EXPERIMENTAL TESTBED FOR ELECTROMAGNETIC ANALYSIS

by

Sangamitrareddy Katamreddy

A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
In Partial fulfillment of
The Requirements for the Degree
of
Master of Science
Computer Engineering

Committee:

_____	Dr. Jens-Peter Kaps, Thesis Director
_____	Dr. Kris Gaj, Committee Member
_____	Dr. Alok Berry, Committee Member
_____	Dr. Monson H. Hayes, Department Chair of Electrical and Computer Engineering
_____	Dr. Kenneth S. Ball, Dean, Volgenau School of Engineering.

Date: _____ Spring Semester 2016
George Mason University
Fairfax, VA

Experimental Testbed for Electromagnetic Analysis

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at George Mason University

By

Sangamitrareddy Katamreddy
Bachelor of Technology
Vellore Institute of Technology, 2013

Director: Dr. Jens-Peter Kaps,Associate Professor
Department of Electrical and Computer Engineering

Spring Semester 2016
George Mason University
Fairfax, VA

Dedication

I dedicate this thesis to all my loved ones.

Acknowledgments

I would like to express my gratitude to my advisor Dr. Jens-Peter Kaps for giving me this opportunity to do the research. I would also thank him for guding me in every step of my thesis without which, it would have been difficult to complete the thesis. Furthermore, I would like thank CERG team and Dr. Peter Pachowicz for helping me with the work whenever needed.

Table of Contents

List of Tables

List of Figures

Abstract

EXPERIMENTAL TESTBED FOR ELECTROMAGNETIC ANALYSIS

Sangamitrareddy Katamreddy, MS

George Mason University, 2016

Thesis Director: Dr. Dr. Jens-Peter Kaps

The electromagnetic fields are generated by electronic devices dictated by the laws of Electromagnetism. These electromagnetic fields in the radio frequency (RF) spectrum disrupt the operation of other neighboring electronic devices. This disruption is called Electro-Magnetic Interference (EMI). The physical characteristics of electronic devices like timing, power consumptions, sound acoustics, temperature variations, electromagnetic fields etc., unintentionally leak secret information because they are correlated to the data being processed by the elctronic device. These characteristics of the electronic device are called side-channels. Side Channel Attack (SCA) make use of these side channels to reveal the secret information. Side channel attacks are focused on the implementation the of the algorithm and not the mathematical weakness of the algorithm. In Electro-Magnetic Analysis (EMA), the RF electromagnetic fields around the electronic device are measured and used for side channel attack. In EMA the origin of electromagentic field, the frequency spectrum of the electromagnetic field and techniques used to capture the electromagnetic field are also studied.

The main purpose of the thesis is to design and build an experimental test bed for electromagnetic analysis. The experimental test bed consists of a motorized 2D scanner, electromagnetic field sensors and amplifiers. First, the theoretical background behind the origin of RF electromagnetic fields around electronic devices and the dependency of the electromagnetic fields on the data being

processed is presented. Generic side-channel analysis techniques using electromagnetic field measurements are discussed. Later, the construction of the motorized 2D scanner is explained. Then the electromagnetic sensors built are characterized in frequency domain.

Chapter 1: Introduction

1.1 Introduction

The security services provided by cryptography are *confidentiality*, which hides the information from unauthorized access, *data authentication*, which ensures that the data is not altered by unauthorized sources, *entity authentication*, which proves the identity of an entity, *non-repudiation*, which provides the proof of identity of the sender of the data. Most of the security services relay on the secrecy of key. The goal of attack model against the cryptosystems is to reveal the secret keys. The attacks on cryptosystems differ in terms of cost, time, complexity and equipment needed. The attacks can be classified into two types, namely *passive attacks*, where in the attacker's primary goal is to just obtain the secret information from the cryptosystem and *active attack*, the inputs and environment of the cryptosystem are manipulated by the attacker and the secret keys are revealed from it's abnormal behavior because of the manipulation. In a passive attack, the inputs, outputs and algorithmic details of the cryptosystem are used to reveal the key. The physical characteristics of the electronic devices can also be considered in a passive attack. The physical characteristics are called side channels and the attacks that use them are called Side Channel Attacks (SCA). SCA can also be called implementation attacks, because the weaknesses in the implementations of cryptographic systems are exploited. Among all the physical characteristics of the electronic device show in the figure 1.1 the power consumption and RF electromagnetic fields are used predominantly.

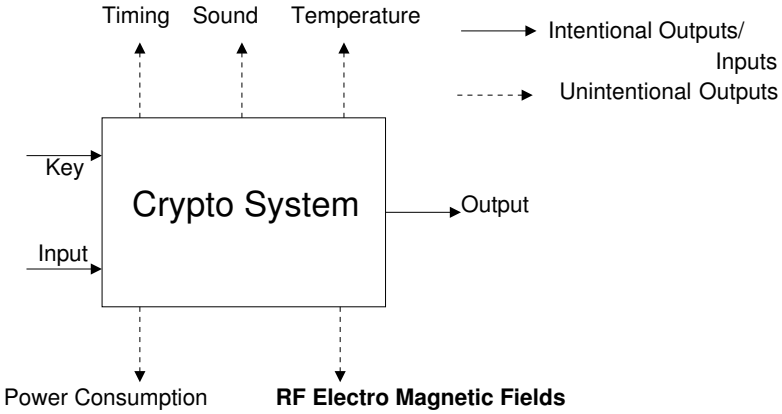


Figure 1.1: Side Channels

The power consumption of the implementation depends on the data being processed and also the algorithm that processes the data. Even the RF electromagnetic radiations, which are seen around the electrical components have the same characteristics as the power consumption. Side channel attacks which use the power consumption of the cryptosystem are called Power Analysis. The SCA which uses the RF electromagnetic fields are called ElectroMagentic Analysis (EMA). In power analysis, the power consumption of the total cryptosystem is considered in general. But in the case of EMA only the electromagnetic field radiations generated by a particular component of the cryptosystem are considered. This is called localization of EMA. The frequency of the RF electromagnetic radiations depends on the physical characteristics of the component of the cryptosystem. The localization and the frequency characteristics of the radiations are additional features of EMA.

1.2 Previous Work

1.2.1 Military Work

The leakage of information through RF electromagnetic radiations was first noticed during the World-War 1. In 1911, the German army was successful in eavesdropping on French and British voice communication. The German army collected the RF electromagnetic radiation over the single insulated wire interconnecting the field phones at the time. The German army managed to pick up the voltage drop of single wire with respect to ground. In 1915 French and British came up with countermeasures to the attack by increasing the distance between their commutation lines and

German trenches and by using twisted pair cable with reduced line currents. The secret messages of the enemies are reconstructed using the RF electromagnetic radiations. This is discussed in the book [32].

Former MI5 scientist Peter Wright in his book "Skycatcher", documented the electromagnetic attack on a French cipher machine. The French secret messages were encrypted using the cipher machine. The British conducted electromagnetic analysis on the French communication by receiving the RF electromagnetic radiations from the telex (switched network for sending messages using teleprinter) cable. A broad-band radio-frequency tap installed on the telex cable was used to pick up the RF electromagnetic radiations and routed the signal to the attacker location. The RF signals are collected by the attacker and analyzed to recover the plaintext given to the cipher machine.

The first covert listening device, "The Thing" was discussed by Peter Wright in his book. This device is gifted to American Ambassador's office in Moscow, in 1951. It is used for transmitting audio signal. The devices consisted of a tiny capacitive membrane connected to an antenna. The radio frequency signals received through the antenna vibrates the capacitive membrane. The radio frequency signal is modulated on the signal produced due vibration and the modulated signals are retransmitted. The modulated signal can travel longer distance. The signals can reach the attacker, who is far away from the target and unnoticed by others. The modulated signals are later demodulated and can be used for recovering the secret information.

Since the early 1960s Military Organizations know that computers generate electromagnetic radiation that not only can interferes with radio reception, but also leaks information about the data being processed. The unintentional broadcast of data by the physical characteristics of the electronic devices is known as *compromising emanation* or *Tempest* radiation. They have been a major concern while evaluating the security of the military applications. *Tempest* is the US military code name referring to a classified US government program, which aims at protection efforts against leakage and spying on the information systems.

1.2.2 Open literature

Electromagnetic Analysis was first documented by Van Eck in his paper [45]. A 5 minute documentation was telecasted on the BBC program "Tomorrow,s World", 1985. The video shows a

demonstration of electromagnetic analysis. The screen content of a video display unit was reconstructed using a TV set with manually controlled oscillators to synchronize with the video display unit frequencies. The process of collecting emanations and specifications of reception equipment was described in [45]. The paper gives us the basic idea of electromagnetic analysis and the dependency of EM analysis on the frequency. With the advent of smart cards use for parking tickets, transportation payment and bank transactions, the attackers started side channel analysis on smart cards. The first attacks were timing analysis and power analysis on smart cards. In power analysis a resistor is inserted at the ground pin of the target device to measure the voltage drop. In the case of electromagnetic analysis the raditions are collected by a probe without touching the target. The EM Analysis was conducted on smart cards by Jean-Jacques Quisquater and David Samyde in 2000/2001. In their paper [37] ean-Jacques Quisquater and David Samyde demonstrate the collection of radiations emitted from a smart card. The experimental setup used for sensing the electromagnetic radiation is discussed.

The paper depicts that EM Analysis is similar to Power Analysis. The electromagnetic radiations are spatially restricted to the functional units of cryptosystem. In 2001, Karine Gandolfi et al. [13] conducted electromagnetic analysis and power analysis on three different cryptosystems DES, COMP128 RSA. They concluded that, Signal to Noise Ratio(SNR) of electromagnetic measurements are more than that of power consumption measurements.

In the same year, in [38] the efficiency of Diffrential ElectroMagentic Analysis (DEMA) over Differential Power Analysis (DPA) is proven by using electromagnetic radiations and power consumption measurements. Sensitivity of the measurements towards the variation in data being processed is analyzed. Dakshi Agrawal et al. discussed in 2002[2], different types of electromagnetic radiations. Direct radiations are emitted from the current carrying conductors and unintentional radiations are modulated signals. The high frequency unintentional signals travel far distances and can be used for far field EMA, when it is impossible for attacker to be at the vicinity of the target cryptosystem.

The authors describe the environmental conditions under which each type is radiated. In 2003, [1] the same research group proposed an advanced side channel attack. Template attacks are a superior data analyzing technique for small key length cryptosystems. Here, an experimental device similar to the target device is used. The cryptosystem algorithm is implemented on the experimental

device. For each possible value of key, the crypto operations are executed on the device with a known set of inputs. The electromagnetic radiations are collected during each crypto operation. A look up table is prepared for each possible value of the key and electromagnetic radiations generated during the crypto operation using the key. Later, the corelation between the measured radiations from the target and the radiations in the look up table is calculated. The key with the highest corelation is the secret key of the target cryptosystem,

In the same year the Dakshi Agrawal et al.[3] proposed another attack using multiple side channels to compromise a device. The measurements from multiple side channels (electromagnetic and power measurements) are considered for the analysis. In December 2003, Markus G. Kuhn has proposed his dissertation [24] on eavesdropping risks of Computer Displays. The dissertation report documents the eavesdropping experiments he conducted on contemporary computer displays. He discussed the nature and properties of compromising emanations from both cathode-ray tube and liquid-crystal monitors. The parameters of the experimental setup, such as synchronization between the emanations from the display unit and the receiver are discussed. In 2005, a classification of EMA is done by B. Preneel in [7]. Simple Electromagnetic analysis (SEMA) exploits the relationship between executed operation and the EM radiations generated by the cryptosystem. In SEMA, the electromagnetic radiations are collected during a single crypto operation with any data input. The Differential Electromagnetic Analysis (DEMA) exploits the relationship between data processed and the EM radiations. In DEMA, the electromagnetic radiations are collected during each of N number of crypto operations with known N data inputs. Almost until 2006, studies concentrated on the extraction of secret data from measured waveforms. Later countermeasures against EMA are used and more complicated devices like FPGAs are considered as targets. Thereafter, better measurement techniques to obtain significant waveforms are introduced. The knowledge of electromagnetic field cultivated in the field of Electro Magnetic Compatibility (EMC) is used for the study of the frequency characteristics of the electromagnetic fields and the sensors used for picking the measurements. In 2007, Trasy et al. documented an overview of SEMA [27]. The Visual Inspection of Trace, Template Attack and Collision Attack are discussed. The practical realization of SEMA is performed by the visual inspection of EM radiation measured during the process of AES and the attack is performed to obtain the secret key. In 2008 Qiang Zhao et al described the relation between the processed

data and the electromagnetic emanations. The effects of variations of the current density in CMOS on the electromagnetic field around device are discussed. The hamming distance and the hamming weight of the data being processed are directly related to the power consumption and electromagnetic radiations. In 2008, Zhao showed a DEMA attack on AES using the Distance of Mean technique [11]. Zhao along with group from Shijiazhuang Mechanical Engineering College showed the experimental setup and the places in the near field on the target where the information leaking emanations can be collected [6]. Thomas Plos documented in 2008 an attack on RFID to obtain the secret through DEMA [36]. In 2008, C. Archambeaus [43] provide theoretical and practical insights in the analysis of the power and EM side-channels and their efficient exploitation with powerful statistical tools. In 2009, Zhao developed a attack namely Correlation EMA [26], which is efficient than Distance of Mean.

