SAND2014-19547C

GDS-II Trojan Detection using Multiple Supply Pad V_{DD} and GND I_{DDQ}s in ASIC Functional Units.

Ian Wilcox and Jim Plusquellic
University of New Mexico

Abstract

We propose a parametric, side-channel-based method designed for detecting malicious changes that have been made to the chip layout, i.e., the GDS-II representation, by an adversary. We measure steady-state leakage currents (I_{DDQ}) from multiple, topologically distributed power ports on the chip and propose a calibration method that significantly improves the Hardware Trojan (HT) signal-to-process-noise detection sensitivity of our statistical-based detection methods. The technique is validated for the first time by measuring I_{DDQ}s from an ASIC with Advanced Encryption Standard (AES) and Floating Point Unit macros, 16 V_{DD} and GND *ports and a set of special HT emulation circuits. I_{DDQ} data is measured from multiple copies of the IBM, 90 nm ASIC.*

1 Introduction

Globalization of the Integrated Circuit (IC) design, fabrication and test industries, as well as increased use of 3rd party IP, increases the ease at which adversaries can insert malicious circuits that are designed to leak confidential information or cause system failure [1][2]. Four general approaches are proposed as a means of detecting malicious circuits or Hardware Trojans (HTs), namely, parametric (side-channel-based) methods, logic testing methods, destructive IC inspection and watch-dog monitors.

The primary advantage of side-channel detection methods is there ability to detect 'partial' activations of the HT circuit, which are much more likely to occur then the 'full' activations attempted by logic-based detection strategies. Moreover, parametric approaches are also able to detect HTs that do not change the base functionality of the circuit, i.e., information leakage HTs. The biggest challenge of parametric approaches is developing methods with adequate *signal-to-noise*, where the signal is defined as the anomaly introduced by the HT and noise refers to uncompensated chip-to-chip and within-die process variations and measurement noise.

In this paper, we propose a parametric approach that is based on the analysis of a chip's I_{DDQ} (steady-state or quiescent current), which builds on work done by the authors of [3][4]. Our proposed technique measures I_{DDQ}s from multiple-supply ports (MSP) across the 2-D surface of the chip as a means of improving *signal-to-noise*, and is an important distnguishing characteristic of our proposed approach over others. MSP provides regional observability and directly addresses the adverse impact of increasing levels of process variations and leakage currents[1]. MSP scales to larger chips with smaller feature sizes that incorporate additional power ports to accommodate the increase in power consumption. The n supply ports available with MSP can improve sensitivity significantly over traditional single supply port (global) measurement methods, up to a factor proportional to n. Calibration methods such as those proposed in [3], further improve signal-to-noise. However, calibration does not account for within-die variations, which remains the biggest challenge for parametric HT techniques.

This paper address the challenge of accounting for within-die variations and proposes a dual detection and localization strategy as a means of reducing false positive detections. The contributions of this paper are summarized as follows:

- Within-die variations are accounted for by using an multiple chip averaging technique, which significantly attenuates random, within-die variations in leakage current.
- A set of vectors, with direction and magnitude, are derived from the scatterplots of currents measured from adjacent pairings of power ports. The vectors are used, in combination wiht outlier analysis, to distinguish between measurement/process noise and HT leakage current anomalies.
- A statistical ellipse-based detection method is described that provides several useful attributes over our previously proposed regression-based techniques.
- Our techniques are demonstrated using data from a set of ASIC chips that incorporate large circuit macros, including Advanced Encryption Standard (AES) and Floating Point Unit (FPU) macros.
- The analysis is performed using data collected from both the V_{DD} and GND power grids, and under several different state vectors, which create different leakage patterns.

The remainder of this paper presents data from multiple copies of ASIC device configured with a set of 16 V_{DD} and 16 GND ports.

