Multiple-Parameter Side-Channel Analysis: A Non-Invasive Hardware Trojan Detection Approach

Seetharam Narasimhan[1], Dongdong Du[1], Rajat Subhra Chakraborty[1], Somnath Paul[1], Francis Wolff[1], Christos Papachristou[1], Kaushik Roy[2] and Swarup Bhunia[1,a]
[1]Case Western Reserve University, Cleveland, Ohio, USA
[2]Purdue University, West Lafayette, Indiana, USA
Email: *sxn124@case.edu*

***Abstract*—Malicious alterations of integrated circuits during fabrication in untrusted foundries pose major concern in terms of their reliable and trusted field operation. It is extremely difficult to discover such alterations, also referred to as "hardware Trojans" using conventional structural or functional testing strategies. In this paper, we propose a novel non-invasive, multiple-parameter side-channel analysis based Trojan detection approach that is capable of detecting malicious hardware modifications in the presence of large process variation induced noise. We exploit the intrinsic relationship between dynamic current (I_{DDT}) and maximum operating frequency (F_{max}) of a circuit to distinguish the effect of a Trojan from process induced fluctuations in I_{DDT}. We propose a vector generation approach for I_{DDT} measurement that can improve the Trojan detection sensitivity for arbitrary Trojan instances. Simulation results with two large circuits, a 32-bit integer execution unit (IEU) and a 128-bit Advanced Encryption System (AES) cipher, show a detection resolution of 0.04% can be achieved in presence of $\pm 20\%$ parameter (V_{th}) variations. The approach is also validated with experimental results using 120nm FPGA (Xilinx Virtex-II) chips.**

***Index Terms*—Hardware Trojan, Side channel analysis, Multiple-parameter test**

I. Introduction

Integrated circuits (ICs) fabricated in untrusted foundries are vulnerable to malicious modifications in hardware during fabrication [1], [2]. Such malicious changes, also referred to as *hardware Trojans*, can give rise to undesired functional behavior of a chip. This can potentially have serious consequences in critical applications spanning the domains of communications, space, military and nuclear facilities. An intelligent adversary will try to hide any tampering in the functionality of an IC in a way that evades conventional post-manufacturing test. Intuitively, it means that the adversary would ensure that the effect of such a tampering is triggered and/or manifested under very rare circuit conditions [2].

We refer to the condition of Trojan activation as the *trigger condition* and the node affected by the Trojan as the *payload* for the Trojan. *Combinational Trojans* consist solely of combinational gates and are activated when a particular set of logic conditions is satisfied at their trigger nodes. *Sequential Trojans* are activated due to a sequence of rare events on internal circuit node(s). Fig. 1 shows the high-level structure of a Trojan and provides examples of combinational and sequential Trojans. The malicious effects of the Trojan payloads can be both *passive* (e.g. leakage of secret information) and *active* (e.g. destructive alteration of original functionality).

Existing approaches for hardware Trojan detection can be broadly classified into: 1) logic testing and 2) side-channel analysis approaches. In logic testing approach, directed structural or functional tests are generated [2], [3] to activate rare events in the circuit and propagate the malicious effect in logic values to primary outputs. Such approaches can be effective in detecting ultra-small Trojans (typically a few gates in size) reliably under large process variations. The main challenges with logic testing approaches, however, are the difficulty to trigger and observe a Trojan, particularly the complex sequential Trojans, and the inordinately large number of possible Trojan instances an adversary can exploit [3]. On the other hand, side-channel analysis approaches depend on measurement of physical "side-channel" parameters like power signature [4]–[6] or delay [7], [8] of an IC in order to identify a structural change in the design. Such approaches have the advantage that they do not require triggering a malicious change and observing its impact at the output nodes. However, reliable detection of Trojan circuits under large process induced variations (e.g. 20X power and 30% delay variations in 180nm technology [9]) emerges as a major challenge for side-channel analysis. Existing side-channel approaches, however, suffer from one or more of the following shortcomings: 1) they do not scale well with increasing process variations; 2) they consider only die-to-die process variations and do not consider local within-die variations; and 3) they require design modifications which incur considerable design overhead and/or can potentially be compromised by an adversary.

In this paper, we propose a novel multiple-parameter side-

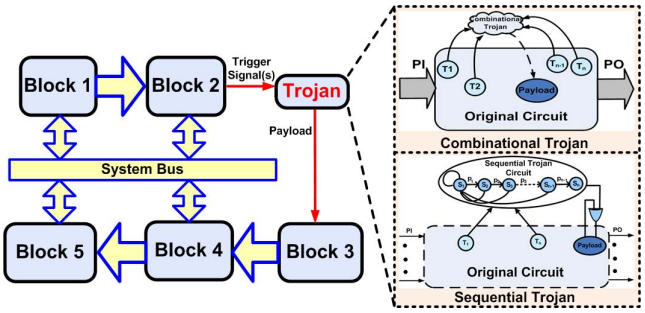


Fig. 1. Examples of different (*combinational* and *sequential*) Trojans incorporated in a design.

