[AIVESC-18]
DOI:10.5281/zenodo.1230368

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

FPGA IMPLEMENTATION OF PATH TIMING METHOD FOR HARDWARE TROJAN DETECTION

O.Vignesh[*1], H.Mangalam[2], T.Sugunabai[3]

[*1] Teaching Fellow, Department of Electronics Engineering, MIT Campus, Anna University
[2] Professor, Department of ECE, Sri Ramakrishna Institute of Technology
[3] PG Scholar, Department of Electronics Engineering, MIT Campus, Anna University

ABSTRACT

Digital Hardware Architecture is widely used in critical applications such as industrial, automotive, medical and military systems. Since FPGA, DSP, GPP are more economical to production of outsource device to off-shore facilities. Malicious modification of hardware during design or fabrication has emerged as a major security concern. Hardware Trojan (HT) are becoming more of a threat to integrated circuits, which is altered the functional behavior and untrusted foundries. This paper aims to analyze the threat posed by hardware Trojan and the methods of deterring them. Hardware Trojan detection method introduces the concept of Side Channel analysis which detects the Trojan by analyzing data path and frequency of Trojan circuit with the Trojan free circuit.

Keywords: Digital Hardware Architecture, FPGA, GPP, Hardware Trojan, Side Channel Analysis.

I. INTRODUCTION

FPGA (Field programmable gate arrays) are integrated circuits, consists of an array of logic blocks and interconnect structure between logic blocks which are programmed and reprogrammed several times post manufacturing to implement logic function. The design implementation of FPGAs does not suffer the increasing NRE (non-recurring engineering) costs of ASIC production. The growing use of FPGAs has been used for cryptographic algorithm which is constructed out of security devices. The security refers to protecting against Intellectual Property (IP) copying, due to the substance financial investment in IP development.

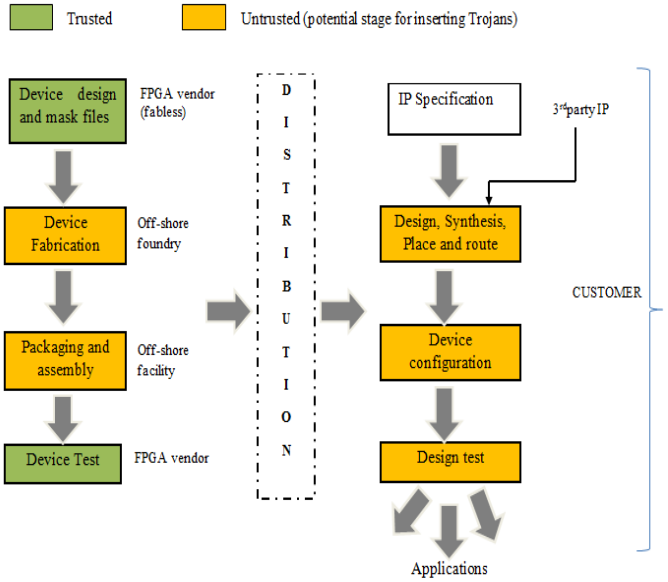

Fig 1 simplified diagram of FPGA design flow for malicious alterations

Malicious alterations to the FPGA design are possible at several stages of design flow [2], are shown in Fig1 the new demand in IC market and globalization of foundries; there raises a question of security. These questions about security result in evolving the new term called hardware cryptography, where the designs can either be in system level, Intellectual Property (IP) level, RTL level, gate level or layout level designs securing from Hardware Trojans. Defense Advanced Research Projects Agency (DARPA) [14] has explained in detailed the TRUST in Integrated Circuits program for validation, including the third party IP. In addition, hardware Trojans are diverse, requiring different levels of resource usage, power consumption, and response time.

Hardware Trojan is a severe threat to the modern integrated circuits, which is posed by the IP business model and untrusted foundries. From third party IP vendor, the most of the modern SoCs several block are licensed where the chances of Trojan insertion is high and Trojan can also be inserted in foundries which are all globalized generally untrusted. The usage of third party IPs is unavoidable to meet the time to market, power, and performance and area requirements. There is high probability of insertion of malicious circuitry or hardware Trojan in that IPs which may affect the functionality or reliability or hack confidential data without the knowledge of the integrator/end user. The insertion of Trojan is also very possible in foundries also because of its globalization [7].

