: Trojan Distribution

Figure 5 illustrates five stages RO where reduction in the number of stages causes increases in oscillation frequency which is more than nine stages ring oscillator's frequency. Figure 6 represents the eleven stages ring oscillator, if number of stages increases then area complexity increases so the delay increases but reduces power consumption.

2. LRAM APPROACH & PROCESS VARIATIONS

NI Multisim v 13.0 is the EDA Tool of National Instruments which is used in this research. NI stands for National Instruments and Multisim is a National Instrument's automation and testing Tool. Multisim provide analog synthesis & digital circuit synthesis, simulation, verification, testing and observation. For Trojan detection of 9 stages RO and length optimization first step is to design schematic & set standards of all required parameters to compare then observed impact of Trojan implementation and detection is established through full statistical comparison. Logic testing as length optimization of 9 stages ring oscillator describes how all the essential parameters changes with reduction and enhancement in the number of stages.

Majorly we are estimating system sensitivity, accuracy and area after Trojan implementation in Table 1, where fundamental parameters like power, current, rise/fall time, dB losses and frequency observed for Trojan detection and Length optimization. Process variations as side channel effects observed in Table 2. We also observed some important parameters which help in Trojan detection like SINAD (Signal to Noise and Distortion Ratio), THD (Total Harmonic Distortion), relative db losses to establish schematic design sensitivity and accuracy of the schematic design.

