ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ασφάλεια υλικού με ανάλυση πτώσης τάσης

Διπλωματική Εργασία

Τάκου Αλεξάνδρα

Επιβλέπων: Σταμούλης Γεώργιος

Βόλος 2020

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Hardware security with voltage drop analysis

Diploma Thesis

Takou Alexandra

Supervisor: Stamoulis George

Volos 2020

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής».

Η Δηλούσα

Τάκου Αλεξάνδρα

Ημερομηνία 08/10/2020

ABSTRACT

In the recent decade, the subject of hardware security has started to concern both the academia and the industries. It involves the insertion of extra, more often than not malicious, hardware during the manufacturing of an integrated circuit when its manufacture is outsourced to a non-trusted party. The extra hardware is called Hardware Trojan and in the course of the years they have been classified by their physical, activation and action characteristics. To help solve this issue, various detection techniques have been developed, like destructive methods, logic testing and side-channel analysis.

In this thesis, we focus on detection techniques based on side-channel analysis, and more specific with voltage drop analysis.

Περίληψη

Την τελευταία δεκαετία ο τομέας της ασφάλειας υλικού ξεκίνησε να απασχολεί τόσο τον τομέα της έρευνας, όσο και τη βιομηχανία. Πρόκειται για την εισαγωγή πρόσθετου, συνήθως κακόβουλου, υλικού κατά τη διαδικασία της παραγωγής ενός ολοκληρωμένου κυκλώματος, όταν αυτή γίνεται από τρίτους, μη έμπιστους συνεργάτες. Το επιπλέον υλικό ονομάζεται Hardware Trojan και ταξινομείται σε διαφορετικές κατηγορίες με βάση τα φυσικά του χαρακτηριστικά, καθώς και τα χαρακτηριστικά ενεργοποίησης και λειτουργίας του. Για τον εντοπισμό τους έχουν αναπτυχθεί τεχνικές όπως καταστροφική αποδόμηση υλικού, λογικός έλεγχος και ανάλυση side-channels.

Σε αυτή την εργασία, θα επικεντρωθούμε σε τεχνικές εντοπισμού βασισμένες σε ανάλυση side-channels, συγκεκριμένα με ανάλυση της πτώσης τάσης.

Table of Contents

CHAPTER 1
INTRODUCTION

Integrated Circuits (ICs) are a huge part of our day to day lives as they are part of mobile phones, computers of any kind and usage, and increasingly in household appliances and therefore they are required to be mass produced. Since, their manufacturing is costly nowadays the task is outsourced to third-party manufacturers. But since ICs may handle encryptions, data processing and data sharing among other things, there is always a possibility of extra unwanted hardware being inserted to the ICs either to leak information or cause a malfunction. The extra malicious hardware is called Hardware Trojan (HT) and in the past years many methods have been developed, with different rates of success, to detect the HTs.

Attention to software security has been drawn since the 1980s. However, it was not until 2008 that the first potential HT presence was reported. The incident involved a critical failure in a Syria radar, which was suspected that was intentionally triggered through a back door in the microprocessor. The microprocessor was built from a third party and it was suspected that it was manufactured with remote kill switches. After that the academia, industry and governments started researching more and in depth the issues called hardware security and HT detection [1].

In this thesis, some techniques are presented in the topic of HT detection. They are focused around HTs that were inserted into the integrated circuits during the manufacturing period and those chips need to be tested after they are delivered.

CHAPTER 2
TYPES OF HARDWARE TROJANS

2.1 Introduction.

No matter the HT, where it is placed or what its purpose is, they all share some common characteristics. First of all, all HTs are placed in the Integrated Circuit in order to be malicious. Either by disrupting the IC's function or by sharing information integral to the function of the general system the IC is part of, HTs' cause is harmful. Secondly, they are stealthy in nature. HTs are not connected with paths or gates in the IC which are easy to control and to be tested. On the contrary, paths and gates are selected that their triggering conditions are uncommon and very specific. Finally, to make the HT more unnoticeable the area it occupies is significantly small compared to the rest of the IC in order to not change the IC's measurements and characteristics [2]

2.2 Trojan Classification.

Beyond these, HT categories branch out and vary depending on the element they choose to focus on. One of the first, and pretty detailed, classifications of Trojans by Tehranipoor and Koushanfar in their [6] was based on their physical characteristics, their activation characteristics and their action characteristics, as shown in Figure 1.

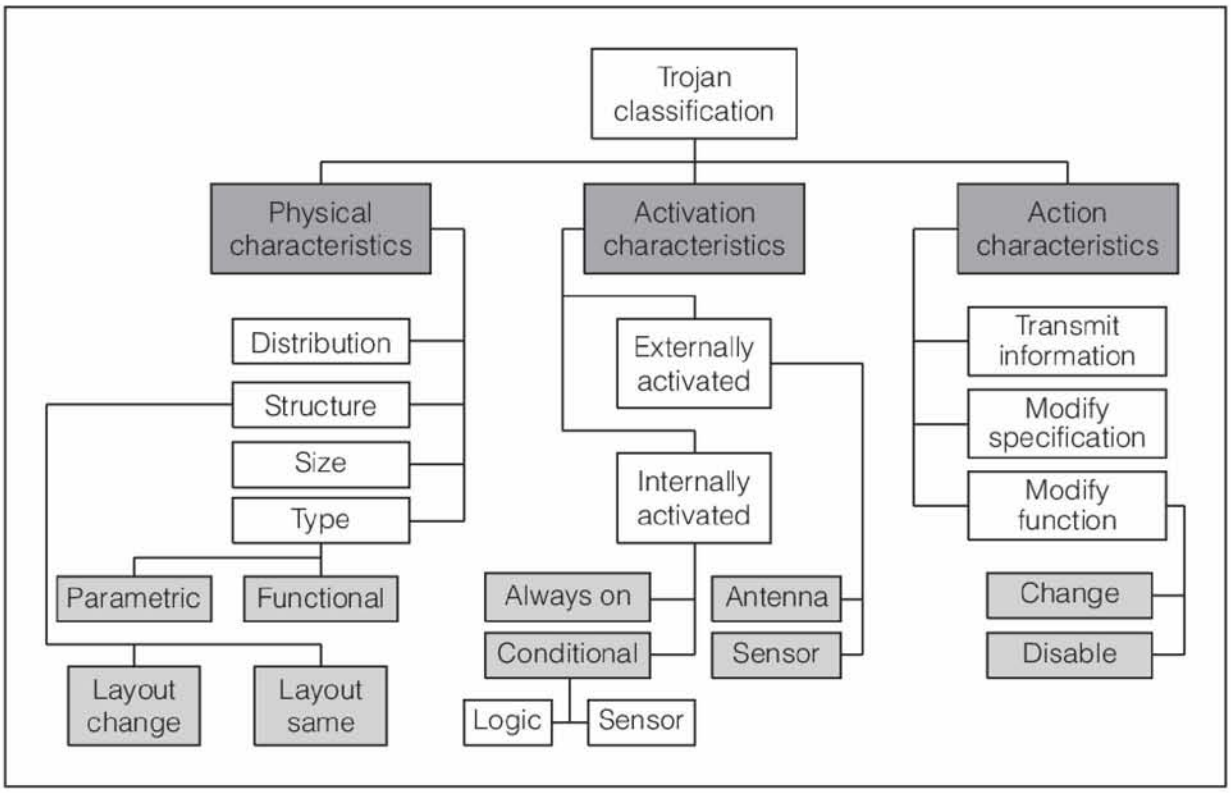


Fig. 1: The classification of HTs by Tehranipoor and Koushanfar [6]

More specifically, the physical characteristics describe how and a Trojan exist within an IC. They include distribution, which refers to where the HT is placed within the IC's layout, structure, which applies to the times the placement of the HT does result in changes to the original IC's design and layout. Size refers to the actual number of the IC's components have been tempered with or added and type splits the HTs to functional class and parametric class. Functional class Trojans add or remove hardware to the original design and parametric class Trojans change the wiring and logic of the existing hardware.