The Hardware Trojan can't be easily detected at fabrication stage but it can be detected by delay and power analysis due to its side channel analysis [4] [8] [15][16]. Logic Testing of FPGA by ATPG (Automatic Test Pattern Generation) is used to detecting the faults. BIST method is one of the best methods to detect the fault and to replace the faulty part with the fault free part in the design [3].

In this paper Section-II explained the concept of Hardware Trojan and their Taxonomy of Trojans. In Section-III the new design method of Trojan circuit is proposed and the detection method is also discussed on section-IV. In Section-V the simulation results is discussed of Trojan circuit and Trojan free circuit. In section-VI, finally it concluded.

II. HARDWARE TROJAN

Hardware Trojan is malicious modification in integrated circuits at different stages of fabrication process [2]. The Trojan can be inserted by third party IP or foundry. The main purpose of Trojan insertion is stealing data/information or change the functionality of the chip or affecting the reliability.

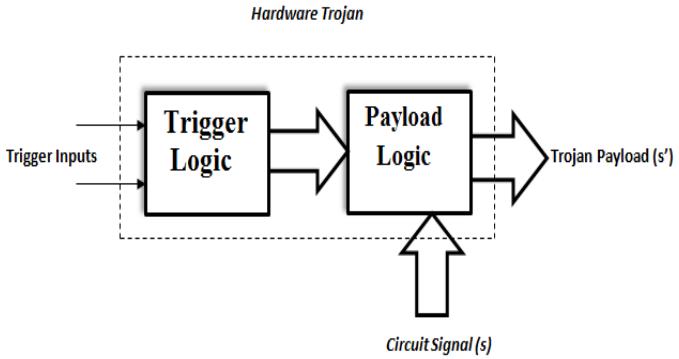

Fig 2.1 Structure of Hardware Trojan

There are two parts in the Trojan they are 1) Trigger and 2) Payload are shown in Fig 2.1. The trigger part monitors a control signal and an undefined instruction interrupt signal. When these two signals are both in low voltage levels, the trigger part will trigger the Trojan and the payload part of the Trojan is activated. The trigger can be divided into digital and analog. The digital Trojan is classified into combinational and sequential. The payload part can also be either analog or digital. The digital Trojan of payload can invert the logic values at internal nodes and analog Trojan may affect the parameters such as power and noise margins

The taxonomy of Trojans suggests the three categories based on Physical, activation and action characteristics [2]. The structure of Taxonomy of Hardware Trojan is shown in Fig 2.2.

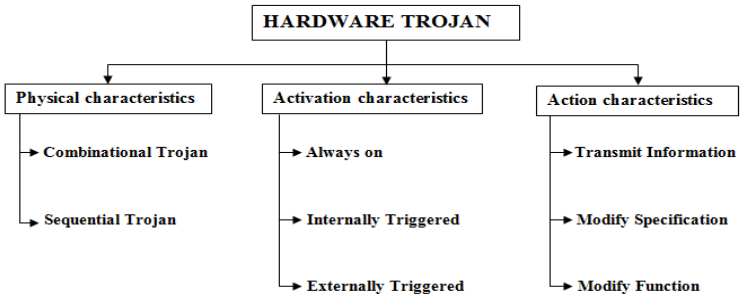

Fig 2.2 Taxonomy of Hardware Trojans

Trojans are also affected in FPGA are classified into two categories. The taxonomy of Trojan attack in FPGA [10] can be in the form of IP blocks, which would load onto a generic FPGA fabric and cause the malicious behavior on the system. Since FPGA IP based Trojans are slightly similar to the ASIC design flow.

Activation characteristics

Hardware Trojan in FPGA can have Activation Characteristics which will based on either be IP dependent or IP independent Trojans.

