Layout-Aware Scan-Cell Reordering for Improving Localized Switching to Detect Hardware Trojans

Hassan Salmani and Mohammad Tehranipoor
ECE Department
University of Connecticut
{salmani_h,tehrani}@engr.uconn.edu

Jim Plusquellic
ECE Department
University of New Mexico
jimp@ece.unm.edu

ABSTRACT

Malicious activities and alterations in integrated circuits have raised serious concerns to government agencies and semiconductor industry. The added functionality, known as hardware Trojan, poses great detection and isolation challenges. This paper presents a novel layout-aware scan-cell reordering method to localize design switching into a specific region and improve hardware Trojan detection. The proposed method forms scan chains by considering the physical information of scan cells. The new scan architecture allows activating any target region and keeping others quiet. This will help magnify Trojan impact on total circuit transient power. Random patterns are used to generate switching in the target regions. The proposed method is aimed at improving the efficiency of power-based side-channel analysis methods for detecting hardware Trojans. The experimental results show that our proposed method significantly increases Trojan-to-circuit power consumption ratio.

1 Introduction

Design and fabrication of Integrated Circuits (ICs) are becoming increasingly vulnerable to malicious activities and alterations with globalization. These vulnerabilities have raised serious concerns regarding possible threats to many critical applications. The third party responsible for design or fabrication can maliciously change the design by inserting extra logic. Such a logic, called hardware Trojan, in a genuine design can be inserted before fabrication such that the design will either fail in the field or act as a backdoor to transmit secret data to adversary [1][2]. Therefore, confidence in imported products is a serious concern especially in mission-critical applications.

Having the knowledge of IC fabrication and testing, an adversary can design a Trojan that cannot to be activated and detected with traditional functional and structural test. However, side-channel signal analysis techniques over power, time, and EM emanation have proved to be highly effective in extracting information about the internal operation of design [3][4][5]. In a power-based side-channel analysis, it is possible to extract Trojan signal by monitoring power pads/ports even in presence of various types of noise, including measurement noise, ambient noise, and other random signal variations that manifest themselves during the circuit operation. Some other kinds of approaches are presented in [6][7][8][9]. Authors in [10] present a detailed taxonomy for Trojans and discuss the issues related to hardware Trojan detection and isolation. We refer reader to [10] for details on the Trojan taxonomy and Trojan examples.

Several methods based on analyzing transient circuit power to detect Trojans are presented in [11][12][13][14][15][16]. The proposed methods are highly dependent on the effectiveness of patterns to magnify Trojan contribution into circuit power consumption. However, a Trojan is expected to have little contribution to the circuit power since either the size of Trojan is too small or circuit activity is high that masks Trojan impact on power signals. Regional activation, in which transitions are limited to a target region of circuit while other regions are kept quiet, is an effective way to increase the ratio of Trojan to circuit power consumption.

1.1 Prior Work

Authors in [12] present a method to generate a power fingerprint of genuine 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 profile of the genuine IC and IUA. However, the method cannot localize Trojans and its effectiveness is limited when targeting small Trojans.

The proposed method in [13] is based on analyzing local IDDT current from power ports on the target chip. To alleviate process variations impact during measurement, a calibration step is performed for each IUA before actual measurement. Trojan-inserted designs are distinguished using outlier analysis. However, the effectiveness of the method is not evaluated for small Trojan circuits in large designs. Further, calibration should be done for each IUA individually which may increase authentication time depending on the number of calibration sites.

In [14][15], two methods are presented to detect and localize Trojan circuits. The methods are based on a test pattern generation technique to generate transitions in a target region while keeping other regions at minimum activity. In the first method [14], a region is defined as a group of a number of flip-flops. To induce activity in a region and keep the other regions idle, random patterns are generated and applied. Those patterns that meet a certain switching threshold are selected and used for Trojan detection. In the second method [15], a region is formed from a group of flip-flops and gates which are logically related to a particular function. Random patterns which limit activity in a target region are selected. The presented results compare how much the selected test patterns are more effective than the random patterns. However, there is the lack of presenting results to demonstrate the methods' success in limiting activity in a target region, and whether the amount of switching difference between Trojan-free and Trojan-inserted circuits is sufficient, in practice, to distinguish the two circuits. Furthermore, the results of the second method are presented for small benchmarks with very low flip-flop count. In case of s3271 benchmark with 116 flip-flops, the results show that there is a small difference (about 2%) in switching activity between Trojan-free and Trojan-inserted circuits.

In [16], the authors present a sustained vector technique. A vector is applied to circuit and for several clock cycles (up to 25) primary inputs are kept unchanged. In this way all transitions in the circuit would be because of state bits and it is expected after some clock cycles activities converge to specific portion of circuit. By applying the next vector another portion of circuit will be targeted. The method, however, does not guarantee the entire circuit is explored for Trojan detection.

In [17], we presented a multiple supply transient current integration method to detect hardware Trojans in IUA. The current is measured locally from various power pads or controlled collapse chip connections (C4s) on the die. Random patterns are applied to increase the switching in the circuit in a test-per-clock fashion [18]. The method can be enhanced by localizing switching activity using our layout-aware scan-cell reordering method which will be described in details in the following sections.

1.2 Contributions and Paper Organization

All the previously proposed power-based analyses to detect Trojans lack an efficient localized switching generation strategy. Note that we do not have any knowledge of the size, type and location of Trojans in a circuit. This makes Trojan detection extremely challenging when compared to common fault detection problem. In this paper, we develop a novel pattern application methodology to address this issue.

In general, scan chains provide increased controllability for circuit-under-test. It has been demonstrated that there is a high correlation between switching activities in the internal nodes of a circuit and the transitions taking place in the scan cells [19]. In this paper, a novel scan-cell reordering method is proposed to localize switching activity. The proposed method is layout-aware and can effectively restrict switching activity within a target region. Experimental results show that by activating one region at a time, it is possible to considerably increase the ratio of Trojan-to-circuit power consumption. Combined with the proposed method in [17], it is shown that Trojan impact on circuit charge can be magnified several times by localizing switching activity. We acknowledge that the scan-cell reordering method can be used in combination with the methods proposed in [11][12][13]

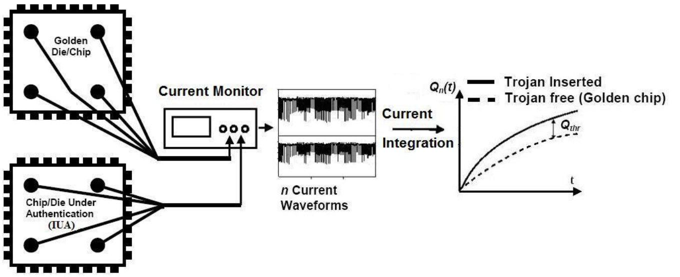


Figure 1: Current integration method.

The paper is organized as following. A brief description on our previously proposed multiple power supply transient current integration method [17] is presented in Section 2. Section 3 presents the proposed scan-cell reordering. Section 4 studies switching localization impact on Trojan detection. In Section 5 impact of process variations on Trojan detection is discussed. Experimental results are presented in Section 6. Finally, Section 7 concludes the paper.

