IC Trojan Detection

Drexel University, Electrical and Computer Engineering Department
sss329@drexel.edu

Abstract- The outsourcing and globalization of IC design and fabrication has become very popular throughout the years with manufactures. This trend creates vulnerabilities in the IC life cycle, corporations, and company Intellectual Properties(IP). As the control over the IC life cycle gets lost, the threat of Trojan injection is spread throughout the whole IC development work flow. With the wide spread concern of hardware Trojan attacks, many detection methods have been developed.

I. Introduction

As the complexity of IC design is increasing, the cost of development is also increasing. In order to keep cost down, companies are relaying on off shore fabrication facilities to fabricate their designs. This workflow has increasingly made the fabrication process vulnerable to malicious activity. The addition of circuitry in these vulnerabilities, can deliberalety make modifications to the IC during fabrication or design. These attacks are known as Hardware Trojan attacks. With the threat of Hardware Trojan attacks increasing, a lot of research has been done in Trojan Detection. There has been many Trojan designs and detection methods developed to combat this issue. This paper will discuss the fabrication work flow and Trojan design and insertion to better understand the techniques being used for Trojan detection. The paper is organized as follows: Section II provides an overview fabrication work flow and background on IC design. In section III Trojan design and taxonomy. Section IV will go over current Trojan detection techniques and challenges. Concluding remarks are provided in Section V.

II. IC Design Work Flow

Understanding the IC design and workflow is very important and is a complicated process. Understanding the possibilities of Hardware Trojan insertion and how to protect the IC against such attacks, are very hard to understand. The development and fabrication process has many stages: the functional design, Fabrication, Test & Validation, and Package & Board level. These stages can be broken down even further into three categories Functional design, Physical design, and testing.

A. Functional Design

The functional Design stage is where the behavior of the circuitry is designed. First the high-level design specifications are created followed by device architecture. In some cases, architectural description languages are used in this stage. Next the logical functionality is designed using RTL or register transfer level description. This is accomplished using hardware description languages such as VHDL or Verilog in order to synthesis the circuit.

B. Physical Design

After the RTL description is synthesized to a netlist, a EDA or electronic design automation tools are used to create the Physical Design of the circuit. Then placement and routing can be done. This process takes the netlist provided and created a two-dimensional floorplan and using the provided design constraints, routing is generated for that floor plan. Once this layout is created a graphic database system version II file is exported, this file is used to send to the third-party foundries to produce the design.

C Testing and verification

Once the device is created programs are developed, to be used to configure and test the IC. This is where functionality tests and manufacturing fault test are built. This is also the stage in which if any firmware is needed for the device the process for applying that firmware is created.

D Fabrication

Before full production can begin, sample ICs are fabricated for validation and ran through the test simulations. Then once the flow is created mass production can begin and the full fabrication process is started.

III Trojan Design and Taxonomy

Figure 1 shows the taxonomy of a hardware Trojan, showing that Trojans consists of three main characteristics: Physical, Activation, and Action. The

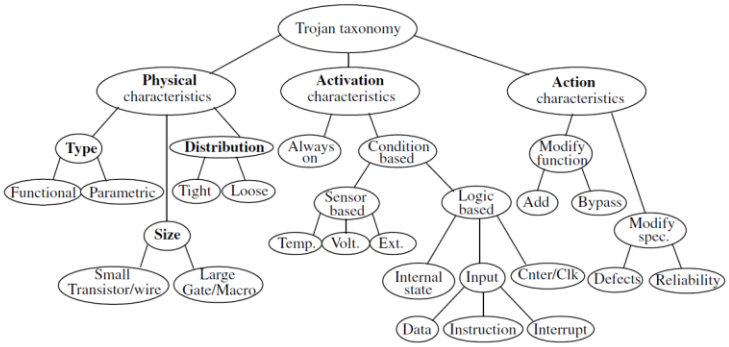

Figure 1: Trojan Taxonomy [3]

Narasimhan[3] extensively describes the Taxonomy of a Trojan and how the Taxonomy describes the design of the Trojan.

A Physical Characteristics

Three parameters: Type, Size, and Distribution describe the physical characteristics of a Trojan. Two fundamental classes, are functional and parametric. The functional subsection of Trojans are Trojans that are additions or deletions of transistors or gates in the design. The number of components in the chip that are added or removed from the design describes the size of the Trojan and the location of the Trojan on the physical chip. The distribution of the Trojan through the design is also another category. This describes the topological layout of the Trojan.

B Trojan Activation Characteristics

Activation characteristics, describe when the Trojan becomes active and starts to carry out its functionality. Narasimhan[3] states that there is two subclasses, always-on and Condition based. Always-on indicates that the Trojan is active from the start and is functioning. The other subclasses, covers Trojans that only activate on some condition whether it be a sensing condition or logic condition. Once one or both conditions are reached the Trojan will start its activity. These conditions con be either sensor based or logical based. Such as temperatures, voltages, EMI. Input conditions means, there is some logic that when passed through the Trojan the Trojan activates.