2 Background

The authors of [5] were the first to address the hardware Trojan (HT) issue. They use transient power supply currents to identify HTs in chips. The authors of [6] propose a method that first determines a set of target 'hard-to-observe' sites for a HT with q inputs and then uses automatic test pattern generation (ATPG) to generate patterns to activate the HT. A HT detection method that measures the combinational delay of a large number of register-to-regis-

1. A region is defined as a portion of the layout that receives the majority of its power from a set of surrounding power ports or C4 bumps.

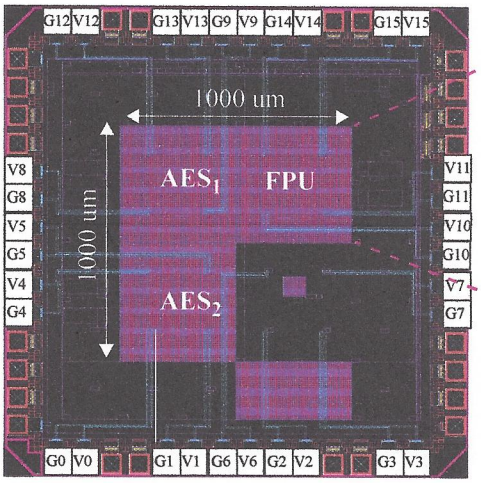

Fig. 1. Chip layout showing macros and 16 V_{DD} and GND ports.

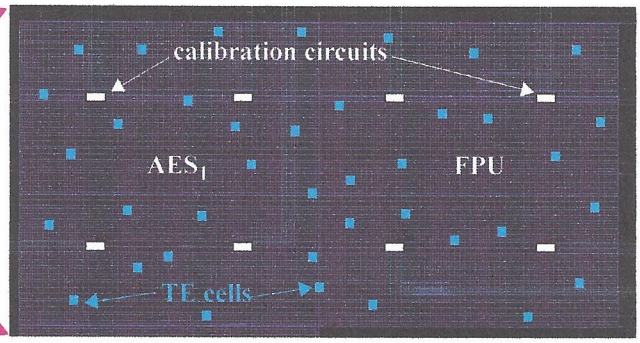

Fig. 2. AES_1 (left) and FPU (right) with Trojan Emulation (TE) cells and calibration circuits (not drawn to scale).

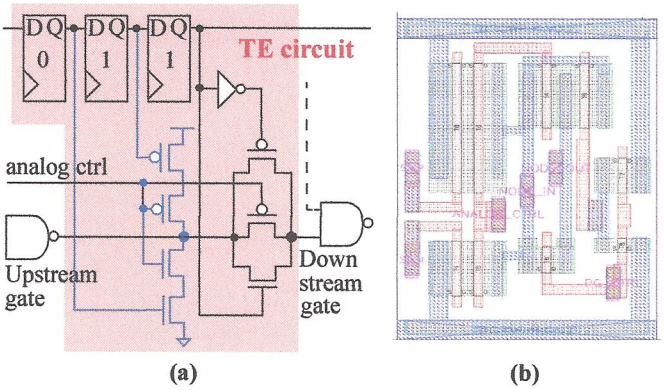

Fig. 3. Trojan Emulation Circuit (a) schematic and (b) layout.

ter paths internal to the functional portion of the IC is proposed in [7]. In [8], the authors propose a region-based stimulation strategy and analyze the global power consumption to detect HTs. In [9], the authors introduce special circuitry that enables the direct control of the least controllable nodes in the circuit as a means of triggering the activation of a HT. In [10], the authors build a path delay fingerprint of Trojan-free chips by running high coverage input patterns. In [11], the authors propose a methodology for reducing noise from circuit switching to improve detection of HTs designed to draw minimal power. A method that leverages the foundry process parameters to model and calibrate for delay variations introduced by process noise is proposed in [12]. [13] investigates the use of a side-channel signature for the chip as a method to model systematic process variations and for detecting HTs. The authors of [19] propose an approach for HT detection using a combination of functional verification, functional profiling (high-speed sampling), and DPA implemented on an FPGA. A scalable circuit partition approach is proposed in [14] using gate-level delay measurements at all circuit locations to find HTs. [15] proposes to use a specific process of fault-injection to force a clock glitch that will decrease the clock period until the setup and hold time is violated while monitoring the output of an AES IP core. The authors of [16] contend that a transmitter can hide in the process noise and leak an AES key. They propose an HT detection that encloses the three largest Principal Components within an ellipsoid of minimum volume. In [17], the authors propose an outlier HT detection method that compares the power signal analysis of an test chip with the training set derived from a genuine IC. The authors of [18] proposes finding HTs using design dependent detection sensors to measure path delays on-chip without the need for a golden model. In [19], the authors propose to detect HTs by comparing the expected correlation of F_{max} and I_{DDT} with that of a golden chip.

