University of Rome "La Sapienza" Infineon Technologies AG

Never stop thinking

Department of Electronic Engineering

# Active probe circuit to implement power analysis techniques

Main supervisor University of Rome "La Sapienza":
Prof. Alessandro Trifiletti

Main supervisor Infineon Technologies AG:
Dr. Dipl. Ing. Raimondo Luzzi

Degree Thesis of Michele Marino
Student number: 792033

Academic Year 2005 - 2006

Ai miei genitori
*Salvatore* e *Teresa*
che mi hanno sempre sostenuto,
e ai miei nipotini
*Francesco Pio*, *Alessia* e *Maria Teresa.*

# Contents

# List of Figures

# List of Tables

# Preface

Side channel attacks can reveal confidential data (i.e. cryptographic keys and user PIN‘s) exploiting the information leaked by the hardware implementation of cryptographic algorithms.

This thesis work is devoted to design an active current probe to implement power analysis attacks on crypto-processors. A short introduction on smart cards and cryptography is reported in Chapter 1. In the second chapter, different types of side channel attacks are discussed. In particular, power analysis attacks, simple and differential, are based on the fact that logic operations feature a power consumption profile dependent on the processed data: with simple statistical analyses of a sufficient number of power traces, the correlation between circuit switching activity and key material can be revealed.

In Chapter 3, an active current probe tested on a *FPGA* in a previous thesis work is shortly discussed, pointing out its main drawbacks. In particular, the maximum amplitude of the input current peaks is limited to about *7mA*, which is not sufficient in some cases.

As a first step, some changes on this first probe have been implemented to improve its performance, by testing different components for both the transimpedance amplifier and the output voltage buffer. The main goal was to achieve a better gain-bandwidth product.

Even if these changes shown some improvement with respect to the initial design, they did not provide the expected advantages, when compared with a resistor-based measuring setup. Moreover, the stability was an issue and the introduction of an additional compensation network was necessary.

For these reasons, a different circuit based on a common base configuration was adopted (Chapter 4), designing a new probe which can measure current peaks close to *100mA*, maximum allowed current consumption in a class A smart card[1]. Experiment results showed a substantial improvement with respect to the original design and a resistor-based measurement as well.

The main features of the three different active current probes evaluated in this work are summarized in Chapter 5, where the better performance of the common-base current probe are pointed out.

In appendix, a description of the Texas Instruments *THS320X* internal structure is reported and a short theory of current feedback amplifiers (*CFA*) is provided. Finally, the measurement of S-parameters is discussed.

I wish to thank **Alessandro Trifiletti**, **Raimondo Luzzi** and **Marco Bucci** for their valuable support.

I wish you a pleasant reading,
**Michele Marino**

[1] Smart cards can be divides in three class (A, B and C) based on their peak current consumptions.

# Chapter 1

# Smartcards & Cryptography

The proliferation of plastic cards started in the *USA* in the early *1950s*. The first all-plastic payment card for general use was issued by the *Diners Club* in *1950*. It was intended for an exclusive class of individual, and thus also served as a status symbol, allowing the holder to pay with his or her 'good name' instead of cash. The entry of *Visa* and *MasterCard* into the field led to a very rapid proliferation of 'plastic money' in the form of credit cards.

Today, credit cards allow travelers to shop without cash everywhere in the world. At first, the functions of these cards were quite simple. They served as data storage media that were secure against forgery and tampering. General information, such as the card issuer's name, was printed on the surface, while personal data elements, such as the cardholder's name and the card number, were embossed. In these first-generation cards, protection against forgery was provided by visual features, such as security printing and the signature panel. Consequently, the system's security depended quite fundamentally on the quality and conscientiousness of the persons responsible for accepting the cards. With the increasing proliferation of card use, these rather rudimentary features no longer proved sufficient, particularly since threats from organized criminals were growing apace. It became apparent that the security features for protection against fraud and manipulation, as well as the basic functions of the card, had to be expanded and improved.

The first improvement consisted of a magnetic stripe on the back of the card, which allowed digital data to be stored on the card in machine-readable form as a supplement to the visual information. This made it possible to minimize the use of paper receipts. This made it possible to finally achieve the long-standing objective of replacing paper-based transactions by electronic data processing. This required a different method to be used for user identification, which previously employed the user's signature. The method that has come into widespread general use involves a secret personal identification number (*PIN*) that is compared with a reference number. However, magnetic-stripe technology has a crucial weakness, which is that the data stored on the stripe can be read, deleted and rewritten at will by anyone with access to the necessary equipment. It is thus unsuitable for storing confidential data.

Most systems use online connections to the system's host computer for reasons of security, even though this generates significant costs for the necessary data transmissions. In order to reduce costs, it is necessary to find solutions that allow card transactions to be executed offline without endangering the security of the system. The development of the smart card, combined with the expansion of electronic data processing systems, has created completely new possibilities for devising such solutions.

Enormous progress in microelectronics in the *1970s* made it possible to integrate data storage and processing logic on a single silicon chip measuring a few square millimeters. The great breakthrough was achieved in *1984*, when the French *PTT* (*Postal and Telecommunications services agency*) successfully carried out a field trial with telephone cards. In this field trial, smart cards immediately proved to meet all expectations with regard to high reliability and protection against manipulation. A pilot project was conducted in Germany in *1984-85*, using telephone cards based on several technologies. Magnetic-stripe cards, optical-storage (*holographic*) cards and smart cards were used in comparative tests. Smart cards proved to be the winners in this pilot study. In addition to a high degree of reliability and security against manipulation, smart card technology promised the greatest degree of flexibility for future applications.

Further developments followed the successful trials of telephone cards. Telephone cards incorporating chips are currently used in more than fifty countries. The integrated circuits used in telephone cards are relatively small, simple and inexpensive memory chips with specific security logic that allows the card balance to be reduced while protecting it against manipulation.

In *1988*, the German Post Office acted as a pioneer in this area by introducing a modern microprocessor card using *EEPROM* technology as an authorization card for the analog mobile telephone network. The positive experience gained from using smart cards in the analog mobile telephone system was decisive for the introduction of smart cards into the digital *GSM* network.

Progress was significantly slower in the field of bank cards, in part due to their greater complexity compared with telephone cards. Modern hardware and software made it possible to implement complex, sophisticated mathematical algorithms that allowed previously unparalleled levels of security to be achieved. Moreover, this new technology was available to everyone, in contrast to the previous situation in which cryptography was a covert science in the private reserve of the military and secret services.

The smart card proved to be an ideal medium. It made a high level of security (based on *cryptography*) available to everyone, since it could safely store secret keys and execute cryptographic algorithms. In addition, smart cards are so small and easy to handle that they can be carried and used everywhere by everybody in everyday life. It was a natural idea to attempt to use these new security features for bank cards. However, the problems associated with making small payments securely but anonymously throughout the world via the public Internet have not yet been solved in a satisfactory manner. Smart cards could play a decisive role in providing an answer to these problems. Besides this, smart cards could plan an important role in introducing electronic signatures.

The predominant practitioners of the *cryptography* were those associated with the military, the diplomatic service and government in general. Cryptography was used as a tool to protect national secrets and strategies. The proliferation of computers and communications systems in the *1960s* brought with it a demand from the private sector for means to protect information in digital form and to provide security services. Beginning with the work of *Feistel* at *IBM* in the early 1970s and culminating in *1977* with the adoption as a *U.S. Federal Information Processing Standard* for encrypting unclassified information, *DES*, the *Data Encryption Standard*, is the most well-known cryptographic mechanism in history. The most striking development in the history of cryptography came in *1976* when *Diffie* and *Hellman* published *New Directions in Cryptography.* This paper introduced the revolutionary concept of *public-key cryptography* and also provided a new and ingenious method for key exchange. In *1978 Rivest*, *Shamir*, and *Adleman* discovered the first practical *public-key encryption* and signature scheme, now referred to as *RSA*. The *RSA* scheme is based on another hard mathematical problem, the intractability of factoring large integers.

One of the most significant contributions provided by public-key cryptography is the digital signature. In *1991* the first international standard for digital signatures (*ISO/IEC 9796 - International Organization for Standardization / International Electrotechnical Commission*) was adopted. It is based on the *RSA* public-key scheme. Regardless of who is involved, to one degree or another, all parties to a transaction must have confidence that certain objectives associated with information security have been met. Some of these objectives are listed in Table 1.1.

Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result.

Whereas information was typically stored and transmitted on paper, much of it now resides on magnetic media and is transmitted via telecommunications systems, some wireless. What has changed dramatically is the ability to copy and alter information.

What is needed then for a society where information is mostly stored and transmitted in electronic form is a means to ensure information security which is independent of the physical medium recording or conveying it and such that the objectives of information security rely solely on digital information itself. One of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing, to mention a few. This signature is intended to be unique to the individual and serve as a means to identify, authorize, and validate. With electronic information the concept of a signature needs to be redressed; it cannot simply be

| | |
|---|---|
| *Privacy or confidentiality* | keeping information secret from all but those who are authorized to see it |
| *Data integrity* | ensuring information has not been altered by unauthorized or unknown means |
| *Entity authentication or identification* | corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.) |
| *Message authentication* | corroborating the source of information; also known as data origin authentication |
| *Signature* | a means to bind information to an entity |
| *Authorization* | conveyance, to another entity, of official sanction to do or be something |
| *Validation* | a means to provide timeliness of authorization to use or manipulate information or resources |
| *Access control* | restricting access to resources to privileged entities |
| *Certification* | endorsement of information by a trusted entity |
| *Time stamping* | recording the time of creation or existence of information |
| *Witnessing* | verifying the creation or existence of information by an entity other than the creator |
| *Receipt* | acknowledgement that information has been received |
| *Confirmation* | acknowledgement that services have been provided |
| *Ownership* | a means to provide an entity with the legal right to use or transfer a resource to others |
| *Anonymity* | concealing the identity of an entity involved in some process |
| *Non-repudiation* | preventing the denial of previous commitments or actions |
| *Revocation* | retraction of certification or authorization |

Table 1.1: Objectives associated with information security

something unique to the signer and independent of the information signed.

There is, however, no guarantee that all of the information security objectives deemed necessary can be adequately met. The technical mean is provided through cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Of all the information security objectives listed in Table 1.1, the following four form a framework upon which the others will be derived:

- *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy.

- *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties.

- *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc.

- *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary.

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

# Chapter 2

# Attacking techniques

## 2.1 Physical Attacks on Smart Cards

The most obvious and direct attack on a smart card is a physical attack on the card itself. In the case of a stored-value card, this sort of attack may even be carried out by the owner of a card. Physical attacks attempt to reverse engineer the card and determine the secret key(s). Such attacks have been demonstrated in practice against commercial secure smart card chips, most notably by three groups of researchers: *Dan Boneh*, *Richard DeMillo*, and *Richard Lipton* of *Bellcore*; *Ross Anderson* of *Cambridge* and *Marcus Kuhn* of *Purdue*; and *Paul Kocher* and colleagues of *Cryptography Research, Inc.*

Tamper resistance is not absolute: an attacker with access to semiconductor test equipment can retrieve key material from a smart card controller by direct observation and manipulation of the chip's components. It is generally believed that, given sufficient investment, any chip-sized tamper resistant device can be penetrated in this way.

In [1] was pointed that *"smart cards are broken routinely"* and to the extent that their secure use requires tamper resistance, smart cards *"should be treated with circumspection"*. The paper describes a number of smart card attacks, many of which can be carried out by amateur attackers with very limited resources. Attacks described include voltage manipulation, temperature manipulation, chip removal (for easier probing), *UV* (*Ultra Violet*) light attacks, and microprobing.

More sophisticated attacks requiring professional equipment and materials involve uncovering the layers of a chip by etching, discerning chip behavior by advanced infrared probing, and reverse-engineering chip logic. The somewhat gloomy conclusion is that, at best, chip designers can only impose costs and delays on attackers, never providing guaranteed security. Many businesses that rely on smart card security realize this and do all they can to manage the risks prudently. Users should do the same. Some caveats: the *Anderson* and *Kuhn* [1] work is somewhat dated and is based on attacks carried out in the lab against conventional *micro-controllers*, which are usually much simpler than today's smart cards. *Micro-controllers* provide a great deal of open access to potential attackers since they are meant to be interactively programmed. For example, micro-controllers often provide an interface for external memory; generally speaking, smart cards don't have this feature. Thus they provide less of a beachhead for attacks.

## 2.2 Fault attacks

In [3] was pointed out that an adversary who can introduce computational errors into a smart card can deduce the values of cryptographic keys hidden in the smart card. The surprising part is that an attacker can do this even without precisely controlling the nature of the errors or even the exact timing of the errors. By comparing the result of an erroneous encryption with the result of a correct encryption of the same data, the attacker can learn something about the correct encryption key. By doing enough of these comparisons, the attacker can learn enough information to deduce the entire encryption key. Boneh et al. classified the faults into three categories. The first type are transient faults which can occur randomly causing a faulty computation to be executed. The second type are latent faults, which are hardware or software bugs that are difficult to locate. The third type are induced faults for which physical access to the hardware is necessary. These are the most interesting because of the active role of the attacker. For example, optical fault induction attacks, as introduced by Scorabogatov and Anderson [4], use a flashgun targeting a transistor to change the state of a memory cell in a microcontroller.

Fault attacks can be considered as the most dangerous implementation attacks as countermeasures usually include complex techniques which are not easy to implement on constrained environment such as smart cards.

In [5], this attack was generalized a technique called *"Differential Fault Analysis"*, which works against a wide range of cryptographic algorithms. The upshot of all this is that unless a smart card cryptography mechanism is very carefully designed, any secret keys stored inside the card might be extracted by a determined attacker.

## 2.3 Side-channel attacks

Cryptographic algorithms are building blocks of many security protocols and can be implemented both in software and hardware. Software solutions are cheaper and more flexible, while hardware implementations provide higher speed and intrinsic security. A trade-off in cost and speed can be achieved by hardware-software co-design.

Namely, attacks on cryptographic algorithms are usually divided into mathematical and implementation attacks. The latter are based on weaknesses in the implementation and can be passive or active. Passive attacks are also called side-channel attacks as they benefit from side channel information, which is collected by measuring some physical quantity. More precisely, while secret data are being processed they can be deduced by observing execution time, power consumption, electromagnetic radiation, etc. The second class of implementation attacks, i.e. the active attacks, is more invasive as they are based on the introduction of faults, which result in erroneous calculations leading to the exposure of the secret key. The usual cause of these faults can be sudden changes, i.e. glitches, in various parameters such as power supply, clock, temperature, etc. An attacker could also use a light flash with equipment such as a camera flash or a laser in order to induce a fault. Figure 2.1 is a conceptual diagram of side-channel attacks.

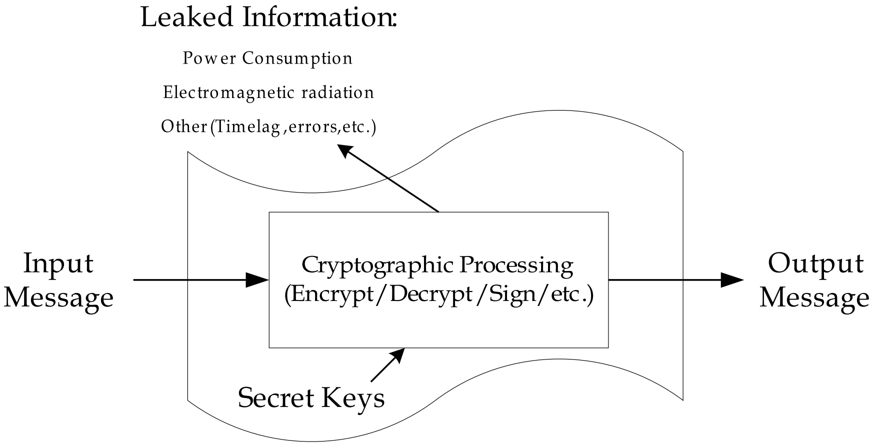

Leaked Information:
Power Consumption
Electromagnetic radiation
Other(Timelag,errors,etc.)
Input Message
Cryptographic Processing (Encrypt/Decrypt/Sign/etc.)
Output Message
Secret Keys

Figure 2.1: Side-channel attacks diagram

### 2.3.1 Timing attacks

Timing analysis attacks are based on the fact that algorithms with a nonconstant execution time can leak secret information. A non-constant execution time can be caused by conditional branches in the algorithm, various optimization techniques, cache hits, etc. Unlike power attacks, the use of these attacks is not restricted to cryptographic tokens. Timing attacks can also be applied to network based cryptosystems [2] and to other applications whenever the attacker can get hold of timing information. The obvious way to prevent timing attacks is to implement cryptographic algorithms with a constant execution time. Almost all modern implementations are resistant against timing attacks, which makes a timing-only attack impossible. However, the threat remains in combining timing information with other side-channels. For example, timing information can be used by an attacker in order to locate specific parts of the algorithm.

### 2.3.2 Power Analysis Foundations

In *1998*, researchers at *Cryptography Research Inc.*, led by *Paul Kocher*, publicly announced a new set of attacks against smart cards called *Power Analysis* (*PA*)

[6]. The *PA* can be carried out successfully against most smart cards currently in production.

The *PA* is a simple attack that relies on statistical inferences drawn on power consumption data measured during smart card computation. The equipment required to perform the *PA* is simple: a modified smart card reader and some off-the-shelf *PCs*. The algorithm itself is quite complex, but details have been widely published.

Chips inside a smart card use different amounts of power to perform different operations. By hooking a card up to an oscilloscope, a pattern of power consumption can be measured. Particular computations create particular patterns of spikes in power consumption. Careful analysis of the peaks in a power consumption pattern can lead to the discovery of information about secret keys used during cryptographic computations. Sometimes the analysis is straightforward enough that a single transaction provides sufficient data to steal a key. More often, thousands of transactions are required. The types of sensitive information that can leak include *PINs* and private cryptographic keys.

Possible solutions include masking power consumption with digital noise or throwing random calculations into the mix. Another potential solution is randomizing the order of card computations so that in the end, the same computation is performed using different patterns of primitives. All of these potential technological solutions are ways to mask the patterns in the power consumption of the card.

*DPA* is actually a variation on an earlier attack discovered by *Kocher*. The earlier attack exploited the fact that some operations require different amounts of time to finish, depending on which values they are computing. In the same way that *DPA* allows an attacker to piece together key information based on variations in power consumption, *Kocher*'s timing attack allows an attacker to piece together a key based on variations in the amount of computing time required to encrypt various values.

One thing to note is that legitimate users of smart cards don't have to worry too much about *DPA* or timing attacks, because the attack requires physical access to the card itself. Unless you lose your card or insert it directly into an attacker's machine, there is not much threat that your card itself will be cracked. The main risk that *DPA* presents is to companies that must concern themselves with widespread fraud of the sort carried out by organized crime.

The best approach is to assume information will leak from a smart card and design systems in such a way that they remain secure even in the face of leaking information. An approach of this sort may preclude smart card systems designed to do all processing offline without a centralized clearinghouse. Since increasingly confidential data are being exchanged on electronic way an ever greater importance is attached to the protection of the data. Where cryptosystems are being used in real applications not only mathematical attacks have to be taken into account. Hard and software implementations themselves present a vast field of attacks. *Side-Channel-Attacks* exploit information that leaks from a cryptographic device. Especially one of these new attacks has attracted much attention since it has been announced. This method is called *Differential Power Analysis* (*DPA*) and was presented in *1998* by *Cryptography Research Inc.*. *DPA* uses the information that naturally leaks from a cryptographic hardware device, namely the power consumption. A less powerful variant, the *Simple Power Analysis* (*SPA*) was also announced by *Cryptography Research Inc.*. What does a *DPA* attack require? First, an attacker must be able to precisely measure the power consumption. Second, the attacker needs to know what algorithm is computed, and third an attacker needs the plain or ciphertexts. The strategy of the attacker is to make a lot of measurements, and then divide them with the aid of some selection function into two or more different sets. Then, statistical methods are used to verify the selection function. If and only if the selection function was right, one can see noticeable peaks in the statistics.

Almost every digital circuit built today is based on *Complementary Metal Oxide Semiconductor* (*CMOS*) technology. Therefore it is necessary to understand the power consumption characteristics of this technology. If a *CMOS* gate changes its state, this change can be measured at the $V_{DD}$ ($V_{SS}$) pin. The more circuits change their state, the more power is dissipated. In a synchronous design, gates are *clocked*[1] which means that all gates change their state at the same time. Power dissipated by the circuit can be monitored by using a small resistor $R_m$ in series between $V_{DD}$, (or $V_{SS}$) and the true source (or ground). The two most essential parts of the power consumption during a change of a state are the dynamic charge resp. discharge (appr. 85%) and the dynamic short circuit current (appr. 15%). This is sketched on the example of an inverter (see Figure 2.2). The output of each gate has a capacitive load, consisting of the parasitic capacity of the connected wires and gates of the following stages. An input transition results in an output transition, which discharges or charges this parasitic capacity, causing a current flow to $V_{DD}$ (or $V_{SS}$). This current is the dynamic charge resp. discharge current. By measuring current flow on $V_{DD}$ we can detect whether the output changed from 0 to 1 or not.

In differential *CMOS* logic, every output appears also in its inverted form, which means a transition always causes charge and discharge on the output and inverted output. By measuring current on $V_{DD}$ or $V_{SS}$ one can't distinguish high and low transitions, but it is possible to detect whether a transition occurred or not. Logic with precharge characteristic always charges the output capacity during a precharge cycle and discharges it during the evaluation cycle, in case that the output value differs from the precharge value. By observing current flow, one can detect changes of the output node. Precharge logic has much higher power consumption than differential or standard *CMOS* logic, because dynamic charge current appears also in situations where the output value doesn't toggle.

[1] In electronics and synchronous digital circuits, such as most computers, a *clock signal* is a signal used to coordinate the actions of two or more circuits.

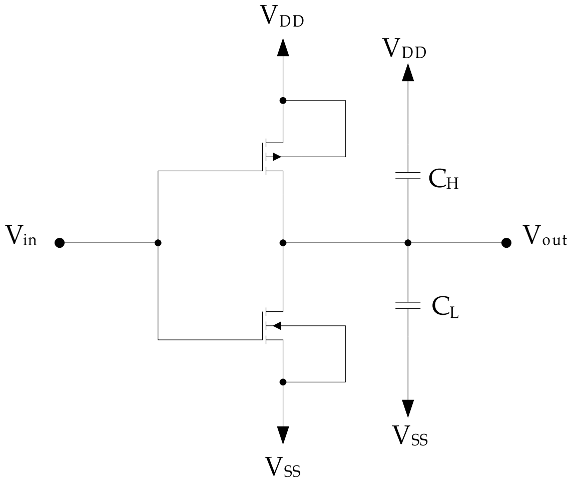


Figure 2.2: *CMOS* Inverter

### 2.3.3 Simple Power Analysis

Most modern cryptographic devices are implemented using semiconductor logic gates, which are constructed out of transistors. Electrons show across the silicon substrate when charge is applied to (or removed from) a transistor's gate, consuming power and producing electromagnetic radiation. To measure a circuit's power consumption, a small (e.g., *50* Ω) resistor is inserted in series with the power or ground input. The voltage difference across the resistor divided by the resistance yields the current. *Simple Power Analysis* (*SPA*) is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. *SPA* can yield information about a device's operation as well as key material.

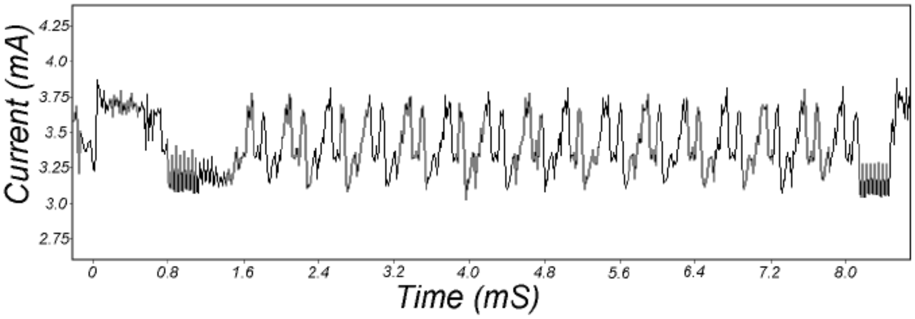


Figure 2.3: SPA trace from a typical smart card during a DES operation [6]

A trace refers to a set of power consumption measurements taken across a cryptographic operation. Figure 2.3 shows an *SPA* trace from a typical smart card as it performs a *DES* operation. Note that the *16 DES* rounds are clearly visible.

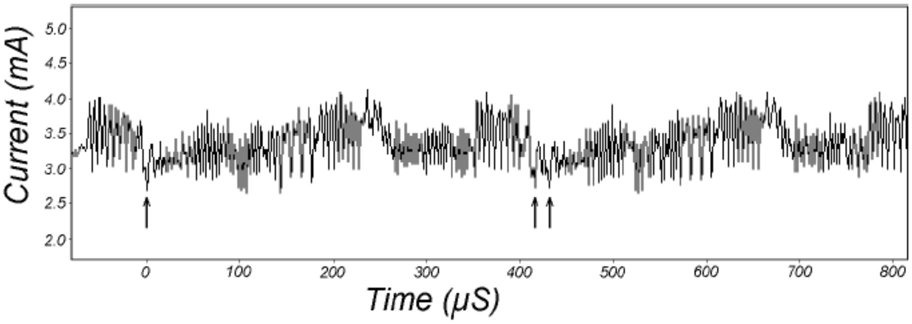


Figure 2.4: Detailed view of SPA trace [6]

Figure 2.4 is a more detailed view of the same trace showing the second and third rounds of a *DES* encryption operation. Many details of the DES operation are now visible. For example, the *28-bit DES* key registers *C* and *D* are rotated once in round 2 (*left arrow*) and twice in round 3 (*right arrows*). Figure 2.5 shows even higher resolution views of the trace showing power consumption through two regions, each of seven clock cycles at *3.5714 MHz*.

The upper trace in Figure 2.5 shows the execution path through an *SPA* feature where a jump instruction is performed, and the lower trace shows a case where the jump is not taken. The point of divergence is at clock cycle *6* and is clearly visible.

Because *SPA* can reveal the sequence of instructions executed, it can be used to break cryptographic implementations in which the execution path depends on the data being processed.

### 2.3.4 Differential power analysis

The *DES* (*Data Encryption Standard*) was invented in *1970* by *IBM*. It is an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of *DES*, the block size is *64 bits*. Before the main rounds, the block is divided into two *32-bit* halves and processed alternately. It has a *Feistel-Structure* and consists of *16* rounds:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

$$wheref(R_{i-1}, K_i) = P(S(E(R_{i-1} \oplus K_i)))$$

The *F-function*, depicted in Figure 2.7, operates on half a block (*32 bits*) at a time and consists of four stages:

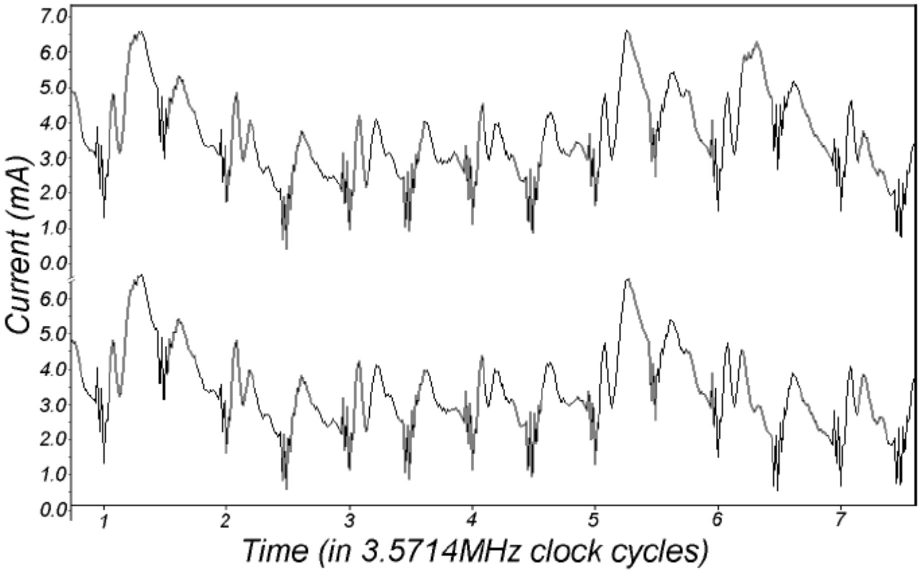


Figure 2.5: Detailed view of SPA trace [6]

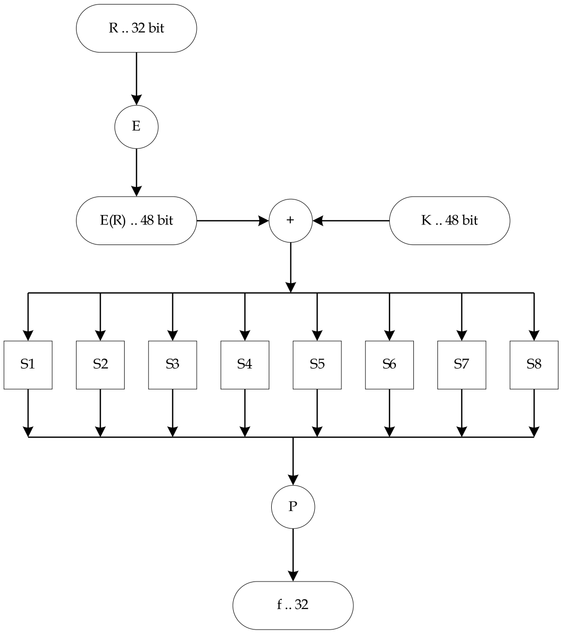


Figure 2.6: DES Algorithm

- *Expansion* - the *32-bit* half-block is expanded to *48* bits using the *expansion permutation*, denoted $E$ in the diagram, by duplicating some of the bits.

- *Key mixing* - the result is combined with a *subkey* using an *XOR* operation. Sixteen *48-bit* subkeys - one for each round - are derived from the main key.

- *Substitution* - after mixing in the subkey, the block is divided into eight *6-bit* pieces before processing by the *S-boxes*, or *Substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The *S-boxes* provide the core of the security of *DES* - without them, the cipher would be linear, and trivially breakable.

- *Permutation* - finally, the *32* outputs from the *S-boxes* are rearranged according to a fixed permutation, the *P-box*.

