Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis

Xiaoxiao Wang, Hassan Salmani and Mohammad Tehranipoor
ECE Department
University of Connecticut

Jim Plusquellic
ECE Department
University of New Mexico

Abstract

This paper addresses a new threat to the security of integrated circuits (ICs). The migration of IC fabrication to untrusted foundries has made ICs vulnerable to malicious alterations, that could, under specific conditions, result in functional changes and/or catastrophic failure of the system in which they are embedded. Such malicious alternations and inclusions are referred to as Hardware Trojans. In this paper, we propose a current integration methodology to observe Trojan activity in the circuit and a localized current analysis approach to isolate the Trojan. Our simulation results considering process variations show that with a very small number of clock cycles the method can detect hardware Trojans as small as few gates without fully activating them. However, for very small Trojan circuits with less than few gates, process variations could negatively impact the detection and isolation process.

1. Introduction

Chip design and fabrication is becoming increasingly vulnerable to malicious activities and alternations with globalization. This has raised serious concerns regarding possible threats to military systems, financial infrastructures, transportation security and even household appliances. An adversary can introduce a Trojan designed to disable and/or destroy a system at some future time (we call it Time Bomb) or the Trojan may serve to leak confidential information covertly to the adversary. Trojans can be implemented as hardware modifications to application specific ICs (ASICs), commercial off the shelf (COTS) parts, microprocessors, or digital signal processors (DSPs), or as firmware modifications, e.g., to field programmable gate arrays (FPGA) bitstreams [1][2].

Unfortunately, the detection of such inclusions is difficult for several reasons: 1) Nanometer IC feature sizes and system complexity make detection through physical inspection and destructive reverse engineering difficult and costly. Moreover, destructive reverse engineering does not guarantee that ICs not destructively inspected are Trojan-free. Additionally, the adversary may insert the Trojan randomly in a large batch of fabricated chips. 2) Trojan circuits are by design activated under very specific conditions, which makes it difficult to fully activate them using random and functional stimuli and detect them using observation points (primary outputs and scan flip-flops). Moreover, existing automatic test pattern generation (ATPG) methods used in manufacturing test for detecting defects do so by operating on the netlist of the Trojan-free circuit specification. Therefore, existing ATPG algorithms cannot target Trojan activation directly.

Trojan detection methods can be applied immediately after the chip is returned to the customer, either as a die on a wafer or as a packaged chip, and/or they can be applied continuously during the lifetime of the system. For the latter case, board level support systems, such as trusted companions, are needed to carry out the monitoring. Although these types of approaches are of interest, the focus of this work is on '*time-zero*' detection methods, i.e., methods applied before the chip is installed in the target system. This phase is referred to as *IC Authentication* that is done after manufacturing testing phase.

1.1 Prior Work

Security has become a new concern in the design and test of chips recently [3][4][5][6]. This trend has become more apparent with the advent of Cryptochips, which implement encryption and decryption algorithms in hardware [7]. Many researchers have been able to show that these chips are highly vulnerable to various power analysis [8][9], timing [10][11], and fault injection [12][13] attacks if not specially designed with countermeasures. If not considered carefully, strong encryption algorithms that would take years to crack by brute force can otherwise be defeated in a manner of weeks, days, or even hours through these side channel attacks. Recently, scan test has become a security risk to the intellectual property on the chip [14][15][16][17]. Such non-invasive attacks have also been used for extracting secret information such as keys used within ICs [3][18]. The Trojan detection is a new topic in hardware security area and there is a very limited prior work in this area. The authors in [19] propose the use of side-channel signals, e.g., transient power supply currents, to identify Trojans in chips. The method uses a global

1550-5774/08 $25.00 © 2008 IEEE
DOI 10.1109/DFT.2008.61

measurement of power supply transient signals to detect the Trojans which makes it difficult to target very small Trojans in presence of process variations.

1.2 Contribution and Paper Organization

Most Trojans inserted into a chip require power supply and ground to operate. The Trojans can be of different types and sizes and their impact on circuit power characteristics could be very large or very small. In this paper, we first develop a multiple supply transient current integration methodology to detect hardware Trojans in integrated circuits. We then develop a Trojan isolation method based on localized current analysis. We measure the current from various power ports 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 [20].