[a]The work is funded by DoD grant FA-8650-08-1-7859.

channel analysis based Trojan detection approach for effective detection of complex Trojans under large process-induced parameter variations. The concept takes its inspiration from multiple-parameter testing [10], which considers the correlation of the leakage current (I_{DDQ}) to the maximum operating frequency (F_{max}) of the circuit in order to increase the sensitivity of I_{DDQ} testing to distinguish fast, intrinsically leaky ICs from defective ones. Instead of using only the power signature (which is highly vulnerable to parameter variations [4], [9]), the proposed side-channel approach achieves high signal-to-noise ratio (SNR) using the intrinsic dependencies between active-mode supply current (I_{DDT}) and maximum operating frequency (F_{max}) of a circuit to identify the ICs affected with malicious hardware in a non-invasive manner. We provide a theoretical analysis regarding the effect of various components of process variations on the relationship between I_{DDT} and F_{max}. The proposed approach requires no modification to the design flow and incurs no hardware overhead. In order to detect small Trojans (of size $< 0.1\%$ of total area) in large multi-module circuits, we investigate a test generation approach to improve the detection sensitivity. It partitions a design into modules and then employs a statistical test generation algorithm to each module in order to maximize the activity in a given module while minimizing the activity of other regions. We also investigate the use of the quiescent current (I_{DDQ}) to increase confidence. We provide both simulation verification and hardware validation (with experimental measurements for FPGA chips) of the proposed approach.

The rest of the paper is organized as follows. Section II presents the proposed multi-parameter Trojan detection methodology including theoretical analysis. Section III presents the simulation as well as measurement results using Xilinx Virtex-II FPGAs for a test circuit and different Trojan instances. Section IV concludes the paper.

II. Methodology

In Trojan detection using side-channel analysis, we need to distinguish between the Trojan contribution and process noise by comparing the side-channel information for the golden and the untrusted ICs. Due to process variations, it is extremely challenging to detect the existence of a Trojan by considering F_{max} or I_{DDT} individually. Average I_{DDT} and F_{max} results for an 8-bit ALU circuit (c880 from ISCAS-85 benchmark suite) are plotted in Fig. 2(a) and Fig. 2(b) for 100 chips which lie at different process corners, assuming only die-to-die or *inter-die* variations in transistor threshold voltage (V_{th}), where all transistors in a die experience similar variations. The spread in I_{DDT} due to variation easily masks the effect of a combinational Trojan (an 8-bit comparator), making it infeasible to isolate from process noise, as shown in Fig. 2(a). To overcome this issue, the intrinsic relationship between I_{DDT} and F_{max} can be utilized to differentiate between the original and tampered versions. The plot for I_{DDT} vs. F_{max} for the ISCAS-85 circuit c880 is shown in Fig. 2(c). It can be observed that two chips (e.g. $Chip_i$ and $Chip_j$) can have the same I_{DDT} value, one due to presence of Trojan and the other due to process variation. By considering only one side-channel parameter, it is not possible to distinguish between these chips. However, the correlation between I_{DDT} and F_{max} can be used to distinguish malicious changes in a circuit under process noise. The presence of a Trojan will cause the chip to deviate from the trend line. A Trojan will cause variation in I_{DDT}, while it will not have similar effect on F_{max} as induced by process variation - i.e. the expected correlation between I_{DDT} and F_{max} will be violated by the presence of a Trojan.

In the proposed multiple-parameter approach, F_{max} is used for calibrating the process corner of a chip. In practice, the delay of any path in the circuit can be used for this purpose, making it difficult for an attacker to know in advance which path delay will be used for calibrating process noise. Since a typical design will have exponentially large number of paths (as a function of the number of circuit nodes), it is infeasible for an attacker to manipulate all circuit paths. Furthermore, even if the particular path used for process corner calibration is guessed correctly by the attacker, a Trojan is likely to increase both delay and activity of the path on which it is inserted. Hence, a chip containing the Trojan will deviate from the expected I_{DDT} vs. F_{max} trend line, where both current and frequency increase or decrease simultaneously. From Fig. 2(c) it can be observed that the difference in the I_{DDT} values between a tampered and a golden IC increases with operating frequency. Hence, we cannot use a fixed threshold value to distinguish the Trojan effect from process noise at all corners.

