2019

Hardware Security In Carbon Based Digital Integrated Circuits

Ahmed Abdelaziz
University of Alabama at Birmingham

HARDWARE SECURITY IN CARBON BASED DIGITAL INTEGRATED CIRCUITS

by

AHMED KHOURSHED

KARTHIKEYAN LINGASUBRAMANIAN, COMMITTEE CHAIR
MOHAMMAD HAIDER
DALTON NELSON
DANEESH SIMIEN
TAUHIDUR RAHMAN

A DISSERTATION

Submitted to the graduate faculty of the University of Alabama at Birmingham,
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

BIRMINGHAM, ALABAMA

2019

HARDWARE SECURITY IN CARBON BASED DIGITAL INTEGRATED CIRCUITS

AHMED KHOURSHED

COMPUTER ENGINEERING

ABSTRACT

Carbon based integrated circuits (ICs) built with Carbon Nanotube Field Effect Transistor (CNTFET) and Graphene Nanoribbon Field Effect Transistor (GNRFET) are established as viable replacement for Silicon based Metal Oxide Semiconductor Field Effect Transistors (MOSFET) in order to meet the demands of future high density ICs with sub-nm channel lengths. Given the inevitability of such development, it is important to establish an understanding of the security vulnerabilities in Carbon based ICs. In this work, we have studied the important hardware security vulnerabilities that plague current MOSFET technology, in CNTFET and GNRFET based ICs. Based on our studies on hardware Trojans and IC counterfeiting, we propose efficient countermeasures for CNTFET and GNRFET based ICs. To handle IC counterfeiting, we propose Ring Oscillator based Physical Unclonable Function (RO-PUF) designs for both CNTFET and GNRFET ICs, by introducing variations in number of CNTs or GNRs in the channel. Our designs are able to achieve near ideal inter and intra hamming distances with a smaller footprint as compared to MOSFET RO-PUFs. We addressed the issue of hardware Trojans, by studying their inclusion in CNTFET and GNRFET based circuits. We used the current methodologies, designed for the detection of Trojans in MOSFET based circuits, to detect Trojans in CNTFET and GNRFET based circuits. The results clearly showed the inadequacy of these methods prompting the need for advanced detection schemes. Based on these studies, we propose a segmentation based detection methodology using sleep transistors. This power gating methodology allows us to seamlessly partition the circuit and enhance detection sensitivity.

Keywords: Carbon Nanotube CNT, Graphene Nanoribbon GNR, CNTFET, GNRFET, Hardware Trojan, IC Counterfeit, PUF, Sleep Transistor

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisor Dr.. Karthikeyan Lingasubramanian for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Besides my advisor, I would like to thank the rest of my thesis committee: Dr. Mohammad Haider, Dr. Dalton Nelson, Dr. Tauhidur Rahman and Dr. Daneesh Simien, for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

Last but not the least, I would like to thank my family: my parents, brothers and sister for supporting me spiritually throughout writing this thesis and in my life.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

LIST OF ABBREVIATIONS

CNT	Carbon Nanotube
GNR	Graphene Nanoribbons
CNTFET	Carbon Nanotube Filed Effect Transistor
GNRFET	Graphene Nanoribbons Filed Effect Transistor
RO	Ring Oscillator
PUF	Physical Unclonable Function

CHAPTER 1
INTRODUCTION

With constantly growing demand for security, silicon chips started to be used not only for control purposes but also for protection as well. The last ten years have seen a big boom in this area. From military and bank applications, the technology involved to everyday life, to prevent the use of unbranded batteries in mobile phones and laptops, to block non-genuine and refilled cartridges for printers, and to restrict the servicing of your appliances to manufacturer service centers. These days we have a sequential battle between manufacturers who got new security solutions learning their lessons from previous mistakes, and the hacker community which is constantly trying to get off the protection in various devices. Both sides are also constantly improving their knowledge and experience. In this endless war, the front line shifts forward and backward regularly. Deep down, the problem concerns both economics and law. On the one hand, when dishonest people try to steal property, there will be a demand to increase security. On the other side, reverse engineering was always part of technological progress, helping to design compatible products and improve existing ones.

There is no such thing as absolute security. A determined hacker can break any protection provided he has enough time and resources. The question is how practical it would be. If it

takes ten years to break a device which in three years' time is replaced by a successor with even better security, then the defense has won.

It is obvious that one of the first steps in any hardware design is choosing the right components. Despite all the electrical, performance and resource parameters which are widely available from all semiconductor manufacturers, information on security protection and implementation is either limited or totally restricted [2,3].

What we are facing right now related to hardware security issues are Trojan attack and counterfeit parts problem. So, we wants to use Nano electronics as a trend for helping overcome the hardware security issues.

Nanoelectronics enable conceptually new and strong security primitives and applications. Nanoelectronic security primitives create intrinsic feedback mechanisms that can provide security comparable to that offered by Shannon's diffusion and confusion principles while subsuming these two fundamental principles as special cases. Nanoelectronic security primitives are potentially more robust than conventional complementary metal oxide semiconductor (CMOS) device-based security primitives [1,2,3]. Emerging, unconventional nanoelectronics have the potential to yield computing systems with miniscule form factors, ultra-low-power consumption, and fast computation times relative to CMOS technologies.

Carbon based integrated circuits (ICs) built with Carbon Nanotube Field Effect Transistor (CNTFET) and Graphene Nanoribbon Field Effect Transistor (GNRFET) are established as viable replacement for Silicon based Metal Oxide Semiconductor Field Effect Transistors (MOSFET) in order to meet the demands of future high density ICs with sub-nm channel lengths. Given the inevitability of such development, it is important to establish an understanding of the security vulnerabilities in Carbon based ICs. In this work, we have studied the important hardware security vulnerabilities that plague current MOSFET technology, in CNTFET and GNRFET based ICs. Based on our studies on hardware Trojans and IC counterfeiting,

Motivation

A variety of materials including Carbon, graphene is being investigated for use in Nano electronics. In this thesis, we will explore the main advantage of using carbon based material like carbon nanotube and graphene nanoribbons in such hardware security problems like Trojan attack and counterfeit. For hardware Trojan detection, we addressed the issue of hardware Trojans, by studying their inclusion in CNTFET and GNRFET based circuits. We used the current methodologies, designed for the detection of Trojans in MOSFET based circuits, to detect Trojans in CNTFET and GNRFET based circuits. The results clearly showed the inadequacy of these methods prompting the need for advanced detection schemes. Based on these studies, we propose a segmentation based detection methodology using sleep transistors. This power gating methodology allows us to seamlessly partition the circuit and enhance detection sensitivity. For IC counterfeit problem, we propose efficient countermeasures for CNTFET and GNRFET based ICs. To

handle IC counterfeiting, we propose Ring Oscillator based Physical Unclonable Function (RO-PUF) designs for both CNTFET and GNRFET ICs, by introducing variations in number of CNTs or GNRs in the channel. Our designs are able to achieve near ideal inter and intra hamming distances with a smaller footprint as compared to MOSFET RO-PUFs. What we found from previous work related to these materials, it's given a very good performance when comparing to traditional methods. Reliability, faster, and less power consumption are most important features we have concluded from the previous work. Also our results in hardware security circuits using these materials gave us a very challenging output compared to traditional one. In our future work, we have to explore current methods to overcome the Trojan attack using neutralization method, as well as counterfeit using new design of PUF circuit method.

CHAPTER 2
BACKGROUND

In this chapter we will cover related work to our work in the dissertation. We will cover first the hardware Trojan problem and how it can effect in circuit operation and second we will cover the counterfeit problem and the proposed designs like physical unclonable function (PUF) to overcome IC counterfeiting.

2.1 Carbon Nanotube FET (CNTFET) and Graphene Nanoribbons FET (GNRFET)

2.2.1 CNTFET

CNTs are named on the basis of derived from their size, since the diameter of a nanotube is on the order of a few nanometers, while they can be up to several millimeters in length. CNTs are divided in to two categories as a single-walled nanotubes (SWNTs) and multi-walled nanotubes (MWNTs) depending upon the number of walls [10]. CNTs may consist of one up to ten and hundreds of concentric shells of carbons with adjacent shells separation of 0.34 nm. The carbon network of the shells is closely related to the honeycomb arrangement of the carbon atoms in the graphite sheets. The excellent advantage of CNT including mechanical and electronic properties of the nanotubes stem in their quasi-one dimensional (1D) structure and the graphite-like arrangement of the carbon atoms in the shells [11].

Thus, the nanotubes have high Young's modulus and tensile strength, which makes them suitable for composite materials with improved mechanical properties. The nanotubes can be metallic or semi conducting depending on their structural parameters [12,13].

Individual transistors made from carbon nanotubes are faster and more energy efficient than those made from other materials. Going from a single transistor to an integrated circuit full of transistors, however, is a giant leap. As in fig.1 [14], its CNTFET and it shows the nanotubes in the channel.

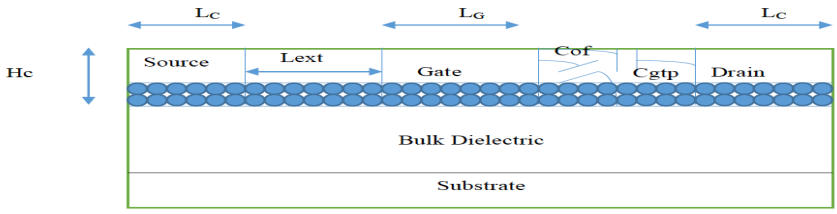


Figure. 1 CNTFET structure with planar top gate and multiple CNTs in the Channel [14].

The promising characteristics of individual CNTFETs has led to initial attempts at integration of several CNTFETs into useful circuits that can perform a logic operation, or function as memories or sensors and a lot of logic gates that helps in hardware security. In the following, we limit our discussion to advances in logic applications circuit. The CNT logic gates have been, in most cases, based on a complementary technology analogous to silicon CMOS, which is important as it may ease integration of CNTs onto this well-established technology. A typical characteristic curve is shown in Fig.2. we used Stanford CNTFET model to do the simulation using cadence simulator.

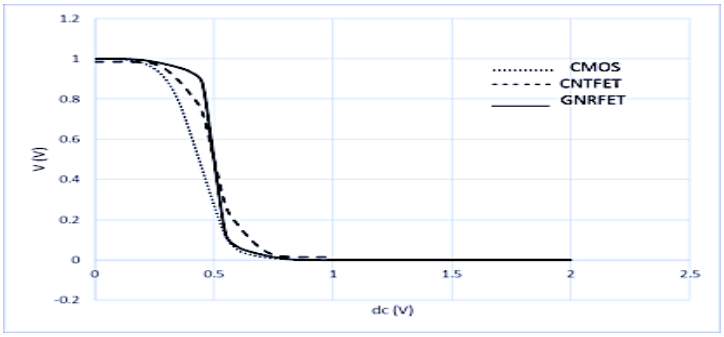


Fig. 2 Inverter Based on Complementary CNTFET

Parameter/Device	CMOS(32nm)	CNTFET(32nm)
Noise Margin Low	0.4 v	0.3 v
Noise Margin High	0.4 v	0.3 v
Propagation Delay	0.05 ns	0.05 ns
Energy Delay Product	3.45*10 -27Js	3.6*10 -28 Js
Total Power Consumption	5.62 µw	0.76 µw

Table 1. Comparison between CMOS and CNTFET at 32nm Channel Length (INVERTER).

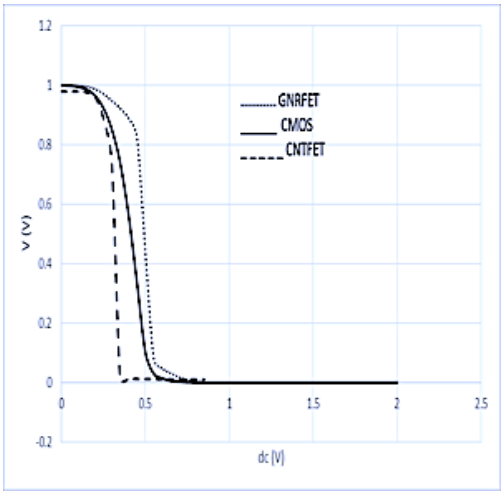


Fig. 3 NAND Gate Using CNTFET.

Parameter/Device	CMOS(32nm)	CNTFET(32nm)
Noise Margin Low	0.3 v	0.2 v
Noise Margin High	0.4 v	0.2 v
Propagation Delay	0.05 ns	0.05 ns
Energy Delay Product	3.5*10 -27Js	8.1*10 -28 Js
Total Power Consumption	6.1 µw	0.85 µw

Table 2. Comparison between CMOS and CNTFET at 32nm Channel Length (NAND).

As we see from table 1 and 2 it's very promising using CNTFET in digital logic circuits as of power and energy wise.

