INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Enhanced Hardware Trojan Detection And Deactivation The Trojan Circuit

A.Dalip Joe
Dept.of ECE, Sri Lakshmi Aammal Engineering, Chennai,India
R.Raju
Asst.Prof,Dept.of ECE, Sri Lakshmi Aammal Engineering College, Chennai,India

Abstract:

Global interconnection has allowed Integrated Circuit (IC) designers to greatly reduce costs by subcontract their manufacturing needs to external fabricators. However, there is a low cost Fabless semiconductor facilities have introduced a new potential for security viruses. Standardized testing and verification procedures cannot guarantee the circuit being tested is precisely the circuit that was designed. Thus, an adversary may insert malicious circuits known as hardware Trojans. Trojan trigger to observe either a faulty output or measurable uncommon on side-channel signals or disable functionality, reduce performance, leak Hidden keys, insert a backdoor within the designed circuit. Transition is modeled by geometric distribution and the number of clock cycles required to generate a transition is estimated. Existing system, a dummy scan flip-flop insertion procedure is proposed aiming at decreasing transition generation time. The procedure increases transition probabilities of nets beyond a specific threshold but this paper presents new hardware trust architecture to magnify functional Trojans activity. In this paper architecture modification done by introducing an LFSR and detecting the Trojan threats there by deactivate Trojan threats

***Key words*:** *Dummy flip-flop insertion, hardware Trojan, By-passing*

1.Introduction

OUTSOURCING style and fabrication method has become a trend in integrated circuit (IC) market attributable to economical profit, with limiting the management of client over IC supply chain. Impelled antagonist takes advantage of such restriction to tamper IC provide chain by maliciously implanting extra logic as hardware Trojan electronic equipment into an IC [2]. Consequently serious considerations rise regarding security and trustiness of electronic systems. An assaulter will modification a style net list or subverts the fabrication method by manipulating design mask, without poignant the most practically of the planning [3]. Hardware Trojan detection is an especially difficult problem and ancient structural and practical tests cannot effectively address it. Trojan circuits have sneaky nature and are triggered in rare conditions. Trojans are styled such that they are silent most of their life time and will have terribly small size relative to their host design, with that includes restricted contribution into design characteristics. These recommend that they presumably hook u with nets with low controllability and/or observability [4]–[5]. It is expected that Trojan inputs are supplied by nets with low transition chances to reduce its impact on circuit side-channel signals loke power and delay. Automatic test pattern generation (ATPG) strategies utilized in manufacturing check for detecting defects do therefore by operative on the netlist of the Trojan-free circuit. So, existing ATPG algorithms cannot target Trojans directly [4].

Trojan detection makes economical pattern generation necessary to disclose Trojan impact on design characteristics on the far side process and environmental variations. Trojan detection strategies using transient power analysis [6] need patterns that increase Trojan activity whereas keep circuit activity low to enlarge Trojan contribution into the circuit power consumption. Methods that are supported delay analysis and need patterns that generate transition on nets that offer Trojan inputs to reveal wiring and input gate resistance and capacitance impact of Trojan on the circuit delay characteristic. From authentication standpoint, it is critical to: 1) analyze time to generate a transition at Trojan input and in Trojan circuit and 2) reduce authentication time.

In this paper, we develop a methodology to extend the probability of generating a transition in functional Trojan circuits and to research the transition generation time and also deactivate the Trojan circuit.

2.Related Work

In [4], the authors present a sustained vector technique. A vector is applied to circuit and for many clock cycles (up to 25) primary inputs are kept unchanged. During this method all transitions in the circuit would be attributed to state bits and it is expected that activities converge to a selected portion of the circuit after some clock cycles. By applying the next vector another portion of the circuit will be targeted. Authors in [8] present a technique to get a power fingerprint of real ICs considering various types of noise in the circuit. Random patterns are applied to IC-Under-Authentication (IUA) to generate a measurable difference between the power profiles of the genuine IC and IUA. The planned technique in [9] is based on analyzing local current measured from power ports on the target chip. A calibration process is performed for each IUA before actual measurement to alleviate process variations impact. Trojan-inserted designs are distinguished using outlier analysis. In a multiple provide transient current integration method is presented to identify hardware Trojans in IUA. The current is measured domestically from various power pads or controlled collapse chip connections (C4s) on the die. Random patterns are applied to extend the switching in the circuit in a test-per-clock fashion.