2 Overview of Current Integration Method

Circuit power is supplied by power pads/ports and required current is submitted to cells through power rails and vias. The power vias connect upper power metal layers to lower power lines which are connected to the cells. In [20], it is shown that there is spatial relation between cells and power vias which supply their required current. The major portion of current in switching cells is supplied by the closest power via. Like other cells, Trojan cells also obtain their required current from the nearest power ports [11][13][17]. Based on this fact, measuring current locally through several power pads/ports can greatly improve Trojan detection and isolation using current/charge-based techniques.

Figure 1 shows our previously presented technique in [17]. Each power port of IC-under-authentication (IUA) is measured separately and compared with that of golden chips. The golden chips are Trojan-free and identified using a comprehensive testing and side-channel analysis considering process variations. The Trojan-free transient power characteristic can be obtained by applying random patterns and monitoring and analyzing the current consumption by probing power ports. The same patterns are also applied to IUA.

The figure shows the current waveform of n number of patterns applied to the chips. The figure also shows the charge variations over time for all the current waveforms obtained after applying the patterns. The charge corresponds to the area produced by each current waveform. *Qn(t)* denotes the accumulative charge after applying n patterns. Q_{thr} is the charge threshold to detect a Trojan which is in fact the resolution measurement defined by the instrument. When applying the patterns, the charge increases and is compared continuously against the worst-case charge calculated for golden chips (dash line in the figure). Once the difference between the two curves, ΔQ, is greater than Q_{thr} we consider a Trojan is detected. In this paper, we assume that the IUA has already been tested and is defect-free. The number of patterns, n is expected to be very small for large Trojans and large for very small Trojans.

By applying this method the small current difference between Trojan-inserted and Trojan-free circuits can be magnified through the charge integration process. By applying more number of patterns to the chip over time, larger current (or charge) difference will be created. In the figure, the curve with solid line shows the Trojan-inserted chips accumulative charge.

Assume that $I_{trojan-free}(t)$ and $I_{trojan-inserted}(t)$ denote the instantaneous supply current drawn by Trojan-free and Trojan-inserted circuit at time t, respectively. The integrated current at time t for Trojan-free and Trojan-inserted circuits ($Q_{trojan-free}(t)$ and $Q_{trojan-inserted}(t)$) can be expressed by the following equations (note that $dQ = I \times dt$)

$$\begin{aligned} Q_{trojan-free}(t) &= \int I_{trojan-free}(t)dt \\ Q_{trojan-inserted}(t) &= \int I_{trojan-inserted}(t)dt \\ &= \int (I_{trojan-free}(t) + I_{trojan}(t))dt \end{aligned}$$

where $I_{trojan}(t)$ denotes the current drawn by Trojan. Since same pattern set is applied to both golden chips and chip under authentication, the difference between $I_{trojan-free}(t)$ and $I_{trojan-inserted}(t)$ comes from (1) the additional current drawn by Trojan gates and (2) changes in the circuit current due to process variations. By integrating the charge along time axis for both chips, their cumulative difference at time t can increase as more number of patterns are applied. Note that process variations can increase or decrease current consumption while a Trojan, if switches, will always increase transient current in the circuit. Thus, integration methodology offers the advantage of alleviating process variations impact on total transient current.

3 Scan Cell Reordering

3.1 Background

Power consumption in CMOS circuits is proportional to the amount of switching that takes place in the cells [21]. The relative impact of a Trojan cell on the overall transient current of design depends on the number of cells switching. Given the probabilities of having 1 and 0 on *Net i* are P_i1 and P_i0, respectively, transition probability of the net will be $P_i = P_i1 \times P_i0$. Transition on the net, as a random variable T_i, can be modeled using geometric distribution with parameter P_i. The geometric distribution is a discrete distribution for $n = 0, 1, \cdots$ having the probability function $P_i(n) = P_i \times (1 - P_i)^n$ [22] . The probability function states that after n clock cycles, in $(n + 1)th$ clock cycle, there will be a transition on *Net i*. Based on geometric distribution, on average, each $(P_i^{-1} - 1)$ clock cycles there will be one transition on *Net i*.

Considering that a design consists of N nets, there are $T_1, T_2, \cdots, T_N$ random variables. There is one transition in the design when there is at least one transition on one of the nets. Further, time between every two consecutive transitions in the design is close to a net of design which has the minimum time interval between each two consecutive transitions. Assuming that transitions on nets are independent geometric distribution variables with different parameter P_i, transition in the design can be stated as

$$T_{Design} = MIN\ T_i \text{ where } 1 \leq i \leq N$$

T_{Design} has geometric distribution with parameter P_{Design} given by

$$P_{Design} = 1 - \prod (1 - P_i)$$

For example, consider a design with 4 nets: *Net* 1 with parameter $P_1 = \frac{1}{5}$, *Net* 2 with $P_2 = \frac{1}{4}$, *Net* 3 with $P_3 = \frac{2}{3}$, and *Net* 4 with $P_4 = \frac{1}{6}$. Hence,

$$P_{Design} = 1 - ((1 - \frac{1}{5}) \times (1 - \frac{1}{4}) \times (1 - \frac{2}{3}) \times (1 - \frac{1}{6})) = \frac{5}{6}$$

and, on average, after each $((\frac{5}{6})^{-1} - 1) = 0.2$ clock cycle there is one transition in the circuit. Therefore, it is expected that in each clock cycle, design experiences $\frac{1}{0.2}$ transitions, which is called transition density. Transition density is defined as the number of transitions occurring in a target area in each clock cycle.

To evaluate impact of transition density on Trojan contribution into circuit power consumption, suppose the design is divided into two regions such that there are two nets in each region: *Net* 1 and *Net* 2 are in region $R1$, and *Net* 3 and *Net* 4 in region $R2$. Further, one region is active at a time while the other one is kept idle. In this way, the probability parameter of region $R1$ (P_{R1}) is $1 - ((1 - \frac{1}{5}) \times (1 - \frac{1}{4})) = \frac{2}{5}$. Therefore, on average, every $((\frac{2}{5})^{-1} - 1) = 1.5$ clock cycles there is one transition in the region $R1$. Transition density of region $R1$ is $\frac{1}{1.5}$, which in comparison with transition density on the entire design, $\frac{1}{0.2}$, is about 7.5 times less. It means that if Trojan is in region $R1$, one transition at Trojan output is manifested among about 7.5 times less number of transitions compared to when activating the entire design. Therefore, Trojan impact can be significantly magnified if just region $R1$ is activated instead of the entire design. In the same manner, for region $R2$ the probability parameter of region $R2$ (P_{R2}) is $\frac{13}{18}$ and each 0.38 clock cycle there is one transition in the region $R2$. Transition density of region $R2$ is $\frac{1}{0.38}$ which is about 2 times less than activating the

