Simulating and interpreting EM side-channel attacks at chip level prior to fabrication

Davide Poggi

THESIS TO OBTAIN THE GRADE OF DOCTOR AT THE UNIVERSITY OF MONTPELLIER

In Microelectronics

Doctoral school Information, Structures et Systèmes (I2S)

Research unit UMR 5506

Simulating and interpreting EM side-channel attacks at chip level prior to fabrication

Presented by Davide POGGI
On April 20, 2022

Under the direction of Philippe MAURINE

In front of the jury composed of

Guy Cathebras, Professor, LIRMM	Jury President
Giorgio Di Natale, Research Director, DR CNRS TIMA	Protractor
Guénael Renault, Professor, ANSSI	Protractor
Philippe Maurine, Associate Professor, LIRMM	Thesis Director
Thomas Ordas, Engineer, STMicroelectronics	Member of the Jury
Alexandre Sarafianos, Engineer, STMicroelectronics	Member of the Jury

UNIVERSITÉ DE MONTPELLIER

Acknowledgement

Despite the difficulties encountered in these three years, the doctorate was an experience full of work and personal satisfaction, but all this would not have been absolutely possible without the support of all the people I want to thank in the next few lines.

First of all, I would like to thank my Thesis Director, Philippe Maurine, for for having supervised me during this journey. Your competence and your incredible support have been the backbone of all the results we have achieved. I am really very grateful to you.

I sincerely thank my two Industrial Tutors, Thomas Ordas and Alexandre Sarafianos, for having accompanied, supported and endured me during these three years. You were essential for the success of the thesis, and also two excellent friends on whom I was able to count.

I would like to sincerely thank the members of the Jury, Guénael Renault, Giorgio Di Natale, Guy Cathebras, Victor Lomné, Jérôme Toublanc, Philippe Maurine, Thomas Ordas, Alexandre Sarafianos for assisting my Ph.D defense. I especially thank Guénael Renault and Giorgio Di Natale for taking the time to read my manuscript.

I warmly thank all the STMicroelectronics CSLab team: Yanis Linge, Ibrahima Diop, Valère Dejardin, Christian Cornesse and Olivier Meynard. Thank you for your professional advice and the great environment we have created at work. Working with you has been a pleasure and made this experience much lighter and more exciting. Thanks also to Daniele Fronte, for his support against the mockery of Italy's football results at the World Cup.

I would also like to thank all the members of the STMicroelectronics Architecure team with whom I have collaborated. Thanks to Christophe Laurencin, Benoît Feix, Simon Landry, Stephane Chesnais, Mathieu Lisart, David Roubinet, Diana Moisuc and Fabrice Marinet.

Thanks to my new boss, David Chomaud, for welcoming me to his IP Design team at the end of my PhD.

Thanks to Lorenzo, my best friend, for your strong friendship. Having both done our PhDs at STMicroelectronics in these three years has been incredible, we've come a long way together since we were neighbors in elementary school! If I have reached this milestone it is also thanks to you.

Finally, I would like to dedicate a deep thanks to my family. Spending these three years away hasn't been easy, but your support has never been lacking. To you Marty, Mamma, Papà, Corrado, Potta, Blaccki and Bimbi. Without you, nothing would matter. And to you, Gnoppi, for having accompanied me during these three years in France and five in my life. With Jef and Fortu, we are building a future together.

Abstract

EM side-channel attacks (SCA), which essentially exploit the magnetic field generated by ICs, are commonly used by adversaries to retrieve secret information manipulated by integrated circuits. Due to the increasing resolution and effectiveness of EM equipment used to perform these attacks, it is becoming increasingly difficult to design secure circuits robust enough to resist these attacks. One reason is that there is no CAD tool in literature allowing to check the robustness of ICs against EM SCA prior to fabrication. Within this context, the first contribution of this thesis is the development of a simulation flow able to reproduce the magnetic field radiated by ICs. This flow is based on an industrial voltage drop tool (ANSYS RedHawk) and on the Biot-Savart law. The second and main contribution is a methodology to localize the root cause of leakages in ICs as well as EM hotspots, i.e. positions above the IC surface where an adversary can place its EM probe to capture secrets. The latter contribution is based on the concept of Noise-to-Add which is introduced in this thesis in order to overcome the absence of noise in simulations (noise which is omnipresent in practice) that limits their interpretability. The soundness of the developed simulation flow is demonstrated by confronting, for the first time, experimental and simulated correlation maps. Finally, the flow is used to evaluate the effectiveness of countermeasures against EM SCA at design stage.

Contents

List of Figures

Chapter 1

Introduction

Contents

Introduction

1.1 History of Smart Cards

In 1948, William Shockley, Walter Houser Brattain and John Bardeen created a device that changed our lives forever: the first transistor. From that moment on, thanks to the use of the transistor, there was a real revolution in the electronic field. Indeed, transistors began to be used within all electronic circuits thanks to their reduced space and the ability to amplify electrical signals more effectively than traditional valves.

The development of the first integrated circuits (ICs) allowed to concentrate a huge computational power in a reduced surface. This is how microelectronics was born which has led over the decades to the creation of devices such as laptops and smartphones. Furthermore, technological developments have made it possible to make these products accessible to all. Nowadays, these devices have literally "invaded" our stores and shopping centers. As a result, the current consumerist era we are experiencing leads us to constantly change and buy new and more performing devices.

Starting from the 70s, a new category of devices, that are detailed in chapter 2, appeared on the market: the Smart Cards. These devices can store personal information, such as the social assistance or telephone numbers, and secret codes such as our credit card PIN (Personal Identification Number) and many other confidential information. The fields of application are vast and numerous. They include banking, medical, military and mobile applications.

If on the one hand Smart Cards have obviously positively changed our lives, on the other hand they have introduced several problems, not least those related to their safety and security. In fact, nowadays, the concepts of confidentiality and privacy occupy an increasingly important place for companies manufacturing secure ICs.

To guarantee the security and confidentiality of data, cryptography, which is defined as the Art of writing secret messages, is used to make the data stored in secure circuits intelligible for non authorized people, and accessible for the one who has the so-called secret key. This explains

why one or more crypto-processors, such as the Advanced Encryption Standard (AES) or the Data Encryption Standard (DES), are normally integrated on Smart Cards to protect secure data.

In recent years and decades, the quantity and diversity of attacks carried out to extract data from Smart Cards have increased significantly and therefore great efforts and new technologies have been employed to develop crypto-algorithms to prevent any kind of external attack. Today's algorithms guarantee a strong robustness against logical attacks, which exploit mathematical weaknesses of crypto-algorithms and design or coding errors that occurred during the security tests. On the other hand, less efforts have been devoted to securing the hardware platforms running crypto-algorithms. As a consequence, today there are hardware attacks capable of recovering the secret information contained in ICs. Next section is devoted to a deeper understanding of these attacks.

1.2 Retrieving secrets from Smart Cards: hardware attacks

Hardware attacks are part of a large family of cryptanalytic techniques. They exploit behaviors, representative of certain steps of the encryption algorithms, which can be easily observed through physical syndromes exhibited by their material implantation. Three categories of physical attacks can be distinguished: invasive, semi-invasive and non-invasive attacks.

Invasive attacks [1], [2] act directly on the device, altering its functioning. They can even lead to its destruction, even if they are carried out by experts with specific equipment and skills.

Semi-invasive attacks [3] are a cross between invasive and non-invasive attacks. Like invasive attacks, they involve the access to the circuit without however definitely deteriorating its functioning. An example of a semi-invasive attack are fault injection attacks (FIA) [4], where transient errors are intentionally generated in ICs during their operations to extract sensitive data.

Finally, non-invasive attacks, also called side-channel attacks (SCA), do not require direct access to the device but are based on the observation of the compromising signals emitted by the device while performing out cryptographic operations. A compromising signal is a physical quantity containing information about the data manipulated by the circuit. These signals can be of different nature including: the current consumed by the circuit [5], [6], the radiated electromagnetic field [7], the time required to process the data [8], the emitted heat [9] or light [10], etc. To extract the secret key from these signals, SCA exploit the statistical link between them and the manipulated

data.

Among these three categories, SCA have proven to be the most effective and dangerous as they do not require high skills nor large financial means to be implemented. One of the most used SCA is the correlation power analysis (CPA) which is based on the Pearson correlation coefficient [11], [12]. It was presented for the first time by E. Brier et al. in [13]. This attack is widely used because it is efficient and easy to apply. The idea of this attack is to look for a linear dependence between the transient current flowing in the circuit and the data it manipulates. This attack represents one of the biggest threats for secure IC designers.

An even more dangerous attack is the one that exploits the electromagnetic emissions generated by the currents flowing in the circuit. This attack is called correlation electromagnetic attack (CEMA) but, for the sake of simplicity, in this manuscript and even in the literature, the abbreviation "CPA" is always used to refer to both power and EM correlation attacks. As described in chapter 2, to carry out EM SCA it is necessary to place a probe (a coil) above the surface of the circuit to collect the electromagnetic field radiated (and more precisely the magnetic field) during cryptographic operations. As with the power attacks, collected EM traces are then correlated with the data manipulated by the circuit to get the secret key.

1.3 Context and objective of the PhD

Many publications have demonstrated the effectiveness of SCA in retrieving secure data from ICs, microcontrollers and System on Chip (SoC) [14]. Some present new attacks while others describe countermeasures, but there is little available research material concerning the verification of the robustness of ICs prior to fabrication. This is particular true for SCA exploiting the EM channel. This represents a serious lack if one considers the resources and costs required to re-design ICs and microcontrollers presenting after characterization weaknesses against SCA.

Despite the few publications that have proposed effective methodologies for verifying the robustness of ICs against power SCA [15], [16], [17], [18], no tools has been developed to state that an IC is free of any EM leakage. In fact, the few power analysis tools presented in the literature allow to identify which gates of a design present some leakages but they do not take into account the physical implementation of the circuit and especially the power delivery network.

Consequently, two ICs with the same netlist but with different physical implementations could have completely different robustness against EM attacks. In fact, the power routing strategy, the physical implementation of the various blocks composing ICs and even their floorplan can have an important impact on the electromagnetic field they radiate and therefore on the ease with which an adversary can exploit their EM radiations to retrieve sensitive data. This is why EM attacks are much more dangerous than power attacks.

In [19] Lomné et al. proposed a methodology to model the magnetic field radiated by an IC, using the Biot-Savart law. However, the paper does not provide attack results nor a simulation flow to identify EM leakages prior to fabrication. One reason is the CPU time required to execute the proposed flow that was too long at that period. Following [19], Kumar et al. [7] used CPUs and provided CPA attack results and proposed the first simulation flow to test the resilience of an IC against EM SCA. However, no comparison between experimental and simulated CPA maps were provided keeping thereby designers from knowing if the EM leakages found by simulation (prior to manufacturing) were the same than that found on silicon.

This is the context in which this thesis entitled *Simulating and interpreting EM side-channel attacks at chip level prior to fabrication* took place. Its main objective was to develop a simulation tool allowing to test the robustness of ICs against EM SCA during the design stage, i.e. prior to fabrication. The main requirement was the possibility to identify the leaking hotspots at simulation stage in order to allow re-designing ICs and the fix the bugs before fabrication. Another important goal was the possibility to test and compare different physical implementations of ICs against power and EM SCA.

Motivations for this work were various. Indeed, predicting the weaknesses of a design before it is manufactured is essential in order to modify the design and sell a safe product. This is all the most true since applying software or hardware patches after fabrication is often economically prohibitive and degrades the system performances.

This PhD project took place over 3 years (2019-2022) thanks to a collaboration between the STMicroelectronics company and the LIRMM research laboratory based in Montpellier (France), where authors of [20] work. The I2S Doctoral School of Montpellier was also part of this project. STMicroelectronics is one of the most famous semiconductor company and, among other things,

design and markets secure ICs. In particular, research activities carried out during this thesis took place at the CSLab team of the Secure Microcontroller Division (SMD) of STMicroelectronics in Rousset, in the south of France. The engineers of this team are specialized in verifying the security of STMicroelectronics products against various types of attacks, among which SCA and FIA. Carrying out these research activities directly within the company was an immense fortune, because it allowed to get in touch with the world of industry and to familiarize with the needs and problems related to the manufacturing and design of electronic components. Furthermore, the work done during this PhD could be integrated into ST design flow.

1.4 Structure of the manuscript

Beyond this short introductory chapter, this manuscript is organized around five chapters describing the researches carried out during this thesis as well as the results obtained and possible perspectives. These researches allowed to propose new ideas and solutions related to the simulation of EM SCA prior to fabrication. Next paragraphs describe the content of each chapter.

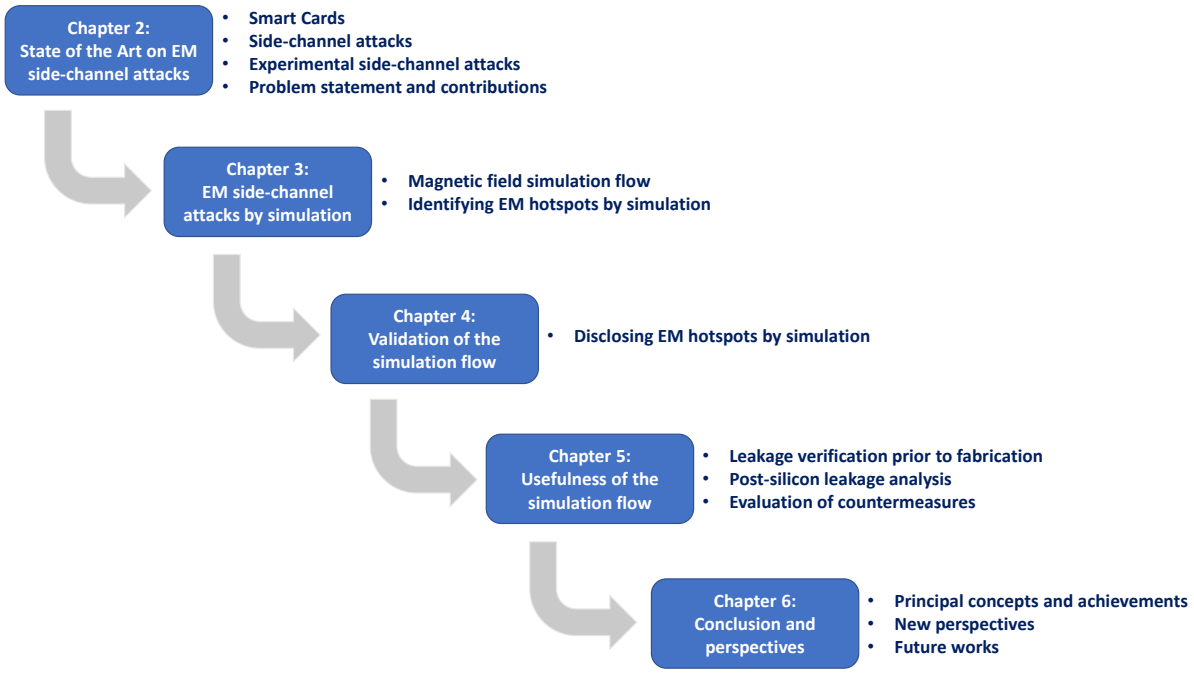

Figure 1: Structure of the manuscript.

- Chapter 2: the first part of this chapter is dedicated to the state of the Art on SCA. Then, it provides all the tools and knowledge needed to understand the following chapters. It also presents the structure of a Smart Card and the AES, the most widely implemented algorithm in such device. In the second part, the methodology and the platforms required to perform both power and EM SCA are described. Finally, a description of the scientific context in which the research subject of this thesis took place is given, as well as the issues to be solved. This last part above all also explains why it is so important to develop a design flow able to identify EM leakages prior to fabrication.

- Chapter 3: it constitutes the heart of the manuscript. It presents a simulation flow of the magnetic field generated by ICs. Then, it proposes a methodology to perform EM SCA by simulation. Given the absence of noise in EM traces simulated with this EM flow, it then explains why it is helpless. This leads to define a new concept, called Noise-to-Add, able to correctly identify EM hotspots by simulation. EM hotspots are the positions above ICs where an attacker can place an EM probe to retrieve a secret.

- Chapter 4: this chapter is dedicated to numerous validations of both the simulation flow and the Noise-to-Add concept. These validations are done by comparing experimental and simulated correlation (CPA) maps obtained on a testchip manufactured by STMicroelectronics.

- Chapter 5: it presents the usefulness of the proposed simulation flow during the design phase of a secure IC. It also highlights the added value of this type of tool compared to a "simple" power analysis tool. In particular, the flow is first used to verify the robustness of an IC against EM SCA during the simulation stage. Secondly, it is used to evaluate the effectiveness of possible countermeasures and to compare different physical implementations of the same design during the design stage.

- Chapter 6: this is the concluding chapter of the manuscript. It consists in a summary of the main works carried out but also of the most important results obtained during these 3 years. It also introduces some perspectives open up for the future and which are, to our opinion, the most interesting leads to investigate in the short and long terms.

After this introductory part, it's time to immerse ourselves in the world of Smart Cards and

SCA. To that aim, next chapters show how dangerous these attacks are and how they can easily break the security of ICs and retrieve sensitive data. This dangerousness sustains the importance of developing tools to verify the robustness of ICs against these types of attacks prior to fabrication. Indeed, once the product has left the foundry it is very expensive, and often too late, to remedy.

Chapter 2

State of the Art on EM side-channel attacks

Contents

Although the data stored in Smart Cards are considered as inviolable and inaccessible, the reality unfortunately shows how more and more attacks allow to retrieve them. EM SCA, which exploit the statistical link between the electromagnetic signals radiated by ICs and the data they process, are among the most dangerous and effective attacks as they do not require exaggerated means and knowledge to be put into practice. This chapter proposes a state of the Art on these attacks.

State of the Art on EM side-channel attacks

2.1 Introduction

This chapter describes in detail the principles of EM SCA and how they can exploit the weaknesses of ICs to retrieve sensitive data from them.

In first part, after an overview on the structure of Smart Cards and on cryptography, it describes an important cryptographic algorithm, the AES, which is nowadays integrated in most Smart Cards. Then, it recalls the most used statistical distinguishers which look for a relation between the power consumed by ICs, or the EM field they radiate, and the data they process. In the second part, an experimental platform allowing to carry out both power and EM SCA is described. An example of EM attack performed on an AES is also provided.

In the third and last part, it is explained why it is so important and urgent to develop a simulation tool allowing to reproduce EM SCA prior to the fabrication of ICs.

2.2 Smart Cards

2.2.1 Brief introduction to Smart Cards

A Smart Card is a device embedding an IC featuring in general a microprocessor and a memory. Smart Cards are therefore capable of storing and manipulating data but also of interacting with the outside world by receiving and exchanging information.

