**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY**

# NEW APPROACHES ON THE ENHANCEMENT OF SIDE CHANNEL ATTACK MEASUREMENTS AGAINST CRYPTOGRAPHIC DEVICES

**M.Sc. THESIS**

**Ahmet Emin BEKMEZCİ**

**Department of Electronics and Communication Engineering**

**Electronics Engineering Programme**

**MAY 2014**

**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY**

# NEW APPROACHES ON THE ENHANCEMENT OF SIDE CHANNEL ATTACK MEASUREMENTS AGAINST CRYPTOGRAPHIC DEVICES

**M.Sc. THESIS**

**Ahmet Emin BEKMEZCİ**
**(504121353)**

**Department of Electronics and Communication Engineering**

**Electronics Engineering Programme**

**Thesis Advisor: Prof. Dr. Serdar ÖZOĞUZ**

**MAY 2014**

**İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ**

# KRİPTO AYGITLARINA KARŞI YAPILAN YAN KANAL ATAK ÖLÇÜMLERİNİN İYİLEŞTİRİLMESİ ÜZERİNE YENİ YAKLAŞIMLAR

**YÜKSEK LİSANS TEZİ**

**Ahmet Emin BEKMEZCİ**
**(504121353)**

**Elektronik ve Haberleşme Mühendisliği Anabilim Dalı**

**Elektronik Mühendisliği Programı**

**Tez Danışmanı: Prof. Dr. Serdar ÖZOĞUZ**

**MAYIS 2014**

**Ahmet Emin BEKMEZCİ**, a M.Sc. student of ITU Graduate School of Science Engineering and Technology 504121353 successfully defended the thesis entitled **"NEW APPROACHES ON THE ENHANCEMENT OF SIDE CHANNEL ATTACK MEASUREMENTS AGAINST CRYPTOGRAPHIC DEVICES"**, which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

| | | |
|---|---|---|
| **Thesis Advisor :** | **Prof. Dr. Serdar ÖZOĞUZ**<br>Istanbul Technical University | ..... |
| **Jury Members :** | **Asst. Prof. Dr. Sıddıka Berna Örs YALÇIN**<br>Istanbul Technical University | ..... |
| | **Asst. Prof. Hakan GÜRKAN**<br>Işık University | ..... |

**Date of Submission :** **5 May 2014**
**Date of Defense :** **30 May 2014**

***To my dear mother,***

## FOREWORD

First and foremost, I would like to thank my supervisor, Prof. Serdar Özoğuz and Asst. Prof. Berna Örs Yalçın for their valuable support and guidance.
I would also like to express my sincerest thanks to TUBITAK(The Scientific and Technological Research Council of Turkey) for providing financial support during my M.Sc. studies.
Finally, I would like to express my gratefulness to my dear mother for her unconditional support.

May 2014

Ahmet Emin BEKMEZCİ
(Electrical and Electronics Engineer)

**TABLE OF CONTENTS**

**Page**

## ABBREVIATIONS

| | |
|---|---|
| **AES** | **:** Advanced Encryption Standard |
| **CCII** | **:** Second Generation Current Conveyor |
| **CMOS** | **:** Complementary Metal Oxide Semiconductor |
| **DPA** | **:** Differential Power Analysis |
| **EM** | **:** Electromagnetic |
| **FPGA** | **:** Field Programmable Gate Array |
| **HF** | **:** High Frequency |
| **RMC** | **:** Resistive Measurement Circuit |
| **RSA** | **:** Rivest-Shamir-Adleman |
| **SCM** | **:** Supply Current Measuring Circuit |
| **SNR** | **:** Signal to Noise Ratio |
| **SPA** | **:** Simple Power Analysis |

**LIST OF TABLES**

**Page**

**LIST OF FIGURES**

**Page**

## NEW APPROACHES ON THE ENHANCEMENT OF SIDE CHANNEL ATTACK MEASUREMENTS AGAINST CRYPTOGRAPHIC DEVICES

### SUMMARY

Cryptographic devices play an important role in modern security systems. They are used to provide secrecy of information. Until recently, the strength of the algorithm was thought to be the main factor to provide information security. In 1998, Kocher stated that the power consumption of cryptographic devices differs according to operation it conducts and by using SPA and DPA attack methods the secret key can be revealed. After this study of Kocher, the confidence for cryptographic devices demolished and it was realised that implementation should be considered as a part of algorithm in cryptographic device design. After this point, in order to see the level of the strength of their devices , designers started to perform side channel attacks against the chip they developed. This approach led to new researches on the improvement of side channel attacks. The success of side channel attack is directly related with the quality of the power measurement. Therefore, enhancement of measurement results is very essential in order to reduce the number of measurement needed to obtain successful attack.

Generally, power measurements are obtained by replacing a small valued resistance between the power supply and cryptographic device. The voltage drop across the resistor is proportional to the power consumption of the chip. The measurements performed with a simple resistor connection do not provide accurate results because of the following reasons: Connected resistance behaves as a filter with the parasitic capacitances of the cryptographic device. This filter characteristic limits the bandwidth between cells of the cryptographic device and the oscilloscope. The connected resistor is a low valued component. Therefore, the measured voltage drop across the resistor becomes low and this causes a reduction in the sensitivity of the measurement. In addition, since the voltage drop across the resistor depends on the current drawn from the cryptographic device, the bias voltage of the cryptographic device is not constant. This unstable bias voltage results in a change of the circuit characteristic.The problems mentioned above are observed with the simulations given in Chapter 3. In order to remove these problems, SCM circuit is proposed in 2006. This circuit provides a stable bias voltage to device under attack with a feedback loop. Therefore, it provides stable circuit characteristic during measurements. In addition, by providing a wide bandwidth between the cells of the cryptographic device and oscilloscope, it ensures accurate tracking of power traces. Also, since the transimpedance of the SCM cirucit is high, the peak values of the power traces can be easily distinguished from the mean value. The measured voltage values of SCM circuit is 8.5 times greater than voltage values measured with resistor. This means a 10dB improvement in signal to noise ratio which corresponds to an improvement in measurement sensitivity.

As an alternative to SCM circuit, second generation current conveyor based SCM circuit(CCII+ based SCM) is introduced in this thesis. According to simulation results, SCM and CCII+ based SCM shows similar performance. Less active elements are used in CCII+ based SCM. Unlike standard SCM, inductor is grounded in CCII+ based SCM. Therefore, it can be replaced by an active only grounded inductance simulator. According to these assessments, it has been seen that CCII+ based SCM is more convenient than standard SCM for CMOS applications. In addition, according to power measurement simulations, measurements conducted by SCM and CCI+ based SCM provide more quality measurement results compared with measurements conducted by resistor. Therefore, the number of power traces namely, the effort to obtain a successful power analysis attack is expected to be decreased by using SCM and CCII+ based SCM as power measurement circuits.

# KRİPTO AYGITLARINA KARŞI YAPILAN YAN KANAL ATAK ÖLÇÜMLERİNİN İYİLEŞTİRİLMESİ ÜZERİNE YENİ YAKLAŞIMLAR

## ÖZET

Kripto aygıtlarında bilgi güvenliğinin sağlanması günümüz emniyet sistemleri için çok önemlidir. Yakın bir zamana kadar, kripto aygıtlarında bilgi güvenliğinin sağlanması için esas faktörün kullanılan algoritmanın kuvveti olduğu düşünülüyor ve araştırmalarda algoritmaların matematiksel olarak nasıl geliştirilebileceği üzerinde duruluyordu. 1998 yılında Kocher, kripto aygıtlarının çektiği gücün farklı işlemler için farklı değerler gösterdiğini ve bunları gözleyip SPA ve DPA atak yöntemlerini kullanarak gizli anahtarın ele geçirilebileceğini gösterdi. SPA atakları daha az mesaj bulunan basit algoritmalar için kullanılırken DPA algoritmaları daha komplike algoritmlar için kullanılıyor. DPA atakları için gereken güç ölçüm sayısı fazla olduğu için bu atakları gerçekleştirmek için güçlü bilgisayarlara ihtiyaç duyuluyor ve DPA atakları oldukça doğru sonuçlar veriyor.

Kocher'in çalışmasından sonra kripto aygıtlarına duyulan güven büyük ölçüde sarsıldı ve kripto cihazlarının güvenliğinin sağlanması için dizayn aşamasında dizaynın gerçeklenmesiyle algoritmanın birlikte düşünülmesi gerektiği ortaya çıktı. Bu andan sonra tasarımcılar aygıtlarının ne kadar güvenilir olduğunu anlamak için tasarladıkları çiplere yan kanal atakları uygulamaya başladılar. Bu uygulamalar yan kanal ataklarının nasıl geliştirilebileceği hususunda çalışmalara yol açtı.

Yan kanal ataklarının başarısı yapılan güç ölçümünün kalitesiyle doğrudan bağlantılıdır. Dolayısıyla ölçüm sonuçlarının iyileştirilmesi atağı başarıya ulaştırmak için gereken ölçüm sayısını azalttığı için çok önemlidir. Güç ölçüm sonuçlarını etkileyen temel kalite kriterleri elektronik gürültü ve anahtarlama gürültüsüdür. Elektronik gürültünün ana unsurları güç kaynağı gürültüsü, saat üretecinin gürültüsü, devre kartı ve arayüz kartı arasındaki etkileşimden kaynaklanan gürültü, manyetik emisyonlar ve kuantizasyon gürültüsüdür. Elektronik gürültü kaynakları her devrede vardır ve bunları bütünüyle elimine etmek mümkün değildir. Anahtarlama gürültüsü ise kripto aygıt hücrelerinin çıkış değerlerinin GHz mertebesinde değişmesi sonucunda çıkmaktadır. Anahtarlama gürültüsü bu makalede anlatılan güç ölçüm devreleri yardımıyla elimine edilebilir.

Güç ölçümleri genel olarak düşük değerli bir direncin kripto aygıtını besleyen güç kaynağıyla kripto aygıtı arasına bağlanarak direncin üzerinde meydana gelen voltaj düşüşünün ölçülmesiyle elde ediliyor. Bu ölçüm şu nedenlerle sağlıklı bir sonuç vermiyor: Bağlanan direnç kripto aygıtının parazitik kapasitansıyla bir filtre gibi davranarak ölçüm cihazıyla kripto cihazındaki hücreler arasındaki band genişliğini limitliyor. Bağlanan direnç değeri düşük olduğu için bu ölçülebilir voltaj değerinin düşük olmasına ve ölçüm duyarlılığının düşmesine neden oluyor. Ayrıca direnç üzerine düşen voltaj değeri kripto aygıtı tarafından çekilen akıma bağlı olduğu için kripto aygıtının besleme gerilimi sabit olmuyor. Bu da kripto aygıtının dengesiz bir gerilimle beslenerek aygıt davranışının değişmesine yol açıyor. Direnç ile yapılan ölçümlerde ortaya çıkan bu aksaklıklar tezin üçüncü bölümünde verilen benzetimlerde

gözlenmiştir. Bu aksaklıkların ortadan kaldırılabilmesi için 2006 senesinde SCM devresi önerilmiş. Bu devre atak yapılan kripto aygıtına geri besleme ile sabit bir besleme voltajı sağlayarak ölçüm yapılırken cihaz karakteristiğinin değişmemesini sağlıyor. Ayrıca ölçüm cihazıyla kripto aygıtındaki hücreler arasında yüksek bir band genişliği ve kazanç sağlayarak ölçümün yüksek doğrulukla takip edilebilmesini ve ölçümdeki tepe değerlerinin ortalama değerden belirgin şekilde ayrılmasını sağlıyor. Ölçülen voltaj değerinin dirençle yapılan ölçümlere kıyasla 8.5 kat fazla olması sebebiyle ölçüm duyarlılığı artıyor ve sinyal gürültü oranında 10dB iyileşme gözleniyor.

Bu makalede klasik yöntem olan direnç üzerinden yapılan ölçümler, SCM devresi kullanılarak yapılan ölçümler ve SCM devresine alternatif olarak sunulan ikinci nesil akım taşıyıcı tabanlı SCM ile yapılan ölçümler devre karakteristikleri, kutuplama voltaj stabiliteleri ve güç ölçüm performansları bakımından incelenmiş ve değerlendirilmiştir. Bilgisayar ortamında yapılan değerlendirmeleri ve benzetimleri daha gerçekçi kılmak adına bahsi geçen güç ölçüm devrelerinin giriş dataları için labaratuvar ortamından akım ölçüm ucuyla alınan güç ölçümleri referans olarak kullanılmıştır. Ayrıca yapılan literatür araştırmaları neticesinde kriptografik FPGA eşdeğer modelinin 50nF'lık bir kapasitör ile 1.3nH'lik bir indüktörden oluştuğu gözlenmiştir. Yine gerçeğe yakın sonuçlar elde etmek için bu eşdeğer kriptografik FPGA modeli bütün benzetimlerde kullanılmıştır.

SCM devresinin alternatifi olarak ikinci nesil akım taşıyıcı(CCII+) tabanlı SCM devresi bu tezde sunulmuştur. Benzetim sonuçlarına göre CCII+ tabanlı SCM devresi, kutuplama voltajı dışında ölçüm duyarlılığı, kazanç ve band genişliği yönünden standart SCM devresi ile benzer performans gösteriyor. CCII+ tabanlı SCM devresinde standart SCM devresine göre daha az aktif eleman kullanılmıştır. Standart SCM'in aksine devre içersindeki indüktör topraklanmış olduğu için bu komponentin yerine sadece aktif elemanlarla oluşturulmuş bir indütör benzetimi kullanılabilir. Bu değerlendirmelere göre önerilen CCII+ tabanlı SCM devresinin standart SCM'e göre CMOS uygulamaları için daha uygun olduğu görülmüştür. Ayrıca yapılan benzetim sonuçlarına göre güç ölçümlerinde standart SCM ve CCII+ tabanlı SCM'in kullanılmasıyla direnç ile yapılan ölçümlere göre ölçüm kalitesinin arttığı sonucuna varılmıştır. Bu sonuca göre güç ölçümlerinde standart SCM ve CCII+ tabanlı SCM kullanıldığı zaman direnç ile yapılan ölçümlere kıyasla atak için gereken ölçüm sayısının, başka bir deyişle atağı sonuca ulaştırmak için harcanan eforun azalacağı öngörülmektedir.

Bunların dışında SCM devresi kullanılarak bilgisayar ortamında diferansiyel güç analizi benzetimi gerçekleştirilmiştir. Bu benzetim için 10000 data noktalı 8500 mesaj kullanılmıştır. Bu benzetimin sonucu olarak korelasyon değerlerinin güç ölçüm sayısına göre değişimi elde edilmiş ve bitler arasındaki ayrımın 3000. data noktasından sonra başladığı tespit edilmiştir.

Sonuç olarak yan kanal atakları için yapılan ölçümlerde SCM devresinin en doğru ve güvenilir sonuçları verdiği görülmüştür. CCII+ tabanlı SCM devresinin standart SCM ile ölçüm duyarlılığı, kazanç ve band genişliği yönünden benzer performans sergilediği ancak kutuplama voltaj stabilitesi yönünden CCII+ tabanlı SCM devresinin zayıf olduğu ve bu dizaynın voltaj stabilitesi yönünden geliştirilmesi gerektiği görülmüştür. Direnç ile yapılan güç ölçümleri ise doğru ve güvenilir sonuçlar vermemektedir çünkü ölçüm duyarlılığı, kutuplama voltaj stabilitesi, ölçüm devresiyle kripto aygıtı arasındaki band genişliği diğer devrelerle yapılan ölçümlere göre oldukça düşüktür. Bu gözlemlere göre güç ölçümlerinde direnç yerine SCM güç ölçüm

devrelerinin kullanılması ölçüm için gereken eforu ve zamanı azaltacaktır.