A comprehensive taxonomy of Trojans in integrated circuits is presented in [3]. Trojans are supported physical, activation, and action characteristics. The physical characteristic studies kind, size, distribution, and structure of a Trojan. In terms of kind, Trojan are often functional or parametric. Functional Trojans are accomplished through adding or deleting of transistors or gates, while parametric ones are accomplished through modification of physical geometry of design to sabotage reliability. The number of gates or transistors that are added or deleted defines Trojan size.

3.Hardware Trojan Classification

This section describes and illustrates what classes of Trojans exist. In literature malicious hardware implantations are called hardware Trojan horse (HTH), malicious circuit or malicious logic. A Trojan is completely characterized by its physical representation and its behavior. So, its characterization can be divided into three parts:

- physical representation
- activation phase (trigger)
- action phase (propagate payload)

4.Physical Characteristics

From the perspective of a malicious circuit designer there are several physical characteristics to plan (figure 1). One of these physical Trojan characteristics is the type. The kind of a Trojan may be either functional or parametric. A Trojan is functional if the person adds or deletes any transistors or gates to the first chip style. The other type of Trojan, the parametric Trojan, modifies the original circuitry, e.g. cutting of wires, weakening of Flip-Flops or transistors, subjecting the hip to radiation, or using Focused Ion-Beams (FIB) to decrease the reliability of a chip. Then, this kind of Trojan is called "parametric Trojan". Furthermore, an malicious designer has to define the size that is the next category. The size of a Trojan is its physical extension or the number of components it is made of. As a result of a Trojan will contain several elements, the designer will distribute the components of a malicious logic on the chip. The extra logic will occupy the chip where it is required to switch, add or neglect a function. If the function of the Trojan demands it, on the one hand malicious elements may be scattered. This is often known as loose distribution. On the other hand a Trojan will contain solely few elements, so the area is little wherever the malicious logic occupies the layout of the chip. In distinction this is often known as tight distribution. If the adversary spares no e ort, then he regenerates the layout, in order that the position of the elements of the IC is altered. In rare cases the chip dimension is altered. These changes are structural alterations.

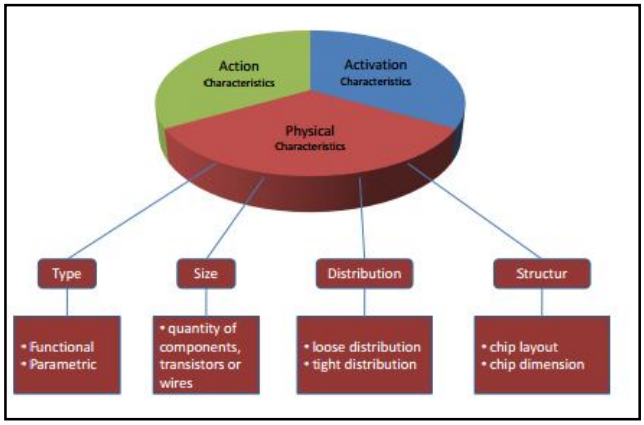

Figure 1: Classification of Trojan (physical aspects)

5.Activation Characteristics

Figure 2 illustrates the activation characteristics. The typical Trojan is condition-based: It's triggered by sensors, internal logic states, a selected input pattern or an interior

counter value. Condition-based Trojans are detectable with power traces to some extent once inactive. That is as a result of the leakage currents generated by the trigger or counter circuit activating the Trojan. Hardware Trojans can be triggered in different ways. A Trojan may be internally-activated, meaning it monitors one or additional signals within the IC. The malicious circuitry could wait for a countdown logic an attacker added to the chip, in order that the Trojan awakes when a selected timespan. The opposite is externally-activated.