C Hardware Trojan Action Characteristics

Action characteristics are the types of malicious behavior the Trojan can induce on the circuit. The two top level subsections are modify function and Modify specifications. As the names imply the activity of the Trojan can harm functionality by removing or bypassing logic. The Trojan can also change the chips parametric properties, such as delay.

D Design

An adversary can use these types of Trojans to compromise the IC During any stage of the IC fabrication process. From Functional design, to the actual fabrication of the final design there are insertion points for every step. The author in [1] has done a survey as to the possible insertion points and how the characteristic model plays a role in where the Trojan can be inserted. As shown in Figure 2. The functional design, is the popular point of insertion and Trojans at that level can have many different functionalities while also being Always on or Condition based.

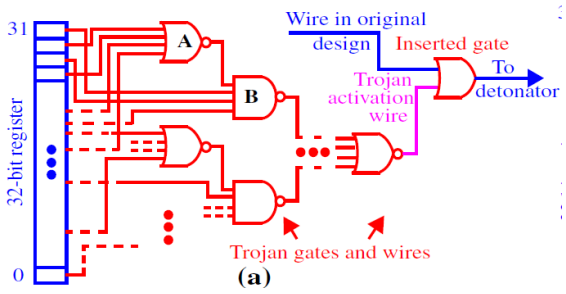

Figure 2: logic activated Trojan with comparator [2]

Table 1 Hardware Trojan survey

	Possible insertion phases	Action characteristics			External trigger	Internal trigger	
		Modify functionality	Transmit information	DoS		Always on	Condition based
Jin and Makris [18]	functional design			•		•	
Chakraborty *et al.* [19]	functional design			•		•	
Agrawal *et al.* [10]	functional design	•					•
King *et al.* [20]	functional design	•			•		
Lin *et al.* [21]	functional design		•			•	
Kutzner *et al.* [23]	functional design		•				•
Muehlberghuber *et al.* [24]	physical design			•	•		
Bhasin *et al.* [25]	physical design	•			•		
Becker *et al.* [26]	fabrication	•				•	

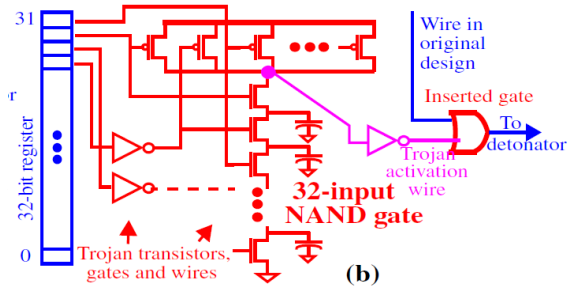

Figure 3: logic gate implementation of a Trojan [2]

IV Trojan Detection techniques

In the previous sections, described the work flow of fabrication and Trojan Characteristics and design. Now Trojan Detection can be identified.

A. Functional analysis and Optical inspection

Optical inspection is a technique used to see any visible changes made to the IC. Chips are revered engineered, by delayering the IC and photographing each layer thoroughly and examined for any malicious circuitry or alterations made to the IC. Rad[2] states that the main drawback to such approach is overhead such as cost and time. But, done effectively the optical images can be cross correlated with the GDSII layout files to verify the IC has not been tampered with.

Another post fabrication approach is functional analysis where the which is cost effective and used to verify that the design is functional working. One big down side here is that this technique fails to pick up dormant Trojans or condition activated Trojans.

B Side-channel analysis and Current sensors design

Side channel analysis is the use of the ICs, power, current and timing, with other statistical analysis to pick up any malicious activity. The drawback to this technique is the noise caused by different variables in the circuit that can hinder the results.

Narasimhan[3] describes a side channel analysis method using on chip sensory network. The currents measured by the sensors located on different regions of the IC will be inherently more sensitivity then that of an external sensor network [3]. In theory, will minimize the noise that the analysis is picking up. The Narasimhan[3] states that this technique uses the Temporal Self-Referring method to eliminate process variations. The method takes the transient response from the current of the supply and is compared for the same die for the same set of vectors over multiple time intervals. This detects any variation in the ICs design from switching activity. Figure 4 shows an example of this on-chip transient current senor, using a resistor in series with the supply node of a circuit under test.

This technique is also like the golden die method. Where the IC is compared to another IC to compare to verify that the IC does not have a Trojan. The difference would be that the sensor network would be off chip. The on-chip method is much more accurate compared to the off-chip approach. Figure 5 shows the difference in the data. The data shows that there is a higher resolution between the chip with the Trojan and without.