# 1. INTRODUCTION

Cryptographic devices are used to securely store secret data. They are the main part of security systems [4]. During the encryption process of cryptographic device, an algorithm is executed. Execution of an algorithm leads to manipulation of secret data such as secret keys. Hence, the cryptographic device has to protect this secret data against accessing of third parties by preventing cloning [6].

The main research topic of cryptanalysis was mainly focused on the investigation of the deficiencies and weaknesses in the algorithms. The physical implementation of the cryptographic chip has been out of concern until, in 1998, Kocher [7] showed that the secret data can be revealed from the cryptographic device by using a novel method: side channel attacks. Side channel attacks are based on the information leakage from the cryptographic device.

In cryptographic device, during the execution of an algorithm, physical quantities such as power consumption, electromagnetic emission and execution timing shows different waveforms based on the operation conducted by the cryptographic device. Therefore, by monitoring these physical quantities, the secret information of the cryptographic device can be reached. This leakage can be reduced by high-cost shielding and power consumption filtering methods but it cannot be removed completely because of the features of CMOS design technology. In CMOS technology, electron flow through the silicon substrate of the transistor during charging or discharging of the transistor's gate capacitance, consumes power and produces electromagnetic radiation [7].

Nowadays, power analysis attacks are taken into account during design steps of cryptographic devices in order to improve device resistance against side channel attacks. Power analysis attacks are based on the measurement of the instantaneous power consumption waveforms, which are also called as power traces from the device under attack [6]. Therefore, the quality of the measurement directly affects the effort(number of power traces) needed to obtain a successful attack.

## 1.1 Purpose of Thesis

Analog power measurement circuits are used between the device under attack and the digital oscilloscope in order to improve the measurement quality and decrease the power traces needed to obtain a successful attack.

In this thesis, three different power measurement circuits are explained, examined and compared with each other. These power measurement circuits are resistive measurement circuit(RMC), supply current measuring circuit(SCM) and second generation current conveyor based supply current measuring circuit(CCII+ Based SCM). Second generation current conveyor based supply current measuring circuit(CCII+ Based SCM) is introduced for the first time in literature by this thesis.

## 1.2 Thesis Outline

This thesis presents general information about side channel attacks in cryptographic devices and the description and application of the three analog circuits that are used in power measurement setups. Chapter 1, gives brief information of the thesis with the review of associated literature. Chapter 2 follows introduction chapter. In this chapter, brief description of side channel attacks against cryptographic devices is given with the information of how power analysis attacks are conducted. Chapter 3 deals with power measurement circuits, detailed review of these circuits with power measurement simulation results are presented. Power measuring circuits that are focused in this chapter are given below:

- Resistive measurement circuit (RMC)
- Supply current measuring circuit (SCM)
- Second generation current conveyor based supply current measuring circuit (CCII+ Based SCM)

Conclusion and recommendations are given in Chapter 4. In addition, model parameters used in PSpice simulations are given in Appendices part.

## 1.3 Simulations

All simulations are performed in PSpice software with the actual current drawn form the chip data given as input and simulation results are interpreted in Matlab software. Actual current drawn from the chip data is taken from the measurements of [1]. Bulk terminal is connected to most positive power supply in PMOS transistors and most negative power supply in NMOS transistors. In order to avoid confusion, bulk terminal is not shown in circuit schematics. Model parameters used in PSpice simulations of the CCII+ in Chapter 3 for NMOS is given in the Appendix A.1 and for PMOS is given in the Appendix A.2.

# 2. SIDE CHANNEL ATTACKS AGAINST CRYPTOGRAPHIC DEVICES

## 2.1 Cryptography and Cryptographic Devices

Cryptographic algorithms are widely used to provide secrecy and unity of private data. These algorithms are mathematical functions that takes a message which is usually called plaintext and encrypts it via cryptographic key. The algorithm used is publicly known but the key is kept secret. The most widely used cryptographic algorithms are Advanced Encrypiton Standard(AES) and Rivest-Shamir-Adleman(RSA) algorithms [4].

Cryptographic devices are electronic devices that are capable of implementing Cryptographic algorithms. Smart cards and Radio-Frequency Identification(RFID) cards are some examples of cryptographic devices.

A strong algorithm is not enough to secure the cryptographic key. Implementation of the cryptographic system is also needed to be focused in order to ensure security.

Figure 2.1 shows a typical cryptography process.

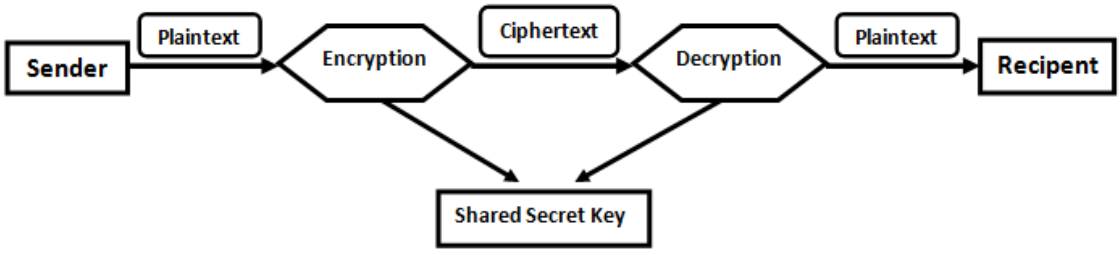



**Figure 2.1**: Typical cryptography process [2].

## 2.2 Attacks on Cryptographic Devices

There are several attacks that try to reveal the cryptographic key. These attacks vary in terms of time, cost and equipment needs. The categorizing is mainly based on whether the attack is passive or active and whether it is invasive, semi-invasive or

non-invasive [4].

In passive attacks the key is obtained by measuring the physical properties of the cryptographic device. Unlike the passive attacks, in active attacks, attacker interferes the device and analyse it accordingly.

In invasive attacks device is de-packed and accessed by direct probing. In semi-invasive attacks the device is again de-packed but this time it is observed without a direct contact. In non-invasive attack, the device is observed by using the external pins of it. Since, the device is not shattered, there is no evidence left behind [4]. Non-invasive attack is the cheapest and easiest way to conduct an attack against cryptographic devices.

Side channel attacks are in the category of passive non-invasive attacks. It includes power analysis attacks [7], timing attacks [8] and electromagnetic attacks [9], [10]. Power analysis attacks are more powerful and easier compared with timing attacks and electromagnetic attacks. Figure 2.2 shows an example of an evaluation board used for side channel attacks.

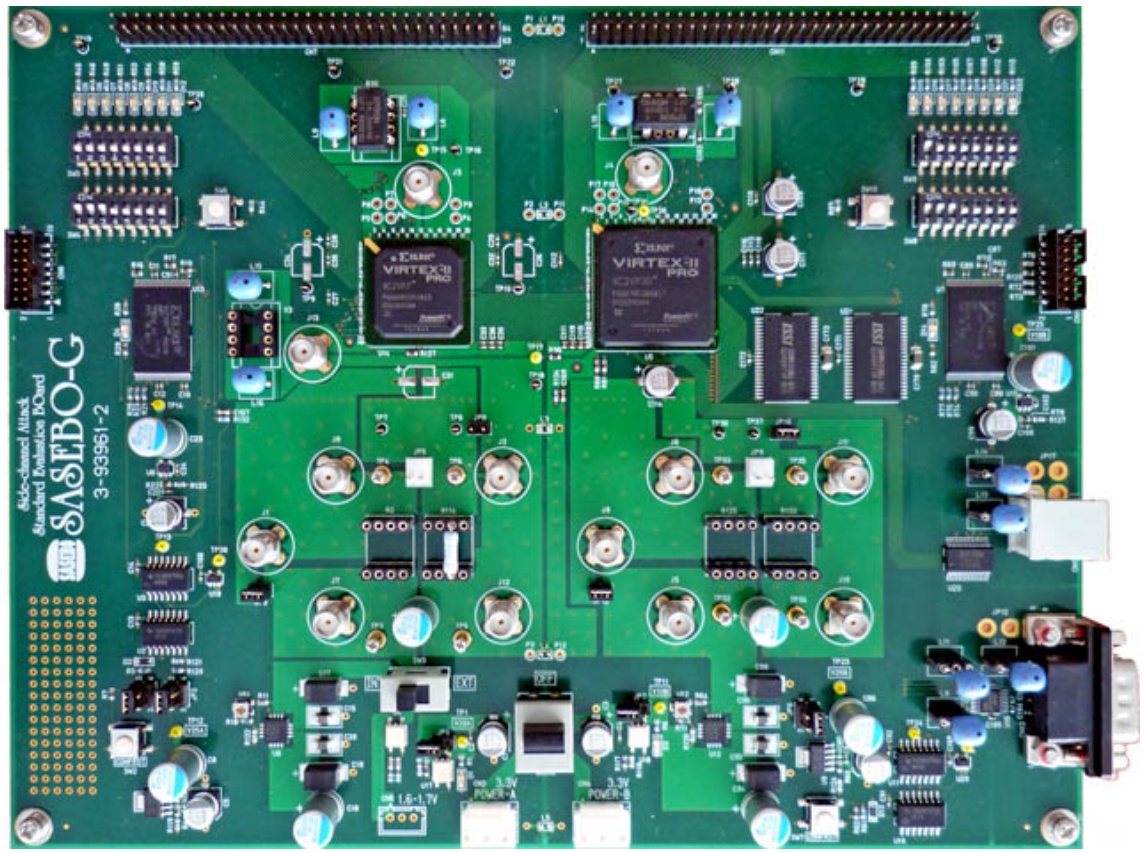



**Figure 2.2**: SASEBO-G side channel attack evaluation board [3].

## 2.3 Power Analysis Attacks

Because of the CMOS design rules, cryptographic device consumes different amount of power during different operations. By observing this power consumption one can reveal the secret key from the cryptographic device. There are two main power analysis attacks. These are simple power analysis(SPA) attacks and differential power analysis(DPA) attacks.

### 2.3.1 Simple power analysis

Simple power analysis(SPA) attack was introduced by Paul Kocher [7].Simple power analysis(SPA) attack is used when there are small number of plaintexts. Therefore, in SPA, attacker deals with only one or few traces [4]. The main disadvantage of this type of attack is that the attacker should have a detailed knowledge about the device under attack.

As an example, Figure 2.3 shows a power trace of a microcontroller while an AES encryption is performed. Power is measured by connecting a 1Ω resistance via the ground connection of the microcontroller. The power trace is uniform except the 10 negative peak points. These 10 negative peak points corresponds to the moments where the AES algorithm is executed. Figure 2.4 shows detailed view of one of these peaks. Since the device consumes different amount of power during different operations, by knowing the used algorithm, the secret key can be found [4].

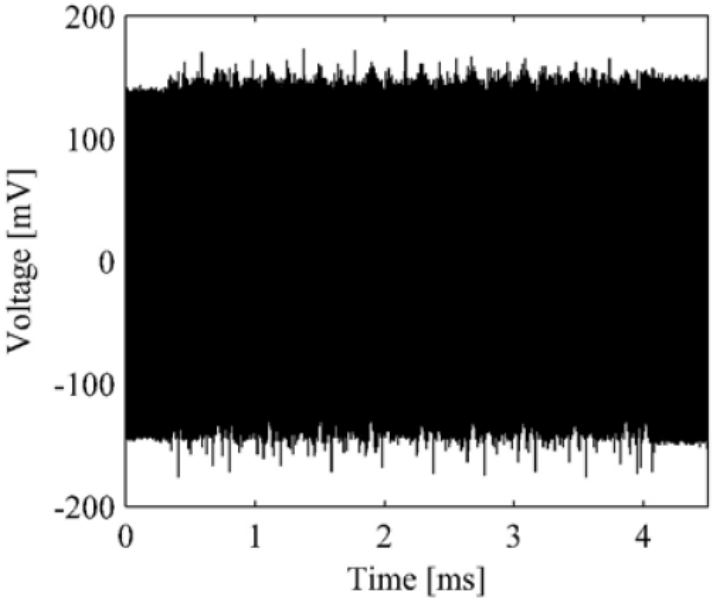



**Figure 2.3**: The power trace of the microcontroller performing AES encryption [4].

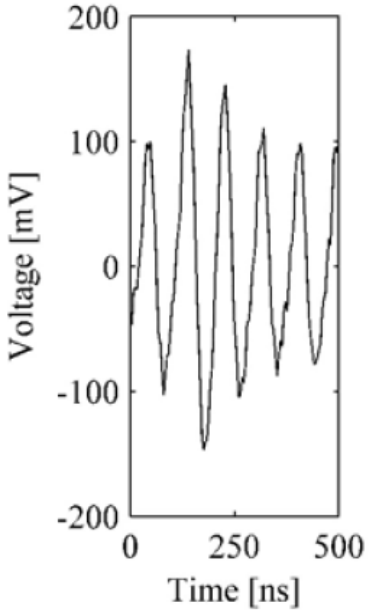



**Figure 2.4**: Detailed view of the power trace [4].

A simple double and add algorithm is given in Table 2.1. It is obvious that during double and add operation cryptographic device will consume more power compared with the double only operation. From the algorithm in Table 2.1, double and add operation corresponds to a key bit 1 and the double only operation corresponds to a key bit 0. The power trace corresponding to this algorithm is given in Figure 2.5. If this power trace is analysed by considering the above fact, it can be easily found that the key is 1001100 [1].

**Table 2.1**: Double and add algorithm [1].

| |
|---|
| 1: $Q \longleftarrow P$ |
| 2: for i from l-2 down to 0 do |
| 3: $Q \longleftarrow 2Q$ |
| 4: if $k_i = 1$ then |
| 5: $Q \longleftarrow Q + P$ |
| 6: end if |
| 7: end for |

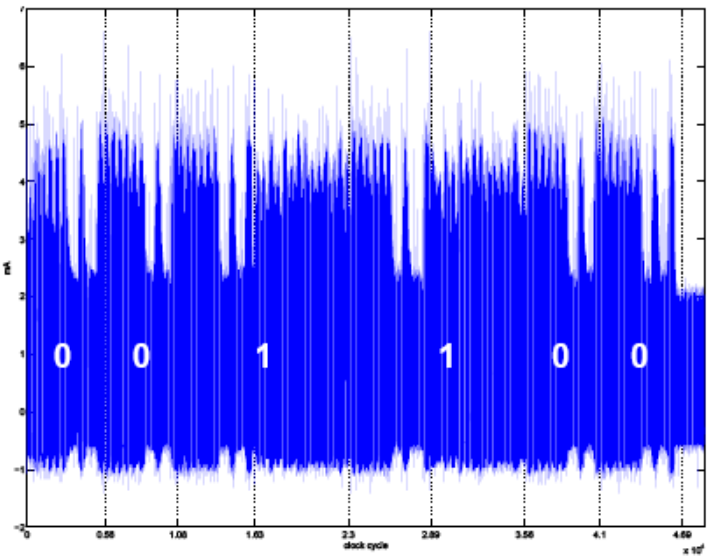



**Figure 2.5**: Detailed view of the power trace [1].

### 2.3.2 Differential power analysis

Differential power analysis(DPA) attack was introduced by Paul Kocher [7]. Differential power analysis(DPA) attack is used when the algorithm is complex and there are many power traces. In DPA attack detailed knowledge of the device is not necessary. This is the main advantage of DPA attack against SPA attack. In addition, DPA attack is analysed at a fixed point, not necessarily at a fixed time [4].

All DPA attacks are based on the following steps illustrated in Figure 2.6 [4]:

1. Choose an intermediate result of the executed algorithm that is a function of plaintext and key.

2. $d$=($d_1$,.....,$d_D$)' where $d_i$ corresponds to the data value of the $i^{th}$ encryption. Encryption of each data block results in a power trace. Measure the power consumption of the cryptographic device during encryption of D different data blocks. With these power traces a $DxT$ size matrix can be formed where T denotes the length of the power trace.

