Integrated Circuit Authentication based on electromagnetic signature

Mosabbah Mushir Ahmed

Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES

Spécialité : OPTIQUE ET RADIOFREQUENCES

Arrêté ministériel : 25 mai 2016

Présentée par

Mosabbah Mushir AHMED

Thèse dirigée par **Etienne PERRET**
et codirigée par **David HELY**, Maitre de Conférence, Communauté Université Grenoble Alpes
et **Maxime BERNIER**, Maître de Conférences, Université Savoie Mont Blanc (USMB)

préparée au sein du **Laboratoire Laboratoire de conception et d'intégration des systèmes**
dans **l'École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS)**

Authentification de puces électroniques par des approches RF et THz non intrusives

Integrated Circuit Authentication based on electromagnetic signature.

Thèse soutenue publiquement le **4 février 2019**,
devant le jury composé de :

Monsieur ETIENNE PERRET
MAITRE DE CONFERENCES, GRENOBLE INP, Directeur de thèse
Monsieur NUNO BORGES CARVALHO
PROFESSEUR, UNIVERSITE D'AVEIRO - PORTUGAL, Rapporteur
Monsieur BRUNO ROUZEYRE
PROFESSEUR, UNIVERSITE DE MONTPELLIER, Rapporteur
Monsieur DAVID HELY
PROFESSEUR ASSOCIE, GRENOBLE INP, Co-directeur de thèse
Monsieur WENCESLAS RAHAJANDRAIBE
PROFESSEUR, UNIVERSITE AIX-MARSEILLE, Président
Monsieur MAXIME BERNIER
PROFESSEUR ASSOCIE, UNIVERSITE SAVOIE-MONT-BLANC, Examinateur

Acknowledgement

Firstly, I would like to express my sincere gratitude to my thesis director Prof. Etienne Perret for providing me the opportunity to do my thesis in LCIS - INP Grenoble. I would like to gratefully thank Prof. Etienne Perret and my co-supervisor Prof. David Hely, of LCIS – INP Grenoble, Valence, for the continuous support of my PhD study and related research, for their patience, motivation, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisors and mentors for my PhD study.

I would also like to thank the rest of my thesis committee: Prof. Romain Siragusa and Prof. Nicolas Barbot of LCIS - INP Grenoble, Valence and Prof. Frederic Garet and Prof. Maxime Bernier, University of Savoie Mount Blanc, Chambery, for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

My special thanks to my office mates Zeshan and Kostas, for extending their amicable relation, support and for all the fun we have had in the last three years. I would like to thank my fellow lab-mates, Marco, Bony, Hatem, Thanos for their valuable support. I would like to extend special thanks to the administrative team of LCIS – Jennyfer Duberville, Carole Seyvet, Romain Doleux and Caroline Palisse for helping with all sorts of pile of administrative papers. My special thanks to M. Cedric Carlotti (IT administrator) for keeping my laptop and system running smoothly throughout my PhD period. Also I thank my friend Kashif Nawaz from UC Louvain, Belgium for discussing all the ideas related to the field of hardware security.

Last but not the least; I would like to thank my wife, for her patience and undue support with me, my parents and to my brothers for supporting me spiritually throughout writing this thesis and my life in general.

Abstract

The advent of nano-scale device or shrinking of integrated circuits (IC) has become a blessing for the human civilization. Nowadays it has become very much common to find piece of electronic devices in different applications and instruments of various sectors. ICs now are not only confined to computers and mobiles but they are integral part of our everyday life. They can be found in our kitchens (in microwaves, oven), in hospitals (instruments such as ECG, MRI etc.), banks, space, telecom, defense etc. It has of course made our lives easier. However everything comes with a price.

The change in economy due to the integration of electronics in different domains has put an extra pressure on companies and manufacturers to produce their product in tighter constraints in terms of cost and time. This has led to companies off shoring their manufacturing units to foundries beyond their direct control. Due to this advent of small and untrusted foundries have been on rise. The rise in various manufacturing units or foundries has given rise to the phenomenon of counterfeiting of electronic components especially ICs. For smaller foundries who do not meet all the specification, if they get hand to the design of the circuit layout, they can produce the IC similar to the one developed by original component manufacturers (OCMs) and sell them into market without consent of OCM and without performing standardized tests. Also, the malicious or untrusted foundries can copy and clone the netlist of devices and sell under the name of OCM. Various types of counterfeit ICs – recycled, remarked overproduced, out-of-spec/defective, cloned, forged documentation, and tampered – have made the supply chain vulnerable to various attacks. However, due to the lack of efficient detection and avoidance techniques, many more instances of counterfeit ICs evade detection than those that are actually detected. Over last few years the rise in the incidents of IC counterfeit has propelled the designer and researchers to develop various testing and standardization methods in place. However, many of these methods can be cumbersome and have huge implications and costs for their implementations. This can be discouraging for the users and OCMs to implement these methods in their product.

In this dissertation, we have worked on the implementation of methodology that can be used to generate fingerprints or signatures form the ICs which can be used for the purpose of their authentication. The method adopted in this work is based on the idea of exploiting the manufacturing induced process variations by implementing the electromagnetic (EM) waves. The manufacturing variability of various devices under test has been exploited through use of EM waves. The use of EM waves has been studied in detail along with the various implications of using and generating them in the IC. This dissertation uses two methodologies to utilize EM wave for the exploitation of the process variation effects. The exploited process variation effects have been subjected to mathematical treatments to quantify the response statistically.

The following tasks have been implemented in this work:

- State of the art study of IC counterfeiting and IC cloning (on both risk and mitigation techniques).
- Measurement set-up: Component choices, board measurement development.
- Circuit configuration to maximize the measurement sensitivity.
- Measurement campaigns using different approaches (RF based).
- Measurement Exploitation in order to extract authentication information from the measurement.

Together with the implementation of EM based approaches on new device, we have also worked on observing the effects of the aging on the devices under test and particularly on the authentication metrics themselves. For this we have setup measurement test benches and put the device under accelerated stress to induce the aging effects.

To validate our work, we have performed our measurements across various devices of same manufacturer and family. This work has focused on using two different semiconductor devices i.e. FPGA and microcontrollers. These are highly used devices and find their application in various domains. The statistical computation after mathematical treatment of responses, gives the error rate which determines the efficiency of the methodologies adopted.

Contents:

List of Figures :

List of Tables:

List of publications:

- Mosabbah Mushir Ahmed, D.Hely, R.Siragusa, E.Perret,N.Barbott,F.Garet, M.Bernier *"**Authentication of Microcontroller board using non-invasive EM emission technique**"* in 3rd International Verification and Security Workshop 2018 (IVSW'18), Costa Brava, Spain. DOI: 10.1109/IVSW.2018.8494883
- Mosabbah Mushir Ahmed, D.Hely, R.Siragusa, E.Perret,N.Barbott,F.Garet, M.Bernier *"**Towards a robust and efficient EM based authentication of FPGA against counterfeiting and recycling**"* in 19th CSI International Symposium on Computer Architecture & Digital Systems, Dec. 2017, IEEE CADS. **DOI:** 10.1109/CADS.2017.8310673
- Mosabbah Mushir Ahmed, D.Hely, R.Siragusa, E.Perret,N.Barbott,F.Garet, M.Bernier *"**Radiated Electromagnetic Emission for Integrated Circuit Authentication**"* in IEEE Microwave and Wireless Components Letters PP(99): 1028 - 1030, Sept 2017, DOI: 10.1109/LMWC.2017.2750078.
- Mosabbah Mushir Ahmed, D.Hely, R.Siragusa, E.Perret,N.Barbott,F.Garet, M.Bernier "***Authentication of IC based on Electromagnetic Signature***" TRUDEVICE - 6th Conference on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE 2016), Barcelona, 14-16 November, 2016. URL: http://hdl.handle.net/2117/99321

1. Introduction

IC or Integrated circuits find their usage in multiple applications across different domains and sectors. They are used in daily home appliances, smartphones, laptops to more sophisticated systems like banking, military and space exploration etc. Given their usability across very domains, it is imperative to safeguard their integrity against any kind of eternal or internal threats. Hence in a nutshell it can be said that IC are root for a trusted hardware system.

However, in recent times, there have been many incidents related to counterfeit of ICs. A counterfeited IC can pose permanent or temporary damage to the life of a system as well as compromises the integrity of information of the system[1][2]. An IC failure due to a counterfeit part is very serious. When the counterfeit IC fails, it can inflict serious injury, or at a minimum interrupt or delay a mission. It ranks with counterfeit drugs that can cause an individual to be over- or under medicated. Owing to the fact that ICs are used in our day-to-day life - both directly and indirectly - counterfeit ICs also pose major threats to the health, safety, and security of the population at large. For example, the failure of a pacemaker due to a counterfeit component can potentially take someone's life. A pilot can lose control of his airplane if the IC or electronic components used in that is fake or counterfeited. Hence it not only causes the reliability issues or failure of the system but also inflicts or has the potential to damage the human lives [1].

In addition to the impact on public safety and security, counterfeit ICs could also cause significant damage to the economy. A semiconductor company spends a huge amount of money in developing and marketing a new product, whereas a counterfeiter requires minimal effort to destroy the authenticity of the product. Hence when a fake component with marking of original component manufacturers (OCMs) fails, it tarnishes the reputation and credibility of the OCM. According to studies conducted in [2], around $100 bn. of revenue is lost by legitimate electronics and semiconductor industry due to the incidents of counterfeit. Indeed Hi-Tech industries are significantly affected by this problem. Based on a 2008 report by the International Chamber of Commerce, it was estimated that the cost of counterfeiting and piracy for G20 nations was as much as US$775 billion every year and will grow to $1.7 trillion in 2015 [2][3].

Over the past several years a specialized service of testing has been created for detecting and avoiding counterfeit components. The components must be authenticated by these tests before being placed in systems. The classical techniques to detect counterfeit that involve physical and electrical inspection can

be very time consuming and also involves the risk of damaging the IC or components under test, permanently or temporarily [3][4] . Second method is based on traceability approach to find identity of devices or ICs by using process variation or PV. As discussed, using PV approach, physical unclonable function (PUF) is dominantly used. It exploits the inherent variability of an IC, caused due to manufacturing variations of IC itself. Each PUF contains pair of challenge and response. For each challenge sent to an IC there is a unique response to that challenge [5][6]. Apart from the IC authentication, PUFs are also used for the purpose of secret key generation for cryptographic applications. Bottleneck of the PUF approach is that it requires dedicated on-chip circuitry which may be complex to process and implement. PUFs also have large database of challenge pair response. Apart from the usage of classical techniques and PUF based solutions, research and studies have been going on to develop new approaches that would be effective against counterfeit problems.

With the miniaturization of IC, there are various constraints that arise for the designing any new circuit element in the IC. Area overhead and ease of implementation is major issues that are topic of concerns on IC made on smaller technological nodes. Hence, in terms of adding any extra dedicated circuitry in the IC for the purpose of authentication can be discouraging in terms of economic viability for any OCM. Therefore, it is very important to find for a solution which takes into account the area constraints of IC while implementing solutions to address the issue of counterfeiting. Second important aspect is that the implemented solution should be safe and must not damage the IC in long or short terms.

1.1 Motivation

The motivating factor to perform this study is to introduce and elaborate techniques that can efficiently create a signature of an IC without using any invasive techniques. This will aid greatly in mitigating the problem of area utilization in miniaturized IC. Also, this is a simple scheme that can be effectively used in resource constraint devices. The work in this dissertation is mainly motivated by the following concerns:

1. Counterfeit avoidance and detection requires the utilization of various physical and electrical design factors of the IC. Hence as also stated above in brief, these factors often lead to higher power consumption or higher area occupancy. In particular higher area occupancy utilizes higher Silicon area which in turn increases the cost of the IC. For example, if the instance of physical unclonable functions (PUFs) is taken into account, it is clear from their design approach that this

technique utilizes a considerable amount of IC area. PUFs require a dedicated post-processing unit which is area as well power hogging [5]. This can be demotivating for an OCM to include any extra circuit in its IC for purpose of authentication because of tight budget and time to market constraints Secondly, this can also cost-ineffective for the consumer, who can then be falsely allured in buying the recycled or remarked IC .

2. Subsequently, it is also observed from the above discussion in section 1, that classical techniques like physical inspection use high powered input sources like X-rays, which can damage the IC under test permanent or temporarily [3]. Secondly, these techniques are slow and time consuming for the end user to deploy. Hence, it can be daunting task for the user to employ such a technique which can damage his component and also consume huge amount of time. The technique in this category of electrical inspection is also very time consuming and highly inefficient in terms of detecting the counterfeit [4].

3. One of the major challenges in counterfeit industry is of the recycled IC. Among various IC counterfeit techniques, recycled IC takes around 80% of whole share. Recycled ICs are old ICs sold as new [7]. Hence it is becoming important to understand the difference aspects of old ICs, their characteristics and difference with the new ones. The various techniques adopted have been towards finding and implementing aging based sensors, but they come up with solution to detect old IC. An IC can become aged or old while being in the field. So any authentication process done after the IC has been in the field can discard that IC by putting it in category of recycled IC and in this way even an authentic IC can be discarded.

4. Extending point 3, with the passage of time, the signatures or fingerprints of IC can vary owing to aging and reliability effects on transistors. An IC is always affected by process, temperature and voltage variation when it is employed in the application. Therefore, there is an issue regarding the reliability and aging effects on the principle functions of IC and how it degrades over its usage over the time. An old IC does not mean a fake IC i.e. if a vendor performs an authentication after a time gap of ‘t’ (period in which IC has been used by genuine vendor), it can show deviation in the fingerprints. Hence, it is imperative to have a solution that is gives a fingerprint of IC resistant to aging effects. This is an important aspect that this covered in this dissertation.

In this dissertation we have made an optimum attempt to give answer for all the concerns highlighted above. The effort has been made to enhance, implement and utilize a scheme for authentication of IC

using non-invasive approaches. The approaches should be efficient in terms of area and implementation, it should not pose any risk to damage the IC and it should be time efficient and cost effective. Subsequently, it is also an important aspect to extend the implemented technique to cater the aging related problems of the IC. This is to prevent the authentic IC from being discarded due to variation in their fingerprint over time. Hence, in a summary this dissertation answers to the following existing problems in the field of IC authentication:

I. Area overhead of IC utilized in present authentication techniques.

II. High cost requirement with the utilization of present techniques.

III. Implementation of authentication techniques in resource constraint devices.

IV. Effects of aging on the obtained fingerprints of IC – authentication valid for lifetime of IC.

To answer these concerns, in the next subsection we have highlighted the contribution done in this thesis work.

1.2 Contributions of this work

In view of the problems discussed regarding the counterfeit ICs, and effects they have on system's reliability and economy; we have made an effort to implement a methodology that is efficient and easy to deploy and handle. It is also discussed in brief in the previous section that there are many studies and research and going to tackle the problem of counterfeiting. This dissertation highlights alternate methods that can be used in order to mitigate counterfeiting of ICs and create fingerprints or signatures of each IC by exploiting their manufacturing process variation or PV.

This dissertation is broadly compiled in the following order.

I. Understanding the effects, features and techniques of counterfeiting of IC.

II. Understanding and analysis manufacturing based process variations.

III. Implement EM based techniques to utilize the PV effects to generate unique response from each IC. Perform the measurement steps suitable and required to get a prudent effects of process variations.

IV. Use statistical techniques to have a statistical and mathematical analysis on the obtained results to attribute each IC with a fingerprints and signatures.

V. Perform aging and reliability analysis and extend metrics that can mitigate the effects of aging of IC on its fingerprints and signatures.

In the following sub-section, we have given a brief introduction to the different adopted authentication metrics performed in this study.

The terms ***fingerprints*** and ***signatures*** have been used interchangeably in this manuscript. Mostly with signature, we tend to point out towards analog signature or response and with fingerprints towards a binary response. However, both of these terms mean same – a unique identifier for the devices under test.

1.2.1 Alternate and proposed authentication metric – Electromagnetic (EM) based

As the bandwidth of today's integrated circuits increases, it is important to characterize their performance over wide frequency ranges. Traditional low frequency parameters—such as resistance, capacitance, and gain - can be frequency dependent, and thus may not fully describe the performance of the IC at the desired frequency. In addition, it may not be possible to characterize every parameter of a complex IC over frequency, so system-level characterization may provide better data [8]. In this work we primarily deal with the study of perturbations of EM (radio-frequency (RF) waves) high frequency wave due to the different electrical and physical features of ICs. The idea is to exploit the process variation using EM / RF based approach. The process variation - No two ICs even built on the mask can have same physical characteristics [9]. The alternate authentication metrics that have discussed in this dissertation is based on exploitation of PV effects through the EM and RF based approaches.

The implemented EM based approaches have been characterized as non-intrusive, that does not require dedicated sensor or marker, is easy to implement and efficient in terms of cost. This dissertation contributes through the two EM based methods:

I. **R**adiated **EM** based **T**echnique or we call it **REMT** in this dissertation.

II. **G**uided **EM** based **T**echnique or **GEMT**.

The detailed preview, analysis and description have been laid out in the succeeding chapters. In our study we have utilized field programmable gate arrays (FPGAs) as our IC under test for all the EM based techniques.

To implement an authentication approach using non-invasive EM based techniques, a detailed analysis and study on different methodologies that is utilized to create fingerprints or signatures for IC for its authentication purposes has been performed. This thesis also contributes to propose the methods to have a stable and robust authentication schemes. The aging or reliability issues of IC are studied in the realm and domain of the authentication mostly.

The aging related issue is an important aspect that an IC has to undergo when it is used in the field for a period of time. With the usage of IC over a period of time, there are changes or degradation in its electrical properties due to electrical and physical changes it has to undergo. For instance, the aging effects result in degradation of switching speed, threshold voltage etc. of a complementary metal oxide semiconductor (CMOS) based transistor. A detailed understanding of it is given in chapter 4. Hence, it is important to understand how the authentication technique can get affected when an IC undergoes aging effects.

A basic high level pictorial description of using EM based technique for the purpose of authentication of IC has been pictorially illustrated in Fig. 1.1. From Fig. 1.1(a), we can observe the steps required for authenticating an IC which has never been used in any application (new IC). Likewise in Fig. 1.1(b), for a used or aged IC the same steps of authentication (EM based) are proposed. The fingerprints or signatures obtained from Fig. 1.1(a) and (b) are compared. This comparison is done to check for the robustness and stability of fingerprints or signatures.

The points that Fig. 1.1 describes is that along with the steps implemented for the EM based authentication for the new IC, it is also imperative to take into the effects of aging of IC when similar measurement technique is applied on the used or old ICs. As IC gets old there signatures can vary and hence they can be wrongly discarded as being un-authentic or fake. Therefore, in this study we have taken the effects of aging into account and implemented approach that has been able to generate robust and stable fingerprints of IC.

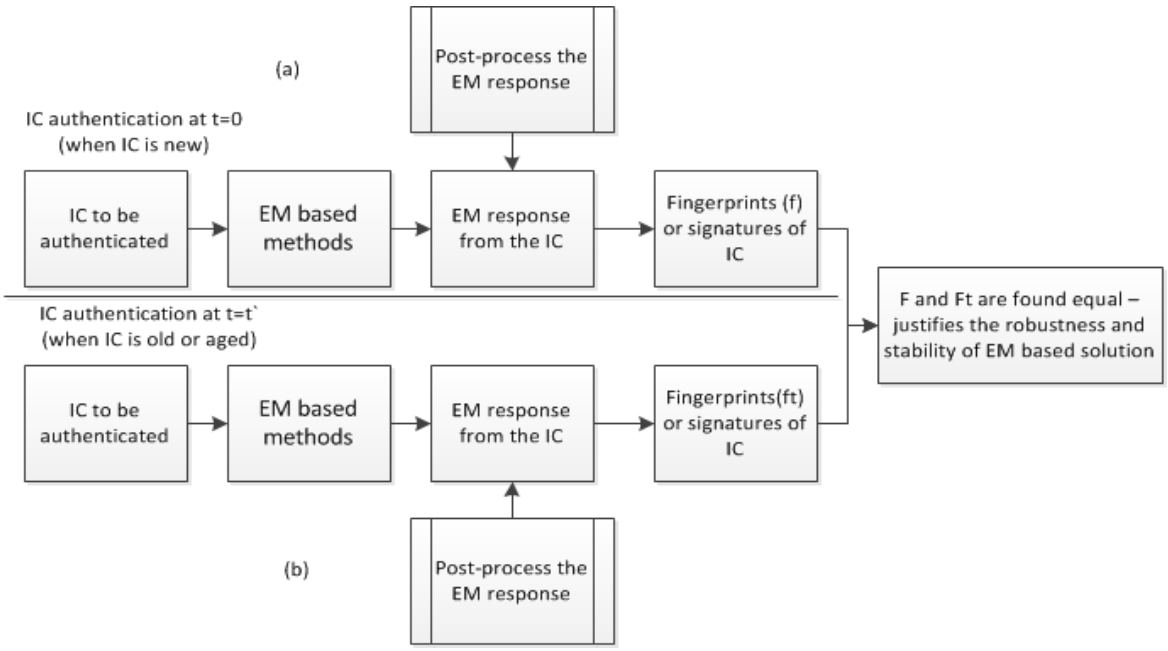


Fig.1.1: A high level illustration of EM based technique for authentication highlighting different steps used. (a) For new IC when it is not used for any application. (b) For an aged or used IC.

With the proposed solution for taking aging effects in to account we have shown in chapter 4, that the fingerprints of IC can remain constant over period of time hence mitigating aging or reliability based effects.

1.2.2 Characteristics of EM based solution

Among other aspects of IC and its authentication nuances, this work primarily focusses on exploiting process variation effects of IC by means of electromagnetic (EM) waves. In later part of the manuscript aging effects of fingerprints or signatures have been investigated and solution is proposed to mitigate the aging effects on fingerprints / signature, as also highlighted in Fig. 1.1(b). The approaches to implement authentication techniques discussed in this study have adhered to the following main characteristics:

I. Exploits manufacturing based process variation or PV of IC. The implemented methodology should be efficient to be able to exploit the intrinsic manufacturing induced PV effects of IC. This is an important aspect in order to create a fingerprint of the IC which is unique to it.

II. Non-intrusive in nature i.e. no or minimal dedicated circuit requirements. It is the major requirement and contribution of this work, the proposed solutions makes sure that the any marker

involved in the working to create the signature of IC is as small or lightweight as possible. The idea to have marker is to exploit the physical and electrical nature of the PV of each IC under test, which finally creates the fingerprint of the IC.

III. Does not require extra dedicated or auxiliary circuit. The approaches used should not require any external circuit or any internal dedicated circuits which would assist in performing measurement or creating fingerprints / signatures. All the fingerprints /signatures creation should be function of only the manufacturing induced intrinsic PV effects.

IV. The methodologies should be robust and stable under different operating conditions. That means, the obtained signatures of IC should be same under different measurements conditions. It should be independent of different PVT effects and environmental noise.

The last part of this thesis work contributes towards utilization of FPGA in RF application. While adopting EM or radio-frequency (RF) based methods for the IC (FPGAs in our study) authentication purpose, we have experienced RF capabilities of FPGA and hence we have decided to leverage them to propose new RF capabilities with classical FPGAs.

1.2.3 FPGA in RF applications

The last part of this dissertation extends new techniques that focusses on utilization of the FPGA as RF devices like passive switches, isolator etc. This part of the work highlights the ease of re-programmability that FPGA brings. Advantages of this proposed work are: *(a)* reprogram same FPGA and make it work as different RF devices; *(b)* efficiently create a prototype of the design for purpose of verification and accurate results. This part of work is also inspired by the fact that in implementing the RF guided wave authentication method, we required aid of external instruments like network analyzer and other RF components. Hence in order to mitigate the extra cost and inconvenience that can come by use of additional components, we have focused one part of our work on deploying FPGA to work in RF range of frequency as RF devices without use of any external clock or analog signal. Furthermore this is feature of FPGA is extended to implement software defined radio (SDR) feature in the FPGA. As an example of this application we have implemented a RF wireless communication between two FPGA boards using OOK based modulation technique.

1.3 Organization of thesis

This thesis is divided into 6 chapters. The motivation, background, and contributions are provided in

Chapter 2 of this thesis focuses on the detailed study, analysis and understanding of the counterfeiting of electronic components, their effects on the reliability and economy of the system. In the same chapter we have discussed about the different counterfeit techniques that are adopted. Furthermore this chapter will talk about the different concepts and techniques that are applied in order to detect and avoid counterfeiting of ICs or electronics components. Lastly we will try to highlight the problems that electronic industry faces in deploying the currently present counterfeit detection and avoidance techniques.

Chapter 3 describes in detail about the theoretical and practical aspects of REMT or radiated EM based method for the authentication of IC. This chapter focuses on understanding of EM radiation from ICs or FPGAs in this study. Effects of process variation of ICs and how it can be exploited by the use of EM radiation methodology. This chapter also focuses on the detailed investigation of variability aware design and use of inherent physical features to exploit the PV effects that can be used by radiated EM wave to create a fingerprint for each IC user test. The use of post-processing steps along with the detail of the same has also been provided. This chapter focuses on using and measurements steps on two semiconductor devices: FPGA and Microcontrollers. The statistical results which justify the efficiency of the methodology have been discussed in details. The utility of this approach against various counterfeit techniques have also been discussed in the inference and conclusion part of this chapter.

Chapter 4 is the extension of chapter 3. In this chapter we have focused on investigating the effects of the aging on the EM based authentication technique on the transistors and CMOS devices. The normal aging related mechanisms NBTI and HCI have been studied in brief. The measurement setup for the accelerated aging is detailed out. This chapter also summarizes the use of intra-die variability to create fingerprint which is resistant to aging. Different post-processing technique – binary encoding schemes based on the pattern obtained from the intra-die variability - have been implemented which is more adapted to be used in the results obtained in this chapter.

Chapter 5 introduces a novel technique that can also be effectively used to generate fingerprint of each. The technique introduced in this chapter uses guided wave EM approach or GEMT. This chapter first introduces various aspects of GEMT. Important details such as the use case and theoretical explanation explaining the usage of GEMT method for the creation of fingerprints of IC for the authentication

purpose. The physical level details which are used in exploitation of PV effects pertaining to internal physics of each IC under test have been investigated. Together with the understanding of various aspects of GEMT a basic simulation and its results have been discussed. Measurement approaches, development of customized PCB have discussed in detail. The post-processing technique based on cosine similarity and Gray coding schemes have been deployed. Also different techniques to mitigate the aging and systematic errors have been introduced. Lastly with conclusion we have compared the utility and implementation approaches of both REMT and GEMT based approaches.

Chapter 6 is an example chapter of the customized PCB developed in chapter 6. This chapter introduces the use of the customized RF FPGA PCB for the various RF applications. This chapter is divided into two parts. The first part details about the use of the FPGA as RF device with the measurement and implementation approach explained. For an example, simple RF switch structures have been developed by programing the FPGAs. The results and improvement on the existing performance have been detailed. The second part of this chapter describes about the implementation of wireless RF communication between two FPGA boards. The various aspects of RF communication viz. programming of FPGAs with the modulator and demodulator circuits have also been described. The chapter also discusses the implementation of distributed logic structure of various FPGA using wireless communication.

References:

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[2] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead," *J. Electron. Test.*, vol. 30, no. 1, pp. 9–23, 2014.

[3] K. He, X. Huang, and S. X.-D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, 2015, pp. 146–151.

[4] U. Guin, D. Forte, and M. Tehranipoor, "Anti-counterfeit techniques: from design to resign," in *Microprocessor Test and Verification (MTV), 2013 14th International Workshop on*, 2013, pp. 89–94.

[5] U. Rührmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 286–300.

[6] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[7] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[8] M. Alam, H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Impact of X-ray tomography on the reliability of integrated circuits," *IEEE Trans. Device Mater. Reliab.*, vol. 17, no. 1, pp. 59–68, 2017.

[9] H. R. Gorrepati, "Secure Split Test for Preventing IC Piracy by Un-Trusted Foundry and Assembly," PhD Thesis, 2015.

[10] "s-parameters-allow-hi-freq-verification.pdf." .Online. [Available]: https://www.analog.com/en/analog-dialogue/articles/s-parameters-allow-hi-freq-verification.html

[11] S. Ghosh and K. Roy, "Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era," *Proc. IEEE*, vol. 98, no. 10, pp. 1718–1751, 2010.

2. Counterfeiting of IC: detection, avoidance and preview on EM based authentication techniques

Objectives

The objective of this chapter is to introduce the concept of counterfeit of IC in details and define the various counterfeit techniques. Secondly we have also described the various proposed methods that have been adopted – their highlights and bottlenecks - in order to avoid and detect the counterfeiting techniques. A brief analysis on the highly used PUF approach has been detailed out. Lastly we have introduced in brief about the two electromagnetic (EM) based methods that have been proposed in this study, for the purpose of IC authentications. A brief description and comparison of PUF based approach with the EM based approach is also drawn out.

Preliminaries

Counterfeit ICs which constitutes a significant part of counterfeit products in electronics and semiconductor industry, pose a significant threat to the government and industrial sectors of the economy because they undermine the security and reliability of critical systems and networks. Due to the widespread use of electronic components in our day-to-day lives - both directly and indirectly – counterfeit ICs also pose major threats to the health, safety, and security of the population at large. For example, the failure of a pacemaker due to a counterfeit component can potentially take someone's life [1][2].

Also discussed briefly in chapter 1, a counterfeit IC cause significant damage to the economy. A semiconductor company invests billions of dollars, time and energy in developing a relevant and important product for an application to perform its best, whereas the counterfeiters spends a minimal cost to just clone or remark or recycle the used component and sell it to the end user. It not only degrades the quality of the products but also undermines the brand of the company under which the counterfeiters sell the fake product [1][2].

Since it's not the counterfeiter's responsibility to take blame for the failed or non-functioning counterfeited product, it becomes duty of original component manufacturer (OCM) to take care of the failed component [2].

Table 2.1: Top-5 Most Counterfeited Semiconductors in year 2011.

Rank	Component Type	Percent of reported incident
1	Analog IC	25.2
2	Microprocessor IC	13.4
3	Memory IC	13.1
4	Programmable logic IC	8.3
5	Transistors	7.6

With the increased complexity of the devices and competition in the market, the large OCMs share their design and development phases over small assembly and foundries. For example, large foundries located in different countries can offer lower prices to the design houses. Untrusted foundries and assemblies can also be capable of selling extra components outside of the number they were contracted to manufacture. This complex supply chain leads to an illicit market willing to undercut competition with counterfeit parts [3].

Recent reports from [4], have shown that there has been surge in the counterfeit ICs in past decades. Table 2.1 shows the details of the top five counterfeited components of the semiconductor companies. The components are as follows: analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors. Together, these five types of components make up around 68% (or, slightly more than two-thirds) of all the counterfeit incidents reported in 2011 [5]. The loss incurred due to the counterfeiting of these components have been more 100 $ billions.

2.1 Counterfeit IC: definition and features

A counterfeit component can be defined as the component which can have one or many of the following features [2][3].

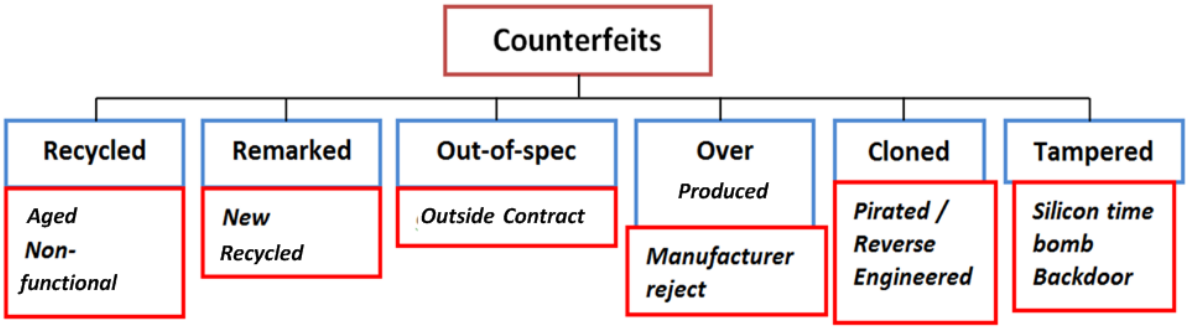


Fig. 2.1: Taxonomy of various techniques of counterfeit ICs.

I. It is an unauthorized copy which does not conform to Original Component Manufacturer (OCM) design, and/or standards.

II. It is produced by unauthorized contractors or manufacturers but not by the OCM.

III. It is defective or malfunctioning and an off-specification component.

IV. Or it is an old OCM product sold as ‘‘new’’ or labeled as OCM original component or, has incorrect or false markings and/or certifications.

The above definition may be extended to include much more and diverse aspects of the present scenario of counterfeiting. The present scenarios where an entity in the component supplies chain source electronic components that are authentic and certified by the OCMs. In today’s supply chain, there can be incidents of theft or cloning of designing. An untrusted foundry or assembly may source extra components without disclosing it to the OCMs [2][3]. Thus an illustrative and pictorial definition of the counterfeit IC can also be understood from the Fig. 2.1.

A ***recycled*** IC refers to the use of the IC that is discarded by the OCM or users and is being sent to the recyclers. Old and used electronic boards (PCB) instead of being sent to the recycler reaches to the counterfeiters who then scrap out the IC from the PCBs and resell it claiming it to be new [1][2][6].

But as discussed by Kai et al [6] today around 80% of counterfeit ICs or their components are recycled. This proves that the high number of fake and counterfeit ICs and electronic components are coming from old, recycled or scrapped electronics boards. Hence recycled IC is another big concern for the semiconductor industry.

Similar to the recycled counterfeit type, ***remarked components*** are also extensively discussed by the government, industry and test labs. Clearly, a component's markings are very important as they represent component's origin and, most importantly, determine how the component should be handled and used. Sometimes the counterfeiters modulate the grading of the components, i.e. alter the marking of low grade component to a higher one and sell into market at higher price. Of course a component made to work in low grade condition if remarked and sold to work in harsh condition would fail miserably and hence may collapse the whole hardware system [1][3].

Given this increasing cost and the complexity of foundries and their processes, the semiconductor business has largely shifted to a contract foundry business model (horizontal business model) over the past two decades. The OCM send their contract to other small foundries in this case. The untrusted foundries here can gain access to the original design and start producing the components without the permission of the OCM. The component produced like this is termed in ***overproduced*** component. Overproduced components may simply end up being used in critical application like military and space, with minimal or no testing for reliability and functionality. Together with the reliability issues, it imposes threat to the economy of the OCM [1][2][3].

An ***out-of-spec or defective*** component as name suggests is the discarded component by OCM. These components do not have proper functionality, fails to meet the required standards and does not conform with the application they are developed for. Hence they should be sent for disposal or should be destructed. However, if they are sold on the open market instead, either knowingly by an untrusted entity or by a third party who has stolen them, there will be an inevitable increase in their risk of failure [1][2].

Cloning is also a major concern for the semiconductor industry. It destroys the intellectual property (IP) rights of the authentic owner of the entity and causes loss of revenues. Cloning can be done by illegal copying of the IP and design netlist [1][2].

A ***forged component or IC*** is also synonym to a remarked component. Each component after being manufactured is given a certification by OCMs. By modifying or forging these certificates, a component can be misrepresented and sold even if it is nonconforming or defective.

Lastly, in the categories of the types of the counterfeit IC is ***tempering*** of the IC. This is done by adding an extra hardware Trojan. The adversaries can add extra circuitry in the IC, which can be like a silicon time bomb. It alters the functionality and consequently reliability of the IC. The added Trojan can also act as backdoor i.e. create a channel to leak important and secretive information to the non-authorized entity [1][2].

After getting to know in brief about the various types of counterfeit ICs, it is also important to understand the different stages of IC's life. We see from [7], a typical stage of development of an IC. The counterfeiting IC can start from the design, the manufacturing stage or packaging stage.

2.1.1 Counterfeit at different stages of IC lifetime

A typical life cycle of IC starts from the design of netlists and layout on the computer using commercially available software. Once the netlist, design and layout are finalized the manufacturer sends it to the foundry for the fabrication stage. A typical lifecycle is given in Fig. 2.2. After the fabrication, there is assembly and packaging of IC. Once ready, IC is tested by the OCM, to test for its reliability and robustness. Finally, when all the tests are done, IC is sent to the market. Each stage can be subjected to vulnerabilities of counterfeiting. We have discussed in brief about counterfeiting technique that can be applied by adversaries in each stage of IC lifetime [7][8]. An analysis of different stages that can causes counterfeiting of ICs (referring Fig. 2.2 also) is described below.

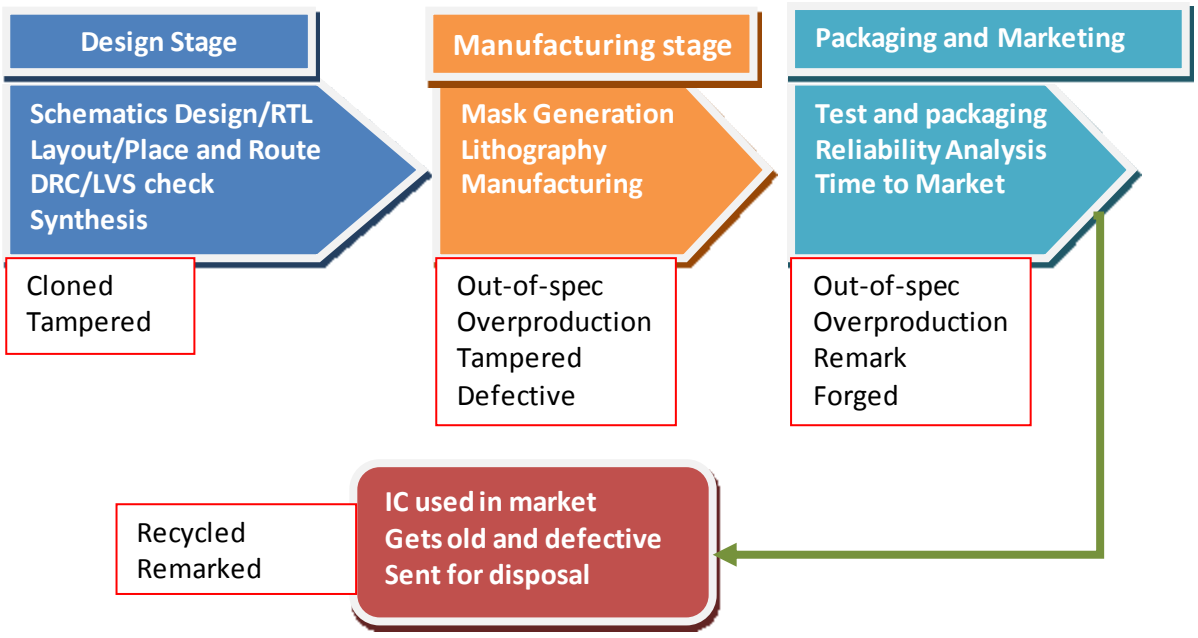


Fig. 2.2: Different stages of IC manufacturing and counterfeiting techniques at various stages of manufacturing.

In the ***design stage***, the original OCM IP design and netlists can be stolen and reused by adversary. The adversaries or untrusted foundries can design an IC with the same functionality, without proper testing and standard conformity; the components are packaged with an OCM label and sold to the market. In other ways, attacks on the design stage can be performed when the counterfeiter can tamper with codes to modify the functionality, create backdoors, etc. This creates two major problems: *(i)* **reliability and standard issue** – the counterfeiters can sell ICs in the market with the same functionality but one of them being an untested and untrusted IC, hence the product sold can degrade the performance of the systems it will be used in, (*ii)* **economic issue** – the low standard untested IC sold under OCM name by counterfeiter give the negative impact they can have on innovation, and credibility of the OCMs.

Secondly, the counterfeiting can also occur in the ***manufacturing stage***. In this stage a malicious or untrusted foundry can gain access to the design or mask of the IC and start production without the permission of actual OCMs or at this stage a foundry could overproduce and sell the ICs with the label of OCM. Adversaries or untrusted foundries can also tamper the design, and source defective and out-of-specification wafers to packaging companies to make finished parts.

Thirdly in a ***packaging stage*** a no-performing IC can be repackaged under an OCM label and can be sold as new IC in the market. An untrusted assembly can: *(i)* build overproduced ICs by hiding the yield information, *(ii)* sell the defective/out-of- 17 specification ICs, and *(iii)* remark, forge, or upgrade a component's marking.

Finally, when the ICs or electronics part become old and sent for recycling, from there the malicious foundries and adversaries can access the e-waste of the electronics component, recycle it, remark it and sell it back to the market as new. The recycled IC has been one of the biggest concerns in the semiconductor industry. Now we have analyzed the types of counterfeit and different stages of the IC which gets impacted by the counterfeiting techniques. The next section in this chapter aims at understanding the present the techniques that are being employed in different studies, research and industrial scenario to combat and mitigate the problem of IC counterfeiting.

2.2 Counterfeit Detection

Over the past several years a specialized service of testing has been created for detecting counterfeit components. The components must be authenticated by these tests before being placed in systems [1][2].

Counterfeit detection has been a big challenge in front of semiconductor industry. Over past several years there has been lots of testing methodologies used in the detection of the counterfeit. The methods are typically classified into three different approaches:

1. Physical Inspection [9]
2. Electrical Inspection [6]
3. Aging Based Fingerprints [6][10]

1. Physical Inspection

The study in [9] shows the various types of Physical Inspection methods. Such inspections are based on physical properties of the materials and components. Physical inspections are usually the first set of tests to be conducted on the incoming components to be authenticated. These tests are based on the physical properties of metals, leads, die etc. of the component. In incoming inspection all components are inspected thoroughly. Low Power Visual Inspection (LPVI) is used for the inspection of the external structure while X-Ray imaging is used for the internal inspection. Other exterior testing methods like SEM, SAM, and Blacktop testing and other tests are used to find defects and anomalies present outside the components. To perform the internal tests the component needs to be de-capped and the internal parts are to be exposed. Optical tests, SEM, Wire pull etc. are some of the test used to perform the internal testing.

Material Analysis is used in the analysis of defects in the materials compositions of the package and components. X-Ray Fluorescence (XRF) , Fourier Transform IR Spectroscopy (FTIR) etc. are used for material analysis [11].

In general, physical methods can be applied to all part types. But the drawback of this method is that some of the methods are destructive and take lot of time to test. As a result, sampling is required to certify a batch of parts by observing a small number of parts. Hence in total this is exhaustive and costly method to test with the risk of destroying parts or whole of IC. A summary of various physical inspection methods have been described in Table 2.2.

Table2.2: Description of physical inspection methods

Physical Inspections			
Incoming Inspection	**Exterior Tests**	**Interior Tests**	**Material Analysis**
Low Power Visual Inspection	Scanning Electron Microscopy (SEM)	Optical Inspection	X-Ray Fluorescence(XRF)
X Ray Imaging	Scanning Acoustic Microscopy (SAM)	Wire Pull	Fourier Transform Infrered Spec.(FTIR)
	Blacktop Testing	Die Shear	Ion Chromotography(IO)
	Microblast Testing	Scanning Electron Microscopy (SEM)	Ramn Spectroscopy
	Hermetically Testing	Scanning Acoustic Microscopy (SAM)	Energy Dispersive Spectroscopy (EDS)

2. Electrical Inspection:

Electrical Inspection is classified into the following broad divisions [6]

1. Parametric Tests
2. Functional Tests
3. Burn-in Tests
4. Structural Tests

These inspections are used to find the shift and defect in the electrical parameters in the IC due to the counterfeit. Parametric Tests are used to verify direct current (DC) and alternating current (AC) of the IC. They can let us know if there is any shift the value due to the over use or out of spec production. Functional analysis can be done using functional test. This test is used to find the defects which impact the functionality of components. Open wire, short circuits, cracks, damaged die etc. can be inspected using functional testing. Burn-In test is used to find the infant mortality failures to assure reliability. In Burn-In test the IC is operated at stressed condition, such as elevated temperature and voltage. In Structural Tests a test pattern is applied through internal scan to find defects in the internal logic, interconnects etc.[12].

Although the conventional electrical test methods are non-destructive as physical inspections are and time efficient, yet they can be very expensive because such techniques are not necessarily designed for

counterfeit detection this adds to one of the biggest drawbacks of the electrical inspection when it comes to detect counterfeit.

3. Aging Based Fingerprint

Aging based technique can be effective against recycled IC detection. An IC goes through aging effects during course of its lifetime. Due to continuous usage over period of time effects like Negative Bias Temperature Instability (NBTI) and Hot Carrier Injection (HCI) degrade the MOSFETs. Recycled ICs brand significantly reduces the functionality and capability of the IC to perform in different conditions [6][10]. There are two methods to detect the aging of IC:

1. Early Failure Rate (EFR) [13]
2. Circuit Path Delay Analysis [14]

Early Failure Rate (EFR) is a statistical approach. It uses a one class classifier training approach. The measurements used to build the classifier are typical results that are obtained from production EFR analysis such as Vmin(minimum voltage), Fmax (maximum frequency) and Iddq (current) [20]. Due to aging there is change in the delay of the path due to change in the resistance of the interconnect. This method is particularly useful for the detection of a single type of counterfeit method i.e. the recycled ICs. On similar lines circuit path delay method is used to detect the change in the path delay due to aging effects on IC. Due to aging effects, such as NBTI/PBTI and HCI, the path delays in recovered ICs will be larger than those in fresh ICs [17]. For a device under test (DUT), the larger the path delays are, the higher the probability there is that the DUT has been used and is a recovered IC.

Though these methods are effective in terms of results but their usefulness is limited in addressing only issues related to old IC. Secondly these solutions (eg. observe from Table 2.3, the ineffectiveness of path based delay method against various counterfeit techniques is not so optimum) may not be adapted to tackle other forms of IC counterfeiting techniques like cloning, remarking, over-production etc. The implementation can be ineffective in terms of: area – sensors require IC area over head and implementation time - not easy to industrialize. Also these methods have to be very appropriate because it is not necessary that every portion of IC is used or aged uniformly.

The effectiveness in detecting various forms of counterfeiting techniques (viz. recycling, cloning, remarking etc.) by the different adopted physical, electrical and aging based methods have been summarized in Table 2.3. The details in Table 2.3 can be really useful in finding which of the present

methods are useful against which counterfeit technique. The summary can be taken as reference which can motivate to probe for further enhanced and robust techniques for the detecting the counterfeit ICs.

Table 2.3: Different methods of counterfeit detection for various counterfeit techniques

Detection Methods	Recycled	Remarked	Overproduced	Out of Spec	Cloned
X Ray	Low	Medium	NA	NA	NA
Scanning Acoustic Microscopy (SAM)	Medium	NA	NA	NA	NA
Scanning Electron Microscopy (SEM)	Medium	Medium	NA	NA	NA
Material Analysis	Medium	Medium	Low	Medium	Low
Parametric Analysis	Medium	Low	Low	Medium	Low
Functional Test	Medium	Low	Low	Low	Low
Path Delay Analysis	Medium	Medium	Low	Low	Low

2.3 Counterfeit avoidance techniques

Given the amount of time, cost and risks that present counterfeit detection techniques pose, there are necessitates for the development of innovative avoidance mechanisms to be incorporated in the design [1]. Counterfeit avoidance techniques necessitates the development of innovative avoidance mechanisms to be incorporated in the design [2][15]. For instance, there can be two different approaches to tackle or avoid the counterfeiting, one based on the incorporation of sensors in the IC and another based on the traceability approach. For instance, in recycled IC a sensor based solution can be effective in determining if the IC is used or not. Secondly, the same approach may not be so effective in the other counterfeiting technique such as overproduced IC. In this section, we have briefly discussed various existing anti-counterfeit measures that can be implemented for new, active, and obsolete parts. The various measures that are in place to avoid counterfeit are:

- CDIR Sensor
- PUF approach
- SST Secure Split Test
- Hardware Metering
- Split Manufacturing
- Package ID

- CDIR Sensor: The Counterfeit Die and IC Recycling (CDIR) sensors are used to prevent the **recycled IC**. In this technique a MOSFET based Ring Oscillator (RO) is used as a lightweight sensor inserted in the chip. The sensor is composed of a Stressed RO and a Reference RO. The sensor relies on the aging effect of MOSFET. The difference between stressed RO and reference RO can give an approximation of the age of the chip in the field [16]. The **major issue** concerning the design of CDIR sensors can be large overheads when implemented on the IC.

- PUF approach: PUF or physical unclonable function exploits the inherent physical variation that comes in an IC during its manufacturing process due to manufacturing defects. PUF based solution is based on traceability approach. The various types of PUFs like Arbiter PUF, RO PUF, SRAM PUF etc. PUFs can be used to prevent **cloned ICs** as they generate unique IDs which result from randomness in the IC manufacturing process that cannot be controlled or cloned. These unique IDs of genuine ICs can be stored in a secured database for future comparison [17] [18]. The **bottleneck of PUFs** is area overhead, instability due to placements constraints and aging effects. A brief analysis of PUF approach has been explained in sub-section 2.5.

- Secure Split Test SST: SST approach is used to prevent **out of spec, cloned and overproduced** IC. It uses a hardware cryptographic approach, a locking mechanism in which only the legal IP owner of the IC can activate the functionality of the IC. SST helps in avoiding the counterfeit and help design house to protect their IP. In this method a unique cryptographic key is added along with a binary identifier. Through this the IP has the key to unlock and verify the test results. This helps in avoiding cloning, overproduction and out of spec IC threats [15]. The major drawback in this approach is high cost.

- Hardware Metering: Hardware metering places a set of security protocols that enable the post fabrication control of the produced ICs. This method helps provide the design house with a unique way to identify the each IC produced from same mask [19]. There are two broad classifications of this method, passive and active types. This method prevents the **overproduction** of IC. The drawback and bottleneck of this approach is the extra cost and time incurred along with overhead required in the IC area

- Split Manufacturing: In this approach, the layout of design is split into two layers: Front End of Line (FEOL) and Back End of Line (BEOL). This is done in order to **mitigate-the-risks–in-manufacturing**. These layers are then fabricated separately in different foundries. FEOL consists of transistors and lower metal levels and BEOL consists of top layer metals. Both FEOL and

BEOL wafers are integrated after the fabrication [15][20]. Extra cost is one of the main issues with this approach with the bottleneck of setting up two parallel manufacturing units.

A summarized detail of various counterfeit avoidance schemes and methods have given in Table 2.4. From Table 2.4, the effectiveness of different avoidance methods against different types of counterfeit techniques can be observed. This summary can be useful in an attempt to find out which methods are useful and if not how we can improvise and adopted different or new avoidance methods.

Table 2.4: Different methods used for the IC counterfeit avoidance

Avoidance Methods	Recycled	Remarked	Overproduced	Out of Spec	Cloned
CDIR Sensor	High	High	NA	NA	NA
PUF	High	Medium	Low	Low	High
Secure Split Test (SST)	NA	NA	High	High	Medium
Hardware Metering	NA	NA	Low	NA	Medium
Split Manufacturing	NA	NA	Low	NA	Low
IC camouflaging	NA	NA	Low	NA	Low

Among various techniques of counterfeit avoidance, PUF technique is widely adopted for the purpose of security and authentication. Also evident from Table 2.4, it is clearly observed that among various counterfeit avoidance schemes like CDIR sensors, SST, hardware metering etc. PUFs fair better and are more potent in avoiding counterfeit of ICs. They are effective against every highly practiced counterfeit technique like recycling, cloning etc. Extending the usability of PUF against counterfeiting we have detailed out basic principles of PUF and its advantages in the section below.

2.4 PUF based approach – authentication principle and advantages

An outline of widely used physical unclonable function or PUF based technique has been given in this section. Among various techniques discussed here in order to avoid counterfeiting, PUF has been one of the widely adopted techniques and has been area of interests. PUFs find their applications in authentication, generating cryptographic keys and securing important information and data on the chip. PUFs are a promising innovative primitive that are used for authentication and secret key storage without the requirement of secure ROMs and other expensive hardware described above. This is possible, because instead of storing secrets in digital memory, PUFs derive a secret from the physical characteristics of the

integrated circuit (IC) [17] [18]. We will discuss in detail about the manufacturing based PV effects of IC in chapter 3.

Each PUF can be modeled as a black-box challenge– response system. In other words, a PUF is passed with an input challenge 'c', and returns a response r = f(c), where f(c) describes the input/output relations of the PUF. Depending upon the number or strength of challenge response pair (CRP), PUFs are categorized as strong or weak PUF. Various types of electrical and non-electrical PUFs have been introduced in studies. No-electrical PUFs include – optical PUF, coating PUF etc. Electrical PUF (CMOS based) – arbiter PUF, ring oscillator PUF, LC PUF etc.[21]. In this study we will not go into details of strong / weak or electrical /non-electrical PUFs. We have discussed in brief the functionality on the basic CMOS based PUF. An example of CMOS based PUF is an arbiter PUF (shown in Fig. 2.3(a)) realized using circuits like MUX, flip flop etc. The functionality of an arbiter PUF depends upon manufacturing variability in gate delay as the source of unclonable randomness.

2.4.1 PUF for authentication of IC

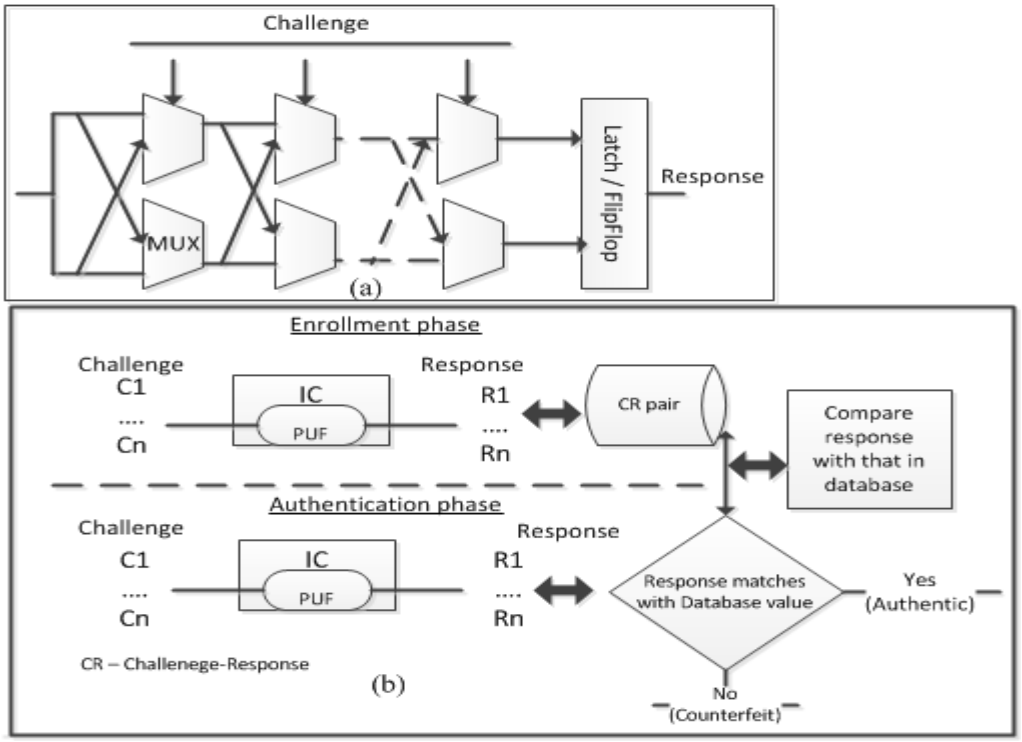


Fig. 2.3: (a) A pictorial description of CMOS Arbiter PUF with MUX and Latch. (b) Typical phases of PUF working to combat counterfeiting.