As stated before, in each of the 16 rounds, the DES encryption algorithm performs eight *S-box* lookup operations. The *8 S-boxes* each take as input six key bits *exclusive-ORed* with six bits of the $R$ register and produce four output bits. The *32* S-output bits are reordered and *exclusive-ORed* onto $L$. The halves $L$ and $R$ are then exchanged. The *DPA* selection function *D(C;b;Ks)* is defined as computing the value of bit $0 \leq b < 32$ of the *DES* intermediate $L$ at the beginning of the *16th* round for ciphertext $C$, where the *6* key bits entering the *S-box* corresponding to bit $b$ are represented by $0 \leq Ks < 2^6$.

To implement the *DPA* attack, an attacker first observes $m$ encryption operations and captures power traces $T_{1 \ldots m}[1 \ldots k]$ containing $k$ samples each. In addition, the attacker records the ciphertexts $C_{1 \ldots\ m}$. No knowledge of the plaintext is required. *DPA* analysis uses power consumption measurements to determine whether a key block guess *Ks* is correct. The attacker computes a k-sample differential trace $\Delta_D[1 \ldots k]$ by finding the difference between the average of the traces for which *D(C;b;Ks)* is one and the average of the traces for which *D(C;b;Ks)* is zero.

Thus $\Delta_D[j]$ is the average over $C_{1 \ldots m}$ of the effect due to the value represented by the selection function $D$ on the power consumption measurements at point $j$. If *Ks* is incorrect, the bit computed using $D$ will differ from the actual target bit for about half of the ciphertexts $C_i$. The selection function *D(Ci;b;Ks)* is thus effectively uncorrelated to what was actually computed by the target device. If a random function is used to divide a set into two subsets, the difference in the averages of the subsets should approach zero as the subset sizes approach infinity. If *Ks* is correct, however, the computed value for *D(Ci;b;Ks)* will equal the actual value of target bit $b$ with probability *1*. The selection function is thus correlated to the value of the bit manipulated in the *16th* round. As a result, the $\Delta_D[j]$ approaches the effect of the target bit on the power consumption as $m \to \infty$. Other data values, measurement errors, etc. that are not correlated to $D$ approach zero. Because power consumption is correlated to data bit values, the plot of $\Delta_D$ will be at with spikes in regions where $D$ is correlated to the values being processed.

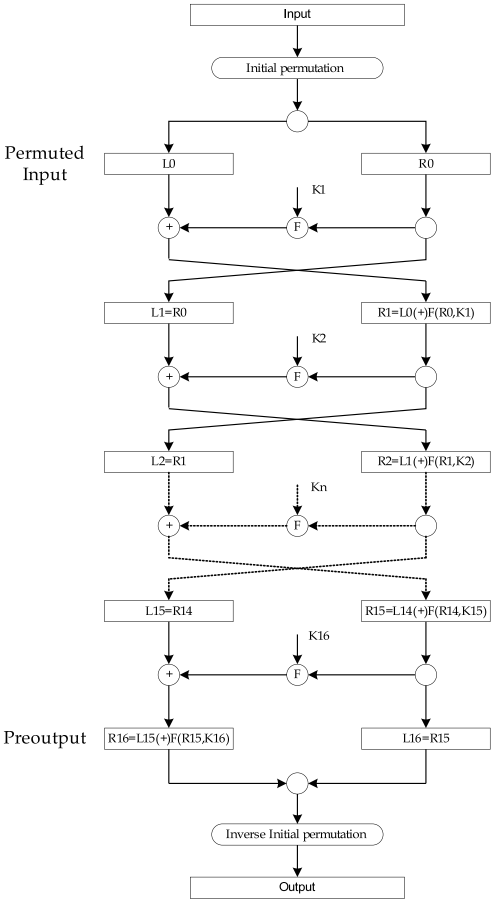


Figure 2.7: Data Encryption Standard (F-function)

The correct value of *Ks* can thus be identified from the spikes in its differential trace. Four values of *b* correspond to each *S-box*, providing confirmation of key block guesses. Finding all eight Ks yields the entire *48-bit* round subkey. The remaining *8* key bits can be found easily using exhaustive search or by analyzing one additional round. *DPA* can use known plaintext or known ciphertext and can find encryption or decryption keys.

Figure 2.8 shows four traces prepared using known plaintexts entering a *DES* encryption function on another smart card. On top is the reference power trace showing the average power consumption during *DES* operations. Below are three differential traces, where the first was produced using a correct guess for *Ks*. The lower two traces were produced using incorrect values for *Ks*.

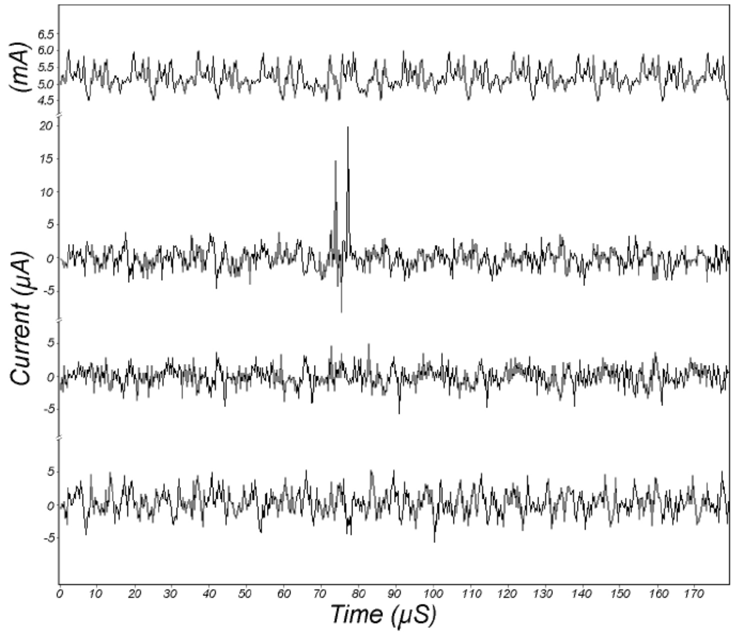


Figure 2.8: *DPA* traces for a DES encryption function [6]

Figure 2.9 shows the average effect of a single bit on detailed power consumption measurements. On top is a reference power consumption trace. The center trace shows the standard deviation in the power consumption measurements. Finally, the lower trace shows a differential trace prepared with $m = 10^4$. Note that regions that are not correlated to the bit are more than an order of magnitude closer to zero, indicating that little noise or error remains.

The size of the *DPA* characteristic is about $40\mu A$, which is several times less than the standard deviation observed at that point. The rise in the standard deviation at clock cycle *6* coinciding with a strong characteristic indicates that the operand value has a significant effect on the instruction power consumption and that there

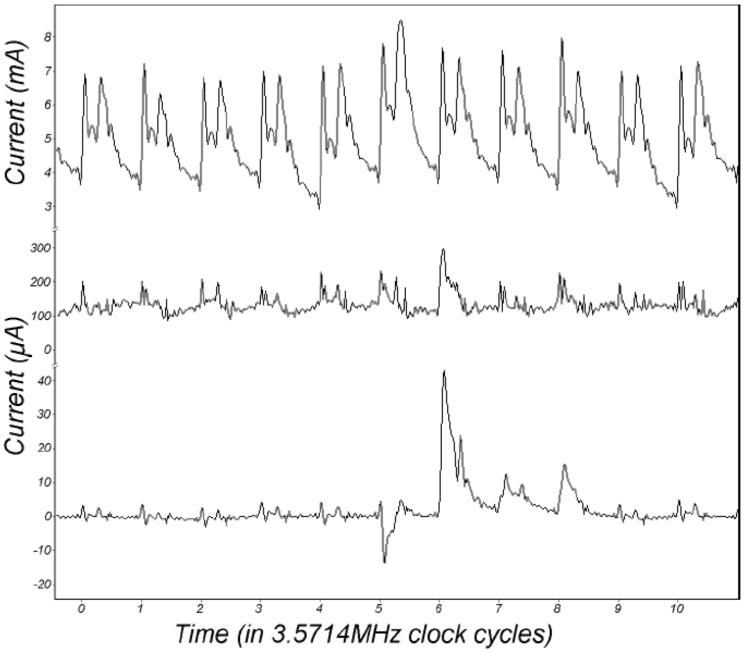


Figure 2.9: Average effect of a single bit on *DPA* attack [6]

is considerable variation in the operand values being manipulated.

Several sources introduce noise into *DPA* measurements, including electromagnetic radiation and thermal noise. Quantization errors due to mismatching of device clocks and sample clocks can cause additional errors. Finally, uncorrected temporal misalignment of traces can introduce a large amount of noise into measurements. Several improvements can be applied to the data collection and *DPA* analysis processes to reduce the number of samples required or to circumvent countermeasures.

## 2.4 Countermeasures

Techniques for preventing simple power analysis are generally fairly simple to implement. Avoiding procedures that use secret intermediates or keys for conditional branching operations will mask many *SPA* characteristics. In cases such as algorithms that inherently assume branching, this can require creative coding and incur a serious performance penalty. Also, the microcode in some microprocessors cause large operand-dependent power consumption features.

In the recent years, a wide spectrum of countermeasures against differential power analysis *DPA* have been proposed in the technical literature. In a classification which takes into account the involved abstraction level during the design flow, three classes can be defined: system-level, gate-level and transistor-level countermeasures.

System-level techniques include adding noise to the device power consumption [7], duplicating logics with complementary operations [8], active supply current filtering with power consumption compensation [9], passive filtering, battery on chip and detachable power supply [10]. Notice that some of the mentioned countermeasures have a pure theoretical interest since, with the current state of the art, their employment to design tamper resistant cryptographic devices (e.g. chipcard microcontrollers) is limited by technological and cost constraints. As gate-level countermeasures, techniques that can be implemented using logic gates available in a standard-cell library are intended, e.g. random masking [11], random pre-charging [12], state transitions and Hamming weight balancing, random delay insertion [13]. Random masking is the most studied but, as it has been recently proved [14],[15], implementations in an automatic synthesis flow starting from a *HDL* description, can be still attacked exploiting glitches generated in the combinatorial networks when the random masks are applied.

Finally, the transistor-level approach is based on the adoption of a logic style whose power consumption is constant or independent of the processed data. In a dual-rail pre-charge (*DRP*) logic style (e.g. *SABL* [16], *WDDL* [17], Dual-Spacer *DRP* [18]), signals are encoded as two complementary wires and power consumption is constant under the hypothesis that the differential outputs of each gate drive the same capacitive load. Dual-rail pre-charge logics are not affected by glitches but building two balanced wires requires a full-custom approach thus increasing design and maintenance costs.

Recently, semi-custom design flows with support differential logic families have been proposed in the technical literature. An approach based on a technique for the automatic routing of balanced complementary lines is reported in [19]. Even if an automatic place and route could sensibly reduce design time and increase the portability, the proposed balanced routing technique does not take into account the dependence of the capacitive load on a line on the logic state of the adjacent wires and, furthermore, introduces additional constraints for the routing tool thus limiting its efficiency and, likely, causing an area overhead especially if only few metal layers are available for the inter-cell routing (as it is the case in a chipcard where the top layers are reserved for shielding). Moreover, in a modern deep submicron technology, intra-chip process gradients cannot be neglected and they are the limiting factor for the load matching accuracy.

A second approach proposed in [20] is based on a masked dual-rail pre-charge logic style (*MDPL*) where, due to the random masking at the gate level, power consumption is randomized. Moreover, since *MDPL* is a dual-rail pre-charge logic, glitches are avoided but, at the same time, the complementary wires do not need to be balanced thus removing the main drawback of the dual-rail circuits. On the other hand, the authors report in [21] a significant penalty in terms of area and, above all, power consumption with respect to a *CMOS* implementation. In [22] is proposed a further approach to the design of a dual-rail pre-charge logic family which is insensitive to unbalanced load conditions thus allowing adopting a semi-custom design flow (automatic place & route) without additional constraints on the routing of the complementary wires.

The new concept is based on a three phase operation where an additional discharge phase is performed after the pre-charge/evaluation steps typical of any dynamic logic style. Although the concept is general, it can be implemented as an improvement of the *SABL* logic with a limited increase in circuit complexity.

# Chapter 3

# Supply and Current Measurement Probe

In this chapter, the design of the supply and current measurement probe (*SCM*) is described. Starting from a first version designed in a previous work [23], an enhanced circuit has been implemented and tested in a DPA attack.

## 3.1 First version: SCM

The starting point for a power analysis attack is the measurement of the instantaneous current consumption of the device under attack. In this work, an active probe for current measurement has been designed to be used to attack the implementation of encryption algorithms on a chip card.

The designed current probe can supply, and at the same time, measure the current consumption of the chip card. This technique shows several advantages with respect to a measurement with a resistance in series to the supply pin. Figure 3.1 shows the standard setup for a resistor-based measurement.

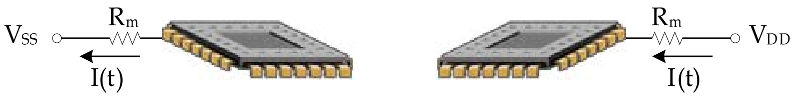


Figure 3.1: Current measurement with a resistor-based setup

The main drawbacks of this simple setup are the followings:

- The parasitic capacitance seen by the resistor introduces a time constant in the circuit that limits the measurement bandwidth. This effect can be neglected if the resistance $R$ has a very small value.

- On the other side, the resistance provides the signal amplification and therefore a trade-off between signal bandwidth and amplification is necessary. A too low value for $R$ can produce too noisy power consumption traces.

- Furthermore, the resistance causes a voltage drop, i.e. an insertion error, and the chip under measurement is supplied with:

$$V_{DD}^{*} = V_{DD} - R \cdot I(t)$$

The active current probe is designed to overcome the limitations of a resistor-based setup. The main features of the *SCM* are a low input impedance, high transimpedance gain and, at the same time, it can supply the chip under test. Figure 3.2 shows the schematic of a first version of the circuit which was presented in a previous work [23].

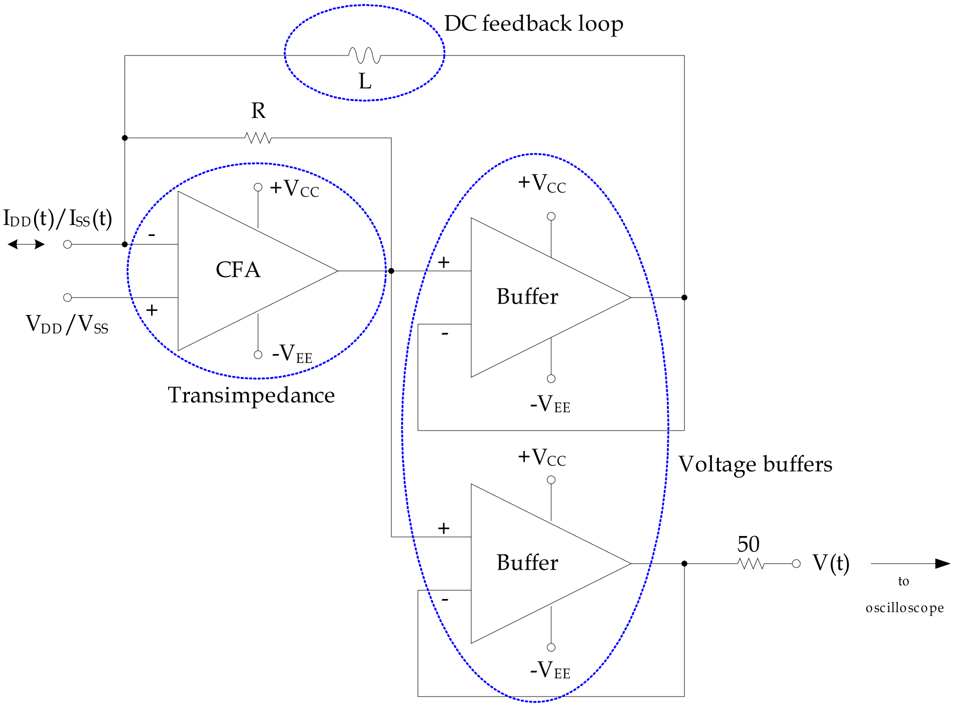


Figure 3.2: SCM general circuit

The main block is a transimpedance amplifier (*TZA*), which drives two voltage buffers, whose reference input is connected to a power supply, either $V_{DD}$ or $V_{SS}$ . The voltage read on the output resistance, due to the voltage partition on the 50Ω resistance, is:

$$V(t) = -\frac{R}{2} \cdot I_{DD}(t).$$

The gain is fixed by the feedback resistance that determines also the circuit stability. The value of the feedback resistance fixes the dynamic of the probe output as well.

Since the supply voltage for the circuit is $\pm 5V$ and the value of $R_F$ is fixed to $560\Omega$, the maximum current spike which can be measured with this probe is about *7mA*. This is quite a low value considering that a chip card is allowed to show current consumption spikes up to *100mA*.

This version of the current probe has been used to supply and measure the current consumption of an *Altera FPGA*[1] *MAX3000A* with a *3.3V* supply voltage. The buffers and the *TZA* are implemented with the *AD8009* from *Analog Device*. This *IC* (*Integrated Circuit*) features a *1GHz* maximum gain-bandwidth product and a *5500V/µs* slew rate.

The device under test is supplied by the probe throughout the upper buffer and the DC feedback loop closed by the inductance $L$. Therefore the probe can supply the measured device with a steady voltage $V_{DD}$ or $V_{SS}$. The measurement signal is derived from the lower buffer, to decouple the TZA from the load shown by the measurement instrument.

As a case study, the circuit shown in Figure 3.3 has been tested. It is a part of the *Serpent encryption algorithm* [24] and includes a *4* bit SBOX with the related output register, a *XOR* with a *4* bit key and a state machine that generates, in *256* clock transitions, a complete transition sequence on the *4* bit input data. The circuit has been synthesized on the FPGA MAX3000A starting from a *VHDL* description.

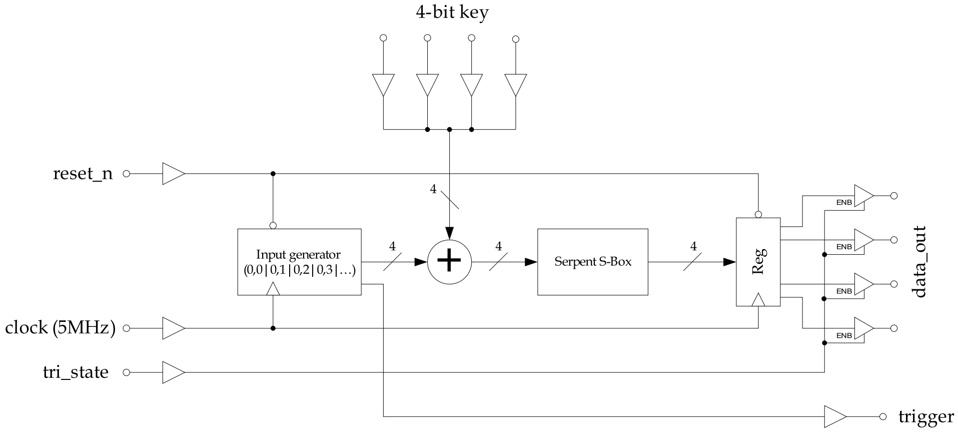


Figure 3.3: Serpent algorithmic

The same measurement has been performed using a resistor-based setup. Figure 3.4 shows that the resistor-base measurement produces spike output of about *50mV*.

[1] *A* ***Field Programmable Gate Array*** *or* ***FPGA*** *is a semiconductor device containing programmable logic components and programmable interconnections.*

This value is about *40* time lower than the value obtained using the *SCM*.

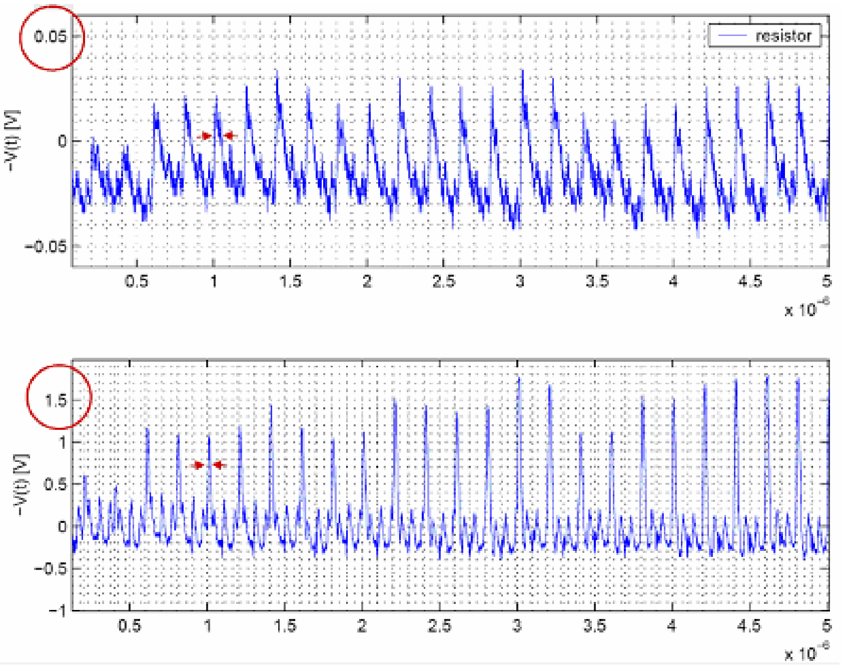


Figure 3.4: Comparison of experimental results obtained with both methods

The main features of the *SCM* circuit are summarized in Table 3.1..

| parameter | Value | Description |
|---|---|---|
| $R$ | $500\Omega$ | Transimpedance resistance |
| $TZA$ | $250V/A$ | Transimpedance gain |
| $BW$ | $> 300MHz$ | Bandwidth |
| $f_L$ | $\approx 1MHz$ | Low frequency cut |
| $+V_{CC}/-V_{EE}$ | $+5/-5V$ | *SCM* supply voltage |
| $+V_{CC}/-V_{SS}$ | $+3.3/0V$ | *FPGA* supply voltage |

Table 3.1: Main features of the SCM circuit

## 3.2 Second version: current probe

The next step consisted in the replacement of the *AD8009* component with a *THS3202* amplifier from *Texas Instruments*, due to the better performance of this components. The THS3202 features a gain-bandwidth product of *2GHz* and a slew rate of $9000V/\mu s$. The circuit has been simulated in *SPECTRE* and showed a very poor stability and high sensitivity to component parametric variations. The circuit was optimized by adding an *RC* input network, as shown in Figure 3.5. The transfer function was analyzed in *MATLAB*: the additional *RC* network introduces a pole at the same frequency of the dominant pole due to the *TZA* and one zero in the negative half plane.

This poles/zero placement can stabilize the circuit with a careful choice of the external components. However, the *THS3202* consists of two *TZA* amplifiers in the same chip and the isolation of the second *TZA* without performance and stability loss was an issue.

For these reasons, the current probe was modified by substituting the *THS3202* with a *THS3201* from *Texas Instruments* (gain-bandwidth product of *1.8GHz* and a slew rate of $10500V/\mu s$), and removing the DC feedback loop and the related voltage buffer. The new circuit is shown in Figure 3.5, where we can see the presence of decoupling capacitors on both *THS3201* inputs and in inductance to shunt the DC component of the current consumption under measurement. Since the measurement circuit is now decoupled from the circuit under test, it does not supply the device as before, but it can only measure its current consumption. This configuration can measure up to *25mA* current spikes and it is more stable than the version with *THS3202*.

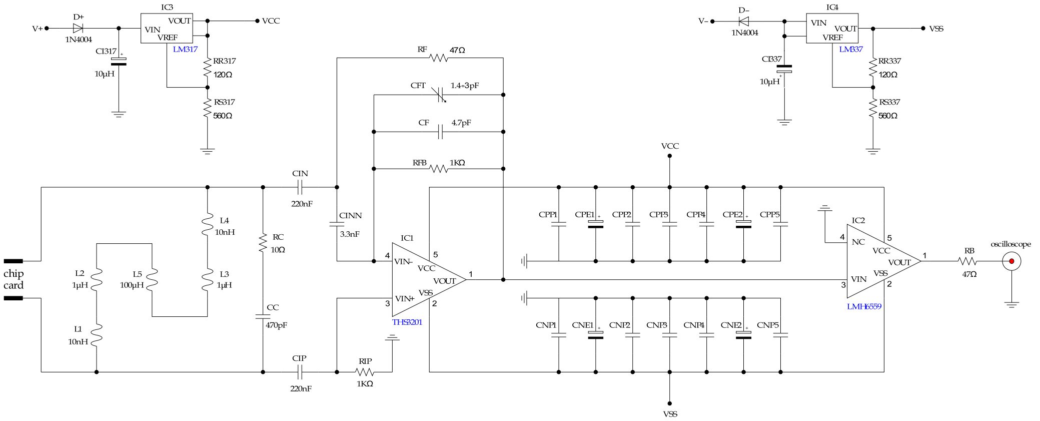


Figure 3.5: *SCM* Schematic of the second version

Another reason for the *DC* decoupling was also to isolate the different ground planes in the board from the ground of the chip under test, thus avoiding noises and spurious oscillations. Figure 3.6 show an *AC* simulation of *SCM* second version circuit.

The high frequency cut is placed at about *550MHz*, while the low frequency cut is at about *4MHz*. The following Figures show the impedance measured looking into the circuit input (measurement input): it results that the input impedance is under *5Ω* in a frequency range between *800KHz* and *600MHz*. This is a value low enough

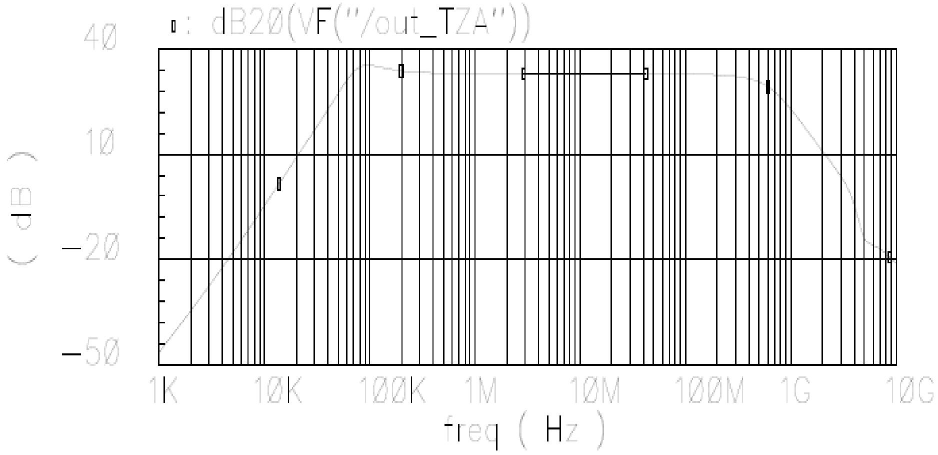


Figure 3.6: *AC* response of the second version

to avoid sensitive effects on the chip card during the current measurement.

## 3.3 Transfer function calculation

Figure 3.9 shows the circuit used for the transfer function calculation where the buffer and transimpedance amplifier are replaced with the respective functional models.

The circuit can be simplified by removing capacitors $C_{IN}$ and $C_{IP}$ since these are very large with respect to the other capacitors and their reactance is very low in the useful frequency range. Furthermore, we can simplify the calculation by neglecting the *TZA* output impedance. Figure 3.10 shows the simplified circuit.