Olivier Meynard et al. proposed pre-characterization of CEMA in [12] . Hidenori Sekiguchi [42] in 2011 analyzed factors on which the reading distances in far field electromagnetic emanations depend. Naofumi Homma et al in 2010 documented an experiment on an FPGA with AES [15] to show how the secret information is leaked from the common mode current. The dissertation [8]] by De Mulder Elke shows the study of the probes, their resolution and the suppression of noise.

1.2.3 Electro Magnetic Analysis in Frequency Domain

In 2011 Sylvain Guilley et al proposed two papers. The first one [31] introduces a method to characterize a cryptosystem in the frequency domain. Amplitude modulated electromagnetic radiations are used for EM analysis. The procedure of this analysis, along with the elimination of interference of clock harmonics are discussed in [35]. The EM emanations differ by the physical characteristics of the target. This is illustrated in [14]. The resonant frequency of electromagnetic radiations depends on the physical characteristics of the target.

1.2.4 Near-Field Probes

In 2001, [13] Gandolfi et al. tested different types of probes such as hard disk heads, integrated inductors, and magnetic probes. They came to the conclusion that a hand-made solenoid yields the best results in their case. Gandolfi et al. proposed that high resolution inductive probes can

be used to collect localized radiations at high resolution. In 2002, [2] Agrawal et al. used a plate shaped electric probe. In the near-field the magnetic fields dominates the electric field. Based on this, magnetic field probes are used in many attacks.

1.2.5 Localization

As we discussed before, the electromagnetic radiations are location dependent. The best results of electromagnetic analysis are seen in specific locations of the target. This is discussed in [4], [7] [34] and [40]. In 2009, the practical resolution limit of the magnetic field sensor is evaluated based on the magnetic field strength and the required minimum output voltage at the probe [**?**]. In the same year, Denis Real [39] proposed indicators to locate the hot-spot where the attacker has to keep the probe to obtain the best results with least amount of samples. Based on this, many experiments were conducted, but the results weren't as expected. The observed areas of signal leakage do not coincide with the placement of the leaking design parts on the floor plan of the FPGA. The resolution of the sensors used is not sufficient. The smaller the dimensions of sensor, the better the sensor is suited for locating specific sources of radiation. High resolution probes are proposed. Kirschbaum and Schmidt [20] used a course resolution probe to present evidence for successfully localizing EM leakage and performed cartographic measurements. Heyszl et al. [16] use a high-resolution probe to show the dependency of information leakage on the measurement location, but clear evidence for the feasibility of localizing leakage of the circuit parts is lacking. In 2013, Johann Heyszl et al. published two papers. One [17] provides evidence for the localization of the emanations, by conducting experiments on FPGAs with two uncorrelated S-boxes and the later paper [28] shows an attack on a Physical Unclonable Function(PUF) based on the localization of emanations.

1.2.6 Cartography of the Target Device

Cartography is the process of collecting radiations on every point on the target device. The magnetic field probe is attached to a scanner. With specific resolution and step size, the probe is move on the device. The probe scans the device in horizontal and vertical direction and collects emanations.

In [9] and [5] Weighted Global Magnitude Squared Incoherence (WGMSI) analysis is proposed. WGMSI to find the positions where DEMA might be successful with a reduced set of traces. In

2009, Sauvage et al. [41] explained how cartography combined with EMA can break a cryptosystem protected by Dual-rail with Recharge Logic (DPL). Sauvage et al.[40] conducted the localized attack on FPGAs and the steps involved in the cartography to obtain secret data are explained.

Masahiro et al.[19] explain how the ground bounce leaks information. Olivier et al. [30] shows that the electromagnetic radiations collected near the ground/power leaks information with high SNR. Denies Real et al. [39] the enhancing cartography tells that the ground bounce is the source of propagations of the leakage. And so the highest leakage is obtained at power/ground pins. As a countermeasure decoupling capacitors are placed on back side of the circuit, then radiations collected from the power/ground pins do not leak information due to the capacitor. But the information is leaked by scanning the capacitor.

1.3 Research Objective

The main objective of the research described in this thesis is to preform cartography on a target device. An XY-Table (motorized scanner) is built for the cartography. Magnetic field probes are built and characterized. Amplifiers used for the measurements are built and characterized. The cartography is preformed using Flexible Open-source workBench fOr Side-channel analysis (FOBOS).

Chapter 2: Side-Channel Analysis Techniques

Side channel attacks using the physical characteristics of electronic device were first proposed by Kocher. He used time [22] and power [21] measurements to reveal the secret data processed on the electronic device. These attacks are named as timing analysis and power analysis. In 2001, Quisquater et al. [37] conducted side channel attack using the electromagnetic field radiated around the target device. This attack is considered as Electro-Magnetic Analysis (EMA). Same analysis techniques are used for both power analysis and electromagnetic analysis.

2.1 Power Analysis

The power consumption of an electronic device is proportional to the electric current drawn from the voltage supply pins. In power analysis, the current is measured by inserting a resister between the target device and the power supply pin. The voltage across the resister is measured. A current sensor can also be used in power analysis to get the measurements. The transient current from the supply pins conducts through a series of parasitic conductors at the supply pins, which acts as low pass filter. So, the power consumption signals are dominant in lower radio frequency spectrum.

The electronic device consists of many components like registers, Random Access Memory (RAM), logic gates, Algorithmic Logic Unit (ALU) etc., The magnitude of transient current measured at the voltage supply pin depends on the power consumption of all these components. Power consumption of a specific component can not be measured so, it is not localized. The instantaneous power consumption is not same for all operations, because the usage of components will be different for each operation. While performing a specific operation, different possible values of data are processed and again the instantaneous power consumption is not same for all. The power consumption varies according to the operation performed and the data processed.

2.2 Electromagnetic Analysis

The radio frequency electromagnetic radiations are generated by moving of electric charges. The strength of the electromagnetic fields are dependent on the magnitude of current and potential difference. In electromagnetic analysis, the electromagnetic field strengths are measured and analyzed. The electromagnetic field strengths are measured using electromagnetic sensors.

2.3 Process of Electromagnetic Analysis

In Electromagnetic Analysis the field strength of the electromagnetic radiations is measured during a particular operation of the cryptosystem. The operation should be chosen such that it depends on the secret data. Having knowledge of the algorithm of the target crypto-system is very important. Based on the algorithm, the type of Electromagnetic Analysis to be performed is determined. The electromagnetic radiations are measured while the algorithm is running on the electronic device. The cryptographic algorithm consists of several functions (operations). The electromagnetic radiations are collected during a part of algorithm or the entire algorithm. The functions are translated into instructions. Each instruction is processing different data and utilization different functional units of the electronic device. Every instruction has a typical electromagnetic trace. The graph of electromagnetic field strength measured using sensor with respect to time is called electromagnetic trace. The electromagnetic sensor measures the electromagnetic field strength. Types of Electromagnetic Analysis are discussed below.

2.3.1 Simple Electromagnetic Analysis

In Simple Electromagnetic Analysis (SEMA), the electromagnetic radiations of target cryptosystem are acquired and analyzed for a part of algorithm or the entire algorithm. The EM radiations are visually inspected to obtain the keys or other private data involved in the target cryptosystem. Irrespective of the inputs given to the cryptosystem, the EM radiations are collected during a single run of the cryptosystem. SEMA exploits the operation dependency of the EM radiations. SEMA is successful only for implementations where the operations executed are dependent on the secret key.

For example, in a SEMA attack on Elliptic Curve Cryptosystem (ECC) [18], the radiations are

obtained during the Elliptic Curve (EC) Point Multiplication of plaintext using the private key. The double and add algorithm of the EC point multiplication is given below

Algorithm 1 Elliptic Curve Point Multiplication

Require:
EC point P = (x, y), integer k, $0 < k < M$, $k = (k_{l=1}, k_{l=2}, \ldots, k_0)_2$, $k_{l=1} = 1$ and M
Ensure: $Q = (x\prime, y\prime) = [k]P$
$Q \rightarrow P$
for i from l−2 downto 0 do **do**
    $Q \rightarrow 2Q$
    if $k_i = 1$ **then** then
        $Q \rightarrow Q + P$
    end if
end for

EC point multiplication involves a series of doubling and addition. The doubling operation is executed in every iteration, however the addition operation is executed only when the corresponding iteration key bit is one. The electromagnetic field strength during execution of doubling and addition is different from electromagnetic field strength during execution of only doubling. This is evident from the figure shown below. The key value is identified by looking at the EM trace.

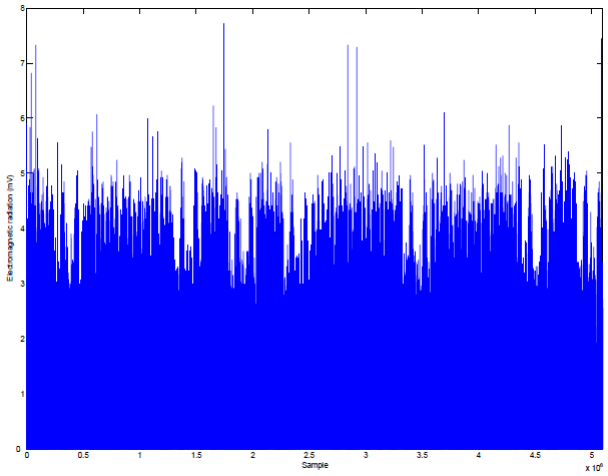


Figure 2.1: Electromagnetioc radiations during Double and add EC point multiplication

In SEMA, knowledge about the data processed in the algorithm is not required. According to [35], the unintentional signals are radiated by AM modulation on the carrier signal with clock frequency. So by AM demodulating at the clock frequency, SEMA is conducted on the demodulated signal. SEMA needs exact time where the target operations are preformed on the device. This

requires complete knowledge about the algorithm and the measurement device should be triggered at the exact time.

2.3.2 Differential Electromagnetic Analysis

The "Always Double and Add" EC point multiplication algorithm is a countermeasure against SEMA. The algorithm is given below. In this algorithm, both doubling and addition are executed in all

Algorithm 2 Elliptic Curve Point Multiplication, always double and add

Require:
EC point P = (x, y), integer k, $0 < k < M$, $k = (k_{l=1}, k_{l=2}, \ldots, k_0)_2$, $k_{l=1} = 1$ and M
Ensure: $Q = (x\prime, y\prime) = [k]P$
$Q \rightarrow P$
for i from l−2 downto 0 do **do**
  $Q_1 \rightarrow 2Q$
  $Q_2 \rightarrow Q_1 + P$
  if $k_i = 1$ **then** then
    $Q \rightarrow Q_2$
  else
    $Q \rightarrow Q_1$
  end if
end for

iterations. The operations executed are not dependent on the secret key. The electromagnetic radiation collected during the algorithm is shown below.

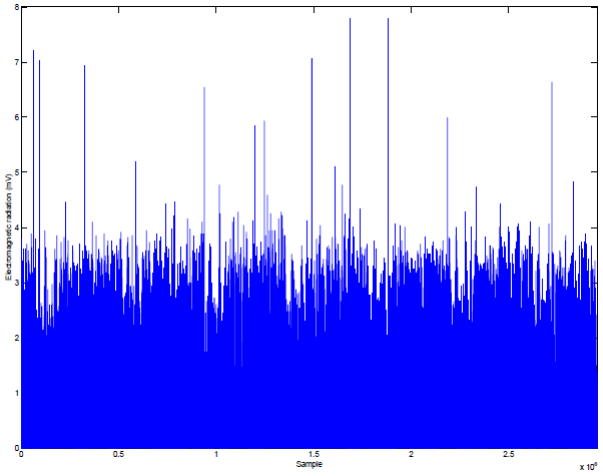


Figure 2.2: Electromagnetic Radiations during Always Double and Add EC Point Multiplication

Since both operations are executed, it is difficult to identify the key by visual inspection.

The data dependency is exploited using Differential Electromagnetic Analysis (DEMA). The

Differential Electromagnetic Analysis (DEMA) requires either known plain text or the known cipher text along with predicted values of the secret data which is the Key in most the cases. Considering a cryptosystem, it takes plain text/cipher text and the key as inputs. The plain text/cipher text and key are processed to obtain the cipher text/plain text. Algorithmic knowledge of the cryptosystem is required to identify the D-Function, where the key and plaintext/ciphertext are processed together. In DEMA, RF electromagnetic radiations are collected during multiple runs of the cryptosystem. EM traces are analyzed and the secret key is obtained.

The secret data and the known data are processed in the cryptosystem. At a point in time, the known data and secret data are processed together in a operation in cryptosystem. This operation is known as the D-Function.

The output of the operation are later processed in the cryptosystem. The EM field strength while processing the output is dependent on the value of the output. In DEMA, a single k^{th} bit of the D-Function output is considered for analysis. The known data can be either ciphertext or plaintext. For M known data values, the crypto system is executed for each value. During M runs of the cryptosystem with M known data values, the EM radiations are collected for each run. The EM field strength is estimated by manually calculating the k^{th} bit of the D-Function output using N maximum possible number of unknown data predictions and M known data values. We have M electromagnetic traces and M*N estimated k^{th} bit values. Each EM trace corresponds to a known data value.