Fig. 2(d) shows the effect of random intra-die process variations on the I_{DDT} and F_{max} values for 1000 instances of the c880 circuit with and without Trojan. We performed Monte Carlo simulations in HSPICE using inter-die ($\sigma = 10\%$) and intra-die ($\sigma = 6\%$) variations in V_{th}. The trend line is obtained by using polynomial curve fitting of order three in

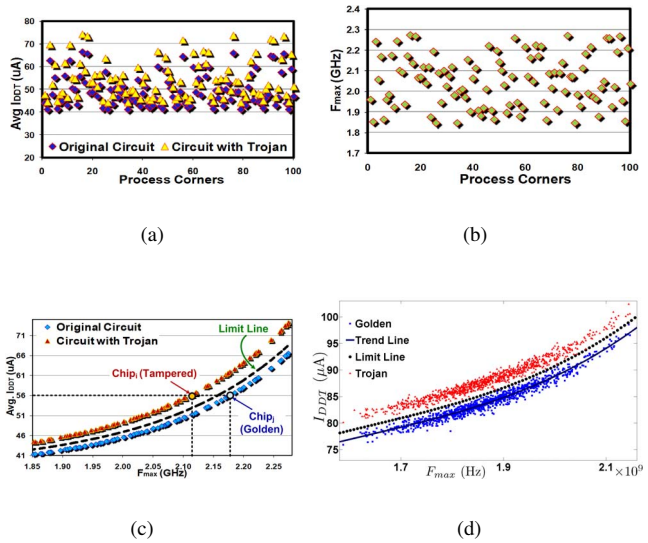


Fig. 2. (a) Average I_{DDT} values at 100 random process corners (with maximum variation of $\pm 20\%$ in inter-die V_{th}) for c880 circuit. The impact of Trojan (8-bit comparator) in I_{DDT} is masked by process noise. (b) Corresponding F_{max} values. (c) The F_{max} vs. I_{DDT} plot shows the relationship between these parameters under inter-die process variations. Trojan-inserted chips stand out from the golden trend line. (d) The approach remains effective under both inter-die and random intra-die process variations. A limit line is used to account for the spread in I_{DDT} values from the golden trend line.

MATLAB, which matches the trend obtained by considering only inter-die process variation effects. We observe that there is a spread in the values from the trend line due to random intra-die variations, but the spread is much less compared to the spread in individual side-channel parameters alone, because we consider the multiple-parameter relationship.

By computing the spread in I_{DDT} values for a given F_{max}, corresponding to a particular inter-die process corner, we can estimate the sensitivity of the approach in terms of Trojan detection. Any Trojan which consumes a current less than the amount of spread will remain undetected. The limit line is obtained by scaling the trend line by a *spread factor*, which is computed using the mean and standard deviation of the spread in I_{DDT} values for a given F_{max} for the sample of ICs.

A. Theoretical Analysis

The basic idea of the multiple-parameter approach is to exploit the correlated changes in I_{DDT} and F_{max} with process variations. For a short channel transistor, the ON current [11] of a switching gate can be expressed as:

$$I_g = k_g(V_{DD} - V_{th})^{\alpha} \tag{1}$$

where V_{DD} is the supply voltage, α is the *velocity saturation index* with $1 \leq \alpha \leq 2$, V_{th} is the transistor *threshold voltage*, and k_g is a gate-dependant constant. Consider the i-th IC from a lot of manufactured ICs. Then, V_{th} can be expressed as the sum of the *nominal* threshold voltage (V_T), the *inter-die* component of variation (ΔV_{Ti}) for the i-th IC, and Δv_{Tg}, the *random* component of variation. The ΔV_{Ti} value is common for every device in the i-th IC, while the Δv_{Tg} value varies from gate to gate. Eqn. (1) can be re-written as:

$$I_g = k_g(V_{DD} - V_T - \Delta V_{Ti})^{\alpha} \left[1 - \frac{\Delta v_{Tg}}{V_{DD} - V_T - \Delta V_{Ti}}\right]^{\alpha} \tag{2}$$

Expanding binomially, assuming $\dfrac{\Delta v_{Tg}}{V_{DD} - V_T - \Delta V_{Ti}} \ll 1$ and discarding higher order terms, the above equation can be approximated as:

$$I_g \approx (V_{DD} - V_T - \Delta V_{Ti})^{\alpha} \left[k_g - c_i \cdot k_g \cdot \Delta v_{Tg}\right] \tag{3}$$

where $c_i = \dfrac{\alpha}{V_{DD} - V_T - \Delta V_{Ti}}$ is a constant that depends on the IC being considered. Summing over all the switching gates in the IC, the total transient current of the i-th IC is given by:

$$I_{\text{ddt,i}} = \sum_{g \in \text{IC}_i} I_g \approx (V_{DD} - V_T - \Delta V_{Ti})^{\alpha} \left[k_{av} n_{\text{tot,i}} - c_i \sum_{g \in \text{IC}_i} k_g \Delta v_{Tg}\right] \tag{4}$$

where $k_{av} \cdot n_{\text{tot,i}} = \sum_{g \in \text{IC}_i} k_g$ and $n_{\text{tot,i}}$ is the total number of switching gates in the IC. The term $\sum_{g \in \text{IC}_i} k_g \Delta v_{Tg}$ represents the sum of several random variables, each distributed with mean $\mu = 0$ and variance (say) σ^2. Hence, by the *Central Limit Theorem*, their sum follows a Normal distribution with mean $\mu = 0$ and a reduced variance $\frac{\sigma^2}{n_{\text{tot,i}}}$, and is approximately zero. Hence, the above equation can be approximated by:

$$I_{\text{ddt,i}} \approx k_{av} \cdot n_{\text{tot,i}} \cdot (V_{DD} - V_T - \Delta V_{Ti})^{\alpha} \tag{5}$$

On the other hand, the gate delay can be expressed as:

$$t_{dg} = \beta_g (V_{DD} - V_{th})^{-\alpha} \tag{6}$$

where β_g is another gate-dependant constant. Applying the same approximations, the delay of the gate is given by:

$$t_{dg} \approx (V_{DD} - V_T - \Delta V_{Ti})^{-\alpha} \left[\beta_g + \beta_g c_i \Delta v_{Tg}\right] \tag{7}$$

Summing the delays for the gates on the critical path of the i-th IC:

$$T_{\text{crit,i}} = \sum_{g \in P_{\text{crit,i}}} t_{dg} \approx \beta_{av} \cdot n_{\text{crit,i}} \cdot (V_{DD} - V_T - \Delta V_{Ti})^{-\alpha} \tag{8}$$

where $n_{\text{crit,i}}$ is the number of gates on the critical path $P_{\text{crit,i}}$ of the i-th IC. Hence, the maximum operating frequency of the i-th IC is given by:

$$f_{\text{max,i}} = \frac{1}{T_{\text{crit,i}}} \approx \frac{1}{\beta_{av} n_{\text{crit,i}}} \cdot (V_{DD} - V_T - \Delta V_{Ti})^{\alpha} \tag{9}$$

Combining equations (5) and (9), the relationship between $I_{\text{ddt,i}}$ and $f_{\text{max,i}}$ is given by:

$$\frac{I_{\text{ddt,i}}}{f_{\text{max,i}}} \approx k_{av} \cdot \beta_{av} \cdot n_{\text{tot,i}} \cdot n_{\text{crit,i}} \tag{10}$$

This shows that the relationship between the transient switching current and the maximum operating frequency of an IC at different process corners is linear, based on first-order approximation. In the presence of a Trojan circuit in the i-th IC with $n_{\text{trojan,i}}$ switching gates, the value of the transient current changes to:

$$I_{\text{ddt,i,trojan}} \approx k_{av} \cdot (n_{\text{tot,i}} + n_{\text{trojan,i}}) \cdot (V_{DD} - V_T - \Delta V_{Ti})^{\alpha}, \tag{11}$$

while the expression for the maximum operating frequency remains unchanged, if the Trojan is not inserted on the critical path. Hence, for the i-th IC, in the presence of Trojan, the relationship between $I_{\text{ddt,i}}$ and $f_{\text{max,i}}$ changes to:

$$\frac{I_{\text{ddt,i,trojan}}}{f_{\text{max,i}}} \approx k_{av} \cdot \beta_{av} \cdot (n_{\text{tot,i}} + n_{\text{trojan,i}}) \cdot n_{\text{crit,i}} \tag{12}$$

Comparing equations (10) and (12), we observe that the primary effect of the inserted Trojan is the change in the slope of the linear relationship between the transient current and the maximum operating frequency in a tampered IC.

The I_{DDT} vs. F_{max} relationship for a Trojan-free design can be determined either at design time by simulation or by monitoring a number of golden ICs. Once the relationship is determined, we need to define the *limit line* that distinguishes variation-induced shift from Trojan-induced one. Judicious selection of the limit line should minimize the probability of false negatives as well as take into consideration other design marginalities (such as cross talk and power supply noise).