The paper is organized as follows. Section 2 provides a taxonomy for Trojans. Section 3 presents the proposed multiple power supply transient current integration methodology. Section 4 presents the Trojan insertion procedure. The process variations' importance and effects when detecting Trojans will be discussed in Section 5. Section 6 presents the simulation results. Finally, Section 7 will conclude the paper.

2. Taxonomy

In order to develop methods designed to improve IC TRUST, it is essential to first define a taxonomy for Trojans. The Trojan classification scheme that we propose is derived from several fundamental characteristics of Trojans, including their physical, activation and action characteristics. Once a framework is established, we will be able to measure the effectiveness of the detection and isolation methods.

Malicious alternations to the structure and function of a chip can take many forms. We decompose the Trojan taxonomy into three principle categories as shown in Figure 1, i.e., according to their *physical*, *activation* and *action* characteristics. The physical characteristics of a Trojan are further partitioned into four categories; *type*, *size*, *distribution*, and *structure*. Our proposed taxonomy, therefore, describes Trojans using six attributes, including four physical, one activation and one action attribute. Although it is possible for Trojans to be hybrids of this classification, e.g., have more than one activation characteristic, we believe this taxonomy captures the elemental characteristics of Trojans and will be useful for defining the capabilities of various detection strategies.

Trojan Physical Characteristics: The *type* category partitions Trojans into *functional* and *parametric* classes. The functional class includes Trojans that are physically realized through the addition or deletion of transistors or gates, while parametric refers to Trojans that are realized through modifications of existing wires and logic. The thinning of a wire, the weakening of a transistor or any modification of a physical geometry designed to sabotage reliability or increase the likelihood of a functional or performance failure are examples of the latter.

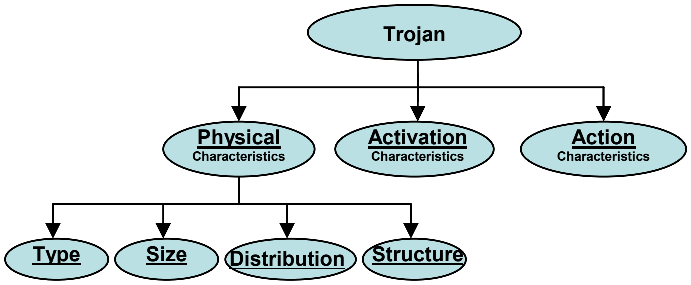

Figure 1. Taxonomy of Trojans.

The *size* category accounts for the number of components in the chip that have been added, deleted or compromised. Size of a Trojan can be an important factor during activation. A smaller Trojan has a higher probability for activation than a Trojan with larger number of inputs. The *distribution* category describes the location of the Trojan in the physical layout of the chip. For example, a *tight distribution* describes a Trojan whose components are topologically close in the layout while a *loose distribution* describes Trojans that are dispersed across the layout of the chip. Finally, the *structure* category describes the change in the layout structure. If the adversary is forced to regenerate the layout to be able to insert the Trojan in the circuitry, then the chip dimensions change. This change could result in different placement for some or all the design components.

Trojan Activation Characteristics: Activation characteristics refer to the criteria that causes the Trojan to become active and carry out its disruptive function. The adversary who inserted the Trojan will make it difficult for the user of the chip to activate it, in an effort to prevent 'accidental' activation and detection during the testing phase(s) of the chip and system. Therefore, activation of a Trojan can be considered a 'rare event' from a statistical perspective.

We use the term *stealthy activation* to describe the adversary's objective in this regard. We partition Trojan activation characteristics into two sub-categories, labeled *Externally-activated* and *Internally-activated*. In Externally-activated category, the Trojan can be activated externally by adversary in his/her time of choosing. This can be done by embedding a receiver or antenna on chip and controlling it through external signals. The Internally-activated category is divided into two subclasses, labeled *Always-on* and *Condition-based*. Always-on, as the name implies, indicates that the Trojan is always active and can disrupt the function of the chip at any time. The Condition-based subclass includes Trojans that are 'inactive' until a specific condition is met.