The activation characteristics, as the name suggests, involve the conditions needed for the HT to execute their function. Externally activated HTs need a stimulation through an antenna or a sensor from outside the IC to start their malicious work. The opposite is an internally activated Trojan and it may be "always on" meaning that a node or a path has been disrupted and are more susceptible to failure and thus the malicious behavior can be manifested at any time. On the other hand, condition-based Trojans stand-by until a condition, either an internal value

or an environmental condition, is met that triggers the Trojan's function. These HTs require extra hardware to be added to the design so they are either combinational or sequential circuits.

Combinational HT circuits relay on the current values of the IC's expected function for a triggering input so they are connected to and rely for that on the pre-existed nets of the design. Considering the fact that HTs want to remain hidden during standard operation or manufacturing tests the triggering inputs and nets chosen are rare combinations and rarely activated respectively. Sequential circuits depend on values from previous clock cycles as well for the triggering condition and that is way sequential Trojans are more difficult to detect since taking into consideration past states is more complex. [2]

The action characteristics focus on the malicious behavior of the Trojan. Modify function Trojans disrupt the IC's original function by altering the original netlist, either by adding logic or by removing or bypassing the existed one. Trojans that modify specifications focus on altering the IC's parametric properties. Finally, the transmit information class refer to the Trojans that leak information through exploitation of side-channel characteristics.

2.3 Types of Detection.

Many methods have been proposed to counter measure HTs. Deconstructing the IC is one of them. Basically, an IC is chosen, and it is unpackaged layer by layer. Each layer is analyzed for a potential HT by reverse-engineering it and then the next layer is analyzed and so on. This kind of methods are very reliable to check the tested IC for HTs, but they are very costly, time consuming and they do not guarantee that the rest of the manufactured ICs are Trojan free [3].

So, non-destructive methods have been developed to overcome the aforementioned problems. The two main philosophies are Design-for-Security (DFS) and to test for HT after the IC's manufacturing. Design-for-Security methods basically are applied during the designing of the IC and taking measures to be able to ensure the validity of the manufactured IC. The latter uses logic testing, side-channel analysis or a combination of them to check the already manufactured ICs. Since both of these philosophies have their difficulties and they are not completely foolproof so they can be combined for better results.

Design-for-security methods can be classified as logic obfuscation, IC metering, hardware watermarking and split manufacturing [4]. Logic obfuscating entails adding extra hardware,

called key-gates, to the original design in order to hide its functionality. To produce the correct output a valid key must be applied [5]. IC metering uses a small part of the design which, at the configuration stage, is configured to have a unique ID, different for each manufactured design instance [7]. Hardware watermarking basically inserts an identification code, that cannot be found by machine analysis, in a design and is embedded as an integral part [8]. Finally, split manufacturing evolves using two or more manufacturing lines for a design and the individual parts are combined afterwards during a joining process [9].

Checking a manufactured IC for HT aims, through various and different tests, to observe an abnormal performance from the IC either to its output or to its side-channel parameters. Logic testing aims at the former by applying multiple input vectors to the IC and checking if the output is the expected. An automatic test pattern generation (ATPG) tool is used to generate the input vectors to be checked. Considering that HTs are stealthy in nature it is assumed that they are activated under rare conditions. As a result, these methods after they figure out these conditions, they try to eliminate low activity nodes. However, one of the downsides is that in order for these methods to produce any accurate result the HT needs to have an effect on the output of the IC, meaning only functional Trojans can be detected. Additionally, considering the ever-growing number of gates which can be fitted in a die due to technology getting ever so smaller, pinpointing the triggering conditions for fully activating a HT by brute-force testing is impossible [10]. Nevertheless, logic testing is still a viable option for small designs or with fewer possible triggering conditions as well as a complementary method to other means of HT detection.

2.3.1 Detection with Side-channel Analysis.

Side-channel parameters, in general, include characteristics that have to do with the function and the execution of the process under question instead of the algorithms and computations that achieve desirable result. Side-channel attacks aim these parameters to discover the information which process created the parameters. Their presence is wide enough that they can even be used to printers to recreate the text printed [11] and pose a threat on any kind of encrypted information either digital [12] [13] or in hardware [14] [15].

In an integrated circuit the side-channel parameters refer to time, power, path delay, current, temperature, radiation frequency, operating frequency etc. Even partially activating a HT in an IC influences the side-channel parameters, so compering their values while testing with the expected values HTs can be detected and that is the basis of HT detection with side-channel analysis which is one of advantages of methods using side-channel analysis. Another advantage is that it can, in most of the techniques, be non-evasive to the design and non-destructive after manufacturing [16]. Detection sensitivity describes how well a method can detect a Trojan. The higher the sensitivity, the better the chances to correctly detect the HT.

The biggest issue with methods using side-channel analysis is process variations. Basically, they are variations that happen during manufacturing of each lot in every chip, even within the same chip, and so they cannot be predicted. They can be variations in the device length, oxide thickness and in the impurity concentration densities [17]. They can be categorized as inter-die and intra-die variations. Inter-die variations refer to the different features of the same device that occur from one die to the next. Intra-die variations describe the differences in a devise within the same die. Although devices that are closer to each other and which are structurally similar have a higher probability to be alike, different lots can have different features between them [18] [19]. A second problem is acquiring a Golden Chip to have as reference for their performance parameters. A chip qualifies as a Golden Chip only if it is surely and without any doubt Trojan-free so Golden Chips are hard and expensive to come by [10].

HTs, to keep their stealthy nature, strive to be a small part of a much larger design making their influence on side-channels as little as possible to mask their presence, so reducing the impact of process variations can help achieve a more sensitive HT detection technique. The use

of a Golden Chip is the main and only source of inter-die variations, by their definition. Eliminating the use of a Golden Chip can result in elimination of the inter-die variations but then there are no reference values to compare in order to understand whether a HT is present in the tested IC. To counteract that problem self-referencing or self-authenticating methods can be used, e.g. comparing the results of a tested value measured at different times on the same die. As for the intra-die variations, since spatial correlation is present, comparing values only to adjacent partitions within an IC is an effective way to reduce the variations and to achieve higher detection sensitivity. Another way is to increase it is by activating a higher number of the Trojan's cell. Methods can be combined and used in unison to achieve that affect, as well as logic testing since it might still activate part of the HT even if it is not fully and enough to have it show its influence on the IC [2].

In this dissertation we focus on power analysis as far as the side-channel parameters go. Total power consumed is the sum of dynamic power and leakage power. Dynamic power refers to the power consumed by the switching of the gates in an IC and thus it has a linear relationship with the number of gates in the IC and HT. Leakage power, in large circuits can be comparable to dynamic power. If the leakage power consumed by the Trojan is significant then the clock frequency changes and that can be used as an indication that a HT is present in the IC. In the occasion that the Trojan has small leakage power, and the process variations are significant, it might not be detectable. A solution for that is to split the IC in partitions and try to increase the Trojan-to-circuit power consumption to achieve higher detection sensitivity. A balance has to be kept on the amount of partition made, since partitioning the IC too much results in HT to be split into many partitions and thus its activation chances to be reduced. Even if an activated partition includes parts of an HT, if the HT's inputs originate from a different partition there is no chance of the HT's parts to be activated and mistakenly thought as Trojan free [2].

CHAPTER 3
METHODS FOR HARDWARE TROJANS DETECTION

3.1: Introduction.

In voltage drop analysis the power and the resistance. The main concern between those two is how to accurately measure the power consumed by the IC. Here some methods to make better the detection sensitivity of power-based detection methods are presented.

