Master's Thesis

Random Variation Aware Hardware Trojan Detection Through Power Based Side-Channel Analysis

Syful Islam

September 11, 2019

Graduate School of Information Science
Nara Institute of Science and Technology

A Master's Thesis
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
Master of Engineering

Syful Islam

Thesis Committee:

Professor Michiko Inoue	(Supervisor)
Professor Yasuhiko Nakashima	(Co-supervisor)
Associate Professor Fukuhito Ooshita	(Co-supervisor)
Assistant Professor Michihiro Shintani	(Co-supervisor)

Random Variation Aware Hardware Trojan Detection Through Power Based Side-Channel Analysis*

Syful Islam

Abstract

Hardware security has become a growing concern in the design and test of chips since its manufacturing processes are becoming increasingly vulnerable due to malicious activities and alterations. These malicious addition and modification of circuits done by the intruders are commonly referred to as hardware Trojan (HT). Currently, power based side channel analysis is one of the most promising techniques in detecting HT. Due to elevated process variations as process technology nodes are rapidly scaled down; obtaining high detection sensitivity using power based side channel analysis is becoming a very challenging task. To overcome this challenge, initially the impact of random variation in detecting HT is analyzed. To accomplish this task, Mote Carlo simulation environment is established for analyzing dynamic power distribution due to random process variation. Based on the analysis of dynamic power variation, a new HT detection condition is derived. Afterward, we propose a new HT detection method named as ANP (Arbitrary neighboring test pattern pair comparison) based on the new HT detection condition. Finally, detectability of the ANP method is evaluated by injecting two type of HTs in benchmark circuits. The result shows that, ANP obtain relatively high detectability (ex:100%) for medium size HT (0.3-0.4% to a whole circuit) and 24%-100% for a small HT (0.07%-0.09% for some circuits) in presence of moderate random variation (0-1% relative standard deviation for

*Master's Thesis, Graduate School of Information Science,
Nara Institute of Science and Technology, September 11, 2019.

transistor delays) and still show some possibility of detection for elevated random variation (2-5% relative standard deviation for transistor delays).

Keywords:

Hardware Trojans (HT), Random process variation, Circuit segmentation, Self-referencing, Power based side-channel analysis, HT Detectability

Acknowledgments

First of all, I would like to remember Almighty Allah for making me capable to complete the Master's Thesis.

I would like to express my deepest appreciation to my honorable Professor Michiko Inoue, whose encouragement, guidance and best support from the initial level to final level helped to develop a very good understanding in my research area. She has literally taught me how to do good research and motivated me with great insights and innovative ideas. She has guided me the ways to visualize the problem with all possible angles and to get a deep insight into the topic. Her continual directions have helped me a lot to go beyond recent methods limitations, and come up with a solution which can compete with current methods. I strongly believe, my supervisor did for me what the best supervisors always do for his/her students to make them successful in life.

To my thesis committee, I would like to thank Professor Yasuhiko Nakashima and Associate Professor Fukuhito Ooshita for their valuable comments and discussion to improve my thesis.

I sincerely thank to my co-supervisor Assistant Professor Michiro Shintani, for his continual support and guidance. For me, my co-supervisor is the best tutor for learning many tools specially writing art. His presence always motivated me to work harder and be simple.

In addition, I would like to thank my labmates in Dependable System lab for great help, support, and encouragement from the beginning to the end.

Finally, I would like to express my most sincere appreciation to MEXT, Japan and NAIST international affair division for all kind of supports.

To My beloved Mother and Great Japanese Nation

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

Due to tremendous growth and recent outsourcing trends in the integrated circuit (IC) industries, malicious alternations like hardware Trojan (HT) has become a significant threat for IC security and reliability. Thus, the hardware security to ensure trust in ICs has emerged as an important research topic in recent years. Unfortunately, the detection of malicious inclusions is challenging for several reasons, such as nanometer IC feature sizes and system design complexity. Besides, the adversary may insert the HT in a small number of chips from a large batch of fabricated chips. Therefore, HT detection through physical inspection and destructive reverse engineering methods are difficult and impractical [1]. Moreover, HT circuits are designed in such a way that it will be activated under very rare conditions [2]. Hence, it is also very difficult to fully activate them by applying the functional test pattern set. On the other hand, the side-channel based analysis facilitates HT detection by reflecting partial activation effect of the HT circuits through the side-channel parameters. However, the side-channel parameters deviate from their nominal values in the manufactured ICs by natural phenomenon termed as process variations. Figure 1.1 shows the main hindrance in detecting HT. In the Fig. 1.1, we observe that the number of element in HT is too small compared to the total number of elements in IC. In addition, the IC is affected by process variation. Therefore, the power increase due to the HT partial activation by applied test pattern is difficult to differentiate from process variation affected HT free IC as shown in Fig. 1.1. In the Fig. 1.1, green line represents power obtained from HT free IC and the red line represents power obtained from HT affected IC.

Traditionally, dynamic power has been considered as weakly sensitive to process

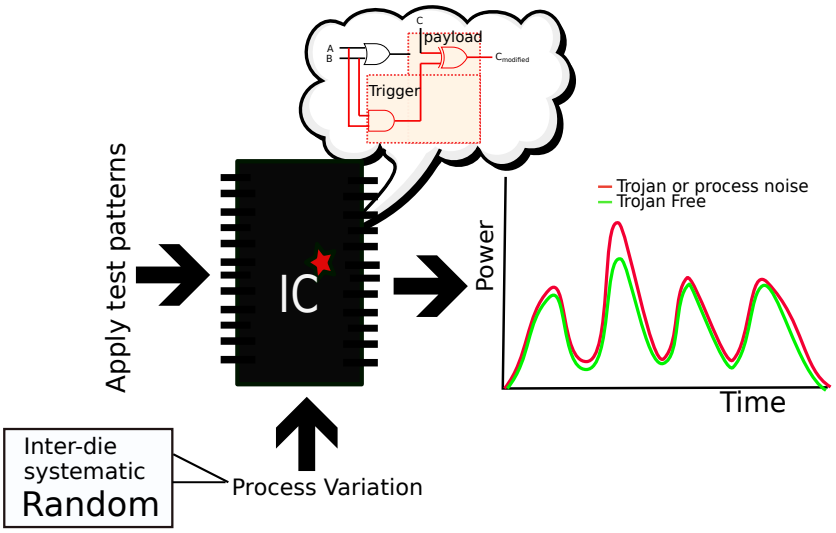


Figure 1.1: HT in ICs with its detection hindrance.

variability [3]. On the other hand, the recent increase in uncorrelated variability sources in ICs due to phenomena like random dopant fluctuation, line edge roughness cause variations in threshold voltage [4] which introduce the random delay variations in combinational logic circuits. Consequently, this uncorrelated delay variability produce transient behaviors which are referred to as glitch effect [3]. The increase in delay variability in circuit, magnifies glitch effect and largely contribute to the dynamic power. According to paper [3], within-die uncorrelated delay variability strongly impacts dynamic power. Thus, the HT effect can be masked due to the presence of the elevated level of random process variation through power based side-channel analysis technique, resulting in low detection sensitivity.

1.2 Motivation

Many researchers around the world propose a lot of methodologies to overcome the challenge imposed by process variation in detecting HT [5–13]. Some of them are golden IC dependent and some of them are golden IC free methods. As dynamic power is sensitive to process variation especially to random variation and due to the technology nodes rapid shrinking, the random variation is now

a dominant contributor in dynamic power variability. In addition, most of the researchers do not consider the random variation in detecting HT. Therefore, we proposed a HT detection method considering the random process variation.

1.3 Contribution of the Research

In this research, we propose a HT detection method named ANP (Arbitrary neighboring test pattern pair comparison) considering the random process variation through power based side channel analysis. The proposed method has the following contributions:

- Establish Monte Carlo simulation environment for analyzing dynamic power deviation due to random process variation.
- Introduce the concept of arbitrary test patterns comparison for increasing the chance of HT detection in presence of random variation. From the analysis of dynamic power deviation it is observed that all test patterns are not equally affected by random process variation. We observed that, some test patterns are highly affected by random variation while some of them are less affected. Hence, comparison of test patterns which are not or less affected by random process variation, and test patterns that sensitize HT, will increase the chance of detectability.
- We compare test patterns within a segment to reduced detection threshold further, since comparison of test patterns within a segment help to establish 100% spatial correlation between two regions created in a segment.
- We introduce new HT detection condition considering random process variation.

1.4 Organization of the Thesis

The rest of the thesis is organized in five (5) Chapters. In Chapter 2, we introduce the basic concept of HT, the phenomena in detecting HT and countermeasures against HT. Then, we summarize some related research on side-channel analysis. In Chapter 3, we show detailed flow of dynamic power variability analysis and

the associated results. In Chapter 4, we derive HT detection condition based on analysis and propose ANP method considering random process variation based on the analysis of Chapter-3. In Chapter 5, we summarize the detectability of HT using our proposed method. Finally, in Chapter 6, we conclude the thesis by showing usefulness of our method in presence of random process variation.

2 Preliminaries and Literature Review

In this chapter, we will introduce the basic concept of HT, examples of HT effect, its classification, and the threat model. Then we will illustrate the countermeasures taken by researchers against HT. Afterward, we will describe side channel analysis and the process variation effect on detecting HT. Finally, in the related work part, we will summarize some recent works on side-channel analysis in detecting HT.

2.1 Hardware Trojans

The HT is a malicious addition or modification of a circuit which can cause malfunctioning, leak security key information, performance degradation, or even denial of service of a safety-critical application.

HT has two main parts. These are trigger and payload.

TRIGGER: The activation conditions of the HT are referred to as trigger condition [14]. It is used to feed the HT to start propagating erroneous value to the original function of a circuit through payload. Generally, the trigger is designed in such a way that, it will be activated for some certain conditions.

PAYLOAD: The nodes of the HT circuit used to propagate erroneous value to the main circuit by modifying functionality are referred to as payload [14]. Selection of payload depends on the type of attack intended to be launched into the design of the circuit. An attacker's viewpoint would be finding out a good trigger-payload combination, which creates such HT instance very hard-to-detect.

Based on logical structure, HT can be divided into two types. They are combinational and sequential HTs. The combinational HT solely consists of a com-

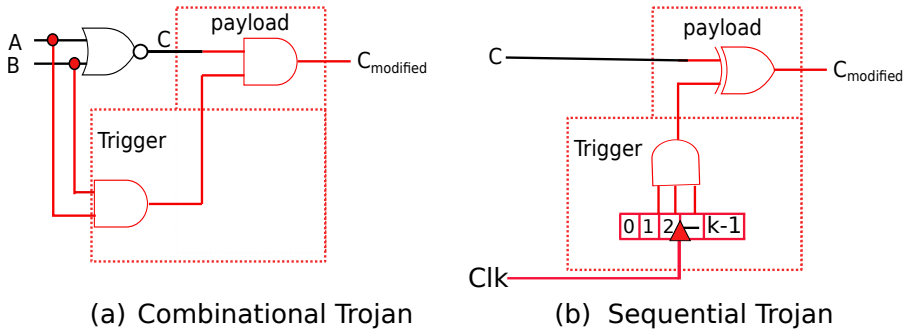


Figure 2.1: Examples of different type of HTs.

bination of logic gates and activated when a particular set of logic satisfies the triggering condition. On the other hand, the sequential HTs are activated due to a sequence of rare events on the internal nodes of a circuit.

Figure 2.1 illustrates the examples of the combinational and sequential HTs. Here Fig. 2.1(a) shows an example of combinationally triggered HT, where the occurrence of condition $A = 0$, $B = 0$ at the trigger nodes A and B causes the payload node C to have incorrect value at $C_{modified}$. Again, Fig. 2.1(b) shows a synchronous sequential k-bit counter HT which acts like a time-bomb. As the counter reaches 2^{k-1} value, the HT will be activated and modify the node C to an incorrect value of node $C_{modified}$.

2.2 Effects of HT

Recently, the HT is becoming a growing concern since it can impose big threats to the security-oriented industries, such as sophisticated medical devices, aircraft manufacturing, and nuclear power plants. Intruders can insert HT in ICs, which may be used in the manufacturing of such systems. Hence, failure of such a system may result in significant damage to properties, environment, and even huge loss of life.

In 2008, an experiment was conducted by the University of Illinois in which researchers designed and inserted a small backdoor circuit that gave access to privileged areas of the memory of the chip [15]. This HT could then be used to change process identifier, that allows hackers to get access to all the data

contained in the memory of the chip. The objective of this research was to understand how financial infrastructures can be vulnerable to HT. HTs of this kind are usually small and very difficult to detect.

In addition to the security industries and financial infrastructures; the consumer industries are also potential targets of an HT attacker. The potential damage that could be caused by such an attack could be enough to disable global corporations, such as the telecommunication network. Moreover, the potential threat to consumer privacy is become a major important issue due to HT. For example, devices such as smartphones and tablets can be hacked by the hackers to steal private information to blackmail users [15].

To prevent these issues, "Trusted Foundry Program" was established to ensure safety-critical equipment's remain free of HT by using the ICs from accredited foundries only. In addition to selecting the foundries, close observation is being paid to the other links in the design and supply chain [15].

2.3 HT Taxonomy

When HTs are non-destructively inserted in any phase of the IC design cycle, the threats remain whenever the system is powered on. It depends on the adversary, the stage of insertion, and the modification an HT would be carried out after infecting the design. Researchers and academicians have gone through rigorous research, and have come down to a detailed level of HT taxonomy, which is most widely accepted among the community. Figure 2.2 shows a detailed classification of different type of HTs depending on various attributes. This comprehensive classification will help us to understand, the possible areas and phases which are vulnerable and also the behavior of HT to understand whether the HT is used for modifying functionality, or gaining unauthorized access to the system.