Trojan Action Characteristics: Action characteristics identify the types of disruptive behavior introduced by the Trojan. We partition Trojan actions into three categories; *Modify-function, Modify-specification,* and *Transmit-info*. As the name implies, the Modify-function class refers to Trojans that change the chip's function through additional logic or by removing or bypassing existing logic. The Modify-specification class refers to Trojans that focus their attack on changing the chip's parametric properties, such as delay. The latter class represents parametric Trojans that modify wire and transistor geometries. Lastly, the Transmit-info class refers to Trojans that transmit key information from design mission mode to an adversary.

3. Current Integration Method

3.1 Trojan Detection

A Trojan, when inserted into a chip, will most likely consume power. However, the Trojan's contribution to the total power consumption of the circuit depends heavily on its size and type. It also depends on its activation, that is, fully activated Trojan can consume more power than that of partially activated. A Trojan inserted in a chip will draw leakage current if it is powered on. Creating switching in the Trojan can further increase the amount of current drawn by the Trojan circuitry. We acknowledge that fully activation of a Trojan using structural and functional patterns would be extremely challenging and prohibitively expensive considering that the size and type of Trojan is unknown to us.

Partial activation of Trojans can be an effective way for Trojan detection and isolation using transient current-based side-channel analysis methods similar to our current integration method. A large number of transitions is generated when applying a pattern to the chip. Some of the Trojan inputs in the chip may also observe the transitions and in turn cause transitions in the Trojan circuitry as well. The switches in the Trojan will increase the local power consumption (i.e. current). The local power refers to the current drawn from the power port near the Trojan circuitry. The more the number of switching on the Trojan inputs and in the Trojan circuitry the larger the transient current. Since small Trojan sizes are expected to be inserted into chips by adversary to reduce the detection capability, the local current impact by Trojan could be more significant than the global current that can be measured only by power pins.

The amount of current a Trojan can draw could be so small that it can be submerged into envelop of noise and process variations effects, therefore, cannot be detected by measurement equipments. However, Trojan detection capability can be greatly improved when measuring currents locally and from multiple power ports/pads. Figure 2 shows our current (charge) integration methodology for detecting hardware Trojans. There are four power ports on the chips. The golden chip can be identified using an exhaustive test for a number of randomly selected chips. It can also be identified using the pattern set that will be used in our current integration method by comparing the results against each other for all the patterns. If the same results are obtained for all the selected chips, they can be identified as Trojan-free. We assume that adversary will insert the Trojans randomly in a selected number of chips. After identifying the golden chips, the worst-case charge will be obtained (dashed-line in the figure) in response to the pattern set. The worst-case charge is based on the worst-case process variations in one of the genuine ICs. Next, the pattern set will be applied to each chip and the current will be measured for each pattern locally via power ports or C4 bumps.

The figure shows the current waveform of *n* number of patterns applied to the chip. The figure also shows the charge variations with time for all the current waveforms obtained after applying the patterns. The charge corresponds to the area produced by each current waveform. $Q_n(t)$ 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 instrumentation. When applying the patterns, the charge increases and is compared continuously against the worst-case charge calculated for golden chips. Once the difference between the two curves ΔQ is greater than Q_{thr} we consider a Trojan is detected. The number of patterns, *n* is expected to very small for large Trojans and large for very small Trojans.

By applying this integration 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 chip's accumulative charge.

Note that in this work, we assume that the IC authentication phase is done after manufacturing test. Therefore, the likelihood of encountering a defect during IC authentication would be very small. The existence of defect depends on the DPPM level for the manufactured chip in the foundry.

