ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Surveillance of integrated circuit for Hardware Trojan and remedies to protect from the Trojan.

Surendar A*, Sharma S, Tejaswi V, and Ramyasri G.

VIgnan's University, Guntur, Andhra University, India.

ABSTRACT

Due to globalization of semiconductor industry and the increasing demand in fabricating digital integrated circuit, are now facing problem with a hardware threat known as hardware Trojan horse. Hardware Trojan (HT) is a malicious, unauthenticated and undesired modification to an integrated circuit (IC), which is a major part of electronics.The modification may leak important information ,causing the system to fail while operating in real time. HT has been found as a problem to military, medical, transportation and other critical systems. It is a major security threat for the integrated circuit like FPGA, ASIC, Microcontroller, microprocessor .Hence it is a major security challenge to prevent and detect the hardware Trojan. In this regard first we have to know the ways in which this HT can be encountered. The most significant way to handle this Trojan problem is to understand the Trojan classification and counter attack techniques. A new taxonomy was presented in this paper to handle the HT,this classification covers theprevention and detection methods.

Keywords: Hardware Trojan horse, Integrated circuit, HT prevention and Detection

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Electronics plays an important role nowadays. In our daily life we depend on electronic gadgets like USB,smart phones,computers,etc..for storage and communication of confidential information. In all these electronic devices there will be an integrated circuit .Since IC'S are major building block of electronic devices.They are used to implement a specific function.The ability to trust these IC's have become a security concern , because with out trust in IC the devices they support cannot be trusted.A Hardware based security threat known as Hardware Trojan is attacking the electronic devices particularly IC .A Hardware Trojan horse is undesired and intentional modification made to an integrated circuit design which results in incorrect operation of device [1]. The main differences between hardware Trojan and software Trojan is in hardware Trojan once the Trojan is inserted in to the IC the Trojan behavior cannot be changed. Whereas in software Trojan , the Trojan is part of the code in software and the Trojan behavior can change.A software Trojan is added to a software through network. Hardware Trojan threats must be identified earlier in integrated circuit design flow.Proper prevention and detection methods must be followed to get rid of this hardware Trojan to some extent.

This paper is divided in to sections and each section contains the following. In section 2 we describe the IC design flow and chances of hardware Trojan insertion in the design flow of an IC. Section 3 elaborates about hardware Trojan horse and their taxonomy .Section 4 and 5 describe about the new classification i.e; prevention and detection of hardware Trojan and finally section 6 offers the conclusion.

IC DESIGN FLOW

The design of an IC comprises several steps. The first step of the process is the conversion of specifications/requirements text in to architecture design and then the description in Hardware design language like verilog/VHDL and the test bench is written to make sure that the HDL description for the device is correct or not. Then the synthesis stage is used to generate a gate level netlist. The place and route or layout in implementation stage gives the netlist a physically realized form.The digital file which is produced is handed to fabrication. After producing the actual circuit by industry ,the testing step ensures for their correct operation and after the assembly and packaging step ,the circuits are headed for use.

