International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Trojan Detection Using EDA Tools

Deepa[1], Monika Gupta[2]

[1]Ajay Kumar Garg Engineering College, 27th Km Milestone, Delhi - Hapur Bypass Road, P.O. Adhyatmik Nagar Ghaziabad, India

[2]Ajay Kumar Garg Engineering College, 27th Km Milestone, Delhi - Hapur Bypass Road, P.O. Adhyatmik Nagar Ghaziabad, India

Abstract: ***Trojan Detection is the process to identify the malicious modification in the circuit design, data pattern, confidential information, logic expressions etc. Trojan Taxonomy is so large but with respect to Hardware Design Trojan could be of any kind like normal noise or Intra Noise or With-in-Die Variations. So we are mainly emphasizing on Activation & Action based Trojans named as Trigger and Payload Trojans. Our aim to protect, maintain the security and privacy of the circuit design using NI Multisim v 13.0.1 EDA (Electronic Design Automation) Tool. In this paper we are validating the nine stages Ring Oscillator as a experimental circuit design as well as statistical observations are used to detect Trojan. I am very thankful to Asst. Professor Monika Gupta as a Guide for her kind support and proper Guidance.***

Keywords: Ring Oscillator, EDA Tools, Statistical Analysis for Trojan Detection, Trigger Trojan, Payload Trojan, Hardware Trojan.

1. Introduction

The goal of my research paper is to detect Trojans using EDA Tools. Trojan detection is the supreme validation method to secure hardware design from unwanted, treacherous, highly risky, dangerous modifications introduced by intruders during fabrication, manufacturing, transmission/reception of data and when designer using some IP (Intellectual Property) modules for proper usage of the system.

Trojans are used to harm, leak private particulars, damage or to increase insecurity so detection is a must case to make things free from Trojan. Insertion of Trojan in hardware design is a difficult task therefore we must go through all the technicalities of circuit design used for Trojan detection. Initial step is to understand the types of Trojan to identify malware modification and its impact on hardware design parameters respectively.

Classification of Trojan is of two kinds: Trigger and Payload. Trigger Trojan is designed to accomplish all the unwanted activations of the signals in the circuit design causes increment in the Power consumption, Rise Time, Fall Time which helps to determine variations and Delays in the hardware design. Trigger Trojan can be implemented using undesired modifications by adding capacitive load in the actual circuit design. Payload Trojan can be inserted as number of gates added in series or parallel of the real circuit design and they used to change logical expressions to obtain malicious modifications. Noise, with-in-die and chip to chip variations may introduced by planned terrifying Trojan insertion.

Trojan detection can take place using EDA Tools, provides virtual environment to deep analyze, simulate & research on relevant subject to achieve final destination. It creates prototype to understand all the functionalities, facts

and realities without wasting much time together with designer should follow all essential precautionary steps before product is going to finalize in foundries for manufacturing. EDA tools bring such a good platform for experimentation to save resources like money, time, energy etc. We are using various stages of Ring Oscillator which are nine, five and eleven stages. But the question arises why we only refer Ring Oscillator circuit because this is the circuit which is made up of series connection of inverter logic gates because of simplicity, ease to design, commonly found as a part of many hardware designs & give fastest switching while detecting Trojan. Further we will summarize what happened when we increased or decreased stages of Ring Oscillator and Statistical Analysis establishes detection procedure.

Ring Oscillator is a group of odd number of inverters connected back to back in a loop between two voltage levels to differentiate input signal with output enable signal. To generate high oscillations in a Ring Oscillator firstly we have to increase the input voltage causes increase in Frequency also increase in Current consumption. Secondly reduce the stages of Ring Oscillator to speed up the oscillations due to this Frequency increases with certain Current consumption. Our future work will base on FPGA Analysis of Ring Oscillator using Digilent Basys 2 100K Spartan 3E FPGA board in contrast with NI Multisim v 13.0.1 and ISE 10.1 Simulator.

2. Experimental Design

To design & detect Trojan in nine stages Ring Oscillator NI Multisim 13.0.1 is used. NI Multisim is an Electronic Workbench to employ Berkley Spice based simulation and schematic design software by National Instruments. For circuit designs connect one NAND Gate, One AND Gate and eight Not Gates (Inverter Logic) back to back in series and make a feedback loop for continuity to develop oscillations