An inverter gate that we created by combining two CNTFETs, a p-type device in the ambient and a vacuum annealed n-type device. A more compact and integrated approach uses potassium doping to convert one of two CNT-FETs built on the same CNT to n-type. The circuit had a voltage gain of about two. After the success of the CN Inverter, other integrated circuits came to substitute that of conventional technology. Various researchers now a day used different approaches to build p and n type CNTFETs and wired the inverters to build complex ICs.

The two main technology constraints that limit the viability of CNTFET technology are the misaligning of CNTs and the presence of metallic CNTs among the semiconducting CNTs, while the CNTs are grown or transferred over a substrate [14] [15]. Metallic CNTs are highly undesirable as they short-circuit the drain and the source of the CNTFET. Electrical burning and Chemical etching of the metallic CNTs are the major techniques addressed so far to remove or break them [16] [17].

There are a few ways at the physical level to get a good alignment of CNTs arrays, and a small percentage of CNTs get yet misaligned and the problem is only partly solved. In spite of superior device characteristics, CNTFET circuits are difficult to get at large scale because of some serious manufacturing challenges like variations in doping and diameter of CNTs, metallic CNTs and misaligned CNTs [14]. As the diameter and doping variations in CNTs cause drain current variations, the major challenge is towards making metallic and misaligned CNTs as they affect the functionality of the gate. Since misaligned CNTs cannot be like avoided by the known CNTFET manufacturing technology, many works are

being implemented to overcome this drawback. One can distinguish the new layout technique that is functionally immune to the CNT misaligning which is referred as misaligned-CNT-immune layouts. This will make the production of standard VLSI cells as well as making tools that allow to go from Layouts to physical cells and then to transistors.

2.2.2 GNRFET

Graphene is an allotrope of carbon; whose structure is one-atom-thick planar sheets of sp2-bonded carbon atoms that are densely packed in a honeycomb crystal lattice. Graphene is most easily visualized as an atomic-scale chicken wire made of carbon atoms and their bonds. The crystalline or flake form of graphite consists of many graphene sheets stacked together [18] [19].

The carbon-carbon bond length in graphene is about 0.142 nanometers. Graphene sheets stack to form graphite with an interplanar spacing of 0.335 nm, which means that a stack of three million sheets would be only one millimeter thick. Graphene is the basic structural element of some carbon allotropes including graphite, charcoal, carbon and fullerenes. It can also be like as an indefinitely large aromatic molecule, the limiting case of the family of flat polycyclic aromatic hydrocarbons [18] [20].

Graphene is an isolated atomic plane of graphite. From this perspective, graphene has been known since the invention of X-ray crystallography. Graphene planes become even well separated in intercalated graphite compounds. In 2004 physicists at the University of Manchester and the Institute for Microelectronics Technology, Chernogolovka, Russia,

first isolated individual graphene planes by using adhesive tape. They measured electronic properties of the obtained flakes and showed their unique properties [21] [22].

Graphene nanoribbons field effect transistor (GNRFET) have appeared only very recently, and demonstrate limited capability to modulate the conductance of a graphene channel at room temperature. The main problem is the need to fabricate extremely narrow nanowires with atomic precision to obtain an energy gap adequate for room temperature operation. Since at the moment the fabrication technology is at its very first steps, computer simulations can be very useful to provide overview of GNR-FETs and to get a high performance [23]. Recent theoretical works have shown that graphene nanoribbons have an energy gap which has an oscillating behavior as a function of width, with average roughly proportional to the inverse width, and that edge states play a very important role in inhibiting the existence of fully metallic nanoribbons. Such behavior cannot be reproduced if one does not consider edge effects [24].

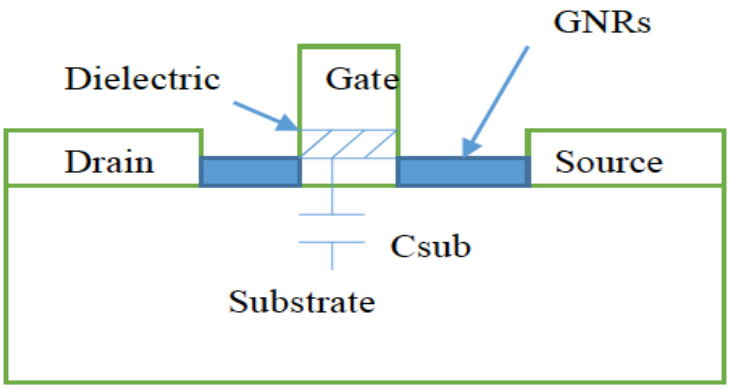


Fig. 4 Illustration of GNRFET Device Model. [25]

As shown in fig.4, this model was designed for GNRFET devices, where each device may have one or more Graphene Nano-Ribbons. The minimum channel length is ~10nm, as various complex quantum mechanisms which describe the sub-10nm regime are not modeled here. Also, the model is based on the assumption of ballistic transport, which is only accurate in a short-channel GNRFET [25] [26]. We used this model in our simulation using cadence simulator.

Also we have implemented some logic gated using GNRFET model and it shows that it very promising in the reliability and less power and energy consumption.

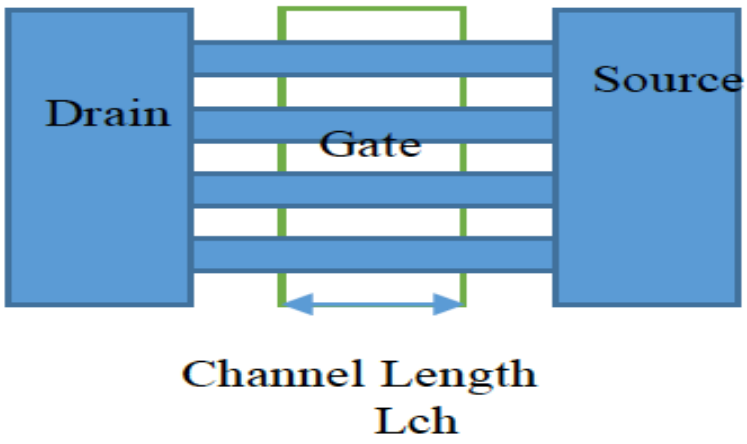


Figure 5. Nanoribbon GNRFET. [27]

As we've seen in fig.5, the width of the GNR is nothing but the circumference when compared to the CNT. The GNR is cut from the graphene sheet. In the Figure 5 we can see that multiple graphene nanoribbons can be laid next to each other where the contact with the source or drain region is made along the width of the nanoribbon.

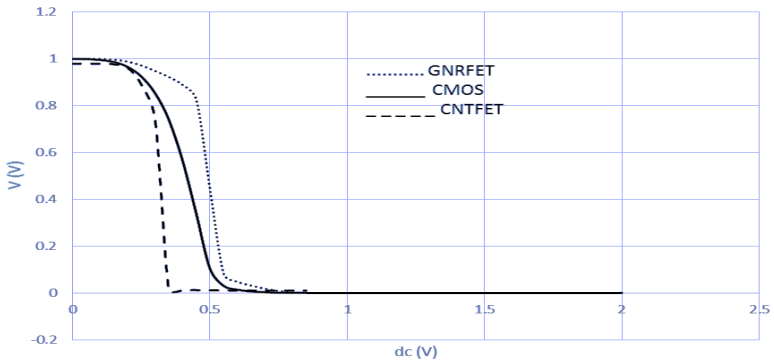


Fig. 6 NAND Gate Using GNRFET

As we seen in fig. 6, basic logic gate using GNRFET model using cadence simulator and it shows promising output than traditional CMOS transistor as we can see in table 3 below.

Parameter/Device	CMOS(32nm)	GNRFET(32nm)
Noise Margin Low	0.3 v	0.3 v
Noise Margin High	0.4 v	0.2 v
Propagation Delay	0.05 ns	0.05 ns
Energy Delay Product	3.5*10 -27Js	1.48*10 -29 Js
Total Power Consumption	6.1 µw	4.907 nw

Table 3. Comparison between CMOS and GNRFET at 32nm Channel Length (NAND).

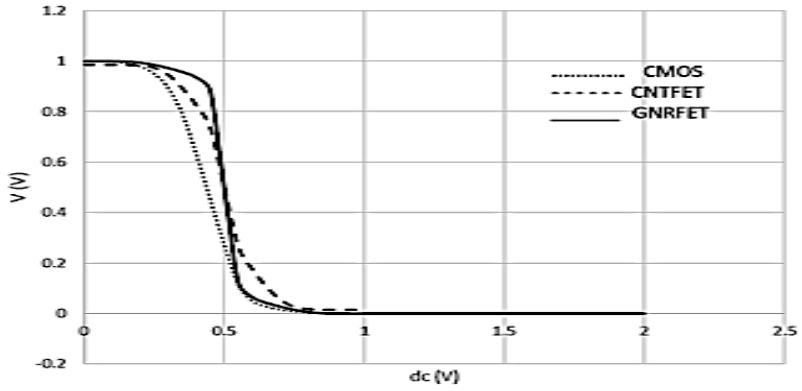


Fig.7 Inverter Gate Using GNRFET.

Parameter/Device	CMOS(32nm)	GNRFET(32nm)
Noise Margin Low	0.4 v	0.2 v
Noise Margin High	0.4 v	0.2 v
Propagation Delay	0.05 ns	0.05 ns
Energy Delay Product	3.45*10 -27Js	1.26*10 -29 Js
Total Power Consumption	5.62 μw	4.1 nw

Table 4. Comparison between CMOS and GNRFET at 32nm Channel Length (INVERTER).

As we see from the previous results, it's challenging to be used in digital logic circuits. We observed that GNRFETs are promising compared to CMOS for low power applications, since they have similar delay with smaller leakage power. It is possible that

GNRFETs would provide higher operating frequency if the threshold voltages were tuned to achieve the same leakage power as CMOS.

2.2 Hardware Security

2.1.1 Trojan Attack

Now a day, we are facing a big problem towards the hardware security, which are hardware trojan and IC's counterfeit. Researchers have tried many methods to detect Trojan or prevent it to happen. To overcome the traditional Trojan detection method, new low-cost testing schemes of high priority to secure the whole design chain in the fabrication foundry also is untrusted. Several Trojan detection schemes have already been proposed, along with two main techniques are functional testing and side-channel fingerprint generation [3]. The assumption is quite weak, since if attackers know the testing scheme, they will surely do the same computation and choose more frequently occurring patterns as triggers. If we know how Trojan inserted chips by comparing the side-channel fingerprints of tested chips with those generated from gold models. It analyzed the common behavior of various types of Trojans and demonstrated the feasibility of building effective fingerprints for an IC family to detect Trojan-inserted ICs. There are two kinds of Trojan, which is trigger and payload. For trigger, it classified into two, which is digital and analog. In digital part, it divided into combinational and sequential. For payload, it classifies into digital, analog, and other. For digital part, circuit nodes and memory content. For analog part is bridging, delay, and activity [4].

When examining the threat posed by a Hardware Trojan, one must first consider its inherent attributes in order to determine its effect on an information system. There have been several Hardware Trojan taxonomies proposed to describe such attributes, with the aim to enable a systematic study of Hardware Trojan characteristics, as in fig.8[4], we gathered security issues kind as between trigger and payload for each analog and digital and other.

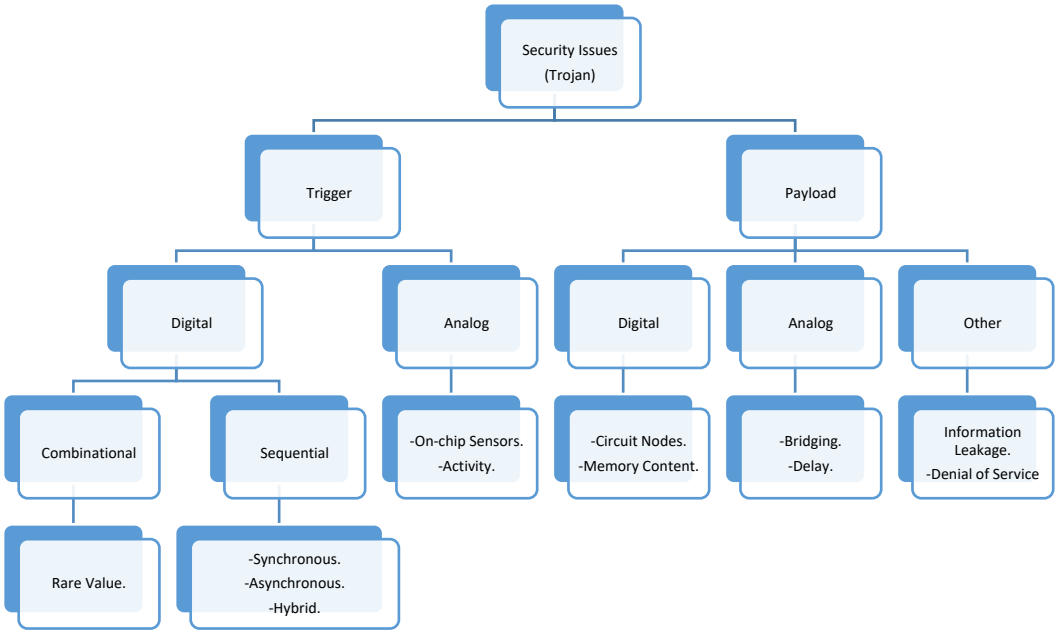


Fig. 8 Taxonomy of Security Issues Kinds [4].