For each unknown data value the M electromagnetic traces are divided into two groups such that, the estimated k^{th} bit value for the corresponding known data value is 1 in one group and 0 in the other. The mean of EM traces in each group is calculated and later the difference of means is calculated. The above process is repeated for all unknown data values. The unknown data value with highest peak of difference of means is the secret data processed in the crypto-system. The radiations are collected over a time period, the highest peak is seen at the point where the target k^{th} bit is processed in the crypto-system.

2.3.3 Correlation Electromagnetic Analysis

In Correlation Electromagnetic Analysis (CEMA), more than one bit of D-functions are consider for analysis. For a single bit, the EM field strength depends on the value of bit and for multiple x bits it depends on either hamming distance or hamming weight of the x bit value. Hamming weight of a binary value is the number of binary ones in it. Hamming distance between two binary values is the number bit positions at which the bit values are different.

For a D-function on cryptosystem, the hamming distance or hamming weight are calculated manually using N maximum possible number of unknown data predictions and M known data values. The estimated outputs of D-function are called as hypothetical values. If we have N possible unknown values and M known values, then we have MxN hypothetical values. The EM radiations are collected for M runs of cryptosystem for the M known data value. For each unknown data value, the correlation between M radiations and M hypothetical values is calculated. The unknown data value with highest peak is the secret data. The distinguishers are used to measure the relation between the hypothetical value and the radiations collected.

2.3.4 Distinguisher

Distinguishers are used to measure the relation between the hypothetical values and the traces collected. These are two type of distinguishers which are prominently used for CEMA.

Pearson Correlation

The linearity of the radiations with the hypothetical values is calculated. Since it is calculating linearity, any hypothetical values which are linear to each other yield same results with the radiations. So the D-Function, which is used to measure the hypothetical value should be non-linear. The Pearson's Correlation of two variables X and Y is given by

$$\rho(X,Y) = \frac{\mathbf{Cov}(X,Y)}{\sqrt{\mathbf{Var}(X)\mathbf{Var}(Y)}}.$$

where $CovX,Y$ is the covariance of X and Y, $VarX$ is the variance of X and $VarY$ is the variance

of Y.

Mutual Information Analysis

The relation between the hypothetical values and traces is measured by the probability density of the hypothetical values and traces. Since linearity is not measured, the D function can be of any type. The Mutual Information Analysis of two variables X and Y is given by

$$I(X;Y) = H[X,Y] - H[X|Y] - H[Y|X]$$

where $H[X,Y]$ is the Joint Entropy of X and Y, $H[X|Y]$ is the Conditional Entropy of random variable X given variable Y and $H[Y|X]$ is the Conditional Entropy of random variable Y given variable X.

2.4 Mechanism behind Electromagnetic Analysis

2.4.1 Complementary Metal Oxide Semiconductor (CMOS)

Complementary Metal Oxide Semiconductor (CMOS) is the basic building block of most electronic devices. The CMOS inverter is composed of P-type metal-oxide-semiconductor (PMOS) and N-type metal-oxide-semiconductor (NMOS). The NMOS is active when the value of input is one and the output is connected to ground. The logic level of the output is zero. The PMOS is active when the value of the input is zero and the output is connected to Vcc. The logic level of the output is one. The CMOS inverter figure 2.3 is given below.

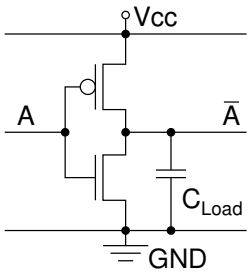


Figure 2.3: CMOS inverter

CMOS gates have three distinct dissipation sources. First, the leakage current in the transistors which contributes to a minimal amount of dissipation. Second, the direct path current which exists during the switching of gate output value. It exists for a short period of time when both PMOS and NMOS transistors are active and current conducts from V_{DD} to ground. Third, the charging and discharging of the load capacitance at the output of CMOS. The direct path current and charging and discharging current are shown in the figure 2.5.

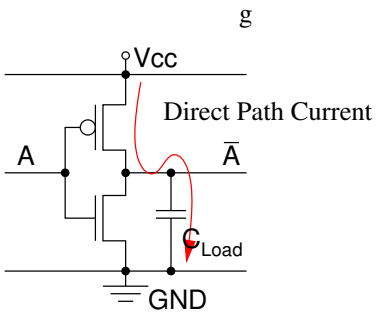


Figure 2.4: CMOS Direct Path Current

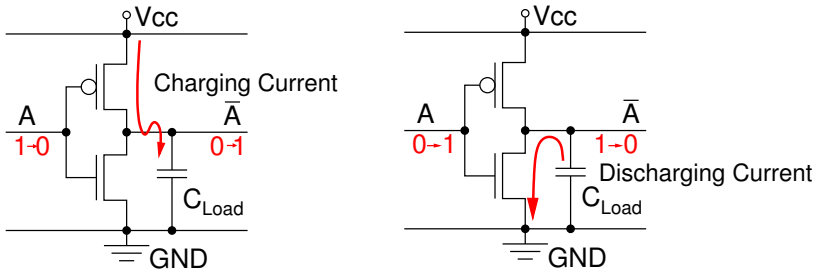


Figure 2.5: Charging and Discharging of Capacitor

The expression for the dynamic power consumption of the CMOS inverter is given by the equation below

$$P_{dyn} = (C_L + C_{dp})V_{DD}^2 P_{0\to1} f. \tag{2.1}$$

where C_L is the load capacitance at CMOS output, C_{pd} is the power dissipation capacitance of CMOS, V_{DD} is the voltage source, $P_{0\to1}$ is the probability of CMOS output switching and f is the frequency of switching. The power consumption and the electromagnetic field generation are dependent on the direct path current and charging current.

2.4.2 Ground Bounce

Ground bounce is seen during the CMOS output transition from 1 to 0. The ground bounce measured during the transition can be seen in figure 2.2. During the transition of output, discharging current is conducted from the output to ground. There are parasitic inductors between die ground and board ground. It can be seen in figure 2.6. Due to discharging current conducting through the inductors, voltage difference is seen across the inductors between die ground and board ground. The die ground potential raises above the board ground. Voltage across the inductors is given by

$$V = -L\frac{\mathrm{d}i}{\mathrm{d}t} \tag{2.2}$$

Here L is the parasitic inductance and i is the discharging current.

The discharging current produced is dependent on the data processed. The ground bounce current can be measured at a ground pin. The electromagnetic field with maximum information is seen at the power/ground pin. Ground bounce also adds to the other dissipations from CMOS. The ground bounce can be reduced by adding capacitors between board power pin and ground pin. Adding a capacitor reduces the Ground bounce in CMOS. The size and position of capacitor should be considered. The capacitor should be placed close to the pins avoiding the parasitic inductance between capacitor and pin. The size of the capacitor should also be considerably small to reduce inductance of the capacitor. If any parasitic inductor is occurred due the capacitor, the ground bounce current flows through the parasitic inductor.

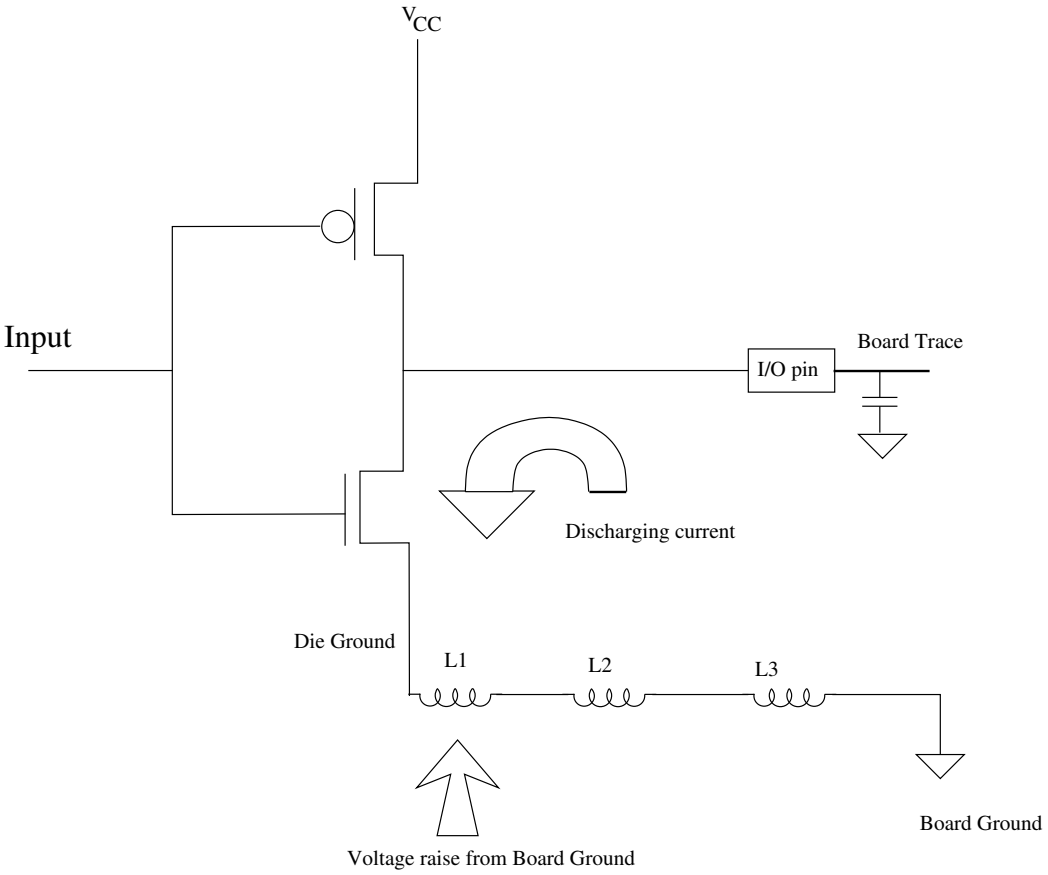


Figure 2.6: Voltage Raise

2.4.3 D-Function

D-Function is the target function chosen in an algorithm and in D-Function known data and key has to be processed together. The D-Function is chosen in such way that the data dependency is reflected in the power consumption and the electromagnetic radiation during this function. The output of the D-function are considered at the gate level or at the register level. In register level the output generated is stored in a register. Again they are two ways of storing values in the register. First, loading the input value at sensitive edge of clock. Here if the register already has a value stored in it, then each bit is changed to new value. The interchanging of bits causes the power consumption and electromagnetic radiations. The power consumption depends on the hamming distance of the new value and old value of the register. Second, the register is loaded with a stream of all binary ones or zeros in the beginning phase of the clock and then loaded with the actual value in the second phase. Here the loading of the bits causes the power consumption. The power consumption depends on the

Table 2.1: Types of Electro Magnetic Analysis

case	Attack type	Attack Target	Attack function	Trace
1	SEMA [18]	Key RSA	Exponentiation	Single trace during Exponentiation
2	DEMA [38]	Key DES	S-Box output	n encryption traces
3	DEMA [34]	SBox	Register level	n encryption traces
4	CEMA [10]	AES	S Box	Cartography
5	SEMA with demodulation [35]	RSA	Exponentiation	Single trace during Exponentiation
6	DEMA with Trojan [25]	PRESENT	Sbox	n encryption traces from trojan
7	CEMA [26]	DES	last round xor	n encryption traces
9	SEMA [27]	AES	ADD ROUNDKEY	Template Attack
10	DEMA [7]	ECC multiplication	Register level	n encryption traces

new value loaded, which is the hamming weight of the bits. When the output of the D-Function at gate level is used for the analysis, the hamming weight of the output is considered. In this is case it assumed that the output value is processed later in algorithm and the power dissipation while processing the value is dependent on number of ones in the value. Therefore, the hamming weight is considered for analysis

Chapter 3: XY table

This chapter explains the construction of a motorized 2D scanner which is controlled by an MSP430 microcontroller. First, we discuss the technical details of the scanner. Later, we focus on describing the MSP430 programming.

3.1 Introduction

The measurement setup is an extension to FOBOS to conduct Electromagnetic Analysis. The measurement setup for Electromagnetic Analysis consists of a XY table (two dimensional scanner), a magnetic field probe to collect electromagnetic radiation from the target,a FPGA controller and a PC. The framework consists of software package with programs for XY table, Device Under Test (DUT) programming, data acquisition and data analysis.

3.2 XY Table Design

The block diagarm of the XY table is shown below **??** The scanning details (step size, start point and stop point) are given as input to the measurement setup. The output is the electromagnetic radiation measurements acquired from the oscilloscope or spectrum analyzer.