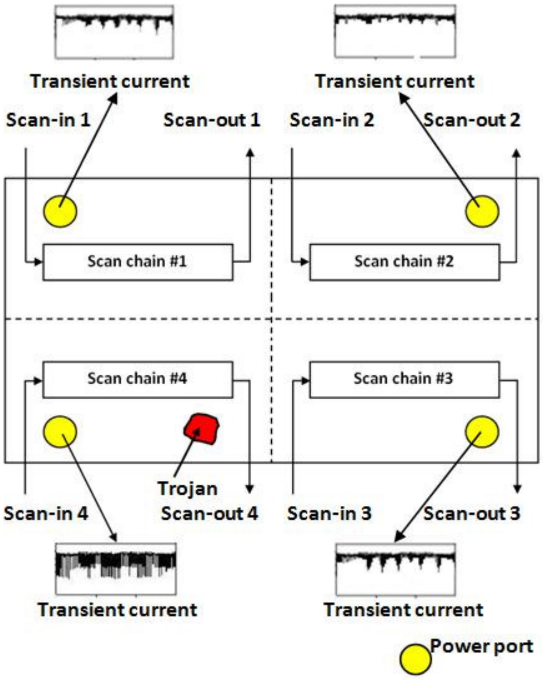


Figure 2: Layout-aware scan-cell reordering concept.

entire design. Therefore, by activating just $R2$, if Trojan is inserted in region $R2$, its impact can be magnified several times in comparison with activating the entire design.

In summary, localizing activity to specific region would increase the relative impact of Trojan, which in turn increases the sensitivity of current/charge-based detection techniques [12][13][17].

3.2 Scan-Cell Reordering Technique

Switching activity in a circuit is a function of primary inputs and scan cells. Due to low controllability, in large designs, using only primary inputs would not be effective in localizing switching activities. Scan architecture is proven to provide easy access to cells in the circuit. During scan-based testing, the total power consumption of the CUT is highly correlated with the total number of transitions in the scan cells. During scan insertion, scan cells are grouped into a number of scan chains. They can be grouped based on different criteria. For instance, Synopsys's Design Compiler simply groups scan cells alphabetically [23]. Since scan cells are grouped without layout information, typically they are scattered across the layout. Therefore, during test, many gates can be activated at the same time. However, reordering of scan cells based on their geometric positions can significantly restrict switching activity into a specific region.

Figure 2 shows the basic concept of layout-aware scan-cell reordering. Assume that four scan chains are inserted in the design. The method would form the chains such that the scan cells placed in each selected region are connected to each other. The objective is to ensure the scan chains have same length but that is not a requirement. Such reordering would increase the localized switching. The method allows us to maximize switching in the target region (e.g. region containing scan chain 4) while minimize switching in all the other regions (1, 2, and 3). This would increase the Trojan-to-circuit power consumption ratio and magnify Trojan impact. Given the limitation on the number of pins used for testing, when the number of regions is large, a compression-like architecture including phase shifter is used.

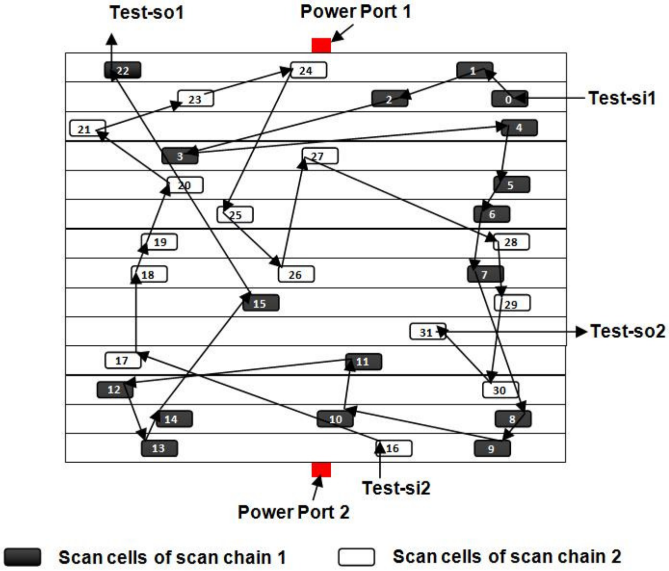


Figure 3: Traditional scan chains organization in s383 benchmark.

As an example, Figure 3 shows the organization of scan chains in s838 benchmark, where 32 scan cells are grouped into two scan chains using Synopsys Design Compiler [24]. The figure shows that each chain, used to generate switching, would practically make the entire circuit experience switching since each scan chain is distributed across the layout. However, our proposed layout-aware scan-cell reordering method would localize switching in one region and limit activation in other regions in the design. Our proposed procedure groups scan cells based on their final physical location in layout. Due to the lack of placement information at front-end phase during scan chain insertion, it is not possible to group scan cells and arrange scan chains based on layout-aware specific criteria. Therefore, we perform layout-aware scan-cell reordering after placement and before routing.

The layout-aware scan-cell reordering procedure uses placement information of scan cells to form scan chains. Although the basic idea is applicable to any design environment, here, the procedure is implemented using Synopsys's Astro [25]. Figure 4 shows the proposed procedure which is implemented by TCL in Synopsys's Astro. First, the placement information of cells is extracted. Then, the connections between scan cells, made using alphabetical order, are removed. Based on the physical information and the number of regions N, scan cells are connected to each other. Finally, the netlist is updated with re-stitched cells to be considered for routing.

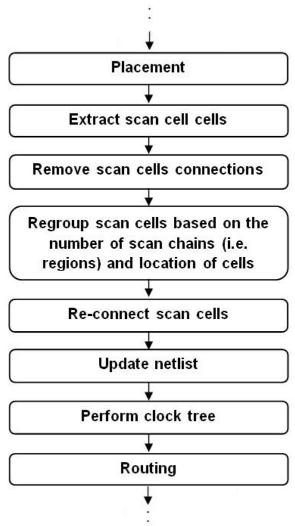

Placement
Extract scan cell cells
Remove scan cells connections
Regroup scan cells based on the number of scan chains (i.e. regions) and location of cells
Re-connect scan cells
Update netlist
Perform clock tree
Routing

Figure 4: Layout-aware scan-cell reordering procedure.

The number of regions, N, determines the size of regions. With large N, each region consists of less number of components. Small region increases Trojan impact on design power profile so it can magnify any transition in Trojan circuit. However, small regions decease the probability of transition in Trojan circuit since some of Trojan inputs can originate from other regions which are kept inactive. Contradictory, large regions can increase the probability of generating transition in Trojan circuit but Trojan impact can be lessened due to decrease in Trojan-to-circuit transient power ratio.

To benefit from the advantages of both cases, it is suggested to divide the design into smaller regions as much as design constrains allow. It is possible to have a large region by activating several small regions simultaneously (e.g. regions 1 and 2 in Figure 2). To increase the probability of generating transition in Trojan circuit, a large region can be activated. To localize Trojan circuit, a large region can be activated partially by activating one or some of its composing smaller regions.