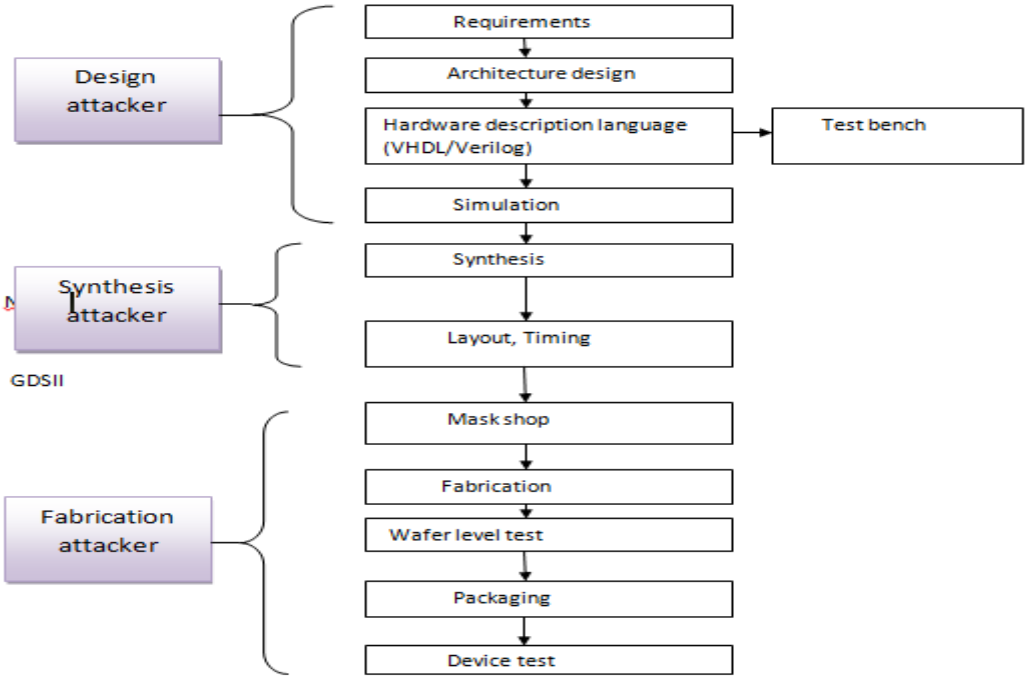

Figure 1: IC development cycle

ISSN: 0975-8585

The figure shows there is a chance of hardware Trojan horse insertion at design ,synthesis and fabrication stage.

HARDWARE TROJAN HORSE AND THEIR TAXONOMY

Hardware Trojan Horse(HTH) is composed of two main components Trigger and Payload. Trigger is used to activate or enable the malicious activity. Payload is used to execute the malicious activity.

HT can serve as a Time bomb Trojan which disables a system at some future time. It can also serve as a data exfiltration Trojan which leaks confidential information over secret channel.In the Hardware Trojan classification, the adversary has access to all stages of the IC.

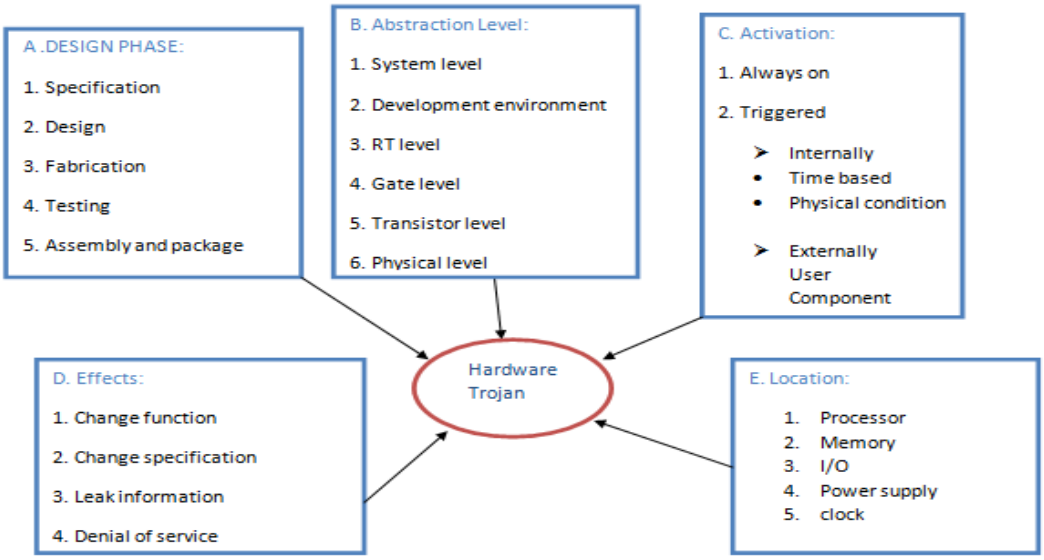

Figure 2. Hardware Trojan Taxonomy

A. Through what ways hardware Trojan is inserted in the design phase?

1. In the Specification phase , many characteristics like expected function,size,power and delay are defined. In this phase the Trojan might be able to change the hardware timing requirements.
2. In the Designphase the designer may use the third party IP blocks , Synthesis and simulation tools and standard cells.Since we are relying on third party and standard cells there is a chance of hardware Trojan insertion in that.
3. In the Fabrication phase Subtle mask changes can have serious effects.In an extreme situations an attacker can substitute with different mask set.
4. In the Testingphase the test cases are applied through Automatic Test Equipment(ATE) to the IC.The adversary changes the test vectors to make Trojan detection difficult.
5. In the Assembly and Package phase the developers assemble the tested IC and other hardware components on a printed circuit board. The adversary have a chance of inserting Trojans into the interfaces during packaging.