The physical characteristics category describes the distribution, structure, size, and type of the HT. Based on the physicality characteristics, the HTs can be classified into functional and parametric type. The functional type includes HTs that are physically realized through the addition or deletion of transistors or gates. On the other hand, the parametric type HTs refers to the HTs that are realized through modifications of existing wires and logic of a circuit. Here, the

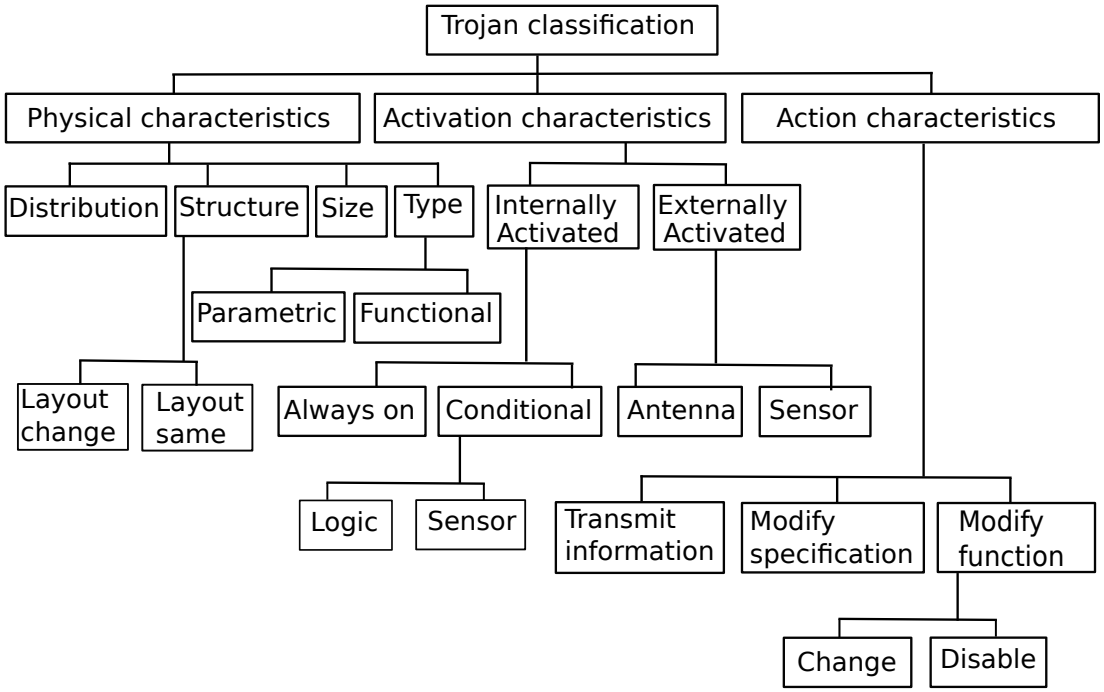


Figure 2.2: Detailed taxonomy based on different characteristics of HT [1].

term size describes the number of elements in the chip that have been added, deleted, or modified. The term distribution describes, location of the HT in the physical layout of the chips. The structure term refers to the cases, where the intruders regenerate the layout of a circuit to insert an HT that can cause different placement for some or all design components.

Activation characteristics refer to the condition which will cause an HT to be activated and carried out its malicious function. Based on the activation characteristics, the HTs can be broadly classified into externally activated and internally activated types. External activation of the HT can be done by the antenna and different types of sensors. On the other hand, internal activation of the HT can be classified into two types, always on and condition-based. Here "Always on" means the HT is always active and can perform propagating erroneous value in the chips function at any time. Again, the condition based subclass includes the HTs that will remain inactive until a specific condition is met. For condition-based HT, the activation condition could be based on the output of a sensor that monitors temperature, voltage, or any external environmental trigger condition

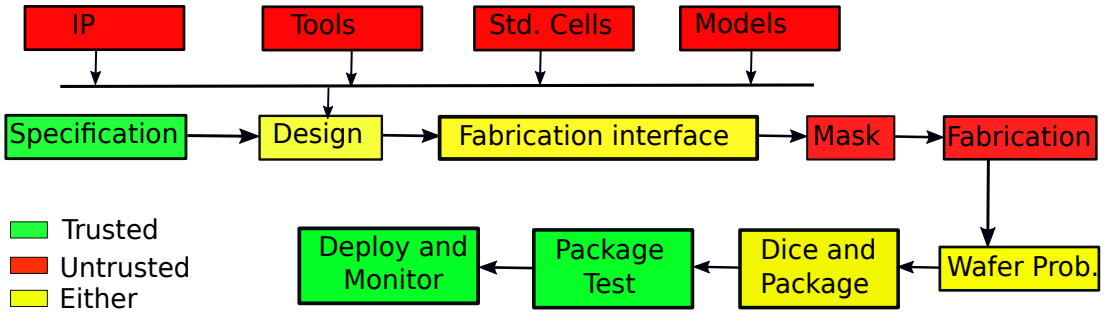


Figure 2.3: Vulnerable steps of modern IC life cycle [16].

such as electromagnetic interference, humidity, altitude, or temperature. Besides, this activation condition could be based on an internal logic state, a particular input pattern, or an internal counter value of an internal or external counter. The HT in these cases is implemented by adding logic gates and/or flip flops to the chip and hence is represented as a combinational or sequential circuit.

Finally, the action characteristics refer to the type of disruptive behavior can be introduced by the HT. Based on action characteristics, HTs can be categorized into transmit information, modify specification, and modify function type. Here, the transmit-information type includes HTs that leaks key information to an adversary. The modify function type refers to HTs that change of the chips functions by adding logic or by removing or bypassing the existing logic of a circuit. The modify-specification class refers to HTs that focus their attack on changing the chips parametric properties, such as delay when an adversary modifies existing wire and transistor geometries.

2.4 Threat Model

Modern ICs have different steps in the manufacturing process. Due to economic reasons, most of the modern ICs are manufactured in off-shore fabrication facilities. Moreover, the current IC manufacturing process involves intellectual properties (IP) core supplied by third-party IP vendor, outsourcing design, and test process as well as electronic design automation tools. Figure 2.3 illustrates the vulnerable steps of modern IC life cycle. Such business model creates a backdoor for intruders to insert malicious circuits in ICs. In this thesis, we consider

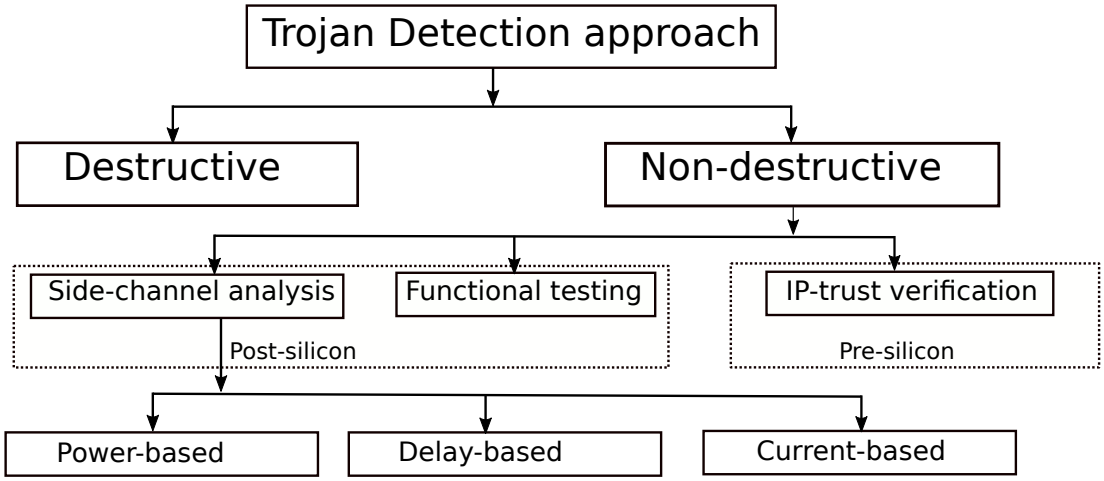


Figure 2.4: Existing HT detection approaches [17].

HTs are inserted in ICs at an untrusted foundry. To develop HT detection technique, we require full control of the design and layout phases. Since the HT detection technique is developed in the design and layout phases, the electronic design automation (EDA) flow is considered trusted to detect HTs effectively.

2.5 Existing HT Detection Approaches

Figure 2.4 illustrates the existing HT detection approaches. According to Fig. 2.4, the HT detection approaches can be classified into two main categories named as destructive and non-destructive technique.

The destructive techniques pick a sample from the manufactured ICs and subjected to DE-materialization using Chemical Mechanical Polishing (CMP) followed by a Scanning Electron Microscope (SEM) image re-construction and analysis [17]. However, the steps of the destructive technique are extremely expensive and time-consuming (destructive analysis of a single chip taking several months) and do not scale well with an increase in transistor integration density. Moreover, the results of analyzing a sample cannot be extrapolated to the entire manufactured lot [17]. Since an adversary might affect only a small population of the manufactured ICs, destructive reverse engineering approaches cannot be effective for the trust validation in ICs. Again, the non-destructive approach

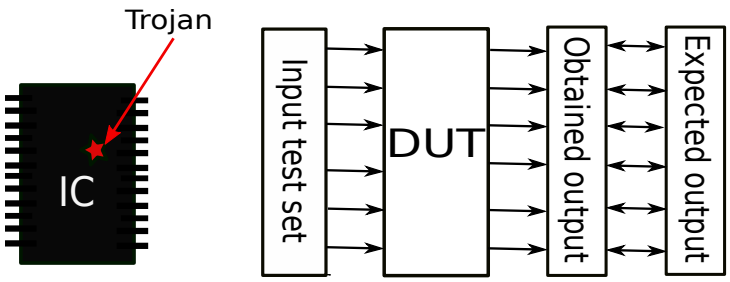


Figure 2.5: Functional testing approach.

is classified into three types named as functional testing, side-channel analysis, and IP-trust verification. Of them, functional testing and side-channel analysis fall into post-silicon category and IP-trust verification falls into the pre-silicon category as shown in 2.4. The detailed explanations are given in the following sub-sections.

2.5.1 Functional Testing Approach

The functional test is conducted through the input-output pins of an IC. The functional test set are generated to activate rare events in the circuit and propagate the malicious effect to the primary output. Figure 2.5 illustrates the concept of functional testing approach. In Fig. 2.5, we observe that a set of the functional test patterns are applied in the target IC and compared the predefined output of the corresponding test patterns. Such an approach is useful to detect small HT under large process variation. The main challenge of functional testing is to generate a triggering condition. Moreover, the exhaustive functional testing is extremely costly and not feasible in large complex ICs [17].

2.5.2 Side Channel Analysis Approach

An alternative to the logic testing approach is to measure the side-channel parameters of an IC like supply current, power, delay, and electromagnetic radiation are referred to as side-channel analysis. Side-channel analysis based methods depend on observing the effect of an HT through physical measurement parameters. Figure 2.6 illustrates the concept of side-channel analysis techniques. In Fig. 2.6, we

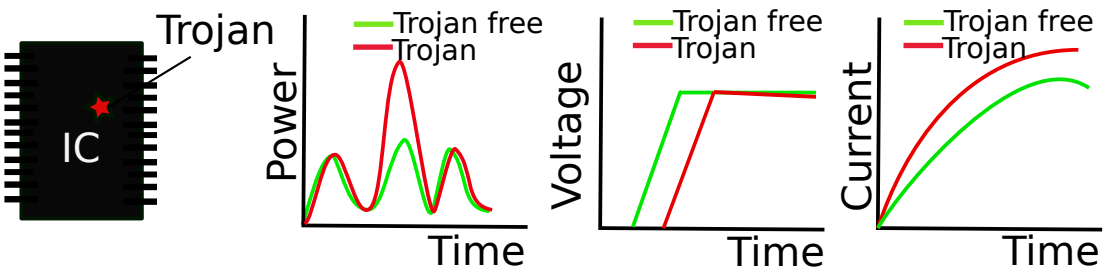


Figure 2.6: Side channel analysis technique.

observe three different side-channel analysis technique based on power, delay and current. Among the three graphs, the left side one is power-based, the middle one is delay-based and the right side one is current based side-channel analysis. The detailed of the three side-channel analysis techniques are described as follows.

When extraneous circuits are added, the delay profile of the main circuit is affected by a particular triggering condition and thus changing the circuit functionality. Based on that assumption, some researchers proposed different HT detection methodologies.

Again, the current based side-channel investigation is the way toward measuring various characteristics of the design to distinguish the irregularities in the behavior of the circuit. The current that moves through the voltage supply line can be utilized to distinguish any abnormal changes.

Along with other side-channel parameters, the power-based side-channel investigation is the way toward measuring various characteristics of the design identified with the power consumption. It has been successfully used to distinguish the irregularities in the behavior of a circuit. The total power consumed in a circuit is the sum of dynamic and leakage power. Here, dynamic power is the power of switching gates in an IC. It depends on capacitance loading-unloading of transistors. Besides, dynamic power has a linear relationship to the number of gates switching in a circuit. Unlike dynamic power, leakage power is the power dissipated by gates when they are in steady-state in an IC. However, total power consumption shifts with the discrepancy of circuit parametric profile. Among numerous reasons behind the disparity in power profiles, switching gates and process variations are most noticeable. This mismatch is coming from process variation of transistors and interconnects inside the IC. Therefore, reduction in the pro-

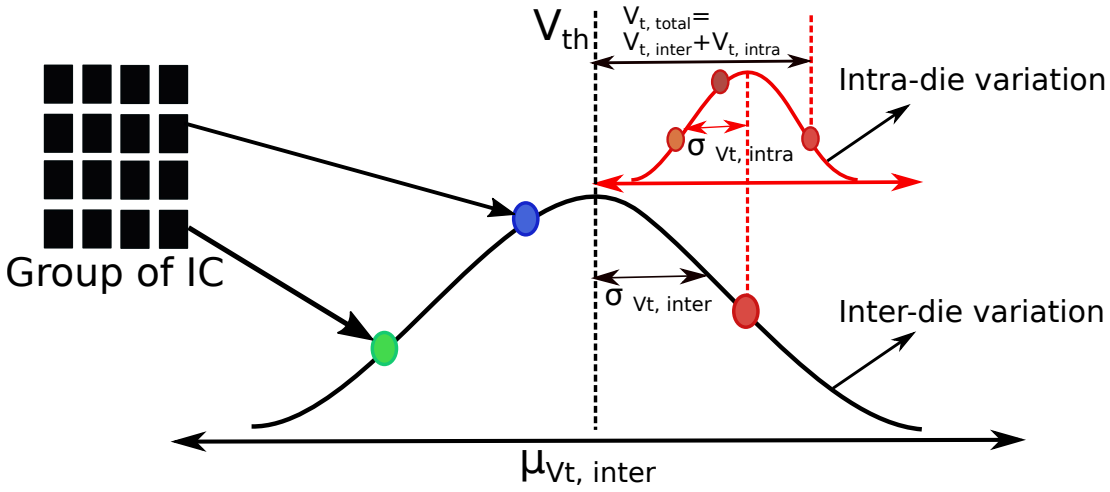


Figure 2.7: Systematic process variation in ICs.

cess variation effects can improve the detection sensitivity in power side-channel analysis.

