International Journal of Pure and Applied Mathematics
Volume 119 No. 17 2018, 3169-3177
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Hardware Security for Digital Circuits from Hardware Trojans

Joshi Hrushikesh

Department of Electronics and Communication Engineering,

Gokaraju Rangaraju Institute of Engineering and Technology

Hyderabad

D.Jayanthi

Department of Electronics and Communication Engineering,

Gokaraju Rangaraju Institute of Engineering and Technology

Hyderabad

N.Arun Vignesh

Department of Electronics and Communication Engineering,

Gokaraju Rangaraju Institute of Engineering and Technology

Hyderabad

K.Jamal

Department of Electronics and Communication Engineering,

Gokaraju Rangaraju Institute of Engineering and Technology

Hyderabad

Abstract

The Integrated Circuit (IC) security is becoming challenging, because malicious activities done by untrusted parties involved in IC manufacturing process. Adversary or attacker maliciously modifies the internal design of an IC. These attacks are considered as hardware Trojans. Proposed security technique can prevent a wide variety of malicious attacks during synthesis. Proposed security technique protects digital systems from hardware Trojan attacks through a combination of special Concurrent Error Detection (CED) techniques and 64-bit Encryption key generator with selective programmability. This technique examines digital circuit in all possible conditions. So faults and hardware Trojans present in the digital circuit can easily detected. Proposed security technique can be applied to any digital circuit, and can be used for traditional and split-manufacturing methods. It Is applicability to both Application Specific Integrated Circuits (ASIC) and Field Programmable Gate Arrays (FPGA).

Key words: *Hardware Trojan, Concurrent Error Detection (CED) techniques, 64-bit Encryption key generator, ASIC, FPGA.*

1. Introduction

IC fabrication process done in several number of stages. IC security is very much important today, because ICs are used in all applications of our day to day lives. Intellectual Property (IP) cores supplied by third party IP providers. In manufacturing process attacker or adversory has more opportunity to insert hard ware Trojan horse logic into IC. Outsourced design and test services, and use automation tools from outside vendors. Because opponent has more opportunities to insert Trojan horse logic IC used in different applications. Today there are no accurate methods to detect Trojan intrusions, an intrusion means a hostile change of a circuit design, a malicious attack that may occurs after operation [10]. Outsourcing designs and tools become new trend in IC market, because to get more profit. Attacker takes advantage of such restriction to manipulate IC

by maliciously adding extra Trojan logic as hardware Trojan into internal logic of an IC. Consequences are become serious problems about security and accuracy of electronic devices. An attacker can corrupt the fabrication process or modifies a design net list by changing design mask, without affecting the actual functionality of the circuit. Hardware Trojan detection is a challenging problem and normal functional tests cannot properly detect it. Trojan circuits have quite and stealthy nature and are triggered in rare conditions. Hardware Trojans are designed such that they are disable most of their life time and may have very small size relative to the area of an IC [7].IC are also effects from piracy, reverse engineering. Reverse engineering may capture the Intellectual Property (IP) information and illegally pirate the circuit design

[1]. Hardware Trojans leaks internal data using existing don't cares. In RTL simulation 'X' represent don't care means unknown signal value,(0 or 1)

[3].Functional Analysis of Nearly unused Circuit Identification (FANCI) method describes how intermediate wires can affect other wires with in a circuit design. By using the idea called control value a methodology is derived for identifying suspicious wires that have the capability to transfer backdoor trigger signals. By using FANCI tool method to analyse truth tables of intermediate outputs in the digital circuit of interest and generates the control value by randomly sampling rows in the truth table

[5]. Hardware Trojans are also detected by using the spatial thermal and power information, power maps has capacity to reveal the Trojan location perfectly. Malicious logic in IC are detected by using multi model post silicon thermal and power maps [4]. Because of variousness hardware Trojans in IC design, detection of hardware Trojans is difficult.

Gate Level Characterization (GLC) and Segmentation for diagnosis of hardware Trojans. Segmentation process makes large circuit into small sub-circuits, based on selected small sub-circuits diagnosis of hardware Trojan done, by tracking gate level power leakage [6]. Addition of reconfigurable logic barriers isolate the inputs from the outputs then input path to output path passes through a logic barrier [7].Built in Self Authentication (BISA) is to fill all unused spaces with in Standard Cells (SC) called BISA cells. BISA cells are has connections to each other to form a combinational circuit. This combinational circuit is not depends on the original circuit, this combinational circuit can have an arbitrary logic function. If an attacker inserts a Trojan by changing any cell in a BISA circuit then designer can easily detect that Trojan. The BISA structure is designed to detect any malicious changes on BISA by generating different sequences than expected. The BIST was developed to apply random test sequences to examine the accuracy of a digital circuit by examining a sequence obtained from the test output