As the PUF output is unique and unpredictable for each IC, provided it is long enough, it is straightforward to identify an IC with the PUF [17][18]. A simple pictorial description of the PUF implementation for the purpose of authentication has been given in Fig. 2.3(b). From Fig. 2.3(b), we can observe that a PUF based authentication is divided into two phases: *(i)* **Enrollment phase** – challenge response pair is created by OCM or manufacturers and the values of challenge and corresponding response is stored in secured database. *(ii)* **Authentication phase** – in this phase, the user (who wants to authenticate the IC), gives same set of challenge (as given by OCM). The response obtained is compared with the values stored in the database created during enrollment phase. In this way it is possible to find the authenticity of the IC through PUF based approach.

2.4.2 Summary of PUF : Advantages and constraints

As we have observed from basic description of PUF that PUFs utilize inherent manufacturing variations to produce hardware tokens or keys that can be used as building blocks for authentication protocols. PUF derive secrets from complex physical characteristics of ICs rather than storing the secrets in digital memory. For example a secret key can be generated whenever there is need for the authentication of the device, rather than storing it in the memory digitally. This reduces the risk of theft of the key by adversaries. Secondly, PUF keys are function of random process variation effects hence they are very hard to predict by the adversaries [17][18][22].

Along with the many advantages the PUF scheme possesses, they also have few bottlenecks. On the resource constraint devices, it is hard to implement PUFs as they require high area owing to complex on-chip post-processing approaches. Also, in terms of industrialization it is difficult to industrialize PUF on every IC for their purpose of authentication. This stems from fact that area and cost of PUFs are not optimized for the implementation on ICs. A detailed overview and description of few bottlenecks of PUF is also given in section below.

The next section details an outline introduction and preview of the EM based methods that will be present extensively in later chapters in this thesis. In the next section we have highlighted in brief the need for another authentication scheme, outlined the proposed EM authentication approaches and compared it with widely adopted PUF approach.

2.5 Preview on EM based techniques for authentication

2.5.1 Need for other authentication approach – variant of PUF

We have clearly observed from the above sections, the definition and techniques of the counterfeiting of ICs. Various techniques of performing counterfeiting of IC have been studied in this chapter along with the impact they have on the semiconductor and electronics industry – reliability and economy. Together with problems in hand, we have also discussed about the present methods that are adopted in order to avoid and detect counterfeiting of ICs. Each method presents its own objective, advantages and challenges. However, given the advent in the assimilation of IC in every hardware application, and advent of internet of things (IoT) and miniaturization of IC, it has become imperative to explore for newer and effective solutions. The demand and requirement for smaller area and power consumption is a driving force which compels to implement and utilize approaches which are better suited in terms of efficiency, power and area of electronics chips or ICs. A more detailed analysis regarding need and importance of introducing other authentication mechanism has been detailed in chapter 3 and chapter 5.

2.5.2 EM based technique for authentication – an outline

In this study we have proposed an alternate (extended) and novel method that utilizes EM based signature to implement authentication of IC. In this section we have given a preview of the two EM based methods that have been proposed and implemented in order to mitigate the effects of counterfeiting of the IC. The two techniques implemented in this thesis work are:

1) **Radiated EM technique (REMT)**

2) **Guided EM technique (GEMT)**

Both the techniques utilize the process variation (PV) effects – like PUF – but the implementation techniques are different to PUFs. The detailed analysis is laid out here and also in chapter 3 and 5 respectively.

Together with the implementation of the techniques, the other very important aspect that is dealt in this work is with regards to the use of mathematical and statistical approaches to post-process the EM based signature that can create distinguishable and unique fingerprints for each IC as depicted in Fig. 2.4. The post-processing steps have been one of the major efforts of this work. The response from the IC can be in different forms or domains. The direct response cannot be easy or efficient to be determined as fingerprint. Hence a mathematical treatment is very important to convert the IC response (see Fig. 2.4)

into a meaningful and understandable fingerprint. To gauge the effects of the aging on the IC and subsequently on the authentication metrics we have performed aging analysis and also developed methodologies that can mitigate the aging effects on the authentication.

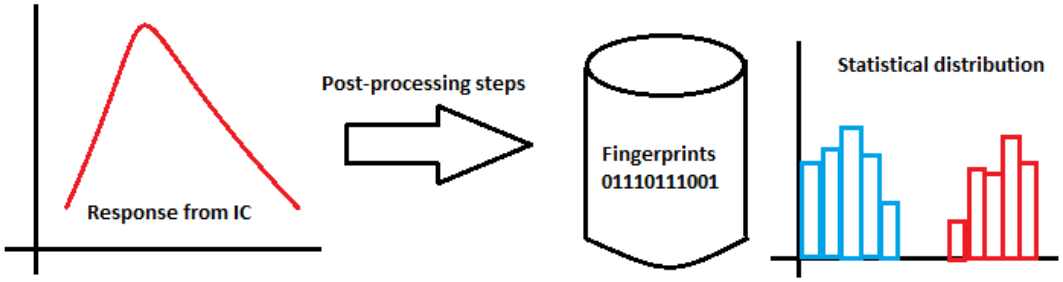


Fig 2.4: Post-processing steps implemented for converting the IC response into fingerprints / signatures.

1. REMT – Radiated EM emission technique for authentication of IC

In the **radiated EM emission technique or REMT**, the utilization of emitted EM/RF wave emission when circuit in the IC is switches on and off continuously has been elaborated. This technique is based on tapping EM emission due to switching of transistors [23]. The switching of transistors depends upon many electrical and physical phenomenon like threshold voltage, resistance, capacitance etc. [24]. All the phenomenon regulating the switching of the transistors do get affected by process variation (PV) effects. A detailed description of REMT based technique is given in the chapter 3. The descriptive analysis performed regarding this part of the study is as follows:

- Understanding the circuits that need to be implemented in the device under test or DUT that is variability aware. This is the first and most important aspect of this part of study. We need a robust, stable, efficient and lightweight circuit that act as our authentication marker to exploit the PV effects.

- The second part of this study is the measurement. The measurement protocol has to be robust. Each measurement should be reversible and should give same results for same DUT at different points of time in different setups.

- The third part is associated with the analysis of the results. This part is important in order to ensure that the response actually comes from the DUT and not from any external noise source. Subsequently this part of study implements statistical post-processing analysis to create a fingerprint from the obtained response from each DUT.

- The fourth part of this study is the extension of the first three points. This part deals with the effects of aging on the ICs / DUT and how that can affect the authentication. In this respect we have deployed alternated methodologies that can be used to mitigate the aging effects.

2. GEMT - Guided wave EM technique for authentication of IC

The second approach in light of non-invasive EM based authentication technique is Guided wave RF approach or GEMT. This approach is novel approach in aspects of IC authentication. This approach also based on utilizing the process variation effects. In this approach we have attempted to use high frequency RF waves. The idea here is to send a guided RF wave in to the IC (not classic RFICs) and observe the effects of IC physics on the output of the wave.

Radio Frequency (RF) is any electromagnetic wave whose frequencies extend from 3 kHz to 300 GHz [25]. The guided RF wave utilizes the manufacturing variation features. Each IC interacts with RF input wave and produces a signature. Each response can be stored in a database and when required it can be used to authenticate an IC. The guided wave traverse in the IC, a part of it reflects back and some part is absorbed or refracted. Based on the physical variations in the IC, amount of reflections, refractions and absorption differs. This difference gives each IC a unique or distinct identification. In the ICs, the amount of reflection, absorption or refraction of the input wave depends on the process variations. The process variation like lithographic defects, variation in gate oxide thickness etc. causes variability in the physics of ICs even from the same mask [26]. This results in a different and unique response for each IC when a guided RF wave interacts with it. This could be further utilized for the purpose of authentication. A detailed description of GEMT based technique is given in the chapter 5.

Of course the implemented circuit to disturb the incoming RF waves is not exactly same as in the radiated EM (REMT) approach. Rather in this technique we have tried to exploit the routing of IC or very small to basic circuit elements that could be possibly utilized. The aim has always been to be non-invasive with cost ad area efficient.

2.5.3. EM based method comparison with PUF

As discussed in section 2.4, that PUF have been one of the most dominant method utilized in the semiconductor industry and is frequently studied in academia also. PUF is based on traceability solution which is dependent upon the intrinsic factor of PV. PUF functions by taking a set of challenge, which owing to the PV effects gives a unique response. For each challenge there is unique response also termed as CRP. For PUFs there is a requirement to have a large number of CRP, which is needed as one challenge cannot be repeated again. Large number of CRP itself can be problematic in certain applications and secondly it is important to safeguard the CRP against eavesdroppers. For the CRP there is need of huge database that has to be maintained which in itself is cumbersome task. Secondly PUF suffers from the problem of large area overhead. The output of PUFs is post-processed in the dedicated circuit in the IC itself. Hence there is need to program or embed the device under test (DUT) with the specialized post-processing technique and circuit. This takes up lot of silicon area and also complicates the implementation. In an era where miniaturization of IC is necessary, the deployment of PUF can be very exhaustive in terms of area and cost. Therefore, even though PUFs do give good results there are always a room for improvement in terms of implementation and methodologies.

Even though these restriction do not completely diminish the importance of PUF in various applications of hardware security, but in this manuscript we have made an effort to extend the elemental PUF based philosophy – PV effects exploitation – to generate fingerprints / signatures of the ICs using the EM based approaches. EM based approaches tend to minimize some of the limitations that traditional PUF solution have in order to generate the fingerprints of ICs. Comparing to the PUF approach, the proposed EM based solutions are highly non-invasive in nature. Even though both the proposed EM based solution also utilizes the PV effects (similar to PUF based techniques), but the exploitation method is completely different. For example in REMT based method, the PV effects are exploited by EM emission when ICs are powered ON. There is no need to give any external challenge to the IC. Similarly in GEMT based approach, the ICs are interrogated by external RF / EM waves. In both the case we do not require any dedicated CRP, as there is no external challenge required in this case. And the output is not dependent upon the input challenge as is in case of PUFs. The EM based response is characteristics of the PV effects which are exploited from IC without any set of input parameters. Secondly in EM based methods do not require any post-processing techniques. Hence there is no need to have a dedicated circuit which processes the data on-chip. This saves a lot of silicon or chip area and makes the design very simple and easy to implement. Hence as a summary, in comparison to PUF, EM based approaches are easy to industrialize, efficient to implement and cost effective. One constraint with the EM based method is that,

due to off-chip post-processing, it is not able to authenticate the chip automatically itself. It depends upon the processing and storing of data outside the IC.

2.6 Conclusion

This chapter has discussed in details about the problems related to the counterfeit of ICs and electronics component. Various counterfeiting techniques that are deployed by the counterfeiters that have impacted the semiconductor and electronics industry have been discussed in detail. Different techniques related to the techniques applied for avoidance and detection of counterfeiting of IC have been discussed in detail in this chapter. The highlights, advantages and disadvantages of each technique haven investigated. We have also discussed about the PUF based technique that uses PV effects of ICs and how they can be used for the purpose of creating a unique identification to combat counterfeit.

However, given the advent in the assimilation of IC in every hardware application, and advent of IoT and miniaturization of IC, it has become imperative to explore for newer and effective solutions. Later on we have focused on the introduction or preview of the EM based techniques that have been used in this work. We have given a brief comparison of the existing PUF based approach with our proposed EM based techniques.

The motivations behind the approach to develop new techniques are to cut the extra cost incurred as in approaches discussed above, avoid the use of extra costly hardware, avoid use of any high powered input which can be dangerous for the components and a method which could be easily industrialized. In the following chapters we will discuss in extensive details about the two authentication metric based on EM technique.

References:

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[2] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead," *J. Electron. Test.*, vol. 30, no. 1, pp. 9–23, 2014.

[3] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[4] "Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security - IHS Technology." [Online]. Available: https://technology.ihs.com/389481/reports-of-counterfeit-parts-quadruple-since-2009-challenging-us-defense-industry-and-national-security.

[5] "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market | IHS Online Newsroom." [Online]. Available: https://news.ihsmarkit.com/press-release/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha.

[6] K. He, X. Huang, and S. X.-D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, 2015, pp. 146–151.

[7] X. Xuan, A. D. Singh, and A. Chatterjee, "Lifetime Prediction and Design-for-Reliability of IC Interconnections with Electromigration Induced Degradation in the Presence of Manufacturing Defects," *J. Electron. Test.*, vol. 22, no. 4–6, pp. 471–482, Dec. 2006.

[8] G. Klutke, P. C. Kiessler, and M. A. Wortman, "A critical look at the bathtub curve," *IEEE Trans. Reliab.*, vol. 52, no. 1, pp. 125–129, Mar. 2003.

[9] S. Shahbazmohamadi, D. Forte, and M. Tehranipoor, "Advanced physical inspection methods for counterfeit ic detection," in *40th International Symposium for Testing and Failure Analysis*, 2014, pp. 55–64.

[10] H. Dogan, D. Forte, and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Amsterdam, Netherlands, 2014, pp. 171–176.

[11] M. Alam, H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Impact of X-ray tomography on the reliability of integrated circuits," *IEEE Trans. Device Mater. Reliab.*, vol. 17, no. 1, pp. 59–68, 2017.

[12] P. Fleming, "Semiconductor perspective on test standards," in *International Test Conference 1988 Proceeding@m_New Frontiers in Testing*, Washington, DC, USA, 1988, pp. 197–198.

[13] K. Huang, J. M. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*, 2012, pp. 7–12.

[14] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, 2008, pp. 51–57.

[15] G. K. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure split-test for preventing IC piracy by untrusted foundry and assembly," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium on*, 2013, pp. 196–203.

[16] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 24, no. 4, pp. 1233–1246, 2016.

[17] U. Rührmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 286–300.

[18] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[19] B. Liu, Y. Jin, and G. Qu, "Hardware Design and Verification Techniques for Supply Chain Risk Mitigation," in *Computer-Aided Design and Computer Graphics (CAD/Graphics), 2015 14th International Conference on*, 2015, pp. 238–239.

[20] H. R. Gorrepati, "Secure Split Test for Preventing IC Piracy by Un-Trusted Foundry and Assembly," PhD Thesis, 2015.

[21] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2012, pp. 302–319.

[22] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9–14.

[23] N. K. Huang *et al.*, "Electromagnetic emissions from the ic packaging," in *Electrical Design of Advanced Packaging and Systems Symposium (EDAPS), 2012 IEEE*, 2012, pp. 65–68.

[24] B. Nikolic *et al.*, "Technology variability from a design perspective," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 58, no. 9, pp. 1996–2009, 2011.

[25] M. Hunter, "The basics of radio system design," in *IEE Colloquium on How to Design RF Circuits*, London, UK, 2000, vol. 2000, pp. 10–10.

[26] S. Ghosh and K. Roy, "Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era," *Proc. IEEE*, vol. 98, no. 10, pp. 1718–1751, 2010.

[27] A. Aryanpour and G. E. Cowan, "A circuit design and fabrication approach to address global process variation," in *Circuits and Systems, 2009. MWSCAS'09. 52nd IEEE International Midwest Symposium on*, 2009, pp. 455–458.

3. Radiated Electromagnetic technique (REMT) for IC authentication

All the methods discussed above for both counterfeit avoidance and detection have their pros and cons. In this manuscript we are going to propose an alternate and new method to detect IC counterfeiting. This approach is based on the measurement of Electromagnetic (EM) signatures. This EM based signature can be used as a parameter to distinguish real and counterfeit IC. We have seen many counterfeit detection and avoidance methods in the last chapter. Our idea is to authenticate the IC, i.e. find a unique parameter for each IC which would serve as its fingerprints or signature. Each IC has its own unique parameters. No two ICs even built on the mask can have same physical characteristics. This differentiation comes due to the manufacturing variations. In this chapter we have first discussed about the effects of PV before going into details of the EM based non-invasive techniques.

3.1 Preliminaries and objectives

The notion of this chapter is about the introduction of the radiated EM technique or REMT based authentication methodology. In this chapter we have discussed in detail about various factors and building blocks that are needed to efficiently implement the REMT based authentication scheme. Before going into the implementation details and results of REMT based authentication methodologies, we have given a brief description of the preliminary background of systems and steps needed to affirm the implantation of REMT based authentication methods. Among other important sub-topics the preliminary information include the introduction and in detail analysis of the factors that effects the selection of REMT based authentication, effects of process variations, post-processing technique steps required etc.

We have discussed in the chapter 2 that there are already many steps and methods to detect the counterfeits. But still there is a need and scope of improvement in the present counterfeit detection and avoidance techniques in terms of – area constraints, power consumption, ease of utilization etc. When compared to some of the present authentication schemes the proposed EM based approach is cost

effective, area efficient and easy to implement. From chapters 1 & 2, we have observed the basic overview of the two EM based techniques that could be used for the authentication purpose.

The first approach – radiated EM technique (REMT), does not need any extra dedicated circuitry. It is relatively cheaper and easier to implement it, compared to the traditional PUF approach or few other approaches if not with all. The PUF for an example requires a lot of silicon area to perform the on-chip post processing which ultimately requires extra cost. But in our EM based approach we aim to perform all the post processing outside the chip, which would reduce the area overhead and thus the cost of implementation. A comparison of REMT and PUF based technique is drawn out in chapter 2 also.

Secondly, along with the low cost of implementation it is relatively easy to industrialize this approach. If we compare it with the PUF approach, we find that PUFs are not so easy to industrialize. As they require a dedicated cost and circuit to implement them. The placement of the PUF circuit is a very important issue. For example if we consider a ring oscillator PUF we find that the placement of ring oscillator inside a PUF is a big issue. If ring oscillator is placed near the power supply the frequency of ring oscillator is affected by the power supply rail and hence results –depends upon the position of the PUF- vary a lot [1] [2]. Also, with the increasing variability in scaled ICs, designing PUFs with consistent outputs is an extremely challenging task. But in EM based approaches that we will discuss we will find that there is no dedicated circuit (or even required it's very lightweight) required, no on-chip processing (low cost), thus it is very easy to implement them in an industrial scale.

In any of the schemes or techniques be it PUF or any other techniques, the nuance to exploit the fingerprints or signature of an IC is by using the manufacturing based PV. Hence, it is very important for us to understand the origin and effects of PV on the present day IC manufacturing. In next sub-section, a detailed analysis of the PV has been explained.

3.2 Process Variations in IC

Variability related to the process parameters can be categorized into two broad areas: *1) spatial and 2) temporal* [3][4]. The variation in device characteristics at t = 0 *s* is due to spatial process variation. Such variation can be subdivided into inter-die and intra-die process variations. A pictorial classification of PV effects in IC manufacturing is described in Fig. 3.1.

3.2.1 Spatial Variability

Spatial variability is the type of variability that occurs in an IC during its manufacturing time (t = 0s) [3]. This type of variation can be subdivided into intra-die and inter-die variation. Spatial variability is depicted pictorially in Fig. 3.1. Parametric variations that come due to variation among different lots (L2L), dies (D2D) or wafers (W2W) are categorized into inter-die variations. Fluctuations in device length (L), oxide thickness (tox), width (W), flat band conduction etc. are the reasons for inter-die variations. Intra-die variation comes due to random variations like line edge roughness (LER), random dopant fluctuations (RDF) etc. Variability (inter and intra) causes variations in electrical properties of transistor such as threshold voltage (Vth). The variations in Vth results in variation in delay, switching and speed of the circuits [5].

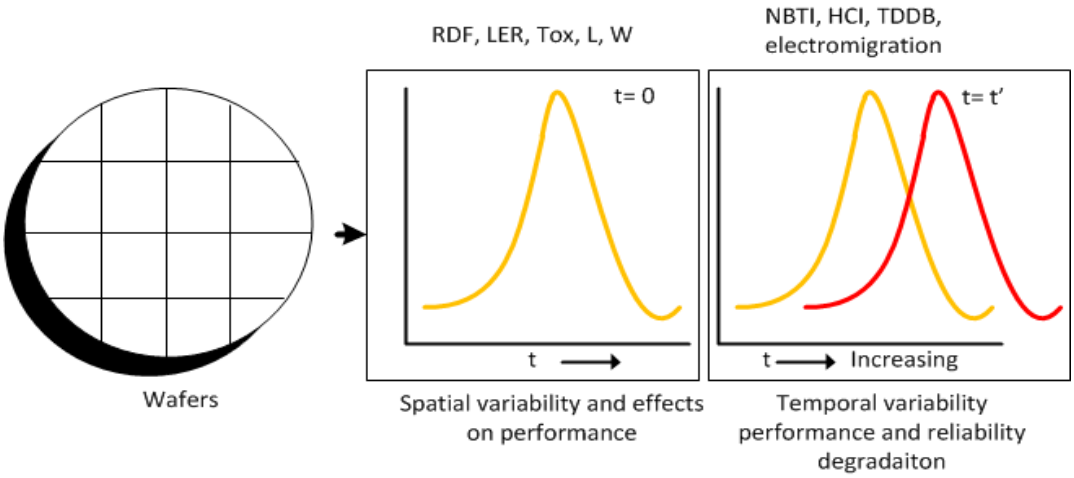


Fig 3.1: Pictorial depiction of process variation in IC manufacturing. Spatial and temporal process variations. The probability density function of chip delay due to temporal degradation has been shown.

3.2.2. Temporal Variability

The temporal variability comes with usage of device over a period of time ranging from a few nanoseconds to a few years depending on its source and applications also shown in Fig. 3.1. From [1][2][3] temporal variability arises due to run-time effects caused due to Negative Bias Thermal Instability (NBTI), Hot Carrier Injection (HCI), Electro-Migration and Time Dependent Dielectric Breakdown (TDDB). NBTI and HCI are of greater interest in this study as they affect the switching speed of transistors and consequently its performance. NBTI has the most effect on the transistor aging among

all other phenomena. It greatly affects the PMOS transistors. NBTI is driven by negative bias voltage, which creates interface traps that leave some permanent defects in the interface region. NBTI increases the Vth of the transistor which lowers the speed. HCI is another aging mechanism that effects the speed and performance of the transistors [6]. It is particularly caused by trap accumulation in the interface which causes increase in Vth resulting in lowering of speed [7].

In this study, the effects of both temporal and spatial variability have been evaluated. The effects of spatial variability are exploited to create fingerprints from devices under test (DUT) and the effect of temporal variability is studied during the phase when aging effects on the fingerprints are evaluated.

A brief observation of the effects and types of process variation (PV) has been detailed in this section. The motivation for the description of PV has already been stated in the initial part of this chapter. After understanding the PV effects and its implications, we now move to describe the methodologies that we have implemented to exploit the underlying PV effects in order to generate signatures for the ICs.

Before going into the authentication process and methodology using REMT based approach, a brief highlight has been given on the EM emission from the IC, its states and nature.

3.3 Electromagnetic (EM) emission in IC

Any oscillating circuit or any digital circuit emits an EM radiation. IC current loops are the primary radiation sources behaving as magnetic dipoles to radiate undesired electromagnetic emission (EMEs) of IC [8][9] .The IC pulsed currents are the consequence of transistor simultaneous switching activities of silicon die which driven by a clock signal. These currents are commonly drawn from source terminal and return via ground terminal of IC. Generally, the pulsed currents flowing along a path consists of package leads, wire bonding and interconnections on silicon die as shown in Fig. 3.2. Referring to Fig. 3.2, it illustrates decomposition of the current loop into two auxiliary components of vertical loop and horizontal loop.

Current and voltage transients related to high frequency switching and short rise/fall times of useful signals cause EM emissions of digital ICs. Resulting voltage glitches are proportional to the switching speed, number of gates that switch simultaneously and the effective inductance of the power line. Any

circuit in which some current flows through various shaped wire arrangements radiates electric and magnetic fields.

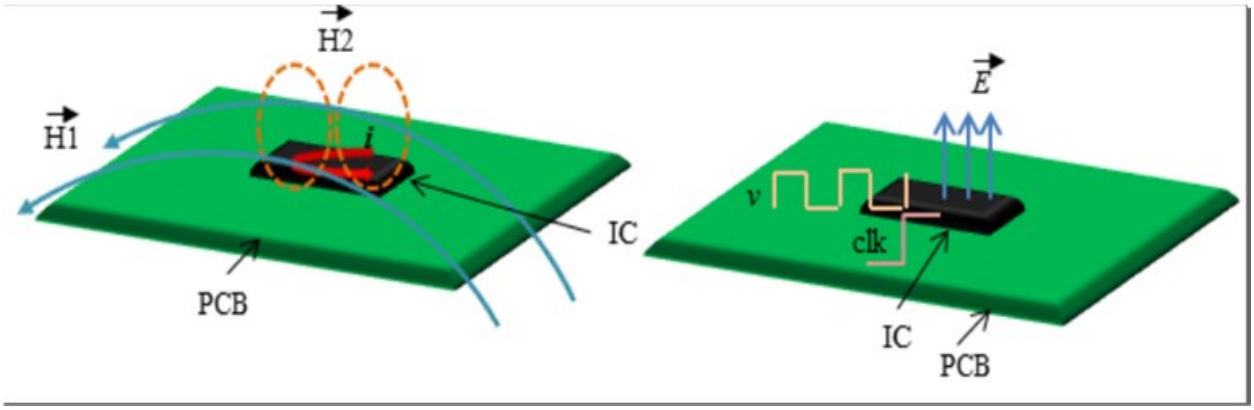


Fig. 3.2: EM field in an IC and depiction of coupling mechanisms of electric and magnetic fields in an IC.

The depictions in Fig 3.2 show a schematic diagram of the emission mechanisms for both the electric and magnetic fields emerging directly from an IC. From Fig 3.2 it is clear that the due to loop of current generated in the IC there is a magnetic field both in vertical and horizontal direction. This emitted magnetic field has been point of interest for our study. As we have captured the H-field using the H-field probe. The detailed description is given in section of this chapter.

Now, we have detailed the information related to the effects and origin of PV along with the emission of EM from IC. The next part of this study is about the implementation of radiated EM emission from ICs for the purpose of their authentication.

3.4 Radiated EM emission for authentication of FPGA-IC

As seen from section 3.3, it is clear that each IC emits a radiated EM emission during flow of current in loop or switching activity of the transistor in the digital logic circuits. We propose a method of authenticating an IC using radiated electromagnetic (EM) or REMT based approach. Thanks to the PV from an IC, each IC has a unique EM signature that can be used as its fingerprint for authentication. This part of study first focuses on field-programmable gate array (FPGA), which is a common target of

counterfeiting. Our method targets to authenticate new FPGAs to prevent theft or counterfeit during the supply from original component maker to the customer.

We have designed and implemented a variability-aware circuit (VAC) in FPGA and attempted to obtain a unique or distinct signature for authentication for each FPGA due to the effect of PV on the variability-aware circuit. A detailed circuit analysis (nature and complexity) of VAC is given in sub-section 3.4.2.

Compared with the existing methods (electrical and physical) to detect counterfeit IC our method is close to being non-intrusive, requires less time and involves no risk of damaging the IC. For the VAC circuit to be efficient it should have some characteristic qualities like:

(i) It should be able to exploit the inherent manufacturing based PV effects of IC. The output of the VAC must be function of underlying PV effects as shown in (1)

$$VAC(OP) \propto f(PVE) \qquad (1)$$

Where, VAC(OP) is output of VAC

PVE – Process variation effects

(ii) It should be able to emit an EM radiation i.e. for REMT based authentication it is important that VAC implemented must emit EM radiations.

Since we are using FPGA, we have focused on the logic switching of the transistors. The switching emits an EM radiation. The operational characteristics of VAC are related to device parameters like transistor switching speed and the capacitive load of the next step. The transistor switching speed depends upon the Vth and geometry (L and W) of the transistor [4]. Capacitive load is affected by geometry and area (L and W) of the transistors [5]. The switching phenomenon which emits EM would be used to characterize the variation in RO frequency. This would create an EM signature for each IC.

3.4.1 Evaluation steps for REMT

As for any authentication scheme there is need of two phases of work one is the enrollment phase in which the responses or generated keys are stored in a database. Second is the comparison phase the generated response of an entity is checked against a list of enrolled responses. When an enrolled response

is found whose distance to the presented response is smaller or equal to the identification threshold, then the entity is identified as the matching entry in the list.

Similarly, for the EM based authentication, there needs to be set of steps that are implemented for successful and efficient implementations of the EM based authentication scheme. A use case description of the different stages of implementation of EM based authentication scheme is described in Fig. 3.3. Also referencing from Fig. 3.3, the working methodology for the REMT can be divided into two main categories:

i) ***Enrollment stage***

ii) ***Authentication / comparison stage.***

In the *enrollment* stage (see Fig. 3.3), a set of measurements is performed on a DUT (by original vendors etc.) which extracts the spectrum of the EM radiation from the DUTs. The major component of the enrollment stage is the identification or recognition of a metric that can be utilized in order to exploit the underlying PV effects. The dependency of such a metric has been function of various electrical parameters like Vth, switching speed, resistance, capacitance etc. of the circuit and interconnects. This part is performed by the use of VAC. The exploited response using VAC is then treated with optimum post-processing solutions which convert the output response to a quantifiable signature.

For example, in a DUT 'D', the OCM or original vendor implements a VAC circuit. Then a set of measurement is performed to extract the radiated EM response. The response *f* is then treated with post-processing tool which converts it into quantifiable signature and to find a statistical distribution. Hence, in this stage signatures of DUT is generated which is can be stored in a secured database for the purpose of authentication in the future.

The next step in the REMT (EM based authentication) is authentication / signature comparison stage. That is when a user / customer want to check for the authenticity of the DUT. In this stage, the DUT to be authenticated is subjected to same set of measurements and post-processing steps and fingerprint is generated as done by the OCM or original vendor during the *enrollment* stage. Suppose that same DUT D is subjected to same set of measurements as is done by vendor in the *enrollment* stage by the end user. The response generated let say be *f'* (there may be some variation owing to process, voltage and temperature change). The signature (*f'*) obtained is compared with the signature obtained originally in

enrollment stage. The further processing are involved in this step to evaluate the degree of similarity between the signatures *f* and *f'*.

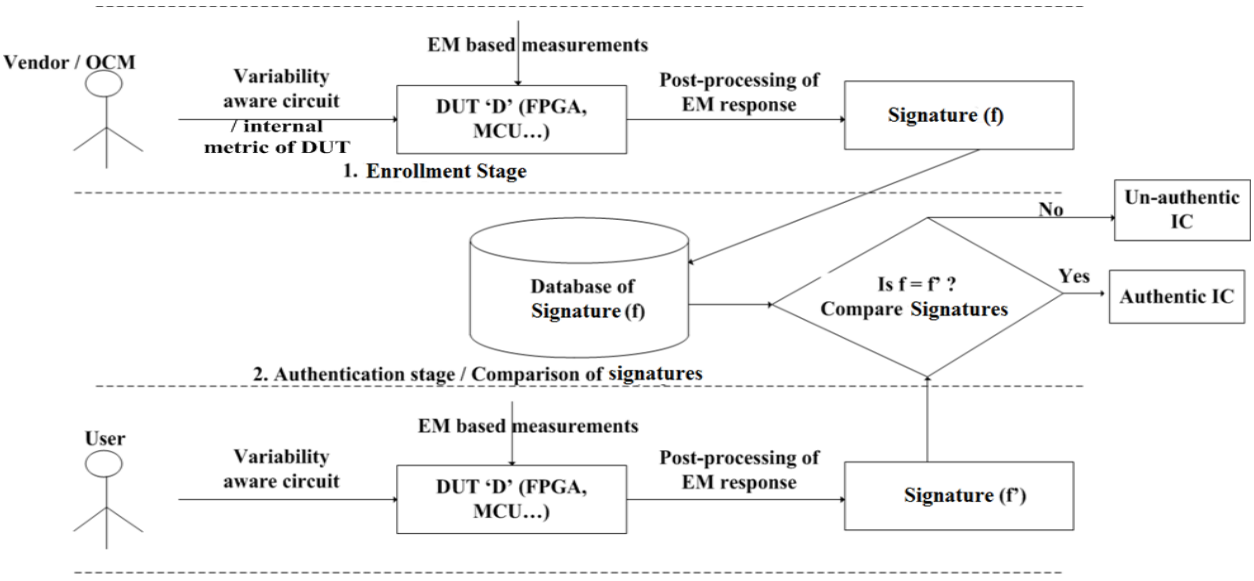


Fig. 3.3: A use case showing various steps required to implement radiated EM based authentication schemes. The vendor or OCM generates and stores fingerprints. A user can use same authentication protocol (EM based) to authenticate the DUT.

A. Conditions for efficient authentication using REMT

For the competent and efficient implementation of the authentication metrics, it is important that the proposed methodology of REMT must have following qualities:

i. Uniqueness of the obtained EM response / signature.

ii. Reproducibility of the obtained EM response / signature.

The uniqueness here refers to the fact that generated EM response from each DUT is unique and pertains to the PV effects from its implemented VAC. This means that with high probability, responses resulting from evaluating the same challenge on different DUTs with same VAC should be dissimilar, i.e. far apart in the considered distance metric. Uniqueness is generally assessed at nominal operating conditions.

Reproducibility is defined with respect to the distribution of the response intra-distance of the entire DUT EM response, i.e. considering evaluations of EM response from same DUT. This means that with high probability, EM responses resulting from the same DUT instance should be similar, i.e. close in the considered distance metric.

After getting the information regarding the evaluations steps and conditions for efficient results, we focus our attention to the detailed description of the implemented VAC and post-processing steps utilized and needed in the efficient implementation of REMT based authentication methodology. Moving forwards we will discuss about VAC, post-processing and measurement steps along with the description of the DUTs used.

3.4.2 Variability Aware Circuit (VAC)

A variability aware circuit (VAC) is used in order to exploit the underlying effects of PV in an IC. Along with the effects of PV the other requirement for our VAC is that it should be able to emit EM emissions. To have VAC that exploits PV effects and as well emit EM emissions, a ring oscillator (RO) circuit is chosen. Indeed RO circuit can be used as a VAC, as it is sensitive to the effect of PV. It is also a viable choice to create EM emission which is function of PV[1]. The implemented RO circuit exploits spatial form of variability. As also discussed in [4], the spatial variability comes due to manufacturing errors, such as random dopant fluctuations, lithographic errors, geometric variation in transistors and interconnects, and so on, which affects the Vth (threshold voltage) and output capacitances of the RO circuit transistors. The voltage Vth and output capacitances affect the switching speed and propagation delay of the transistors of each inverter of RO circuit [10].

The RO typically consists of an odd number of inverters (delay elements) in a cycle. The last stage of the RO is connected to the first stage as a feedback which causes a sustained oscillation by the circuit. For a sustained oscillation, the ring must provide a phase shift of 2π, where each inverter stage provides a phase shift of π/n (where n is number of inverters), the another π phase shift comes from DC inversion and the gain at frequency of operation should be unity [11].

[1] It is not always necessary that there is need of external circuit to be embedded that works like a VAC but rather internal circuit state or configuration could also be used to exploit the PV. This is validated through our work on MCUs in which there is no external VAC but rather an internal circuit feature is used to exploit PV effects.

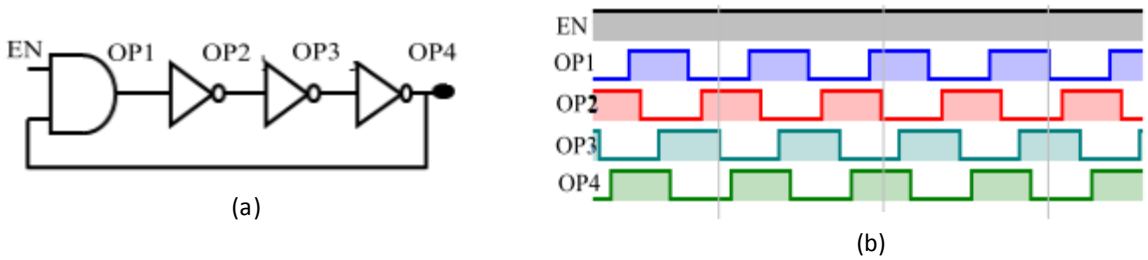


Fig 3.4: Three-stage RO. (a) Circuit diagram of three-stage RO. (b) Timing diagram of three-stage RO.

A single inverter with the feedback does not provided enough phase shift for a sustained oscillation because of which RO must have minimum of three inverters. From [4][5], the variation in the frequency of oscillation in RO is related to device parameters like transistor switching speed and the capacitive load of the next step. In this work we have implemented a 3 inverter RO with an AND gate as shown in Fig. 3.4(a). The equation for frequency of the RO circuit considering the delay due to inverter and an AND gate, can be given by [11][12]

$$fn = 1/(2\ (n\ td + \tau\ )) \qquad (2)$$

where

n is the number of inverters;

td is the propagation delay due to a single inverter;

τ is the delay due to the AND gate.

The post-layout response of the timing diagram from RO circuit of Fig. 3.4(a) is given in Fig. 3.4(b) - highlighting the effects of delays of each elements and interconnects.

A. EM Emission from Ring Oscillator

A CMOS inverter consists of PMOS and NMOS transistors and its operation depends upon the switching of the transistors from one logic state to another as also shown in Fig. 3.5. The switching from one logic state to another causes change in voltage level of logic which results in current flow (from Vdd to output and output to ground – see Fig. 3.5), this in turn produces magnetic field from the inverter circuit. From Fig. 3.5 an input-output waveform is depicted for an inverter circuit. It is clear from Fig 3.5 that whenever there is switching of the voltage, a current is generated resulting in magnetic field (EM emission). The

frequency of the RO is related to device parameters like transistor switching speed and the capacitive load of the next step.

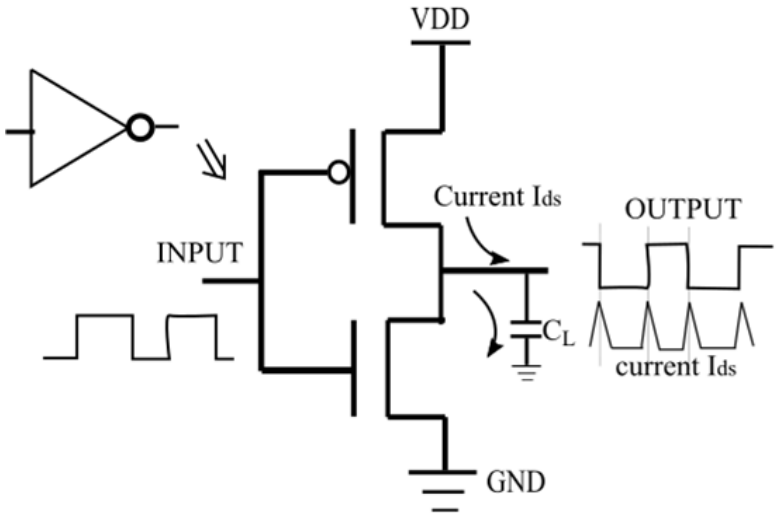


Fig 3.5: CMOS inverter with input-output waveform and output current (Ids).

The transistor switching speed depends upon the Vth and geometry (L and W) of the transistor [9][10]. Capacitive load is affected by geometry and area (L and W) of the transistors. With the dependency of RO frequency on the device parameters, we aim to observe a variation in the frequency even when RO is implemented in two similar ICs.

From (2), it is clear that the number of inverters is inversely proportional to RO frequency which is also shown in Fig. 3.6. The spectral response in a bandwidth ranging between 100 and 800 MHz, for three different configurations of RO circuit is shown in Fig. 3.6. The peaks seen in Fig. 3.6 corresponds to the switching activity of the RO circuit, it is directly proportional to the frequency of operation of the RO circuit. These responses are an earlier measurement in which an EM emission from the RO circuit is captured using H-field probe. The detailed steps of measurements in given in the section below (section 3.5). In this bandwidth range (100-800 MHz), the spectrum of RO fundamental frequency, the first and second harmonics are shown in Fig. 3.6. As the order of harmonic increases, the magnitude of signal decreases which is also clear from Fig. 3.6. In this study, we have used only the fundamental frequency of the RO circuit.

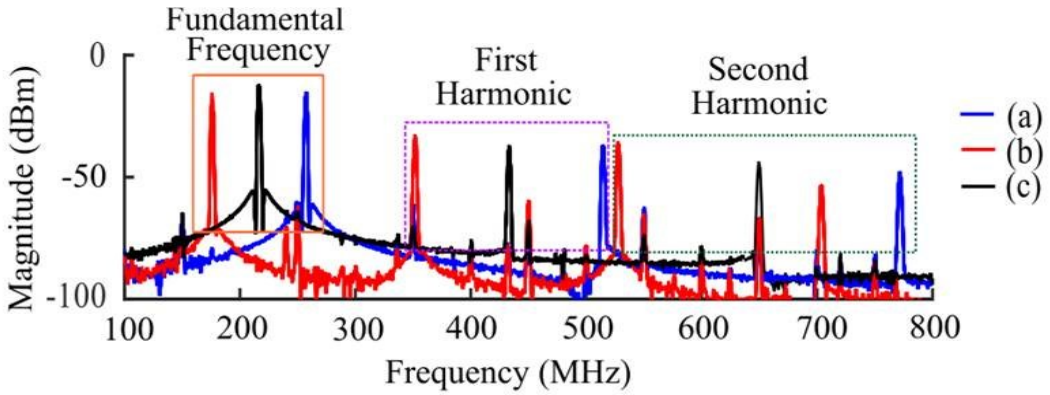


Fig 3.6: Frequency of RO for varying interconnects lengths and no. of stages of inverter (showing fundamental frequency as well as the higher harmonics). (a) A 3-stage inverters RO (b) A 5-stage inverter RO (c) A 3-stage inverters RO with longer interconnect length between logic elements.

3.4.3. Post-processing steps for REMT

The post-processing approach is used to quantify the data obtained after the measurements and experimentations. The use of post-processing approach is that it generates signatures from the measured response. This response can be analog in nature and the results may not be able to give required information for the purpose of authentication. Secondly, for the authentication purpose it is important to find a statistical distribution that shows the probability of error. For the authentication purpose, the generated response of an entity is checked against a list of previous enrolled responses. An authentication attempt is respectively expressed as the False Rejection Rate or FRR, and as the False Acceptance Rate or FAR of the system. FAR expresses the security of an authentication system. FRR on the other hand expresses the robustness or usability of a system [13]. For a usable authentication system, both FAR and FRR need to be as small as possible.

There are many techniques to understand and study the similarity between the datasets. Techniques like correlation, Euclidean Distance, Cosine Similarity etc. are used to quantify the similarity of two data sets. Cosine similarity calculates the score between the two data sets, higher the score more similar are the data sets [14][15]. We have used cosine similarity (CS) as our post-processing tool to quantify the similarity in the datasets of two devices under test (DUT) spectral response. From [15], CS gives a score based on the similarity of two vectors in higher dimensional space. Understanding mathematically from (3), suppose

X=[x*1*,x*2*...x*n*] are the EM response after measurement of one DUT and Y=[y*1*,y*2*...y*n*] of another DUT. From Cosine similarity yields a score calculated by:

$$CS(X,Y) = \frac{X.Y}{||X||||Y||} \qquad (3)$$

CS based computation uses the comparison between data sets obtained after repetitive measurements on same DUT and between two different DUTs. The term **I**ntr**a**-**D**evice **V**ariation (IADV) is used here to compute the correlation between datasets obtained from the repeated measurements of one particular DUT. And for the comparison among different DUTs over repetitive measurements, **I**nt**e**r-**D**evice **V**ariation or IEDV is used.

3.4.4. Devices under test (DUT) and measurement steps

A. Devices under test (DUT)

For the first part of investigation of REMT based approach for authentication FPGAs have been selected as DUT. In later part of the study we have also deployed microcontroller unit (MCU) as DUT. But in this part of chapter we have focused on the description, measurement and results from FPGA. FPGAs are powerful devices in terms of flexibility and programmability.

Before giving more description about interaction of RF and FPGA with RO circuit, we have first highlighted in brief about the FPGA and its internal structure. This is done in order to understand the placement and routing of the programmed circuits. As in this study we are dealing with the effects of physical effects of process variation so it is important to have an understanding of the internal physical and electrical structure of FPGA.

B. Field Programmable Gate Array (FPGA) - an overview

Field programmable Gate Arrays (FPGAs) are pre-fabricated silicon devices that can be electrically re-programmed in the field to function as different circuits or logic elements in various applications [36]. FPGAs provide cheaper solution and faster time to market as compared to Application Specific Integrated Circuits (ASIC) which normally require a lot of resources in terms of time and money to obtain first

device or prototype [35]. Any changes incorporated in the final product can be easily upgraded by downloading a new application bitstream [36]. However, the flexibility of FPGA is also the major cause of its draw back. Flexible nature of FPGAs makes them significantly larger, slower, and more power consuming than their ASIC counterparts. These disadvantages arise largely because of the programmable routing interconnect of FPGAs which comprises of almost 90% of total area of FPGAs. But despite these disadvantages, FPGAs present a compelling alternative for digital system implementation due to their less time to market and low volume cost. Normally FPGAs comprise [16]

- Programmable logic blocks which implement logic functions.
- Programmable routing that connects these logic functions.
- I/O blocks that are connected to logic blocks through routing interconnect and that make off-chip connections.

After understanding the basics of the FPGAs the next subsection here details about the interaction of RF and EM waves with FPGA. The different aspects involved in generating EM responses from FPGA i.e. measurement setup, steps and results from the measurement etc.

3.5. EM emission from FPGA – Measurements and Results

It has been shown in [11] that a periodic oscillating RF signal can even be generated inside that component. The signal frequency can be higher (up to 500 MHz) than the ones typically used for classical operations. One way to detect this RF signal is to use a magnetic probe placed just above the FPGA. The idea here is to observe that the RF signal produced by the FPGA can be used for authentication purpose in the RF domain. Indeed, ring oscillator (RO) circuit is a variability-aware circuit because the oscillating signal frequency it generates is sensitive to the manufacturing induced PV in IC. It is one of the commonly used oscillator circuit in RF applications and has the advantages of power efficiency, low area occupancy of chip, and rail to rail voltage swing [10]. The oscillation of RO circuit depends upon switching speed of the transistors of inverter.

In our measurements, two different families (technologies) of FPGAs from Xilinx® are considered: ARTIX-7 (28 nm) and SPARTAN-3E (90 nm). ARTIX-7 from Digilent Nexys 4 and SPARTAN – 3E

from Digilent NEXYS 2 boards has been used. From [8], as the CMOS scales down sub-90-nm technology, the effect of PV is more noticeable. Our aim is to observe the effects of PV on RO in two different families of FPGA and determine which gives a higher degree of uniqueness or distinction in the signatures. Frequency of RO circuit in two families differs because of the difference in switching speed of transistor (28-nm FPGA would switch faster), internal routing structure of each family and other layout difference in the IC. A single RO circuit is placed at the center of FPGA and the probe is moved over several positions.

To extract the EM emission from the FPGA, an H-field near-field RF-U 5–2 probe from Langer EMV Technik GmbH is used (also depicted in Fig. 3.8(a)). The RF-U 5-2 H-field probe is designed for detecting magnetic fields at broad conducting paths, cables, connectors, electronic components and their connections. The probe functions like a coupling clamp. The RF-U 5-2 is a small and handy, passive near-field probe. For best coupling, the probe head should be positioned directly onto the component. Field lines from other sources entering the probe laterally or in a straight line are also detected. It has a current attenuating stealth and its upper side is electrically shielded. It can be connected to a spectrum analyzer or an oscilloscope with a 50 Ω input [17]. The technical parameters of the magnetic probe used are shown in Table 3.1.

Table 3.1: Description of the EM probe

Frequency Range	*30 MHz ... 3 GHz*
Resolution	*~ 5 mm*
Probe head dimension	*~ (6 * 6) mm*
Max forward power	*1 W*
Connector – output	*SMB , male , jack*

3.5.1 Measurement setups for REMT based approach

A complete flow of the measurement steps is depicted in Fig. 3.7. From the measurements it is observed that we have used two different families of FPGAs – SPARTAN-3E (90nm) and ARTIX-7 (28nm) and performed exactly same measurement steps.

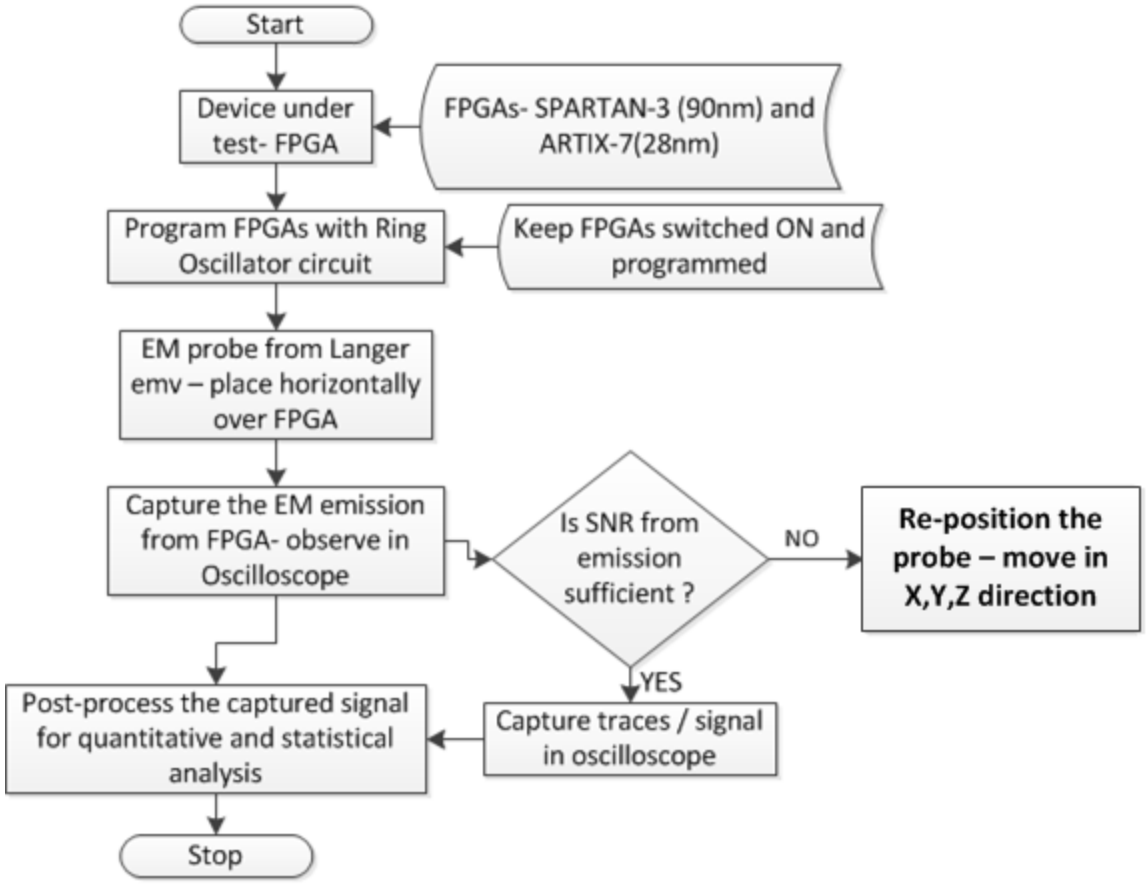


Fig. 3.7: A complete flowchart describing the measurement steps performed for capturing the EM emission from the FPGA DUTs.

Referencing from measurement flowchart in Fig. 3.7 all the FPGAs - devices under test - are programmed with one RO circuit, preferably placed at the center of the FPGA. For programing we have used Xilinx ISE and VIVADO (depends on the FPGA technology). The RO is manually placed (programmed and placed using constraints files) in the FPGA. The input of RO or enable of the AND gate (from Fig. 3.4(a)) is controlled from external switch on the FPGA board.

Also given in Fig. 3.7 the magnetic field probe is oriented horizontally to measure the field emitted vertically from the FPGA IC. In order to get good signal strength the probe is placed as close to the FPGA as possible (touches top of FPGA IC). Measurements are repeated 15 times to see the robustness of the result. The spectrum range is observed up to 2 GHz with 64 points averaging. A movable bench setup is used which allows the near-field H-probe to move in X,Y,Z directions, to find the spot over FPGA where

the signal to noise ratio (SNR) of EM emission due to the RO is maximum. A summarized description of the devices, technology and measurement repetition is given in Table 3.2.

Table 3.2: Description of devices under test used in the EM measurement.