IP-dependent Trojans:

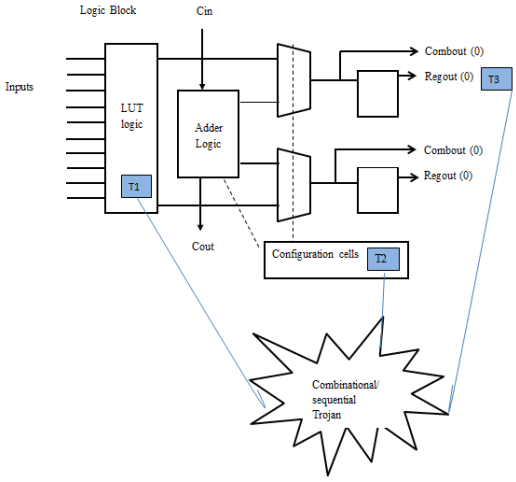

Fig 2.3 Logic Block for trigger points of Trojans

An adversary can insert a malicious circuit which can monitor the logic values of several LUT in the FPGA is shown in Fig 2.3. When triggered the values, such a Trojan can cause malfunction and corrupt other LUT values, or configuration cells in the interconnect network will cause incorrect routing values.

An intelligent attacker can insert the Trojan into an FPGA chip which is independent of the IP loaded into it. Such Trojan can occupy a small portion of FPGA resources such as digital clock manager (DCM) is shown in Fig 3.4. Thus the Trojan are increasing or decreasing the clock frequency by employing the SRAM cells of the DCM unit, it can cause the sequential circuits will be failure.

ISSN 2348 – 8034
Impact Factor- 5.070

Payload characteristics

In payload the FPGA device-based Trojans can be inserted for causing malfunction or leakage information of the IP loaded onto FPGA.

Malfunction:

In FPGA devices the insertion of Hardware Trojan can cause logical malfunction by corrupting LUT, which is also causing physical damage or affecting the functionality of the implemented IP to the FPGA. For e.g. the I/O port is configured as an input, the configuration cells in the I/O block should disable the O/P block to prevent internal conflicts. An adversary can insert the counter-based Trojan in the device that detects the I/O port and being counting. The counter counts the final value; the Trojan may enable the output logic. This may because a flow of high short-circuits current between the external device and FPGA, mostly damaging the system

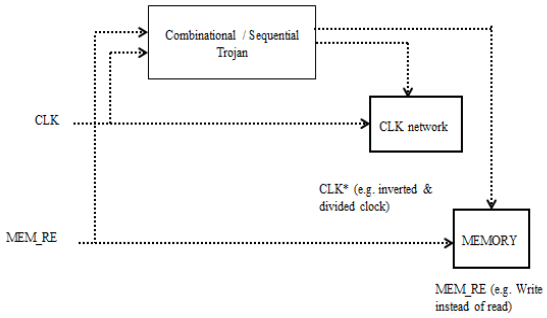

Fig 2.4 Payload that can be altered by an implemented Trojan

IP-Leak Trojans

FPGAs may offer encrypted bit stream in order to protect the IP on to an FPGA device. So, such encryption prevents an unauthorized read back by software. Hardware Trojan may circumvent such protection of leaking the encrypted key or even the entire IP.

III. DESIGN METHODOLOGY

Trojan free circuit

In Trojan free Circuit, the 4-bit Asynchronous counter is used for normal counting. The first one 4-bit Asynchronous counter considered as the total, the clock is connected to the input of other three 4 bit Asynchronous counter through the OR gate. If any one of the input of OR gate is high, it will triggered to the input of 4-bit counter. The clock 1 will trigger means it is counted from 0000 to 1111 i.e. 16 combination is done. Similarly the clock 2 and clock 3 is counted.

The power dissipation will be analyzed and the path delay will be considered. In this Asynchronous counter path delay analysis of t_{co} is analyzed which means clock to output, it has delay of 11.985ns from the clock of clk 2, JK1|q1 to q1 [0]. The t_{su} (setup time) and t_h (hold time) of delay analysis will be calculated. The Fig 3.1 shows the circuit diagram of Trojan free digital hardware architecture.