[2]. Trojans are also detected by using GLC. GLC generates characteristics of each gate of the design by using measurements [9]. Concurrent Error Detection (CED) is an good technique in which by using an error-detecting code to encode the outputs of a circuit and a checker that examine the outputs of the circuit and calculates the error signal when mismatch occurs. Two types of systematic codes are used for concurrent error detection, they are Berger codes and parity-check codes [11]. Security needs the checkers are not visible to attacker .This paper proposes a security architecture, which can be applicable to any digital circuit. Digital circuit is implemented with proposed security architecture gives secured and accurate operation. Proposed security architecture technique detects and prevents the hardware Trojans.

Section 2 presents the architecture of proposed main project work architecture for protecting any arbitrary digital circuit. Section 3 describes the simulation and synthesis results of proposed work. Section 4 compares with existing work approach. Section 5 concludes this paper.

2. Main Project work Architecture

This paper describes a security architecture shown in Fig 1, which can be applied to any digital circuit. Digital circuit is implemented with this security technique gives secured and accurate and desired operation. Integrated Circuit (IC) fabrication process done in several number of stages. Malicious logic added to the internal logic of an IC from outside, it modifies the design. Due to this modification IC lost its functionality and generates undesired output. These malicious modifications are referred as hardware Trojans. To secure Digital Circuits from these attacks this security technique is proposed. This security technique detects and prevents the malicious logic. Let us consider a digital system, it has several number of chips. Each chip in the digital system is implemented with this technique. Consider a 16-bit X 16-bit Multiplier logic circuit, the logic circuit with this security technique is shown in Block diagram.

2.1 Block diagram

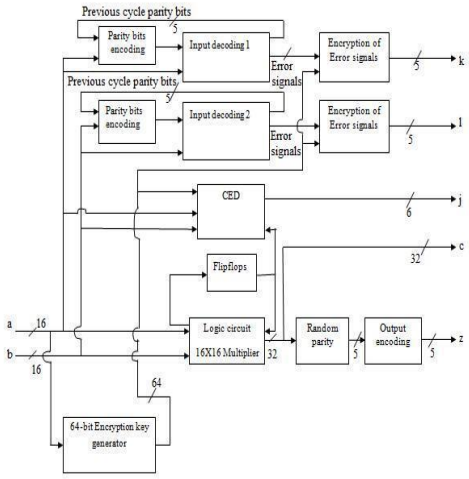

Fig 1: Main Project work Architecture

2.2 Logic circuit: 16-bit X 16-bit Multiplier

Main project is proposed to secure a 16-bit X 16-bit Multiplier logic circuit, it is implemented by using 2-bit X 2-bit Multiplier, 4-bit X 4-bit Multiplier and 8-bit X 8-bit Multiplier.

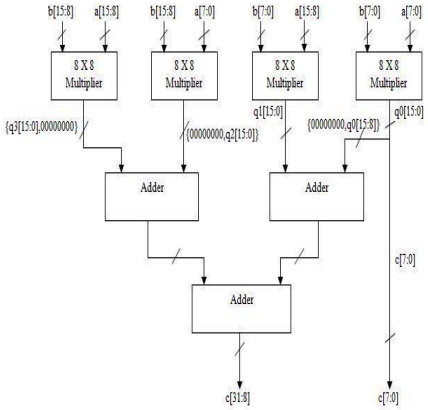

Fig2 : 16-bit X 16-bit Multiplier

2.3 Output bits encoding

Fig 3 shows 32-bit output of 16-bit X 16-bit Multiplier is applied to Random Parity generator, it calculates six parity bits, here even parity is considered. These parity bits are placed in 2^0, 2^1 ,2^2 , 2^3, 2^4 , 2^5 positions of a randomized parity code word. Purpose of parity bit is to detect errors during transmission of binary data, if an error is detected the received parity bit doesn't correspond with transmitted parity bit. A randomized parity code word calculated for each clock cycle. For every clock cycle this parity bits XORed with previous cycle generated parity bits. The result encoded output parity bits stored in D-Flipflops, which is used in next clock cycle.