For Trojan classification, it has physical characteristic, activation characteristic, and action characteristic as we see in fig.9[4] taxonomy.

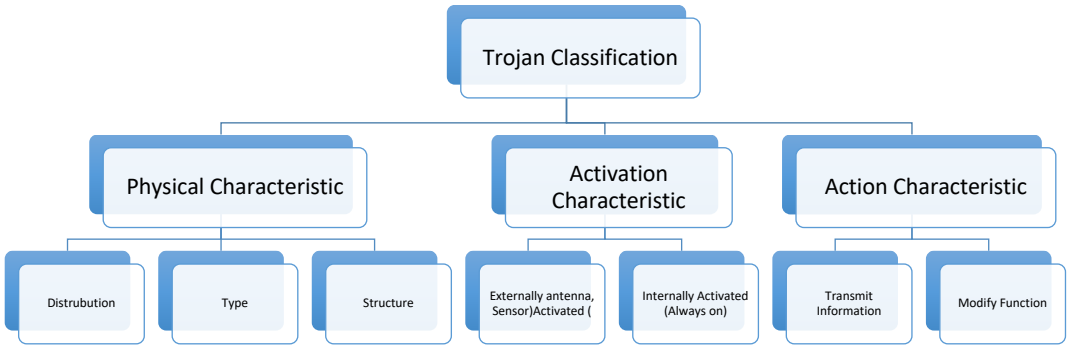


Fig. 9 Trojan Classification [4]

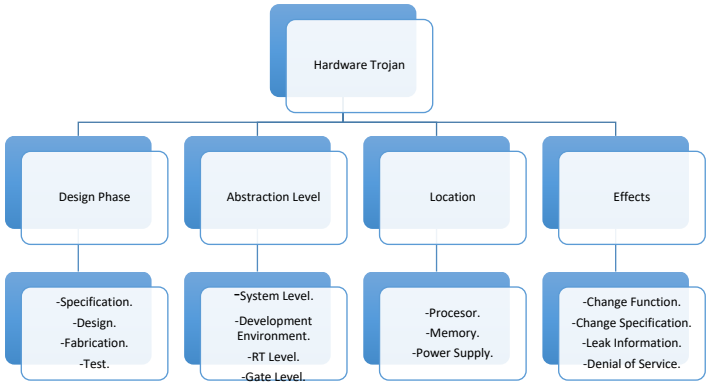


Fig. 10 Hardware Trojan. [5]

Fig. 10 shows the hardware trojan with the location that it can be founded. It can be inserted through the design phase like fabrication or test, abstraction level like gate and RT level, and it's effect include leak information, change function, and change specification.

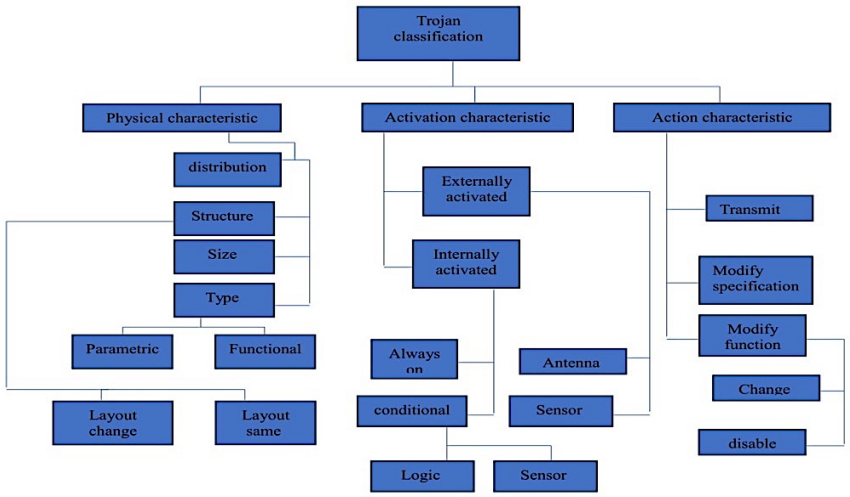


Fig. 11 Detailed taxonomy showing physical, activation, and action characteristics of Trojans[45]

In fig. 11, it shows detailed taxonomy physical, activation, and action characteristic of hardware trojans developed by Wang, Tehranipoor, and Plusquellic. This taxonomy allows

researchers test their own methods for different Trojan types. Technically, it's a metrics for evaluating in industry the effectiveness of methods in detecting Trojans[45].

Trojans could be hybrids of this classification (for instance, they could have more than one activation characteristic), this previous figure indicates the elemental characteristics of Trojans and is suitable in evaluating the capabilities of different detection methods[45].

A Hardware Trojan can be added in different locations that can yield to different operation of the required design. The location is not necessarily limited to a single component but also can be distributed across multiple components such as the processor, memory, IO, power supply. A particular location influences the complexity of design, difficulty of insertion, as well as the actions or system effect of a Trojan.

Hardware Trojan as we see in fig. 12, we use ISCAS85 benchmark circuit, c17. It has 5 inputs G1, G2, G3, G4 & G5 and 2 outputs G10 & G11.

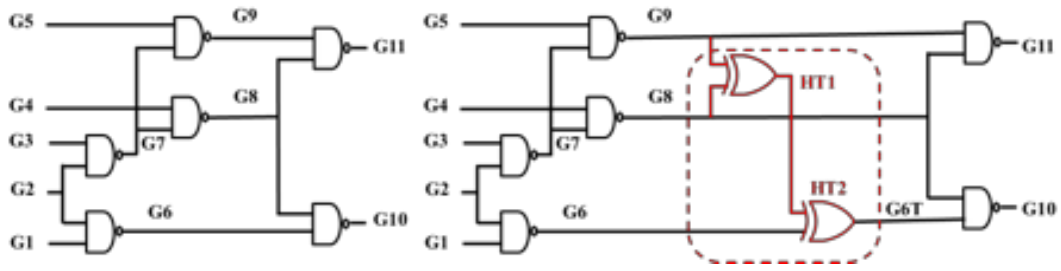


Fig. 12. (a) Logic circuit of C17 benchmark circuit (b) Logic circuit of C17 with Trojan

A typical hardware Trojan which is consists of two XOR gates is inserted, which is activated depending on the internal signals of the circuit as in Fig 11(b). Trojan one of the XOR gate basically is a comparator its output will be logic 1 only when its inputs are unequal. The comparator output is connected to another XOR gate which is trojan two. Trojan gets activated flipping the signal G6T when the activation signal is 1 and obviously

producing error at the outputs G10. When the Trojan is not activated, it is hard to detect it, since is treated as a black box with primary inputs and outputs at the manufacture test phase. The Trojan gets activated only 6 times out of 32 possible input vectors, that means constitute only 18.75% of the entire input space. Technically , it will be difficult to detect Trojans in such a circuit using post manufacturing functional tests.

Trojan activation characteristics divided into two categories: externally activated and internally activated. The activation could be based on the output that tracks temperature, voltage. On the other hand, this condition could be based on an internal logic state, like internal counter measurements. The Trojan in these cases is developed by adding logic gates to the chip. Researchers have designed a lot of methods to evaluate Trojans detection techniques in an IC[45].

Hardware Trojans have only laterally get the researcher attention, thus to date very few actual published implementations exist. Those referred to in current publications typically are simplistic single hard coded solutions that have been used solely for the purpose of experimenting with detection and countermeasures verification. Very few in-depth consideration has been given to the system-wide effects of a single or coordinated Hardware Trojan attack, or the practicalities associated with implementing command and control for such attacks [5].

2..1.2 Counterfeit Problem

For the second section to our investigation, we are facing in hardware security problem related to counterfeit integrated circuits (ICs). A major source of concern in the electronic

component supply chain as of reliability and security issues, are impacting many industrial sectors, including computers, and even military systems. The consequences can be dramatic when critical systems begin to fail due to the use of counterfeit or low-quality components [6]. Due to legitimate electronics, companies miss about $100 billions of global revenue every year due of counterfeiting [6]. In addition, the high technology industry affected by counterfeiting activity. Around 1% of semiconductor sales are estimated to be those of counterfeited units. The tools and technologies used by counterfeiters have become more sophisticated and well financed. In turn, this also calls for more complicated methods to detect counterfeit electronic parts that enter the market [7].

The counterfeiters are getting better, more skilled. They have improved machines for demarking and remarking which altered top marking looks genuine. They can now micro machine the laser marks off a package and then remark with their own laser the part number. There is something even more frightening with this situation: many low-grade legitimate parts are being related to a higher grade and coming into critical electronic systems [8]. When that happens, the counterfeit inferior parts will work suitably for a short time, but only for a while. They are stressed from the outset and it is highly likely that they will fail. Counterfeit has different types, which is recycled which is nonfunctional, remarked as a recycled, overproduced fabrication, out of specifications defective as performance and manufacture reject, and tampered like silicon time bomb as we will see in the next taxonomy in fig. 15 [9].

There are different types of counterfeit and also different detection methods. In the following taxonomy, it shown different counterfeit types and the avoidance methods.

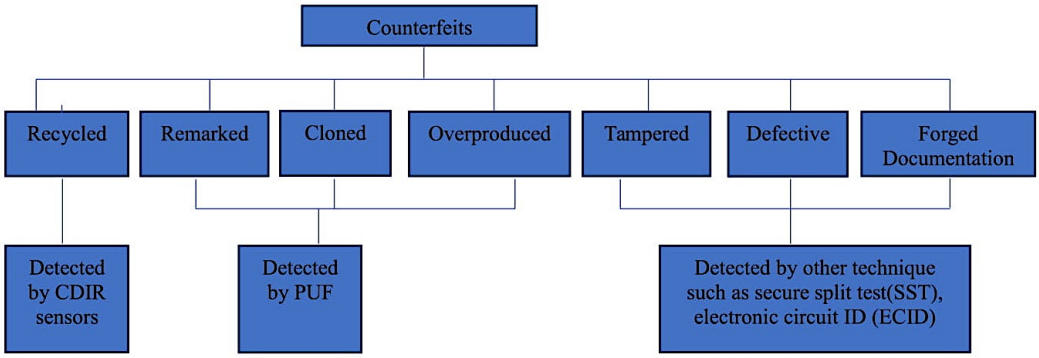


Fig13. Taxonomy of counterfeit types and avoidance methods[42]

Counterfeit electronic parts has seven different categories as shown in Fig. 13. Recycled counterfeit can be detected by CDIR sensors, remarked, cloned, and overproduced can be detected by PUF method as we will see in the next section, tampered, defective, and forged documentation can be detected by other technique like secure spilt test (SST), and electronic circuit ID (ECID).

Detecting counterfeit components has been created in the past several years for testing. The components must be authenticated by these tests before get inserted in systems. Fig. 14 shows a taxonomy of counterfeit detection methods. The methods are classified into physical and electrical inspections[43].

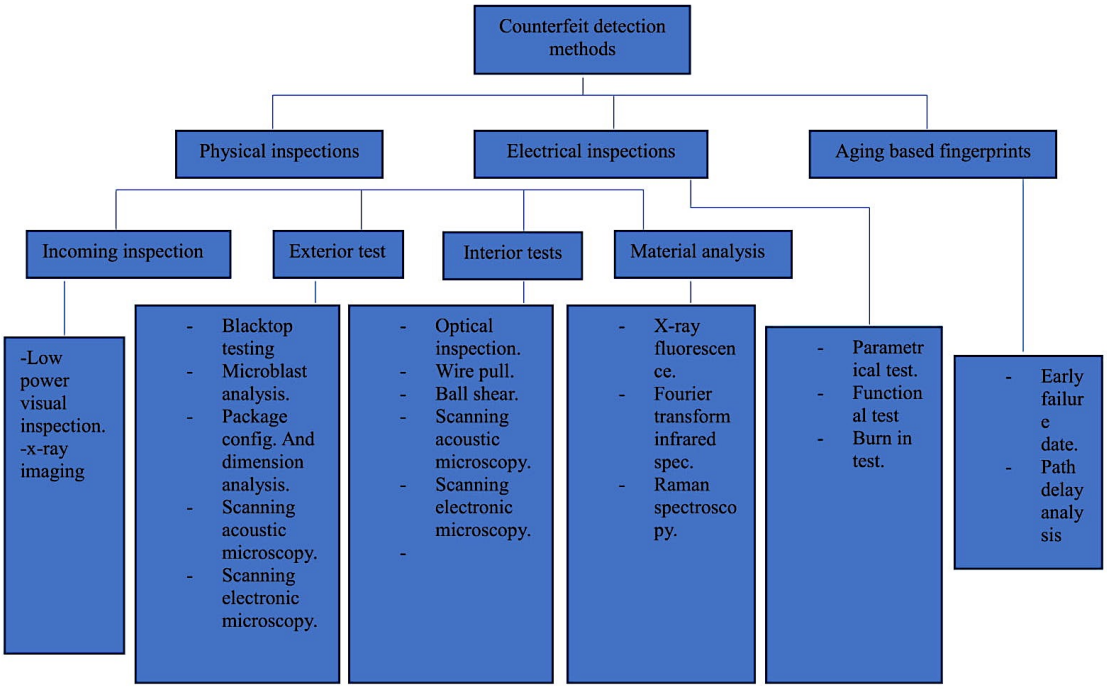


Fig. 14 Taxonomy of counterfeit detection methods.[43]

As fig.14 shows, detecting counterfeit has three different sections, physical inspections, and electrical inspections, and aging based fingerprints.