Adversary can put Trojan cells in any region while their inputs can come from several other regions which can make Trojan detection hard. The probability of Trojan activation reduces by activating few numbers of regions. Further, the Trojan-to-circuit power consumption ratio decreases by activating more numbers of regions. In addition, trying any combination of regional activation can be too time-consuming in a design with large number of regions. Assuming the design is divided into N regions, there are $\left(\binom{N}{1} + \cdots + \binom{N}{N}\right)$ combinations of regions. However, in practice it is not necessary to examine every combination of regions.

The number of inputs of components is limited by technology library. Even adversary cannot develop and use a component with high fan-in to reduce its activity since such a component greatly impacts the delay characteristics of design. Based on this fact, given the largest number of inputs to a component in a technology library is I_{max}, the number of combinations to try would be $\left(\binom{N}{1} + \cdots + \binom{N}{I_{max}}\right)$.

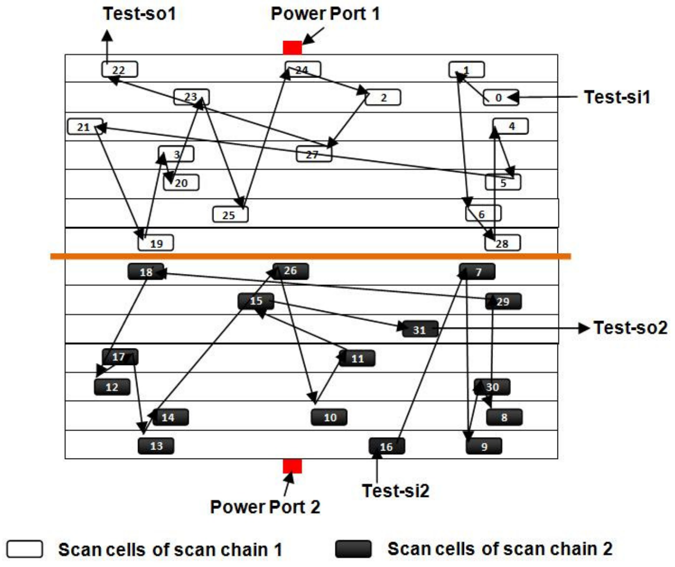
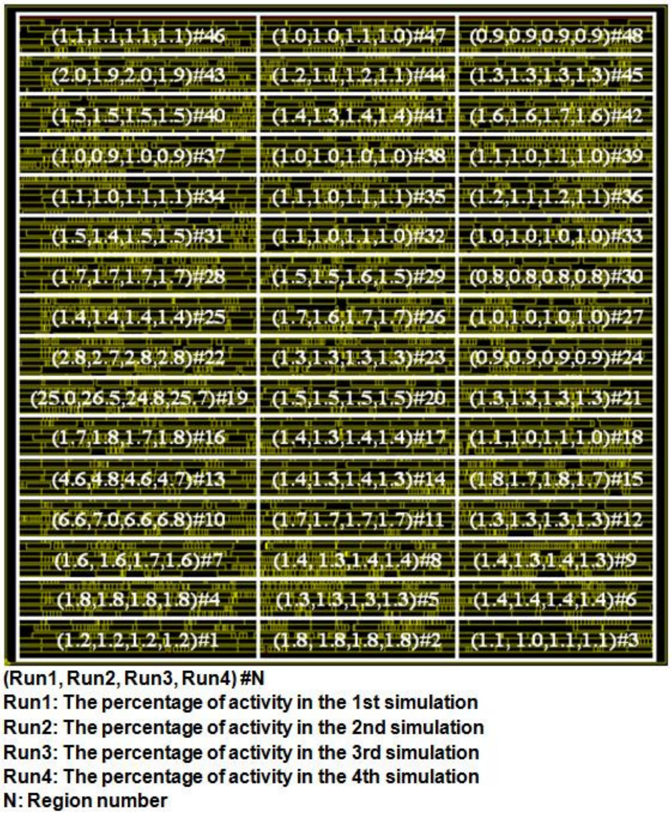


Figure 5: Scan chain organization in s383 benchmark using our layout-aware scan-cell reordering.

Consider s38417 layout is divided into 48 regions, and a tester with clock frequency of 250MHz is used. If I_{max}=4, at the first step, every region is examined individually, which means 48 runs. Then, at the second step, every two regions is examined, which means $\binom{48}{2}$ runs, and at the third step, every three regions, which means $\binom{48}{3}$ runs, and finally every four regions, which means $\binom{48}{4}$ runs. Therefore, totally 213,052 runs are required. Consider the longest scan-chain has 42 scan-cells. So, 42 clock cycles are needed for initialization of design and in the following 42 clock cycles for scanning-in vectors, and finally 42 clock cycles for scanning-out scan chains. Scanning-out and initialization can be the same, and totally each run needs 84 clock cycles. Hence, totally $84 \times \frac{10^{-6}}{250} \times 213,052 = 0.07$ second is required to test design.

Figure 5 shows the new organization of scan chains in s838 benchmark after performing our layout-aware scan-cell reordering. In this design, the scan cells are grouped into two regions, N=2, as if the circuit is divided by 2 based on the location of the cells, assuming that there are two power ports in the circuit one on the top and the other on the bottom shown as power port 1 and 2 in the figure. Note that, in this paper, hereafter, term "power port" is used to represent power pad and C4 bump.

To evaluate the effectiveness of scan-cell reordering in limiting switching activity in any target region, benchmark s38417 with 6497 components consisting of 1564 flip-flops and 4933 gates is selected for further analysis. Scan cells are grouped into N=48 scan chains using our layout-aware scan-cell reordering method. The simulation is run four times and each run consists of three patterns and each pattern 42 vec-



(1.1,1.1,1.1,1.1)#46	(1.0,1.0,1.1,1.0)#47	(0.9,0.9,0.9,0.9)#48
(2.0,1.9,2.0,1.9)#43	(1.2,1.1,1.2,1.1)#44	(1.3,1.3,1.3,1.3)#45
(1.5,1.5,1.5,1.5)#40	(1.4,1.3,1.4,1.4)#41	(1.6,1.6,1.7,1.6)#42
(1.0,0.9,1.0,0.9)#37	(1.0,1.0,1.0,1.0)#38	(1.1,1.0,1.1,1.0)#39
(1.1,1.0,1.1,1.1)#34	(1.1,1.0,1.1,1.1)#35	(1.2,1.1,1.2,1.1)#36
(1.5,1.4,1.5,1.5)#31	(1.1,1.0,1.1,1.0)#32	(1.0,1.0,1.0,1.0)#33
(1.7,1.7,1.7,1.7)#28	(1.5,1.5,1.6,1.5)#29	(0.8,0.8,0.8,0.8)#30
(1.4,1.4,1.4,1.4)#25	(1.7,1.6,1.7,1.7)#26	(1.0,1.0,1.0,1.0)#27
(2.8,2.7,2.8,2.8)#22	(1.3,1.3,1.3,1.3)#23	(0.9,0.9,0.9,0.9)#24
(25.0,26.5,24.8,25.7)#19	(1.5,1.5,1.5,1.5)#20	(1.3,1.3,1.3,1.3)#21
(1.7,1.8,1.7,1.8)#16	(1.4,1.3,1.4,1.4)#17	(1.1,1.0,1.1,1.0)#18
(4.6,4.8,4.6,4.7)#13	(1.4,1.3,1.4,1.3)#14	(1.8,1.7,1.8,1.7)#15
(6.6,7.0,6.6,6.8)#10	(1.7,1.7,1.7,1.7)#11	(1.3,1.3,1.3,1.3)#12
(1.6, 1.6,1.7,1.6)#7	(1.4, 1.3,1.4,1.4)#8	(1.4,1.3,1.4,1.3)#9
(1.8,1.8,1.8,1.8)#4	(1.3,1.3,1.3,1.3)#5	(1.4,1.4,1.4,1.4)#6
(1.2,1.2,1.2,1.2)#1	(1.8, 1.8,1.8,1.8)#2	(1.1, 1.0,1.1,1.1)#3