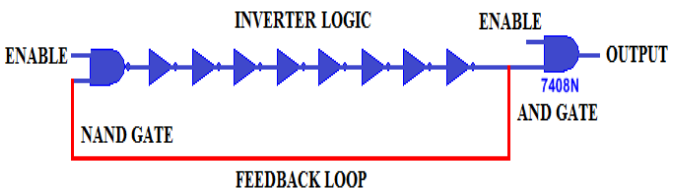

Figure 1: (a) Nine Stage Ring Oscillator without Trojan

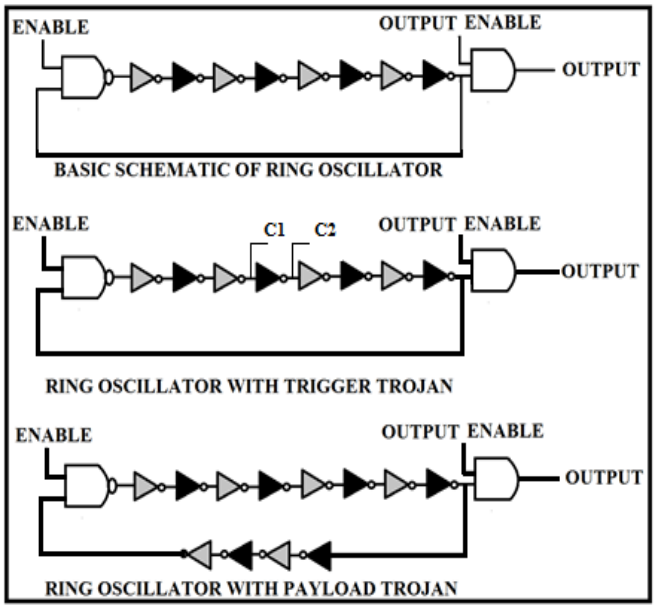

Figure 1: (b) Nine Stage Ring Oscillator with Trojan

In place of this we can also detect any circuit topology. Fig. 1 has two parts Fig. 1 (a) showing Trojan Free nine stages Ring Oscillator and Fig. 1 (b) representing Trigger & Payload Trojan insertion in Trojan free Circuit design.

3. Simulated Designs & Results

Using NI Multisim v 13.0.1 we designed nine stages Ring Oscillator and observed all required parameters to reach at the conclusion that if we reduce number of inverter stages we obtained good quality attributes in terms of high speed and if we increase the stages see its adverse effects. We also study what happened when we introduced Trigger Trojan and Payload Trojan in the Trojan free Ring Oscillator circuit design. We detected Trojan by comparing its parameters i.e. Current, Frequency, Power and Delay in Trojan Free, Trigger Trojan and Payload Trojan with statistics values. For following figures we have taken first Voltage Source (Enable) as 1 V peak & another one is on 5 V peak (Output Enable).

In "Fig. 2" a Trojan Free nine stage Ring Oscillator is observed and we found magnitude of Current is 20.096 mA and Frequency is 2.828 MHz.

In "Fig. 3" Rise Time is 58 ns and Fall Time is 101.844 ns and Power Consumption is 4.449 Watt.

In "Fig. 4" Five stages Ring Oscillator is designed and due to the reduction in stages Frequency increased beyond nine stages Ring Oscillator's Frequency is 4.845 MHz, certain Current is 18.514 mA.

In "Fig. 5" Rise Time &, Fall Times are 17.538 ns, 41.597 ns and Power is 1.823 Watt.

In "Fig. 6" Eleven stages Ring Oscillator include more stages due to this oscillations started decreasing that's why decrease in Frequency up to 1 kHz and Current will obtained as compare to normal nine stages Ring Oscillator which is 10.504 mA.

Oscillation Period, $T = n*2tp$ (1)

Frequency, $f = 1/T = 1/ (2*n*tp)$ (2)

Propagation Delay, $tp = 1/ (2*n*f)$ (3)

Angular Velocity, $w = 2*\pi*f$ (4)

Quality Factor, $Q = 1/ (w*R*C)$ (5)

$V (t) = V \text{ peak}*\text{Sin} (wt)$ (6)

$V \text{ peak} = \sqrt{2} V \text{ rms}$ (7)

In "Fig. 7" Trigger Trojans are detected just by comparing values of simple nine stage Ring Oscillator which is considered as Trojan Free Circuit Design. After insertion of Trigger Trojan in the form of capacitive load we observed the difference occurred in Power and Delay parameters. Finally we conclude that if more will be the capacitive load more Power will be consumed and Delay increases. Here the Power consumption increased to 5.849 Watt from 4.449 Watt, Rise Time and Fall Time are 229.739 µs, 231.746 µs respectively.

In "Fig. 8" Payload Trojans appeared as customized logical functions according to intruder therefore numbers of logical gates are inserted. Increased Fan-out causes more Delay but not much impact on Power consumption which will be approximately near by the Trojan free nine stage Ring Oscillator's Power consumption which is coming out as 4.24 Watt, Rise Time is 95.903 ns and Fall Time is 94.366 ns.

To study Noise measurement see "Table I", we have taken 12 data sets of Current and Frequency while input source supply does not exceeding 1.5 Volt. One enable terminal is connected with 1 V peak and another one is on 1.5 V peak. Standard Deviation is referred as Noise measurement and their average is known as measure of noise for whole process. Measurement noise as Standard Deviation for Current is 5.28 mA and for Frequency is 0.24 MHz. Data sets and their respective Currents, Frequencies, Mean, Standard Deviation and 3 Sigma value which is given in "Table I". 3 Sigma value is a statistical analysis helps to detect Trojan occurred when the Current and Frequency goes above and below from upper and lower 3 Sigma limit. Fig. 9 and Fig. 10 showing graphical representation of all relevant statistical values obtained from above mentioned experiment with 12 data sets.