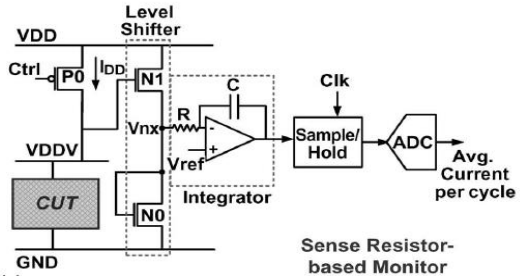

Figure 4: on-chip sensor [3]

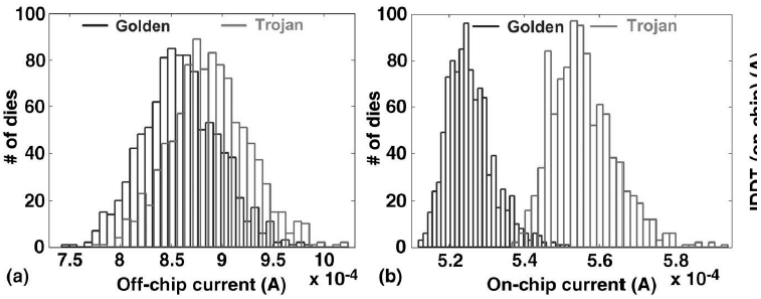

Figure 5: on-chip vs. off-chip [3]

C Power supply transient analysis

Rad[2] uses the side channel approach to Trojan detection, proposed is a power supply transient analysis technique for detection. This technique is used to truncate the process variations from die to die. In this technique, a Detection algorithm is used. The algorithm is based off statistical analysis done on power ports of the IC. Then a graph is populated as show in in Figure 6 to develop a Prediction ellipse.

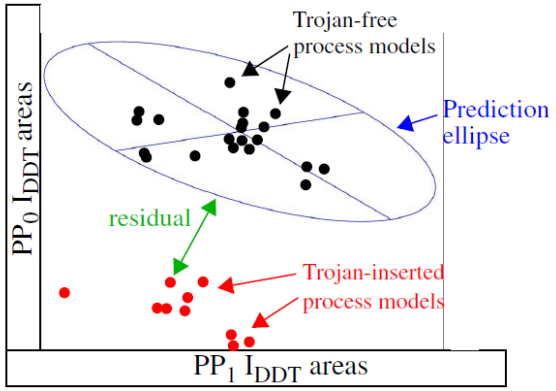

Figure 6: Prediction ellipse[2]

Along with the detection algorithm a calibration is used. The full signal processing diagram is Shown in Figure 7. The data is used in each iteration is get a better prediction ellipse to detect if the circuit has been infected or not.

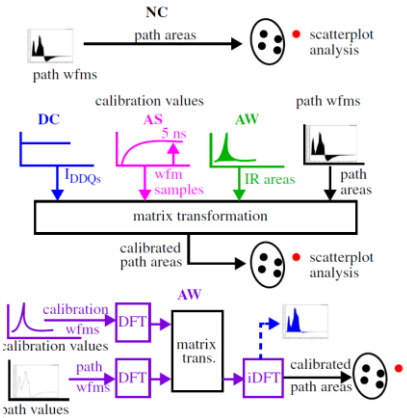

Fig. 7. Signal Calibration Processes

V Conclusion

The vulnerabilities in the IC fabrication process has led to the introduction of malicious circuitry called Hardware Trojans. The introduction of these Hardware Trojans happens at different venerable stages of the fabrication process. To counter act these attacks Trojan Detection techniques have been developed and researched. Such as side channel analysis, optical and function verifications, and mathematical modeling of the data collected by sensory networks on-chip and off. These technigues all have their strengths and weaknesses. Most of all most of these techniques introduce delay, power consumption, or area to the circuit. But, as seen in Figure 5 the technique that allows for more granularity of detection is on-chip detection. Combining the on-chip sensor and the other analysis detection of a Trojan can be increased.

References

[1]N. Jacob, J. Heyszl, G. Sigl, and D. Merli, "Hardware Trojans: Current challenges and approaches," *IET Computers & Digital Techniques*, vol. 8, no. 6, pp. 264–273, Nov. 2014.

[2]R. M. Rad, "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans," in *2008 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Piscataway, NJ, USA: IEEE, 2008, pp. 632–9.

[3]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 of Computers, vol. 29, no. 5, pp. 37–46, Oct. 2012.

[4]Y.-M. Tsai, "A CHIP ARCHITECTURE FOR COMPRESSIVE SENSING BASED DETECTION OF IC TROJANS," in *2012 IEEE Workshop on Signal Processing Systems (SiPS)*, Los Alamitos, CA, USA: IEEE Computer Society, 2012.