DUT description	**Number of devices**	**Technology**	**VAC used**	**Measurement repetitions**
SPARTAN- 3E	8	90nm	Ring Oscillator (3 stages)	15
ARTIX - 7	4	28nm	Ring Oscillator (3 stages)	15

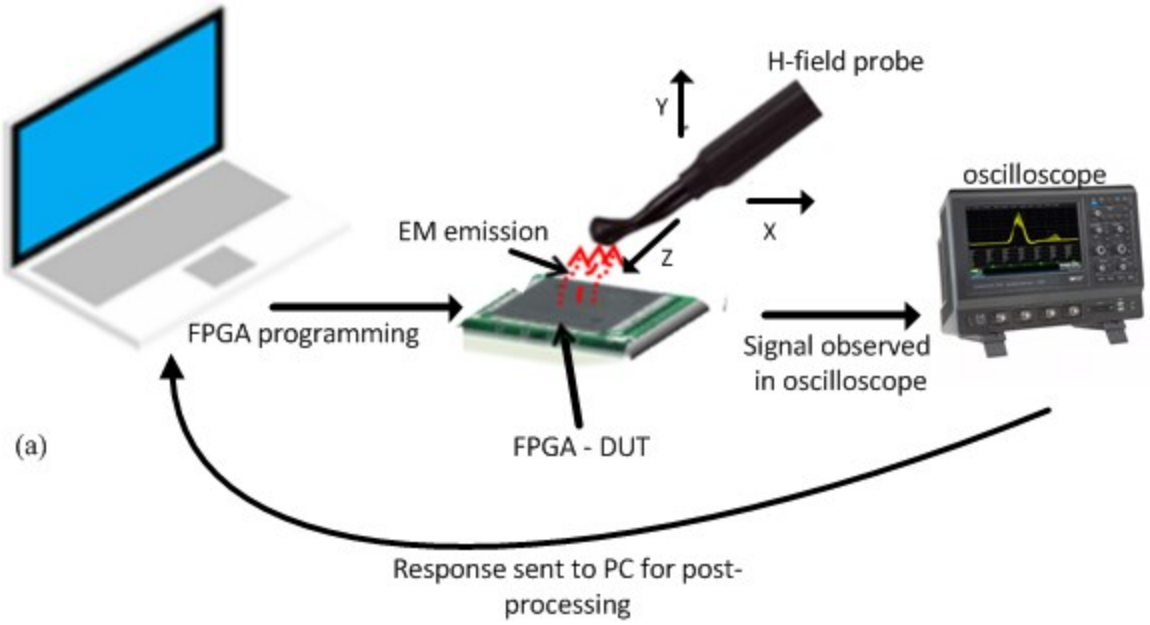
A complete schematic of the measurement setup has been depicted in Fig. 3.8(a). From Fig. 3.8(a), a setup for preforming the measurement setup is shown which highlights different equipment and instrument setup required along with the DUT. Different equipment and instruments used are:

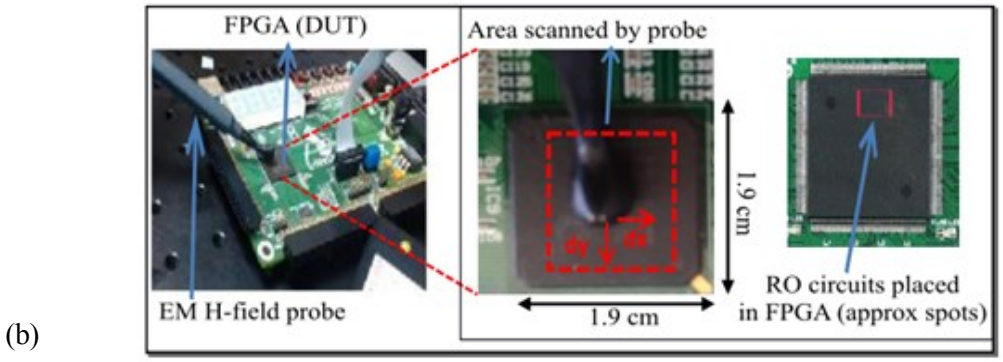
***Probe station*:** this contains a setup that holds the DUT (fixed up) and an EM H-field probe. The table allows the H–field probe to move in XYZ direction.

Oscilloscope – for acquiring the signals from EM emission. In this work we have used Teledyne Lecroy™ oscilloscope which has bandwidth of up to 4 GHz.

H-field probe – to capture the EM signals from the DUT and The placements and orientations of the H-field probe placed horizontally over the FPGA has been depicted in Fig. 3.8(b). From Fig. 3.8(b), the placement of RO circuit and the dx, dy area scanned by the H-field probe has also been depicted. All FPGAs of same family were fixed on same spot and the H-field probe was moved in X, Y, Z directions. This is done in order to have homogeneity in measurements.

The same measurement setup has been used in preforming the experiment over both the FPGA devices. The total number of devices for ARTIX- 7 is 4 and for SPARTAN - 3E is 8. All the FPGAs have been new and there is no results biasing due to usage or aging of the device. This method can be efficiently adapted to mitigate or detect the counterfeiting of new FPGA techniques like overproduction, supply chain theft, cloning, remarking etc.





(b)

Fig 3.8: Measurement setup: FPGA board with probe (a) REMT measurement steps employed in the study with different instruments. (b) Inset: area scanned by H-field probe in XY-direction, where dx = dy = 1 mm is the unit distance and approximate spot, where RO circuit is placed in the FPGA.

After understanding about the required measurement setups that would accentuate the performance of experimental and provide a successful and efficient results, the next part of this chapter focuses on the analysis of results from the two FPGA families used to conduct this study.

3.5.2 Results: ARTIX- 7

As seen from (2), three-stage RO gives maximum frequency of oscillation; taking this into consideration we have implemented a three-stage RO in the FPGA. The same three-stage RO has been implemented on

four different ARTIX-7 FPGAs. To reduce the area overhead, the RO was placed in a single configurable logic block (CLB). Each EM based measurement has been carried out 15 times with the setup shown in Fig. 3.8, following the same experimental protocol. Each device under test has been removed and repositioned between each measurement in order to take into account the systematic errors. With the continuous switching activity of the transistors in the RO circuit, the spectrum of the frequency has been captured.

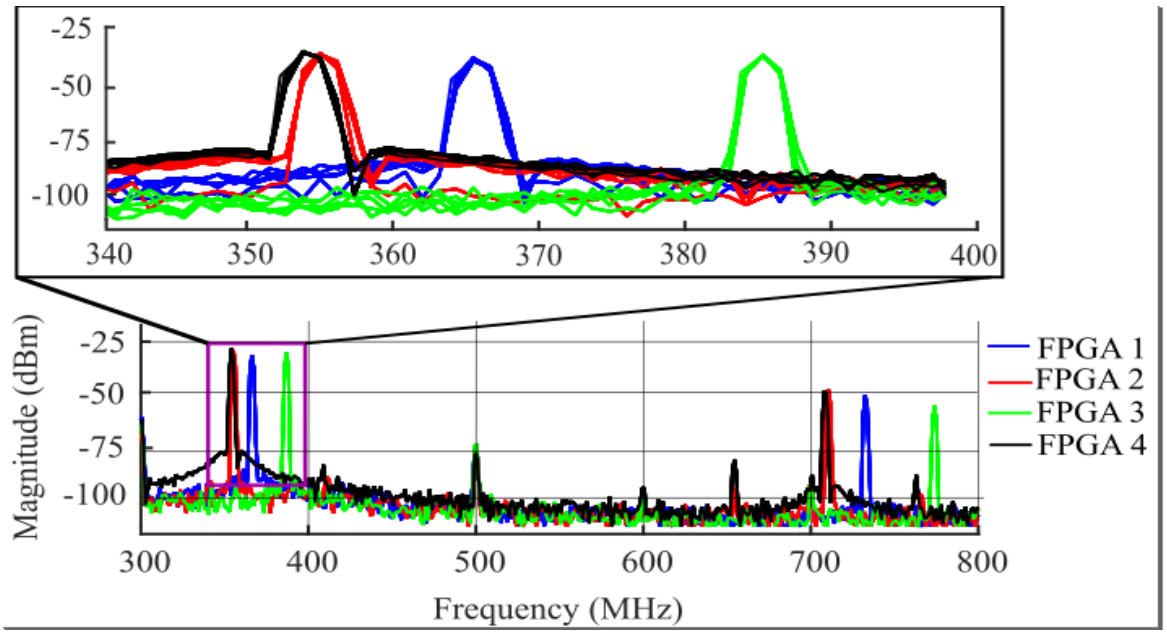


Fig 3.9: RF signals emitted by four different ARTIX-7 FPGAs with the same RO circuit in bandwidth up to 800 MHz and (inset) a zoomed-in view around the fundamental frequency peak (exhibiting the repetitive measurements).

The results of EM emission from four ARTIX-7 DUTs repeated over 15 times have been depicted in Fig. 3.9. Although the total bandwidth of the measurement performed is up to 1 GHz but Fig. 3.9 shows only the fundamental frequency of the RO circuit. This is the frequency range of our interest. From Fig. 3.9 we can observe that even the FPGAs are of same family, same manufacturer, and same age but still there is considerable difference in the frequency response of same RO circuit implemented in same spot and measured with the exact same protocol. The variation naturally comes from the effects of process variations. From Fig. 3.9 it is also observed that the difference in the frequency of the FPGA3 is much higher than from those of three other FPGAs. The difference between FPGA2 and FPGA4 are less.

All this non-deterministic variation is due to stochastic and random nature of manufacturing induced PV effects.

Table 3.3: Frequency of ARTIX-7 and SPARTAN-3E FPGAs measured in MHz for different numbers of boards in test.

Device	FPGA1	FPGA2	FPGA3	FPGA4	FPGA5	FPGA6	FPGA7	FPGA8
Artix-7	366.2	355.2	387	354	----	----	----	----
Spartan-3E	246.6	245.4	242.9	257.6	251.5	247.8	250.2	258.8

3.5.3 Post-processing of ARTIX results

To determine the results obtained in previous section for ARTIX-7 FPGAs into a quantifiable and statistically viable form, we have adopted to utilize cosine similarity as the post-processing tool. In classical PUF based approaches [11][16], mostly the Hamming distance between the obtained binary code is used.

In classical PUF based authentication approach, there is the conversion of analog output or response into binary coded format based on various metrics e.g. In RO PUF the difference between two adjacent ROs is coded as 1 or 0 based on the sign of the difference. However, we are using an RO based approach but we have used only one RO to generate a unique frequency pertaining to each FPGA. So we have not opted to utilize or convert our obtained results into binary or digital format rather we have used the above discussed cosine similarity approach to distinguish the response from various FPGAs. From now on, we use the terms **I**ntr**a**-**D**evice **V**ariation (IADV) and **I**nt**e**r-**D**evice **V**ariation (IEDV), to refer to the CS computed from two measurements performed on a single DUT, and computed from two different DUTs, respectively.

The CS has been performed on complex part of the signal which also uses phase information of the signal. The total combinations obtained for IADV is 420 and for IEDV is 1350 from 15 measurements on four DUTs. CS is performed in two spectral ranges: 1) entire range (0 to 2 GHz) of spectrum and 2) in the particular range of fundamental frequency (approximately in the window of ≈ 5-MHz centered on fundamental frequency). In both the cases, results of CS are comparable.

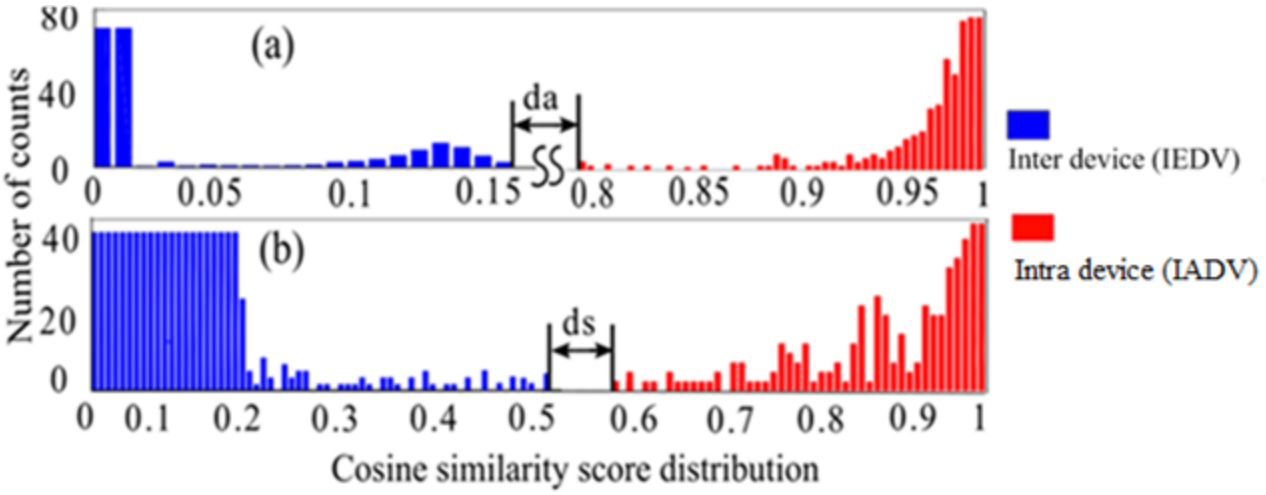


Fig 3.10: Cosine Similarity score distribution of inter and intra variability for all measurements of: (a) ARTIX-7, and (b) SPARTAN-3E FPGA.

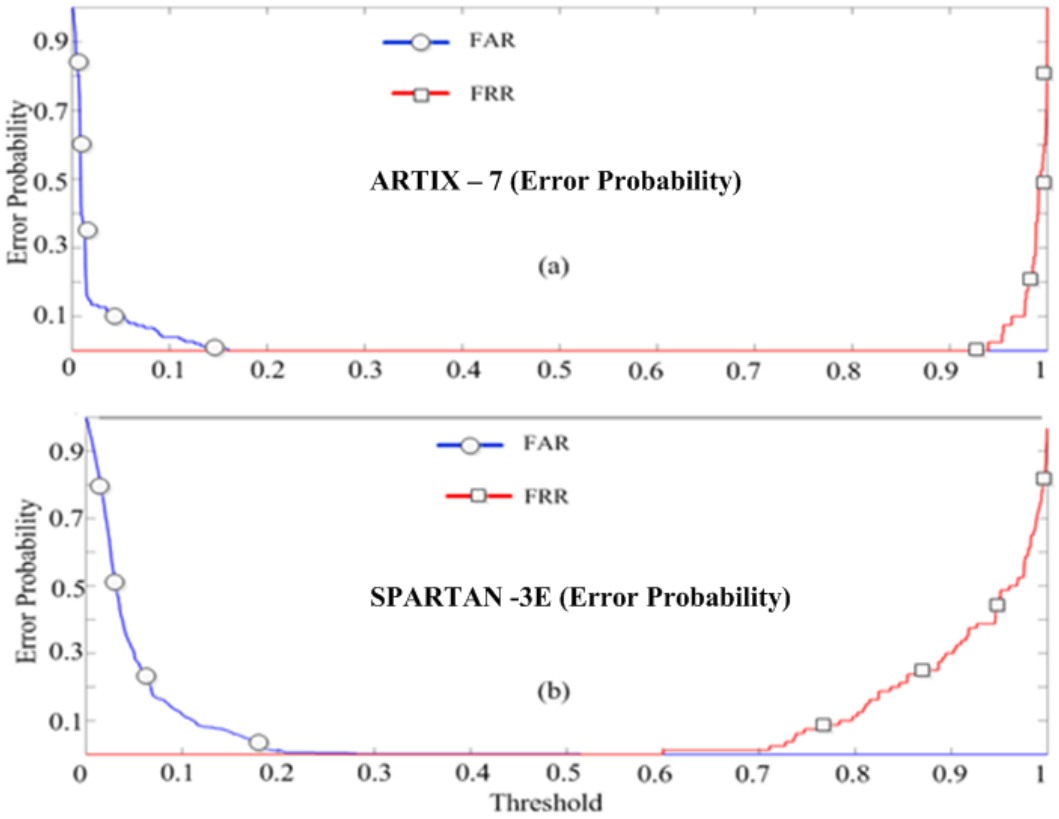


Fig. 3.11: Error probability curves depicting FAR and FRR for: (a) ARTIX- 7. (b) SPARTAN -3E.

The observed CS scores are worst case IEDV ≈ 0.16 and IADV ≈ 0.82 for each measurement of all four DUTs. Although the spectrum of DUT 2 and 4 are closer, the CS computation gives IEDV score under 0.16; this is because of high quality factor (Q-factor) of the signal. The difference between worst case IADV and IEDV distribution is highlighted with 'da (≈ 0.1)' in Fig. 3.10(a).

This determines that even the statistical overlapping of the IADV and IEDV values is not forbidden, but due to the high Q-factor of the obtained EM signals from the FPGAs, the overlap in IADV and IEDV values is null in all our measurements. Therefore, the observed error- probability is null, this validates that a single frequency of resonance to compute or extract a fingerprint is sufficient if the Q-factor of signal is high. Low error probability shown in Fig. 3.11(a), justify the fact that overlapping of FAR with FRR is approximately null, thence, the probability of judging the one FPGA with another FPGA is negligible – very efficient distinction between FPGAs of same series, manufacturers, family etc. Also, based on the results from Fig. 3.11(a), Table 3.3, and the CS score distribution in Fig. 3.10, we can interpret that each FPGA has a unique EM emission due to the effect of PV on RO circuit which can be attributed s its signature for the purpose of authentication.

3.5.4 Results: SPARTAN- 3E

The results from ARTIX-7 show that using only one RO circuit, it is possible to extract signature in form of RO frequency using the H-field EM probe. The results give an encouraging sign. The process has been ultra-lightweight and completely non-invasive. As also described in the above section that we have implemented same non-invasive approach on two different families of FPGAs. The similar measurements steps have been put into the SPARTAN-3E FPGAs. We have 8 SPARTAN – 3E FPGAs as DUT.

The same three-stage RO has been implemented on eight different SPARTAN-3E FPGAs. The spectral responses are shown in Fig. 3.12 over a bandwidth spreading from 100 to 560 MHz, show first harmonics along the fundamental frequencies of each eight DUTs. Table 3.3 shows the unique frequency values of each SPARTAN-3E FPGA. Similar post-processing steps are performed as is done in ARTIX-7 case. The CS score distribution is can be referred from Fig 3.10(b). The results obtained for the CS score is, worst case score for IADV≈ 0.5 and IEDV ≈ 0.6. Fig. 3.10(b) shows the CS score distribution of all eight DUTs, where ds(≈ 0.1) indicates the difference between the worst case of IADV and IEDV scores. Similar to ARTIX-7 case, the observed error- probability is null, this validates that a single frequency of

resonance is sufficient to compute or extract a signature that is unique, if the Q-factor of signal is high. Error probability curve is observed in Fig. 3.11(b) for SPARTAN- 3E. Low error probability from Fig. 3.11(b), justify the fact that overlapping of FAR with FRR is approximately null, thence, the probability of judging the one FPGA with another FPGA is negligible – better distinction of each FPGA characteristics based on EM emission. The total combination of IADV is 840 and the total combination of IEDV is 6300 for 15 measurements on eight DUTs.

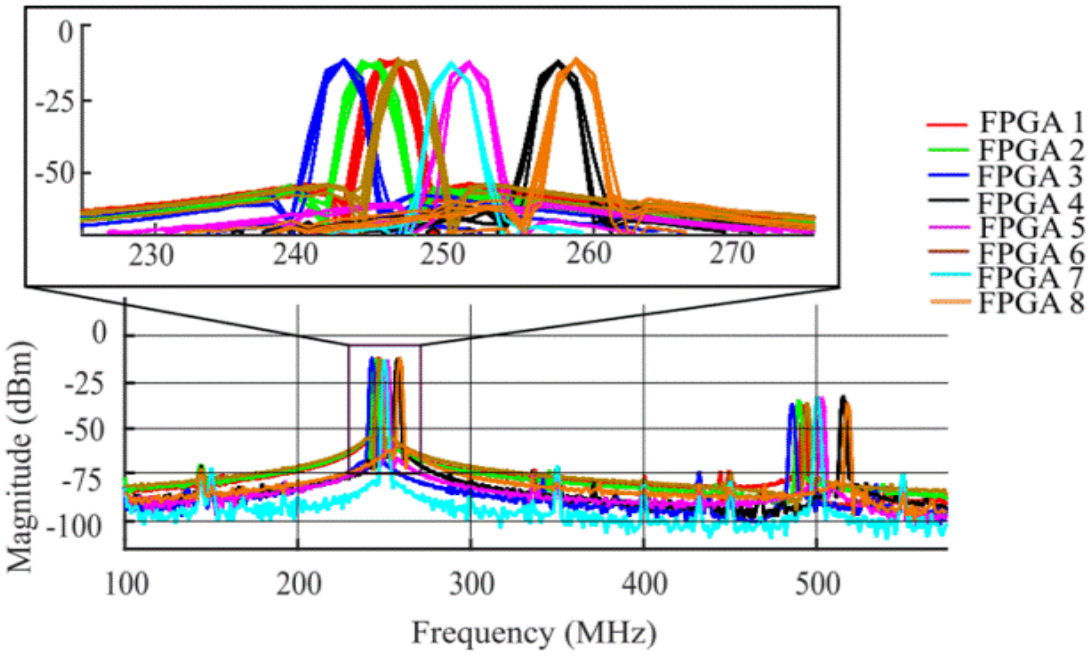


Fig 3.12: EM signals emitted by eight different SPARTAN-3E FPGAs with the same RO circuit in bandwidth up to 500 MHz and (inset) a zoomed-in view around the fundamental frequency peak (exhibiting the repetitive measurements).

3.5.5 Inferences and discussions from FPGA results

It is clearly evident that by using only one RO circuit (VAC) we are able to exploit signature for each FPGAs of two different families. The proposed methodology does not require any dedicated circuit for post-processing and even the implemented VAC is ultra-lightweight in terms of area, power and cost. By using post-processing techniques we have been able to statistically quantify the spectrum from EM radiation into usable signature for the authentication of FPGAs.

The results in the above section show that signatures can be obtained for each FPGA using EM measurement technique with a very light-weight marker and off-chip post-processing technique. To summarize some of the key features of this approach observed are:

I) Low Area usage of chip - cost effectiveness.

II) Uniqueness in response for each DUT - efficient for authentication.

III) Off chip robust post-processing.

IV) Robustness of response - shown by repeated measurements.

In comparison to the other technique like CDIR sensor or PUF based (discussed in chapter 2), the proposed used method used a very lightweight marker. FPGA is programmed with only one RO circuit and does not require any auxiliary circuit to implement the functionality. The process is non-invasive as no external signal or input has been used to perturb the circuit. There is no need to install or embed any specialized circuit; hence effort needed to implement this approach is very less.

Owing to the lightweight effort and ease of implementation, this approach can be easily used to authenticate circuits and ICs. Secondly with advent of internet of things (IoT) and scaling of IC size it is viable to employ an approach which is non-invasive and light in weight. The REMT based approach can be effective in detecting counterfeit technique like overproduction, supply chain theft, cloning and remarking. This method can be easily integrated on the user side or on the customer side. Hence it is highly possible to implement this approach for mitigating the counterfeiting of IC.

The extension of this part of the work is applied to the other semiconductor family of devices. The next section details about the usage of MCUs as DUT. We have used same principle of radiated EM emission and aim at creating fingerprints for each MCU under test. The next section details the implementation of the authentication method using REMT based technique for MCU devices.

The next section details the following two main descriptions with respect to the MCUs based implementation:

- Study of MCUs- as they have different internal structure than that of FPGAs.
- Identification of the metric / electrical / physical properties of MCU which can be used to exploit its PV effects.

3.6. MCU authentication – EM emission technique

The objective of this part is to extend the work done in FPGA part, and use the same methodology of EM emission to authenticate the Micro-controller (μC/MCU) boards. We have used new μC boards in this work. The idea is to exploit non-intrusively the design, periphery and architecture of μC such that a viable fingerprint can be obtained which can be used for authentication purpose. The term MCU and μC have been interchangeably used in this study they both refer to micro-controllers.

There is major architectural difference between FPGA and μC. Understanding from [16][19], the structure of a μC is comparable to a simple computer placed in a single chip with all of the necessary components like memory and timers embedded inside. It is programmed to do some tasks for other hardware. FPGA on other hand is an integrated circuit that could contain millions of logic gates that can be electrically configured to perform a certain task. The very basic nature of FPGAs allows it to be more flexible than most μC. Owing to the flexibility and re-programmability feature of FPGA, in REMT for FPGA, we have programmed FPGA with a variability aware circuit which exploited its underlying PV to create fingerprints for the authentication. However, μC already have their own circuitry and instruction set that the programmer must follow in order to write code for that μC which restricts it to certain tasks [18].

The main aspect in this part of work is that there has not been any extra circuitry (or marker) implemented or programmed in the μC as has been done with FPGAs in section 3.5. Unlike FPGA, we cannot make modifications of the μC to add a VAC. Instead our idea has been to directly measure the EM signals which are intrinsically emitted by the μC. The non-intrusive nature of the work compels to use only the implemented hardware and peripheral sets of μC, and utilize them such a way that they: *1)* generate an EM emission and *2)* generated EM emission is unique to each μC. The first part of this work focuses on studying and utilizing the hardware architecture of the μC to interpret a prominent EM emission. In the later part of this work we have performed post-processing of the EM response from μC boards, to get a statistical response for the authentication of the μC. This idea is extension of work done by Ahmed et.al. in [20] that has been elaborated in previous chapter.

3.6.1 Understanding MCU – DUT description

In this study, twelve STM32F103 Nucleo-64 µC boards from ST Microelectronics have been used as DUT. It has ARM Cortex processor with 128k flash memory. Among the different interesting aspects of µCs, in this study our focus is mainly on the working and understanding of clock and reset circuit. The clock of µC plays an important role when EM radiation technique is explored.

The oscillating nature of clocks emits EM radiation on powering up. It is important to distinguish the source of frequency harmonics in the µC. It will be shown later that, external reset circuit in our work plays a role to set the metric that can be used to generate fingerprints for each µC. In the succeeding sections, we will first discuss about the clock schemes and then, we move to discuss about reset, its exploitation to create fingerprints and results.

A. Clock scheme of STM32F103 µC

Three different clock sources can be used to drive the system clock (SYSCLK): i) High speed internal (HSI) clock. The HSI clock signal is generated from an internal 8 MHz RC oscillator. The HSI RC oscillator has the advantage of providing a clock source at low cost (no external components). ii) High speed external (HSE) oscillator clock generated using HSE ceramic resonator or external user clock. iii) Low speed internal (LSI) clock, generated using on chip RC oscillator [21]. Each clock source can be switched on or off independently when it is not used, to optimize the power consumption. In next subsection, the EM emission from the clock of STM32 is discussed.

B. Clock and EM emissions from µC

In this work, HSI clock is selected. It is configured to run at 8 MHz to program / configure the clock. The STM32CubeMX tool from ST Microelectronics has been used. STM32CubeMX is a graphical tool that allows an easy configuration of STM32 microcontrollers and generates corresponding initialization C code through a step-by-step process. To capture the EM emission from the µC clock, a magnetic (H-probe - as used with FPGAs in previous cases – section 3.5) from Langer emv. is used, which is also shown in Fig. 3.13. The output is observed in oscilloscope, which has bandwidth of 10 GHz, 75000 number of points, hamming window and spectrum of signal observed from 0 to 100 MHz.

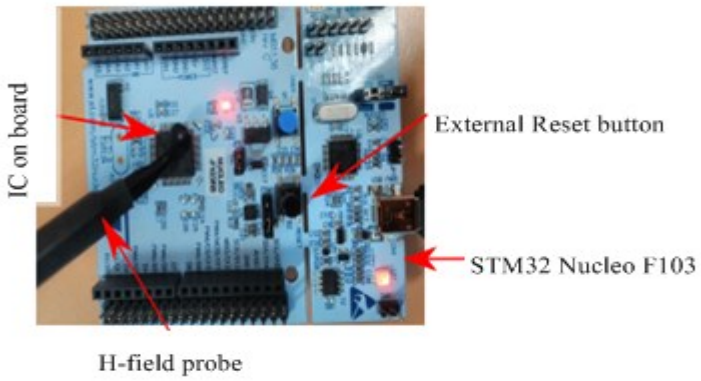


Fig. 3.13: Measurement steps for STM32 µC: Localized EM probe horizontally placed over the IC of µC board.

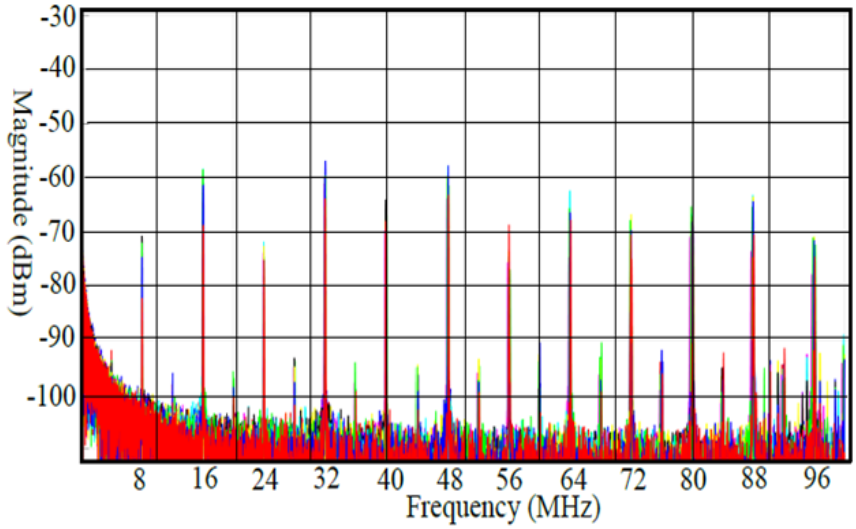


Fig. 3.14: EM emission due to clock from the different MCUs. The EM emission is captured using H-field probe and observed in oscilloscope / spectrum analyzer.

Given the small size of the IC comparable to the H-probe, there is no need to move the probe in horizontal direction to capture the high SNR value of EM emission. The emission power is reasonable in all part over the IC. So the probe is fixed at one particular place for all the measurements steps for all 12 µC boards. The HSI clock configured at 8 MHz emits EM emission at harmonics of 8 MHz as shown in the Fig. 3.14. The HSI clock is generated using RC oscillator, which do get effected by PV, but on observing Fig. 3.14, it is evident that the distinction in peaks due to HSI clock for the 12 µCs is not very clear or noticeable (all peaks superimpose on each other).

3.6.2 System reset overview for STM32F103 µC

In this part of study, we have explored and utilized external reset as a mean to produce EM emission from µC (apart from clock) and characterize it as a metric to obtain fingerprint for each µCs. Before illustrating the measurement steps and results using external reset as metric, we first discuss about the different aspects of the overall system reset of this STM32 µC family.

A system reset sets all registers to their reset values. The STM32 µC can be reset in several ways. The different ways to generate systems reset for STM32 is : 1) low level on the NRST pin or external reset, 2) window watchdog end-of-count condition (WWDG reset), 3) independent watchdog end-of count condition (IWDG reset), 4) software reset (SW reset) and 5) low-power management reset [21] [22]. An illustrated diagram of the system reset circuit is shown in Fig. 3.15.

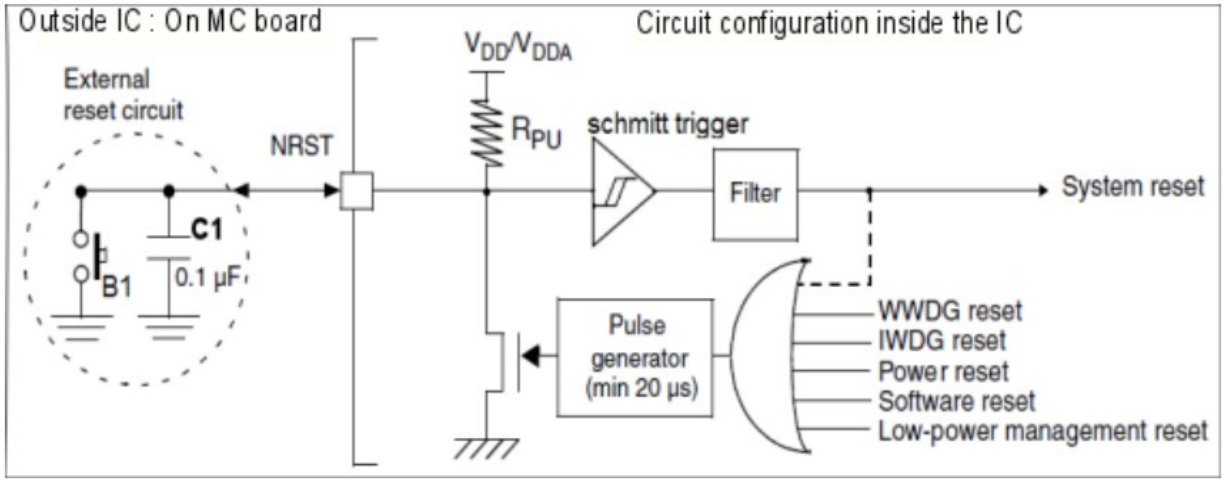


Fig. 3.15: Description of the RESET circuit of STM32F103RB.

The description in Fig. 3.15 highlights division of the reset circuit into two parts. One part consisting of resistor (Rpu), NMOS transistor, filters and Schmitt trigger are inside the ARM Cortex IC and other part consisting of capacitor, NRST and external switch outside the µP on the µC board. Although we have limited information owing to information constraints from the manufacturers.

The system reset signal provided to the device is output on the NRST pin. The pulse generator guarantees a minimum reset pulse duration of 20 µs for each internal reset source. In the case of an external reset, the reset pulse is generated while the NRST pin is asserted low. The µCs are typically specified with a

minimum reset pulse width t(rst); for a general μC, if the pulse applied does not meet the specification, the reset action may become invalid. However, the STM32 enforces proper reset by holding the reset signal universally for 20 μs. This means that if a reset is ever initiated, it is always going to do its work. Additionally, there is a Schmitt trigger attached to the input, which allows the signal to have a rather long rise/fall time [22]. After comprehending the overview of system reset that is deployed in our DUT, in the following section we focus on the working of external reset and different current switching that results in EM emission.

3.6.3 External RESET: VAC for MCU

Normally a VAC is implemented circuit in an IC which gives prudent information of the PV effects. In case of FPGA also a lightweight marker (RO) is programmed in a FPGA for PV exploitations. But in the case of MCU, no external marker been used rather the attempt has been made to exploit PV effects using the inherent physical features of the MCU itself through the use of external reset switch.

The goal in this section of the chapter is to highlight the hardware (circuit) description of each part of the external resets. This description is essential as it describes how different circuits of external reset can be utilized to generate EM emission. Owing to the PV effects on different circuit elements of reset, the generated EM emission from each DUT is unique but this is described in detail in the next section of measurements and results. External reset is activated by turning on the switch B1 shown in Fig. 3.16.

Switching on the B1 pushes NRST pin to low. EM emission occurs when there is a sudden switching of the current. The following points along with descriptions in Fig. 3.16 outlines a brief summary of the mechanisms and effects of charging / discharging of capacitor (C1) and electrical phenomenon of other circuits on activation of external reset switch B1.

- When B1 is pressed, the capacitor C1 discharges through path B1.
- The Schmitt trigger uses the hysteresis and produces a pulse at the output.
- Pulse generated from the Schmitt trigger is fed back to NMOS transistor through the pulse generator.
- The NMOS transistor when high, pulls the current down through it.
- Consecutively there is a switching of current between Rpu - C1 and C1 - NMOS.

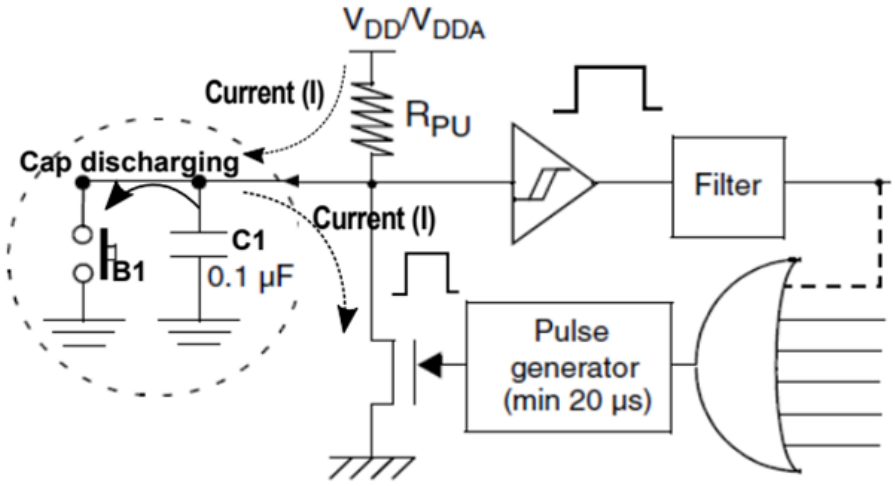


Fig. 3.16. Effects of switch B1 (external reset) on current switching in the different circuit elements of reset circuit (viz. charging discharging of capacitor).

But there could be some other effects from other parts of µC circuits on getting reset pulse, which could also play a role in the EM emission, like clearing out of the registers which could result in sudden voltage drop and hence causing sudden switching of current. The next subsection focuses on measurements steps, which makes it clear if it is possible to use external reset as a metric to generate considerable EM emission that could be used as a prudent metric for authentication.

3.6.4 EM emission results from Microcontrollers

This section details the EM emission from the 12 µCs. All the µCs are of same manufacturer, same series and of same age. Before going into details of the EM emissions and results first we discuss about the procedure to generate and capture the EM emission. The test and measurement is carried out by locally placing the H-probe on µCs and following same measurement protocols as is done when capturing the emission from clock in section 3.6.1(B). The measurement steps are discussed below:

- Program the µC boards under test (or DUT) to run with only HSI clock.
- Measure the peaks (or clock harmonics) using EM probe on spectrum analyzer.
- Press the external reset button. Once the reset button is pressed, it results in extra peaks (harmonics) generation.

- Measure the harmonics coming due to reset, and find out if these harmonics are distinct or unique for each μC.

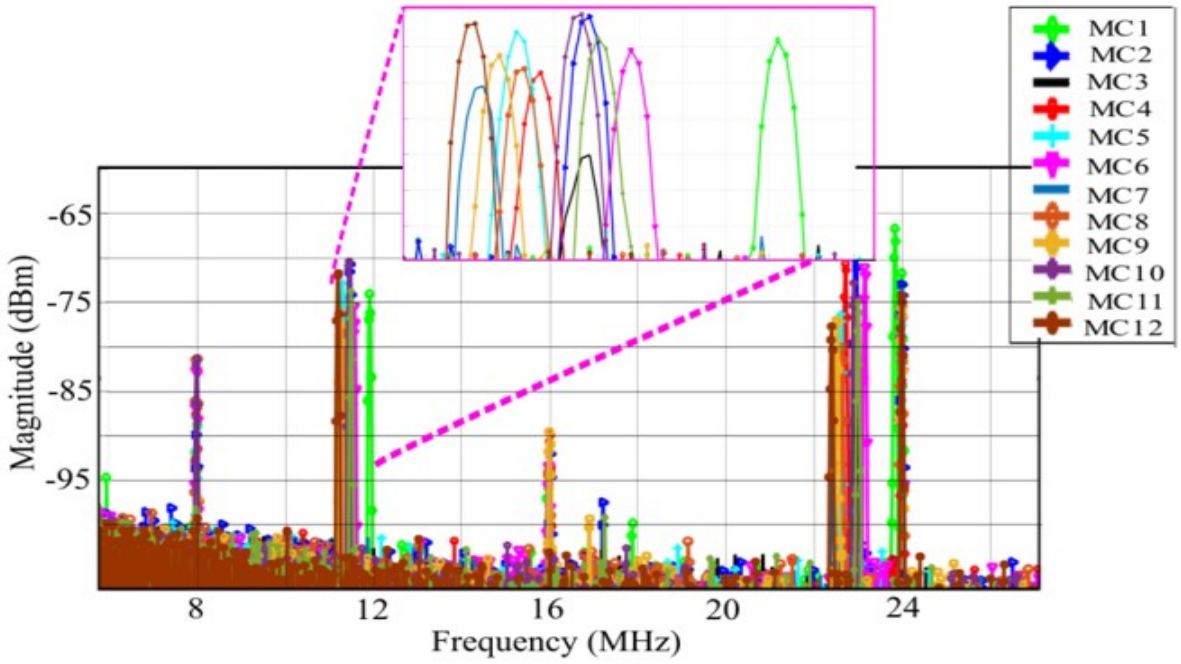


Fig. 3.17: EM emitted by 12 different MCUs (MC in legend of figure) due to external reset depicted in the bandwidth up to 25 MHz and (inset) a zoomed-in view around the fundamental frequency peak.

The measurement is carried out on 12 μCs using the above mentioned steps and the emission due to the external reset is shown in the Fig. 3.17 for all 12 μCs. From Fig. 3.17, it is clear that on using the external reset, switching of currents occurs (detailed in previous section), which gives a considerable EM emission and for each μC. The measurement is repeated five times to account for the measurement and systematic errors.

The spectral responses in Fig. 3.17 are shown over a bandwidth spreading from 0 to 25 MHz. Although the total spectral response of the measurement is up to 100 MHz, Fig. 3.17 highlights the spectral response only up to 25 MHz to show the clarity of the spectrum. In this bandwidth range, first harmonics are observed along the fundamental frequencies of each DUTs. The post-processing (discussed in next subsection) of the signal is done around the fundamental frequency of the spectrum. From the spectral responses of different DUTs in Fig. 3.17, it is evident that the frequency peaks are clearly different for all 12 μCs. Each frequency peak corresponds to a particular μC. The spectral responses for each DUT are

distinct owing to the PV effects on different circuit elements of reset circuit. Owing to non-deterministic behavior of the PV, some µCs like µC1, µC7 and µC12 vary too much while some other of them have overlapping response.

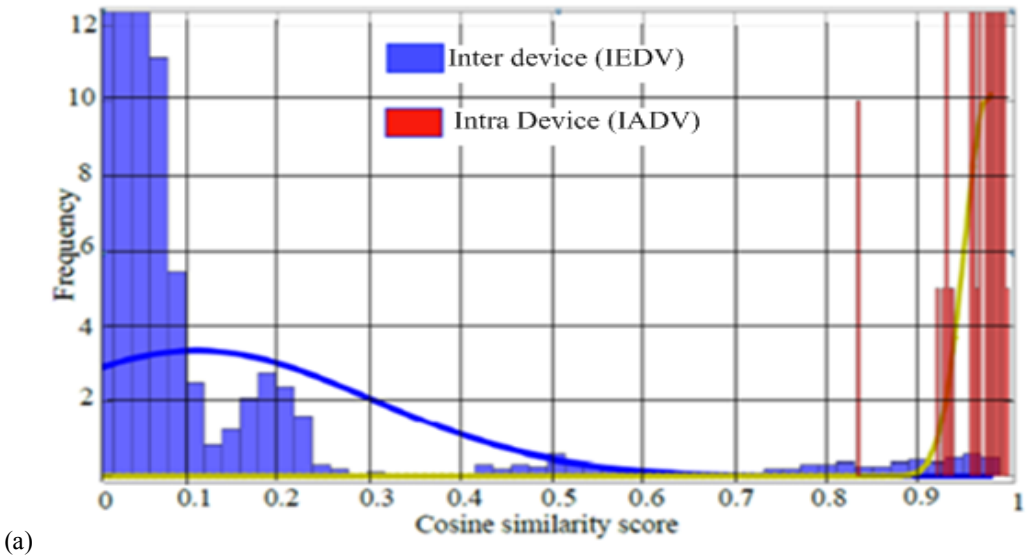
The variation in frequency response of all the 12 µCs, even if they are of same manufacturer, same family and same age justifies that utilizing only external reset, an inherent feature of µC, PV can be exploited for µCs that can be applied for purpose of their authentication. Even though it may be unclear to point out which part of µC board contributes to maximum EM emission, but this does not deter the objective of this study. As even if the large share of EM emission is outside the IC, we are still able to exploit the PV of the circuit elements of the board and use it to authenticate the whole µC board rather than only the IC (processor).

3.6.5 Statistical Analysis of results

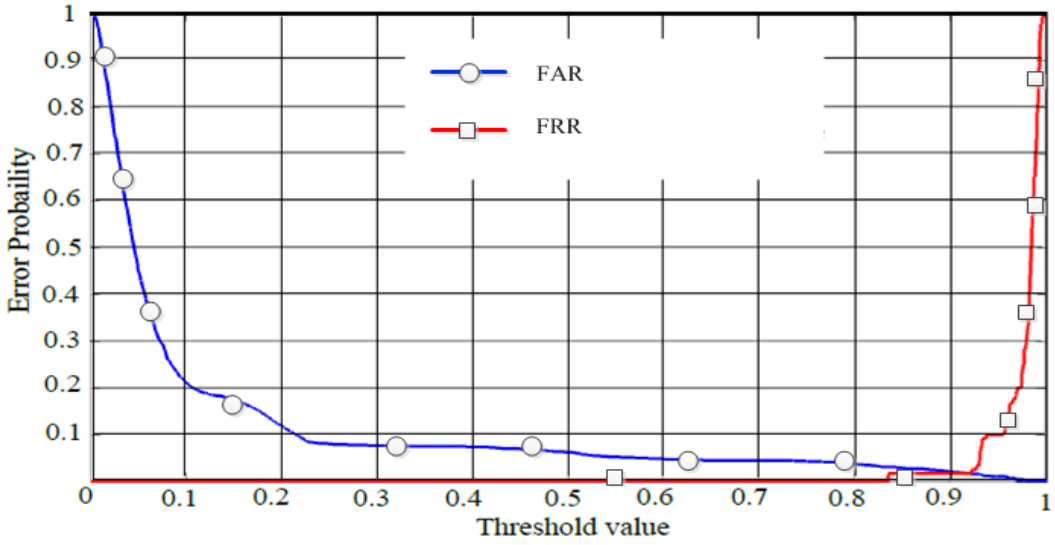
To perform the statistical post-processing on data sets (spectral response of µCs), the signal is compared in complex frequency domain where both the magnitude and phase of signal is taken into account. CS is performed in the particular range of fundamental frequency of the reset signal (approximately in the window of 1 MHz centered on fundamental frequency (11-12 MHz range)). Fig. 3.18 shows the CS score distribution, illustrating a histogram with normal distribution fit of intra and inter device variability for all 12 DUTs over repeated measurements.

Table 3.4: Mean and 3 sigma of inter and intra variability.

	Mean	3*sigma=(3µ)
Auto-Correlation	**0.977**	**0.076**
Cross-Correlation	**0.11**	**0.57**



(a)



(b)

Fig: 3.18: Statistical distribution of the inter and intra variability. (a) Histogram showing distribution of inter and intra variability. (b) Error probability curve to observe the overlap of the FAR and FRR curve.

The statistical values for **Intra Device Variability** (IADV) and **Inter Device Variability** (IEDV) are discussed in Table 3.4. The values from Table 3.4 show that the 3µ value of IADV is up to 0.076 and for IEDV is 0.57. The overlap of curves of IADV-IEDV from Fig. 3.18(a) is beyond 3µ values of IADV and IEDV values. Despite having some overlap in the frequency responses among few µCs viz. µC3 and µC4, but from Fig. 3.18(b) the overall probability of error between false positive and false negative is observed around $1.7*10^{-3}$. The high quality factor (Q-factor) of the signal is one of the major factors resulting in

low rate of error probability. The low error rate justifies the fact that using only EM emission through the switching of reset circuit, enough distinction among 12 μCs can be obtained. This can give them a signature for the purpose of authentication.

3.7 FPGA and MCU: final discussion

The results have shown that using non-invasive REMT based technique it is possible to effectively create a RF DNA or signatures of the semiconductor devices. To validate the methodology, two different families of devices (which are characteristically different from each other) have been used for the measurements.

From the section 3.5 and 3.6 we can clearly observe that EM based technique is a viable option to exploit the PV effects of ICs (viz. FPGA and μC). The obtained distinction in the frequency spectrum responses when coupled with a qualitative post-processing scheme give signatures uniquely attributed to each DUT. The obtained signatures have been distinct enough to give a very less error probability rate, which provides an efficient method for the authentication of DUTs. We have been effectively able to authenticate two different semiconductor families (FPGAs and microcontrollers) without the need of additional circuit. In both of our work, our focus has been to remain non-invasive and cost efficient. This can prove to be significant for authentication purpose by using non-invasive and low cost methods for other semiconductor products e.g. Analog ICs and other application specific ICs.

A summary of the highlights and effectiveness of the proposed EM based technique is given below:

- The proposed technique has been *cost efficient*- we have not used any dedicate external circuit or components,
- This technique is most importantly *non-invasive* in nature. No external signal sent inside the DUT that could damage the DUT.
- This technique has been *area efficient* as there is not extra dedicated circuit for post-processing technique – hence low silicon occupancy.
- This technique is *easy to implement* and effective in its operation. We have used all our measurement on the commercially available boards and did not need any extra addition to DUTs.

In the above study we have claimed that all our DUTs are new and of same age. None of them were ever

used before; hence, there are no aging related issues on any of them. However, when ICs go through various applications in the field, they are subjected to electrical and thermal stresses. These effects cause temporary and permanent shifts in the performance of ICs. In section 1 (introduction) we have given a brief introduction about the effects of the aging on the electrical response of IC. This can be detrimental in the realm of authentication.

In comparison to highly used PUF based approach, the REMT based method has advantage of being ultra-lightweight. PUF need large IC area not only for the implementation of marker circuit but also for the post-processing part. The shrinking IC size can be discouraging for OCM and companies to involve PUF as they get area and economic constraints. The PUF based approach is efficient in developing keys for authentication as well as protection of important information; however such large marker may not be optimized in the areas of IoT or lightweight IC applications. REMT based is ultra-lightweight and highly non-invasive in nature. It gives a good perspective to generate fingerprints or signatures for IC without the trouble of extensive development of layout of dedicated circuits.

The only bottleneck with this approach is that it requires specialized measurement setups. Secondly with the off-chip post-processing technique the chip or DUT cannot perform self-authentication. From use case scenario discussed previously in Fig. 3.3, we have already seen that an end user compares the fingerprints of IC with the vendor's database (authentic database) when he / she wants to authenticate it. If an IC that has undergone thermal or electrical stress (becomes old) then its fingerprint would vary considerably. In this way even an authentic IC, if subjected to authentication after a period of time can be discarded or termed as fake. Hence it has become important to determine a metric that can keep the fingerprint of IC constant throughout its lifetime. In the next chapter we have reviewed and described in detail about an EM based technique that has been adopted to mitigate the aging related effects on ICs.

References:

[1] A. Wild, G. T. Becker, and T. Güneysu, "On the problems of realizing reliable and efficient ring oscillator PUFs on FPGAs," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2016, pp. 103–108.

[2] A. Maiti, I. Kim, and P. Schaumont, "A Robust Physical Unclonable Function With Enhanced Challenge-Response Set," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 333–345, Feb. 2012.

[3] S. Ghosh and K. Roy, "Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era," *Proc. IEEE*, vol. 98, no. 10, pp. 1718–1751, 2010.

[4] A. Aryanpour and G. E. Cowan, "A circuit design and fabrication approach to address global process variation," in *Circuits and Systems, 2009. MWSCAS'09. 52nd IEEE International Midwest Symposium on*, 2009, pp. 455–458.

[5] K. Qian, "Variability modeling and statistical parameter extraction for CMOS devices," PhD Thesis, UC Berkeley, 2015.

[6] Zhang XiaoWen and En YunFei, "The HCI effect reliability evaluation of CMOS process," in *2014 IEEE International Conference on Electron Devices and Solid-State Circuits*, Chengdu, China, 2014, pp. 1–2.

[7] A. Chenouf, B. Djezzar, A. Benadelmoumene, and H. Tahi, "Deep experimental investigation of NBTI impact on CMOS inverter reliability," in *2012 24th International Conference on Microelectronics (ICM)*, Algiers, Algeria, 2012, pp. 1–4.

[8] N. K. Huang *et al.*, "Electromagnetic emissions from the ic packaging," in *Electrical Design of Advanced Packaging and Systems Symposium (EDAPS), 2012 IEEE*, 2012, pp. 65–68.

[9] "EMC at IC Level - Part 2: Determination of IC EM Emission Characteristics," *Interference Technology*, 05-Dec-2011.

[10] B. Nikolic *et al.*, "Technology variability from a design perspective," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 58, no. 9, pp. 1996–2009, 2011.

[11] S. Docking and M. Sachdev, "A method to derive an equation for the oscillation frequency of a ring oscillator," *IEEE Trans. Circuits Syst. Fundam. Theory Appl.*, vol. 50, no. 2, pp. 259–264, Feb. 2003.

[12] M. Bhushan, A. Gattiker, M. B. Ketchen, and K. K. Das, "Ring Oscillators for CMOS Process Tuning and Variability Control," *IEEE Trans. Semicond. Manuf.*, vol. 19, no. 1, pp. 10–18, Feb. 2006.

[13] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2012, pp. 302–319.

[14] S. Mare, M. Baker, and J. Gummeson, "A study of authentication in daily life," in *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, 2016, vol. 6.

[15] "Cosine Similarity - ML Wiki." [Online]. Available: http://mlwiki.org/index.php/Cosine_Similarity. [Accessed: 04-Oct-2018].

[16] "fpgas_for_dummies_ebook.pdf." [Online]. Available. https://www.amiq.com/consulting/misc/free_pdf_books/fpgas_for_dummies_ebook.pdf

[17] "Overview all near field probes Langer EMV-Technik GmbH.pdf."[Online]. Available: https://www.langer-emv.com/fileadmin/Overview%20all%20near%20field%20probes%20Langer%20EMV-Technik%20GmbH.pdf

[18] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[19] R. M. Sweeney, C. Spagnol, and E. Popovici, "Comparative study of software vs. hardware implementations of shortened Reed-Solomon code for Wireless Body Area Networks," in *2010 27th International Conference on Microelectronics Proceedings*, 2010, pp. 223–226.

[20] M. M. Ahmed *et al.*, "Radiated Electromagnetic Emission for Integrated Circuit Authentication," *IEEE Microw. Wirel. Compon. Lett.*, vol. 27, no. 11, pp. 1028–1030, Nov. 2017.

[21] "STMMicro1.pdf." [Online]. Available: http://www.st.com/content/ccc/resource/technical/document/datasheet/33/d4/6f/1d/df/0b/4c/6d/CD00161566.pdf/files/CD00161566.pdf/jcr:content/translations/en.CD00161566.pdf.

[22] "en.STM32F7_System_RCC.pdf." [Online]. Available: https://www.st.com/content/ccc/resource/training/technical/product_training/group0/c8/9e/ff/ac/7a/75/42/d1/STM32F7_System_RCC/files/STM32F7_System_RCC.pdf/_jcr_content/translations/en.STM32F7_System_RCC.pdf

4. Effects of aging on authentication of FPGA using REMT based approach

Objectives and Preliminaries

Parameters such as temperature or supply voltage cause variations in delay that are orders of magnitude greater than the manufacturing variations we are interested in. Owing to this fact, in this chapter, we investigate the effects of aging or thermal stress on the FPGA fingerprints or signatures that have been used for the purpose of their authentication. The thermal stress is a part of temporal variability and results in accelerated aging of the device. Thermal stress causes ramifications such as negative bias thermal instability or NBTI and hot carrier injection or HCI that significantly affect the performance of CMOS transistors [1][2]. This chapter is dedicated to the understanding the effects of aging on the CMOS devices (in our case: ARTIX-7, 28nm CMOS). Primarily with this we have also investigated the effects of aging on the REMT based authentication metrics. In order to be useful in practical security applications, the fingerprint or signature generated by the REMT based method should be reliable or stable (i.e., not change over time). It is relatively well known that aging and environmental variations lead to performance degradation. This chapter is committed to study of aging effects and proposing aging resistant mechanism for REMT based technique for authentication. The understanding of the CMOS aging mechanisms is first presented. Then, the effects of aging on the REMT based authentication approach is study and the procedure used to mitigate the aging effects on REMT based authentication metric is finally proposed.