3.2.1: Technique Introduction and Testing Specifications.

Hossain proposed and tested three methods in his dissertation [2] to heighten the detection sensitivity. It is assumed that the Trojan is inserted in the ICs at an untrusted foundry and as such the Electronic Design Automation (EDA) flow, placement, routing and power optimization are considered trusted and Trojan free. For the testing ISCAS'89, ITC'99 benchmark circuits were used and two practical circuits the RS232 micro URT and the AES-128 cryptoprocessor from Trust-HUB [20][21][22] as shown in Figure 2. Synopsys design compiler and IC compiler with 90nm technology library were used for synthesizing the designs.

Circuit	Number of Combinational cells	Number of Sequential cells	Total cell area(um^2)
s1238	284	18	2928
s5378	500	163	10716
s13207	497	330	17119
s35932	3133	1728	101543
s38584	3982	1172	80108
s38417	3455	1564	94562
b19	58836	6042	826117
RS232	1097	438	25224
AES-128	162561	6720	1631531

Fig. 2: The circuits and HTs used for testing[2]

As for the Trojans to be detected, two modified types of Trojans from Trust-HUB [20][21][22] were used. The first one (T1) is composed of two combinational 8-bit comparators with two FFs. Its trigger consists of two comparators, which drive the clock inputs of two flip-flops in their outputs, and the inverted test enable signal to ensure activation only in the functional mode. The second Trojan (T2) used is a rare vector triggering circuit. The original Trojan consisted of a 32-bit adder and a 32-bit counter but it was scaled down to a 4-bit counter and a 16-bit comparator due to the original being too big to be inserted in small circuits like ISCAS'89 and to be considered a challenge to be detected. Finally, for the HTs insertion to the circuits an Engineering Change Order (ECO) option was used for placement and routing, meaning that the Trojans were inserted without changing the layout of the original circuit.

In the scope of this technique, a scan based segmentation was used. Scan is a design technique used in IC manufacturing to increase the overall testability of a circuit. Scan tests are generated by ATPG tools and cover stuck-at-faults, caused by manufacturing problems. Scan chains are used to shift-in and shift-out test data in order to make every point in the IC controllable and observable. They are formed by flops being connected in a chain with the output of one flop being connected to the next one [23]. As the IC gets bigger the scan chains get bigger as well to confidently ensure full observability. As a result, the shift operations during the scan testing increase the power consumption and the switching activity [24]. A way to counter this problem is scan partitioning, where the scan is split into segments and only the needed segment for the testing is activated each time [25]. In order to activate only one partition each time a clock-gating technique can be used, meaning a controller is placed to each segment that can block the clock signal and prevent the segment from activating if that segment is not needed for a computation [26].

Hossain proposes in [2] that the segmentations are determined during the design phase to find their maximum number possible for a netlist as well as to ensure that each chain is composed by scan cells that are neighboring. Scan cell reordering is used to help achieve the latter part in the case that the chains do not fulfill the neighboring condition. Controller circuits are inserted in the IC's design during the place and route phase to activate the needed scan chain and an Eco option is used so that there is minimum impact.

Using the specifications and tools above Hossain developed the following three methods for heightening HT detection sensitivity while using power-based side channel analysis.

3.2.2: Scan Based Segmentation.

This method can be divided into two phases, shown in Figure 3, the design phase, and the Trojan Detection Golden Pattern generation, and it results to a hardware overhead linearly proportionally to the number of FFs in the circuit. The first step of the method is using a clustering technique to the circuit, which physical layout is known, to find the closest to each other scan cells. The second one entails reordering the scan cells to ensure they are neighboring, and the scan chains are formed. Scan segmentation is then applied, and the clock-gating circuits are applied to each of the segments. A set of test patters is generated with the ATPG tool and is then

reduced to a set, which was named Trojan detection golden patterns (TDGPs), through power simulation to help reduce the detection time. The reduced set is applied both to the circuit under authentication and to the Golden chip, the power values are measured, and the results are compared to determine if a HT is present in the circuit under authentication.

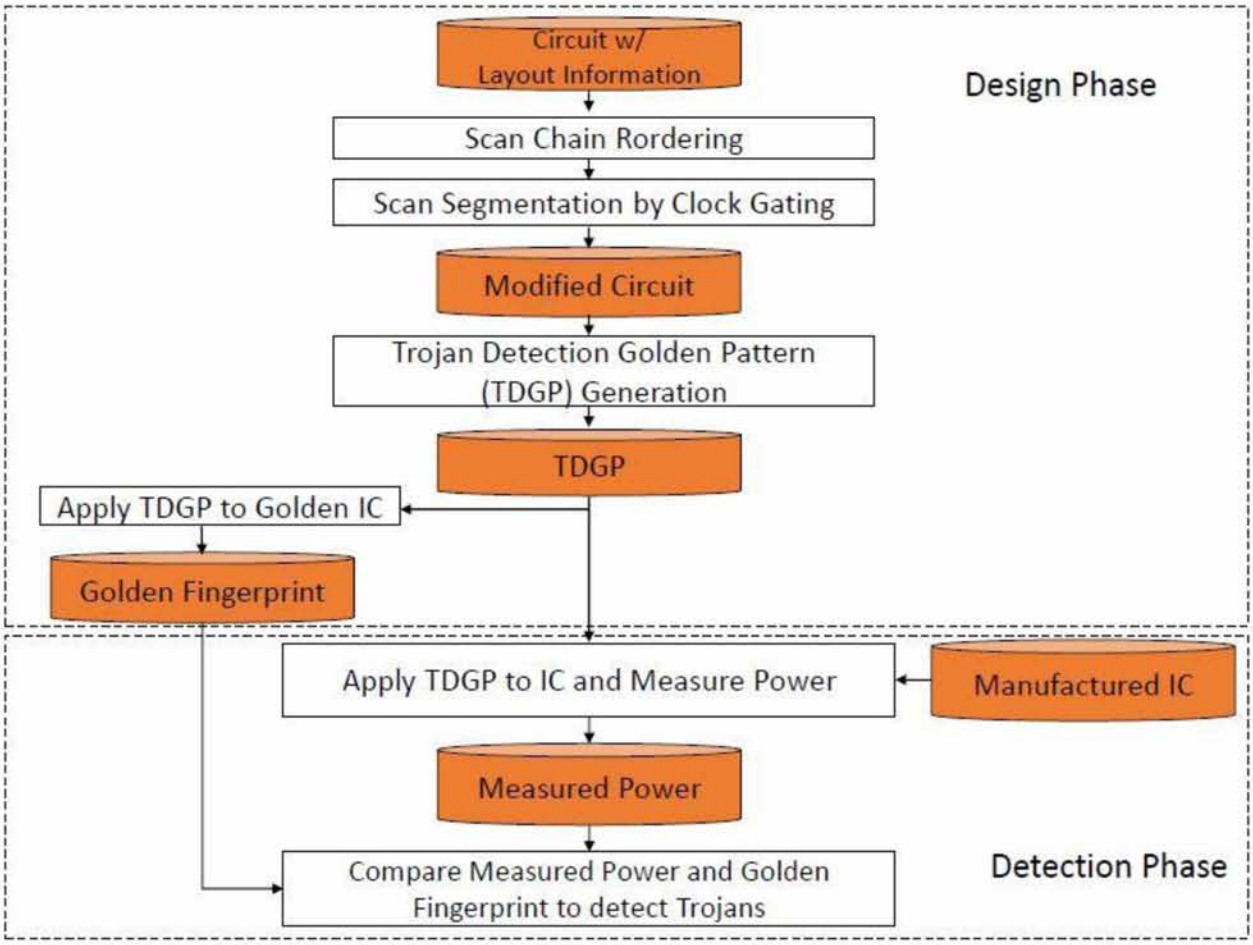


Fig. 3: Overview of the proposed technique [2]

For the clustering of the circuit the technique in [27] was used. It basically creates the clusters taking in consideration the geometric position of each scan cell. The reordering technique is created by Hossain and it creates the new scan chains after doing the reordering it deems necessary based on the scan sells distance from each other so they are close. The segmentation step includes splitting the newly created scan chains into a fixed number of length-based segments and the gated clock controllers are placed so as all the segments can be controlled.