The feedback resistance and capacitance show an impedance:

$$Z_{FB} = \frac{R_{FB}}{1 + sR_{FB}C_{FB}}; [Y_{FB} = \frac{1 + sR_{FB}C_{FB}}{R_{FB}}] \tag{3.1}$$

Similarly, input inductance and chip card load model are equivalent to an impedance:

$$Z_{IN} = \frac{sL_F}{1 + s^2L_FC_O}; [Y_{IN} = \frac{1 + s^2L_FC_O}{sL_F}] \tag{3.2}$$

The goal of the calculation is to write the *TZA* transfer function as ratio between output voltage $V_O$ and input current $I_{IN}$ generated by a test current source. The first step is to write equations at nodes A and B:

$$A) \ldots (V_B - V_A)sC_{INN} = V_AsC_{TZA} + (V_A - V_O)Y_{FB} \tag{3.3}$$

$$B) \ldots I_{IN} = V_BY_{IN} + (V_B - V_O)G_F + (V_B - V_A)sC_{INN} \tag{3.4}$$

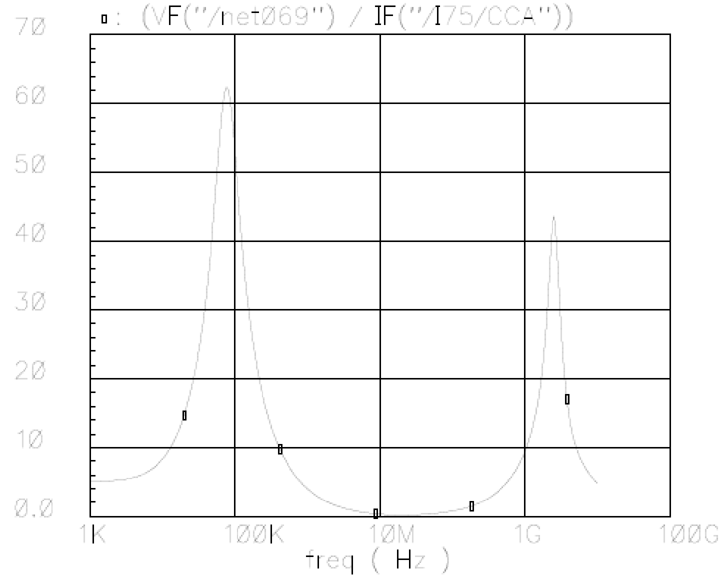


Figure 3.7: Input impedance

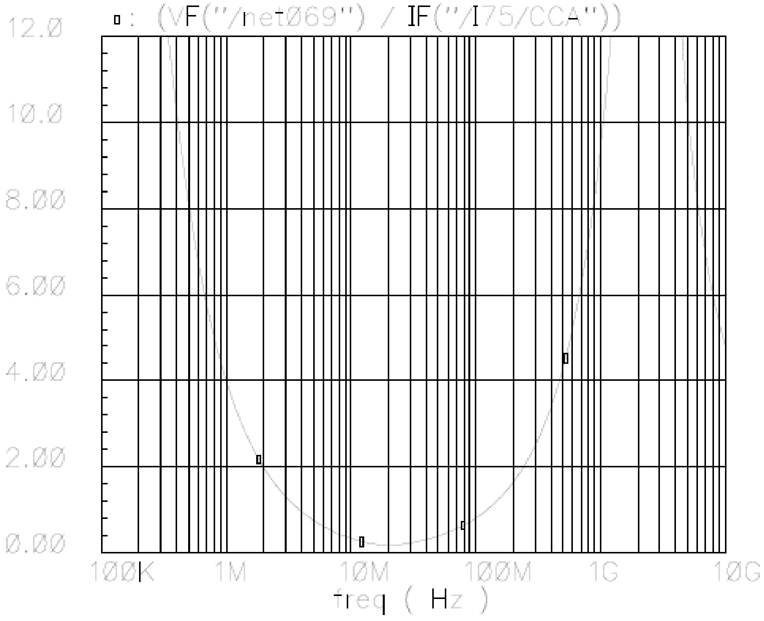


Figure 3.8: Zoomed input impedance in the useful frequency range

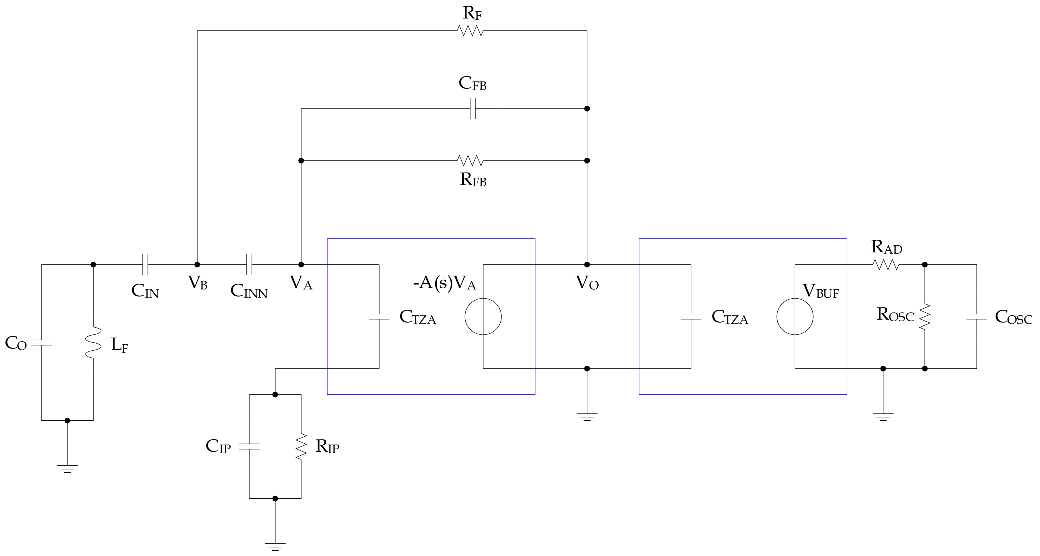


Figure 3.9: Circuit for calculation of the transfer function

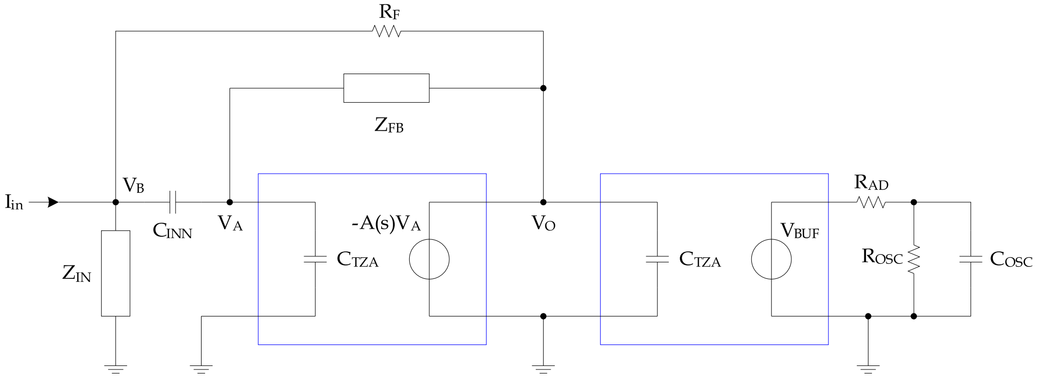


Figure 3.10: Simplified schematic for transfer function calculation

From the schematic, it holds that the output voltage is a function of node A voltage across the *TZA* open loop transfer function:

$$V_O = -A(s)V_A \rightarrow V_A = -\frac{V_O}{A(s)} \tag{3.5}$$

By substituting (3.5) in the equation relative to node A (3.3), it follows:

$$A)\ldots \left(V_B + \frac{V_O}{A(s)}\right) sC_{INN} = -\left(\frac{V_O}{A(s)}\right) sC_{TZA} - \left(\frac{V_O}{A(s)} + V_O\right) Y_{FB} \tag{3.6}$$

After some algebraic manipulations, we obtain the voltage in B:

$$V_B = -V_O \left[\frac{sR_{FB}C_{TZA} + sR_{FB}C_{INN} + 1 + sR_{FB}C_{FB} + A(s) + sR_{FB}C_{FB}A(s)}{R_{FB}A(s)}\right] \tag{3.7}$$

The same computation can be applied at node B, by substituting (3.5) in the node B equation (3.4), obtaining:

$$I_{IN} = V_B Y_{IN} + (V_B - V_O)G_F + \left(V_B + \frac{V_O}{A(s)}\right) sC_{INN} \tag{3.8}$$

By substituting (3.7) into (3.8), it follows:

$$\begin{aligned} I_{IN} = -V_O &\left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + (1 + A(s))(1 + sR_{FB}C_{FB})}{R_{FB}A(s)}\right] \cdot \\ &\cdot \left(\frac{1 + s^2 L_F C_O}{sL_F}\right) + \\ -V_O G_F &\left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + (1 + A(s))(1 + sR_{FB}C_{FB})}{R_{FB}A(s)} + 1\right] + \\ +V_O sC_{INN} &\left[\frac{1}{A(s)} - \left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + (1 + A(s))(1 + sR_{FB}C_{FB})}{R_{FB}A(s)}\right]\right] \end{aligned} \tag{3.9}$$

Dividing by the output voltage $V_O$ , we get the *TZA* transconductance:

$$\begin{aligned} \frac{I_{IN}}{V_O} = -&\left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + (1 + A(s))(1 + sR_{FB}C_{FB})}{R_{FB}A(s)}\right] \cdot \\ &\cdot \left[\frac{1 + s^2 L_F C_O}{sL_F} + G_F + sC_{INN}\right] - \frac{G_F}{R_{FB}A(s)} + \frac{sC_{INN}}{A(s)} \end{aligned} \tag{3.10}$$

For the *TZA* amplifier, for simplicity, we assume a single pole open loop transfer function:

$$A(s) = \frac{A_{v0}}{1 + \tau s} \tag{3.11}$$

By substituting (3.11) into the transfer function (3.10), we obtain:

$$\begin{aligned}\frac{I_{IN}}{V_O} = -\left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + \left(1 + \frac{A_{v0}}{1+\tau s}\right)(1 + sR_{FB}C_{FB})}{R_{FB}A_{v0}}\right] \cdot \\ \cdot \left[\frac{1 + sL_FG_F + s^2L_FC_O + s^2L_FC_{INN}}{sL_F}\right](1 + \tau s) + \\ + \left[\frac{sR_{FB}C_{INN} - G_F}{R_{FB}A(s)}\right]\end{aligned} \tag{3.12}$$

After some algebraic manipulations, it follows:

$$\begin{aligned}\frac{I_{IN}}{V_O} = -\left[\frac{sR_{FB}(C_{TZA} + C_{INN})(1 + \tau s) + (A_{v0} + 1 + \tau s)(1 + sR_{FB}C_{FB})}{R_{FB}A_{v0}}\right] \cdot \\ \cdot \left[\frac{s^2L_F(C_O + C_{INN}) + sL_FG_F + 1}{sL_F}\right] + \\ + \left[\frac{(sR_{FB}C_{INN} - G_F)(1 + \tau s)}{R_{FB}A(s)}\right]\end{aligned} \tag{3.13}$$

Multiplying the factors in brackets at the numerator in (3.13), we obtain the equation:

$$\begin{aligned}\left[\frac{sR_{FB}(C_{TZA} + C_{INN}) + s^2R_{FB}(C_{TZA} + C_{INN})\tau + 1 + sR_{FB}C_{FB} + s\tau}{R_{FB}A_{v0}} + \right. \\ \left. + \frac{s^2R_{FB}C_{FB}\tau + sR_{FB}C_{FB}A_{v0}}{R_{FB}A_{v0}}\right] \cdot \left[\frac{s^2L_F(C_O + C_{INN}) + sL_FG_F + 1}{sL_F}\right] + \\ + \left[\frac{sR_{FB}C_{INN} + s^2R_{FB}C_{INN}\tau - G_F - sG_F\tau}{R_{FB}A_{v0}}\right]\end{aligned} \tag{3.14}$$

To simplify the expressions, we define the variables:

$$C_\alpha = C_{INN} + C_{TZA} + C_{FB} \tag{3.15}$$

$$C_\beta = C_O + C_{INN} \tag{3.16}$$

Multiplying the factors in brackets at the numerator in (3.14), we have:

$$
\begin{aligned}
s^4 R_{FB} L_F C_\alpha C_\beta \tau + s^3 R_{FB} L_F G_F C_\alpha \tau + s^2 R_{FB} C_\alpha \tau + \\
+ s^3 L_F \left[ R_{FB} \left( C_\alpha + C_{FB} A_{v0} \right) + \tau \right] C_\beta + s^2 L_F G_F \left[ R_{FB} \left( C_\alpha + C_{FB} A_{v0} \right) + \tau \right] + \\
+ s \left[ R_{FB} \left( C_\alpha + C_{FB} A_{v0} \right) + \tau \right]
\end{aligned}
\tag{3.17}
$$

while the denominator in (3.14) is:

$$
s R_{FB} L_F A_{v0} \tag{3.18}
$$

We can further simplify the calculation by defining the variable:

$$
X_\gamma = \left[ R_{FB} \left( C_\alpha + C_{FB} A_{v0} \right) + \tau \right] \tag{3.19}
$$

Collecting the factors with the same s degrees and adding the factor previously neglected, we obtain:

$$
\begin{aligned}
\frac{s^4 R_{FB} L_F C_\alpha C_\beta \tau + s^3 (R_{FB} L_F G_F C_\alpha \tau + L_F X_\gamma) + s^2 (R_{FB} C_\alpha \tau + L_F G_F X_\gamma)}{s R_{FB} L_F A_{v0}} + \\
+ \frac{s X_\gamma}{s R_{FB} L_F A_{v0}} + \frac{s^2 R_{FB} C_{INN} \tau + s (R_{FB} C_{INN} - G_F \tau) - G_F}{R_{FB} A_{v0}}
\end{aligned}
\tag{3.20}
$$

From (3.20), for the numerator it follows:

$$
\begin{aligned}
s^4 R_{FB} L_F C_\alpha C_\beta \tau + s^3 L_F (R_{FB} G_F C_\alpha \tau + X_\gamma) + s^2 (R_{FB} C_\alpha \tau + L_F G_F X_\gamma) + \\
+ s X_\gamma + s^3 R_{FB} L_F C_{INN} \tau + s^2 L_F (R_{FB} C_{INN} - G_F \tau) - s L_F G_F
\end{aligned}
\tag{3.21}
$$

while at denominator we have:

$$
s R_{FB} L_F A_{v0} \tag{3.22}
$$

Finally, we obtain:

$$
\begin{aligned}
[NUM] = s^4 R_{FB} L_F C_\alpha C_\beta \tau + s^3 L_F \left[ R_{FB} (G_F C_\alpha + C_{INN}) \tau + X_\gamma \right] + \\
+ s^2 \left[ R_{FB} C_\alpha \tau + L_F \left[ R_{FB} C_{INN} + G_F (X_\gamma - \tau) \right] \right] + s (X_\gamma - L_F G_F)
\end{aligned}
\tag{3.23}
$$

$$
[DEN] = s R_{FB} L_F A_{v0} \tag{3.24}
$$

$$\frac{I_{IN}}{V_O} = \frac{[NUM]}{[DEN]} = Y \tag{3.25}$$

Since we are interested in the $TZA$ transimpedance, by inverting the last expression, it follows:

$$\frac{V_O}{I_{IN}} = \frac{[DEN]}{[NUM]} = TZA \tag{3.26}$$

which can be written as:

$$\frac{sa_1 + a_0}{s^4 b_4 + s^3 b_3 + s^2 b_2 + sb_1 + b_0} \tag{3.27}$$

$$a_0 = b_0 = 0 \tag{3.28}$$

$$a_1 = R_{FB} L_F A_{v0} \tag{3.29}$$

$$b_1 = X_\gamma - L_F G_F \tag{3.30}$$

$$b_2 = R_{FB} C_\alpha \tau + L_F [R_{FB} C_{INN} + G_F (X_\gamma - \tau)] \tag{3.31}$$

$$b_3 = L_F [R_{FB} (G_F C_\alpha + C_{INN}) \tau + X_\gamma] \tag{3.32}$$

$$b_4 = R_{FB} L_F C_\alpha C_\beta \tau \tag{3.33}$$

## 3.4 Small signal analysis

Figure 3.11 shows the small signal circuit, obtained short-circuiting the capacitors. Since the inductor admittance is infinite in the useful range frequency, we can neglect it.

Firstly, we analyze the part of circuit related to output buffer. We want to calculate the buffer transfer function. The node $O$ equation is:

$$O) \ldots (v_O - v_B) g_{IBUF} = [v_B - A_{VBUF}(v_O - v_B)] g_{OBUF} + v_B \left( \frac{g_{AD} g_{OSC}}{g_{AD} + g_{OSC}} \right) \tag{3.34}$$

Multiplying the factors we have:

$$\begin{aligned} v_O g_{IBUF} - v_B g_{IBUF} = {} & v_O g_{OBUF} - v_O A_{VBUF} g_{OBUF} + \\ & + v_B A_{VBUF} g_{OBUF} + v_B \left( \frac{g_{AD} g_{OSC}}{g_{AD} + g_{OSC}} \right) \end{aligned} \tag{3.35}$$

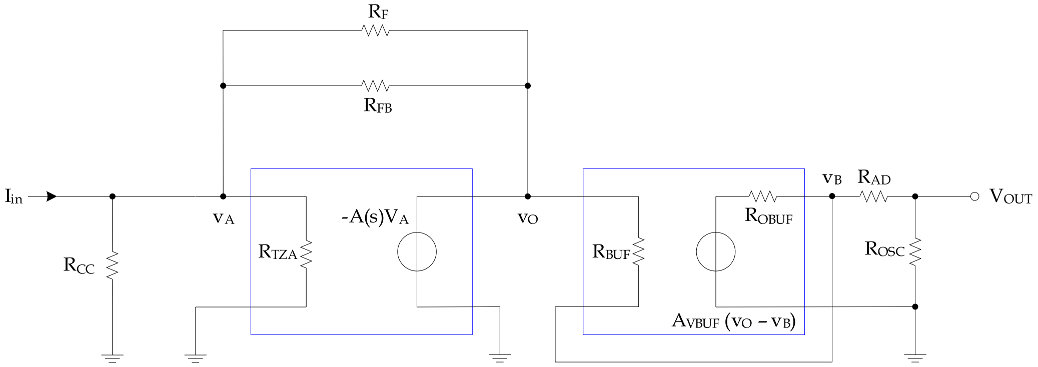


Figure 3.11: Small signal circuit for SCM second version

By collecting the factors in (3.35), we obtain:

$$
\begin{aligned}
&v_O(g_{IBUF} - g_{OBUF} + A_{VBUF}g_{OBUF}) = \\
&= v_B\left(g_{IBUF} + A_{VBUF}g_{OBUF} + \frac{g_{AD}g_{OSC}}{g_{AD} + G_{OSC}}\right)
\end{aligned} \tag{3.36}
$$

The output buffer's transfer function, which is a voltage gain, is given by the ratio between the output and input voltage. This gain has a value close to 1, as we expect:

$$
A^{CL}_{VBUF} = \frac{v_B}{v_O} = \frac{g_{IBUF} + A_{VBUF}g_{OBUF} - g_{OBUF}}{g_{IBUF} + A_{VBUF}g_{OBUF} + \frac{g_{AD}g_{OSC}}{g_{AD}+g_{OSC}}} \cong 1 \tag{3.37}
$$

The buffer input impedance is:

$$
G^{CL}_{IBUF} = \frac{i_{BUF}}{v_O} = \frac{(v_O - v_B)g_{IBUF}}{v_O} \tag{3.38}
$$

$$
G^{CL}_{IBUF} = \left(1 - \frac{v_B}{v_O}\right)g_{IBUF} = \left[1 - \left(\frac{g_{IBUF} + A_{VBUF}g_{OBUF} - g_{OBUF}}{g_{IBUF} + A_{VBUF}g_{OBUF} + \frac{g_{AD}g_{OSC}}{g_{AD}+g_{OSC}}}\right)\right]g_{IBUF} \tag{3.39}
$$

By substituting (3.37) into (3.38), we have:

$$
G^{CL}_{IBUF} = \left(\frac{\frac{g_{AD}g_{OSC}}{g_{AD}+g_{OSC}} + g_{OBUF}}{g_{IBUF} + A_{VBUF}g_{OBUF} + \frac{g_{AD}g_{OSC}}{g_{AD}+g_{OSC}}}\right)g_{IBUF} \tag{3.40}
$$

Simplifying the factors at the numerator in (3.40) and looking for the most significant one, with respect to the other factors at denominator, for the buffer input impedance it follows:

$$G^{CL}_{IBUF} \cong \frac{g_{OBUF} g_{IBUF}}{A_{VBUF} g_{OBUF}} = \frac{g_{IBUF}}{A_{VBUF}} \rightarrow 0 \Rightarrow R^{CL}_{IBUF} \rightarrow \infty \tag{3.41}$$

The transimpedance can calculated with reference to a parallel-parallel feedback model, as shown in Figure 3.12.

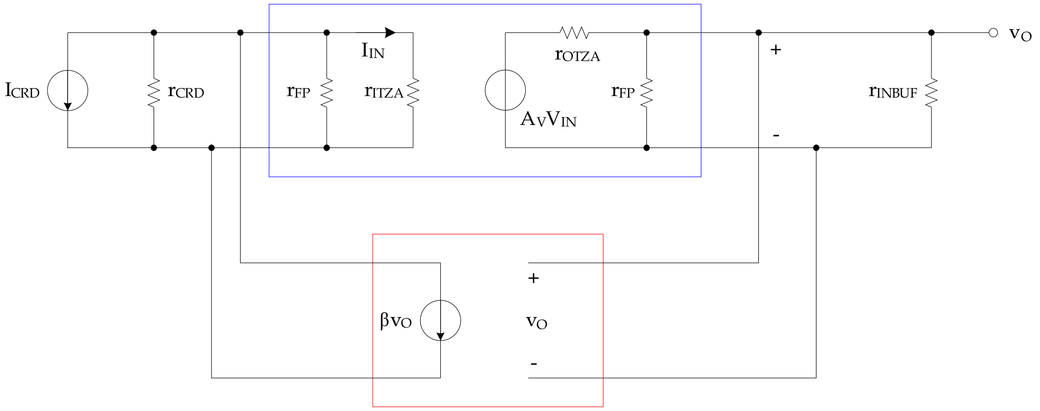


Figure 3.12: Block model for the parallel-parallel feedback

We can simplify the schematic moving the load effect of the feedback block to the input and output of the direct amplification block. Figure 3.13 shows the new circuit, where:

$$r^{‘}_{ITZA} = r_{ITZA} // r_{FP} \tag{3.42}$$

$$r^{‘}_{OTZA} = r_{OTZA} // r_{FP} \tag{3.43}$$

$$\beta = \frac{1}{r_{FP}} \tag{3.44}$$

The transfer function of the new network is calculated starting from the value of output voltage:

$$v_O = A_{VTZA} v_{IN} \left( \frac{r_{FP}}{r_{FP} + r_{OTZA}} \right) \tag{3.45}$$

The new value for the voltage gain of the direct amplifier is:

$$A^{‘}_{VTZA} = \frac{v_O}{v_{IN}} = A_{VTZA} \left( \frac{r_{FP}}{r_{FP} + r_{OTZA}} \right) \tag{3.46}$$

The controlled generator at the output is a function of the input voltage and we have:

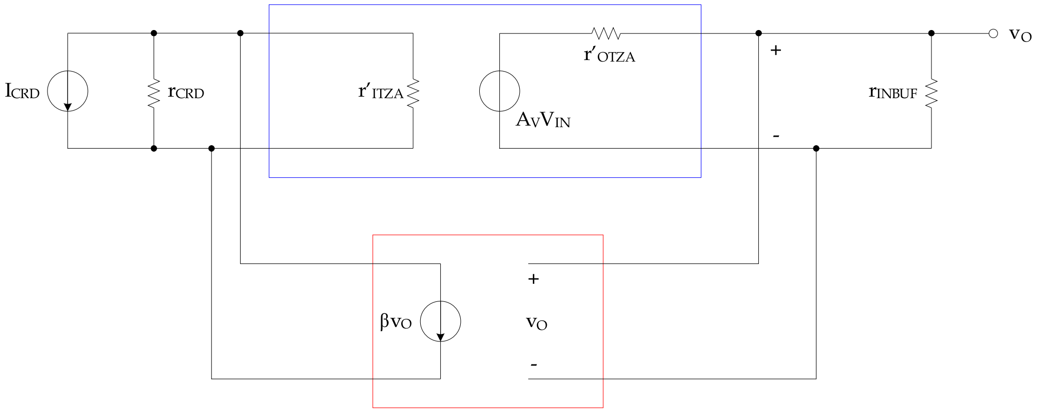


Figure 3.13: Schematic block with load effect in the direct amplification block

$$v_{IN} = i_{IN}(r_{FP}//r_{ITZA}) \tag{3.47}$$

By substituting (3.47) into (3.45), we obtain the new value for the trans - impedance:

$$v_O = A_{VTZA} i_{IN}(r_{FP}//r_{ITZA}) \left( \frac{r_{FP}}{r_{FP} + r_{OTZA}} \right) = A^{‘}_{VTZA} i_{IN}(r_{FP}//r_{ITZA}) \tag{3.48}$$

$$TZA^{‘} = \frac{v_O}{i_{IN}} = A^{‘}_{VTZA}(r_{FP}//r_{ITZA}) \tag{3.49}$$

The second step of the analysis is the calculation of the output loaded transimpedance, by calculating the output voltage in presence of buffer:

$$v_O = A^{‘}_{VTZA} v_{IN} \left( \frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}} \right) \tag{3.50}$$

Once again, the new voltage gain value is:

$$A^{“}_{VTZA} = \frac{v_O}{v_{IN}} = A^{‘}_{VTZA} \left( \frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}} \right) \tag{3.51}$$

By substituting (3.47) in (3.50), we have the loaded transimpedance:

$$v_O = A^{‘}_{VTZA} i_{IN}(r_{FP}//r_{ITZA}) \left( \frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}} \right) = A^{“}_{VTZA} i_{IN}(r_{FP}//r_{ITZA}) \tag{3.52}$$

$$TZA^{‘}_{L} = \frac{v_{O}}{i_{IN}} = A^{“}_{VTZA}(r_{FP}//r_{ITZA}) =$$

$$= A^{‘}_{VTZA}\left(\frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}}\right)(r_{FP}//r_{ITZA}) = TZA^{‘}\left(\frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}}\right) \tag{3.53}$$

Now we can consider even the input load, which is represented by the chip card resistance. Then we will obtain the new value for the *TZA* input impedance:

$$r^{“}_{ITZA} = r^{‘}_{ITZA}//r_{CRD} \tag{3.54}$$

The output voltage is similar to (3.50) and it is obtained by substituting the new gain value (3.51):

$$v_{O} = A^{‘}_{VTZA}v_{IN}\left(\frac{r_{IBUF}}{r^{‘}_{OTZA} + r_{IBUF}}\right) \tag{3.55}$$

On the other side, since the input network is a parallel connection, for the *TZA* input current we have:

$$i_{CRD} = i_{ITZA}r^{“}_{ITZA} + \beta v_{O} \tag{3.56}$$

$$i_{TZA} = i_{CRD} - \beta v_{O} \tag{3.57}$$

The *TZA* input voltage is:

$$v_{IN} = (i_{CRD} - \beta v_{O})r^{“}_{ITZA} \tag{3.58}$$

By substituting (3.58) and using the new input impedance value represented by (3.54), for the output voltage it follows:

$$v_{O} = A^{“}_{VTZA}(i_{CRD} - \beta v_{O})r^{“}_{ITZA}\left(\frac{r_{IBUF}}{r_{IBUF} + r^{‘}_{OTZA}}\right) \tag{3.59}$$

We can separate the factors related to voltage and current. In this way we obtain the new transimpedance value which is close to the total feedback resistance:

$$v_{O}\left[1 + \beta A^{“}_{VTZA}r^{“}_{ITZA}\left(\frac{r_{IBUF}}{r_{IBUF} + r^{‘}_{OTZA}}\right)\right] = A^{“}_{VTZA}i_{CRD}r^{“}_{ITZA}\left(\frac{r_{IBUF}}{r_{IBUF} + r^{‘}_{OTZA}}\right) \tag{3.60}$$

$$TZA^{“} = \frac{v_{O}}{i_{CRD}} = \frac{A^{“}_{VTZA}r^{“}_{ITZA}\left(\frac{r_{IBUF}}{r_{IBUF}+r^{‘}_{OTZA}}\right)}{1 + \beta A^{“}_{VTZA}r^{“}_{ITZA}\left(\frac{r_{IBUF}}{r_{IBUF}+r^{‘}_{OTZA}}\right)} \cong \frac{1}{\beta} = r_{FP} \tag{3.61}$$

Finally, considering the output matching network, the oscilloscope input voltage is:

$$v_{ICABLE} = v_O \left( \frac{r_{OSC}}{r_{OSC} + r_{AD}} \right) \tag{3.62}$$

The conclusion is that the whole transfer function, with $r_{OSC} = r_{AD}$, is:

$$TZA_{TOT} = \frac{v_{ICABLE}}{i_{CRD}} \cong r_{FP} \left( \frac{r_{OSC}}{r_{OSC} + r_{AD}} \right) = \frac{r_{FP}}{2} \tag{3.63}$$

For the *TZA* closed loop input impedance, we can connect one voltage test source at the input and close with a short circuit the output. Figure 3.14 shows the schematic for the closed loop transfer function calculation.

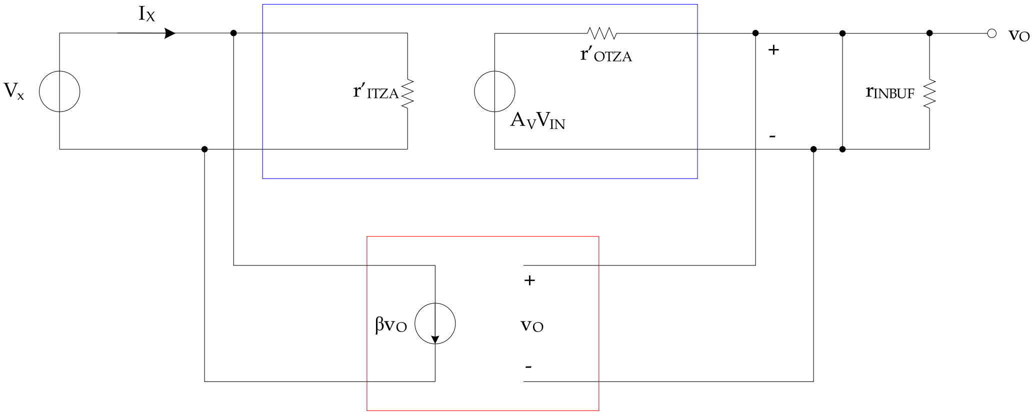


Figure 3.14: Equivalent block diagram for the calculation of the input impedance

At the input node we have:

$$I_X = i_{IN} + \beta v_O \tag{3.64}$$

while the tail current in the *TZA* input impedance is:

$$i_{IN} = \frac{V_X}{r^{\text{‘}}_{ITZA}} \tag{3.65}$$

For the output voltage controlled source we have:

$$v_O = A^{\text{‘}}_{VTZA} v_{IN} = A^{\text{“}}_{VTZA} V_X \tag{3.66}$$

By substituting (3.66) into (3.64), we obtain:

$$I_X = A^{\text{“}}_{VTZA} \beta V_X + \frac{V_X}{r^{\text{‘}}_{ITZA}} \tag{3.67}$$

Finally, we can calculate the *TZA* closed loop input impedance whose value is, as expected, very low:

$$\frac{V_X}{I_X} = R^{CL}_{ITZA} = \frac{r^{`}_{ITZA}}{1+\beta A^{``}_{VTZA} r^{`}_{ITZA}} = \frac{r^{`}_{ITZA}}{1+\beta TZA^{`}_{L}} \tag{3.68}$$

The following figures show the transient response for three current pulses of *1mA*, *10mA* and *100mA* amplitude respectively. In each plot, the upper trace is the buffer output, the middle trace is the *TZA* output and the lower trace is the input current pulse [2].

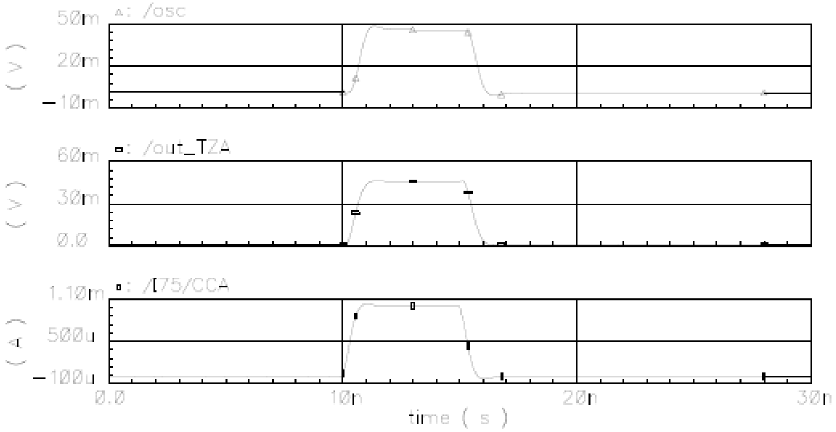


Figure 3.15: Transient response for $i_p$ = *1mA*

Figure 3.18 and Figure 3.19 shows the final *SCM* probe mounted on a six layers *PCB*.