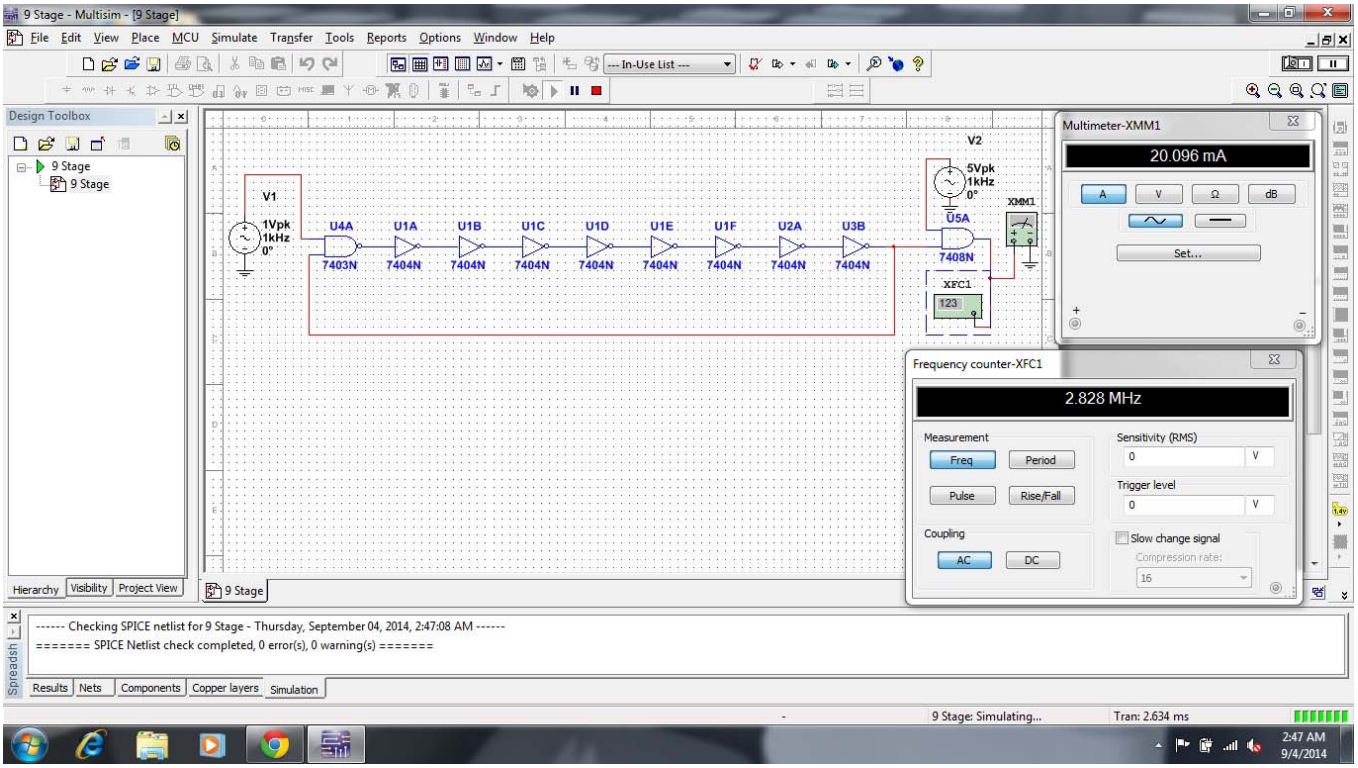

Figure 2: Nine Stage Ring Oscillator: Current and Frequency

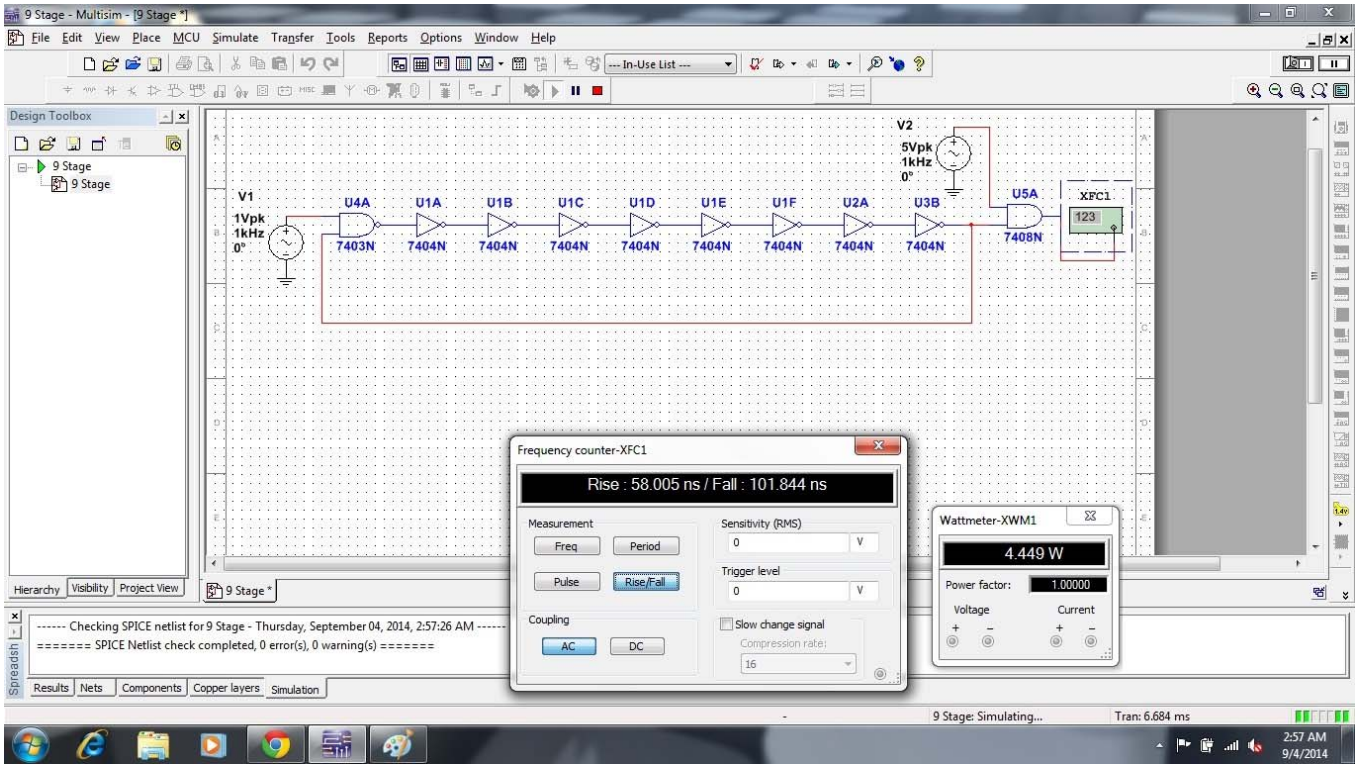

Figure 3: Nine Stage Ring Oscillator: Rise Time, Fall Time and Power

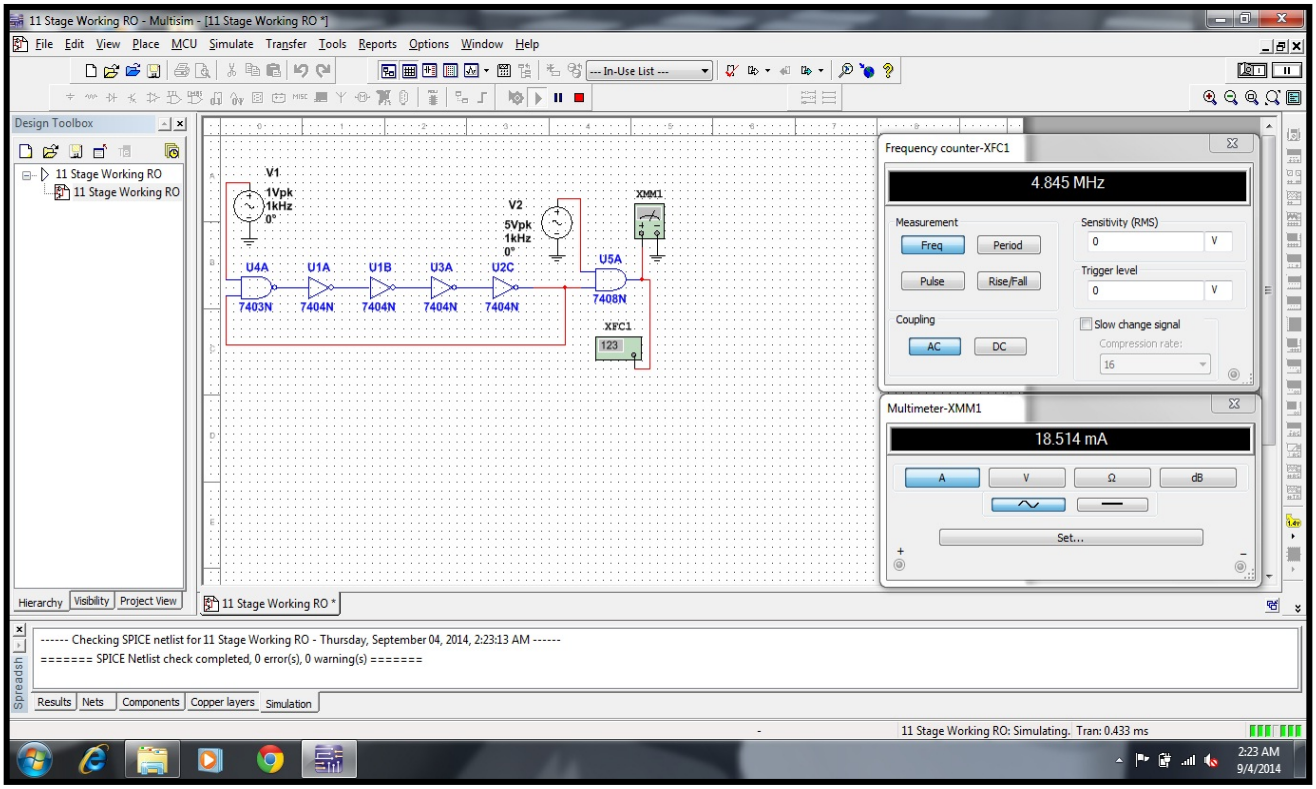