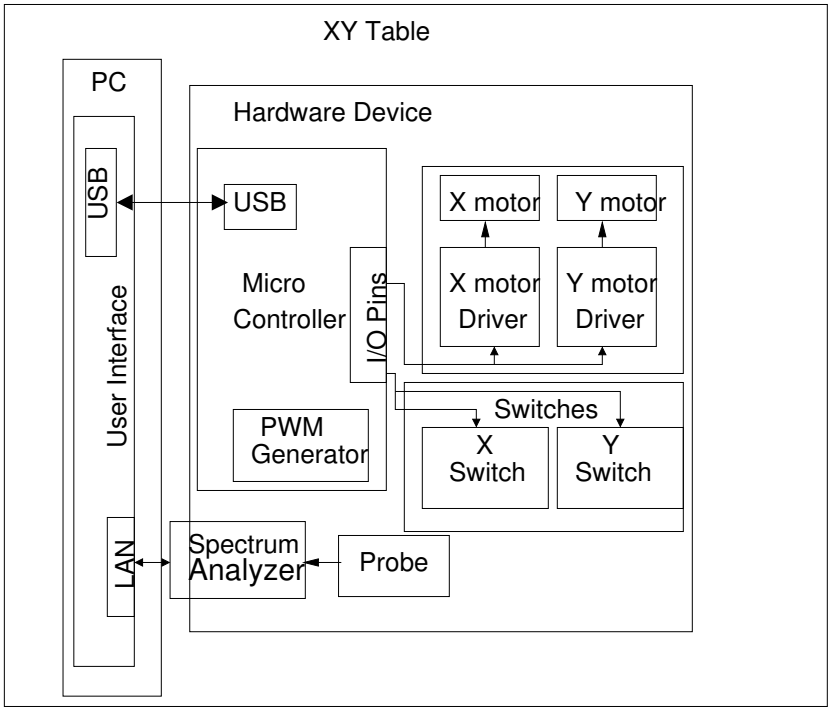


Figure 3.1: Level_2 Design

3.2.1 XY Table

Proxxon XY Table

The Proxxon XY Table is used as base for the 2D Scanner. The Proxxon XY Table has X and Y axis. The stepper motors are connected to each axis.

Stepper Motors

The bipolar stepper motors are used for motorization of XY Table. The step size of motor is 1.8 degree. Bipolar stepper motors are assembled to the XY table. Bipolar stepper motors have two coils, so two H-bridges are required for each motor. The working of the bipolar stepper motors is explained in Appendix.

H-Bridge

The motors are connected to the microcontroller through H-bridge. The motors are connected to the MSP430 through H-bridge (SN754410). Using H-bridge the voltage can be applied on either directions of the motor coil. The Integrated Circuit (IC) SN754410 is selected because it has two H-bridges. The voltage is applied on the coil only when the enable is high. On the Printed Circuit Board (PCB) circuit, four H-bridges are connected to the MSP430. Port P1 pins 2,4,5,6 are assigned to the H bridge inputs. The Port P2 pins 0,2,5 are assigned as enables for motor X,Y and Z.

Limit Switch

On the either ends of the X and Y axis the switches are glued. Interrupt is occurred when either of the switch is pressed.

The interrupt is occurred when the limit switch is pressed and the respected axis is locked. The axis is locked until it is moved in the opposite direction. The Port P2 pins 3, 4, 6 and 7 are assigned as interrupts for home signals X and Y. The pins for the interrupts along with their respective axis and direction are listed in the table 3.1.

Table 3.1: Limit Switches

Interrupt	Pin	Direction	Unlock Axis
X0	P2.3	X Right	X Left
X1	P2.4	X Left	X Right
Y0	P2.6	Y Forwards	Y Backwards
Y1	P2.7	Y Backwards	Y Forwards

MSP430

The XY table motors are controlled by the MSP430F5529 microcontroller .

3.2.2 PC

3.2.3 Probe

The Probe is stable and attached to the XY Table. The target is placed on the axis. The axis move according to the instructions given through the python code. The Electromagnetic radiations

captured by the probe

3.2.4 Oscilloscope

The electromagnetic radiations are measured by connecting the probe to oscilloscope or spectrum analyzer. The measured data is transferred to the computer by the python code over Local Area Network (LAN).

3.3 XYTable

3.3.1 Interface

The XY table is designed such that, the MSP430 is interfaced with the PC using Universal Serial Bus (USB) Communication Port (COMPORT) interface. The data connection is created between the MSP430 and the USB host (PC) through Communication Device Class (CDC) of the USB Application Programming Interface (API). The explanation about the USB API stack is included in the MSP430 USB Programmer's Guide. The COM port is used for the communication between MSP430 and the PC. The python code running on PC opens the COM port to which the MSP430 USB interface is connected. The descriptor tool is used to establish the interface between MSP430 and PC. The MSP430 USB interface related information given to the descriptor tool and descriptor is generated. Descriptor communicate the device's identity to the host. The process for generating the descriptor and the driver software is included in the MSP430 USB Programmer's Guide. The MSP430 project for USB interface is created in an Integrated Development Environment (IDE). The descriptor tool generates four files, among them "descriptor.h","descriptor.c", "UsbIsr.c" should be added under "USB_config" project folder and .inf extension file is used for driver installation in windows OS. In windows Operating System (OS) the CDC API communicates over virtual COM port. The driver software is required to install virtual COM port on the USB host (PC). The driver software can be installed by the .inf file generated by the descriptor tool. But, we faced a problem while installing the .inf file generated by the descriptor tool. So we used the driver software file (inf File) that is already provided for the CDC API examples in MSP430 USB developer package.

3.3.2 MSP430 Protocol

USB_ setup(TRUE, TRUE); is used to initialize USB and enable all USB events. The H-bridge input, the motor input and the motors enables are initialized. We enabled the interrupts for the limit switches. In a continuous loop, then the state of the USB is checked to continue. The input to the motors are given only in "Enumerated Active" state in which, the interface between MSP430 and host is active. Once the program enters the "Enumerated Active" state, it waits until the data is received over the COM port. The function bCDCDataReceived() is true when the data is received. The interrupt file USB_ISR has all event interrupts including data_receive event. If the receive event occurr, the received data is analyzed and the operations are done according to the commands received. Figure 3.2 explains the flow chart for MSP430 programming and table 3.2 shows the commands used and their respective functions. For the multi step movement of motor, "MICM" command followed by the number of steps should be given.

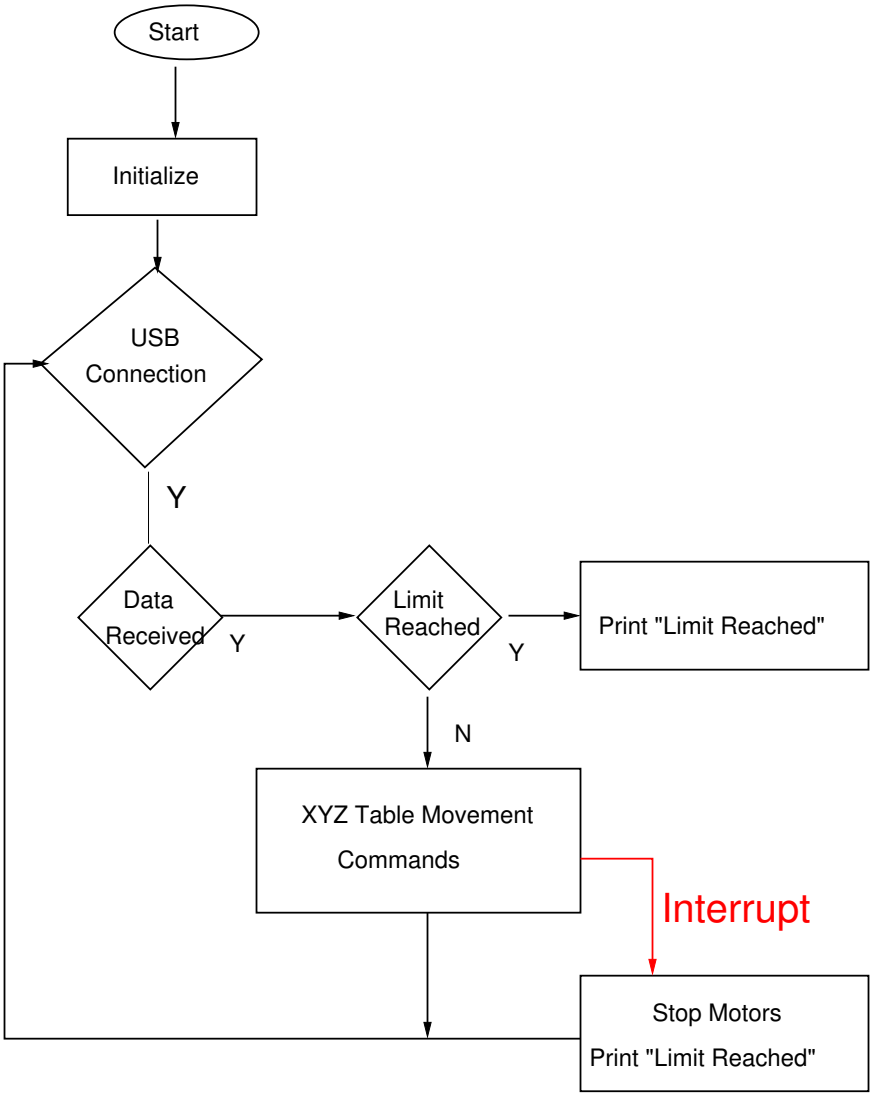


Figure 3.2: MSP430 Flow chat

Given the command

Table 3.2: Commands

Mode	**Motor1**		**Motor2**		**Motor3**	
	Clockwise	Anticlockwise	Clockwise	Anticlockwise	Clockwise	Anticlockwise
Continious	M1CC	M1AC	M2CC	M2AC	M3CC	M3AC
One Step	M1CO	M1AO	M2CO	M2AO	M3C0	M3AO
Multi Step	M1CMXY	M1AMXY	M2CMXY	M2AMXY	M3AMXY	M3AMXY

3.3.3 Python Programming

The python programming is used to send commands to the MSP430 over the COM port. The commands are sent to MSP430 according to the protocol. First, the motors go to the home position, then the python code will ask for the start point and the stop point inputs from the user. The start point and the stop points can be given by the navigation switches of the keyboard. While user is navigating the XY table, the python code records the number of steps moved and saves it as the start point and same repeats with the stop point. Then the python code ask for the step size. Later, the XY table starts scanning. While scanning the XY table goes to the start position and then scans in the X direction with the required step size and at each step it waits until the task completed (crypto operation). Once it is done with the X-axis scanning, the XY table moves back to the X-axis's home position and goes to the next step on the Y axis. It starts scanning once it reaches the X-axis start point. While moving back to the home position on either axis, the python code will be continuously listening to the MSP430 for interrupts, until it reaches the home position. Figure 5.1 explains the flow chart for python programming.

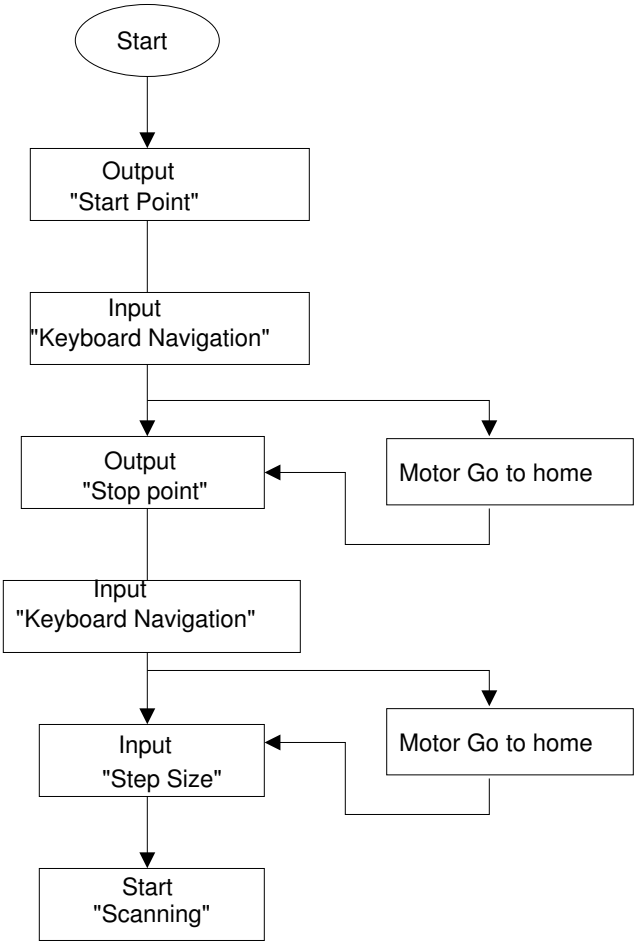


Figure 3.3: Python Programming Flow Chart

The flow chart for scanning is shown in figure 3.4

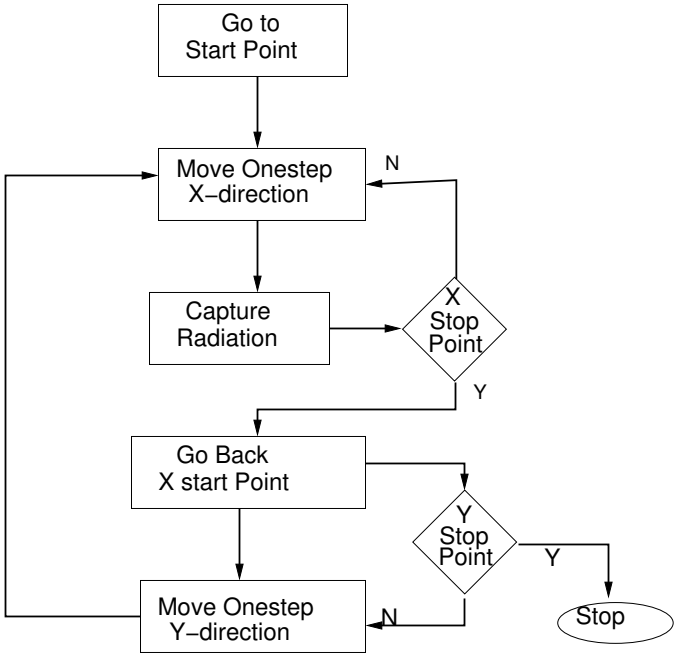


Figure 3.4: Scanning Flow Chart

Key Board Input

The inputs to the XY Table is given through a keyboard. The python programming is dependent on the input given using the keyboard. The python in-built module "Getch()" is used to read the keyboard input. It returns the string of characters that represent the key pressed. The python in-built function "ord()" is used to get the unicode point of the character. The unicode points of the characters returned while the keys pressed in Linux and Windows OS is given below in the table 3.3

Table 3.3: Unicode Points

Key	Unicode Linux	Unicode Windows
Enter	'13'	'13'
Home	'27' '91' '72'	'224' '71'
End	'27' '91' '70'	'224' '79'
Delete	'27' '91' '51'	'224' '83'
↑	'27' '91' '64'	'224' '72'
↓	'27' '91' '66'	'224' '80'
→	'27' '91' '67'	'224' '77'
←	'27' '91' '68'	'224' '75'

The module Getch() works only with windows. The libraries ssy and termos are used in Linux OS to get the input keys. For navigating the XY Table towards the start point and the stop point, the arrows are used. When "Enter" is pressed, the python stops navigating and goes for the next task. Figure 3.5 explains the flow chart for keyboard navigation.