4.1 CMOS Transistor Aging Mechanisms

CMOS devices suffer from the following aging related phenomenon: HCI, BTI, and TDDB stress under standard digital operating conditions. These phenomenons happen over a period in which transistors are used in field (for various applications) and get subjected to various form of temporal variability. TDDB or time dependent breakdown is permanent damaging mechanism which can be split up into two stages [3].

The first stage is called soft break down (SBD). With time, traps in the gate oxide are generated and these traps eventually form a conducting path through the oxide. Once a conducting path has been established, new traps are generated due to thermal damages. The new traps result in higher currents, the temperature in the oxide is further increased and even more traps are formed. This condition is called thermal runaway and finally leads to a hard break down (HBD) and the transistor suddenly fails. The phenomenon that electrons carry metal atoms along a wire is called electro-migration. Electro-migration causes shorts or opens in signal wires and especially in supply wires [4]. These phenomenons – TDDB and electro-migrations - are equally effective in disrupting the functionality of IC (transistors). Their detailed analysis in this thesis is not carried because our aim has been to investigate the effect of drift related aging phenomenon that are common problem whenever ICs are powered ON or used.

Aging effects that cause a parameter drift or changes degrade the transistor characteristic, which in turn, leads to a degradation of the gate performance. Hence, it is important to consider the drift-related aging effects for an aging or temporal analysis. The two dominant effects that cause a parameter drift are the negative bias temperature instability (NBTI) and the hot carrier injection (HCI). Both effects are described in detail in the following subsections.

In this thesis, our aim is to describe and investigate the effects of HCI and NBTI related effects on the authentication methods. However, before divulging into the details about that, we have first highlighted in brief about the two mechanisms with examples.

4.1.1 Negative Bias Temperature Instability (NBTI)

NBTI is considered as the most severe form of the deterministic effects of the aging on CMOS technology. NBTI only affects PMOS transistors. The stress mechanism of NBTI is a negatively biased gate terminal with respect to source and drain. The main impact of NBTI on a PMOS transistor is the increase of the absolute value of the threshold voltage. A PMOS transistor has a negative threshold voltage. Due to NBTI the threshold voltage becomes more negative. The convention is to say that NBTI increases (the absolute value of) the threshold voltage |Vth|. NBTI is accelerated by an increased temperature and an increased supply voltage, but a stronger and faster effect is produced by their combined action [1][5].

As the operating voltage increases, the negative bias of the PMOS transistors increases, which in turn

increases the NBTI degradation. Scaling of technology node leads to high electric fields at the gate, causing NBTI. Higher operating voltages result in higher electric fields across the device junction resulting in higher stress.

The effect of NBTI worsens at an elevated temperature. Typical stress temperatures range from 80°C to 250°C, encountered during burn-in [6]. During extremely high performance applications, possibly at the highest operating frequencies, the higher toggling activity of signal nets can result in formation of local hot-spots inside the chip's functioning major parts, resulting in an elevated temperature in some parts of the chips.

4.1.2. Hot Carrier Injection (HCI)

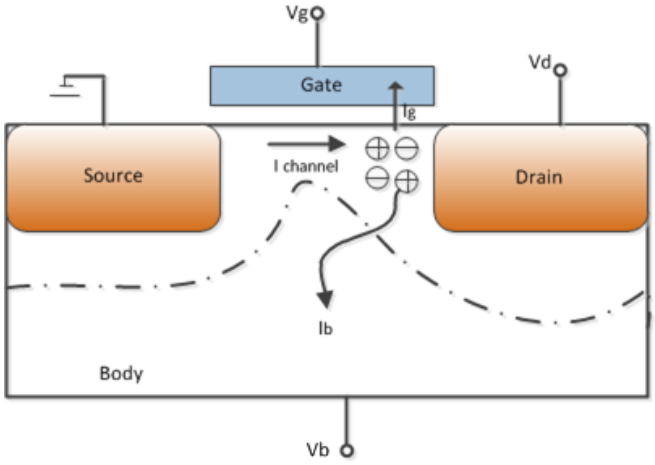


Fig.4.1: HCI based aging mechanism in a NMOS CMOS based transistor.

HCI has become less prominent with the reduction of operating voltages, but it remains a serious concern due to the large local electric fields in scaled devices [2]. Hot carriers (i.e., those with high kinetic energy) accelerated toward the drain by a lateral electric field across the channel lead to secondary carriers

generated through impact ionization[2] (see Fig.4.1). Either the primary or secondary carriers can gain enough energy to be injected into the gate stack. This creates traps at the silicon substrate/gate dielectric interface, as well as dielectric bulk traps, and hence degrades the device characteristics such as the threshold voltage (Vth). These "traps" are electrically active defects that capture carriers at energy levels within the bandgap. Like NBTI, HCI effects can also be accelerated by increased voltage and temperature. A pictorial depiction of the HCI based mechanism in a NMOS is given in Fig. 4.1.

4.2 Effects of NBTI and HCI on the digital circuit

Static CMOS logic is the primary design style used in digital integrated circuits. Every CMOS logic gate consists of a pull-up and a pull-down network. Those complementary networks represent two switches, with exactly one switch being closed for every input combination. A pictorial depiction of effects of HCI and NBTI on a CMOS based inverter is shown in Fig. 4.2.

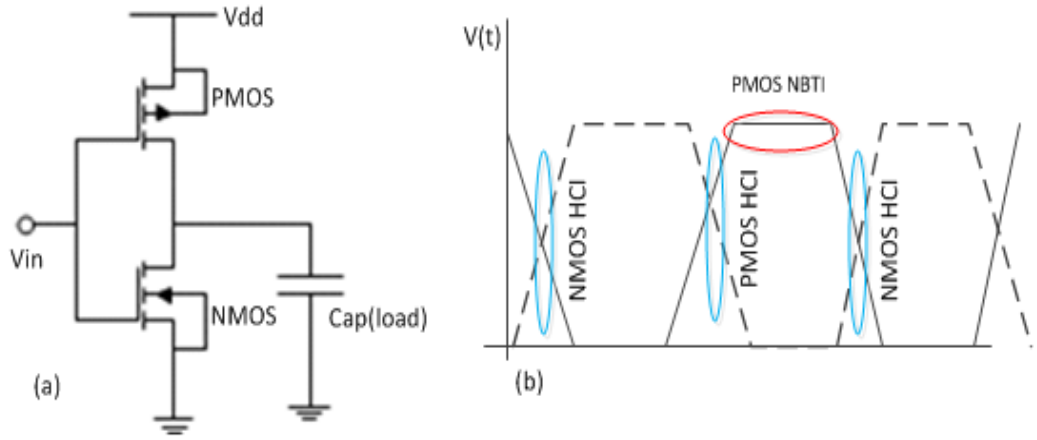


Fig. 4.2: Various stages of inverter outputs showing the effects of HCI and NBTI. (a) A basic CMOS inverter circuit design depicting NMOS and PMOS. (b) Effects of HCI and NBTI on the digital output of the inverter.

[2] Impact-ionization is a three-particle generation process. Carriers that gain high energies while traveling through high field regions undergo scattering events with bonded electrons in the valence band. The excess energy is transferred to this electron which is lifted into the conduction band creating a new electron-hole pair. This secondary electron-hole pair can also have a rather high energy. In this case the avalanche effect is triggered and the carrier density increases heavily.

The pull-up network, composed of PMOS transistors, is connected to the supply voltage VDD (logic "1") and the pull-down network, composed of NMOS transistors, is connected to ground (logic "0"). The gate delay is determined by the time the pull-up/pull-down network takes to recharge the output capacitance.

The simplest logic gate is the inverter. Its pull-up and pull-down networks just consist of one transistor. From Fig 4.2 various aspects of the input-output relation and effects of two major aging phenomenon i.e. NBTI and HCI are depicted on a CMOS inverter circuit. The stress time window for NBTI and HCI is illustrated in Fig. 4.2 for an inverter circuit. This stress time window is characterized by the device duty cycle, which is application specific. Furthermore, NBTI degradation has a well-known recovery sub-process when the stress is released [7].

NBTI only affects PMOS transistors, hence, only the pull-up network is degraded. This increases the gate delay just for a falling input transition. In a digital operation, NBTI degrades the output slope as well. The output slope of the preceding stage serves as the input slope for next logic gates. If the input slope degrades, the gate delay increases as well. Due to this, the gate delay for a rising input signal can increase as well. For HCI, a strong lateral electrical field is needed that accelerates the carriers in the channel. This is true for the NMOS transistor of the inverter (see Fig. 4.2) when a rising transition is applied to the inverter input. When the signal at the input is still logic "0", the NMOS transistor is in its non-conducting and the PMOS transistor is in its conducting state. The drain of the PMOS transistor is at VDD, the voltage drop and the electric field across the transistor are maximal. As soon as the NMOS transistor begins to conduct, hot electrons are generated which damage the transistor.

As discussed in previous chapter, a ring oscillator (RO) circuit used as variability aware circuit or VAC in FPGA authentication. A RO circuit is composed of inverter in a feedback loop as discussed in details in previous chapter. From Fig. 4.2, it is clear that a logic circuit composed of logic inverter gates is affected by both NBTI and HCI effects. The electrical phenomenon generated by HCI and NBTI are:

- The defects as created by HCI in turn lead to shifts in the electrical characteristics of the transistor such as a shift of the Vth, the current factor β and the output conductance g_o.
- Vth shift due to the HCI effects follows a power law model.

NBTI is typically observed as a Vth shift after a bias voltage has been applied to a MOS gate at elevated temperature. It is evident from the above three points that the most prominent effected phenomenon due to stress and aging of CMOS is its threshold voltage (Vth). The Vth voltage is primary factor that dictates when a particular transistor switches ON. It is the minimum voltage required to create conducting

channel. From Fig. 4.3, depiction of the increase in the Vth voltage has been shown. This clarifies that the aging effects increases the Vth which in turn can slow down the speed of turning ON the transistors.

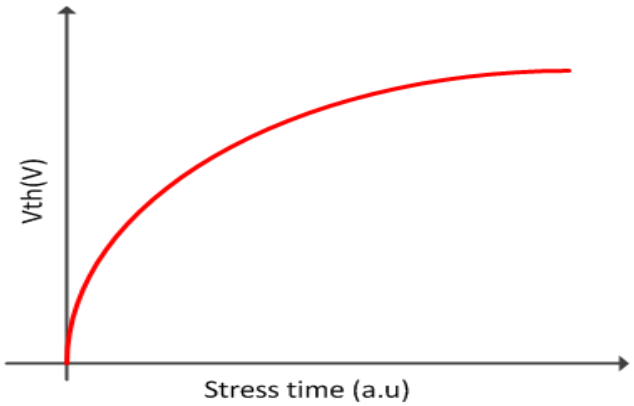


Fig. 4.3: Effects on the Vth voltage due to the aging phenomenon such as HCI and NBTI. The effect is modeled with power law time dependence.

The slower speed of conduction or switching speed of transistors can affect the frequency of operation in a RO (CMOS inverter based circuit) circuit. With the aging the transistor switches slowly and that can impact the logic switching in a RO circuit which can ultimately lead to slower operational frequency. This can severely impact the fingerprint creation for the purpose of authentication.

The next sections give an insight on the effects of the aging and elevated stress on the fingerprint creation using REMT method. Furthermore along with the problems that aging causes on the fingerprint creation and ultimately on the authentication metrics.

4.3 Effect of aging on the authentication of FPGA using RO

The idea here is to find the effects of aging on the REMT based authentication method (discussed in chapter 3) by accelerated aging the FPGA. The results or response from single RO is examined and it is determined if one RO technique is suitable enough to keep the signature of FPGA stable as it gets older (used in field). After discussing the results from single RO, we have detailed the idea of using multiple

ROs that can be more effective in terms of dealing with the aging effects. A use case scenario describing the effects of aging on the authentication using REMT method is shown in Fig. 4.4.

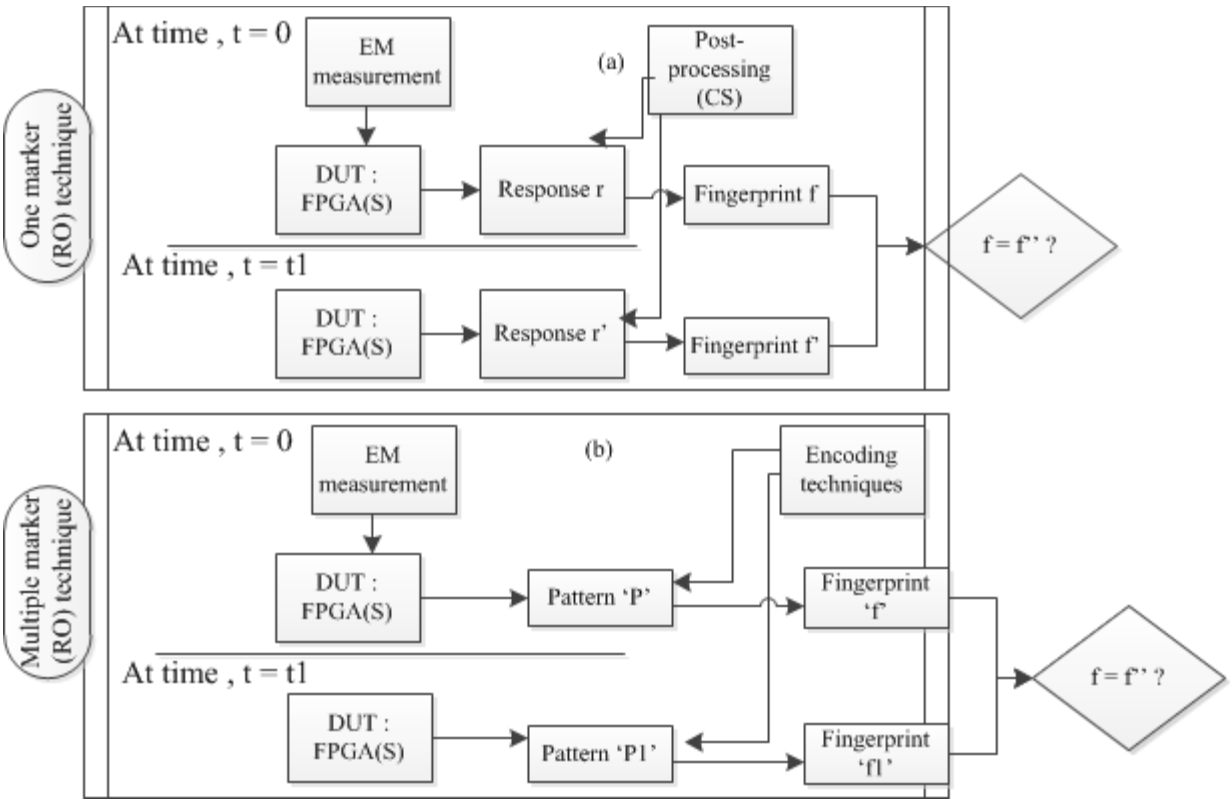


Fig. 4.4: A use case scenario we have defined explaining the effects of aging on the authentication methodologies. (a) One RO technique is depicted and its subsequent responses with and without aging effects. (b) Multiple ROs technique is depicted along with the responses with and without aging effects.

The use case of Fig. 4.4 is divided into two phases:

- Single RO radiated EM technique for authentication (REMT) method at time t = 0 (when FPGA is new – Fig. 4.4(a)) and at time t= t' (when FPGA is old). In this stage, the same measurement is performed on FPGA with one RO in both the conditions – new and old. The signatures are compared of both conditions.

- Multiple RO REMT method at time t = 0 (when FPGA is new) and at time t= t' (when FPGA is old – Fig. 4.4(a)). Similar to single RO technique, here also the measurement is carried out in

both conditions –new and old and the signatures are compared. The post-processing technique in this case is different owing to the fact that number of ROs is more.

To highlight the effects of aging on the single RO REMT, an accelerated aging mechanism has been setup. The effects such as HCI and NBTI are the prominent factors that affect any digital IC as they get older. Hence, it is important to understand which parameters or factors can depicts or mimic these effects with the growing age of IC.

Before going into details about the use of the multiple REMT approach, the effects and drawbacks of single RO REMT is discussed. From [6], it is stated that with the use of single RO PUF, the effects of the aging can give unwanted impact on the RO frequency.

Understating from the use case scenario depicted in Fig. 4.4, the scenario of using single and multiple ROs for the authentication when the aging effects are taken into consideration. The measurement, post-processing techniques and results from use of single ROs in FPGAs have already been discussed in chapter 3. The signatures from the single RO (in Fig 4.4(a)) are compared when the FPGA in both cases i.e. when FPGA is new and when the same FPGA gets old. On comparison it is decided if the technique is effective and results have enough confidence to claim that the single RO technique can generate robust signature from FPGA even after it is old.

From Fig. 4.4(b) multiple RO techniques have been described. The FPGA is programmed with multiple ROs and their EM signatures are captured when they are new as well as when they are old. The results are compared and it is determined if the multiple RO technique is effective or not. A detailed understanding of the measurement steps on both single and multiple RO along with the accelerated aging technique is discussed in detail in the following sections.

The next sub-section describes about the single RO based measurement results in both new and old conditions of same FPGA. The sub-section details out the aging related experimental setup and how the results of single RO is effected by the thermal stress (or aging).

4.3.1 Single RO REMT and aging effects

As a recap from previous chapter (chapter 3) on REMT, in the initial measurement to capture EM emission from FPGAs, only one RO circuit is programmed in all the FPGAs. The H-field probe is place

horizontally over FPGA and the response is captured in oscilloscope / spectrum analyzer. The RO circuit in all the FPGAs is of same configuration, number of delay elements and interconnect length. The response from a single RO on four FPGAs is depicted in Fig. 4.5. All results are of ARTIX-7 (28nm CMOS) FPGAs.

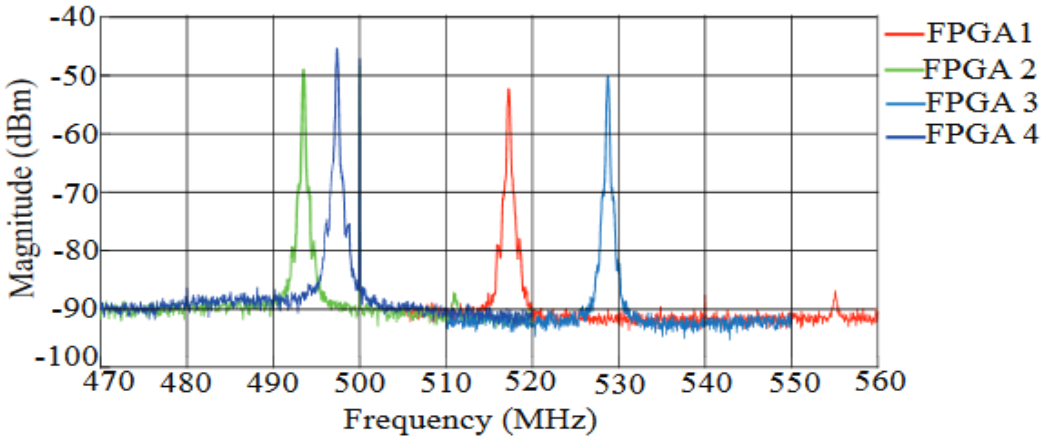


Fig 4.5: RO frequency obtained using radiated EM emission of four ARTIX-7 FPGAs when fresh (no aging effects).

The results of Fig. 4.5 highlight a recap on the results from the four ARTIX-7 FPGAs with single RO using REMT method. This is done in order to review how the single RO frequency shifts with the effects of aging the results in the Fig. 4.5 are from FPGAs which do not have any aging effects (new FPGAs).

The challenge here is will the RO frequency (subsequently fingerprints of FPGAs) of the four FPGAs remain constant, after the FPGAs have been aged or stressed? The temporal variability effects like NBTI, HCI etc. determines the challenges posed on FPGAs fingerprints over the time. To understand the effects on fingerprints when FPGA is in stress conditions, we have performed an analysis in the next section.

To observe the effects of stress on FPGA and subsequently on the fingerprints, we have performed thermal stress on one FPGA. The next subsection describes the measurement steps and the results performed for the accelerated aging of FPGA.

4.3.2 Measurement steps of accelerated aging

The aging mechanisms such as HCI and NBTI are majorly caused by two factors such as thermal stress and voltage stress. In this work, the voltage stress has not been applied owing to some constraints (our DUT was not adaptable to change the voltage supply) only elevated thermal stress has been applied on the IC (FPGA). Along with the thermal stress the RO has been left in operational mode. This type of measurement is optimized to track the effects of the HCI and as well as the NBTI effects.

The measurement setup to perform accelerated aging by thermal stressing of the FPGA is shown in Fig. 4.6. The FPGA under stress is subjected to high temperature of 85° C in a hot plate and covered with a lid to have a constant temperature stress over the board. The temperature of the FPGA under stress is monitored using infra-red thermometer. The temperature of FPGA is found to be close to 83-84° C. Total duration of the aging measurement is of two weeks.

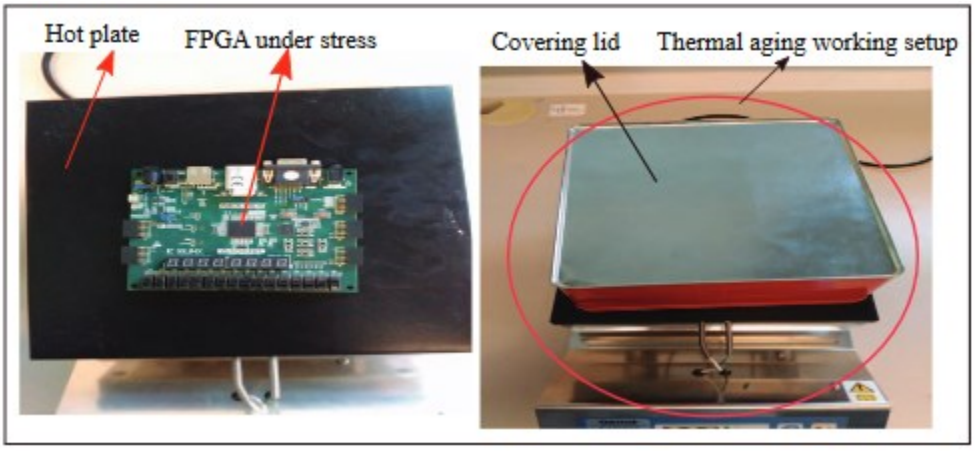


Fig. 4.6: Experimental setup adopted to age the FGPA through accelerated thermal stress.

The following points elaborate the steps implemented to do the accelerated aging of FPGA using thermal stress:

I. FPGA to be stressed (aged) is selected.
II. Before the aging process starts, FPGA RO frequency is measured under normal temperature.
III. Put FPGA under the stress condition with the RO powered ON and running.
IV. Keep FPGA under the stress condition for 48 hours continuously.
V. Measure the frequency of the RO; before measurement the FPGA is taken out of stress condition and is allowed to cool down to room temperature.
VI. Keep the FPGA back in stress condition.

VII. The same procedure is repeated for 14 days of time which is approximate to 4 years aging of FPGA [48].

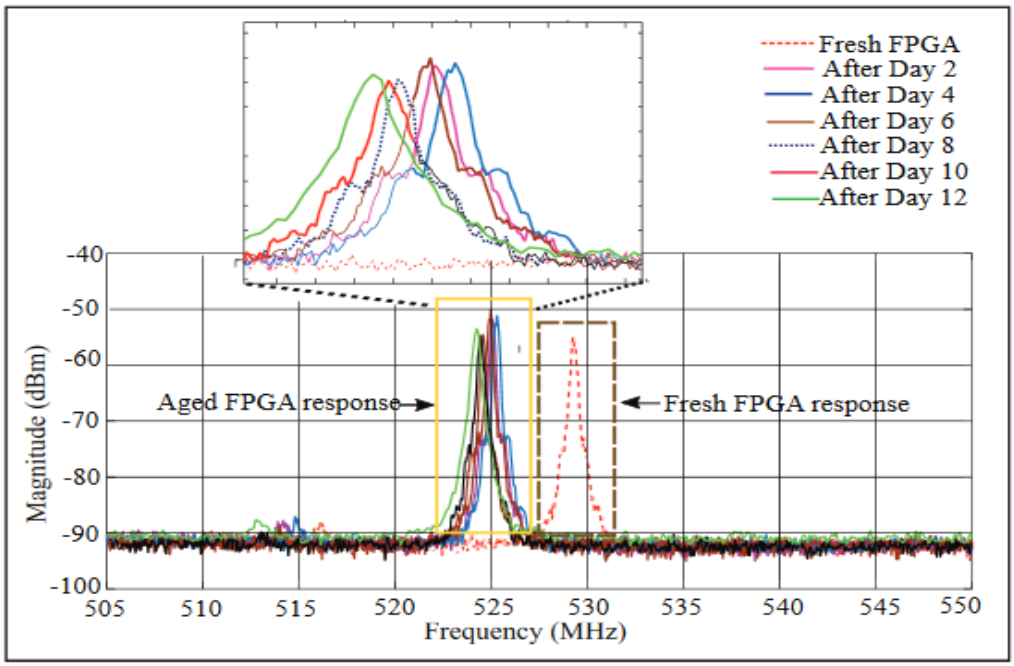


Fig. 4.7: Shift in RO frequency with aging. The insert zoom shows a zoom on the RO frequency after accelerated aging.

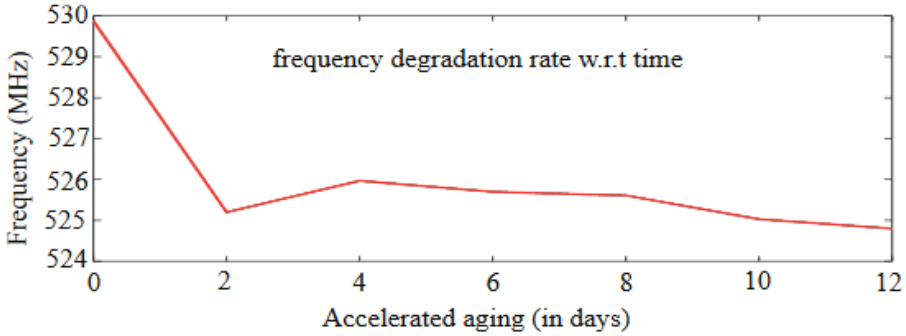


Fig. 4.8: RO frequency degradation curve of frequency with time.

From Fig. 4.7, we see that the RO frequency shifts with the aging of the FPGA. There is a considerable change in the frequency when the FPGA is new and when it is stressed for the first time. After the subsequent days of aging stress, the frequency degradation becomes constant. A graph showing

degradation rate of frequency versus time of aging has been plotted as shown in Fig. 4.8. Studies in [8] have also discussed that the degradation rate of newer and fresh FPGA is more than that of old and used FPGA.

Observing from Fig. 4.7 we observe the change in the absolute value of RO frequency. Due to the change in the absolute magnitude of the RO frequency with respect to time (aging), absolute magnitude of RO frequency cannot considered as a reliable metric for the purpose of authentication of the FPGA. The RO frequency values of even authentic FPGA or DUT when subjected to PVT effects or aging effects can deviate from its original value (when it was new). This deviation can lead to discard of the authentic FPGA or DUT. Hence we can observe that due to usage of absolute magnitude, the authentication metric may fail to give a robust and stable outcome with respect to process and temporal variations.

To overcome this, we propose to use relative methods based on digital metrics which are quantifiable and do not change with time. Multiple ROs are then stressed/aged by following the same measurement procedures as described in the above sections. The obtained results from the multiple RO approach are then treated with the relative method based encoding schemes which produces a quantifiable data from the EM response from the four FPGAs.

4.3.3 Multiple RO REMT and measurement

A multiple ROs technique has been investigated in this sub-section. The idea of multiple ROs is to implement an aging resistant mechanism that can be deployed in order to utilize the REMT based authentication methods even when FPGAs are not new under various process and temperature conditions. The multiple ROs also exploit the intra-die variations (as also studied in [9)] in FPGA, which leads to different characteristic frequencies on the same FPGA for different ROs. Intra-die variability is the spatial variation in the physical characteristics of the same IC or die due to the effects of process variations.

For our measurement and experimentations we have deployed 16 ROs. The number of ROs is not very strict. It depends upon the application, setting of the ROs etc. to increase or decrease the number of ROs. In our case, we have 16 switches (external) on FPGA board; hence it was convenient to control the 16 ROs externally through these switches. Of course with the higher or lower number of ROs, the essence of the, methodology and its results will not be greatly impacted.

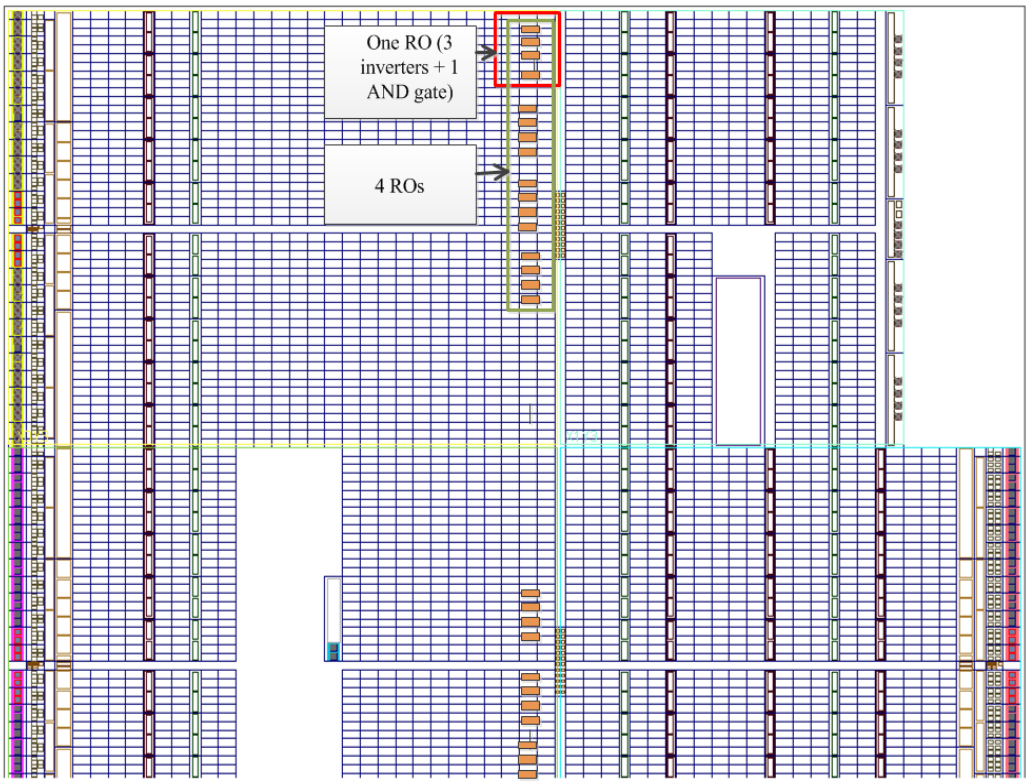


Fig. 4.9: A pictorial depiction highlighting the placement floor plan of FPGA that is used to place 16 ROs manually across the FPGA.

Each 16 ROs is of identical length, placed across the FPGA (ARTIX-7: 28nm technology). A pictorial depiction (for better understanding) of the 16 ROs placement is shown in Fig. 4.9. Fig. 4.9 highlights the floor-planning of FPGA that is used while placing the ROs manually. Due to the intra-die variability in the FPGA, no two identical ROs in the same FPGA have exact same RO frequency [9]. We have harnessed this property for the authentication using REMT based method in our published work in [10].

Similar measurement setup is used for the measurements of 16 ROs (multiple ROs) as is done in the initial measurements of REMT based method also briefed in section 4.3.1. To capture the EM response, at a time only one RO is enabled keeping all other ROs in OFF state. To understand the procedure of enabling one RO at a time, we can refer to Fig. 4.10. Suppose RO1 is enabled, then until all the measurement steps are done and results captured in spectrum analyzer for RO1, the other ROs are not enabled. This is done in order to avoid any interference or coupling effects which may arise when multiple ROs are enabled at the same time. The process is then repeated for all the subsequent ROs.

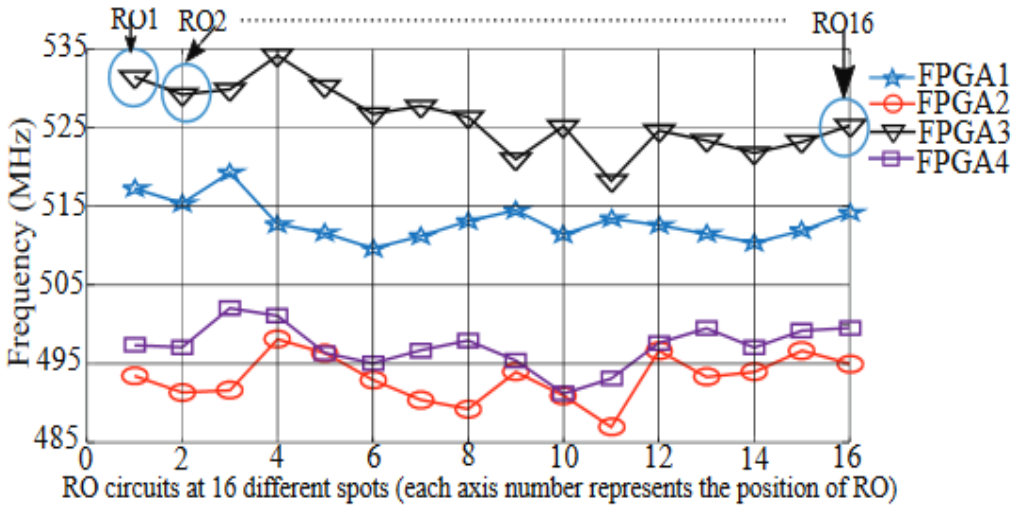


Fig. 4.10: Pattern (response) of 16 RO frequencies for four FPGAs. Each FPGA has distinct pattern due to 16 ROs (intra-die variability).

Measurement results of 16 ROs frequencies from four FPGAs are depicted on Fig. 4.10. We can clearly that the frequencies of resonance of ROs for each FPGA are different. The difference in the RO frequencies even if they are on the FPGA comes from the effects of intra-die variability. After understanding the response of multiple ROs we have focused on finding its suitability against aging effects in the section below.

4.4 Effects of aging on multiple ROs technique

In this section we have subjected one FPGA with multiple ROs subjected with the thermal stress. The exact same measurement steps have been performed as shown in Fig. 4.6. The temperature stress has been around 85°C for the FPGA for two weeks of time. FPGA named as FPGA3 (see Fig 4.10) has been subjected to aging effects. Given the fact that the aging effects degrade the FPGA or IC, we could only perform the accelerated aging with multiple ROs on one FPGA. The study aims at demonstrating the utility of EM based technique when the aging effects are considered. The response after aging is shown in Fig. 4.11.

The result from the Fig. 4.11 shows the effects of aging on the multiple ROs of same FPGA when subjected to thermal stress for around 2 weeks of time.

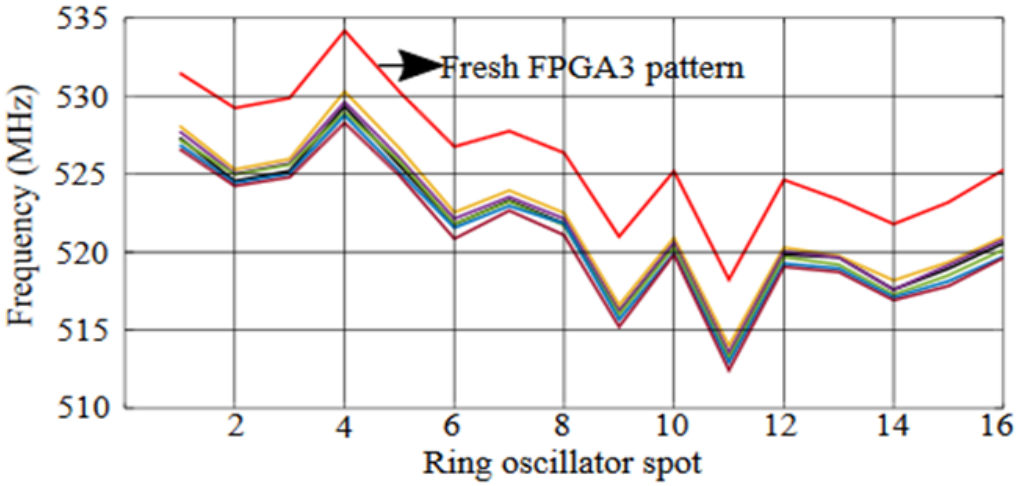


Fig. 4.11: Shift or change in the pattern of RO frequencies after FPGA (ROs I FPGA) have been subjected to accelerated aging through thermal stress for two weeks of time.

After performing the thermal stress (accelerated aging), the results obtained for the 16 ROs frequency for that particular FPGA shows that the pattern of the RO frequencies have remained intact or constant even after it has been subjected to the thermal stress. From Fig. 4.11 it is clear that for all the ROs, the frequencies shift in the same coherent order (constantly) even after thermal stress. Comparing new and aged FPGA patterns (Fig. 4.11), it is observed that the pattern has remained constant even after the degradation due to the thermal stress. This is due to the fact that effect of thermal stress (aging) on all the ROs has been homogenous or equi-proportional, therefore the shift in frequency of each ROs is coherent. To encode the response from Fig 4.11, we have deployed two different encoding techniques that convert the responses into binary fingerprints. The detailed description of the two techniques is given in the section below.

4.5 Post-processing techniques (Encoding metrics)

The notion here is to propose post-processing or encoding techniques that is utilized in quantifying EM response from multiple ROs into a dataset (fingerprints). The encoding methods used in this manuscript take into account the relative values of the ROs frequencies. The objective of the encoding scheme is to convert the response from the multiple ROs based technique into binary fingerprints. In single RO technique we have used the resonance frequency of one RO and post-processed it into signature (see

chapter 3). However, in multiple ROs we have utilized the relative approach i.e. perform mathematical treatment on the relation between the 16 ROs frequencies and converts the responses into binary fingerprint. Later on, we have also highlighted the effectiveness of the used encoding schemes for the purpose of mitigating the effects of aging from the REMT based authentication scheme.

The measurement results from previous section and subsection have shown that due to the PV effects, each FPGA of the same family have a distinct EM response when programmed with same RO circuits. The two encoding techniques proposed and used in this study quantify the EM responses into a binary vector. The purpose of quantification is to create a dataset to apply mathematical operations and store conveniently in a database for future uses. The other important aspect for an encoding technique is that, it should be reliable and robust. In this subsection we have first introduced the idea of two post-processing techniques we have used and then apply it on the EM response from multiple RO measurement result.

a) Mean based encoding technique

The first proposed encoding schemes is based on finding the mean value of all the implemented ROs frequencies and calculate the deviation of each RO frequency from that mean value. Algorithm 1 represents a pseudo-code for the mean value based encoding scheme. The employed algorithm details a finite sequence of discrete steps.

Algorithm 1 mean based encoding vector

procedure BINARYVALUEUSINGMEAN(BV)
  $P_{m,i} = P_{m,i}\{R_1, R_2 ... R_i\}$
  $P_{m,i}$ is the *m*th FPGA and with *i* no. of ROs under test
  $R \subset \mathbb{R}$ frequency in MHz of *i* number of ROs
  compute $E(P_{m,i})$
  $E(P_{m,i})$ is the mean value of RO frequencies in *mth* FPGA
  for j=1 to i **do**
    if $P_{m,i}(R_j) > E(P_m)$ **then**
      assign $B_{mj} = 1$, where $B = \{0,1\}^n$
      else $B_{mj} = 0$
    end if
  end for
  Return B_m
end procedure

Each step is an operation or instruction that can be performed by the DUT expected to carry out the procedure. Thus, the algorithm represents a set of steps for performing mean based encoding. It presents a sufficient precision and detail in an appropriate logical form, which is completely and unambiguously interpretable and executable by the particular DUT intended to perform the procedure.

Algorithm 1 is illustrated here with an example. Consider one FPGA P1, with *i* number of ROs, consider *i*=16 to represent 16 ROs for the FPGA. For 16 ROs the frequency R = {R1, R2...R16} is calculated. Subsequently, the mean (E) value of the 16 ROs, is computed for FPGA P1. Afterwards, each single frequency R1,R2...R16 is compared with the value of E, and R which are greater than that of E is assigned a binary code B as 1 and values of R less than E are assigned as binary code B of '0'. Suppose that E is 100 MHz. The value say R2 is 102 MHz, it is assigned as '1' and say R8 is 97 MHz then it is assigned as '0'. A pictorial illustration of the mean based encoding is also shown in Fig. 4.12. From Fig. 4.12, all the values above the mean is assigned as binary '1' and every value below mean is assigned a '0'. Therefore, using this shift from the mean, we create a 16-bit vector, B, which is identified as a fingerprint for that FPGA. Using our proposed encoding methodology described in Algorithm 1, the binary vector generated for the four FPGAs (DUTs) is shown in Table 4.1.

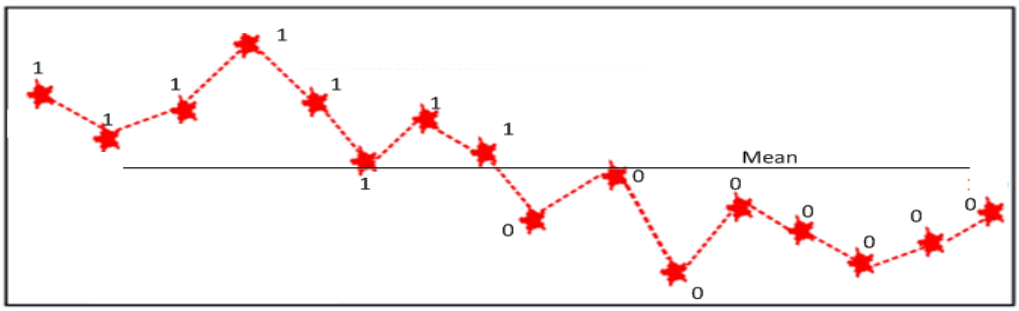


Fig. 4.12: Mean based encoding scheme illustrated with a pictorial depiction.

Table 4.1: Binary vector for each FPGA using Mean deviation methodology

DUT	Binary Vector
FPGA1	1 1 1 0 0 0 0 1 1 0 1 0 0 0 0 1
FPGA2	1 0 0 1 1 0 0 0 1 0 0 1 1 1 1 1
FPGA3	1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
FPGA4	1 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1

From Table 4.1, we can observe that for each FPGA, a binary vector has been created. The binary vectors are discriminated between two FPGAs using Hamming Distance (HD), which eventually computes the bitwise XOR between two binary vectors [11]. In this part of study taking cue from[11][12] we have computed the percentage HD, that gives by how much in percent the bits differ in two binary patterns. This metric is computed over multiple measurements on the same FPGA taking into account the repeatability errors in the measurements setup. Despite the measurement errors, percentage HD between the different measurements on same FPGA remains same (≈ 0%). On the other hand, when the percentage HD is computed between the four FPGAs, the best case obtained is ≈ 62% and worst case is ≈ 32%. Ideally, HD of 50 % is optimal because this is the case; when exactly one half devices generate a bit 0 and the other half devices generate a bit 1. Also, in the security it is important that the device generate equal number of 0 and 1 in order to have high randomness. This also dictates the optimal percentage of HD. Furthermore, as the number of devices increase in the processing optimal HD observed is close to 50 %. Also in terms of biasing, an unbiased bit should have an outcome close to 50 %, which is the case when half of the devices generate the bit as 0 and the other half generate it as 1. An outcome of 0 % (or 100 %) means that the bit was 0 (or 1) on all devices, which is an indicator for poor inter-device uniqueness [13]. Although the values obtained from HD is not close to its optimal value of 50 %, this gets restricted by the fact that the number bits generated is only 16. The HD differentiator used just to highlight the difference among the binary fingerprints between different FPGAs of same family, manufacturer etc.

b) Frequency Pair Encoding

The second encoding scheme that we have used in this work is based on exploiting the frequency pair difference. In this scheme, frequencies of two adjacent ROs are compared and if the succeeding RO has higher frequency than the preceding one then a value of 1 is assigned else 0 is assigned. Similar to the previous encoding scheme, to give a logical and unambiguous understanding of this encoding scheme an algorithm, named Algorithm 2, has been implemented.

A simple illustration of Algorithm 2 can be seen in Fig. 4.13. Using the procedure from Algorithm 2 and illustration shown in Fig. 4.13, it is clear that for n number of ROs used in the FPGA, we get $n-1$ number of bits. For the four FPGAs used as DUT in this work, the binary vector obtained using frequency pair encoding scheme is given in Table 4.2. To find the weight of difference in the binary vectors, we apply the same percentage HD as differentiator, as is done with the previous metric. For this metric, the best

case percent HD obtained is ≈ 53% and worst case is ≈ 20%. The HD of around 53 % verifies a high amount of uniqueness among the devices. But given the fact that we have used only 16 bits (16 ROs) it is possible that HD among few devices can be lower than the optimal value of 50%.

Algorithm 2 frequency pair difference

procedure PAIRWISECOMPARISION(PC)
  $P_{m,i} = P_{m,i}\{R_1, R_2 ... R_i\}$
  $P_{m,i}$ is the mth FPGA and with i no. of oscillators under test
  $R \subset \mathbb{R}$ frequency in MHz of i number of ROs
  for j=1 to i **do**
    compute $[R_{j+1} - R_j]$
    if $R_{j+1} > R_j$ **then**
      assign $B_{mj} = 1$, where $B = \{0,1\}^{n-1}$
      else $B_{mj} = 0$
    end if
  end for
  Return B_m
end procedure

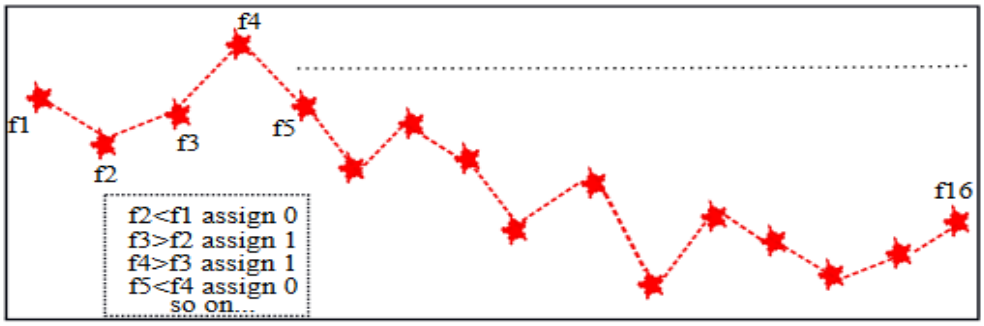


Fig. 4.13: A graphical illustration of frequency pair comparison metric.

Table 4.2: Binary vector for each FPGA using frequency pair difference

DUT	Binary Vector
FPGA1	0 1 0 0 0 1 1 1 0 1 0 0 0 1 1
FPGA2	0 1 1 0 0 0 0 1 0 0 1 0 1 1 0
FPGA3	0 1 1 0 0 1 0 0 1 0 1 0 0 1 1
FPGA4	0 1 0 0 0 1 1 0 0 1 1 1 0 1 1

Using the above proposed metrics and applying percent HD as differentiator, we can clearly see that each FPGA has a fingerprint associated with it. This fingerprint can be used for authenticating the FPGAs. The next step is to evaluate the proposed relative method based encoding schemes against aging effects. This is done in order to determine the robustness and stability of the metrics and thus the fingerprints against aging effects on FPGA. The next subsection describes in detail the results obtained on the multiple RO after accelerated aging.

4.5.1 Effectiveness of encoding method against aging effects

In this section we have demonstrated how the binary encoding methods – mean based and frequency pair – can be applied on the response of the accelerated aged FPGA. We have applied the encoding metrics on both conditions – without accelerated aging (thermal stress) and with accelerated aging (thermal stress). This way we have been able to justify the effectiveness of the encoding techniques in keeping a fingerprint of FPGA robust over period of time when it is used.

Table 4.3: Binary vectors using both metrics after accelerated aging of FPGA3 (FPGA under stress)

FPGA3	Binary Vector (Fresh FPGA)	Binary Vector (accelerated aged FPGA)
Mean Based Metric	111111111000000	111111111000000
Frequency Pair Comparision	011001001010011	011001001010011

From the Table 4.3 we can clearly observe that the binary fingerprints from both encoding metrics have been same on both the conditions –before and after aging. This validates the fact that with the proper deployed encoding techniques the fingerprints from the FPGAs using multiple RO can be kept constant and stable. This can be very useful in way to mitigate the effects of aging from the authentication using REMT based method. Even genuine FPGAs when subjected to the field or stresses (thermal/electrical) go under aging effects. Using one RO as we have seen from subsection 4.3.2, there is considerable shift in the RO frequency, which can change the EM signature of the FPGA over a period when it is working. Hence using relative based approach – encoding techniques proposed – we can get a stable, robust and aging resistant fingerprint of the FPGAs using radiated EM based authentication technique.

4.5.2 Limitations and Drawbacks of this method

One of the limitations has been that accelerated aging (thermal stress) can disrupt the electrical characteristics of the devices hence; this hampers the number of devices one can use in the measurement. Also, aging experiment is a time taking process, and has to be dealt with proper accuracy as the slight miscalculation can cause big changes in the results. Once the device has been stressed, the probability of its recovery to its original or new state is very low or negligible. Secondly, owing to the fact that all the post-processing has been done outside the chip, it is time taking and may not be optimum for all kind of devices- where auto-authentication is required.

Owing to the constraints of not disrupting the voltage supplies, we got restricted to the use of the temperature based aging effects. Hence, the voltage scaling and its effects on the aging can be an interesting area to work on.

4.6 Inferences from the aging effects on multiple RO

In the light of the results obtained in Fig. 4.13 and Table 4.3, it is validated that with the use of the multiple RO technique there are many folds of benefits:

- The intra-die variability gives a unique pattern for each IC which can be used to generate a binary code.
- The pattern obtained using intra-die variability does not vary after performing the thermal stress (aging effects).
- The fingerprints obtained could be coded into binary scheme which is more convenient to store and treat it mathematically.

With the distribution of the aging effects equally throughout the IC, it has been possible to get a result that is robust and stable with respect to aging. The pattern remaining intact justifies that the applied binary encoded fingerprints remains constant even if the IC or FPGA has been subjected to aging effects. This methodology hence is robust against aging effects and would help in achieving a fingerprint that is uniform throughout its lifetime.

This method can help in reducing the discard of the genuine IC by mistaking them as recycled or old IC. The method has been robust against aging effects, stable over period of time and easy to implement. . Using the two proposed encoding metrics, our results show encoding metrics the results show that a stable and aging resistant fingerprint for FPGAs is obtained by using EM based measurement. In comparison to classic RO PUF, this method uses very less chip area as we did not require any on-chip post-processing technique, hence it is cost effective and easy to implement. This methodology can be extended to authenticate ASICs as part of future work.

4.7 Conclusion from REMT – along with aging effects

The measurement and their associated results from the previous chapter and this chapter concludes that with the use of the REMT methodologies, a lightweight, non-intrusive technique can be used to authenticate IC using radiated EM technique. The proposed technique of utilizing the radiated EM emission can be highly efficient while tackling the common counterfeiting problems like overproduction, supply chain theft, cloning and recycling. The proposed method provides the ease of usage, little area overhead and does not require any extra dedicated post-processing circuit. Hence as also discussed in chapter 3, REMT based method can be easily applied for the authentication of various semiconductor devices commonly used.

Extension of chapter 3 to understand and investigate the aging implications, it has been observed in this chapter that using multiple RO technique, the aging effects can be mitigated. Secondly the post-processing steps have been different than that of chapter 3, this also indicates that during the course of work we have adopted different mathematical treatment mechanisms as per the application requirements. The results from this chapter after subjecting the IC to thermal stress confirms the fact that by using multiple RO in REMT based method the aging effects of the IC can be mitigated. This can be useful in finding and implementing ways to authenticate an IC which has been in the field for some time. Hence, authentic but old IC will not be removed from the operation by the user. This method also creates a fingerprint that remains stable throughout the lifetime of IC making it deterministic.

The work done in chapters 3 and 4 validates the fact that REMT based method is viable option to authenticate ICs with very less area and time consumption. The investigation of aging effects also shows how we can use REMT based method against PVT variations and still have a stable fingerprints.

References:

[1] A. Chenouf, B. Djezzar, A. Benadelmoumene, and H. Tahi, "Deep experimental investigation of NBTI impact on CMOS inverter reliability," in *2012 24th International Conference on Microelectronics (ICM)*, Algiers, Algeria, 2012, pp. 1–4.

[2] Zhang XiaoWen and En YunFei, "The HCI effect reliability evaluation of CMOS process," in *2014 IEEE International Conference on Electron Devices and Solid-State Circuits*, Chengdu, China, 2014, pp. 1–2.

[3] H. J. Lee and K. K. Kim, "Analysis of time dependent dielectric breakdown in nanoscale CMOS circuits," in *2011 International SoC Design Conference*, Jeju, Korea (South), 2011, pp. 440–443.

[4] K. He, X. Huang, and S. X.-D. Tan, "EM-based on-chip aging sensor for detection and prevention of counterfeit and recycled ICs," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, 2015, pp. 146–151.

[5] K. K. Saluja, S. Vijayakumar, W. Sootkaneung, and X. Yang, "NBTI Degradation: A Problem or a Scare?," in *21st International Conference on VLSI Design (VLSID 2008)*, Hyderabad, India, 2008, pp. 137–142.

[6] A. Sengupta, D. Kachave, S. Neema, and S. H. Panugothu, "Reliability and Threat Analysis of NBTI Stress on DSP Cores," in *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Bhopal, 2017, pp. 11–14.