Figure 4: Five Stage Ring Oscillator: Current and Frequency

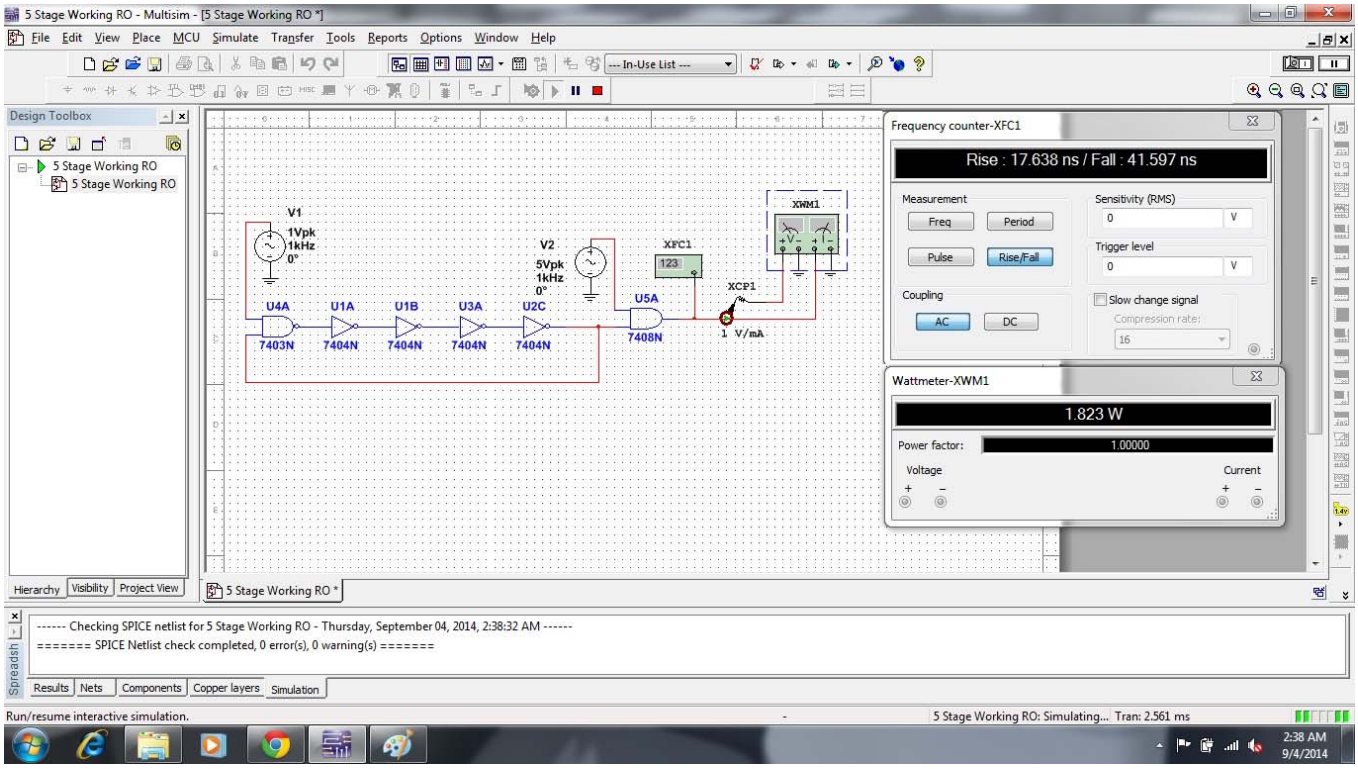

Figure 5: Five Stage Ring Oscillator: Rise Time, Fall Time & Power

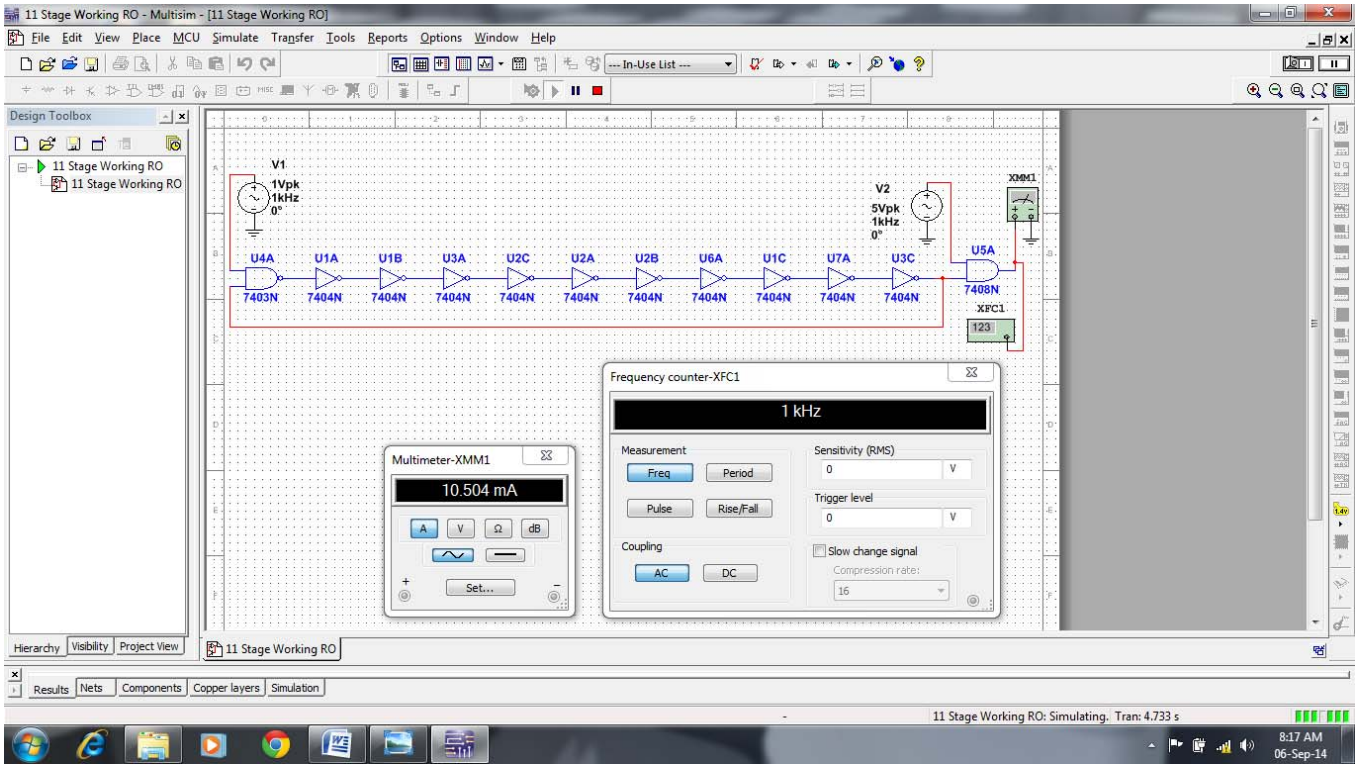

Figure 6: Eleven Stage Ring Oscillator: Current and Frequency

Table 1: Statistical Analysis Using 12 Data Sets

S. No.	*Current*	*Frequency*
Data Set 1	24.738 mA	2.772 MHz
Data Set 2	31.671 mA	2.826 MHz
Data Set 3	23.61 mA	2.758 MHz
Data Set 4	31.881 mA	2.73 MHz
Data Set 5	22.241 mA	2.825 MHz
Data Set 6	32.019 mA	2.797 MHz
Data Set 7	21.344 mA	2.827 MHz
Data Set 8	32.103 mA	2.832 MHz
Data Set 9	20.777 mA	2.27 MHz
Data Set 10	32.445 mA	2.31 MHz
Data Set 11	20.381 mA	2.22 MHz
Data Set 12	32.174 mA	2.85 MHz
Mean	27.11533333 mA	2.668083333MHz
Standard Deviation	5.282183628 mA	0.245243277 MHz
3 Sigma Value	16.08 mA	0.735 MHz