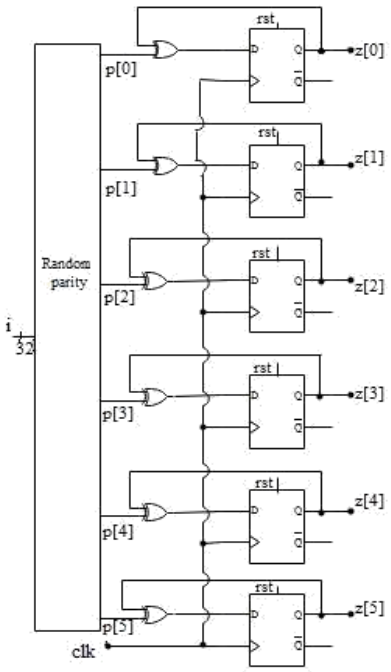

Fig 3: Output bits Encoding

2.4 64-bit Encryption key generator

In proposed method to encode encrypt error signals 64-bit Encryption key generator is used. Let us consider 16-bit input a, each bit of bus a spreaded into four bits, these are XORed with 4-bit orthogonal code to generate 64-bit encryption key for every clock cycle shown in Fig 4. To encrypt error signals, some bits are selected randomly from 64-bit encryption key. 64-bit Encryption key generator can ensures logic circuit security.

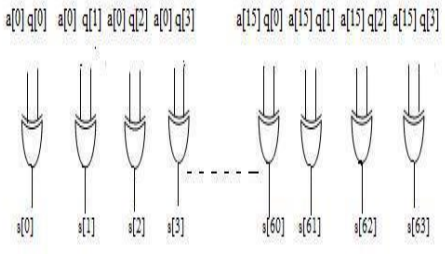

Fig 4: 64-bit Encryption key generator

2.5 Input bits decoding

16-bit inputs a applied to Parity bits encoding block to generates 5-bit encoded input parity bits bus p . In every clock cycle input encoded parity bits XORed with previous cycle parity bits to generates expected randomized parity bits. The input bits are used to generate actual randomized parity bits, XOR operation of these two parity bits generates error signal. These error signals are encrypted by using randomly selected 5-bits of 64-bit Encryption key generator. k is 5-bit encrypted error signal bus. Same process error signals of input b calculated.

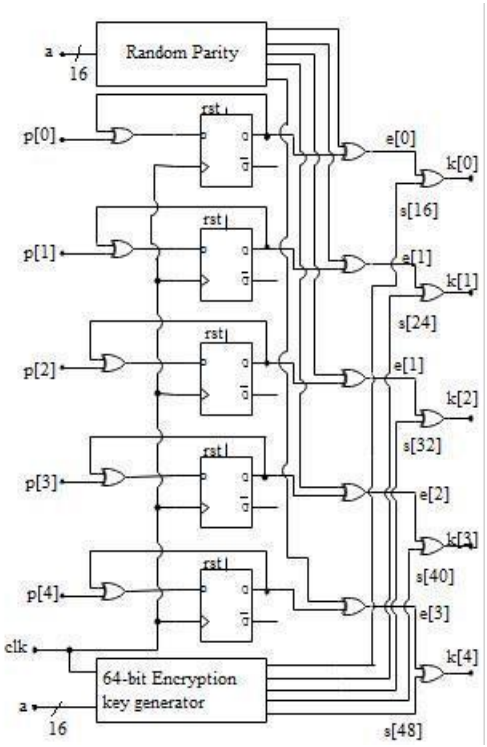

Fig 5: Input bits Decoding

2.6 Concurrent Error Detection (CED)

Output bits encoding and input bits decoding are prevent the malicious attacks at the input and output ports. The logic circuit is secured by using Concurrent Error Detection (CED) shown in Fig 6. Proposed security architecture derived from the concept of CED technique. CED technique has three

modules Output Characteristic Predictor (OCP) and logic circuit and checker. For each input the logic circuit generates 32-bit primary output, for each input OCP predicts parity bits of primary output bits.

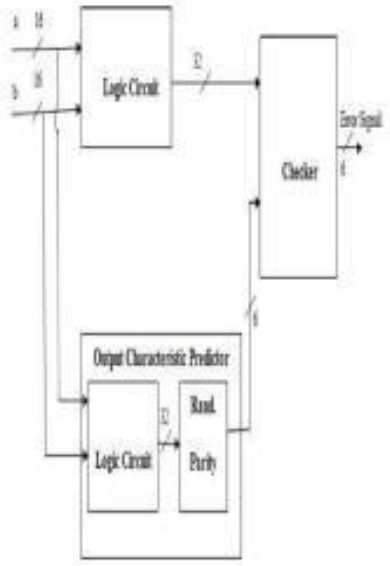

Fig 6: Concurrent Error Detection (CED)

Checker calculates the actual parity bit bus A and compares against with predicted parity bit bus P to generate error signals. An attacker can change error signals by inserting hardware Trojan logic i.e; it shows no error in the circuit even though error present in the logic circuit. A 64-bit encrypted sequence is generated for every clock cycle by using 64-bit Encryption key generator, it is used to prevent an attacker from understanding of the meaning of error signal. Error signals are encrypted with randomly selected 6-bits i.e; s[8],s[16],s[24],s[32],s[40],s[48] of 64-bit Encryption key generator. If no attack is present in checker, checker output encrypted error signal is equal to selected bits of 64-bit Encryption key generator, any other values indicates an error present in the circuit.