3 Test Chip Design

A block diagram of the test chip design is shown in Figure 1(a). It consists of three macros, AES_1 and AES_2 and FPU, each of which are 500 μm square. Large, low resistance M9 wires route from a set of periperial V_{DD} and GND pads, labeled V_0/G_0 through V_{15}/G_{15}, to a 4x4 grid of tap points distributed at 250 μm intervals across the macros. The M9 tap points connect down to the V_{DD} and GND grids, which are routed across the lower 8 metal layers. The M9 wires emulate an area I/O array configuration (also called a C4 array), which allows our MSP technique to fully leverage the regional observability available in commercial C4 implementations.

Fig. 2 shows a blow-up of the upper portion of the layout, illustrating the the V_{DD} and GND tap points, a set of 8 calibration circuits positioned underneith the tap points, and a set of 38 Trojan Emulation (TE) circuits (discussed below). The function of the calibration circuits is to allow a controlled short to be inserted between V_{DD} and GND (using shorting transistors). The calibration circuit design and process used here are similar to those described by the authors of [3].

3.1 Trojan Emulation Circuit

The purpose of the Trojan emulation (TE) circuit is to enable a systematic approach to evaluating the sensitivity of our methods. We inserted 57 TE circuits in the layout (19 in each macro). The details of the TE circuit are shown in Fig. 3. The three scan chain FFs control the state of the TE circuit, which can be configured to enable one of several types of signal anomalies, including controlled impedance shorts and opens[1]. The TE circuit is inserted in series between an Upstream and Downstream gate. The FF state

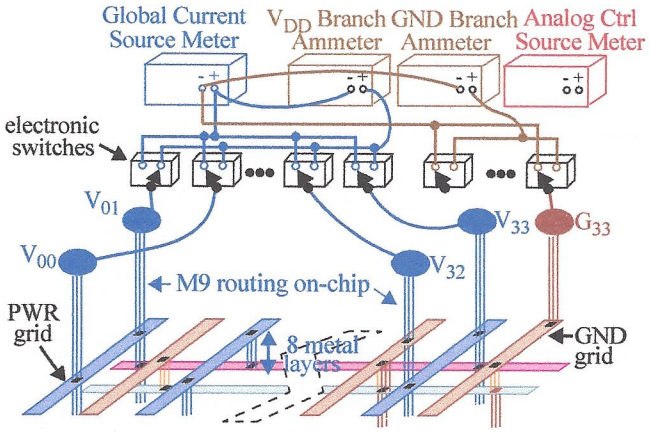

Fig. 4. Instrumentation Setup.