## 3.5 Stability analysis

In this section, the stability of the *SCM* is discussed, assuming a simple model for the transimpedance amplifier. Figure 3.20 shows a small signal circuit for the stability analysis, where the load (chip card) is modeled as a capacitance and a resistance. Capacitor $C_L$ represents the capacitance seen on the power supply pad of the chip under measure while, resistor $R_L$, represents the resistance of the interconnection between *SCM* and supply pad. The voltage at the input node is called $V_I$ while, the voltage at the output node is $V_O$.

The schematic can be simplified defining the following impedances:

$$Z_L = R_L + \frac{1}{sC_L} = \frac{1+sR_LC_L}{sC_L} \tag{3.69}$$

[2] The current pulses represent the spike consumption of the chip card during an encryption operation.

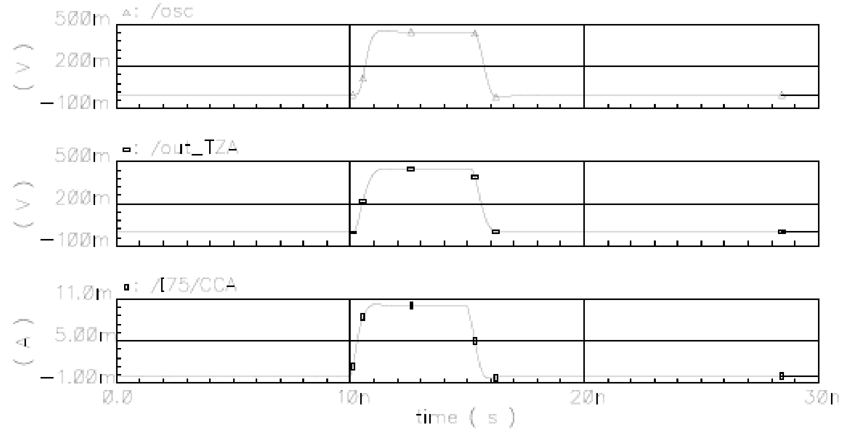


Figure 3.16: Transient response for $i_p$ = *10mA*

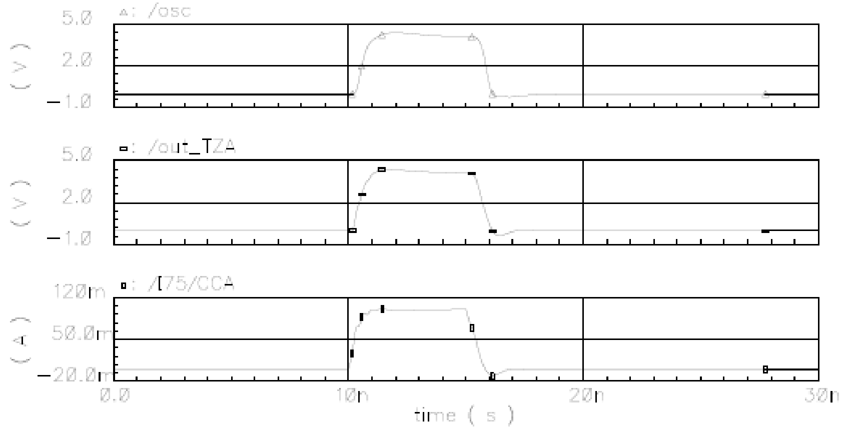


Figure 3.17: Transient response for $i_p$ = *100mA*

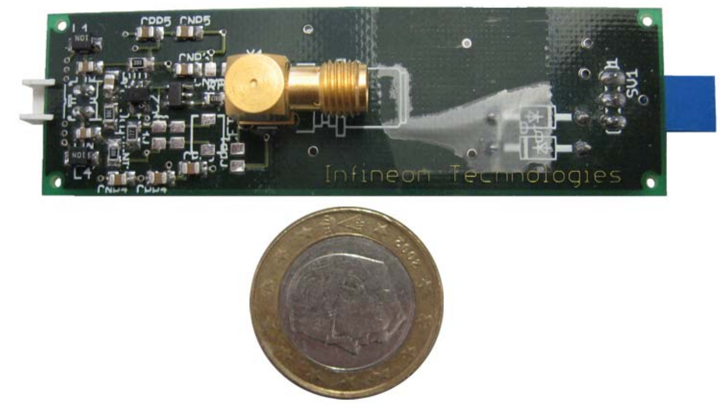


Figure 3.18: Front view of SCM second version

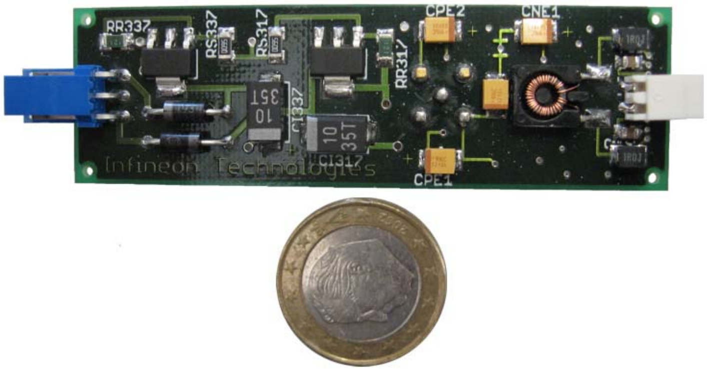


Figure 3.19: Back view of SCM second version

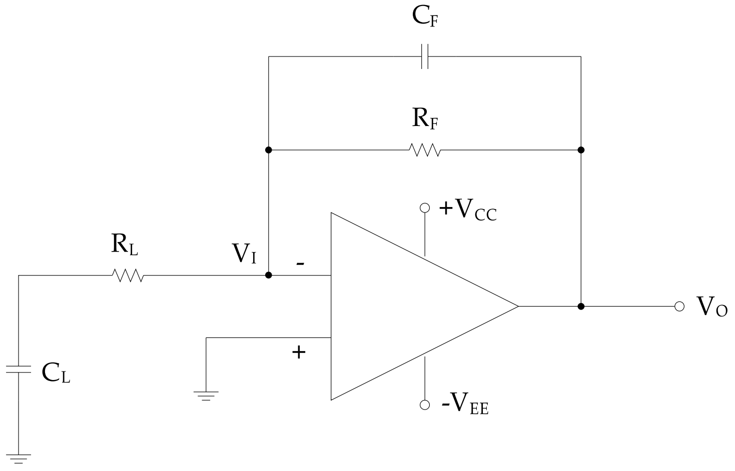


Figure 3.20: Circuit for stability analysis

$$Z_F = \frac{\frac{R_F}{sC_F}}{R_F + \frac{1}{sC_F}} = \frac{R_F}{1 + sR_FC_F} \tag{3.70}$$

With these definitions, the new schematic is shown in Figure 3.21.

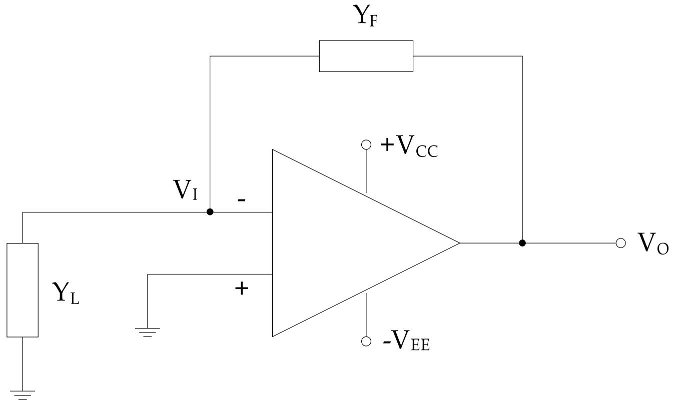


Figure 3.21: Simplified circuit for stability analysis

Breaking the loop we can calculate the open loop gain (Figure 3.22).

Figure 3.23 shows the new schematic with the loop open.

The current loop equations relate to the input and output loop are given below along with the equation relating $I_1$ e $I_2$:

$$V_{TI} = I_2(Z_F + Z_L//Z_B) \tag{3.71}$$

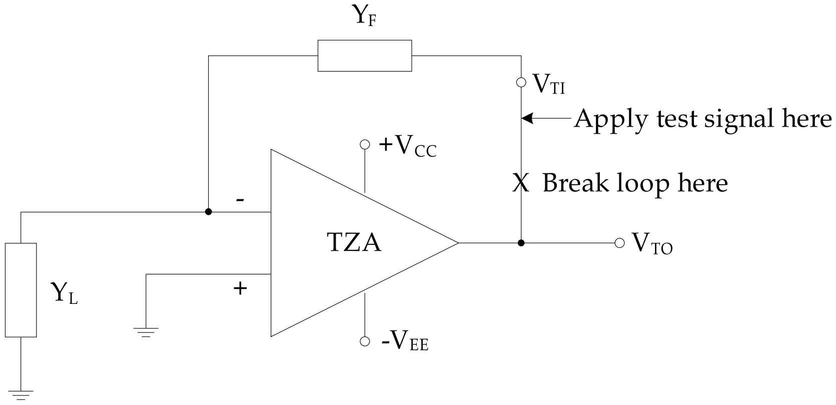


Figure 3.22: Break loop for open loop gain analysis

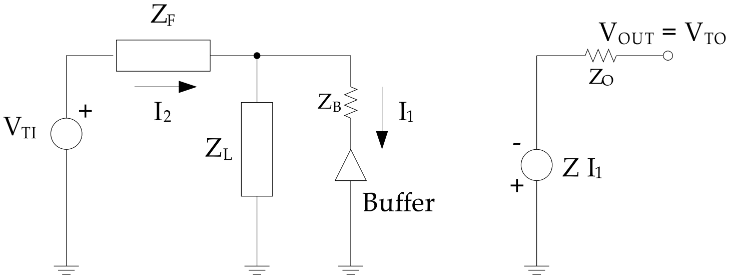


Figure 3.23: Schematic with loop open

$$V_{TO} = ZI_1 \tag{3.72}$$

$$I_1 = I_2\left(\frac{Z_L}{Z_L + Z_B}\right) \tag{3.73}$$

We will assume a unity gain buffer ($G_B = 1$). From the relation between $I_1$ and $I_2$, we obtain:

$$V_{TI} = I_1\left(\frac{Z_L + Z_B}{Z_L}\right)(Z_F + Z_L//Z_B) \tag{3.74}$$

From (3.72) we obtain:

$$V_{TI} = \left(\frac{V_{TO}}{Z}\right)\left(\frac{Z_L + Z_B}{Z_L}\right)(Z_F + Z_L//Z_B) \tag{3.75}$$

The open loop gain is given by:

$$\frac{V_{TO}}{V_{TI}} = \left(\frac{Z_L Z}{Z_L + Z_B}\right)\left(\frac{1}{Z_F + Z_L//Z_B}\right) \tag{3.76}$$

Simplifying the last expression, it follows:

$$\frac{V_{TO}}{V_{TI}} = \frac{Z}{Z_F\left(1 + \frac{Z_B}{Z_F//Z_L}\right)} \tag{3.77}$$

We will consider the open loop gain how the ratio between two transfer functions, $Z$ and $SYS$, where $SYS$ is the numerator of the open loop gain equation:

$$\frac{V_{TO}}{V_{TI}} = \frac{Z}{SYS} \tag{3.78}$$

From (3.69) and (3.70), it follows:

$$Z_F//Z_L = \frac{R_F(1 + sR_LC_L)}{(1 + sR_FC_F)(1 + sR_LC_L) + sR_FC_L} \tag{3.79}$$

At the denominator we have:

$$\begin{aligned} SYS_{NUM} = s^2R_F^2C_FR_LC_LZ_B + \\ +sR_F[R_LR_FC_L + Z_B[R_F(C_L + C_F) + R_LC_L]] + \\ +R_F(R_F + Z_B) \end{aligned} \tag{3.80}$$

while the numerator is:

$$SYS_{DEN} = s^2R_F^2R_LC_LC_F + sR_F(R_FC_F + R_LC_L) + R_F \tag{3.81}$$

After these steps the $SYS$ function is given by:

$$SYS = \frac{SYS_{NUM}}{SYS_{DEN}} \tag{3.82}$$

We will consider the Z function as a two pole transfer function:

$$Z = \frac{K}{(1 + \tau_1 s)(1 + \tau_2 s)} \tag{3.83}$$

where:

$$\begin{aligned} K &= 10^6 \\ \tau_1 &= 10^{-8} \\ \tau_2 &= 10^{-9} \end{aligned}$$

This transfer function has been simulated with the *MATLAB* script listed in Appendix D, where the transfer function is given as ratio between the $Z$ function and the $SYS$ function.

This first simulation refers to the circuit without additional compensation components. The following values have been assumed for the circuit components:

$$\begin{aligned} R_L &= 10\Omega \\ C_L &= 50pF \\ R_F &= 330\Omega \\ C_F &= 3pF \\ Z_B &= 11\Omega \end{aligned}$$

Figure 3.24 shows the bode plot for the open loop gain transfer function. As we can see, the phase shift reaches $-180°$ before the amplitude falls below 0dB. It is also clearly visible a peak in the amplitude response. That shows that the system is unstable.

In addition, Figure 3.25 shows the root locus of the open loop gain. Also in this case, we can see that the pole moves into the positive half plane (red and green arcs), so the system is unstable.

The Figure 3.26 shows the same schematic as before, where a compensator capacitance $C_C$ and a resistance $R_C$ at the input has been added.

We have the same form for the open loop gain equation as in (3.77), but in this case we have:

$$Z_L' = Z_L//Z_C = \frac{sC_C(1 + sR_LC_L)}{s^2C_CC_L + (1 + sR_LC_L)(1 + sR_CC_C)} \tag{3.84}$$

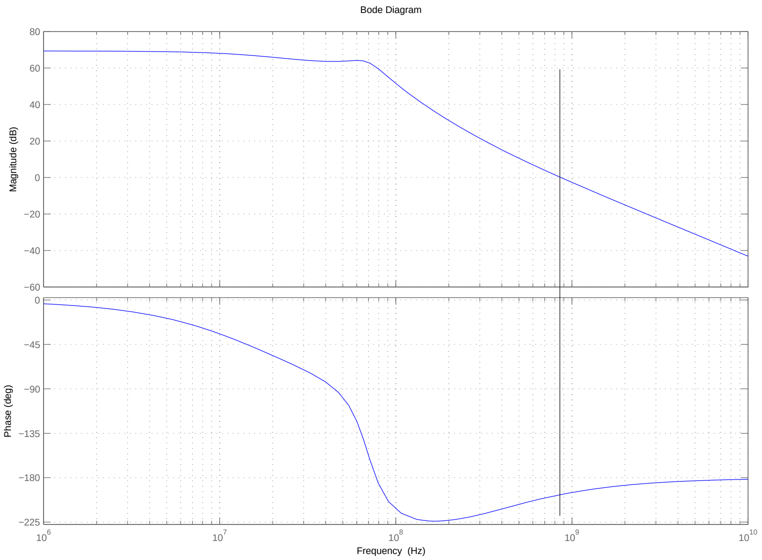


Figure 3.24: Bode plot for the system open loop gain

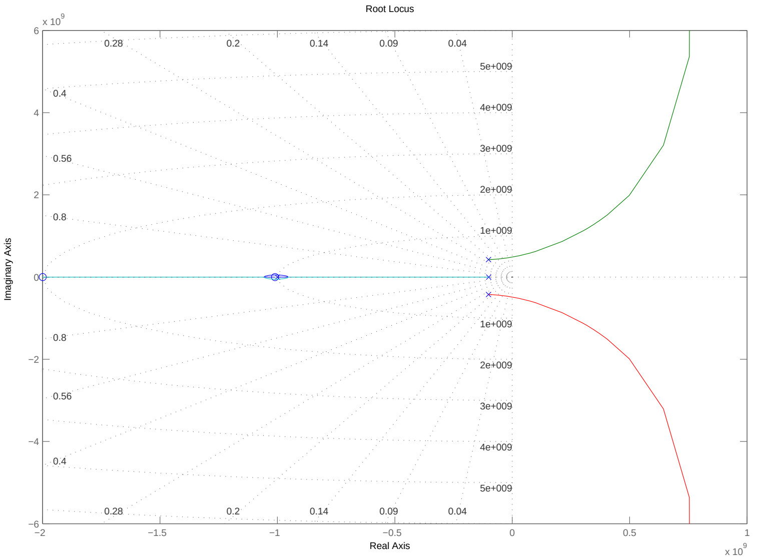


Figure 3.25: Root locus for the system open loop gain

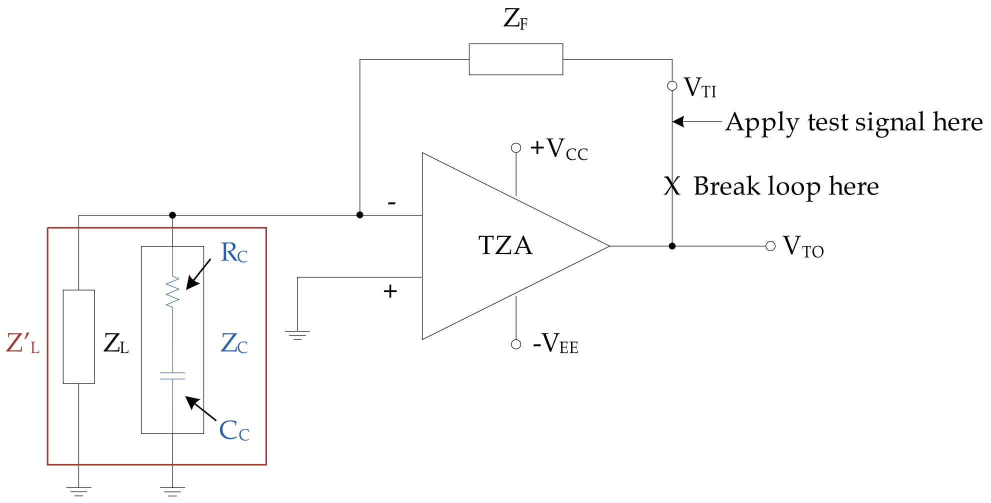


Figure 3.26: Schematic with compensation network

and:

$$\begin{aligned}\frac{1}{Z'_L//Z_F} = {} & \frac{sC_C(1+sR_LC_L)(1+sR_FC_F)}{sR_FC_C(1+sR_LC_L)} + \\ & + \frac{R_F[s^2C_CC_L+(1+sR_LC_L)(1+sR_CC_C)]}{sR_FC_C(1+sR_LC_L)}\end{aligned} \tag{3.85}$$

The new *SYS* function numerator is given by:

$$\begin{aligned} SYS_{NUM} = s^3R_F^2R_LC_LC_FC_CZ_B + \\ +s^2R_F[R_FR_LC_LC_C + Z_B[R_FC_C(C_F+C_L) + R_LC_LC_C(1+R_FR_C)]] + \\ +sR_F[R_FC_C + Z_B[C_C + R_F(R_LC_L + R_CC_C)]] + R_F^2Z_B \end{aligned} \tag{3.86}$$

while the *SYS* function denominator is given by:

$$SYS_{DEN} = s^3R_F^2R_LC_FC_LC_C + s^2R_FC_C(R_FC_F + R_LC_L) + sR_FC_C \tag{3.87}$$

The SYS function is given by (3.82).

This transfer function has been simulated with the *MATLAB* script listed in Appendix D as before, with the same values for the *Z* function and the other components.

Figure 3.27 shows the bode plot for the compensated system, where we can see that now the amplitude fall to 0dB before the phase shift reach −180°.

Figure 3.28 shows the root locus, where we can see that zeros and poles are all in the left half plane. This mean that the system is stable. The drawback is a reduction of the gain bandwidth product.

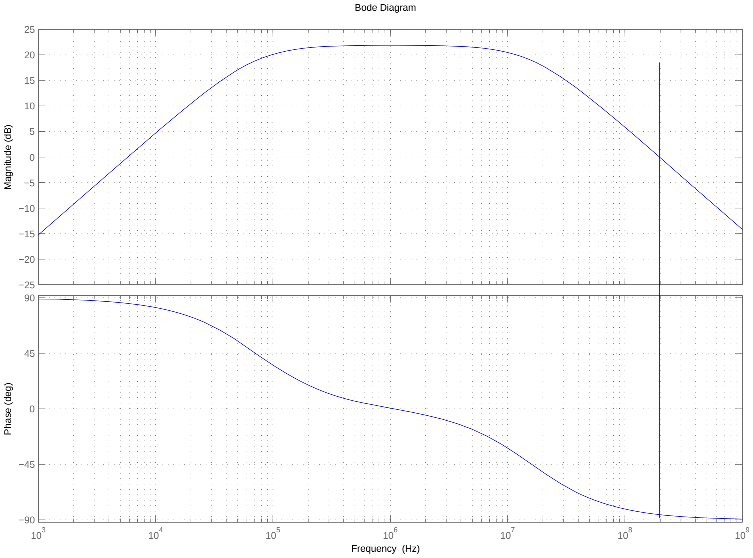


Figure 3.27: Bode plot for the compensated system open loop gain

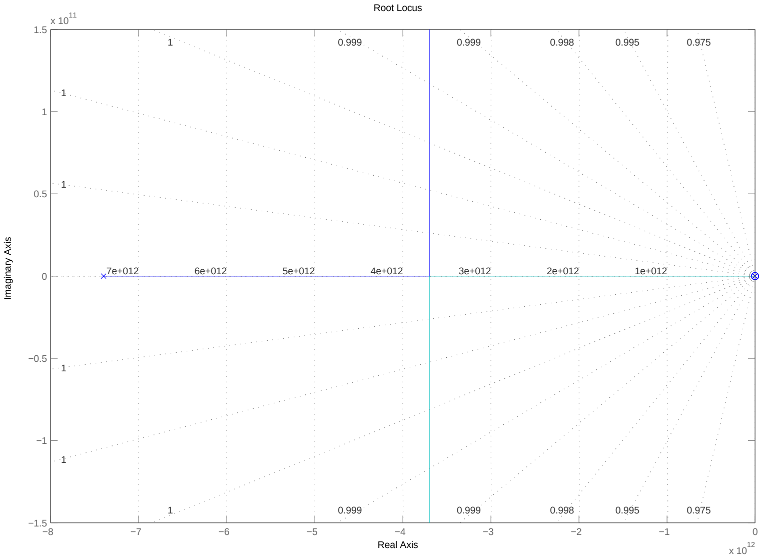


Figure 3.28: Root locus for the compensated system open loop gain

## 3.6 S-Parameters measurement

The s-parameters have been measured using the network analyzer *8753D* from *Hewlet Packard/Agilent*. The range of frequency supported by the instrument is from *30KHz* to *3GHz*. For the measurement, the instrument has been calibrated with a full 2-port configuration and the range of frequency was fixed from *30KHz* to *1GHz*. Figure 3.29 shows the $S_{21}$*-parameter* for the current probe (second version) using the *THS3202* and a feedback resistor of 700Ω. How we can see, there is a low frequency cut due to the input network. The high frequency cut is about at *600MHz*, but with this configuration the dynamic range is much tightened.

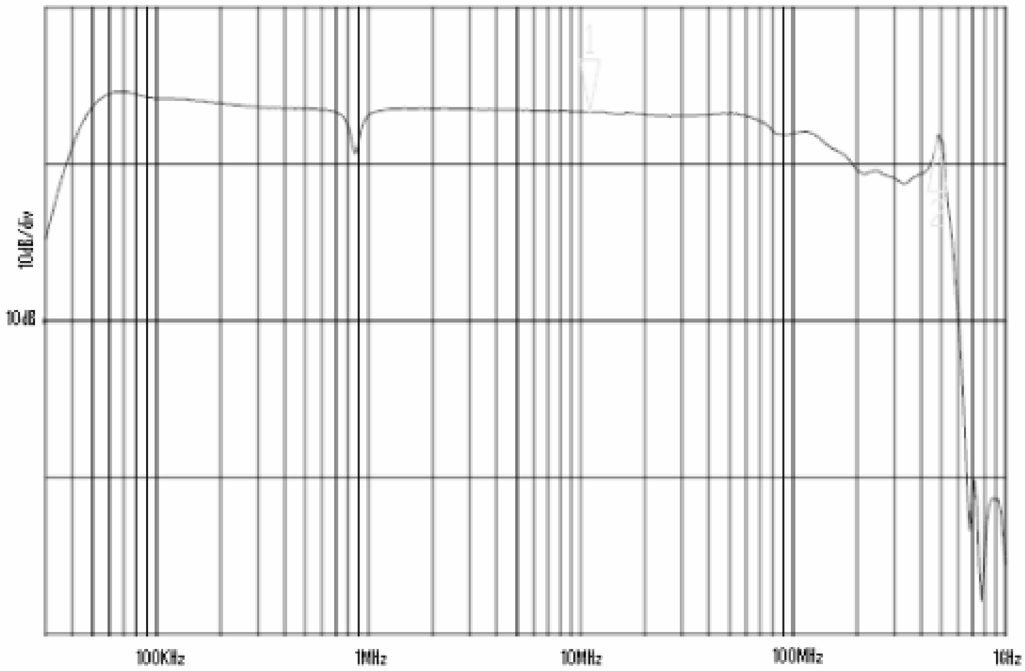


Figure 3.29: $S_{21}$ parameter for the SCM with THS3202 and $R_{FB} = 700\Omega$

Figure 3.30 shows the same circuit with a feedback resistor of 300Ω. Notice that the frequency response shows a peak at about *500MHz*, that rely to think a system instability.

Figure 3.31 shows the $S_{21}$*-parameter* using the *AD8009*. With this amplifier the circuit is stable even with a resistor of 220Ω. We have a flat bandwidth between *20KHz* and *550MHz* with a good dynamic range. With this current probe we are able to measure peaks of about *25mA*.

From the *S-parameters*, the transimpedance and the input impedance of the current probe can be derived. Figure 3.32 shows the graph for the *TZA* of the current probe. The response begins to fall at about *450MHz*.

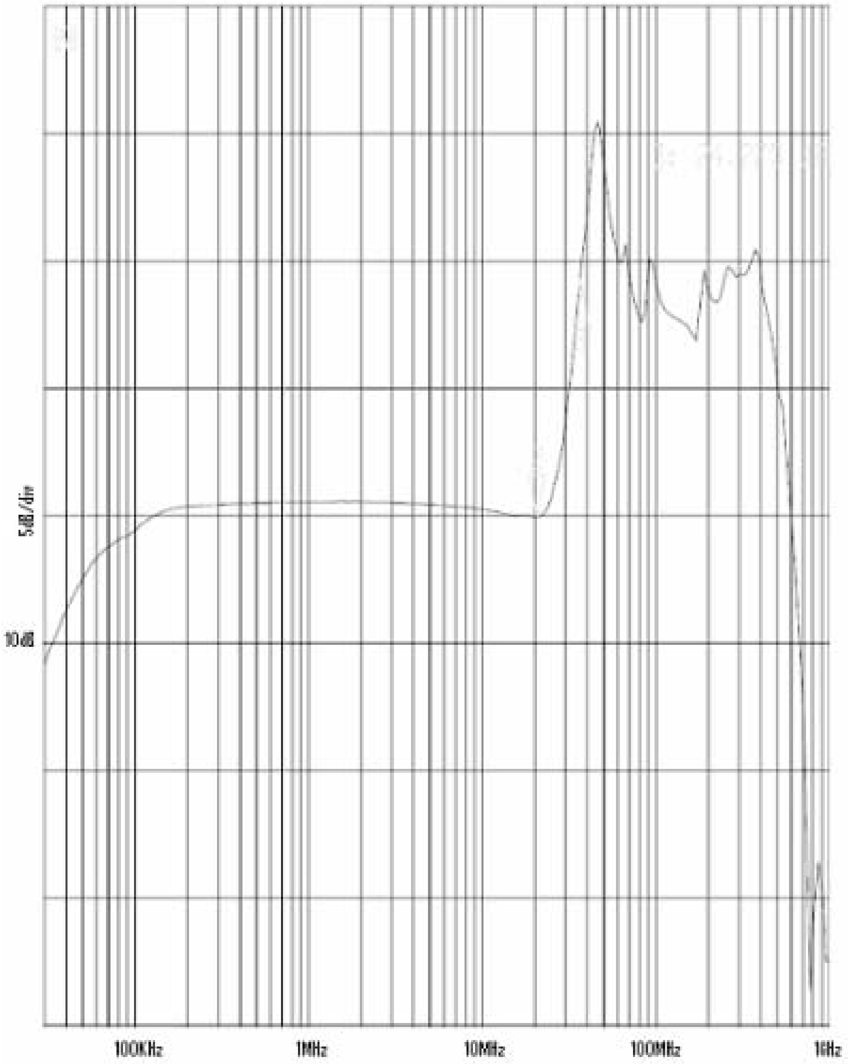


Figure 3.30: $S_{21}$ parameter for the SCM with THS3202 and $R_{FB} = 300\Omega$

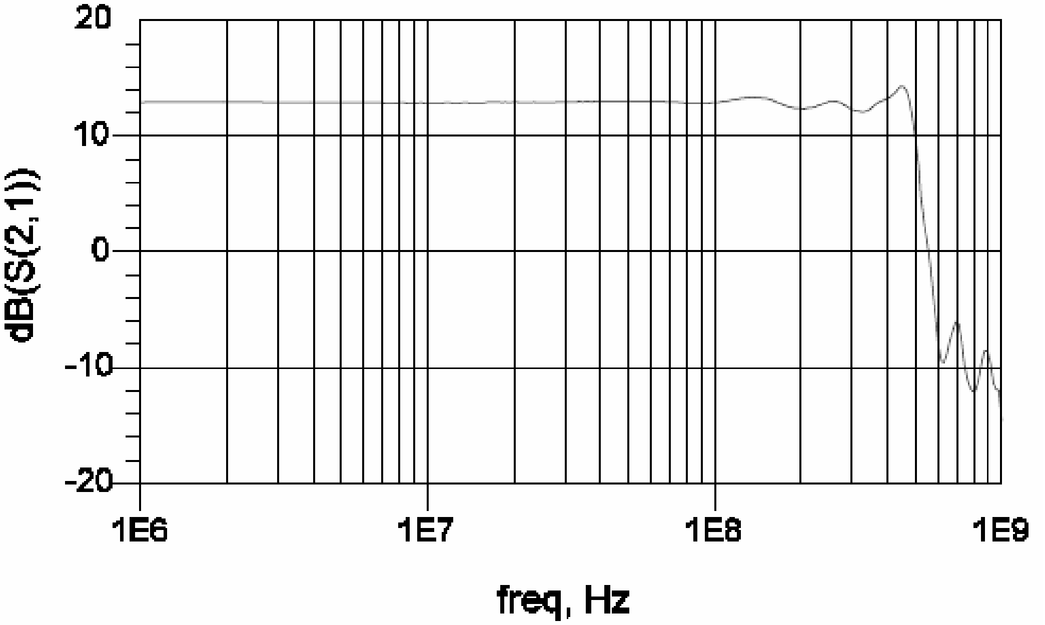


Figure 3.31: $S_{21}$ parameter for the SCM with AD8009 and $R_{FB} = 220\Omega$

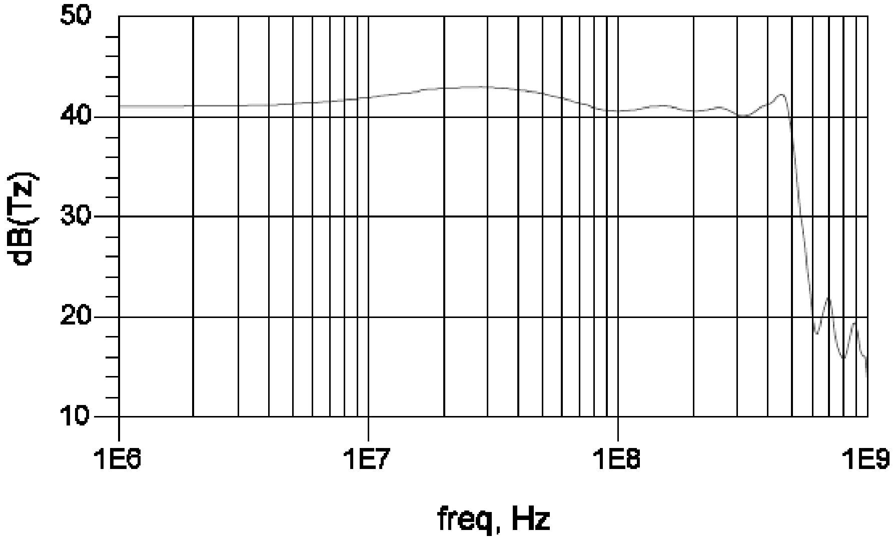


Figure 3.32: Transimpedance gain for the current probe (second version)

Finally, Figure 3.33 shows the input impedance. Here is clear that the input impedance starts increasing after about *10MHz* and reaches 50Ω at about *70MHz*.