The advantage of these approaches lies in the fact that even if the HT circuit does not cause an observable malfunction in the circuit during testing, the presence of the extra circuitry can be reflected in some side-channel parameters and facilitate HT detection. Later we will examine several side-channel analysis techniques based on delay, current, and power that have been proposed by different researchers.

2.6 Process Variation

The Process variations are naturally occurring phenomenon during IC fabrication process. The main sources of variations are gate oxide thickness, random dopant fluctuations, device geometry, and lithography in the nanometer region. Due to the variation in different parameters of transistors like length, width, oxide thickness; the measured values deviate from their nominal values. Process variation can be broadly classified into two categories named as systematic and random variations [3].

2.6.1 Systematic Process Variation

The variation that depends on the location is referred to as systematic variation, i.e., systematic variation has spatial co-relation [3]. Systematic variation can be broadly classified into two categories: inter-die and intra-die systematic variation. Figure 2.7 illustrates the systematic process variation in IC for inter-die and intra-die cases. According to the Fig. 2.7, the systematic variation of threshold voltage (v_{th}) vary from inter-die and intra-die basis, where inter-die ($\sigma_{vt,inter}$) variation is dominant compared to intra-die systematic variation ($\sigma_{vt,intra}$).

Inter-die Variation

The inter-die variations occur from one die to another die, meaning that the same device on the different die has different features [18]. The variations due to the manufacturing processes are the main sources of IC performance variability. An example of inter-die variation is, one chip operates faster than another.

Intra-die Variation

The variation that occurs among the various elements inside the same chip is referred to as intra-die variations. It occurs in certain areas of the chip, either due to design (layout) characteristics or due to some artifact of manufacturing, such as cross-chip gradients [19].

2.6.2 Random Process Variation

The random variation is also related to the manufacturing imperfections that occur randomly across the chip. This uncorrelated variability affects each transistor of the IC independently on a within-die basis. Generally, random variation arises from extrinsic causes like manufacturing control and intrinsic cause like random dopant fluctuation and line edge roughness [20], etc. The random variation can be further categorized into two types named as short-range mismatch and random across the chip.

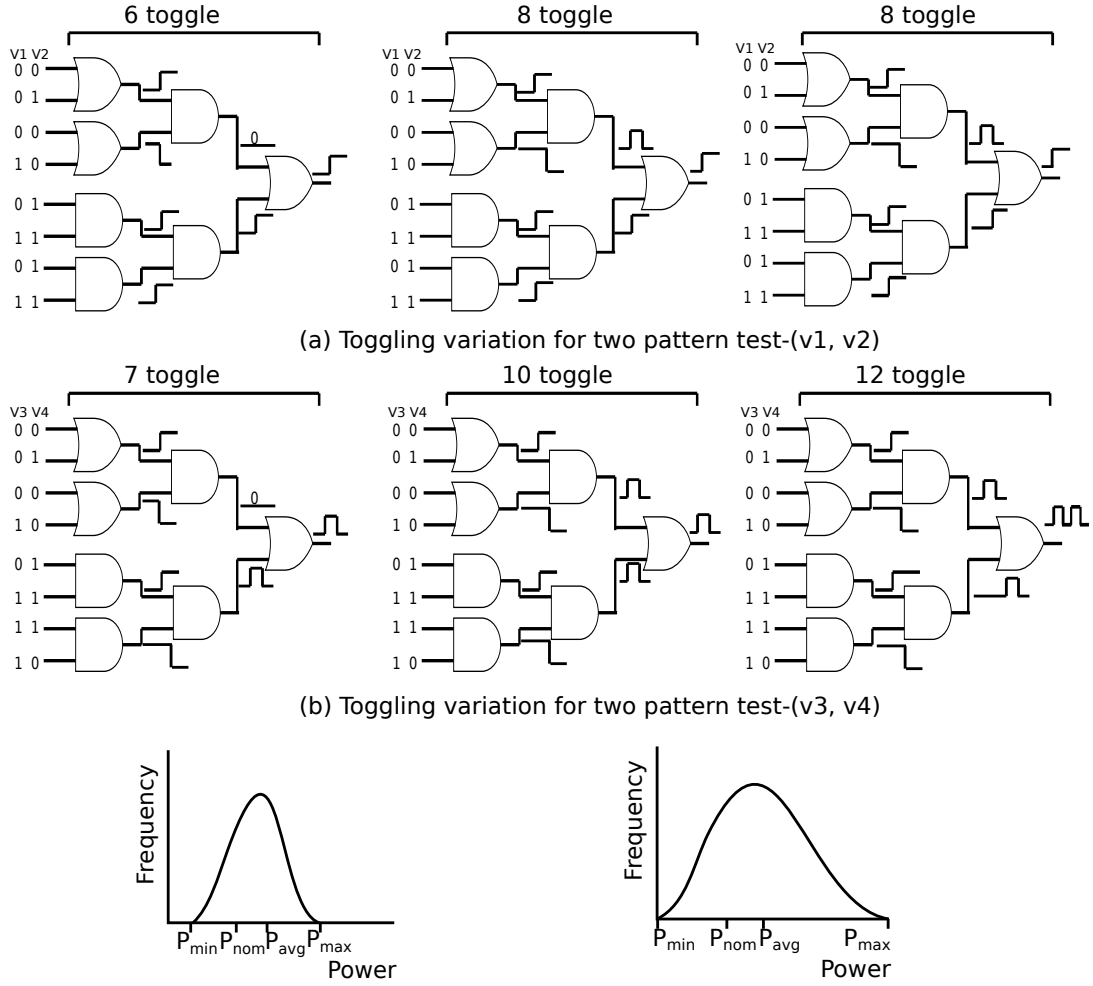


Figure 2.8: Random variation effect on dynamic power.

2.7 Random Variation Effect on Dynamic Power

The random process variation causes delay variation in the circuit. This delay in combinational logic produces transient behaviors known as glitch [21]. Glitches are responsible for consuming a significant amount of dynamic power. This spurious transition activity in the gate output can be generated or propagated type glitch. The glitch that occurs at the gate output due to the imbalance in input arrival times is called generated glitch [22]. On the other hand, a glitch that is transported from one of the gate inputs to another is referred to as propagated

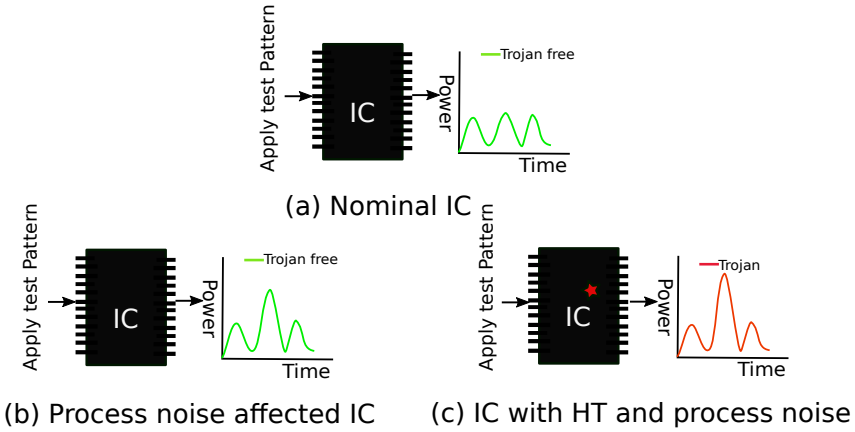


Figure 2.9: Partial activation of HT and its effect.

glitch. Due to the effect of generated and propagated glitch in the circuit, toggling variation occurs. Since dynamic power is proportional to switching activity and width of glitch, the power variability will be increased with toggling variability.

Figure 2.8 shows the effect of toggling in the dynamic power variation. In Fig. 2.8, we have three samples of a circuit with different delay variations. To show how the toggling vary, we pick two pattern tests ($v1$, $v2$) and ($v3$, $v4$). Here in ($v1$, $v2$) and ($v3$, $v4$), the first patterns (ex. $v1$) is used to initialize the circuit, and the second pattern (ex. $v2$) is used to launch transitions. We apply this two pattern tests to the sample circuits. From Fig. 2.8(a), we observe the toggling variation (6, 8, and 8) for the two pattern test ($v1$, $v2$) while in Fig. 2.8(b) the toggling variation (7, 10, and 12) for the two pattern test ($v3$, $v4$). It is observed that the two pattern test ($v1$, $v2$) is less sensitive to random variation than the two pattern test ($v3$, $v4$). As a result, the dynamic power variation will be high for the two pattern test ($v3$, $v4$) due to generated and propagated glitch as shown in Fig. 2.8(c) and 2.8(d).

2.8 Challenges of Side Channel Analysis

The main challenges associated with side-channel analysis are large process variation in modern nanometer technologies and measurement noise, which can mask the effect of the HT circuit, especially for small HTs. Figure 2.9 illustrates how

the process variation noise can impose challenge in HT detection. According to the Fig. 2.9, we have three sample chips, where two is HT free and another is HT affected. Figure 2.9(a) shows the power obtained from nominal chip and Fig. 2.9(b) shows the power obtained from the chip, where there is a high power pick compared to other picks due to the effect of process variation. If we compare power obtained from HT affected chip and nominal chip, we can easily differentiate the HT chip from the HT Free chip. But, there is no practical existence of nominal chip. Hence, considering process variation if we compare power obtained from the HT affected chip and the HT free but process variation affected chip, the partial activation of HT is very difficult to differentiate as shown in Fig. 2.9(b) and Fig. 2.9(c). Therefore, a successful HT detection requires both overcoming the challenges imposed by process noise and increasing the chance of HT activation to get higher power difference from the HT free circuit.

2.9 Related Works

There exist several methods based on side-channel analysis parameters (such as delay, current, and power) to detect HTs. These methods can be broadly classified into two categories named as golden IC dependent and golden IC free methods.

2.9.1 Golden IC Dependent Methods

In [5], the IC fingerprinting concept is introduced. To obtain HT free ICs, a limited number of ICs are reverse engineered to ensure they are HT Free. Then, random test patterns are applied and the power measurement is performed. Once the reference signature is obtained, the same random patterns are applied to ICs under authentication. This method is dependent on HT to circuit size. Therefore, in the presence of elevated process variation; the effect of small HT will be masked.

In [6], a path delay based behavior-oriented HT detection method is proposed and divide the HTs into two categories named as explicit payload HT and implicit payload HT. The path delays of nominal chips are collected to construct a series of fingerprints, each one representing one aspect of the total characteristics of a genuine design then chips are validated by comparing their delay parameters to the fingerprints. The comparison of path delays makes small HT circuits

significant from the delay point of view for the explicit type of HTs. This method needed to be developed further if detection of implicit payload HTs required.

To increase HT to circuit size ratio, some researchers introduce the concept of circuit segmentation. In [7], an HT detection method is proposed, where segmentation is done for the whole design by creating many small regions to detect HTs more effectively. Then, test patterns are applied to the targeting regions to maximize toggling activities in the HT suspected region. The main limitation of this method is the number of regions can be too high for a large circuit; hence, the computational complexity will be increased.

In [8], a scan-based segmentation technique is proposed. In this method, a fine-grained scan based circuit segmentation is done to enhance the HT-to-circuit power consumption while reducing the various effects in the detection threshold. The aim of performing the circuit segmentation is to selectively activate a segment and freezing the others to restrict background noises. Finally, a test pattern application technique is adopted to activate a segment at launch cycle in a launch-on-capture (LOC) mode. Here, at LOC mode the transition at the fault sites is launched in the capture period and the launch vector is derived from combinational logic.

All the methods mentioned above are golden IC dependent, therefore they are highly affected by process variation noise. Also, due to the stealthy nature of the HTs, detecting small HT is a challenging task.

2.9.2 Golden IC Free Methods

To overcome the challenge imposed by process variation due to golden IC dependency, some of the researchers propose golden IC free HT detection methods.

In [9], an on-chip power monitoring structure by placing ring oscillators in the chip and performing statistical analysis of the data from different locations is proposed. Although this technique eliminates the necessity of golden ICs, effectiveness is highly dependent on the accuracy of the number of ROs and used a statistical model.

A structural self-similarity blocks based analysis is presented in SeMIA [10]. This method partitions circuits by functionally similar blocks and activates two adjacent blocks to compare within the chip. The dynamic currents are compared

between two identical structures and the deviation due to the HT attacks are observed. As blocks are functionally partitioned, this method depends on the structure of the circuit.

Another authors propose a statistical test generation technique named as MERS [11]. The methodology is based on the concept of statistically maximizing the switching activity in all the rarely triggered circuit nodes. They showed that the switching current consumed by HTs could be boosted by switching rare nodes multiple times. Multiple excitation's of rare nodes in a circuit are explored with N-detect test patterns to increase cell toggling of low controllable nets. The detectability of this method depends on HT to circuit ratio i.e. if the HT is very small and then a small percentage of HT activation can be masked by the high process variability. Hence, improving the HT to circuit ratio is very important. Therefore, an improved detection sensitivity remains as a significant outstanding challenge for the HT detection technique.

In [12], a golden IC free technique named as equal power (EP) method is proposed. Self-referencing is done through a novel clock-tree based circuit partitioning. The EP method helps to eliminate the inter-die variation effect to increase HT detection sensitivity.

Then in [13], intra-die variation aware self-referencing is proposed. Here, an equal-power neighboring pattern selection is proposed to minimize the effect of intra-die systematic variation in the detection threshold and thus increasing more HT detection sensitivity.

In summary, it can be expressed that an increased HT detection sensitivity in the power side-channel analysis can be accomplished through three observations. They are increasing the HT-to-circuit power consumption; diminishing the variation effect in the detection threshold, and increasing the number of toggling for HT cells. In addition, from the above literature review, we observe that none of the methods address the random process variation effect. Throughout this thesis, we consider every one of these factors, including random process variation, to enhance the HT detection sensitivity.