The detection sensitivity of the proposed approach reduces with decreasing Trojan size and increasing circuit size. In order to extend the approach for detecting small sequential/combinational Trojans in large circuits (with $> 10^5$ transistors), we need to improve the SNR using appropriate side-channel isolation techniques. In a single V_{th} (or F_{max}) point, the sensitivity can be expressed as:

$$Sensitivity = \frac{I_{tampered} - I_{original}}{I_{original}} \times 100\% \tag{13}$$

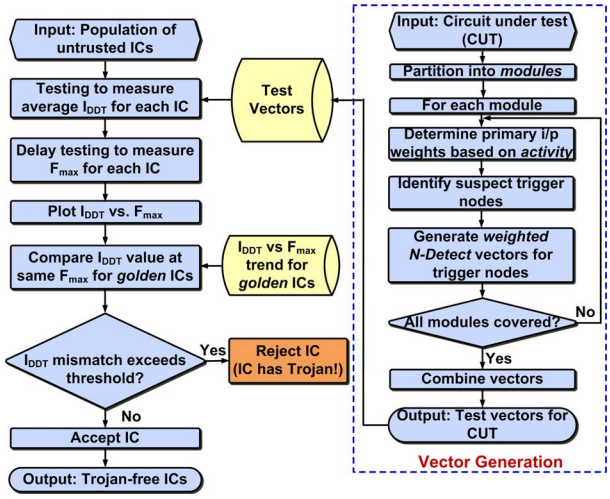


Fig. 3. Major steps in the multi-parameter based Trojan detection approach.

Clearly, the sensitivity can be improved by increasing the current contribution of the Trojan circuit relative to that of the original circuit. Next, we describe a test generation technique used to reduce $I_{original}$ and increase its difference from $I_{tampered}$.

B. Test Vector Selection

The goal of our test generation approach is to maximize the contribution of arbitrary Trojan instances in supply current while minimizing the effect of background current. To achieve this, first, we partition a multi-module design into non-overlapping functional blocks. Any large functional block is further partitioned using a conventional *hypergraph partitioning* step. We then consider one block at a time. We use connectivity analysis and simulations with random vectors to identify a set of random input patterns S, which can maximize the switching activity in the partition, while the activity in the other modules is minimized. Then, we apply a modified version of the statistical test generation technique proposed in [3] to each block which generates the modified set of patterns S' starting from S. The technique ensures that the test set (S') increases the activity in an arbitrary Trojan circuit. Fig. 3 illustrates the overall methodology for the proposed multiple-parameter Trojan detection technique, along with the major steps of the test vector generation algorithm. For each IC from a population of untrusted ICs, the dynamic current

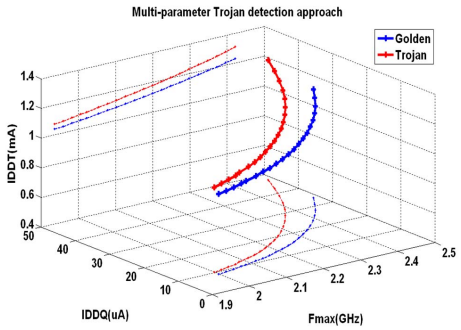


Fig. 4. The correlation among I_{DDT}, I_{DDQ} and F_{max} can be used to improve Trojan detection confidence.

(I_{DDT}) values are collected for a pre-defined set of test vectors. The test set is generated with the vector generation algorithm. The operating frequencies (F_{max}) for these ICs are determined using structural or functional delay testing approach. Next, average I_{DDT} vs. F_{max} measurements for the untrusted ICs are compared against that of a golden IC for each test pattern. Considerable deviation in the I_{DDT} vs. F_{max} space allows us to identify a Trojan by effectively removing the contribution of process noise.

C. Use of Other Side-channel Parameters

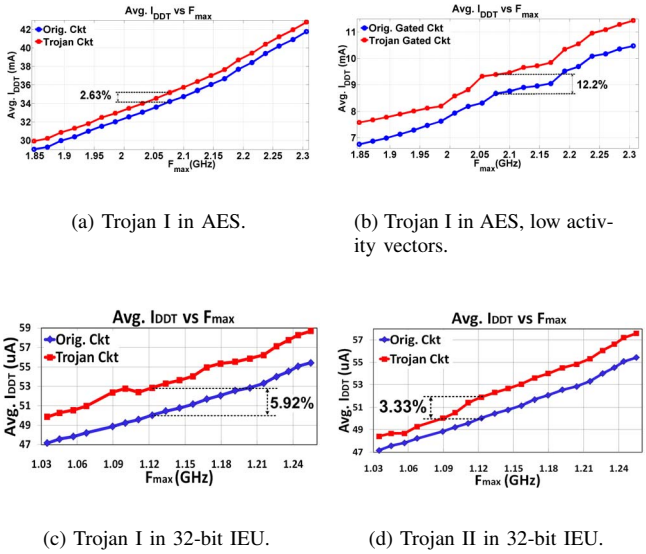
Besides I_{DDT} and F_{max}, other circuit parameters such as quiescent or leakage current (I_{DDQ}) can also be used to increase the confidence level. Apart from contributing to the dynamic current (I_{DDT}), a Trojan will also contribute to the leakage current (I_{DDQ}). Moreover, similar to I_{DDT}, the value of I_{DDQ} increases monotonically with the F_{max} for a given design from one process corner to another [10]. Thus any decision derived from studying the I_{DDT} vs. F_{max} relation can be reinforced by observing the I_{DDQ} vs. F_{max} relation for the same set of ICs. For example, if one of the ICs is observed to have considerably larger I_{DDT} and I_{DDQ} values but smaller F_{max} compared to the other, then it is highly likely to be due to a Trojan intrusion. To understand the joint dependence of the three variables, we simulated the c880 circuit with and without an 8-bit comparator Trojan. Fig. 4 shows a 3-D plot of I_{DDT}, I_{DDQ} and F_{max}, with projections on the I_{DDQ}–F_{max} and I_{DDT}–F_{max} planes. We can observe that a Trojan instance clearly isolates a chip in the multiple-parameter space from process induced variations.