Similarly the 8-bit Asynchronous counter is used for counting, the four output of counter is counted from 00000000 to 11111111 i.e. 256 combination is required. The power, data path and frequency are analyzed and it is compared to the Trojan circuit. The Fig 3.1 shows the Trojan free circuit, the delay path is mentioned and it is shown below. This Trojan free circuit is compared with the Trojan circuit and finding the path delay of these two circuit And analyze the Trojan functionality

ISSN 2348 – 8034
Impact Factor- 5.070

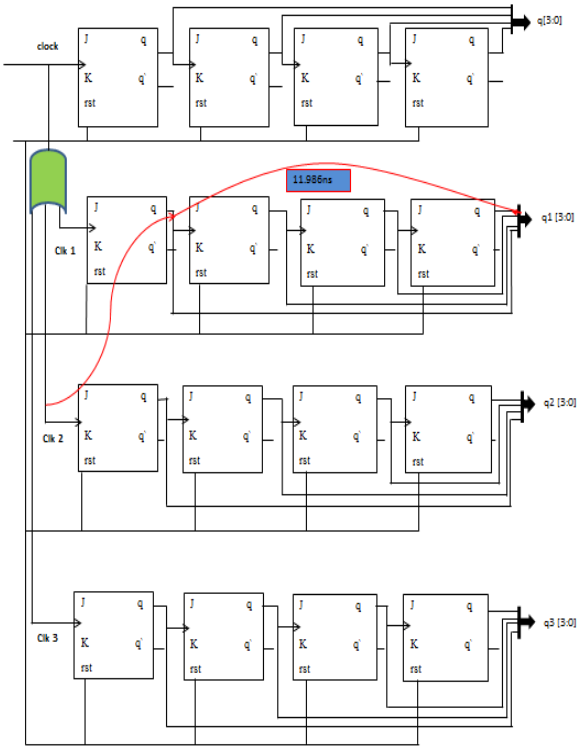

Fig 3.1 Trojan free circuit

Trojan circuit

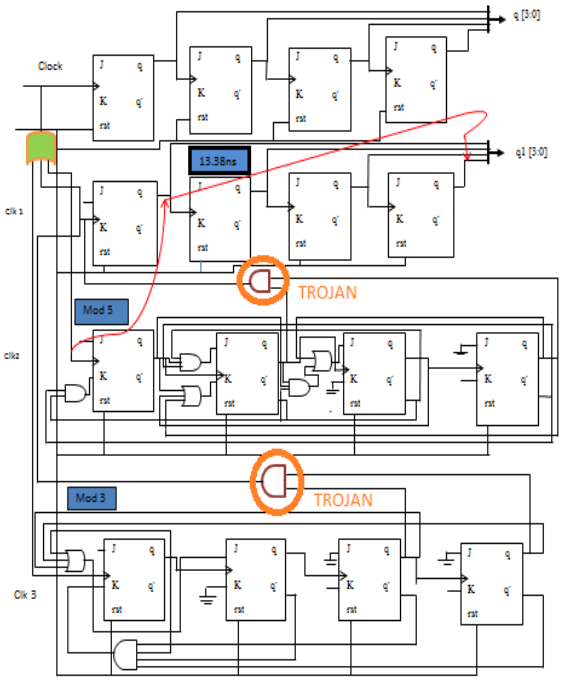

Fig 3.2 4-bit Trojan Circuit

[AIVESC-18] ISSN 2348 – 8034
DOI:10.5281/zenodo.1230368 Impact Factor- 5.070

In Trojan Circuit, the 4-bit Asynchronous counter, mod3 and mod5 are used for counting. The OR gate will triggered when any one of the input is high, so any one of the input will activated. It acts like malicious circuit, whereas the Mod3 counter counts until 3 and then it will count the 4-bit asynchronous counter. Similarly the Mod 5 counter counts until 5 then count the asynchronous counter. In this the circuit has act like as a third party IPs. So the malfunction will be which is referred to Trojan.

Here the Trojan circuit can be detected by using the algorithm of Side channel analysis. The power dissipation of Trojan circuit is high compared to Trojan free circuit and also compares the critical path. The delay path of this circuit has t_{co} which means clock to output; the delay has 13.320ns from the input clock of clk2 through JK5 q1 to the output of q1 [0]. The Fig 3.2 shows the circuit diagram of Trojan free digital hardware architecture.

The path delay analysis of Trojan circuit has longest path compared to the Trojan free circuit. Similarly the 8-bit Asynchronous counter is used for counting; it is counted from 00000000 to 11111111 i.e. 256 combination is done. The output response of 4-bit Asynchronous counters Trojan circuit has 4 output, the first one 4-bit Asynchronous counter is normally counted until 1111. The clk 1 input of 4-bit Asynchronous counter is counted and mod 3 counter output is 0011 when it is counted 3 then it will count the clk 1 input, so the clk 1 4-bit asynchronous counter is incremented using AND gate.