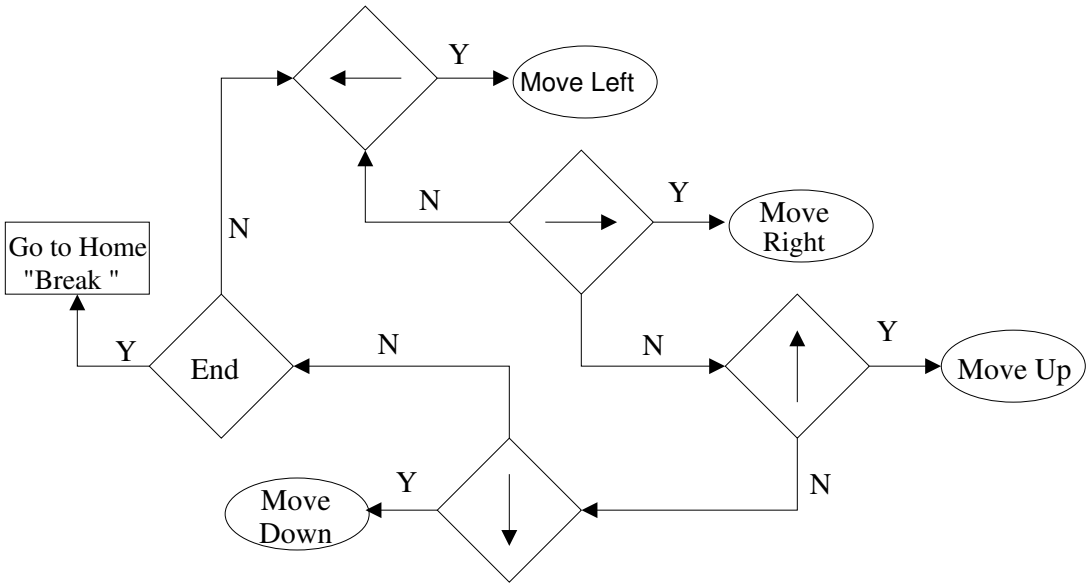


Figure 3.5: Keyboard Navigation flow chart

3.3.4 Hardware

3D Printing and Assembly

The XY table is motorized by connecting bipolar stepper motor to X and Y axis. The plastic components and shaft couplers are required to assemble motors with XY table. The plastic components are printed using 3D printer. The instructions for assembling, the 3D printing source files and the other parts list are found in the link on Thingiverse website. The link is given below. 3D print thing files

Chapter 4: Sensor

This chapter explains the sensor used for collecting the electromagnetic radiations.

4.1 Measurement of Electromagmnetic Radition

4.1.1 Maxwell's Equation

The electromagnetic measurements are based on the Maxwell's Equations. The Maxwell's Equations describes the generation of the Electric and Magnetic Field due to electric charges and the currents conducting in the device. The change in each field is reflected on the other.

$$\nabla \cdot \vec{E} = \frac{\rho}{\varepsilon_0} \tag{4.1}$$

$$\nabla \cdot \vec{B} = 0 \tag{4.2}$$

$$\nabla \times \vec{E} = -\frac{\partial B}{\partial t} \tag{4.3}$$

$$\nabla \times \vec{B} = \mu_0 \vec{J} + \mu_0 \epsilon_0 \frac{\partial E}{\partial t} \tag{4.4}$$

where $\vec{B}$ is the Magnetic Flux Density, $\vec{E}$ is the Electric Field Strength, ϵ_0 is the Electric Permittivity, μ_0 is the Magnetic Permeability, ρ is the Electric Charge Density, $\vec{J}$ is the Electric Current Density, $\nabla\cdot$ is Divergence Operator, which is the three dimensional scalar multiplication and $\nabla\times$ is Curl Operator, which is the three dimensional vector multiplication.

From Maxwell's Equation 4.4, it is clear that the Magnetic Flux Density is directly proportional to the variations in the current. The current drawn in the device is related to the data being processed and the operation being performed. So by measuring the magnetic field the secret information can be obtained.

4.1.2 Sources of Electromagnetic Field

The major concern in near field measurements is the predominant field in the particular range and efficiency of the field sensor. The predominant field depends on the physical and electrical characteristics of the device and the relative size of the sensor with respect to the device [23]. According to Elke De Mulder [8], the magnetic field is predominant in the near field. We can tell this from the history of electromagnetic analysis, the magnetic field is mostly measured compared to electric field. In [28], Ring Oscillator PUFs are attacked by the Magnetic Field Probe. The Electromagnetic attacks on FPGAs [41],[17] and Smart Cards [33] are conducted using magnetic field probe. Though the electric field contains information about the operations on the device, it is not considered in electromagnetic analysis because magnetic field yields more information than electric field in the near field.

4.2 Electric Field Probes

The electric field probe shown in Figure 4.1 works based on Maxwell's Equation 4.1. The electric field induces an electric charge on conductors. According to Gauss's Law, the charge induced is given by

$$Q = \oint_S \vec{E}(t).dS \cdot \epsilon_0$$

where, $\vec{E}$ is the Electric Field Strength, Q is the electric charge induced on conductor, S is the surface of the conductor and ϵ_0 is the Electric Permittivity of air.

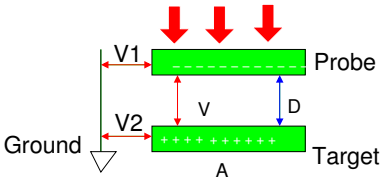


Figure 4.1: Electric Field Probe

In the figure 4.1, the charge Q is induced on the conductor plane of electric field probe. The

potential difference V exists between the electric field probe and Device Under Test (DUT).

$$\nabla \cdot \vec{E} = \frac{\rho}{\varepsilon_0}$$

The derivative of the above equation is

$$V = \frac{Q}{C}$$

where, Q is the local electric charge on the electric field probe, C is capacitance of the capacitor between the conductor plane of the electric field probe and the DUT. The capacitance is given by

$$C = \frac{A\varepsilon_0\varepsilon_r}{D}$$

where A is area of the conductor plane of the probe, D is the distance between the two conductor planes, ε_0 is electric permittivity of air, ε_r is the relative electric permittivity of the core of the capacitor. The voltage V is produced across the capacitor. V_1 is the voltage produced by the electric field probe, which can be measured by connecting it to an oscilloscope or spectrum analyzer. V_2 is the voltage of the DUT conductor plane. V_1 is the voltage of the probe conductor plane, which is measured by the oscilloscope.

$$V = V_1 - V_2$$

The required voltage of the DUT V_2 is given by the equation 4.5.

$$V_2 = V_1 - V \tag{4.5}$$

4.3 Magnetic Field Probes

The functioning of the Magnetic Field Probe is described below in the figure 4.2 below

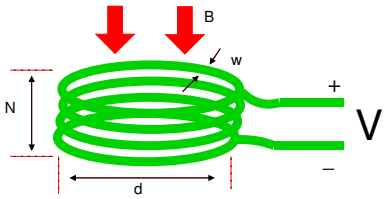


Figure 4.2: Faraday Law

where ω=2πf is the angular frequency, N is the number of turns of probe, A is the Area of the loop, B is the Magnetic Flux Density, $\vec{H}$ is the Magnetic Field Intensity, μ_0 is the Magnetic Permeability of air and cμ_0 is the Relative Magnetic Permeability of medium.

The magnetic probes work based on the Faraday's law

$$V = -\frac{d\phi}{dt} \tag{4.6}$$

where ϕ is the magnetic flux, V is the voltage produced across the loop.

The Faraday's law can be written as

$$V = \omega \cdot N \cdot A \cdot B \tag{4.7}$$

where ω is the angular frequency, N is the number of turns of probe, A is the area of the loop, B is the magnetic flux density.

The magnitude of the voltage depends on various factors. For a target and test environment the angular frequency and the magnetic flux density is constant. The voltage can be increased by increasing the area and the number of turns of the loop. The radius of the loop and number of turns are limited by the conditions given below:

- The total length of the loop should be less than tenth of the higher wavelength of the selected bandwidth.
- The resonant frequency should be greater than ten times the higher frequency of the bandwidth selected.

4.3.1 Types of Magnetic Field Probe and Their Characteristics

The different types of Magnetic Field Probe are

1. Coaxial Cable Probe (Show in figure 4.3)

2. Thin Film Probe(Show in figure 4.4)

3. Handmade Probe (Show in figure 4.5)

Figure 4.3: Coaxial Cable Probe

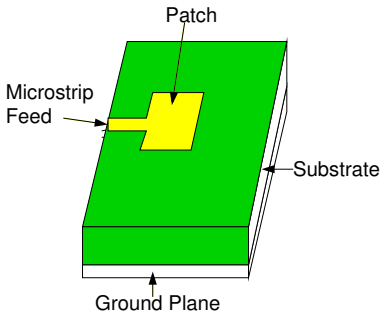


Figure 4.4: Micro Strip Probe

Figure 4.5: Handmade Coil Probe

The required characteristics of magnetic field probe

1. Shielding: Shields the magnetic field probe from the electric field.
2. High Resolution: The probes with smaller dimensions have higher resolution. high resolution probes are required to efficiently measure the radiation for localized electromagnetic analysis without overlapping the measurements.
3. Sensitivity: The sensitivity is the ratio of voltage generated at the probe to the magnetic field strength measured.
4. Cost: The cost and the difficulty in building the Magnetic Probe.

Shielding for a coaxial cable probe and a thin film probe is provided by three conductors, outer conductor, inner conductor and center conductor. In the case of the coaxial cable probe, the skin effect plays a important role in the formation of three conductors. The skin effect makes the current density concentrate near the surface of the conductor. Due to this, the outer layer and the inner layer of the shield are electrically separated. Thus, the outer conductor and the inner conductor of the shield are formed. The skin effect is applicable to conductors with thickness less than the skin depth of the material. For copper, the skin depth is 65.1956μm at 1MHz. So for the thin film probe whose thickness is usually less than 10μm, three conductors cannot be formed. Here three different layers of conductors are physically formed using lithography. The coil probe does not have shielding from the electric field. There is a trade-off between the resolution and the sensitivity of the probe. The sensitivity, as said before, is the ratio of the voltage generated to the magnetic field strength. From the equation 4.7, we see that the voltage is proportional to the area A of the loop. This means,

that the voltage is proportional to the dimensions of the probe. For the higher resolution probes, the higher sensitivity is obtained by increasing the number of turns and changing the core of the probe [44]. The coaxial cable probe and the coil probe can be built at low cost. But the thin film probe is expensive than other probes. The Table 4.1 summarizes the characteristics of the three different magnetic field probe.

Table 4.1: Characteristics of Magnetic Field Probe

Probes	Shielded	Minimum Resolution	Cost
Coaxial Cable Probe	Yes	5mm	cheap
Thin Film Probe	Yes	1μm	expensive
Coil Probe	No	Less than 1mm	cheap

4.4 Shielded Magnetic Field Probes

4.4.1 Balance

The shielded magnetic field probes are built using coaxial cable. The first required characteristic of the magnetic field probe is balance with respect to the measuring device. The concept of balance is explained below. The balanced connection is shown in the figure 4.6.

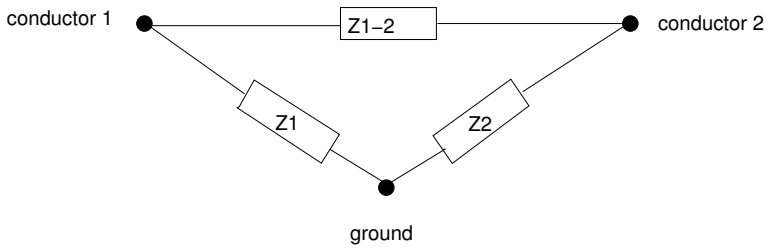


Figure 4.6: Balanced Connection

Z_1 is the impedance of the device, Z_2 and Z_3 are the impedances of the connectors. The electrical component is balanced only when Z_2 and Z_3 have same magnitude and it is unbalanced when they are not equal. The coaxial cable is unbalanced because the outer conductor is connected to ground

and the center conductor is connected to the load. Connecting a balanced probe to an unbalanced cable makes the current flow through the outer conductor, which leads to a loss of information.