B. Through what ways hardware Trojan is inserted in the abstraction phase?

1. At System level Trojans can be triggered by hardware module. Example: By interchanging the ASCII values of keyboard inputs.
2. At Development environment an adversary can use CAD tools to insert Trojans.
3. At RT level developers describe each functional module in terms of registers,signals and Boolean functions
4. At gate level the design is represented in the form of interconnection of logic gates. In this Trojan might be a simple comparator consisting of xorgates which monitors the chip internal signals.

5. At transistor level the transistors are mainly used for building logic gates. Transistors can be added or removed to modify circuit functionality. Transistors sizes can be modified to change circuitparameters.
6. At physical level Trojan can be inserted by adversary by modifying the layout and wiring

C. How a Trojan will be activated?

Some Trojans will be always on while others will be triggered when an event like internal or external arises. On the occurrence of event only Trojan will be activated. Once triggered they remain active forever or remain dormant for some time.

1. An internally triggered Trojan gets activated by an event which occurs within the target device. The event can be of time based or physical condition based. Time bomb comes under time based. The physical condition based Trojan will be activated when it exceeds the physical conditions such as temperature, humidity, atmospheric pressure. For example when a chip temperature exceeds 56 degree centigrade a Trojan will be triggered.
2. An externally triggered Trojan will be activated when the target module receives external input. The external trigger may be user input or component output. User input can be pushbuttons, switches and keyboards.

D. Effects of a Hardware Trojan?

Trojans resultsin undesirable modifications to the system. Their effects range from small disturbance to the critical system failures.

1. Changing the function of the hardware device by a Trojan results in some precise errors which may be difficult to detect.
2. A Trojan can change by modifying the parameters like size, power and delay.
3. A Trojan might leak sensitive information. Information can be leaked through interfaces like RS232 and JTAG and also by optical and thermal.
4. Denial of service Trojan results in preventing the operation of a function. For example it causes the processor to ignore the interrupts from any specific peripheral. A Trojan may cause the hardware module to exhaust resources like battery power.

E. Where will be the Trojans located?

A Trojan can be inserted in one or many components. Trojans can be located in a processor, memory, Input/Output units, powersupply and clock. Trojans inserted in multiple components can act independently or even as a group.

1. A Trojan in the processor may change the order of execution of instructions.
2. A Trojan in the memory alter the values stored in memory. For example a Trojan might change the PROM contents in an integrated circuit.
3. A Trojan can be there in the printed circuit board and even in the chip peripherals. If a Trojan is inserted in the RS-232 module then for data transmission the baud rate is higher than the original 9600 baud rate which results in leakage of sensitive information.
4. In power supply units Trojans change the voltage and current supplied to the device and cause the failure of a device.
5. Trojans inserted in the clockgrids changes the clock frequency

Validation for the above mentioned taxonomy can be referenced in [2].

PREVENTION

Since we know the ways in which hardware Trojan can be inserted in to the design. One way to protect the design against this threat is by preventing them from being inserted at any stage of integrated circuit design flow.

The most significant way is to control the process from end to end in an integrated circuit. It is always best to use trusted synthesis and simulation tools for designing and also fabricating in trusted foundry so that there will be less chances in malicious modifications.

Generally Trojans remains active in some nodes of circuit where there will be less chances of observing and controlling. Hence by concentrating at that areas and developing ideas to observe at that node will disables the Trojan activities.

The prevention can be done in design, layout level, Fabrication and at Post-Fabrication stages of an IC development cycle [1].

Prevention at Design stage:

Prevention at this stage can be done by avoiding use of untrusted EDA tools and untrusted third party Intellectual Property(IP) blocks in the design . One way to avoid Trojans at this stage is to use all the hardware resource at all the times that is on all clock cycles. All the resources must be used properly in such a way they are required to satisfy the correct function of an integrated circuit.

Prevention at Layout level:

Circuit layout containing unused spaces, unused routing channels and noncritical pathsare more susceptible to hardware Trojan insertion.

Prevention against hardware Trojan can be done by filling the unused spaces in the layout of a design with functional standard cells instead of non-functional filler cells this is done by using a technique called BISA [7]. The unused space can also be filled by flip-flops, multiplexers, lookuptables by using a technique called dummy logic [3]. While filling this unused space some routing issues arises so some routing algorithm must be developed to tackle down this problem.

Prevention at Fabrication:

Prevention at this stage can be done by avoiding fabrication from untrusted foundries. Jin and Makrisproposed a system that has IP consumer providing security related properties. IP consumer and IP producer must agree to those properties translation to get rid of the Trojan.