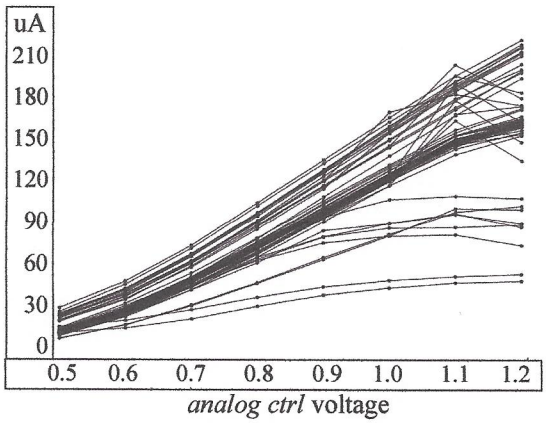

Fig. 5. TE circuit chip-wide current characteristics for different applied *analog ctrl* voltages using $CHIP_1$.

shown as "011" disables the TE circuit and represents the Trojan-free state. The 2 states investigated in this paper are "001" and "111" which enable the upper-most PFET and lower-most NFET in the 4 transistor stack, respectively. These two states in combination with the *analog ctrl* signal allow a controlled impedance short to be introduced between the V_{DD} and GND rails, resp., and the Upstream gate. Therefore, the TE circuit allows the controlled introduction of 'power anomalies' at various places on the V_{DD} and GND grid. We refer to these as **shorting scenarios** in this paper.

The CADENCE Encounter are used to place and route the macros so the position of the Upstream gate is likely to be close to the corresponding TE circuit in the layout but will vary for each TE instance. Therefore, the (x,y) position in the layout where the current is sourced from the V_{DD} grid and where it is sinked into the GND will be different. Also note that only one of "001" or "111" will create a short, and this is determined by the output state of the Upstream gate. For example, if the output state is '0', then configuring the TE circuit with "001" will create a short, with current proportional to the magnitude of the *analog ctrl* signal (with 1.2 V disabling the short and 0 V fully enabling it), and the state and geometry characteristics of the Upstream gate. The *analog ctrl* signal routes to all copies of the TE circuit and to an analog pin (not labeled) on the pad frame shown in Fig. 1. It can be controlled to any value between 0 and 1.2 V using an off-chip voltage meter.

The external instrumentation setup for measuring the individual power port (PP) branch currents is shown in Fig. 4 for a subset of the PPs. We use a Keithley 2400 source meter as the Global Current Source Meter (GCSM) and two Agilent 34401A for the V_{DD} and GND Branch (current) Ammeters (BC or BC), each with resolutions of less than 1 μm. Any of the 16 branch currents can be measured through the Ammeters by configuring the electronic switches appropriately. We use an Agilent E3626A for the Analog Ctrl Source Meter to drive the *analog ctrl* signals at values of 0.0 V, 0.1V, ... 1.2 V, in 100 mV steps, to emulate HT leakage sources of various magnitudes.

Fig. 5 plots the TE circuit current characteristics as a function of the applied voltage on *analog ctrl* for a typical chip. The x-axis plots the applied voltage in cases where the NFET stack transistors were used to create the short. The corresponding PFET voltages begin with 0.7 on the left and decrease to 0.0 on the right. There are 57 curves, one for each of the TE circuits on this chip. In most cases, the current monotonically increases as voltage is increased for NFET (decreased for PFETs). At the smallest applied voltages, the currents can be very small, i.e., in the range of approx. 10 uA.

We use the TE circuit to model the presence of extra gates, and/or a regional redistribution of gates in the layout, either or both of which would occur when an adversary tampers with the layout. The TE circuit injects current as a 'point source' and not over a region as would be true of extra gates or a redistribution of gates. However, from the perspective of the PP currents, the two different physical implementations are indistinguishable in cases where the modified region is constrained to a relatively small region, e.g., < 100 μm^2. Therefore, we believe the TE circuit is a good representation for HTs under these conditions, which in our opinion, covers most scenarios.

4 Trojan Emulation Experiments

The hardware experiments are designed to investigate the capabilities of our methods for detecting emulated Trojans, hereafter referred to as Trojans, that connect to the power grid at various places. To accomplish this goal, we selected nine locations to emulate Trojans as shown in Figure 3. The grid of rectangles represent the 80x50 array of TCs. The Trojans are emulated by enabling the Trojan emulation transistors, one at a time, at each of nine labeled locations.