ISSN: 2278 – 909X

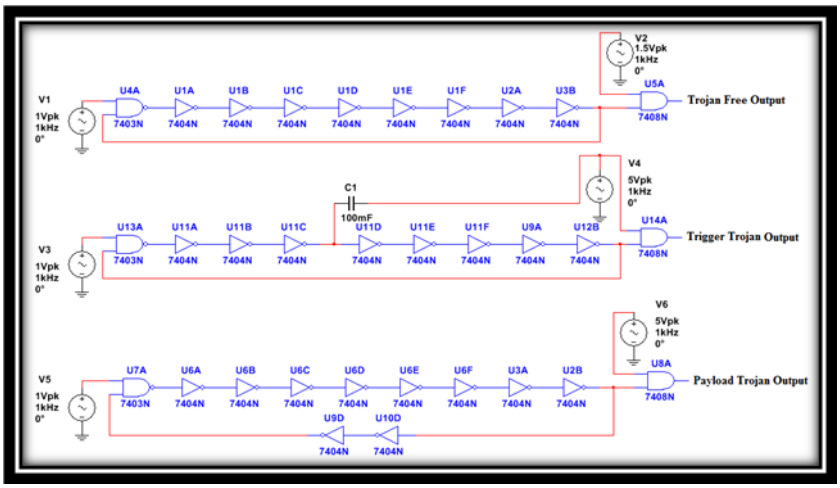

Figure 4: 9 Stage RO with Trojan

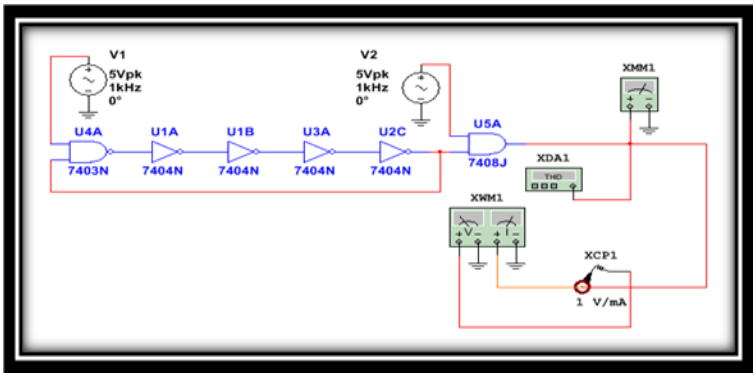

Figure 5: Reduced Stage (5) - Ring Oscillator

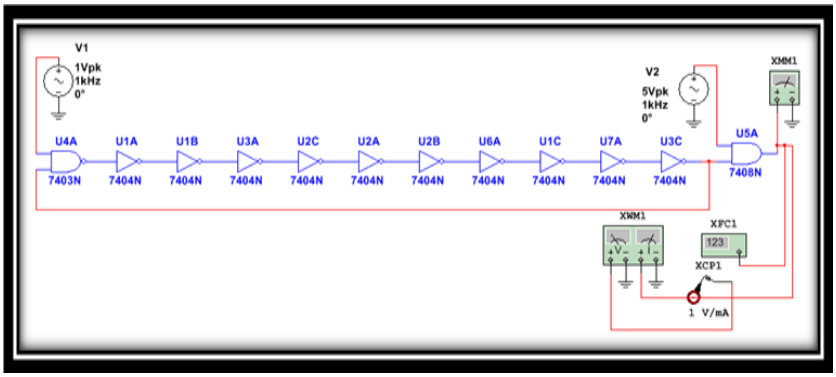

Figure 6: Increased Stage (11) - Ring Oscillator

Table 1: Trojan Detection & Length Optimization

Parameters	Trojan Free (9 Stage RO)	5 Stage RO	11 Stage RO	Trigger Trojan (9 Stage RO)	Payload Trojan (9 Stage RO)
Current Measured (mA)	20.096 mA	18.514 mA	10.509 mA	11.949 mA	21.93 mA
Frequency Measured	2.828 MHz	4.845 MHz	1 kHz	1.056 MHz	2.349 MHz
Rise Time	58.005 ns	17.638 ns	235.914 µA	223.202 ns	95.903 ns
Fall Time	101.844 ns	41.597 ns	242.297 µA	164.475 ns	94.366 ns
Power (W)	4.449 W	1.823 W	313.4 mW	5.849 W	4.240 W
SINAD (db)	2.983	4.799	11.130	1.312	8.750
THD (%)	95.214	5.7	28.901	74.812	33.724
Relative Loss (db)	8.088	3.122	3.079	40.799	9.018