3 Dynamic Power Variability Analysis

In this chapter, analysis of the dynamic power variability due to random process variation is discussed. During the study, we will introduce with benchmark circuit specifications, clock tree-based circuit segmentation, and test pattern generation since they are important parts of the dynamic power analysis. Then by adopting Monte Carlo simulation and best fit distribution finding program, we will observe the distribution and deviation of dynamic power per test pattern to reveal the necessity of addressing random process variation in HT detection.

3.1 Dynamic Power Analysis

The dynamic power dissipation of a CMOS VLSI circuit depends on the signal activity at the gate outputs. The activity includes the steady-state logic transitions as well as glitches. Delay variations in combinational logic produces transient behaviors known as glitches. These glitches are responsible for consuming a significant amount of power. To address random process variation in HT detection, analysis of dynamic power variation due to random process variation is essential. The purpose of this analysis is to understand the variability of test patterns due to random variation. We are also aiming to check the distributions followed by test patterns due to random variation. To accomplish this issue, an experimental environment is established. The overall analysis flow is shown in Fig. 3.1. It has two major parts: Monte Carlo simulation with random variation and finding the best-fit distribution. Before moving to Monte Carlo simulation, we will be introduced with benchmark circuit specification, clock-tree based circuit segmentation, and test pattern generation process which are initial setup of dynamic

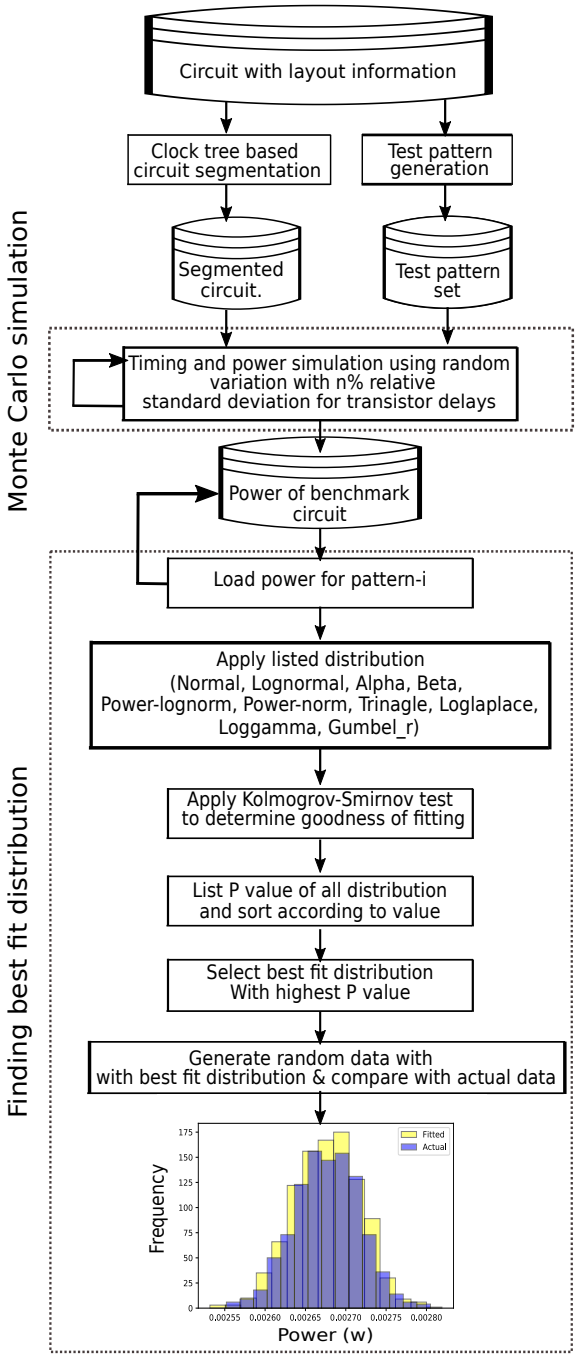


Figure 3.1: Dynamic power analysis.

Table 3.1: Summary of benchmark circuits

Circuits	Number of FFs	Number of logic cells	Total area(μ_meter^2)
s35932	1728	3133	1,01,543
s38417	1564	3455	94,562
s38584	1172	3982	80,108
AES-128	6720	1,62,561	16,31,531

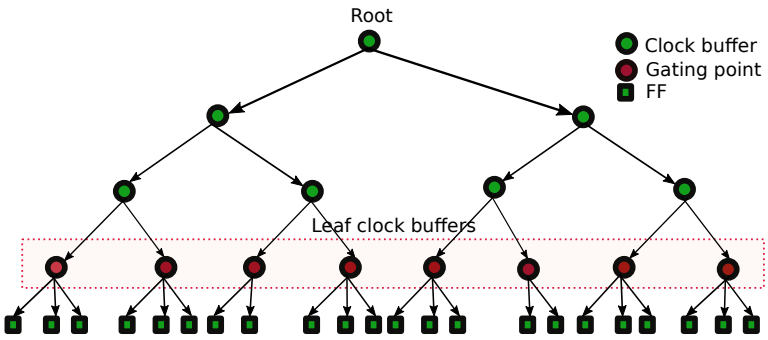


Figure 3.2: Clock tree-based segmentation.

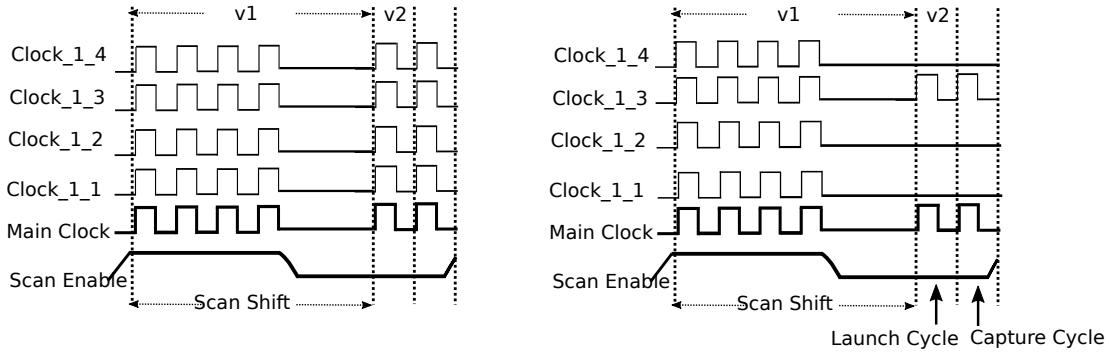
power analysis environment.

3.1.1 Benchmark Circuit Specification

To perform our experiment, we use four benchmark circuits from Trust-HUB [23]. Of them, three benchmark circuits are from ISCAS'89 and another one is AES-128 crypto-processor. The ISCAS'89 circuits are s35932, s38417, and s38584, respectively. Table 3.1 shows a detailed description of the benchmark circuits. The circuits are synthesized using Synopsys design compiler and IC compiler with 90nm technology library.

3.1.2 Clock Tree Based Circuit Segmentation

A segment is defined as a small part of the circuit, where a set of flip-flops (FF) and logic gates are grouped through the clock gating technique. Segmentation is the way to activate a small part rather than activating the whole circuit. To



(a) Typical clock in circuit (b) After applying clock gating technique

Figure 3.3: Activation of small segment of circuit.

accomplish this task, synthesis, placement, and routing are performed using Synopsys tools for the chosen benchmark circuits. Among the three phases, the clock tree is synthesized in the placement phase and then routing is done. Thereafter, the clock tree-based circuit segmentation is done by assigning gating point in each leaf clock buffer. Figures 3.2 and 3.3 show an example of clock tree-based segmentation. The example clock tree has eight leaf clock buffer nodes. Hence, we will assign eight gating points for creating eight segments. The initial state of the clock tree without applying segmentation is shown in Fig. 3.3(a). After application of segmentation, how a particular segment is activated is shown in Fig. 3.3(b). In the Figs. 3.3(a) and 3.3(b), for a two pattern test ($v1$, $v2$), the first pattern ($v1$) is used to initialize the circuit, and the second pattern ($v2$) is used to launch transitions. Table: 3.2 shows the number of segments obtained after application of clock tree-based segmentation approach for each benchmark circuit. The advantage of this approach is to reduce background noise and increase HT to circuit ratio.

3.1.3 Test Pattern Generation

Test pattern generation is an important part of Monte Carlo simulation because effective test pattern generation can deliver higher toggling coverage of a circuit. In the test pattern generation part, we adopt transition delay fault test patterns set since transition delay fault model (Slow to fall and Slow to rise) cares about

Table 3.2: Test pattern per segment summary of three benchmark circuits

Circuit	No of Segments	Test patterns
s35932	10	52
s38417	10	165
s38584	8	244
AES-128	50	454

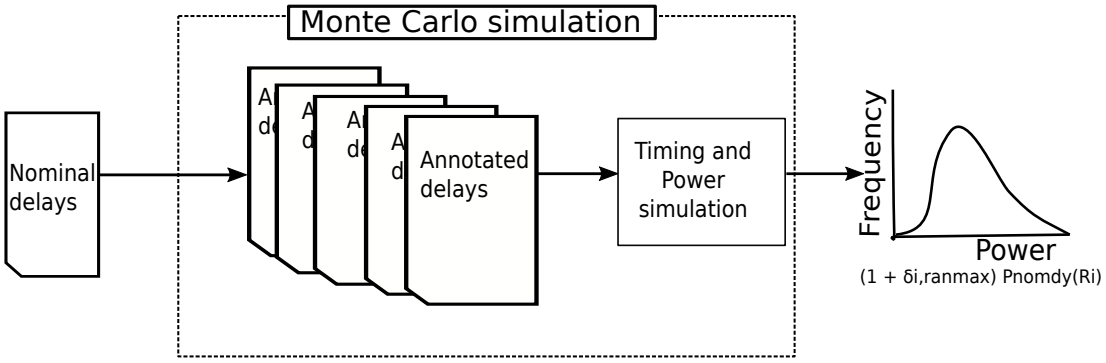


Figure 3.4: Monte Carlo simulation process.

the propagation delay of gates; therefore an accurate dynamic power profile can be achieved. Here, pattern generation is done by Tetramax ATPG tool. Table: 3.2 shows, the number of transition delay fault test patterns obtained for the four benchmark circuits. After application of transition delay fault test patterns by adopting LOC (Launch on capture) test application technique to each segment of the circuit, dynamic power is obtained by toggling of cells of each segment.

3.1.4 Monte Carlo Simulation

In dynamic power variability analysis, the Monte Carlo simulation is adopted as a way to understand the variability of dynamic power due to random process variation. To accomplish this task, random variation with $n\%$ (here n=1,2,3,..,5) relative standard deviation is done by annotating $n\%$ relative standard deviation of transistor delays are added to the nominal delays of every transistor in the benchmark circuits. Then, the timing and power simulations are performed for each variation to obtain dynamic power deviation value. Figure 3.4 illustrates

the concept of Monte Carlo simulation.

3.1.5 Finding Best Fit Distribution

Finding the best fit distribution is the way to learn about the distribution of data. To know the list of distributions which are followed by dynamic power obtained from the Monte Carlo simulation; power values of each test pattern are checked by 10 different distributions (normal, log-normal, alpha, beta, power log-normal, power normal, triangle, log Laplace, log gamma, Gumbel_r, etc.). Then, to obtain the best fit distribution from the applied list of distributions, the Kolmogorov-Smirnov test is applied and sort them according to their P-value. Finally, based on the P-value (largest), the best-fit distribution is chosen. After obtaining the best fit distribution, random samples are generated to observe the goodness of fitting. Figure 3.1 illustrates the flow of finding the best fit distribution per the test patterns of a segment in the circuit.

3.2 Summary of Dynamic Power Analysis

To accomplish the task of dynamic power analysis and obtain best fist distribution, four benchmark circuits s35932, s38417, s38584, and AES-128 (First three segments) circuits are chosen. Then, the Monte Carlo simulation is done using random variation with $n\%$ (here n=1, 2, 3, .., 5, .., 20) relative standard deviation for transistor delays in each segment of the circuit. In addition, the random variation with 0.1874% [24, 25] relative standard deviation for transistor delays are used to address real variability for 90 nm technology ICs. This relative standard deviation of transistor delays are obtained by decomposing the within-die relative standard delay deviation value [24] into systematic (84%) and random (14%) [25] relative standard delay deviations. In random variation with 0.1874% relative standard deviation for transistor delays, the dynamic power variations of the test patterns follow normal distribution except some test pattern while for AES-128 circuit different test patterns follow different distributions as shown in Table: 3.3.