The methods that we propose are statistically based and make use of 'golden models' of the chip to establish statistical limits of Trojan-free chip behavior. The golden models are derived by extracting RC-transistor models from the layout of the (Trojan-free) chip using a set of pro-

1. The TE circuit allows the insertion of a resistive connection between the output of the Upstream gate and the input of the Downstream gate as a means of introducing additional delays but this usage scenario is not investigated in this work.

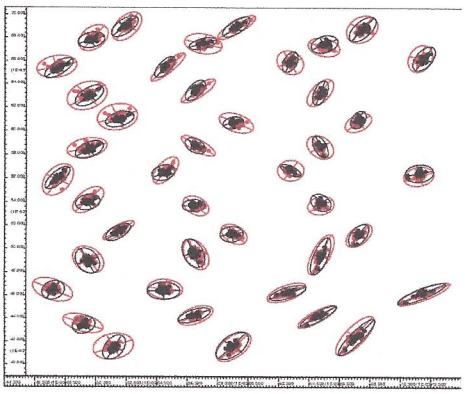

Fig. 1. Illustration of Calibration process. Red data point ellipses are uncalibrated while black is calibrated.

cess parameters that characterize the chips to be tested. Since we have control over the insertion of the Trojan in our chips, we instead derive the statistical limits from a Trojan-free configuration of the chips themselves in this work. The advantage of this strategy is that our characterization of Trojan-free chip behavior is determined from actual hardware. The drawback is that such an approach is difficult to implement in practice because it is not known which chips (if any) are Trojan-free. We plan to investigate the alternative 'simulation-defined' golden models approach in future work.

The *Trojan-free* configuration is implemented in our experiments by disabling all Trojan emulation transistors and setting the TESM to 0.9V. A Trojan-free data set is collected for each chip by measuring the global and local currents through each of the power ports. This process produces a set of four global and four local currents for each chip.

4.1 Regression Analysis

We implement our statistical analysis method using scatter plots. The scatter plots are created by plotting the currents measured from one PP (power port) against the corresponding values measured at a second PP. Figure 6 illustrates the six PP pairings used in the construction of the scatter plots. As an example, Figure 6 plots the raw PP currents, I_{01}, along the x-axis against the corresponding I_{11} on the y-axis for the 45 chips, measured without any Trojan emulation transistors enabled. These points are identified as *Trojan-free data points* in two separate data sets, labeled **Uncalibrated data** and **Calibrated data** (to be discussed). The following applies to either data set.

Since the individual ICs each have a unique leakage current associated with them, the Trojan-free data points are dispersed along the line labeled *regression line*. The regression line is actually derived from the Trojan-free data points and can be thought of as the 'best fit' line through them. The data points are not co-linear because of measurement noise and process variation effects, such as regional leakage current variations. Two parabolic curves, labeled *3 σ limits*, represent the prediction limits of the Trojan-free data points. The curves delimit a region in which 99.73% of the data points from Trojan-free chips are expected to fall. We use 3 σ for our limits because it is the most commonly used value in experiments carried out by industry, and is considered the industry standard.

The statistical limits are used to detect the Trojans. We consider a Trojan detected when its data point(s) falls outside these limit curves, i.e., above the top curve or below the bottom curve, **in at least one** of the scatter plot pairings (in our experiment, there are six pairings). For example, the data points labeled "Chip C_1, Trojan #4 at each TESM voltage" in Figure 6 are the ten data points produced under the Trojan emulation experiments for chip C_1. Each data point represents the currents measured at PP_{01} and PP_{11} under one of the applied TESM voltages. The same is true for the data points labeled "Chip C_2, Trojan #4 at each TESM voltage". In the *Uncalibrated* data set, none of the Trojan data points fall outside the limits and therefore these Trojans are considered undetected in this scatter plot pairing (if the same holds true in the other scatter plots then the Trojan escapes detection). The same is not true in the *Calibrated* data set however. The Trojans under larger voltage drops, e.g., TESM voltages 0.85 through 0.80, are detected in both chips.