For physical inspections it has incoming inspections, exterior test, interior test, and material analysis. In electrical inspections, it contains parametrical test and burn in test. The last one is aging based fingerprints which has early failure date, and path delay analysis.

Some researchers have got some method to overcome the counterfeit problem with all the verities of the counterfeit. By using new technology like Carbon Nanotube and Graphene Nanoribbons as a new technology will help in enhancing and increase the probability to

get rid of the counterfeit parts. The counterfeit is classified to several categories as in fig. 15, which include recycled, remarked, overproduced, out of specification defects, tampered, and forged documentation. All of these are several types of counterfeit that are not eligible. In addition, there are a method to detect the counterfeit parts, which is physical inspections, electrical inspections, and aging based fingerprints [9]. Also by using PUF method, which will be discuss later, using the two technology to implement PUF by carbon and graphene will enhance the ability to overcome the counterfeit problem.

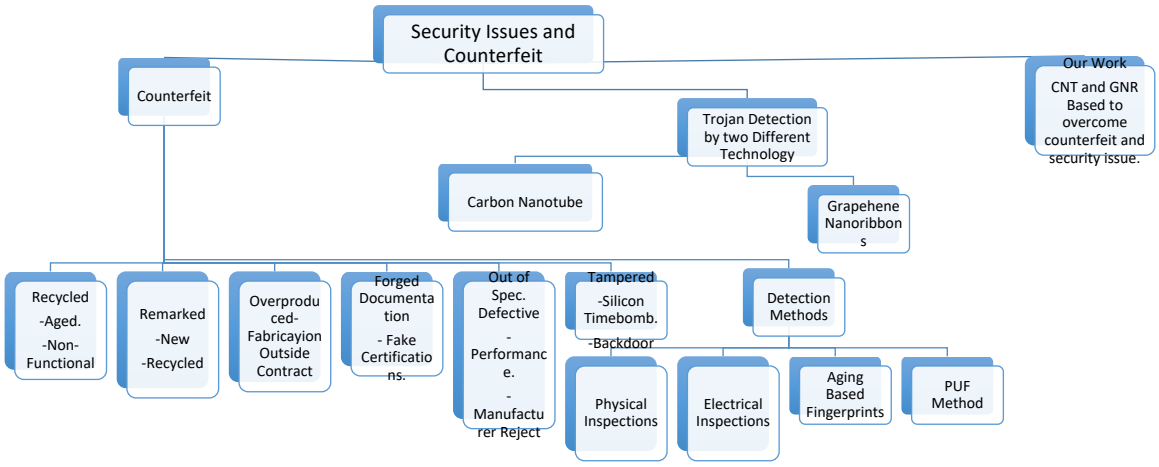


Fig. 15 Taxonomy of Counterfeit Categories includes CNT and GNR models [9].

In the upcoming section we will talk on carbon nanotube field effect transistor (CNTFET) and graphene nanoribbons filed effect transistor (GNRFET) and how we can use them to help in solving the previous problems we mentioned.

2.3 Motivation

As we have seen from the background section, carbon based materials are very promising to be used instead of silicon in the future. In the next chapters, we will explore these

advantages of carbon and graphene filed effect transistor to overcome problems like hardware trojan attack and IC's counterfeit. In hardware trojan attack, we used traditional method in detecting trojan by measuring the circuit sensitivity in terms of static and dynamic power. On the other hand, we also used methodology called segmentation based detection using sleep transistors. This method is dividing the whole circuit into blocks so that it could be easier to detect Trojan when you look at specific portion of the circuit at one time. The second problem that we are investigating is the IC's counterfeit problem. We proposed ring oscillator based physical unclonable function designed for CNTFET and GNRFET using the appropriate model for each one of them. We relied on using the process variation associated with the two models. For carbon nanotube field effect transistor, we used the advantage of changing the number of nanotubes as it's a random value in the manufacturing process. For graphene nanoribbons, we relied on changing the number of dimer lines which is directly proportional to the channel width. Our proposed models are able to produce results near to the ideal case in terms of inter and intra hamming distance, which is much better than Mosfet results.

In the future work, we wants to explore neutralization method to enhance the hardware trojan detection and also come up with a new design using less number of transistor to overcome the IC's counterfeit problem.

2.4 Prior Work

Carbon Nano Tubes and Graphene Nanoribbons in Hardware Security

As from previous discussions, Nano transistors will be the main demand of the technology in the next years as for high performance in technology. Therefore, using CNTFET and GNRFET in such a hardware security will be the more challenging in the future, as it will be more efficient in detecting the Trojans and it will faster and more reliability, so we can use CNT and GNR in PUF method so we can use all the advantage of both in PUF by different methods. As of now, we make different researches in using both of them in hardware security [28].

For the reliability, it has two different feature that enhance the reliability and gain it more advantage, first, strong impact of physical variations, and second, regular design that can make the design easier.

2.3.1 What is PUF?

Authentication is a procedure that has been used by societies over the years to identify individuals. Forms of authentication have evolved as per the needs. In this digital age, scope of authentication has increased with complexity of business and the increased number of personal devices with sensitive personal information.

An attacker can succeed in gaining access to the secured information that is stored in a particular location in the database. Similarly, an attacker may gain physical access to smart cards and personal devices. However, how we can make it more difficult for them to gain

access to the information. One way is to use intrinsic features from its hardware circuitry that are prone to process variations and do not require physical storage. The motivation is to get this random but repeatable information to generate an authentication key in real-time. This method is called a Physical Unclonable Function (PUF) [29] [30].

PUFs are random functions, they must some properties depending on the application and its requirements. Here are some properties of PUF's as described in the below points[44]:

1) The Challenge Response Pair (CPR) is preferred to be random.

2) Depend on the application, the challenge response pair have to be generated in a short time.

3) It must not be possible to model the PUF from a set of challenge response pairs.

4) A PUF based implementation must have low attack variety, even if the attacker is able to extract the CRP in one occasion, it should not be possible to extract CRPs at other time occasions.

5) It needs to satisfy the Strict Avalanche Condition (SAC) to realize greatest security[44].

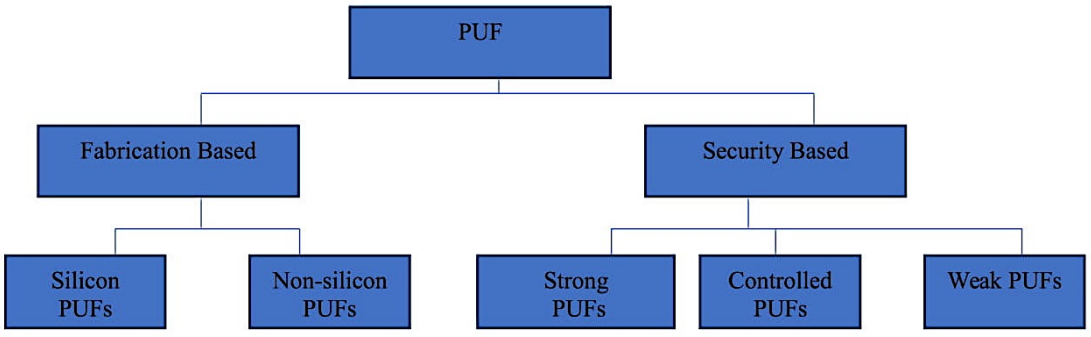


Fig. 16 PUFs Classification[46]

PUFs can be classified based on fabrication method and security strength, as shown in Fig. 16[44]. For fabrication based, it has silicon and non-silicon PUFs. In security based, it consists of strong, controlled, and weak PUFs.

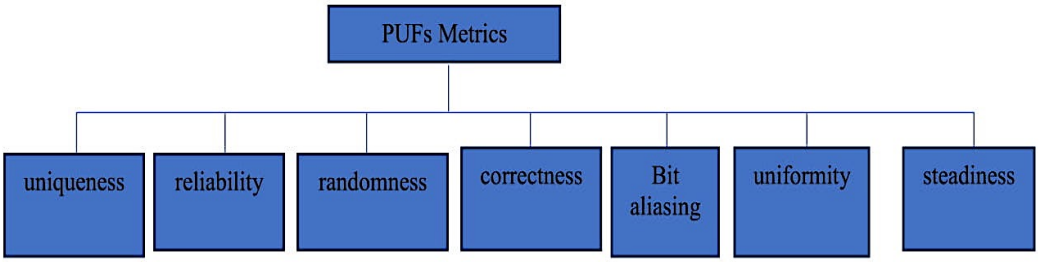


Fig. 17 PUFs Metrics[47][48]

There are different metrics for PUFs to be tested as shown in fig.17, below are the metrics that should be considered for testing PUFs design[44]:

1) Uniqueness: It is a measure of the average inter-chip Hamming Distance (HD) of the response obtained from a group of chips. An ideal PUF has a uniqueness value of 50% which means that approximately half the bits in the responses of the PUFs should be flipped in the output response.

2) Reliability: It is a measure of how much reliable is the CRP under noise and environmental variations. The ideal value for reliability is 100% which means that the PUF should produce the same response for the same challenge in the same instance under different environment conditions like changing in temp. and voltage.

3) Randomness: It is a measure of balance between “0”s and “1”s in the response bits of the PUF and measures the randomness. The ideal value is 100% .

4) Correctness: It is a measure of correctness of the response under different operating conditions. The ideal value is 100%.

5) Bit Aliasing: It is a measure of biasness of a particular response bit across several chips. The ideal value is 50%[49].

6) Uniformity: It is a measure of how random is the CRP. For a response to be random, the number of “0”s and “1”s in the response should happen with equal probability.

7) Steadiness: The measure of biasness of a response bit for a given number of “0”s and “1”s over a total number of samples gives the steadiness. The ideal case for steadiness is 100%.

There are different PUF applications as shown in Fig. 18. PUFs can be used in applications of randomness during their operation[44]. PUFs can be used in Radio-Frequency Identification (RFID) tags, secret key generation, and in device authentication. PUFs is also used in consumer devices for low-cost authentication purposes[44].

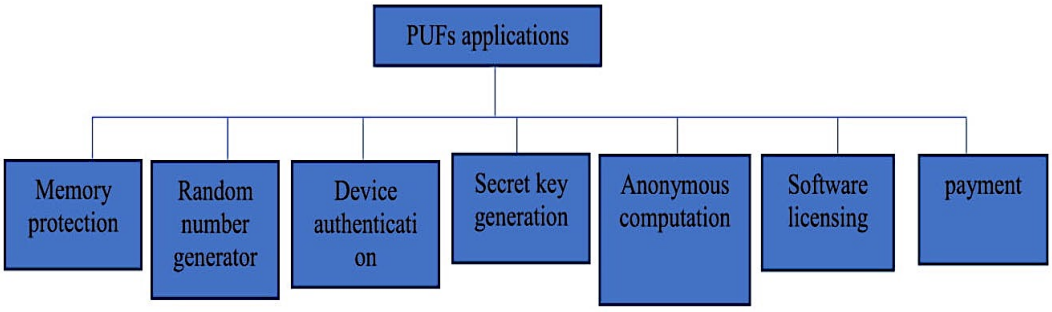


Fig. 18 PUFs applications[44]

PUFs applications as shown in fig.18 has several purposes that can be used in. it includes memory protection, random number generator, device authentication, secret key generator, anonymous computation, software licensing, and payment.

As of now, most PUF circuits are based on silicon devices, and are focused on improving randomness, reliability and robustness without tracking how much of the power consumption. Semiconductor industry is scaling logic devices for high speed, low voltage and low power consumption, to scale down the silicon channel length has some limitations. At a certain limit, it cannot be reduced more due to degradation of gate control on the channel and it will not act as a proper switch. The addition of doping density in the channel can counter the effect but it will lower the carrier mobility. Carbon based materials like the carbon nanotube (CNT) and graphene are promising candidates as we will investigate them in the upcoming sections.