IV. HARDWARE TROJAN DETECTION METHOD

Side channel analysis
Logic based testing may not be effective for Trojan detection of combinational and sequential Trojans due to the large number of possible trigger nodes. Side channel analyses are the basic method of a running IC, including timing, power consumption, delay measurement and electromagnetic radiation proposed in [1] [6] [11]. Side channel analysis is the powerful technique for detect the malicious insertion. In this section, the power consumption can be obtained to detect the Trojan. The analysis of side-Channel Attack AES [1] is described.

Power analysis
A device is used to the amount of power which is influenced by the data being processed; the measurements of power consumptions contain information about a circuit's calculations. Even the effects of single counters, while not directly observable in power measurements from large devices, do appear as weak correlations. Data-dependent power usage can expose these secrets to attack, when a device is processing cryptographic secrets.

First process of power analysis is to collect one or more than one traces from the target device. An element is a sequence of measurements taken across a cryptographic operation or sequence of operations.

Some characteristic of power analysis due to side channel signal analysis are following below

- An adversary can insert the Hardware Trojans in chip can change the power consumption characteristics.
- Through power analysis and isolation can significantly detect the Tight or loose distribution of Trojans.
- Activation of Trojan can be intensely valuable of power analysis.

In our experiment Asynchronous counter Trojan circuit is used and it is inserted in the genuine circuit. It only makes the circuit to consume more power and increase some path delays. Since the signal to trigger the counter has larger capacity loads and slower than usual.

V. RESULTS AND DISCUSSION

Altera Quartus -II is used for designing the circuit without Trojan and to get the power analyses and then comparing it with the circuit with Trojan.

[AIVESC-18]
DOI:10.5281/zenodo.1230368

ISSN 2348 – 8034
Impact Factor- 5.070

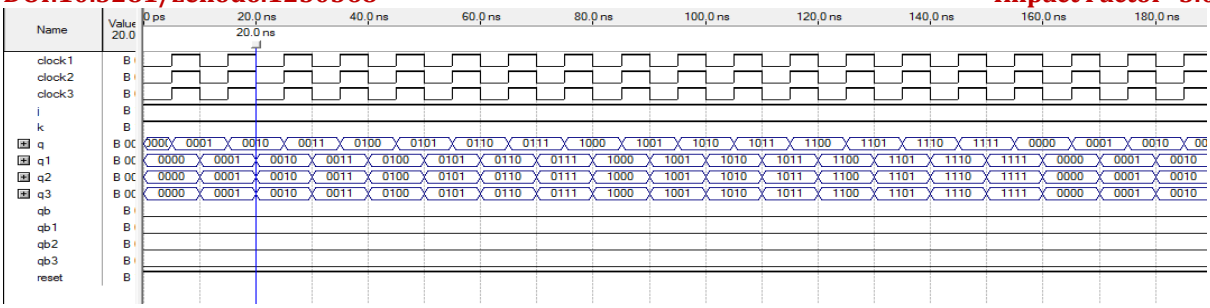

Fig 5.1 simulation result of without trojan

The output response of without trojan is require the input of j,k,clock 1, clock2, clock3 and reset. The j, k, reset is configuired as high and the clock value is normal. Then the output of q, q1, q2, q3 will be normally counted from 0000 to 1111 when the reset is high.