3. $k$=($k_1$,.....,$k_K$)' where $k_i$ denotes the $i^{th}$ key value which is also called as key hypotheses. K is the total number of possible key values. Calculate hypothetical intermediate values matrix V with size $DxK$.

$$V_{i,j} = f(d_i, k_j) \tag{2.1}$$

4. Map the hypothetical intermediate values V to hypothetical power consumption values H by using Hamming-Distance or Hamming-Weight simulation techniques. The quality of the mapping simulation determines the success of the DPA attack.

5. Make a comparison of hypothetical power consumption matrix H and power trace matrix T. The result of this comparison leads to a matrix R with a size $KxT$. The highest value of matrix R indicates the index of the used intermediate result and the key. If the values of R are close to each other such that it is difficult to distinguish the maximum value, it means there are not enough power traces to conduct a relationship between hypothetical power consumption matrix and power trace matrix. More power traces means more H and T columns and more definite result. The elements of R which are also called as correlation coefficients can be found by using the following equation where $\overline{h_i}$ and $\overline{t_j}$ denotes the mean values of $h_i$ and $t_j$:

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i}) * (t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{D}((h_{d,i} - \overline{h_i})^2) * \sum_{d=1}^{D}((t_{d,j} - \overline{t_j})^2)}} \tag{2.2}$$

$(t_{d,j} - \overline{t_j})$ term in Equation 2.2 approaches to zero while $t_{d,j}$ approaches to $\overline{t_j}$. Namely, for a chosen key value if the peak values of the power traces approach to its neighbourhoods then it becomes difficult to distinguish the maximum value of R matrix. Hence, it becomes harder to find a definite result from DPA attack. Therefore, higher peak values in power trace measurements increases the probability of attack success.

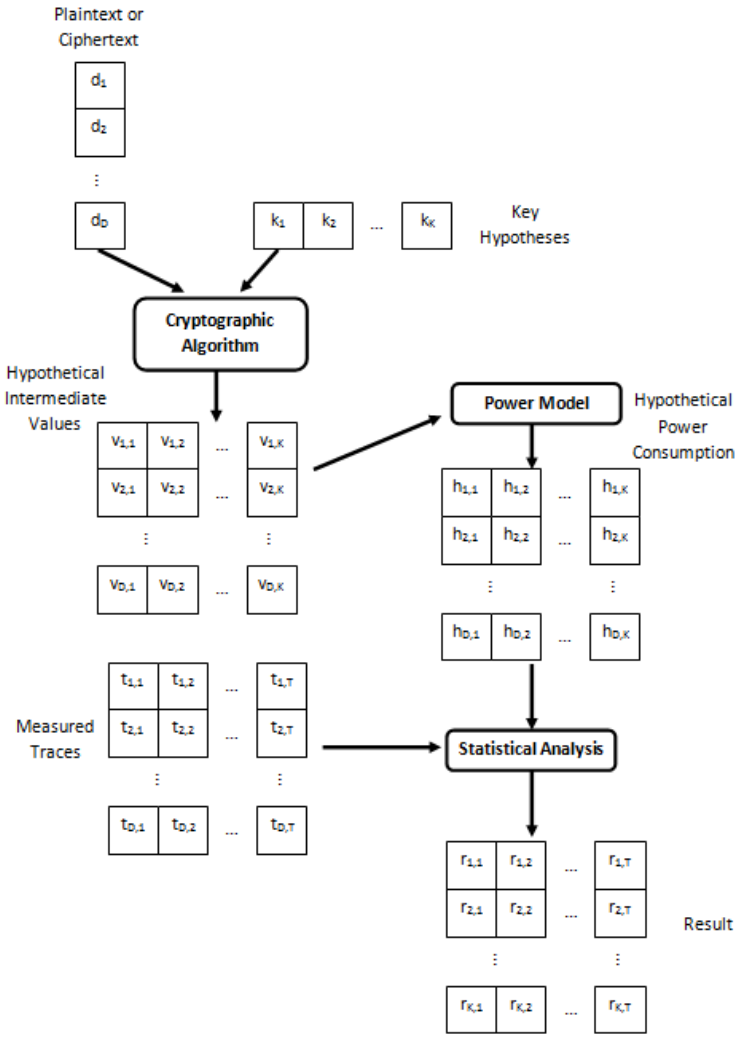



**Figure 2.6**: Block diagram of DPA attack steps [4].

## 2.4 Measurement Setup

Measurement setup of a typical power analysis attack consists of several components. As shown in Figure 2.7, these components are [4]:

- Cryptographic Device
- Clock Generator
- Power Supply
- Power Measurement Circuit or Electromagnetic(EM) Probe
- Digital Sampling Oscilloscope
- Computer

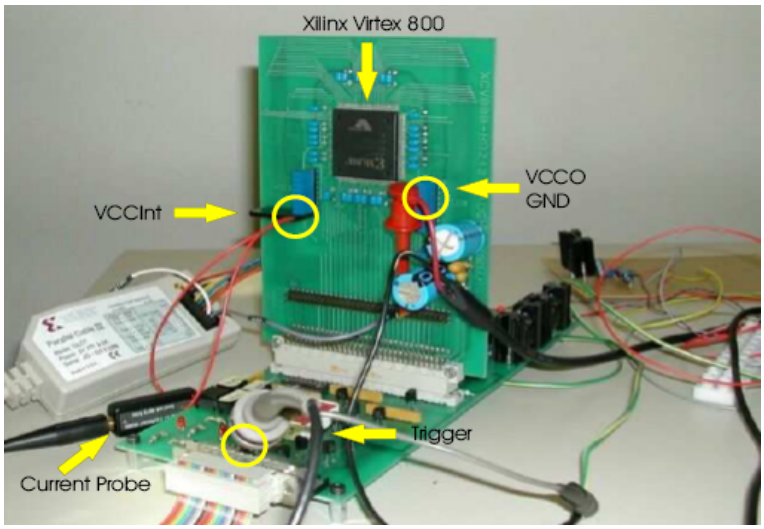



**Figure 2.7**: Typical measurement setup [1].

A block diagram of a typical measurement setup is given in Figure 2.8.

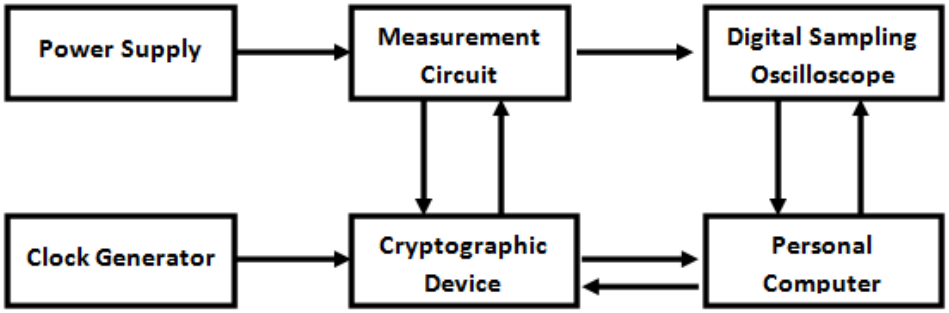



**Figure 2.8**: Block diagram of typical measurement setup [4].

First cryptographic device is powered up with a stable external power supply and supplied with a clock signal. Now device is ready for encryption. Then, computer sets the oscilloscope and sends command to cryptographic device to start encryption. During the encryption power consumption of the cryptographic device is measured by a power measurement circuit or an EM probe and recorded by oscilloscope. Then, output of cryptographic algorithm and recorded power traces are received by the computer. These steps are repeated until necessary number of power traces obtained [4].

## 2.5 Quality Criteria for Measurements

The power consumption of a cryptographic device is an analog high frequency(HF) signal. Therefore, the power consumption of the individual cells are in the range of GHz [4]. Furthermore, there are many factors that effect the quality of the

measurement. These are thermal noise, reflections on wires, crosstalk, filtering and other interferes of the environment [4]. In order to obtain a correct measurement, measurement setup should cope with the these factors. Hence, it is a challenging work to measure the power traces of a cryptographic devices and the success of the power analysis attack is directly related with the measurement precision.

The effects of thermal noise, reflections on wires, crosstalk, filtering and other interferes of the environment can be observed as noise in the measurement of power traces. The noise level in the power traces indicates the quality of the measurement. It is also possible to conduct power trace measurement in a noisy environment. However, noise increases the required number of power traces to obtain a successful attack. There are two important noise components. These are electronic noise and switching noise [4].

### 2.5.1 Electronic noise

Repeated power trace measurements with the same inputs result in different outputs. The reason between this discrepancy is the electronic noise. Electronic noise appears in every measurements and it is not possible to completely remove it [4]. The most important electronic noise sources are given below [4]:

◦ **Power Supply Noise:** Any fluctuation in the power supply of the attacked cryptographic device appears as noise in the power trace measurement. Hence, a very stable power supply is a must.

◦ **Noise of the Clock Generator:** Correct alignment of power traces decreases the effort needed to obtain a successful attack. Also, the noise in the amplitude of the clock signal directly effects the power traces. In order to obtain accurate measurement of power traces, stable clock frequency and stable clock signal amplitude is needed. Therefore it is reasonable to use a sinusoidal clock signal instead of a rectangular one.

◦ **Conducted Emissions:** The measurement board and the interface board should be separated and isolated in order to eliminate the noise caused by conducted emissions.

◦ **Radiated Emissions:** The effect of the noise caused by the radiated emissions can be eliminated by putting the device under attack into a Faraday cage and shielding the communication and measurement lines.

◦ **Quantization Noise:** Analog-to-digital conversion conducted by oscilloscope causes

the quantization noise. Higher conversion resolution results in lower quantization noise. Since there is a trade-off between the resolution and sampling rate of the oscilloscope, it is important to choose a proper resolution. 8-bit resolution is sufficient for power analysis attacks.

### 2.5.2 Switching noise

Cryptographic device cells switch their output at the rate of GHz during the execution of the cryptographic algorithm. This switching operation causes high power consumption. In power analysis attacks, the power consumption of the relevant cell is important. Power consumption of all other components contributes to noise. To eliminate this noise, precisely positioned small EM probes are used to perform measurement. However, in practise it is not an easy job to precisely locate EM probes. Usually instead of this method, the total power consumption is measured by inserting an electronic circuit between the power supply and the attacked device. In this method, two main factors effect the switching noise. These are bandwidth of the connection between oscilloscope and logic cells and clock frequency of the device under attack [4].

### 2.5.3 Bandwidth

As mentioned before the power consumption of the individual cells are in the range of GHz [4]. Therefore, in order to precisely measure the power consumption of the cells, a path with the bandwidth range of GHz is necessary. This is not practical because of the parasitics on the measurement path. For example, power supplies are usually built with a high capacitance between VDD and GND ports in order to provide stable bias. However, this connection compromise a big parasitic in the path of the power consumption signal. Also, the connections established between the power supply and the GND and VDD pins of the cryptographic device via bonding wires add parasitic inductance to the path of the power consumption signal. This parasitic inductance with the on-chip bypass capacitance constitute a filter on the power signal path. The bandwidth of this filter limits the bandwidth of the original power consumption signal [4]. The effects of this undesirable filter can be reduced with the circuits given in Chapter 3 of this thesis but cannot be removed completely. Figure 2.9 shows the

impedance measurement of a cryptographic FPGA [5]. From this figure, it is obvious that the equivalent model of a cryptographic FPGA is composed of a capacitance of 50 nF and an inductance of 1.3 nH.

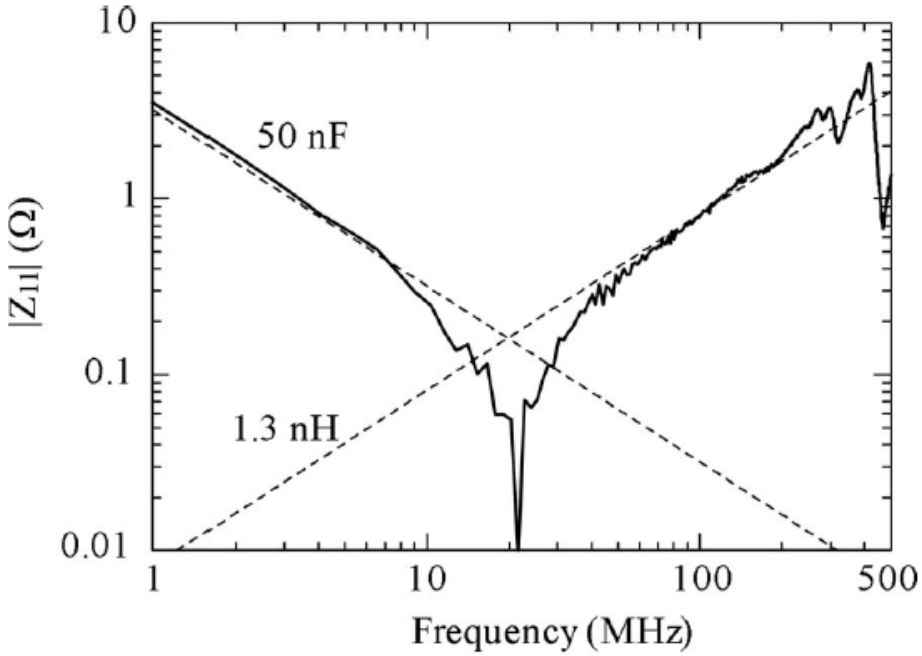



**Figure 2.9**: Impedance measurement of a cryptographic FPGA [5].

### 2.5.4 Clock frequency

Clock frequency is another contributor to switching noise. If very high clock frequency is used for the device under attack, then the measured power signals of consecutive clock cycles may overlap resulting in a wrong measurement. If the cryptographic device specification permits, it is better to attack with low clock frequency in order to reduce switching noise.

# 3. POWER MEASUREMENT CIRCUITS

Power measurement circuits are used to measure the power consumption of a cryptographic device. There are some factors limiting the quality of the measurement that are mentioned previously. However, to conduct a successful attack the power measurement should be precise. Hence, it is very crucial to design and use fast, reliable power measurement circuits.

In this chapter, widely used resistive measurement circuit(RMC) and supply-current measuring circuit(SCM) are explained. In addition to these circuits, a new SCM circuit based on a second generation current conveyor(CCII+) is introduced. Also, a comparison of these circuits is given at the end of this chapter.

Power consumption data of a cryptography chip shown in Figure 3.1 was taken from laboratory environment [1]. As stated in [1] the clock frequency applied to the chip is around 300 kHz and the sampling frequency of the oscilloscope is 250 MHz. This data is used as input to power measurement circuits to conduct a realistic simulation profile. From now on this data will be referred as actual chip current.