(Run1, Run2, Run3, Run4) #N
Run1: The percentage of activity in the 1st simulation
Run2: The percentage of activity in the 2nd simulation
Run3: The percentage of activity in the 3rd simulation
Run4: The percentage of activity in the 4th simulation
N: Region number

Figure 6: The percentage of switching activity in each region of s38417 after running four simulations. Each region is shown as (Run1, Run2, Run3, Run4) #N, where N is region number.

tors. The first pattern initializes all scan chains with '0'. The second pattern applies random '0' and '1' to scan chain 19 while '0' to the other scan chains. Four different patterns are used in four runs. The third pattern scans out the scan chains while scanning in '0'. To increase randomness, the circuit is always set in scan mode by keeping scan-enable input active. The percentage of activity in each region is reported in Figure 6 as (Run1, Run2, Run3, Run4). The results clearly indicate that in all four cases switching activities are mostly limited to the region covered by scan chain number 19 while other regions are kept inactive.

4 Switching Localization Impact on Trojan Detection Strategies

Power consumption of a Trojan is expected to be negligible compared to the circuit under authentication when Trojan is small. Hence, to improve Trojan detection, the ratio of Trojan-to-circuit power consumption must be increased.

The power consumption of a circuit is defined as $\mathbf{p(t)} = \mathbf{i(t)} \times \mathbf{v(t)}$ where $\mathbf{i(t)}$ is the amount of current which is drawn from power source by switching cells and $\mathbf{v(t)}$ is the voltage of power source. In a Trojan-inserted circuit extra power consumption, relative to original design, is expected. To magnify the impact of Trojan using power-analysis-based method, Trojan power consumption must be a measurable portion of the circuit power consumption in presence of variations and measurement noise.

Assume that the design consists of M components and K power ports. Each component of circuit impacts the power ports in proportion to their distance from the power ports, i.e., the closer the component is to a power port the more impact it will have on the power port. Therefore, the power measured from power port k (PPk) can be stated as

$$P_{PPk-trojan-free} = \sum_{1}^{M} d_i P_{comp\#i}$$

where d_i denotes the distance of component i from P_{PPk}, and $P_{comp\#i}$ is the amount of power consumed by the ith component.

Any extra cell as Trojan impacts each power port and increases P_{PPk}. When the entire design is activated, the ratio of Trojan-to-circuit power consumption (TCP) at power port k (PPk) is

$$TCP_{PPk} = \frac{d_{trojan} P_{trojan}}{\sum_{1}^{M} d_i P_{comp\#i} + d_{trojan} P_{trojan}}$$

TCP_{PPk} would be negligible when either Trojan is far from PPk or many components are active at the same time. Therefore, it is expected that TCP increases by activating only a part of the design. If design is divided into N regions, the Trojan-to-circuit power consumption at PPk will change to

$$TCP_{PPk} = \frac{d_{trojan} P_{trojan}}{\sum_{1}^{N} d_{region\#n} P_{region\#n} + d_{trojan} P_{trojan}}$$

where $d_{region\#n}$ is the average distance of region n from PPk, $d_{region\#n}$ is a function of the distances of components located in region n, and $P_{region\#n}$ is the amount of power consumed by the nth region. Here, the assumption is that there is no information about the Trojans power consumption since the size and type of Trojan is unknown. Generating transitions in a target region and keeping other regions idle can increase Trojan-to-circuit power consumption ratio since it reduces the amount of circuit power consumption. In other words, since only one out of N regions is active during power-based analysis, TCP_{PPk} would significantly increase.

As an example, a Trojan consisting of a NAND2x1 and an INVx1, where the output of NAND is the input of INV, is inserted into an unused space in s38417 layout. The Trojan is very small compared to the circuit size (about 0.0076%). Two Trojan-inserted designs are generated: (1) Without reordered scan-cells and (2) With reordered scan-cells. In the original design, without scan-cells reordered, all scan chains are fed randomly at the same time. Figure 7(a) shows the ratio of Trojan-to-circuit power consumption (TCP). The TCP ratio is 0.0026. In reordered scan-cells design only one scan chain surrounding Trojan cells is fed by random patterns. Figure 7(b) shows the results obtained after applying

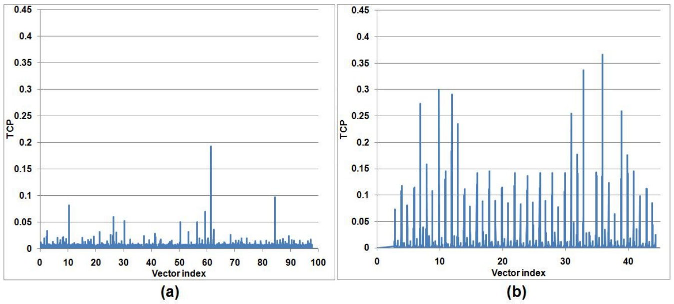


Figure 7: Trojan-to-circuit power consumption (a) without scan-cells reordering and (b) with scan-cells reordering.

random inputs to the scan chain in the target region. The results show that the TCP ratio increases by about 5 times (0.0103 on average).

5 Process Variations

Process variations have raised serious concerns in nanometer regime. Parameters such as device geometry, dopant density, threshold voltage, channel length, and oxide thickness determine delay characteristic and power profile of a design. Process variations must be considered in Trojan detection methods that rely on side-channel signals analysis. As in [17], process variations can either help or harden the Trojan detection process.

The following two scenarios will make the Trojan detection more difficult when considering process variations:

1. When process variations in Trojan-free circuit increase the transient current. This will make the current measured from a Trojan-free circuit closer to that of the Trojan-inserted circuit. It is recommended to obtain a large number of Trojan-free ICs so that a more accurate average impact of process variations on circuit power can be obtained.

2. When the process variations in Trojan-inserted circuit decrease the current consumption. This will also make the current measured from the Trojan-inserted circuit closer to that of the Trojan-free circuit.

Similarly, the scenario that helps make the Trojan detection process easier is:

1. When process variations in Trojan-inserted circuit increase the current consumption.

We acknowledge that process variations should be considered, in practice, during Trojan detection. However, in the following section, the experimental results are presented only to evaluate our proposed scan-cell reordering method.