Carbon Nanotube FET (CNTFET) based PUFs as we will see in the next sections results, aim to achieve better reliability, low energy and power consumption instead of using

silicon based. In CNTFET transistors, CNTs are used in the channel instead of bulk silicon. The process variations that can be used in the design for CNT are chirality, number of nanotubes, diameter, growth density, misalignment, doping concentration. The chirality variation can be used to generate secret digital bits. Chirality of CNTs is the direction in which the graphene sheet is rolled. It consists of three different types, chiral, zigzag, and armchair. It can be metallic or semiconducting depending on the chirality. There is a design made in [32] with CNTs. A serial connection of CNTPUF parallel elements as shown in Fig. 13, can be used, each CNTPUF-PE consists of parallel CNTFETs sharing a common gate voltage. Each CNTFET consists of a large number of semiconducting CNTs and a small number of metallic CNTs. As shown in Fig. 13, each CNTPUF-PE consists of one distinct state, each for high input gate voltage and low input gate voltage. Because of process variations, these states changes in each stage, and then compared in the final stage to give the response bit [32]. In fig. 19 the design was implemented by using CNTFET in PUF method and it shows a good advantage using CNTFET instead of traditional transistor [32].

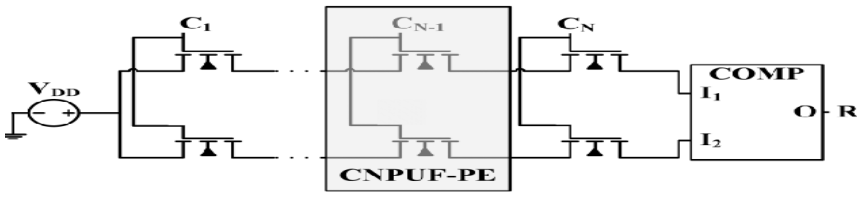


Fig. 19 Row of the CNPUF design. A series of CNPUF-PE are evaluated by a comparator (COMP) to generate the output bit [32].

Another material that we have focused on related to carbon based is graphene nanoribbons. Graphene has a high mobility and its advantages as channel material in FETs for very high speed operation. Graphene is a 2-D carbon atom placed on a honeycomb lattice, and it's a graphite. Graphene is strong in almost all directions. There are a lot of interesting properties in graphene that it can be replaced the silicon in future technology. We have investigate the use of graphene nanoribbons as in FETs as we will discuss in the next chapter the advantage of using graphene in PUF design.

Hardware security has emerged as an important field of study aimed at mitigating issues such as piracy and side channel attacks. The most important solution for such hardware security attacks and counterfeit are physical unclonable functions (PUF) which provide a hardware specific unique identification as we discussed before [29] [31]. The uniqueness of a PUF depends on intrinsic process variations within individual integrated circuits. As process variations become more prevalent due to technology scaling into the nanometer regime, CNT in PUF method has discovered a lot of advantage in the power and high performance side.

In Fig.20 it shows the previous work for both counterfeit problem and Hardware Trojan Detection.

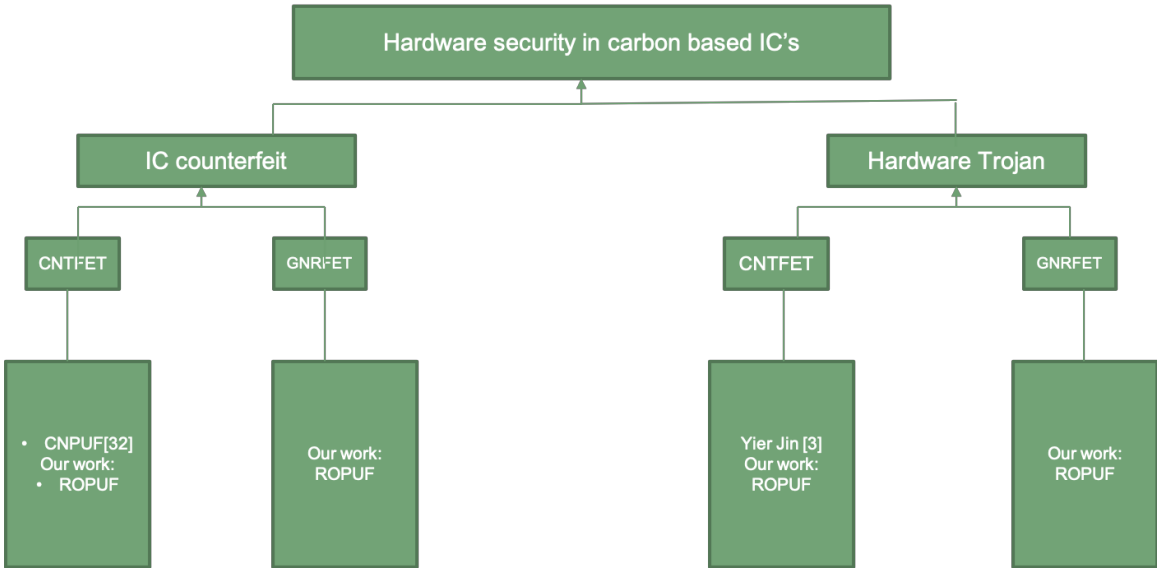


Fig. 20 Taxonomy of Previous Work of Carbon Based Material in Both Counterfeit and Trojan Detection.

According to the investigation that made on that side, CNPUF (carbon Nano tube physical unclonable function) achieves higher reliability against environmental variations and also increased resistance against modeling attacks. Also, CNPUF has a considerable power and energy reduction in comparison to previous ultra-low power PUF designs using traditional method of 89.6% and 98%, respectively [32]. Additionally, CNPUF allows power-security tradeoff. Moreover, CNTs have great potential in all applications. So if we observe the main advantage of using CNTFET we will see that it will considerable reduction in footprint by using CNTFET unique properties to reduce the transistor count, so if we see the different between regular PUF and after include CNT in the design, we will observe that extremely low power and energy consumption that is 89.6% and 98% lower than ultra-low power current based PUF at 90 nm, very high reliability in different applications and a very accurate experimental evaluation in two different settings, an extended design that performing a power-security tradeoff, highly relevant for practical usage scenarios, and

evaluation of PUF behavior with different CNT technology. CNPUF provide the future basis for more authentication and secret key generation by making security at a very low area and power cost [32].

2.4 Contribution

Our contribution is using CNTFET and GNRFET in IC counterfeit and hardware trojan detection. Second section is to do analysis using CNTFET and GNRFET for hardware trojan detection relying on the sensitivity by measuring static and dynamic power. The third section is using sleep transistor method based on power gating method.

CHAPTER 3
DESIGN

In this chapter we are going to discuss out methodology for our design and how we used the advantage of using CNTFET and GNRFET in the design.

3.1 Ring oscillator physical unclonable function (RO-PUF) With CNTFET and GNRFET

3.1.1 Single-bit ROPUF

Physical unclonable function (PUF) its idea is to use the physical structure of the device to generate a set of unique data. PUF is using in security for hardware devices and its used as a key generators or challenge response authentication methods.

There are many types of PUF, we used ring oscillator PUF (RO-PUF) as It's simple to test our objective for using different models to test what is the best. We implemented 512 response bits PUF with 3-stages of inverter. The inverters followed by two mux's to choose from the RO's serial according to the challenge being applied to the mux input. The next stage to count the ring oscillator cycle chose by each mux using counter for each chosen one. The comparison is the last stage to compare between the two frequencies, if freq.1 greater than freq.2 the response is equal to 1, otherwise, is equal to 0. Fig.21 shows the illustration of ring oscillator puf used in out simulation process [33].

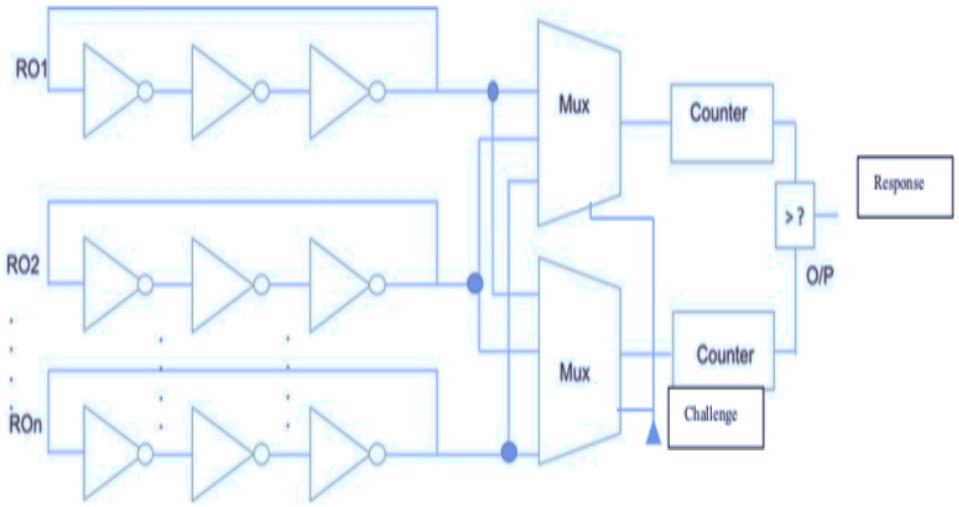


Fig.21 Ring oscillator PUF [33]

3.1.2 Process variation

Proof of Concept

Before we implement our design we ran a single bit ROPUF at different number of N's used in our design and we observed at each value of N we're getting different cycles output from the counter as shown in the following table.

N	Cycle (Sec)
6	$1.32*10^{-10}$
7	$1.24*10^{-10}$
9	$1.11*10^{-10}$
10	$1.07*10^{-10}$
13	$9.73*10^{-11}$
16	$8.99*10^{-11}$

Table 5. CNT N Variation

N	Cycle (Sec)
6	$6.84*10^{-11}$
7	$5.61*10^{-10}$
9	$5.90*10^{-11}$
10	$6.56*10^{-11}$
13	$3.007*10^{-11}$
16	$9.26*10^{-11}$

Table 6. GNR N Variation

3.2.1 CNTFET

In this section we are going to discuss our design approach and steps we did to enhance the RO-PUF design with using different models with introducing new parameters in the

process variation steps. We have implemented RO-PUF using carbon nanotube, graphene nanoribbons, and BSIM CMOS models. We introduced for CNT and GNR models a new process variation to the RO_PUF design mentioned by each models specifically than the traditional method for CMOS. In CNT model, we changed the number of carbon nanotubes as a process variation [34] [35]. As it's shown in fig.22 the place between drain gate and source gate is the carbon nanotubes [36].

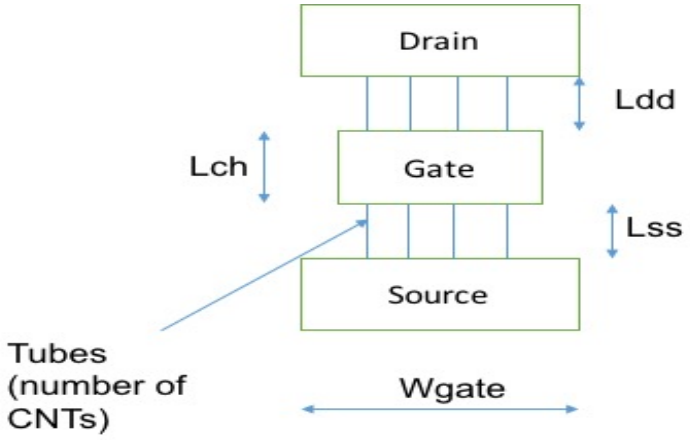


Fig.22 CNTs between drain gate and source gate [36].

CNT's could be metallic or semiconducting [35]. CNTFET can't be metallic as the current of the metallic can't be controlled by the gate voltage, so it will cause a short between the source and drain. As in [35] [37], 1/3 of CNT's are metallic according to random distribution of CNT chirality. In Stanford model, they assumed that that metallic can be removed by a perfect removal process rather than electrical burring or chemical etching [38] [37]. However, the number of CNT semiconducting becomes a variable which will result to vary the drive current as in eq.1[37].

Where, $$I_{CNFET} = n.g_{CNT}(V_{dd} - V_{ss'} - V_{th,CNT}) \quad \text{Eq.1}$$

I_{CNFET}: CNTFET on current

n: number of CNTs per device.

$V_{th,CNT}$: Threshold voltage.

g_{CNT}: Transconductance per CNT.

AND,

$$V_{ss'} = (I_{CNFET}L_s\rho_s)/n \quad \text{Eq. 2 [37]}$$

Where,

L_s is the source length.

ρ_s is the source resistance per unit length of doped CNT.