Again, Table 3.4, Table 3.5, and Table 3.6 illustrate the summary of the analysis using random variation with 1-20% relative standard deviation for transistor

Table 3.3: Power distribution for 0.1874% relative standard delay deviation

Distributions	Circuit			
	s35932	s38417	s38584	AES-128
Beta	0	1	2	164
Normal	520	1640	1949	233
Log normal	0	1	0	17
Alpha	0	0	1	86
Power log normal	0	1	0	91
Power normal	0	2	0	176
Triangular	0	0	0	24
Log gamma	0	4	0	282
Gumbel_r	0	0	1	279
Log Laplace	0	0	0	10

Table 3.4: Power distribution for 3% relative standard delay deviation

Distributions	Circuit			
	s35932	s38417	s38584	AES-128
Beta	68	211	259	380
Normal	218	691	993	122
Log normal	17	51	24	85
Alpha	40	0	93	10
Power log normal	51	167	117	268
Power normal	53	132	207	284
Triangular	4	26	22	11
Log gamma	49	151	148	153
Gumbel_r	20	113	89	49
Log Laplace	0	0	0	0

delays for applied test patterns in the benchmark circuits. According to the result it is observed that, as relative standard deviation for transistor delays are increased to 1-20%; the power variability of the test patterns increased and the beta distribution is found as the most frequently followed distribution by most

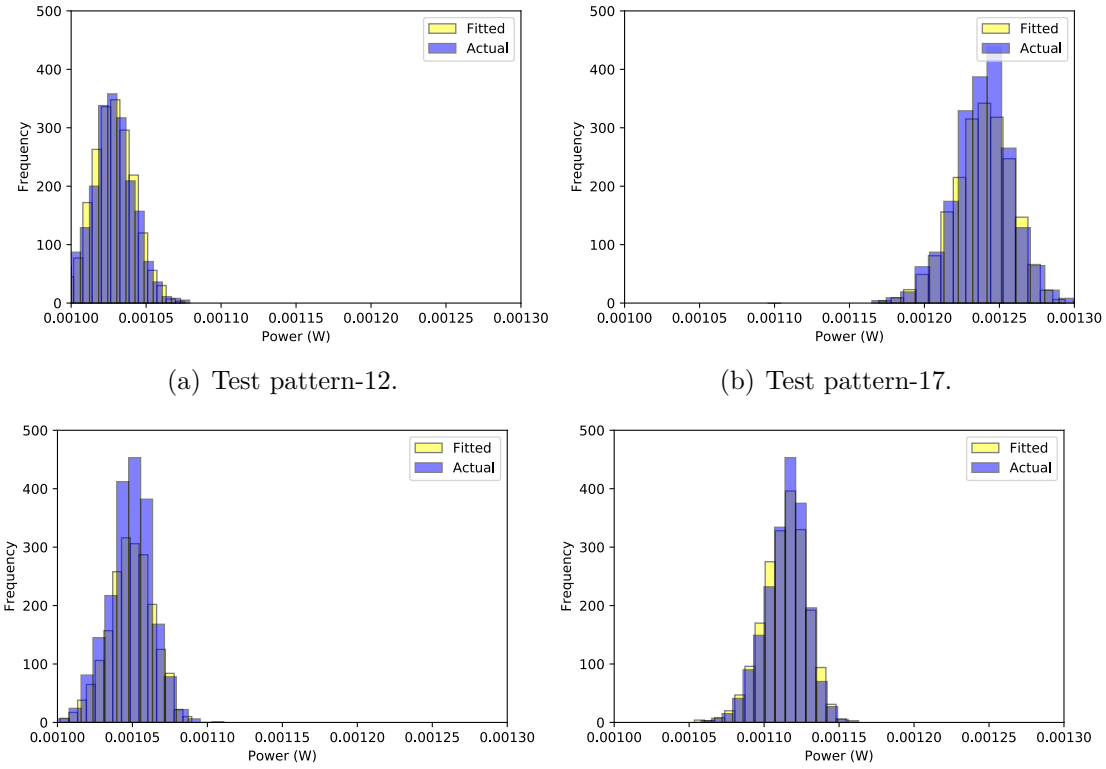
Table 3.5: Power distribution for 5% relative standard delay deviation

Distributions	Circuit			
	s35932	s38417	s38584	AES-128
Beta	168	218	264	342
Normal	64	789	1015	127
Log normal	25	65	53	88
Alpha	17	87	57	26
Power log normal	96	161	141	283
Power normal	113	143	213	300
Triangular	0	20	12	15
Log gamma	21	92	128	149
Gumbel_r	16	75	69	31
Log Laplace	0	0	0	0

Table 3.6: Power distribution for 20% relative standard delay deviation

Distributions	Circuit			
	s35932	s38417	s38584	AES-128
Beta	193	344	551	415
Normal	18	127	213	63
Log normal	95	251	243	75
Alpha	6	0	109	37
Power log normal	86	244	262	288
Power normal	100	139	257	298
Triangular	1	28	24	29
Log gamma	20	119	186	97
Gumbel_r	1	194	125	57
Log Laplace	0	0	0	3

of the test patterns due to random delay variation for the s35932 and AES-128 circuits while normal distribution is most frequent case for s38417 and s38584 circuits. Then, the second most frequent distributions are power normal, power log-normal distribution while a few of the test patterns follow others.



(a) Test pattern-12.

(b) Test pattern-17.

(c) Test pattern-19.

(d) Test pattern-20.

Figure 3.5: Distribution of test patterns for s38584 circuits.

Figure 3.5 shows actual and best fit distributions of four test patterns dynamic power for segment-1 in s38584 circuit.

From the dynamic power analysis, it is observed that different test patterns follow different distributions in the presence of high random process variation. As, different test patterns follow the different distributions and with different deviations, it is impractical to model dynamic power variation using the normal distribution. Since we could not find any universal distribution, we need to apply the Monte Carlo simulation to get the deviation of each test pattern. Therefore, to obtain dynamic power deviation between two test patterns (i,j) due to random process variation, maximum possible deviation range (α_{i,ran_max}, α_{j,ran_min}) is obtained from the Monte Carlo simulation.

4 Proposed Method

In beginning of this chapter, we will introduce the concept of ANP (Arbitrary neighboring test pattern pair) and its usefulness to detect HT in presence of random variation. Then, we will provide a detailed explanation on the derivation of detection condition considering random process variation. Finally, we will propose the ANP method which will be random process variation aware.

4.1 Idea of ANP

In the dynamic power variability analysis, it is observed that dynamic power is highly sensitive to random process variation. Moreover, dynamic power of test patterns follow different distributions with different deviations. In [13], the concept of equal power neighboring is introduced which restrict paring of test patterns among neighboring segments if they are equal. The main limitation of this concept is, they consider dynamic power variation as normal distribution without analysis of its distribution due to random variation. Moreover, comparing test patterns only for equal power pair cases may have the chance to deliver low detectability of HT. Thus, obtaining high detection sensitivity under large random variation is a remaining challenge. To overcome this challenge, we propose the arbitrary test pattern pairing concept by comparing all possible combination of test patterns arbitrarily while maintaining the neighboring relationship. APN pairing concept is useful in random variation perspective since test patterns comparison which are less affected by random variation and test patterns which sensitize HT have higher chance of achieving high detectability. Figure 4.1 illustrates the necessity of arbitrary neighboring test pattern pairing concept for obtaining high detectability of HT in presence of random process variation.

According to the Fig. 4.1, three test patterns t_i, t_j, and t_k are applied in

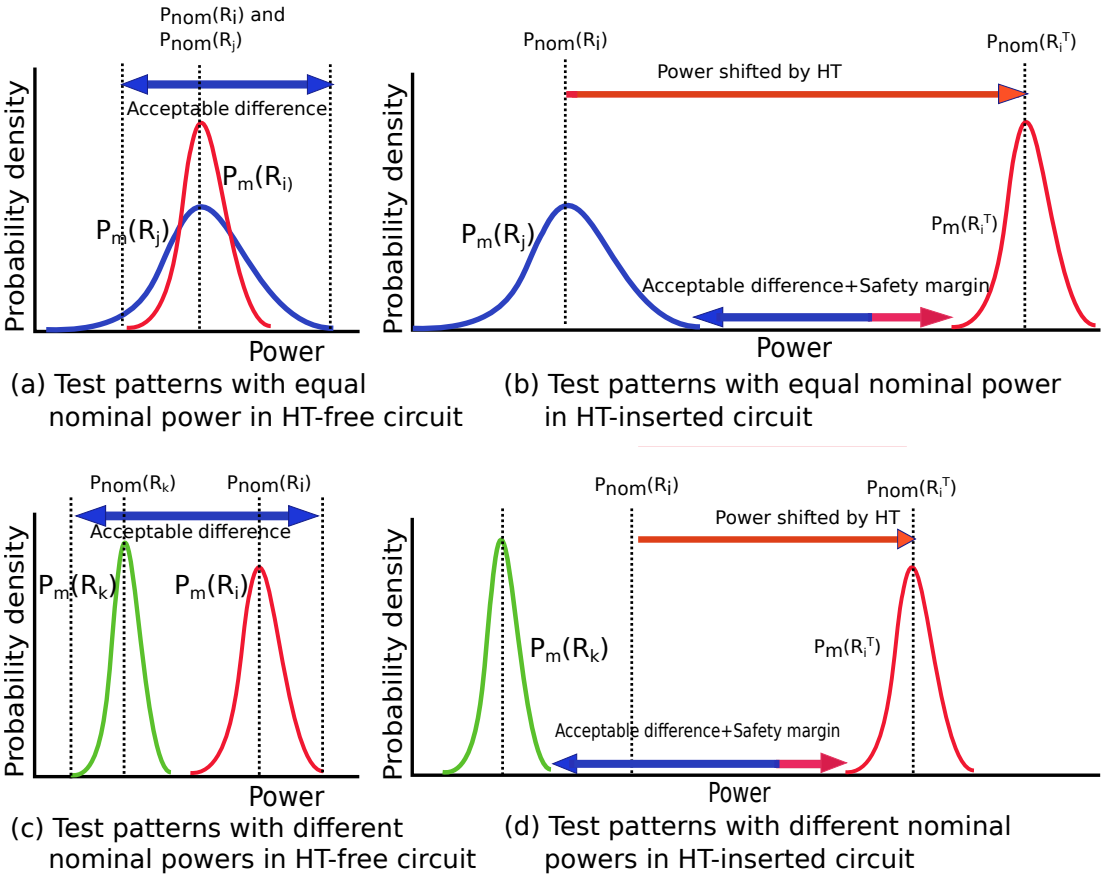


Figure 4.1: The concept of ANP.

neighboring segments and the obtained measured power are $P_m(R_i)$, $P_m(R_j)$ and, $P_m(R_k)$, respectively. Here, t_i and t_j have equal nominal power values while t_k has different value. Dynamic power variations of t_i, t_j, and t_k are medium, large, and small, respectively due to random process variation. Assume that, test pattern t_i activate HT. When comparing t_i and t_j, their acceptable measured power difference is shown in Fig. 4.1(a). If HT shift the power of t_i as shown in Fig. 4.1(b), we can detect HT.

In case of t_i and t_k, now t_k has small variation. In this case, their acceptable measured power difference is shown in Fig. 4.1(c). To detect HT, it is enough to shift power shown in Fig. 4.1(d). Thus, the arbitrary test pattern pair (t_i, t_k) has higher possibility to detect smaller Trojan than the equal power test pattern pair (t_i, t_j).

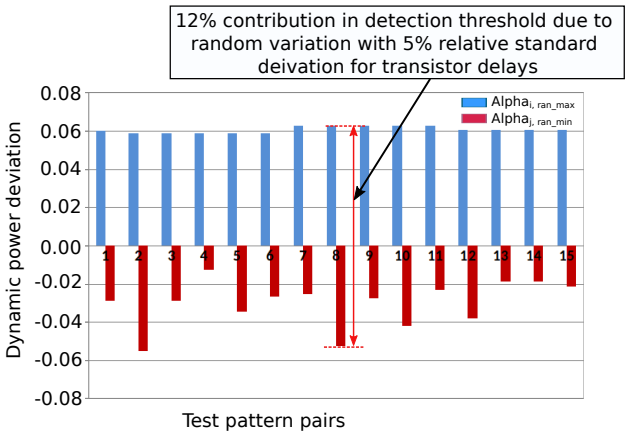


Figure 4.2: Dynamic power deviation in s38584 circuit.

Figure 4.2 illustrate a case study using s38584 benchmark circuit that shows the dynamic power deviation due to random process variation per test pattern pair and its contribution to the detection threshold. From Fig. 4.2, we observed that different test patterns have different power deviations i.e., some test patterns are less affected and some test patterns are highly affected by the random process variation.

4.2 Derivation of Detection Condition

In our proposed HT detection condition, all the test patterns of a segment are simply compared with the test patterns of another segment arbitrarily while maintaining the neighboring relationship. Here, the test patterns comparison between two neighboring segments within a chip diminishes the inter-die variation and intra-die systematic variation effects while the random variation effect is independent of the region of a circuit. A mathematical analysis will help us appropriately account for inter-die variation, intra-die systematic, and random variation effects to accurately detect HT.

Let us define the dynamic power deviation due to spatial correlation as $\delta_{i,j,intra\_sys} Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j))$ of the intra-die systematic variation to express their difference $(\delta_{i,intra\_sys} P_{nom\_Dy}(R_i) - \delta_{j,intra\_sys} P_{nom\_Dy}(R_j))$, where $\delta_{i,intra\_sys} P_{nom\_Dy}(R_i)$ and $\delta_{j,intra\_sys} P_{nom\_Dy}(R_j)$ are deviated power value

due to intra-die systematic variation by test pattern t_i and t_j, respectively. Let us consider $\alpha_{i,j,intra\_sys}Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j))$ denotes the worst case value of $\delta_{i,j,intra\_sys}Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j))$, assumed $3\sigma_{i,j,intra\_sys}$ in this thesis, where $\sigma_{i,j,intra\_sys}$ is the standard deviation of the normal distribution of $\delta_{i,j,intra\_sys}$. On the other hand, the random variation effect does not follow any specific distribution. Therefore, we model random variation effect using, test pattern power deviation to range (α_{i,ran_max}, α_{j,ran_min}). Here maximum and minimum RPD (relative power difference) of each test pattern is obtained using

$$\alpha_{i,ran\_max} = \frac{P_{i,max} - P_{i,nominal}}{P_{i,nominal}} \tag{4.1}$$

$$\alpha_{j,ran\_min} = \frac{P_{j,min} - P_{j,nominal}}{P_{j,nominal}} \tag{4.2}$$

where $P_{i,max}$, $P_{j,min}$, $P_{i,nominal}$, and $P_{j,nominal}$ means maximum power of pattern-t_i, minimum power of pattern-t_j, nominal power of pattern-t_i, and nominal power of pattern-t_j, respectively.

Consider we have two test pattern t_i and t_j and the associated activated regions are R_i and R_j respectively. Here, the region is defined as the set of FF and logic gates activated by a test pattern. Let the measured power of region R_i and R_j are $P_m(R_i)$ and $P_m(R_j)$, respectively. It is expected that the measured power difference for HT free circuit will be less than equal to the detection threshold imposed by process variations. Therefore, a HT in region R_i can be effectively detected if the measured power difference $(P_m(R_i^T) - P_m(R_j))$ for test pattern pair exceeds the detection threshold imposed by inter-die variation, intra-die systematic and random variation effect.