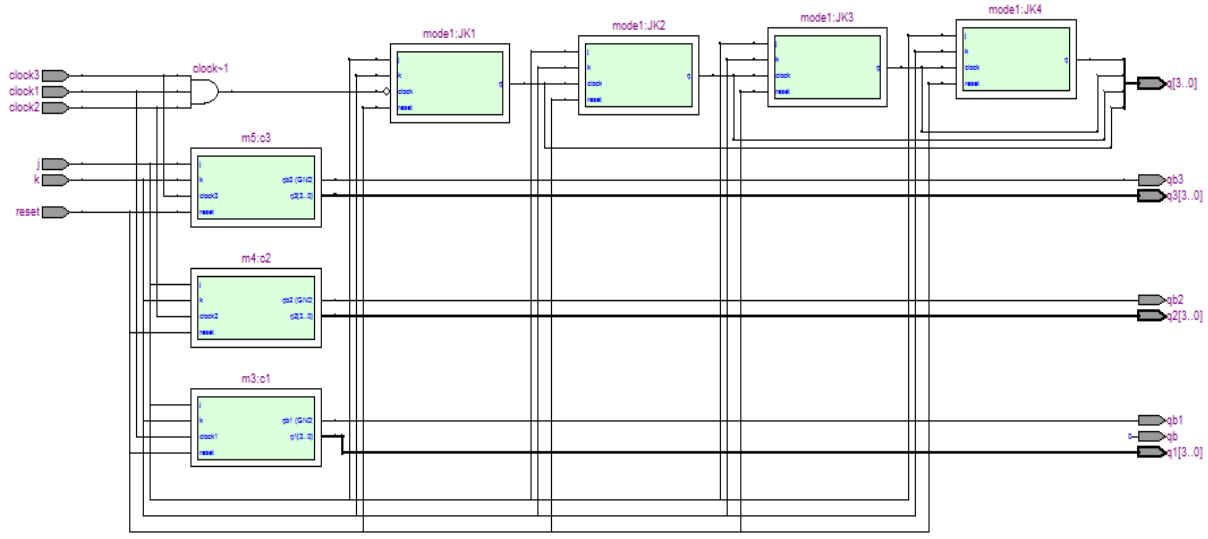

Fig 5.2 RTLviewer of without trojan

Output response of without trojan

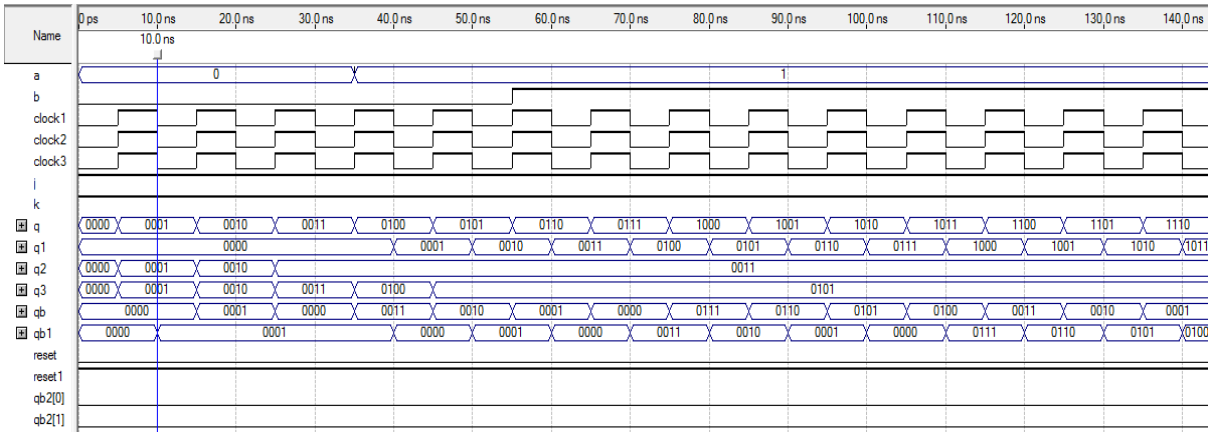

Fig 5.3 simulation results of trojan

[AIVESC-18]
DOI:10.5281/zenodo.1230368
ISSN 2348 – 8034
Impact Factor- 5.070

The output response of with trojan is require the input of j,k,clock 1, clock2, clock3 and reset, reset1. The j, k, reset1 is configuired as high and the clock value is clocked. Then the output of q will be normally counted from 0000 to 1111 when the reset is high and q2 is counted untill 0011 and q3 output is 0101 and q1 is counted normally. The a is configured as output of mod 3 counter and b is configured as mod5 counter. When a and b is the input of OR gate, if any one is low the output of OR gate is clocked to the 4-bit Asynchronous counter and it is normally counted.