ISSN: 2278 – 909X

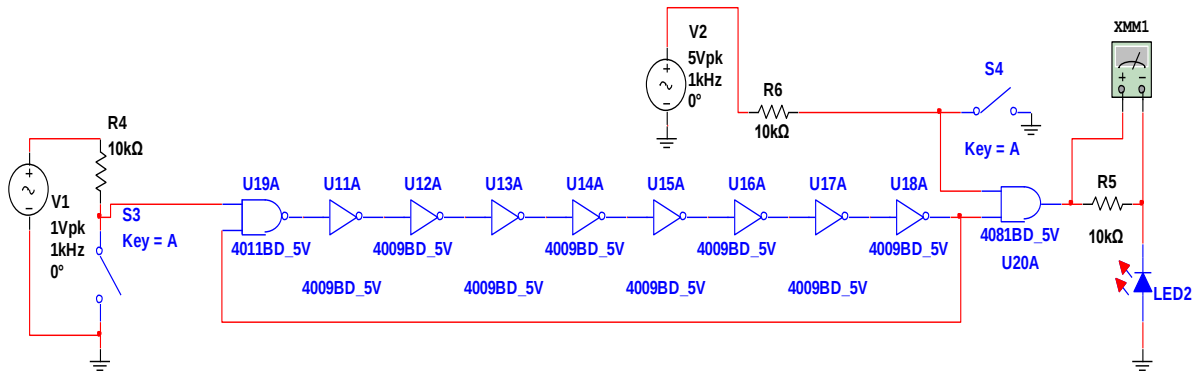

Figure 7: CMOS RO Design

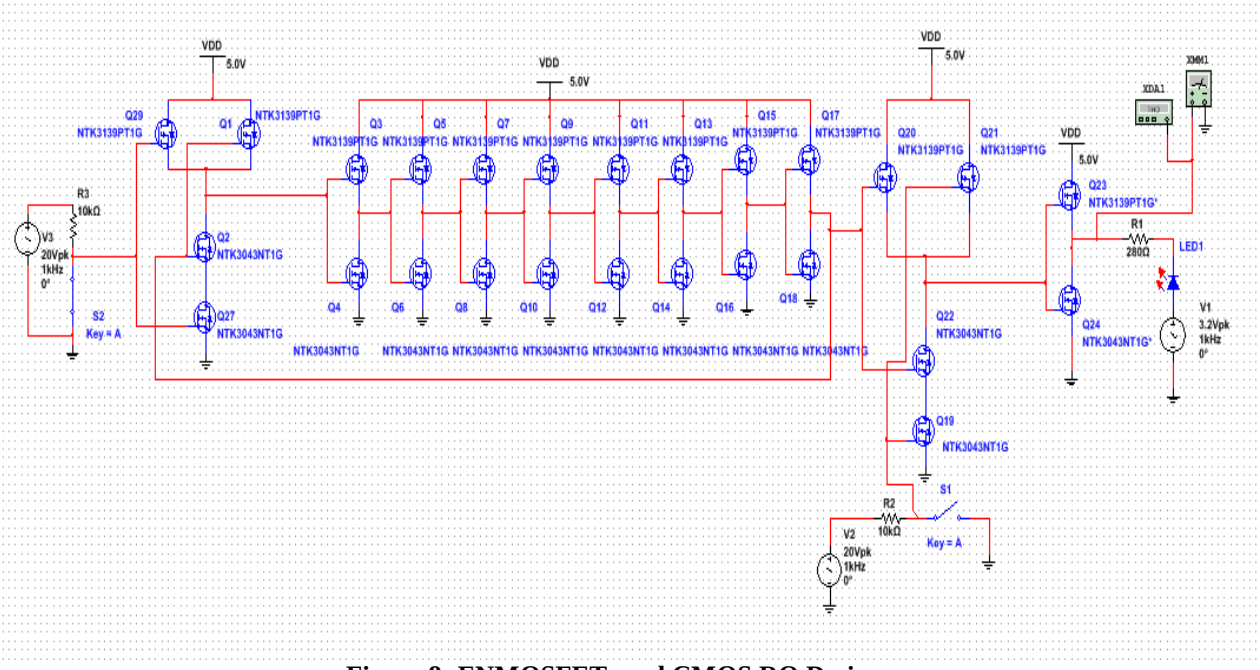

Figure 8: ENMOSFET used CMOS RO Design

Table 2: Process Variation Detection

Parameters	Predesigned CMOS Based RO	Enhancement MOSFET CMOS Based RO
SD Current	0.569 µA	1.288 µA
Frequency	1 kHz	1 kHz
THD	63.426 %	43.659 %
SINAD	5.364 dB	7.944 dB
Db Loss	-21.23 dB	-22.145 dB

Table 3: LRAM Trojan Detection

Statistics	Trojan Free 9 Stage RO	Reduced 9 Stage RO	9 Stage RO With Trigger Trojan	
			C = 10uF	C = 1000mF
Total Number of Pins	70	56	72	72
Pins in a Net	29	27	34	33
Not Connected Pins	41	29	38	39
Test Pins	0	0	0	0
Total Number of Connections	18	16	20	20
Completion	100%	100%	100	100
Total Number of Parts	5	4	6	6
Total Number of Nets	11	11	14	13