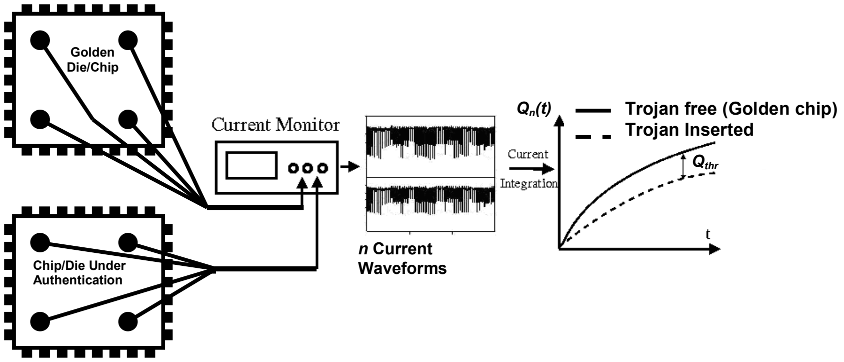

Figure 2. Current (Charge) Integration Method

If $I_{trojan\_free}(t)$ and $I_{trojan\_inserted}(t)$ denote the instantaneous supply current drawn by Trojan-free and Trojan-inserted circuit at time *t*, respectively, then the integrated current at time *t* for Trojan-free and Trojan-inserted circuit ($Q_{trojan\text{-}free}(t)$ and $Q_{trojan\text{-}inserted}(t)$) can be expressed by equations (1) and (2) (note that $dq = I\ .\ dt$)

$$Q_{trojan\text{-}free}(t) = \int I_{trojan\_free}(t)\ .\ dt \tag{1}$$

$$Q_{trojan\text{-}inserted}(t) = \int I_{trojan\_inserted}(t)\ .\ dt = \int (I_{trojan\_free}(t) + I_{trojan}(t))\ .\ dt \tag{2}$$

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.

Since we perform multiple power supply transient current analysis, the proposed integration method can be used for detecting both tight and loose distributed Trojans. During Trojan detection phase, the total supply current is integrated for chip-under-authentication and the golden chip separately. All Trojan gates located on chip will contribute to overall current consumption. Therefore, the total supply current's difference beyond the predefined threshold between the two chips will imply the existence of Trojan. We will show our simulation results in Section 6 for loosely distributed Trojans (e.g. Comparators).

3.2 Trojan Isolation

Trojan isolation process is done after detecting a Trojan in a chip. The Trojan isolation is essential in identifying the location of Trojan and possibly identifying the type of Trojan especially in terms of action characteristics. It is extremely valuable to find out what the adversary intended to carry out with the inserted Trojan.

Trojan isolation process is based on the fact that Trojan gates (similar to circuit gates) will draw more current from their nearest power port therefore more current difference occurs on the power ports near the Trojan gates. To further demonstrate the impacts on local power ports, we have inserted a Trojan (a 3-bit counter, tightly distributed) in ISCAS'89 s38417 benchmark which contains 8709 gates and 1636 FFs. In s38417 benchmark, we have considered 49 (7 × 7) power ports.

We have generated the layout of the circuit and inserted the Trojan circuit in a dead space in the layout and connected the clock to the Trojan. The Trojan was inserted close to power port 17 exactly at the coordinates of (950μm, 100μm) in the physical layout. Figure 3 shows the charge difference (*ΔQ*) of an array of power ports between Trojan-inserted and Trojan-free circuit obtained using post-layout simulation [21]. As seen, the maximum *ΔQ* happens on power port 17. The supply current difference falls drastically on neighboring power ports.

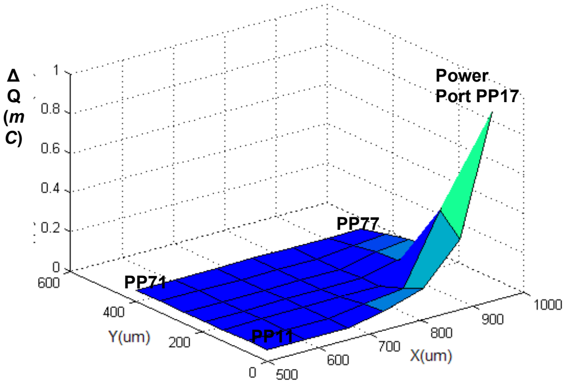

Figure 3. Current difference measured on power port 17

During Trojan isolation process the current of each power port is measured, integrated and compared with golden chip's current integration result separately for each power port. When there is a clear difference (depending on the pre-defined threshold) between the two chips, then the Trojan is assumed to be near the power port. However, if, for example, the Trojan is located right between power ports 13, 14, 23, and 24, then it will impact more than one power port when switching (see Figure 3). By comparing the currents drawn by each power port after applying the patterns, we will be able to identify the location of the Trojan between them. If the adversary distributes the Trojan in the entire circuit, the isolation process will be more difficult since the smaller portion of the Trojan will draw currents from different power ports.