[7] C. Yilmaz, L. Heiss, C. Werner, and D. Schmitt-Landsiedel, "Modeling of NBTI-recovery effects in analog CMOS circuits," in *2013 IEEE International Reliability Physics Symposium (IRPS)*, Anaheim, CA, 2013, pp. 2A.4.1-2A.4.4.

[8] H. Dogan, D. Forte, and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," in *2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Amsterdam, Netherlands, 2014, pp. 171–176.

[9] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," *IEEE Trans. Emerg. Top. Comput.*, pp. 1–1, 2015.

[10] M. M. Ahmed *et al.*, "Towards a robust and efficient EM based authentication of FPGA against counterfeiting and recycling," in *2017 19th International Symposium on Computer Architecture and Digital Systems (CADS)*, Kish Island, 2017, pp. 1–6.

[11] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2012, pp. 302–319.

[12] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[13] D. Forte, A. Srivastav, "On improving the uniqueness of silicon-based physically unclonable functions via Optical Proximity Correction" in 2012 DAC Design Automation Conference, San Fransisco, US, pp. 96-105.

5. Guide Electromagnetic based Authentication Techniques for IC

Overview and Objectives

In previous chapters (chapter 1 & 2) we have seen the prevalent effects of IC counterfeiting and various steps taken in order to mitigate its effects. Approaches like embedded sensors, PUF etc. have widely been used. In chapters 3 and 4 we have proposed to use an alternative method of utilizing radiated EM radiation technique (REMT). The REMT based method already has shown a considerable amount of advantages over classical PUF based method. This can be highly effective in analyzing the security of the IC when there is constraint in terms of area and power. The REMT based technique can also be designed to be robust against aging effects also. We have already seen the detailed explanation of the REMT methodology implementation on two semiconductor devices like FPGA and MCUs. The results have shown conclusively that REMT based method is a viable solution in implementing non-invasive technique for authentication.

In recent years there have been upsurge of using active devices (ICs of different technologies to work in high or RF frequency ranges). The RF IC or radio frequency ICs implement several applications in the field of wireless technology that works for high range of frequency up to several GHz. There have been many instances in which RF testing on semiconductor devices and wafers have been carried out. One such example can be observed from [1] , in which the membrane probe card is a production test board for high-volume RF wafer testing. Similarly in [2], a membrane probe capable of working in high power capacity have been used with discrete and partially matched transistors at microwave frequencies. Both physically and electrically, the membrane probe resembles the components and packaging of the final product. Die tested using a properly designed membrane probe card should exhibit RF performance comparable to an assembled component. Hence from previous works it has been validated that wafer level of testing using RF input power has been possible.

This chapter proposes to employ a novel technique for obtaining signatures of IC using guided wave EM technique where a guided EM wave is transferred through the RF port of the DUT, and physical

variability of the DUTs are interrogated. The idea of using guided wave EM technique or GEMT also adheres to the fact that it is highly non-invasive in nature, does not need extra post-processing area in the IC. The idea revolves around the fact of bridging the EM and IC interaction, characterizing the physical features of IC based on EM wave perturbation and finding the unique parameters that can be used for the purpose of authentication.

An overview of a setting in which IC can be plugged or placed in the socket of a PCB which is capable of working in RF is depicted in Fig. 5.1. In Fig. 5.1, we can observe that an IC or DUT to be authenticated can be plugged in to a PCB set up with proper input-output (IO) connectors to support the transfer of RF power. This technique can facilitate the usage of various ICs of similar package to be subjected to guided RF waves, and their IO response can be characterized. This characterization can be further extended for the purpose of generating signature.

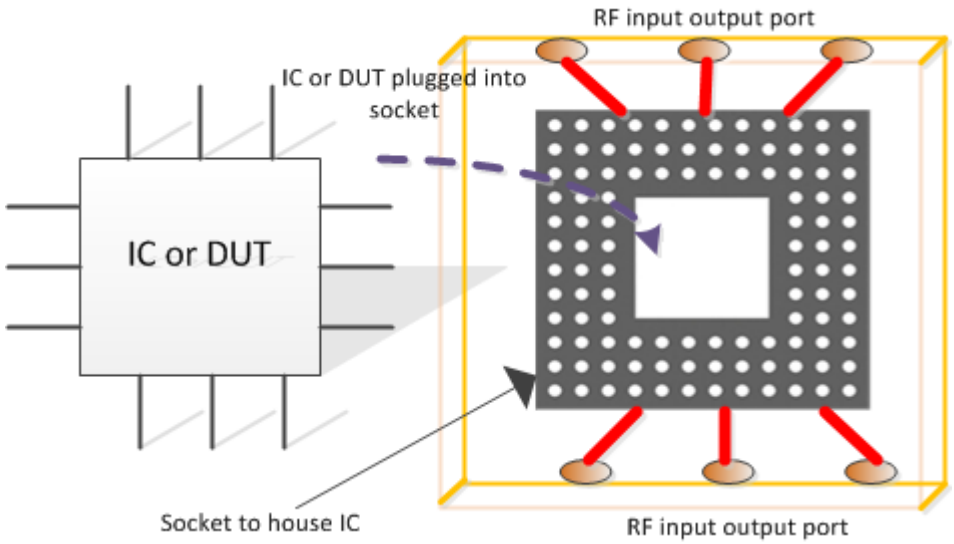


Fig. 5.1. An illustration of using IC on a pluggable socket to be characterized with the guided RF waves. In this type of measurement a dedicated PCB is used that incorporates all RF features (RF ports etc.) for the purpose of measurement.

The GEMT based technique discussed in this chapter suffices the use of EM technique i.e. excite the underlying process variation effects through the EM waves. In EM based methodology discussed in this chapter, we have focused on examining the idea that utilizes the incoming EM waves to exploit the underlying the process variation (PV) effects. This method has been applied in this work to characterize

the interaction of EM waves with IC to generate a setting to employ the security mechanism based on this approach.

When compared to some of the present authentication schemes this approach is non-invasive and area efficient. The PUF based approach for an example requires a lot of silicon area to perform the on-chip post processing which ultimately requires extra time and effort. A detailed discussion on the utilization and drawback of the PUF based approach has been drawn out in chapter 2. As also discussed earlier in our EM based approaches - GEMT or REMT approach - the post-processing technique has been performed off the chip which reduces the area overhead of the implementation. The drawback is that in return a dedicated measurement bench (instrument / device) has to be used.

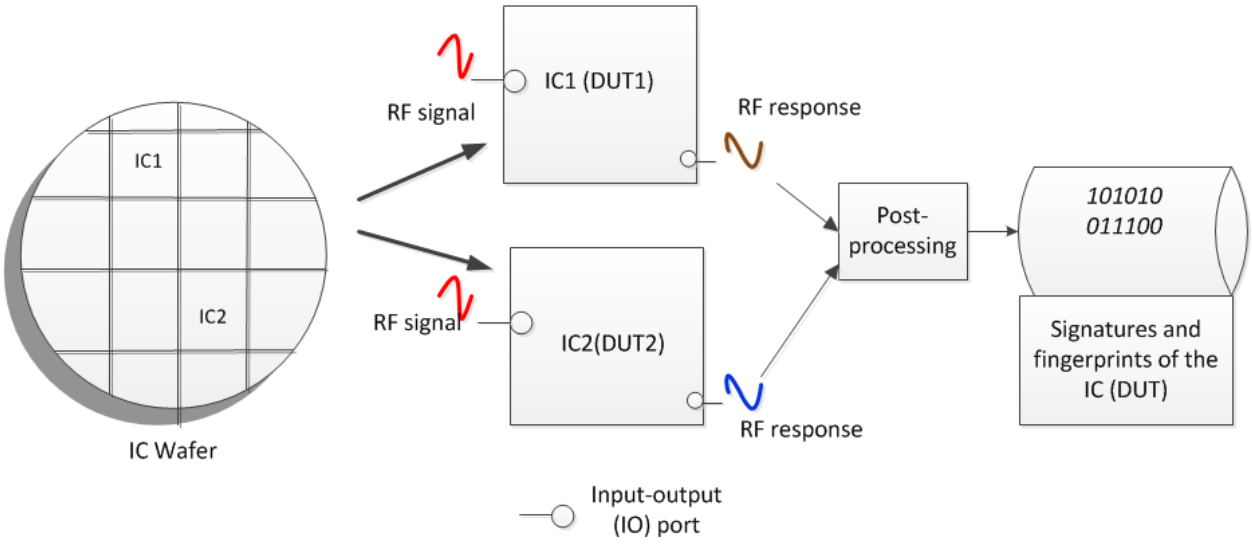


Fig. 5.2: A pictorial depiction of using ICs from same wafer (manufacturer, series) to perform a guided RF wave measurement for the purpose of generating their signature or fingerprint.

The motivation in this study is to maneuver the PV effects of the IC using a guided wave approach. The study focusses on utilizing the basic internal physical features rather than implementing any kind of marker or sensors. The idea is to find out the amount of disruption an internal guided wave experiences when it interacts with the physical inconsistency of the IC. The distinction of each IC (due to PV) can be exploited this way also and could be used for generating a fingerprint distinct for each IC. A pictorial overview is given in Fig 5.2. From Fig. 5.2 we can observe the ICs (IC1 and IC2) from same wafer (same manufacturer) has been used as device under test (DUT). Both the ICs have been subjected to the same guided RF wave as input. Owing to the PV based physical effects, the variation both the ICs even from same manufacturer, series etc. gives a distinction in the RF responses. The RF response from both the ICs

is treated further with post-processing steps in order to obtain a signature or fingerprint that can be used for the purpose of authentication of ICs.

A detailed overview of the proposed GEMT based approach is discussed in section 5.1. In the section 5.1, we have discusses the various issues with respect to the implementation of this approach, such as:

- Guiding the RF signals into the IC - how RF waves can be traversed in an IC.
- Operations that can be performed on the classical of RF signal when traversing through the IC (ASIC or FPGA).
- And the measurements issues that can come with this kind of setting.

In this approach we have made an endeavor to utilize inherent parametric variations which come during the manufacturing of IC. Each IC has its own manufacturing defects. Even no two ICs from the same die have similar physical characteristics due to inhomogeneity of manufacturing process. Each IC then has unique physical features which can be exploited and used as its fingerprint. The guided RF wave utilizes the manufacturing variation features [8]. Each IC interacts with RF input wave and produces a signature, and we want to show that this signature is unique and can be used for authentication applications.

5.1 GEMT based authentication method – an overview of principle

A high level use case showing a methodology for usage of guided RF signal for IC authentication is given in Fig 5.3.

From Fig. 5.3 we can observe the various steps that need to be involved in developing the proposed GEMT based method for the authentication of IC. The steps require the measurement of IC with the incoming guided RF waves, extracting the response from the IC – transmission and reflection characteristics - and preforming the required post-processing techniques. The steps can be divided into stages, viz. enrollment stage and comparison stage. During the enrollment stage, a set of measurements is performed, the obtained RF response is post-processed and the obtained signature is stored in the database. During the comparison stage, the IC or DUT which has to be authenticated is subjected to similar measurement steps (as in enrollment stage). The RF response is post-processed and the obtained

signature is compared with that in the database. The decision is made if the signature of both stages is same of not – IC authentic or not.

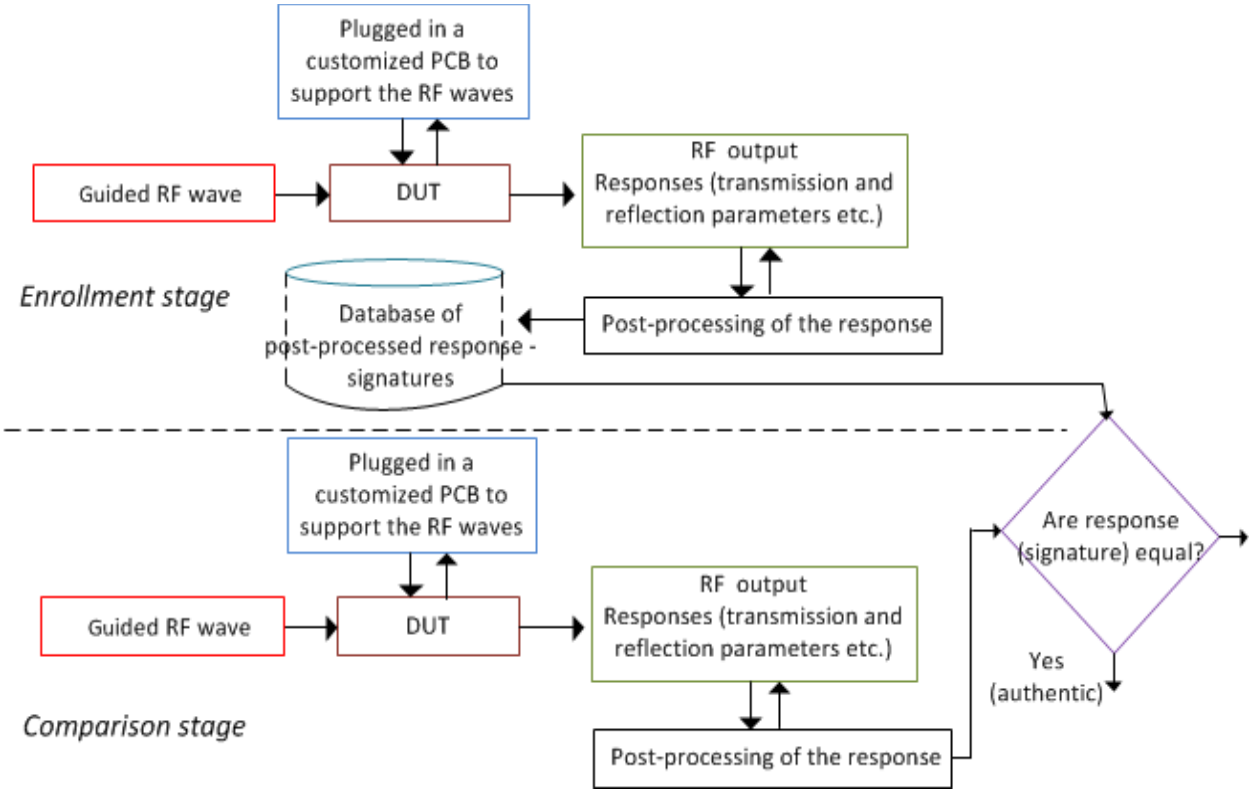


Fig. 5.3: Use case showing a methodology for guided RF usage for IC authentication.

Indeed guided RF wave interacts with the physics of IC which can be used for distinguishing the real IC from a counterfeit and recycled IC. Here the inherent variation of the IC which comes due to manufacturing variations has been exploited. Using this information, we have exploited the PV effects of IC using guided RF waves and quantified it in order to generate a signature for the ICs. The generated response can be stored in a database for the future reference when the user wants to authenticate the IC, the values or signature can be compared with the database values (see Fig. 5.3). The methodology and objectives of measurement of GEMT approach is to observe the following few key factors:

I. Excite the IC (in ON state) with a guided RF signal.

II. Measure the amount of transmission and reflection of the RF wave due to interaction with the IC.

III. Measure other non-linear effects coming due to the interaction of IC with RF.

IV. Observe the amount of internal coupling or interactions in the IC.

V. Observe the possibility to configure logic circuit in FPGA depending on the FPGA architecture.

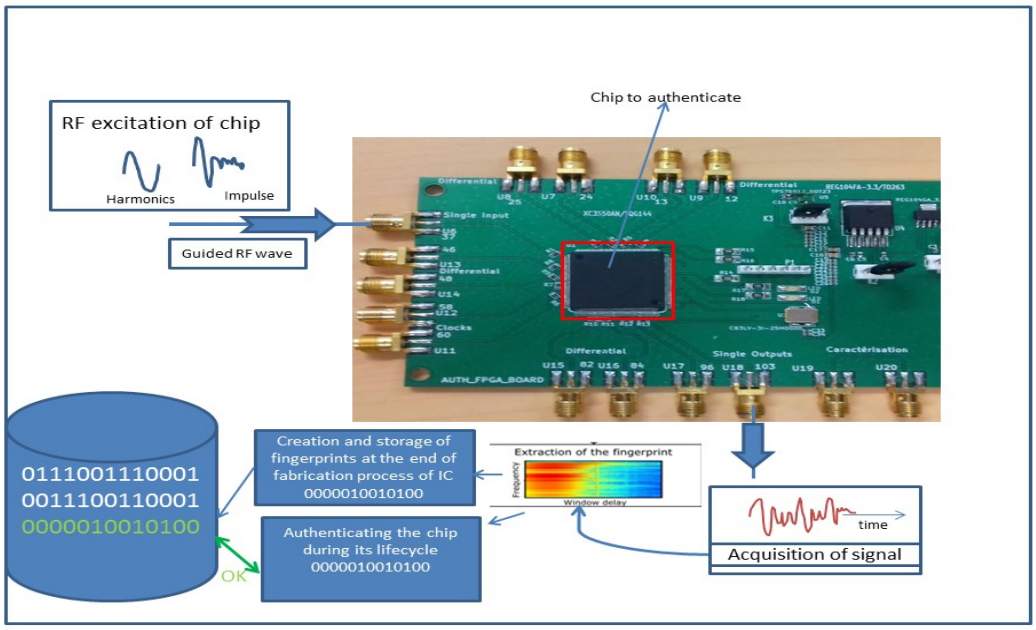


Fig. 5.4: Proposed hardware model of EM based authentication with a testbench. This testbench is specifically made to use RF signal as excitation to the IC.

The illustration observed in Fig. 5.4 shows the model we have proposed for using guided RF wave to authenticate an IC. For the measurement purpose, we have designed a PCB board. The PCB contains a FPGA (as device under test), regulators, oscillator, LED and SMA connectors for the EM/RF input and output.

The guided wave traverse in the IC and a part of it would be reflected and some absorbed or refracted back. The response of the guided RF wave is linked to the architecture or internal physical structure of the IC (FPGA in Fig. 5.4). The amount of absorption or reflection is dictated by how the internal physical features of IC interact with the incoming guided RF wave. Therefore, based on the physical variations in the IC the amount of reflections, refractions and absorption would differ. This difference would give each IC a distinct identification. This could be further utilized for the purpose of authentication.

In order to have an efficient performance of this GEMT based approach for the authentication purpose of ICs, the setup – measurement condition, choice of DUTs, experimental parameters etc. should adhere to the following points:

I. The obtained RF response should be unique for each IC.

II. The obtained RF response should be stable under all operating conditions.

III. Response should be same even after repeated measurements and not get affected by aging, NBTI, HCI and other measurement related errors.

In other instances, it is possible (also depending upon applications) to characterize several ICs of similar packages on the same PCB enabled with RF capabilities. An example of plug and use system has already been pictorially described in Fig. 5.1. Secondly, if the PCB is customized so that the IC can be removed from the board or PCB, it would be useful to characterize the noise and harmonics of the PCB only. This can ensure in removing the effects of the PCB noise from the final measurement results.

To characterize the systematic error from PCB, a measurement can be setup without the IC or DUT and its response stored or saved. Next, the IC or DUT is plugged in the PCB and the measurement is performed and response is noted. The response from the empty measurement can be subtracted from the response from the measurement involving the DUT or IC. The subtracted response is the response which does not have effects of systematic error. Although in this work, we have not used plug and use PCB. But we have also demonstrated how the PCB based systematic error effects and aging effects can be mitigated from our test-bench. Before, going into the authentication methodologies using GEMT based scheme, we have summarized the overview and principles of the GEMT based authentication methodology.

The idea discussed in this section points towards the principle of interoperability of low cost FPGA – devices used only for digital operations - with the guided RF waves. The use of FPGA with the required PCB board explores the flexibility of FPGA to be used with the RF signals. This adds the usefulness of using FPGA in the RF frequency ranges for various applications. To the best of our knowledge, for the first time, an interaction of RF and FPGA has been established in order to implement the authentication scheme of the IC among various other applications.

The next section discusses about the implementation of the GEMT based authentication measurement and implementation in details.

5.2 GEMT based authentication – objective

After understanding the proceedings and factors that attribute to the utilization of guided RF waves in order to generate the distinct signature of ICs, the next important aspect to discuss is the objective that we need to set before performing any experimental setup. The objective of using this technique where RF wave interacts with the ICs – FPGA in our study – is to validate the fact that it is possible to have an IC interact with RF wave and produce a distinct response.

I. To find the optimized mechanism (technique) that could optimize the interaction of RF with IC or DUT.
II. To show interaction of IC with external RF excitation when IC is in operating mode.
III. To obtain a fingerprint from each IC this would serve as its unique identifier.

The primary objective is to find the amount of interaction an IC can have with the guided incoming RF waves. Secondly it is also important to find out the amount of difference when the IC is switched ON and when it is switched OFF. It is important to see how the electrical functionality (electrical non-linear effects due to active and passive components of IC) of IC would alter the RF waves. After the first two objectives are achieved the focus on the third objective is shifted that could aid in extracting a meaningful signature for authentication purpose could be fulfilled.

With the utilization of FPGA as DUT, there is a large extent of possibility with it. FPGA offers the flexibility with respect to the re-configurability when compared to application specific integrated circuits [3]. As FPGAs are re-programmable device, and many of its internal physical features can be exploited using different circuit configurations – routing architecture, digital logic implementations etc. –Therefore, there is always a possibility to improve the interaction of device (FPGA) with the external guided RF waves. This can give a better and prudent response that can be utilized effectively for the authenticating purpose.

Elaborating the three objective points first it is important to find and show that the EM wave can be altered by internal structures of IC (FPGA, Analog). Secondly it is important to find a metric which could be used for the measurement and differentiation. Metric could be a physical parameter as also discussed in chapter 3 that can be used as a reference to check the behavior of two similar ICs to a same input. In the sections below we have explained each aspect that is related to the implementation and performance of this novel technique. For the measurement purpose we have taken an FPGA into consideration which

are one of the most prominent targets for the counterfeiter as they find their applications in various important semiconductor applications. Before detailing about the measurement steps with the developed RF-PCB on several FPGAs, we have performed a basic simulation in CST software, with an IC model. The idea of this simulation is to establish a state of art about the effects guided RF wave on the IC.

5.3 Simulation model of IC in CST

The simulation steps in CST simulation tool are done in order to validate the fact that the physical variations in the IC can cause a significant amount of change in the output response of the injected EM wave. The RF wave is guided using the micro-strip line on the Printed Circuit Board (PCB) shown in Fig. 5.5. The wave enters the IC and based on its encounter with the components inside IC it will either reflect, refract or get absorbed by the IC components. The parameter that is used to quantify the amount of reflection or absorption of the guided is the S -Parameter.

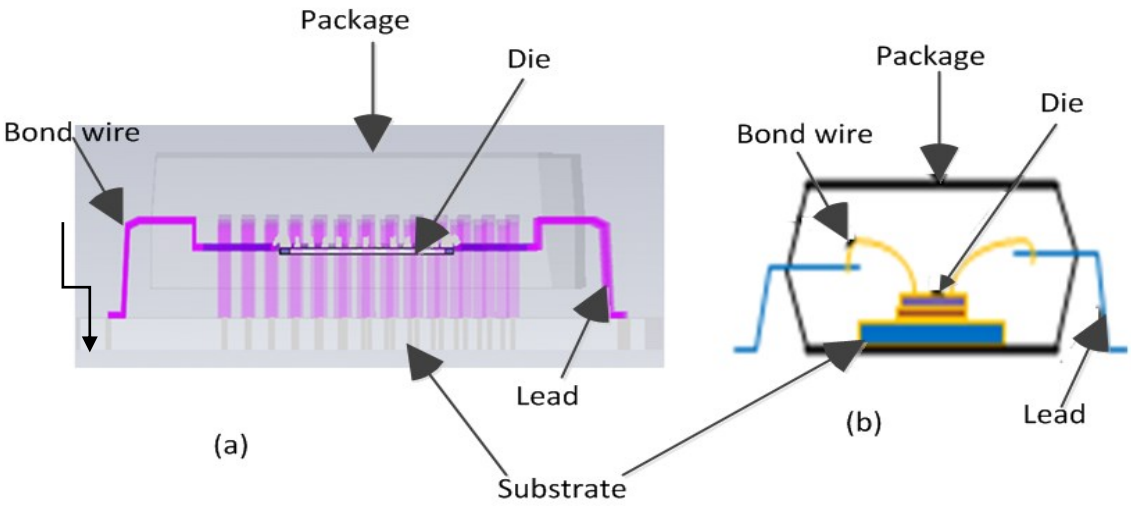


Fig. 5.5: Physical model and structure of IC. (a) CST model of a 56 pin IC. (b) A physical model of IC.

In Fig. 5.6 a 56 lead package mounted on a Roger RO3003 substrate has been depicted. The pins connecting the die to the external IO are made of lead and wire bonds are made of copper. The dimension of the IC package used as depicted in Fig. 5.6(a) and (b) is: width = 8.77 mm and length = 9.78 mm. The model uses discrete port on each lead which would input the RF wave inside the IC package. The package is a CST based IC package and we have used it for the simulation purpose. The simulation has been

carried out in the frequency range up to 20 GHz. Fig. 5.6(b) shows the different IO ports used to inject RF waves. Two lead pins are chosen and an interconnect is implemented between these two lead pins / ports and S-Parameter response is simulated between these two leads/ports.

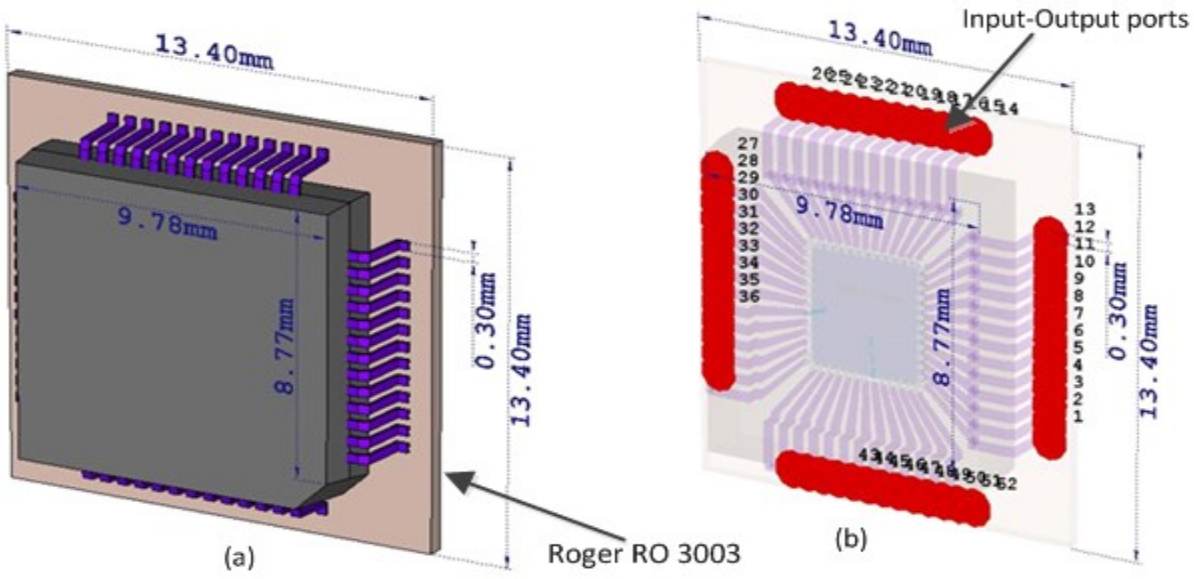


Fig. 5.6: CST chip model description: (a) CST Chip Model of package with dimensions. (b) Discrete port used for S parameter.

This simulation is done in order to verify that guided wave when enters the chip get disturbed or perturbed by the internal physical characteristics of the chip. The discrete port is used in two lead pins of the chip. In this simulation different cases are used:

I. When there is no interconnect between the pins/ports.

II. When there are interconnects of different lengths between the pins /ports.

The trace in Fig. 5.7 (no interconnect between the ports) is for the S21 parameter i.e. transmission coefficient between the ports of electronic device as shown in Fig. 5.6(b). We can observe a very low transmission coefficient of about -30 dB. Note that there is no interconnect or path between IO ports (for IO port refer Fig. 5.6(b)). Next, we observe how the S-Parameters vary with the presence of the interconnect between the ports. Similarly another interconnect of different length is made and we could

observe a clear difference in the S21. The shift in length of interconnects in IC (in CST model) in shown in Fig. 5.8. The shorter length shown in Fig. 5.8 has been named as Length 2 and longer one as Length 1.

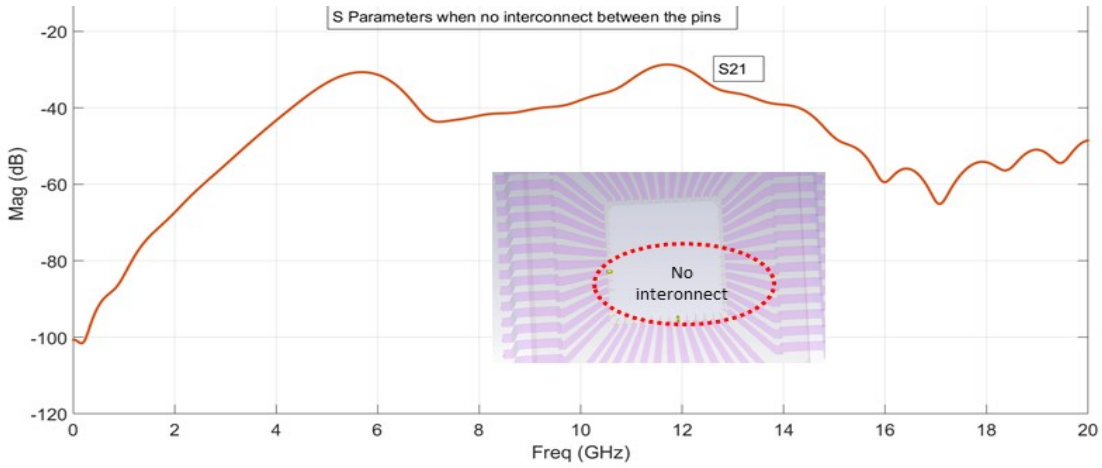


Fig. 5.7: S21 response without any interconnect, amount of power transmitted is very low around -30dB.

A simulation on the two interconnect lengths (Length 1 and 2) to obtain S21 parameter have been performed. We can see the result (S21 response) in the Fig. 5.9. From Fig. 5.9 it is clear that resonance occurs at around 9 GHz and lowest S21 magnitude is around 6 GHz. From Fig. 5.10, we can infer a pictorial description of surface current at two frequencies viz. at 6 GHz. and 9 GHz.

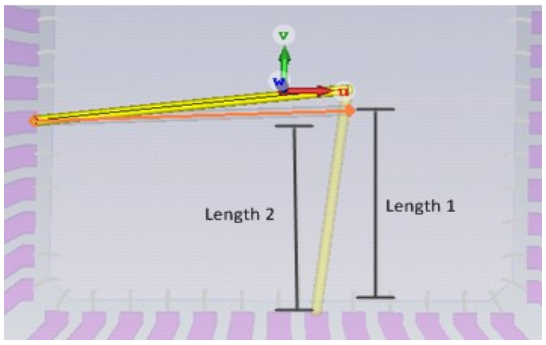


Fig. 5.8: Shift in the length of interconnects in the IC model in CST simulation. The difference between Length1 and Length2 is around 0.05mm.

The Fig. 5.9 also shows the variation in the length and its effect on the S21 parameter. Hence the routing length or to that matter any physical variations does effect the RF / EM waves. Because, when the signal includes frequency component then the length of interconnect becomes an important factor.

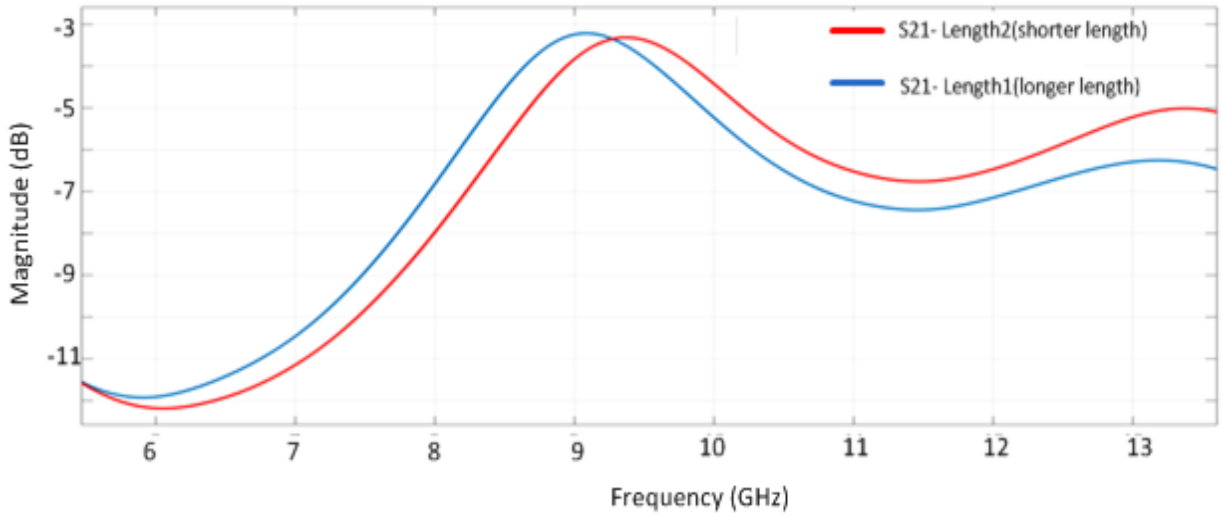


Fig. 5.9: S21 (transmission coefficient) difference due to change in route inside IC, observe the shift in the frequency of S21 due to routing lengths differences.

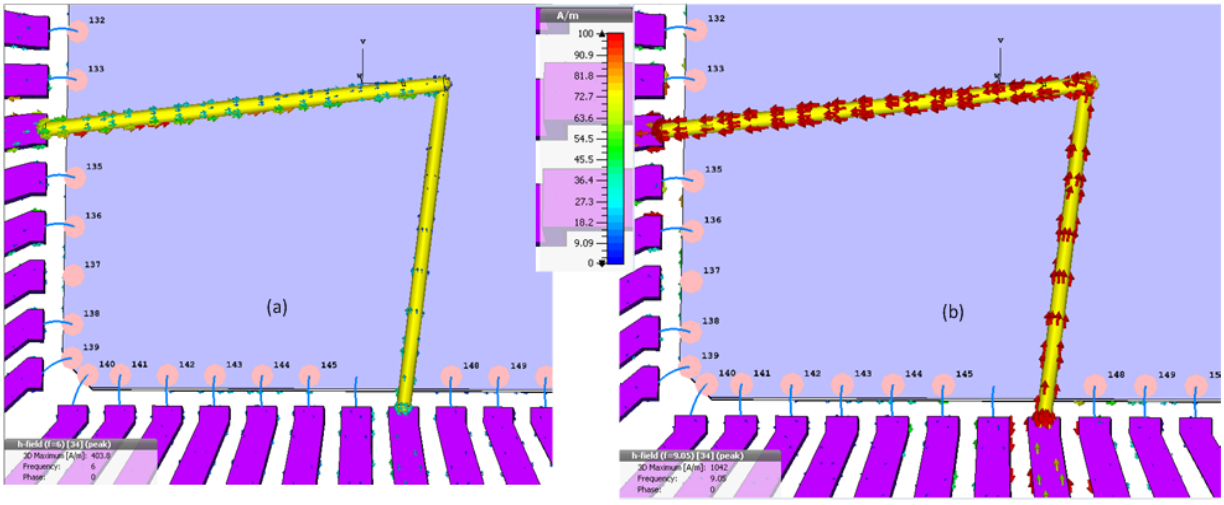


Fig. 5.10: Surface current on the route established between input-output port in CST simulation of an IC at two frequencies (a) at 6 GHz and (b) 9 GHz.

The surface current at two frequencies is shown in Fig. 5.10. This is shown in order to demonstrate and highlight the difference in the current when the resonance occurs (at around 9 GHz) and when the output magnitude in very low (outside the resonance, at around 6 GHz).

The results from Fig. 5.9 and 5.10, clearly show that the guided wave does get disturbed by the physical variation inside the IC. This method can be applied further for the authentication. In real IC application, the physical variations can be very small; also that there can be lots of circuit elements (active or passive) inside an IC between the IO ports. Hence it is interesting to observe if the guided EM waves are able to generate a response pertaining to the physical variability of each IC.

Based on the simulation results obtained in this section, we attempt to setup a measurement where we could exploit the routing changes inside an FPGA and then observe the difference in the S-parameters due to change in the routes. This measurement is described in details in the next section. The difference with the simulation and actual implementation in FPGA is the presence of buffer logic (active block) in FPGA, which needs a biasing voltage to turn ON and conduct.

In this study, only one configuration has been implemented utilizing buffer along the IO ports. However, with FPGAs there can be several other more complex configurations (circuits) that can be implemented for further utilizations.

5.4 Hardware Design and Measurement for GEMT method

We have designed a FPGA PCB board for the measurement purpose. FPGA is low cost device mostly used for the purpose of digital applications clocked by internal clock system for synchronous applications. FPGA has the features of being re-programmable.

The PCB contains a SPARTAN-3A FPGA (90nm CMOS), SMA connectors with RF IO and other external circuits. The PCB is equipped to provide adequate systems that would assist in programming FPGA – using JTAG pins - and as well in providing in the external RF signals. From our best of knowledge, this type of configuration to establish the direct connection between FPGA and RF wave has not been devised earlier. Like most of digital circuits, the FPGA has high impedance input-output (IO) pins. In order to allow the RF signals to traverse through the component - FPGA (re-programmable) - the

simplest way, we have added a 50Ω resistor parallel with the component. The Fig 5.11 shows a pictorial depiction of PCB used in the measurement.

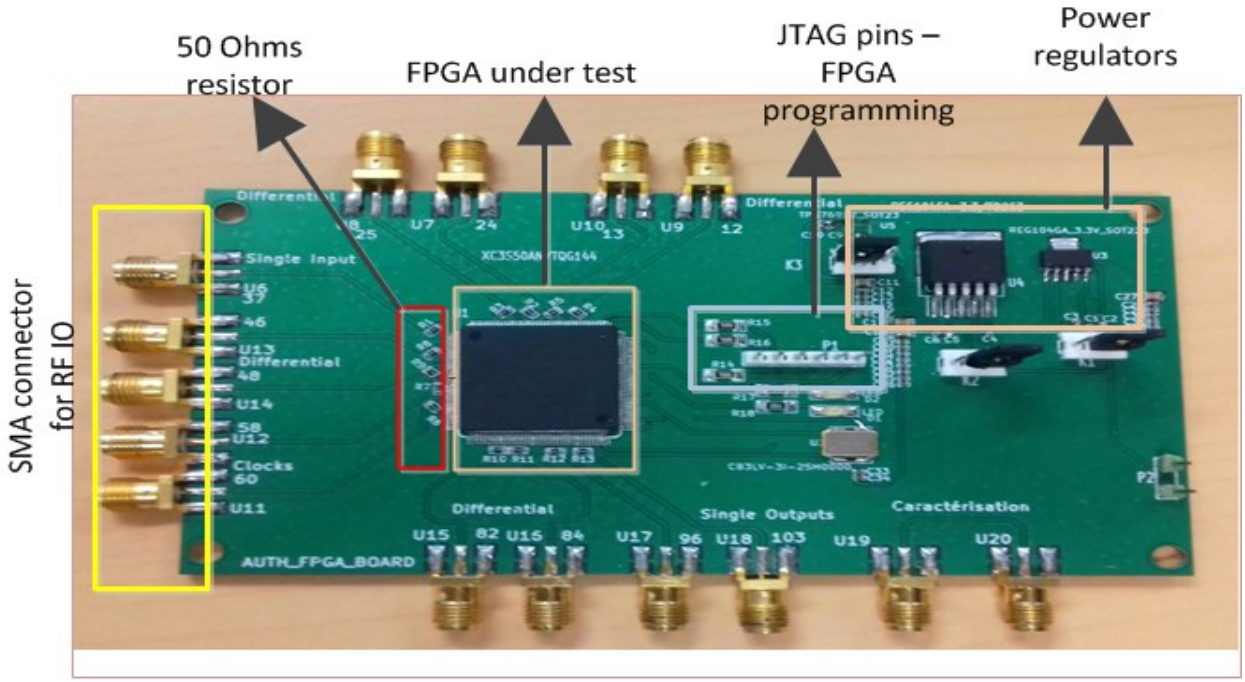


Fig. 5.11: PCB Board for the measurement for SPARTAN 3A FPGA. The detailed illustration shows the various circuit components used along with the SPARTAN-3A FPGA. For RF IO connection SMA connectors are used.

5.4.1 Measurement setup for GEMT based methodology

As previously explained, to perform the testing and measurement, a customized 4 layer RF PCB is developed, which has SPARTAN-3A FPGA from Xilinx as device under test (DUT). For programming, placement and routing of the logic elements in the DUT, Xilinx ISE tool is used. Along the FPGA, there are auxiliary regulator circuits for power management.

A pictorial depiction of the FPGA PCB with the RF auxiliary components and measurement setup is shown in Fig. 5.12. This is the customized PCB that has been designed by commercial KICAD® tool. For the fabrication of the PCB we have sent the design and layout to an external vendor.

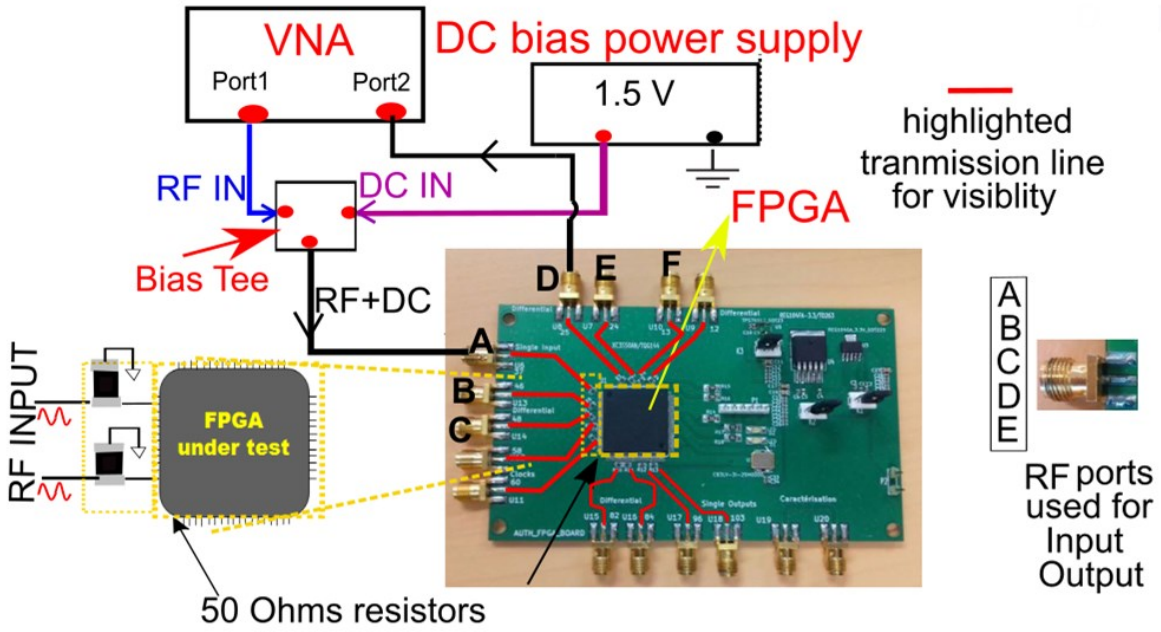


Fig. 5.12: Measurement setup on the customized FPGA PCB to perform the RF test. Inset zoom shows an enlarge description of 50 Ohms resistors used with the transmission for proper matching. Input-Output (IO) ports naming is described which is used throughout this study.

As evident from Fig. 5.12, for the measurement purpose, a vector network analyzer (VNA) is used, which measures the S-parameter from multiple IO to the FPGA. For injecting DC bias, voltage along the RF input into the FPGA input port, a bias tee is used. Input DC bias for the circuit programmed in FPGA is set at 1.5V. At DC bias of 1.5V a proper operating condition is established which supplies a steady voltage for device to operate. The RF input power level generated from VNA is set at 10 dBm. The discussion about the DC bias interaction with the RF wave continues in chapter 6 also.

To realize it, a PCB has been designed to allow the FPGA to be connected to external as RF equipment where 50Ω transmission lines and SMA connectors are used. Like most of digital circuits, the FPGA has high impedance Input- Output (IO) pins. In order to allow the RF signals to penetrate through the component - FPGA - the simplest way, we have added a 50Ω resistor parallel with the component. A detailed understanding and discussion about the matching and its utility with the FPGA has been given in chapter 6.

5.4.2 Exploitation of PV effects – GEMT based approach

The main aspect in creating the fingerprints or signatures is to exploit the underlying manufacturing based PV effects of IC. Similarly in this study also, we have made an attempt to exploit the PV effects by injecting RF waves in the FPGA under test. All known methodologies against IC counterfeiting like PUF etc. rely on intrinsic PV occurring during the manufacturing process of silicon chips. Going down in nano-scale technologies, there are increased effects of PV due to lithographic error and dopant fluctuation etc. This intrinsic and stochastic nature of PV effects cause a difference in the electrical functionalities (like Vth, switching speed, cut off frequency etc.) of ICs even if they are of same mask [6]. In other studies i.e. using REMT based techniques [7] or in PUF based approaches [8], the authors have deployed variability aware circuits (VAC) that exploits the underlying PV effects of the IC.

In this work we have not opted for any VAC, but rather our objective has been to exploit the PV effects from regular circuit elements like a basic logic block (configurable logic block in FPGA) and input-output routing (interconnect). The FPGAs in this work have been programmed with a single buffer. The injected RF wave gets perturbed by interconnect and buffer circuit it finds in its traversing path. This issue can also be linked with the signal integrity.

Because we have utilized a digital design, we know that such a device can suffer by issues associated with transmission line effects. At lower frequencies the signals remain within data characterization and the system performs as designed. But as system speeds increase, the higher frequency impact on the system means that not only the digital properties, but also the analog effects within the system must be considered [9]. These problems are likely to come to the forefront with increasing data rates for both I/O interfaces and memory interfaces, but particularly with the high-speed system (RF system in this study) being embedded into FPGAs. Transmission line effects can have a significant effect on the data being sent. At low speeds, the frequency response has little influence on the signal, unless the transmission medium is particularly long. However, as speed increases, high-frequency effects take over and even the shortest lines can suffer from problems such as ringing, crosstalk, reflections, and ground bounce, seriously hampering the integrity (response) of the signal [10].

The interconnects established in the FPGA can be defined as a conductive connection between an input and output port capable of carrying a signal. At low frequencies a wire or an interconnect track may be considered to be an ideal circuit without resistance, capacitance, or inductance. But at high frequencies, AC circuit characteristics dominate, causing impedances, inductances, and capacitances to become

prevalent in the wire [11] also shown in Fig. 5.13. The length and width etc. physical features are not same on two ICs of same batch, configuration, mask etc.

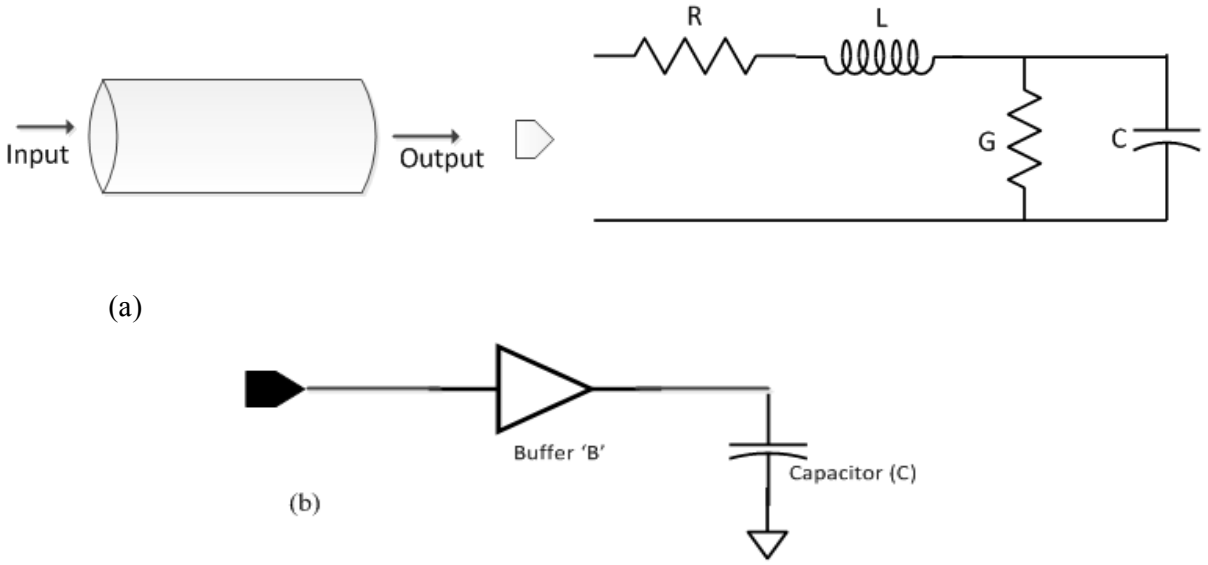


Fig. 5.13: Equivalent models. (a) An equivalent circuit model for a wire. (b) An equivalent capacitive load for the buffer circuit.

In terms of the physical layout, the effects like line edge roughness (LER) can effectively cause variations in the R, L, C dimensions even if the same exact protocols and layout masks have been used. The incoming RF wave can get disturbed by the effects of the physical features of interconnect and hence the response of two similar ICs can be distinguished by only the use of interconnects [12]. An equivalent model of wire and buffer circuits is shown in Fig. 5.13(a). This shows the electrical break up of a higher level circuit and the physical features that an incoming RF wave encounter when it meet wires and buffer circuits [13].

The output of the buffer circuit contains mostly the capacitive load (see Fig.5.13 (b)). The non-linear effects from the buffer circuit – consisting of various RC parasitic on its transistor level modeling – causes a considerable effects and perturbation to the incoming RF wave along with the interconnects [12] [14]. Hence owing to the PV effects the buffer circuit along with interconnects can have a unique cut off frequency for each DUT or FPGA. The results are dealt in detail in the section below.

5.5 Results from GEMT measurements

In order to exploit the PV effects and henceforth generate fingerprints from the IC or FPGA, the FPGAs are programmed with a single buffer circuit. The concept is to investigate the amount of the effect the underlying PV effects of routing (wire) and transistors of buffer circuit can have. In this sub section, we have investigated and detailed the measurements results of GEMT approach on the FPGA and subsequently generated the fingerprints which can be used for the purpose of the authentication. All measurement results are observed in VNA.

5.5.1 Measurement results

The FPGA under test have been programmed with a buffer circuit. Taking reference from Fig. 5.12, the input port is 'A' and the output port is 'D'. The buffer 'B' is programmed in the one FPGA with two different routing lengths between IO ports. For example a buffer 'B' is programmed in FPGA 'X'. Say the length of interconnect is 'L' between IO ports. Again, the same FPGA 'X' is programmed with 'B' but this time the interconnect length is 'L1' between the IO ports. Hence on same FPGA on two instances same buffer circuit 'B' is programmed with the varying interconnects lengths (L and L1). A pictorial depiction of this is shown in Fig. 5.14. It is clear that in Fig. 5.14(a) the length of interconnect from 'A' to 'D' (through buffer 'B') is shorter in comparison to that in Fig. 5.14(b). The measurement steps on both the varying length of route / interconnects have been done separately.

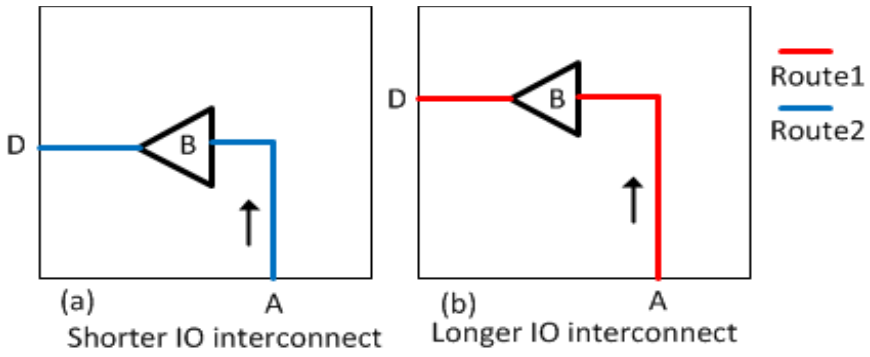


Fig. 5.14: Two different routes implemented for same buffer "B" on same input-output ports (A and D). (a) Shorter interconnect(route) between IO 'A' and 'D'. (b) Longer interconnect (route) between IO 'A' and 'D'.

The S21 response is shown in Fig. 5.15 for the two different routes for the 11 FPGAs. Each FPGA has been measured 10 times with the setup shown in Fig. 5.12, following the same experimental protocol. The graphs from Fig. 5.15 clearly depicts that the S21 curves for 11 FPGAs have been different in both of the routes – route 1 (shorter route) and route 2 (longer route). This difference in S21 response for each FPGA can be utilized to differentiate them.

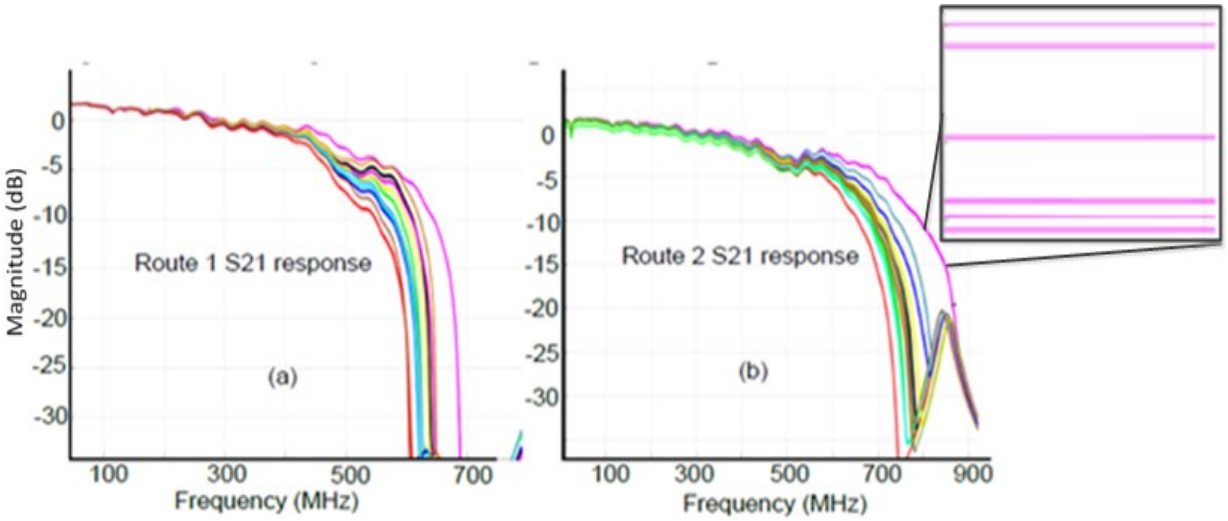


Fig. 5.15: S21 response from the 11 FPGA for two different routes with each measurement done 10 times. Inset zoom on one of FPGA response to show the repeatability of measurement for 10 times.