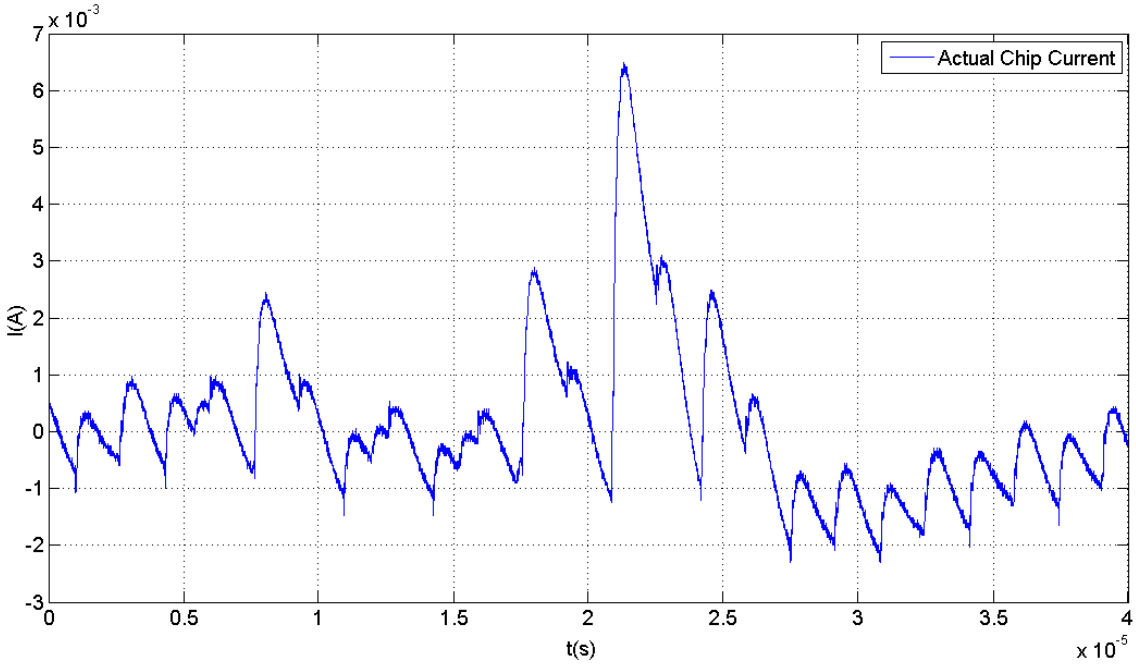



**Figure 3.1**: Actual current drawn from the chip.

### 3.1 Resistive Measurement Circuit

Resistive Measurment Circuit (RMC) consists of a small resistor connected between the VDD or VSS pins of the cryptographic device and the power supply.

#### 3.1.1 Circuit description of RMC

The circuit schematic of RMC is given in Figure 3.2. The voltage drop across the resistor is proportional to power consumption of the chip.

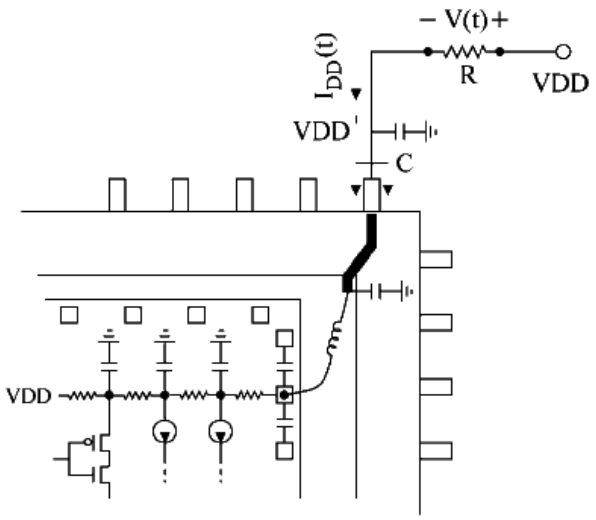



**Figure 3.2**: Resistive measurement circuit(RMC) [6].

This circuit is very easy to implement. However, it is very hard to obtain good quality results because of the following limitations [6]:

1. Because of the parasitic capacitances of the cryptographic device, there occurs a time constant $R.C$. This time constant limits the bandwidth of the power signal. Hence, low values of R should be used in this configuration.

2. R is the amplification factor of the measured current signal. If the value of R chosen low, then the output voltage level will be low. Hence, it will be harder to measure the output voltage level. This means a reduction in the sensitivity of the measurement. Therefore, if low values are chosen for R value to increase the bandwidth, then sensitivity of the measurement would be lower. There is a trade-off between bandwidth and sensitivity of RMC.

3. The resistor R causes a $I(t) * R$ voltage drop. Hence, the bias voltage of the cryptographic chip becomes $VDD' = VDD - I(t) * R$. Since, this expression depends

on the drawn current, it is not stable. This unstable bias voltage affects the behaviour of the cryptographic chip and results in misleading evaluations.

### 3.1.2 Main characteristics of RMC

The resistive measurement simulation circuit based on the equivalent cryptographic FPGA model is given in Figure 3.3. The measurement resistance R is chosen as 50Ω. $C_{fpga}$ is 50nF and $L_{fpga}$ is 1.3nH. 3.3V $V_{DD}$ bias voltage is used for the attacked FPGA.

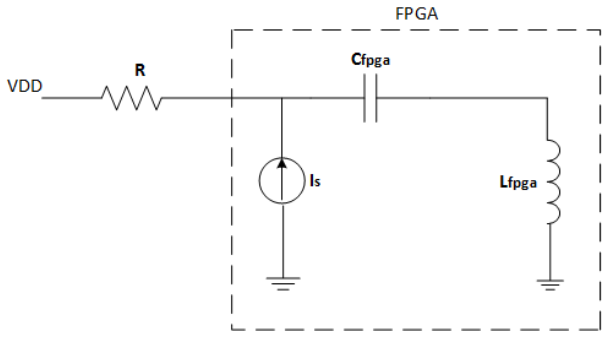



**Figure 3.3**: RMC simulation circuit.

The bias voltage of the FPGA in RMC is shown in the Figure 3.4. It can be seen that the bias voltage is not stable.

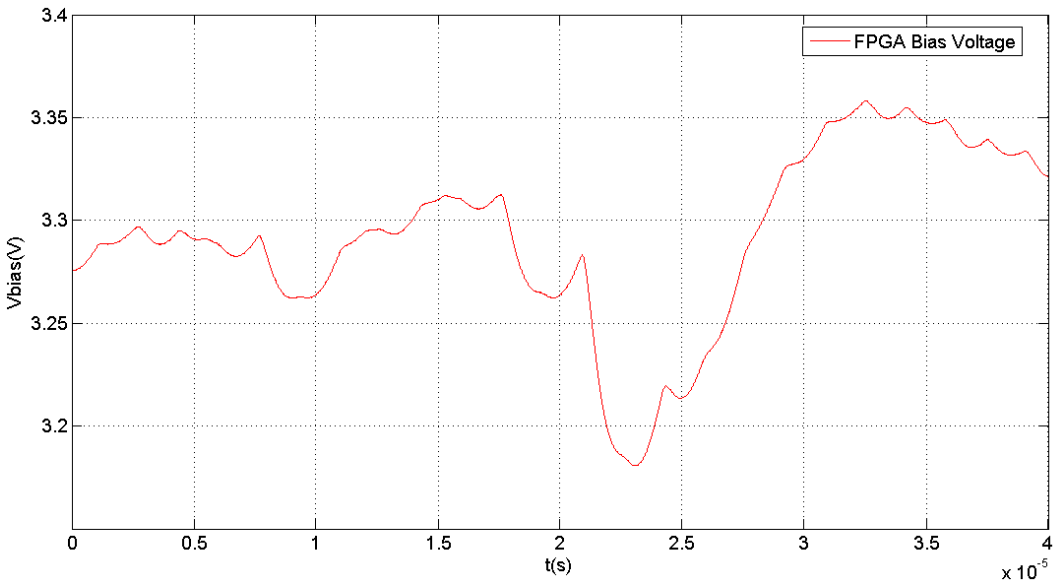



**Figure 3.4**: Bias voltage of the FPGA in RMC.

The frequency dependence of input impedance is shown in Figure 3.5. As expected it shows a series RLC characteristic.

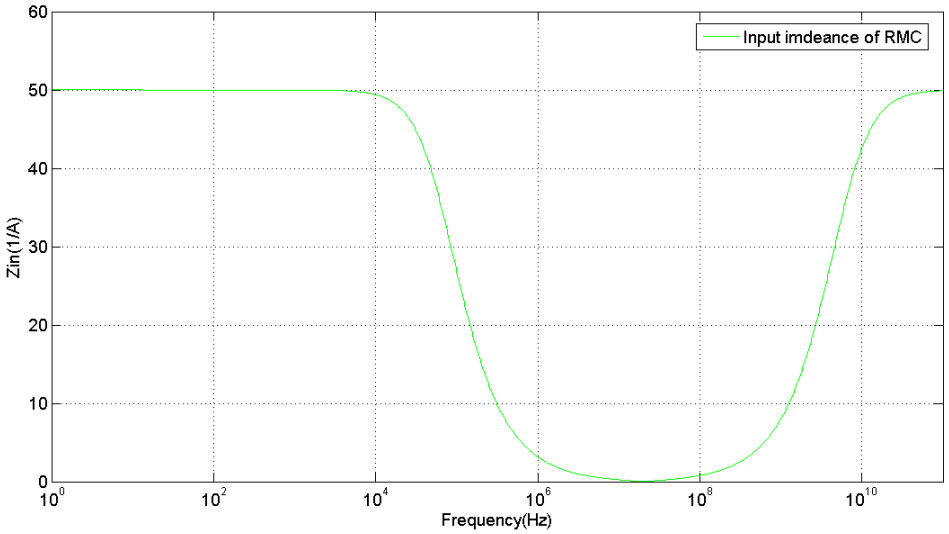



**Figure 3.5**: Input impedance characteristic of RMC.

### 3.1.3 Power measurement simulation of RMC

The power measurement simulation result of RMC is given in Figure 3.6. It can be seen from the figure that the RMC output is not able to follow the actual chip current because of its limited bandwidth. Also, RMC output is attenuated. 0.11V max voltage level shows that the sensitivity is very low.

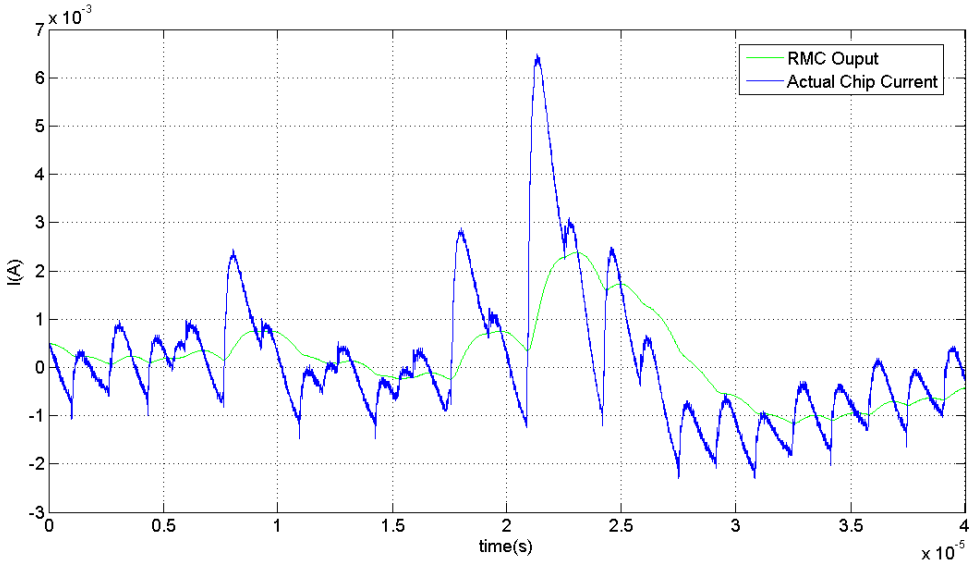



**Figure 3.6**: Power measurement simulation of RMC.

## 3.2 Supply Current Measuring Circuit(SCM)

Supply current measuring circuit(SCM) is introduced by Bucci in 2006 [11]. This circuit is an active circuit that measure the instantaneous current consumption of the device under attack while at the same time supplying the device with a stable bias voltage. By supplying stable bias voltage, power analysis attacks can be conducted with high precision without disturbing the operation of the device under attack. SCM circuit denotes a low impedance current measuring input and high transimpedance gain while providing a stable bias [6]. Therefore, SCM circuit exhibits higher bandwidth, higher sensitivity and more stable bias compared with RMC.

### 3.2.1 Circuit description of SCM

The circuit schematic of SCM is given in Figure 3.7. Current consumption signal $I_{in}(t)$ is read from the device under attack. The reference input $V_{DD}$ is connected to the positive terminal of the input opamp. A stable bias voltage $V_{DD}$ is provided to the device under attack at the negative terminal of the opamp via low-frequency voltage feedback loop closed after a voltage buffer [6].

High slew rate and low noise were the main criteria for the selection of the discrete components [6]. AD8009 has been chosen for opamps. In order to eliminate the oscillation, $10pF$ value has been chosen for the compensation capacitance $C_f$. 500 Ω value has been chosen for $R_f$ to obtain a transimpedance gain of 250 V/A. 100 $\mu$H value has been chosen for inductance L. +5V/-5V bias voltage is used for the SCM and 3.3 V $V_{DD}$ bias voltage is used for the attacked FPGA.

The output voltage of the SCM can be expressed as follows:

$$V_{out}(t) = -\frac{R_f}{2} I_{in}(t) \tag{3.1}$$

Then, the transimpedance gain is,

$$T(s) = \frac{R_f}{2} \tag{3.2}$$

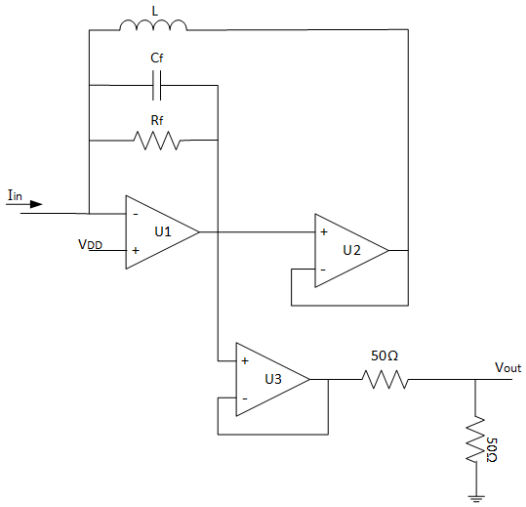



**Figure 3.7**: Supply current measurement circuit.

For $A_v$(voltage gain of the transimpedance amplifier) $\gg 1$, transfer function of SCM can be formulated as follows:

$$\frac{V_{out}}{I_{in}}(s) \simeq -\frac{1}{2}\frac{R_f Ls}{R_f + Ls + R_f C_f Ls^2} \tag{3.3}$$

Assuming poles of the transfer function apart from each other such that $p_1 \gg p_2$, routine transfer function analysis yields the following pole locations:

$$(s+p_1)(s+p_2) = R_f + Ls + R_f C_f Ls^2 \tag{3.4}$$

$$s^2 + s(p_1+p_2) + p_1 p_2 = R_f + Ls + R_f C_f Ls^2 \tag{3.5}$$

$$p_1 = \frac{1}{R_f C_f} \tag{3.6}$$

$$p_2 = \frac{R_f}{L} \tag{3.7}$$

DC analysis of SCM for U1 opamp yields the following equations:

$$A_v(V_{2,+} - V_{2,-}) = V_{2,out} \tag{3.8}$$

$$A_v(V_{1,out} - V_{2,out}) = V_{2,out} \tag{3.9}$$

$$V_{2,out} = \frac{A_v}{A_v + 1} V_{1,out} \tag{3.10}$$

$$V_{2,out} \simeq V_{1,out} \tag{3.11}$$

Using Equation 3.11, DC analysis for U1 opamp yields:

$$A_v(V_{1,+} - V_{1,-}) = V_{1,out} \tag{3.12}$$

$$A_v(V_{1,+} - V_{1,out}) = V_{1,out} \tag{3.13}$$

$$V_{1,+} = \frac{A_v + 1}{A_v} V_{1,out} \tag{3.14}$$

$$V_{1,+} = V_{DD} \simeq V_{1,out} \simeq V_{1,-} \tag{3.15}$$

Equation 3.15 shows that the voltage feedback provides stable bias to device under attack which is connected to negative terminal of U1 opamp.