It is expected that process variations impacts decrease by activating a small portion of a design since fewer components are active at any clock cycle relative to the entire design.

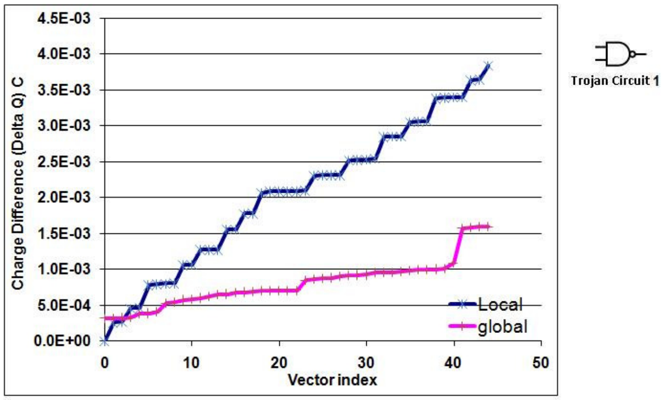


Figure 8: The charge difference accumulation of circuits containing Trojan circuit 1 using local and global activations.

6 Experimental Results

In this paper, functional-type Trojan circuits are targeted for detection [10], i.e. combinational or sequential Trojans. Parametric-type Trojans [10], which are realized through thinning of a wire or weakening of a transistor, are not considered here. Trojan cells can be put together in one place (tight) or scattered across the layout (lose) [10]. In this paper both kinds of distribution are addressed. In [11][13][17] we were able to effectively detect Trojan circuits as small as few NAND gates in presence of process variations. In this paper, the examined Trojan circuits' size is about 0.005% of the entire design and they are mostly just one NAND gate.

To evaluate the effectiveness of scan-cell reordering on detecting Trojans, different Trojan circuits are inserted in s38417 layout which is divided into 48 regions. In the following subsections, we present the results of analyzing different cases: two small combinational Trojan circuits, a sequential Trojan with just one flip-flop, the impact of Trojan on a power port in relation with their distance, distributed Trojan detection, and the impact of neighboring cells to Trojan on its detection.

In this section, we use term "local activation" for applying patterns to a target region when using reordered scan cells and term "global activation" when traditional scan-cell insertion is used. As mentioned earlier, random patterns are applied in a test-per-clock fashion. To compare local activation and global activation, the accumulation of charge differences is obtained from the first time when there is a transition in Trojan circuit. In addition, the term "vector index" indicates the number of clock cycles after the first transition in Trojan circuit. For the figures, the x axis shows the vector index, and y axis shows the integration of charge difference ΔQ between Trojan-inserted and Trojan-free circuits for both local and global activations.

6.1 Combinational Trojans

Two Trojan circuits are inserted into s38417 layout which is divided into 48 regions. Inputs of the first level of Trojan circuits are the outputs of a scan cell and an AOI21x1 gate. Any other placement of the Trojan would give similar results.

Trojan circuit 1 consists of only one NAND2x1 gate whose size is 0.0042% of the design. Figure 8 compares the effectiveness of local activation to global activations. The results show that after applying the same number of random patterns, local activation results in 3 times more charge difference than global activation.

Trojan circuit 2 consists of one NAND2x1 gate and one INV2x1 and Trojan size is 0.0076% of the circuit. Figure 9 presents the results of global and local activations in this case. The results show localizing switch activity using scan-cell reordering results in about 4 times more charge difference than activating the entire circuit.

6.2 Sequential Trojan

Any sequential Trojan circuit needs clock to drive its flip-flops. Therefore, sequential Trojan circuits consume power even when there is not any transition at the outputs of Trojan cells. Thus, without applying any patterns charge difference between Trojan-free and Trojan-inserted circuits can be measured and analyzed. In this experiment, only one D flip-flop Trojan is inserted. Its D-input is intentionally stuck at '1' to measure the impact of inserted Trojan flip-flop on clock-tree power consumption.

Figure 10(a) shows that there is significant charge difference due to extra load on clock tree coming from wiring and Trojan clock input gate. Further, the results indicate that there is not any difference between global activation and local activation since no pattern is being applied. To study the impact of applying pattern, only region 46 of Figure 6 where Trojan is inserted is activated in local activation whereas the entire design is activated in global activation. The results, in Figure 10(b), show that charge difference is decreased about 30% in global activations while it remains roughly the same in local activation.

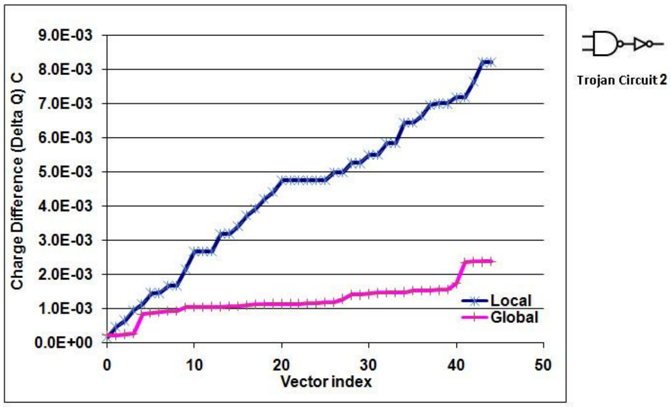


Figure 9: The charge difference accumulation of circuits containing Trojan circuit 2 using local and global activations.

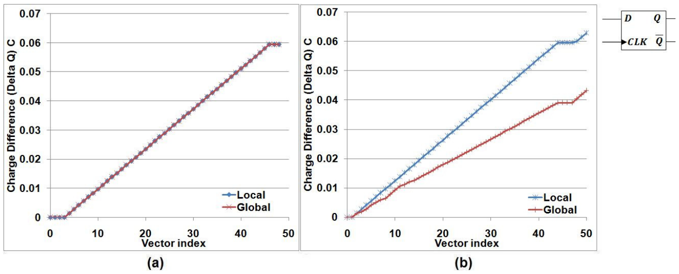


Figure 10: The charge difference accumulation of circuits with D flip-flop Trojan (a) when no pattern is applied and (b) when a pattern is applied.

6.3 Analyzing the Impact of Trojan Location

This experiment studies the impact of Trojans on a power port in relation with their distance in local activation. In a region in s38417 layout, two power ports on the right and left sides of the region are assumed. Three NAND2x1 Trojan gates are inserted in the region: one of them (Trojan A) is placed in one row and the two others (Trojan B and Trojan C) are placed in another row. Trojan A is closer to the left power port, Trojan B is roughly at the middle of two power ports, and Trojan C is closer to right power port. Three experiments are run, and only one Trojan is activated in each experiment. The impact of each Trojan on two power ports is then individually studied. To focus on the distance parameter in charge consumption of Trojan cells, for all three NAND2x1 Trojan gates, one input is always '1' and the other input is connected to the output of one of scan cells in the region.