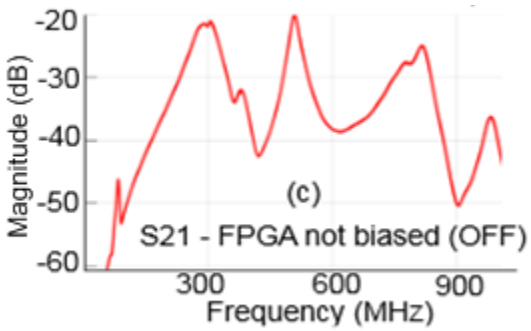


Fig. 5.16: Magnitude of the S21 response when FPGA is not powered or biased.

As even FPGA is not biased or OFF as suggested from Fig. 5.16, the S21 value is below -20 dB which suggests that beyond -20 dB the response is not due to the internal circuit (buffer and routing) but rather it is due to external factors like coupling between 50 Ω lines for instance.

From Fig. 5.15 it is observed that each FPGA of same family etc. with same buffer circuits and routing gives a different S21 response. The cut off frequency is determined by sort of filter behavior of the buffer and R, L, C components of the wire / interconnect / routing. This determines even if the devices are of same family and configuration; their PV effects can be exploited by the guided EM waves that can accentuate a difference in the response from each device. As stated in this section, S21 parameters are different for same family FPGAs when subjected to exact similar measurement (RF wave etc.). These differences in the S21 have been utilized in the further part of the study to determine a sort of identification for each FPGA. The illustration has been described in the following part of the chapter.

The next sub-sections demonstrate about using two post-processing techniques that have been applied on the S21 response from the measurements shown in this section. Indeed, in GEMT based technique for authentication, we have implemented two post-processing techniques. One technique is cosine similarity (CS) based that is more towards finding the amount of overlap between inter and intra device scores. The other approach is implementing a binary fingerprint from the same measurement responses.

5.5.2 Cosine Similarity based post-processing

Similar to the post-processing technique of the REMT based authentication as discussed in chapter 3, we have utilized Cosine similarity (CS) with this approach also. The detail description about the CS has already been done in chapter 3. For the cosine similarity, we have used the complex domain taking into account both the frequency and phase information. CS is calculated in the bandwidth of approx. 550 MHz to 750 MHz, where the distinction is highest among all the response (see Fig. 5.15). For an authentication, the entity is checked with the previously stored values of database. An authentication attempt is respectively expressed as the false rejection rate or FRR, and as the false acceptance rate or FAR of the system. FAR expresses the security of an authentication system. A detailed description of FAR and FRR has already been discussed in chapter 3.

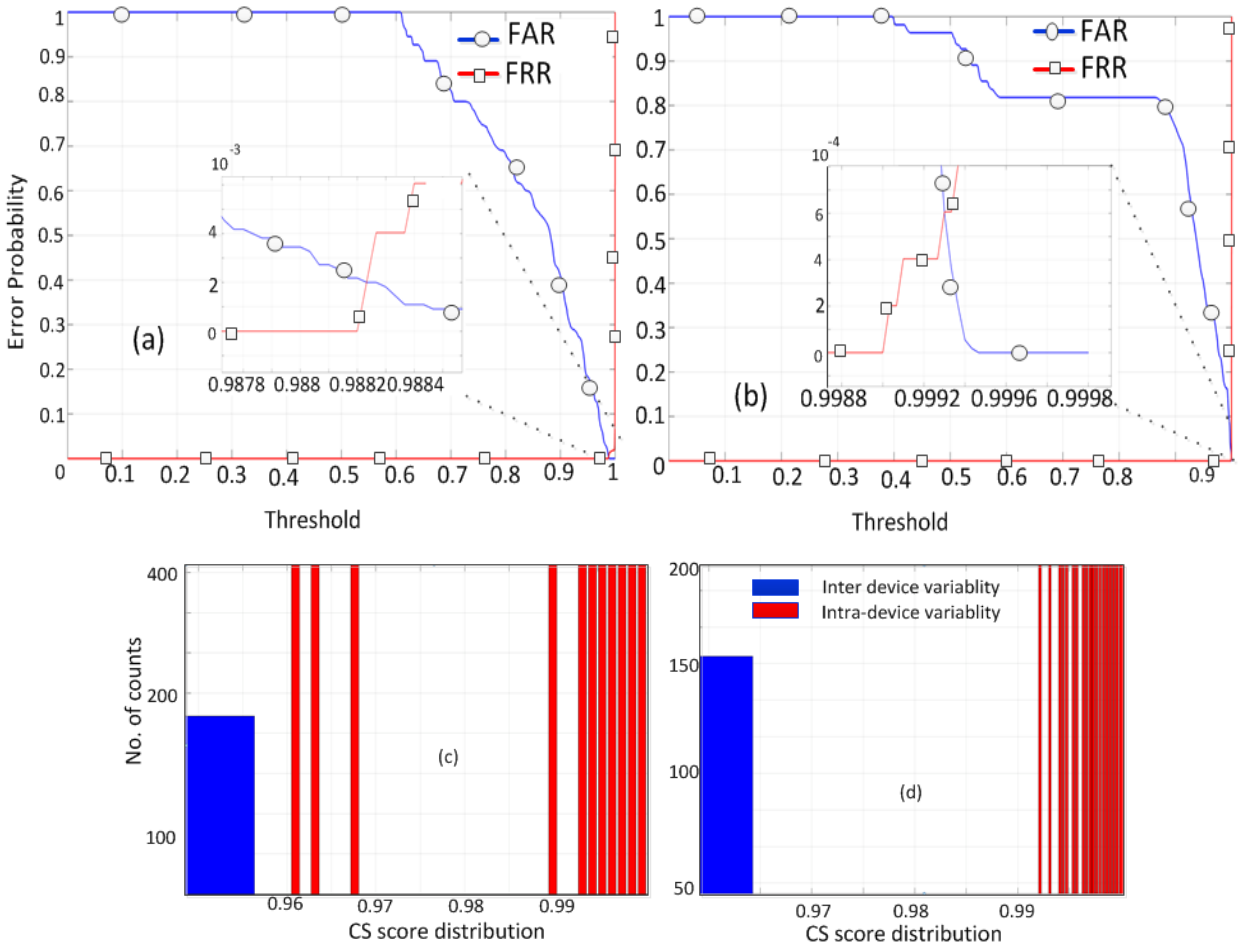


Fig. 5.17: The error probability curves showing the distinction and overlap between FAR and FRR with inset zoom on overlap of FAR and FRR. (a) Error probability curve for route 1. (b) Error probability curve for route 2. (c) CS score distribution of inter and intra variability for route 1. (d) CS score distribution of inter and intra variability for route 2.

From the results of Fig. 5.17, it is clear that the overlap error or error probability between the inter device and intra device variability for all the FPGAs have been very less. The distribution of CS score of all measurements of both routes highlighting inter and intra device variability is depicted in Fig. 5.17 (c) and (d). For route 1(shorter route) in Fig. 5.17 (a) it is observed to be around $2*10^{-3}$ and similar for route 2(longer route) in Fig. 5.17(b) it is round $6*10^{-4}$. Such low values of error probability (for both route) validates that it is possible to implement such an approach to distinct devices (FPGAs) based on their RF characteristics. This can be effective for the purpose of authentication of FPGAs using guided RF waves. Hence based on the S21 responses, we have been able to find a good distinction between two FPGAs even if they are of same family, series or manufacturers.

5.5.3 Concatenation (combination) of responses from two routes – post-processing

In the above part, we have used the results from the routes individually. The other approach that can be applied is the concatenation or combination of two routes to generate a combined signature. The idea of concatenation of the routes is to increase the effects of PV the FPGA (DUT) by increasing the physical randomness. The combined response from two routes can be assigned as one signature for that FPGA and using that (signature from combined route) the error probability can be calculated. An illustrative description is given in Fig. 5.18. From Fig. 5.18 we can observe that individual responses from FPGA 1 - 'R1' and 'R2' - can be used together to create a combined response 'R' for same FPGA. The concatenated response 'R' can be attributed as a response of the FPGA, which can be used further for authentication of the FPGA1. This procedure has been adopted on the response of all the 11 FPGAs.

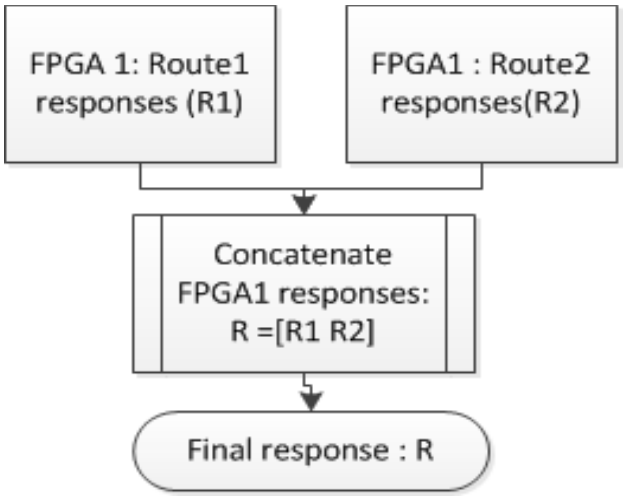


Fig. 5.18: A use case showing the concatenation of two routes response for one FPGA.

To find the effect or usability of the concatenation of the response of the two routes, we have evaluated the error probability of the concatenated response. We can observe the error probability from Fig. 5.19(a). From error probability curve shown in Fig. 5.19(a), we can observe that error rate is around $5*10^{-8}$. This error probability is much lower than that observed by doing CS based post-processing on the response from the routes separately. Secondly, the observed error probability (in Fig. 5.19(a)) with concatenated routes is approximately equal to the multiples of the error probabilities of the two routes separately.

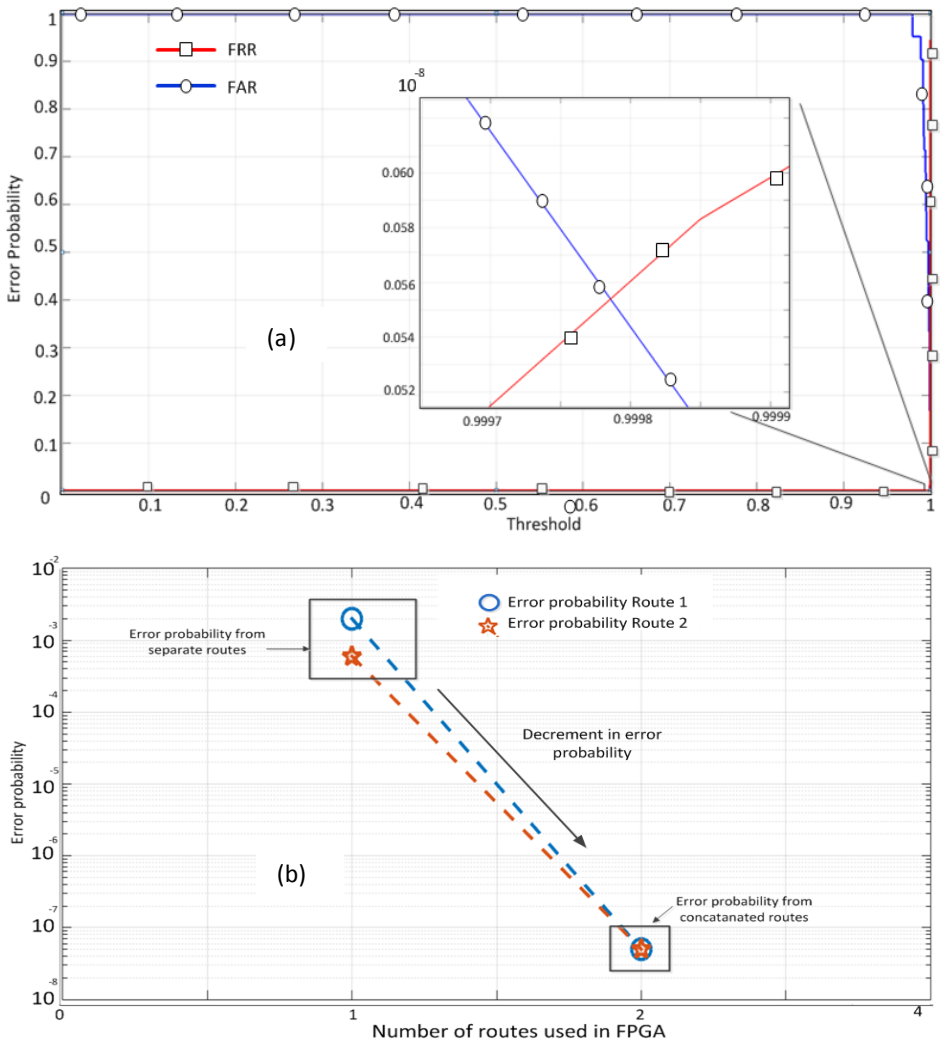


Fig. 5.19: Results after concatenating the routes. (a) The error probability curves showing the distinction and overlap between FAR and FRR when the processing is done with the combined or concatenated routes for all the FPGAs. Inset zoom of overlap of FAR and FRR. (b) Change (decreasing trend) in error probability between separate and concatenated routes.

From Fig. 5.19(b), a decreasing trend of error probability when single route (separately) is used and when two combined or concatenated routes are used. Also, when separate route are used the error probability is about $10^{-2} \sim 10^{-4}$ and for the concatenated routes it is around 10^{-8} (refer Fig. 5.19(b) also).The results from concatenated routes (see Fig. 5.19(b)) points to the fact that using more than one routes on the same FPGA (on same IO ports), we can obtain a lower error probability than using only one route. This result justifies that we can use multiple routes (increase the PV effects) on same FPGA on the same IO ports in order to increase the distinction in the response between two FPGAs of same family, manufacturer etc. Furthermore, the multiple routes (two routes in the case here) can also be utilized to counter for the

systematic error from the PCB and aging related effects. The detailed analysis of mitigation of systematic errors and aging related issues has been given in section 5.7.

Extending the post-processing approaches in this chapter we have also opted to convert the response from the S21 parameter into binary fingerprint and compute the error probability between the inter and intra FPGA distribution.

5.6 Binary fingerprint generation

Along with the signatures generated in the preceding part of this chapter, it would be advantageous if we can also generate binary fingerprints from the same measurement and results of two routes. The usefulness of binary fingerprints is that it is easy to store them digitally. The response from Fig. 5.15 (section 5.5.1) is utilized for these steps.

As observed from the above part, S-parameters are used to characterize electrical networks using matched impedances. S-parameters allow a device to be treated as a black box with inputs and resulting outputs [7]. Note that S-parameter is an analog complex signal. To quantify the output responses into binary fingerprint, we have converted the analog response into binary streams using Gray coding scheme.

5.6.1 Converting S21 response into binary

The idea in this part of manuscript is to convert the S21 response into binary fingerprint. To do so, for a particular chosen magnitude level of S21 response, its corresponding frequency value (magnitude) is selected. The magnitude of the frequency value is converted into binary form by using Gray coding scheme. The utility and advantages of Gray code has been discussed in the next sub-section.

In order to utilize the S21 curve into generating the binary fingerprints, the steps adopted is shown in the Fig. 5.20. Applying the procedure from Fig. 5.20, we can utilize the frequency and forward transmission coefficient (FTC) relationship. This relationship determines the selection of few points over the curve which can give frequency values, which are further encoded into binary fingerprints. In order to generate

the binary fingerprints from the response, the results from the two curves have been concatenated or combined together. A detailed procedure is given below in next sub-section.

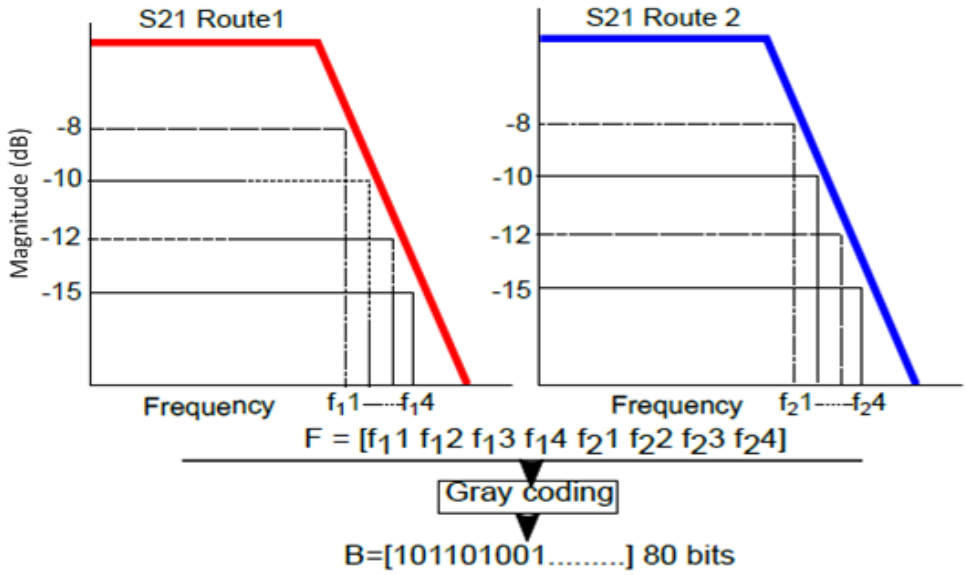


Fig. 5.20: Generating binary coded fingerprints using binary encoding technique code from S21 curves response from two routes. The relation between power and frequency is used as a metric.

The idea has been to extract the information between FTC and frequency of the S21 curve as shown in Fig. 5.20. We have only considered the magnitude of the S21 response in order to perform the post-processing technique using binary encoding method.

5.6.2 Procedure for conversion of FTC into binary code

A systematic approach that has been used in this manuscript for getting a binary response from the S21 response has been detailed out in this sub-section.

Let us say at FTC level '–X' dB, for an *n*th FPGA, we get a frequency value of *fn*, this value of *fn* is converted into binary stream using Gray code. The choice of the FTC levels depends upon following factors. The S21 magnitude should be above -20 dB value. Following the above three points, the magnitude level selected in this study are -8 dB, -10dB, -12dB and -15dB. In this study the response of two routes are concatenated as shown in (1):

Routes R = {R1 , R2}

Magnitude level (P) = {-8,-10,-12,-15}dB

Fingerprint *FR1* = R1{P} i.e. R1{-8}R1{-10} so on

Fingerprint *FR2* = R2{P} i.e. R2{-8}R2{-10} so on

Fingerprint from two responses *Ftot* = [R1{P} R2{P}]

Concatenated Fingerprint *Ftot* = [f_n1 f_n2 f_n3…$f_{n+1}1$ $f_{n+2}2$ $f_{n+3}3$] ---------- (1)

The theoretical description to get a binary fingerprint from the S21 curve has been given in (1). In the implementation, we have opted to use a small range of S21 magnitude - (small range of -0.0006 dB). For the varying range of S21 magnitude in that small range, there are different frequency values. Finally, the mean or average of the different frequency values is calculated. A pictorial description has been given in Fig. 5.21. We can observe from Fig. 5.21 that for magnitude level between -10 dB to -10.0006 dB, several frequency values (in ranges of 689.9255 to 689.9231 MHz) are obtained. In Fig. 5.21, we have named the frequency values as '*f*'. The mean value of *f* is calculated. The obtained mean value is subjected to conversion to the binary fingerprint using Gray coding scheme.

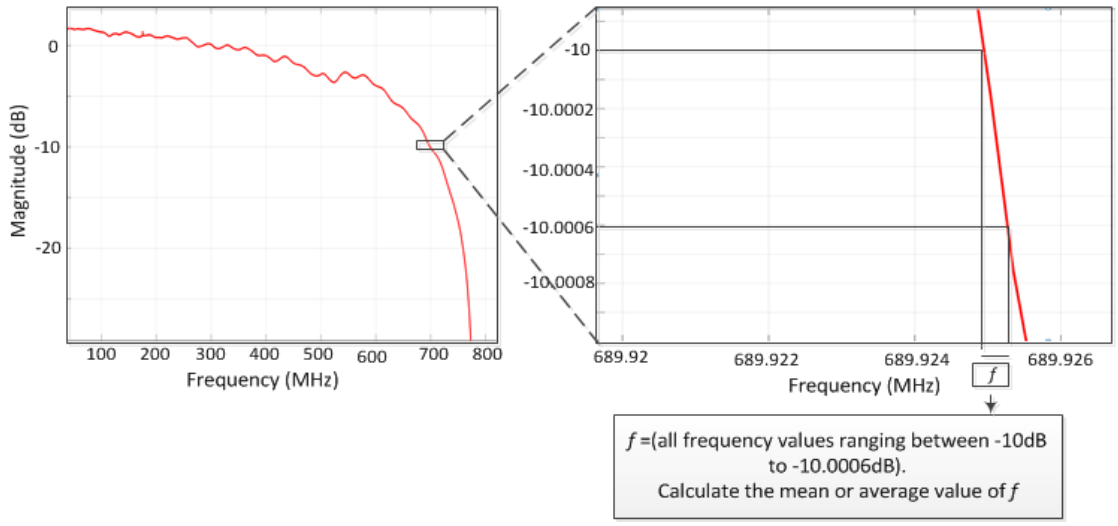


Fig. 5.21: An illustration to highlight the steps used in using the FTC response in order to convert the frequency values into binary fingerprints. Inset zoom on the small range of S21 magnitude used.

The obtained fingerprint values from particular FTC and frequency curve are adaptable to be in 10 bits range. The total number of bits is concatenated from two routes and finally 80 bits fingerprint is generated for one FPGA. Fingerprints obtained in above section can be effectively used for the authentication of

FPGAs. To determine the authenticity and randomness, the obtained hamming distance and entropy has been used as metric.

5.6.3 Advantages of using Gray code for binary encoding

Since we have utilized Gray coding technique for binary encoding, hence we have given a small description of the uses and advantages of Gray coding technique over conventional decimal to binary conversion. A Gray Code represents numbers using a binary encoding scheme that groups a sequence of bits so that only one bit in the group changes from the number before and after. The Gray code scheme is used because there is only one bit difference between two successive numbers. We chose the Gray code because difference between two consecutive numbers in Gray code is always equal to 1. This property makes this code very useful for the steadiness of the responses. Conversely, the binary code can lead to errors in the analysis of steadiness [15].

A simple example stating the difference in the Gray and binary code has been depicted in Table 5.1. It is detrimental from Table 5.1 that the use of binary code when there is change around 2^n value, there can be difference of more than 1 bit even if the decimal difference is 1. For example the difference between 31 and 32 in decimal is 1 however in binary digit there is difference of 6 bits. However in Gray code there is difference of only 1 bit which is more in coherence with the decimal value difference [8].

Table 5.1: Example of the difference between gray and binary code for two consecutive values

Decimal Value	Binary Value	Gray code
$31 = 2^5 - 1$	00011111	00100000
$32 = 2^5$	00100000	01100000
Hamming Distance (31,32)	6	1

5.6.4 Results from binary encoding technique

After performing the conversion of S21 response to binary using Gray coding technique, we have opted to find the error probability and statistical distribution to determine the difference between an inter and intra device variations.

The determination of the FAR and FRR based on the overlap of the inter- and intra-Hamming -distance (HD) histograms are shown in Fig. 5.22(a). The inter HD which quantifies the uniqueness of the response is around 38 % (which is slightly less than optimal value of 50%). HD of 50 % is optimal because this is the case, when exactly one half devices generate a bit 0 and the other half devices generate a bit 1. Also, in the security it is important that the device generate equal number of 0 and 1 in order to have high randomness. This also dictates the optimal percentage of HD. Furthermore, as the number of devices increase in the processing the optimal HD observed is close to 50 %. Also in terms of biasing, an unbiased bit should have an outcome close to 50 %, which is the case when half of the devices generate the bit as 0 and the other half generate it as 1. An outcome of 0 % (or 100 %) means that the bit was 0 (or 1) on all devices, which is an indicator for poor inter-device uniqueness [18].

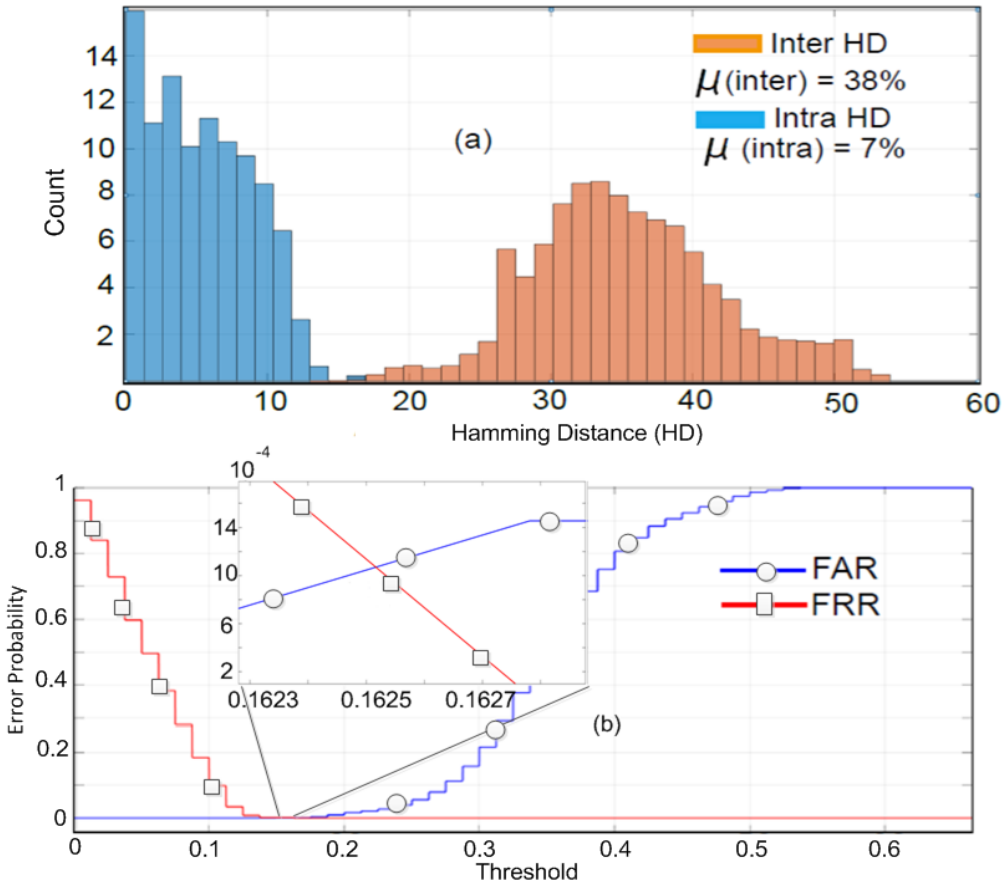


Fig. 5.22: Hamming Distance and error probability curves. (a) Hamming distance between inter and intra devices. (b) Error probability curves between FAR and FRR. Inset zoom on overlap of FAR and FRR.

The error probability or overlap between FAR and FRR as depicted in Fig. 5.22(b) is very less and is less than 10^{-4}. The lower error probability shows that using this methodology and post-processing technique it is efficient to find distinction or separation among the various devices (FPGAs) of same family, series, manufacturer etc. This can be effective for the purpose of authentication of FPGAs using guided RF waves. The maximum bit entropy (metric of randomness of bits) is 0.98 and minimum is around 0.92 for all the 11 FPGAs over 10 repeated measurements.

The results observed from Fig. 5.22 justifies that with 80 bits signature obtained using non-invasive guided wave RF approach it is possible to find an optimal HD and error probability to determine the inter and intra device variation for 11 FPGAs. The threshold is used to decide on a positive identification depends on the separation between the intra-distance and the inter-distance histograms. If both histograms do not overlap, an errorless identification can be made by placing the threshold somewhere in the gap between both histograms. From Fig. 5.22(a) we can observe the intra and inter HD for different measurements done on 11 FPGAs. Also, from Fig. 5.22(b), an error probability of around 10^{-4} has been observed. The result from Fig. 5.22 validates the fact that using binary fingerprint also we can clearly find the distinction between 11 FPGAs of same family, manufacturer etc. This can be used for the authentication of FPGAs.

Before, going into the next section, we would like to summarize the results obtained from two post-processing techniques. Using CS based, the error rate observed for both the routes are in the range of 10^{-3} to 10^{-4} - fairly low. Secondly, in the binary generation schemes the overlap of inter and intra HD has been low of around 10^{-4}. Of course, the mathematical treatment using CS is different than that of the binary fingerprint technique.

In CS based technique, we have used both the magnitude and phase response of the response. However, in the binary fingerprint technique, the frequency magnitude has been encoded into binary format. Even though both the post-processing techniques have been different, both the results give a fairly high confidence in using the GEMT based setting in order to find distinct signature and fingerprints for the authentication purpose from FPGAs of same family, manufacturer, series etc.

The next sections are dedicated to investigate the methodology to mitigate the effects of systematic error coming from external source such as PCB, power line etc. Along with this we have also detailed a technique which can be used with GEMT method in order to overcome the aging effects on this authentication methodology.

5.7 Multi-route implementations in GEMT based method

After obtaining the results from both the post-processing techniques we have extended our approaches to implement a setting that can mitigate the effects of systematic errors and other external disturbances. On the PCB, the signal propagates not only into the DUT but also on transmission line of the PCB. Difference in realization of this line (but also soldering effects) can affect the signal, so the difference observed previously are also affected by the PCB effects but not only linked to the DUT. In other application, where a plug and use setting can be done, in that case we do not need any technique (described below) to counter for the systematic error.

One of the methods to do is to implement a multi-route structure. The multi-route setting can be used to remove the effects of systematic error coming from the PCB [16] and other external errors. In the multi-route structure we have implanted two routes on same or different IO ports and calculated the difference between the responses of two routes. This way we have made an endeavor to suppress the effects of systematic error and aging related issues which FPGA or DUT faces. We have already studied and implemented in detail about the effects of aging based stress on the ICs in chapter 4. Here we want to use the same principle i.e. compare to route after aging effects. The results should be independent from aging. The other aspect using more than one routes also points to that fact that we are not restricted to use only one route between IO ports but rather multiple routes can be involved in this study. The different techniques (routing techniques etc.) that can be applied for the purpose of countering the systematic errors have been discussed in the sub-section below.

5.7.1 Two routes on same IO ports

Using single buffer on one route can be easily impacted by the aging effects, systematic error etc. This can of course cause adverse effects on the authentication protocols. Therefore, if the device gets old it can become complicated and inefficient to utilize this methodology.

This technique is aimed at calculating the difference between the S21 responses on multiple routes. One of the factors that can effects the response and measurement is systematic error and aging effects coming from the PCB. This can have huge implications on the results. In order to determine the effects coming from the PCB and aging effects, we have implemented a methodology that can mitigate its effects. To do so, we have implemented two routes on the same IO ports. The two different routes have been established

on the same IO ports. The setting in Fig. 5.23 is similar to the one that we have used in section for the purpose of generating signatures for authentication purpose (see section 5.5). The same approach is utilized here in order to understand its utility in countering the systematic errors. The effects of PCB systematic error and aging effects act upon the two routes uniformly or equi-proportionally. Therefore, if we chose to use the difference between two routes, the effects of systematic error and aging effects on both the routes can be reduced.

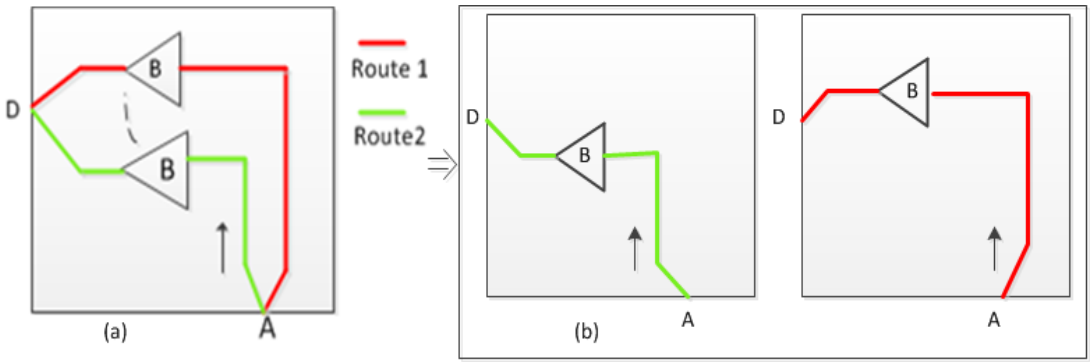


Fig. 5.23. Multi-route technique adopted in order to mitigate error and aging effects. (a) Depiction showing the two or multiple routes on same IO ports. (b) Both the routes have been separately shown for clarity.

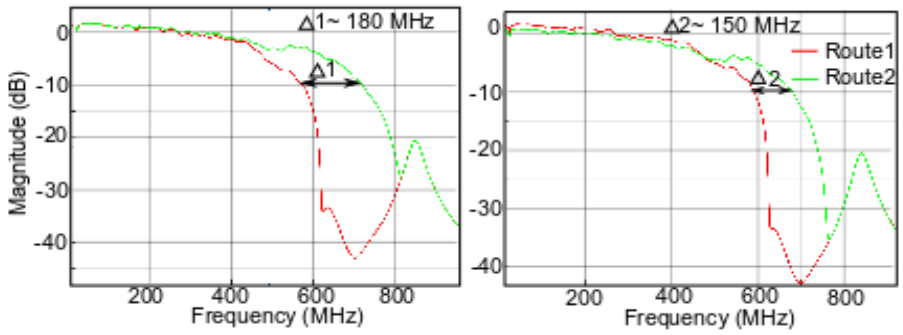


Fig. 5.24: S21 response from the two routes and the differences between the responses from two routes on two FPGAs.

This way it is possible to mitigate any disturbance or error coming from the PCB itself. A pictorial depiction is given in Fig. 5.23(a) and (b) which highlights the two routes being implemented between same IO ports viz. 'A' and 'D'. From Fig. 5.23, we can observe that a buffer circuit has been implemented across different routing on same IO port.

I. Difference in frequency values at particular S21:

One approach to process (mathematically) on the two routes technique (multi-route) is to find the ***difference in frequency values of the particular S21 magnitude***. This treatment method can be applied in cases where the effects of aging are encountered. Taking reference from chapter 4, which shows that aging based variation affects the FPGA homogeneously, similarly here also the two routes would get effected equally with the effect of aging on the FPGA – their difference remains constant with time (or aging). The results from the implementation depicted in Fig. 5.23 have been shown in Fig. 5.24. In Fig. 5.24, we have highlighted the frequency difference at around -10 dB of S21 magnitude. This difference is calculated multiple times (for multiple measurements) to have robustness of results. The results in Fig. 5.24 uses the difference between the frequency values at particular magnitude of S21 can be used to mitigate the aging related effects.

II. Difference between two routes S21 responses:

Another approach is to find the ***difference in the S21*** response from the two routes. This approach also encounters for the systematic and aging related error that FPGA can encounter when subjected to the measurement, considering that systematic errors and aging effects are equi-proportional and affects the two routes homogeneously.

From Fig. 5.25 we can observe the difference in the magnitude of the S21 responses from the two routes Observing from Fig. 5.25(b) the difference in relation with the external part of the FPGA (or IC) is the same for the two routes, so by doing the difference, this variation which is not linked to the FPGA can be easily removed. In Fig. 5.25(b) the results for difference of some FPGAs have been shown in magnitude only. However, while calculating the error probability, we have used the complex domain.

The error probability observed for 11 FPGAs over repetitive measurements is depicted in Fig. 5.25(c). In this case error probability is around $1.82 * 10^{-2}$. This is slight higher than what we obtained for previous cases (separate routes and concatenated routes cases in section 5.5) but with the difference we are able to remove the systematic errors. Also, by increasing the number of routes, and calculating difference by taking one route as reference, we would be able to reduce the error probability further and simultaneously reduce the systematic errors also.

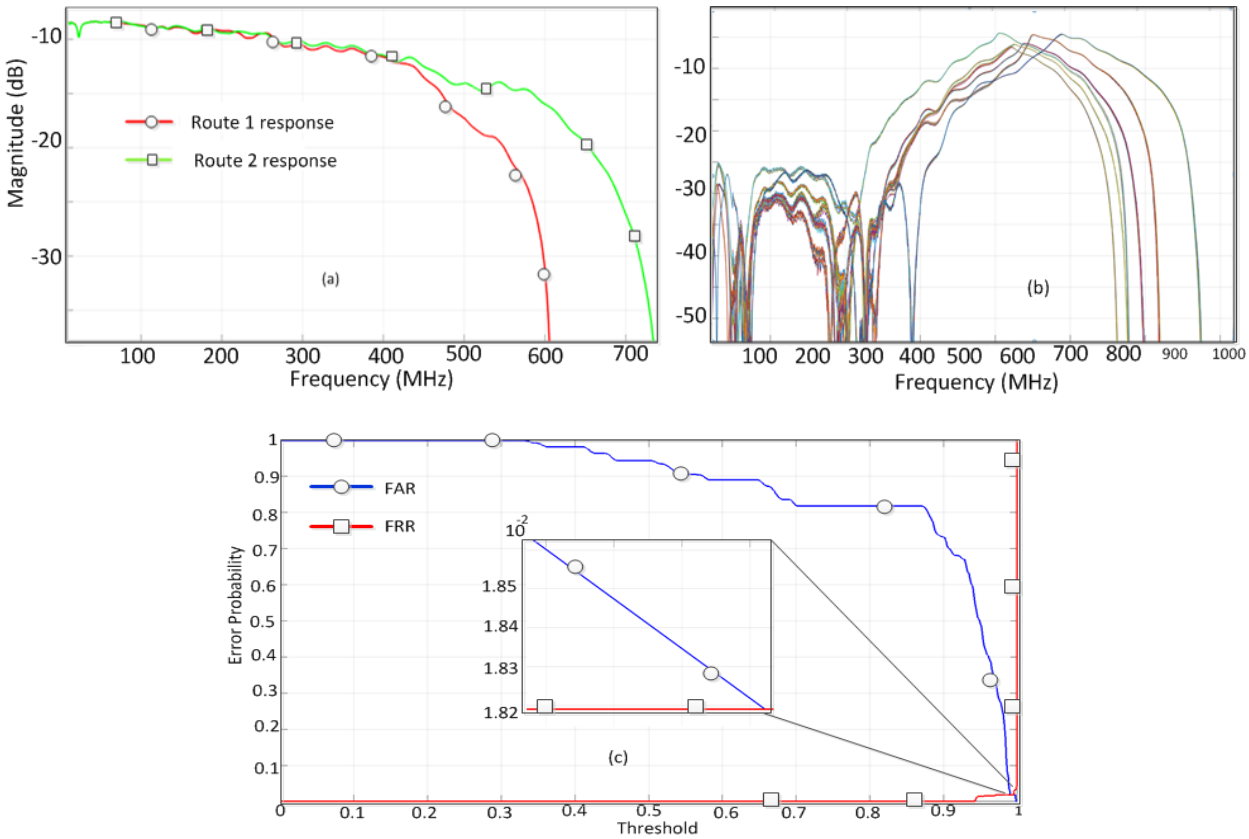


Fig. 5.25: Difference in the magnitude of S21 response to mitigate the effects for systematic and aging related error. (a) S21 response from the two routes. (b) Difference in magnitude of the S21 response for various FPGAs. (c) The error probability curves showing the distinction and overlap between FAR and FRR when the processing is done with the difference of the routes for all the FPGAs. Inset zoom of overlap of FAR and FRR.

Therefore, multiple route technique along with the calculation of the difference between routes is a suitable choice because it can remove the error from measurements (systematic), so the final signal after difference is directly linked to the FPGAs (IC) not to any other components.

This technique can also be useful in mitigating aging effects; however this part of study has not been done here.

5.7.2 XOR Gate based approach – two routes with XOR

Another approach to find difference between two routes in a FPGA is by implementing a XOR gate between the two inputs. The XOR gate can work like a phase detector [17]. Hence based on the difference

of the phase between the two guided waves on two input ports, it is possible to find the difference using XOR gate. An implementation example for XOR with the input-output wave from is shown in Fig. 5.26.

From Fig. 5.26, it clear that as the response or phase of the two input signals are same the output is zero and if the two input waves have difference in the phase the output is high. This technique can be applied on multiple routes, where in the phase of same incoming RF wave can vary when traversing through the FPGA, based on the length of the route. This technique can be used in generating a signature and identity of the FPGA also. Along with this differential approach, aging and systematic error can also be mitigated. An illustrative implementation is shown in Fig. 5.26.

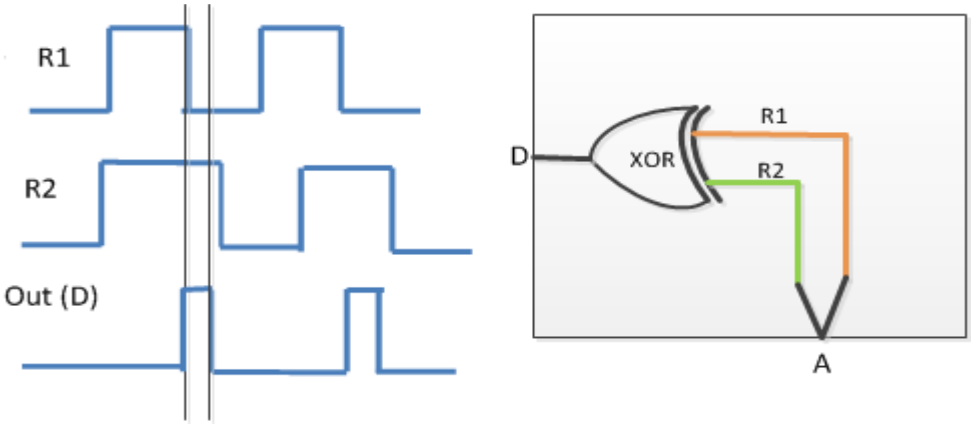


Fig. 5.26: Implementation of XOR gate to find the difference between two routes – based on phase difference between RF waves on two routes.

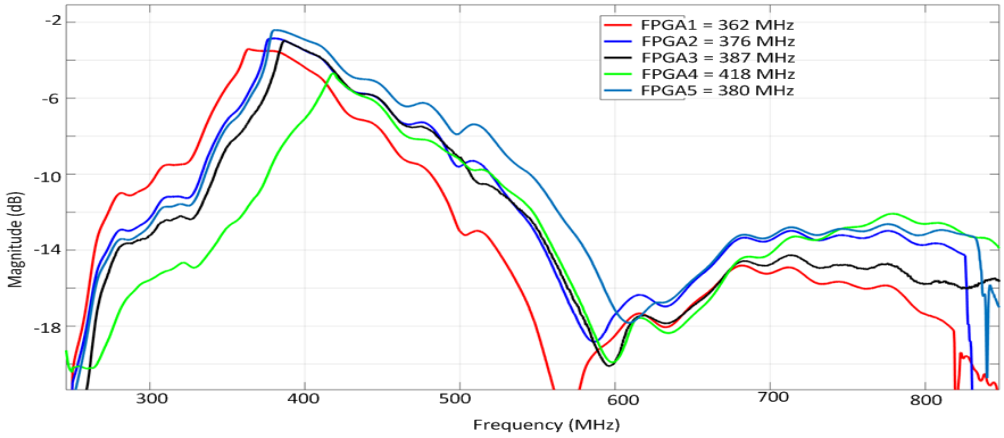


Fig. 5.27: The response from the XOR based implementation on 5 FPGAs. The peak frequencies have also been shown in legend.

For implementing the structure shown in Fig. 5.26, we have programmed the FPGA with a XOR gate between IO ports. Owing to slight differences between the routing lengths from input port A to the output port through two paths of the XOR gate, there is a phase difference between the incoming RF waves. This difference is detected by the XOR gate. The output for the few FPGAs tested with this approach has been shown in Fig. 5.27. The response from Fig. 5.27 can also be used to generate the signature of FPGA for the purpose of authentication.

The response from Fig. 5.27 shows a distinction which points for the fact that FPGAs can be distinguished using this technique also. The authentication part of the study using the XOR based technique can be one of the interesting aspects for the future work.

From the multi-route based implementation we have shown that it is possible to implement multiple logics or settings in the FPGA and perform RF guided wave measurements. The multi-route technique can be used in many aspects viz. mitigating systematic error and aging effects, generate signature from FPGA etc. Many of the aspect can be broadly studied and has been part of ongoing and future work.

5.8 Limitations and drawbacks of GEMT based technique

Given the novelty of this approach, there can be few aspects that may need to improve in the future works to make the methodology more robust and efficient in implementation. As a proof-of-concept this study shows that a new methodology to investigate the authenticity of IC can be implemented without the need of extensive VAC implementation or post-processing circuit.

Some of the drawbacks or the areas to be worked upon are:

I. For a real implementation, characterization with a higher number of DUT has first to be done

II. The measurement setup can be cumbersome and specialized. It requires the incorporation of various tools and instrument settings. Hence for a non-industrial set up this method can be too heavy to be executed.

III. The DUT requires a customized special PCB. Hence it can be time taking and may not be easily adapted to some of the IC package. However, given the advancement in technology, there are many PCB which can allow plug and play situation. So several ICs of same package can be

embedded on the same PCB and the measurements can be performed. Hence, this can mitigate the need to develop a customized PCB.

IV. The post-processing part in this study can always be improvised upon. In this work however a proof-of-concept of different fingerprint creation mechanism has been detailed. Therefore post-processing scheme can be made robust.

Even if improvement can be done on the present method, the results obtained can be a very positive sign. It shows that even without using any specialized circuit or markers in the DUT (FPGA) it is possible to generate signatures and binary fingerprints which are distinct in nature for each FPGA. Of course there can few aspects which may need improvement; the present concept can be used as a backbone going forward.

In the REMT technique also we have seen that aging can play a vital role in the determining the robustness of the authenticity of the IC. ICs do get affected by variations from external factors or from their own usage over period of time. In GEMT based method, we have however not performed the aging measurement (thermal stress etc.), rather this can become an interesting work for the future use. Even if there is no measurement results for aging in GEMT based scheme, we have made an effort to optimize our implementations which can be used to mitigate the aging effects in the future work.

5.9 Conclusion and discussion of GEMT based approach

This chapter has given an overview of utilizing the guided EM wave as a mean to interrogate the underlying PV effects of the IC. The idea is to generate signature and fingerprints of ICs by being non-intrusive in our effort. There is no requirement to dedicate a particular area of IC for the implementation of any variability aware circuit (VAC) or post-processing circuit. With the size of IC shrinking it is very important that the vendors or manufacturers investigate on approaches that are non-intrusive, low area consuming and easy to implement.

The proposed novel method of GEMT based approach; along with CS based signature generation also has been effectively used to generate binary key pertaining to each DUT by using very basic circuit elements. There is no stringent requirement to implement a particular type of circuit to exploit the PV effects. The obtained fingerprints and signatures after post-processing has been subjected to mathematical treatment to

observe the error probability, entropy rate, uniqueness and robustness parameters. The results have shown that it is possible to extract signatures and binary fingerprints that have enough randomness to be unpredictable, fairly unique and robust. The error probability obtained using CS based technique has been fairly low. We have also shown that using more than one routes in a FPGA, error probability can be decreased further hence enhancing the distinction between the FPGAs.

The strength of key generated in binary fingerprint technique can be further increased given the fact that S21 parameters or curve provides enough information to generate fairly large number of key length. The study conducted has shown a proof-of-concept that even without the implementation of the dedicated circuit, the PV effects of an IC can be exploited. Through the study we have focused only on using the basic buffer circuit (as logic element of FPGA) and interconnect (or wire). These two circuit elements have provided electrical and physical variability enough to be exploited by the incoming EM waves.

As a summary we can conclude this chapter by highlighting few points:

I. The EM waves have been used as viable option to interrogate the underlying PV effects of IC. The response from EM waves for each IC has been used to generate a set of fingerprints that can be used for the authentication purpose.

II. Physical implementation shows that the area overhead involved is minimal. As we have only used basic circuit elements of buffer and interconnects or wires.

III. The methodology along with the post-processing technique has shown that PV effects interrogated with the EM waves have been able to generate a strong key which can serve as ID or fingerprint for each FPGA or DUT.

The study so far conducted validates that GEMT based method can be efficiently used to mitigate counterfeiting techniques applied on new ICs. The counterfeiting techniques such as overproduction, supply chain theft, cloning etc. which are performed on newly manufactured ICs can be thawed by using GEMT based approach. The effects of PVT variations has not been taken into account when conducting the study of GEMT approach but it has been shown that extending the adopted technique further, in future effects of PVT variations can be taken in account along with the techniques that can mitigate the effects of aging or other anomalies. Through multi-route approach, it has been shown that systematic error from PCB etc. can be mitigated.

5.10 Overall summary of authentication mechanism

5.10.1 Comparison of REMT and GEMT

This section summarizes both the REMT and GEMT based techniques. Here we have made a final summary of both REMT and GEMT based authentication techniques. The next chapter (chapter 6) highlights the application of RF FPGA PCB for the purpose of RF and wireless applications. Hence we have summarized the work, results and conclusion related to authentication in this section.

On the lines of EM based techniques we have also adopted two methods: one based on EM emission and other one is based upon the use of the guided EM waves or GEMT. The GEMT based technique has one limitation that it requires a customized PCB. Secondly, the idea of GEMT is based on interrogating the physical variability of the FPGAs using an incoming EM wave. Indeed, the effects of variation due to the input power can be taken into account. However, in this study we have used only one power level but in future work this parameter can be studied. A comparison between GEMT and REMT is detailed out in Table 5.2.

Table 5.2: Comparison of REMT and GEMT methodologies for authentication of IC.

	REMT	**GEMT**
Non-intrusive	Yes	Yes
Dedicated circuit or VAC	Somewhat	Not exactly
Ease of implementation	Yes	Somewhat
Dedicated setup required	Somewhat	Yes
Efficiency of method	High	Not so high

Both the approaches however can be used in mitigating counterfeiting of components. The implementation of the REMT can be done with the end user more practically, but in case of GEMT, it is more viable choice for an end user which is an industrial setup. REMT can be applied in business to customer forefront but GEMT is better choice for the business to business scenario.

5.10.2 Discussion – Overall authentication based on EM approaches

This work (up to chapter 5) has been based upon finding unique fingerprint for an IC which can be further used for the purpose of authentication. The study has focused on using non-invasive methods that can be implemented by using EM based approaches. An IC emits considerable amount of EM emission during its switching states. This EM emission itself is a function of various PV effects of the IC hence emitted EM from each IC has been processed for the purpose of generating unique signature for each IC.

To validate the approach we have implemented the measurement across various FPGAs of different families and MCUs respectively. The response has been treated by off the chip post-processing evaluation methods which have been able to find a statistical distinction among the fingerprints of various DUTs. The results have clearly shown that a lightweight non-invasive technique can be easily used that can generate response for each DUT. Also with REMT based method in chapter 3, we have shown that even if dedicated variability aware circuits not expendable to be implemented in a device (like in microcontrollers - MCU), still exploiting EM signature is a viable option. Especially in case of MCU we can observe that without using any external implantation we have been able to authenticate 12 of MCU boards. Of course going forwards more enhanced techniques can be implemented but the current study validates the fact that it is very much possible to authenticate an IC without using expensive external implementations in the IC. Also with REMT, there is no need to perform any kind of changes to the PCB design etc.

The GEMT based method has been also utilized which also offers a highly efficient solution pertaining to non-invasive method using EM approaches. The idea as described in above parts of this chapter uses the fact that incoming guided EM wave can be disturbed by nano-scale related physical variability of the IC. This has been used to generate fingerprints and signatures using a post-processing technique.

References:

[1] S. A. Wartenberg, "Six-Gigahertz Equivalent Circuit Model of an RF Membrane Probe Card," *IEEE Trans. Instrum. Meas.*, vol. 55, no. 3, pp. 989–994, Jun. 2006.

[2] A. Persano *et al.*, "Wafer-level thin film micropackaging for RF MEMS applications," in *2016 Symposium on Design, Test, Integration and Packaging of MEMS/MOEMS (DTIP)*, Budapest, Hungary, 2016, pp. 1–5.

[3] "fpgas_for_dummies_ebook.pdf.".[Online].Available: https://www.amiq.com/consulting/misc/free_pdf_books/fpgas_for_dummies_ebook.pdf

[4] "SPARTN3AN.pdf.".[Online].Available: https://www.xilinx.com/support/documentation/data_sheets/ds557.pdf

[5] P. K. Ikalainen, "An RLC matching network and application in 1-20 GHz monolithic amplifier," in *IEEE MTT-S International Microwave Symposium Digest*, Long Beach, CA, USA, 1989, pp. 1115–1118.

[6] S. Ghosh and K. Roy, "Parameter variation tolerance and error resiliency: New design paradigm for the nanoscale era," *Proc. IEEE*, vol. 98, no. 10, pp. 1718–1751, 2010.

[7] M. M. Ahmed *et al.*, "Radiated Electromagnetic Emission for Integrated Circuit Authentication," *IEEE Microw. Wirel. Compon. Lett.*, vol. 27, no. 11, pp. 1028–1030, Nov. 2017.

[8] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 1, pp. 97–109, Jan. 2018.

[9] A. E. Abdulhadi, S. Mandev, and R. Abhari, "Signal integrity and EMI evaluations of an RFID-Sensor tag for internet-of-things applications," in *2015 IEEE Symposium on Electromagnetic Compatibility and Signal Integrity*, Santa Clara, CA, USA, 2015, pp. 128–132.

[10] X.-P. Chen, "Analysis and application for integrity of PCB signal," in *2010 2nd IEEE International Conference on Information and Financial Engineering*, Chongqing, China, 2010, pp. 328–331.

[11] H. Kinzelbach, "Statistical Variations of Interconnect Parasitics: Extraction and Circuit Simulation," in *2006 IEEE Workship on Signal Propagation on Interconnects*, Berlin, Germany, 2006, pp. 33–36.