The TDGPs are chosen from the transition delay fault patterns, since they are meant to cause a lot of switching activity. The algorithm created to make the selection considers the transition delay fault patterns, the set of segments that comprise the circuit and the requested maximum number of TDGPs. The transition delay fault patterns are applied to each segment and the toggled gates are counted. The patterns that have toggled the most gates are chosen for the TDGP set in a greedy fashion until the maximum toggling coverage is reached or have reached the maximum number of TDGPs. Since this process is applied to every segment, there is a chance that the number of TDGPs will be different for each segment.

The Figure 4 shows the results of the technique when tested. RPD refers to a ratio of relative power difference of the nominal power of a circuit containing the Trojan to nominal power of the same circuit without the presence of the Trojan, and it represents the detection sensitivity. T1 refers to the Trojan, that is composed of the combinational 8-bit comparators and T2 to the rare vector triggering Trojan and Sx refers to segments of the circuit. The results are associated with 1.2V DC and 250 MHz operating frequency.

The HTs were inserted in the circuits and the tests were run. The first batch of tests were conducted without the segmentation and the power difference and the max RPD were measured and calculated. After that, the proposed segmentation was implemented, and the same values were once more calculated. Comparing the max RPD before and after the segmentation, it is clear that the detection sensitivity is higher with the proposed technique.

Benchmark	Inserted Trojans		Trojan Detection scenarios			
			W/o segmentation		W/segmentation	
Circuit	Trojan type	HT site	Power diff. (uW)	Max RPD (%)	Power diff. (uW)	Max RPD (%)
s1238	T1	S2	27.2	23.05	26.87	45.58
s5378	T1	S1, S2	146.8	15.64	98.3	64.38
	T2	S1, S2	151.3	16.47	149.4	69.20
s13207	T1	S15	116	6.74	115.7	28.82
	T2	S4	93	5.72	80.7	22.91
s35932	T2	entire	80.0	0.61	40	2.95
s38584	T1	S9	187	3.17	168	14.14
	T2	S9	61	0.73	54.9	5.89
s38417	T1	S14, S15	200	2.71	165.4	21.09
	T2	Entire	90	0.81	85.5	9.56
RS232	T1	S1	72.9	9.1	66.9	41.66
	T2	S2	55.3	10.5	54.5	31.23
AES	T2	S1, S22	460	1.19	413	13.00

Fig. 4: Experimented results of the scan-based segmentation technique [2]

However, this proposed technique requires extra hardware to be inserted into the circuit. For the circuits used for the testing the hardware overhead was calculated, reaching as high as 16%. It is increased with the increase of sequential elements but not because the number of segments. Figure 5 shows in detail the hardware overhead, number of sequential cells and of the segments.

Circuit	Number of Sequential cell	Number of segments	Hardware overhead% (clock gate)
s1238	18	4	7.84
s5378	163	6	1.61
s13207	330	8	16.26
s35932	1728	16	14.03
	-	32	14.19
	-	64	14.43
s38584	1172	16	12.09
s38417	3455	16	13.63
	-	32	13.82
	-	64	14.08
RS232	438	6	14.56
AES-128	6720	42	3.39
	-	64	3.42

Fig 5: Hardware overhead caused by the scan-based technique [2]

3.2.3: Self-referencing Technique with Equal Power pairs.

The previous method needs extra hardware and the existence of a Golden chip, both of which are a big disadvantage for realistically and industrially using this method for Trojan detection. The second detection method proposed is referred as EP (Equal-Power) self-referencing and aims to solve the need of a Golden chip, and the inter-die variation effect as a result, and the hardware overhead and improve the detection sensitivity for small Trojans compared to the circuit. It replaces the scan cells partitioning with a new one based on layout-aware clock tree to achieve less hardware overhead since one clock buffer is able to control several FFs. The partitions are created so they consume equal power so they can be used as a reference for authentication to other equal power segments. The algorithm created for generating test patterns chooses the ones that trigger the equal power segments for checking the presence of HT, and its steps are shown in Figure 6.

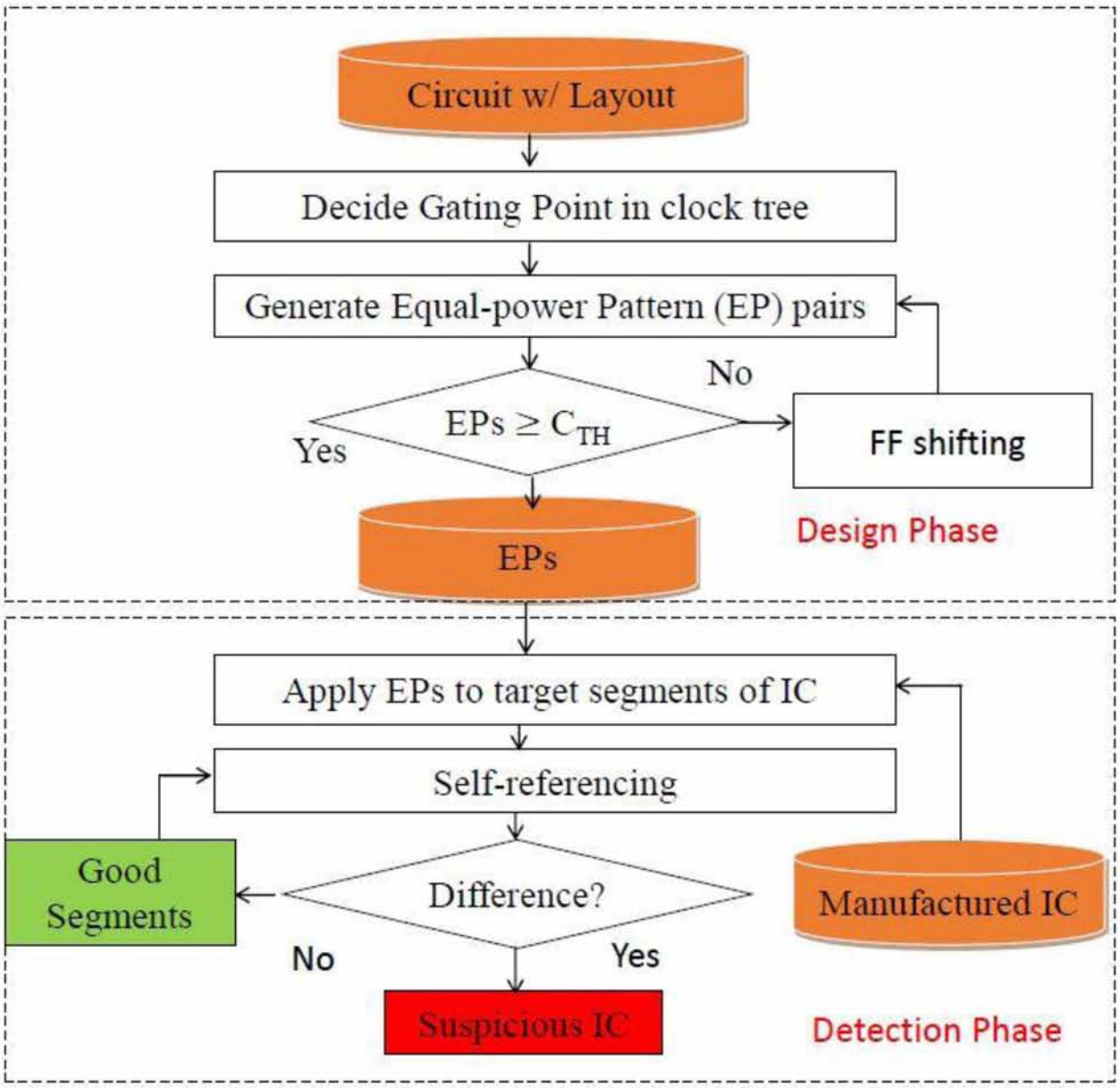


Fig 6: Overview of the EP technique [2]

The method utilizes an algorithm which firstly determines some segments, calling them gating points, based on the clock tree, the circuit layout information that is given as input and taking into consideration that the mean value of dynamic powers is equal between segments. A threshold of minimum EP pairs is set, and power simulations are run to find them. If that condition is not met and not enough EP pairs have been produced, an algorithm named FF shifting adjusts the segments, so more EP pairs appear. That concludes the design phase.