U2 opamp is used to prevent input current flowing in the reverse direction through the inductor. If direct connection made between $V_{1,out}$ and the inductor, the output of the U1 opamp $V_{1,out}$ would be affected.

Low impedance value at the input of the SCM is essential in order not to load the cryptographic device. As shown in Equation 3.17, theoretical input impedance is very low.

$$Z_{in} = \frac{1}{1 + A_v}(Rf // \frac{1}{sC_f} // sL) \tag{3.16}$$

$$A_v \gg 1, Z_{in} \longrightarrow 0 \tag{3.17}$$

### 3.2.2 Main characteristics of SCM

The supply current measuring circuit based on the equivalent cryptographic FPGA model is given in Figure 3.8.

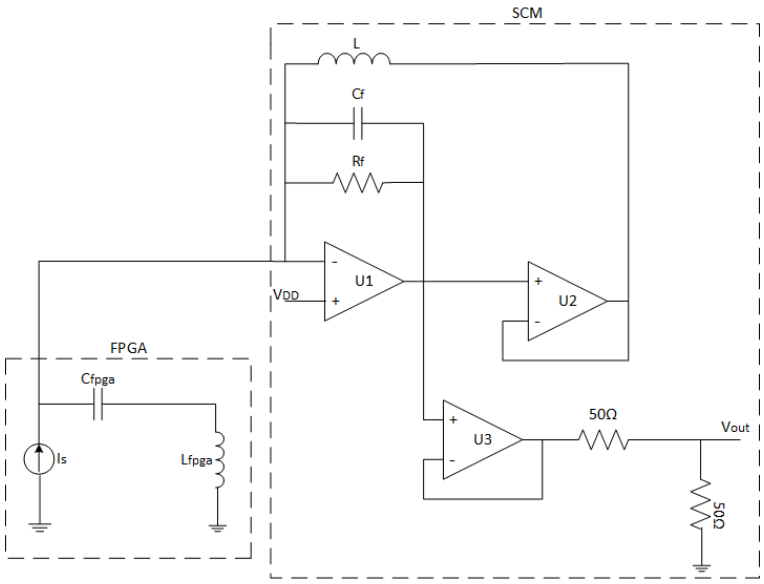



**Figure 3.8**: SCM simulation circuit.

The bias voltage of the attacked FPGA in SCM is shown in the Figure 3.9. It can be seen that attacked FPGA is biased with a stable 3.3V.

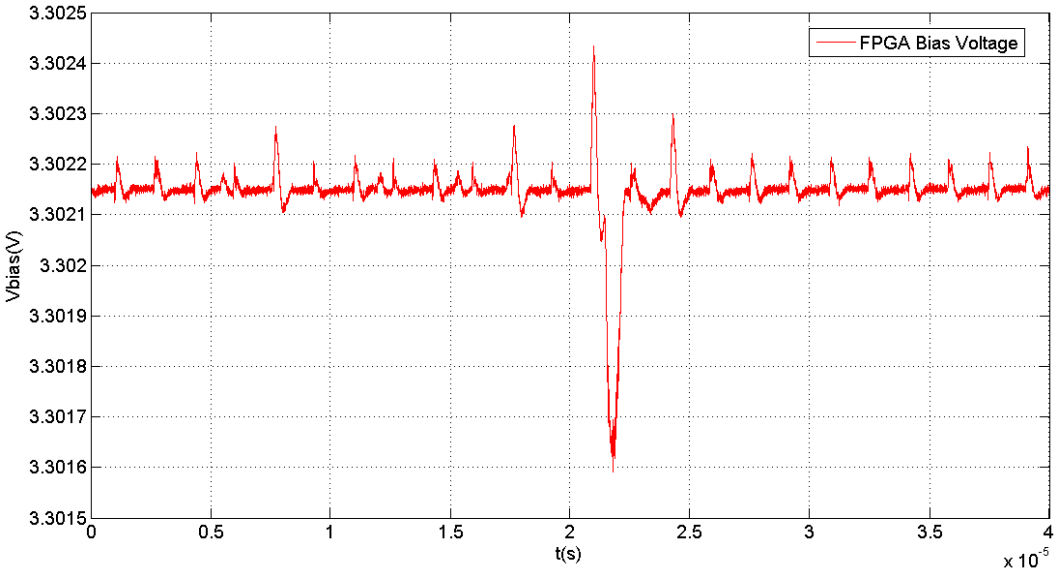



**Figure 3.9**: Bias voltage of FPGA in SCM.

The frequency response of the transimpedance gain for SCM compared with ideal characteristic given in Equation (3.3) is shown in Figure 3.10.

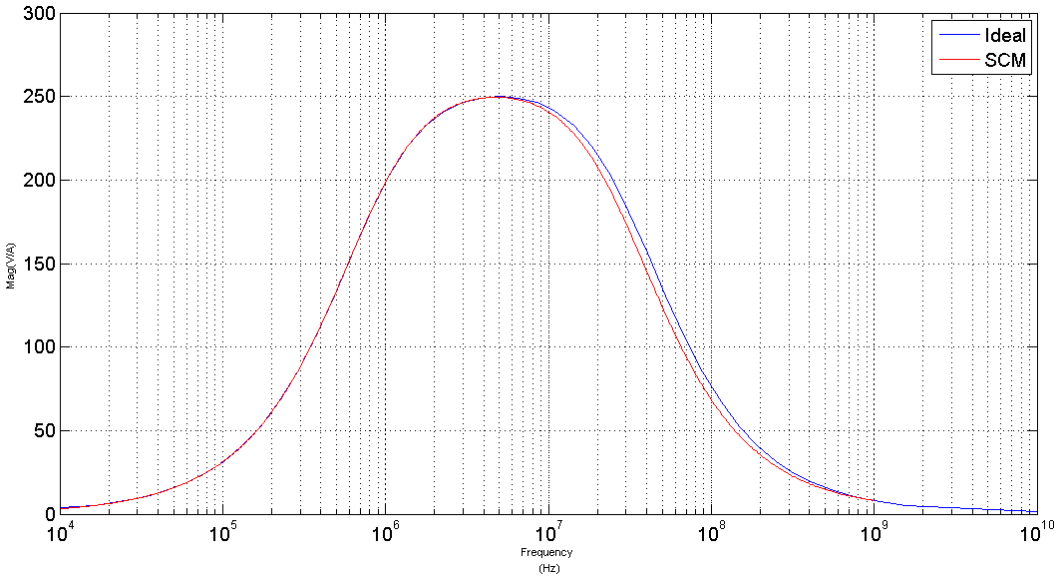



**Figure 3.10**: Frequency response of transimpedance gain for SCM compared with ideal response.

The frequency dependence of input impedance for SCM is shown in Figure 3.11. It can be seen that input impedance is low as expected.

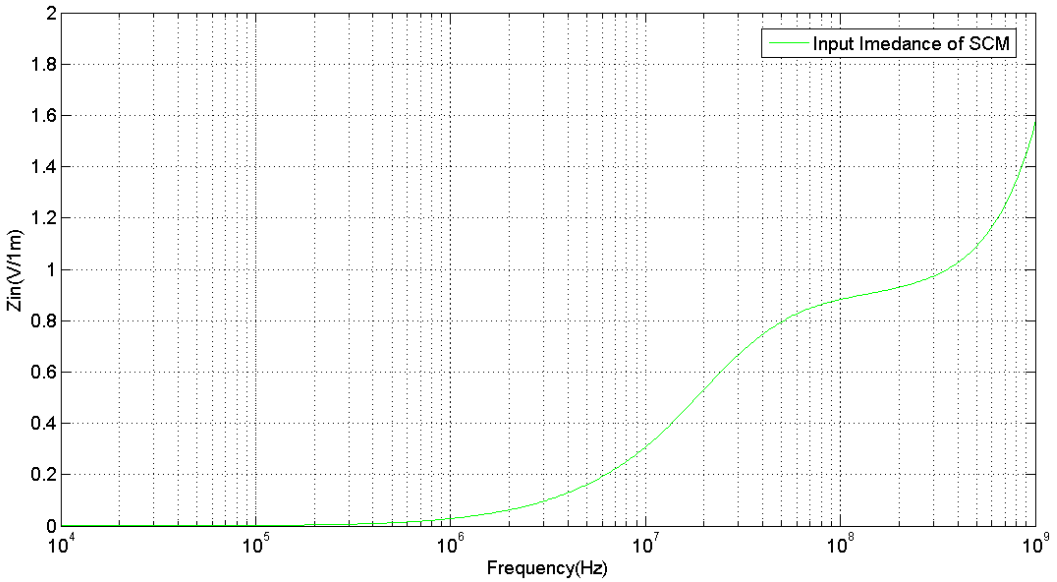



**Figure 3.11**: Input impedance characteristic of SCM.

### 3.2.3 Power measurement simulation of SCM

The power measurement simulation result of SCM is given in Figure 3.12. It can be seen from the figure that the SMC output follows the actual chip current successfully. Since peak values are amplified and the difference between the maximum valued consecutive peaks are increased, the difference between correlation coefficient values in R matrix becomes more distinctive. Hence, the number of power traces needed to conduct a DPA attack is significantly reduced. Furthermore, peak amplitudes ranging from 0.1V to 0.9V shows an improvement in the sensitivity.

## 3.3 CCII+ Based Supply Current Measuring Circuit

Second generation current conveyor(CCII) is a multi-purpose analogue component that is widely used in signal processing applications and it constitutes a building block for universal active element design [12]. It is introduced by Sedra and Smith in 1970. Since 1970, different types of current conveyor designs have been introduced [13] [14].The block diagram of an ideal CCII is given in Figure 3.13. Basically, an ideal CCII is a three terminal device with terminals X, Y and Z. There is a voltage follower

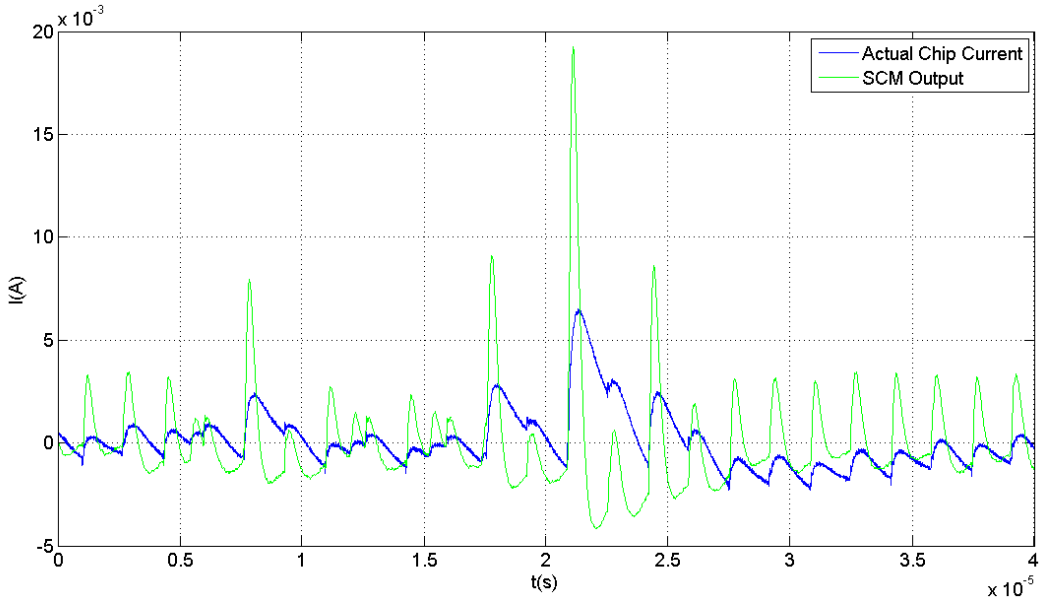



**Figure 3.12**: Power measurement simulation of SCM.

between X and Y terminals and a positive CCII+ or a negative CCII- current follower between X and Z terminals [15] Terminal relations of an ideal CCII is given in Equation 3.18.

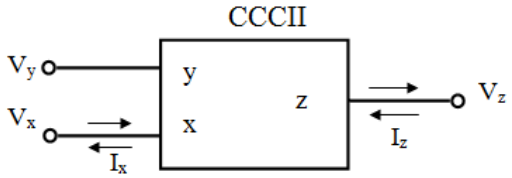



**Figure 3.13**: Block diagram of an ideal CCII.

$$\begin{bmatrix} i_y \\ v_x \\ i_z \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & R_x & 0 \\ 0 & \pm 1 & 0 \end{bmatrix} \begin{bmatrix} v_y \\ i_x \\ v_z \end{bmatrix} \tag{3.18}$$

A CCII+ based SCM circuit design is proposed in this part of the thesis. This power measurement circuit operates with the same principle of the SCM circuit explained in the previous section. However, CCII+ based SCM circuit constructed with less active elements and since the inductor is grounded it can be replaced with an active only grounded inductor simulator [16]. By this way CMOS realisation of SCM circuit becomes feasible.

### 3.3.1 Circuit description of CCII+ based SCM

Schematic of a typical second generation translinear current conveyor circuit is given in Figure 3.14. 3.3V bias voltage is needed for FPGA. The typical translinear CCII+ shown in Figure 3.14 is not able to supply this voltage at Y terminal. Hence, this topology is modified. The realisation of the modified CCII+ used in SCM circuit is shown in Figure 3.15. Transistor aspect ratios are given in Table 3.1.

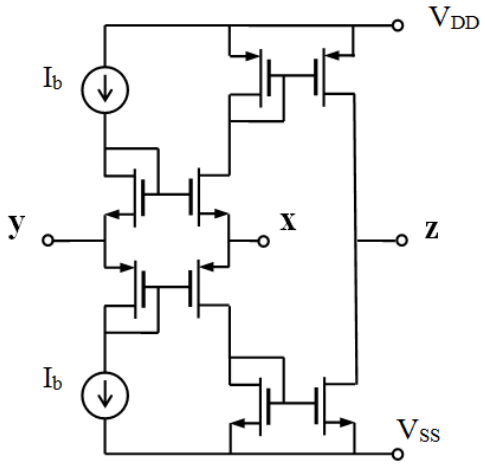



**Figure 3.14**: Schematic of a typical translinear CCII+ circuit.

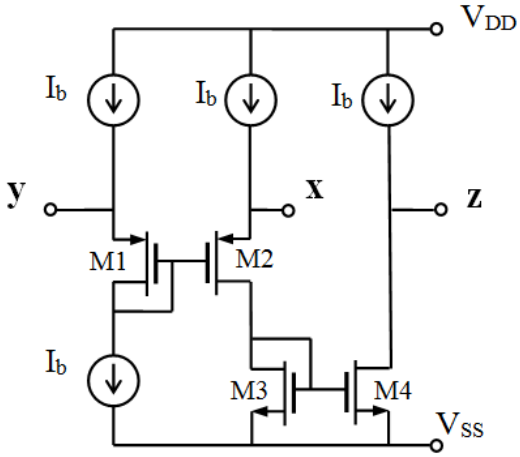



**Figure 3.15**: Realisation of modified CCII+.

**Table 3.1**: Transistor aspect ratios of designed CCII+.

| Transistors | W | L |
|---|---|---|
| $M_1$-$M_2$ | 150 | 1.2 |
| $M_3$-$M_4$ | 125 | 1.2 |

Small signal resistance at X terminal of CCII+ can be expressed with the following equation:

$$r_x = \frac{1}{g_{m2}}(1+\frac{r_{o3}}{r_{o2}}) = \frac{1}{g_{m2}}(1+\frac{\frac{1}{g_{m3}}}{r_{o2}}) \tag{3.19}$$

This relationship shows that $r_x$ is approximately equal to $\frac{1}{g_{m2}}$ which is expected to be in the range of hundred Ωs.