Fig. 2 shows a generic Smart Card. These cards are usually thin and rectangular to easily fit into our wallets and document holders. However, they are also available in other formats and shapes, for instance in passports and ID cards.

Fig. 3 shows the connection pads of Smart Cards. As shown, Smart Cards usually have an 8-pin flat connector embedded on the top of the card. The GND pin is the voltage reference and

Figure 2: A generic Smart Card.

is set to $0V$. The VCC pin supplies the IC with voltages normally ranging between $3.3V$ and $5V$. The Reset is used to reboot the Smart Card during its functioning. There is also the clock signal, which mainly serves to time the communications of the device with a Smart Card reader. Indeed, nowadays, Smart Cards also have an internal clock generator for security reasons. More precisely, if for any reason the external clock signal does not work, the Smart Card must be able to carry out cryptographic operations regardless of what happens outside. The I/O pin is used for exchanging data with readers. Finally, VPP is the programming voltage input (optional pad) and the Reserved pad is dedicated to possible future applications.

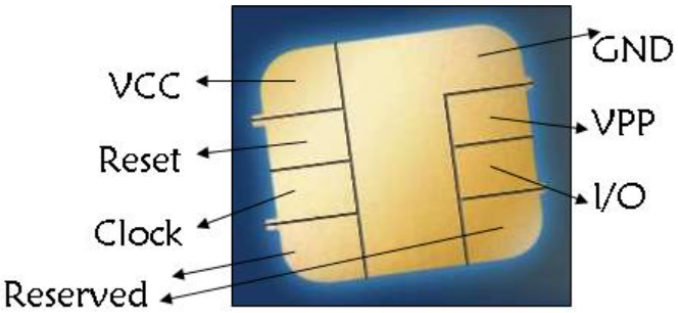

Figure 3: 8-pin flat connector of a Smart Card.

A Smart Card looks like an unassailable device, designed to withstand any type of attack. Unfortunately, the reality is different. New attacks are continually developed and existing ones are enhanced. Companies, such as STMicroelectronics, invest huge resources in developing increas-

ingly reliable and robust countermeasures. Nevertheless, it is always possible to find a way to break the security of a Smart Card. To do so, one needs to dispose of the card, to know the structure and functioning of the embedded crypto-processors, and to have the necessary material to carry out attacks.

For these reasons, few people may be able to seriously attack a Smart Card. However, this is not a risk that can be ignored. This is especially true if one considers EM SCA which are easier to put into practice than other attacks as they do not need to reverse engineer the component and require very little material to be performed.

2.2.2 Architecture of a Smart Card

Fig. 4 shows the standard architecture of a Smart Card. As illustrated, Smart Cards are mainly constituted by three key elements, which are the processor, the I/O system and the memory.

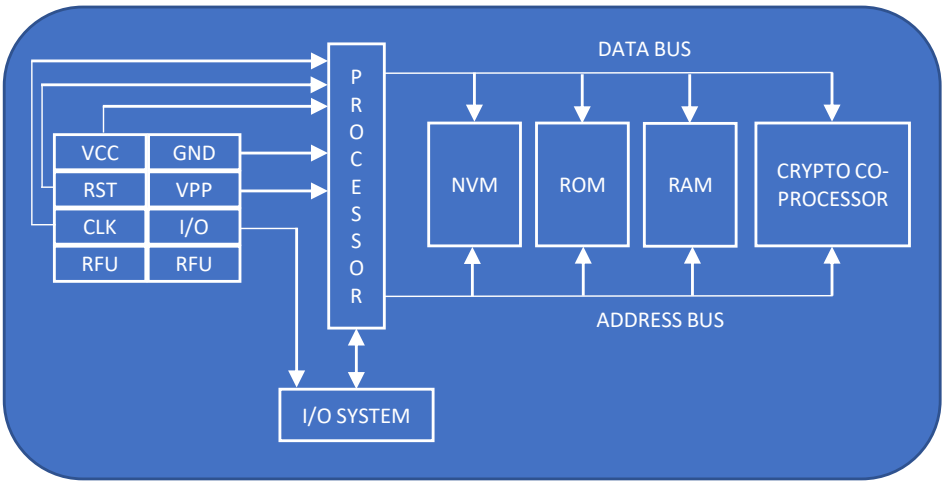

Figure 4: Architecture of a Smart Card.

Processor

This is the key element of the Smart Card, which differentiates it from other types of cards that are only used to store data. Its role is to direct operations and ensure their execution. It continuously queries other blocks of the card to request data or move them to the memory. Moreover, the

processor on Smart Cards is there for security. Indeed, the host computer and card reader "talk" to the processor, and the latter enforces access to the data on the card.

The processor includes three main components such as the ALU (Arithmetic Logic Unit), the control unit and the buses. The buses are fundamental, as they allow the transit of data to and from the processor to the other elements of the card and to peripherals.

Smart Cards often integrate one or several cryptographic co-processors as well. These are hardware modules that include a processor specialized for encryption and related processing. Such devices are built with numerous protection features that prevent unauthorized retrieval of data as well as from having their circuits reverse engineered. Furthermore, the co-processor is used to speed up the calculations.

I/O system

This block performs some input/output functions. It is necessary to allow the card to communicate and exchange information with the outside world. It includes a logic block to work in symbiosis with the processor, to control the timing of operations and the flow of data that are stored in the card memory.

Memory

The memory blocks occupy a large part of the surface of a Smart Card: about 60%. They are manufactured with semiconductor materials, and include cell arrays designed with transistors.

Three types of memories are integrated on Smart Cards. Among them, one can find the RAM (Random Access Memory) which is a volatile memory. This means that it can only save data if the card is connected to the power supply. Data is lost if the power is damaged or disconnected. It is then used as a temporary data repository.

One can also find the ROM (Read Only Memory) which is a memory capable of storing data permanently, even if it does not receive power supply for long periods. It is a read-only memory that is used to contain and distribute firmware, bios and other programs necessary in the boot phase of the device itself. Its content is not editable, except in the design or fabrication phase.

Non-volatile memories (NVM) are also permanent and keep the data even if they are not supplied. However, unlike the ROM, their data can be modified during the operation of the card.

Consequently, NVM are used for saving the user's useful data and applications, even after manufacturing. One of the most used memory is the EEPROM (Electrically Erasable Programmable Read-Only Memory). The latest technological advances have made it possible to develop even more advanced and performing memories such as FLASH memories, which guarantee very fast writing and reading times.

In addition to these blocks and other minor digital blocks, Smart Cards also integrate analog blocks, such as DC-DC converters. These circuits serve to convert one voltage into another and are more and more integrated in low-power designs which use increasingly smaller surfaces and very low power supply voltages (up to $1.2V$). An example are linear regulators. Starting from a fixed voltage (usually coming from a bandgap circuit) they can regulate the output voltage through an internal feedback. Among the regulators, one of the most used is the LDO (Low Dropout Regulator). The advantages of this component are, among others, a smaller device size and a greater design simplicity.

Finally, there is another category of blocks of interest: the cryptographic block ciphers. These blocks are hardened implementations of ciphering algorithms for protecting the data manipulated by ICs from external attacks.

In the first part of next section, after an introduction of cryptology and cryptography, the most common algorithm, the AES, is presented. Then, SCA exploiting the current consumption of CMOS gates to retrieve secrets from secure ICs are described.

2.3 Side-channel attacks

2.3.1 Introduction to cryptology and cryptography

Cryptology was born two millennia ago. It is defined as the science of secrecy, or the ability of a group of people to communicate without other people being able to understand or interpret the information they exchange. A clear message is transformed into an encrypted message by an encryption algorithm, using a secret key.

Cryptology is divided into two branches: "cryptography", which is the Art of writing and reading secret messages, and "cryptanalysis" which includes all the techniques to decrypt a secret mes-

sage. In some cases, cryptanalysis experts have even made it possible to decide the fate of a conflict and thus that of millions of people. For instance, it happened during the Second World War when the British Alan Turing was able to decipher the famous Enigma machine.

Cryptographic algorithms are divided into two large families: symmetric key and asymmetric key algorithms.

Symmetric key, or secret key, algorithms use the same key for both encryption and decryption. In order to communicate, the interlocutors must agree on its value and exchange it. The most widespread symmetric algorithms are the AES and the DES. The advantage of these symmetric algorithms is to have an excellent level of robustness in the face of a not exaggerated key size (less than 256 bits). On the other hand, it is not so easy to speak with the person with whom one wants to agree on a common key, due to the enormous amount of encrypted communications that one daily has through telephones, PCs and televisions.

Asymmetric key, or public key, algorithms solve this problem by using two different keys: one to encrypt and one to decrypt. To send a message to a recipient, one only needs to know its public key to be able to encrypt the message. Once the message is encrypted, it is unreadable, even if the public key is known. To decrypt the message the recipient uses his private key which is known only to him. The biggest disadvantage is that to guarantee the security of these algorithms it is necessary to use large keys. An example of asymmetric algorithm is the Rivest Shamir Adleman (RSA). The key length for this algorithm must be greater than or equal to 2048.

During this thesis products embedding an AES were mainly analysed. For this reason, in the next paragraph this algorithm is studied in greater depth.

2.3.2 Advanced Encryption Standard

The AES, also knows as Rijndael Algorithm, was invented in 1997 by Belgian cryptographers Joan Daemen and Vincent Rijmen for the AES process of the same year. As mentioned, it is a symmetric key algorithm and has been adopted as a standard by the US government and the National Institute of Standards and Technology (NIST). This algorithm is very effective, secure and does not require a lot of memory. It has thus gradually replaced its predecessor, the DES, which is more vulnerable.

As all the encryption algorithms, the goal of the Rijndael Algorithm is to encrypt a plain-text

thanks to a cipher-key. In the AES, the plain-text has a fixed length of 128 bits, while the key can have a length of 128, 192 or 256 bits. Hence the notations AES-128, AES-192 and AES-256 which are used.

The encryption operation of a plain-text is divided into rounds. The number of rounds varies according to the key length: 10 for the AES-128, 12 for the AES-192 and 14 for the AES-256. During the rounds the AES processes two types of data: the *round key*, which is obtained at each round from the original key, and the *state*, which is the temporary result of the latest round. Both the plain-text and the key are composed by matrices composed by N octets. For the AES-128, the state has 4 rows and 4 columns, i.e. 16 octets. If the state is 32 bit longer, the matrix has one more column, and so on up to 256 bits.

As shown in Fig. 5, one can subdivide the AES algorithm in 2 parts: the *Encryption Process*, which serves to generate the cipher-text, and the *Key Schedule*, which allows to derive the round keys from the key. In next paragraphs, these two processes are described for an AES-128.

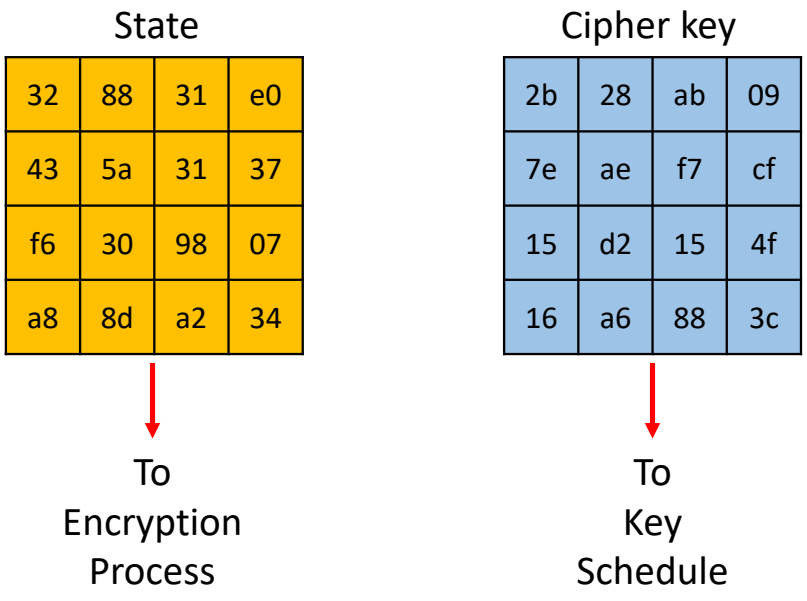

Figure 5: The two processes of the AES algorithm.

Encryption Process

This process starts with the *AddRoundKey* operation which performs an XOR (eXclusive OR), bit per bit, between the secret key and the plain-text. Then, 9 identical rounds made of four 4 basic

operations are performed. The operations are the *SubBytes*, the *ShiftRows*, the *MixColumns* and the *AddRoundKey*. They are described below. For each of these rounds, a round key is generated with the *Key Schedule* process described in the next paragraphs. Finally, there is a 10^{th} round where aforementioned functions are executed except the *MixColumns*. Fig. 6 shows all these functions and their order of execution.

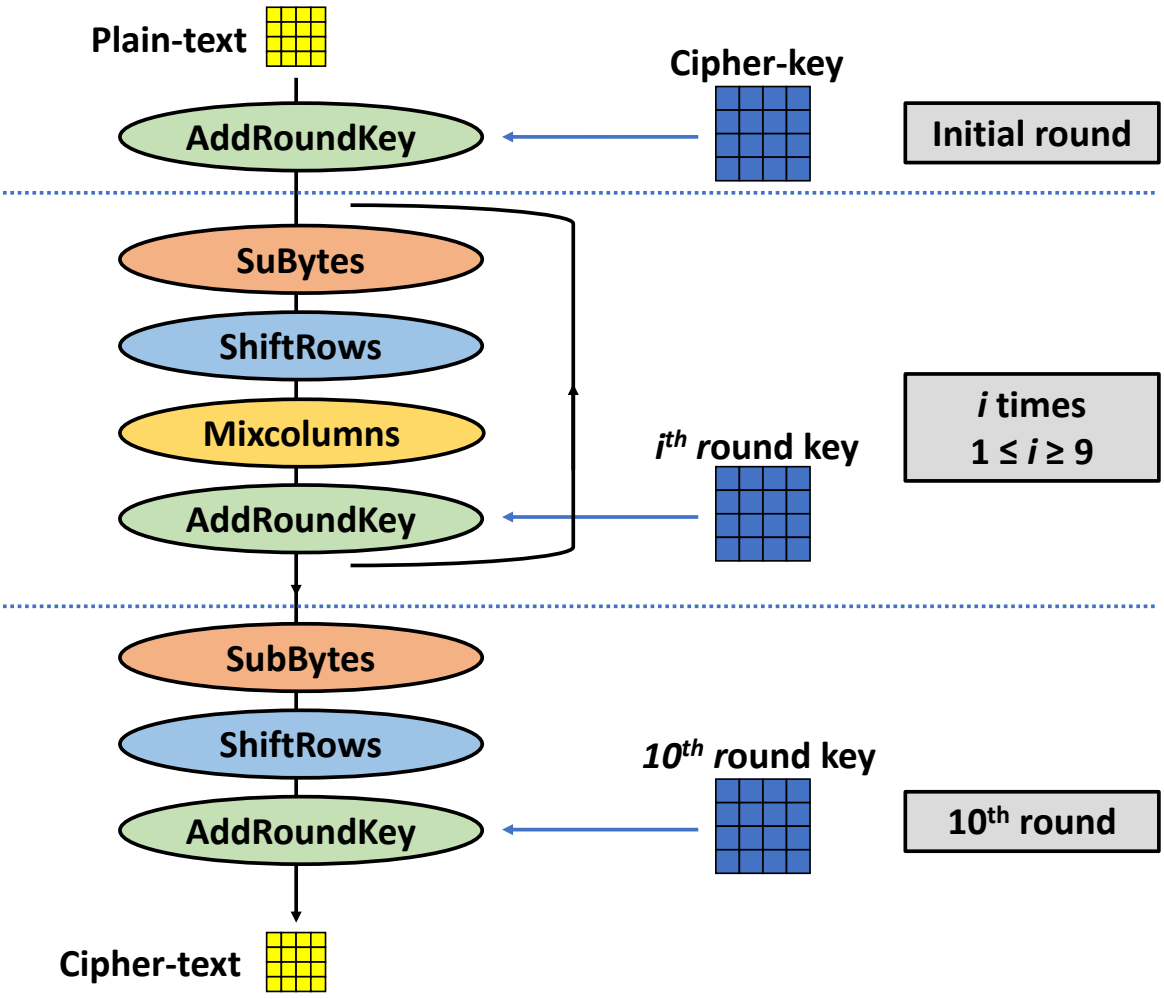

Figure 6: Encryption process of the AES-128.

AddRoundKey. The initial round of the algorithm is just a bitwise XOR (eXclusive OR) between each octet of the round key and the state. To do that, the length of the round key and the state is the same. Note that the first *AddRoundKey* operation is performed with the original key.

SubBytes. This operation is shown in Fig. 7. It consists in replacing each of the 16 octets of the state (4x4 matrix) by another octet. This substitution occurs using an *Sbox*. This latter is a two-input matrix derived from an inverse function in the finite GF field (2^8), often precalculated and stored in a Lookup Table (LUT). Fig. 8 shows the possible values of the *Sbox* in hexadecimal format. In the example of Fig. 7, if the element $a_{2,2}$ is equal to 19, it is replaced by the *Sbox* value found in line 1 and column 9 ($d4$). Then, this element becomes the new octet $b_{2,2}$ of the matrix. *SubBytes* is the only non-linear operation of the AES algorithm.

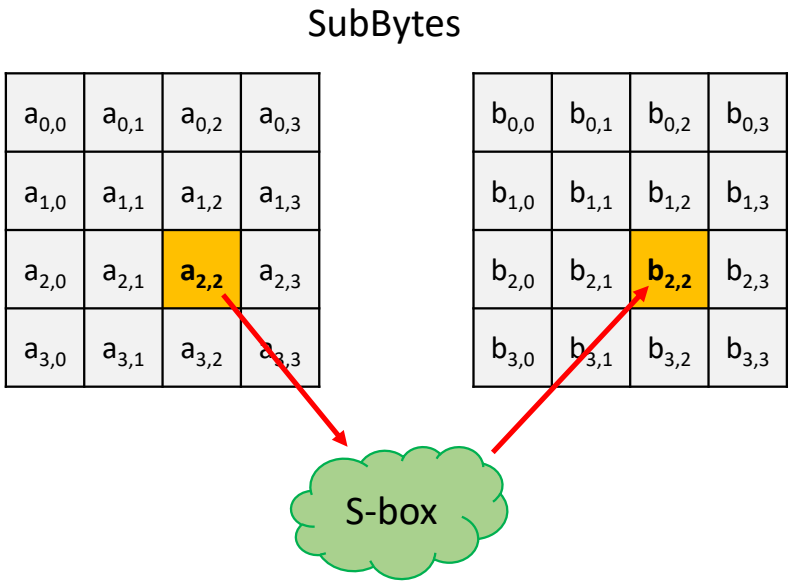

Figure 7: SubBytes operation of an AES-128.