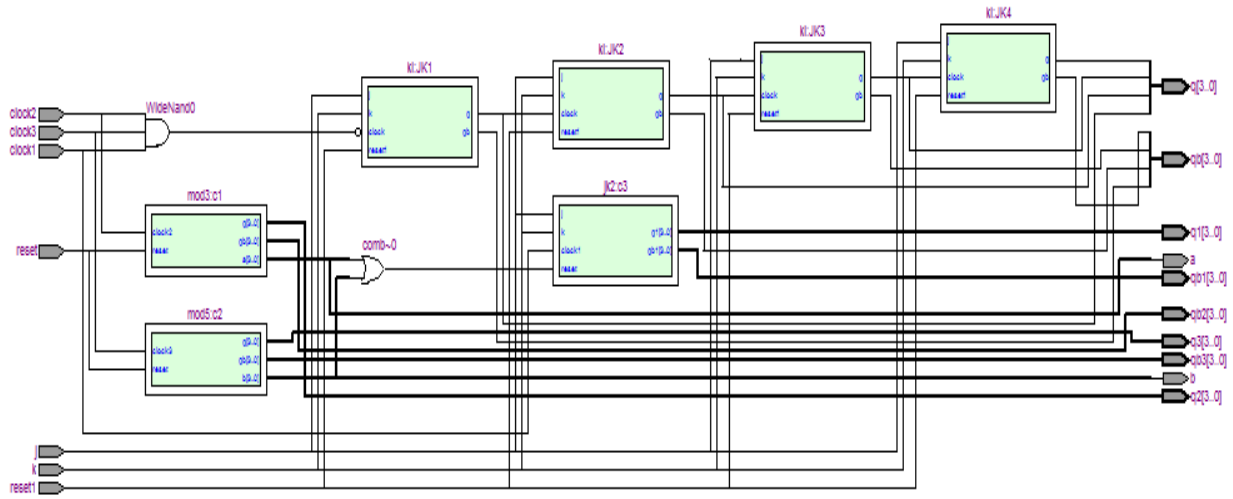

Fig 5.4 RTL viewer of with trojan

Power analysis

Table 1 comparision of Power analysis for Trojan free and Trojan circuit

Family Cyclone-II	Static power	Dynamic power	I/O Thermal power	Total Thermal Power	Total no Of Logic elements
Without Trojan	80.07mW	1.07mW	71.65mW	152.80mW	18
WithTrojan	80.14mW	8.97mW	86.32mW	175.43mW	40

Frequency analysis:

Table 2 comparision of Frequency analysis for Trojan free and Trojan circuit PATH

TYPE	CLOCK 1	CLOCK 2	CLOCK 3
WITH TROJAN	450.05MHZ (PERIOD=2.22ns)	420.17MHZ (PERIOD=2.380ns)	392.00MHZ (PERIOD=2.551ns)
WITHOUT TROJAN	450.05MHZ (PERIOD=2.22ns)	450.05MHZ (PERIOD=2.22ns)	450.05MHZ (PERIOD=2.22ns)

[AIVESC-18]
DOI:10.5281/zenodo.1230368
ISSN 2348 – 8034
Impact Factor- 5.070

Delay (with trojan)

Table 3: Delay analysis of Trojan free circuit

TYPE	*ACTUAL TIME*	*FROM*	*TO*	*FROM CLOCK*	*TO CLOCK*
WORST-CASE t_{su}	4.245ns	Reset1	Mode1:JK qb	-------	Clk1
WORST-CASE t_{co}	13.320ns	Kl:JK5 q1	q1[0]	Clk 2	-------
WORST-CASE t_h	6.783ns	j	Kl:JK4 qb	Clk1	--------

The path delay analysis of trojan free circuit is analyzed the t_{su}, t_{co}, t_h of setup time,clock to output time and the hold time. The t_{su} has the actual time of 4.245ns from the reset1 to JK qb, and the t_{co} is from he clock 2 to q1[0] and also t_h of hold time has 6.783 from j to JK4 qb.