4.2 Signal Calibration

The dispersion in the data points among the Trojan-free chips is caused primarily by chip-to-chip variations in the power grid resistance and the series resistance variations to the power ports from the power supply[1]. The differences in series resistances occur within the package and on-chip and as contact resistance variations in the clam-shell-style ZIF socket on the test board. In any case, these resistance variations adversely affect the sensitivity of our analysis to small Trojan current anomalies.

In previous work, we developed and demonstrated a process and environmental (PE) calibration technique [23][24] outlined here to deal with these chip-to-chip variations. The method makes use of the data collected from a special set of "calibration circuits" (CC), that are similar in design to the TCs shown in Figure 1(b) without the Trojan emulation transistor. Under the proposed signal calibration scheme, one CC is placed underneath each PP. Figure 1(a) shows the positions of the TCs, labeled $TC_{0,1}$, $TC_{0,77}$, etc., that are used as the CCs in our experiments. The calibration data is collected by enabling the shorting inverter in each of the TCs, one at a time, and measuring the PP and global currents. Leakage measurements are also made and subtracted from the shorting inverter currents. The shorting inverter currents are then normalized by dividing through by the global current.

The matrix of data collected under the calibration tests is used to calibrate the PP currents measured under subsequent Trojan tests. This is accomplished using the matrices obtained from a chip, C_x, and the data collected from calibration tests applied to a simulation model, S. The simula-

1. A second, less significant source for the dispersion is leakage current variations, to be discussed.

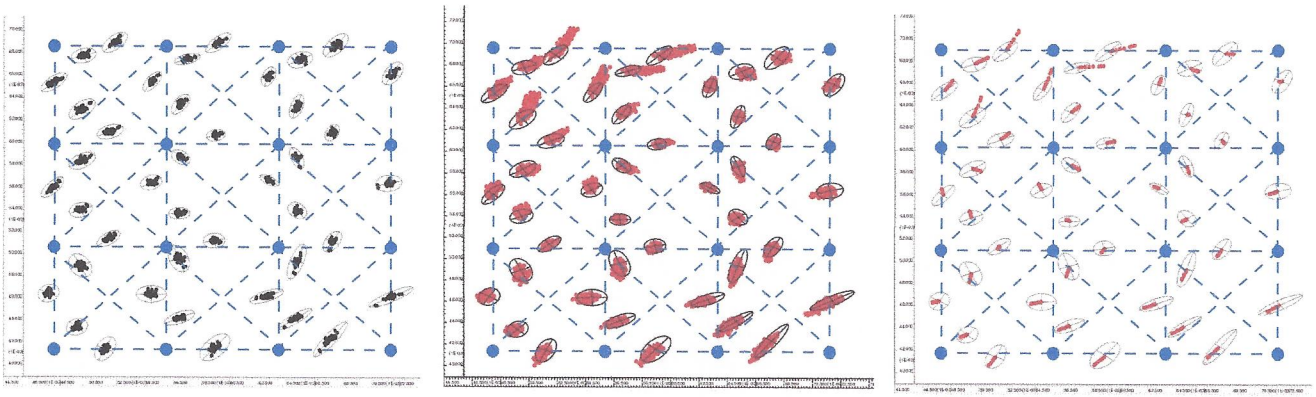

Fig. 6. Power port pairing combinations/

tion model serves as the reference or 'golden chip' standard. For the chip and simulation model, the matrix is 4x4 in our experiments because the power grid has only 4 PPs. Equation (1) gives the expression for computing the transformation matrix, X. Once X is obtained, the four PP currents from C_x, measured using a test designed to detect Trojans, are calibrated using the linear transformation operator defined by Equation (2).

$$X = C_x^{-1} * S$$

$$\begin{bmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{23} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{bmatrix} = inv\left(\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \right) \times \begin{bmatrix} r_{00} & r_{01} & r_{02} & r_{03} \\ r_{10} & r_{11} & r_{12} & r_{13} \\ r_{20} & r_{21} & r_{22} & r_{23} \\ r_{30} & r_{31} & r_{32} & r_{33} \end{bmatrix}$$

Eq. 1.

$$N_1 = I_1 * X$$

$$\begin{bmatrix} N_0 & N_1 & N_2 & N_3 \end{bmatrix} = \begin{bmatrix} I_0 & I_1 & I_2 & I_3 \end{bmatrix} \times \begin{bmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{23} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{bmatrix}$$

Eq. 2.