[12] F. J. Twaddle, D. R. S. Cumming, S. Roy, A. Asenov, and T. D. Drysdale, "RC Variability of Short-Range Interconnects," in *2009 13th International Workshop on Computational Electronics*, Beijing, China, 2009, pp. 1–3.

[13] "The Wire.pdf." .[Online]. Available http://bwrcs.eecs.berkeley.edu/Classes/icdesign/ee141_f01/Notes/chapter4.pdf

[14] A. Kayssi, "Macromodeling C- and RC-loaded CMOS inverters for timing analysis," in *Proceedings of the Sixth Great Lakes Symposium on VLSI*, Ames, IA, USA, 1996, pp. 272–276.

[15] W. Liu and W. Zeng, "Scalable Non-Binary Distributed Source Coding Using Gray Codes," in *2005 IEEE 7th Workshop on Multimedia Signal Processing*, Shanghai, 2005, pp. 1–4.

[16] Y. Zhao, Yan Wei, Feng Zhiming, Y. Luo, Li Shijin, and Yue Dong, "Investigation on radiated EMI noise identification for high speed digital PCB," in *2009 5th Asia-Pacific Conference on Environmental Electromagnetics*, Xian, China, 2009, pp. 297–300.

[17] O. Bjorndal, S.-E. Hamran, and T. S. Lande, "Square wave architectures for radar-on-chip," in *2016 46th European Microwave Conference (EuMC)*, London, United Kingdom, 2016, pp. 1485–1488.

[18] D. Forte, A. Srivastav, "On improving the uniqueness of silicon-based physically unclonable functions via Optical Proximity Correction" *in 2012 DAC Design Automation Conference*, San Fransisco, US, pp. 96-105.

6. Application of RF-FPGA PCB: Reconfigurable RF platform and RF wireless communication

Preliminaries and Objectives:

As understood from the previous chapter, for the purpose of guided wave IC authentication, a customized RF PCB board has been developed. Furthermore owing to the fact that guided wave or GEMT based authentication requires an external RF instruments and measurement setups. The objective in this chapter is to investigate that if the customized RF-FPGA PCB can be utilized to implement a reconfigurable RF platform using FPGA. From chapter 3 we have observed that FPGAs generate electromagnetic (EM) emissions that have been used in order to generate their signature for authentication purpose. One of the applications that can be realized using RF-FPGA PCB is the transmission of the EM signatures (discussed in chapter 3) through RF communication, from different FPGAs to a single or a master FPGA where all the mathematical post-processing is carried out. This type of authentication scheme (distributed) can be useful in industrial applications, internet-of-things (IoT) and applications, where devices have restricted computational capabilities and they can communicate through RF communication to a master device or server for further computation of the data / signal. For an efficient realization of the RF wireless communication, it is also important to equip the FPGAs with some RF devices to carry out basic tasks like signal transmission, isolation, switching, power division etc.

In this work, we have shown that the reconfigurable or re-programmable feature of a FPGA can be exploited to make a single FPGA function as basic RF devices like isolator, switches etc. Furthermore the same re-configurability feature has been used to deploy the RF wireless communication between multiple FPGA boards. The motivation behind these approaches is to reduce the gap between RF and digital system.

In this chapter, the first part focuses mainly on the realization and implementation of basic RF devices such as isolator, switches and power divider in the FPGA using only the digital blocks and interconnects of FPGA. In the second part, we have implemented a RF wireless communication between two FPGAs by implementation of the On-Off key modulation scheme. Of course, this is a basic implementation of applying RF-FPGA PCB, there can be room for improvement in the future works. Also our work has been mainly towards implementation of a proof-of-concept.

6.1 Motivation: FPGA based RF devices

FPGA devices are very powerful devices in terms of their flexibility and re-programmability. They are being used in many applications like digital design, memory applications etc. However, owing to their re-programmability feature, FPGA devices have been widely adopted in the applications of RF and DSP [1] [2]. In RF and DSP applications, FPGA devices are typically used for the technology of software defined radios (SDR) due to their re-configurability and programmability. However, FPGA devices are mostly applied to perform the precise operations in the RF or DSP tool chains. By precise, we mean to highlight that FPGAs in DSP or RF chain have been used primarily to perform the mathematical and logical computation after the signals are converted into digital format. Hence, significant analog and RF components are still needed to fulfill the radio communication requirements [3]. Predominantly, the RF components are designed as application specific integrated circuit (ASICs) and Monolithic Microwave Integrated Circuit (MMIC), e.g. for the realization of RF switches field effect transistor based switches [4]. The bottleneck with ASICs and MMICs is that, they are full custom therefore they require higher development costs in order to design and implement. Moreover, unlike the FPGAs chips, they are not re-programmable and therefore a change requires again cost and time [5].

In this study we have developed a proof-of-concept to make FPGA - not a RF device - analogous to a RF device to work in UHF range. For the first time, the programmable logic and interconnections present in a FPGA, typically utilized in digital electronic circuits, is used to route, and to guide an RF signal. FPGA of limited clock speed of 50 MHz is made to function as a RF device in frequency range of up to 800 MHz. Here no data sampling is used, FPGA clock is not used at all, and the RF functionalities are implemented asynchronously. Furthermore, since we do not use only digital signal or clock signal (no sampling), hence it is not a simple use of higher harmonics or overclocking. But the idea has been to realize RF system-on-chip (SoC) that can function like RF generator, mixer amplifier, transceiver and transmitter circuit.

Our focus is on using FPGA as a RF device, wherein the RF input-output (IO) is directly connected to the FPGA IO ports. RF IO ports can be used with an antenna that is useful in communication purpose. In comparison to [1][3], no external clock is used to sample the data on IO ports. Secondly, our focus is not only on digitizing the RF and DSP components as shown in [2] [3], but instead we have utilized FPGA as a reconfigurable RF device compatible with basic transmission functions. By re-configurability of FPGA, we mean to say that FPGA has the ability to repeatedly change and rearrange the programmable logic and interconnections to implement a basic RF functionality in a cost-effective way. In order to validate our

proposed model, we have first described the transfer of RF power from input to the output pins and then extended the approach to implement the FPGA in switch configurations.

6.2 Motivation: FPGA based RF wireless communication

Over past two decades, wireless communication has witnessed a phenomenal growth in terms of users, mobile devices, and throughput requirements to drive multimedia services. This has led to increase in the implementation of new techniques to be adopted in order to meet the future demands in wireless communication. A number of new ideas and concepts are being suggested and evaluated by the industry and academia for evolution of communication technologies, such as massive MIMO, exploitation of higher RF bands, such as millimeter wave band, and centralized radio access networks for highly digital radio access networks [6][7]. However with increase in the number of device connected to the wireless communication in various applications, the density of network will increase in the future. This demand for more flexible, heterogeneous and reconfigurable architecture to implement the wireless communication.

In this study, we have explored the re-configurability and re-programmability feature of FPGA to implement an end-to-end RF communication between FPGAs. As already explained in the beginning of this chapter, our idea to implement RF communication has been mainly motivated by the fact of communicating the signatures (for authentication) from devices through RF communication. We have made an endeavor to keep the end-to-end communication scheme as simple as possible. With regards to all FPGA based RF communication, there have been similar studies as done in which have implemented all digital RF communication on FPGAs as discussed in [1] and [3]. But in comparison to [3], we have not used any external clock for synchronization. Likewise in [1] authors have used external clock generation, to digitize their transceiver architecture using FPGA. A typical way to generate a digitized RF implementation has been through implementation of software defined radio (SDR). In SDR from [3][8], all the RF functionalities are realized using software installed on computer or processors. However as also stated in [3], current SDR implementations still require significant amount of analog components. For example a significant portion of data conversion is not part of SDR architecture.

In comparisons to existing approaches of software defined radio (SDR) in [1][3][8][9], the architecture we have proposed is fully implemented in FPGA. All the signals are generated using logic blocks of

FPGAs only (even if it is analog sine wave); no external device or signals are used. Hence it has provided a solution of complete FPGA based re-configurable architecture that implements a RF wireless communication. The advantages of FPGA are that we can re-configure the architecture (on-fly) as per our requirement. The architecture is realized on customized RF-FPGA PCB (ref. Fig. 6.1(a)). This allow the FPGA to operate in a 50 Ohms environment like a RF or communication device [10]. The realization of customized PCB has mitigated the need to integrate external analog or RF devices, to connect antenna for communication [11].

This chapter details the implementation and development of FPGA into a re-configurable RF platform. The first part of this chapter details out the theoretical as well as the measurements setup for the implementation of the basic RF circuits like transmitter, switches etc. using FPGA. The next part details the analysis and theory related to the wireless communication - modulation and demodulation techniques, implementation of the wireless systems etc. A detailed analysis of implementation of FPGA in RF communication (with pictorial description) is given from section 6.4.

6.3 FPGA as RF devices – implementation and results

First we have discussed about utilizing the FPGA as RF device. This involves the possibility of exciting FPGA with RF input for transmission through FPGA and also for implementing a switch structure, power splitter etc. highlighting the usability of FPGA in different RF applications. In previous chapter (chapter 5) we have introduced the concept of utilizing the FPGA on a RF PCB. From chapter 5, we have shown how the FPGA (and its logic blocks – buffers etc.) interacts when excited with an external RF signal. Extension of that principle has been applied here in this section. We have exploited the same concept of exciting the FPGA with guided RF waves and characterizing its output for realization of various RF devices. In this realm we have realized basic RF devices like transmitter, isolator, switches and power splitters on FPGA without the use of any external RF components.

6.3.1 Measurement overview

To realize FPGA as RF device, a PCB has been designed (already shown in chapter 5, but discussed again in section below) to allow the FPGA to interact with external RF signal that can optimize it to work as a RF device. The input-output (IO) transmission lines has 50 Ohms load which connect FPGA with other

RF equipment viz. SMA connectors. Like most of digital circuits, the FPGA has high impedance pins. In order to allow the RF signals to enter the component - FPGA (re-programmable) - the simplest way, we have added a 50Ω resistor parallel with the component. A complete description of the realized PCB design (test-bench) viz. details of measurement instruments, IO ports on PCB, DC bias power supply etc. is shown in Fig. 6.1(a).

The methodology to perform RF functionalities with the PCB is divided mainly into few steps:

a. Create data bit-streams (BS) for different RF functionalities, viz. switches and isolator etc. in this work.

b. Program FPGA with BS.

c. Perform testing and measurements.

The created BS contains information pertaining to placements and routing of logic block and IO ports, respectively. The placements and routings of logic blocks and IO routes play the most significant role in achieving the desired output; the RF functionality is build based on that, viz. in using FPGA in classical non RF functions. On the IO pins of FPGA, there are IO buffers. Hence an incoming RF wave encounters an IO buffer, when traversing through FPGA. The logic blocks in the FPGA are placed in look up tables or LUTs. A brief detail of FPGA has been given in chapter 3.

As already mentioned, to perform the testing and measurement, a customized 4 layer RF PCB (see Fig. 6.1(a)) is developed, which has SPARTAN-3A FPGA from Xilinx as device under test (DUT). For implementing a proof-of-concept only few of the input pins of FPGA have been used. For programming, placement and routing of the logic elements in the DUT, Xilinx ISE tool is used. Along the FPGA, there are auxiliary regulator circuits for power management.

As evident from Fig. 6.1(a), for the measurement purpose, a vector network analyzer (VNA) is used, which measures the S-parameter from multiple IO to the FPGA. Also evident from Fig. 6.1(a) that a bias tee is in place along with the VNA and DC power supply. This is useful for injecting DC bias voltage along the RF input into the FPGA input port. The DC biasing is done to bias the buffer circuits at FPGA IO ports to provide proper voltage for its operation. Input DC bias for the circuit programmed in FPGA is set at 1.5V. While calibrating the VNA, the bias tee is not connected to the VNA cables. The bias tee is added in the measurement after the calibration is performed for the ports.

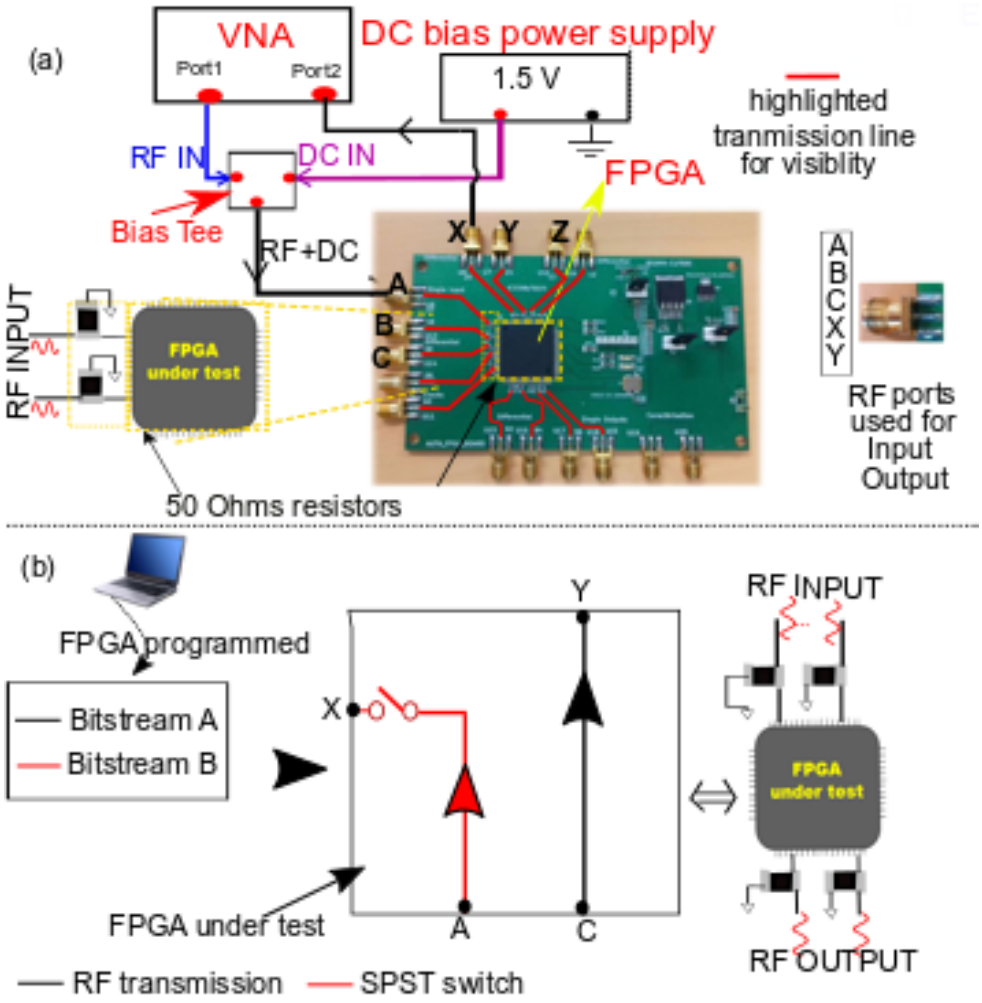


Fig. 6.1: (a) Measurement setup on the customized FPGA PCB to perform the RF test. Inset zoom shows an enlarge description of 50Ω resistors used with the transmission for proper matching. Input-Output (IO) ports naming is described which is used throughout this letter. (b) Proposed methodology to make a FPGA work as RF device by generating different bit streams e.g. Switches depending on the input output chosen.

To highlight the validity of this scheme, we have implemented few basic RF devices using FPGAs. In the sections below we have given an elaborated description of each RF devices implemented in FPGA.

6.3.2 RF transmission through FPGA

The first idea investigated in this work is to show that FPGA can be excited by an external RF signal. To obtain that, an input DC bias of 1.5 V is set for the circuit programmed in FPGA. At DC bias of 1.5V, a

proper operating conditions is established which supplies a steady voltage for device to operate. Indeed the IO operations of FPGA are designed for digital signal, and the first internal component after the pin is a buffer. So the incoming RF wave encounters a buffer circuit in a FPGA, which requires proper DC to switch ON. This is why to be compatible with this digital component; a DC voltage of 1.5 V is added along the RF signal. So during the positive cycle of RF input, the buffer corresponds to one state and vice-versa during negative cycle. As no clock signal is used in the FPGA (asynchronous implementation), the periodicity of signal going through the FPGA is directly linked to the RF input signal. Hence, if there is no DC biasing, the transmission through FPGA is not possible. The RF input power level generated from VNA has been varied in the bandwidth of 10 MHz to 3 GHz. Also to investigate the effect of the power, the RF input signal has been varied from 0 dBm to 12 dBm in steps of 2 dBm.

To determine the transfer of RF wave, the FPGA has been programmed with a route or interconnect. The route establishes connection between the IO pins of FPGA (or IO SMAs of PCB). An equivalence of programmed interconnect circuit has been shown in Fig. 6.1(b). The input RF signal is sent through port 'C' and output through port 'Y' as described in Fig. 6.1(b). This establishes a connection from the input to output SMA port of the PCB, through interconnect of the FPGA. The results that validate the proposed setup of utilizing the FPGA with a RF signal are shown in Fig. 6.2. The result from Fig. 6.2 shows the S21 response. This result infers two main aspects: (I) amplification behavior of the FPGA and (II) bandwidth of operation.

I. ***Amplification behavior of FPGA***: It is clear form Fig. 6.2(a) that in such configuration, the FPGA allows propagation of a RF signal but also plays the role of an amplifier. Thus, an amplification of more than 10 dB can be obtained when the input power is 0 dBm. The relationship between input power and output power (as also described in (1)) has been depicted in Fig. 6.2(b) at two different frequencies, 100 MHz and 500 MHz. The amplification can be explained by the fact that FPGAs are active components, where input and output buffer (directly connected to its pins) power up the signal in a specific range. The forward, S21 depicted in Fig. 6.2(a), and the reverse transmission, S12 shown in Fig. 6.3, are different as the DC bias is injected only on input port 'C'. In such configuration the FPGA can be used as an isolator [12] with more than -20 dB of isolation on the entire frequency range considered here. To obtain a symmetric scattering matrix two DC bias have to be used (not shown here).

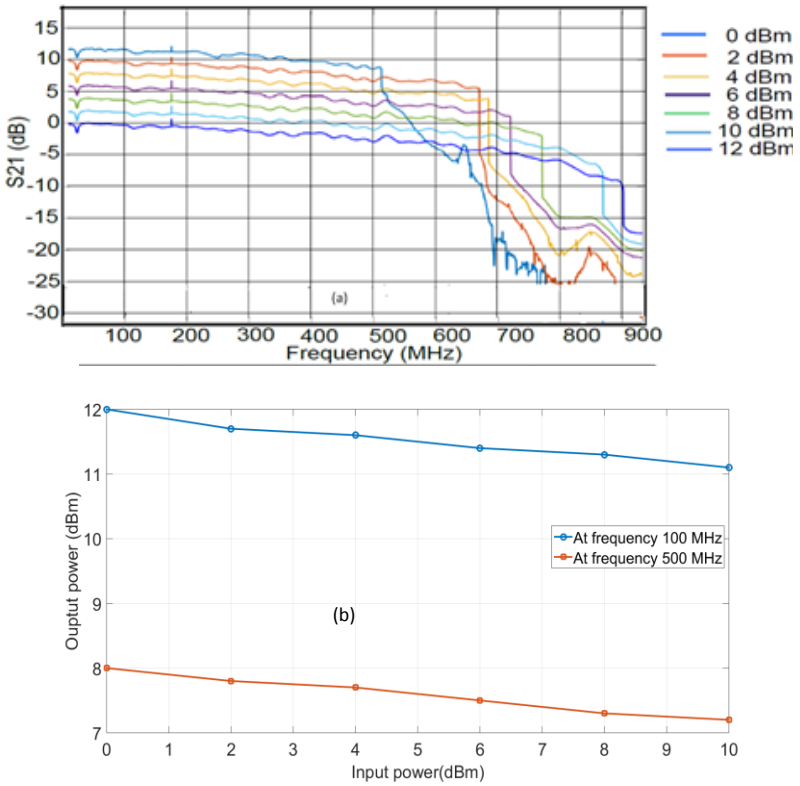


Fig. 6.2: Transmission characteristics and input-output power relationship. (a) Transmission characteristics (S21) for different power levels. The input RF signal is sent through port 'C' and output through port 'Y' as described in Fig. 6.1(b). (b) Relationship between input and output power at frequency 100 MHz and 500 MHz.

The relationship between input and output power at 100 MHz and 500 MHz frequencies (shown in Fig. 6.2(b)) has been calculated using (1)

$$Pout = Pin + |S21|^2 \qquad (1)$$

Pout is the output power in dBm.
Pin is the input power applied in dBm.

From Fig. 6.2(b) also we can observe that as the input power increases, there is decrement in the output. This stems from the fact that the buffers circuit of FPGA has limited output handling, therefore due to the limited output handling capacity of the buffer output power level decreases with increase of input power.

II. ***Bandwidth of operation***: From Fig. 6.2(a) it is also clear that the bandwidth of operation is approximately up to range of 500-800 MHz Owing to the fact that as the device gain increases bandwidth decreases. Maximum bandwidth that we have been able to achieve is in range of up to

800 MHz with a compromise on the gain. Thus, the input power level can be set as per the requirement and application.

With only the use of a simple parallel 50Ω resistance, as seen in Fig. 6.3(a) a poor matching is obtained for frequencies higher than 200 MHz. But due to the active behavior of the FPGA observed in Fig. 6.2, this poor matching does not have significant impact on the RF transmission. To quantify more clearly this impact, a better matching circuit on a narrow range around 300 MHz (based on R,L,C elements) has been implemented. In Fig. 6.3(a), we can clearly see S11 for the two cases - without proper matching and with RLC matching network. With the RLC circuit, a good matching is obtained on a narrow band frequency around 300 MHz. However, the S21 value for both matched and un-matched cases have been equal - approx. around 10 dB for 0 dBm input power (not shown here). This justifies the fact that due to the presence of buffer, similar S21 are observed which mitigates the necessity to better match the device for our expected applications.

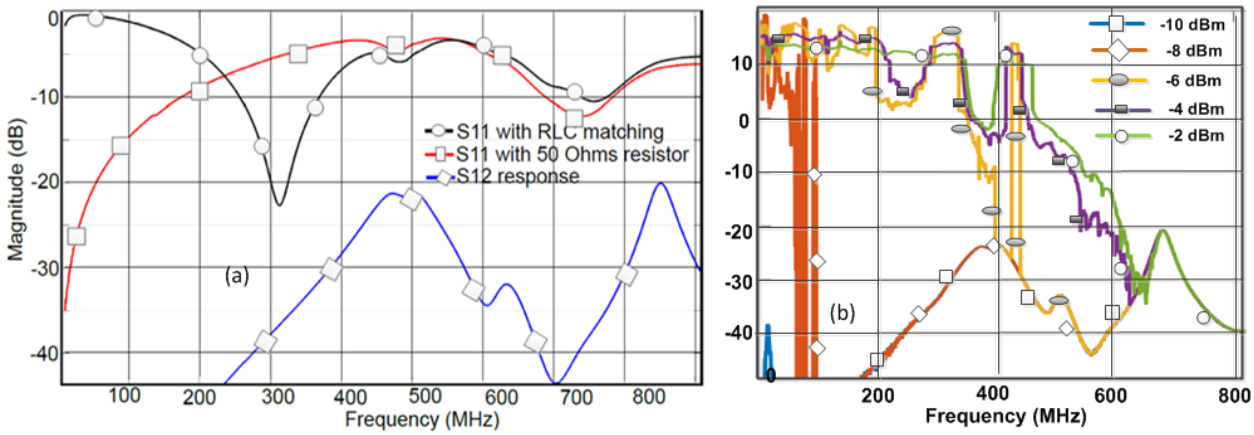


Fig. 6.3: Characteristics of S-parameter with and without matching and S21 characteristics for lower input power range. (a) S11 parameter response measured without DC bias - direct transmission lines with 50 Ohms resistors and with RLC network. Also shown is S12 parameter (without DC bias on port 2). (b) S21 characteristics for very low input power level up to frequency of 1 GHz.

Although from the Fig. 6.2(a), we have observed that there is clear amplification at 0 dBm input power due to the FPGA (buffer circuit of FPGA). We get maximum output power at 0 dBm input power. Also, another important aspect is to observe the S21 response for the input power level of below 0 dBm. The response for the input power below 0 dBm is shown in Fig. 6.3(b). It is clear from Fig. 6.3(b) that for lower power levels like -8 dBm and -10 dBm, there is insignificant output (close to -20 dB |S21|). Even as

power increase to -4 dBm and -2 dBm, the output is highly unstable and cannot be useful for any application or characterization.

A. Time Domain response

The time domain results from Fig. 6.5, shows the time response at around 200 MHz (better amplitude response) and 700 MHz (lower amplitude, close to cut off frequency) together with their associated fast Fourier transform (FFT). The time domain response is obtained by injecting the RF signal through RF generator at 0 dBm input power with the DC bias tee. The output is observed on the oscilloscope. The complete pictorial depiction of the time domain measurement is shown in Fig. 6.4.

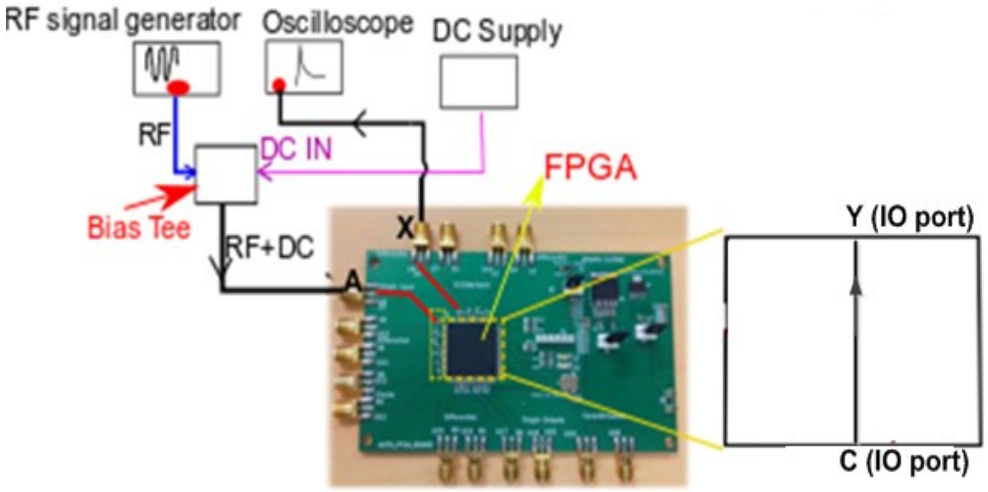


Fig. 6.4: A time domain measurement setup. The instruments used are: RF signal generator to inset RF signal. DC bias tee for the voltage biasing. Oscilloscope is used to observe the output.

As also discussed earlier, that the IO pin of FPGA consists of buffer. From Fig. 6.5, we can observe that at low frequency a rectangular pulse with sharp rise/fall time is observed. We can also observe that at low frequency the buffer switches its state from high to low and that gives a pulse like waveform.

At higher frequency (up to 800 MHz), the behaviors is different. The variation of the RF signal (period of the signal) is higher, and the buffer still can follow these variations but as the buffer has limited capability to switch between its states, the transition from high to low and vice versa is not linear. Note that by using a more recent FPGA, a significant improvement in the rise time / fall time of the buffer can be obtained, and so a higher frequency band of operation is expected.

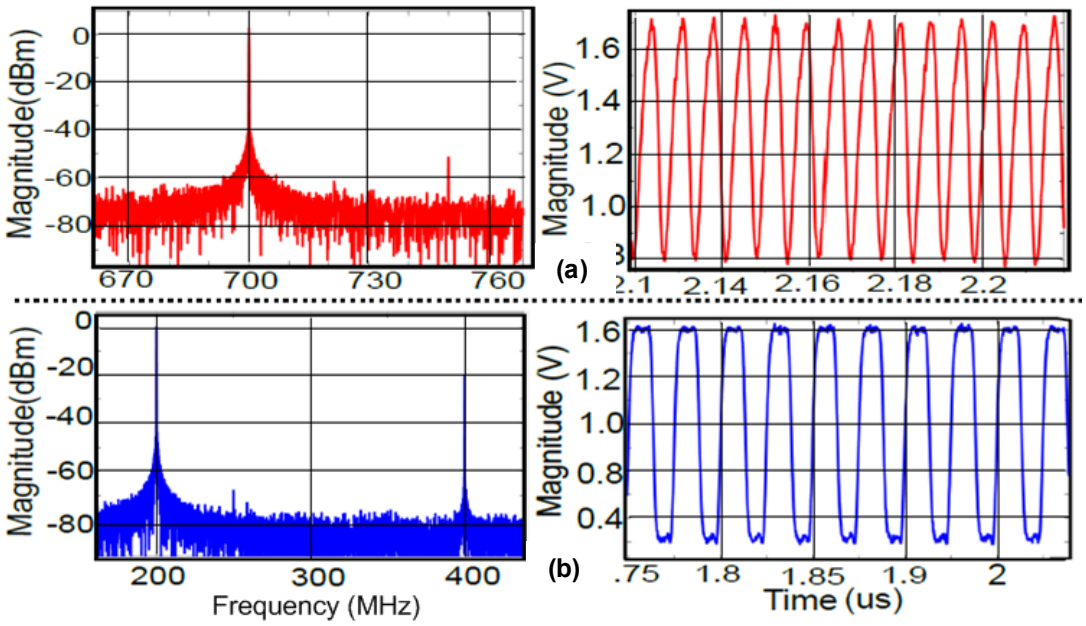


Fig. 6.5: Time and Frequency domain (FFT of time domain) response at : (a) 700 MHz (b) 200 MHz at its higher harmonics at around 400 MHz.

6.3.3 FPGA as RF switch

This section describes the implementation of two RF switches (i) Single pole single throw (SPST) and (ii) Single pole double throw (SPDT) in the FPGA, together with the measurement results. Before going into the detailed analysis of the FPGA based implementations, we have given an overview of the different configurations of switches i.e. SPST and SPDT switches respectively. RF switches are ideal for instrumentation, communications, military and aerospace applications [13]. RF switches feature higher power handling, better linearity and wider frequency band of operation compared to their digital CMOS counterparts.

a) SPST or single pole single throw switch :

A SPST or single pole single throw switch is a simple switch configuration. It has got one input and one output, which means two terminals [14]. A basic implementation of SPST is shown in Fig 6.6(a).

The switch will either be closed or completely disconnected. SPSTs are perfect for on-off switching. They're also a very common form of momentary switches. The activation of the switch is generally

obtained by using two more wires - 4 port structure in such a case: 2 are control by DC signals – not shown on the Fig. 6.6(a).

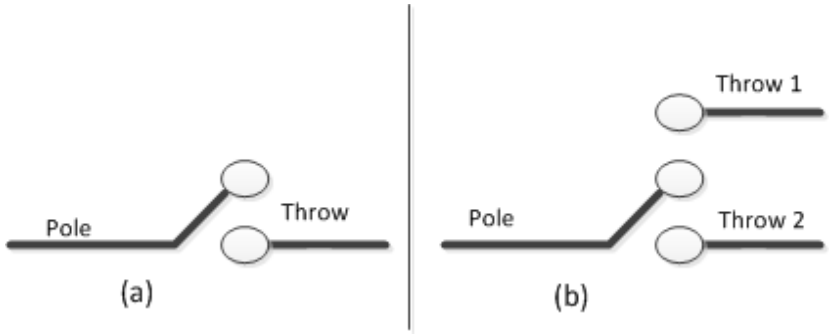


Fig. 6.6: Classical RF switches schematics. (a) Single pole single throw (SPST) switch. (b) Single pole double throw (SPDT) switch.

b) SPDT or single pole double throw switch :

Another common switch-type is the SPDT. SPDTs have three terminals [14]: one common pin and two pins which vie for connection to the common. SPDTs are great for selecting between two power sources, swapping inputs, or whatever it is you do with two circuits trying to go one place. A typical description of SPDT switch is given in Fig. 6.6(b).

6.3.4 FPGA implementation of SPST switches

In our study, we have implemented a logic structure in FPGA which acts as a RF SPST switch structure. To implement FPGA as a RF switch, AND gate logic circuit has been used. An AND gate works in logic conjunction. This means that its output will be high only when both the inputs are in high (’1’) state. To make it work like a switch (SPST/SPDT), we have used one of the two input pins of the AND gate as a control input. Note that an AND gate is implemented in FPGA as a look up table (LUT). For the simplicity we have shown an equivalent AND gate schematic in Fig. 6.7.

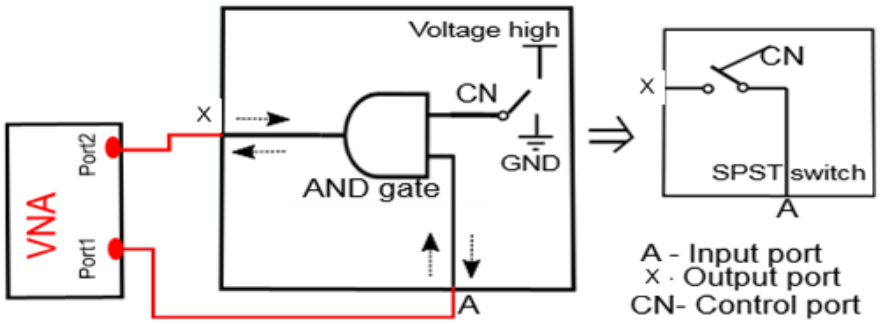


Fig. 6.7: FPGA programmed with AND gate to realize a RF SPST switch. Port 'A' is used as input and port X as output. Ports 'A' and 'X' are connected to port 1 and 2 of the vector network analyzer (VNA), respectively. In FPGA internally, an AND gate is implemented as look up table. For simplicity an equivalent AND gate schematic is shown here.

The control input of the AND gate in this work is configured internally and does not have an external port connection. The switch configuration between IO and control ports is shown in Fig. 6.7. As seen in Fig. 6.7, 'A' is configured as the input port, 'X' as output port and an internal logic setup is made which configures the control port (CN) to high or low state. Similar to AND gate, a multiplexer circuit (MUX) can also be used.

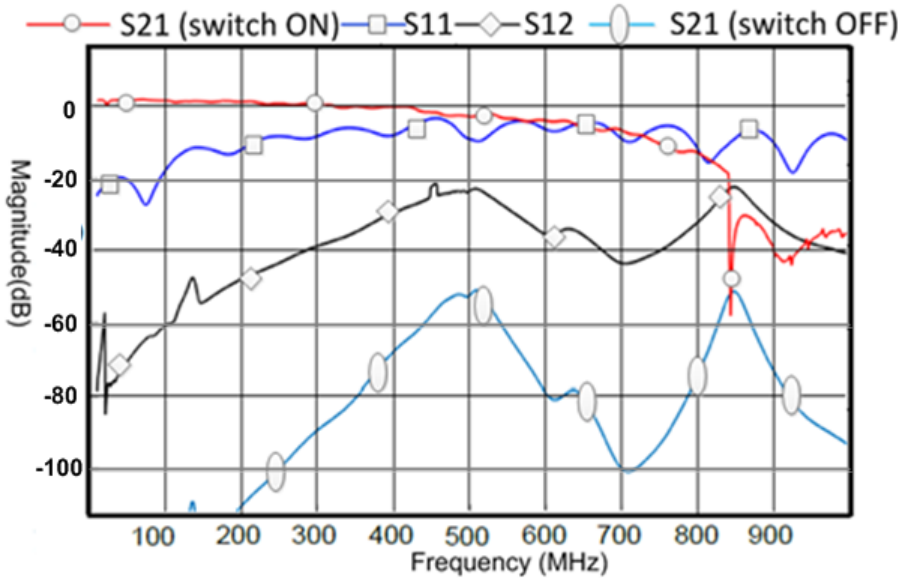


Fig. 6.8: Response from FPGA with a buffer configured between port A(input) & port X (output) for input power of 10 dBm : Transmission (S21),reverse transmission (S12) ,reflection (S11) and isolation (switch OFF) curves.

The idea of using MUX has also been tested in this work and it gives an identical result to that of AND gate. The results with the MUX have not been shown in this manuscript. The frequency domain responses are depicted in Fig. 6.8. The measurement is performed with the setup described in Fig. 6.1(a).

In Fig. 6.8, the S-parameter response is observed for the switch implemented in Fig. 6.7. These responses depict three important parameter pertaining to the characteristics of the switch: (i) frequency range, (ii) isolation, and (iii) return loss of in frequency domain.

These three parameters can be used to characterize the figure of merit (FOM) of the configured switch. The forward (S21) and the reverse transmission (S12) are different as FPGA is an active device and also the fact that only the DC bias is injected on input port 'A'. The isolation is around -40 dB when the switch is in non-conducting state. The cut off frequency defined at -10 dB from maximum S21 value of 0 dB is observed at around 700 MHz.

The results demonstrate that with a FPGA of limited clock frequency, not designed to operate in RF range, it is viable to make it function as RF device working in frequency range of around 800 MHz by just reconfiguring the routing structure. Even though the responses from Fig 6.8 may not be so optimized as other existing RF devices but the idea of re-programmable or re-configurable RF device is totally novel. In future, much work can be done in this area and better results are expected.

6.3.5 FPGA implementation of SPDT switches

For utilizing the FPGA in single input multiple output configuration, two AND gates are programmed with one input of both the AND gates connected to the input RF port and the other inputs to control ports. From Fig. 6.9, we can observe that this obtained behavior of the device is analogous to a SPDT switch configurations. The IO ports for this configuration is: 'B' as input, and 'C' and 'E' as output. The selection of IO ports is arbitrary and does not change the aspect of results. Fig 6.9(a) shows the configuration when connection is made from 'B' to 'E' with its corresponding frequency domain responses. Similarly, Fig. 6.9(b) shows the results for connection from 'B' to 'C'. The control port, 'CN' is internally connected to voltage high or ground as per the required configuration. The 'CN' port is used in order to configure the state of switch. If 'CN' port is connected to a high one port-throw combination works and vice versa.

The S-parameter results from Fig. 6.9(a) & (b) establish that for SPDT switch configurations, the working frequency of the FPGA reaches up to 750 MHz (approx.), with isolation power of up to -40 dB in the non-conducting state. This justifies our approach to utilize FPGA as a RF device, i.e. like a RF switch in the above cases. The results for different configurations of switch validates that a FPGA with proper RF PCB layout and terminations can function like a RF device close to UHF frequency range.

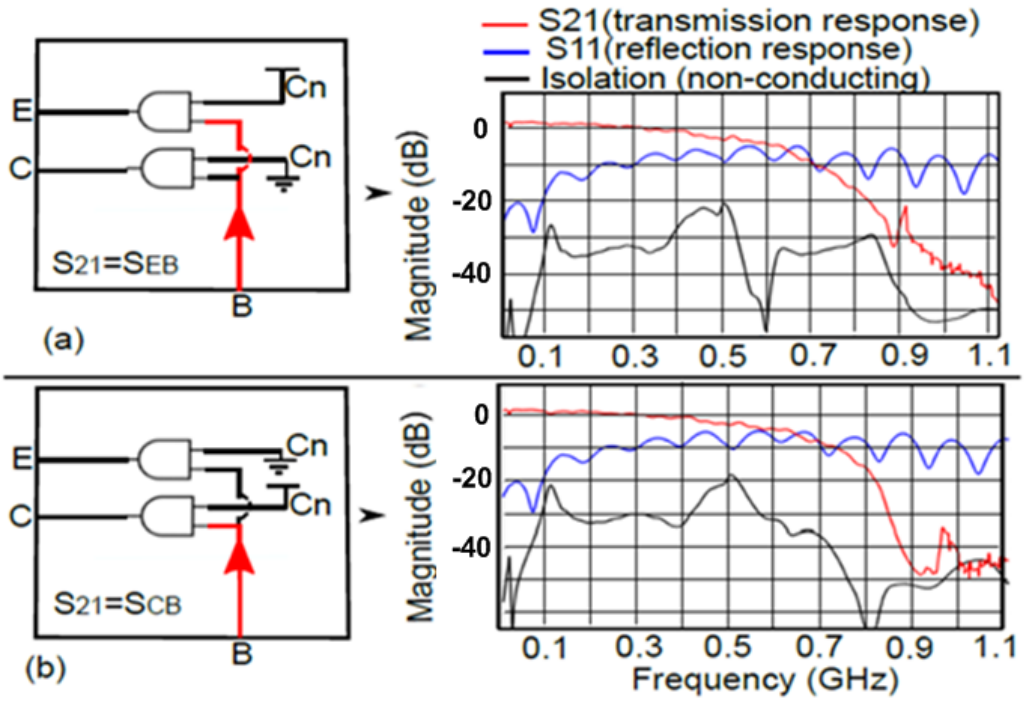


Fig. 6.9: (a) Switch configuration analogous to a SPDT switch implemented in FPGA. Port B as input and E as output and its S-parameter response, similarly in (b) Port B as input and port C as output and it S-parameter response. In FPGA internally, an AND gate is implemented as look up table. For simplicity an equivalent AND gate schematic is shown here.

6.3.6 FPGA as power splitter

Power splitter is another extension of the applications that have been realized using FPGA. In communication system, we often need to split an input power into some load circuits, which could be actualized by power splitter [15]. In this section a power splitter circuit is implemented in the same FPGA DUT, by reconfiguring the routing in the FPGA, as is done in case of switches. Using FPGA as power

splitter gives the flexibility to change the IO ports and number of outputs (say 1X2, 1X4 etc.). In this part of the study we have established a 1X2 power splitter on same FPGA devices. In order to have a better phase response of the output port, for power splitter we have used buffer circuit, to establish a connection between two ports. The IO ports used are: 'B' as input and 'C' and 'E' as output as in Fig. 6.10(a). From Fig. 6.10(b) it is clearly observed that power on the two output ports ('C' and 'E') is equally divided up to 600 MHz. The isolation observed between the two output ports is approximately around -22 dBm. Although there is a small phase difference as seen from Fig. 6.10(c) but that can be adjusted by re-ordering the route length. Hence, using FPGA as power splitter we have achieved a good isolation, considerable wide bandwidth with cost efficiency and reconfigurable design.

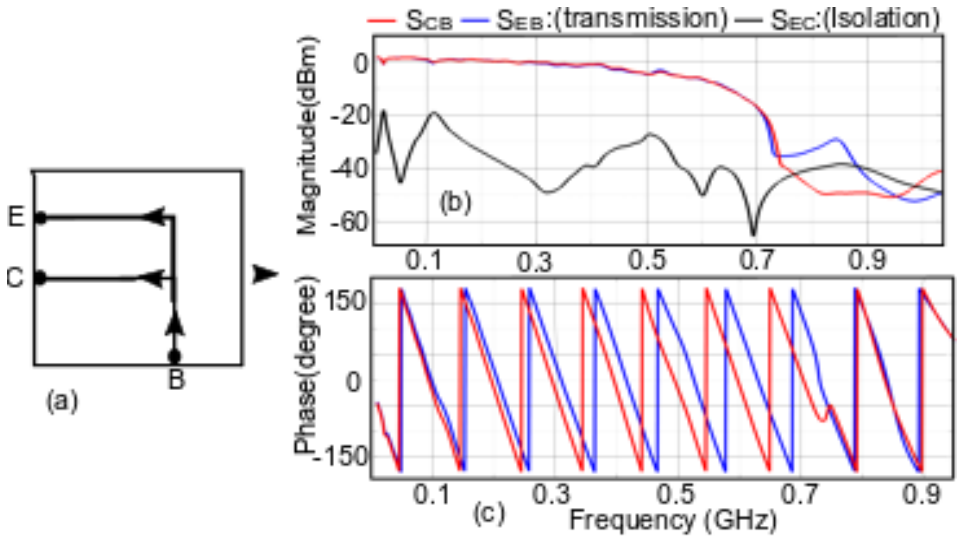


Fig. 6.10: Power splitter and its responses. (a) FPGA configured as a power splitter using two buffers circuit. (b) S-parameter responses of the power splitter. (c) Phase difference between two routes.

6.3.7 Inference from RF FPGA devices

The results obtained from the implementation of the basic RF functionalities have been adopted in this part of study. From the results we can observe clearly that by utilizing the re-programmability feature of FPGA, it can be made to work like a RF switch or device. The S11 parameters need few improvements, but the idea is very novel and its implementation can always be improved upon in the future work. But the results from the S21 parameters can be very useful metric in understanding the cut off frequency of the switch structure. The approximate presented by the buffer circuit and interconnect of FPGA has been around 800 MHz this confirms the useful of this re-configurable platform in the range of UHF bandwidth.

Secondly the re-configurability feature of FPGA also shows that same FPGA device has been used to implement the two kinds of switch configurations and power splitters.

From this study it has been shown that using FPGA, we are able to transfer the RF power through the FPGA device which is meant to function for low frequency digital applications. Also, owing to dependency of the DC polarization, we can use the FPGA as a non-reciprocal device like an isolator. In this work, frequency of up to 800 MHz is achieved for different implementations. The work proposed here can be significant in going forward to have more adaptable and reconfigurable circuits which can work in RF and high frequency range. This work highlights a proof of concept.

6.4 RF wireless communication between FPGA boards

In this part of manuscript, we have detailed about the implementation of a complete RF wireless communication architecture, only using logic gates in FPGA. The entire signal except the use of antenna, processing from the baseband up to the RF stage for the transmitter, and the opposite for the receiver, is completely performed in the digital domain. The architecture is realized on the customized RF FPGA PCB already presented. A complete end-to-end communication architecture between two FPGAs, together with description of PCB, has been detailed in Fig. 6.11.

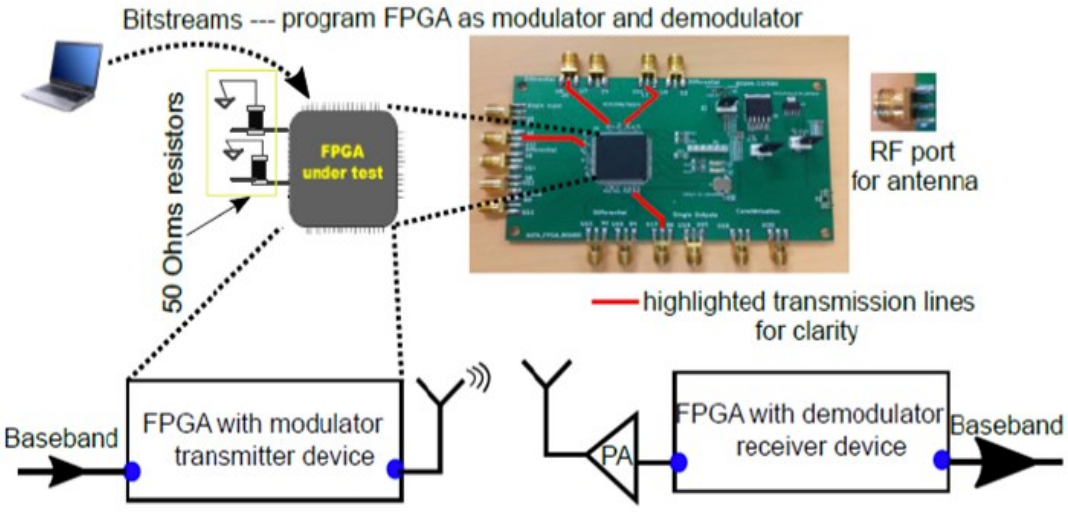


Fig. 6.11: Description of PCB for communication system, the programming scheme of the FPGA to generate bitstream, and an end-to-end wireless communication between two FPGAs.

The modulation technique is based upon off keying (OOK) modulation scheme that is implemented using circuit blocks consisting of signal generator or oscillator, switch (detailed description in next section). For the demodulation, a basic detector technique (envelope detection) is used which filters out the carrier wave (CW) signal and baseband signal is recovered at the receiver side. Furthermore, in the study we have highlighted the idea of using XOR gate phase detection to increase the CW frequency without the use of any external synchronization circuit.

Before concluding, in this manuscript we have also implemented a basic logic operation over wireless communication, in order to substantiate the utility of this approach for distributed logic and digital operations over wireless medium. A very practical application of such an implementation (distributed network) can be the development of a complete system-on-chip which houses a receiver and transmitter as well logic blocks for the further computation. Also, this can be useful in developing a complete RF system on digital platforms where computer and mobile devices can be connected with the RF peripherals and communicate and utilize the FPGA based RF devices like switches, isolators etc. for sending and processing the digital data.

6.4.1 Implementation of modulator and demodulator in FPGA

In this section, a detailed description is given about the implementation of different logic blocks in a FPGA, such that they work equivalent to transmitter and receiver circuit respectively. Like previously, the whole end-to-end RF transmission chain is realized on Xilinx SPARTAN-3A FPGA (90nm CMOS). This is a low end FPGA, which has clock frequency of 50 MHz. Before going into the implementation in FPGA, we have discussed in brief about OOK modulation and demodulation technique. Before we go in details about implementation in FPGA, a brief highlight on the fundamental of OOK modulation is given below.

A. Fundamentals of On-Off Keying (OOK) – classic techniques

Understanding the basics from [16], OOK is a variant of Amplitude Shift Keying (ASK). It is a type of digital modulation scheme which represents digital data as variation of the amplitude of the carrier wave (CW). This type of modulation scheme is more often used with digital communication. In OOK, if there is a binary 1 (or signal is high) at the baseband signal then CW is transmitted else at 0 (signal is low), CW is absent.

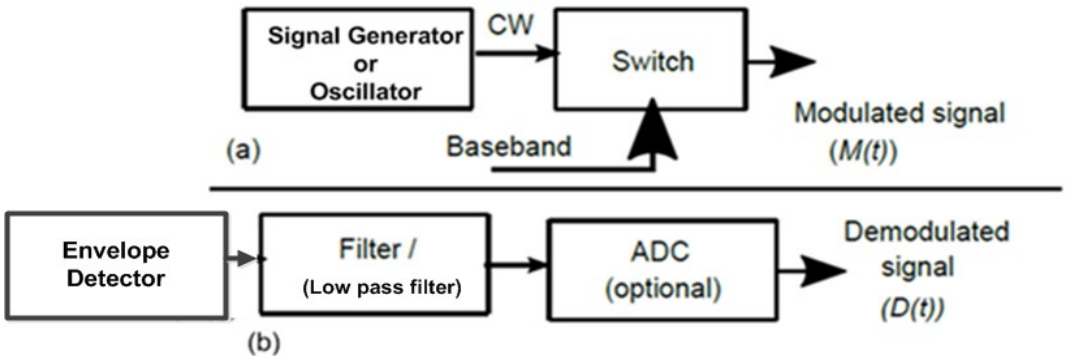


Fig. 6.12: OOK transmitter and receiver block classically implemented. (b) Modulator / Transmitter block. (b) Receiver / demodulator block.

Classically, for an OOK modulation the simplest technique is based on a switch which uses the presence of a CW to indicate a binary 1 and its absence to indicate a binary 0 [16]. A simplest form of OOK modulator is described in Fig. 6.12.

From Fig. 6.12(a), it can be observed that in a simple OOK based transmitter requires a signal generator which generates CW signal of high frequency. The next block is a switch, which is controlled by baseband signal. When baseband signal is high it switches CW to high values else there is no signal at the output. Similarly, on the receiver side as depicted in Fig 6.12(b), the simple idea is to implement a detector. Taking the reference from Fig. 6.12, we have programmed the FPGA such that the logic functionality of FPGA is analogous to that of an impulse generator and switch for the transmitter circuit; and on the receiver side a detector circuit - envelope detector. Before we go into analysis and implementation of modulator and demodulator circuits, we have given a little insight on the impact of IO buffers of FPGA that have on the incoming and outgoing signals from FPGAs.

As we have also discussed in previous part of this chapter that IO pin of FPGA consists of buffers, hence any incoming or outgoing signal (be it RF or digital) encounter a buffer in their path. The generated signal inside the FPGA also gets passes through IO; hence there is an added effect of buffer on the incoming or outgoing signals in FPGA. Understanding the effects from buffer to incoming signal we can refer to Fig. 6.2, where only an interconnect (with IO buffers) establishes connection between IO ports. We can observe from Fig. 6.2, that with only interconnect between IO ports and intrinsic IO buffers at the IO ports, the FPGA is able to transmit up to 800 MHz of frequency. Also, the results of buffer in time domain from Fig. 6.5, the rate of switching from 0 to peak voltage are determined by the frequency of operation. Therefore, along with the circuit elements that realizes RF modulator or demodulator circuit

there are also effects of IO buffers on the incoming and outgoing signals. Hence, the presence of IO buffers can be determining factor in achieving the maximum frequency range.

6.4.2 Transmitter circuit implementation in FPGA

This section presents and explains the proposed architecture for the transmitter (Tx) implemented digitally in the FPGA. A pictorial depiction of the entire modulator block implemented in FPGA has been described in Fig. 6.13. The components or logic blocks shown in Fig. 6.13 are used to implement an OOK modulation scheme in FPGA. The different OOK blocks in classical implementation and its FPGA counterpart have been described as follows:

1. ***Impulse Generator:*** An impulse generator is used to generate high frequency signal that generates CW wave. In FPGA, for the CW generation i.e. analogous of impulse generator, a ring oscillator circuit of 3 stage inverters and AND gate for enable is used. The three stage RO circuit generates a CW signal of around 245 MHz. The analogous modulator scheme implemented in FPGA is shown in Fig. 6.13.

2. ***Switch***: The second block on the transmitter side is that of a switch. The switch is implemented in the transmitter FPGA using multiplexer circuit or MUX (see Fig. 6.13). The output of RO is fed to the one input of multiplexer (MUX) which works like a switch circuit. The control input of MUX is connected to the baseband signal.

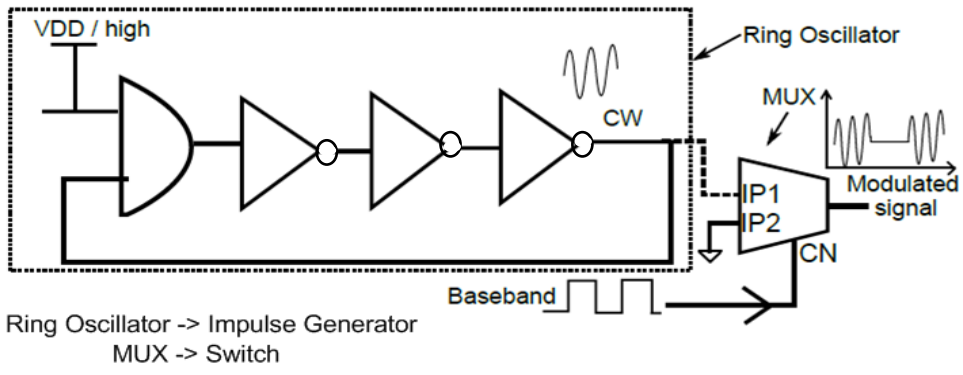


Fig. 6.13: OOK modulator circuit implemented in FPGA using RO and MUX circuit. RO circuit is used in order to generate a CW signal of high frequency. MUX is used as a switch where baseband signal of low frequency is externally fed which controls the state of MUX output.