3.3 Pattern Generation and Application

To detect and isolate a Trojan, a pattern set must be generated and applied to the chip during IC authentication step. Since the proposed method measures the current from various power ports, the patterns that generate localized switching would be most effective. However, generating such patterns will be computationally intensive. In this paper, we use random patterns that are effective in generating a large number of transitions in the circuit thus increasing the probability of partial activation of hardware Trojans.

The pattern generation for targeting a fault or defect is fundamentally different from targeting Trojans. For example, when detecting interconnect open defect, we generate patterns such that they target every node in the circuit for an open defect. However, this will not be the case for Trojan. A Trojan cannot be activated by activating a node. A transition on a node does not ensure a gate in the Trojan will be activated. To be able to activate a gate in the Trojan, we need to perform a procedure similar to multiple stuck-at faults [20] by generating switching on all combinations of two nodes assuming that there are two-input gates in the Trojan circuit. This procedure does not seem practical due to very high complexity. As mentioned earlier, the size, type, and location of a Trojan is unknown to us. To improve the probability of detection of a Trojan, it's best to increase number of switching in the circuit.

Another major difference between ATPG for defect/fault and Trojan is that a node is targeted with every pattern for defect/fault-oriented ATPG while a region is targeted using every pattern for Trojan-oriented ATPG. In both case, a large number of patterns must be applied. The total number of patterns to detect all fault depends on the number of nodes in the circuits but there is no limit on the number of patterns for Trojan detection. The number of patterns required to detect Trojans depends on the size and type of Trojans. A sequential Trojan that uses clock continuously consumes more power compared to monitor-like Trojans. Therefore the detection depends on the number of clock cycles needed to reach Q_{thr} charge over the worst-case charge. Note that in this work, there are no logic observation points. The patterns should generate switching in the circuit and the power ports are in fact the observation point for the side-channel signal, here current/charge. Also note that we use primary inputs and scan cells to apply patterns to the circuit. The pattern application is similar to *test-per-clock* [20] where a pattern is applied in every clock cycle. A random bit is shifted into the scan chain to generate a new random pattern in addition to applying a random pattern to primary inputs in every clock cycle. In a test-per-clock approach, the pattern application time will be quite short.

In this work, we apply random patterns to the chips. Some patterns may generate switching at the input of the Trojan and some may not. Those that do not generate a switching, will impact the charge based on the genuine gates switching and process variations. But, those patterns that activate part of the Trojan or its inputs, can have a extra current over the process variations and genuine gates switching current. Also, note that, since we apply the same patterns to Trojan-free and Trojan inserted circuit, the charge induced by genuine gates switching would be same and the difference is in process variation-induced current and Trojan gate switching.

3.4 Trojan Insertion

An adversary can exploit the dead spaces in the physical layout to insert small or large hardware Trojans. In this work, we generate the physical layout for ISCAS'89 s38417 benchmark. We then generate several copies of this benchmark to insert Trojans. In each layout, we use dead spaces to insert Trojan gates/circuitry. We insert two types of Trojans, *Counter* and *Comparator*, in a tightly and loosely distributed fashion, respectively. For distributed Trojan, we utilize small dead spaces to insert Trojan gates and connect them. When inserting Counter, we use those already existed Counters in standard cell library. We place them in available dead spaces in the physical layout. When designing a Comparator, however, we intentionally distribute the gates in difference locations on the layout. In all cases, we ensure not to change the s38417's original layout's form-factor.

We assume that the adversary has the knowledge of IC fabrication and testing, so he/she can design the Trojan circuit such that it will not to be detected during manufacturing test. The adversary is expected to ensure the layout of Trojan-inserted and Trojan-free circuits remain same by avoiding re-designing the physical layout. Any modifications to the layout of the circuit will change the position of cells and makes it easier to be detected, for instance, using circuit delay analysis.