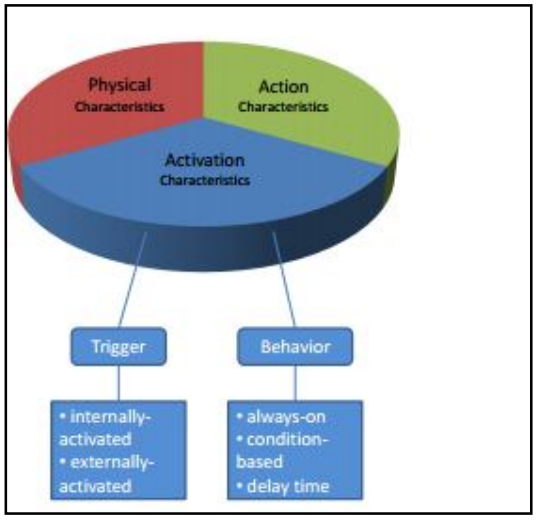

Figure 2: Classification of Trojan (Activation)

6.Action Characteristics

A HTH may modify the chip's function or changes the chip's parametric properties (e.g. provokes a process delay). Confidential information can also be transmitted to the adversary (transmission of key information).

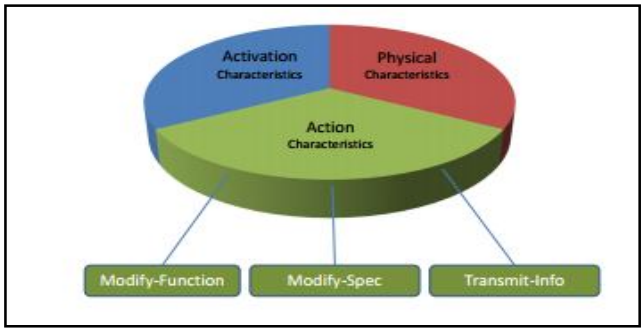

Figure 3: Classification of Trojan (Action)

7.Trojan Activation Time Detection

7.1.D Flip-Flop

The primary electronic flip-flop was fabricated in 1918 by William Eccles and F. W. Jordan. It had been at first known as the Eccles–Jordan trigger circuit and consisted of two active elements (vacuum tubes). Such circuits and their transistorized versions were common in computers even after the introduction of integrated circuits, though flip-flops made from logic gates are also common now. Early flip- flops were known variously as trigger circuits or multivibrators. A multivibrator is a two-state circuit; they come in several varieties, based on whether each state is stable or not: an astable multivibrator is not stable in either state, so it acts as a relaxation oscillator; a monostable multivibrator makes a pulse while in the unstable state, then returns to the stable state, and is known as a one-shot; a bistable multivibrator has two stable states, and this is the one usually known as a flip-flop. The D flip-flop tracks the input, making transitions with match those of the input D. The D stands for "data"; this flip-flop stores the value that is on the data line. It can be thought of as a basic memory cell. A D flip-flop can be made from a set/reset flip-flop by tying the set to the reset through an inverter. The result may be clocked.

7.2.Dummy Scan Flip-Flop

The structure of dummy scan flip-flop (dSFF) in addition to an extra gate (AND or OR). If probability of “0” on target net Net_i P_i0, is less than its probability of “1”, P_i1 , an AND gate is placed after scan flip-flop and net Net_i rest itched through the AND gate to increase P_i0 , as depicted in figure. However, if P_i1 is less than P_i0, an OR gate is being used to increase P_i1, as . In this work, dSFF-AND and dSFF-OR represent dummy scan flip-flops with AND and OR gates, respectively. Accompanying a net having low transition probability with a dSFF would increase the nets and following nets’ transition probabilities. When Test Enable (TE pin) is active, the output of scan flip-flop is supplied by Scan Input (SI pin). The inserted dummy scan flip-flop has no impact on the functionality of the circuit. In normal functional mode, the output of scan flip-flop is supplied by either “0” or “1” depending on the gate type at the output of scan flip-flop to avoid changing the functionality of Net_i .The probabilities of “1” and “0” at the output of scan flip-flop are 1/2. Assume that of is much greater than its P_i1 where