A. Modulation of baseband signal in FPGA : working overview

The maximum frequency of operation for the RO circuit obtained has been around 245 MHz even though the routing length was minimum and number of stages of inverter used is only 3 shown in Fig. 6.13. The RO circuit has been placed in the FPGA manually. The baseband signal is a square wave of 500 kHz, generated from an external frequency generator. The baseband signal can also be generated internally from clock also or externally depending upon the type of application and frequency of operation. There is no restriction of the origin of the baseband signal. The control input (CN) of multiplexer (MUX) is connected to the baseband signal of 500 kHz (see Fig. 6.13). In previous part of this chapter we have used an AND gate in the switch configuration. Of course same implementation (AND gate) can also be used here. It does not change the functionality and result of the implementation. Furthermore, it depends upon the designer to choose between logic gates that can be implemented in order to suffice the implementation.

Referring from Fig. 6.13, that implements the OOK modulation scheme in FPGA, for the MUX, one of its input, (IP1), is connected to the output of RO (CW signal), and the second input of MUX (IP2) is connected to the ground state. Based on the state of baseband signal (high or low), the output of MUX works. If baseband is in high state, then CW signal from RO is the output of MUX and vice-versa.

B. Modulation of baseband signal in FPGA : Results

After the complete implementation of the modulation scheme, we evaluate how efficient are the modulation results. The results of the modulation are shown in Fig. 6.14. The results in Fig. 6.14 cover both the frequency domain as well as time domain aspects. For frequency domain, we have observed the results in spectrum analyzer or VNA and for time domain the results are obtained in oscilloscope. From Fig. 6.14 (b) we can observe that the peak to peak voltage is from 0 to 1.2 V for CW. Of course this shift is due to the fact that FPGA circuits are designed to operate from 0 to +Vpeak. They do not have any capability to operate on negative voltage level. The results from Fig. 6.14(a) highlight the frequency peaks of the baseband and well as CW signals.

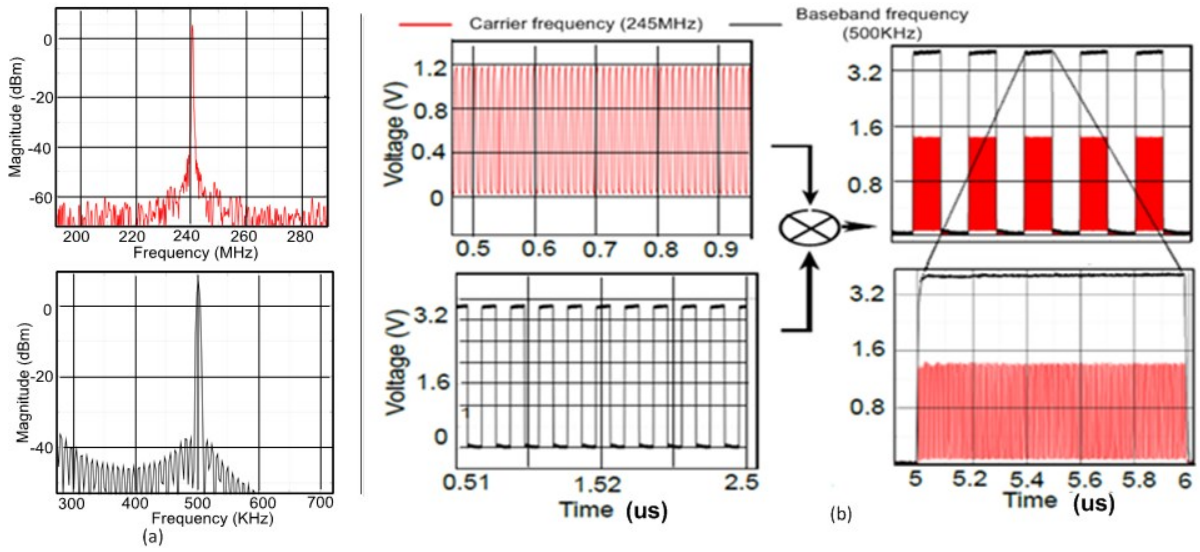


Fig. 6.14: Description of CW and baseband signals in time and frequency domain. (a) CW signal and baseband signal in frequency domain. (b) CW and baseband signal in time domain representation. Inset an enlarged representation of the modulated signal.

The waveforms from Fig. 6.14, it can be clearly seen that CW of 245 MHz is modulated as per OOK modulation scheme, by baseband signal of 500 kHz. Hence, by programming FPGA with a RO and MUX circuit, we are able to modulate a very high frequency signal (VHF) with a low frequency baseband signal. The RO frequency limits the frequency of CW signal. Now we shift our focus on understanding and implementation of receiver circuit in FPGA.

6.4.3 Receiver circuit implementation in FPGA

In this section, the receiver (Rx) architecture is described, considering an OOK modulation scheme, which has CW frequency of about 245 MHz. The implementation of OOK demodulator is done by using envelope detection technique, i.e. use diode with a low pass filter to filter out the CW frequency.

For demodulation circuit, we can refer from Fig. 6.12(b). From Fig. 6.12(b), classically, the envelope detector is realized using diodes and a few other components and as a result it is a very low cost circuit block within an overall receiver [16][17]. The envelope detector is the combination of a half wave rectifier and low pass filter [18]. In this work, to implement a circuit analogous to an envelope detector, we have used series of buffers. Before the description of envelope detector implementation in FPGA

using logic gates (buffers), we first discuss the effects buffers when a RF high frequency signal is sent to them as an input.

A. Buffer as demodulator – theory and simulation

In our study, we have programmed a series of buffers that has been used for to perform demodulation. The idea of using buffers stems from the fact that buffer can act as an envelope detector. Because, buffer based on CMOS technology has limited switching speed - rise time and fall time. This is affected by its physical and electrical characteristics as well as its resistance and capacitance (RC) parasitic and load referenced also in Fig. 6.15(a). In terms of the capacitive load only, each buffer has to charge/discharge its capacitive load, and as the frequency of input signal goes higher, the capacitor does not get charged / discharged at same frequency.

As high input CW modulated by low frequency baseband signal is sent to buffer, due to the limited the switching speed of the buffers it is not able to charge discharge at high frequency (245 MHz) of CW input. Hence it follows only the low frequency baseband signal which is at 500 kHz. An equivalent approximate simulation using Ltspice® tool has been carried out. In this simulation, the frequency of the CW wave is around 1MHz and baseband signal around 500 kHz. The simulation uses an approximated buffer model (using CMOS technology). The output capacitive load of 10nF and parasitic load resistor of 100k has been used. The results in Fig. 6.15(b) shows that using number of buffers in series, equivalent envelope detection is achieved which can be used for demodulation. The simulation is done just to justify the utility of buffers for demodulator of OOK signal. From Fig. 6.15(b), it can be observe that envelope of the baseband square has been recovered and the high frequency CW signal is removed by series of buffers. Of course, the model and technology of buffers used in FPGA is not same as that we have used in simulation but the approach and theory is same. The number of buffers is determined by the frequency of CW signal that should be removed in order to recover the baseband signal. Increasing number of buffers in series increases the capacitive effects and hence a higher frequency signal or CW wave can be removed.

The frequency domain results (S21 response) obtained in VNA for different numbers of buffers is shown in Fig. 6.15(c). The measurement for frequency response is done at around 10 dBm of input power. It is clear from Fig. 6.15(c) that as the number of buffers in series increase the cut off frequency decreases and vice versa. The number of buffers can be adjusted as per the CW frequency

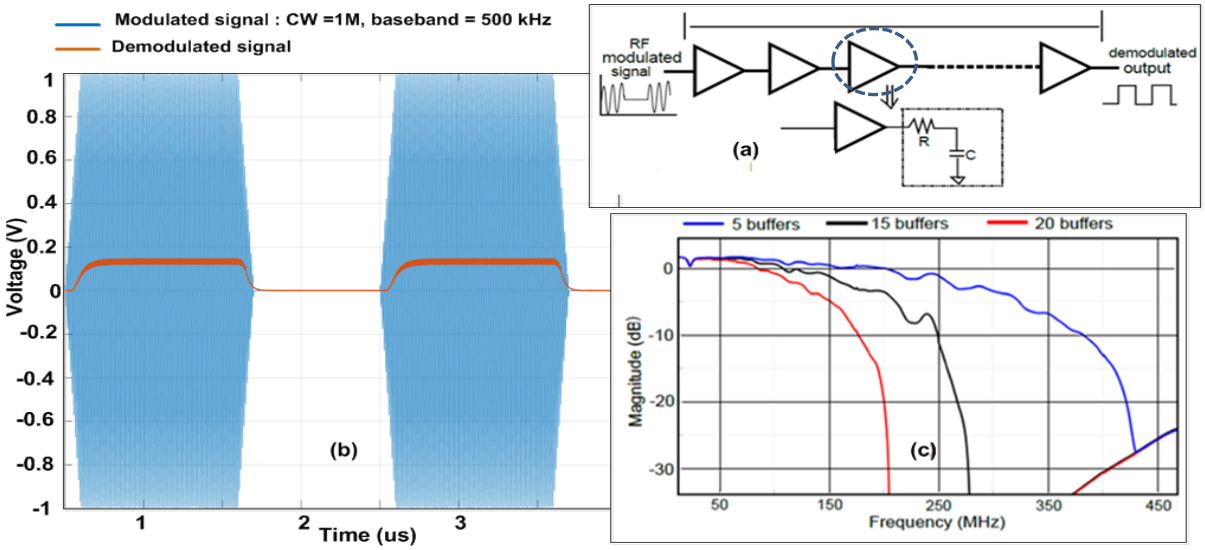


Fig. 6.15: Buffers used for the OOK demodulation. (a) Series of buffers that can be depicted as envelope detector for demodulation of OOK signal. (b) Simulation results of implementing series of buffers as OOK demodulator in LTSpice®. (c) Frequency domain response by varying the number of buffers in series.

B. Envelope detection using buffers– practical implementation

Taking cue from the simulation results of Fig. 6.15 (b), we have implemented series of buffers in FPGA to test for their utility as envelope detector for demodulation of OOK signal. To test for the implementation of the series of buffers as an envelope detector in FPGAs, we have used a pulse width modulated (PWM) input signal with amplitude ranging from –Vpeak to +Vpeak. In order to check for the equivalency of the buffers as envelope detection, we have used a –Vpeak to +Vpeak voltage signal (no DC offset).

The measurement is carried out by injection a modulated PWM signal of from the external RF generator. The modulated PWM signal is sent through series of buffers and the output is observed in the oscilloscope. The result is observed in Fig. 6.16. From Fig. 6.16 the response also confirms that buffers can act like an envelope detector to demodulate OOK signal. The theoretical analysis has already been discussed pertaining to the reasons why buffers can be an optimum choice for the demodulation of OOK signal. Of course there can be enhancement and improvement in future with regards to the implementation of demodulator circuit, but in this study as per our applications and requirement we found buffers as optimum choice for the demodulator circuit. As a summary of simulation and measurement test

results, buffers in the FPGA performs half wave rectification (like diode) as well as low pass filter action. This has been implemented in this study for the purpose of demodulation of OOK signal.

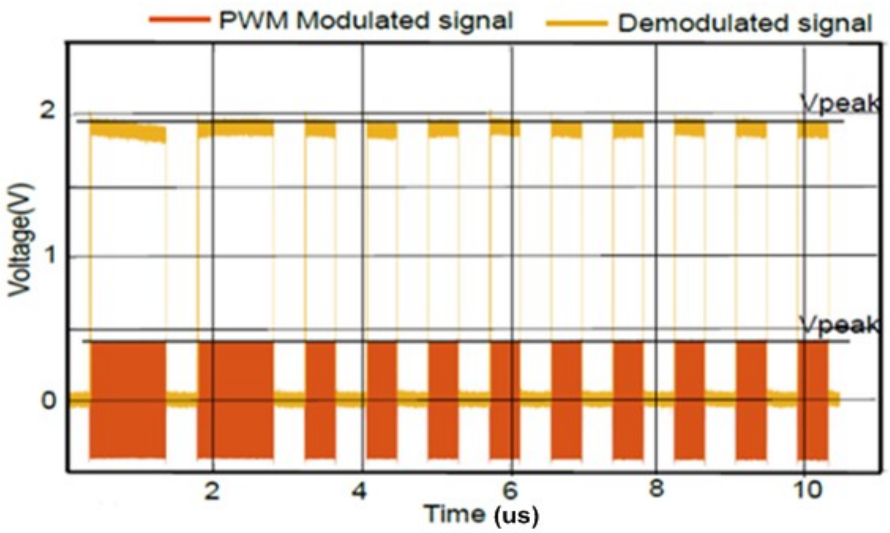


Fig. 6.16. Measurement results - buffers as demodulator with PWM modulated input. The response is observed using oscilloscope.

After basic simulation, implementation and comprehension of the working of modulator and demodulator circuits in FPGAs, the next task is to establish a wireless communication between the two FPGAs. In the next subsection, we have given a detailed description of the wireless communication between the FPGAs using a customized half wave dipole antenna.

6.4.4 Antenna for wireless communication

To establish a wireless communication between two FPGAs, we have developed a customized half wave dipole antenna of copper wire that operates in the frequency band between 240 to 270 MHz.

Half-wave dipole is the most basic and popular antenna. A dipole antenna can be of any length, but it most commonly is just under 1/2 wavelength long [11]. A dipole with this length, known as a resonant or half wave dipole, has (at the resonance frequency) an input impedance that is purely resistive and is approximately equal to 73Ω, which provides a good match to commercially available 50Ω coaxial cables as well as commercial transmitters and receivers [19]. A typical structure of a half wave dipole antenna is shown in Fig. 6.17(a).

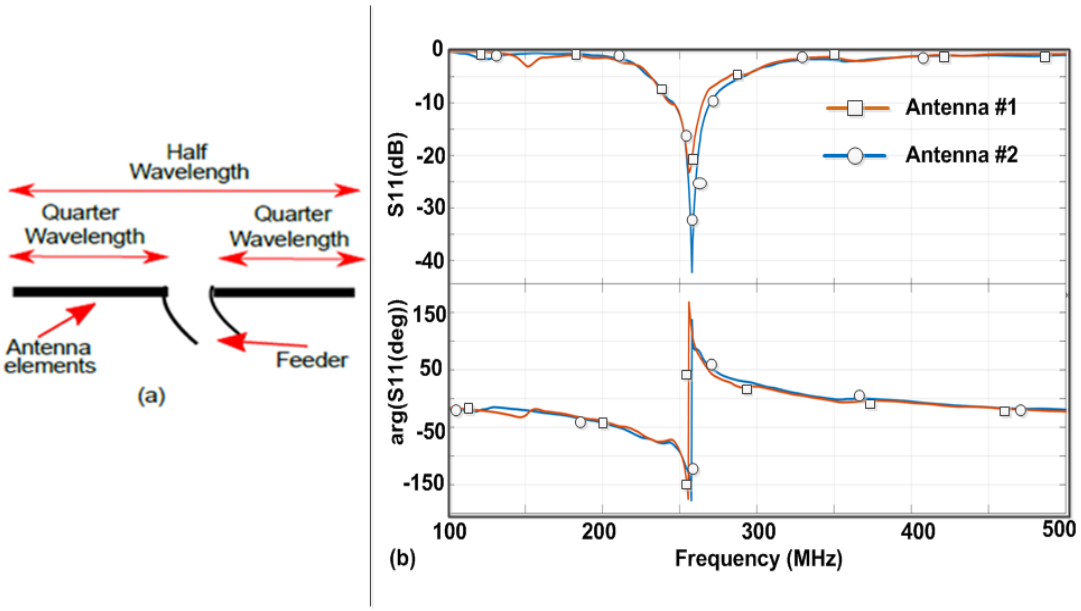


Fig. 6.17: Description of the customized dipole antenna used. (a) Structure of the half wave dipole antenna. (b) Frequency response (S11) and phase response of the antenna.

The S-parameters response (frequency domain response) and phase response of the two customized antenna (one made for the emitter, the other one for the receiver) is shown in the Fig. 6.17(b). From the S11 response of the two antennas it can be clearly inferred that the resonant frequency of the antenna is around 250 MHz with a narrow bandwidth ranging from 240 MHz to 260 MHz.

6.4.5 FPGA Communication results

To implement a complete wireless communication between transmitter and receiver FPGAs, we have used an in-house developed dipole antenna that has been discussed in the previous sub-section. The measurement (wireless communication experiment) has been carried out in real environment, not in anechoic chamber.

The complete experimental setup used in the wireless communication is shown in the Fig. 6.18. The pictorial depiction in Fig. 6.18(a) gives a basic block diagram of the communication between transmitter and receiver FPGAs using the in-house developed dipole antenna.

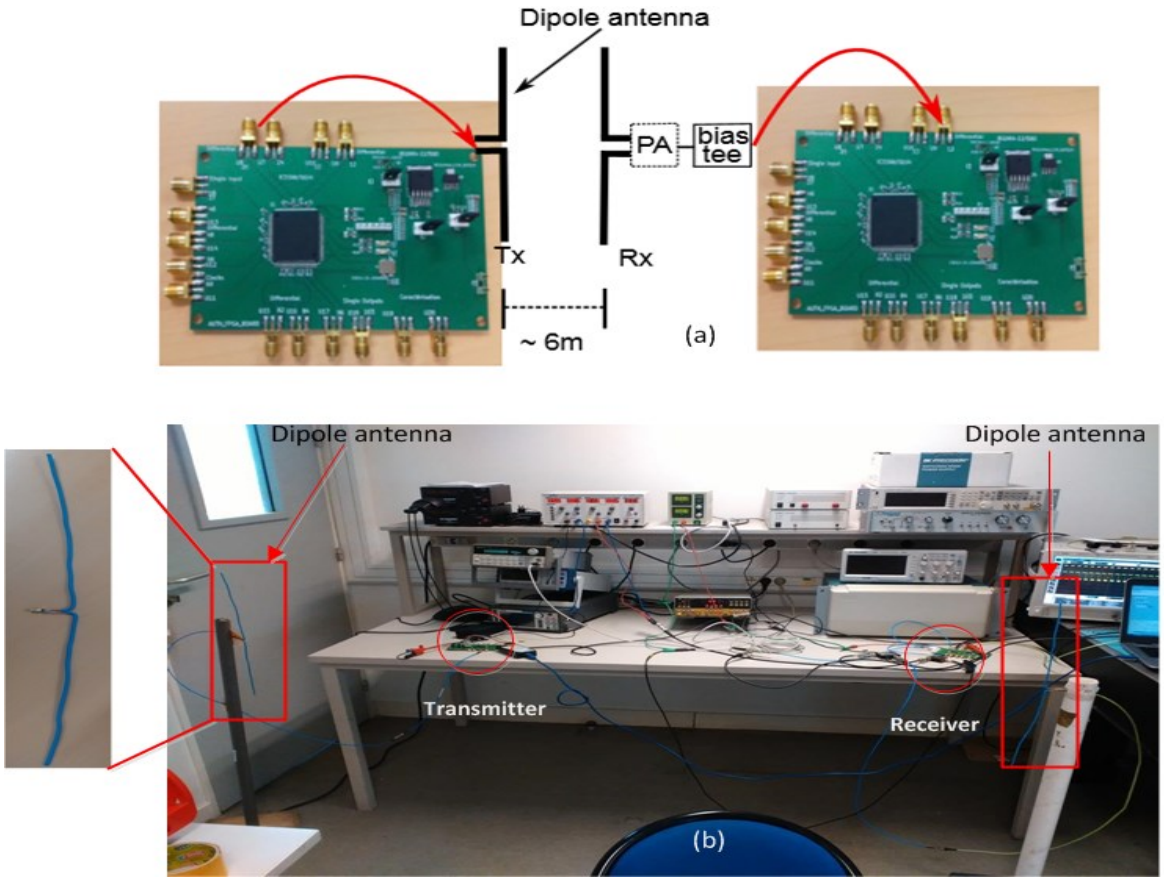


Fig. 6.18: Measurement setups. (a) Measurement setup used in transmission of wireless data between two FPGAs using customized dipole antenna. After the antenna on the Rx side, we have the option to use PA. (b) Actual measurement setup used in experimentation in real environment. (Inset) the half wave dipole antenna developed in-house for bandwidth of around 240 MHz.

The distance covered for the communication is around 6 meters. From Fig. 6.18(b), we can observe the real measurement picture for the communication between the transmitter and receiver. The output signal is observed using oscilloscope and spectrum analyzer. During the measurement steps prescribed in Fig. 6.18, the use of pre-amplifier (PA) after antenna is optional (receiver part). The PA affects the range of communication that can be covered. With PA we have achieved a larger distance of communication than that without PA. On the receiver side there is also use of bias tee in order to give proper DC bias to the buffers of the demodulator circuit.

The results of the communication are shown in Fig. 6.19, shows the baseband (transmitted) and demodulated signal (received) after the wireless transmission using PA on the receiver side.

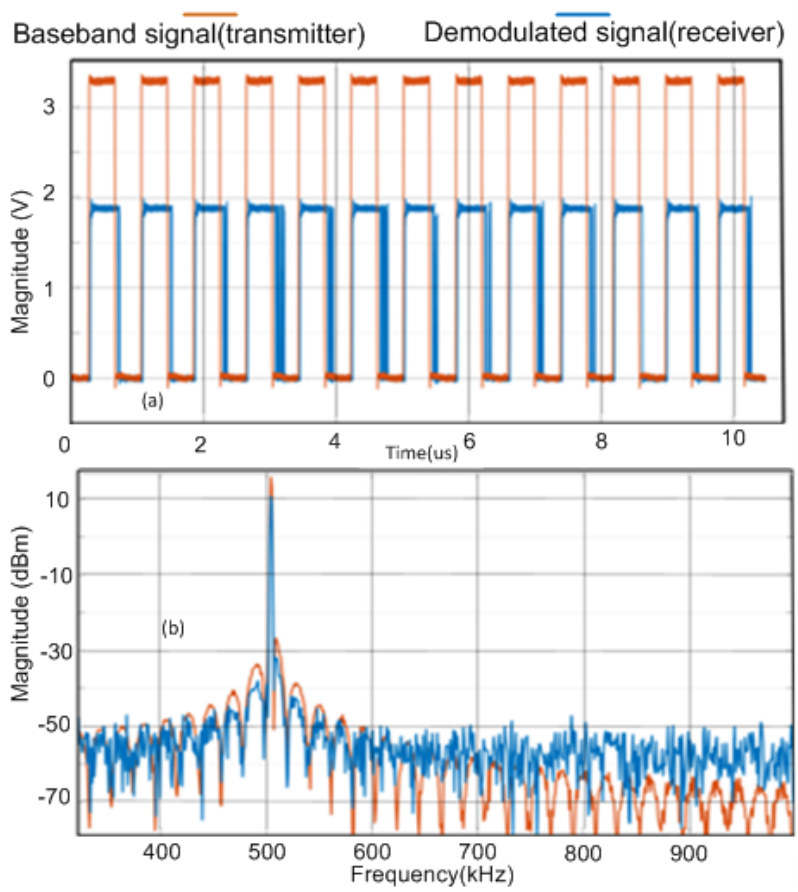


Fig. 6.19: Waveforms showing the input baseband signal and the output demodulated signal at the receiver (Rx) FPGA. (a) Time domain response of the transmitted and received (demodulated signal) observed in oscilloscope. (b) Frequency domain response of the transmitted and received signal observed in spectrum analyzer.

The baseband signal as also discussed in the above sections is around 500 kHz and CW signal is around 245 MHz. The modulated signal is sent through wireless communication and demodulated using the series of buffers (envelop detection) on the receiver side. The results in time domain as well as its frequency domain after communication between the Tx and Rx part is shown in Fig. 6.19. The results from Fig. 6.19 have been observed in oscilloscope (for time domain- Fig. 6.19(a)) and spectrum analyzer (for frequency domain- Fig. 6.19(a))). From Fig. 6.19(a), the received or demodulated signal has few glitches on the edges of the signal. This stems from the fact that there can be effects of environmental noise as all the measurement is carried out in real environment.

From waveform of Fig. 6.19, it is clear that the demodulator circuit implemented in FPGA using chain of buffers in series is able to detect the baseband signal by filtering out the CW signal communication range established is around 6 meters between Rx and Tx FPGA. The noise in the receiver side (from Fig. 6.19(b)) can be corrected by using a Schmitt trigger circuit [20]. This circuit or its analogous has to be implemented digitally in FPGA. Although this has not been implemented in this study but it is part of future work.

The results in Fig. 6.19 justify that FPGAs can be effectively used in deploying the RF wireless communication by programming the FPGA with the required logic blocks. The work done in this study does not require any external synchronization clock or any external ASIC to assist in deploying the RF wireless communication. Hence this is an effective way to establish basic RF communication between digital circuits without use of external circuit elements. In future work it is clear that more complex architecture could be implemented with more robust modulation scheme using FPGAs (all digital circuit). The effort made here has been mainly to implement a proof-of-concept

6.4.6 An applications of wireless communication in distributed network

The efficient implementation of wireless communication can be very instrumental in implementing different logic operations which involves various FPGAs. Hence this strategy can be effectively utilized in the areas of short communication viz. internet of things (IoT) applications etc. Secondly, increase in the digitization of the communication systems, implementing an all FPGA wireless communication can be very suitable solution. FPGA do provide the ease of re- programmability therefore this adds an advantage to create a prototype of the design for purpose of verification and accurate results.

An application of this digitizing the wireless communication scheme on the FPGA is to distribute a logic operation. This is equivalent to divide a large logic or mathematical operation into several FPGAs also depicted in Fig. 6.20. From Fig. 6.20, we can see a graphical illustration of distributing a large task ‘T’ into sets of smaller tasks ‘T1’,’T2’ so on. The smaller sets of tasks are distributed to every FPGA devices which they perform in order to complete the original complex task ‘T’. The distributed approach can be used in IoT applications, cryptographic systems etc. [21]. The distributed operation is more cost-efficient to obtain the desired level of performance by using a cluster of several low-end devices, in comparison with a single high-end FPGA. A distributed system can provide more reliability than a non-distributed system, as there is no single point of failure [15]. In this order to demonstrate the effectiveness of this

implementation to perform distributed logical applications, we have performed a basic digital operation of addition of two signals. The procedure of this part of implementation is detailed in the section below.

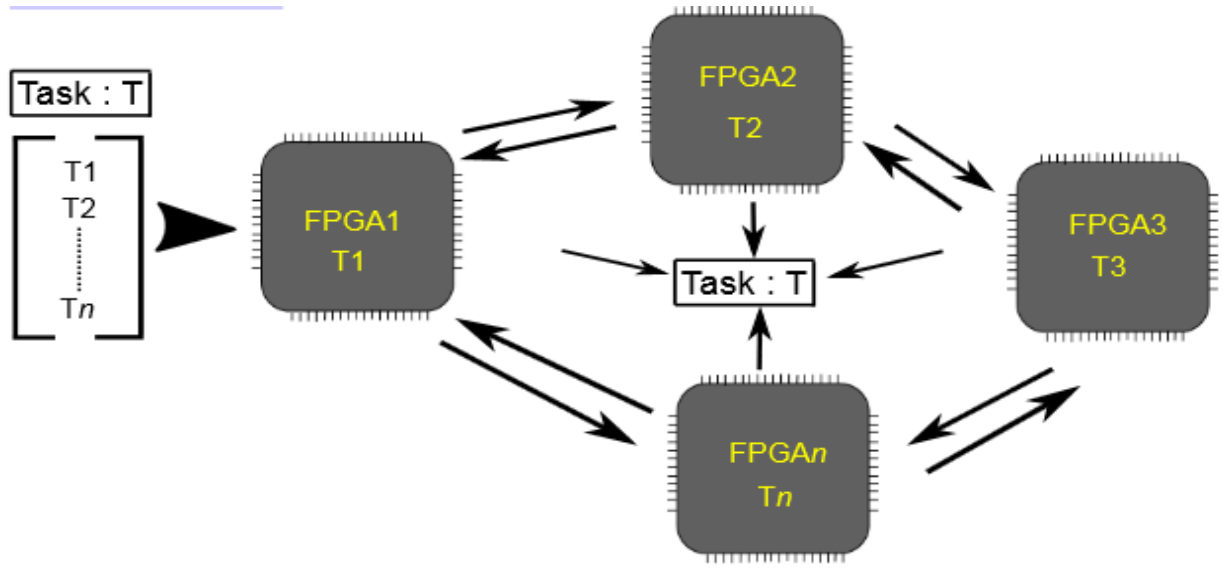


Fig. 6.20: Distribution of small sets of a big task to different FPGA devices. Each device contributes its time and resource to collectively complete the task.

A. Logic operation in wireless transmission

This section gives detail an example about the implementations of a logic operation using wireless communication between two FPGAs. As a proof-of-concept of implementing a distributed logic operation we have used an adder circuit. This type of operation can be deployed in applications where RF communication as well as logical operation is needed to be performed. For one example, we can use it in communicating the EM signatures; divide any security mechanism in distributed chain rather than on one single device in order to avoid the various types of attacks like modeling attack etc. Also such type of applications can be used in scenario such as industrial and medical IoT etc. The concept shown in this study is a basic one but in future aspects better and more complicated tasks can be implemented using similar approach.

B. Half Adder implementation

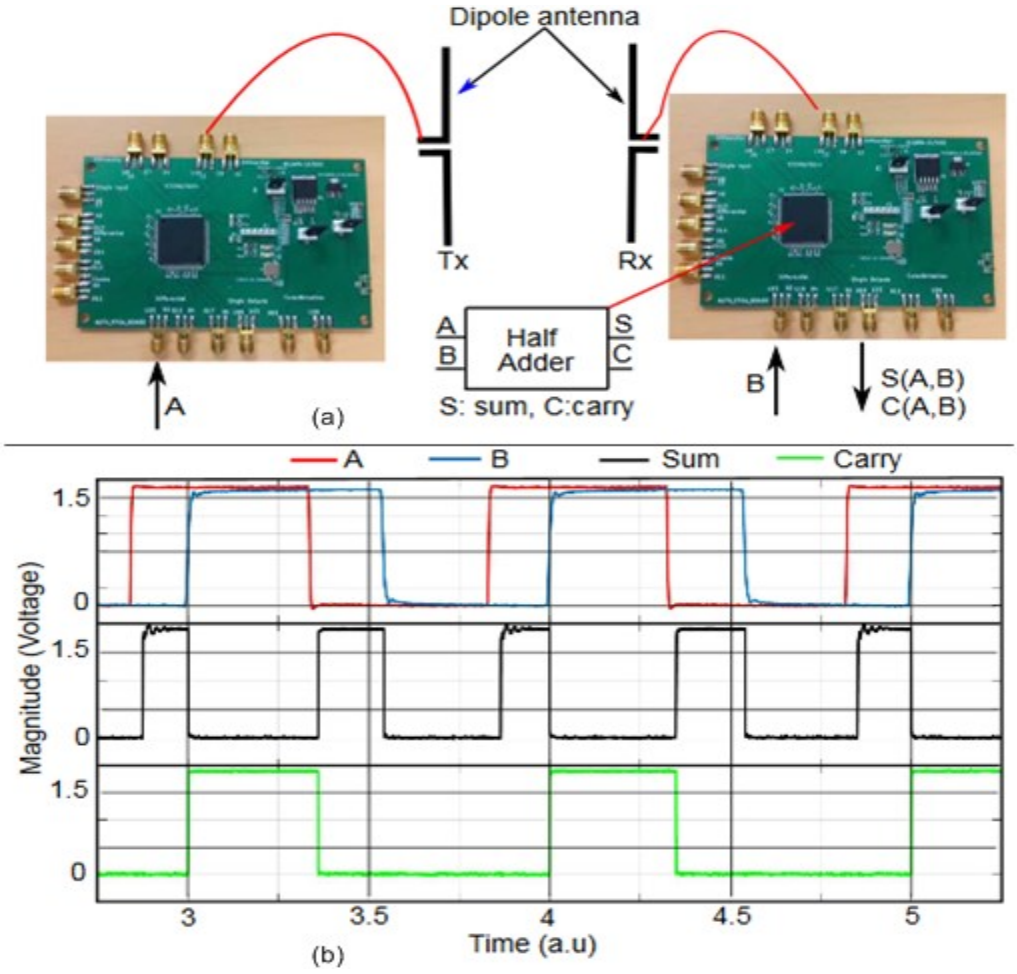


Fig. 6.21: An example of distributed task over two FPGAs. (a) A half adder implementation implemented on two FPGAs. Signal 'A' on transmitter FPGA is added with signal 'B' on the receiver FPGA. (b) Waveform of the input 'A' and 'B' and their sum and carry is shown.

As basic implementation to justify the distributed setup using FPGA based RF communication, we have implemented a basic half adder circuit. The signal from transmitter (Tx) side is added to one of the signal on the receiver (Rx) side.

The adder circuit is implemented at the receiver FPGA, wherein the signals - one from the Tx FPGA is sent over wireless communication is added to another signal on Rx FPGA. Fig. 6.21(a) shows the schematic and measurements used to perform the addition of two signals. One signal 'A' is transmitted from the Tx side through the implemented modulation scheme as described in the above sections

(modulator/demodulator implantation). The second signal 'B' is externally fed to the receiver FPGA. The receiver (demodulation part) FPGA is programmed with a half adder (HA) circuit.

On the Rx side, the base signal 'A' is demodulated, and it is fed to one input of the half adder (HA) circuit as also depicted in Fig. 6.21(a). The other input to HA is 'B' which is fed directly to Rx FPGA. The final output from the HA circuit on the receiver FPGA is sum (S) and carry (C) of the inputs 'A' and 'B'. The results of addition of two signals, is shown in Fig 6.21(b). It is clear from Fig. 6.21(b) that signals 'A' and 'B' are efficiently added and final sum and carry are obtained. This shows that with the implementation of a wireless digital communication, it is possible to implement various logical and mathematical operations distributed over several FPGA devices.

The carrier frequency is low in our case and we have focused on improving the carrier frequency by various means such as using mixer (XOR gate – phase detector) etc. which could double the carrier frequency.

6.4.7 Increasing the carrier frequency in FPGA

After the successful implementation of OOK modulation using RO circuits in the FPGA, we have made an attempt to mitigate the bottleneck of having a low CW frequency due to limitations of the FPGA.

To have a higher CW frequency we have implemented an XOR gate with the ring oscillator (RO). An XOR gate works like a phase detector mixer circuit. It detects the phase difference between the two inputs and gives the output which is the difference of the two input phases as shown in the Fig. 6.22(a). We have used the property of XOR gate to produce a phase detection based output. This can be used for the purpose of frequency doubler.

For the implementation, the output of RO (used as a RF generator) is divided into two parts:

(a) One output is directly fed to the input 'A' of the XOR gate,
(b) Other output from the RO circuit is passed through two buffers, which give it a 90 degree phase shift by adding delay to the output.

Then it is fed to input 'B' of the XOR gate. The whole scheme is described clearly in Fig. 6.22(b). Using the scheme described in Fig. 6.22 on same RO circuit (as discussed in OOK implementation of FPGA earlier in this chapter - section 6.4.1), we are able to double the CW frequency. The RO frequency in the

earlier modulator circuit implemented in above section 6.4.1 is around 245 MHz. The output of RO is divided into two parts (see Fig. 6.22(b)), out of which one is given to one input XOR gate and the other part of the divided RO output is sent through two buffers. The number of buffers used is arbitrary. It depends upon how many buffers are needed to generate the required phase shift. In order to have a correct and required phase shift of 90 degrees, we have implemented buffers that give required phase shift. However, if this phase shift of 90 degrees is not achieved, then the output frequency cannot be twice or what we expect. Hence, we have carefully programmed, and placed buffers that give the required 90 degrees phase shift between the two inputs 'A' and 'B' (see Fig. 6.22(b)).

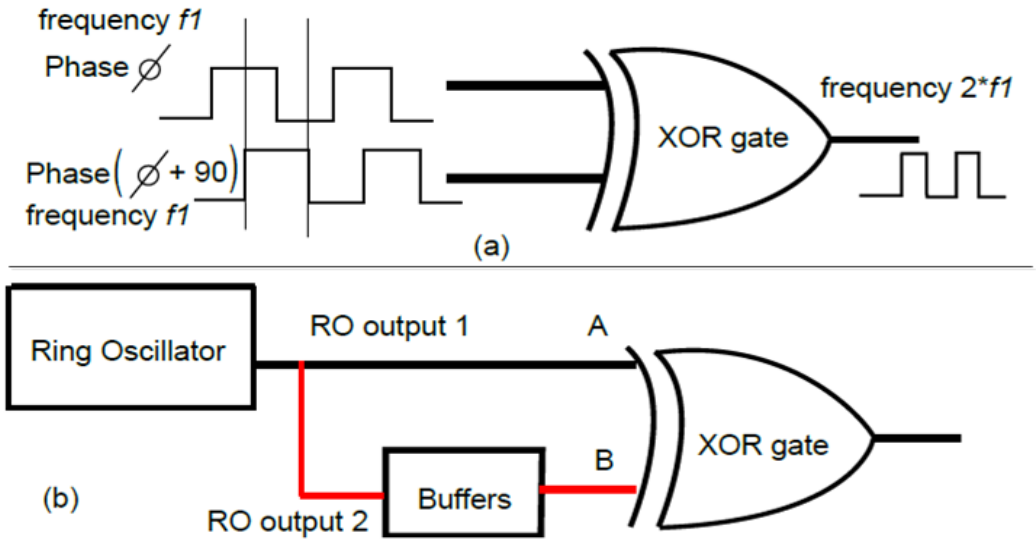


Fig. 6.22: Description of increasing CW frequency by using XOR gate. (a) General description of XOR gate and its input-output waveform. (b) Scheme incorporated to enhance the CW frequency of modulator on FPGA.

The results of the response are given in Fig. 6.23. From Fig. 6.23(a), it can be observed that the output through the use of XOR gate is almost doubled (245*2 = 490 MHz) for same RO which is used in implementation of signal generator (section 6.4.1). If phase shift between 'A' and 'B' is 0 degrees, the output frequency does not change, same is the case if the phase difference between 'A" and 'B' to 180 degrees. Also evident from Fig. 6.23(b), the power level for both (RO and RO+ $\pi/2$) is same; however, this can vary based on the phase shift also because change in phase other than 90 degrees gives an uneven duty cycle.

Hence, by using only one RO, few buffers and an XOR gate we are able generate a higher CW frequency. This would of course reduce the length of dipole antenna in order to implement a wireless communication between the FPGAs.

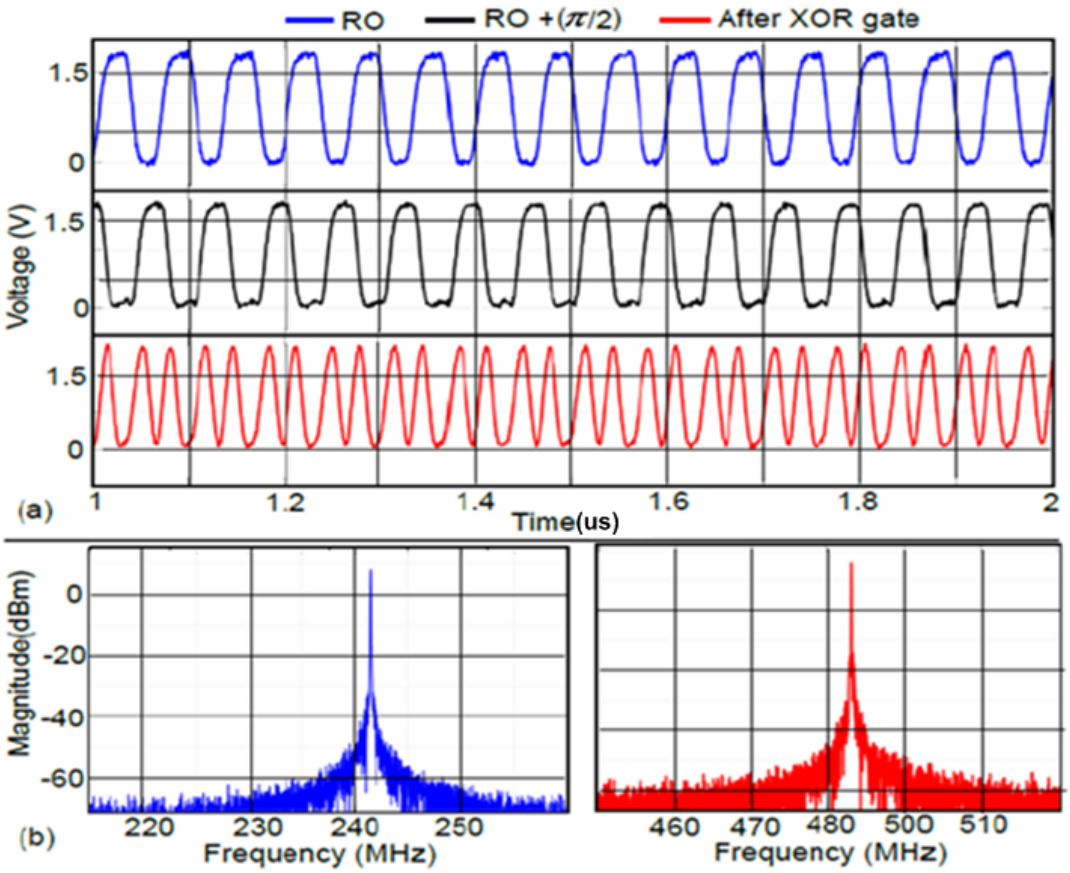


Fig. 6.23: Results waveforms for the XOR operation to increase CW frequency. (a) Time domain representation of the RO, RO+ π/2 and after XOR gate waveforms. (b) Frequency domain representations of original RO (CW frequency) and CW frequency after using XOR gate.

6.4.8 Inference from FPGA based RF wireless communication

In this study we have shown that how FPGAs can be utilized to implement digital communication. By utilizing the re-programmability feature of FPGA we are able to equip FPGA with circuits used in RF, DSP and communication applications. Throughout the study we have not used any external clock generation feature or any circuit element to aid in our application implementation. The transmitter Tx chain implements OOK modulator using simple RO circuit. On the receiver side Rx, we have implemented a chain of buffers in order to detect the envelope of the original baseband signal. Using a customized dipole antenna tuned to work at the given modulator frequency, it has been made possible to implement a communication channel between different FPGA boards. Furthermore the implementation of logic application (adder in this study) using distributed paradigm also makes it a useful application going

forward.

Also the use of XOR based phase shifting has mitigated the problem related to the low carrier frequency. From the detailed and careful implementation we have been able to achieve double the carrier frequency using same RO that we have used in earlier part of OOK implementation in this chapter.

Furthermore, as also discussed in the beginning of this chapter that the main aim of this implementation has been to show if there is possibility of implementing a RF configuration and communication between FPGAs in order to implement an authentication scheme that can distributed over wireless configuration. This type of configuration can be effective with the aid of RF circuits, switch, mixers etc.

6.5 Conclusion

This chapter highlights the fact that even FPGAs –used mostly for digital operation on low frequency range - can be effectively used as RF devices for different RF and wireless applications. The idea of this implementation is to bridge the gap between the RF and digital side of electronics. With the rise of mixed mode devices in various applications like health and home scale IoT, it is utter important that the implemented devices and circuits have processing capabilities to tackle problems of various domains.

The first part of this chapter has been dedicated to the implementation of RF devices in a FPGA – low end with limited clock frequency of 50 MHz. Same FPGA has been used to implement multiple RF devices such as isolator, transmitter and switches. Also the working frequency of all these RF implementation has been up to 800 MHz. All the implementations have been asynchronous and do not need any external circuit to aid in the implementation.

The second part of this chapter has efficiently implemented a RF wireless communication between FPGAs. This has been achieved by programming FPGA such that they can be used to implement an OOK based modulation on Tx side and an envelope detection at Rx side. Furthermore, the XOR based phase shifter has been used which increases the carrier frequency of the modulator. Also we have been able to implement a distributed logic system using different FPGAs to distribute a big task through wireless communication among various FPGAs in the network.

Of course the results and performance can be enhanced and made more efficient but this work shows a proof-of-concept to utilize a FPGA for applications other than digital operations. Secondly the

implementation of FPGAs as RF switch is a stepping stone towards using FPGA as RF devices. This will be highly useful because of re-programmability feature of FPGAs. ASIC or MMIC based device suffer from higher NRE and once they fail to meet certain application specifies they cannot be re-configured according to the need of applications. With FPGA it is possible to put in multiple RF devices on same board as per the requirement and also change the characteristics of the logic implementation on fly.

6.6 Overall Conclusion

In this study our main focus has been to implement a non-invasive, lightweight authentication scheme that uses RF and EM techniques. These techniques can be effective against various commonly used counterfeiting mechanisms like recycling, overproduction, remarking and cloning. We have performed a comparative analysis with the other authentication schemes mainly with the highly used PUF. The main highlight of our work has been towards the implementation of a technique that does not involve lot of chip area, is easy to implement and does not have danger of destroying the chip / IC.

We have shown in this work that two different schemes related to the utilization of RF and EM techniques that can be used for the purpose of authentication of IC. Both the techniques have been such that they effectively exploit the underlying manufacturing based process variation effects to generate signatures of the ICs. In chapter 3, from EM radiated scheme, using a single ring oscillator (RO) marker, we have been successfully able to generate EM signatures for Xilinx FPGAs of two different technologies – 28nm and 90nm. FPGAs of same family, series and age have been used in measurement. Also, REMT based approach has been efficiently implemented to authenticate microcontrollers of STM32 family. In microcontrollers we have utilized only its internal peripheral circuit (RESET circuit in our case) no marker have been involved with microcontrollers case. The EM responses from FPGAs and microcontrollers by implementing REMT based techniques have been treated with the post-processing techniques. In the REMT based authentication approach, we have adopted majorly the cosine similarity approach. The overall statistical distribution has been generated that gives the rate of error probability between false positive and false negative. The error probability have been low to which have been able to distinguish FPGAs and microcontrollers of same family, series etc. Of course going forwards more enhanced techniques can be implemented but the current study validates the fact that it is very much possible to authenticate an IC without using expensive external implementations in the IC. Also with REMT, there is no need to perform any kind of changes to the PCB design etc.

Extension of the REMT approach has been done in chapter 4, where we have detailed about the effects of aging or thermal stress on the reliability of REMT based authentication scheme. In chapter 4, a detailed analysis and experimentation have been carried out using thermal stress of FPGA of 28nm technology. Also, the use of intra-die variability has been proposed that exploits the unique pattern of each FPGA to generate fingerprints. Based on the results we have focused to use different and alternate post-processing schemes that can keep the fingerprints of FPGA valid throughout its lifetime.

In chapter 5, we have shifted our focus to use guided wave approach or GEMT. In the GEMT based approach also, we have used FPGA from Xilinx but in this part of study we have developed a customized 4 layer RF-PCB. The RF wave is sent through the guided transmission line and it traverses through the FPGA or device under test. The idea here has been to exploit the process variation effects of FPGA by just implementing the interconnect between the input and output ports that guides the external RF signal from input to output ports. The results (S21 response) have shown that there is considerable difference among the response of S21 from FPGAs even if they are of same family, series etc. The post-processing techniques in this chapter adopt two schemes, one that uses cosine similarity and another that is based on the binary technique. The error probability and Hamming distance have been metrics that statistically justify the differentiation in the response from each FPGA. In the end of this chapter, we have shown how the PCB systematic errors and aging effects can be mitigated using two routes (multi route approaches).

To sum up we have been efficiently able to exploit the process variation effects of FPGAs and microcontrollers using REMT and GEMT based schemes respectively. This process variation exploitation has been effectively applied for the purpose of generating signatures for authentication of the devices. The post-processing tools like cosine similarity, Hamming distance analysis have been effectively applied that highlights the differentiation among the response from the different devices of same family, series, age etc. Also, we have given consideration to the fact that with the aging of the device, its electrical and physical mechanisms vary. Hence, aging related studies and techniques been adopted which could mitigate the aging effects on EM based authentication approaches.

As part of future work, we will focus on making the post-processing available on-chip. Also, along with the authentication, these schemes will used for other hardware security issues like Trojan detection, EM based Side channel analysis etc. Also, different other devices like analog ASIC circuit can be brought under such kind of EM measurement scheme to determine if the proposed method is efficient enough to generate signatures from the ASIC devices also.

The last chapter, chapter 6 has been an added chapter which gives proof-of-concept to use FPGAs as RF devise for RF applications. The idea in this chapter has been to facilitate the use of RF signal with the digital operations. As the boundary between RF and digital systems is getting thinner it is inevitable to introduce the concept that can interface both. In chapter 6, we have been able to realize RF basic devices like isolator, switches and power splitter. Also the later part of the chapter focused on the implementation of basic RF wireless communication using OOK based modulation scheme. The communication setup facilities the development of distributed systems that can be used in several industrial and low power applications.

References:

[1] R. F. Cordeiro, A. Prata, A. S. R. Oliveira, J. M. N. Vieira, and N. B. De Carvalho, "Agile All-Digital RF Transceiver Implemented in FPGA," *IEEE Trans. Microw. Theory Tech.*, vol. 65, no. 11, pp. 4229–4240, Nov. 2017.

[2] P. Graham and B. Nelson, "Frequency-domain sonar processing in FPGAs and DSPs," in *Proceedings. IEEE Symposium on FPGAs for Custom Computing Machines (Cat. No.98TB100251)*, 1998, pp. 306–307.

[3] Z. Ye, J. Grosspietsch, and G. Memik, "An FPGA Based All-Digital Transmitter with Radio Frequency Output for Software Defined Radio," in *2007 Design, Automation & Test in Europe Conference & Exhibition*, Nice, France, 2007, pp. 1–6.

[4] A. Bettidi, D. Carosi, F. Corsaro, L. Marescialli, P. Romanini, and A. Nanni, "MMIC Chipset for wideband multifunction T/R Module," in *2011 IEEE MTT-S International Microwave Symposium*, Baltimore, MD, USA, 2011, pp. 1–4.

[5] A. Amara, F. Amiel, and T. Ea, "FPGA vs. ASIC for low power applications," *Microelectron. J.*, vol. 37, no. 8, pp. 669–677, Aug. 2006.

[6] M. Torlak and T. M. Duman, "MIMO communication theory, algorithms, and prototyping," in *2012 20th Signal Processing and Communications Applications Conference (SIU)*, 2012, pp. 1–2.

[7] Z. Hraiech, A. Omri, M. O. Hasna, M. Siala, and F. Abdelkefi, "Best available relay and user selection scheme for interference management in wireless cooperative communication networks," in *2013 7th IEEE GCC Conference and Exhibition (GCC)*, 2013, pp. 334–338.

[8] H. Harada, "A small-size software defined cognitive radio prototype," in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, Cannes, France, 2008, pp. 1–5.

[9] A. Blaickner, S. Albl, and W. Scherr, "Configurable computing architectures for wireless and software defined radio - a FPGA prototyping experience using high level design-tool-chains," in *2004 International Symposium on System-on-Chip, 2004. Proceedings.*, 2004, pp. 111–116.

[10] "Considerations for PCB Layout and Impedance Matching.pdf." .

[11] E. E. Altshuler, "A method for matching an antenna having a small radiation resistance to a 50-ohm coaxial line," *IEEE Trans. Antennas Propag.*, vol. 53, no. 9, pp. 3086–3089, Sep. 2005.

[12] E. Moradi, M. W. A. Khan, L. Sydanheimo, L. Ukkonen, and G. S. Bova, "Metamaterial isolator for RFID based biomedical repeater system," in *2017 IEEE International Symposium on Antennas and*

Propagation & USNC/URSI National Radio Science Meeting, San Diego, CA, USA, 2017, pp. 227–228.

[13] Jeong-sun Moon, H.-C. Seo, and D. Le, "High linearity 1-ohm RF switches with phase-change materials," in *2014 IEEE 14th Topical Meeting on Silicon Monolithic Integrated Circuits in Rf Systems*, Newport Beach, CA, USA, 2014, pp. 7–9.

[14] "Switch Tutorial | DigiKey." [Online]. Available: https://www.digikey.be/en/articles/techzone/2017/sep/switch-tutorial. [Accessed: 04-Oct-2018].

[15] Y. Wang, H. Hu, and J. Xu, "A New Broadband Miniature RF Power Splitter," in *2008 IEEE MTT-S International Microwave Workshop Series on Art of Miniaturizing RF and Microwave Passive Components*, 2008, pp. 180–182.

[16] "AMPLITUDE SHIFT KEYING MODULATION, DEMODULATION, AND PERFORMANCE," in *Digital Communications with Emphasis on Data Modems*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017, pp. 227–250.

[17] B. Zhao, Y. Sun, W. Zou, Y. Lian, Y. Liu, and H. Yang, "An energy efficient fully integrated OOK transceiver SoC for wireless body area networks," in *2013 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, 2013, pp. 441–444.

[18] "(2) (PDF) A novel RF envelope detector with Ultra-Wide operation frequency range and enhanced transient response speed," *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/312380101_A_novel_RF_envelope_detector_with_Ultra-Wide_operation_frequency_range_and_enhanced_transient_response_speed. [Accessed: 12-Nov-2018].

[19] C. A. Balanis, "Antenna theory: a review," *Proc. IEEE*, vol. 80, no. 1, pp. 7–23, Jan. 1992.

[20] V. Katyal, R. L. Geiger, and D. J. Chen, "Adjustable hysteresis CMOS Schmitt triggers," in *2008 IEEE International Symposium on Circuits and Systems*, 2008, pp. 1938–1941.

[21] D. Fergusson, E. van der Meer, M. Atkinson, and D. Romano, "Distributed Computing Education, Part 1: A Special Case?," *IEEE Distrib. Syst. Online*, vol. 9, no. 6, pp. 2–2, Jun. 2008.

[22] T. Dramlitsch, G. Allen, and E. Seidel, "Efficient techniques for distributed computing," in *Proceedings 10th IEEE International Symposium on High Performance Distributed Computing*, San Francisco, CA, USA, 2001, pp. 435–436.