ShiftRows. This operation involves moving each row of the matrix of Fig. 7 (i.e. the state) differently. The first row remains unchanged, the second is moved by one position to the left, the third by two positions and the fourth by three. The operation is shown in Fig. 9. It can be observed that the last column (elements $a_{0,3}$, $a_{1,3}$, $a_{2,3}$, $a_{3,3}$) of the starting matrix constitutes the diagonal of the new matrix after the *ShiftRows* operation.

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 8: Sbox for an AES-128.

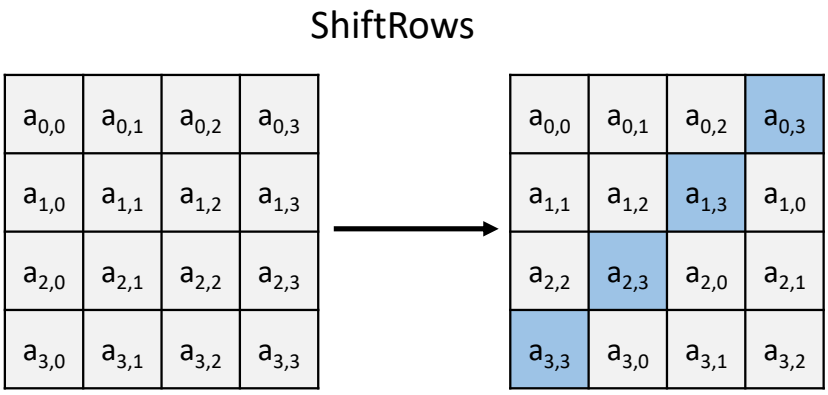

Figure 9: ShiftRows of an AES-128.

MixColumns. This is a linear operation consisting in modulo multiplying the four numbers of one column by a given matrix, as showed in Fig. 10.

In the following paragraph, the procedure allowing to generate all the round keys, namely the *Key Schedule*, which are used during the *AddRoundKey* step is described.

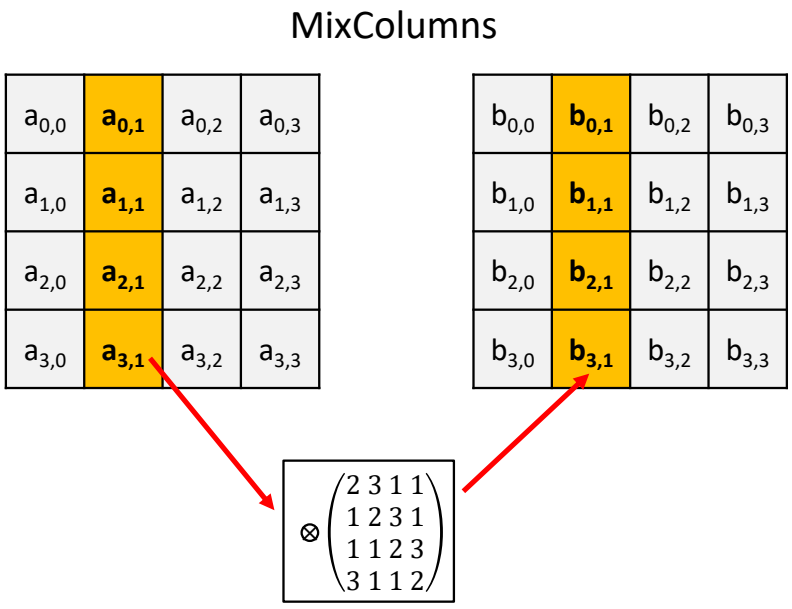

Figure 10: MixColumns of an AES-128.

Key Schedule

This process consists in expanding the original cipher-key into 11 partials keys: the round keys. These keys are used in the initial round, the 9 main rounds and the final round. The expanded key is an array of 44 columns, numbered from 0 to 43, each of which is a 32-bit word (4 octets of 8 bits). The first 4 columns are filled with the 128-bit original cipher-key (16 octets). So the expanded key consists in 44 words, with the following notation: $w_0, w_1, ..., w_{43}$, where each w_i is a word.

The *KeySchedule* process is possible thanks to the *Rcon* matrix (shown in Fig. 11), which contains 10 constants in hexadecimal format, and two operations, *SubWord* and *RotWord* which are described below:

- *SubWord*: it consists in applying the *Sbox* at each word w_i (1 column, 4 octets).
- *RotWord*: this operation rotates the word w_i one position to the left.

The previous paragraphs have described the processes and operations performed by an AES-128 to encrypt a message. Similar processes are carried out by AES-192 and AES-256, but with obviously more bytes and operations.

02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00

Figure 11: Rcon matrix.

Even if the AES or other algorithms are very robust against logical and hardware attacks, adversaries can find a way to access the secret data they process. In the next paragraphs, one of the methods used to break the security of crypto-algorithms is described: the aforementioned non invasive SCA. SCA consist in observing physical signals produced by an IC during its operation, such as the power consumption or its electromagnetic radiations. Next section is of help to understand how the CMOS gates dissipate power and how it is possible to model this power dissipation in order to identify the secret key.

2.3.3 Current consumption of CMOS gates and leakage models

It has been introduced how SCA can break the security of cryptographic algorithms by exploiting the power consumption or the magnetic field of ICs. These physical signals are called leakages. These leakages are created by logic gates implemented in CMOS technology. In fact, the total amount of power dissipated by ICs (and thus the magnetic field they radiate) depends on the number of CMOS logic gates in the circuit, the connections between them and the way they are designed (transistor sizing). It also depends on the switching activity of the CMOS gates, i.e. on the changes of their output state: possible states being of course the logic values “1” and “0”.

The source of power dissipation of CMOS gates can be divided into two contributions: the static and the dynamic power consumption. The static power consumption is the energy consumed by the circuit at rest, that is when there is no functional activity, except that of the analog or mixed blocks which are constantly active. Ideally, the static power dissipation should be zero, but in reality it is not because transistors are not ideal switches. As a result, they exhibit the so-called leakage

currents even when they are at rest. These currents are very weak ($\sim pA$ or nA) but still contribute to the overall power consumption of the circuit since they occur all the time (as soon as the IC is powered).

The dynamic power consumption, on the other hand, groups all the dissipation sources linked to the functional activity of the circuit. Among these, the most important is the energy dissipated by CMOS gates to charge and discharge their output. These commutations, which are the transitions from one logical state to another ("0" to "1" or "1" to "0"), are initiated by clock edges. Therefore the average power dissipated by a logic gate is usually expressed relatively to the period of the clock signal $T_{clk} = 1/f_{clk}$, as shown in the expression below (1):

$$P = Vdd^2 \cdot C_L \cdot \alpha \cdot f_{clk} \tag{1}$$

where Vdd is the supply voltage, C_L the capacitor modeling its charge, α the activity rate of the gate and f_{clk} the clock frequency. The contribution of the dynamic power is usually much more important than the static one, except for very low clock frequency ICs.

To analyse the link between the current consumption and the switching of logic gates one can refer to the CMOS inverter because all D-type-Flip-Flop have as input and output stages an inverter, but also because the switching process of any gate can be modeled by inverters. This model may seem simplistic but in the literature it is widely demonstrated (as in [21] and [22]) that the switching process of all logic gates can be modeled using a simple inverter. This analysis is very important because it allows to introduce the concept of "leakage model". From [23] some considerations can be drawn:

- The transitions "0-0" and "1-1" of the output of a CMOS gate causes a power consumption, and therefore a call of current on the IC power grids, which is almost null. On the other hand, the "0-1" and "1-0" transitions require a much more important call of current. Furthermore, the "1-0" ("0-1") transitions induce higher current peaks than the "0-1" ("1-0") on Gnd (Vdd) rails respectively.

- The consumption of a CMOS gate depends on its output load C_L. In fact, for small values of C_L the current is proportional to the square root of the charge. Exceeded a certain value, the maximum current consumption is limited by the maximum saturation current that the MOS transistor can conduct.

- The maximum value of the current consumed by a CMOS gate is inversely proportional to the rise and fall times of the input ramp [23].
- The activity rate of a CMOS gate is the number of switchings it experiences during a clock cycle in average. From this last consideration, one can derive the definition of the activity rate of a circuit. It is the number of logic gates that switch during a clock cycle in average.

This last point is of particular interest. In fact, it allows to introduce the concept of "leakage model". A leakage model describes how the transitions at the output of CMOS logic gates are related to the measured current consumption.

According to this definition and that of the activity rate, the latter can be associated to two specific leakage models which are described below: the Hamming distance and the Hamming weight models.

The Hamming distance model

This model was first introduced and used by Richard Wesley Hamming in the Information Theory [24]. The Hamming distance (HD) between two strings is the number of characters that must be changed in order to convert one string into the other. A trace of current flowing in an IC can be described by the number of logic gates that switch in a certain time lapse. So, the HD counts the number of "0-1" and "1-0" transitions that occur during a time interval. Following [13], the current consumption of an IC over the time interval $[t, t+1]$ can be defined by calculating the HD between two vectors, x_1 and x_2, representing the bits of two consecutive output states of the CMOS gates:

$$\mathscr{C}(t) = c \times HD(x_2(t+1), x_1(t)) + \eta \tag{2}$$

where $HD(x_2(t+1), x_1(t))$ is the HD between x_1 and x_2, c a constant related to the CMOS technology and η the measurement noise assumed Gaussian with zero mean.

It is thus necessary to know the value of the two consecutive state vectors of the targeted calculation of the crypto-algorithm in order to calculate the HD.

The Hamming weight model

The Hamming weight (HW) is a particular case of the HD model, as one of the two vectors is filled with zeros. As already mentioned, the output of CMOS gates constitutes a variable in the form

of "1" and "0". When one or more bits of a variable change, the load capacitors of CMOS gates are charged ("1-0") or discharged ("0-1"). The HW model counts the number of non-null bits of a variable x_1, i.e. how many CMOS gate outputs must be charged to store that variable. This resumes as in [25] as modeling the power consumption of an IC by:

$$\mathscr{C}(t) = c \times HW(x_1(t)) + \eta \tag{3}$$

where $HW(x_2(t))$ is the HW of x_2.

The HD and HW models of the power consumption of ICs defined above are the basis of SCA; namely the detection of a link between the current or EM traces and the data manipulated by the targeted IC. According to this basis, when an adversary targets the key of an AES-128, he has to detect the sixteen strongest links between the current or EM traces and the 16×256 possible models of the power consumption, i.e. one per byte of the key and one per possible value of this byte.

Next section presents how to generate the power models associated to the 16×256 key hypotheses and and how to identify the correct one using statistical power attacks.

2.3.4 Statistical power attacks

Statistical power attacks are commonly used by adversaries to retrieve secret information manipulated by ICs. These attacks are very popular because no exaggerated means or important skills are needed to identify the secret key manipulated by crypto-algorithms. Indeed, unlike simple power analysis (SPA) ([6], [26]), no detailed knowledge of the structure and implementation of the device is necessary. One only needs to know the algorithm which is executed by the device. On the other hand, collecting a large number of power or EM traces is mandatory. This means that one must have at disposal for a certain time the device in order to perform these attacks, i.e. to collect the required traces.

When collecting power or EM traces, their length (number of samples) is not fundamental. What is most important is the (vertical) resolution of these instantaneous traces because the goal of statistical power attacks is looking for a statistical link between the power consumption $\mathscr{C}(t)$ and

the data processed by the device at a specific instant of time. The vertical resolution of the used oscilloscope is thus important.

The execution of statistical power attacks can be divided in different steps that are listed below. The statistical analysis is the same whether power or EM attacks are performed. What it is different is the methodology used to collect the traces, as described in section 2.4.2.

Collection of traces

The first step is recording the power consumption or EM radiations of the device while the algorithm is executing n cryptographic operations. For this purpose, one needs to known the n processed plain-texts (or cipher-texts), S, of the algorithm. The power traces are then stored in a matrix O with dimension $n \times t$, where t is the length of each trace, i.e. the number of samples. Each power trace o_i, corresponding to the processing of the i^{th} state value ($i \in \{1,...,n\}$), constitutes a row of the O matrix and is denoted as a vector $o_i = [o_{i,1},...,o_{i,t}]$. During the acquisition of the traces, it is very important to set the trigger of the digital oscilloscope so that all the power traces are synchronized on the time axis. This ensures that each column of the O matrix corresponds to the same time and thus to the same operation or processing.

Choice of the intermediate value

The acquisition done, the next step consists in choosing a target value for the attack. This is a specific intermediate operation of the crypto-algorithm. The intermediate value is always a function $\mathscr{F}(s_i,k)$, where s_i is the plain-text (or cipher-text) and k is a byte of the key, denoted sub-key afterwards. On AES block ciphers, it can be for example the i^{th} output of the Sbox.

Then, for each sub-key hypothesis in the set K of possible sub-keys, the intermediate value is computed and stored in a matrix Q. The size of the resulting matrix Q is $n \times K$. Each intermediate value $q_{i,j}$ of the Q matrix is function of the i^{th} plain-text, s_i, and of the j^{th} sub-key hypothesis k_j:

$$q_{i,j}(s_i,k_j) = \mathscr{F}(s_i,K_j), \qquad i \in \{1,...,n\}, \qquad j \in \{1,...,K\} \tag{4}$$

Construction of the power models

Then, one needs to build the $H = (h_{i,j})$ matrix containing all the hypothetical power consumption values by applying the leakage models described in section 2.3.3. If the HW is chosen, this leads to:

$$h_{i,j}(s_i, k_j) = HW(q_{i,j}(S_i, k_j)) \tag{5}$$

Once the models have been elaborated, one has to identify the one representing at best the measures (traces). The set of power traces is then confronted to the 256 power models for each sub-key, time sample by time sample to identify the correct sub-key. This is done by checking the value of a statistic between the K variables $H_j = [h_{i,j}, ..., h_{k,j}]$ and the t variables $P_j = [o_{1,j}, ..., o_{t,j}]$, i.e. the columns of the matrices Q and O.

Comparison between measured traces and model

The more power traces have been acquired, the more n and thus the P_i and H_j variables are long and the more precise the measure of the statistical link is. There are several statistical distinguishers (statistics) to compare these variables. Some of them are described below.

Distinguishers

- Difference of means: it was first introduced by Kocher et al. in [6] to set up the famous differential power analysis (DPA). In order to find out if a sub-key hypothesis k_j is the correct one, the O matrix is split in two sets of power traces according to H_j. The first set $\mathscr{M}_0^j$ contains the traces o_i with $h_{i,j} = 0$ and the the other set $\mathscr{M}_1^j$ those with $h_{i,j} = 1$. Then, two vectors M_1^j and M_0^j are defined. They represent the mean of $\mathscr{M}_0^j$ and $\mathscr{M}_1^j$ respectively. The sub-key used by the device can be individuated by computing the difference between M_1^j and M_0^j (6) for all $j \in K$. In fact, if k_j is the correct key hypothesis, there is a significant difference between M_1^j and M_0^j in some instants of time. If k_j is a wrong hypothesis the difference is small. This leads to estimate the correct key from all the others with the following estimator:

$$\hat{k} = \underset{j}{\operatorname{argmax}}\{max(|M_1^j - M_0^j|)\} \tag{6}$$

- Distance of means: as for the previous method, the two vectors M_1^j and M_0^j are created and the difference of mean computed. But the latter is divided by the standard deviation, V_j of all traces at the corresponding time.

$$W^j = \frac{M_1^j - M_0^j}{V_j} \tag{7}$$

The key is then estimated using:

$$\hat{k} = \underset{j}{\text{argmax}}\{|W^j|\} \tag{8}$$

This approach is close to the use of the T-test [27]. Besides, some people prefer this solution.

- Correlation coefficient: it is involved in the Bravais-Pearson test [11] and is one of the most popular distinguisher. It was first used by E. Brier et al. to set up the well known CPA [13]. The correlation coefficient is used to measure the intensity of an eventual linear link between the two random variables H_j and P_i [11]. The correlation ρ takes a value between $[-1,1]$. The closer ρ is to 1 or -1, the stronger the relationship between the two random variables is. In the case of a SCA, ρ is used to determine a correlation between the P_i and H_j vectors. The correct key k is then estimated using 9:

$$\hat{k} = \underset{j=\{1,\ldots,K\}}{\text{argmax}} \left\{ \max_{i=\{1,\ldots,t\}} \left(\left| \frac{COV(H_j, P_i)}{\sqrt{V(H_j) \cdot V(P_i)}} \right| \right) \right\} \tag{9}$$

In next section, the minimal experimental platform needed to perform power and EM attacks is described. The link between the current and the magnetic field is introduced through simple notions of electromagnetism later.

2.4 Experimental side-channel attacks

2.4.1 Relationship between current and magnetic field

The methodologies exposed so far to attack an IC by exploiting the link between the current consumption and the data manipulated by crypto-processors are also applicable to electromagnetic

radiations. In fact, there is a direct link between the current $I(t)$ flowing in the power grids of ICs and the magnetic field they radiate. Indeed, the Biot-Savart law tells that the magnetic field radiated by a current-carrying wire of finite length L is directly proportional to the current (10):

$$\overrightarrow{B}(t) = \frac{\mu_0}{4\pi} \int_L \frac{I(t) \cdot \overrightarrow{dl} \times \widehat{r}}{r^2} \tag{10}$$

where $\overrightarrow{B}(t)$ is the magnetic field at point P due to an element $\overrightarrow{dl}$ of a wire of finite length L carrying a current $I(t)$; r is the distance from $\overrightarrow{dl}$ to P, $\widehat{r}$ is a unit vector that points from $\overrightarrow{dl}$ to P and μ_0 is the vacuum permeability.

The power and ground network (PGN) of an IC could be seen as a whole of finite wires, each carrying a current and generating EM radiations contributing to the whole magnetic field at point P. Thus, Eq. 10 can be used to model the magnetic field radiated by each of these wires, starting from the current which flows through them. This methodology is described in more detail in chapter 3. The more the variations of these currents are intense, the greater is the radiated magnetic field. Normally, the magnetic field is very intense close to the pads of ICs due to the high currents flowing close to them.

In the following paragraph, the minimal platform needed to perform CPA by exploiting the power consumption or the magnetic radiations of ICs is described.

2.4.2 Measurement setup for CPA attacks

In this section a basic description of a classical measurement setup and its main components is given. Fig. 12 shows the block diagram of such a platform. Below, a look to these components, and how they communicate with each other, is proposed.

- Cryptographic device: this could be a Smart Card or an IC embedding a crypto-processor that is the target of the attack. This device has an interface to communicate with the computer. It receives the plain-text from the computer, which is encrypted and sent back to the computer.
- Power supply: it supplies the power to the cryptographic device under attack. Usual supply voltages for Smart Cards are $5V$, $3V$ or $1.8V$.