Therefore, the final on current will be as in eq. 3,

$$I_{CNFET} = \frac{n.g_{CNT}(v_{dd} - v_{th,CNT})}{1 + g_{CNT}L_s\rho_s} \quad \text{Eq. 3 [37]}$$

As mentioned in Eq.3, the drive current increases with increasing the number of CNT, however the threshold voltage is decreasing with more CNT in the device.

Although, the threshold voltage is depending on the CNT diameter as in Eq.4.

$$V_{th} = \frac{\sqrt{3}}{3}\frac{aV_{\pi}}{eD_{CNT}} \quad Eq.4$$

CNT's count N is dependent on width, however, it decides the value of drive current, but, extracting all the distribution is time consuming [34]. To indicate the CNT count distribution is only by the mean and variance of CNT spacing [37].

The index of dispersion of the CNT count distribution can be calculated from the coefficient of variation of the inter-CNT spacing ($\gamma = \sigma_S / \mu_S$) as in the following equation 5 [38] [37],

$$\frac{\sigma^2[N(W)]}{\mu[N(W)]} = \left(\frac{\sigma_s}{\mu_s}\right)^2 = \gamma^2 \qquad Eq.5$$

The index of dispersion is a major factor in measuring the variation in CNTFET circuit. The previous equation applies to any type of CNT's either metallic or semiconducting.

As we use 32nm technology in our circuit simulation, to minimize the performance variation for the minimum sized device with $W_{g,min}$=1.5Lg, at least 200 CNTs/μm is desired[37].

So, for maximizing the highest performance at the 32 nm node, CNT density of 200 CNTs per μm gate width should be desired. Increasing the number of CNTs per device will increase the total current drive, and also illustrates the trade-off between the speed and energy consumption. With 1 to 10 CNTs per device, the FO1 speed of CNTFET circuits is about 2× to 10× faster compared to CMOS circuits, the energy consumption per cycle is about 7× to 2× lower, and the energy-delay product is about 15× to 20× lower. Increasing the number of CNTs per device is the most effective way to improve the circuit speed [34] [38].

Number of Semiconducting-CNT and Metallic-CNT in a CNTFET can't be predicted because of the probabilistic nature of the growth process for CNT. Due to this problem, delay variations in CNTFET- based logic circuits get performed. Even if an ideal removal process could use to get rid of m-CNTs in the growth process. It can still do a random number of S-CNT in CNTFET device, which will vary the number of CNT [34].

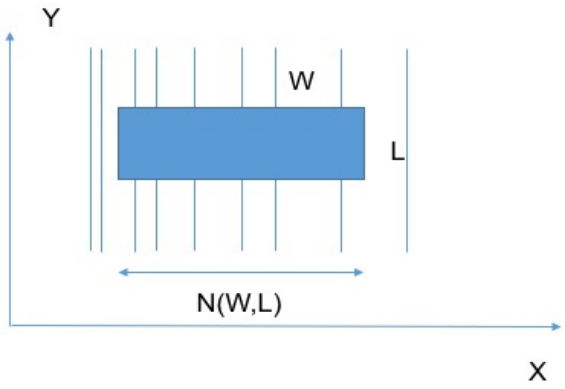


Fig.23 CNT Count Model [34]

As it's shown in fig.23 [34], CNTFET refers as a rectangular box with length and width, the number of CNT passes through the box is the number of CNT count (N). N is random value depends on the place of the box.

Multiple tubes per device are allowed under the same gate. In the model that we used, multiple nanotubes in the same device are handled by the model. The gate width that's been used is 6.4nm as a global parameter.

CNT count variations caused by CNT density variations and by the elimination of some

CNTs when a m-CNT removal process like electrical burning and chemical etching are applied.

Table 1 shows the relation between the gate width and CNT count as mentioned in [34] [37].

Gate Width(nm)	CNT count
16	8 (max)
16	3 (optimal)
32	16(max)
32	6(optimal)

Table 7 Gate width and CNT count [37]

3.2.2 GNRFET

For the next section, I will discuss the process variation parameter used in graphene nanoribbons model invented by Illinois university. In our simulation, we varied the width by changing the number of dimer lines N [39] which is function in the device width as it's shown in the following equation 6 and in illustration of fig. 24 [39] [40]

$$W_{ch} = \sqrt{3} d_{cc} (N + 1)/2 \qquad \text{Eq. 6[41]}$$

where, d_{cc}=0.142nm carbon-carbon bond distance.

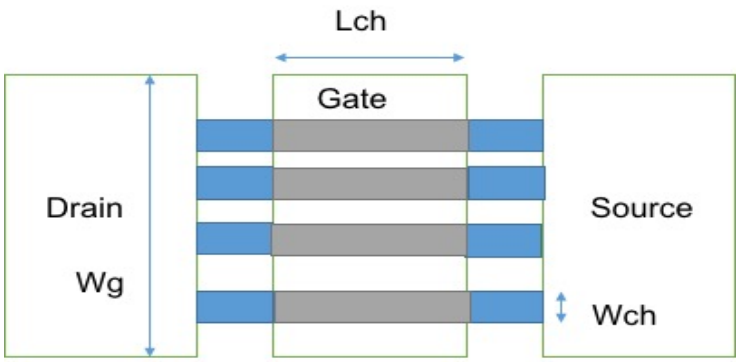


Fig. 24 GNRFET device [41]

The band gap of GNRs is inversely proportional to the width. The wide of the width will has small band gap and low value of Ion/Ioff ratio and it will not be suitable for digital circuits. The suggested value of N has been mentioned in the reference paper of the model. For N= 8, 11, 14, and 17, the band gap is very small which will cause low ratio of Ion/Ioff. For N= 6, 9, 12, 15, and 18, the band gap is moderate and will result a high ratio for Ion/Ioff and high on current. For N= 7, 10, and 13, the band gap is very high, which will result to highest Ion/Ioff ratio but with Ion lower as for large band gaps there are a problem for carriers to occupy the channel. For our simulation I used the N values associated for moderate band gap and we changed the values as a Gaussian distribution [39].

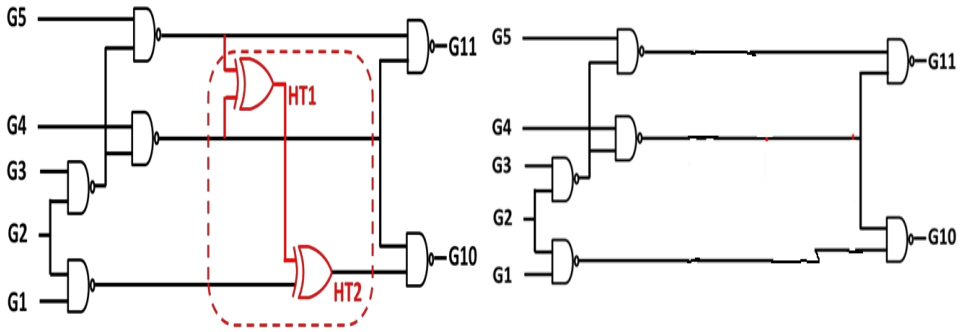
As they mentioned in [39] [40], the GNRFET model has been tested after fabrication. The result shows the change in Ion and Ioff by varying the number of dimer lines.

In our simulation for using GNRFET in RO-PUF design, we used N to introduce the process variation in the simulation. We chose N values as mentioned earlier to get a moderate band gap and high Ion/Ioff ratio value [39].

3.2 Hardware Trojan :Results and Analysis

In this section we analyzed multiple circuits using static and dynamic power. We measured sensitivity from the static and dynamic power. We have made a comparison between regular CMOS, CNTFET, and GNRFET. The circuits that we used are C17, C432, C499, C880, and C1355.

The shown figure 25 is for C17 circuit with trojan's been inserted.



(a) (b)

Fig. 25 C17 Circuit with Trojan (a) and without Trojan (b)

We have used the trojan circuit in C17 to be inserted in the other remaining circuits. We provided the static and dynamic power for both cases with trojan and without trojan. Results will be showed in the following chapter.

3.3 Hardware Trojan Detection using Sleep Transistor

In this section I have used power gating method which uses sleep transistors in segmented blocks. We used a 32bit-ALU circuit as an instance as in fig. 26. The whole 32bit-ALU circuit is provided by Vdd=1V, and common ground is provided at the bottom circuit. Leakage power can be measured by the current Idd at quiescent state when the inputs are

constant, hardware Trojan will consume leakage power and it can be detected by comparing the leakage power.

Trojan is implemented to 32-bit ALU circuit with same Vdd, a change in leakage power will be a sign for detecting the trojan. We have used a Trojan of 3-bit comparator, comparing to 32-bit ALU unit (7208 transistors, 1280 gates), and the size is 0.58% of 32-bit ALU in transistors level.

We have measured TCR which is the ratio that shows the leakage power proportion of a Trojan on the circuit.

$$\mathrm{TCR} = \frac{|P_{TI} - P_{TF}|}{P_{TF}}$$

P_{max}= the maximum value in leakage power distribution

P_{min}= the minimum value in leakage power distribution

P_{avg}= the average value of leakage power

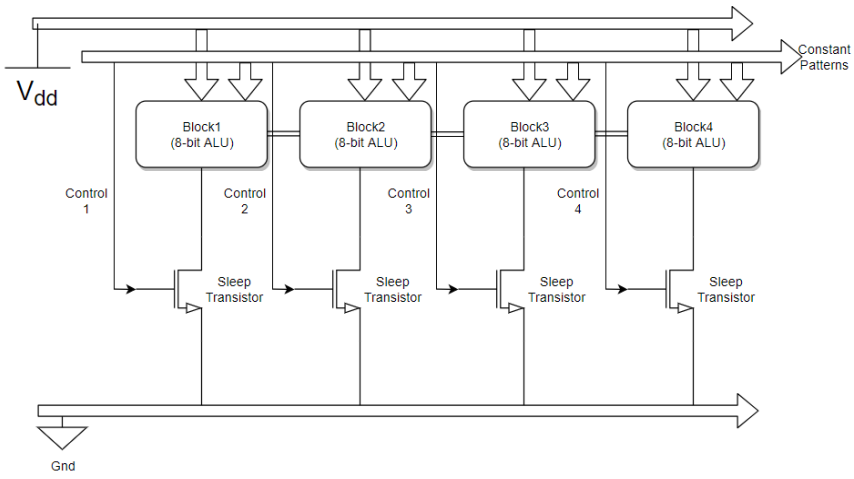


Fig. 26 Power-gating technique in 32 bits ALU

In fig. 27 we segmented the ALU into 4 different blocks so that detecting trojan would be much easier if it's found in one of these blocks rather than testing the whole circuit.

In the following figures, the trojan is found in one of the 4 blocks as shown.

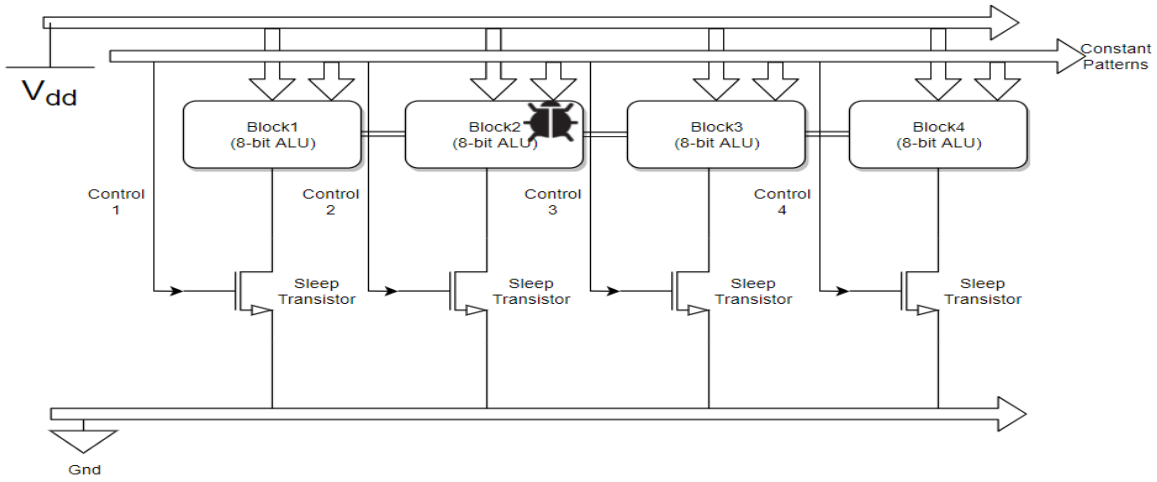


Fig. 27 32-bits ALU with trojan in block2

In the following flow chart in fig. 28, the steps for detecting the trojan is being discussed as follows.