III. Results

A. Simulation Verification

1) Test Setup: We used two test cases to validate the proposed Trojan detection approach: 1) an AES cipher circuit with an equivalent area of slightly over 25,000 two-input NAND gates (i.e $> 10^5$ transistors) and about 30% of the total area contributed by memory elements and 2) a 32-bit pipelined Integer Execution Unit (IEU) with about 20,000 two-input gates. We introduced four types of Trojan circuits in the AES core, with each Trojan type having an area an order of magnitude smaller than the previous type. Trojan I, II and III are sequential Trojans, containing 24, 10 and 3 flip-flops, respectively, clocked by rare events in internal node values. Trojan IV is a combinational comparator which triggers a malfunction when a particular rare 8-bit value is observed on an internal bus. Both designs were synthesized using Synopsys Design Compiler and mapped to a LEDA library. Circuit simulations were carried out for the 70nm *Predictive Technology Model* (PTM) using the Synopsys *Nanosim* power simulator [12]. To consider the effect of process variations, we used $\pm 20\%$ variation over the nominal V_{th} in our simulations.

2) Results: Fig. 5(a) shows a plot of I_{DDT} vs. F_{max} for the AES circuit, with and without Trojan. From this plot, it is observed that the current differential due to the Trojan circuit is only 2.63% at different process corners. For smaller Trojan circuits (Trojan II-IV), this difference can be less prominent



(a) Trojan I in AES.

(b) Trojan I in AES, low activity vectors.

(c) Trojan I in 32-bit IEU.

(d) Trojan II in 32-bit IEU.

Fig. 5. I_{DDT} vs. F_{max} relationship for both golden and tampered AES and IEU circuits showing the sensitivity of our approach for detecting different Trojan circuits.

and is, therefore, likely to be masked by process noise or design marginalities. Fig. 5(b) shows the average I_{DDT} vs. F_{max} plots for Trojan I, with proper test vector selection which increases the sensitivity from 2.63% (Fig. 5(a)) to 12.2%. The sensitivity for different Trojan sizes is shown in Table I. Fig. 5(c) and 5(d) show I_{DDT} vs. F_{max} trends for the 32-bit IEU circuit, which shows sensitivity reduction with decrease in Trojan size. Fig. 6 shows the results of performing Monte Carlo simulations for 1000 instances of the 32-bit IEU circuit with and without Trojan IV inserted. Here, we consider both die-to-die and within-die variations as well as uncorrelated variations between NMOS and PMOS threshold voltages. Using a 20% sensitivity limit line, we obtain 99.3% Trojan detection accuracy, with 0.3% false alarms. Hence, the multiple-parameter approach is shown to work even under random process variation effects on top of inter-die variations.

B. Hardware Validation

1) Test Setup: Hardware validation of the proposed multi-parameter approach was performed using an FPGA-platform where FPGA chips were used to emulate the ASIC scenario. We wanted to observe the effectiveness of the proposed approach to isolate the Trojan effect in presence of process variations, when a golden design and its variant with Trojan are mapped to the FPGA devices. Such an FPGA-based test setup provides a convenient platform for hardware validation using different Trojan types, sizes and even different designs.

TABLE I
TROJAN DETECTION SENSITIVITY FOR DIFFERENT TROJAN SIZES IN AES.