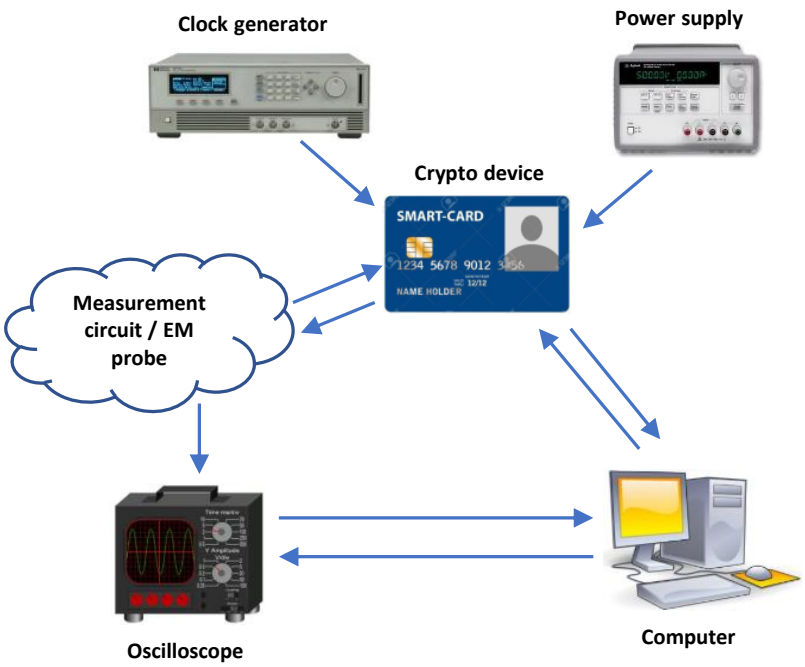

Figure 12: Measurement setup for CPA attack.

- Clock generator: it provides the clock signal to the device under attack. Smart Cards can work with a clock frequency of a few tens of MHz.
- Oscilloscope: it allows visualizing and recording the current or EM traces before sending them to the computer to be stored and processed. Normally, a digital sampling oscilloscope is used.
- Power measurement circuit or EM probe: it measures the power consumption of the device when power analyses are performed. Otherwise, it collects the EM field radiated by the device when performing EM analyses.
- Computer: it manages the communication between all the tools of the platform. It configures the oscilloscope and stores the measurement traces.

To perform both power and EM attacks, the first step is to provide the power supply and the clock signal to the cryptographic device. Then, the computer configures the oscilloscope so that it is ready to record the measurement traces. After this configuration step, the computer sends instructions to the cryptographic device, which starts to execute the crypto-algorithm, such as the

AES. The power consumption or the magnetic field radiated by the device are collected, via the measurement circuit or the EM probe, and then recorded on the oscilloscope and the computer. In parallel, the computer also receives the result of the crypto-algorithm (the cipher-text). This process is often repeated millions of times when performing CPA attacks, mainly because of the noise that affects the measurement traces and makes it harder to correlate the traces with the data manipulated by the device.

Digital oscilloscopes can only measure voltage signals and no other type of physical quantity. Therefore, in order to measure the power consumption or the electromagnetic field it is necessary to generate voltages that are proportional to these physical quantities. One way is to insert a resistor, usually with a value in the 1-10Ω range, between the power or ground pads of the device under attack and the supply source. In this way one can measure the voltage across the resistor extremities which is proportional to the current flowing in the resistor. This is the technique to perform power attacks.

On the other hand, there are several way to perform EM attacks. The most widely used technique is the near-field measurements of the IC, which consists in placing a very tiny EM probe (a coil with a diameter ranging between $50\mu m$ and $500\mu m$ [28]) over the device surface in order to exploit the EM radiations. As shown in details in chapter 3, the variation in time of magnetic lines which pass through the surface of the EM probe generates a voltage across the extremities of this latter. This voltage is the signal recorded by the oscilloscope and sent to the computer to be analysed and correlated with the data manipulated by the device. The measurement setup needed to perform EM attacks has thus more elements that are motorized stages, driven by the computer, able to displace the EM probe over the IC surface with high accuracy ($\sim 1\mu m$). In order to obtain the best possible signal to noise ratio (SNR), one has to place the probe as close as possible to the IC surface ($< 100\mu m$) if silicon is accessible.

Fig. 13a shows an EM probe manufactured by the Langer company. These probes are widely used in the side-channel community because of their high spatial resolution, their large bandwidth and their practical form factor (see Fig. 13b). The latter allows approaching the probe end really close to the IC surfaces enclosed in cavities constituted by the package and the bonding wires. In chapter 3, it is shown that if on one hand this form factor is a key advantage, it also creates a shield that has to be taken into account when one wants to reproduce EM attacks by simulation. What is

important to hold back is the fact that both attacks exploit the current activity of the device. The difference is that power attacks exploit the "global" current activity by measuring the voltage over a resistor, while EM attacks exploit the "local" current activity by capturing the magnetic field radiated by portions of the IC using an EM probe.

In the following section, what has been learnt in section 2.3.4 about statistical power attacks and in this section about the experimental side-channel platform are combined to give an example of CPA attack (thus based on the correlation coefficient) exploiting the EM radiations of an AES-128.

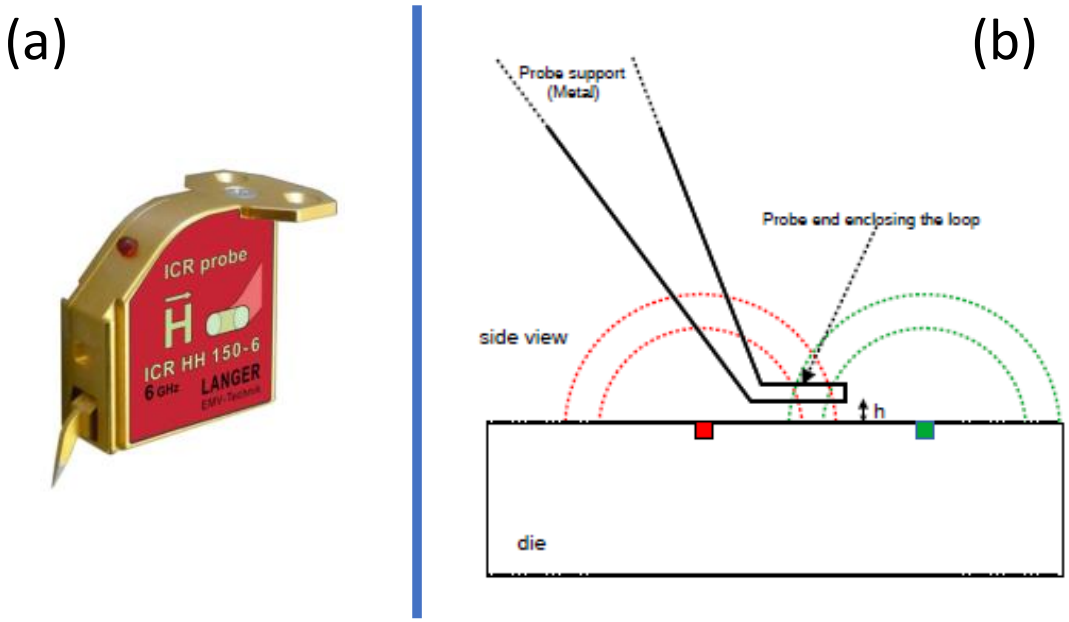

Figure 13: (a) EM probe from Langer company. (b) Form factor of Langer probe.

2.4.3 Example of an EM attack on an AES-128

The CPA exploiting the EM side-channel reported as an example of EM attacks in this section, has been performed on a testchip manufactured by STMicroelectronics. This IC embeds an AES-128. More details about it are given in chapter 3. The performed attack targeted the first output byte of the first Sbox (*SubBytes* operation, see 2.3.2) of the first AES round. This intermediate value was thus a function of the plain-text and the secret key.

The first step done was to place a Langer EM probe (Fig. 13b) over a known leaky position of the testchip surface. Then, 5000 EM traces, corresponding to the encryption of 5000 plain-texts

by the AES, were collected and recorded with a digital sampling oscilloscope. The time sampling was set to $10GS/s$ and the traces were measured over a time window of duration equal to $10\mu s$. As a consequence, the recorded traces had a length of 100000 points. Once all the traces have been recorded, a matrix O with dimension 5000×100000 was obtained.

The measurements achieved, all the possible intermediate values associated to the 256 sub-key hypotheses were computed. This gave a matrix Q with coefficients $q_{i,j}$ defined as:

$$q_{i,j}(s_i,k_j) = Sbox(s_i,k_j), \qquad i \in \{1,...,5000\}, \qquad j \in \{1,...,256\} \tag{11}$$

where s_i is the first byte of the i^{th} plain-text encrypted by the AES and k_j the first byte of the first round key. The resulting Q matrix had dimension 5000×256.

From this matrix Q, the H matrix containing all the hypothetical EM values was computed using the HW model (section 2.3.3). The values of the H matrix are expressed by:

$$h_{i,j}(s_i,k_j) = HW(q_{i,j}(s_i,k_j)) \tag{12}$$

Finally, the last step was to compute the R matrix with dimensions $K \times t$ and coefficients $\rho_{i,j}$ (with $i \in \{1,...,t\}$ and $j \in \{1,...,K\}$. This matrix contained all the correlation traces: one for each sub-key hypothesis, obtained by calculating the correlation coefficient between the measured EM traces and the power models H_j, time sample by time sample. This matrix had therefore dimension equal to 256×100000.

To visualize the results, the modulus of each correlation trace were plotted on a graph which has the time as x-axis and the correlation value as y-axis. Fig. 14 shows the results. One can observe there is one trace, corresponding to one key hypothesis, that stands out from all others. It is related to the secret sub-key used by the device. Furthermore, this graph provides other important information. The instants of time at which the AES processes the targeted output byte of the first Sbox is one of them.

This attack targeted the output of AES first Sbox. However, SCA can target other intermediate values of an AES (or other crypto-algorithms). Indeed, all the intermediate operations which depends on a known variable, such as the plain-text or the cipher-text, and on an unknown variable, such as the secret key, can be easily attacked if the number of key hypotheses remains low ($< 2^{16}$).

The next and last section of this chapter describes in detail the objectives of the Ph.D. The

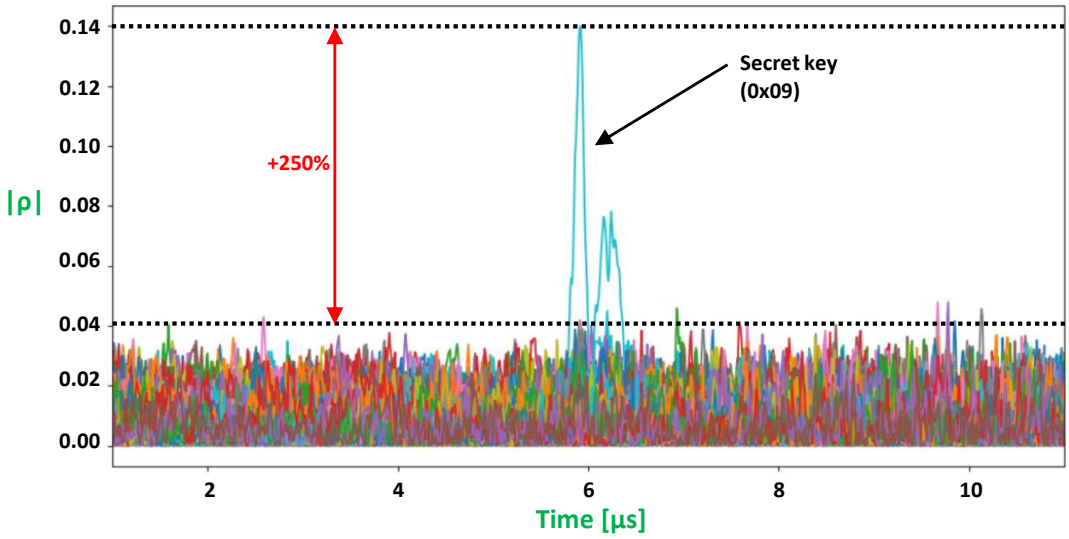

Figure 14: The 256 overlapped correlation traces obtained by attacking the first output byte of the first Sbox of the first round of an AES-128.

limits of the power and EM analysis tools available in literature are also discussed to motivate the development of a simulation flow allowing not only to check if a design is free of any power leakage but also to identify eventual EM leakages prior to fabrication.

2.5 Problem statement and contributions

SCA have demonstrated their potential to reveal secrets from ICs, such as secure micro-controllers and even Systems on Chip [14]. Many of these attacks are now public [6], [29], [13], [30] and the threat is still growing with the emergence of deep learning based techniques [31]. Furthermore, as shown in the previous sections, carrying out these attacks is relatively simple because it is neither necessary to know in detail the algorithm implementation nor to have excessively expensive tools and equipment at disposal. Despite this, few industrial techniques have been developed to verify the robustness of ICs against these attacks prior to fabrication or during the design phase.

This is especially true for attacks exploiting the EM channel. Indeed, while the scientific community has proposed some solutions to simulate power attacks on secure ICs, there is no complete work in the literature allowing to predict EM leakages, i.e. positions over the IC where an attacker

can place an EM probe to capture a leakage and retrieve the secret key.

This has led to relevant problems in the fabrication process of secure devices. Indeed, the costs of fabricating leaking micro-controllers for a foundry as well as the time and resources employed to tediously re-design and suppress leakage sources are enormous.

Because those costs are often prohibitive for ICs already deployed in their operating environment, software patches are often applied to suppress or limit the risk. However, this solution usually degrades the performances.

Among the publications proposing a solution to assess the robustness of circuits against power attacks, one can find [15]. In the latter, authors did use back-annotated Hspice simulations to assess the efficiency of a countermeasure (a new logic style named wave dynamic differential logic) against DPA. A major drawback of such an approach is the CPU-time cost of Hspice simulations and therefore its limitation to small size circuits or logic blocks. To overcome this limitation, it was later proposed in [17], [16] to use Synopsys Nanosim rather than Hspice. Despite this enhancement, such an approach remains limited to low complexity circuits such as DES and AES crypto-processors or small processors.

With this approach limited to low complexity devices, authors of [18] suggested the use of SystemC simulators to assess the robustness of embedded codes running on processors or systems on chip. However, this came at the cost of simulation accuracy. Indeed, applying this approach requires replacing Hspice simulation models by a simpler power model, namely the HW of processed words. Such simulators should thus be viewed as a technique to detect major security flaws in embedded codes rather than in physical implementations.

Reproducing EM attacks by simulation is more complex. In fact, the required simulation tool must be able to take into account the magnetic field radiated by each block of the IC and the coupling effects that are created between them. The first models [32], [33], [34] used to emulate the magnetic field emitted by ICs were found to be effective. However, they are too coarse grain for the design of secure ICs, or they present too long and expensive execution times.

[19] is one of the first works which introduces a solution allowing to simulate the electromagnetic field radiated by modern micro-controllers with high spatial and time resolutions and reasonable CPU time costs. The proposed technique is based on the use of voltage drop analysis tools, commonly involved in the final verification of timings, to derive the currents flowing in

all wire segments constituting the PGN. With such data, authors demonstrated that by using the Biot-Savart law (Eq. 10) one can reconstruct maps of the electromagnetic field radiated by entire circuits. However, they did not propose any attack results as it is the case in [7].

The authors of [7] followed the same approach than [19] and gpus to speed up electromagnetic field calculations. As a result, they were able to perform CPA by simulation. CPA was first introduced in [13] and, since then, has become the most common SCA. Even if this work is quite interesting, its major limit is that there is no comparison between experimental and simulated correlation maps.

After this quick overview about the techniques to reproduce power and EM attacks by simulation, one may wonder why is it necessary to verify the robustness of ICs against EM attacks if there are tools allowing to state that a design is free of any power leakage? If a design does not present power leakages, why could it present EM leakages? And why could an EM probe be able to capture a leakage which has not been disclosed by a power analysis tool?

These questions are legitimate, especially considering that, as shown in section 2.4.2, both attacks exploit the same physical variable: the current consumption. In fact, in both cases one measures the voltage that is related to the current consumption of the crypto-processor integrated on the device. However, there is an important difference between power and EM analyses which makes this latter more powerful: its locality. Indeed, power attacks can only measure the global power dissipated by ICs, while an EM probe can be placed on specific positions of ICs and over specific components (such as the AES, the RAM, etc...). In this way, one can get information only related to the component on which the probe is placed. This means that the EM radiations captured by the probe are less influenced by all the non-cryptographic operations performed by the device which may obfuscate the critical activity in crypto-processors. This is why EM probe can capture leakages that are not identified by a power analysis, especially if the probe is placed very close to the IC surface (few μm) in order to have the best possible SNR.

As a result, and as reported in the literature through concrete examples, EM attacks are able to retrieve the secret key more effectively (with fewer traces) than power attacks. This is also because by placing the probe very close to the crypto-processor one can isolate leaking blocks from the rest of the IC. This means that EM attacks are less sensitive to the noise coming from other blocks [7].

Above all, as aforementioned, power analysis tools do not take the physical implementation

of the circuit into account. For instance, the power and ground grids supplying the CMOS gates are not considered by these tools. As a results, different place-and-route strategies do not change the robustness of the chip against power attacks performed by simulation while this is the case in practice. As a consequence, many secure IC designers have to face the following problem: it consists in choosing between two implementations A and B of the same netlist as shown in Fig. 15. Power analysis is performed on both products, showing the same power leakages. However, it could happen that A and B present totally different robustness against EM attacks due to their different physical implementations and power rail distributions. This is obviously not acceptable for designers, as they need to be able to test the vulnerability of a design solution (an implementation) prior to fabrication and not only a netlist.

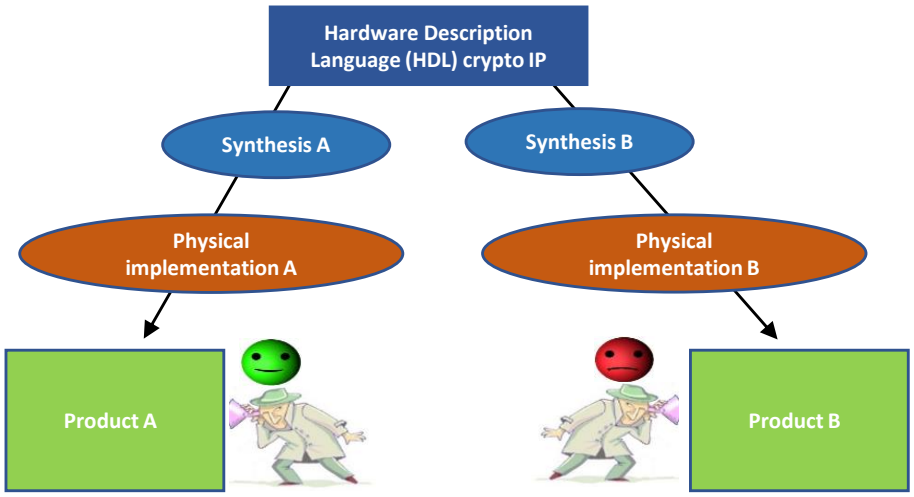

Figure 15: Two products having the same netlist but a different robustness against EM attacks.