Next is the detection phase. Test patterns in EP pairs are applied to the manufactured IC being checked for HT. The EP pairs have should have equal or almost equal currents, depending the process variations, so measuring them and comparing them is the self-authentication merit, and thus bypassing the inter-die variations of this method. If the values between the measured values of the EP pairs differ significantly then the presence of a HT is confirmed. High accuracy of the measurements on the IC can be ensured with already existing on-chip current sensors [28].

The second column in the Figure 7 refers to the leaf nodes of the clock tree and the third refers to the number of segments after the proposed technique is applied. The LOC patterns are the initial patterns per circuit and the last column shows the toggling coverage after applying the EP pairs, whose population is shown in the sixth column. It is illustrated that almost full coverage is achieved using the developed technique for the EP pairs.

Circuit	No. of leaf nodes N_{Leaf}	No. of segments S_{SEL}	Hardware overhead in % (clock gate)	LOC patterns	EP pairs	Cell toggling count
S35932	10	10	0.383	380	558	99.87%
S38584	8	7	0.459	2080	848	96.62%
S38417	10	10	0.411	1740	1778	99.92%
b19	44	21	0.112	34923	231650	97.58%
AES-128	50	42	0.091	19488	65356	99.92%

Fig. 7: The experimental results of the EP technique (1 of 2) [2]

The Figure 8 has gathered the information about the success of the proposed method. It shows the segments that the HTs were inserted. The max RPD is presented, since it is the parameter illustrating the detection sensitivity, both for the combinational T1 and the sequential T2 Trojans, as well as the translation of it to the percentage that was actually detected.

Circuit	Trojans	Trojan insertion	Max *RPD*	Detectability (15% inter & 3% intra)
S35932	T2	2 segments	16.05%	65.14%
S38584	T1	3 segments	14.43%	24.09%
S38417	T1	1 segment	34.22%	100.00%
b19	T2	1 segment	12.74%	2.74%
AES-128	T2	1 segment	11.42%	0.20%

Fig. 8: The experimental results of the EP technique (2 of 2) [2]

3.2.4: Self-referencing Technique with Equal Power Neighboring pairs.

With the partitioning of the IC and grouping of segments based on equal power consumption the inter-die variations and the need of a Golden IC as a reference are eliminated. Hossain in [2] decided to expand on the EP method to diminish the intra-die variations as well and to further improve the detection sensitivity, shown in Figure 9. The main idea to achieve the former is instead of using segments from across the IC for the equal power pairs, only segments that are close to each other are paired up, thus giving the name equal-power neighboring (EPN) pairs. For the latter, creating an augmented pattern set by using the algorithm developed in the first suggested method and depending on the results using additional ones to increase the toggling coverage, with the chance of new EPN pairs to be created. achieves improved detection sensitivity.

The initial EPN pairs are decided in a similar way as described in the previous method suggested by Hossain. The algorithm having the layout of the IC and figuring out through power simulations with the transition delay fault patterns the dynamic power consumption of the segments discovers the equal power segments in the IC. The segments are created based on the layout of the clock tree. Two segments, according to the method, are considered neighboring if the maximum Euclidean distance between any FFs belonging to the segments does not surpass a predetermined threshold. Taking to consideration the results of the simulations and of the measuring of the Euclidean distance between the segments the initial EPN pairs are decided.

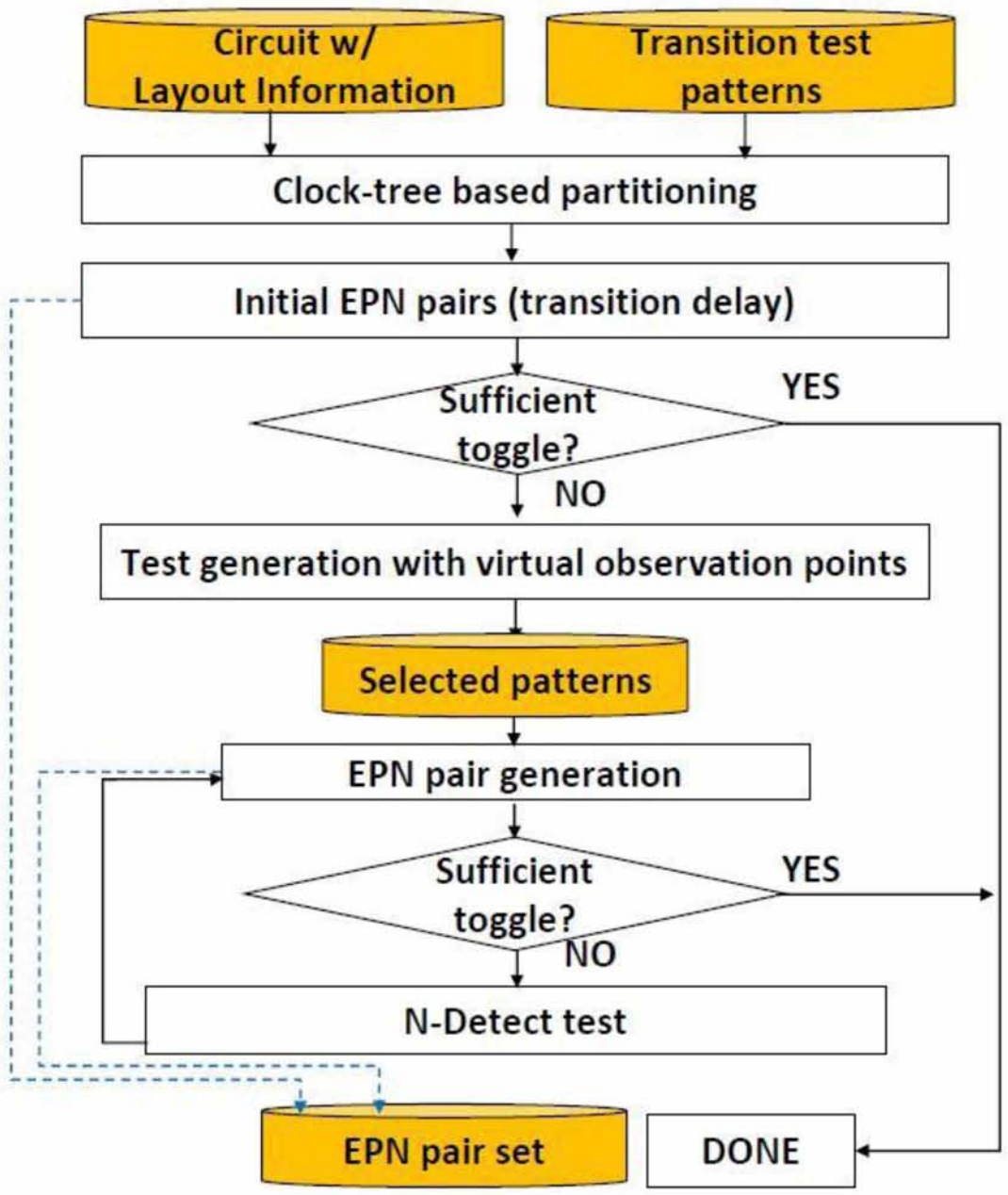


Fig. 9: Overview of the EPN technique [2]