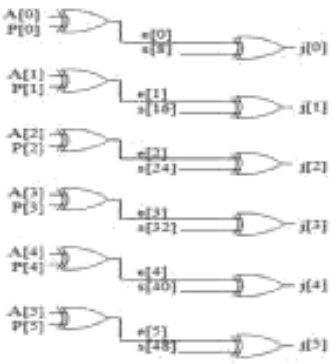

Fig 7: CED Checker

3. Simulation Results

The software used to do compilation and simulation is Xilinx ISE 14.1. A test bench is created to execute the simulation. Proposed security architecture has many security applications in dealing with malicious attacks. In this paper, modules of proposed security architecture have been implemented in Verilog.The output bits encoding and input bits decoding and CED and 64-bit Encryption key generator of security architecture using various modules and their simulation results are shown in below test bench wave forms.

3.1 Simulation result of 64-bit Encryption key generator

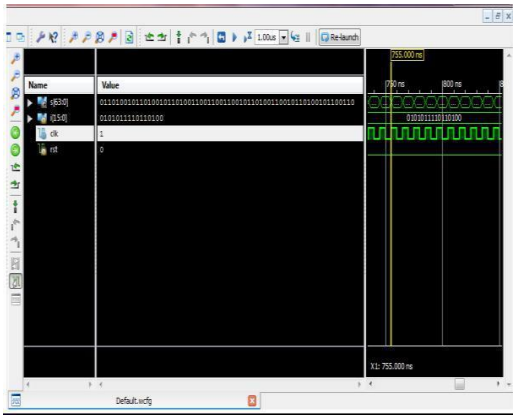

Fig 8: Simulation result of 64-bit Encryption key generator

Each bit of 16-bit input bus a spread into 4-bits, these bits are XOR operation with 4-bit Orthogonal code to generates a 64-bit encryption key s for every clock cycle. .

3.2 Simulation result of Main Project work

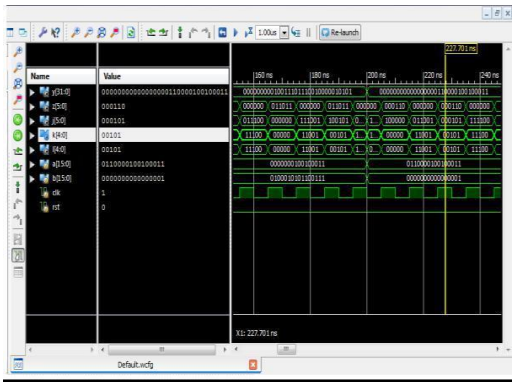

Fig 9: Simulation result of main project work

Input variables are clk, rst and 16-bit bus a and 16-bit bus b, output variables are 32-bit bus y, 6-bit output parity bit bus z, , 6-bit encrypted error signal bus j for CED error signal , 5-bit encrypted error signal bus k for input bus a , 5-bit encrypted error signal bus l for input bus b. If reset (rst) is 1 output is to 0. 16-bit primary input bits are applied to 16-bit X 16-bit Multiplier to generate 32-bit output, output bits are applied to random parity to generate randomized parity code. Parity bits of this randomized parity codeword XORed with previous cycle input parity bits to calculates 5-bit Output parity bits bus z. Input bits and encoded input parity bits are applied to input decoding module, input parity bits XORed with previous cycle input parity bits to calculate expected randomized parity bits. Primary input bits are used to generate actual randomized parity bits. These expected and actual randomized parity bits are applied to the checker. Checker generates 5-bit error signal bus as k, by comparing parity bits of input bus a and 5-bit input encoded parity bus p to generate 5-bit error signal bus as l, for comparing parity bits of input bus b and 5-bit input encoded parity bus q. Error signal encryption done by64-bit encryption key generator.

Primary input bits are applied to OCP to generate predicted output parity bits, these bits are compared against parity bits of output to generate error signals, this error signals XORed with randomly selected 6-bits of 64-bit Encryption key generator bits to generate 6-bit encoded error signals bus as j.