4. Process Variations Impact on Trojan Detection

As technology scales to 45nm and below, the impact of process variations on current/power consumption is expected to be more significant than ever. Therefore, process variations should be considered during Trojan detection methods that rely on side-channel signals. Process variations can either help or harden the Trojan detection process. According to equation (4), which is current drawn by a single gate, decreasing voltage threshold V_{th}, channel length L, as well as oxide thickness T_{ox} will increase gate current. Conversely, increasing V_{th}, L and T_{ox} will decrease gate current consumption (I_D).

$$I_D = \frac{\mu C_{ox} W}{2L}(V_{GS} - V_{th})^2(1 + \lambda V_{DS}) \quad (4)$$

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.
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 two scenarios that help make the Trojan detection process easier are:

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

To generate the worst-case charge, we need to apply the worst-case process corners. Based on the above analysis, process corners that increase current consumption of a Trojan-free chip and decrease current for Trojan-inserted chip are the most difficult scenarios for Trojan detection. Although process variations may decrease the charge difference between the two charge curves (Trojan-inserted and Trojan-free), the current integration method would still be effective in detecting small Trojans since the integration effect can successfully increase the gap between the two curves with applying more patterns.

5. Simulation Results

The current integration method is applied for detecting Trojans inserted into s38417 benchmark. First, we generate 7 layouts for original s38417 benchmark using Synopsys physical design tools [21] in 180*nm* technology [22]. 1-bit, 3-bit, 7-bit, 9-bit Counter and 3-input, 5-input, 20-input Comparator Trojans are inserted into these seven layouts separately (i.e. only one Trojan in each layout). Table 1 shows the type, size, distribution and structure of the inserted Trojans in the layout. We also investigate the impact of process variations on Trojan detection. The wors-case process variations that we consider for a genuine IC during our simulation are shown in Table 2.

We first start with the results obtained from the circuits containing Counter Trojans. Figure 4 shows the simulation results obtained using Synopsys Nanosim [21] for s38417 containing a 1, 3, 7, and 9-bit Counters. The patterns are shifted into the scan chain with a frequency of 100MHz. As seen in the figure, for all four Trojans, after applying 15 clock cycles (equals 15 patterns), $\Delta Q >> Q_{thr}$ where Q_{thr} is considered to be in the range of μC, which is easily detectable using measurement devices. The 1-bit Counter used here is a flip-flop with self loopback. The isolation method by measuring current on each power port would also be effective in detecting such Trojans. In general, detecting a Counter would be easier than a combinational Trojan since the Counter continuously receive the clock and consumes power. No process variations were considered for the results shown in Figure 4, although the process variations would not be significant enough to change the detection outcome for such Trojans.

Table 1. Trojan characterization

Trojan	Type	Size	Distribution	Structure
Counter	1-bit	0.04%	tight	no-change
	3-bit	0.10%	tight	no-change
	7-bit	0.31%	tight	no-change
	9-bit	0.42%	tight	no-change
Comparator	3-input	0.02%	loose	no-change
	5-input	0.04%	loose	no-change
	20-input	0.15%	loose	no-change

Table 2. Worst-case process variations applied to Trojan-free circuit during Trojan detection

	Inter-die	Intra-die
Threshold Voltage (V_{th})	5%	20%
Channel Length (L)	2%	8%
Oxide Thickness (T_{ox})	1%	4%

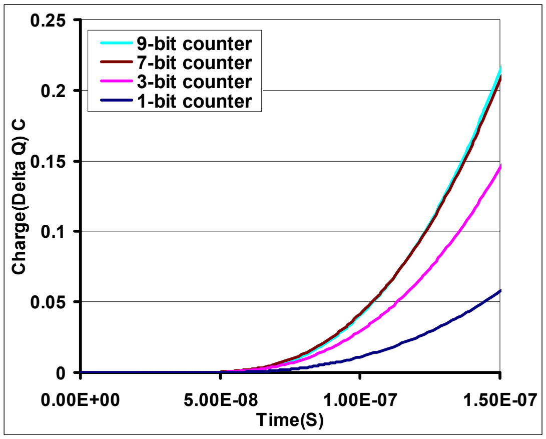

Figure 4. Charge measurement for s38417 with four Counter Trojans inserted into s38417

Figure 5 shows the simulation results for the circuit containing 3-bit Counter while considering the process variations for both Trojan-inserted and Trojan-free circuits. The process variations used in the Trojan-free circuit increases the current in the Trojan-free circuit while the variations used in the Trojan-inserted circuit reduced the total current. As seen, the Trojan-inserted circuit with process variations is still consuming more current when compared to the Trojan-free circuit with process variations. Our simulation for 5, 7, and 9-bit Counters have also shown similar results. The charge induced by worst-case process variations in presence of Trojans was still below the amount of charge contributed by the Trojans. Our simulation results showed that for the smaller Trojans, such as 2-bit and 1-bit Counters, the detection was not possible when considering worst-case process variations. However, we were able to detect 1-bit Counter when considering average process variations.