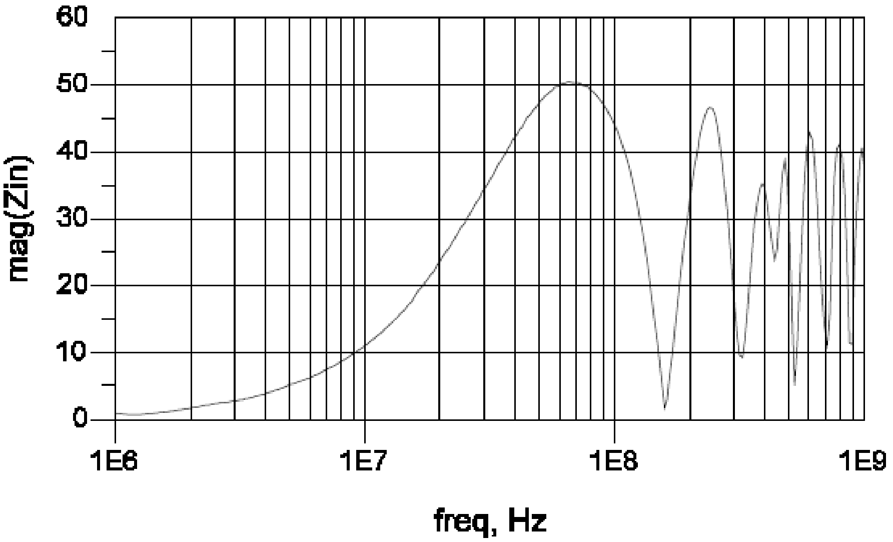


Figure 3.33: Input impedance for the SCM second version

## 3.7 DPA attack results

In order to compare the performance of the designed current probe with a resistor-based setup, a DPA attack has been performed. The following oscilloscope snapshots show a current peak measured both with a resistance and the current probe. As expected, the measurement performed with the current probe shows a higher amplification and larger bandwidth.

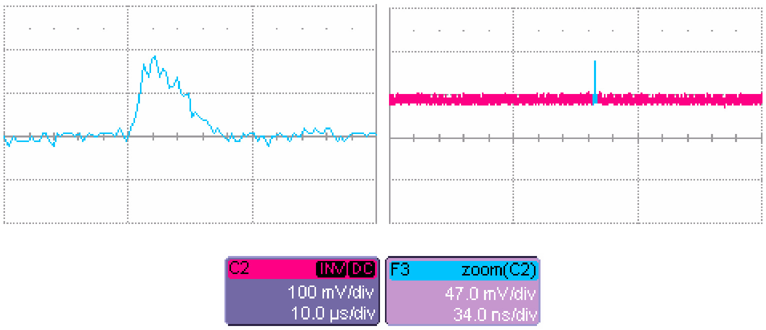


Figure 3.34: Current peak measured with resistance (zoom on the left)

The time scale is fixed to *34ns/div* while the amplitude scale is fixed to $47mV/div$, so we have a peak of about:

$$v_p \approx 90mV$$

with using a resistance $R_m = 22\Omega$, corresponding to a current peak of:

$$i_{pres} = \frac{v_p}{R_m} = \frac{90mV}{22\Omega} \cong 4mA.$$

The same measure has been performed with the current probe and Figure 3.35 shows the same peak as shown as in the resistor case.

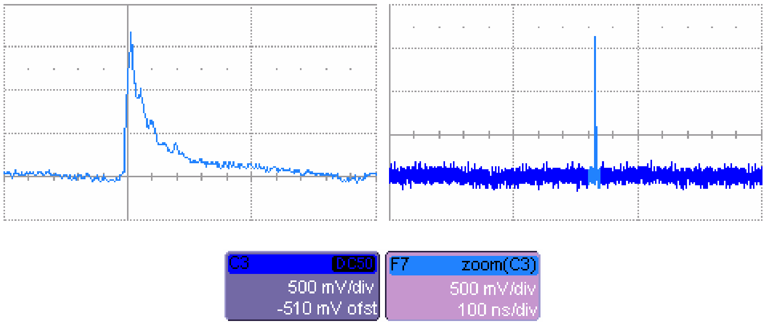


Figure 3.35: Current peak measured with the current probe (zoom on the left)

The time scale is fixed to *100ns/div* while the amplitude scale is fixed to $500mV/div$, so we have a voltage peak on the oscilloscope of about:

$$v_{OSC} \approx 1.7V$$

In this case, considering the matching network on the output of the current probe, we have a voltage peak whose value is half the voltage shown on the oscilloscope:

$$v_p = \frac{v_{OSC}}{2} = 0.85V$$

The gain of the *TZA* is given to the feedback resistor $R_f = 220\Omega$, which results in a current peak:

$$i_{pscm} = \frac{v_p}{R_m} = \frac{0.85V}{220\Omega} \cong 3.8mA$$

Both measurement results in comparable values of the measured current peak, with the current probe providing a higher amplification.

A *DPA* attack on a software *DES* implemented on a *8051* microcontroller has been performed with both methods. The used oscilloscope is a *LeCroy WaveMaster 8500A*. Using a $47\Omega$ resistor, *512* traces have been collected from the oscilloscope at a sample rate of *250MS/s*, acquiring *250000* samples for the computation. The

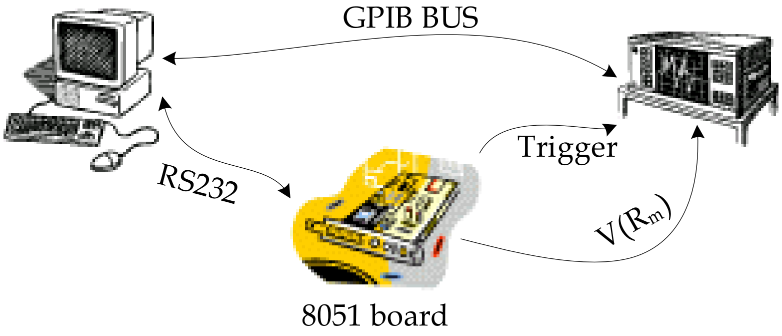


Figure 3.36: Measurement setup

traces were acquired by *GPIB* and Figure 3.36 shows the complete measurement setup.

For this first attack, a differential probe *LeCroy D600* has been used and the result is shown in Figure 3.37. The $x$-axis and $y$-axis scales are the same for both attacks. Although we can see a peak for the correct value of the *key* (black curve), it is below or comparable to several other ghost peaks (peaks corresponding to wrong values of the key).

Figure 3.38 shows a *DPA* attack performed with the current probe (second version). Notice that the trace corresponding to the correct key shows higher peaks which are above the ghost peaks, even with only *256* curves. Experimentally, we have seen that the resistor-based setup begins to provide good results with a number of traces greater than *1024*.

However, by improving the resistor-based setup (in particular, the contacts between the differential probe/current prove and the chip under attack were too long) and repeating the acquisition connecting the probes closer to the chip, we have seen a better behavior for both methods. Using a sample rate of *500Ks/s* acquiring only *250000* samples (second half of traces), Figure 3.39 and Figure 3.40 show the *3D* graph for the resistance and the probe with the improved setup respectively. The vertical scale is now doubled, meaning that the peaks are higher than what obtained in the first measurements and the trace corresponding to the correct key guess is well defined in both cases. This result demonstrates the importance of the connection between the used probe (either an active current probe or a differential voltage probe and a probing resistor) and the chip under analysis.

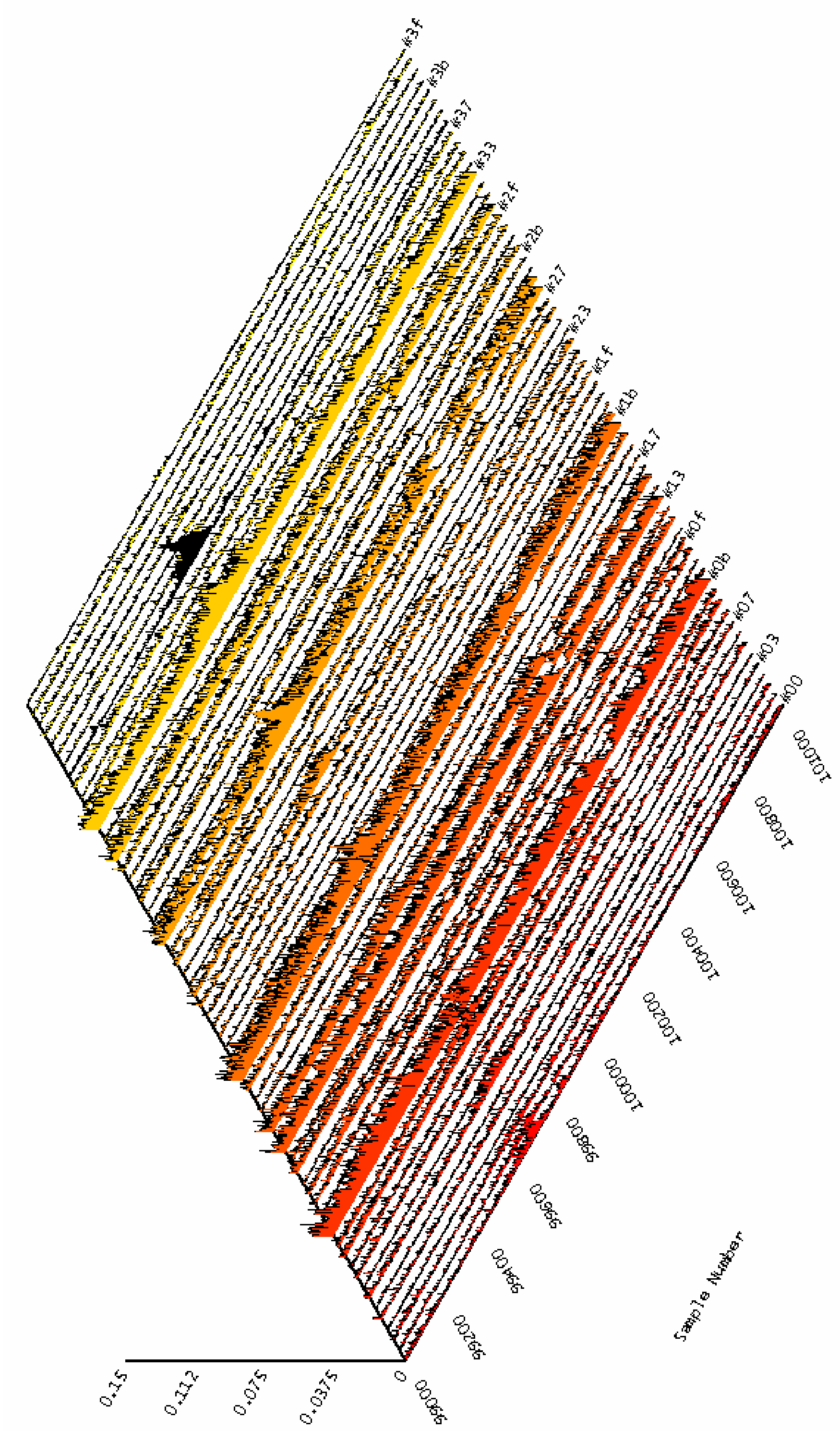


Figure 3.37: 3D Graph for the *DPA* attack using a resistor

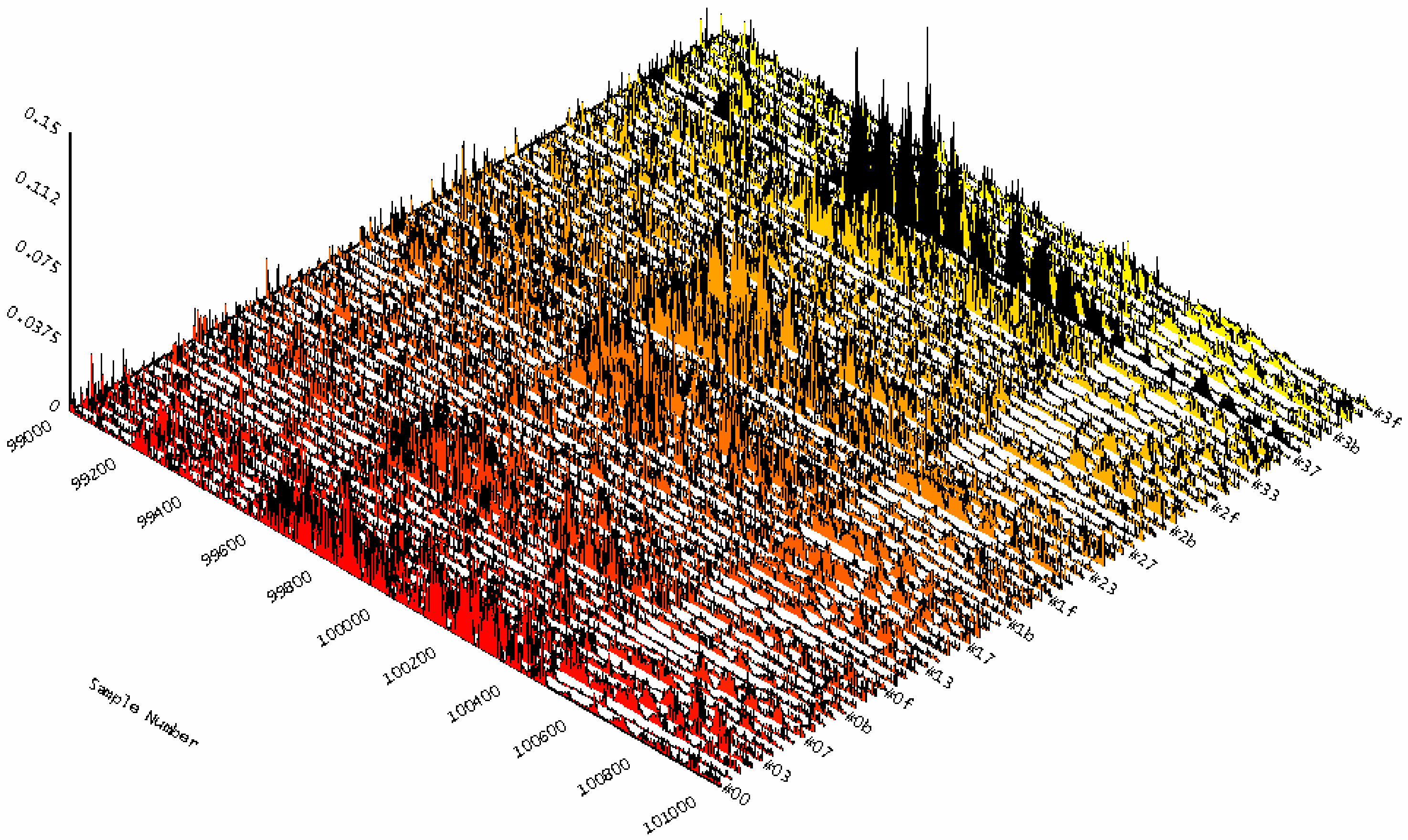


Figure 3.38: 3D Graph for the *DPA* attack using the current probe

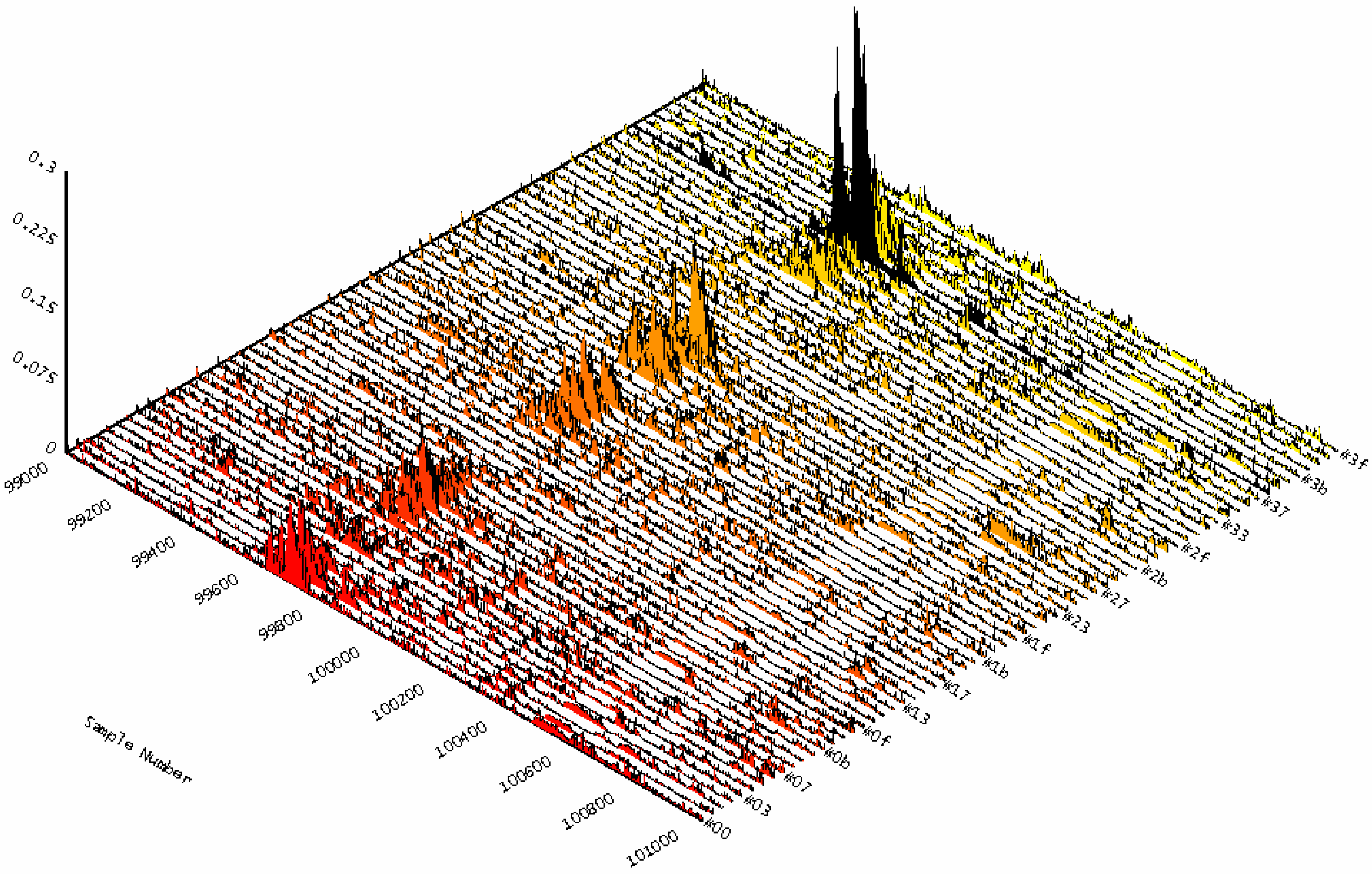


Figure 3.39: 3D Graph for the *DPA* attack using a resistor with improved setup

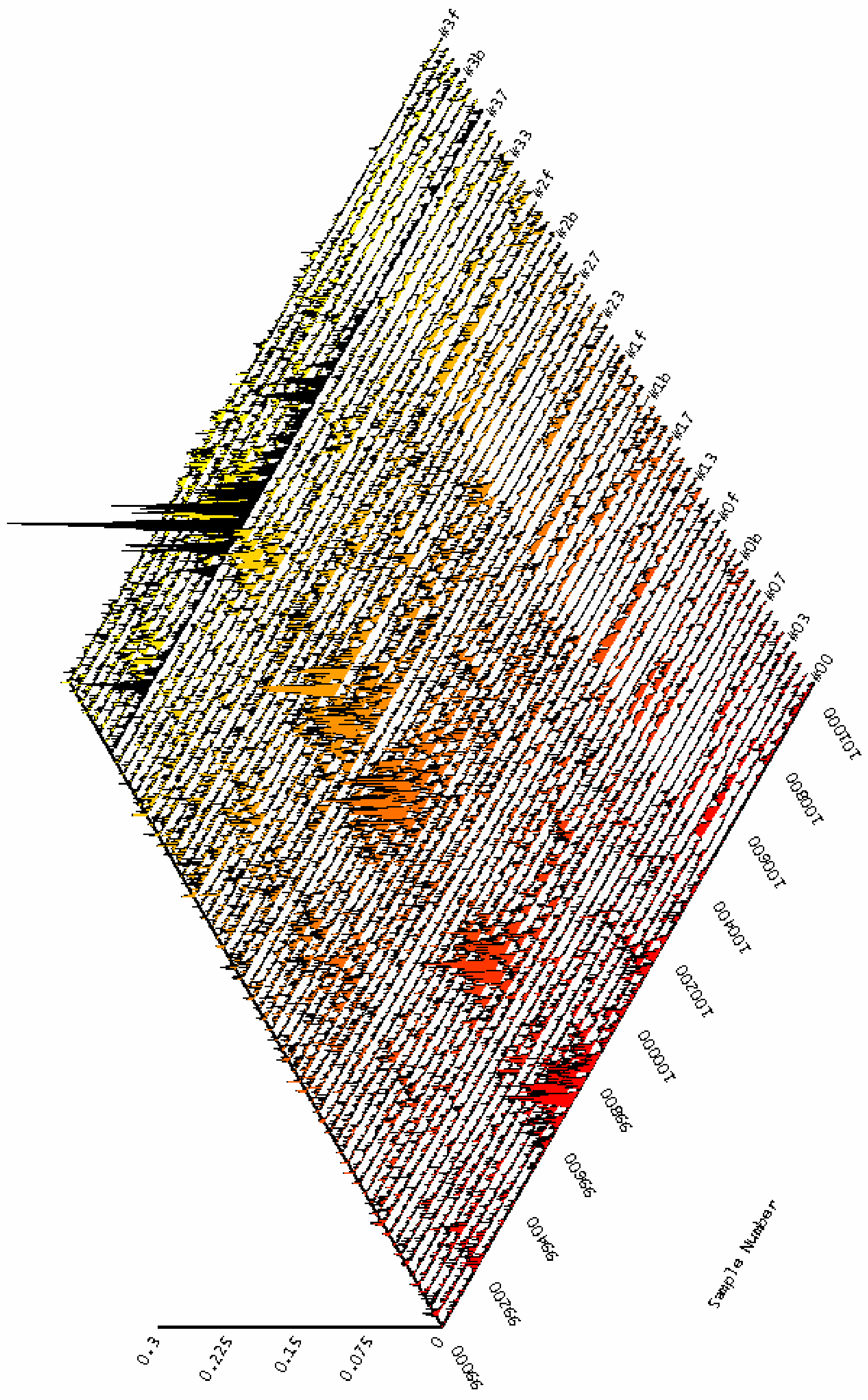


Figure 3.40: *DPA* attack results using the current probe with improved setup

# Chapter 4

# Common Base Current Probe (CBCP)

With the current probe reported in the previous chapter, we can measure current peaks of maximum *25mA*. The next step in this work was to design a second probe which could manage larger current signals. We assumed as target a dynamic range of about *100mA* which is sufficient to attack even large *FPGA*. This is useful to test the implementation of encryption algorithms in a *FPGA-based* prototyping environment.

It consists of a bipolar transistor in common base configuration and, in the following, we refer to this circuit as *Common Base Current Probe* (*CBCP*). Using this configuration, a unit current gain and a voltage gain proportional to the voltage drop on the collector resistance can be achieved. Figure 4.1 shows the schematic for the *CBCP*.

Figure 4.2 shows a *BJT* in common base configuration. The input is applied on the emitter while the output is taken on the collector.

Figure 4.3 shows the $\pi$ equivalent model for small signal analysis.

This model is uncomfortable for the analysis since the controlled generator is connected across input and output. The behavior of the circuit does not change if we place the controlled current generator with two generators with the same value. One generator is connected across collector and base and the other one is connected from the base toward the emitter. The modified circuit is shown in Figure 4.4.

The current generator connected between base and emitter is controlled by the voltage that is present on its own terminal. Therefore, we can substitute this generator with a resistor with value $1/g_m$. The last one is in parallel with $r_\pi$ and they are replaced by the emitter resistance $r_e$:

$$r_e = \frac{1}{g_m + \frac{1}{r_\pi}} = \frac{\alpha_0}{g_m}$$

Figure 4.5 shows the new $T$ model for this configuration.

Neglecting $r_o$, $r_\mu$ and $r_b$ to simplify the analysis, the small signal circuit used in the analysis is shown in Figure 4.6.