Prevention at Post-Fabrication:

A reconfigurable logic is placed in between output of some integrated circuit and input of some other integrated circuit, this is done to hide the design from an adversary who has access to RTL. This makes the attacker lack of knowledge about the working of an integrated circuit and help us to prevent the device from hardware Trojan.

DETECTION

As mentioned earlier it is not completely possible to prevent hardware Trojan horse insertion in an IC design. Preventive measures are provided to protect the device from hardware Trojan horse insertion. Whereas detection methods are used to detect the hardware Trojan. Nowadays currently lot of research is going on the detection of hardware Trojan which is gaining lot of significance.

Hardware Trojan detection approaches can be classified in to two types destructive and non-destructive. In destructive method of hardware Trojan detection it fully destroy the integrated circuit they examine. In order to have confirmation that there is no hardware Trojan in the integrated circuit it must be completely reverse engineered. However reverse engineering a complex integrated circuit is time consuming process. Basically reverse engineering of an IC means analyzing the integrated circuit internal structures and their connections in order to know how it is designed and how it operates. A reverse engineering flow includes the following steps they are de-capsulation, de-layering, image reconstruction, annotation, schematic creation and analysis. Destructive method is costly and very time consuming.

ISSN: 0975-8585

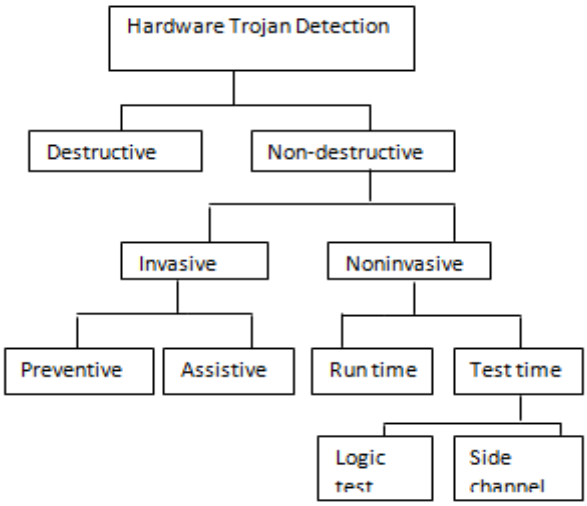

Figure3: HardwareTrojan Detection Techniques

The hardware Trojan canbe inserted in a circuit by adding or removing the logic gates. since VLSI circuits contains billions of logic gates and if hardware Trojan is inserted in that and if destructive method is used to detect Trojans in such a case it takes a lot of time to identify.To determine whether the chip is Trojan free or not it is compared with the Golden IC i.e; IC which is Trojan free.

Due to high costs of destructive detection mechanism we came for nondestructive mechanism. The non destructive mechanism will not destroy the IC being examined. These are classified as invasive and non-invasive.Non-invasive technique leave the design unchanged, whereas invasive technique change the design. Non-invasive technique is divided in to run time and test time ,under test time there are logic test and side channel.

Run Time Monitoring Approach:

Detection of all types of Trojans during post silicon test may be infeasible practically ,so online monitoring of critical tasks can increase the trust level with respect to Trojan threats. On detection of any malicious logic or function change these run time approach disables the chip or bypass it and allows only reliable operation. One such online monitoring approach is addition of reconfigurable logic, which is referred to as DEsign For Enabling Security(DEFENSE)logic in the soc to enable real time monitoring. When any malicious deviation from original circuit function is observed this approach identifies it and the reconfigurable logic implements the infected logic function and it in turns disable or bypass it.

A combined hardware-software approach has been proposed for hardware Trojan detection. This approach attempts to detect DOS (Denial Of Service) attack, this can be detected by using hardware guards which sits on memory bus. A hybrid hardware-software approach called blue-chip is proposed for run time monitoring.If any unused circuitry is undergoing any design verification tests it marks it as suspicious. At runtime the malicious/suspicious circuitry is replaced with some exception logic, which trigger a software exception so that malicious modifications will not be done.This approach is designed to bypass hardware Trojan which is similar to software Trojan in this purpose. These Trojans aims atescalating the privilege of program to superuser mode ,granting access to restricted memory or initiating denial of service attacks, which is similar to malicious code execution. These Trojan circuits are inserted in hardware IP getting mapped to reconfigurable logic in FPGA.