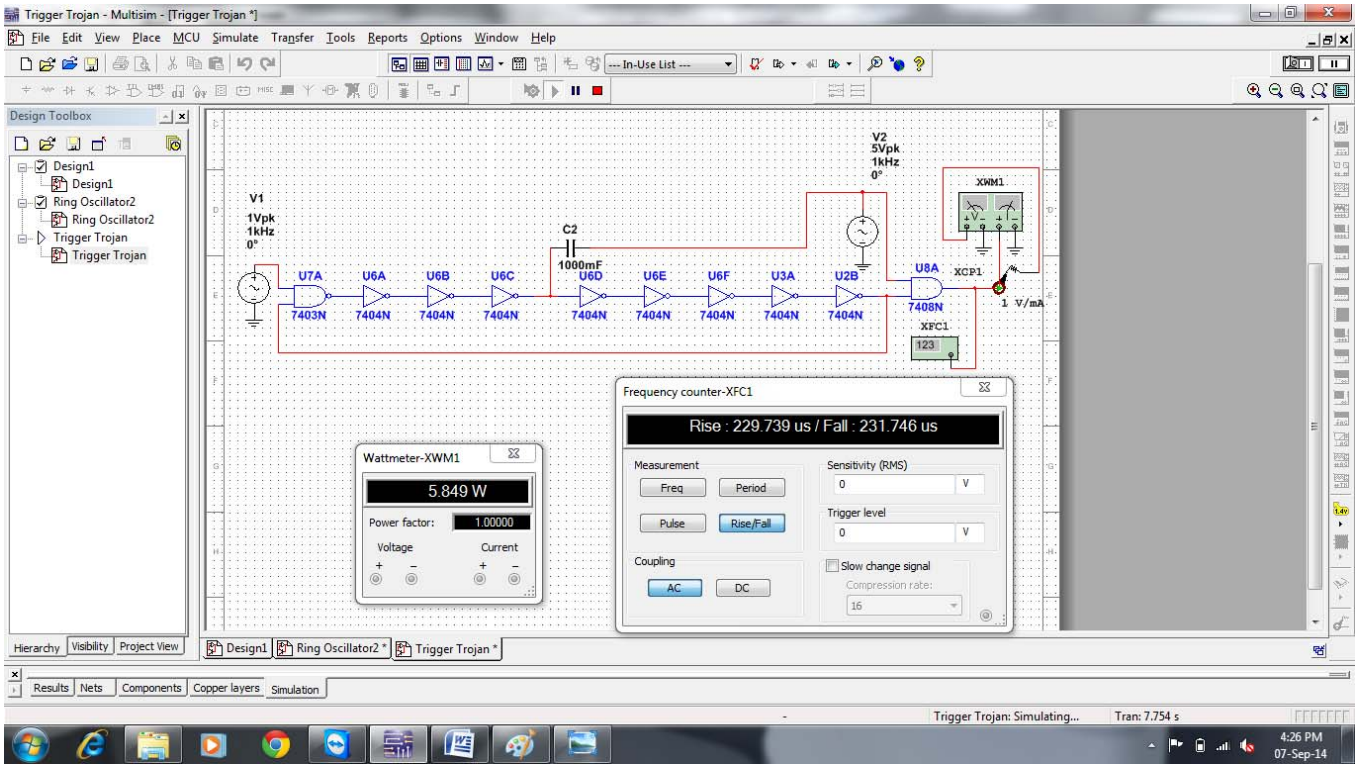

Figure 7: Trigger Trojan: Rise Time, Fall Time & Power

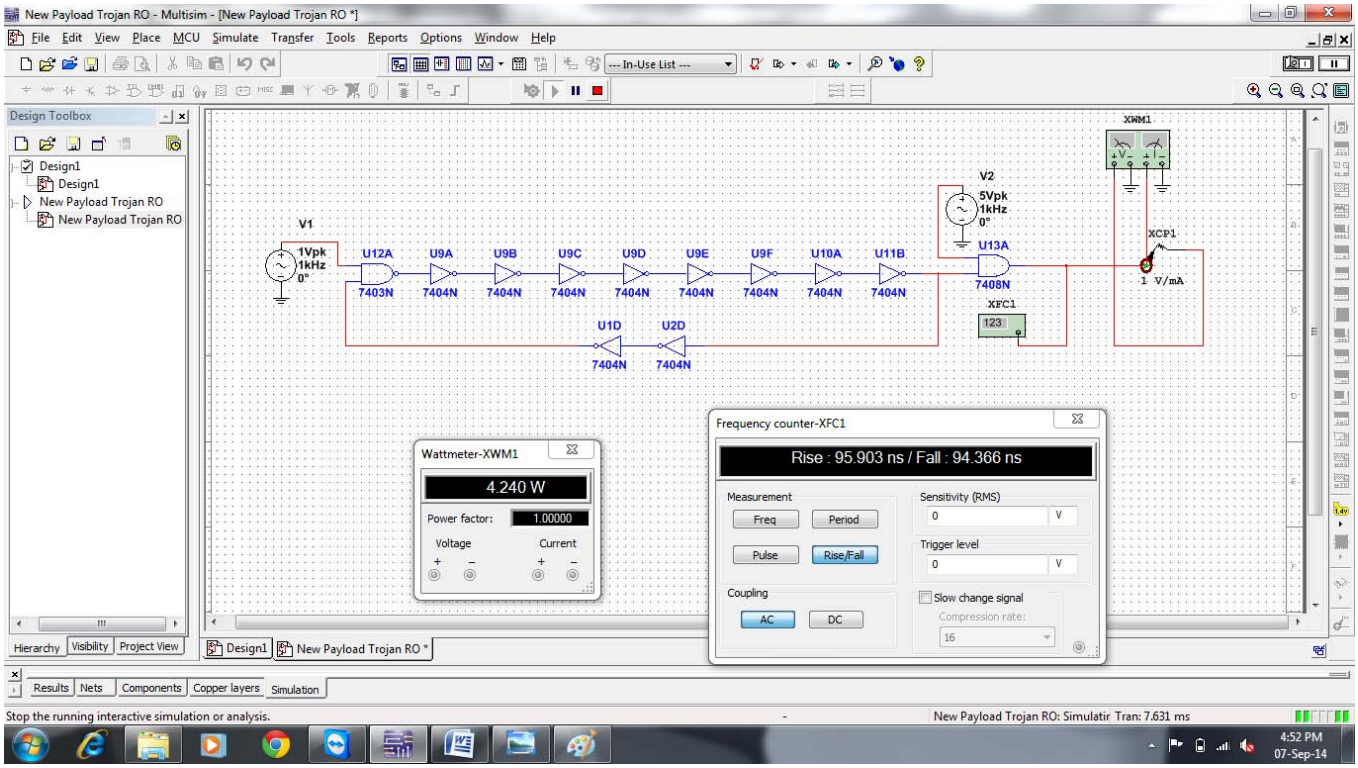

Figure 8: Payload Trojan: Rise Time, Fall Time & Power

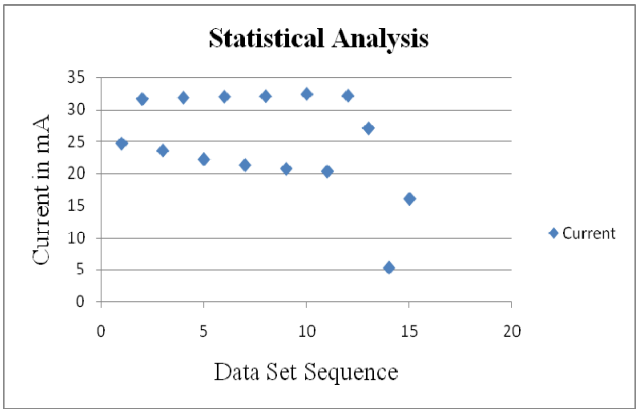

Figure 9: Noise Measurement for Current

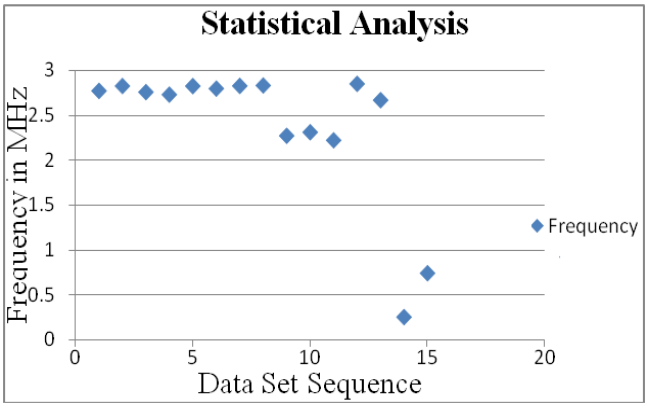

Fig.10 Noise Measurement for Frequency

4. Conclusion

We took Trigger and Payload Trojans and observed their impacts successfully. Trojan Detection is established using data comparison and 3 sigma upper and lower limits. 3 Sigma limit determines the 99.73 % accuracy to detect Trojan. Our further aspect is to design the multiple copies of Ring Oscillator Circuit on Digilent Basys 2 Spartan 3E FPGA board for deep study of with-in-die variations by calculating average Standard Deviation of multiple Ring Oscillators.

Acknowledgment

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 guidance.

References

[1] A. Baumgrten, M. Clausman, J. Zambreno, "A Case Study in Hardware Trojan design and implementation", Springer.
[2] Jim Aarested, Dhruva Acharya, Reza Red and Jim Plusquellic, "Detecting Trojans Trough leakage current analysis using multiple supply pad IDDQs", IEEE transaction on information forensics, VOL. 5, No.4, 4 December 2010.
[3] Yier Jin, Nathan Kupp and Yiorgos Makris, "Experiences in Hardware Trojan design and implementation", IEEE, 2009.