The fact that the pairs are neighboring has as a result that the test pattern pairs to satisfy enough toggling of the EPN pairs are reduced, so the test pattern generation has been expanded and extra methods are used, if need be, to address the problem. The first method to attain more

test pattern pairs, virtual observation points (VOPs) are inserted in the netlist at the end of untoggled gates for the ATGP to generate test cases to toggle the nets that are not covered. These points are virtual since they are added only on the netlist and not in the actual IC so to not have hardware overhead, which increases linearly for large circuits. New test patterns using ATGP are generated and the EPN pairs are checked and changed based on them. In case the new test patterns provide sufficient toggling, the process is finished. Otherwise, N-Detection tests are run for the VOPs in the netlist with repeatedly increasing the detection level parameter. The EPN pairs are renewed using the additional test pattern set generated by the N-Detection tests. If the desired toggling of the segments is not achieved the last part of the process is repeated until it is achieved. That results in acquiring more EPN pairs with more toggled cells than before, as shown in Figure 10 and Figure 11.

Circuit	Number of segments	LOC patterns	EPN pairs (Initial)	EPN pairs (Additional)
s35932	10	380	238	658
s38417	10	1778	717	1641
AES-128	42	19488	34119	58764

Fig 10: Results of the EPN pairs created [2]

The final EPN pairs and test pattern set are applied on the IC being checked for a HT presence and the authentication is provided by checking the power consumption between the pairs. If the power difference is significant the existence of a HT can be confirmed, although it is acknowledged that two neighboring segments might not provide a sufficient power difference.

Circuit	No. of routed cells	No. of untoggled cells before VOP	No. of untoggled cells after VOP
s35932	4861	6	0
s38417	5019	4	0
AES-128	169281	131	0

Fig. 11: Number of untoggled cells after using VOPs [2]

The Figure 12 summarizes the results from testing the proposed technique. Since the current method is an extension of the previous method form Hossain, the results from the EP are included for comparison. The low, average, high detectability for the EPN indicates three variation cases, where the tests took place.

Circuit	Max RPD(%)	Detectability (%)			
		EP	EPN		
		Low	Low	Average	High
S35932	16.05	65.14	100.00	100.00	99.94
S38584	14.43	24.09	100.00	99.97	99.14
S38417	34.22	100.00	100.00	100.00	100.00
b19	12.74	2.74	100.00	98.53	91.52
AES-128	11.42	0.20	98.14	80.91	64.27

Fig. 12: Experimental results of the EPN technique [2]

3.3: HT Detection using Multiple Parameter Side-channel analysis.

3.3.1: Technique Introduction and Testing Specifications.

In [16] a noninvasive HT detection technique utilizing multiple parameters, mainly the maximum operating frequency (F*max*,) and the transient supply current (I*ddt*), side-channel analysis to counteract the process variations. The technique is developed around the concepts that a golden design is available for test vectors generation, some golden chips can be found among the manufactured ICs under testing by destructive reverse-engineering and that from the die-to-

die variations only the ones in transistor threshold voltage (Vth) are considered. The rest of them can be modeled as variations in Vth. The golden design is used for setting the golden trend line in presence of process variation induced noise.

For testing the effectiveness of the technique both simulation verification and an FPGA-based measurement setup for hardware validation were used. As far as the simulation test is concerned two test cases were used, an AES cipher circuit and a 32-bit pipelined integer execution unit (IEU) both mapped to a LEDA library. The AES cipher has an area of a bit over 25,000, two-input NAND gates and 30% of the overall area is occupied by memory elements. The IEU has an area of about 20,000 two-input gates. To ensure technology scalability both 250-nm TSMC models and 70-nm predictive technology model (PTM) [29] were used. For the Trojans to be detected four types were used. Three of them are sequential Trojans, the first being 24 flip-flops (Type I), the second 10 flip-flops (Type II) and the last 3 flip-flops (Type III) taking their clock signal from nodes of the circuit with rare values. The last one is a small combinational 8-bit comparator circuit (Type IV), corresponding to the 0.04% of the AES circuit area. For the hardware validation the FPGA device used was the Xilinx Virtex-II XC2V500 fabricated in 120-nm CMOS technology. The test circuit mapped on the FPGA was the 32-bit IEU with a five-stage pipelined multiplier, using 90% of the FPGA slices. The HT inserted was a sequential counter circuit with its size being varied between 256 flip-flops, 1.76% of the design size, and 4 flip-flops, 0.03%.

3.3.2: Multiple Parameter Detection Technique.

The idea behind the technique developed in [16] is that checking only one parameter for deducing whether a HT is present can be misleading because of the process variations so two-parameters are utilized. The I*ddt* and the F*max* were used for that reason. The F*max* is used to calibrate the process noise. Usually the delay of longest path is used to calculate the F*max* but in reality, any path in the circuit can be used to calculate the delay, thus reducing the chance of the adversary figuring out the delay used for calibrating the process noise. The way to counteract this is knowing the process variation for each and every path of each chip, which is a difficult piece of information to get before the fabrication of the chip [30]. As a way to achieve better sensitivity the leakage current (I*ddq*) can be taken into account.

Monte Carlo simulations were performed in HSPICE, with inter-die variations being σ = 10 % and intra-die variations being σ = 6% in Vth, on the golden designs and a trend line was calculated from the spread in I*ddt* values for a fixed F*max*, value by using polynomial curve fitting in MATLAB. The limit line, which defines the sensitivity of the Trojan detection of the technique, is computed by scaling the trend line by the spread factor. The spread factor is found by using the mean and standard deviation of the actual spread in I*ddt* values for a given F*max*. A HT is detected in the case it consumes extra current over the limit line.

In the left half of the Figure 13 the steps of the proposed method are shown in detail.