Let us assume that, the measured power $P_m(R_i)$ differ from its nominal power $P_{nom} = (P_{nom\_Dy} + P_{nom\_leak}; \textit{dynamic and leakage power})$ with a factor of inter-die variation δ_{inter} and intra-die variation $\delta_{i,intra}$ for dynamic power and a factor of θ_{inter} for leakage power. Let α_{inter} denotes the worst case deviation of δ_{inter}, assumed $3\sigma_{inter}$ in this thesis where, σ_{inter} is the standard deviation of the normal distribution of δ_{inter}. We assume the nominal value of leakage powers are equal and independent of the particular test pattern for whole circuit (C). Thus, the measured power for region R_i and R_j can be written as

$$P_m(R_i) = (1 + \delta_{inter} + \delta_{i,intra})P_{nom\_Dy}(R_i) + (1 + \theta_{inter})P_{nom\_leak}(C) \quad (4.3)$$

$$P_m(R_j) = (1 + \delta_{inter} + \delta_{j,intra})P_{nom\_Dy}(R_j) + (1 + \theta_{inter})P_{nom\_leak}(C) \quad (4.4)$$

Then, the measured power difference for test pattern pair (t_i, t_j) can be derived as follows:

$$\begin{aligned} P_m(R_i) - P_m(R_j) &= (1 + \delta_{inter} + \delta_{i,intra})P_{nom\_Dy}(R_i) \\ &\quad - (1 + \delta_{inter} + \delta_{j,intra})P_{nom\_Dy}(R_j) \\ &= (1 + \delta_{inter} + \delta_{i,intra\_ran})P_{nom\_Dy}(R_i) \\ &\quad - (1 + \delta_{inter} + \delta_{j,intra\_ran})P_{nom\_Dy}(R_j) \\ &\quad + \delta_{i,intra\_sys}P_{nom\_Dy}(R_i) - \delta_{j,intra\_sys}P_{nom\_Dy}(R_j) \end{aligned} \quad (4.5)$$

For HT free circuit, the measured power difference will be

$$\begin{aligned} P_m(R_i) - P_m(R_j) &= (1 + \delta_{i,intra\_ran})P_{nom\_Dy}(R_i) \\ &\quad - (1 + \delta_{j,intra\_ran})P_{nom\_Dy}(R_j) \\ &\quad + \delta_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ &\quad + (\delta_{i,j,intra\_sys})Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned} \quad (4.6)$$

Since we are comparing test pattern pairs (t_i, t_j) in arbitrary level; as a result one test pattern dynamic power consumption can be higher than another. Hence, measured power difference will have two possible cases which can be further derived as follows:

$Case\_1 : P_{nom\_Dy}(R_i) \geq P_{nom\_Dy}(R_j)$

$$\begin{aligned} P_m(R_i) - P_m(R_j) &\leq (1 + \alpha_{i,ran\_max})P_{nom\_Dy}(R_i) \\ &\quad - (1 + \alpha_{j,ran\_min})P_{nom\_Dy}(R_j) \\ &\quad + \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ &\quad + (\alpha_{i,j,intra\_sys})Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned} \quad (4.7)$$

$Case\_2 : P_{nom\_Dy}(R_i) \leq P_{nom\_Dy}(R_j)$

$$\begin{aligned} P_m(R_i) - P_m(R_j) \leq\ & (1 + \alpha_{i,ran\_max})P_{nom\_Dy}(R_i) \\ & - (1 + \alpha_{j,ran\_min})P_{nom\_Dy}(R_j) \\ & - \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ & + (\alpha_{i,j,intra\_sys})Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned} \tag{4.8}$$

For HT inserted circuit, the measured power difference will be

$$\begin{aligned} P_m(R_i^T) - P_m(R_j^T) = & \delta_{inter}P_{nom\_Dy}(R_i^T) \\ & + (1 + \delta_{i,intra\_ran})P_{nom\_Dy}(R_i^T) \\ & - \delta_{inter}P_{nom\_Dy}(R_j^T) - (1 + \delta_{j,intra\_ran})P_{nom\_Dy}(R_j^T) \\ & + (\delta_{i,j,intra\_sys})Mean(P_{nom\_Dy}(R_i^T), P_{nom\_Dy}(R_j^T)) \end{aligned} \tag{4.9}$$

Therefore, if the measured power difference exceeds an acceptable difference, HT can be doubted. Finally, considering β as safety margin the detection threshold is derived as

$Case\_1 : P_{nom\_Dy}(R_i) \geq P_{nom\_Dy}(R_j)$

$$\begin{aligned} P_m(R_i^T) - P_m(R_j^T) > & (1 + \alpha_{i,ran\_max})P_{nom\_Dy}(R_i) \\ & - (1 + \alpha_{j,ran\_min})P_{nom\_Dy}(R_j) \\ & + \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ & + (\alpha_{i,j,intra\_sys} + \beta)Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned} \tag{4.10}$$

$Case\_2 : P_{nom\_Dy}(R_i) \leq P_{nom\_Dy}(R_j)$

$$\begin{aligned} P_m(R_i^T) - P_m(R_j^T) > & (1 + \alpha_{i,ran\_max})P_{nom\_Dy}(R_i) \\ & - (1 + \alpha_{j,ran\_min})P_{nom\_Dy}(R_j) \\ & - \alpha_{inter}(P_{nom\_Dy}(R_i) - P_{nom\_Dy}(R_j)) \\ & + (\alpha_{i,j,intra\_sys} + \beta)Mean(P_{nom\_Dy}(R_i), P_{nom\_Dy}(R_j)) \end{aligned} \tag{4.11}$$

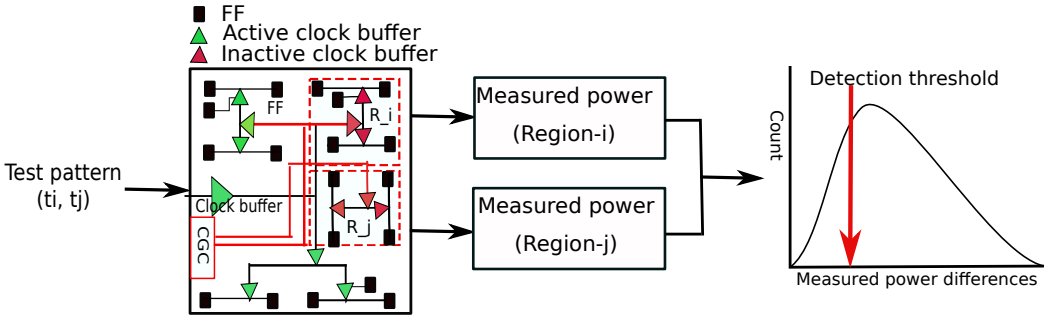


Figure 4.3: HT detection using measured power difference.

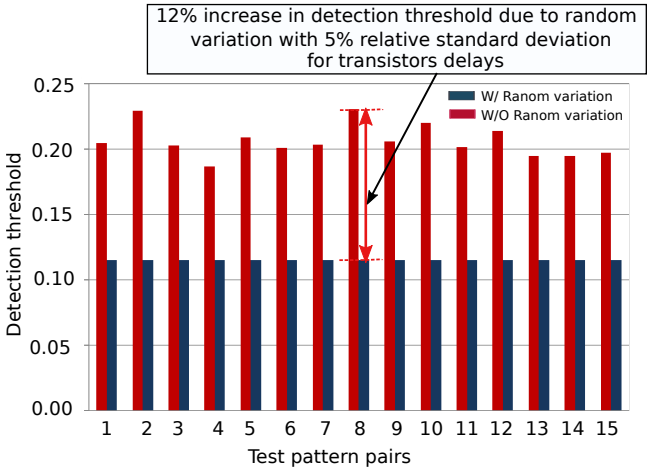


Figure 4.4: Detection threshold variation of s38584 circuit.

Figure 4.3 illustrates the concept of HT detection using measured power difference for the test pattern pairs. In the figure, two test patterns t_i and t_j are applied in two neighboring segment and obtained dynamic power from region R_i and R_j. After obtaining the measured power difference between the test patterns t_i and t_j, the value is compared with the detection threshold. Finally, Fig. 4.4 illustrates a practical example using s38584 circuit, where we can observe, how detection threshold varies per test pattern pairs due to random process variation. Thus, the application of arbitrary test pattern pair which are less affected by random process variation will impose less detection threshold and increase the probability of HT detectability.

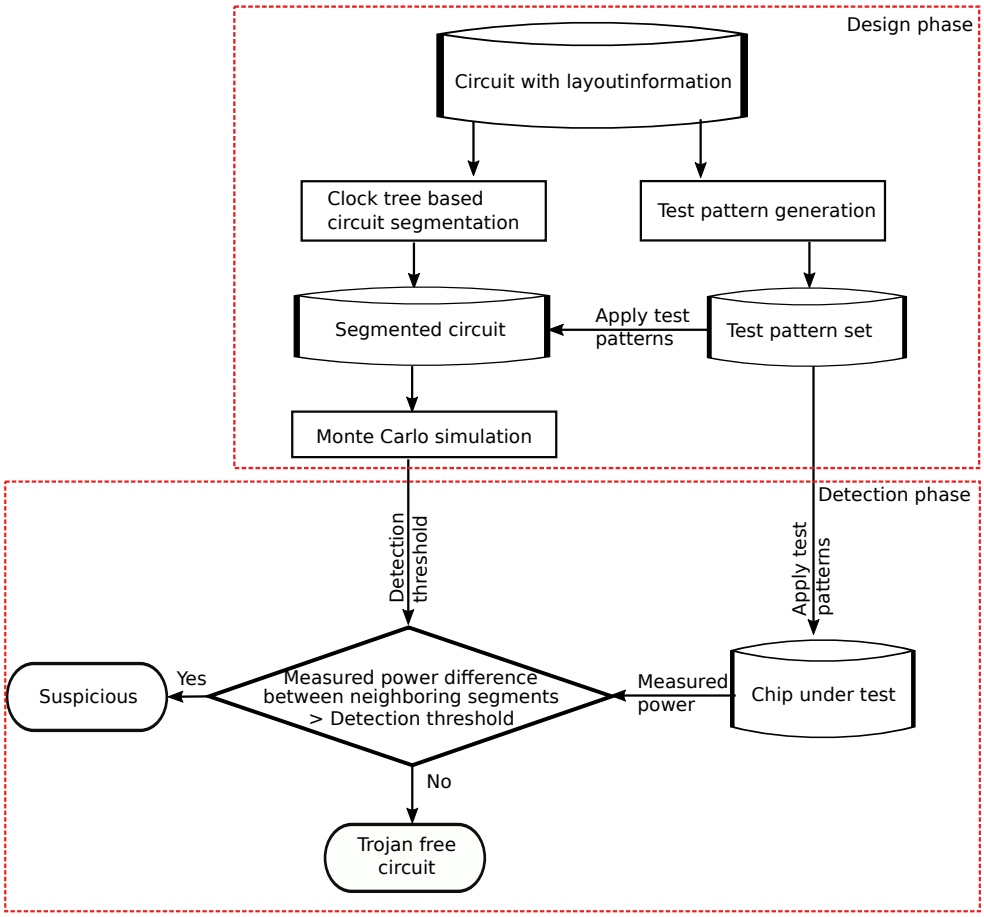


Figure 4.5: Overview of ANP method.

4.3 Proposed ANP Method

The overview of the proposed ANP method to detect hardware Trojan is illustrated in Fig. 4.5. According to Fig. 4.5, the ANP method has two major parts.These are the design phase and the detection phase. Here, the design phase has three parts: clock tree based circuit segmentation, test pattern generation and Monte Carlo simulation. Firstly, we have circuit with layout information where the clock tree-based circuit segmentation technique is applied to obtain segmented circuit. This technique helps to activate the small part of the circuit rather than activating the whole and thus improve Trojan to circuit power ratio. Secondly, the test pattern set is generated by ATPG tool from the initial

circuit with layout on formation. Thirdly, Monte Carlo simulation is performed by applying the test pattern set to the segmented circuit to obtain dynamic power deviation due to random variation with $n\%$ relative standard deviation for transistor delays. Afterward, considering the possible process variation effect including random variation, the detection threshold is devised by comparing test patterns arbitrarily between neighboring segments to from ANP pairs. Here, comparison of test patterns within and the neighboring segments help to eliminate or diminish systematic variation effect since systematic variations are spatially correlated which consequently reduce detection threshold. Thus, considering all process variations, HT detection condition is derived. In the detection phase, the test patterns stored in the database are applied on the chip under test (CUT) to obtain the measured power per test pattern. Then, the measured power per test patterns are compared by maintaining neighboring relationship to obtain measured power difference per ANP pair and compare with the detection threshold. If the measured power difference of ANP pair is greater than the detection threshold, then we will consider the CUT is suspicious to HT, otherwise CUT is HT free.

5 Results

In this chapter, we will briefly discuss on the experimental environment and results. In the experimental setup section, we will be introduced with the HTs inserted in benchmark circuits with their insertion scenario and the process variation parameters used to evaluate the detectability of the HTs. Then, a real case study will be presented to get an understanding of how ANP is useful in detecting HT. Finally, we will illustrate the detailed results and comparison of detectability between the equal power pairs and the arbitrary neighboring pairs in the presence of random process variation.

5.1 Experimental Setup

5.1.1 HTs Description

To test the effectiveness of our method, HT $T1$ (s38417-T200) and $T2$ (s15850-T100) are extracted from Trust-Hub [23]. Here, $T1$ is a combinational HT which consists of 11 logic elements (4 NOR gates, 3 AND gates, and 8 OR gates) and $T2$ is a sequential HT which consists of 26 elements (23 AND gates, 2 DFFs, and 1 inverter). Figure 5.1 shows the logical structure of the two HT used in our experiments. The trigger of HT $T2$ consists of two comparator and one flip-flop at the output of each comparator. The comparator drives the clock inputs of the flip-flops. The data input of the first flip-flop is 1 and the output of the flip-flop is connected to the data input of the second flip-flop. The output of the second flip-flop is gated by the inverted test enable signal to ensure HT activation only in the functional mode. When the HT will be activated, it will leak an internal signal through the specified port. On the other hand, the trigger of $T1$ is a comparator which consists of logic gates only. As the trigger activates, the HT payload propagates erroneous values over four internal signals.