Small signal resistance at Y and Z terminals of CCII+ can be expressed with the following equations:

$$r_y \simeq \infty \tag{3.20}$$

$$r_z = r_{o4} \tag{3.21}$$

The circuit schematic of CCII+ based SCM is given in Figure 3.16. The bias voltage $V_{DD}$ connected to y terminal appears at the x terminal of CCII+. Hence, $V_{DD}$ voltage becomes the bias voltage of the FPGA under attack. The current drawn from the FPGA is conveyed to z terminal and filtered with a parallel RLC circuit. The values for RLC circuit are chosen as $R_f$=250Ω, $C_f$=10$pF$, L=100$\mu$H. A voltage buffer is used at the output stage. The transfer function expression of CCII+ based SCM is identical to SCM transfer function given in Equation 3.3.

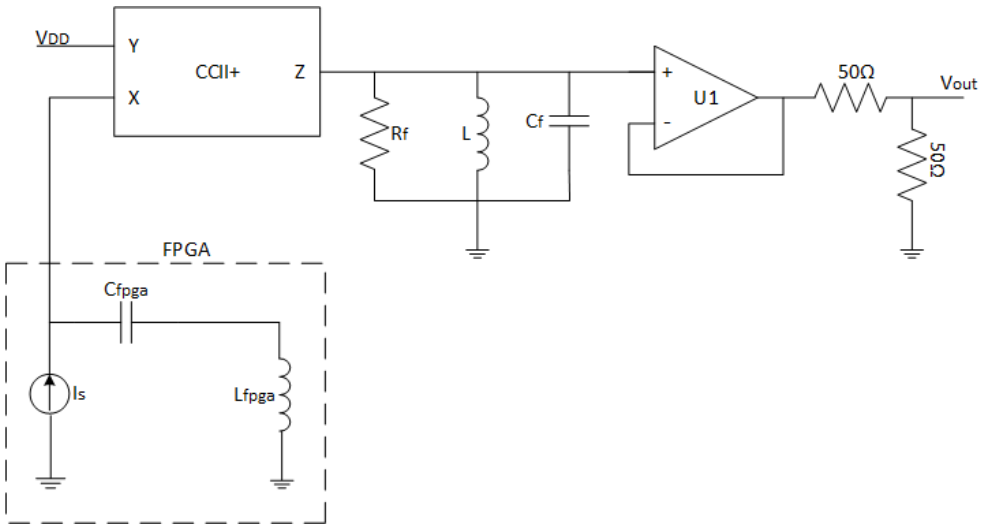



**Figure 3.16**: Schematic of CCII+ based SCM circuit.

### 3.3.2 Main characteristics of CCII+ based SCM

In this section main characteristics of the designed CCII+ is given before the main characteristics of CCII+ based SCM. CCII+ circuit simulations are obtained for a bias

current of 2mA. The voltage transfer characteristics of CCII+ is given in Figure 3.17. It indicates a close voltage ratio between input voltages 2V to 5V. The current transfer characteristic of CCII+ is shown in Figure 3.18. There is a DC current gain of 2.11 between $i_x$ and $i_z$. The DC current gain is advantageous for the operation of SCM because it increases the measured peak values of the power traces.

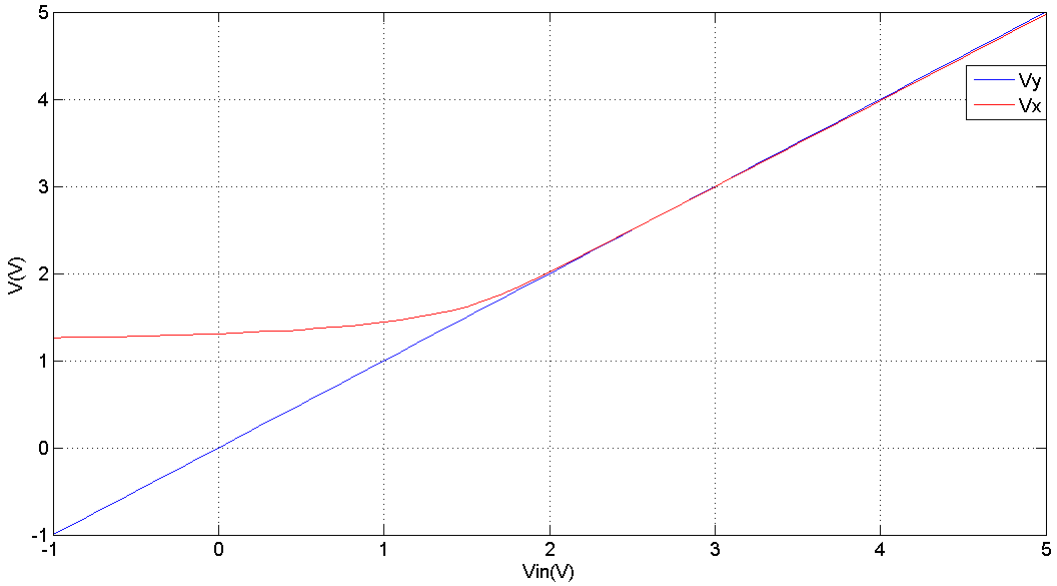



**Figure 3.17**: Voltage transfer characteristic of CCII+.

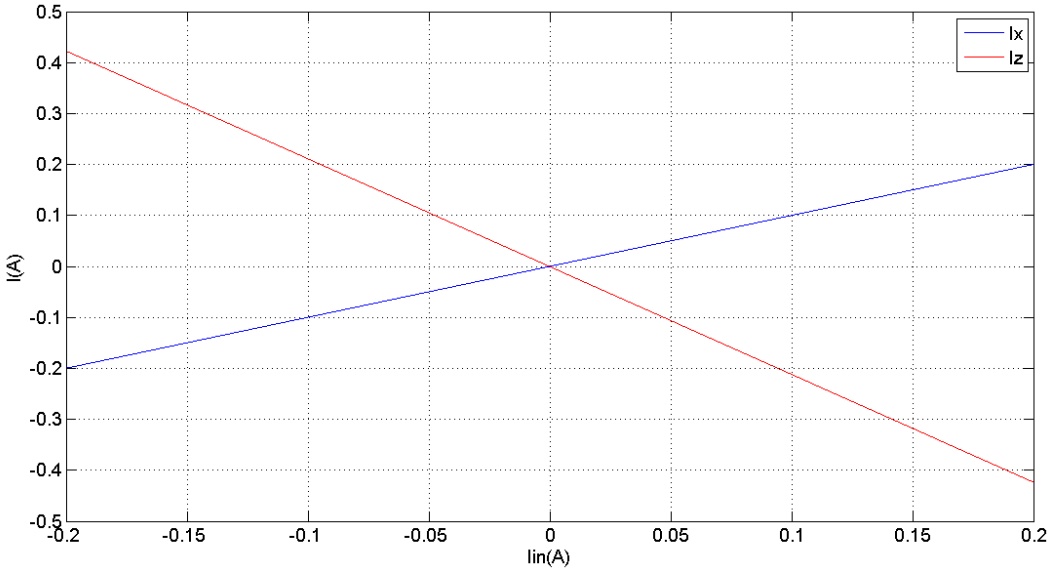



**Figure 3.18**: Current transfer characteristic of CCII+.

Frequency response of the voltage gain between Y and X terminals is given in Figure 3.19. The voltage bandwidth is exceeding 100MHz.

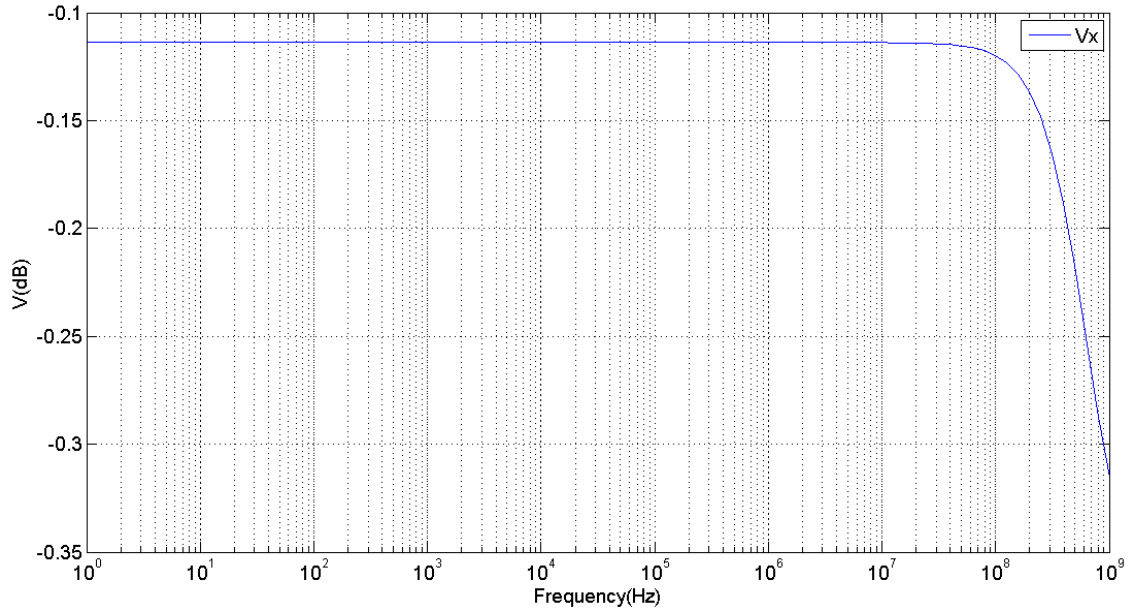



**Figure 3.19**: Frequency response of voltage gain between Y and X terminals of CCII+.

Frequency response of the current gain between X and Z terminals is shown in Figure 3.20.

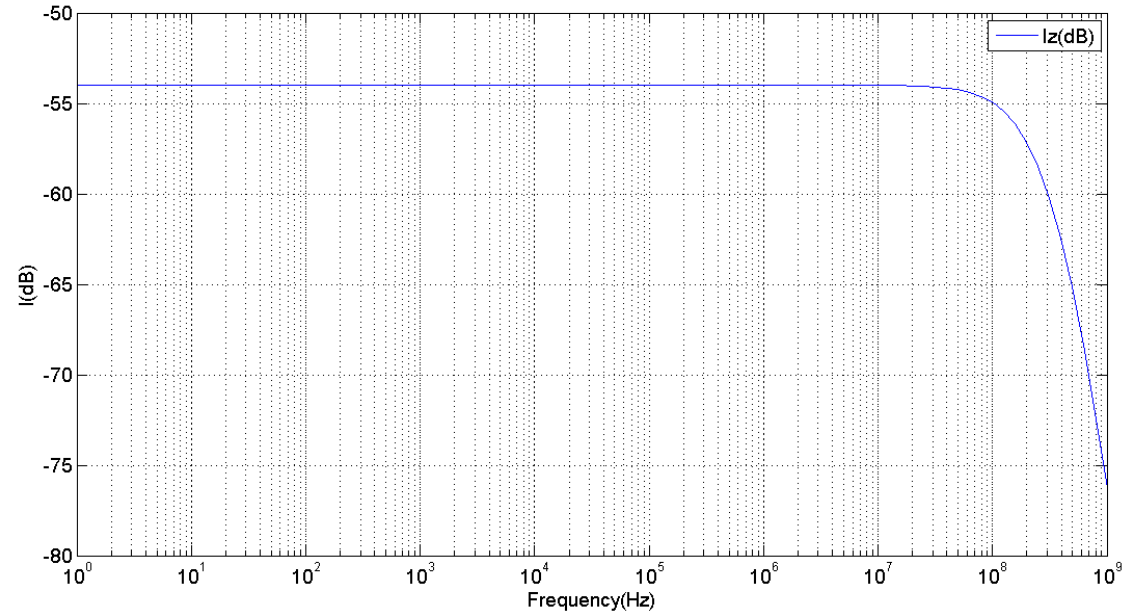



**Figure 3.20**: Frequency response of current gain between X and Z terminals of CCII+.

The frequency dependency of the parasitic resistance at X terminal of CCII+ is shown in Figure 3.21. It exhibits 245Ω value.

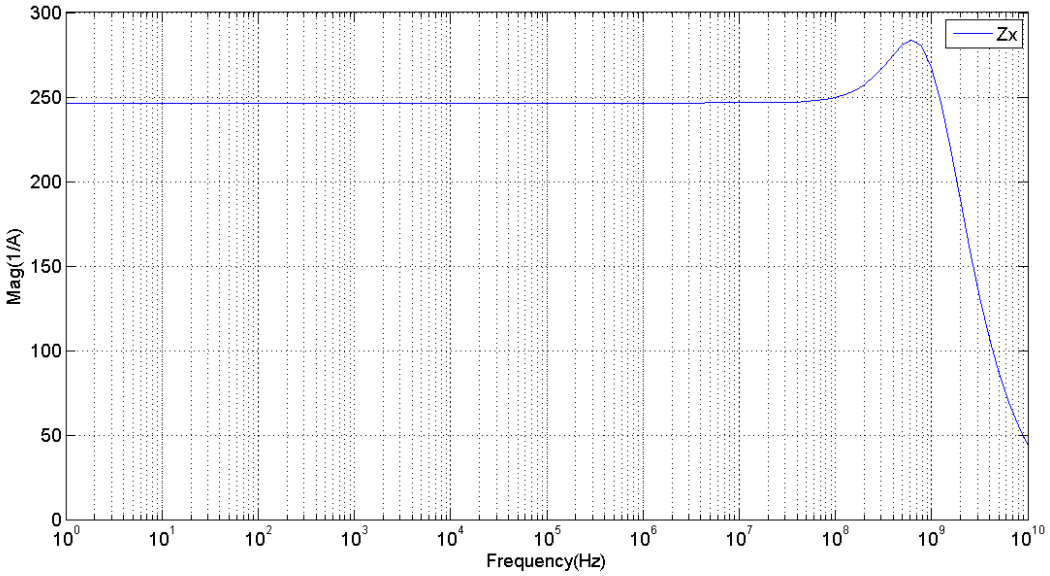



**Figure 3.21**: Frequency dependency of the parasitic resistance at X terminal of CCII+.

The bias voltage of the attacked FPGA connected to X terminal of CCII+ based SCM is shown in the Figure 3.22. The bias voltage is not stable. The stability can be increased by further improvement of the CCII+ design.

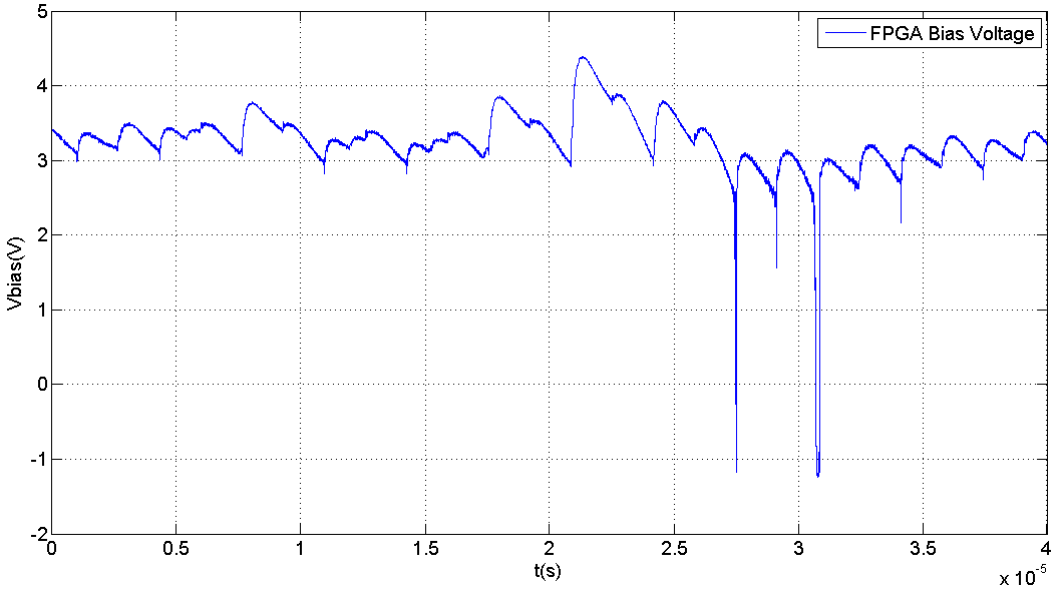



**Figure 3.22**: Bias voltage of FPGA in CCII+ based SCM.

The frequency response of the transimpedance gain for CCII+ based SCM compared with ideal characteristic given in Equation 3.3 is shown in Figure 3.23.