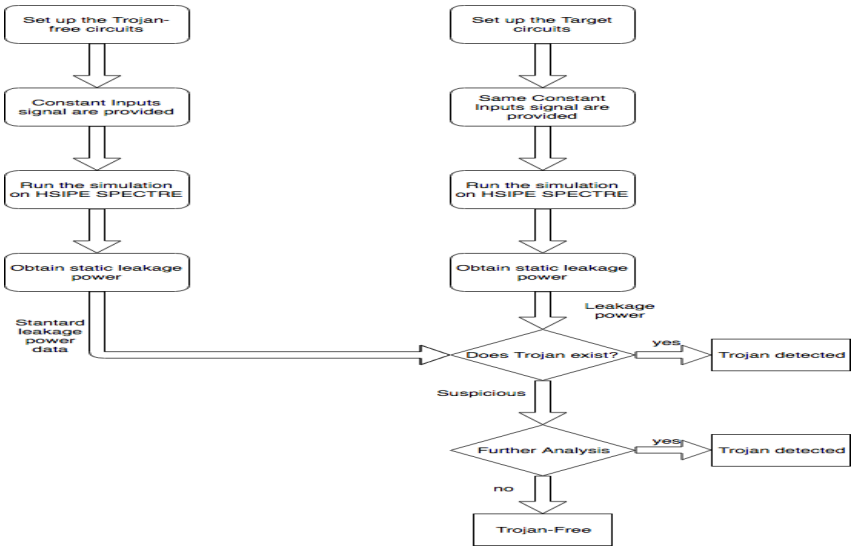


Fig. 28 Flow chart of trojan detection in power gating.

As we've noticed in the previous figure, the process of detection takes one more step to double check if trojan found in one of the blocks or not. This is makes power gating method good candidate in trojan detection. In the next chapter we will explain the results and how trojan detection has been improved using this method.

CHAPTER 4

RESULTS

In this chapter we will present our results in both section, hardware security Trojan detection and PUF. First, we will present the hardware Trojan detection using CNTFET and GNRFET and second section will be discussing ring oscillator PUF using the previous two models CNTFET and GNRFET. In this section we will present the result for using CNTFET and GNRFET in ring oscillator PUF to measure inter and intra hamming distance and how it is better than traditional Mosfet.

4.1 Ring Oscillator PUF with CNTFET and GNRFET

4.1.1 Intra Hamming

Voltage	CNTFET	GNRFET	Mosfet%
0.825	0.025	0.16	0.091
0.8125	0.023	0.04	0.095
0.8	0.017	0.06	0.1
0.7875	0.011	0.09	0.1
0.775	0	0	0.10

Table 8 Intra Hamming Distance (Voltages Varies)

Temperature	CNTFET	GNRFET	Mosfet%
25	0	0	0.57
50	0.005	0.015	0.70
75	0.005	0.046	0.87
100	0.005	0.060	0.91
125	0.007	0.082	0.96

Table 9 Intra Hamming Distance (Temp. Varies)

In the next table, it shows the inter hamming distance between the three models and it shows that CNTFET and GNRFET their results are near to the ideal case(50%).

4.1.2 Inter Hamming

CNTFET	GNRFET	Mosfet (Previous)
0.49	0.49	0.46

Table 10 Inter Hamming Distance

The previous results was implemented for 3-stage ring oscillator. I have also ran the simulation for 7 and 11 stages. The same results for inter hamming distance has been noticed, however, for intra hamming distance, there is a slightly different in the output as shown in table 11 and 12 but still has a good reliability under temp. and voltage variations.

Voltage	CNTFET (7-stages)	CNTFET (11-stages)	GNRFET (7-stages)	GNRFET (11-stages)
0.825	0.021	0.01	0.11	0.01
0.8125	0.019	0.012	0.015	0.01
0.8	0.012	0.01	0.02	0.011
0.7875	0.01	0.01	0.02	0.11
0.775	0	0	0	0

Table 11. Intra Hamming Distance (Voltages Varies) 7&11-stages RO

Temperature	CNTFET (7-stages)	CNTFET (11-stages)	GNRFET (7-stages)	GNRFET (11-stages)
25	0	0	0	0
50	0.002	0.001	0.012	0.011
75	0.002	0.001	0.023	0.012
100	0.001	0.001	0.041	0.011
125	0.003	0.002	0.062	0.02

Table 12. Intra Hamming Distance (Temp. Varies) 7&11-stages RO

We have also checked the flipping bits and frequency degradation from two selected ring oscillator from the two mux's, as we can notice in fig. 29 that there is no any crossover between the two ring oscillator which means it has a good reliability.

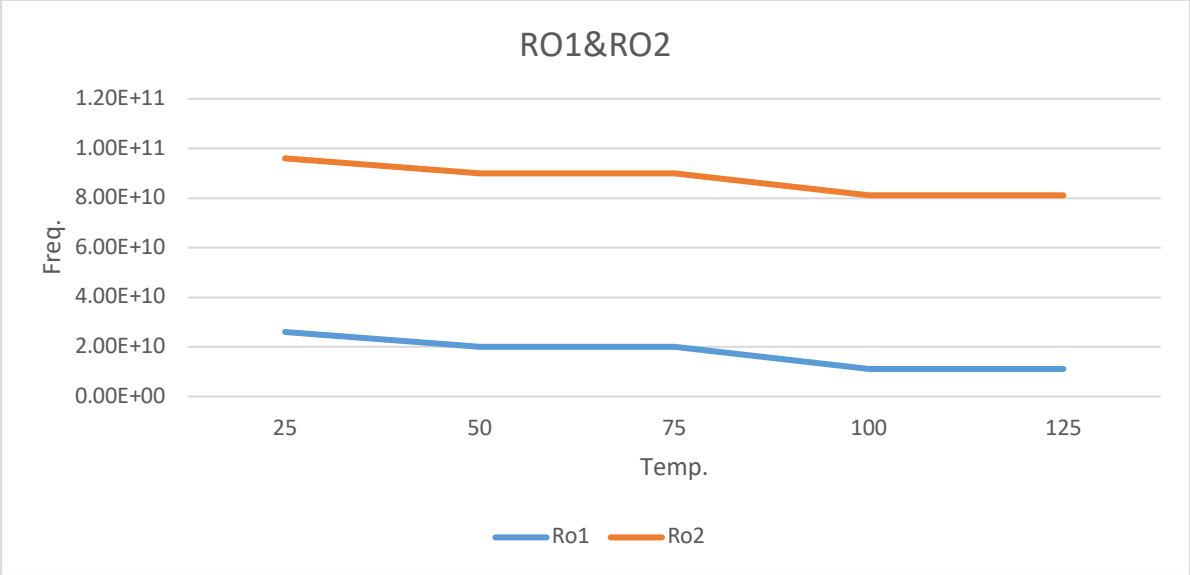


Fig.29 Freq. Degradation between two RO

In this section, we implemented Ro-Puf in Spectre cadence using three different models carbon nanotube, graphene nanoribbons, and CMOS models. We calculated Intra and Inter hamming distance to measure the reliability and uniqueness of the implemented puf. Carbon nanotube model has been used from Stanford university and graphene nanoribbons model from Illinois University. For conventional CMOS model, BSIM model 16nm has been used from PTM website. For testing the reliability of the three models in the RO-puf design, we measured the intra- hamming distance; CNT has the lead rather than GNR and CMOS. It's almost zero, which has the same output at different voltage and temperature values. GNR takes the second place after CNT in reliability. For inter hamming distance measurement, we have used 125 instance for RO-PUF for each model. CNT and GNR are the same value, which is 48%, which is near the ideal case for intra hamming distance

(50%). For CMOS model, we have provided different inverter stage, starting by 3 stages like CNT and GNR, following by 11 and 21 stages to show that CNT and GNR models works perfect by just 3 stages of inverter without any need to increase the stages number. For voltages variations, we used the nominal voltage values for the three models 0.8v and we varied it by 0.0125 as a step. Using CNT and GNR in puf implementation are promising as a good candidate for enhancing the performance of PUF and better result than traditional CMOS. We used for CMOS 16nm channel length at 0.7v nominal voltage, and 125 instances using montecarlo simulation generated with 10% inter-die, 10% intra-die, and 3 sigma variations for L (channel length of transistor), Vth, and Tox (gate oxide thickness). We have implemented 512 RO-puf as a response bit for the three models. For CNT, we have introduced process variation using advantages of varying the number of nanotubes in the device. We varied the nanotubes between 1 to 20 using Gaussian distribution. For GNR, we changed the nanoribbons number between 1 to 20 according to model specification for getting a sufficient band gap at specific values between 1 to 20. After comparing all models, CNT and GNR seems to have the lead for the upcoming PUF implementation than CMOS with lower number of inverter stages and at low voltage values.

4.2 Hardware Trojan Analysis in IC's Build with CNTFET/GNRFET

We have established a basic circuits using the traditional CMOS model, CNT model, and Graphene model using cadence simulator. We used the three models at different channel length and different nominal voltage to test the models variation. We calculated the static and dynamic power for each circuit. Also we implemented these circuit with and without Trojan to test all the possibilities.

4.2.1 Hardware Trojan Sensitivity

Static Power(Sensitivity)

Circuits	CNTFET/ No Trojan	CNTFET Trojan	Sensitivity	Sensitivity%
C17	0.29n	0.64n	0.35n	120.69
C432	53.699 µ	53.6993 µ	0.0003 µ	0.0006
C499	27.4008n	27.7462n	0.34n	1.26
C880	25.3442n	25.6878n	0.34n	1.36
C1355	30.8903n	31.2339n	0.34n	1.11

Table 13 Static Power CNTFET 32nm

Circuits	CMOS No Trojan	CMOS Trojan	Sensitivity	Sensitivity%
C17	30n	100n	70n	233.33
C432	132.315 µ	132.38 µ	0.06 µ	0.05
C499	5.31415 µ	5.38532 µ	0.07 µ	1.34
C880	4.07137 µ	4.13657 µ	0.06 µ	1.60
C1355	4.41295 µ	4.47813 µ	0.06 µ	1.47

Table 14 Static Power MOSFET 32nm

Circuits	CMOS No Trojan	CMOS Trojan	Sensitivity	Sensitivity%
C17	75.6321n	228.832n	153.2n	202.56
C432	87.2951 µ	87.4483 µ	0.15µ	0.17
C499	13.1812 µ	13.3558 µ	0.17µ	1.32
C880	10.1016 µ	10.2548 µ	0.15µ	1.51
C1355	9.53886 µ	9.69208 µ	0.15µ	1.61

Table 15 Static Power CMOS16nm

Circuits	GNRFET/ No Trojan	GNRFET Trojan	Sensitivity	Sensitivity%
C17	5.02828n	10.9935n	5.96n	118.63
C432	115.397 µ	115.403 µ	0.006µ	0.0005
C499	0.491183 µ	0.497583 µ	0.006µ	1.30
C880	0.429998 µ	0.435963 µ	0.006µ	1.38
C1355	0.528708 µ	0.534673 µ	0.006µ	1.12

Table 16 Static Power GNRFET 16nm

Dynamic Power

Circuit	CMOS No Trojan	CMOS Trojan	Sensitivity	Sensitivity %
C17	230n	580n	350n	152.17

Table 17 Dynamic Power CMOS 32nm

Circuit	CNTFET No Trojan	CNTFET Trojan	Sensitivity	Sensitivity %
C17	110n	130n	20n	18.18

Table 18 Dynamic Power CNTFET 32nm

Circuit	CMOS No Trojan	CMOS Trojan	Sensitivity	Sensitivity %
C17	0.2060 µ	0.470394 µ	0.26 µ	128.35

Table 19. Dynamic Power CMOS 16nm

Circuit	GNRFET No Trojan	GNRFET Trojan	Sensitivity	Sensitivity %
C17	83.8012n	48.0732n	35.72n	42.63

Table 20 Dynamic Power GNRFET 16nm

4.3 Hardware Trojan Detection Using Sleep Transistor build with CNTFET and GNRFET

In this section, it represents the results of the sleep transistor method which depends on power dissipation calculation. We implemented ALU 32 bits using the three different models includes the MOSFET model. Our results shows that carbon based material are much better that silicon transistor.

	8 Sleep Transistors		16 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	1.861E-07	2.39E-07	3.897E-08	6.070E-08
TCR (%)	28.42		56.04	

Table 21. TCR with 8 and 16 sleep transistor using CNTFET

	8 Sleep Transistors		16 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	1.651E-07	2.15E-07	2.787E-08	4.160E-08
TCR (%)	30.30		49.6	

Table 22. TCR with 8 and 16 sleep transistor using GNRFET

	8 Sleep Transistors		16 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	2.08E-07	2.28E-07	8.897E-08	1.070E-07
TCR (%)	9.61		20.24	

Table 23. TCR with 8 and 16 sleep transistor using MOSFET

	32 Sleep Transistors		64 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	4.178E-8	6.874E-8	4.676E-8	8.998E-8
TCR (%)	64.84		92.37	

Table 24. TCR with 32 and 64 sleep transistor using CNTFET

	32 Sleep Transistors		64 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	3.167E-8	4.862E-8	3.575E-8	6.889E-8
TCR (%)	53.52		92.69	

Table 25. TCR with 32 and 64 sleep transistor using GNRFET

	32 Sleep Transistors		64 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	4.699E-08	6.508E-08	2.531E-08	4.343E-08
TCR (%)	38.50		71.64	

Table 26. TCR with 32 and 64 sleep transistor using MOSFET

I have done the same ALU 32 bits circuits for the different sleep transistors after introducing the same proses variation to CNTFET's and GNRFET's model.