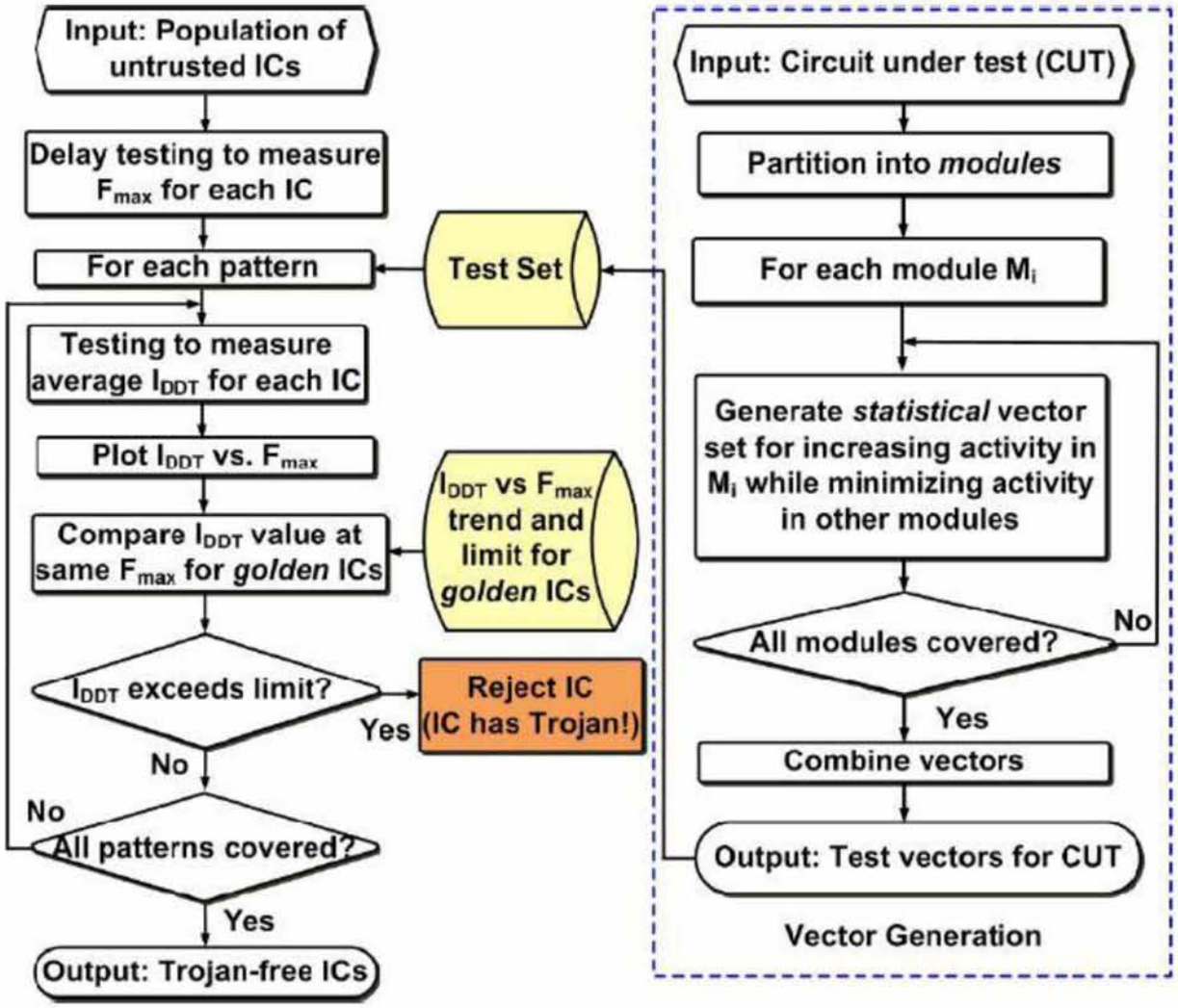


Fig 13: Overview of the multiple parameter detection technique [16]

To complement the multiple-parameter approach and enhance its detection sensitivity a vector generation method based on the statistical test generation approach (MERO) was presented [31]. It composes a set of patterns with the goal of heightening the activity of the Trojan circuit and minimizing the background noise, providing better signal-to-noise ratio, following the steps shown in Figure 13. The first partition into modules step is based on their input dependences. If a large segment exists then extra partitioning is done using existing region-based approaches that aim to keep the segments large enough to neutralize the random parameter variations while still being small enough to keep in check the background current and to help increase the activity of one segment and keeping the activity of the rest low.

After that the test vectors are generated with the conditions that they should activate one segment at a time keeping the rest of them as inactive as possible and that they should trigger rare conditions to try to activate a trojan. For every segment input vectors are generated, using a graph-based functional simulation approach, and are sorted based on the first condition. Then, from those input vectors the ones covering rare trigger signals, possibly trigger conditions for a Trojan, and that can achieve the rare values enough times for increasing the activation possibility of the potential HT are chosen. When all the regions have gone through the process all the vectors are gathered and the method is complete.

The Figure 14 illustrates the results from running tests on simulations in the AES. The trojan size is shown in comparison to the whole of the circuit. I*ddq* refers to the leakage current consumed by each type of HT used for testing. The last two columns show the sensitivity achieved. Figure 15 give the same kind of information for the simulation tests in the IEU.

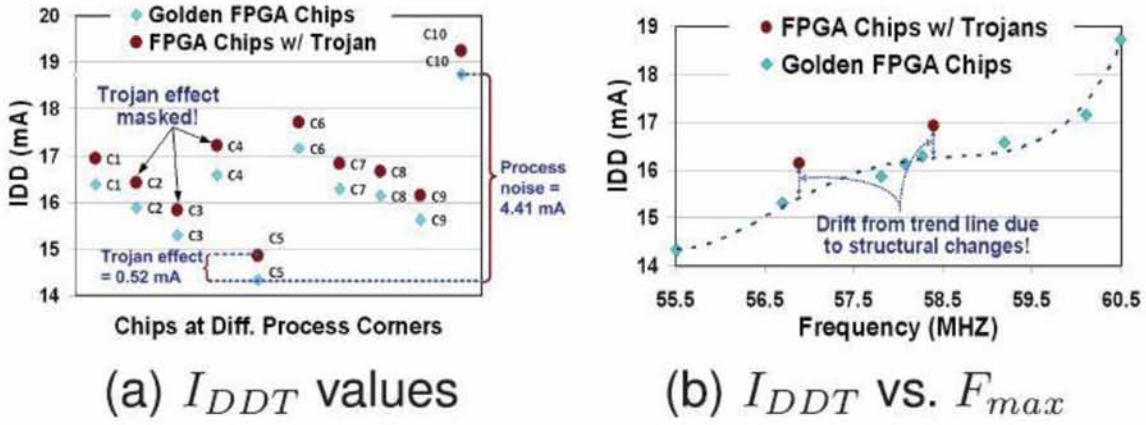
Trojan Type	Trojan Size	Sensitivity	
		w/o gating	w/ gating
I (seq, 24-FF)	1.10%	2.63%	12.20%
II (seq, 10-FF)	0.40%	1.70%	8.60%
III (seq, 3-FF)	0.11%	0.81%	3.53%
IV (comb, 8-bit)	0.04%	0.23%	1.12%

Fig. 14: Experimental results of the simulations on the AES [16]

Trojan Type	Trojan Size	Sensitivity		
		I_{DDQ}	I_{DDT} (vec 1)	I_{DDT} (vec 2)
I	14.0%	17.1%	6.79%	12.22%
II	4.0%	6.93%	2.82%	5.92%
III	1.14%	2.00%	1.12%	3.33%
IV	0.5%	0.21%	0.45%	2.01%

Fig. 15: Experimental results of the simulations on the IEU [16]

For the hardware validation using the circuits on FPGAs the experimental results are shown in the Figure 16. The data were collected from 10 FPGA chips, where 8 were confirmed trojan free and 2 had 16-bit sequential trojan. The Figure 16.a illustrates that just by considering the I*ddt* values the trojan may not be discovered because of the presence of process variations. On the other hand, following the proposed technique and using the relation between I*ddt* and F*max* the detection of the trojan infected chips were easily detected, as shown in Figure 16.b.



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

Fig. 16: Experimental results on the FPGAs. (a) the values from the IC under test are compared only with the I*ddt* values (b) the values are compared with the I*ddt* and F*max* trend line[16]

Chapter 4
OBSERVATIONS

4.1: Discussing the Methods.

The first method mentioned entails scan chain reordering using a clustering technique while having the physical layout, creating scan segments by clock-gating, and adding the hardware so that can be achieved. Then the TDGPs are created, applied to the golden IC to get the reference values and to the manufactured ICs to check for the existence of a HT, by comparing them. The tests run and their results show an improvement of the detection sensitivity almost 4 times better using this segmentation technique. However, this technique requires a Golden IC, which is a very difficult thing to come around and it includes the need for extra hardware to be inserted on the design. Although for the testing of this technique the hardware overhead is low, on other circuits the amount of extra hardware might be prohibiting for actual industrial usage.