Variations in leakage current add to the measurement noise and the corresponding dispersion in the Trojan-free data points. The calibration process described earlier subtracts leakage current from the shorting inverter current and therefore is not able to correct for these variations. We define the calibration process this way to avoid needing to carry out calibration for every Trojan test that is applied (each Trojan test defines a different core logic state and corresponding leakage variation pattern). However, we give an analysis in Section 5.2 that demonstrates a moderate improvement in Trojan sensitivity when leakage is not subtracted, which shows that calibration can, in fact, correct for leakage variations.

5 Experimental Results

5.1 Global Current Analysis

In order to determine the improvement of our strategy over conventional power supply methods, we first carry out a global current analysis. Figure 14 plots chip number (x-axis) against the measured global current (y-axis) from the chips under both the Trojan-free and Trojan experiments. The 3 σ upper and lower limits are derived using the data point from the first 20 Trojan-free data points while chip numbers 21 and above serve as **control samples**. The purpose of the control samples is to determine the potential for false positives. By excluding these Trojan-free samples from the data used to compute the limits, they are evaluated against the limits in the same way as the Trojan data points.

5.2 Regression Analysis

As indicated earlier, a Trojan is counted as 'detected' in our regression analysis procedure if **at least one** of its data points falls outside the limits in the 6 scatter plots constructed from the 4 power port pairings (see Figure 6). We use the term **false positive** for Trojan-free data points that fall outside the limits. The term *limit-setting* is used in reference to the Trojan-free chips used to establish the statistical limits, while *control* samples is used for the remaining Trojan-free chips.

5.3 Trojan "Hit" Analysis

Unlike the manufacturing test whose objective is to identify *every* defective chip, the objective of Trojan detection is to find at least one chip that contains a Trojan. Although finding one is sufficient, given the non-zero probability that any given chip may have a manufacturing defect (defects also produce current anomalies) suggests that the appropriate metric is to determine if a suspect anomaly is present in a larger group of chips. The chance that an entire group of chips is defective in the same way is very small because most defects are random in nature[1]. Therefore, the level of confidence that a measured anomaly is caused by a Trojan increases if the same pattern exists in more than one chip.

6 Conclusions

In this paper, we carried out hardware experiments in which Trojans are emulated in a set of 45 chips fabricated in a 65 nm technology. A multiple supply port technique, in

1. There are also systematic types of defects that can produce similar anomalies to the pattern expected for Trojans. The simultaneous presence of systematic defects may increase the level of false alarms.

combination with a power signal calibration technique, are shown to increase detection sensitivity dramatically (by a factor of at least 49) over a global power signal analysis method. Given that large commercial grids incorporate hundreds (sometimes thousands) of power ports, we expect that enhancements in sensitivity to Trojans could exceed three orders of magnitude when such techniques are applied in practice.

We emulated Trojans that sink as little as 8 μA of current. Detecting such small current anomalies is not possible using conventional global power signal analysis methods. By using additional test patterns that control background leakage currents in different ways, we believe that our methods are capable of detecting all emulated Trojans investigated in our experiments.

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] J. Aarestad, D. Acharyya, R. Rad and J. Plusquellic, "Detecting Trojans Though Leakage Current Analysis Using Multiple Supply Pad IDDQs", *Trans. on Information Forensics and Security*, Volume: 5, Issue: 4, pp. 893-904, 2010.