Figure 6 shows the simulation results when inserting a 20-input Comparator in s38417 circuit. The Comparator circuit is connected to 20 randomly select nodes in the circuit. This type of Trojan falls into the category of "loose distribution" and requires activation to generate transient current since it is a combinational circuit. Since fully activation is very time consuming and prohibitively expensive, we rely on partial activation of such hardware Trojan by applying random patterns. Figure 6 shows the results after applying random patterns to the circuit with and without Trojan considering process variations. As shown, the Trojan can be easily detected using the method in presence of worst-case process variations considered for Trojan-free circuit to identify the worst-case charge for genuine ICs. Lower variations were considered for Trojan-inserted circuit.

However, the results shown in Figure 7 shows the increase in charge difference between the two circuits, Trajan-free and Trojan-inserted. As seen, the current difference is significantly greater than Q_{thr} after applying only 8 random patterns. This shows that the patterns were able to partially activate the Trojan. We have also simulated the

Trojan-inserted circuit with the worst-case process variation but we were not able to clearly detect the Trojan. However, we acknowledge that using a lower process variation could potentially detect the Trojans. This was the case for 3-input Comparator as well. To further increase the probability of detection, more test patterns must be applied. The application time depends when the Trojan-inserted circuit results falls outside the Trojan-free circuit with worst-case process variations.

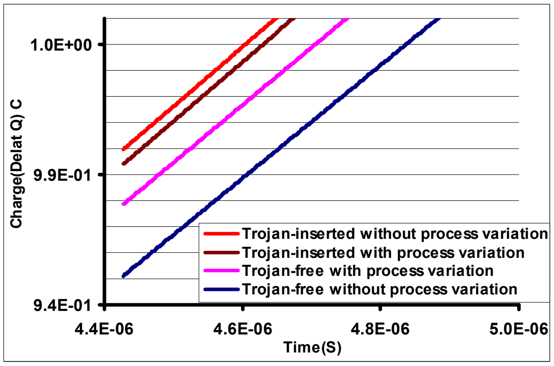

Figure 5. Charge measurement for s38417 with 3-bit Counter considering the worst-cased process variations for Trojan-free circuit

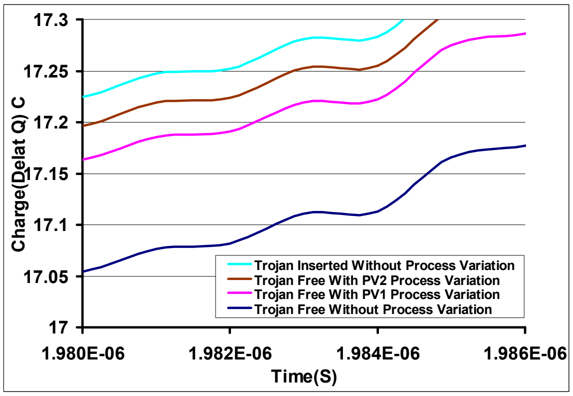

Figure 6 Charge measurement for s38417 with 20-input Comparator (here, PV2 represents the worst-case variations and PV1 represents lower variations)

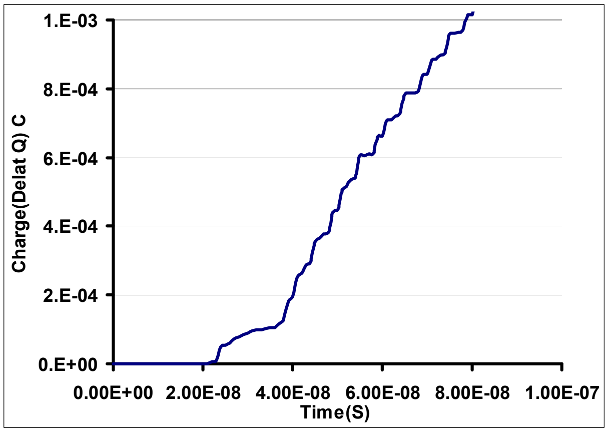

Figure 7. Charge measurement for s38417 with 5-input Comparator with no process variations