ISSN: 2278 – 909X

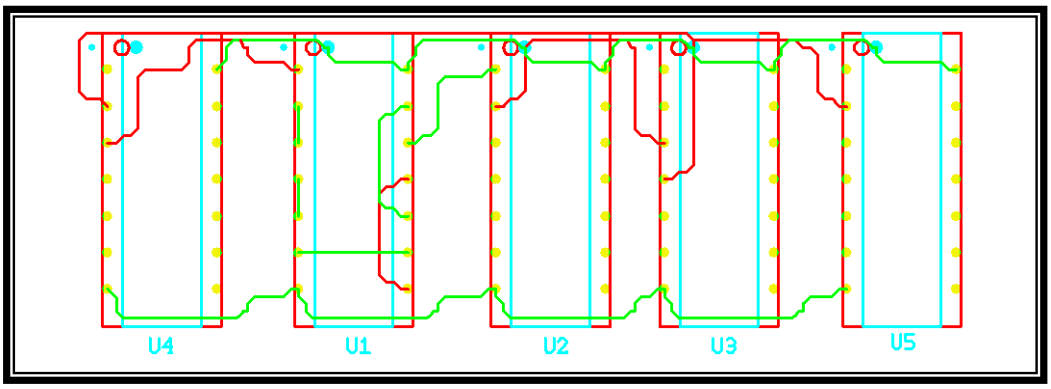

Figure 9: Designed RO PCB

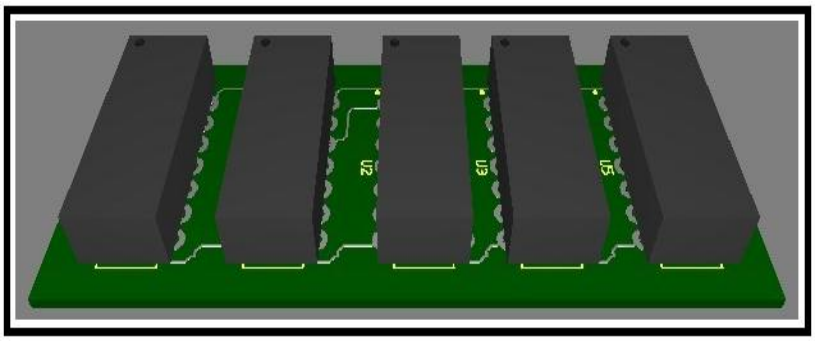

Figure 10: 3 Dimensional PCB View

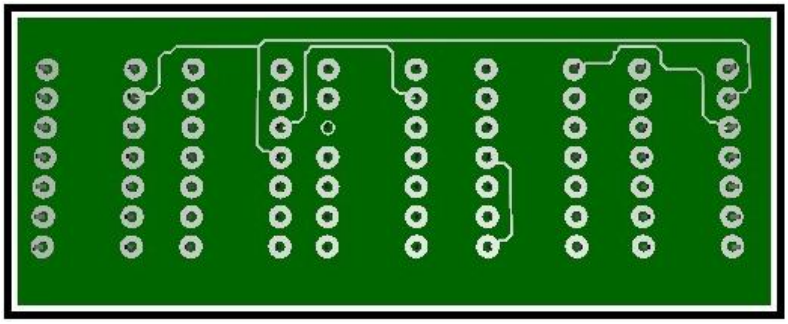

Figure 11: 3 Dimensional Routing

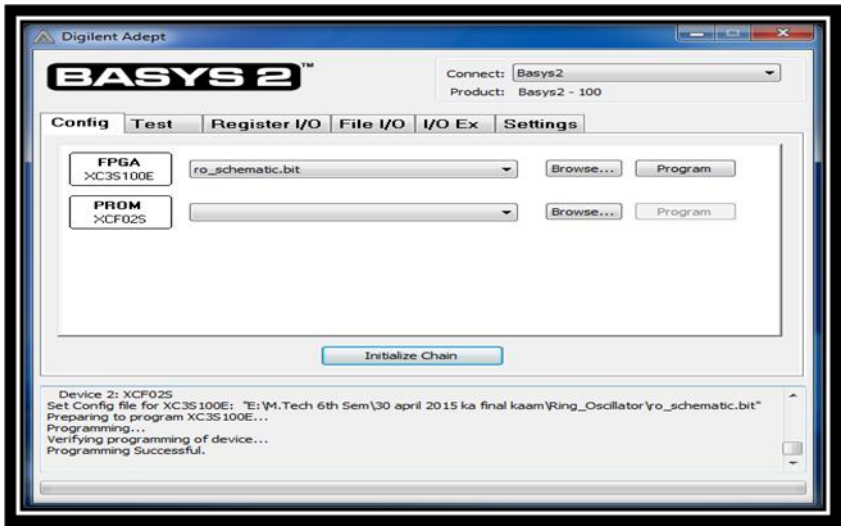

Figure 12: FPGA Configuration using Adept

ISSN: 2278 – 909X

Figure 7 shows change in power supply and connected particular amount of resistor to reduce current across the output which helps in reduction of power consumption. In this RO is designed using predesigned CMOS technique based gates, which causes less leakage and more sensitive schematic design as compare to previously designed TTL based 9 stages RO. Figure 8 shows enhancement MOSET used CMOS designing of 9 stages RO which provides more accurate signal measurement with highest sensitivity with less losses.

An approach is developed named as LRAM (Layout, routing and microwave integrated design) for Trojan detection with deep analysis of layout & routing of the designed PCB. This approach gives detail for statistical comparison to optimize impact of Trojan after PCB design.

Figure 9 shows PCB layout of 9 stages RO, extracted from Multisim schematic file is transferred to NI Ultiboard as a standard design. Figure 10 represents 3D view of designed PCB and Figure 11 gives routing and connectivity illustration. Trojan can be inserted as extra components are inserted then it can be detected easily through deep study of part placement and routing activity.

Furthermore we also can check basic factors permittivity, dielectric constant, trace width, capacitance, frequency etc. across the PCB for comparative analysis with Trojan inserted PCB. Optimized Trigger Trojan by inserting one or more capacitors in the original design and reduced number of stages in 9 stages RO by keeping the functionality intact. PCB Trojan detection is summarized in Table 3.

IV. FPGA BASED SIMULATION

FPGA Deployment of 9 Stages RO is implemented using ISE Simulator 10.1, Adept Software with Digilent Basys 2 FPGA board. Primarily schematic capture is designed through ISE Simulator and then it is transferred to Basys 2 board with the help of Adept software which works as an interfacing tool by successful programming of generated bit file of schematic design shown in Figure 12.