Within this context the main objectives of this Ph.D are:

- Developing a tool able to reproduce EM attacks prior to fabrication and taking into account the design implementation of the circuit. To reach this objective, the first step was to develop a simulation flow allowing to emulate the total magnetic field radiated by an IC, with very high spatial and time accuracies. Home made Python scripts have been developed for this purpose. As described in next chapter, they collect and process data obtained with an IR drop tool: RedHawk from ANSYS [35].

- Proposing a rational technique to interpret results obtained with the simulation approach proposed in works [19] and [7]. Indeed, as shown later, drawing correlation maps with such a simulation flow in order to localize electromagnetic (EM) hotspots is no help. This is due to the absence of noise in simulations and above all to a mathematical property of the correlation coefficient from Bravais-Pearson.

- Presenting a simple technique to identify the sources (root causes) of the EM leakages in ICs. These origins, which are denoted as leakage hotspots afterwards, are different from EM hotspots which are defined as the coordinates at which EM probes must be placed above the IC to effectively capture leakages.

- Using the developed flow to test different power routing strategies by simulation and possible countermeasures against EM attacks during the design stage.

- Providing numerous comparisons between simulations and experimental EM SCA to support the soundness of the proposed approach.

2.6 Conclusion

The first part of this chapter has proposed a general introduction to the world of Smart Cards and its main blocks, among which the crypto-processors implementing cryptographic algorithms used to protect confidential data from external attacks. Because the AES is one of the most popular crypto-algorithms, the latter has been presented in detail.

Because secure data are stored under the principle of confidentiality ensured by our electronic documents and bank cards, cryptanalysis techniques aiming at retrieving the secret key stored by secure devices have been developed. The second part of the chapter has thus presented one of the most effective: the SCA. These attacks exploit some physical signals, such as the power consumption or the magnetic field, in order to find a link between the secret data manipulated by the device and these compromising signals. These signals, generated by the switching activity of CMOS gates, are called “leakages” and can be modeled (with leakage models such as the HW) and analysed using different statistical distinguishers. Among them, the well known correlation coefficient involved in the CPA has been introduced.

In the third part of the chapter, the mathematical relationship that binds the current flowing in the power grids of ICs and the magnetic field radiated has been presented as well as the measurement setup needed to perform power and EM attacks. An example of an EM attack on an AES-128 has also been presented.

Finally, it has been shown why power analysis tools are not sufficient to design secure ICs and why EM attacks can find a leakage even in designs free of any power leakage. Thus, the importance of developing a simulation tool able to reproduce the magnetic field radiated by entire ICs (whose PGN can be modeled as a set of current-carrying wires of finite length) and to predict the EM leakages and their sources prior to fabrication has been highlighted.

Next chapter is dedicated to the presentation of the developed simulation flow. In a first step it presents how to model the magnetic field of an entire IC starting from the model of the magnetic field generated by a simple current-carrying wire of finite length.

Chapter 3

EM side-channel attacks by simulation

Contents

SCA exploiting the EM emanations of ICs have demonstrated their effectiveness in retrieving secrets from secure ICs. As a consequence, it has become more and more difficult to design ICs free of any leakage as EM SCA need only one leaky position over the IC surface to extract the secret key. Hence, the importance of developing a methodology to identify EM hotspots during the design stage of a chip in order to be able to fix the leakages and design robust ICs. This chapter proposes, to the best of our knowledge today, the first and complete solution to overcome the lack of such a tool in the literature.

EM side-channel attacks by simulation

This chapter presents a simulation flow able to perform EM SCA by simulation. Furthermore, it overcomes the lack of noise in simulations by introducing an innovative methodology to draw correlation (CPA) maps by simulation.

3.1 Introduction

The contributions of this chapter are manifold.

First, it presents a simulation flow able to model the magnetic field radiated by entire ICs starting from the analysis of the magnetic field radiated by a simple current-carrying wire. This flow is part of the continuity of [19] and is based on RedHawk, a commercial IR drop tool from ANSYS.

Second, it shows that because simulations are noise-free correlation maps are not helpful in identifying EM hotspots by simulation. To overcome this problem, a new methodology called Noise-to-Add is introduced. It allows to correctly interpret simulated correlation maps.

Third, the difference between leakage and EM hotspots is discussed and the origin of this difference is explained.

The following paragraphs start by presenting the testchip on which both experiments and simulations have been carried out during this thesis. They also show how performing an EM side-channel analysis on such a circuit with the near-field scan method. Then, all the steps allowing to reproduce faithfully these analyses by simulation are presented. These steps include the extraction of all the currents flowing in the IC, all the electromagnetic computations needed to emulate the magnetic field radiated by the IC and finally the computation of the signal collected by the EM probes used to perform such attacks.

Modeling the magnetic field of an entire IC is really complex. In fact, a circuit is composed of numerous analog and digital blocks and of different memories. All these elements are supplied by

metal lines constituting the PGN. In order to model the magnetic field generated by an IC, its PGN can be seen as a set of wires carrying a current and generating EM radiations. Thus, one needs first to model the magnetic field radiated by a single wire of finite length and, then, to apply this model to all the wires of the circuit in an efficient manner. Next section illustrates such a model starting from the Biot-Savart law.

3.2 Magnetic field simulation flow

3.2.1 Near-field scan on a STMicroelectronics testchip

This first section aims at presenting the testchip on which EM attacks have been carried out. Moreover, it details how to practically perform EM SCA applying the so-called near-field scan analysis. This step is necessary in order to understand next sections. In fact, one needs to understand how to draw experimental correlation maps in order to be able to reproduce these maps by simulation.

All the analyses reported in this chapter were carried out on a testchip, denoted TCA afterward. The latter is manufactured by STMicroelectronics (Fig. 16). Designed with a $40nm$ low power CMOS technology, it embeds different functional blocks. Among them one can find a full hardware AES-128 co-processor operating at $50MHz$ and placed at the center of the die. The latter is supplied by $1.2V$. The length and width of the die are both equal to $2.2mm$.

Fig. 17 shows the hardware equipment used to communicate with the testchip and the elements needed to perform EM attacks. These equipment are the following:

- Testchip (1): it is mounted over a daughter-board and needs to receive the clock signal and the power supply via external BNC connectors.
- EM probe (2): probes from Langer have been used for our experiments. Probes are driven by motors allowing to displace them with a very high accuracy ($\sim 1\mu m$) over the testchip surface.
- Aardwark adapter (3): it allows the communication between the board and the computer.
- Camera (4): this very high resolution camera allows to visualize the position of probes over the IC surface during a near-field scan.

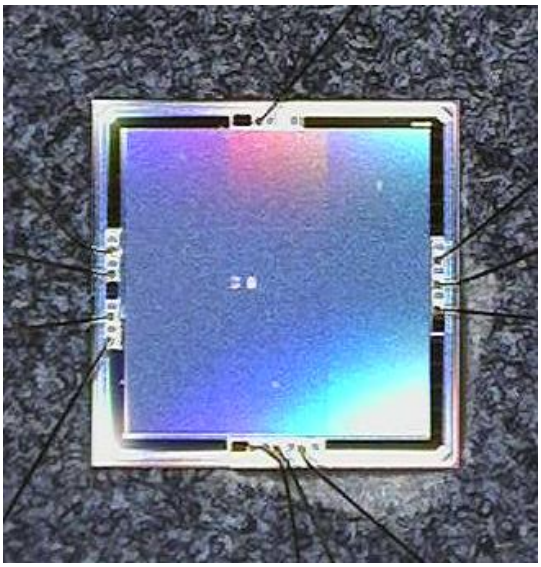

Figure 16: Testchip *TCA* manufactured by STMicroelectronics.

- Clock signal (5): an external clock is provided to the testchip. The clock is generated with a square waveform generator and provided to the board through a BNC connector. The frequency of the clock must be set to $50MHz$ or to a lower value, and the peak-to-peak amplitude must be equal to $5V$ with an offset equal to $2.5V$.
- Power supply (6): the power supply must be delivered through an external source. $5V$ must be applied to the VCC external connector of the mother board.
- Motor (7): three motors are used to drive the probe in each direction of the space (x, y, z) over the IC surface.
- Oscilloscope (8): a Teledyne LeCroy digital oscilloscope is used to record the EM traces collected with the EM probe.
- PC (9): the PC drives all the components of the bench and allows the communication between them.

A Python flow has been developed in order to drive all the elements of the bench. A graphic platform is available for users to precisely place the probe over the IC, select the area to be analysed and launch the attack.

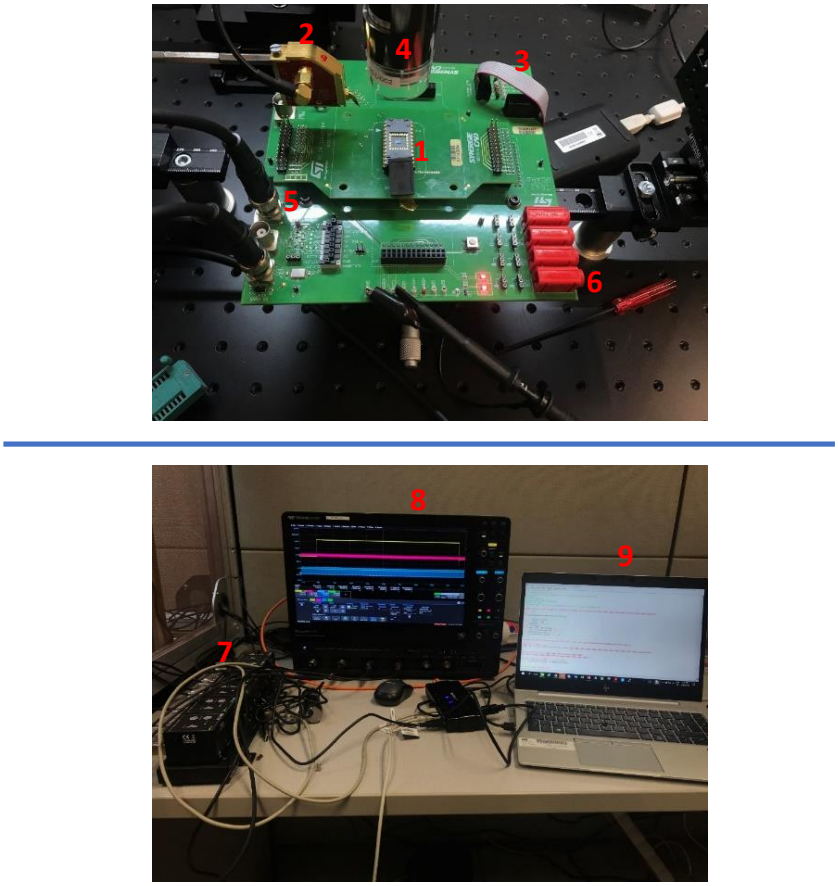

Figure 17: Hardware equipment to communicate with the testchip and perform EM side-channel analyses.

As anticipated in section 2.4.2, the most widely used technique to perform EM SCA is the near-field scan. This technique involves placing a tiny EM probe, with a diameter varying from $50\mu m$ to $500\mu m$ [28], very close to the IC surface (at a height ranging between few microns and $1mm$) in order to have the best possible SNR on the collected EM traces. The probe is thus placed at a given height with the motors (in the so-called "near-field" zone, i.e. no more than one wavelength away from the IC surface [36]) and then displaced over the IC with a displacement step ranging typically between $20\mu m$ and $100\mu m$.

Let's now consider an adversary aiming at performing a near-field scan on TCA in order to draw a correlation (CPA) map disclosing eventual EM hotspots. To that aim, he places a Langer ICR HH100 probe (horizontal probe with diameter $d = 100\mu m$) at a height $z = 100\mu m$ over the

TCA surface (Fig. 18a). Then, he sets the sampling rate of the oscilloscope to $5GS/s$ before launching the main Python script to start the near-field scan.

Many parameters must be provided to the script. Among them one can find the number of curves n to be collected at each position of the scan. Let's consider the adversary sets this parameter to 5000 traces per position. This corresponds to the ciphering of 5000 plain-texts by the AES. This done, he has to select the area to scan and the displacement step of the probe. The probe displacement shown in Fig. 18c is equal to $100\mu m$. As shown in Fig. 18b and 18c, it is possible to scan only the central part of TCA because of the bonding wires limiting the scannable area. Then, starting from the initial position, he displaces the probe over the IC surface and collect 5000 EM traces at each position (Fig. 18c). He then stores the traces in the PC in order to analyse them.

The traces acquired and stored, the analysis he performs consists in applying a CPA to each set of 5000 traces, i.e. at each position of the probe. This done, he draws a correlation map. Each point of this map contains the maximal (absolute value) of the correlation trace obtained with the correct key, k^*, if this value is greater than the values obtained with the other key hypotheses. Otherwise the point contains a 0. Mathematically, this criterion can be expressed as follows:

$$|\rho^*| = \begin{cases} |\rho^{k^*}| \quad \text{if} \quad |\rho^{k^*}| \geq |\rho^k|, \quad \forall k \in K \\ 0 \quad \text{otherwise} \end{cases} \tag{13}$$

with K the set of all the sub-key guesses.

The standard deviation is preferred to the variance.

Fig. 19 shows the resulting correlation map an adversary can obtain for TCA. As shown, there are several EM hotspots, i.e. positions above the IC where it is possible to place a probe to retrieve the secret key.

This simple example highlights that verifying the presence of EM hotspots during the simulation stage of a circuit is of primary importance to design secure ICs. Within this context, next sections aim at presenting a flow able to faithfully reproduce by simulation the experimental near-field analysis an adversary can get. This flow starts with the magnetic field model of a finite length wire. This model is important because, as aforementioned in section 3.1, the PGN of a circuit can be modeled as a set of wires, each of which carrying a current.

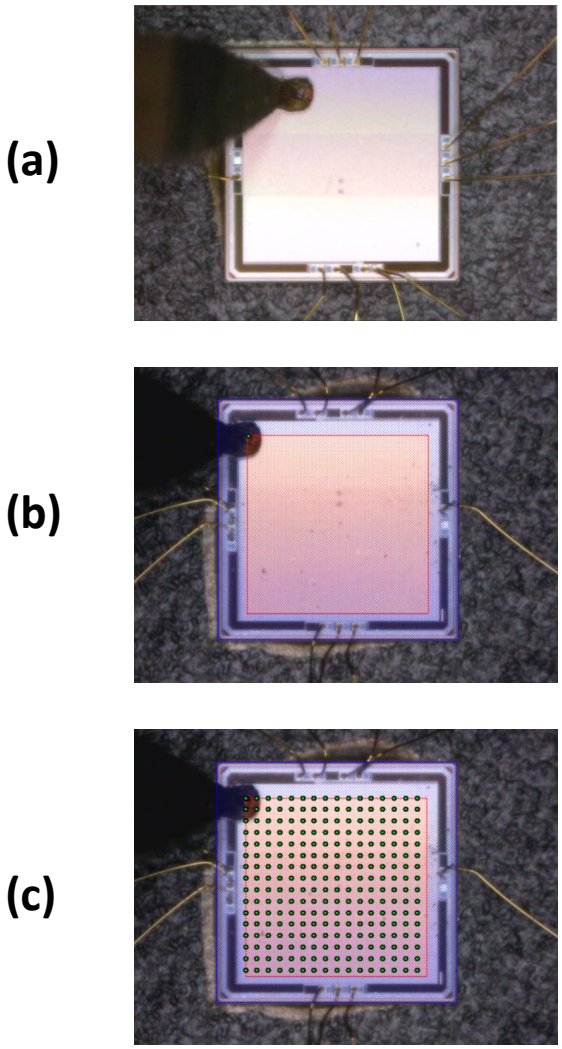

Figure 18: Near-field scan of TCA. (a) Placement of the EM probe over the IC surface. (b) Selected scan area. (c) Collection of n EM radiations at each (x, y) position of TCA.

3.2.2 Metal layers and magnetic field captured by EM probes

Before presenting the magnetic field model of a wire, two important points need to be highlighted in order to ease the reading of next sections. First, performing electromagnetic analyses and near-field scans (as well as reading related publications) has shown that adversaries usually use EM probes made of a single wire loop, most of them fabricated by Langer company. These probes are placed very close to the IC surface (few tens of microns) in order to minimize the measurement noise that pollutes the EM radiations collected by the probe and decreases the attack efficiency.

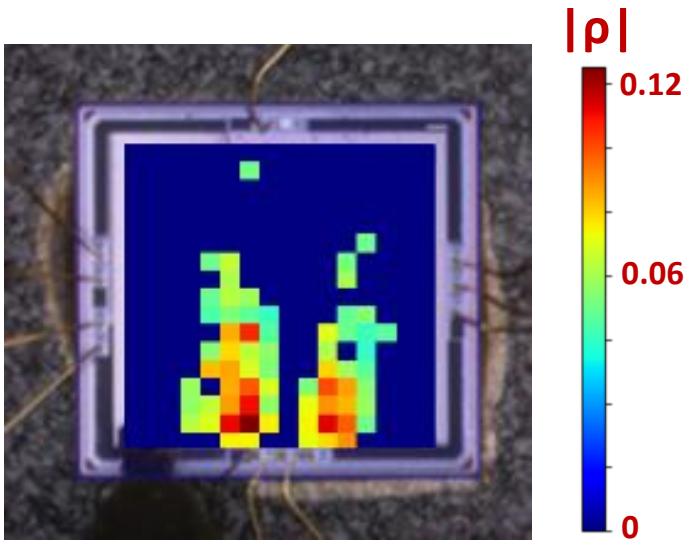

Figure 19: Correlation (CPA) map revealing the leaking areas of *TCA*.

Second, the observation of various layouts jointly with electrical simulations shows that the strongest currents flow in the upper wires of the PGN supplying CMOS gates. These wires, which are the closest to the EM probe (when EM attacks are performed front-side), have a width in a range of $1\mu m$ to $5\mu m$. Comparing the order of magnitude of wire dimensions and the distance separating them with the typical diameter of EM probes ($\sim 100\mu m$), one can thus consider them as finite length wires with negligible width. Therefore, the Biot-Savart law can be used to compute the magnetic field radiated by ICs. In certain cases, one can find n times larger metal wires (width greater than $10\mu m$). In this case, it is preferable to split these large wires into n smaller parallel wires each traversed by a n times smaller current.