3.3 RTL Design of Main project work

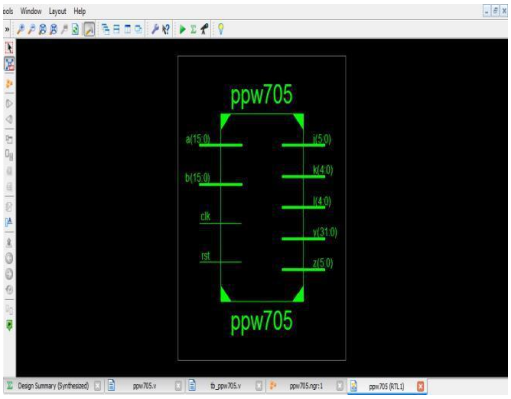

Fig 10: RTL Design of Main project work

3.4 Timing report

	Default period analysis for clock 'clk'	Default OFFSET IN BEFORE for clock 'clk'	Default OFFSET OUT AFTER for clock 'clk'	Dafult Path analysis
FDR	0.722 ns	0.349 ns	0.730 ns	-
INV	0.392 ns	-	0.396 ns	-
IBUF	-	0.290 ns	-	0.394ns
OBUF	-	-	0.000 ns	0.000ns
LUT2			0.376ns	0.376ns
Total Delay	1.115 ns	0.639 ns	1.107 ns	0.771ns

Table I : Timing report

4. Comparison between Main project work and existing work

In existing method to encode error signals of logic circuit, 3-bit Linear Feedback Shift Register

(LFSR) was used.In this paper 64-bit Encryption key generator is used for encrypting error signals.

	3-bit LFSR	64-bit Encryption key generator
Number of Flipflops	3	4
Number of XOR Gates	1	64
Number of Random patterns	2^3	2_{64}
Number of possible ways to select random bits for encoding CED error signals	${}^3C_3$	${}_{64}C_6$
Number of possible ways to select random bits for encoding Input decoding error signals	$3C_3$	$64C_5$
Security	Moderate	High

Table 2 :Comparison between 3-bit LFSR and 64-bit Spreading code random pattern generator

5. Conclusion

The proposed technique can secure digital circuits from Faults and malicious attacks like hardware Trojan attacks by using 64-bit Encryption key generator and CED technique. Error signals are encrypted with randomly selected bits of 64-bit bit Encryption key generator. The obtained area overhead for the Main project work is minimum 50%.There is no attack present in the system encrypted error signals is equal to selected bits of random pattern generator.

6. References

[1] Jiliang Zhang "A Practical Logic Obfuscation Technique for Hardware Security." *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS*, VOL. 24, NO. 3, MARCH 2016, pp. 1193-1197.

[2] K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self authentication technique to prevent inserting hardware Trojans*," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 33, no. 12, Dec. 2014,pp. 1778–1791.

[3] N. Fern, S. Kulkarni, and K. T. T. Cheng. "Hardware Trojans hidden in RTL don't cares Automated insertion and prevention methodologies". *Test Conference (ITC), IEEE International*, Dec.2015, pp. 1-8.

[4] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 33,no. 12, Dec. 2014 pp. 1792–1805.

[5] A. Waksman, M. Suozzo, and S. Sethumadhavan, "FANCI: Identification of stealthy malicious logic using Boolean functional analysis," *Proceedings of theACMComputerandCommunications Security'13(CCS'13),* Berlin, Germany, Nov. 2013, pp. 697–708.

[6] Sheng Wei and MiodragPotkonjak "Scalable Hardware Trojan Diagnosis" *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS*, VOL. 20, NO. 6, JUNE 2012, pp. 1049-1057.

[7] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware Trojan detection and reducing Trojan activation time," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20,no. 1, Jan. 2012, pp. 112–125.

[8] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers,"*IEEE Des. Test Comput*.vol. 27, no. 1, Jan./Feb. 2010 ,pp. 66–75.

[9] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," *Proceedings of the 46th ACM/IEEE Design Automation'09 (DAC'09) conference*, San Francisco, CA, USA, Jul. 2009, pp. 688–693.

[10] M. Abramovici and P. Bradley, "Integrated circuit security: New threats and solutions*," Article No.55, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research'09 (CSIIRW'09),* Knoxville, TENNESSEE, USA, Apr.2009, pp. 1–3.

[11] N. A. Touba and E. J. McCluskey, "Logic synthesis of multilevel circuits with concurrent error-detection," *IEEE Trans. Comput.-Aided DesignIntegr. Circuits Syst.*, vol. 16, no. 7, Jul. 1997, pp. 783–789.