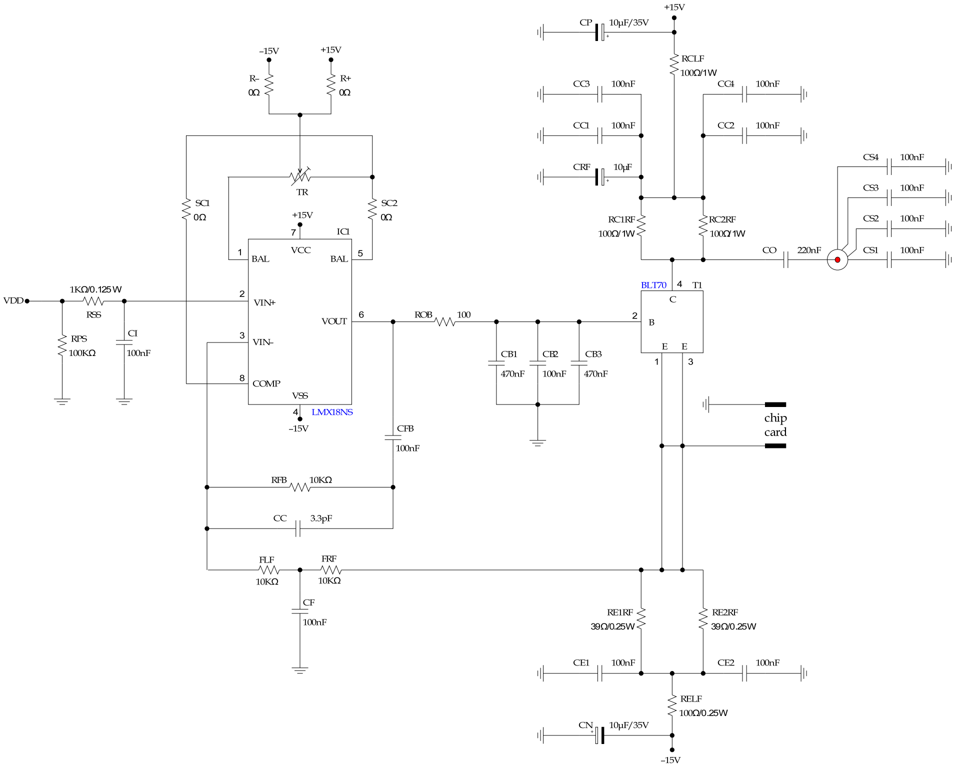


Figure 4.1: Common Base Current Probe schematic

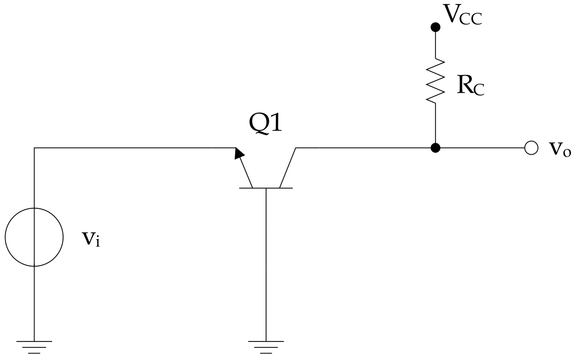


Figure 4.2: Common base configuration

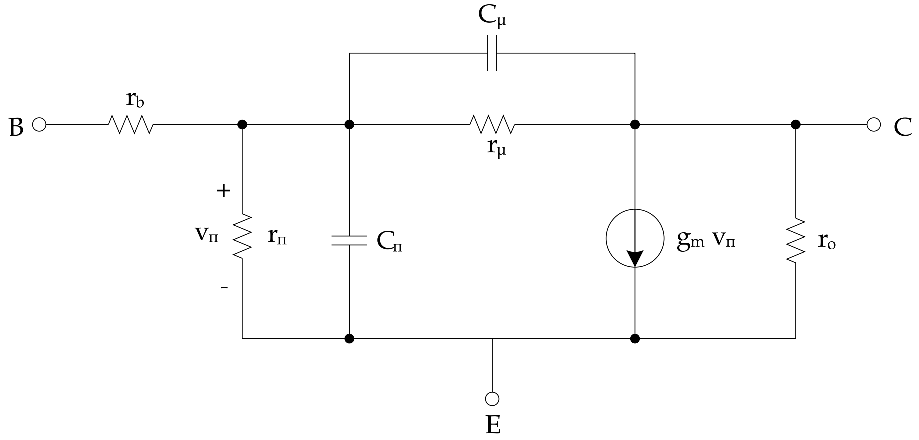


Figure 4.3: Small signal equivalent circuit

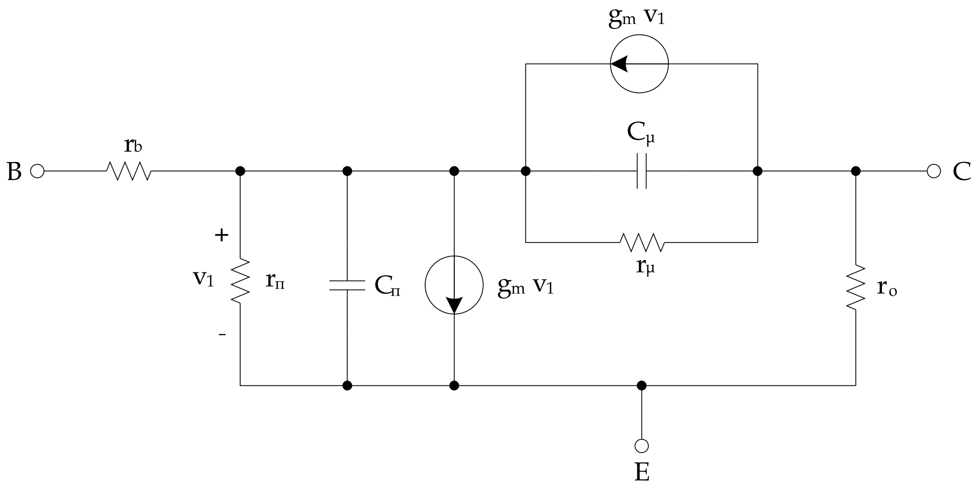


Figure 4.4: Equivalent circuit with two controlled generators

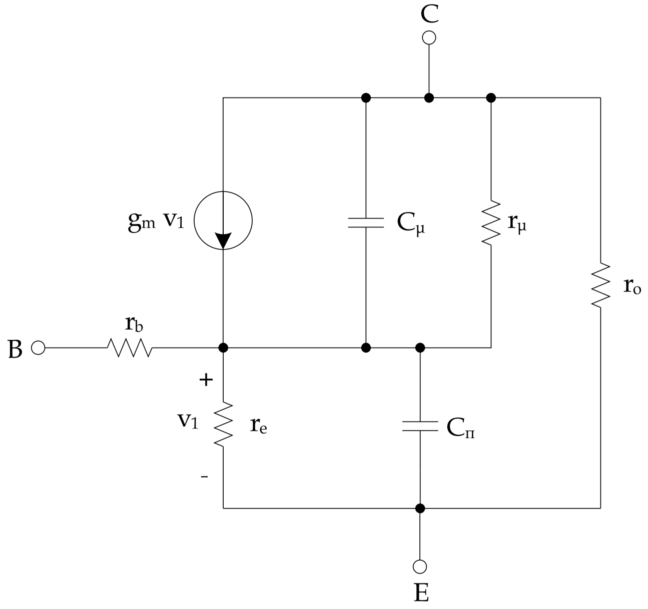


Figure 4.5: Generation of the emitter-current-controlled T model

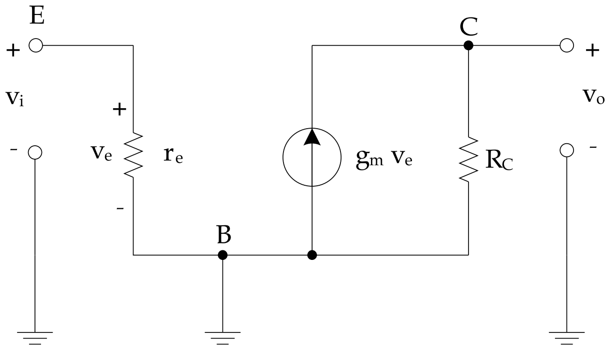


Figure 4.6: Low frequency, small signal equivalent circuit

The input resistance is given by:

$$R_i = r_e$$

while the output resistance (assuming $r_o$ much greater than $R_c$) is:

$$R_o = R_c$$

Furthermore we have:

$$v_o = -g_m R_c v_1$$

$$v_1 = -v_i$$

$$v_o = g_m R_c v_i$$

thus the open loop voltage gain is given by:

$$a_v = g_m R_c$$

Shorting the output we obtain the output current $i_o$:

$$i_o = g_m v_1$$

$$v_1 = -v_i$$

$$v_i = -r_e i_i$$

$$i_o = g_m r_e i_i$$

Finally the short circuit current gain is:

$$a_i = g_m r_e = a_0$$

When $R_c$ becomes comparable to $r_o$, we cannot neglect the last one. In this condition, we insert $r_o$ in the small signal circuit to evaluate the right value of the output impedance. The transistor in a common base configuration guarantees an input impedance reduced by a factor $1 + \beta_0$ and a current gain less than one, thus providing a very low input impedance and a very high output resistance. As a further useful advantage, the collector-base capacitor ($C\mu$) does not introduce a feedback between the output and input at high frequency, as in the common emitter configuration.

We can see one useful advantage: the collector-base capacitor ($C\mu$) won't close the circuit with loop between the input and the output at high frequency. This effect is present in the common emitter configuration.

The transistor used in this design is the *BLT70* from *Philips Semiconductor*. As we can see in Figure 4.1, the *BLT70* is connected in a common base configuration and it is supplied with a balanced voltage $\pm 15V$. The $h_{fe}$ of *BLT70* is about *25*. The collector bias voltage is chosen equal to $15/2 = 7.5V$ to obtain a maximum dynamic of $\pm 7.5V$ for the output. Assuming a bias current of *100mA*, the resistance we need on the collector is:

$$R_c = \frac{15 - 7.5}{100 \cdot 10^{-3}} = 75\Omega$$

Resistance $R_c$ is split into three standard resistance values ($R_{CLF} = 22\Omega$, $R_{C1RF} = R_{C2RF} = 100\Omega$) in order to have $50\Omega$ for the $AC$ component of the current signal under measurement. In fact, from the signal view point, capacitances $C_{C1}$ and $C_{C2}$ implement a short circuit to ground, and the resistance seen on the collector is $R_{C1RF}//R_{C2RF} = 50\Omega$. The capacitance $C_{RF}$ is an electrolytic device. Because we have a resistance of $50\Omega$ and a maximum current peak of *100mA*, we need a dynamic of $\pm 5V$. This is bounded from the previous computation, which gave an output dynamic of $\pm 7.5V$.

It is useful to suppress the low frequency overshoot and extend the bandwidth down to very low frequencies. The capacitance $C_O$ is used to decouple the oscilloscope from the probe output. The used resistors can manage *1W* since the power on each resistance is at least:

$$P(R_{C1RF}) = P(R_{C2RF}) = 100 \cdot \left(50 \cdot 10^{-3}\right)^2 = 0.25W$$

$$P(R_{CLF}) = 22 \cdot \left(100 \cdot 10^{-3}\right)^2 = 0.22W$$

We could choose resistors of *0.5W*, but they are not available as *SMD* (*Surface Mount Device*). At the emitter side we have about *100mA* bias current and a voltage drop of *-15+0.7=-14.3V*, assuming *0.7V* for the transistor $V_{BE}$ . Therefore, the resistance we need:

$$R_E = \frac{|-15 + 0.7|}{100 \cdot 10^{-3}} = 143\Omega$$

Even in this case $R_E$ is split into three resistors, $R_{ELF} = 100\Omega$, $R_{E1RF} = R_{E2RF} = 39\Omega$, equivalent to about $120\Omega$. For the same reason as before, from the signal view point, we will see only $R_{E1RF}//R_{E2RF}$ on the emitter.

Finally, for the signal input (chip card input, Figure 4.1), we will see the parallel $R_{E1RF}//R_{E2RF}//F_{RF}//R_{\pi}$. This is a very small impedance as we had to obtain. For the $AC$ analysis the base is shorted to ground by the three capacitors $C_{B1}$, $C_{B2}$ and $C_{B3}$. The *VFA* shown in Figure 4.1 is an *LM318* from *National Semiconductor*. It is used to fix the voltage on the base-emitter voltage of the bipolar transistor.

The *LM318* is used as a voltage buffer with two loops, one for the $DC$ component and one for the $AC$ component respectively. The $DC$ loop is composed by $F_{LF}$ and $F_{RF}$ because the capacitance $C_{FB}$, from this point of view is an open circuit. For the signal, we have a loop closed by $R_{FB}$, since $C_{FB}$ and $C_F$ are short circuits in this case. The capacitance $C_C$ is useful for the compensation if necessary. The resistor trimmer and other components are used to compensate the voltage offset. The goal is to have a high $DC$ precision and stable bias point.

The non-inverting input of the *LM318* is connected to the voltage reference ($V_{DD}$ in the schematic). This reference fixes the voltage on the base of the *BLT70*. The

*Common Base Current Probe* can perform current measurements on the *GND* pin of the *chip card/FPGA* connecting the reference voltage to *GND*. For measurements on the positive supply, the reference voltage must be fixed to the supply voltage of the chip under analysis.

It is clear that if we connect the *chip card/FPGA* directly on the emitter of the transistor, it is supplied with a negative voltage and the transistor is not biased because ($V_{BE} = 0$) if we suppose the reference to ground. Therefore, to bias the circuit is necessary to connect the reference to a voltage at least of *0.7V*. In this way, we have a $V_{BE} = 0.7V$ and the transistor has a good bias point. In this case, the voltage on the emitter, and thus on the device under analysis is fixed to *0V* (*GND*). Actually, the *DC* loop avoids this problem and the emitter voltage is automatically clamped to the voltage reference value. Since the voltage on the collector is fixed to *7.5V* and the resistance is fixed to 50Ω, it follows that the maximum current peak the circuit can manage is about *100mA*.

| **Symbol** | **Parameter** | **Conditions** | **Min** | **Max** | **Unit** |
|---|---|---|---|---|---|
| $V_{CBO}$ | collector-base voltage | open emitter | - | 16 | V |
| $V_{CEO}$ | collector-emitter voltage | open base | - | 8 | V |
| $V_{EBO}$ | emitter-base voltage | open collector | - | 2.5 | V |
| $I_C$ | collector current (*DC*) | - | - | 250 | mA |
| $P_{TOT}$ | power dissipation | $T_S = 60°\text{C}$ | - | 2.1 | W |
| $T_{STG}$ | storage temperature | - | -65 | +150 | °C |
| $T_J$ | junction temperature | - | - | 175 | °C |

Table 4.1: BLT70 limiting values

As we can see in Table 4.1, the maximum $V_{CE}$ is specified to *8V*. However, we tested the used transistor in laboratory obtaining a higher value. In particular, we connected the base to ground, fixing the emitter voltage to *-2V* across a 120Ω resistor. In this way, the tail current on the emitter is given by:

$$I_E = \frac{|-2 + 0.7|}{120} \cong 10mA$$

Then, with a power supply (*Hewlet Packard E3631A*), we limited the current for the positive supply to *20mA* and the negative supply to *10mA*. Switching the supply on, by increasing the positive voltage on the collector, the current is constant until we reach the breakdown region. In this condition we can observe that the current for the positive branch becomes greater than *10mA*. The $V_{CE}$ voltage was read with a digital tester connected between collector and emitter of the *BLT70*. This measurement confirmed that the circuit works properly for $V_{CE}$ up to *15V*. This is a sufficient for our applications.

Figure 4.7 and Figure 4.8 shows the final common base current probe mounted on a six layers *PCB*.

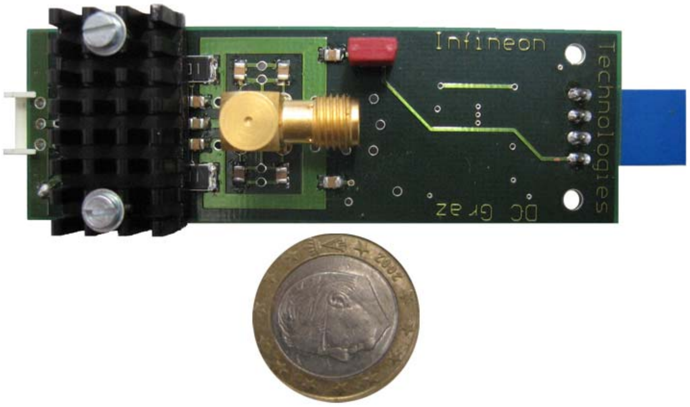


Figure 4.7: Front view of the common base current probe

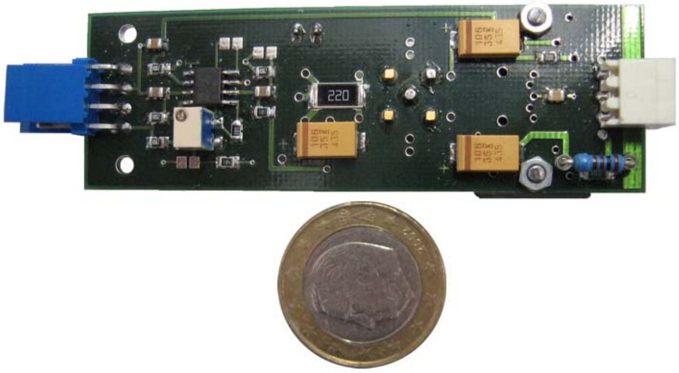


Figure 4.8: Back view of the common base current probe

## 4.1 S-Parameters measurement

As done for the current probe discussed in the previous chapter, s-parameters have been measured for the *Common Base Current Probe* as well, using a network analyzer *8753D* from *Hewlett Packard/Agilent*. The frequency range supported by instrument is from *30KHz* to *3GHz*. For this measurement the instrument has been calibrated with full 2-port configuration over a frequency range from *30KHz* to *1GHz*. Figure 4.9 shows the $S_{21}$*-parameter* for the *CBCP* and the bandwidth is about *500MHz*. With this current probe we are able to measure peak of about *100mA*.

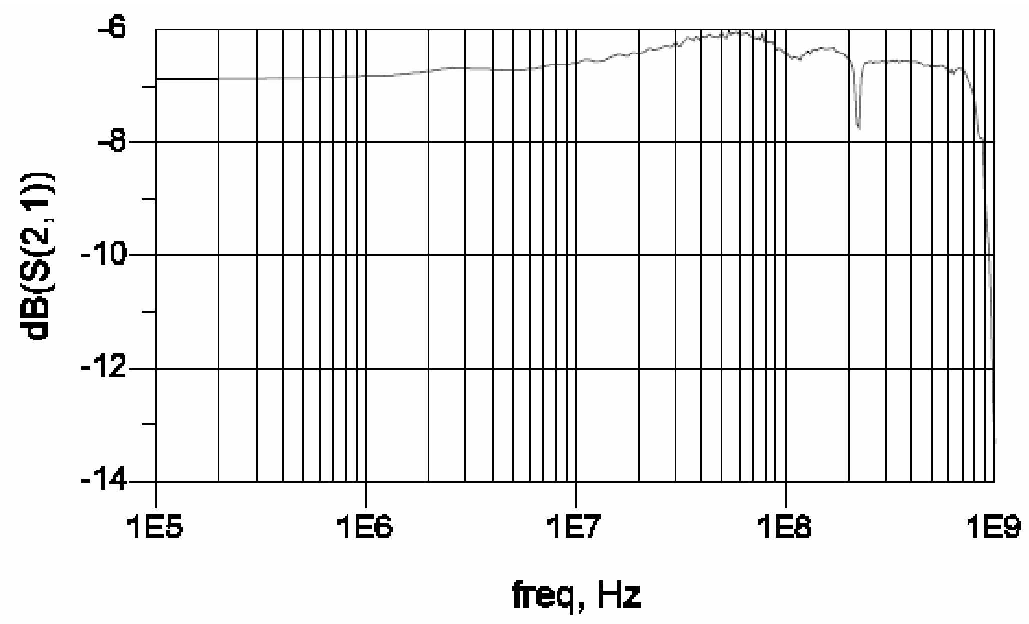


Figure 4.9: $S_{21}$ parameter for the *CBCP*

By elaborating the four *s-parameters* is possible to derive the transimpedance and the input impedance of the *CBCP*. Figure 4.10 shows the graph for the *TZA* for the common base current probe. The graph shows a high frequency cut off at about *700MHz*.

Finally, Figure 4.11 shows the input impedance: it is constant at 50Ω until about *700MHz*.

## 4.2 DPA Attack Results

With the same setup as before, a DPA attack with the common base current probe has been performed and the result is shown in Figure 4.12.

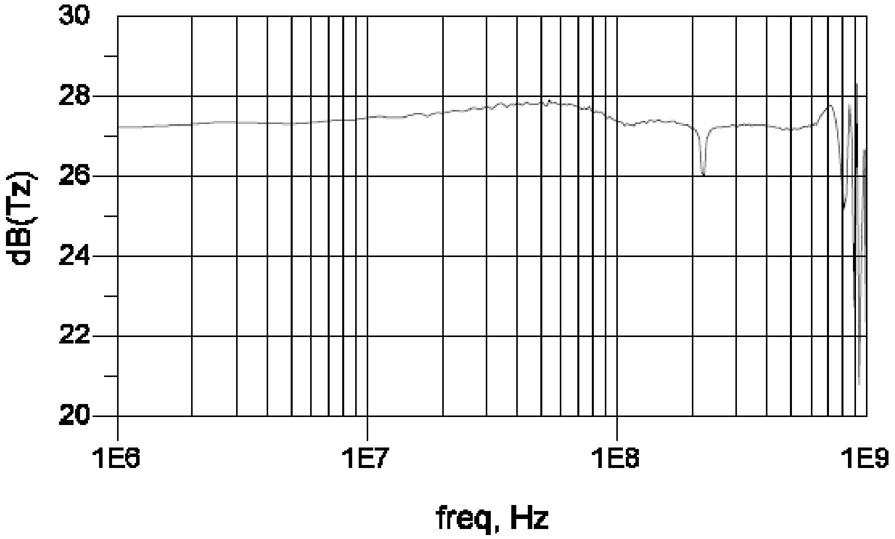


Figure 4.10: Transimpedance characteristic for the *CBCP*

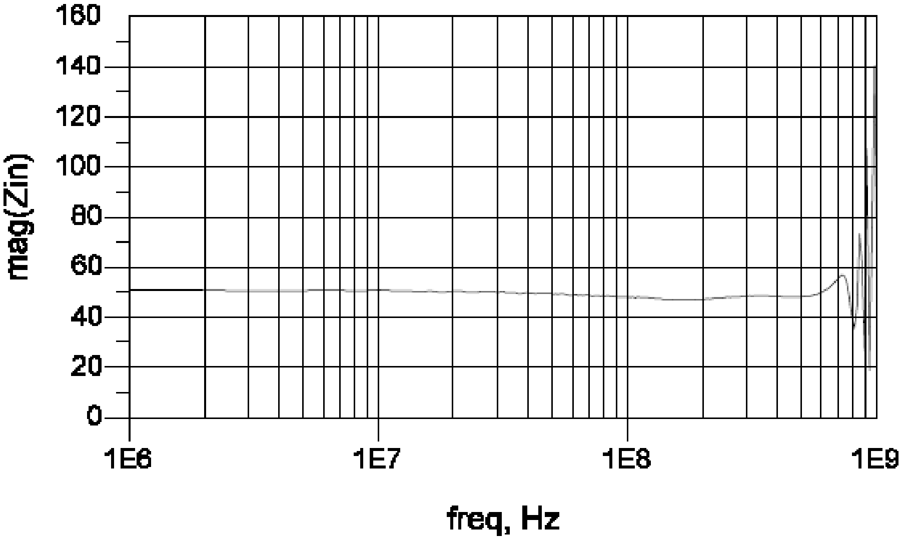


Figure 4.11: Input impedance for the *CBCP*

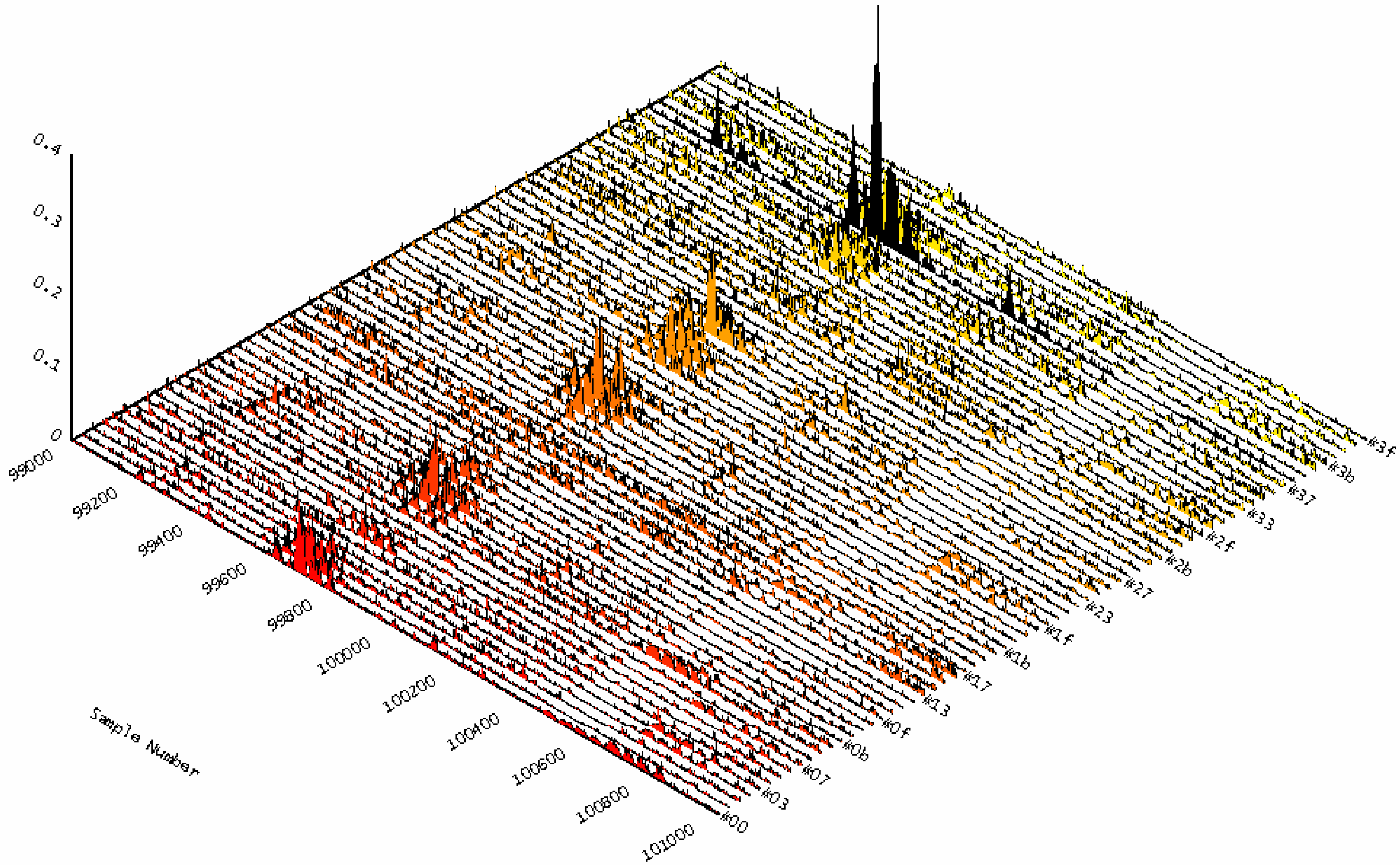


Figure 4.12: 3D Graph for the *DPA* attack using the *CBCP*

For comparison, Figure 4.13 shows the result of a DPA with the resistor-base setup (see Section 3.7): the *CBCP* shows some improvement in the height of the correlation peak for the correct key guess with respect to the resistor-based setup.

However, one of the relevant outcomes from this work is that the main parameter affecting the quality of a current measurement for a *DPA* attack is the electrical interface between probe and device under analysis (length of the contacts). This was experimentally verified with the network analyzer by measuring a normal adapted cable with a resistance of $50\Omega$ in series. Shorting the circuit at different distances from two contacts connected to the cable through an *SMA* connector, even a few millimeter difference in distance causes large impedance variations.

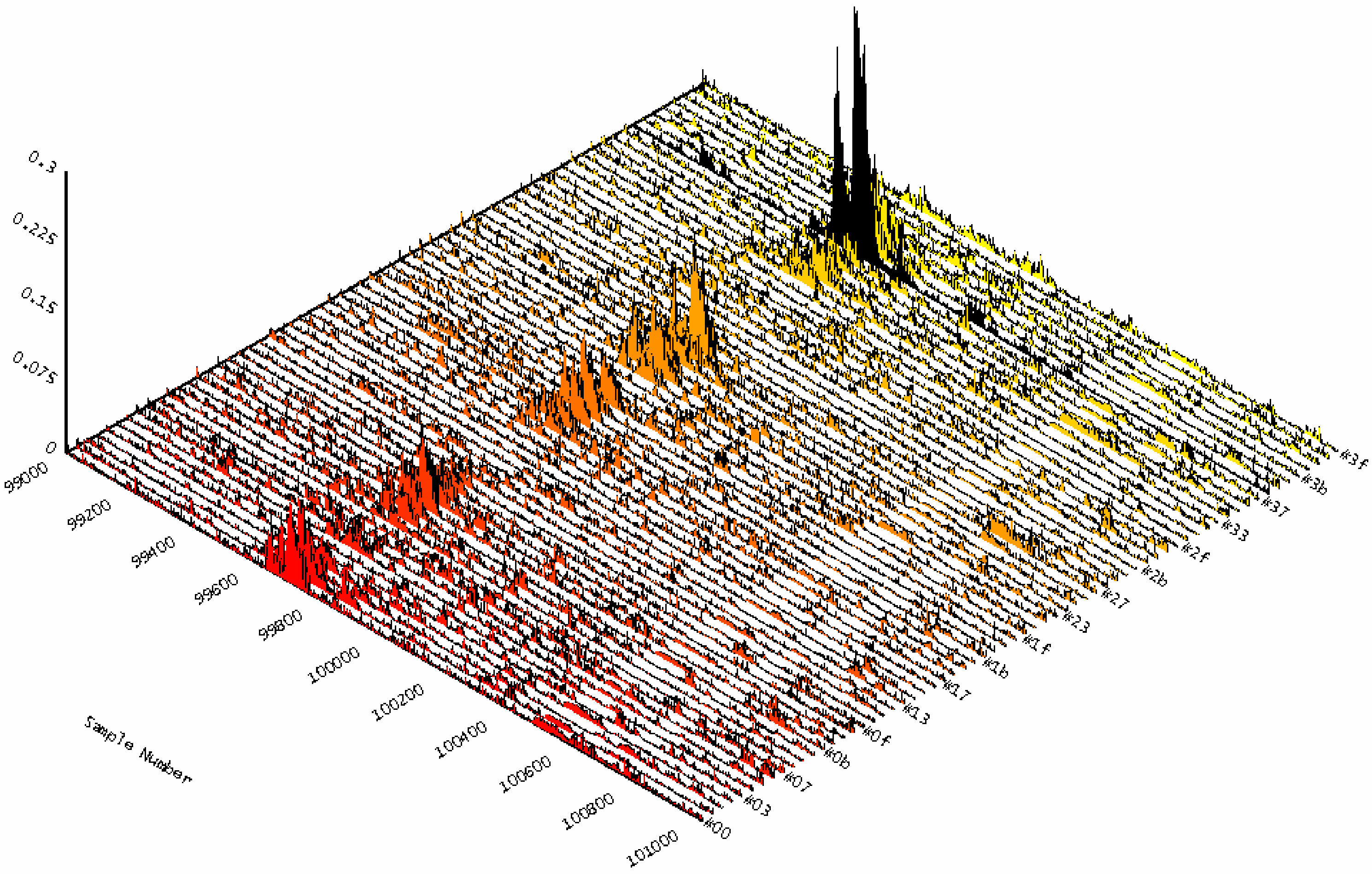


Figure 4.13: 3D Graph for the *DPA* attack using the resistor-based setup

# Chapter 5

# Feature comparison

Table 5.1, Table 5.2 and Table 5.3 show the main features of the three tested current probes. From Table 5.1, it follows that the first version of the *SCM* has a quite high feedback resistance thus limiting the dynamic range for the output voltage. The maximum current peak is closed to about *5mA*. This is too low, especially for performing a *DPA* attack on large *FPGA*. The bandwidth is close to about *300MHz*.

Table 5.2 shows the features for the second version of the *SCM*. It is basically the same circuit as the first version, but the new design is more compact and optimized. The feedback resistance is about half the value used before. The supply voltage is $\pm 10V$ which provides, after the regulators, a $\pm 7V$ power supply for the transimpedance amplifier. The voltage output swing is increased and the maximum current peak that the probe can read is about *25mA*. How shown in Table 5.2, the bandwidth is increased as well and the low frequency cut is now at about *100KHz*.