Fig. 20 gives a simple sketch of the supply network. It explains why the currents flowing in the upper metal layers of the power and ground grids are stronger than those flowing in the lower metal layers. As shown, the main reason is that the upper part collects all currents from CMOS gates and conveys them to the pads. Fig. 20 also indicates why they are stronger close to the pads. To give numbers, in TCA the top metal layer (AluCap) wires have a width of $5\mu m$ while those routed in Metal1 have a width of only $0.2\mu m$. This means obviously that the Metal1 layer is much more dense than the AluCap layer. Nevertheless, the current flowing in the AluCap layer is about 38 times stronger than in Metal1 ($450\mu A$ and $12\mu A$). For these reasons, one can simplify the model of the magnetic field radiated by ICs by only considering the current flowing in top metal layers.

In fact, given that these layers carry the strongest currents (the current density in these wires is ~ 2 times greater), one can assume that modeling their EM radiations is enough to get an accurate model of the magnetic field. This assumption will be verified, trough concrete examples, in sections 4.2.3 and 4.2.4.

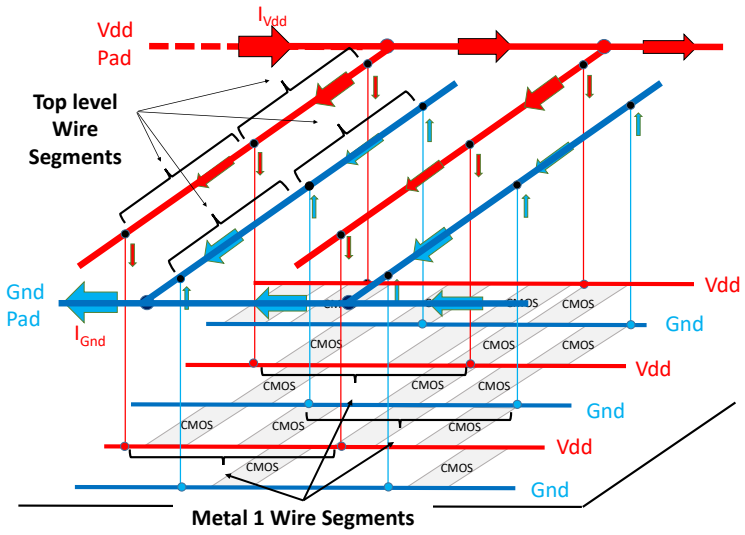

Figure 20: Sketch of the supply network showing the current flows.

3.2.3 Magnetic field radiated by a current-carrying wire

In section 2.4.1, it has been shown that there is a relationship between the current and the magnetic field. Indeed, Eq. 10 states that the magnetic field radiated by a current-carrying wire of finite length in a point P in the vicinity of the wire is directly proportional to the intensity of the current and inversely proportional to the square of the distance r separating the wire and P.

However, the formulation of this law is not convenient for our purposes. Indeed, the magnetic field radiated by the wire has to be expressed as a function of the coordinates x, y and z (see Fig. 21) and, furthermore, the orientation of the current has to be considered. Indeed, all the wires that compose the power rails of ICs are either vertical or horizontal, i.e. parallel to the x or y axis. For this purpose, let's consider Fig. 21. It illustrates a wire of length $\overline{AB}$ crossed by a current $I(t)$ and generating a magnetic field $|\overrightarrow{B}(t)|$ in its neighborhood. One can express the amplitude of $|\overrightarrow{B}(t)|$ as a function of x, y and z, at point P of a surface S placed at a height z over the wire and parallel to it by using Eq. 14:

$$|\overrightarrow{B}(x,y,z,t)| = \frac{\mu_0 \cdot I(t)}{4\pi} \cdot \frac{x}{\sqrt{x^2+z^2}} \left[\frac{1}{\sqrt{(x-x_A)^2+(y-y_A)^2}} + \frac{1}{\sqrt{(x-x_B)^2+(y-y_B)^2}} \right] \quad (14)$$

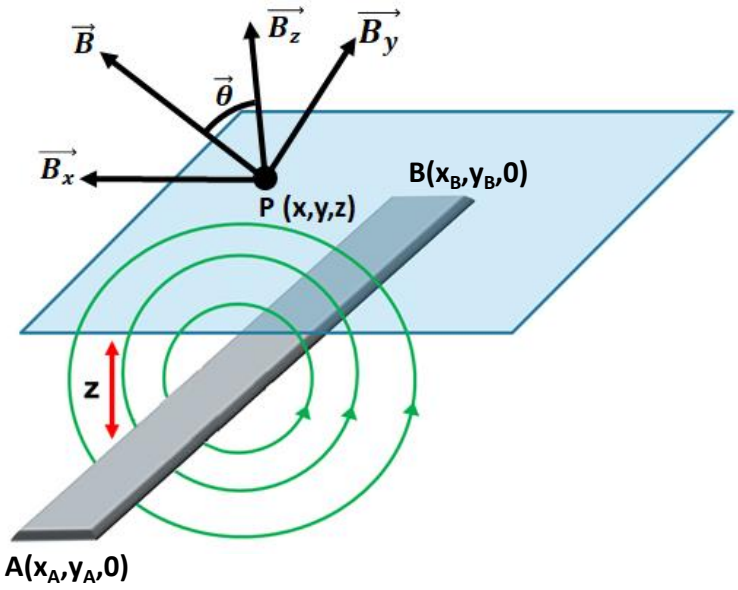

Figure 21: Magnetic field radiated by a wire in its neighborhood.

Eq. 14 expresses the magnetic field radiated by a wire as a function of x, y and z, allowing to get its value at each point (x,y,z) of the surface S over the wire.

One can now determine the expression of the three components of the magnetic field, $|\overrightarrow{B_x}(x,y,z,t)|$, $|\overrightarrow{B_y}(x,y,z,t)|$ and $|\overrightarrow{B_z}(x,y,z,t)|$. The z component is of primary importance because adversaries usually perform EM SCA by using horizontal probes, i.e. probes with coil parallel to the IC surface so that to capture the vertical magnetic field. Eq. 15 and Eq. 16 express the vertical component of the magnetic field depending on whether the wire is vertical or horizontal, respectively:

$$|\overrightarrow{B_{z,v}}(x,y,z,t)| = \frac{\mu_0 \cdot I(t)}{4\pi} \cdot \frac{x^2}{x^2+z^2} \left[\frac{1}{\sqrt{(x-x_A)^2+(y-y_A)^2}} + \frac{1}{\sqrt{(x-x_B)^2+(y-y_B)^2}} \right] \quad (15)$$

$$|\overrightarrow{B_{z,h}}(x,y,z,t)| = \frac{\mu_0 \cdot I(t)}{4\pi} \cdot \frac{y^2}{y^2+z^2} \left[\frac{1}{\sqrt{(x-x_A)^2+(y-y_A)^2}} + \frac{1}{\sqrt{(x-x_B)^2+(y-y_B)^2}} \right] \quad (16)$$

With these equations, it is possible to determine the distribution of the magnetic field generated by a finite wire over a rectangular surface S above it. To that aim, S is split into $(2p+1)\cdot(2q+1)$ small squares of side length w (which must be chosen significantly lower than the diameter of EM probes) so that the center of the matrix coincides with that of the finite wire. One can then compute the two unitary (reference) distributions of the vertical magnetic field over S generated by an horizontal and vertical finite wire using either Eq. 15 or Eq. 16. This leads to the two matrices B^*_H and B^*_V with coefficients:

$$B^*_{V/H}(l,c,z) = \frac{B_{z,v/h}(l,c,z)}{I(t)} \tag{17}$$

with $l \in [-p,...,p]$ and $c \in [-q,...,q]$ and l,c the indexes of the matrix coefficients.

Fig. 22 shows the distributions of the vertical magnetic field of a wire according to its orientation. The wire is placed at the center of the maps and has length $20\mu m$. In this example the maps represent the field over a surface S of $400 \times 400\mu m^2$ obtained with $w = 20\mu m$.

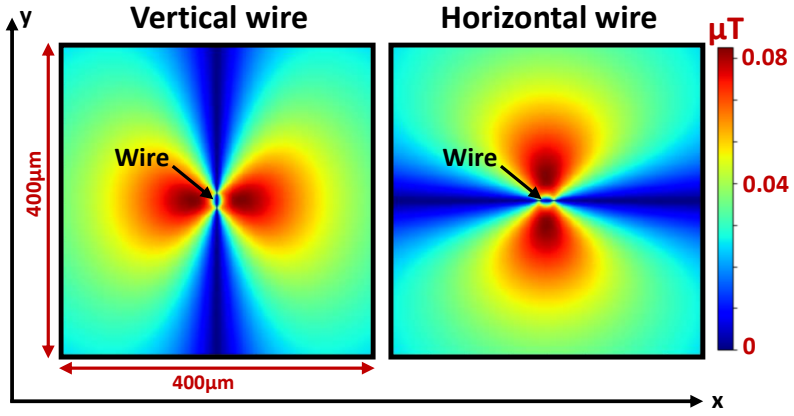

Figure 22: Magnetic field distribution of a vertical (left) and horizontal (right) wire.

These two unitary distributions are of prime importance for the computation of the magnetic field radiated by an IC because their intensive use allows speeding up the calculations. Indeed, several thousands of finite wires are usually necessary to solely model the top layers of the power and ground distributions.

Observing now Fig. 23, which shows the vertical magnetic field radiated by a vertical wire at different heights, one can get important information. First, the vertical component of the magnetic field, radiated by the wire segment, at the vertical of this segment, is null.

Second, when measured over a surface, it reaches its maximal value at a distance from the wire segment which directly depends on z. In the example of Fig. 23, this distance is equal to $26\mu m$ and $4\mu m$ for z equal to $100\mu m$ and $25\mu m$, respectively.

Third, the greater z is, the more the vertical magnetic field can be perceived further from the wire segment, with respect to its maximal amplitude. These observations are illustrated in Fig. 23b and 23c that give maps of $|\overrightarrow{B_z}(x,y,z,t)|$ at different heights (with $x_A = x_B = 0\mu m$ and $y_A = -y_B = 10\mu m$) and the normalized evolution of $|\overrightarrow{B_z}(x,y,z,t)|$ along the bisecting line D. All these observations mean that near-field scans of the vertical magnetic field can not be directly used to determine, with a high accuracy, the origin of leakages in ICs. However, one can observe that reducing z significantly reduces the localization errors.

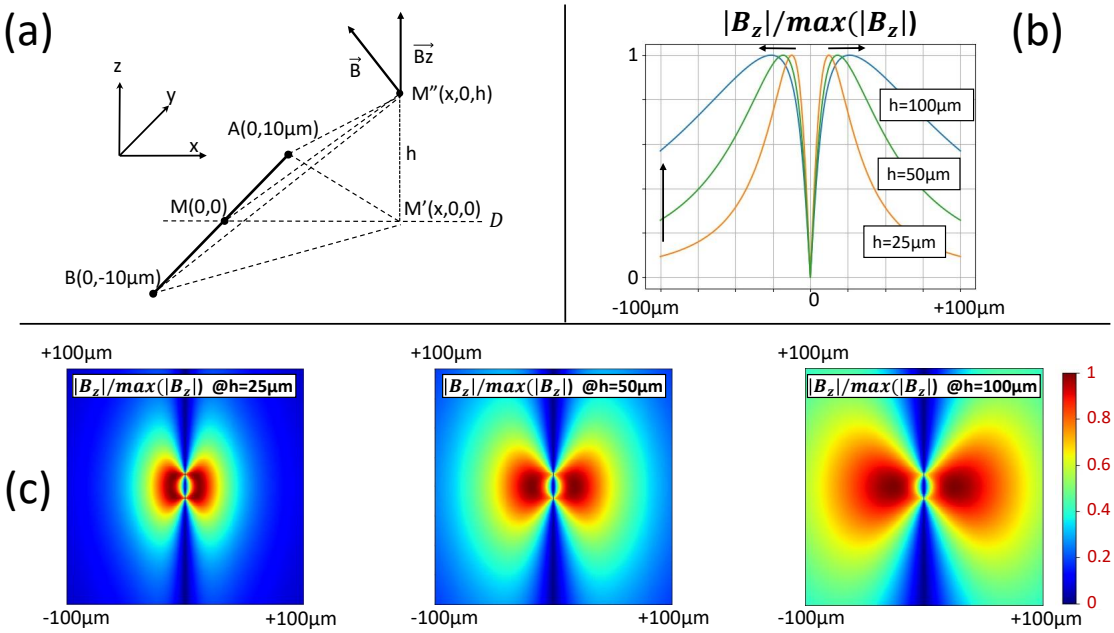

Figure 23: (a) Illustration associated to Eq. 15 and 16. (b) Evolution of the normalized vertical magnetic field along the bisecting line D for different values of z. (c) Maps of the normalized magnetic field for different values of z.

In the following section it is shown how to apply the unitary distributions of the magnetic field to all the wires of an IC in order to get the distribution of the magnetic field it radiates.

3.2.4 Magnetic field radiated by an entire IC

With these unitary distributions over S, the computation of the distribution of the magnetic field generated by an IC over its surface S_{IC} is straightforward. To that aim, the unitary distribution of the magnetic field corresponding to the correct orientation of the considered wire is applied to each wire of the IC. In this manner, a 3D matrix B_Z representing the evolution in time of the magnetic field distribution over a surface S' is obtained. Fig. 24 shows the procedure to compute this matrix. The proper unitary distribution is translated over each wire of the IC so that the position of the wire in the circuit is correctly taken into account. As shown in Fig. 24, S' must be greater than S_{IC} in order to reproduce the magnetic field it generates in its neighborhood.

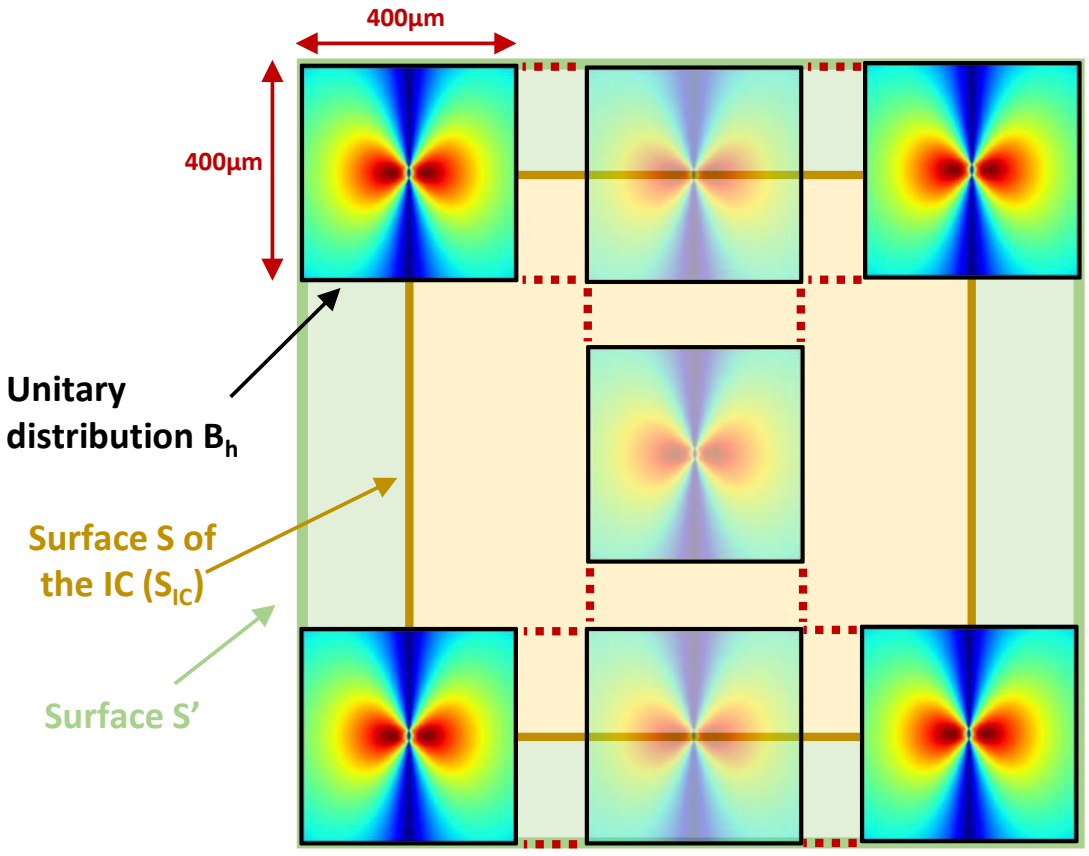

Figure 24: Computation of the matrix B_Z by translating the unitary distribution over the surface of the IC.

With these precautions, the coefficients of B_Z are:

$$B_Z(l,c,z,t) = \sum_i \mathscr{T}_i(B^*_{V/H}(l,c,z)) \cdot I_i(t) \tag{18}$$

with $l \in [-p,...,p]$ and $c \in [-q,...,q]$, $I_i(t)$ a vector of size t representing the current crossing the i^{th} wire segment of the IC and $\mathscr{T}$ the required translation of $B^*_{V/H}(l,c,z)$ to take its position in the circuit into account.

One can observe that this procedure is efficient since it consists in adding in B_Z at the correct position (required translation) the unitary distributions in a wider matrix after proper multiplication by $I_i(t)$. Of course after this procedure, only the central part of S', corresponding to S_{IC}, is kept.

In section 2.4.2 it has been anticipated that digital oscilloscopes record the voltage across the extremities of EM probes. In next section the origin of this voltage and the phenomena that trigger it are taken into account.

3.2.5 Electromotive force induced in EM probes

EM probes do not measure the magnetic field radiated by ICs but provide a voltage which is proportional to the electromotive force ε induced by changes in the magnetic flux ϕ_Z crossing the coil they are made of.

The magnetic flux is defined as the sum of the magnetic field force lines passing through the surface of the probe. In order to obtain its expression, one can assume, for the sake of simplicity, that the coil is a square of side length equal to $(2d+1) \cdot w$, with d the side length of the probe. Under this assumption, ϕ_Z is then defined as follows:

$$\phi_Z(l,c,t) = \sum_{\substack{i \in [l-d,l+d] \\ j \in [c-d,c+d]}} B_Z(i,j,t) \tag{19}$$

The variation of ϕ_Z in time induces a current, I_{ind}, in the probe loop and therefore a potential difference at the probe ends. This is called the electromotive force (ε). Mathematically, it is the derivative of ϕ_Z with respect to time.

$$\varepsilon(l,c,t) = -\frac{\partial \phi_Z(l,c,t)}{\partial t} \tag{20}$$

Note that there is a minus sign in Eq. 20. Indeed, the magnetic field generated by I_{ind} has an opposite direction with respect to the magnetic field that generates it (Lenz's law) [37].