Without trojan

Table 4: Delay analysis of Trojan circuit

TYPE	**ACTUAL TIME**	**FROM**	**TO**	**FROM CLOCK**	**TO CLOCK**
WORST-CASE t_{su}	4.457ns	Reset1	Mode1:JK1 q	-------	Clk1
WORST-CASE t_{co}	11.986ns	m3:c1|mode1:JK1 q1	q1[0]	Clk 2	-------
WORST-CASE t_h	5.422ns	k	m3:c1|mode1: JK8 q	Clk1	--------

VI. CONCLUSION

An adversary can insert the malicious alteration to a design are possible at various stages of design flow. In this method the digital hardware architecture can be considered to insert the malicious changes that can cause the logical and physical malfunction. Here present the Taxonomy of trojan which is based on activation and payload characteristics. The trojan circuit will be detected by using the methodof delay path timing. The Trojan free circuit and Trojan circuit is designed, so the power analysis, and the path delay timing is done between both the designs. And it is found that power consumed by the Trojan free circuit is comparatively less when compared to the Trojan circuit. The power consumed by the Trojan free is 80.07mW. Wheras power consumed by the Trojan circuit consumes 80.14mW respectively

ISSN 2348 – 8034
Impact Factor- 5.070

REFERENCES

1. *Sudeendra K., Sauvagya S. and Abhishek M., "Analysis of side-Channel Attack AES Hardware Trojan Benchmarks against Countermeasures" IEEE Computer Society Annual Symposium on VLSI, july-2017.*
2. *Kento H. and Masao Y. and Nozoma T., "Design and validation for FPGA Trust under Hardware Trojan Attacks" Proc. Transactions on Multi-Scale Computing Systems,"IEEE Trans.,on multiscale computing systems., vol.2, no.3,pp.186-198,june-2016.*
3. *vignesh o, "a built-in self reair analyer for word-oriented memories", global journal of engineering science and researches, published by gjesr. vol. 2, no.5, pp. 150-156 (2015).*
4. *N. Yoshimizu, "Hardware Trojandetection by symmetry breaking in path delays," in Proc. IEEE Int. Symp. Hardware-Oriented Security Trust, 2014, pp. 107–111.*
5. *Swarup Bhunia, Michael S. Hsiao, Mainak Banga, Seetharam Narasimhan., "Hardware Trojan Attacks: Threat Analysis and Countermeasures," IEEE Trans., vol.102,issue:8,pp.1229-1247,Aug.2014.*
6. *S. Narasimhan, D. Du, R. Chakraborty, S. Paul, F. Wol_, C. Papachristou, K. Roy and S. Bhunia. "Hardware Trojan detection by multiple-parameter side-channel analysis," IEEE Transactions on Computers, 62(11), pp. 2183-2195, 2013.*
7. *S. Narasimhan, W. Yueh, X. Wang, S. Mukhopadhyay, and S. Bhunia, ''Improving IC security against Trojan attacks through integration of security monitors,'' IEEE Design Test Comput., vol. 29, no. 5, pp. 37–46, Oct. 2012.*
8. *H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware Trojandetection and reducing Trojanactivation time," IEEE Trans. Very Large Scale Integration Syst., vol. 20, no. 1, pp. 112–125, Jan. 2011.*
9. *R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware Trojandetection," in Proc. 11th Int. Workshop Cryptographic Hardware Embedded Syst., 2009, pp. 396–410.*
10. *Mohammad Tehranipoor, Farinaz Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Design and Test of computers., vol.27, no.1,Jan-Feb.2010.*
11. *Jim A., Dhruva A., Reza R. and Jim P., (2010) "Detecting Trojans through Leakage Current Analysis Using Multiple Supply Pad I_{DDQ}s" in IEEE Transactions on Information Forensics and Security, Vol.5,no.4, December 2010.*
12. *R. chakraborty, s. narasimhan and s. bhunia., " hardware trojan: threats and emerging solutions," IEEE International on High level Design Validation and Test Workshop., noov-2009.*
13. *DARPA, TRUST in Integrated Circuits (TRUST), 2008. [Online]. Available:http://www.darpa.mil/mto/programs/trust/index.html*
14. *X.Wang,M. Tehranipoor, J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in Proc. IEEE Int.Workshop Hardware-Oriented Security Trust, 2008, pp. 15–19.*
15. *D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, ''Trojan detection using IC fingerprinting,'' in Proc. IEEE Symp. Security Privacy, pp. 296–310,2007*
16. *O.Vignesh and H.Mangalam " An Efficient 1-Bit Full Subtractor Circuit using Hybrid CMOS logic" Asian Journal of Information technology, 2016, pp 2948-2953, 2016*