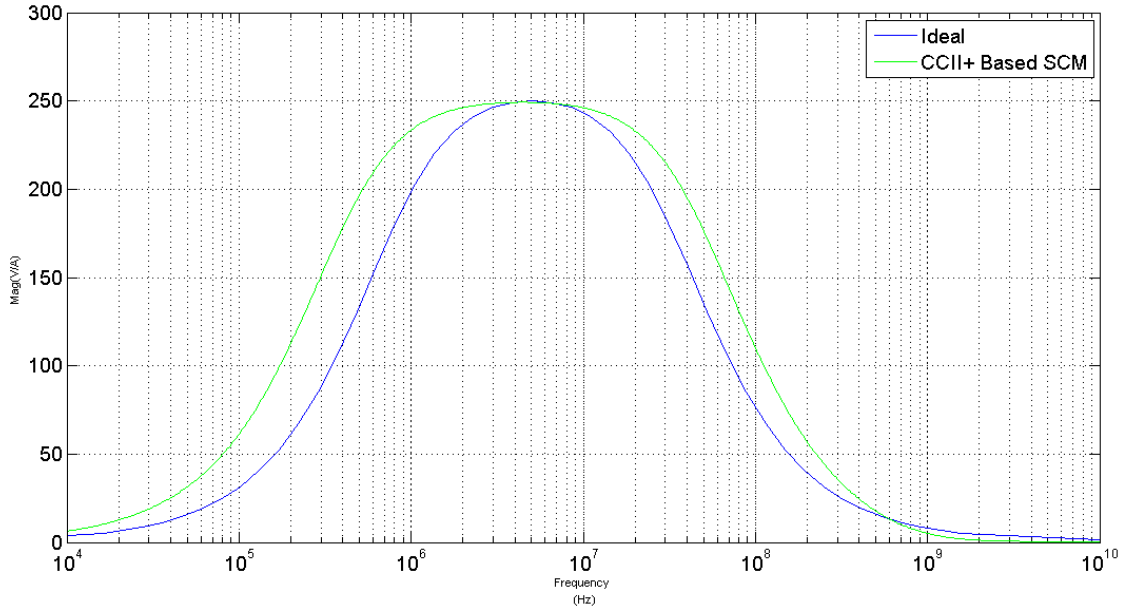



**Figure 3.23**: Frequency response of transimpedance gain for CCII+ based SCM compared with ideal response.

### 3.3.3 Power measurement simulation of CCII+ based SCM

The power measurement simulation result of CCII+ based SCM is given in Figure 3.24. CCII+ based SCM follows the actual chip current with high precision. In addition, it amplifies the peak values while increasing the bandwidth of the current signals. Therefore, it provides a prosperous measurement of power traces and decreases the effort needed to conduct a DPA attack.

## 3.4 Comparison of Power Measurement Circuits

Brief comparison of the power measurement circuits explained in the previous sections is given in this section. Comparison is based on bias stability, measurement accuracy and the degree of sensitivity. Also, a comparison of frequency response of transimpedance gain for standard SCM and CCII+ based SCM with the expected ideal response is given at the end of this section.

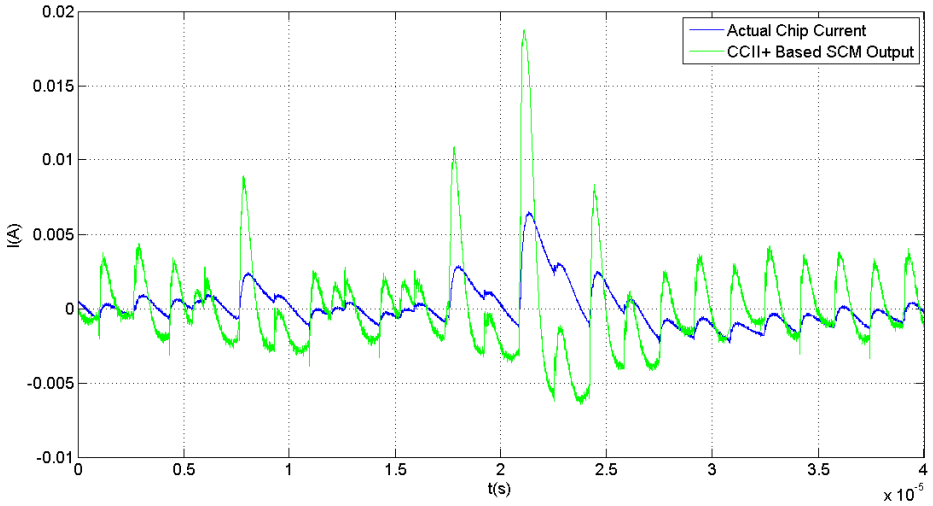



**Figure 3.24**: Power measurement simulation of CCII+ based SCM.

Comparison of bias voltages supplied to FPGA under three different power measurement configuration is shown in Figure 3.25. It can be seen from the figure that standard SCM provides more stable bias voltage compared with RMC and CCII+ based SCM. The reason behind this performance is the low frequency voltage feedback loop provided by an inductor. CCII+ based SCM is expected to supply more stable bias, however the parasitic gate capacitances of the input transistors pose an obstacle to it. Bias stability of CCII+ based SCM can be increased by a more effective design that eliminates the effect of the input parasitic capacitances. In RMC, since there is no feedback loop compensating the variations of bias voltage, the bias voltage will change in accordance with the current drawn from the FPGA.

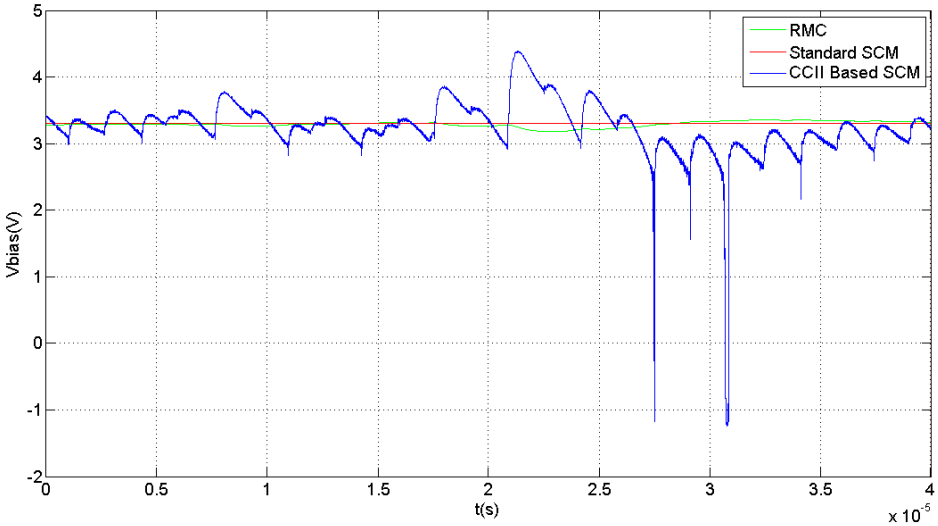



**Figure 3.25**: Comparsion of bias voltages supplied to FPGA.

Comparison of power measurement simulations with supplied actual chip current in terms of measurement accuracy is given in Figure 3.26. Because of the high bandwidth and transimpedance gain of standard SCM and CCII+ based SCM, they show excellent performance while tracking actual chip current. On the other hand, RMC could not able to follow the actual chip current due to its bandwidth limitation. The wide difference between bandwidths can be interpreted by comparing the peak durations. According to these results the following inference can be made: If a DPA attack is conducted using RMC, standard SCM and CCII+ based SCM with the same number of power trace measurement , it will be easier to distinguish the maximum correlation coefficient value in R matrix in attacks performed by standard SCM and CCII+ based SCM.

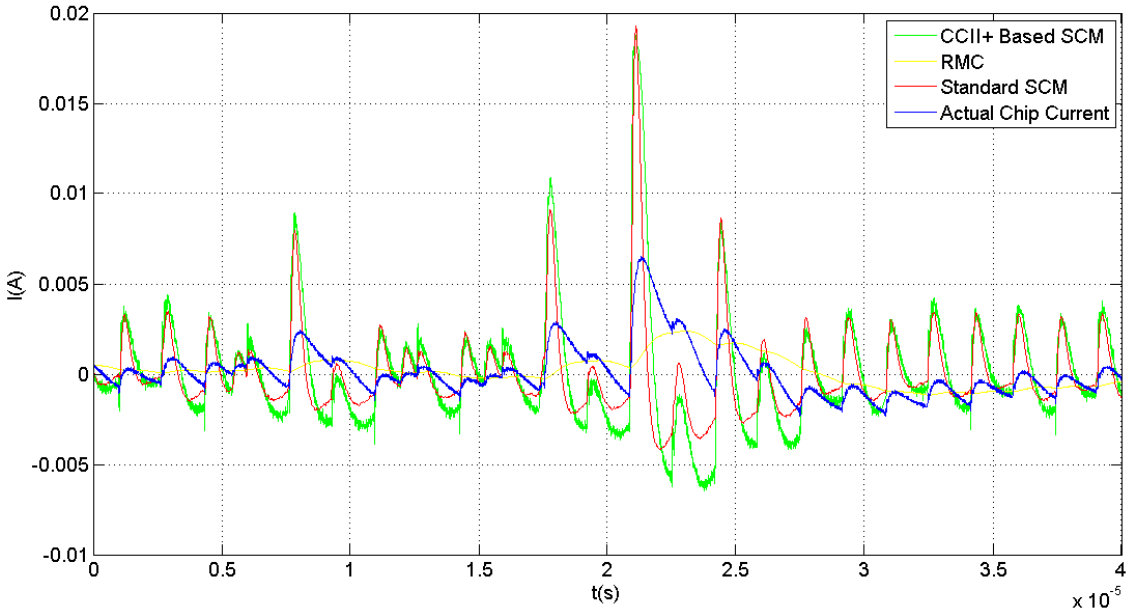



**Figure 3.26**: Comparison of power measurement simulations.

Comparison of maximum peak levels for RMC, standard SCM and CCII+ based SCM is given in Figure 3.27. For standard SCM and CCII+ based SCM peak amplitudes are ranging from 0.1V to 0.94V. On the contrary, maximum peak amplitude for RMC is 0.11V. The maximum peak amplitude of RMC is 8.5 times smaller than peak amplitude of standard SCM and CCII+ based SCM. Equation 3.22 shows signal to noise ratio(SNR) expression. If Equation 3.22 is taken as a figure of merit at sensitivity comparison, standard SCM and CCII+ based SCM shows 10dB improvement in the sensitivity to the current consumption variations of a device under attack [6].

$$SNR = 10log(\frac{S}{N}) \tag{3.22}$$

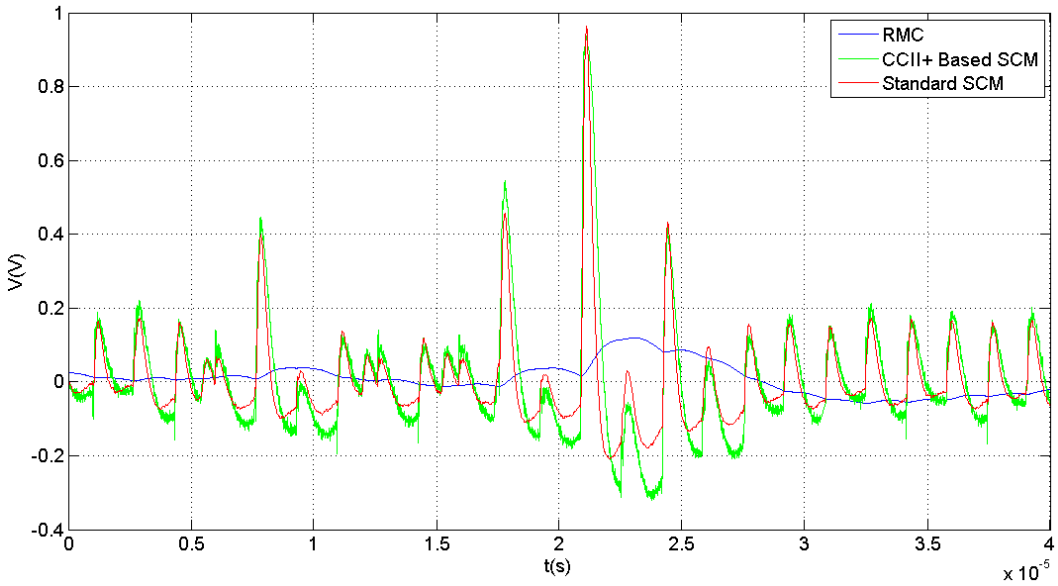



**Figure 3.27**: Comparison of maximum peak levels.

Comparison of frequency response of transimpedance gain for standard SCM and CCII+ based SCM with the expected ideal response based on Equation 3.3 is shown in Figure 3.28. As it can be seen from the Figure 3.28, theoretical transfer characteristic obtained in Equation 3.3 fits substantially with the simulation results.

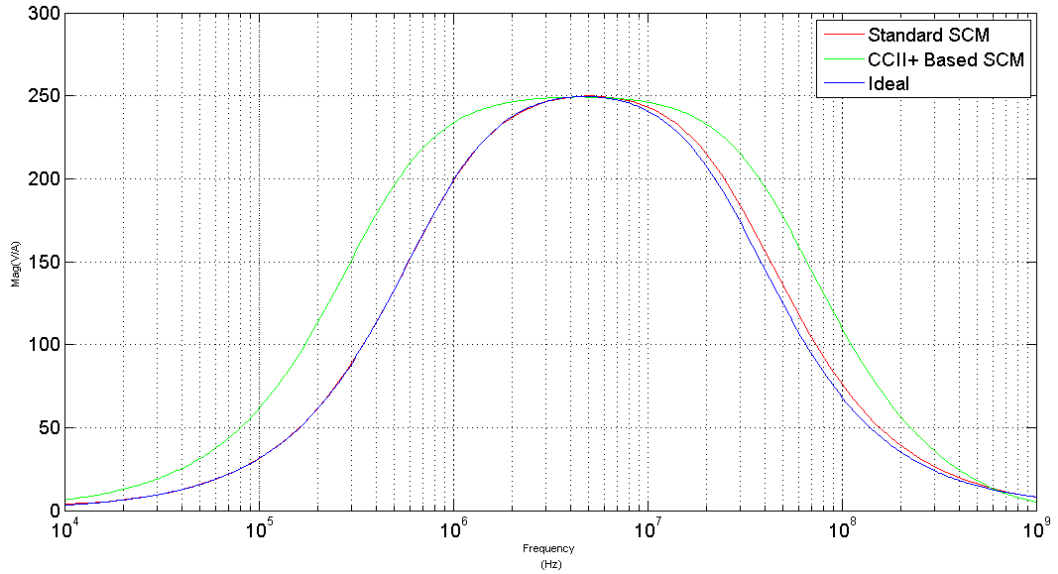



**Figure 3.28**: Comparsion of frequency response of transimpedance gains with ideal response.

### 3.4.1 Simulated correlation values of DPA by using SCM circuit

Simulated correlation values of power analysis attack conducted can be seen from Figure 3.29. Blue graph corresponds to "1" bit and red graph corresponds to "0" bit. As it is seen from Figure 3.29, separation begins after 3000 power trace. Therefore, it can be concluded that corresponding bit is 0.