Logic Testing method:

Constructing a test vector to cover the entire logical space in an integrated circuit is computationally infeasible. So to overcome this some statistical approach is followed [5].Logic testing performs checking at the

pre-silicon design stage and it includes generation of test patterns through Automatic Test Pattern Generation(ATPG) in order to excite critical paths during testing of a chip.Based on IC's logic structure analysis this method is divided in to functional behavior analysis method and find hidden features method [6].

Coming to the functional behavioral analysis test vectors are inserted in to the inputs of electronic circuit and the output is observed. If the output is not compatible with the input then a deviation/modification is recognized. This method is generally used for detection of functional errors and detection of parametric hardware Trojan(hardware Trojans are added by modifying the structure of the circuit) and cannot detect functional hardware Trojan(hardware Trojans are added by adding/subtracting some elements in the circuit).The disadvantage of this logic test functional behavior analysis method is large scale of test environment in integrated circuits. For large IC's applying all possible test cases to cover everything in the IC is impossible. To overcome thisdisadvantage Jha proposed a method which is based on Randomization.

Find hidden features method mostly focus on identifying IC structure characteristics that is not well known to everyone. The research in this is performed on hardware instead of performing on some simulation environment. They mainly concentrated on JTAG interface of field programmable gate arrayIn this regard some hidden commands are detected in JTAG by some power analyzing. They found that one of the hidden command requests a 128 bit block of data by using 128 bit as a key, some of the chip features which are previously unavailable are now activated and programmable.

Since Logic testing method is resistant against noise effects and also against fabrication modification, this method is used for detecting small Trojans. There are two difficulties in this method they are the Trojan may be inactive while testing and the Trojan detection requires more test vectors which is time consuming. By using the technique involving random test vectors the Trojan can be detected. By also using the statistical measure we can know which nodes is prone to the Trojan inclusion.

Side Channel Analysis:

Side channel analysis method detect the hardware Trojan by observing the change in circuit Parameters because hardware Trojans generally results in modification of circuit parameters like power,timing,delay,temperature,sound, electromagneticwave and current . By comparing the above mentioned circuit parameters with healthy and suspicious chip we can detect hardware Trojan.

In power based analysis the Trojan is detected by comparing the golden integrated circuit (which is Trojan free) with integrated circuits that are required to be authenticated .If they match then that integrated circuit is Trojan free and is authenticated. If they did not match then that integrated circuit is considered as suspicious. In order to obtain the power signature of golden ICs number of input random vectors are applied to the circuit yielding a power spectrum which is considered as reference. The power spectrum covers static,dynamic, transient or combination of three areas. Similarly for the integrated circuits which are under authentication for them also number of input random vectors are applied and these are expected to give the power spectrum similar to that of reference one. The circuit is divided into areas and random vectors are applied and power spectrum is estimated for each area [4].

The current that a Trojan can draw is very small and it can be hided into the noise and process variation effects and it is not detectable by conventional measurement equipment. However detection of Trojans can be done by measuring the currents locally and from many power ports/pads. The more information can be obtained from [8],[9]

The Trojan included in a circuit results in variation of size of transistor and number of logic gates. Hence the size of the capacitor changes in specific routes, the route delay, rise and fall times will undergo change. Next after the time we measure the delay or frequency to distinguish healthy circuit from suspicious circuit which has been said in [10],[11],[12],[13]. Merging of power, delay and current has been applied in [14],[15].

Although side channel analysis method is lost cost and bring desirable results there are also some difficulties faced by this method they are the nanometer chip dimensions led to lowered circuit currents which are mistaken with noise. The same is true for delay also.

ISSN: 0975-8585

Advantages and Disadvantages of all Detection Techniques:

Table 1: Summary of detection techniques

SL.NO.	Detection Methods	Advantage	Disadvantage
1.	Logic Testing	• For detecting small Trojans this method is effective. • Robust under process noise	• Large Trojan detection is challenging • Test vectors generation is complex
	Functional behavior analysis	Used for detection of functional errors and Parametric hardware Trojans	• Cannot detect functional hardware Trojans. • Entire test is impossible in large ICs
2.	Side Channel	• For detecting large Trojans this method is effective • Test vectors generation is easy • Cost is low • High Performance • Reliable and so used in security systems to protect the system against the Trojan.	• Small Trojan detection is challenging • Not robust under process noise • Requirement to Golden IC
	Delay Analysis		Measurement of short path is difficult
	Power Analysis		Undesired effect of noise and process variations in measurement
3.	Multiple parameter side channel analysis	• Provides effective detection of complex Trojans under large process induced parameter variations • This method can be integrated with • Logic testing approach for reliable detection of Trojans of all types and sizes	For small Trojans this method may suffer from reduced sensitivity
3.	Reverse Engineering	• For Trojan detection this method isreliable	• High cost • For complex IC it is Time consuming • Not suitable for large scale Trojan detection
4.	Built in self-test(BIST)	• Tests hardware with our requiring any external test equipment • Produce accurate results • Runs at Full functional clock speed • Improving security	• It provides fault detection but not fault Isolation • It adds area to the chip
5.	Temperature variation based hardware Trojan detection through ring oscillator	• This method is effective for small scale Trojans with small number of trigger points. • Used as complementary to side channel analysis based detection	• High false alarm probability