Finally, Table 5.3 summarizes the features of the last current probe designed with a single common-base bipolar transistor. The impedance seen on the collector is about $50\Omega$. This resistance represents the load for the transistor, adapted with the $50\Omega$ cable. The supply voltage is fixed to $\pm 10V$ and the maximum current peak is about *100mA*. That allows attacking also large *FPGA*. Table 5.3 shows also the improved bandwidth for the common base current probe (up to *0.5GHz* with a low frequency cut at about *50KHz*). From the laboratory tests, it results that the current probe works properly with up to a $\pm 13V$ power supply. In fact, higher supply voltages improve the probe performance ($I_C$ increases and $g_m$ increases proportionally) and the limitation becomes the junction temperature of the used transistor (about $175^{\circ} C$). With a good heat sink, the probe can be operated safely up to $\pm 13V$.

| **Parameter** | **Value** | **Description** |
|---|---|---|
| $R$ | $500\Omega$ | Transimpedance resistance |
| $TZA$ | $250V/A$ | Transimpedance gain |
| $BW$ | $> 300MHz$ | Bandwidth |
| $f_L$ | $\approx 1MHz$ | Low frequency cut |
| $+V_{CC}/-V_{EE}$ | $+5V/-5V$ | *SCM* supply voltage |
| $+V_{DD}/-V_{SS}$ | $+3.3V/0V$ | *FPGA* supply voltage |

Table 5.1: Main features of the *SCM* - first version

| **Parameter** | **Value** | **Description** |
|---|---|---|
| $R$ | $220\Omega$ | Transimpedance resistance |
| $TZA$ | $110V/A$ | Transimpedance gain |
| $BW$ | $> 400MHz$ | Bandwidth |
| $f_L$ | $\approx 100KHz$ | Low frequency cut |
| $+V_{CC}/-V_{EE}$ | $+10V/-10V$ | *SCM* supply voltage |

Table 5.2: Main features of the *SCM* - second version

| **Parameter** | **Value** | **Description** |
|---|---|---|
| $R$ | $50\Omega$ | Transimpedance resistance |
| $TZA$ | $25V/A$ | Transimpedance gain |
| $BW$ | $> 500MHz$ | Bandwidth |
| $f_L$ | $\approx 50KHz$ | Low frequency cut |
| $+V_{CC}/-V_{EE}$ | $+10V/-10V$ | *SCM* supply voltage |

Table 5.3: Main features of the common base current probe

# Chapter 6

# Conclusions

The main goal of this thesis work was the performance optimization of an active current probe for the implementation of power analysis attacks on cryptographic devices.

The critical design parameter is the amplitude of the current peak that the probe is able to measure. In the first current probe evaluated in a previous thesis work, the maximum value was about *7mA*, which is not sufficient especially for the evaluation of crypto-processor prototypes on large *FPGA*'s. In an improved version designed in this work, the value was increased to about *25mA* and, finally, adopting a different circuit topology, it was possible to reach almost *100mA*.

Both current probes designed in this work have been tested performing a *DPA* on a software DES implemented on a *8051* processor. The results using the *SCM* probe are very similar to what could be obtained using a simple resistor-based measurements. On the contrary, an improvement has been observed using the *CBCP* probe. However, considering that the measurements have been performed only an a software DES, the improved gain-bandwidth product and dynamic response of the active probe are not fully exploited. Better results could be achieved on hardware implementations.

In addition, operating the designed active current probes is straightforward and no particular know-how on current measurements for *DPA* is needed, thus allowing to obtain fast measurements during the design phase of cryptographic devices.

# Appendix A

# THS320X internal structure

The amplifier used in the second version of the current probe is a current feedback amplifier (*CFA*) from *Texas Instruments* (*THS3201*). It has a gain-bandwidth product of *1.8GHz* and a slew rate of $10500V/\mu s$. Figure A.1 shows the input stage rebuilt from the Spice netlist. How we can see, the inverting input pin is connected to the emitter of $Q\_Q4$, across an inductance of *1.15nH*. For this reason, its input impedance is very low. The non-inverting input is connected to voltage controlled source $E\_E4$, across an inductance of *200pH*. In agreement with the theory of CFA's (see Appendix B), this pin shows a high impedance, since it is the input of a buffer.

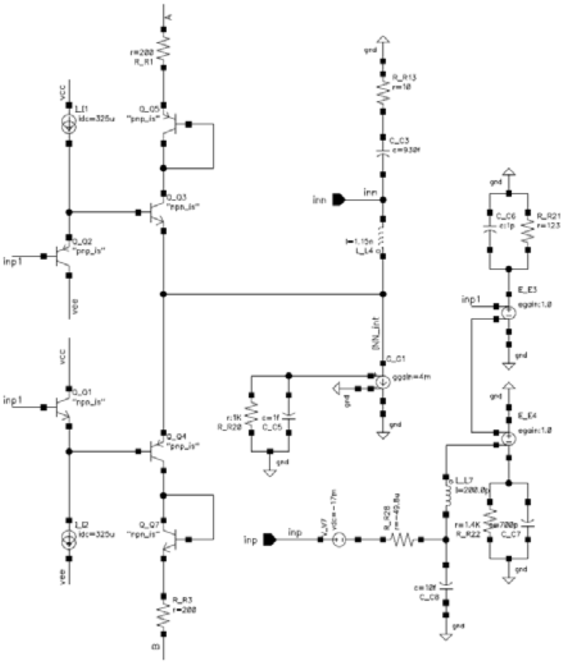


Figure A.1: Internal structure of *THS3201* model input stage

The $V\_V7$ voltage generator is an offset voltage, while the current sources $I\_I1$ and $I\_I2$ avoid that the voltage on the emitter of transistors $Q\_Q1$ and $Q\_Q2$ go toward the supply rail. The inverting input is connected to the emitter of transistors $Q\_Q3$ and $Q\_Q4$ so this is a low impedance node. The base of transistor $Q\_Q1$ is controlled by the $E\_E3$ output voltage. This voltage is a function of the non-inverting input voltage. Actually, controlled generators $E\_E3$ and $E\_E4$, used for modeling the high impedance of non-inverting input, have a unity gain. For this reason the *inp1* node is at the same voltage as to the non-inverting input *inp* (minus the offset voltage represented by *V_V7*). Now we will refer to the circuit composed by transistors $Q\_Q1$, $Q\_Q4$ e $Q\_Q7$. We can see that the base of transistor $Q\_Q4$ is controlled by $Q\_Q1$ transistor. The $Q\_Q4$ transistor is loaded by $Q\_Q7$ transistor that is diode connected, with an emitter degeneration. Following the network composed by $Q\_Q1$ and $Q\_Q4$, between *inp1* and the inverting input there are two $V_{BE}$, equal and opposite in sign so they cancel each other. This group of transistors is the *CFA* input buffer.

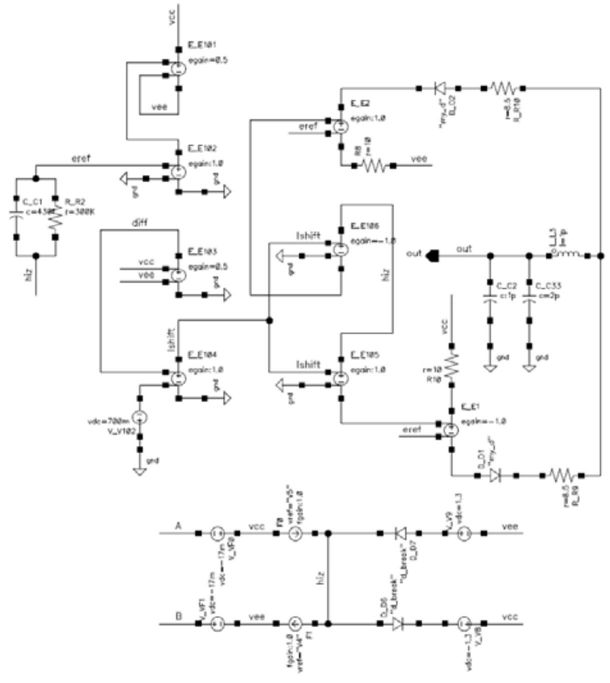


Figure A.2: Internal structure of *THS3201* model output stage

On the other hand, each branch is composed by two cascaded emitter followers, so the gain between the two inputs is close to one. The *THS3201* output stage is shown in Figure A.2 where on the lower side we can observe the presence of some controlled sources connected to the node *hiz* (*High Impedance Node*). These sources represent the *ZI* controlled source in the *CFA* theory. The *THS3202* output is placed on the output of a buffer which is modeled with a network of voltage controlled sources. The current injected in the *hiz* node is a function of the tailed current from the supply rails $V_{CC}$ and $V_{EE}$. This current has a limited value and is modeled by this sub-circuit:

.SUBCKT cswil 1 2 3 4 5 6

+ PARAMS:

+ $I_L$ = 15m ;

$V_1$ 1 2 0

Gout 3 4 value=limit(V(5,6)/12.4,0.88,-0.88)*limit(I($V_1$),$I_L$,-$I_L$);

.ENDS cswil

For A node, the pins are mapped in this order:

$$1 \rightarrow V_{CC}; 2 \rightarrow A; 3 \rightarrow V_{CC}; 4 \rightarrow hiz; 5 \rightarrow V_{CC}; 6 \rightarrow V_{EE}$$

Between nodes *1* and *2*, or between positive supply and node A, is present a zero voltage generator. This is used for the control of the tail current injected in the *hiz* node. The value of this current is:

$$limit(V(5,6)/12.4, 0.88, -0.88) * limit(I(V_1), I_L, -I_L) \qquad \text{(A.1)}$$

The limit function is defined in this way:

| | |
|---|---|
| limit(x,min,max)= | min if $x < min$ |
| limit(x,min,max)= | max if $x > max$ |
| limit(x,min,max)= | x otherwise |

Therefore, the range value for the current injected in the *hiz* node, since the parameter value is $I_L = 15mA$, is:

$$-0.88 * 15 * 10^{-3} \leq I_{hiz} \leq 0.88 * 15 * 10^{-3}$$

$$-13.2mA \leq I_{hiz} \leq 13.2mA$$

Finally, this current drives the voltage controlled sources of the output stage. Actually, the connection between input and output stage is implemented with other two transistors, connected on the base of the diode on the collector of $Q\_Q3$ and $Q\_Q4$. In this way, the tail current in the collector of $Q\_Q3$ and $Q\_Q4$ transistors is mirrored in the *hiz* node . This current is fixed by choosing the optimal form factor of the current mirror. Figure A.3 shows the simplified schematic with current mirrors for the *THS3201* input buffer.

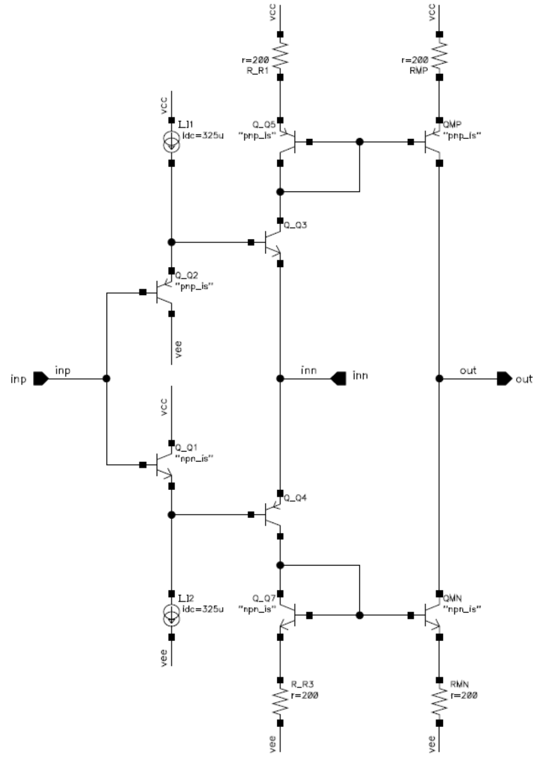


Figure A.3: Simplified schematic for the *THS3201* input buffer

# Appendix B

# Current Feedback Amplifier

The *CFA* (*Current Feedback Amplifier*) has a reduced *DC* precision with respect to a *VFA* (*Voltage Feedback Amplifier*) in a trade-off for increased slew rate and bandwidth that is relatively independent from the closed loop gain. Although the CFA's do not reach the *DC* precision of their *VFA* counterparts, they are good enough to be *DC* coupled without sacrificing too much the dynamic range. The slew rate of CFA's is not limited by the linear rate of rise that is seen in VFA's, so it is much faster and leads to faster rise/fall times and less intermodulation distortion.

## B.1 Development of the general feedback equation

Referring to the block diagram shown in Figure B.1, (B.1), (B.2) and (B.3) can be written by inspection if it is assumed that there are no loading affects among the blocks. This assumption is implicit in all block diagram calculations, and requires that the output impedance of a block is small enough in comparison to the input impedance of the following the block. Algebraic manipulation of (B.1), (B.2) and (B.3) leads to (B.4) and (B.5) which are the defining equations of the feedback system.

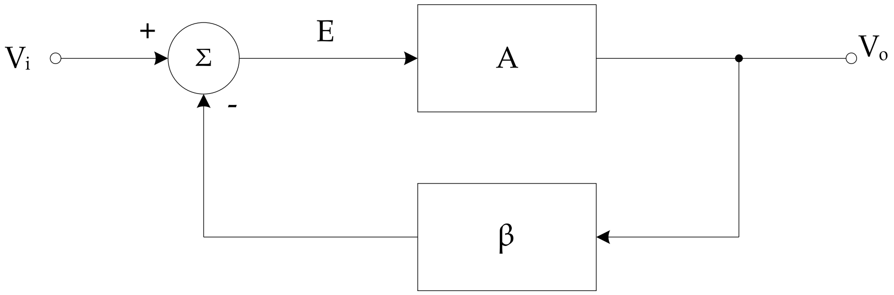


Figure B.1: Feedback system block diagram

$$V_o = E * A \tag{B.1}$$

$$E = V_i - \beta V_o \tag{B.2}$$

$$E = \frac{V_o}{A} \tag{B.3}$$

$$\frac{V_o}{V_i} = \frac{A}{1 + A\beta} \tag{B.4}$$

$$\frac{E}{V_i} = \frac{1}{1 + A\beta} \tag{B.5}$$

In this analysis, parameter $A$, which usually includes the amplifier and thus contains active elements, is called the direct gain. The parameter $\beta$, which normally contains only passive components, is called the feedback factor. Notice that in (B.4), as the value of A approaches infinity, the $A\beta$ quantity, which is called loop gain, becomes much larger than one; thus, (B.4) can be approximated with (B.6):

$$\frac{V_o}{V_i} = \frac{1}{\beta}$$

for

$$A\beta \gg 1$$

(closed loop gain)

(B.6)

Because the direct gain is not included in (B.6), the closed loop gain (for $A\beta \gg 1$) is independent from the amplifier parameter variations. This is the major benefit of feedback circuits.

Equation (B.4) is sufficient to describe the stability of any feedback circuit because these circuits can be reduced to this generic form through block diagram reduction techniques. The stability of the feedback circuit is determined by setting the denominator of (B.4) equal to zero:

$$1 + A\beta = 0 \tag{B.7}$$

$$A\beta = -1 = |1|\angle - 180 \tag{B.8}$$

Notice that, from (B.4) and (B.8), if the magnitude of the loop gain reaches one when the phase shift is equal to −180 degrees, the closed loop gain is undefined because of the division by zero. The undefined state is unstable causing the circuit to oscillate at the frequency where the phase shift equals −180 degrees. If the loop gain at the oscillation frequency is slightly greater than one, it will be reduced to one by the reduction in gain due to the active elements as they approach the saturation. If the value of $A\beta$ is much greater than one, the circuit may oscillate between the saturation limits.

A good starting point for discussing stability is finding an easy method to calculate it. Figure B.2 shows that the loop gain can be calculated from the block diagram by opening the current inputs (shorting voltage inputs respectively), breaking the circuit and calculating the response $V_{TO}$ to a test input signal $V_{TI}$:

$$\frac{V_{TO}}{V_{TI}} = A\beta \tag{B.9}$$

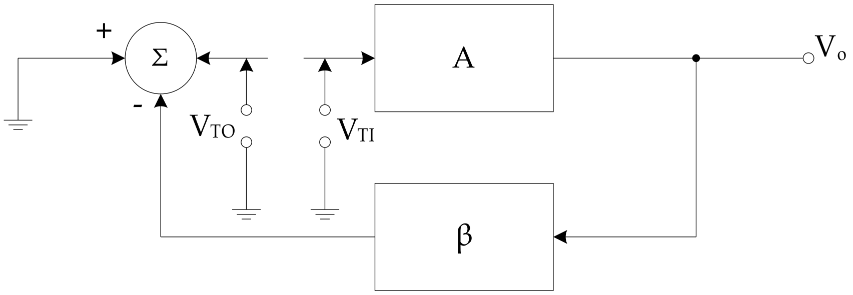


Figure B.2: Block diagram for computing the loop gain

## B.2 Current feedback stability equation

The *CFA* model is shown in Figure B.3. The non-inverting input is connected to the input of a buffer thus presenting a high impedance, similar to what can be obtained with a bipolar *VFA*'s. The inverting input is connected to the buffer output; $Z_B$ models the buffer output impedance, which is usually very small, often less than $50\Omega$. The buffer gain, $G_B$, is close to one and it will be neglected in this analysis. The output buffer must present low impedance to the load. Its gain, $G_{OUT}$, is one and is neglected for the same reason as for the input buffer.

The output buffer's impedance, $Z_{OUT}$, affects the response when some output capacitance is considered; otherwise, it can be neglected unless *DC* precision is required when driving low impedance loads. Figure B.3 is used to develop the stability equation for both the inverting and non-inverting configurations.

Breaking the loop at the point *X*, inserting a test signal $V_{TI}$, and calculating the output signal $V_{TO}$, provides the stability equation. The circuit is redrawn in Figure B.4 to make the calculation easier. Notice that the output buffer and its impedance have been removed because they do not affect the stability. Although the input buffer is shown in the Figure B.5, it will be neglected as well.

The current loop equations related to the input and output loop are given below together with the equation relating $I_1$ e $I_2$:

$$V_{TI} = I_2(Z_F + Z_G//Z_B) \tag{B.10}$$

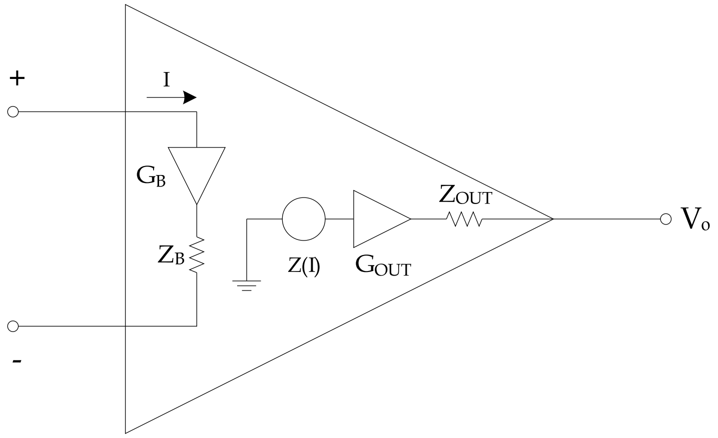


Figure B.3: Current feedback amplifier model

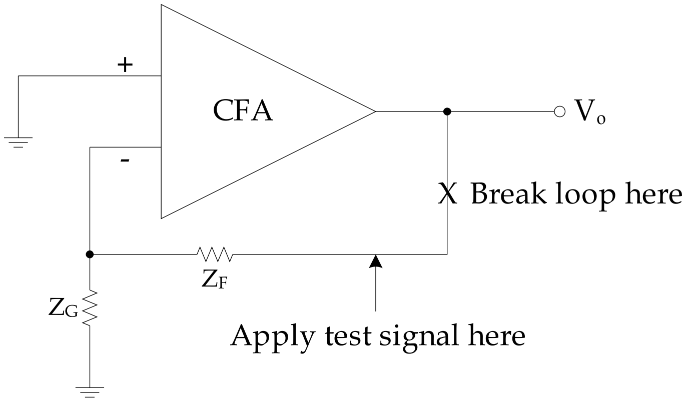


Figure B.4: Block diagram for stability analysis

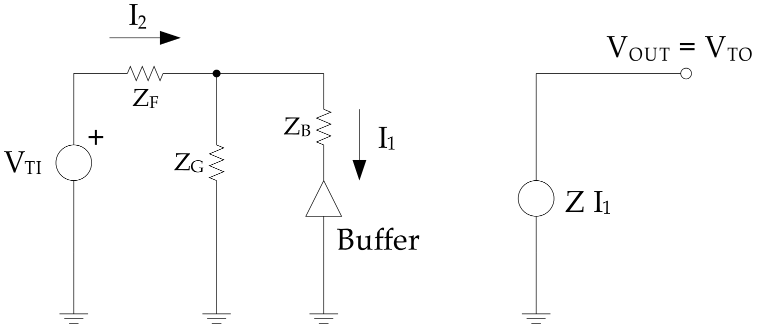


Figure B.5: Internal circuit for stability analysis

$$V_{TO} = I_1 Z \tag{B.11}$$

$$I_2(Z_G//Z_B) = I_1 Z_B; G_B = 1 \tag{B.12}$$

Equation (B.10) and (B.12) are combined to obtain the (B.13):

$$V_{TI} = I_1(Z_F + Z_G//Z_B)\left(1 + \frac{Z_B}{Z_G}\right) = I_1 Z_F \left(1 + \frac{Z_B}{Z_F//Z_G}\right) \tag{B.13}$$

Dividing (B.11) by (B.13), (B.14) is derived which is the defining equation for stability analysis.

$$A\beta = \frac{V_{TO}}{V_{TI}} = \frac{Z}{Z_F\left(1 + \frac{Z_B}{Z_F//Z_G}\right)} \tag{B.14}$$

## B.3 Developing the non-inverting circuit equation

Equation (B.15) is the current equation at the inverting input of the circuit shown in Figure B.6. Equation (B.16) is the loop equation for the input circuit, and (B.17) is the output circuit equation. Combining these equations gives the (B.18), in the form of (B.4), which is the non-inverting circuit equation.

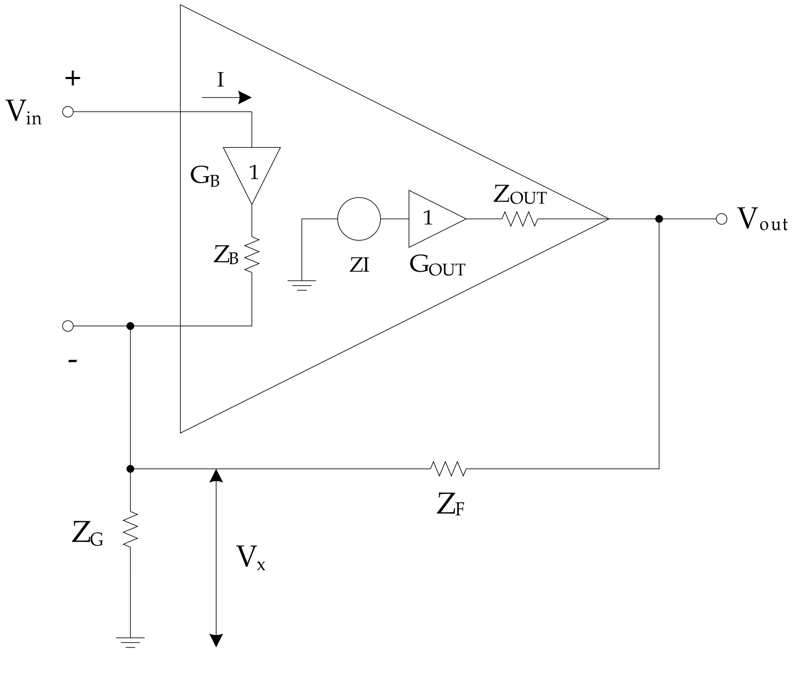


Figure B.6: Non-inverting configuration circuit

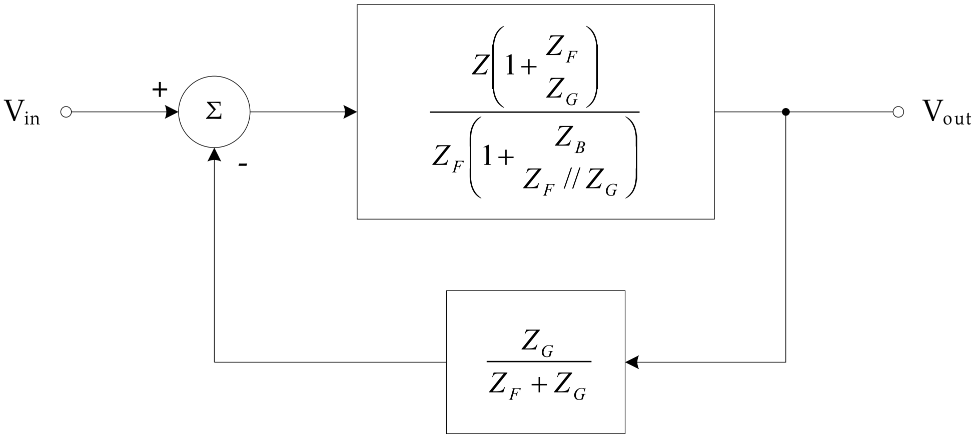
$$I = \left(\frac{V_x}{Z_G}\right) - \frac{(V_{out} - V_x)}{Z_F} \tag{B.15}$$

$$V_x = V_{in} - Z_B I \tag{B.16}$$

$$V_{out} = ZI \tag{B.17}$$

$$\frac{V_{out}}{V_{in}} = \frac{\frac{Z\left(1+\frac{Z_F}{Z_G}\right)}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}}{1+\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}} \tag{B.18}$$

The equivalent block diagram for the non-inverting configuration is shown in Figure B.7.



$V_{in}$
+
Σ
-
$\frac{Z\left(1+\frac{Z_F}{Z_G}\right)}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}$
$V_{out}$
$\frac{Z_G}{Z_F+Z_G}$

Figure B.7: Block diagram of the non-inverting *CFA*

## B.4 Developing the inverting circuit equation

Equation (B.19) is the current equation at the inverting input of the circuit shown in Figure B.8. Equation (B.20) defines the dummy variable $V_x$, and the (B.21) is the output circuit equation. Equation (B.22) is derived by substituting (B.20) and (B.21) into (B.19), simplifying the result, and manipulating it into the form of (B.4). This last equation is related to the inverting configuration.

$$\frac{V_{in} - V_x}{Z_G} + I = \frac{V_x - V_{out}}{Z_F} \tag{B.19}$$

$$Z_B I = -V_x \tag{B.20}$$

$$ZI = V_{out} \tag{B.21}$$

$$\frac{V_{out}}{V_{in}} = -\frac{\frac{Z}{Z_G\left(1+\frac{Z_B}{Z_F//Z_G}\right)}}{1+\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}} \tag{B.22}$$

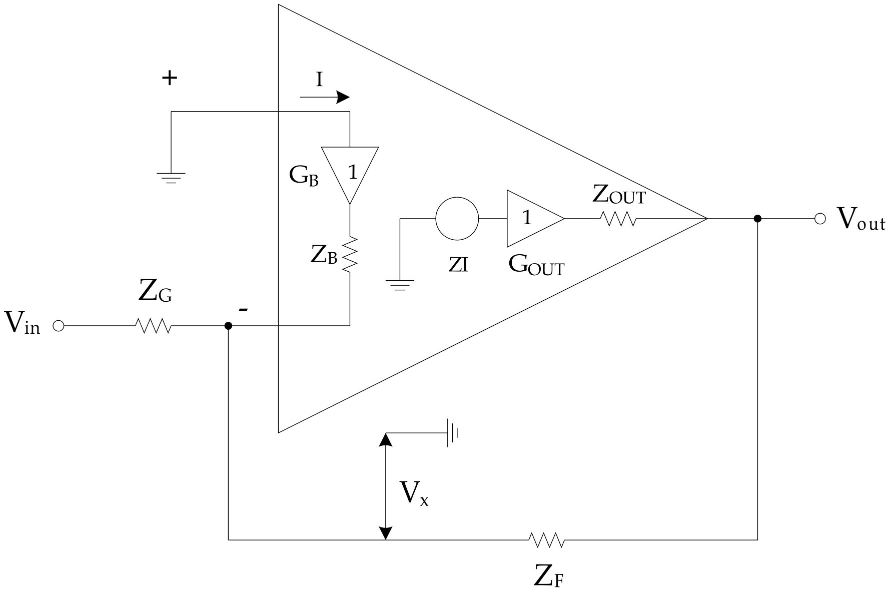


Figure B.8: Inverting circuit diagram

The equivalent block diagram for the inverting configuration is given in Figure B.9.

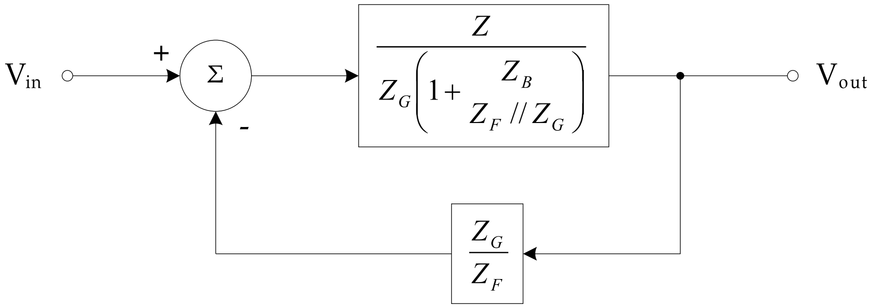


Figure B.9: Block diagram of the inverting *CFA*

## B.5 Stability analysis

Equation (B.8) states the criteria for the stability of a CFA. There are several methods for evaluating the stability of a feedback system, the method used in this explanation is the Bode plot. A sample Bode plot of a single pole circuit is shown in Figure B.10.

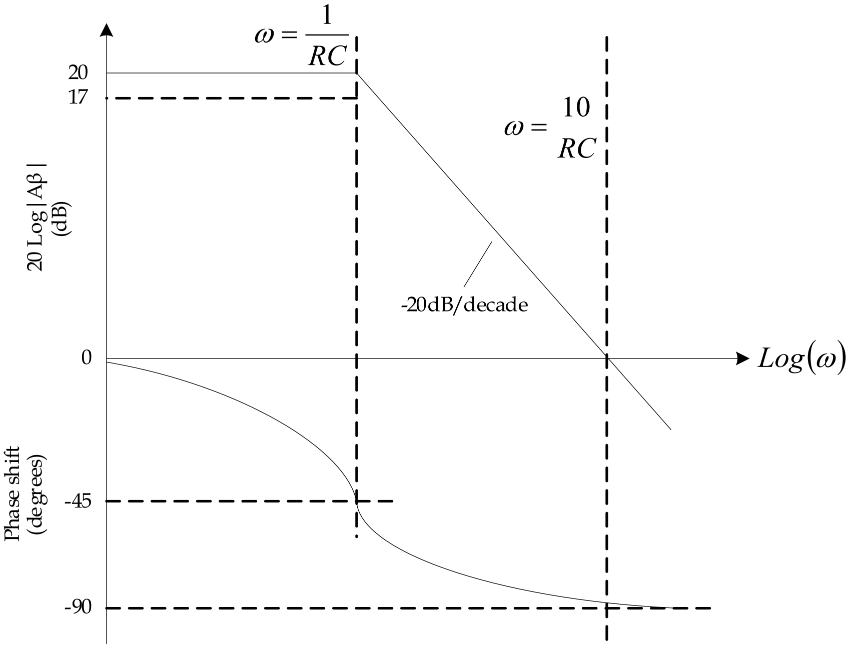


Figure B.10: Sample Bode plot for a single pole circuit

Referring to Figure B.10, notice that the *DC* gain is *20dB*, the amplitude is down *3dB* at the break point, and the phase shift is -*45* degrees at this point. The circuit can not become unstable because the maximum phase shift of the response is -*90* degrees.