The next one creates segments choosing gating points in the clock tree and then, through simulations, creating equal-power pairs between these segments. Test patterns are then applied to the manufactured circuits and the power values are measured. The authentication is achieved by comparing the power values between the equal-power paired segments. The results of the tests show that in case of a sequential HT the detectability is high but in the case of a sequential the method proposed is not as successful. On the other hand, by creating and using the EP pairs the need of a Golden IC is eradicated, making it a more viable option

The third technique is an enhancement of the EP pairs. The partitioning is created based on the clock tree. The segments with equal power are found once again but instead of searching in the whole of the circuit only neighboring segments are take into consideration. With that the intra-die variations are diminished, making the detection sensitivity higher. Choosing neighboring segments leads to fewer test patterns so extra methods, like virtual observation points and N-Detect tests, are used to get sufficient toggle. Following this technique, the previous method is improved since even more of the process variations are diminished even if the test pattern generation is getting a bit more complicated.

The last one is based on the logic that even if the process variations mask the effect on a single parameter from trojan, a relation of two or more parameters will be masked by them. Following that logic, the relation between I*ddt* and F*max* is chosen, so their values are measured from a batch of Golden ICs and are correlated to get a trend line. F*max* can be measured from any possible path in the IC, not just the longest one, to reduce the chance of an attacker guessing it. Every other IC under question has its I*ddt* vs F*max* plot compared to determine whether a HT is present in the tested IC or not. A complementary method of generating test vectors was also presented to heighten the sensitivity, as well as the use of a third parameter, I*ddq*, for reference. The testing of this method was done with simulations and on FPGAs. The fact of a Golden IC to get the accurate values of I*ddt*, F*max* and possible of I*ddq*, gives this technique a small disadvantage, since acquiring one is difficult.

4.2: Conclusion.

HTs are known for over a decade but the need of methods to detect the presence of one has increased the last years with the increase of outsourcing the manufacturing of ICs to third-party manufacturers. Checking side channel analysis parameters, especially voltage drop analysis, is one of the ways to determine the presence of a HT.

The biggest challenge to overcome with detection techniques using voltage drop analysis is the noise created by the random process variations created after the actual manufacturing of a circuit. Process variations can be either intra-die, meaning variations occurring in the same die, or inter-die, meaning variations occurring between different dies. The latter is a challenge because one of the ways to authenticate the presence of a trojan is through the usage of a Golden IC. To avoid the inter-die variations, some self-authenticating techniques have been developed.

In this thesis four techniques where presented, two requiring a Golden IC for authentication and two being self-authenticating. All of them achieve good levels of detection sensitivity and parts of them can be used in other techniques and methods to help achieve better results. Since the last years more attention has been brought to the matter of hardware security, more and better methods and techniques will keep emerging to ensure trojan free ICs.

REFERENCES

1. K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor. "Hardware Trojans: Lessons Learned after One Decade of Research." *ACM Transactions on Design Automation of Electronic Systems (TODAES)* 22, no. 1 (2016): 1–23.
2. Fakir Sharif Hossain. "Variation-Aware Hardware Trojan Detection through Power Side-Channel Analysis." Nara Institute of Science and Technology, 2018.
3. G. Di Natale, S. Dupuis, and B. Rouzeyre. "Is Side-Channel Analysis Really Reliable for Detecting Hardware Trojans?," 2012.
4. U. Guin, Z. Zhou, and A. Singh. "Robust Design-for-Security Architecture for Enabling Trust in IC Manufacturing and Test." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 26, no. 5 (May 2018): 818–30.
5. J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. "Security Analysis of Logic Obfuscation," 83–89, 2012.
6. M. Tehranipoor, and F. Koushanfar. "A Survey of Hardware Trojan Taxonomy and Detection." *IEEE Des. Test Comput.* 27, no. 1 (February 2010): 10–25.
7. F. Koushanfar, and G. Qu. "Hardware Metering," 490–93, 2001.
8. A. B. Kahng et al. "Constraint-Based Watermarking Techniques for Design IP Protection." *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* 20, no. 10 (October 2001): 1236–52.
9. R. W. Jarvis, and M. G. McIntyre. Split manufacturing method for advanced semiconductor circuits. Patent 7 195 931 B2, issued March 27, 2007.
10. Ghobad Zarrinchian, and Morteza Saheb Zamani. "Latch-Based Structure: A High Resolution and Self-Reference Technique for Hardware Trojan Detection." *IEEE Transactions on Computers* 66, no. 1 (January 1, 2017).
11. M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder. "Acoustic Side-Channel Attacks on Printers." Washington, DC, USA, 2010.
12. S. Chen, R. Wang, X. Wang, and K. Zhang. "Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow," 2010.
13. D. Brumley, and D. Boneh. "Remote Timing Attacks Are Practical," Vol. 12, 2003.
14. L. Lin, M. Kasper, T. Güneysu, C. Paar, and W. Burleson. "Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering," 382–95. Springer, Berlin, Heidelberg, n.d.
15. Fx. Standaert. "Introduction to Side-Channel Attacks," 27–42. Springer, Boston, MA, 2010.
16. S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, G. Wolff, C. A. Papachristou, K. Roy, and S. Bhunia. "Hardware Trojan Detection by Multiple Parameter Side-Channel Analysis." *IEEE*

17. Sowmya yadala. "Process-Voltage-Temperature (PVT) Variations and Static Timing Analysis," n.d. https://asic-soc.blogspot.com/2008/03/process-variations-and-static-timing.html.
18. J. Plusquellic, D. Acharyya, and K. Agarwal. "Measuring Within-Die Spatial Variation Profile through Power Supply Current Measurements," 1–5. IEEE, 2011.
19. N. Drego, A. Chandrakasan, and D. Boning. "All-Digital Circuits for Measurement of Spatial Variation in Digital Circuits." *IEEE Journal of Solid-State Circuits* 45, no. 3 (2010).
20. "Trust Hub," n.d. https://www.trust-hub.org/home.
21. H. Salmani, M. Tehranipoor, and R. Karri. "On Design Vulnerability Analysis and Trust Benchmarks Development," 471–74. IEEE, 2013.
22. B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor. "Benchmarking of Hardware Trojans and Maliciously Affected Circuits." *Journal of Hardware and Systems Security* 1, no. 1 (2017): 85–102.
23. Crouch L. Alfred. *Design-For-Test For Digital IC's and Embedded Core Systems*. Prentice Hall, 1999.
24. N.Z. Basturkmen, S.M. Reddy, and I. Pomeranz. "A Low Power Pseudo-Random BIST Technique." *Journal of Electronic Testing* 19, no. 6 (2003): 637–44.
25. L. Whetsel. "Adapting Scan Architecture for Low Power Operation." In *Proceedings International Test Conference 2000 (IEEE Cat. No. 00CH37159)*, 863–72. IEEE, 2000.
26. J. Shinde, and SS Salankar. "Clock Gating-A Power Optimizing Technique for VLSI Circuits," 1–4. IEEE, 2011.
27. Y. Bonhomme, P. Girard, L. Guiller, C. Landrault, S. Pravossoudovitch, and A. Virazel. "Design of Routing-Constrained Low Power Scan Chains," 1:62–67. IEEE, 2004.
28. Laurenciu, Nikoleta Cucu, Yao Wang, and Sorin D. Cotofana. "A Direct Measurement Scheme of Amalgamated Aging Effects with Novel On-Chip Sensor." *2013 IFIP/IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC)*, 2013, 246–51.
29. "Predictive Technology Model," http://ptm.asu.edu/, 2013.
30. S. Borkar et al., "Parameter Variations and Impact on Circuits and Micro-Architecture," Proc. Design Automation Conf., pp. 338-342,2003
31. R. S. Chakraborty et al., "MERO: A Statistical Approach for Hardware Trojan Detection," Proc. 11th Int'l Workshop Cryptographic Hardware and Embedded Systems, 2009.