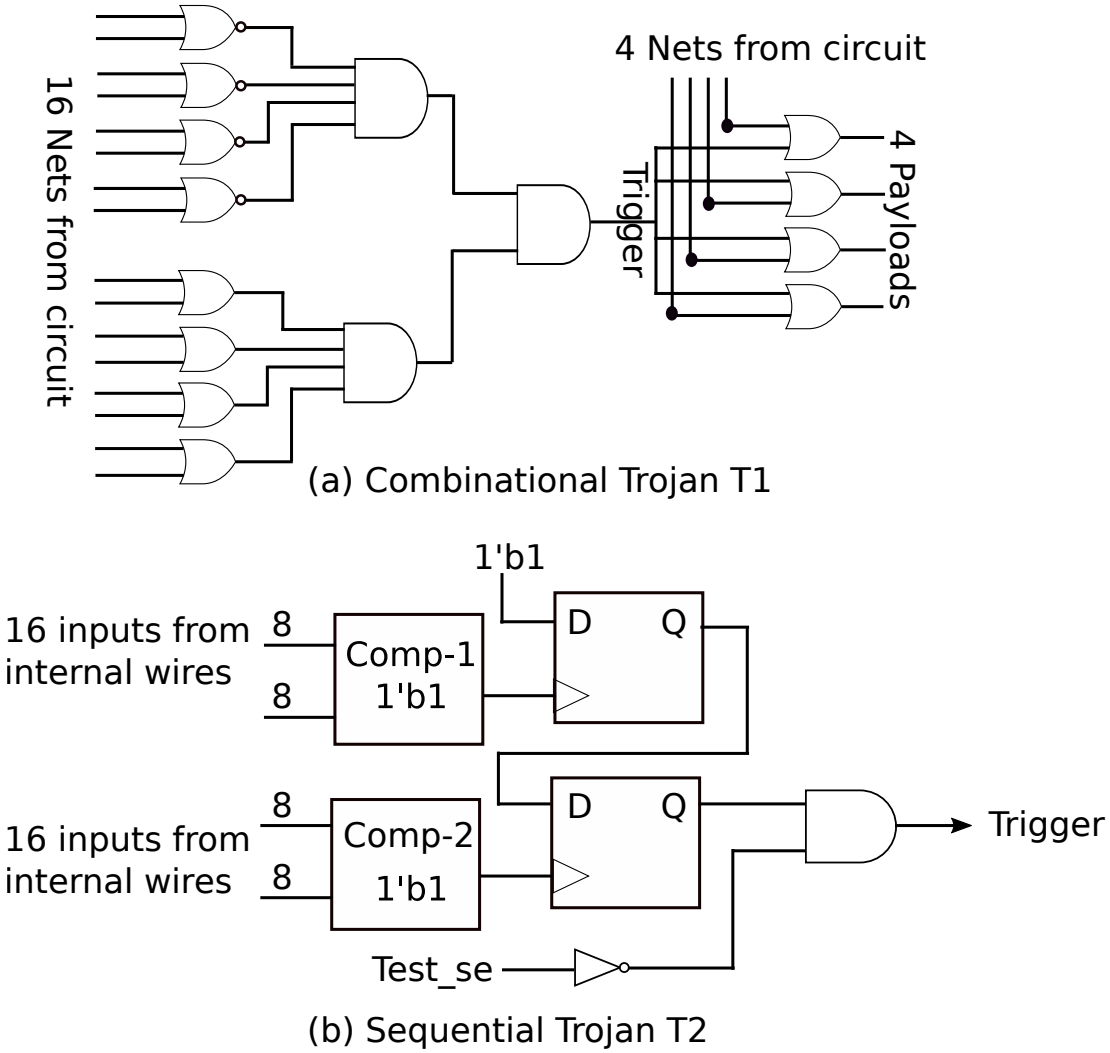


Figure 5.1: Structure of HT circuits.

5.1.2 HT Insertion Scenario

To evaluate our proposed ANP method using three benchmark circuits, the HTs are inserted in each segment of a circuit. Since HT circuits are stealthy in nature and also connected to the original circuits in such a way that, it can trigger after meeting very rare conditions. To accomplish this task, HT $T1$ and $T2$ are inserted in low controllability (0 or 1) nets according to the corresponding level-0 nets of the HTs. For example, if AND gate is a level-0 element of an HT, then it

Table 5.1: Summary of HTs to circuits size ratio

Circuit	HT	size ratio
s35932	$T1$	0.000732
s38417	$T1$	0.000804
s38584	$T1$	0.000937
s35932	$T2$	0.0034137
s38417	$T2$	0.003676
s38584	$T2$	0.004287

Table 5.2: Test pattern pair summary of three benchmark circuits

Circuit	No of Segments	Test patterns	Equal power pair	arbitrary neighboring pair
s35932	10	52	2500	90064
s38417	10	165	8255	896775
s38584	8	244	20655	1634800

will be connected to zero (0) controllability nets so that it may trigger at a very rare condition. Table 5.1 is the summary of HT to circuit ratio. Here, HT $T1$ is smaller than $T2$ according to Table 5.1.

5.2 Test Pattern Pair Summary

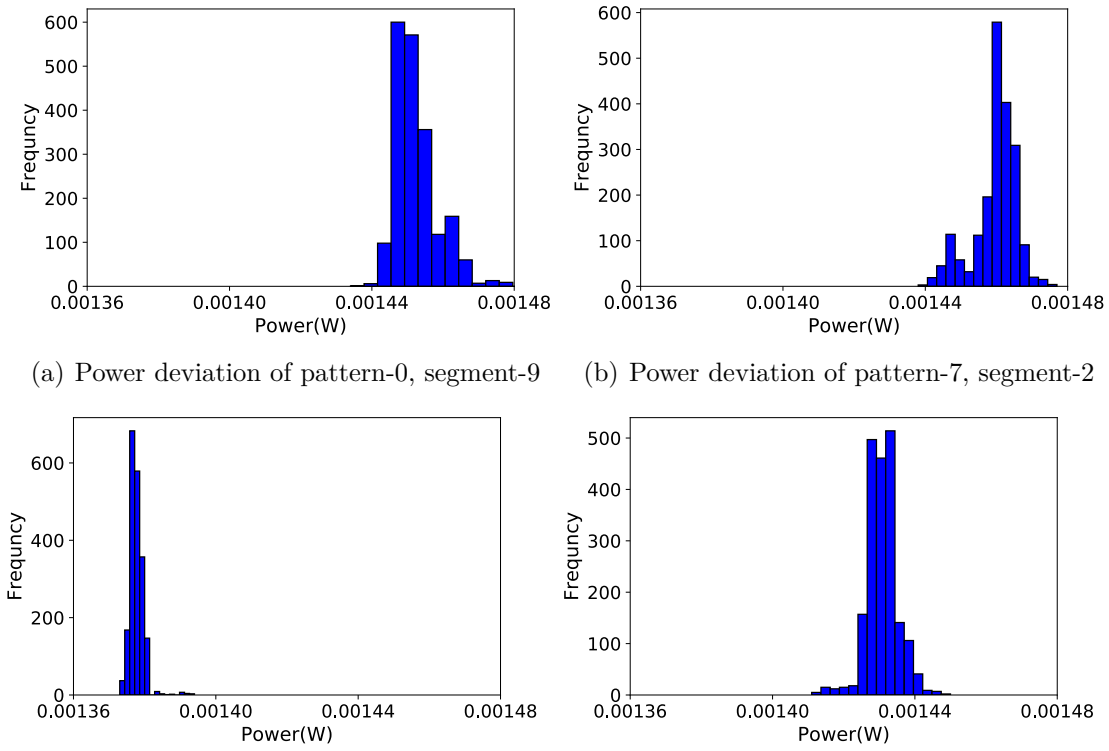
Generating test pattern pair is an important part of our analysis, since we are comparing the effectiveness of the equal power pairs and the arbitrary neighboring pairs. Two test patterns in neighboring segments will be considered as equal power pair if the difference between them is less than 0.00001. On the other hand, the arbitrary test pattern pairs are formed by simply comparing all test patterns arbitrarily while maintaining neighboring relations. Hence, the equal power pairs are a subset of the arbitrary neighboring pairs. Table 5.2 shows the summary of number of segment obtained after clock tree based segmentation, initial number of transition delay fault test patterns, number of equal power pairs and the arbitrary neighboring pairs in respective benchmark circuits.

5.2.1 Experimental Evaluation Parameters

To evaluate the effectiveness of our method, 100 sample HT circuits are simulated with each test pattern. For testing the arbitrary neighboring pairs detectability, we consider inter-die relative standard delay deviation σ_{inter_die} as 5%, the intra-die systematic relative standard delay deviation co-relation $\sigma_{i,j,intra\_sys}$ as 0.135%. On the other hand, if test patterns are compared within a segment, the intra-die systematic relative standard delay deviation co-relation $\sigma_{i,j,intra\_sys}$ is considered as 0%. In addition, safety margin β is taken as 10%. Moreover, to address random process noise, random variation with n% (n=1,2,3,.., 5) relative standard deviation for transistor delays are obtained from Monte Carlo simulation. To evaluate the detectability of 90 nm technology ICs, process variation parameters are taken from paper [24]. They refer intra-die relative standard delay deviation as 3.5% and inter-die relative standard delay deviation as 15%. To decompose the intra-die relative standard delay deviation into systematic and random component, we use paper [25], where they refer that, for 90 nm technology node 14% of intra-die relative standard delay deviation is random and rest of it is systematic relative standard delay deviation. Thus, intra-die relative standard delay deviation ($\sigma = 1.167\%$) is decomposed as intra-die systematic relative standard delay deviation as 1.1517% (σ) and random variation as 0.1874% relative standard deviation for transistor delays. Finally, the detectability of HT is calculated as the ratio of detection to the total number of tested circuits.

5.3 Case Study of Detecting HT using ANP Method

To show the HT detection effectiveness using ANP method, an example is devised using s35932 benchmark circuit and HT $T2$ (s15850-T100). Here, HT $T2$ is inserted in segment-9 using low-controllability nets of the circuit. To evaluate the result, we consider, the inter-die relative standard delay deviation σ_{inter_die} as 5%, the intra-die systematic relative standard delay deviation co-relation $\sigma_{i,j,intra\_sys}$ as 0.135%, and random variation as 2% relative standard deviation for transistor delays. To obtain dynamic power deviation due to the random process variation,



(a) Power deviation of pattern-0, segment-9

(b) Power deviation of pattern-7, segment-2

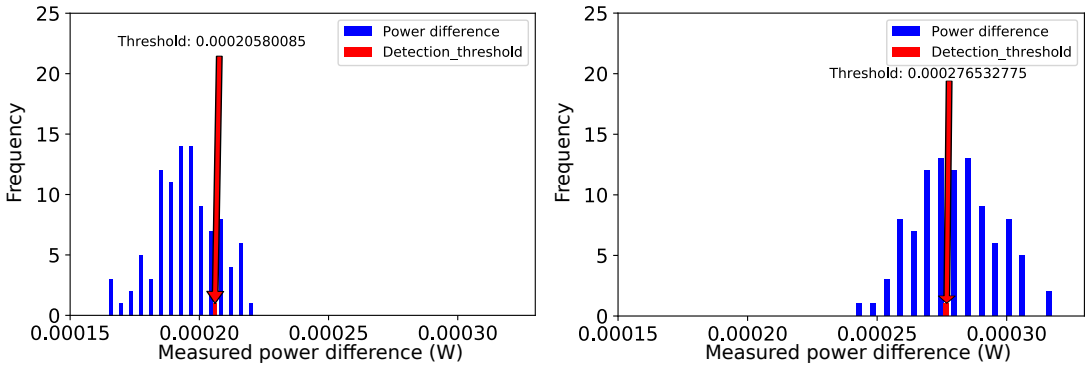
(c) Power deviation of pattern-5, segment-8

(d) Power deviation of pattern-7, segment-7

Figure 5.2: Dynamic power deviation due to 2% random variation.

Monte Carlo simulation with 2% relative standard deviation for each transistor delay is done. The dynamic power distribution due to 2% relative standard delay deviation for each transistor is shown in Fig. 5.2. Then to test the detectability of HT, 100 sample HT circuits are created with 2% relative standard delay deviation for each transistor of s35932 circuit.

After obtaining all required parameters, test pattern pairs (equal power and arbitrary neighboring) are compared. Let us consider an equal power pair (P_0, P_7), where P_0 stands for test pattern-0 from segment-9, P_7 stands for test pattern-7 from neighboring segment-7. Again, consider an arbitrary neighboring pair (P_0, P_5), where P_0 stands for test pattern-0 from segment-9 and P_5 stands for test pattern-5 from neighboring segment-8. After application of test pattern pairs, measured power of the corresponding activated regions are obtained. Then applying detection condition to the measured power difference of the test pattern



(a) Equal power pair (0,7) of segment(9,2)

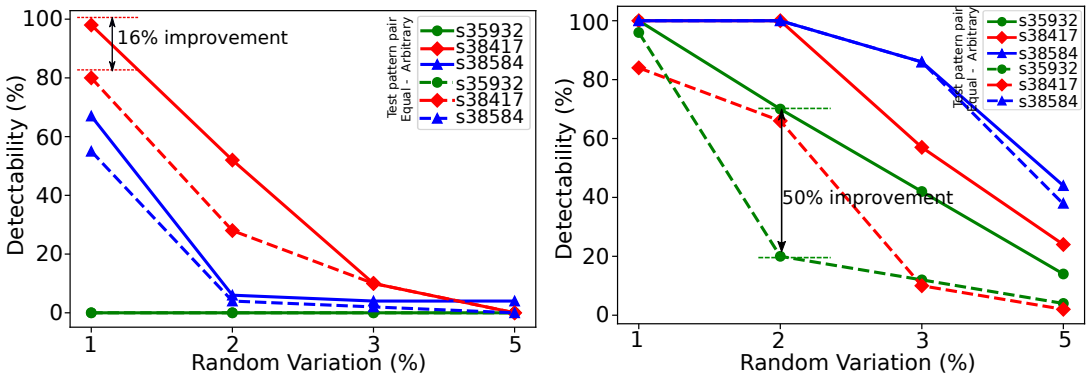
(b) Arbitrary neighboring pair (0,5) of segment(9,8)

Figure 5.3: Detectability comparison between test pattern pairs.

pairs (equal and arbitrary) , the equal power pair shows 20% detectability and the arbitrary neighboring pair shows 70% detectability in presence of 2% relative standard delay deviation for each transistor. Figures. 5.3(a) and 5.3(b) shows the result of equal and arbitrary neighboring test pairs. Thus, the arbitrary neighboring test pattern pairs shows higher detectability than the equal power pairs in presence of random process variation.