*CFA* circuits often oscillate, intentionally or not, thus meaning that there are at least two poles in their loop gain transfer function. Actually, there are multiple poles in the loop gain transfer function, but the *CFA* circuits are represented by two poles for two reasons:

- A two pole approximation gives satisfactory correlation with laboratory results.
- The two pole mathematics are well know and easy to understand.

Equation (B.14) can be written in polar form as (B.23) and (B.24):

$$20Log|A\beta| = 20Log\left|\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}\right| \tag{B.23}$$

$$\Phi = Arctg^{-1}\left(\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}\right) \tag{B.24}$$

The module, $20Log|A\beta|$, has the form $20Log\frac{x}{y}$ which can be written as $20Log\frac{x}{y} = 20Log(x) - 20Log(y)$ . The numerator and denominator of (B.23) are plotted independently and then added graphically for the analysis. Using this procedure the independent variables can be manipulated separately to show their individual effects. Figure B.11 is the plot of (B.23) and (B.24) for a typical *CFA* where $Z = \frac{1M\Omega}{(\tau_1 s+1)(\tau_2 s+1)}$, $Z_F = Z_G = 1K\Omega$ and $Z_B = 70\Omega$.

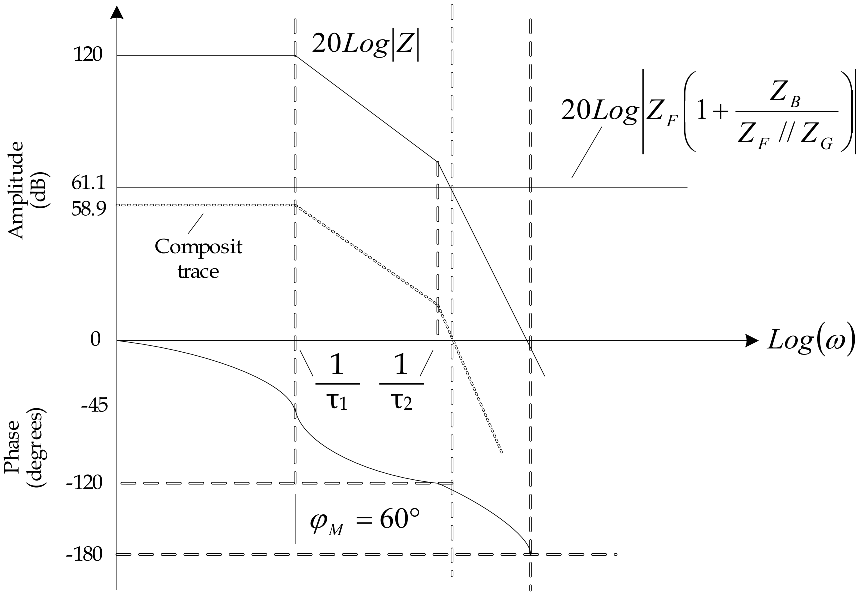


Figure B.11: *CFA* transimpedance plot

If $20Log\left|Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)\right|$ were equal to *0dB* the circuit would oscillate because the phase shift of $Z$ reaches *-180* degrees before $20Log|Z|$ decreases below zero. Since , $20Log\left|Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)\right| = 61.1dB\Omega$ the composite curve moves down by that amount to $58.9dB\Omega$ where it is stable because it has *60* degrees phase margin. If $Z_B = 0dB\Omega$ and $Z_F = R_F$, then $A\beta = \frac{Z}{R_F}$. In this special case, the stability is dependent on the transfer function of $Z$ and $R_F$, and $R_F$ can always be specified to guarantee stability.

The first conclusion drawn here is that $Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)$ has an impact on stability, and that the feedback resistor is the dominant part of that quantity so it has the dominant impact on stability. The main selection criterion for $R_F$ is to obtain the widest bandwidth with an accepted amount of peaking; *60* degrees of phase margin equivalent to approximately *10%*, or *0.83dB* overshoot.

The second conclusion is that the input buffer's output impedance $Z_B$, will have a minor effect on stability because it is small compared to the feedback resistor, even though it is multiplied by $\frac{1}{Z_F//Z_G}$ which is related to the closed loop gain. Rewriting

(B.14) as $A\beta = \frac{Z}{Z_F+Z_B\left(1+\frac{R_F}{R_G}\right)}$ leads to the third conclusion, that the closed loop gain has a minor effect on stability and bandwidth because it is multiplied by $Z_B$, which is a small quantity relative to $Z_F$. It is because of this fact that closed loop gain versus bandwidth independence for the *CFA* is often claimed. However, this is dependent on the value of $Z_B$ relative to $Z_F$.

*CFAs* are usually characterized at a closed loop gain ($G_{CL}$) of one. If the closed loop gain is increased then the circuit becomes more stable, and there is the possibility of gaining some bandwidth by decreasing $Z_F$. Assuming that $A\beta_1 = A\beta_N$ where $A\beta_1$ is the loop gain at a closed loop gain of one and $A\beta_N$ is the loop gain at a closed loop gain of *N*, insures that stability stays constant. Through algebraic manipulation, (B.14) can be rewritten in the form (B.25) and solved to give (B.27) and a new $Z_{FN}$ value:

$$\frac{Z}{Z_{F1}+Z_B\left(1+\frac{Z_{F1}}{Z_{G1}}\right)} = \frac{Z}{Z_{FN}+Z_B\left(1+\frac{Z_{FN}}{Z_{GN}}\right)} \tag{B.25}$$

$$\frac{Z}{Z_{F1}+Z_BG_{CL1}} = \frac{Z}{Z_{FN}+Z_BG_{CLN}} \tag{B.26}$$

$$Z_{FN} = Z_{F1} + Z_B(G_{CL1} - G_{CLN}) \tag{B.27}$$

The difference between the predicted and the measured results is that $Z_B$ is a frequency dependent term which adds a zero in the loop gain transfer function that has a much larger effect on stability. The equation for $Z_B$ is given below.

$$Z_B = h_{IB} + \frac{R_B}{\beta_0+1}\left(\frac{1+\frac{S\beta_0}{\omega_T}}{1+\frac{S\beta_0}{(\beta_0+1)\omega_T}}\right) \tag{B.28}$$

At low frequencies $h_{IB} = 50\Omega$ and $\frac{R_B}{\beta_0+1} = 25\Omega$ which corresponds to $Z_B = 75\Omega$, but at higher frequencies $Z_B$ will vary according to (B.28). This calculation is further complicated because $\beta_0$ and $\omega_T$ are different for *NPN* and *PNP* transistors, so $Z_B$ also is a function of the polarity of the output. Refer to Figure B.12 and Figure B.13 for plots of the transimpedance ($Z$) and $Z_B$. Notice that Z starts to level off at *20MHz* which indicates that there is a zero in the transfer function. $Z_B$ also has a zero in its transfer function located at about *65MHz*. The two curves are related, and it is hard to determine mathematically exactly which parameter is affecting the performance, thus considerable lab work is required to obtain the maximum performance from the device.

Equation (B.27) is an good starting point for designing a circuit, but strays and the interaction of parameters can make an otherwise sound design perform poorly. After the math analysis an equal amount of time must be spent on the circuit *layout* if an optimum design is going to be achieved. Then the design must be tested in detail to verify the performance, but more importantly, the testing must determine that unwanted anomalies have not crept into the design.

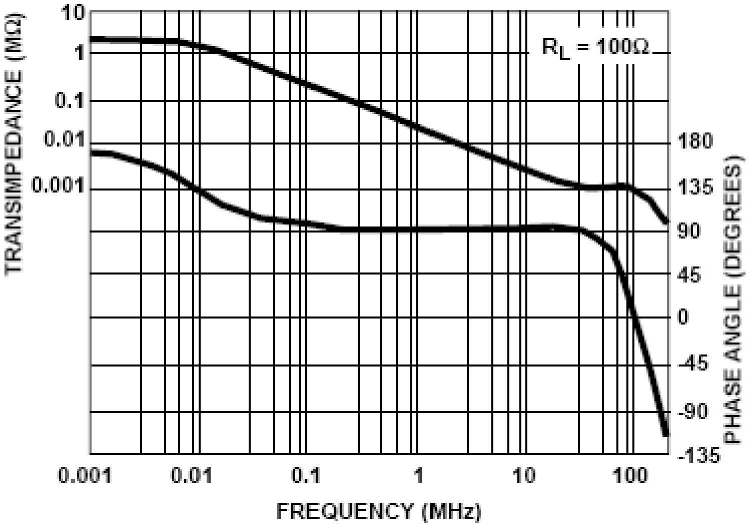


Figure B.12: Transimpedance $Z$ vs frequency

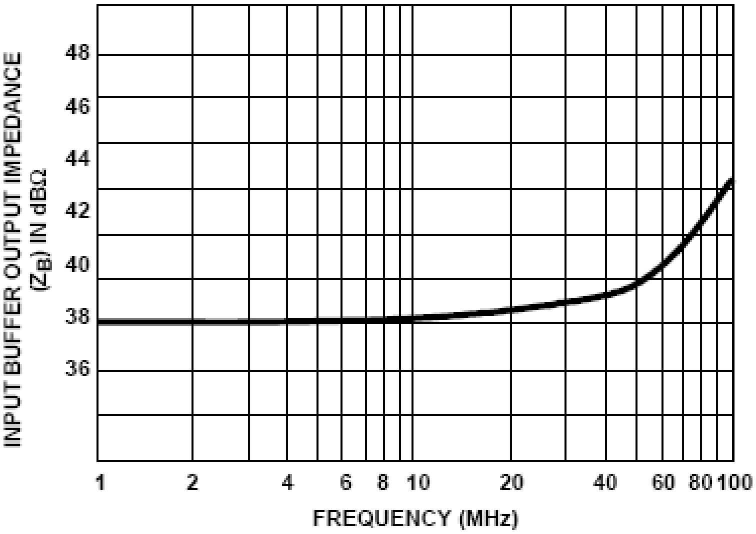


Figure B.13: Input buffer output resistance vs frequency

## B.6 Performance Analysis

Table B.1 shows that the closed loop equations for both the *CFA* and *VFA*, are the same, but the direct gain and loop gain equations are quite different. The *VFA* loop gain equation contains the ratio $\frac{Z_F}{Z_I}$, where $Z_I$ is equivalent to $Z_G$, which is also container in the closed loop gain equation. Because the loop gain and closed loop equations contain the same quantity, they are interdependent. The amplifier gain $a$ is contained in the loop gain equation so the closed loop gain is a function of the amplifier gain. Because the amplifier gain decreases with an increase in frequency, the direct gain will decrease until at some frequency it equals the closed loop gain. This intersection always happens on a constant *-20dB/decade* line in a single pole system, which is why the *VFA* is considered to be a constant gain-bandwidth device.

| **Circuit configuration** | **CFA** | **VFA** |
|---|---|---|
| | **Non-inverting configuration** | |
| Direct gain | $\frac{Z\left(1+\frac{Z_F}{Z_G}\right)}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}$ | $a$ |
| Loop gain | $\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}$ | $\frac{aZ_G}{Z_G+Z_F}$ |
| Closed loop gain | $1+\frac{Z_F}{Z_G}$ | $1+\frac{Z_F}{Z_G}$ |
| | **Inverting configuration** | |
| Direct gain | $\frac{Z}{Z_G\left(1+\frac{Z_B}{Z_F//Z_G}\right)}$ | $\frac{aZ_F}{Z_G+Z_F}$ |
| Loop gain | $\frac{Z}{Z_F\left(1+\frac{Z_B}{Z_F//Z_G}\right)}$ | $\frac{aZ_G}{Z_G+Z_F}$ |
| Closed loop gain | $-\frac{Z_F}{Z_G}$ | $-\frac{Z_F}{Z_G}$ |

Table B.1: Summary of *OPAMP* equations

The *CFA*'s transimpedance, which is also a function of frequency, shows up in both the loop gain and closed loop gain equations, (B.18) and (B.22) respectively. The gain setting impedances, $Z_F$ and $Z_G$, do not appear in the loop gain as a ratio unless they are multiplied by a secondary quantity, $Z_B$, so $Z_F$ can be adjusted independently for maximum bandwidth. This is why the bandwidth of *CFA*'s are relatively independent of closed loop gain. When $Z_B$ becomes a significant portion of the loop gain the *CFA* becomes more of a constant gain bandwidth device. Equation (B.5), which is rewritten here as (B.29), expresses the error signal as a function of the loop gain for any feedback system.

$$Error = \frac{V_I}{1+A\beta} \tag{B.29}$$

Consider a *VFA* non-inverting configuration where the closed loop gain is *+1*; then the loop gain, $A\beta$, is $a$. It is not uncommon to have *VFA* amplifier gains of

*50000* in high frequency op amps, so the *DC* precision is then:

$$100\%\frac{1}{50000} = 0.002\% \tag{B.30}$$

In a good *CFA* the transimpedance is $Z = 6M\Omega$, but $Z_F = 1K\Omega$ so the *DC* precision is:

$$100\%\frac{1075\Omega}{6M\Omega} = 0.02\% \tag{B.31}$$

The *CFA* often sacrifices *DC* precision for stability. The *DC* precision is the best accuracy that an op amp can obtain, because as frequency increases the gain $a$ or the transimpedance, $Z$, decreases causing the loop gain to decrease. As the frequency increases the constant gainbandwidth *VFA* starts to lose gain first than a *CFA*. There is a crossover point, which is gain dependent, where the $AC$ accuracy for both op amps is equal. Beyond this point the *CFA* has better $AC$ accuracy. The *VFA* input structure is a differential transistor pair, and this configuration makes it is easy to match the input bias currents, so only the offset current generates an offset error voltage.

The method of inserting a resistor, equal to the parallel combination of the input and feedback resistors, in series with the non-inverting input causes the bias current to be converted to a common mode voltage. *VFAs* are very good at rejecting common mode voltages, so the bias current error is canceled. One input of a *CFA* is the base terminal of a transistor while the other input is the output of a low impedance buffer. This explains why the input currents do not cancel each other, and why the non-inverting input impedance is high while the inverting input impedance is low. Some *CFAs*, have input pins which enable the adjustment of the offset current. Finding solutions to the *DC* precision problem in *CFAs* is an active research topic.

## B.7 *CFA* summary

The *CFA* is not limited by the constant gain-bandwidth property of the *VFA*, thus the feedback resistance can be adjusted to achieve the best performance for any given gain. The stability of the *CFA* is very dependent on the feedback resistance, and a good start point is the device data sheet, which lists the optimum feedback resistance value for various gains. Decreasing $R_F$ tends to cause ringing, possible instability and an increase in bandwidth, while increasing $R_F$ has the opposite effect. The choice of $R_F$ is critical in a *CFA* design; it is typical to start from data sheet recommendation, test the circuit thoroughly, modify conveniently the value of $R_F$ and then test some more.

As the feedback impedance $R_F$ reach the zero value, the stability decreases while the bandwidth increases; thus placing diodes or capacitors across the feedback resistor will cause oscillations in a *CFA*. The very important point during the *CFA* design is the laboratory work because so much of the performance depends also on the PCB layout. Much of this work can be avoided starting with the recommended manufacture layout rules; it is very useful to use an evaluation board provided by the manufacturer because the layout effort has already been spended in designing it. Remember ground planes and ground connections are fundamental in a radio frequency design. It is difficult that this circuit will function properly without a good ground connection.

Another important point is the use of surface mount components, which avoid phantoms and ghost effects. Several equations are reported in this section, and they are a good design tool, if the assumptions behind them are respected. A typical *CFA* has enough gain bandwidth to ridicule most assumptions under some conditions. All of the *CFA* parameters are frequency sensitive to some degree, and the art of circuit design is to push the parameters to their limit. Although *CFAs* are harder to design with than *VFAs*, they offer more bandwidth, and the *DC* precision is getting better.

# Appendix C

# S-parameters measurement

Considering a two port network inserted in a transmission line, we have the four traveling waves shown in Figure C.1. For example, $E_{r2}$ is made up of that portion of $E_{i2}$ reflected from the output port of the network as well as that portion of $E_{i1}$ that is transmitted through the network. Each of the other waves is a similar a combination of two waves.

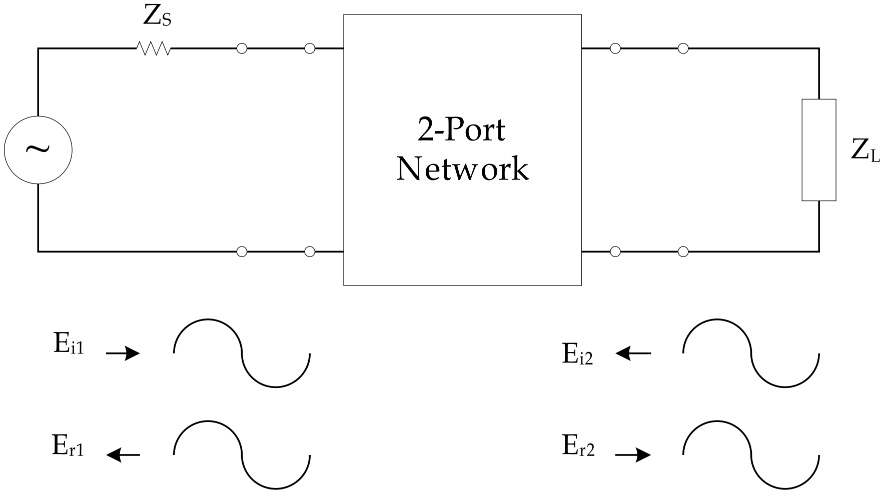


Figure C.1: Transmission line with two-port network tampered

It should be possible to relate these four traveling waves by some parameter set. While the derivation of this parameter set will be made for two-port networks, it is applicable for n-ports as well. Starting from the *H-parameter* set ( C.1):

$$\begin{aligned} V_1 &= h_{11}I_1 + h_{12}V_2 \\ I_2 &= h_{21}I_1 + h_{22}V_2 \end{aligned} \tag{C.1}$$

$$
\begin{aligned}
&V_1 = E_{i1} + E_{r1}; V_2 = E_{i2} + E_{r2} \\
&I_1 = \frac{E_{i1} - E_{r1}}{Z_0}; I_2 = \frac{E_{i2} - E_{r2}}{Z_0}
\end{aligned}
\tag{C.2}
$$

By substituting the expressions for the total voltage and total current (C.2) on a transmission line into this parameter set, we can rearrange these equations such that the incident traveling voltage waves are the independent variables and the reflected traveling voltage waves are the dependent ones (C.3):

$$
\begin{aligned}
&E_{r1} = f_{11}(h)E_{i1} + f_{12}(h)E_{i2} \\
&E_{r2} = f_{21}(h)E_{i1} + f_{22}(h)E_{i2}
\end{aligned}
\tag{C.3}
$$

The functions $f_{11}$, $f_{21}$ and $f_{12}$, $f_{22}$ represent a new set of network parameters relating traveling voltage waves rather than total voltages and total currents. In this case, these functions are expressed in terms of *H-parameters*. They could have been derived from any other parameter set. It is appropriate that we call this new parameter set "*scattering parameters*", since they relate those waves scattered or reflected from the network to those waves incident upon the network. These scattering parameters will commonly be referred to as *S-parameters*.

If we divide both sides of these equations by $\sqrt{Z_0}$, the characteristic impedance of the transmission line, the relationship will not change. It will, however, give us a change in variables (C.4). The following the new variables are defined:

$$
\begin{aligned}
&a_1 = \frac{E_{i1}}{\sqrt{Z_0}}; a_2 = \frac{E_{i2}}{\sqrt{Z_0}} \\
&b_1 = \frac{E_{r1}}{\sqrt{Z_0}}; b_2 = \frac{E_{r2}}{\sqrt{Z_0}}
\end{aligned}
\tag{C.4}
$$

Notice that the square of the magnitude of these new variables has the dimension of power. $|a_1|^2$ can then be thought of as the incident power on port one; $|b_1|^2$ as power reflected from port one. These new waves can be called traveling power waves rather than traveling voltage waves. Looking at the new set of equations in a little more detail, we see that the *S-parameters* relate these four waves in this fashion (C.5):

$$
\begin{aligned}
&b_1 = S_{11}a_1 + S_{12}a_2 \\
&b_2 = S_{21}a_1 + S_{22}a_2
\end{aligned}
\tag{C.5}
$$

For $S_{11}$, we terminate the output port of the network and measure the ratio $b_1$ to $a_1$ (C.6). Terminating the output port with an impedance equal to the characteristic impedance of the transmission line is equivalent to setting $a_2 = 0$, because a traveling wave incident on this load will be totally absorbed. $S_{11}$ is the input reflection coefficient of the network. Under the same conditions, we can measure $S_{21}$, the forward transmission through the network. This is the ratio of $b_2$ to $a_1$ (C.7). This could either be the gain of an amplifier or the attenuation of a passive network.

$$S_{11} = \left[\frac{b_1}{a_1}\right]_{a_2=0} \tag{C.6}$$

$$S_{21} = \left[\frac{b_2}{a_1}\right]_{a_2=0} \tag{C.7}$$

By terminating the input side of the network, we set $a_1 = 0$. $S_{22}$, the output reflection coefficient, and $S_{12}$, the reverse transmission coefficient, can then be measured (C.8), (C.9).

$$S_{22} = \left[\frac{b_2}{a_2}\right]_{a_1=0} \tag{C.8}$$

$$S_{12} = \left[\frac{b_1}{a_2}\right]_{a_1=0} \tag{C.9}$$

# Appendix D

# MATLAB script for stability analysis

```
%SCM MATLAB Script
close all;
rf=0;
cf=0;
rl=0;
cl=0;
cc=0;
rc=0;
while (rf==0)
rf=input('Please insert the feedback resistance value:');
end;
while (cf==0)
cf=input('Please insert the feedback capacitance value:');
end;
while (rl==0)
rl=input('Please insert the load resistance value:');
end;
while (cl==0)
cl=input('Please insert the load capacitance value:');
end;
rc=input('Please insert the compensation resistance value:');
cc=input('Please insert the compensation capacitance value:');
cf=cf*10^-12;
cl=cl*10^-12;
cc=cc*10^-12;
zb=11;
tau1=10^-8;
tau2=10^-9;
az0=10^6;
bz2=tau1*tau2;
bz1=tau1+tau2;
bz0=1;
```

```
numz=[az0];
denz=[bz2 bz1 bz0];
z=tf(numz,denz)
na_0=rf*(rf+zb);
na_1=rf*(rl*rf*cl+zb*(rf*cl+rf*cf+rl*cl));
na_2=rf^2*rl*cl*rf*cf*zb;
da_0=rf;
da_1=rf*(rf*cf+rl*cl);
da_2=rf^2*cf*rl*cl;
numa=[na_2 na_1 na_0];
dena=[da_2 da_1 da_0];
sys_a=tf(numa,dena);
sys=z/sys_a
figure;
bode(sys);
grid;
figure;
rlocus(sys);
grid;
nb_0=rf^2*zb;
nb_1=rf*(rf*cc+zb*(cc+rf*(rl*cl+rc*cc)));
nb_2=rf*(rf*rl*cl*cc+zb*(rf*cc*(cf+cl)+rl*cl*cc*(1+rf*rc)));
nb_3=rf^2*rl*cl*cf*cc*zb;
db_0=0;
db_1=rf*cc;
db_2=rf*cc*(rf*cf+rl*cl);
db_3=rf^2*rl*cf*cl*cc;
numb=[nb_3 nb_2 nb_1 nb_0];
denb=[db_3 db_2 db_1 db_0];
sys_b=tf(numb,denb);
sys=z/sys_b
figure;
bode(sys);
grid;
figure;
rlocus(sys);
grid;
```

# Bibliography

[1] Ross Anderson, Markus Kuhn *'Tamper Resistance a Cautionary Note'* Proceedings of the Second Usenix Workshop on Electronic Commerce, 1996.

[2] D. Boneh and D. Brumley *'Remote timing attacks are practical proceedings of the 12th Usenix Security Symposium'*, 2003.

[3] Dan Boneh, Richard A. DeMillo, Richard J. Lipton *'On the Importance of Checking Cryptographic Protocols for Faults'* Lecture Notes in Computer Science, 1997.

[4] S. P. Scorabogatov and R. J. Anderson *'Optical fault induction attacks'* in B. S. Kaliski Jr., Ç. K. Koç and C. Paar, editors, Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2523 of LNCS, pages 2-12, 2002, Springer-Verlag.

[5] Eli Biham, Adi Shamir *'Differential Fault Analysis of Secret Key Cryptosystems'* Lecture Notes In Computer Science; Vol. 1294, 1997.

[6] P. Koscher, J. Jaffe, and B. Jun *'Differential Power Analisys'* Proc. Advances in Cryptology (CRYPTO '99), Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999.

[7] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, F. Pro *'Energy-aware design techniques for differential power analysis protection'* Proc. Design Automation Conf. (DAT '03), pp. 36-41, 2003.

[8] H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, and W. Zhang *'Masking the energy behavior of DES encryption'* Proc. Design, Automation and Test in Europe Conf. (DAT '03), pp. 84-89, 2003.

[9] G. B. Ratanpal, R. D. Williams and T. N. Blalock *'An On-Chip Suppression Countermeasure to Power Analysis Attacks'* IEEE Trans. Dependable and Secure Computing, Vol. 1, no. 3, pp. 179-189, July-Sept. 2004.

[10] A. Shamir *'Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies'* Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '00), Lecture Notes in Computer Science, vol. 1965, Springer-Verlag, pp. 71-77, 2000.

[11] J. Dj. Golic and R. Menicocci *‘Universal Masking on Logic Gate Level‘* Electronics Lett., vol. 40, no. 9, April 2004.

[12] M. Bucci, M. Guglielmo, R. Luzzi and A. Trifiletti *‘A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors‘* Proc. Int.l Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS ‘04), Lecture Notes in Computer Science, vol. 3254, Springer-Verlag, pp. 481-490, 2004.

[13] M. Bucci, M. Guglielmo, R. Luzzi and A. Trifiletti *‘A Countermeasure against Differential Power Analysis based on Random Delay Insertion‘* Proc. IEEE Int.l Symp. Circuits and Systems (ISCAS ‘05), pp. 3547-3550, 2005.

[14] S. Mangard, T. Popp and B. M. Gammel *‘Side-Channel Leakage of Masked CMOS Gates‘* Proc. Cryptographers‘ Track at the RSA Conference (CT-RSA ‘05), Lecture Note in Computer Science, vol. 3376, Springer-Verlag, pp. 351-365, 2005.

[15] S. Mangard, N. Pramstaller and E. Oswald *‘Successfully Attacking Masked AES Hardware Implementations‘* Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES ‘05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 157-171, 2005.

[16] K. Tiri, M. Akmal and I. Verbauwhede *‘A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards‘* Proc. IEEE 28th European Solid-State Circuit Conf. (ESSCIRC ‘02), 2002.

[17] K. Tiri and I. Verbauwhede *‘A Logic Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation‘* Proc. Design, Automation and Test in Europe Conference and Exposition (DATE ‘04), pp. 246-251, 2004.

[18] D. Sokolov, J. Murphy, A. Bystrov and A. Yakovlev *‘Improving the Security of Dual-Rail Circuits‘* Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES ‘04), Lecture Notes in Computer Science, vol. 3156, Springer-Verlag, pp. 282-297, 2004.

[19] K. Tiri and I. Verbauwhede *‘Place and route for secure standard cell design‘* Proc. Smart Card Research and Advanced Application IFIP Conf. (CARDIS ‘04), 2004.

[20] T. Popp and S. Mangard *‘Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints‘* Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES ‘05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 172-186, 2005.

[21] T. Popp and S. Mangard *‘Implementation Aspects of the DPA-Resistant Logic Style MDPL‘* Proc. IEEE Int.l Symp. Circuits and Systems (ISCAS ‘06).

[22] M. Bucci, L. Giancane, R. Luzzi and A. Trifiletti *‘Three-phase Dual-rail Precharge Logic‘* Proc.Workshop on Cryptographic Hardware and Embedded Systems (CHES ‘06), Lecture Notes in Computer Science, vol. 4249, Springer-Verlag, pp. 232-241, 2006.

[23] M. Bucci, L. Giancane, R. Luzzi, G. Scotti and A. Trifiletti *‘Enhancing Power Analysis Attacks against Cryptographic Devices‘* Proc. IEEE Int. Symp. Circuits and Systems (ISCAS ’06), pp. 2905-2908, 2006.

[24] R. Anderson, E. Biham and L. Kundsen *‘A proposal for the Advanced Encryption Standard‘* AES proposal, 1998.
Available at http://www.cl.cam.ac.uk/ftp/users/rja14/serpent.pdf

[25] W. Rankle and W. Effing *‘Smart Card Handbook‘* 3rd ed., John Wiley & Sons, New York , 2003.

[26] M. Hendry *‘Smart Card Security and Applications‘* Artech House , Boston, 1997.

[27] S. Almanei *‘Protecting Smart Cards from Power Analysis Attacks‘* May 28, 2002.

[28] Manfred Aigner and Elisabeth Oswald *‘Power Analysis Tutorial‘* Institute for Applied Information Processing and Communication University of Technology Graz.

[29] Agilent *‘S-Parameter Design‘* Application Note AN154.

[30] Intersil *‘Current Feedback Amplifier Theory and Applications‘* Application Note AN9420.

[31] Paul R. Gray, Paul J. Hurst, Stephen H. Lewis, Robert G. Meyer *‘Analysis and design of analog integrated circuits‘* 4th ed., John Wiley and Sons Inc., New York, 2001.