Figure 11 shows the impact of Trojan A on left and right power ports. Clearly the results show that Trojan A has more impact on closer power port (left one). To further analyze Trojan distance parameter from power ports, both Trojans B and C are placed in one row. Since both Trojans are connected to the same power line, the RC characteristic of their power lines are close. Therefore, their placements on the row and so their distances from power ports more strongly determine the amount of their impacts on power ports. Figure 12 shows the impact of Trojan B on the two

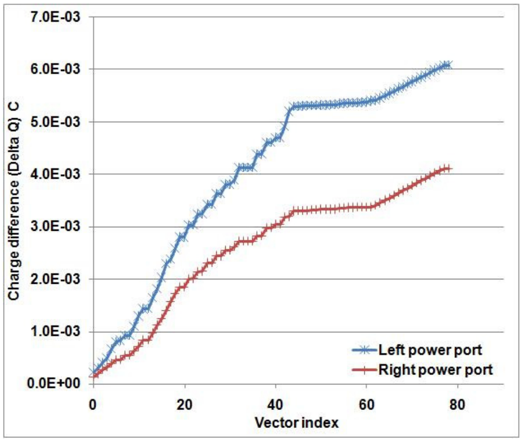


Figure 11: The impact of Trojan A on power ports.

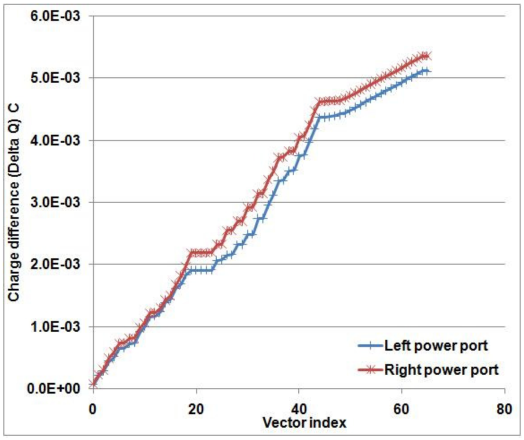


Figure 12: The impact of Trojan B on power ports.

power ports. As Trojan B is approximately located at the middle of row, it has almost same impact on both power ports. Impact of Trojan C on two power ports is presented in Figure 13. As it is expected Trojan C has more impact on right power port than left power port since it is closer to the right power port.

Note that to analyze Trojan location impact on power ports we inserted the Trojan close to a scan flip-flop, thus Trojan is highly active. However, decreasing the number of transitions at Trojan output will not change the trend in the reported results.

6.4 Distributed Trojan

This experiment is to demonstrate the effectiveness of local activation over global activation in detecting distributed Trojans. In this experiment, two NAND2x1 Trojan cells, Trojan A and Trojan B, are inserted in regions number 1 and 48 in Figure 6, respectively. The output of Trojan A is one of inputs of Trojan B. The other input of Trojan B is connected to the output of a scan cell in region 48. The two inputs of Trojan A are '1' and output of a scan cell in region 1.

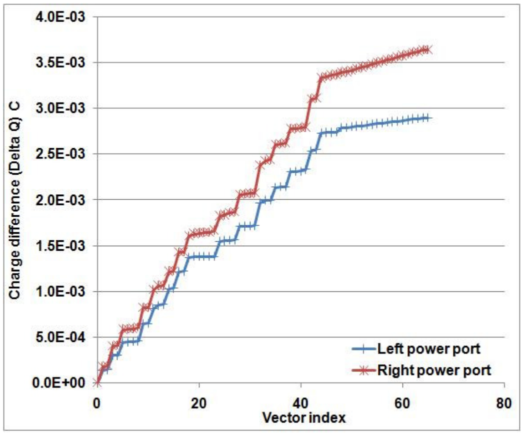


Figure 13: The impact of Trojan C on power ports.

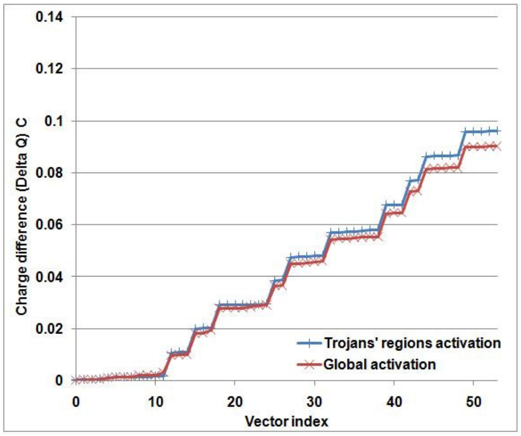


Figure 14: The charge difference of distributed Trojan with two NAND gates in global activation and regions 1 and 48 activation together.

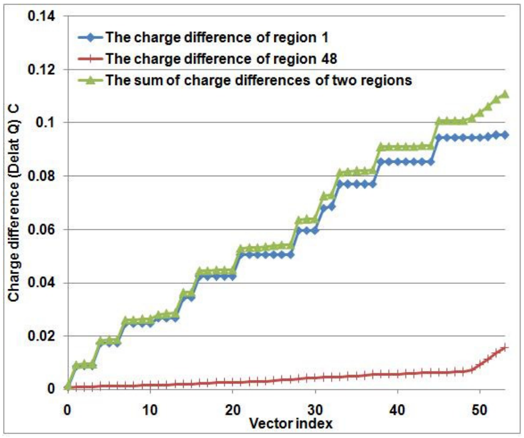


Figure 15: The charge difference of distributed Trojan with two NAND gates when the two regions are activated individually.

In global activation, the entire circuit is activated by applying random patterns to all scan chains. Figure 14 shows the charge difference accumulation between Trojan-inserted and Trojan-free. Then only regions 1 and 48 are activated. In Figure 14 the results show that by reducing activity of circuit and limiting switching to the target regions, Trojan impact can be increased. In this case, the results show about 10% more charge difference relative to the first case. Finally, it is expected to see more impact of Trojans on power profile by activating each region separately. In this case, regions 1 and 48 are activated one by one. Figure 15 shows the accumulative charge difference in each region and the sum of charge differences. The results show there is about (i) 16% more charge difference in this case relative to the case where the two regions are activated together and (ii) 28% relative to the case where the entire circuit is activated.

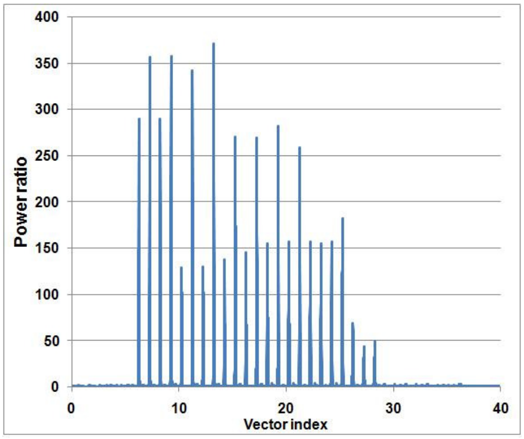


Figure 16: The power ratio of high transition density (16) region over low transition density region (43).