Trojan Type	Trojan Size	Sensitivity	
		high act. vectors	low act. vectors
I (seq, 24-FF)	1.10%	2.63%	12.20%
II (seq, 10-FF)	0.40%	1.70%	8.60%
III (seq, 3-FF)	0.11%	0.81%	3.53%
IV (comb, 8-bit)	0.04%	0.23%	1.12%

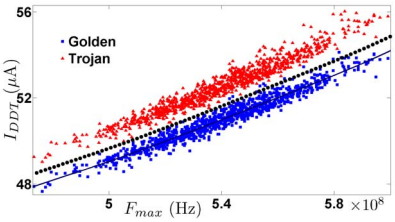
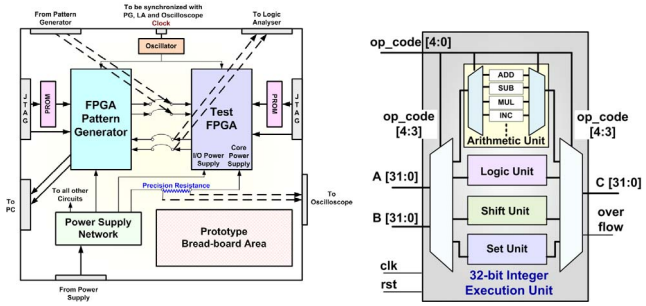


Fig. 6. Effect of random process variations is observed by performing Monte Carlo simulations with inter-die $\sigma = 10\%$ and random intra-die $\sigma = 6\%$ for the 32-bit IEU circuit with Trojan IV inserted. Using a 20% sensitivity limit line to accommodate for the random process variation effects, we can obtain 99.3% detection accuracy and limit the false alarms to 0.3%.

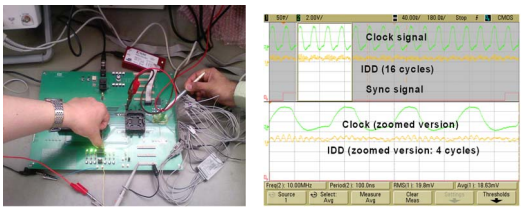
The selected FPGA device was Xilinx Virtex-II XC2V500 fabricated in 120nm CMOS technology. We designed a custom test board with socketed FPGAs for measuring current from eight individual supply pins as well as the total current, using 0.5Ω precision current sense resistors. The test circuit was the 32-bit IEU with a 5-stage pipelined multiplier which has a logic utilization of 90% of the FPGA slices. The Trojan circuit was a sequential circuit (input-triggered counter) with different number of flip-flops. I_{DDT} was monitored for two types of input vectors: those which performed low-activity logic operations and those which performed high-activity multiplication operations. The Trojan size was varied from 256 (1.76% of design size) to 4 (0.03%) flip-flops.

In order to measure I_{DDT}, we measured the voltage drop across the sense resistor, using high-side current sensing strategy. To increase accuracy of measurements amidst measurement noise, the sense resistors were connected between the core V_{DD} pins and the bank of bypass capacitors. A differential probe was used to measure the voltage waveforms, which



(a) Test Board schematic

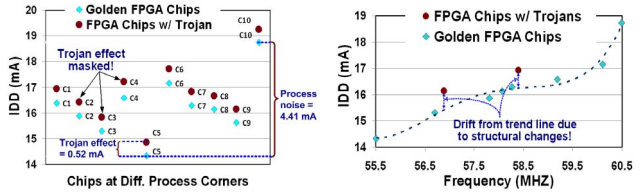
(b) Schematic of IEU



(c) Experimental Setup

(d) Recorded waveforms

Fig. 7. (a) Test PCB schematic. (b) Test circuit schematic. (c) Experimental setup. (d) Snapshot of measured I_{DDT} waveform from oscilloscope.

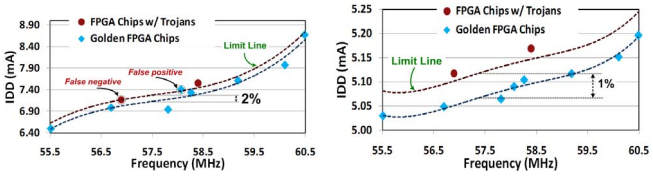


(a) I_{DDT} values (b) I_{DDT} vs. F_{max}

Fig. 8. Measurement results for 10 FPGA chips showing I_{DDT} vs. F_{max} trend for the IEU test circuit with and without a 16-bit sequential Trojan inserted in the *Arithmetic Unit* (0.14% of original design).

were recorded using an Agilent mixed-signal oscilloscope (100MHz, 2Gsa/sec). The waveforms were synchronized with a 10 MHz clock input and were recorded over 16 cycles corresponding to a pattern of 16 input vectors. Frequency (an estimate of F_{max}) was measured using a 15-inverter chain ring oscillator circuit, mapped to different parts of the FPGA, with an on-chip counter. We performed experiments with 10 FPGA chips from the same lot, which were placed in the same test board using a BGA socket, with the same design mapped into each chip. The test setup is shown in Fig. 7.