5.4 Evaluation of ANP pairs in presence of random variation

The detection sensitivity comparison between the equal power neighboring pairs and the arbitrary neighboring pairs are prepared by evaluating the detectability of HT $T1$ and $T2$. Here, the HTs are inserted according to SCOAP (Sandia Controllability and Observability Analysis Program) value of the nets in each segment. Figure. 5.4 illustrates the comparison of detectability between the two types of test pattern pairs for best case segments. From the figure, we can observe that in the presence of random process variation, the arbitrary neighboring test pattern pairs are more effective than the equal power pairs. For example, in case of HT $T2$, arbitrary neighboring pairs obtain 70% detectability while equal power pairs obtain only 20% detectability for random variation with 2% relative standard



(a) HT $T1$ (b) HT $T2$

Figure 5.4: Comparison between equal and arbitrary neighboring pairs.

Table 5.3: Comparison between equal and arbitrary neighboring pairs for $T1$

Best Segment Case												
Variation	0% Random		0.1874% Random		1% Random		2% Random		3% Random		5% Random	
Circuit	Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs	
	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary
s35932	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
s38417	100%	100%	100%	100%	80%	98%	28%	52%	10%	10%	0%	0%
s38584	100%	100%	41%	41%	16%	24%	4%	6%	2%	4%	2%	4%
Average Segment Case												
s35932	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
s38417	50%	52%	28%	29%	18%	22%	9%	12%	4%	4%	0%	0%
s38584	50%	50%	19%	19%	9%	11%	1%	2%	0%	1%	0%	1%
Worst Segment Case												
s35932	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
s38417	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
s38584	0%	2%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%

deviation for transistor delays. Again, in case of HT $T1$, arbitrary neighboring pairs obtain 100% detectability while equal power pairs obtain 84% detectability for random variation with 2% relative standard deviation for transistor delays.

Also, Table 5.3 and Table 5.4 represent the summary of HT detectability for three benchmark circuits s35932, s38417, and s38417. To summarize the detectability, we use three cases (best, average, and worst). Here, the best case represents the detectability of the segment, where arbitrary neighboring pair shows the highest detectability. The average case represents the detectability obtained by averaging the detectability of all segment of a circuit while the worst-case

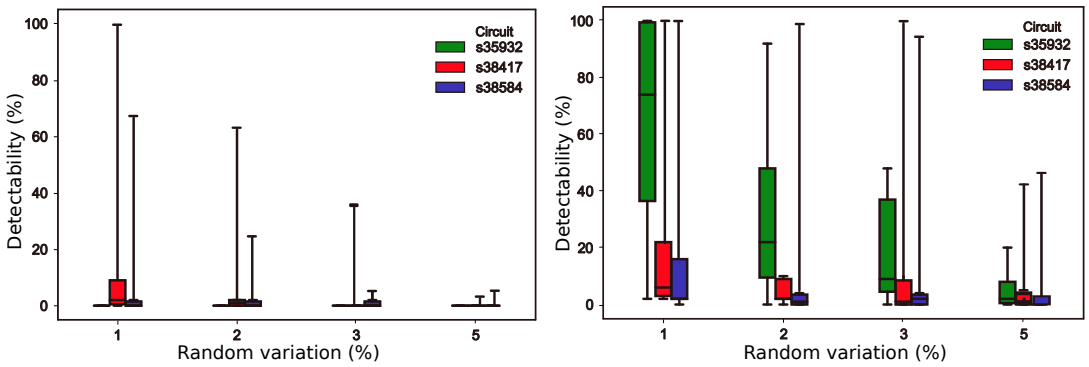
Table 5.4: Comparison between equal and arbitrary neighboring pairs for $T2$

Best Segment Case												
Variation	0% Random		0.1874% Random		1% Random		2% Random		3% Random		5% Random	
Circuit	Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs		Test pattern pairs	
	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary	Equal	Arbitrary
s35932	100%	100%	100%	100%	98%	100%	20%	70%	12%	42%	4%	14%
s38417	100%	100%	100%	100%	84%	100%	66%	100%	10%	57%	2%	24%
s38584	100%	100%	100%	100%	100%	100%	100%	100%	86%	86%	42%	42%
Average Segment Case												
s35932	82%	83%	80%	82%	62%	65%	21%	32%	11%	19%	2%	5%
s38417	62%	69%	35%	45%	19%	26%	17%	23%	11%	17%	4%	8%
s38584	67%	67%	49%	50%	28%	30%	25%	26%	16%	17%	6%	7%
Worst Segment Case												
s35932	34%	34%	24%	25%	0%	2%	0%	0%	0%	0%	0%	0%
s38417	0%	2%	0%	2%	0%	2%	0%	0%	0%	0%	0%	0%
s38584	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

represents the segment, where the arbitrary neighboring pair shows the lowest detectability. According to Table 5.3 and Table 5.4, we observe that as HT $T1$ is smaller compared to $T2$, the detectability of $T1$ is lower than $T2$ in presence of elevated random process variation. For HT $T2$, in the best cases, we can obtain 100% detectability even at random variation with 0-1% relative standard deviation for transistor delays. Again, at random variation with 2-3% relative standard deviation for transistor delays, HT $T2$ has 42-100% detectability for the arbitrary neighboring pairs. On the other hand, the equal power pair has much lower detectability compared to the arbitrary neighboring pairs for 2-3% relative standard deviation for transistor delays as shown in Table 5.4. Overall, for all the three cases, the arbitrary neighboring pairs shows possibility of obtaining relatively higher detectability than the equal power pairs in presence of random process variation.

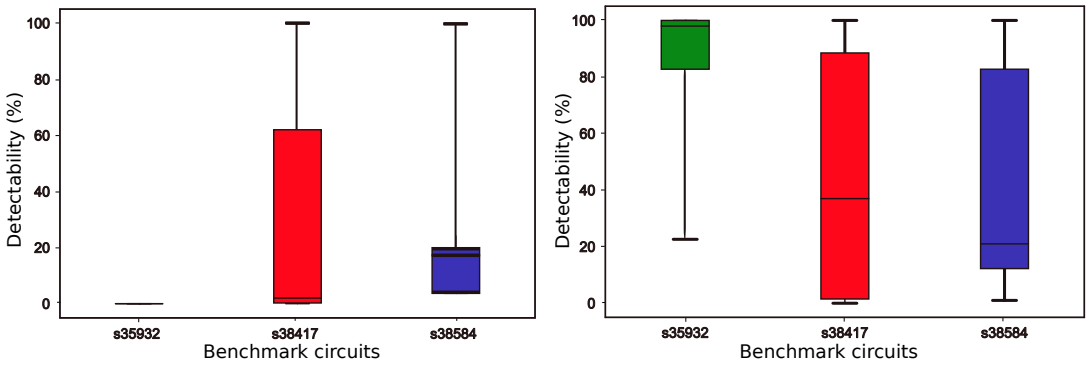
5.5 Evaluation of HT Detectability for ANP method

The ANP method is evaluated for two types of process variation cases: Process variation we consider and process variation parameters from 90 nm chip. To evaluate effectiveness of our proposed ANP method, we use the same HT $T1$ and $T2$ as before. Here, the HTs are inserted according to SCOAP (Sandia Control-



(a) HT $T1$ (b) HT $T2$

Figure 5.5: Detectability of ANP method for 1-5% random variation.



(a) HT $T1$ (b) HT $T2$

Figure 5.6: Detectability of ANP method for 90 nm chip process parameters.

lability and Observability Analysis Program) value of the nets in each segment of the benchmark circuits (s35932, s38417, and s38584). Figure. 5.5 shows the detectability of HT $T1$ and $T2$ using ANP method for our considered process variation parameters. From the figures, we observed that for small random variation cases (ex:1%) the ANP method achieve high detectability for HT $T2$ (ex: 100% detectability for all circuits). On the other hand, ANP method achieve low detectability (ex: s35932 has 0% detectability) and few circuits have relatively high detectability (ex: s38417 has 100% detectability) for HT $T1$ in presence of small random variation (ex: 1%). Moreover, We also observed that as random

variation increases the detectability of ANP method decreases.

Again, Fig. 5.6 shows the detectability of the ANP method for real 90 nm chip parameters. Since real chip process variation parameters are smaller than our considered process variation parameters, APN method achieve high detectability for HT $T2$ and while $T1$ has still low detectability for some cases (ex: s35932 has 0% detectability for all segments).

6 Conclusion

In this thesis, a detailed analysis of dynamic power variation and its effect on detecting hardware Trojans (HT) is shown. From the experimental analysis, it is observed that dynamic power is sensitive to random process variation. Therefore considering this challenge, we propose the ANP (arbitrary neighboring test pattern pair) method which is random process variation aware. In this method, the ANP pairing concept is introduced since comparison of test patterns which are less affected by random variation and test patterns which sensitize HT have higher chance of achieving good detectability. Moreover, self-referencing technique of this method can significantly reduce inter-die variation effect and neighboring segment comparison diminish intra-die systematic variation effect by establishing spatial co-relation. Besides, comparison of test pattern within a segment to form pairs help to eliminate the effect of systematic variation by establishing 100% spatial co-relation. Finally, the detectability evaluation result shows that the ANP method achieve high detectability (ex: 100%) for HT $T2$ and low detectability (except few cases have high detectability; ex: s38417 has 100% detectability) for HT $T1$ in presence of small random variation. In addition, the detectability of ANP method degrades as the random process variation increases. Therefore, further research will be done to improve the detection sensitivity of ANP method for small Trojan (ex: HT $T1$) in presence of high random process variation .

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, pp. 10–25, 2010.

[2] G. Di Natale, S. Dupuis, and B. Rouzeyre, "Is side-channel analysis really reliable for detecting hardware trojans?" in *Conference on Design of Circuits and Integrated Systems*, 2012, pp. 238–242.

[3] D. Kamel, C. Hocquet, F.-X. Standaert, D. Flandre, and D. Bol, "Glitch-induced within-die variations of dynamic energy in voltage-scaled nano-cmos circuits," in *Proceedings of the European Solid-State Circuits Conference*. IEEE, 2010, pp. 518–521.

[4] "Semiconductor engineering," https://semiengineering.com/knowledge_centers/low-power/low-power-design/power-consumption/, online, Accessed on: 2018-09-20.

[5] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using ic fingerprinting," in *Symposium on Security and Privacy*. IEEE, 2007, pp. 296–310.

[6] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *International workshop on hardware-oriented security and trust*. IEEE, 2008, pp. 51–57.

[7] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," in *International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2008, pp. 40–47.

[8] F. S. Hossain, T. Yoneda, and M. Inoue, "An effective and sensitive scan segmentation technique for detecting hardware Trojan," *IEICE TRANSACTIONS on Information and Systems*, vol. 100, no. 1, pp. 130–139, 2017.

[9] X. Zhang and M. Tehranipoor, "RON: An on-chip ring oscillator network for hardware Trojan detection," in *Design, Automation & Test in Europe*. IEEE, 2011, pp. 1–6.

[10] Y. Zheng, S. Yang, and S. Bhunia, "SeMIA: Self-similarity-based ic integrity analysis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 37–48, 2015.

[11] Y. Huang, S. Bhunia, and P. Mishra, "MERS: statistical test generation for side-channel analysis based Trojan detection," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 130–141.

[12] F. S. Hossain, T. Yoneda, M. Inoue, and A. Orailoglu, "Detecting hardware Trojans without a golden ic through clock-tree defined circuit partitions," in *European Test Symposium*. IEEE, 2017, pp. 1–6.

[13] F. S. Hossain, T. Yoneda, M. Shintani, M. Inoue, and A. Orailoglu, "Intra-die-variation-aware side channel analysis for hardware Trojan detection," in *Asian Test Symposium*. IEEE, 2017, pp. 52–57.

[14] M. Tehranipoor, H. Salmani, and X. Zhang, "Integrated circuit authentication," *Switzerland: Springer, Cham. doi*, vol. 10, pp. 978–3, 2014.

[15] S. Mitra, H.-S. P. Wong, and S. Wong, "The Trojan-proof chip," *IEEE Spectrum*, vol. 52, no. 2, pp. 46–51, 2015.

[16] B. Sharkey, "Trust in integrated circuits program," *Defense Advanced Research Projects Agency, available at: http://www. darpa. mil/MTO/solicitations/baa07–24/Industry_Day_Brief_Final. pdf (accessed 21 july 2019)*, 2007.

[17] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[18] A. Agarwal, D. Blaauw, V. Zolotov, S. Sundareswaran, M. Zhao, K. Gala, and R. Panda, "Path-based statistical timing analysis considering inter-and intra-die correlations," in *Proceedings of the International Workshop on Timing Issues in the Specification and Synthesis of Digital Systems*, 2002, pp. 16–21.

[19] L. Scheffer, "Explicit computation of performance as a function of process variation," in *Proceedings of the international workshop on Timing issues in the specification and synthesis of digital systems*. ACM, 2002, pp. 1–8.

[20] S. Saxena, C. Hess, H. Karbasi, A. Rossoni, S. Tonello, P. McNamara, S. Lucherini, S. Minehane, C. Dolainsky, and M. Quarantelli, "Variation in transistor performance and leakage in nanometer-scale technologies," *IEEE Transactions on Electron Devices*, vol. 55, no. 1, pp. 131–144, 2007.

[21] J. D. Alexander and V. D. Agrawal, "Algorithms for estimating number of glitches and dynamic power in cmos circuits with delay variations," in *IEEE Computer Society Annual Symposium on VLSI*. IEEE, 2009, pp. 127–132.

[22] S. Bathla, R. M. Rao, and N. Chandrachoodan, "A simulation-based metric to guide glitch power reduction in digital circuits," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 27, no. 2, pp. 376–386, 2018.

[23] "Trust-Hub," https://www.trust-hub.org/benchmarks/, online, Accessed on: 2019-05-01.

[24] L.-T. Pang and B. Nikolic, "Measurements and analysis of process variability in 90nm CMOS," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 5, pp. 1655–1663, 2009.

[25] H. Onodera and H. Terada, "Characterization of wid delay variability using RO-array test structures," in *International Conference on ASIC*. IEEE, 2009, pp. 658–661.