6.5 Analyzing the Impact of Transition Density

The transition density of a region where Trojan is inserted directly impacts Trojan detection. A region with high transition density can lower the Trojan-to-circuit power consumption (TCP). Contradictory, Trojan impact would be more significant in a region with low transition density. To evaluate region transition density impact on Trojan detection, regions 16 and 43 of Figure 6 with different transition densities are selected. Figure 16 shows the power ratio of region 16 (with high transition density) over region 43 (with low transition density). On average, region 16 consumes about 7 times more power than region 43. One Trojan NAND2x1 gate is inserted in each region, and one input of Trojan gate is ‘1’ and the other input is connected to the output of one of scan cells in corresponding region. The results in Figure 17 show that Trojan impact in the low transition region 43 is about 3 times more than that of the high transition density region 16.

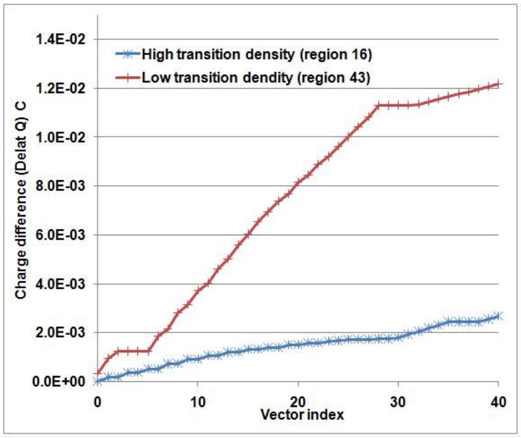


Figure 17: The impact of transition density of a region in which Trojan is inserted on its detection.

7 Conclusions and Future Work

This paper presented a new layout-aware scan-cell reordering method to limit switching activity to a specific region. The results showed that switching in most of non-target regions can be reduced significantly. It was also shown that it is possible to increase the ratio of Trojan-to-circuit power consumption by decreasing design contribution to the total power using the proposed method. By localizing switching and using current integration method which is measured from each power port individually, the experimental results showed that Trojan impact on circuit transient power can be increased significantly making it easier to detect smaller Trojans in presence of process variations. We will be working on adding process variations to our flow using Monte Carlo simulation and the results of Trojan detection in presence of variations will be presented in the final version of the paper, if the paper is accepted for publication in ITC’2009.

AKNOWLEDGEMENT

The work of Hassan Salmani and Mohammad Tehranipoor was supported in part by the National Science Foundation Grant CNS-0716535. The work of Jim Plusquellic was supported in part by NSF grant CNS-0716559.

References

[1] *http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf*

[2] S. Adee “The Hunt for the Kill Switch,” *http://www.spectrum.ieee.org/print/6171*

[3] P. C. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis,” in Proc. of the *CRYPTO*, vol. 1666 of Lecture Notes in Computer Science, pp. 388-397

[4] P. C. Kocher, “Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems In Neal Koblitz,” in Proc. of the *CRYPTO*, vol. 1109 of Lecture Notes in Computer Science, pp. 104-113

[5] D. Agrawal, B. Archambeault, J. R. Rao and P. Rohatgi, “The EM side-channel(s),” in Proc. of the *International Workshop CHES*, vol. 2523, pp. 29-45, 2002.

[6] Y. Jin and Y. Makris, “Hardware Trojan detection using path delay fingerprint,” in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust(HOST 2008)*, pp. 51-57, 2008.

[7] F. Wolff, C. Papachristou, S. Bhunia and R.S. Chakraborty, “Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme,” in Proc. of the *Design, Automation and Test in Europe(DATE ’08)*, pp. 1362-1365, 2008.

[8] J. Li and J. Lach, “At-speed delay characterization for IC authentication and Trojan Horse detection,” in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust(HOST 2008)*, pp. 8-14, 2008.

[9] S. Jha and S. K. Jha, “Randomization Based Probabilistic Approach to Detect Trojan Circuits,” in Proc. of the *IEEE High Assurance Systems Engineering Symposium(HASE08)*, pp. 117-124, 2008.

[10] X. Wang, M. Tehranipoor and J. Plusquellic, “Detecting malicious inclusions in secure hardware: Challenges and solutions,” in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust(HOST 2008)*, pp. 15-19, 2008.

[11] R. Rad, J. Plusquellic and M. Tehranipoor, “Sensitivity analysis to hardware Trojans using power supply transient signals,” in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust(HOST 2008)*, pp. 3-7, 2008.

[12] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, “Trojan Detection using IC Fingerprinting,” in Proc. of the *Symposium on Security and Privacy*, pp. 296-310, 2007.

[13] R. Rad, X. Wang, J. Plusquellic and M. Tehranipoor, “Taxonomy of Trojans and Methods of Detection for IC Trust,” in Proc. of the *International Conference on Computer-Aided Design (ICCAD08)*, pp. 632-639, 2008.

[14] M. Banga, M. Chandrasekar, L. Fang and M. Hsiao, “Guided Test Generation for Isolation and Detection of Embedded Trojans in ICs,” in Proc. of the *Symposium on Very Large Scale Integration*, pp. 363-366, 2008.

[15] M. Banga and M. Hsiao, “A Region Based Approach for the Detection of Hardware Trojans,” in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 43-50, 2008.

[16] M. Banga and M. S. Hsiao “A Novel Sustained Vector Technique for the Detection of Hardware Trojans,” in Proc. of the *International Conference on VLSI Design*, pp. 327-332, 2009.

[17] X. Wang, H. Salmani, M. Tehranipoor and J. Plusquellic, “Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis,” in Proc. of the *International Symposium on Fault and Defect Tolerance in VLSI Systems (DFT08)*, pp. 87-95, 2008.

[18] M. Bushnell and V. Agrawal, “Essentials of Electronics Testing,” Kluwer Publishers, 2000

[19] R. Sankaralingam, R. R. Oruganti and N. A. Touba, “Static Compaction Techniques to Control Scan Vector Power Dissipation,” in Proc. of the *IEEE VLSI Test Symposium (VTS’00)*, pp. 35-40, 2000.

[20] C. Tirumurti, S. Kundu, S. Sur-Kolay and Y. Chang, “A Modeling Approach for Addressing Power Supply Switching Noise Related Failures of Integrated Circuits,” in Proc. of the *Design, Automation and Test in Europe Conference and Exhibition Volume II (DATE’04)*, pp. 21078-21083, 2004.

[21] S. Devadas and S. Malik, “A Survey of Optimization Techniques Targeting Low Power VLSI Circuits,” in Proc. of the *Design Automation Conference(DAC95)*, pp. 242-247, 1995.

[22] D. D. Wackerly, W. Mendenhall III and R. L. Scheaffer, “Mathematical Statistics with Application, 7th edition” Thomson Learning, Inc., 2008

[23] Synopsys Inc., “User Manual for DFT Compiler User Guide Vol. 1: Scan (XG Mode) Version Y-2006.06,“ Synopsys, Inc., 2006.

[24] Synopsys Inc., “Design Compiler User Guide Version Y-2006.06,“ Synopsys, Inc., 2006.

[25] Synopsys Inc., “Astro User Guide Version Y-2006.06,“ Synopsys, Inc., 2006.