2) Results: The experimental results for multi-parameter testing approach are shown in Fig. 8. The results show that while measurements of I_{DDT} only (Fig. 8(a)) may not be able to capture the effect of a Trojan under parameter variations, multi-parameter based side-channel analysis can be effective to isolate it. For a set of golden chips, I_{DDT} vs. F_{max} follows an expected trend under process noise and deviation from this trend indicates the presence of structural changes in the design. Fig. 8(b) shows this scenario for 10 FPGA chips, 8 golden and 2 with Trojans (16-bit sequential Trojan). The ones with Trojans stand out from the rest in the I_{DDT} vs. F_{max} space. Fig. 9(a) shows the measured I_{DDT} vs. F_{max} trend for a 4-bit sequential Trojan, which occupied 0.03% of logic resources in the FPGA. By drawing a limit line with a sensitivity of 2%, we get some errors in Trojan detection. Lowering the sensitivity to 1% will decrease the number of false negatives (Trojan chips classified as golden), but increase the number of false positives (golden chips classified as Trojan). To improve the sensitivity of Trojan detection, we subtracted the background current (current measured with no input activity) for each chip and the corresponding I_{DDT} vs. F_{max} trend is shown in Fig. 9(b). Even with a sensitivity of 1%, we can now clearly



(a) With background current. (b) Without background current.

Fig. 9. Measured I_{DDT} vs. F_{max} results for 8 golden and 2 Trojan chips for the IEU circuit with and without a 4-bit sequential Trojan inserted in the *Set Unit* (0.03% of original design).

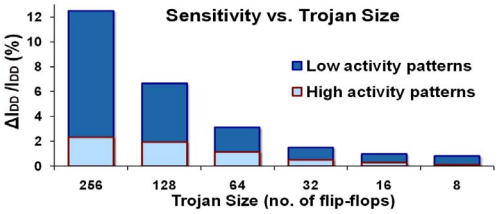


Fig. 10. Sensitivity of Trojan detection decreases with Trojan size but improves by proper test vector selection.

identify the Trojan chips without any errors. Fig. 10 shows the variation in Trojan detection sensitivity with Trojans of various sizes and with sets of input test vectors with differing activity levels. It is clear from this graph, that the sensitivity of Trojan detection decreases with decrease in Trojan size, and for very small Trojans, we need to use sensitivity improvement techniques like appropriate test vector application for reducing background current to avoid classification errors.

IV. Conclusion

We have presented a multiple-parameter side-channel analysis based hardware Trojan detection approach that exploits the intrinsic relationship between active-mode current (I_{DDT}) and maximum operating frequency (F_{max}) to achieve high signal-to-noise ratio in presence of process variations. The approach is scalable with respect to increasing die-to-die and within-die process variations in nanometer technologies. We have also presented appropriate test vector generation and use of I_{DDQ} as a third parameter to improve the detection sensitivity. The approach is validated using both simulation as well as hardware measurements using 120nm FPGA chips. We show that the proposed approach can detect complex sequential Trojans with high confidence in presence of large process variations. For ultra-small Trojans, the proposed approach may suffer from reduced sensitivity. For such Trojans, logic testing can be more effective. Hence, the proposed approach can be combined with complementary logic testing approach for reliable detection of Trojans of all sizes.

References

[1] DARPA, "TRUST in Integrated Circuits (TIC)", 2007. [Online]. Available: http://www.darpa.mil/MTO/solicitations/baa07-24.

[2] F. Wolff *et al*, "Towards Trojan-free trusted ICs: Problem analysis and detection scheme", *DATE*, 2008.

[3] R.S. Chakraborty *et al*, "MERO: A statistical approach for hardware Trojan detection", *CHES Workshop*, 2009.

[4] D. Agrawal *et al*, "Trojan detection using IC fingerprinting", *IEEE Symp. on Security and Privacy*, 2007.

[5] M. Banga and M.S. Hsiao, "A region based approach for the identification of hardware Trojans", *HOST*, 2008.

[6] R. Rad, J. Plusquellic and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions", *IEEE TVLSI*, 2010.

[7] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint", *HOST*, 2008.

[8] D. Rai and J. Lach, "Performance of delay-based Trojan detection techniques under parameter variations", *HOST*, 2009.

[9] S. Borkar *et al*, "Parameter variations and impact on circuits and micro-architecture", *DAC*, 2003.

[10] A. Keshavarzi *et al*, "Multiple-parameter CMOS IC testing with increased sensitivity for IDDQ", *IEEE Trans. VLSI*, 2003.

[11] T. Sakurai and A.R. Newton, "Alpha-power law MOSFET model and its applications to CMOS inverter delay and other formulas", *JSSC*, 1990.

[12] Predictive Technology Model, [Online] http://www.eas.asu.edu/∼ptm/