At this point all the electromagnetic phenomena useful to reproduce the radiations that are captured by the EM probes have been explained. The primary origin of all these phenomena is the current flowing in the power and ground rails of ICs. Moreover, Eq. from 15 to 20 indicate that one needs to know the (x, y) coordinates (and the orientation) of each wire of the IC and the current $I_i(t)$ flowing in it in order to correctly estimate the magnetic field by simulation. One possible tool among others providing these information is RedHawk, a commercial IR drop tool provided by the ANSYS company.

3.2.6 Current extraction with RedHawk from ANSYS

RedHawk is a widely used IR drop and Electromigration Signoff tool for Digital IP and SoCs. It allows to draw maps showing the dynamic and static voltages in ICs. These maps are data dependent. In fact, one has to provide VCD (Value Change Dump [38]) files to RedHawk, indicating which data are processed by the IC. Such VCD files are commonly used to run data dependent and cycle accurate simulations. Among other functionalities, RedHawk allows to get the temporal evolution of the current flowing in each piece of the metal layers constituting the PGN. To that aim, one has to place virtual probes along those grids between vias and analyse one or more metal layers in parallel.

Different files need to be charged on RedHawk in order to extract the current flowing in the power rails using virtual probes. The most relevant are:

- Library Exchange Format (LEF): it is a file containing, for each cell, an abstract view of the layout indicating the cell boundaries, the pin positions and forbidden place and route areas.
- DEF (Design Exchange Format): this file basically contains placement information of macros, standard cells, vias, I/O pins and other physical entities.
- Liberty Timing File (LIB): it is a standard file containing LUT of cell delays, cell transition times and setup and hold times of D-Flip-Flop (DFF).

- Ploc (Power/Ground Bump Location): it contains the (x, y) coordinates of all the virtual probes placed on the power and ground grids.
- Timing Window File (TWF): it contains the window time over which the simulation has to be run.
- Value Change Dump (VCD): is an ASCII file which contains header information, variable definitions and the value changes for specified variables (or all variables) in a given design.

In our case, each VCD file charged on RedHawk corresponds to the encryption (or decryption) of one plain-text (or cipher-text) by the AES crypto-processor integrated in *TCA*. The Ploc file is generated by home made Python scripts. It allows to regularly place virtual probes every $X\mu m$ along the power and ground grids. Each virtual probes provides a current trace during a simulation (a VCD file). In order to run the EM flow on these current traces, the distance between two consecutive probes (on the same power line) is considered as a finite length wire (see Fig. 25) carrying the extracted current.

Fig. 25 gives an example. In that case, the virtual probes are placed every $20\mu m$ along the upper metal layer (AluCap) of *TCA* (Fig. 25a). Fig. 25b also shows a current trace provided by one of these virtual probes with a sampling rate of $200ps$. The latter shows the ten rounds associated to the ciphering of a plain-text (a VCD file) by the AES.

Fig. 26 shows the vertical magnetic field (for two consecutive time samples) radiated by *TCA* for one VCD file (one message charged in the AES). This figure has been obtained by placing about 30000 probes with RedHawk on the upper metal layer (AluCap) of *TCA*. Then, all the current traces were extracted with a sampling rate of $200ps$. This done, the simulation flow previously described has been applied in order to obtain the magnetic field distribution of the entire IC.

The last step of the development of this simulation flow, aiming at reproducing SCA, was related to the impact of the characteristics of EM probes used to perform these attacks. It is described in next section.

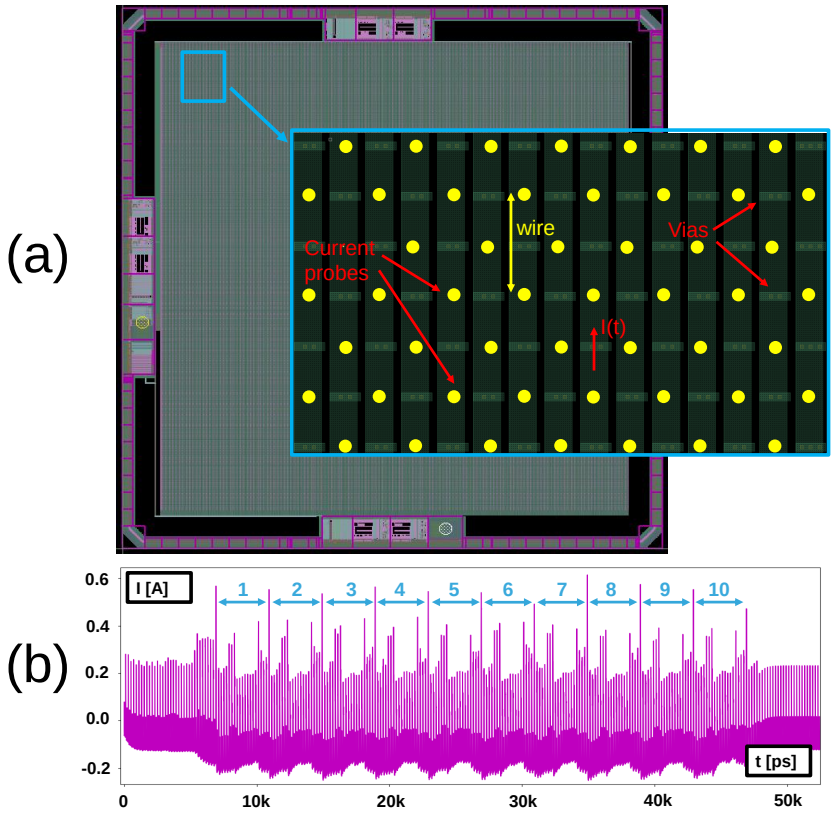

Figure 25: (a) Distribution of the virtual probes on metal layers. (b) A trace of current showing the ten round of an AES-128.

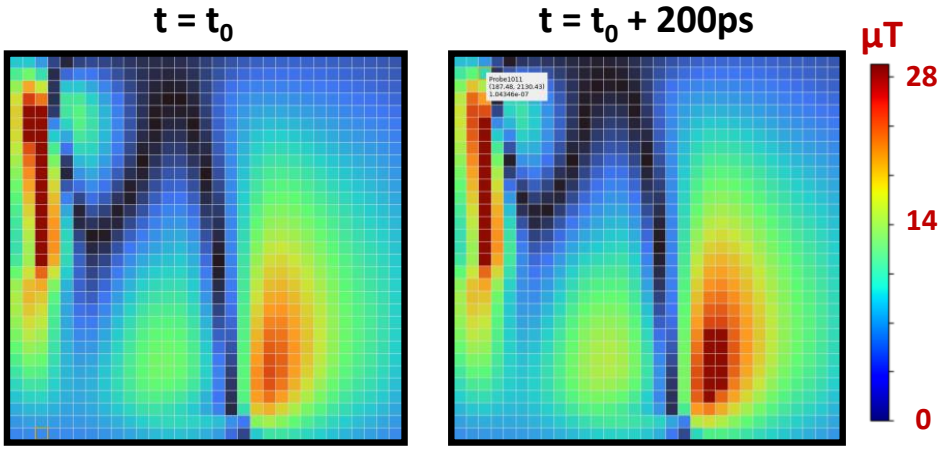

Figure 26: Distribution of the vertical magnetic field B_Z radiated by the testchip for two consecutive times samples (2 points of a trace).

3.2.7 Shielding effect of EM probes

ICR probes developed by the Langer company are commonly used in the side-channel community because of their high spatial resolution, large bandwidth and practical form factor shown in Fig. 27. The latter allows to approach the probe tip end really close to IC surfaces enclosed in cavities constituted by the package and the bonding wires. If this form factor is a key advantage for adversaries to collect traces with high SNR and to enhance the spacial resolution of attacks, it also constitutes a shield hiding some emanations of the IC during measurements. Indeed, as illustrated in Fig. 27a, the metal rod of the ICR probe supporting the loop cuts the path (red dot lines) of certain magnetic field lines. As a result, the magnetic fields radiated by all wire segments in a sharp cone on a side of the probe rod are ignored during measurements. Thus, someone trying to compare measurements acquired with Langer ICR probes with simulated data must consider this effect.

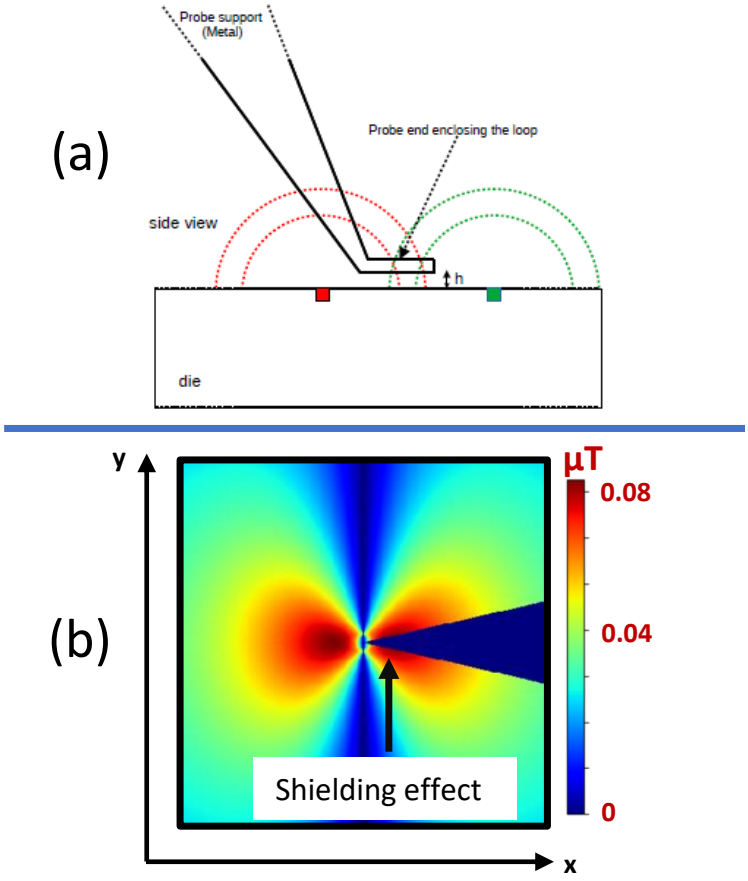

Figure 27: Shielding effect of a Langer probe on the magnetic field radiated by a single wire placed at the center of the map.

This shielding effect also implies that the emanations of a given wire segment are not captured from any position of the EM probe. Fig. 27b illustrates this by showing the magnetic flux map crossing the probe loop (of diameter $100\mu m$) during a near-field scan of a surface enclosing at its center a single vertical wire of length $20\mu m$. In this case, the EM probe has its end oriented toward the left and its rod creates a cone (oriented toward the right) where the emanations of the wire at the center of the map are not measurable.

Next section focuses on the effectiveness of the simulation flow described in the preceding paragraphs. The experiments and results it reports aim at verifying that the simulation flow correctly reproduces the EM phenomena observed in practice. It also aims at demonstrating that the flow allows to identify EM hotspots prior to fabrication. This is done by confronting experimental and simulated correlation maps.

3.2.8 Ineffectiveness of simulated correlation maps to identify EM hotspots

In this section the simulation flow previously exposed is applied to the testchip *TCA*. The goal was to crosscheck experimental and simulated correlation maps and to compare the leaking areas found on silicon and by simulation. The experimental correlation map showed in Fig. 28a is the same as that showed in Fig. 19. It was thus obtained by collecting 5000 EM traces at each position of *TCA* with a Langer ICR HH100 probe placed at a height $z = 100\mu m$.

The simulated correlation map shown in Fig. 28b was obtained by placing about 30000 virtual probes along the PGN of *TCA* with RedHawk. Following the assumption done in section 3.2.2, the virtual probes were placed only on the upper metal layer (AluCap) of the *PGN*. Then, 1000 VCDs were run (corresponding to the ciphering of 1000 plain-texts by the AES) and the currents of all virtual probes were extracted with a sampling rate of $200ps$. Finally, the magnetic field and flux as well as the electromotive force induced in a probe with diameter $d = 100\mu m$ and placed at a height $z = 100\mu m$ were calculated.

One can observe in Fig. 28 that the result was very disappointing: the maps were totally different. Indeed, the experimental map reveals reduced leaking areas while the simulated one shows that the CPA nearly discloses the key everywhere over the surface of *TCA*. In addition, a strange and further disappointing result is that experimental and simulated maps are quasi complementary (i.e.

give opposite results): CPA works in simulation where it does work experimentally. This means that the flow previously described is not efficient enough to reproduce EM SCA by simulation.

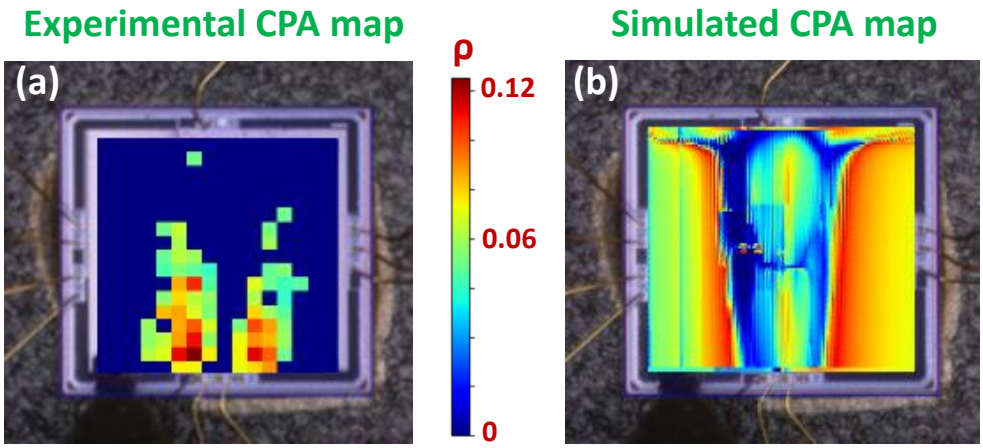

Figure 28: Comparison between experimental (a) and simulated (b) correlation maps performed on *TCA*.

It has thus been necessary to get back to basics to analyse once again the behavior of a simple finite wire carrying a leakage. More precisely, one has to verify if the EM hotspots generated by such a wire can correctly be predicted by simulation.

To that aim, specific simulations were run. They consisted in computing the vertical magnetic field, B_z, radiated at $z = 100\mu m$ by an IC embedding only a $20\mu m$ length wire crossed by a current I having a great leakage with respect to the HW of the secret. 1000 traces of current were simulated to perform this test.

As shown in Fig. 29a, the correlation between the HW and the current ($\rho(HW, I)$) is very high at the wire position and of course null everywhere else. On the other hand, Fig. 29c shows that the correlation between the HW and the vertical magnetic field ($\rho(HW, B_z)$ is high and constant over the entire surface (except along the vertical line supporting the wire) irrespective of the magnetic field distribution shown in Fig. 29b. This example clearly indicates that simulated correlation maps are ineffective in identifying EM hotspots.

There are two main reasons explaining why correlation maps are no help in identifying EM hotspots by simulation. The first is the lack of measurement noise in simulation which is obviously present in practice and can be assumed normal with zero mean and constant variance over the IC

surface. Indeed the noise, absent in simulation, reduces or totally annihilates the correlations at positions where the EM radiations have a low amplitude with respect to its variance.

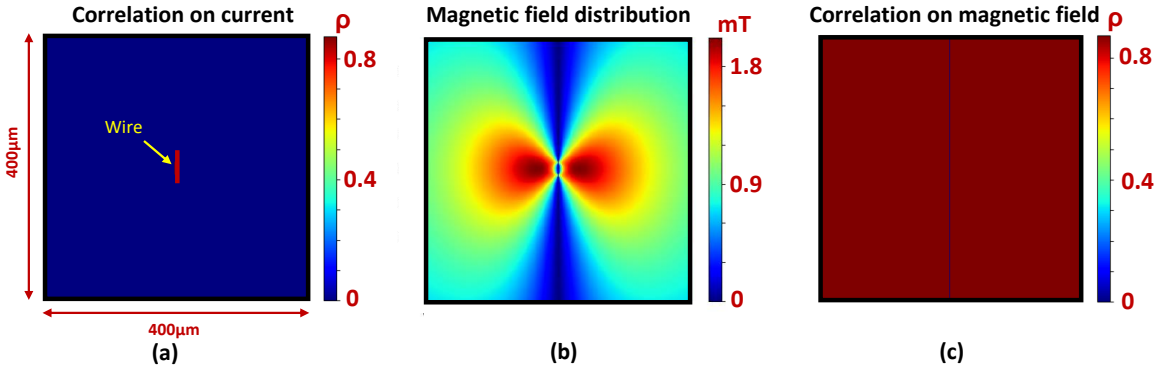

Figure 29: (a) Correlation attack on the current flowing in the wire. (b) Magnetic field distribution of a vertical wire (without the shielding effect of the EM probe). (c) Correlation attack on the magnetic field radiated by the wire.

The second reason lies in the expression of the correlation coefficient (ρ) involved in the significance test of a correlation coefficient [11], [12]:

$$\rho(H,S) = \frac{COV(H,S)}{\sqrt{V(H)\cdot V(S)}} \tag{21}$$

where S and H are the simulated EM signal and the leakage model (for instance the HW) of the intermediate data processed by the IC, respectively. $V(H)$, $V(S)$ and $COV(H,S)$ are instead the variances of both variables and the covariance between them, respectively.

One playing with Eq. 21 can observe that $\rho(H,S) = \rho(H,1e9 \times S)$. This effect is due to the denominator of Eq. 21 which acts as a normalization term. This means that by simulation it is possible to catch a leakage even above positions over the IC where only few nA of fA flow. This is impossible in practice, due to the measurement noise that wipes out the correlation at positions where the EM signals have a very low amplitude.

In next section, a solution to these problems is proposed in order to correctly interpret simulated correlation maps. This solution, called Noise-to-Add, is to the best of our knowledge the first methodology allowing to identify EM hotspots by simulation.

3.3 Identifying EM hotspots by simulation

3.3.1 Noise-to-Add concept

As aforementioned, the invariance of the correlation coefficient is due to the normalization of its value by the product of the standard deviations appearing at the denominator of Eq. 21. One can thus solve the problem, and therefore obtain more valuable simulated near-field scans, by simply replacing the correlation by the covariance. However, the covariance has no real meaning for designers and is hard to relate to any physical quantity such as the SNR, a key figure of merit to decide if a leakage can be easily exploited or not by an adversary.