$$P_i0 = \frac{K}{N} \quad \text{and} \quad P_i1 = 1 - \frac{K}{N}$$

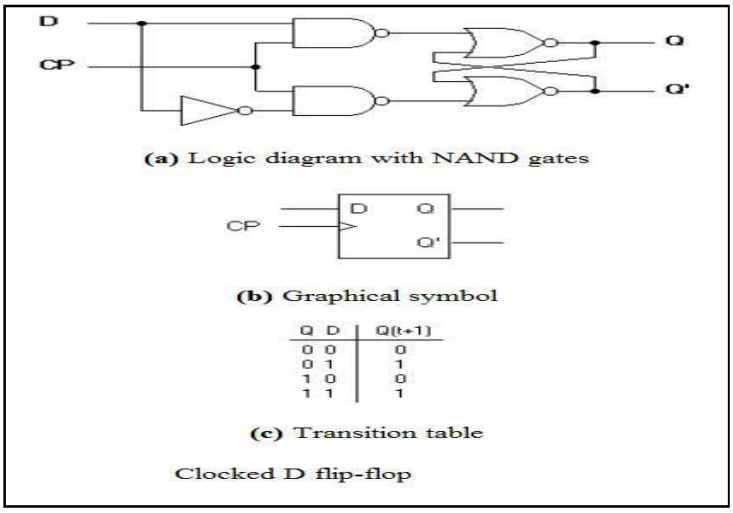

Figure 4: D Flip-Flop using NAND gate

7.3.Trojan Detection

Automatic test pattern generation (ATPG) methods used in manufacturing test for detecting defects do so by operating on the net list of the Trojan-free circuit. Therefore, existing ATPG algorithms cannot target Trojans directly. Trojan detection makes efficient pattern generation necessary to disclose Trojan impact on design characteristics beyond process and

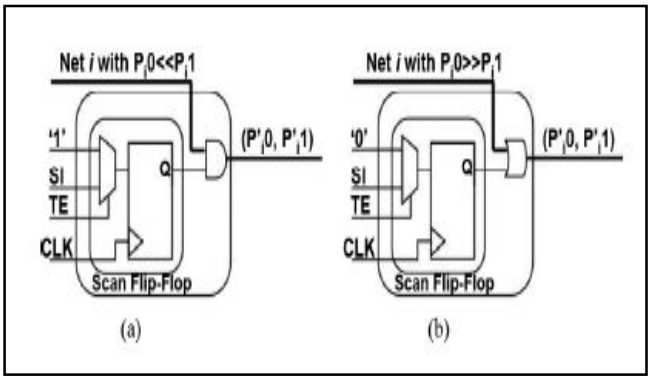

Figure 5: (a) Dummy scan flip-flop using OR gate

(b) Dummy scan flip-flop using AND gate

environmental variations. From authentication standpoint, it is critical to: 1) analyze time to generate a transition at Trojan input and in Trojan circuit. we develop a methodology to increase the probability of generating a transition in functional Trojan circuits and to analyze the transition generation time.

7.4.Trojan Activation time detection without Dummy scan flip-flop

Trojan consists of two parts: Trigger and Payload .The Trigger circuit is mostly inactive by nature with no Payload effect. Under certain rare conditions or events, the Trojan is activated (triggered) and then Payload injects an error to the circuit. Generating transition in Trojan circuit depends on its implementation. Switching at the first level gates of Trojan circuit depends on its preceding cells. The next levels of Trojan circuit are similar to the first level; therefore, in the following, we focus on generating switching in one Trojan gate at the first level of a Trojan circuit to carry out our detailed analysis

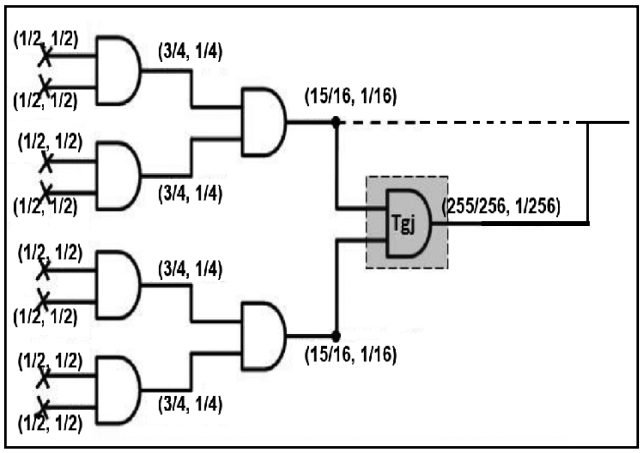

Figure 6: Circuit without Dummy scan flip-fliop

- Transition probability at trojan output = 255/65536
- Average clock cycle per transition by GD = 255.6
- Average clock cycle per transition by simulation =250