[4] B. Hargreaves, H. Hult, and S. Reda, "Within-die process variations: How accurately can they be statistically modeled" in Proc. Asia South Pacific Des. Autom. Conf., 2008.
[5] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in Proc. Int. Conf. Field Programmable Logic and Appl., 2009.
[6] L. Jie and J. Lach, "At-speed Delay characterization for IC authentication and Trojan horse detection," in Proc. Workshop on Hardware-Oriented Security and Trust, 2008.
[7] P. Sedcole and P. Y. K. Cheung, "Within-die Delay variability in 90 nm FPGAs and beyond," in Proc. Int. Conf. Field Programmable Technology, 2006.
[8] B. Hargreaves, H. Hult, and S. Reda, "Within-die process variations: How accurately can they be statistically modeled" in Proc. Asia South Pacific Des. Autom. Conf., 2008.

Author Profile

Deepa (M.Tech Scholar) pursuing M.Tech in VLSI Design Engineering (Batch: 2012 - 2014) from AKGEC Ghaziabad, received B.Tech Degree in Electronics and Communication Engineering from SBIT Sonepat, 2011. Also completed 3 year's Diploma in Digital Electronics and Microprocessor System Design from Kasturba Polytechnic for Women Delhi 2008.

Monika Gupta (Guide) received M.Tech Degree in VLSI Design (Gold Medalist) from MNIT Jaipur, PGDBM in Finance from Symbiosis Pune and B.E honors in E&C Engineering with total rich work experience of 5 yrs as an Academician. Currently working as an Asst. Professor (Dept. of ECE) in AKGEC, Ghaziabad, India