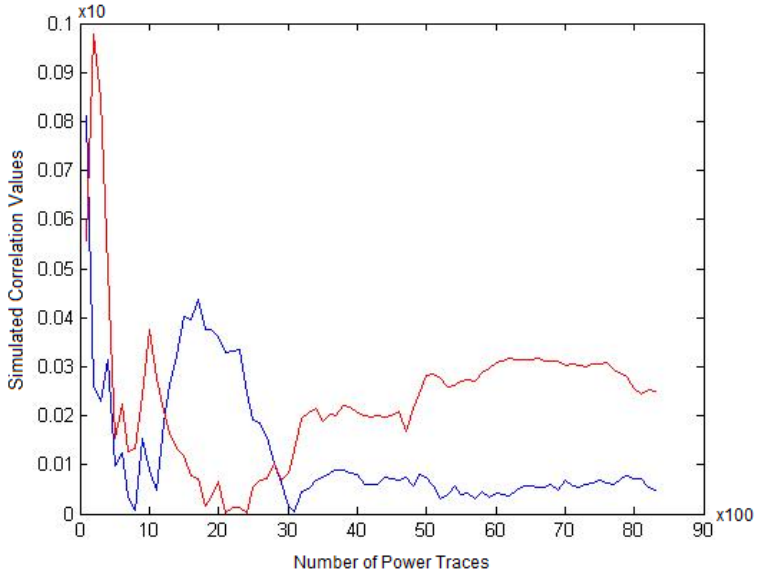



**Figure 3.29**: Simulated correlation values of DPA by using SCM circuit.

# 4. CONCLUSIONS AND RECOMMENDATIONS

Cryptographic devices are the main part of security systems [4]. No information should leak during encryption process. However, Kocher showed that there is an information leakage that could be obtained by monitoring power consumption, electromagnetic emission and execution timing [7]. The monitoring of such physical quantities of cryptographic device is called side channel attack.

Power consumption simulations are performed both by designers and attackers. Attackers use these simulations to reveal the secret key of the cryptographic chip whereas designers use it to predict the resistance of their designs against side channel attacks.

Typical measurement setup to perform a power analysis attacks is composed of a power supply, a clock generator, a measurement circuit, a digital sampling oscilloscope and the attacked cryptographic device [4]. These components are easy to find and low cost in such a way that one can perform this attack at anywhere. There are two main power analysis attacks. These are simple power analysis(SPA) and differential power analysis(DPA). Both are introduced by Kocher. DPA is a more effective attack compared with SPA for sophisticated cryptographic devices.

The success of power analysis attack highly depends on the quality of the measurements. The figure of merit of power analysis measurements is signal to noise ratio(SNR) of measured power trace. Noise in power measurements consists of two components. These are electronic noise and switching noise. Switching noise is highly depends on the clock frequency of the cryptographic device and the bandwidth of the connection between logic cells and oscilloscope [4]. It is not possible to completely remove electronic noise and switching noise. However, by using SCM and CCII+ based SCM power measurement circuits explained in Chapter 3, the SNR of the measured power waveform can be improved.

The power analysis measurements can be performed with the circuits given in Chapter 3. The resistive measurement circuit(RMC) is widely used in power measurement applications. However, RMC is not able to give good quality measurement results

because its bandwidth and sensitivity is limited and it is not able to supply stable bias to device under attack [6] SCM circuit introduced in 2006 and CCII+ based SCM circuit introduced in this thesis provide significant improvement in terms of bandwidth, sensitivity and bias stability. The results of these improvements can be seen from the power simulations obtained in Chapter 3. These improvements are expected to lead a reduction in the number of power traces needed to perform power analysis attacks. The newly introduced CCII+ based SCM circuit showed a similar performance with standard SCM. There are two main advantages of CCII+ based SCM. It has less active elements than standard SCM. Also, since the inductor is grounded in CCII+ based SCM, it is more suitable for CMOS realisation. Hence, the newly introduced CCII+ based SCM circuit can be used as an alternative to standard SCM circuit. However, it is hard to provide stable bias with CCII+ based SCM.

## REFERENCES


[1] **De Mulder, E.**, **Örs, S.B.**, **Preneel, B. and Verbauwhede, I.** (2007). Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems, *Computers and Electrical Engineering*, ***33***, 367–382.

[2] **Url-1**, `http://www.idga.org`, access date: 26.04.2014.

[3] **Url-2**, `http://www.rcis.aist.go.jp`, access date: 26.04.2014.

[4] **Mangard, S.**, **Oswald, M.E. and Popp, T.** (2007). *Power Analysis Attacks - Revealing the Secrets of Smart Cards*.

[5] **Iokibe, K., A.T.O.K. and Toyota, Y.** (2013). Equivalent circuit modeling of cryptographic integrated circuit for information security design, *IEEE Transactions on Electromagnetic Compatibility*, ***55***, 581–588.

[6] **Bucci, M.**, **Giancane, L.**, **Luzzi, R.**, **Scotti, G. and Trifiletti, A.** (2008). Enhancing power analysis attacks against cryptographic devices, *IET Circuits, Devices and Systems*.

[7] **Kocher, P. C., J.J. and Jun, J.** (1999). Differential Power Analysis, *Advances in Cryptology: Proceedings of CRYPTO' 99*, Santa Barbara, California, USA.

[8] **Kocher, P.C.** (1996). Timing Attacks on Implementations of Diffie-Helman, RSA, DSS, and Other Systems, *Advances in Cryptology: Proceedings of CRYPTO' 96*, Santa Barbara, California, USA.

[9] **Gandolfi, K.**, **Mourtel, C. and Olivier, F.** (2001). Electromagnetic Analysis : Concrete Results, *Cryptographic Hardware and Embedded Systems — CHES 2001*, ***2162***, 251–261.

[10] **Quisquater, J.J. and Samyde, D.** (2001). Electromagnetic analysis (ema): Measures and counter-measures for smart cards, *Smart Card Programming and Security*, 200–210.

[11] **Bucci, M.**, **Giancane, L.**, **Luzzi, R.**, **Scotti, G. and Trifiletti, A.** (2006). Enhancing power analysis attacks against cryptographic devices, *2006 IEEE International Symposium on Circuits and Systems*.

[12] **Smith, K. and Sedra, A.** (1970). "A second-generation current conveyor and its applications, *IEEE Transactions on Circuit Theory*, ***17***, 132–134.

[13] **Minaei, S.**, **Sayin, O. and Kuntman, H.** (2006). A new CMOS electronically tunable current conveyor and its application to current-mode filters, *IEEE Transactions on Circuits and Systems I: Regular Papers*, ***53***.

[14] **Becvar, D.**, **Vrba, K.**, **Zeman, V. and Musil, V.** (2000). Novel universal active block: a universal current conveyor, *2000 IEEE International Symposium on Circuits and Systems. Emerging Technologies for the 21st Century. Proceedings (IEEE Cat No.00CH36353)*, ***3***.

[15] **Calvo, B., C.S.M.P. and M. T., S.** (2003). Novel high performance CMOS current conveyor, *Microelectronics Reliability*, volume 43, pp.955–961.

[16] **Yamacli, S., O.S.K.H.** (2011). New active-only grounded inductance simulator employing current-mode approach suitable for wide band operation, *International Journal of Electronics*, ***98***, 981–994.

**APPENDICES**

**APPENDIX A.1 :** PSpice Model Parameters for NMOS
**APPENDIX A.2 :** PSpice Model Parameters for PMOS

**APPENDIX A.1**

```
* *** Flags ***
+MOBMOD =1.000e+00 CAPMOD =2.000e+00
+NLEV =0
* *** Threshold voltage related model parameters ***
+K1 =6.044e-01
+K2 =2.945e-03 K3 =-1.72e+00 K3B =6.325e-01
+NCH =2.310e+17 VTH0 =4.655e-01
+VOFF =-5.72e-02 DVT0 =2.227e+01 DVT1 =1.051e+00
+DVT2 =3.393e-03 KETA =-6.21e-04
+PSCBE1 =2.756e+08 PSCBE2 =9.645e-06
+DVT0W =0.000e+00 DVT1W =0.000e+00 DVT2W =0.000e+00
* *** Mobility related model parameters ***
+UA =1.000e-12 UB =1.723e-18 UC =5.756e-11
+U0 =4.035e+02
* *** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =3.085e-02 ETAB =-3.95e-02
+NFACTOR=1.119e-01
* *** Saturation related parameters ***
+EM =4.100e+07 PCLM =6.831e-01
+PDIBLC1=1.076e-01 PDIBLC2=1.453e-03 DROUT =5.000e-01
+A0 =2.208e+00 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =1.178e+05 AGS =2.490e-01
+B0 =-1.76e-08 B1 =0.000e+00 DELTA =1.000e-02
+PDIBLCB=2.583e-01
* *** Geometry modulation related parameters ***
+W0 =1.184e-07 DLC =8.285e-09
+DWC =2.676e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
+WW =0.000e+00 WWL =0.000e+00 WLN =1.000e+00
+WWN =1.000e+00
* *** Temperature effect parameters ***
+AT =3.300e+04 UTE =-1.80e+00
+KT1 =-3.30e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00
+PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =2.100e-10 CGSO =2.100e-10 CGBO =1.100e-10
+CGDL =0.000e+00 CGSL =0.000e+00 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =6.043e+02
```

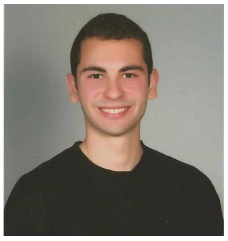
```
+CDSC =0.000e+00 CDSCB =0.000e+00 CDSCD =8.448e-05
+PRWB =0.000e+00 PRWG =0.000e+00 CIT =1.000e-03
* *** Process and parameters extraction related model parameters ***
+TOX =7.700e-09 NGATE =0.000e+00
+NLX =1.918e-07
* *** Substrate current related model parameters ***
+ALPHA0 =0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.400e+00 KF =2.810e-27 EF =1.000e+00
+NOIA =1.000e+20 NOIB =5.000e+04 NOIC =-1.40e-12
* *** Common extrinsic model parameters ***
+LINT =-1.67e-08 WINT =2.676e-08 XJ =3.000e-07
+RSH =8.200e+01 JS =2.000e-05
+CJ =9.300e-04 CJSW =2.800e-10
+MJ =3.100e-01 MJSW =1.900e-01
+PB =6.900e-01 TT =0.000e+00
+PBSW =9.400e-01
* ____________________________________________________-
```

**APPENDIX A.2**

```
* *** Flags ***
+MOBMOD =1.000e+00 CAPMOD =2.000e+00
+NLEV =0
* *** Threshold voltage related model parameters ***
+K1 =5.675e-01
+K2 =-4.39e-02 K3 =4.540e+00 K3B =-8.52e-01
+NCH =1.032e+17 VTH0 =-6.17e-01
+VOFF =-1.13e-01 DVT0 =1.482e+00 DVT1 =3.884e-01
+DVT2 =-1.15e-02 KETA =-2.56e-02
+PSCBE1 =1.000e+09 PSCBE2 =1.000e-08
+DVT0W =0.000e+00 DVT1W =0.000e+00 DVT2W =0.000e+00
* *** Mobility related model parameters ***
+UA =2.120e-10 UB =8.290e-19 UC =-5.28e-11
+U0 =1.296e+02
* *** Subthreshold related parameters ***
+DSUB =5.000e-01 ETA0 =2.293e-01 ETAB =-3.92e-03
+NFACTOR=8.237e-01
* *** Saturation related parameters ***
+EM =4.100e+07 PCLM =2.979e+00
+PDIBLC1=3.310e-02 PDIBLC2=1.000e-09 DROUT =5.000e-01
+A0 =1.423e+00 A1 =0.000e+00 A2 =1.000e+00
+PVAG =0.000e+00 VSAT =2.000e+05 AGS =3.482e-01
+B0 =2.719e-07 B1 =0.000e+00 DELTA =1.000e-02
+PDIBLCB=-1.78e-02
* *** Geometry modulation related parameters ***
+W0 =4.894e-08 DLC =-5.64e-08
+DWC =3.845e-08 DWB =0.000e+00 DWG =0.000e+00
+LL =0.000e+00 LW =0.000e+00 LWL =0.000e+00
+LLN =1.000e+00 LWN =1.000e+00 WL =0.000e+00
+WW =0.000e+00 WWL =0.000e+00 WLN =1.000e+00
+WWN =1.000e+00
* *** Temperature effect parameters ***
+AT =3.300e+04 UTE =-1.35e+00
+KT1 =-5.70e-01 KT2 =2.200e-02 KT1L =0.000e+00
+UA1 =0.000e+00 UB1 =0.000e+00 UC1 =0.000e+00
+PRT =0.000e+00
* *** Overlap capacitance related and dynamic model parameters ***
+CGDO =2.100e-10 CGSO =2.100e-10 CGBO =1.100e-10
+CGDL =0.000e+00 CGSL =0.000e+00 CKAPPA =6.000e-01
+CF =0.000e+00 ELM =5.000e+00
+XPART =1.000e+00 CLC =1.000e-15 CLE =6.000e-01
* *** Parasitic resistance and capacitance related model parameters ***
+RDSW =1.853e+03
+CDSC =6.994e-04 CDSCB =2.943e-04 CDSCD =1.970e-04
+PRWB =0.000e+00 PRWG =0.000e+00 CIT =1.173e-04
* *** Process and parameters extraction related model parameters ***
```

```
+TOX =7.700e-09 NGATE =0.000e+00
+NLX =1.770e-07
* *** Substrate current related model parameters ***
+ALPHA0 =0.000e+00 BETA0 =3.000e+01
* *** Noise effect related model parameters ***
+AF =1.290e+00 KF =1.090e-27 EF =1.000e+00
+NOIA =1.000e+20 NOIB =5.000e+04 NOIC =-1.40e-12
* *** Common extrinsic model parameters ***
+LINT =-8.14e-08 WINT =3.845e-08 XJ =3.000e-07
+RSH =1.560e+02 JS =2.000e-05
+CJ =1.420e-03 CJSW =3.800e-10
+MJ =5.500e-01 MJSW =3.900e-01
+PB =1.020e+00 TT =0.000e+00
+PBSW =9.400e-01
* _____-
```

**CURRICULUM VITAE**



**Name Surname:** Ahmet Emin Bekmezci

**Place and Date of Birth:** Seyhan, 15.10.1990

**E-Mail:** ahmetemin_3@hotmail.com

**B.Sc.:** METU, Electrical and Electronics Engineering (2012)

**Professional Experience and Rewards:**

**02/2012-05/2012 : Part-Time Engineer**
Micro-Nano Devices Design Division,
Microelectronics,Guidance and Electro-optics Division (MGEO)
ASELSAN Electronic Industries Inc., Ankara

**06/2011-07/2011: Summer Internship**
Micro-Nano Devices Design Division,
Microelectronics, Guidance and Electro-optics Division (MGEO)
ASELSAN Electronic Industries Inc., Ankara

**07/2011-08/2011: Summer Internship**
Radar Division,
DHMİ Adnan Menderes Airport Electronics Directory, İzmir

**2010-2011: Undergraduate Researcher**
Advisor: Assoc. Prof. Ali Özgür Yılmaz
Research Area: Radar Signal Processing
Middle East Technical University(METU), Ankara