7.5.Analysis With Dummy Scan Flip-Flop

The proposed dSFF insertion procedure. Netswith transition probabilities greater than determined transition probability threshold (P_{th}) and close to nets with transition

probabilities lower than P_{th} are good candidates for dSFF insertion since each of them can impact several low transition nets at their fanout cone at once.

- Transition probability at trojan output = 8415/262177
- Average clock cycle per transition by GD = 30
- Average cycle per transition by simulation=33.4

In this case, mathematical analysis shows that inserting a dSFF-OR on upper input net of gate in Figure 6, reduces the number of clock cycles per transition from 255.6 to 30 on average at the output of gate. Furthermore, simulation results also closely confirm 33.4 clock cycles per transition. TE pin is active during test mode and Trojan circuit can be designed to become active when TE pin is inactive, which in turn makes dummy flip-flop technique ineffective.

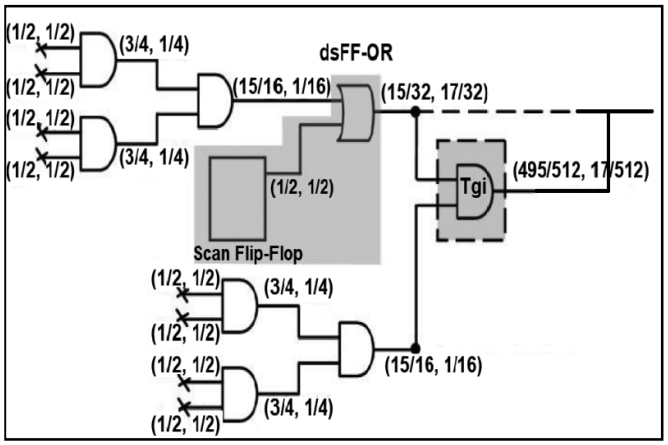

Figure 7: Circuit with Dummy scan flip-flop using OR

8.Proposed Method

8.1.Trojan Detection Through LFSR

The benchmark circuit output will give to the comparator the comparator compare the output of the benchmark circuits and test data these tested date is located in look up table. if any output of the benchmark circuit is mismatch with tested data it should be stored in RAM. Its detection rate is very high compared to Dummy scan flip-flop.

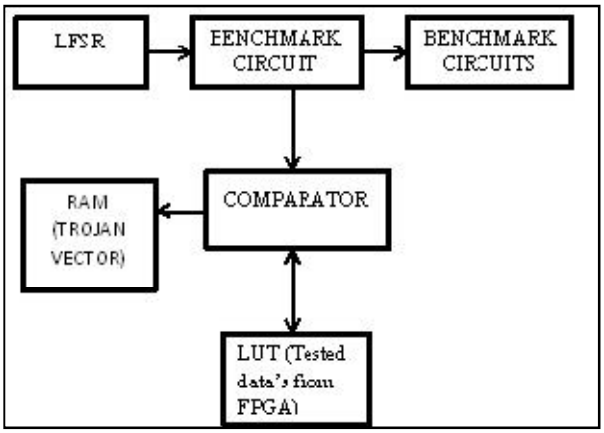

Figure 8: Block diagram of Trojan detection circuit

9.Trojan Deactivation Through By-Passing Method

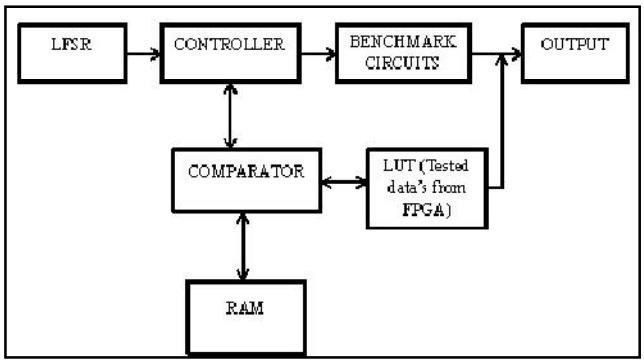

Figure 9: Block diagram of deactivation using By-Passing method

LFSR output will give to controller. The controller compares the LFSR output and stored RAM data. If any vector is mismatch with LFSR output then it will be given to look up table these look table contain tested data from FPGA it have Trojan thread free data so that mismatch vector find it output from look up table and these output is bye-pass the benchmark circuit output it give Trojan free output.