LED is placed in series of output of RO, and it will glow only when Enable 2 remains active high. Simulation is shown below in Figure 13, 14, 15 and 16 as follows:

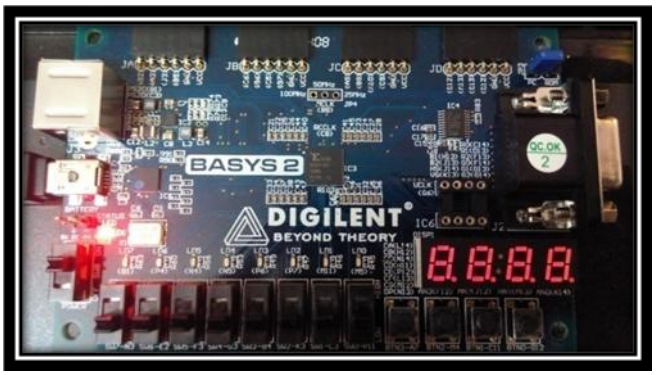

Figure 13: Enable 1 is Low and Enable 2 is also Low

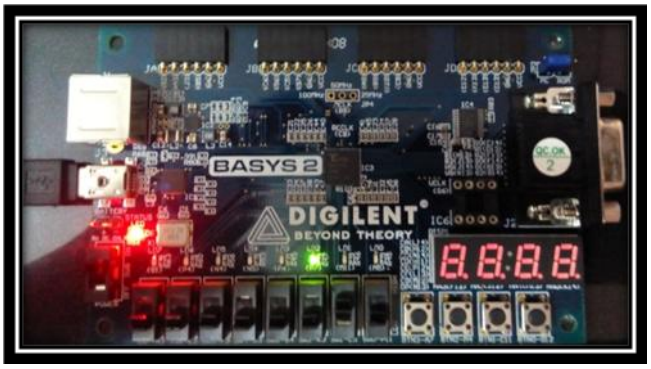

Figure 14: Enable 1 is Low and Enable 2 is High

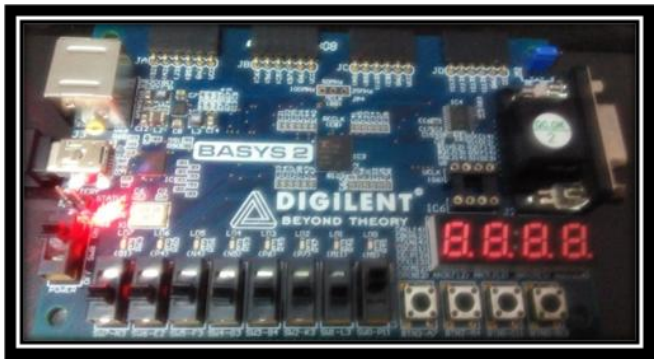

Figure 15: Enable 1 is High and Enable 2 is Low

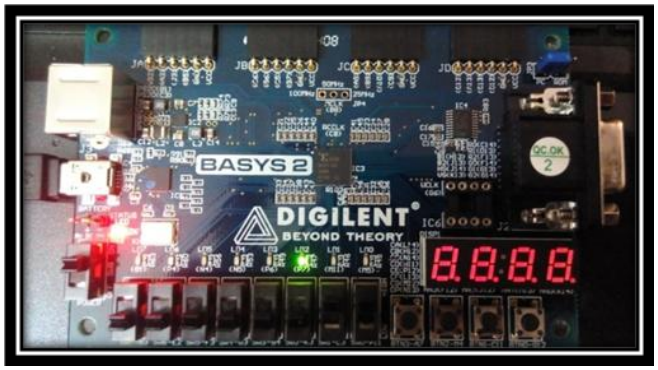

Figure 16: Enable 1 is High and Enable 2 is also High

V. CONCLUSION

This paper proposed Trojan detection implementation & detection of 9 stages RO. Trojan is detected through length optimization, LRAM and process variation approaches. By increasing number of stages of schematic design become more sensitive and less accurate. Increasing input voltage supply and reducing number of stages of ring oscillator reduces noise causes system works faster. We observed Trigger Trojan activates malicious modifications and payload Trojan adds logics to the system design trying to keep circuit functionality same as Trojan free system design. FPGA configuration is established to observe the RO simulation. Future work is concerned with deep analysis of FPGA based Trojan detection and functional verification.