	8 Sleep Transistors		16 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	2.511E-07	3.27E-07	4.576E-08	7.050E-08
TCR (%)	30.22		54.06	

Table 27. TCR with 8 and 16 sleep transistor using CNTFET under process variation

	32 Sleep Transistors		64 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	5.157E-8	8.243E-8	5.232E-8	9.897E-8
TCR (%)	59.8		89.16	

Table 28. TCR with 32 and 64 sleep transistor using CNTFET under process variation

	8 Sleep Transistors		16 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	2.211E-07	3.11E-07	1.386E-08	2.250E-08
TCR (%)	40.66		62.33	

Table 29. TCR with 8 and 16 sleep transistor using GNRFET under process variation

	32 Sleep Transistors		64 Sleep Transistors	
	Without Trojan	*With Trojan*	*Without Trojan*	*With Trojan*
Power Dissipation (W)	2.153E-8	3.512E-8	2.385E-8	4.669E-8
TCR (%)	63.12		95.76	

Table 30. TCR with 32 and 64 sleep transistor using GNRFET under process variation

A high value of TCR is helping to improve the detecting results as shown in the previous tables. Leakage power of golden model, leakage power of Trojans, and number of sleep transistors contribute to Trojan-Circuit Ratio. The data shows that TCR is approximately doubles when the number of Sleep Transistor doubles. The measurement of static power-

based side-channel analysis based on power gating method is more powerful in hardware Trojan detection. It improved with increasing the TCR percentage, which is directly proportional to the number of sleep transistors. These kind of measurements are very powerful in detecting a tiny-size Trojan on a large-scale circuit and it is also can detect trojan in different circuit locations.

CHAPTER 5

CONCLUSION

In conclusion, we have implemented ring oscillator PUF using carbon based materials (CNTFET/GNRFET), and the results are near to the ideal case. For hardware trojan detection, first, we have done analysis by measuring sensitivity in terms of static and dynamic power. We have used also sleep transistor method in hardware trojan detection and the results shows that implementing circuits with CNTFET and GNRFET are very promising in this method.

5.1 Future Work

We are planning in Implementing PUF with different process variations, as well as hardware trojan analysis using different process variations under non ideal case.

REFERENCE

[1] M. Tehranipoor and C. Wang (eds.), Introduction to Hardware Security and Trust, DOI 10.1007/978-1-4419-8080-9 7, © Springer Science+Business Media, LLC 2012.

[2] Jeyavijayan Rajendran, Ramesh Karri, James B. Wendt, Member, Miodrag Potkonjak, Member, Nathan McDonald, Garrett S. Rose and Bryant Wysocki "Nanoelectronic Solutions for Hardware Security".

[3] Da Xia, Yue-Fei Zhu, "A Research on Detection Algorithm of Failure-Type Hardware Trojan", Multimedia Information Networking and Security (MINES) 2012 Fourth International Conference on, pp. 918-921, 2012.

[4] Tehranipoor, Mohammad, and Farinaz Koushanfar. "A survey of hardware trojan taxonomy and detection." IEEE Design & Test of Computers 27.1 (2010).

[5] Yuan Cao, Chip-Hong Chang, Shoushun Chen, "A Cluster-Based Distributed Active Current Sensing Circuit for Hardware Trojan Detection", Information Forensics and Security IEEE Transactions on, vol. 9, pp. 2220-2231, 2014, ISSN 1556-6013.

[6] Guin, Ujjwal, et al. "Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain." Proceedings of the IEEE 102.8 (2014): 1207-1228.

APA.

[7] Church, Sara E., et al. "Counterfeit deterrence and digital imaging technology." Electronic Imaging. International Society for Optics and Photonics, 2000.

[8] Grand, Joe, and Grand Idea Studio. "Introduction to embedded security." Black Hat USA, Las Vegas, NV (July 2004) (2004).

[9] Guin, Ujjwal, Daniel DiMase, and Mohammad Tehranipoor. "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead." Journal of Electronic Testing 30.1 (2014): 9-23.

[10] Smalley, Richard E. Carbon nanotubes: synthesis, structure, properties, and applications. Eds. Mildred S. Dresselhaus, Gene Dresselhaus, and Phaedon Avouris. Vol. 80. Springer Science & Business Media, 2003.

[11] Dresselhaus, Mildred, and Phaedon Avouris. "Introduction to carbon materials research." Carbon nanotubes (2001): 1-9.

[12] Gojny, F. H., et al. "Carbon nanotube-reinforced epoxy-composites: enhanced stiffness and fracture toughness at low nanotube content." Composites science and technology 64.15 (2004): 2363-2371.

[13] Thostenson, Erik T., Zhifeng Ren, and Tsu-Wei Chou. "Advances in the science and technology of carbon nanotubes and their composites: a review." Composites science and technology 61.13 (2001): 1899-1912.

[14] Wong, H-S. Philip, et al. "Carbon nanotube electronics-materials, devices, circuits, design, modeling, and performance projection." Electron Devices Meeting (IEDM), 2011 IEEE International. IEEE, 2011.

[15] Zhang, Jie, et al. "Carbon nanotube correlation: promising opportunity for CNTFET circuit yield enhancement." Design Automation Conference (DAC), 2010 47th ACM/IEEE. IEEE, 2010.

[16] Choi, Hyoung Joon, et al. "Defects, quasibound states, and quantum conductance in metallic carbon nanotubes." Physical Review Letters 84.13 (2000): 2917.

[17] Kleiner, Alex, and Sebastian Eggert. "Band gaps of primary metallic carbon nanotubes." Physical Review B 63.7 (2001): 073408.

[18] Barone, Verónica, Oded Hod, and Gustavo E. Scuseria. "Electronic structure and stability of semiconducting graphene nanoribbons." Nano letters 6.12 (2006): 2748-2754.

[19] Yang, Xiaoyin, et al. "Two-dimensional graphene nanoribbons." Journal of the American Chemical Society 130.13 (2008): 4216-4217.

[20] OuYang, Fangping, et al. "Chemical functionalization of graphene nanoribbons by carboxyl groups on stone-wales defects." The Journal of Physical Chemistry C 112.31 (2008): 12003-12007.

[21] Dutta, Sudipta, and Swapan K. Pati. "Novel properties of graphene nanoribbons: a review." Journal of Materials Chemistry 20.38 (2010): 8207-8223.

[22] Wu, Zhong-Shuai, et al. "Efficient synthesis of graphene nanoribbons sonochemically cut from graphene sheets." Nano Research 3.1 (2010): 16-22.

[23] Upadhyay, Devendra, and Sudhanshu Choudhary. "Understanding the impact of graphene sheet tailoring on the conductance of GNRFETs." Bulletin of Materials Science 38.7 (2015): 1705-1709.

[24] Fiori, Gianluca, and Giuseppe Iannaccone. "Simulation of graphene nanoribbon field-effect transistors." IEEE Electron Device Letters 28.8 (2007): 760-762.

[25] Chen, Ying-Yu, et al. "A SPICE-compatible model of graphene nano-ribbon field-effect transistors enabling circuit-level delay and power analysis under process

variation." Proceedings of the Conference on Design, Automation and Test in Europe. EDA Consortium, 2013.

[26] Iannaccone, G., et al. "Perspectives of graphene nanoelectronics: probing technological options with modeling." Electron Devices Meeting (IEDM), 2009 IEEE International. IEEE, 2009.

[27] Chin, Huei Chaeng, et al. "Enhanced device and circuit-level performance benchmarking of graphene nanoribbon field-effect transistor against a Nano-MOSFET with interconnects." Journal of Nanomaterials 2014 (2014).

[28] Bi, Yu, et al. "Leveraging emerging technology for hardware security-case study on silicon nanowire fets and graphene symfets." Test Symposium (ATS), 2014 IEEE 23rd Asian. IEEE, 2014.

[29] McGrail, B. P., P. F. Martin, and C. W. Lindenmeier. "Accelerated testing of waste forms using a novel pressurized unsaturated flow (PUF) method." MRS Proceedings. Vol. 465. Cambridge University Press, 1996.

[30] Paral, Zdenek, and Srinivas Devadas. "Reliable and efficient PUF-based key generation using pattern matching." Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on. IEEE, 2011.

[31] Maiti, Abhranil, and Patrick Schaumont. "Improved ring oscillator PUF: An FPGA-friendly secure primitive." Journal of cryptology 24.2 (2011): 375-397.

[32] Konigsmark, ST Choden, et al. "Cnpuf: A carbon nanotube-based physically unclonable function for secure low-energy hardware design." Design Automation Conference (ASP-DAC), 2014 19th Asia and South Pacific. IEEE, 2014.

[33] ‘A Ring Oscillator-Based PUF with Enhanced Challenge–Response Pairs’ Canadian Journal of Electrical and Computer Engineering, VOL. 39, NO. 2, SPRING 2016.

[34] ‘Carbon Nanotube Circuits in the Presence of Carbon Nanotube Density Variations’ Technical Report (part of this work was submitted to DAC 2009) – updated 2/14/2009.

[35] ‘Variation-aware design of carbon nanotube digital VLSI circuits’ A dissertation submitted to the department of electrical engineering and the committee on graduate studies of Stanford university.

[36] ‘Stanford University Carbon Nanotube Field Effect Transistors (CNTFET) HSPICE Model’ A Quick User Guide.

[37] ‘Device modeling and circuit performance evaluation for Nanoscale devices: silicon technology beyond 45 nm node and carbon nanotube filed effect transistor’ A dissertation submitted to the department of electrical engineering and the committee on graduate studies of Stanford university.

[38] ‘carbon nanotubes electronics’ A dissertation submitted to the department of electrical engineering and the committee on graduate studies of Stanford university.

[39] ‘Highly Accurate SPICE-Compatible Modeling for Single- and Double-Gate GNRFETs with Studies on Technology Scaling’ Morteza Gholipour, Ying-Yu Chen, Amit Sangai, and Deming Chen Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL.

[40] ‘A SPICE-Compatible Model of Graphene Nano-Ribbon Field-Effect Transistors Enabling Circuit-Level Delay and Power Analysis Under Process Variation’ Ying-Yu Chen1, Artem Rogachev, Amit Sangai, Giuseppe Iannaccone, Gianluca Fiori and Deming

Chen Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL

[41] ‘Graphene Nano-Ribbon Field-Effect Transistor (GNRFET) HSPICE Model’ Ying-Yu Chen, Morteza Gholipour, Amit Sangai, Artem Rogachev, and Prof. Deming Chen. Electrical department, Illinois university.

[42] Zimu Guo, Xiaolin Xu , Md. Tauhidur Rahman , Mark M. Tehranipoor , Domenic Forte ‘An SRAM-Based Countermeasure Against IC Recycling’ IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 26, NO. 4, APRIL 2018

[43] Ujjwal Guin, Student Member IEEE, Ke Huang, Member IEEE, Daniel DiMase, John M. Carulli, Jr., Senior Member IEEE, Mohammad Tehranipoor, Senior Member IEEE, and Yiorgos Makris, Senior Member IEEE. ‘Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain’

[44] Shital, Saraju P, and Elias ‘ everything you want to know about PUFs’.

[45] Mohammad Tehranipoor, Farinaz Koushanfar ‘A Survey of Hardware Trojan Taxonomy and Detection ‘IEEE Design & Test of Computers January/Februray 2010.

[46] Rührmair, Ulrich, Heike Busch, and Stefan Katzenbeisser. "Strong PUFs: models, constructions, and security proofs." In Towards hardware-intrinsic security, pp. 79-96. Springer, Berlin, Heidelberg, 2010.

[47] Maiti, Abhranil, Vikash Gunreddy, and Patrick Schaumont. "A systematic method to evaluate and compare the performance of physical unclonable functions." In Embedded systems design with FPGAs, pp. 245-267. Springer, New York, NY, 2013.

[48] Rahman, MD Tauhidur, Fahim Rahman, Domenic Forte, and Mark Tehranipoor. "An aging-resistant RO-PUF for reliable key generation." IEEE Transactions on Emerging Topics in Computing 4, no. 3.

[49] Rahman, M. Tauhidur, Alison Hosey, Zimu Guo, Jackson Carroll, Domenic Forte, and Mark Tehranipoor. "Systematic correlation and cell neighborhood analysis of sram puf for robust and unique key generation." Journal of Hardware and Systems Security 1, no. 2.