[4] R. Rad, J. Plusquellic, M. Tehranipoor, "Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals", *HOST*, 2008, pp. 3-7.

[5] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, "Trojan Detection using IC Fingerprinting", Symposium on Security and Privacy, 2007, pp. 296 - 310.

[6] F. Wolff, C. Papachristou, S. Bhunia, and R. Chakraborty, "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme", *DATE*, 2008, pp. 1362-1365.

[7] Jie Li and John Lach, "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection", *HOST*, 2008, pp. 8-14.

[8] M. Banga and M. S. Hsiao, "A Region Based Approach for the Identification of Hardware Trojans", *HOST*, 2008, pp. 40-47.

[9] R. S. Chakraborty, S. Paul and S. Bhunia, "On-Demand Transparency for Improving Hardware Trojan Detectability", *HOST*, 2008, pp. 48-50.

[10] Y. Jin and Y. Makris, "Hardware Trojan Detection Using Path Delay Fingerprints", *HOST*, 2008, pp. 51-57.

[11] H. Salmani, M. Tehranipoor, "Layout-Aware Switching Activity Localization to Enhance Hardware Trojan Detection", *Trans. on Information Forensics and Security*, Vol. 7, Issue: 1, Part: 1, 2012, pp. 76-87.

[12] C. Byeongju and S. K. Gupta, "Efficient Trojan Detection via Calibration of Process Variations", *Asian Test Symposium*, 2012, pp. 355-361.

[13] J. Zhang, Y. Haile and X. Qiang, "HTOutlier: Hardware Trojan Detection with Side-Channel Signature Outlier Identification", *HOST*, 2012, pp. 55-58.

[14] W. Sheng and M. Potkonjak, "Malicious Circuitry Detection using Fast Timing Characterization via Test Points", *HOST*, 2013, pp. 113-118.

[15] I. Exurville, J. Fournier, J.-M. Dutertre, B. Robisson and A. Tria, "Practical Measurements of Data Path Delays for IP Authentication & Integrity Verification", *International Workshop on Reconfigurable and Communication-Centric Systems-on-Chip*, 2013, pp. 1-6.

[16] Y. Lu, Y. Jin and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation", *ICCAD*, 2013, pp. 399-404.

[17] L. Wang, H. Xie and H. Luo, "A Novel Analysis Method of Power Signal for Integrated Circuits Trojan Detection", *International Symposium on Physical and Failure Analysis of Integrated Circuits*, 2013, pp. 637-640.

[18] A. Davoodi, L. Min and M. Tehranipoor, "A Sensor-Assisted Self-Authentication Framework for Hardware Trojan Detection", *IEEE Design & Test*, Vol. 30, Issue: 5, 2013, pp. 74-82.

[19] S. Narasimhan, D. Dongdong, R. S. Chakraborty, S. Paul, F. G. Wolff, C. A. Papachristou, K. Roy and S. Bhunia, "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis", *Transactions on Computers*, Vol. 62 , Issue: 11, 2013, pp. 2183-2195.

[20] D. Acharyya and J. Plusquellic, "Hardware Results Demonstrating Defect Detection Using Power Supply Signal Measurements", *VTS*, 2005, pp. 433-438.

[21] J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor and C. Patel, "Quiescent Signal Analysis: a Multiple Supply Pad IDDQ Method," *IEEE Design and Test of Computers*, vol. 23, no. 4, pp. 278-293, 2006.

[22] X. Wang, M. Tehranipoor and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions", *HOST*, 2008, pp. 15-19.

[23] D. Acharyya, J. Plusquellic, "Calibrating Power Supply Signal Measurements for Process and Probe Card Variations", *IEEE International Workshop on Current and Defect Based Testing*, 2004, pp. 23 - 30.

[24] R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic, "Power supply signal calibration techniques for improving detection resolution to hardware Trojans", *ICCAD*, 2008, pp. 632 - 639.