6. Conclusions and Future Work

We have presented a new current (charge) integration methodology for Trojan detection and isolation. The method measures the current locally from the on-die power ports. Comparing the results obtained for golden chips against the chip-under-authentication, the Trojan can be detected if the current integration results fall outside the golden chip results. We have shown that our method can easily detect Trojans as small as 0.1% the circuit area. We plan to improve the quality of test patterns using the layout-aware test pattern generation procedure we are developing. We also plan to deal with process variation impact in more accurate way by performing Monte Carlo simulation for all Trojan-free and Trojan-inserted circuits and measure the effectiveness of the proposed method.

5. AKNOWLEDGEMENT

The work of Xiaoxiao Wang, Hassan Salmani and Mohammad Tehranipoor was supported in part by NSF 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] http://www.darpa.mil/mto/solicitations/baa07-24/index.html
[3] B. Yang, K. Wu, and R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard," in *Proc. of the IEEE Int. Test Conf. (ITC)*, pp. 339.344, 2004.
[4] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," in *Proc. of the 17th Intl. Conf. on VLSI Design*, pp. 605.611, 2004.
[5] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, and S. Ravi, "Security as a New Dimension in Embedded System Design," in *Proc. of the 41st Annual Conference on Design Automation*, pp. 753.760, June 2004.
[6] K. Tiri and I. Verbauwhede, "A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs," in *Proc. of Design, Automation and Test in Europe*, pp. 58.63, Mar. 2005.
[7] K. Hafner, H. C. Ritter, T. M. Schwair, S.Wallstab, M. Deppermann, J. Gessner, S. Koesters,W.-D. Moeller, and G. Sandweg, "Design and Test of an Integrated Cryptochip," *IEEE Design and Test of Computers*, pp. 6.17, Dec. 1991.
[8] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Lecture Notes in Computer Science*, vol. 1666, pp. 388.397, 1999.
[9] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 3, pp. 179.188, 2004.
[10] P. C. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems," *Lecture Notes in Computer Science*, vol. 1109, pp. 104.113, 1996.
[11] J. Kelsey, B. Schneier, D.Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," in *Proc. of the European Symposium on Research in Computer Security*, pp. 97.110, Sep. 1998.
[12] D. Boneh, R. A. Demillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," *Lecture Notes in Computer Science*, vol. 1233, pp. 37.51, 1997.
[13] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *Lecture Notes in Computer Science*, vol. 1294, pp. 513.527, 1997.
[14] R. Goering, "Scan Design Called Portal for Hackers," Oct. 2004. [Online]. Available: http://www.eetimes.com/news/design/showArticle.jhtml?articleID=51200154
[15] S. Scheiber, "The Best-Laid Boards," Apr. 2005. [Online]. Available: http://www.reed-electronics.com/tmworld/article-/CA513261.html
[16] J. Lee, M. Tehranipoorand J. Plusquellic, "A Low-Cost Solution for Protecting IPs Against Side-Channel Scan-Based Attacks," in Proc.*VLSI Test Symposium (VTS'06)*, 2006.
[17] J. Lee, M. Tehranipoor, C. Patel and J. Plusquellic, "Securing Scan Design Using Lock & Key Technique," in *Proc. Int. Symp. on Defect and Fault Tolerance in VLSI Systems (DFT'05)*, 2005.
[18] D. H´ely, M.-L. Flottes, F. Bancel, B. Rouzeyre, N. B´erard, and M. Renovell, "Scan Design and Secure Chip," in *Proc. of the 10th IEEE Intl. On-Line Testing Symposium*, 2004.
[19] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, "Trojan Detection using IC Fingerprinting", Symposium on Security and Privacy, 2007, pp. 296 - 310.
[20] M. Bushnell, V. Agrawal, *Essentials of Electronics Testing*, Kluwer Publishers, 2000.
[21] Synopsys, "User Manual for SYNOPSYS Toolset Version 2005.09," Synopsys, Inc., 2005.
[22] http://crete.cadence.com, "0.18m standard cell GSCLib library version 2.0," Cadence, Inc., 2005.