4.4.2 Impedance Matching

The characteristic impedance of the coaxial cable is 50Ω. Here coaxial cable is a wave-guide. The probe is the input to the coaxial cable and measuring device is the load of coaxial cable. Impedance matching is required to avoid reflections at input and load [8].

4.4.3 Construction of Coaxial Cable Probes

1. Non-Shielded Probe [Figure 4.7]: The center conductor is wound at one end of the coaxial cable and the other end is connected to the oscilloscope. The sensor is not balanced and its impedance is not 50Ω.

2. Symmetric Shielded Probe [Figure 4.7] : The coaxial cable is bent. The outer conductor and the center conductor are connected at one end to the outer conductor of the cable at other end. The probe has a slit at the outer conductor to not allow the current to flow on outer conductor. This is not balanced.

3. Balanced Shielded Probe [Figure 4.9]: The coaxial cable is bent with the slit at the top of the outer conductor. The probe is balanced by connecting both coaxial cable ends to the measurement device and the potential difference between them is measured.

4. Moebius Shielded Probe [Figure 4.10]: The Moebius Probe is the same as the balanced shielded probe, except for two turns. In the first turn, at Slit the outer conductor of one end is connected to the center conductor of the other end and vice-verse for the second turn.

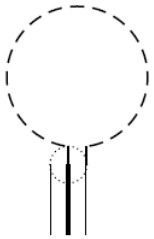


Figure 4.7: Non-Shielded Probe

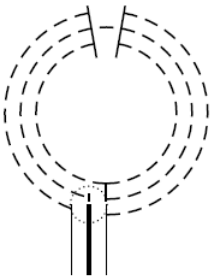


Figure 4.8: Symmetric Shielded Probe

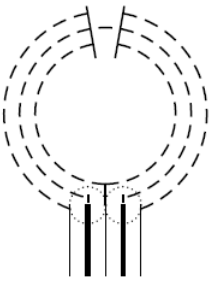


Figure 4.9: Balanced Shielded Probe

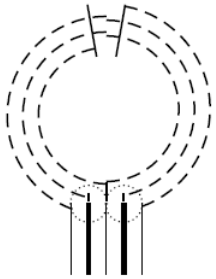


Figure 4.10: Moebius Shielded Probe

4.4.4 Working of Shielded Probe

The outer conductor of the shielded probe acts as an antenna. Due to the magnetic field, a current is induced in the outer conductor. According to Faraday's Law, the voltage difference is generated at the slit. Due to the voltage difference at slit, the current flow in the inner conductor. The current in the outer conductor and the inner conductor are equal and opposite in directions. An electric equilibrium occurs between outer conductor and inner conductor. The electric field induces a charge on the conductor in the vicinity. As the outer conductor cannot accommodate extra charge, the electric field generated by external devices shows no effect on the outer conductor. So, the outer conductor acts as a shield for the electric field. The short circuit current at the other end of the probe is measured. The Probe is connected to the measuring system and the voltage produced is linear to the current in the DUT. The probe works in flux mode shown in figure 4.11.

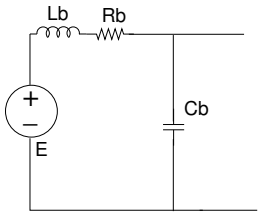


Figure 4.11: Shielded Probe in Flux Mode

4.5 Hand Made Magnetic Probe

The hand made coil is built using copper wire. The copper wire is wound to a loop of a small diameter. One end of the copper wire is connected to the center conductor of the SubMiniature version A (SMA) connector and the other end is connected to the outer conductor of the SMA connector. Based on the radius of the loop and the thickness of wire, the inductance and resistance of the loop are calculated. The voltage generated across the hand made probe is directly given to the measuring device. The hand made probe works in Lenz mode shown in figure 4.12

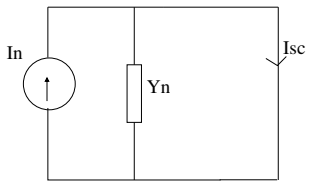


Figure 4.12: Hand Made Probe in Lenz Mode

The hand made coil (figure 4.13) is made with the single conductor. So, it cannot shield from an electric field. Shielding to the electric field is nothing but rejecting the electric field, which is produced by the common-mode current. Rejecting the common-mode current at the output also rejects the electric field captured. The common-mode current can be rejected by a differential amplifier.

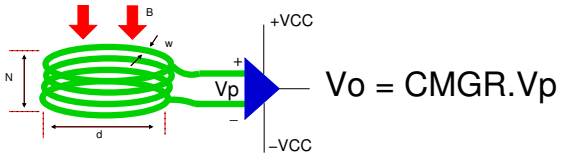


Figure 4.13: Handmade Coil with Differential Amplifier

The differential amplifier PCB shown in figure 4.15 bought from Chipwhisperer[33] is used to reject the common mode current.

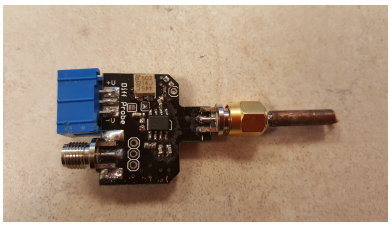


Figure 4.14: The Coil Probe with Differential Amplifier

The diffrential amplifier has a 6-pin socket, to which the supply voltages are given. The other SMA Cable is connected to the oscilloscope or spectrum analyzer. The Amplifier is good at rejecting the noise of the probe. They is distortion after 10MHz.

4.5.1 Amplifier

Differential Amplifier

Using a PCB board of Chipwhisperer's differential probe assembly, the differential amplifier is built in feedback mode. The working of the amplifier is stable for frequency less than 10MHz. The working of the amplifier for different voltage supplies is described in the table 4.2 below.

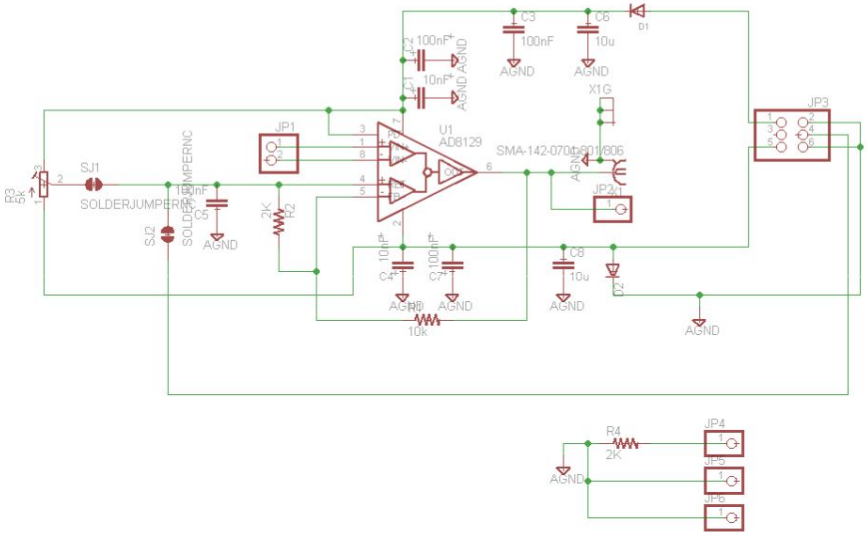


Figure 4.15: Diffrential Probe Schematic from Chipwhisperer

Table 4.2: Ranges

V_s	-V_s	Input Range
1.5V	1.5V	1mV to 10mV
3V	3V	10mV to 1V
10V	10V	0.8V to 1.8V

Low Noise Amplifier

A low noise amplifier is used to amplify the voltage of the probe used to measure the magnetic field. The magentic field mesurements are done at high frequencies. The wideband amplifier BGA2801 is used. The low noise amplifier used is designed by chipwhisperer. The PCB design of the LNA is shown in figure 4.20 The frequency response of the LNA is shown in the figure 4.17

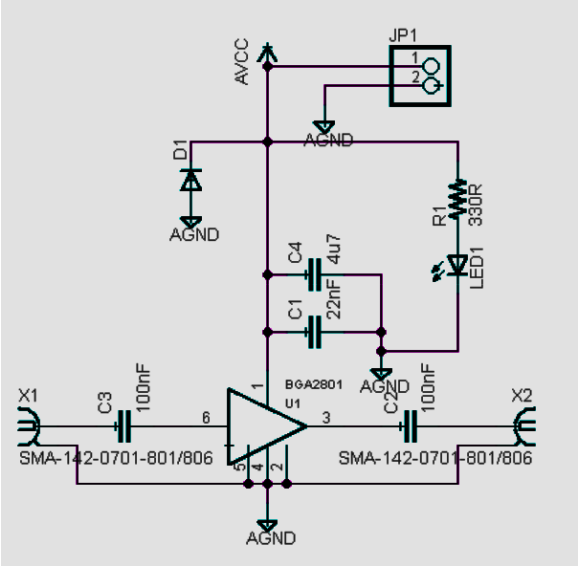


Figure 4.16: PCB of LNA

Figure 4.17: Frequency Response of LNA

4.5.2 Magnetic Shield

The magnetic shield can only redirect the magnetic field. The magnetic field lines travel from north pole to south pole of the magnet. We cannot obstruct the magnetic field lines, but we can redirect them. The field lines should be redirected such that the coaxial cable carrying the current is not affected by the surrounding magnetic field. The magnetic field lines are more attracted towards the materials with high magnetic permeability. The ferro magnetic material is the best option for a magnetic shield. We surrounded the coaxial cable with ferro powder.

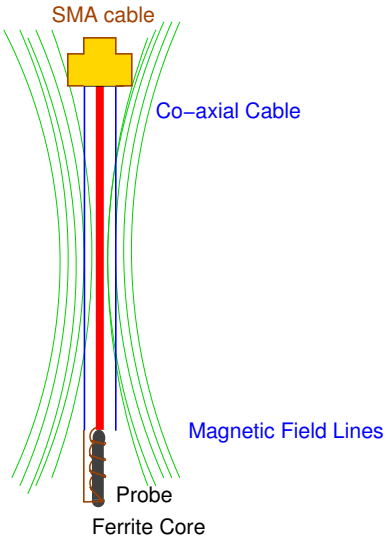


Figure 4.18: Magnetic Field Lines Interrupting the Propogation

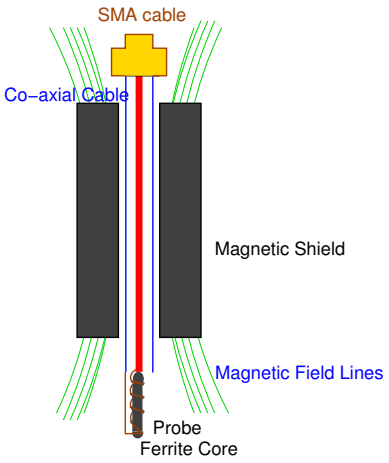


Figure 4.19: Magnetic shield

4.5.3 Probes Used Till Date

The probes used till date in electromagnetic analysis are tabulated in the table 4.3.

Table 4.3: Probes Used Till Date

Paper	**Company**	**Amplifiers**	**Target**
1 [25]	ETS Lindgren 7405 NF EM	Pre amplifier 100 Khz to 3 Ghz	Smart Cards
2 [17]	Langer ICR HH 150-6 (Inductive)	Builtin amplifier with NF 4.5dB, gain 30dB	FPGA Sbox
3 [8]	Handmade (Inductive)	not specified	FPGA ECC Multiplication
4	MT-545 probe	HD24248amplifier	FPGA DES
5	Riscure EM Scan ((Inductive)		FPGA DES
6	HZ -15	Amplified 60dB	FPGA against WDDL
7 [28]	Langer ICR HH 150-6 (Inductive)	30db amplifier	FPGA PUF
8 [12]	HZ -15 loop probe	Amplified 60dB	FPGA AES
9 [10]	500um diameter loop		FPGA DES
10 [16]	100um loop inductive probe	gain 30dB	FPGA ECC
11 [30]	MT-545	Rohde Schwarz FSQ8(Receiver)	RSA
12 [6]	RF 2 and hand made coil probe	not specified	FPGA DES Sbox
13 [29] and [31]	MT-545	MITEQ AM-1594-9907	FPGA Sbox

4.5.4 Characterization of Probes Built

Air Core Probes

The formula for air core probes are given below The voltage generated at the probe is given by

$$|V| = \omega \cdot N \cdot A \cdot B \tag{4.8}$$

The probe is connected to the measurement equipment and voltage across the measurement equipment is given by

$$V = \omega \cdot N \cdot A \cdot B \frac{Z}{j\omega L + R + Z} \tag{4.9}$$

where L is the inductance of the probe, R is the resistance of the probe and Z is impedance of the measuring system.

$$L = N^2 \mu_0 r_l (ln(\frac{8r_l}{r_w}) - 2) \tag{4.10}$$

$$R = \frac{2\pi r_l N}{\sigma\pi(r_w^2 - (r_w - \delta)^2)}, \quad with \delta = \sqrt{\frac{2}{\mu_0 \omega \sigma}} \tag{4.11}$$

where μ_0 is the magnetic permeability of air, r_l is radius of the loop,r_w is radius of the cross section of the wire, δ is skin depth of the material and σ is electric conductivity of the wire.