For the Trojan not to be detected by any delay and power based techniques Trojan triggers and payloads are having two characteristics: They are

1. Should be connected to nets with low transition probability
2. Trojan should be placed on a path in such away that the path with maximum delay is not a critical path.

CONCLUSION

This paper attempted to provide information about Hardware Trojan ,which is a ongoing threat to the security of electronic systems all over the world. The most ideal way to tackle down this problem is to clearly understand about the taxonomy of hardware Trojan and their counter attack techniques .In this paper, a new classification was proposed that is prevention and detection. Each prevention and detection technique were mentioned with their advantages and disadvantages. Having clear idea about the prevention and detection techniques and using the appropriate method at the right place one can protect the electronic device from hardware Trojan. The future work is to develop efficient delay and power based detection techniques to detect the hardware Trojan.

REFERENCES

[1] Mark Beaumont, Bradley Hopkins and Tristan Newby “Hardware Trojans – Prevention, Detection, Countermeasures” .

[2] J. Rajendran, E. Gavas, J. Jimenez, V. Padman and R. Karri “Towards a comprehensive and systematicclassification of hardware Trojans”

[3] BehnamKhaleghi, Ali Ahari, HosseinAsadi, and SiavashBayat-Sarmadi “FPGA-Based Protection Scheme against HardwareTrojan Horse Insertion Using Dummy Logic IEEE embedded systems letters, June2015

[4] Rad R, PlusquellicJ,Tehranipoor M. Sensitivity analysis to hardware Trojans using power supply transient signals. IEEE International Workshop on Hardware-Oriented Security and Trust. 2008 Jun; p. 3-7.

[5] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware Trojan detection," in Cryptographic Hardware and Embedded Systems-CHES 2009, ed: Springer, 2009, pp. 396-410.

[6] EhsanSharifi, Kamal Mohammadiasl, MehrdadHavasi and Amir Yazdani“ Performance analysis of Hardware Trojan detection methods”. International Journal of Open Information Technologies ISSN: 2015

[7] Xiao K, Forte D, Tehranipoor M. A Novel Built-In Self- Authentication Technique to Prevent Inserting Hardware Trojans.Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on. 2014 May; 33(12):1778-91.

[8] M. Tehranipoor and F. Koushanfar, “A survey of hardware Trojan taxonomy and detection,” *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010

[9] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, “HardwareTrojan detection and isolation using current integration and localized current analysis,” in *Proc. IEEE Int. Symp. Defect Fault Toler. VLSISyst.*, Boston, MA, USA, 2008, pp. 87–95.

[10] S. Jha, "Randomization based probabilistic approach to detect Trojan circuits," in High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 2008, pp. 117-124

[11] Agrawal D, Bostor N, Yaghma N. Trojan detection using IC fingerprinting. SP’07, IEEE Symposium on Security and Privacy, 2007, IEEE. 2007 May; p. 296-310.

[12] Jin Y, Makris Y. Hardware Trojan detection using path delay fingerprint. 2008 HOST, IEEE International Workshop on Hardware-Oriented Security and Trust. 2008 Jun; p. 51-57.

[13] Salmani H, Tehranipoor M, Plusquellic J. A novel technique for improving hardware trojan detection and reducingtrojan activation time. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on. 2012 Jun; 20(1):112-25.

[14] Hu K, Her N, Kim C, Cheng K. High-sensitivity hardware trojan detection using multimodal characterization. IEEE, In Design, Automation & Test in Europe Conference & Exhibition (DATE). 2013 Mar; p. 1271-76.

[15] Narasimhan S. Multiple-parameter side-channel analysis: A non-invasive hardware Trojan detection approach. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). 2010 Jun; p. 13-18.

[16] S. Narasimhan*et al.*, "Hardware Trojan detection by multiple parameter side-channel analysis," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2183–2195, Nov. 2013.