ISSN: 2278 – 909X

VI. ACKNOWLEDGEMENT

I would like to thank Ajay Kumar Garg Engineering College for providing all the required resources for this work and their faculty members for their precious guidance.

VII. REFERENCES

[1]. Charles Lamech, Reza M. Rad, Mohammad Tehranipoor, and Jim Plusquellic, 2011 "An Experimental Analysis of Power and Delay Signal-to-Noise Requirements for Detecting Trojans and Methods for Achieving the Required Detection Sensitivities", vol. 6, No. 3, pp. 1170 - 1179.

[2]. Hassan Salmani, Mohammad Tehranipoor and Jim Plusquellic, 2010 " A layout aware approach for improving localized switching to detect hardware Trojans in integrated circuits" *IEEE International Workshop on Information Forensics and Security*, pp. 1 - 6.

[3]. Jie Li, Charles L. Brown and John Lach, 2008 "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection" *IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 8 - 14.

[4]. Yier Jin, Nathan Kupp, and Yiorgos Makris, 2009 "Experiences in Hardware Trojan Design and Implementation" *IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 50-57.

[5]. Ramesh Karri et.al, 2010, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans" *IEEE Computer Journal*, Vol. 43, Issue - 10, pp. 39 - 46.

[6]. J. Aarestad, D. Acharya, R. M. Rad, and J. Plusquellic, 2010 "Detecting Trojans though leakage current analysis using multiple supply pads," *IEEE Transactions on Information Forensics and Security*, vol. 5, NO. 4, pp. 893 - 904.

[7]. Abhranil Maiti and Patrick Schaumont, 2009 "Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators" *IEEE International conference on Field Programmable Logic and Applications*, pp. 703 - 707.

[8]. Kazuya Katsuki, Manabu Kotani, Kazutoshi Kobayashi and Hidetoshi Onodera, 2006 "Measurement Results of Within-Die Variations on a 90nm LUT Array for Speed and Yield Enhancement of Reconfigurable Devices" *IEEE, Asia and South Pacific Conference on Design Automation.*

[9]. S. Narasimhan, Dongdong Du, R.S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy and Swarup Bhunia, 2010 "Multiple-Parameter Side-Channel Analysis: A Non-Invasive Hardware Trojan Detection Approach" *IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 13 – 18.

[10]. Devendra Rai and John Lach and Charles L. Brown, 2009 "Performance of Delay Based Trojan Detection Techniques under Parameter Variations" *IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 58 – 65.

[11]. Reza M. Rad, Xiaoxiao Wang, Mohammad Tehranipoor and Jim Plusquellic, 2008 "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans" *IEEE/ACM International Conference on Computer-Aided Design*, pp. 632 – 639.

[12]. Pete Sedcole and Peter Y. K. Cheung, 2006 "Within-die Delay Variability in 90nm FPGA's and Beyond" IEEE International Conference on Field Programmable Technology, pp. 97 – 104.

[13]. Brendan Hargreaves, Henrik Hult and Sherief Reda, 2008 "Within-die Process Variations: How Accurately Can They Be Statistically Modeled" *IEEE Design Automation Conference*, pp. 524 – 530.

[14]. M. Rozkovek, Jiri Jenicek and O. Novak, 2012 "An evaluation of the application dependent FPGA test Method" *IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, pp. 22 - 25.

[15]. Raheem A. Beyah et.al, 2002 "Invisible Trojan: An Architecture, Implementation and Detection Method" *IEEE 45th Midwest Symposium on Circuits and Systems*, pp. Vol. 3, pp. 500 - 504.

Authors Profile

Deepa (M.Tech Scholar) pursuing M.Tech in VLSI Design Engineering from AKGEC Ghaziabad, received B.Tech Degree in Electronics and Communication Engineering from SBIT Sonipat, 2011. Also completed 3 year's Diploma in Digital Electronics and Microprocessor System Design from Kasturba Polytechnic for Women Delhi, 2008.

Richa Srivastava is pursuing Ph.D. (Thesis submitted) from N.S.I.T, Delhi. She received M.Tech Degree in VLSI Design from Banasthali Vidyapith, Jaipur, and B.Tech. in E&C Engineering with total rich work experience of 4.5 yrs as an Academician. Currently working as an Asst. Professor (Dept. of ECE) in AKGEC, Ghaziabad, India

ISSN: 2278 – 909X