Ferrite Core Probes

The voltage generated at the probe is proportional to magnetic permeability of the core of the probe. Ferrite material has high magnetic permeability and magnetic reluctance so it can absorb more magnetic energy. The voltage generated at the ferrite core is given by:

$$V = \mu_0 \cdot \mu_r \cdot n \cdot A \cdot \frac{dH}{dt} \tag{4.12}$$

Characterization of Probes

The probes are characterized using network analyzer. The network analyzer is a mode of the spectrum analyzer. In the network analyzer mode, the trace generator signal is generated. The trace generator output is controlled by trace generator attenuation setting. The trace generator signal is given as input to the DUT and the output of the DUT is given to the RF input. The spectrum of the output of the DUT is measured for the specific input given over the frequency domain. The spectrum of the trace generator signal can be measured by connecting the trace generator to the RF input. Later, the trace generator spectrum and the DUT output spectrum can be compared to get the gain of the DUT. The spectra are compared using the "Trace Math" application on the spectrum analyzer.

The characterization of the probes is done using a directional coupler. The trace generator is connected to the input of the directional coupler and the probe is connected at the output. The reflected signal from the directional coupler is given to the spectrum analyzer input. The figures 4.22 shows the reflected signal of the probes.

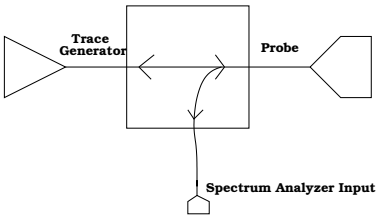
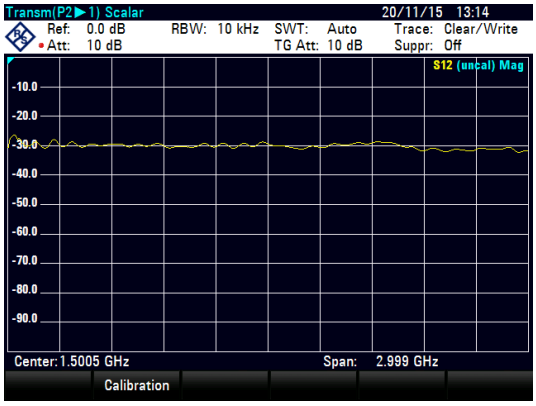
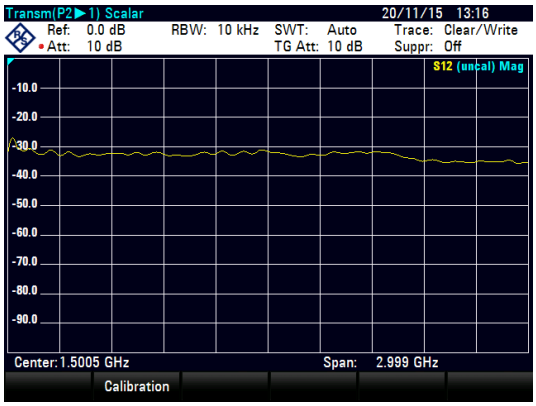


Figure 4.20: Probe connected to the Directional Coupler

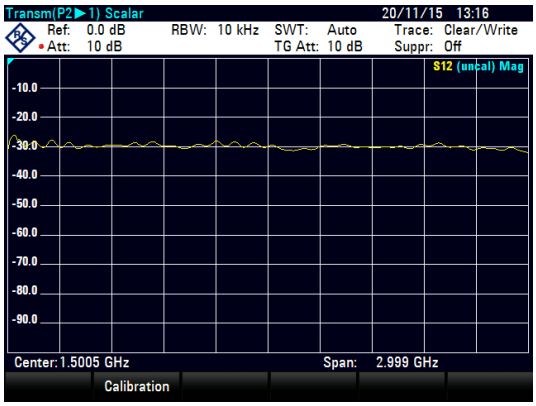


(a) Air core probe with 5 loops



(b) Ferrite core probe with 5 loops

Figure 4.21: Comparison of air and ferrite core probes



(a) Air core probe with 10 loops

(b) Ferrite core probe with 10 loops

Figure 4.22: Comparison of air and ferrite core probes

Chapter 5: Cartography

5.1 Data Acquisition and Control

An oscilloscope and the spectrum analyzer are used for measuring Electromagnetic Radiations. Those measuring devices are equipped with Network Interface Cards(NIC) and can be integrated in the Local Area Network. The devices can be remotely controlled over LAN. The remote control commands include establishing connection between Device and LAN, setting the device's attribute configuration, requesting the transfer of captured data and so on. The LAN connection IP address and device port number are used to establish connection between the device and PC. The data acquisition process for the oscilloscope and the spectrum analyzer is described below. The data acquisition process starts with configuring the attributes. The electromagnetic radiations are measured based on the trigger input and trigger settings given to the system. After measurement, the data is transferred to the PC.

5.1.1 Spectrum Analyzer

The attributes are configured by the remote commands. The frequency span, start frequency, end frequency, sweep time and sweep count are the important attributes, that should be configured before data acquisition. The sweep is the series of consecutive data points measured over time period. The time period is given by the attribute sweep time. The number of points to be measured in a sweep is given by sweep points. The sweep count determines the number of sweeps. The acquisition starts by initializing the sweeps. Once the sweeps are completed, the data can be transferred to the PC. The incoming data is written to a file. The file can be processed later for data analysis. An external gated trigger given to the spectrum analyzer can also be used for measuring the data. The measurements are triggered based on the external trigger, gate delay and the gate length. The spectrum analyzer measures the data only when the gate is active. The gate delay is the delay between the trigger signal and the gate activation. The gate length is the time duration for which the gate is active.

The gate trigger process of a spectrum analyzer is explained by the figure.

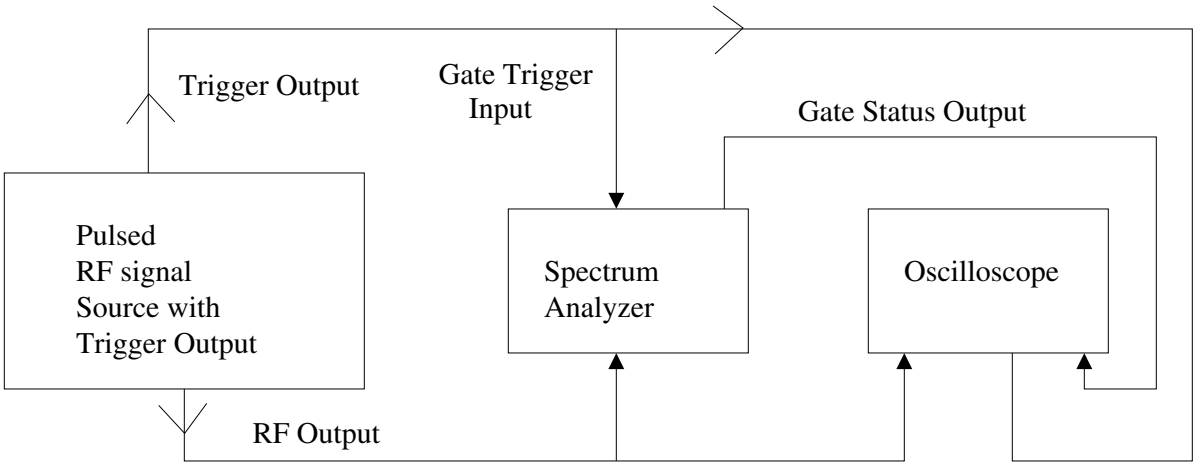


Figure 5.1: Trigerring Spectrum Analyser

5.1.2 Oscilloscope

The attributes of the Oscilloscope that should be configured before the measurement are Y-axis scaling, X-axis scaling, trigger source, trigger edge and number of points to be collected after trigger. The triggering enables the oscilloscope to capture the electromagnetic radiations given as input to the oscilloscope. A preamble is generated by the oscilloscope which describes the features of the data measured. The preamble can be used for plotting the data. The data measured is transferred to the PC. The remote commands for the oscilloscope are elaborated in Appendix.

5.2 Controller

The controller is used for starting the operation on the target system, sending inputs to the target system, collecting the output and sending the trigger signal to the measuring device. The input sent to the target and the output of the target can be used for data analysis.

5.3 Data Analysis

The Data Analysis includes pre-processing and the mathematical relationship calculations between the hypothetical data and the radiations.

Alignment

While preforming DEMA and CEMA, the measurements are collected during a target operation processing different data. The alignment of the data is very much important because the correlation of the trace and the hypothetical is calculated for each discrete time. At a particular discrete time all trace should correspond to the same operation on the target.

Filtering

The unwanted frequency bands are filtered before analysis. The electromagnetic radiations are high frequency signals. The low frequency bands can be filtered before correlation calculation.

Remove Noise

Consider M data samples are processed on the target crypto-system. The m electromagnetic radiations are collected during each M data operations. The mean of the M radiations collected shows the operation dependent part of the signal. For CEMA and DEMA, only the data depended part is considered for correlation calculation. In this case the operation depended part is considered as noise. Therefore, the mean of M radiations is considered as noise. By subtracting the mean from all M radiations, the unwanted signal can be removed.

Resampling

During the acquisition process, the sampling frequency i sgiven as an input. To avoid losses the sampling frequency should be higher than the Nyquist frequency. The Nyquist frequency is two times the maximum frequency of the signal.

Compression

The data acquired from the measurement system is compressed. The data is compressed by calculating mean, maximum peak or minimum peak for each clock cycle. The compressed signal makes

the data analysis faster. The compressed signal gives comparetively less correlation coefficient than the uncompressed signal.

5.3.1 Absolute Value

According to Lenz Law, the sign (direction) of the magnetic field is based on the direction of the current in the closed loop. To exploit data dependency, only the magnitude of current is considered. So the absolute value of the magnetic field is taken.

5.3.2 Pre-Processing

To make cartography efficient, the pre-process should be done. In pre-process, the hot-spots and the frequency bands, where the information depended radiations SNR is high are figured. The enhancement techniques are Magnitude Squared Incoherence and the Maximal Difference. MSI is based on the basics of electromagnetic radiations. The electromagnetic radiations are produced from the flow of charges through wires from the logic gates and also voltage supply in the current. This leads to data dependent emanations from the gates to spread in the complete spectrum. The MSI proposes technique to know about the emanations behavior in the frequency domain. The basic guidance for the approach is while analyzing two cryptographic operations some characteristics of the data dependent emanations are coherent (same) and some are incoherent (change). In Magnitude Squared Incoherence, the spectral incoherence analysis of two time domain signals is done in MSI. The MSI value lies between 0 and 1. If the value is 1 the time domain signals are incoherent and vice-verse The MSI of two time domain signals $w_1(t)$ and $w_2(t)$ is given by

$$MSI_{w1,w2} = \frac{P_{w1,w2}(f)}{P_{w1,w1}(f) \cdot P_{w2,w2}(f)} \tag{5.1}$$

Here $P_{w1,w1}(f)$ and $P_{w2,w2}(f)$ are the power spectral densities of signals $w_1(t)$ and $w_2(t)$. $P_{w1,w2}(f)$ is cross power spectral density of $w_1(t)$ and $w_2(t)$ The data dependent behavior of the EM emissions is disclosed. Let us consider N plaintext are encrypted using the target cryptography system, during the encryption process the time domain EM traces are acquired based on the triggering given by the controller. For each pair of time domain EM trace, the MSI is calculated. We have N(N-1)

incoherence calculated on the frequency domain. Since the emanations are collected over encryption of different data, the incoherence among the radiations shows the data dependency of radiations. The frequency band with high data dependency can be estimated by MSI technique.

5.3.3 Hot Spots

The localized spots on target where the CEMA and DEMA values are high are considered to be hot spots. Using cartography the hot spots can be recognized. The electromagnetic radiations are collected from all points on the target using a scanner. The correlation coefficient for the radiations collected from each point is calculated. The spots with high correlation coefficient are hot spots for electromagnetic analysis. From the previous study the clock net , P/G Network trails, Cryptographic system, on chip capacitors are considered as hot spots. While performing electromagnetic analysis, only the radiations from the hot spots can be considered for data analysis.

5.3.4 Conclusion

The 2D scanner is built, the magnetic field probe are built and charecterised in the frequency domain. By integrating these in to FOBOS, Electromagentic Analysis can be successfully accomplished.

Appendix 6: Appendix

6.1 MSP430-USB

USB_setup(TRUE,TRUE)

This is USB api call. It is used to initialize USB. It connects the api to host.

_enable_interrupt()

The interrupts of the msp430 are enabled.

cdcReceiveDataInBuffer((uint8_t*)pieceOfString, MAX_STR_LENGTH, CDC0_INTFNUM)

The command stores the received data over CDC interface in the buffer. pieceOfString is the buffer, the strlen(pieceOfString) is the length of the buffer and CDC_INTFUM is name of the CDC Interface.

cdcSendDataInBackground((uint8_t*)pieceOfString, strlen(pieceOfString),CDC0_INTFNUM,0);

The command sends user buffer over CDC interface. pieceOfString is the buffer, the strlen(pieceOfString) is the length of the buffer and CDC_INTFUM is name of the CDC Interface.

retInString(wholeString))

The function is true when the buffer has return character.

move_con()

The function makes the motor rotate continuously.

move_step()

The function makes the motor rotate for single step and here the step size is 1.8^o

move_steps(steps_dig1)

The function makes the motor rotate for given number(steps_dig1) of steps.

wrng_command())

When the string sent over the CDC interface is none of the XY-Table command, the function warns the user to send valid command.

TIMER_A_stop(TIMER_A0_BASE)

The function is used to stop the specific timer.