10.Conclusion And Results

We demonstrate that the topology of a circuit and the number of primary inputs and flip-flops determine switching activity of the circuit. In the following, transitions are modeled using GD and the number of clock cycles taking to generate a transition is estimated on average. Furthermore, it is shown that inserting dummy scan flip-flop can reduce

transition generating time. This realization leads to develop a dummy flip-flop insertion procedure aiming at augmenting transition probabilities of nets in a design, and increasing activity of hardware Trojans in Integrated Circuits. The simulation results for s38417benchmark demonstrate that it is possible to significantly increase switching activity in Trojan circuits. Smaller Trojans may be fully activated and cause functional failures. We would like to make improvements to the methodology presented in this paper. Detecting the Trojan circuit from given s38417benchmark and bypass the Trojan activation by using LUT technique.

11.Acknowledgement

We wish to express our sincere thanks to all the staff member of ECE Department, Sri Lakshmi Aammal Engineering College for their help and cooperation.

12.Reference

1. Hassan Salmani, Student Member, IEEE, Mohammad Tehranipoor, Senior Member, IEEE, and Jim Plusquellic, Member, IEEE, "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time"
2. U.S.D. Of Defense, "Defense science board task force on high performance microchip supply," Washington, D.C., 2005 Available: http://www.acq.osd.mil/dsb/reports/2005-02
3. S. Adee, "The hunt for the kill switch," IEEE Spectrum, 2008. Available:http://www.spectrum.ieee.org/print/6171
4. X.Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in Proc. IEEE Int. Workshop Hardware-Oriented Security Trust (HOST), 2008, pp.15–19.
5. R. S. Chakraborty and S. Bhunia,(2009) "Security against hardware Trojan through a novel application of design obfuscation," in Proc. Int. Conf. Comput.-Aided Des., pp. 113–116.
6. M. Banga and M. S. Hsiao,(2008) "A region based approach for the identification of hardware Trojans," in Proc. IEEE Int.Workshop Hardware-Oriented Security Trust (HOST), pp. 40–47.
7. Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar, "Trojan detection using ic fingerprinting," in Security and Privacy, 2007. SP '07. IEEE Symposium on, 2007, pp. 296–310.
8. [8] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B.Sunar, (2007) "Trojan detection using IC fingerprinting," in Proc. Symp. Security Privacy, pp. 296–310.
9. M. Banga and M. Hsiao, ''A Novel Sustained Vector Technique for the Detection of Hardware Trojans,'' Proc. 22nd Int'l Conf. VLSI Design, IEEE CS Press, 2009, pp. 327-332.
10. M. Tehranipoor and F. Koushanfar,(2010) "A survey of hardware Trojan taxonomy and detection," IEEE Des. Test Comput., pp. 10–25
11. J. Li and J. Lach,(2008) "At-speed delay characterization for IC authentication and Trojan horse detection," in Proc. IEEE Int. Workshop Hardware-Oriented Security Trust (HOST), pp. 8–14.

12. Y. Jin and Y. Makris,(2008) "Hardware Trojan detection using path delay fingerprint," in Proc. IEEE Int. Workshop Hardware-Oriented Security Trust (HOST), pp. 51–57.
13. D. D.Wackerly,W.Mendenhall, III, and R. L. Scheaffer, (2008) Mathematical Statistics With Application, 7th ed. Belmont, CA: Thomson Learning Inc.
14. I. Verbauwhede and P. Schaumont, ''Design Methods for Security and Trust,'' Proc. Design, Automation and Test in Europe Conf. (DATE 07), EDA Consortium, pp. 672-677.