TIMER_A_configureUpMode(TIMER_A0_BASE, TIMER_A_CLOCKSOURCE_ACLK, TIME

The function is used to configure the specific timer. The clock source, clock source frequency divider, the counter value, the interrupt values are given ad inputs.

TIMER_A_startCounter(TIMER_A0_BASE, TIMER_A_UP_MODE);

The fuction is used to start specific timer in specific mode.

6.2 Bipolar Stepper Motor

6.3 Remote Control Commands

Standard Commands for Programmable Instruments(SCPI) are used to control measurement devices. SCPI defines a standard for syntax and commands.

6.3.1 Spectrum Analyzer

"*IDN?"

Queries the instrument identification. <InstrumentName>,<SerialNumber/Model>,<FirmwareVersion> of the Spectrum Analyser are returned.

"*ESE"

Enable staus event register to value given.

"*RST"

Sets the instrument to the default state.

"*CLS"

Clears the status byte, the standard event register to zero. It cleaars the output buffer.

"*ESR?"

Query the status register value ans sets staus register value to zero.

"FREQ:INP:MODE <InputMode>"

"FREQ:CENT <Frequency>"

The centre frequnecy is defined

"FREQ:SPAN <Span>"

The Span can be given manually or can be set to FullSpan

"FREQ:CENT:STEP <StepSize>"

"FORM <Format>" + "

The format of the data to be transferred is given by the <Format>

"INIT:CONT <SweepMode"

SweepMode is ON for continous sweep and OFF for single sweep

"INIT"

Initiates the new measurement sequence.

"*WAI"

Waits unitil the single sweep is completed.

"SENS:SWE:COUN<SweepCount>"

The number of sweeps in a single sweep are given by SweepCount.

"DET <Detector>"

The detector used for transmission of the data collected is given. The detector are MAX, MIN, SAMPLE and RMS

"TRAC:DATA? TRACE1"

This the query for sending the data captured.

"DISP:TRAC:Y <DispalyRange>"

The range of Y axis is given by the <DisplayRange> value.

6.3.2 Oscilloscope

":CHANNELx:IMPEDANCE <value> "

The input impedance value of the channel is given.

":CHANNELx:RANGE <value>"

The range value of the y axis of the channel is determined.

":TIM:RANG <value>"

":TIMEBASE:REFERENCE <value>"

":TRIGger:EDGE:SOURce <edge> "

":TRIGGER:MODE <mode>"

":TRIGGER:SWEEP "

":TRIGGER:EDGE:LEVEL <value>"

":TRIGGER:EDGE:SLOPE <"

":ACQUIRE:TYPE "

It tells whether normal/average/resolution/peak

":ACQUIRE:MODE "

":ACQUIRE:COMPLETE "

6.4 Data Analysis- Python Functions

Nyquist Formula The sampling frequency should be geater than double the maximum frequency of the signal. Coherence Calculation The coherence is calculate dby giving the signals and the sampling rate. FFT Calculation The FFT is calulated by the fourier transform of the signals. FREQ Calculation The frequency of the fourier transform is given by

$$\Delta f = \frac{1}{T\_0} and T\_0 = nT \tag{6.1}$$

where, T_0 is the sampling window time,T is thesampling interval and n is number of samples.

Bibliography

Bibliography

[1] Dakshi Agrawal, Bruce Archambeault, Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Advances in side-channel cryptanalysis electromagnetic analysis and template attacks. *RSA Laboratories Cryptobytes*, 6(1):20–32, 2003.

[2] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The EM side-channel (s). In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 29–45. Springer, 2003.

[3] Agrawal, Dakshi and Rao, Josyula R and Rohatgi, Pankaj. Multi-channel attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2003*, pages 2–16. Springer, 2003.

[4] Isabelle Attali and Thomas Jensen, editors. *Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September 19-21, 2001. Proceedings*, volume 2140. Springer Science & Business Media, 2001.

[5] Caniggia, S and Maradei, F. Equivalent circuit models for the analysis of coaxial cables immunity. In *Proceedings of 2003 IEEE International Symposium on Electromagnetic Compatibility*, volume 2, pages 881–886, 2003.

[6] Chen, Kaiyan and Zhao, Qiang and Zhang, Peng and Deng, Gaoming. The power of electromagnetic analysis on embedded cryptographic ICs. In *Embedded Software and Systems Symposia, 2008. ICESS Symposia 2008. International Conference on*, pages 197–201, 2008.

[7] E. De Mulder, P. Buysschaert, S.B. Örs, P. Delmotte, B. Preneel, G. Vandenbosch, and I. Verbauwhede. Electromagnetic analysis attack on an FPGA implementation of an elliptic curve cryptosystem. In *IEEE International Conference on Computer as a Tool, EUROCON 2005.*, volume 2, pages 1879–1882. IEEE, Nov. 2005.

[8] Elke De Mulder. *Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices.* PhD thesis, Katholike Universiteit Leuven, Nov. 2010.

[9] Dehbaoui, A and Lomne, V and Maurine, P and Torres, L. Magnitude squared incoherence EM analysis for integrated cryptographic module localisation. *Electronics letters*, 2009.

[10] Dehbaoui, Amine and Lomne, Victor and Maurine, Philippe and Torres, Lionel and Robert, Michel. Enhancing electromagnetic attacks using spectral coherence based cartography. In *VLSI-SoC: Technologies for Systems Integration.* Springer, 2011.

[11] Guo-liang Ding, Jie Chu, Wen-fei Yang, and Qiang Zhao. Cryptanalysis for embedded systems based on electromagnetism emission. In *ISAPE 2008. 8th International Symposium on Antennas, Propagation and EM Theory, 2008*, pages 1021–1024. IEEE, 2008.

[12] Enhancement of simple electro-magnetic attacks by pre-characterization in frequency domain and demodulation techniques. Meynard, Olivier and Real, Denis and Flament, Florent and Guilley, Sylvain and Homma, Naofumi and Danger, J-L. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2011*, 2011. mutual information analysis- AES.

[13] Gandolfi, Karine and Mourtel, Christophe and Olivier, Francis. Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems-CHES 2001*, pages 251–261. Springer, 2001.

[14] Hayashi, Yasuhiro and Homma, Noriyasu and Mizuki, Takaaki and Aoki, Toyohiro and Sone, Hidekazu and Sauvage, Laurent and Danger, Jean-Luc. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *Electromagnetic Compatibility, IEEE Transactions on*, 2013.

[15] Hayashi, Yu-ichi and Sugawara, Takeshi and Kayano, Yoshiki and Homma, Naofumi and Mizuki, Takaaki and Satoh, Akashi and Aoki, Takafumi and Minegishi, Shigeki and Sone, Hideaki and Inoue, Hiroshi. Information leakage from cryptographic hardware via common-mode current. In *IEEE International Symposium on Electromagnetic Compatibility (EMC), 2010*, pages 109–114. IEEE, 2010.

[16] Heyszl, Johann and Mangard, Stefan and Heinz, Benedikt and Stumpf, Frederic and Sigl, Georg. Localized electromagnetic analysis of cryptographic implementations. In *Topics in Cryptology–CT-RSA*. Springer, 2012.

[17] Heyszl, Johann and Merli, Dominik and Heinz, Benedikt and De Santis, Fabrizio and Sigl, Georg. *Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis*. Springer, 2013.

[18] Naofumi Homma, Yu-ichi Hayashi, and Takafumi Aoki. Electromagnetic information leakage from cryptographic devices. In *International Symposium on Electromagnetic Compatibility(EMC EUROPE, 2013),Brugge, Belgium*, pages 401–404. IEEE, September 2013.

[19] Masahiro Kinugawa, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Information leakage from the unintentional emissions of an integrated rc oscillator. In *Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 2011 8th Workshop on*, pages 24–28. IEEE, 2011.

[20] Kirschbaum, Mario and Schmidt, Joern-Marc. Learning from electromagnetic emanations-A case study of iMDPL. In *Second International Workshop on Constructive Side-Channel Analysis and Secure Design-COSADE*, pages 50–55, 2011.

[21] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Introduction to differential power analysis and related attacks. *Cryptography Research*, pages 1–5, 1998.

[22] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology - CRYPTO 96*, volume 1109 of *Lecture Notes in Computer Science (LNCS)*, pages 104–113, Berlin, 1996. Springer-Verlag.

[23] Kraz, Vladimir. Near-Field Methods of Locating EMI Sources. In *RF EXPO WEST*, pages 392–397, 1995.

[24] Markus Guenther Kuhn. Compromising emanations: eavesdropping risks of computer displays. Technical report, University of Cambridge, Wolfson College., 15 JJ Thomson Avenue,Cambridge CB3 0FD, United Kingdom., December 2003.

[25] Lakshminarasimhan, Ashwin. Electromagnetic side-channel analysis for hardware and software watermarking. Master's thesis, University of Massachusetts Amherst, 2011.

[26] Guo liang Ding, Jie Chu, Liang Yuan, and Qiang Zhao. Correlation Electromagnetic Analysis for Cryptographic Device. In *Circuits, Communications and Systems, 2009. PACCS09. Pacific-Asia Conference on*, pages 388–391. IEEE, 2009.

[27] Zdenek Martinasek, Vaclav Zeman, and Krisztina Trasy. Simple electromagnetic analysis in cryptography. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, 1(1):269–286, 2012.

[28] Merli, Dominik and Heyszl, Johann and Heinz, Benedikt and Schuster, Dieter and Stumpf, Frederic and Sigl, Georg. Localized electromagnetic analysis of RO PUFs. In *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, 2013.

[29] Meynard, Olivier and Guilley, Sylvain and Danger, Jean-Luc and Hayashi, Yu-Ichi and Homma, Naofumi. Characterization of the Information Leakage of Cryptographic Devices by Using EM Analysis.

[30] Meynard, Olivier and Hayashi, Yu-ichi and Homma, Naofumi and Guilley, Sylvain and Danger, J. Identification of information leakage spots on a cryptographic device with an RSA processor. In *Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on*, pages 773–778, 2011.

[31] Meynard, Olivier and Rëal, Denis and Guilley, Sylvain and Flament, Florent and Danger, Jean-Luc and Valette, Frëdëric. Characterization of the electromagnetic side channel in frequency domain. In *Information Security and Cryptology*, pages 471–486, 2011.

[32] Great Britain. Army. Royal Corps of Signals. Egypt Mobile Divisional Signals and R.F.H. NALDER. *The Royal Corps of Signals. A History of Its Antecedents and Development, Circa 1800-1955. By ... R.F.H. Nalder, Etc. [With Maps.].* London, 1958.

[33] Oswald, David. *Implementation attacks: from theory to practice.* PhD thesis, Ruhr-Universität Bochum, 2013.

[34] Peeters, Eric and Standaert, François-Xavier and Quisquater, Jean-Jacques. Power and electromagnetic analysis: Improved model, consequences and comparisons. *Integration, the VLSI journal*, 2007.

[35] Perin, Guilherme and Torres, Lionel and Benoit, Pascal and Maurine, Philippe. Amplitude demodulation-based EM analysis of different RSA implementations. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012*, pages 1167–117. IEEE, 2012.

[36] Plos, Thomas. Susceptibility of UHF RFID tags to electromagnetic analysis. In *Topics in Cryptology–CT-RSA 2008*, pages 288–300. Springer, 2008.

[37] Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In *Smart Card Programming and Security, Proceedings of E-smart*, volume 2140 of *Lecture Notes in Computer Science (LNCS)*, Berlin, 200–210 2001. Springer-Verlag.

[38] Josyula R Rao and Pankaj Rohatgi. Empowering side-channel attacks. *IACR Cryptology ePrint Archive*, 2001:37, 2001.

[39] Denis Real, Frederic Valette, and Mhamed Drissi. Enhancing correlation electromagnetic attack using planar near-field cartography. In *Proceedings of the Conference on Design, Automation and Test in Europe*, 2009.

[40] Laurent Sauvage, Sylvain Guilley, and Yves Mathieu. Electromagnetic radiations of FPGAs: High spatial resolution cartography and attack on a cryptographic module. *ACM Trans. Reconfigurable Technol. Syst.*, 2(1):1–24, Mar 2009.

[41] Sauvage, Laurent and Guilley, Sylvain and Danger, Jean-Luc and Mathieu, Yves and Nassar, Maxime. Successful attack on an FPGA-based WDDL DES cryptoprocessor without place and route constraints. In *Proceedings of the Conference on Design, Automation and Test in Europe*, 2009.

[42] Hiroto Sekiguchi and Shinji Seto. Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment. In *IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 942–945. IEEE, 2011.

[43] Standaert, François-Xavier and Archambeau, Cedric. Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. In *Cryptographic Hardware and Embedded Systems–CHES 2008*. Springer, 2008.

[44] Tumanski, Slawomir. Induction coil sensors - A review. *Measurement Science and Technology*, 18(3), 2007.

[45] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

Curriculum Vitae

Sangamitrareddy Katamreddy was born on August 12th, 1992 in Tirupathi,India.She received her Bachelor of Technology degree from Vellore Institute of Technology, Tamilnadu, India in 2013. She started working towards her master's degree in George Mason University from August, 2013. She was involved in teaching various undergraduate courses at George Mason University as a graduate teaching assistant. She is a reasearch student at Cryptographic Engineering Research Group (CERG) with interest in Side Channel Analysis,Electromagnetic Analysis.