The solution proposed is therefore different while remaining simple. It consists in computing, for each coordinate of the near-field scan, the variance $V(\eta)$ of the noise η of zero mean that must be added to the signals to hide the leakage, i.e. to render the correlation insignificant. In other words, the idea is to add a noise of null mean and variance η to the traces in order to force the correlation to fail the significant test whose hypotheses are:

$$\begin{cases} H0 : \rho = 0 \\ H1 : |\rho| > 0 \end{cases} \tag{22}$$

However this should be done without performing additional simulations that are time consuming. To that end, let's consider that the measurement noise is independent of the signal. With η a sample of the noise. This leads to write:

$$COV(H, S+\eta) = COV(H,S) \quad and \quad V(S+\eta) = V(S) + V(\eta) \tag{23}$$

and to express the link between the correlation, ρ, obtained with the noise-free simulated traces and the correlation, ρ_η, after introduction of the noise in traces:

$$\rho_\eta = \sqrt{\frac{V(S)}{V(S)+V(\eta)}} \cdot \rho \tag{24}$$

Considering now that the statistic of this test:

$$T = \frac{\rho \cdot \sqrt{n-2}}{\sqrt{1-\rho^2}} \tag{25}$$

follows a Student distribution (with $(n-2)$ degrees of freedom, n being the number of traces) to decide, with a confidence level $(1-\alpha)$, if ρ_η is null or not, one gets the critical values of T and the correlation, T_{crit} and ρ_{crit}, above which ρ_η must be considered significant ($H0$ rejected). It comes:

$$\rho_{crit} = \sqrt{\frac{V(S)}{V(S)+V(\eta)}} \cdot \rho \tag{26}$$

Finally, from Eq. 26, the variance $V(\eta)$ of the noise that must be added to simulated traces to render the correlation insignificant can be deduced:

$$V(\eta) = V(S) \cdot \left[\frac{\rho^2}{\rho_{crit}^2} - 1 \right] \tag{27}$$

Because ρ and $V(S)$ are known from simulations and because ρ_{crit}^2 is fixed by the choice of the confidence level $(1-\alpha)$, $V(\eta)$ can easily be computed in an automated manner. However, as shown by Eq. 27, $V(\eta)$ could be positive (if $|\rho| > |\rho_{crit}|$) or negative (if $|\rho| < |\rho_{crit}|$).

A positive value defines the minimal measurement noise required to hide the leakage. A negative value is of course not acceptable for a variance. In that case, the obtained value simply means that no measurement noise is required to render the correlation insignificant and thus $V(\eta)$ must be considered equal to zero.

From Eq. 27 and as part of the continuity of [39], one can determine an important information that is the minimal SNR, SNR_{min} (Eq. 28), required to retrieve, at a given coordinate of the IC, a significant EM hotspot. The computation of SNR_{min} is straightforward from Eq. 27:

$$SNR_{min} = \frac{V(S)}{V(\eta)} = \frac{\rho_{crit}^2}{\rho^2 - \rho_{crit}^2} \tag{28}$$

Eq. 28 thus constitutes a very useful information for secure IC designers. In fact, expert designers usually know the typical level of the signal that is sufficient to disclose a leakage in a design and thus they know if this leakage must be considered as critical or not. Furthermore, assuming that the correlation value quickly converges with few simulated traces, this SNR_{min} value can easily

be adjust to the n number of traces an adversary processes in practice. Indeed, ρ_{crit} is a function of this number. The greater n is, the smaller the SNR_{min} is.

Applying the Noise-to-Add concept to the simple wire of Fig. 29, it is possible to draw a map showing the standard deviation, $\sqrt{V(\eta)}$, of the noise that must be added to the magnetic field radiated by the wire, carrying a leaky current, to render the correlation $\rho(HW, B_z)$ insignificant. As shown in Fig. 30, the $\sqrt{V(\eta)}$ map is really close to the distribution of the magnetic field of Fig. 29b. This is a direct demonstration of the effectiveness of this method.

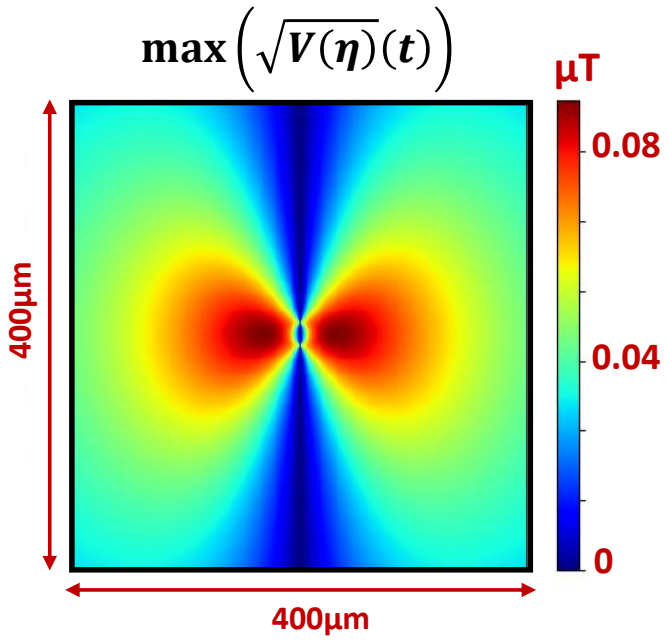

Figure 30: Distribution of $\sqrt{V(\eta)}$ showing the level of noise to be added to the magnetic field radiations to render a correlation insignificant.

However, next section shows that the methodology described above is not sufficient to identify an EM hotspots by simulation. To reach this objective, it is necessary to combine the Noise-to-Add and the Key Guess Ranking concepts.

3.3.2 Combining Noise-to-Add and Key Guess Ranking concepts

Noise-to-Add only gives an information about the significance of a correlation and which noise level must be added to the signal to render the correlation insignificant. Even if this is an interesting

information, it is not sufficient to decide if there is an exploitable EM leakage at a given coordinate above an IC. Indeed, CPA ranks all key hypotheses. This ranking is done according to the absolute value of the correlation between the signal and the HW of the target intermediate value processed by the circuit. If there is a leakage, the correct key is ranked in first position (with the greatest absolute correlation value). If there is no leakage its rank is between 2 and 256 in case of an 8-bits intermediate value. Thus, to state there is an exploitable leakage, the absolute value of the correct key guess, $|\rho^{k^*}|$, must be higher than those obtained with the other key guesses, $|\rho^k|$ (Eq. 13). However, one aiming at using the Noise-to-Add concept has to verify if the ranking obtained with it is identical to that obtained with the correlation. The answer is yes because, from Eq. 27, if $|\rho^i| \geq |\rho^j|$ then $\sqrt{V(\eta)^i} \geq \sqrt{V(\eta)^j}$. This property indicates that the correlation ρ could be replaced by the Noise-to-Add $V(\eta)$ during an attack without loss of efficiency.

To experimentally verify the soundness of this result, a set of 1000 simulated traces is considered. A standard CPA and a CPA based on $V(\eta)$ were simultaneously performed in order to compare the ranks of the correct key k^* provided by both solutions after the processing of the $n \in \{50, 100, 200, 250, ..., 950\}$ same traces. This procedure was repeated after adding a Gaussian noise to the traces. The variance of the added noise was successively set to be equal to 0.5, 2 and 8 times the noise to render the correlation obtained with 1000 traces insignificant. Fig. 31 reports the ranks obtained with $V(\eta)$ versus those obtained with ρ. As expected, all couples $(rank_\rho; rank_{V(\eta)})$ pile up on the first bisector.

As aforementioned, EM hotspots are positions above the surface of an IC where an attacker can place an EM probe to collect a leaky EM signal and retrieve secret data. EM hotspots must not be confused with leakage hotspots, which are sections of standard cell rows where the leakage occurs. Of course, because of the propagating properties of EM waves, these two types of hotspots are different and constitute different parts of the IC surface.

Despite the differences, the criterion proposed to identify leakage and EM hotspots by simulation is the same and is given below:

$$\sqrt{V^*(\eta)} = \begin{cases} \sqrt{V^{k^*}(\eta)} & \text{if } |\rho^{k^*}| \geq |\rho^k|, \quad \forall k \in K \\ 0 & \text{otherwise} \end{cases} \tag{29}$$

with K the set of all the sub-key guesses and k^* the correct one.

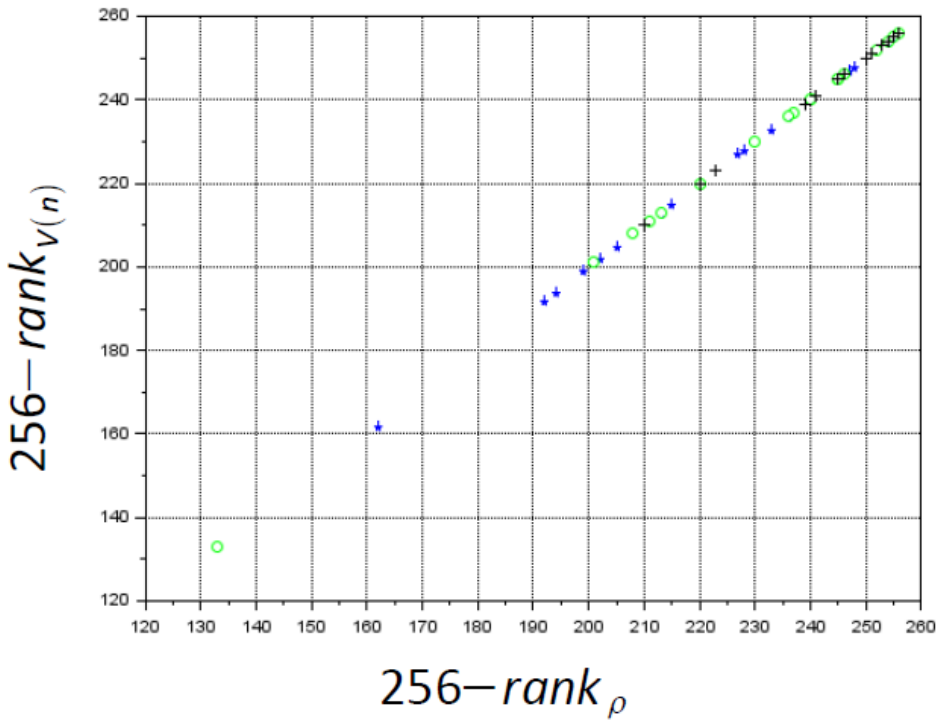

Figure 31: Ranking of $V(\eta)$ vs ranking of ρ. '+', 'o', and '*' correspond to different levels of the Gaussian noise added to traces.

This criterion consists in drawing maps, called Noise-to-Add maps, containing, at each coordinate, the value of $\sqrt{V(\eta)}$ related to the correct key guess only if the correlation of the latter is higher than the other key guesses, and 0 otherwise.

This criterion is mathematically identical for both leakage and EM hotspots. The only difference is the physical quantity manipulated by Eq. 29. Indeed, to identify leakage hotspots it is applied to the currents flowing in the lowest metal layer (normally Metal1) of the PGN. This part is indeed the part of the PGN the closest to CMOS gates which are the only elements of ICs manipulating data and are thus necessarily the root cause of the leakages. Thus, applying it to an upper level of metal necessarily gives a less precise localization of hotspots because the currents consumed by CMOS cells progressively disperse in the upper part of the PGN while propagating toward the power and ground pads. In addition, the upper part of the supply networks is coarser than at Metal1 level.

On the other hand, to identify EM hotspots, Eq. 29 is applied to the simulated electromotive force $\varepsilon(t)$, induced in an EM probe capturing the vertical magnetic field $B_z(t)$. $\varepsilon(t)$ is computed

starting from the current traces, collected using RedHawk, flowing in the upper metal layers of the PGN.

3.4 Conclusion

In this chapter, a simulation flow able to reproduce experimental near-field scans was presented. It allows identifying EM hotspots prior to fabrication. It is based on the Biot-Savart law used to model all the electromagnetic phenomena observed on silicon and on RedHawk, an IR drop tool provided by the ANSYS company allowing to extract the temporal evolution of the currents flowing in IC power and ground grids.

To accurately model the magnetic field radiated by ICs, it has been assumed and then verified that considering only the currents flowing in the upper metal layers of the PGN is sufficient, as the latter are crossed by much more intense currents. In this developed simulation flow, the PGN is modeled as a set of current-carrying wires and the Biot-Savart law is applied to all to get the magnetic field radiated by the entire circuit.

A focus on EM probes has been done. In particular, it has been described how to model the electromotive force induced in EM probes used to measure the magnetic field of ICs. A shielding effect caused by the form factor of Langer probes has also been highlighted.

A first test of the flow has shown great differences between experimental and simulated correlation maps. The main reason is that simulations are noise-free. As a result, correlation maps cannot be used to identify EM hotspots by simulation. To overcome this problem, an innovative methodology, called Noise-to-Add, has been introduced. It allows to correctly interpret simulated correlation maps.

In the next chapter both the magnetic field simulation flow and the Noise-to-Add concept are applied to a testchip. The goal is to validate the entire simulation methodology and demonstrate its effectiveness in identifying leakage and EM hotspots prior to fabrication and to show how powerful this tool can be for designing secure ICs.

Chapter 4

Validation of the simulation flow

Contents

SCA exploiting the EM emanations of ICs have demonstrated their effectiveness in retrieving secrets from secure ICs. As a consequence, it has become more and more difficult to design ICs free of any leakage as EM SCA need only one leaky position over the IC surface to extract the secret key. Hence, the importance of developing a methodology to identify EM hotspots during the design stage of a chip in order to be able to fix the leakages and design robust ICs. This chapter proposes, to the best of our knowledge today, the first and complete solution to overcome the lack of such a tool in the literature.

Validation of the simulation flow

This chapter is of primary importance because it provides a strong validation of both the simulation flow and the Noise-to-Add concept. The validations include numerous comparisons between experiments and simulations. All the results presented in this chapter have been presented and published in two international conferences, COSADE 2021 [40] and EMC Compo 2021 (to be held in March 2022), and in one international journal (IEEE TCAD [20]).

4.1 Introduction and objectives

This chapter presents validations of all the concepts presented in chapter 3. Each step of these validations has been carried out throughout comparisons between experimental and simulated correlation attack maps.

First of all, it has been verified that the magnetic field flow is able to correctly take into account the effects of the probe characteristics and localization, i.e. changes of the diameter and height of the probe used to perform EM attacks. Placing the probe closer to IC surface allows to increase the SNR of the collected EM radiations. Similarly, the larger the probe diameter is, the greater the magnetic flux trough the probe is, as a larger number of magnetic force lines is captured by the probe. All these effects need obviously to be faithfully reproduced by the simulation flow.

EM attacks have also been performed with probes measuring either the horizontal or vertical magnetic field, in order to sustain the assumption done in section 3.2.2. The latter states that only upper metal layers need to be considered to accurately model the magnetic field captured by an EM probe placed close to the IC surface. To further sustain this assumption, a comparison between attacks performed with *TCA* mounted in front-side and back-side has been conducted.

As a last proof of the effectiveness of the flow, a link between the Noise-to-Add concept and the number of traces needed to find retrieve a secret in practice has been investigated.

4.2 Disclosing EM hotspots with the simulation flow

Before presenting the results of the validations that have been done, next section gives information about the time needed to acquire both experimental and simulated traces.

4.2.1 Experimental and simulated maps

The experimental near-field scans reported in next sections have been carried out by displacing EM probes from Langer company every $100\mu m$ over the surface of TCA and collecting 5000 EM traces (corresponding to the ciphering of 5000 plain-texts by AES) at each considered position. All the probes used during these scans have a frequency bandwidth equal to $[30MHz - 6GHz]$. The sampling rate of the digital oscilloscope was set to $5GS/s$.

The length and width of TCA being both equal to $2.2mm$ and the displacement step of the probe equal to $100\mu m$, $20 \times 20 = 400$ (20 along the x-axis and y-axis) positions were scanned (the bonding wires limited the scanning surface to a square of side length $2mm$) to obtain a matrix with dimensions 20×20 containing a total of 2 million EM traces (400×5000). The time spent to collect 5000 traces at a position was about 5 minutes. As a consequence, the total acquisition time to complete a near-field scan was around 36 hours.

For each set of 5000 traces, a CPA attack was performed on the first output byte of the first Sbox of the first AES round. In this manner, each point of the drawn maps shows the maximal absolute value of the correlation obtained with the correct key if this latter is greater than the correlations obtained for the other key hypotheses; otherwise, it shows a 0 value because no leakage was found (the correct key is indistinguishable from the others) at this position.

On the other hand, about 30000 virtual probes (spaced by $20\mu m$ one from the other) were placed with RedHawk on the AluCap (top layer) grids of TCA. In this manner, 30000 wires of length $20\mu m$ were obtained. Then, 1000 VCDs (corresponding to 1000 different plain-texts processed by the AES) were run with a sampling rate equal to $200ps$ (this corresponds to $5G/s$). Once the current traces were extracted, the magnetic field flow was applied to simulate the inducted electromotive force in a probe displaced over the IC surface by steps of $100\mu m$. The distance between the power rails being equal to $10\mu m$, the B_Z (Eq. 18) was computed considering $w = 10\mu m$. This results at the end in a B_Z matrix of dimensions 220×220. This done, the magnetic flux and the electromotive

force were computed for a probe diameter $d = 100\mu m$, placed at a height $z = 50\mu m$ and $z = 100\mu m$ and displaced by $100\mu m$ above the IC surface. All these settings allowed to have the same conditions for the experimental and simulated scans.

The time spent to run 1000 simulations was ranging between 24 and 48 hours according to the charge of our calculation server. The only encountered difficulty was the memory occupied by the currents traces. In fact, 30 million current traces were generated by RedHawk: this number corresponds to the product of the number of virtual probes (30000) implemented to monitor the PGN by the number of plain-texts passed to the AES (1000).

To solve this problem, Python scripts were developed to translate results provided by Redhawk in $HDF5$ (Hierarchical Data Format version 5) format. This operation slightly extends the total processing time but has an enormous impact on the size of the data stored. At best 1.38 traces/second have been simulated, i.e. $1.38s$ were required to get the 30000 current traces associated to the 30000 current probes spread over the power and ground grids.

The translation done, the electromotive force induced in the considered EM probe was computed by applying the simulation flow. The procedure of Eq. 29 was thus applied on the resulting traces. If the $\sqrt{V^*(\eta)}$ of the correct key stands out from the other key guesses, the associated point in the map shows the noise to be added at the specific position of the circuit in order to hide the leakage; otherwise the point contains a 0.

4.2.2 Effect of the probe height and diameter in EM attacks

In order to provide a first corroboration of the effectiveness of the entire simulation flow, two experimental near-field scans of TCA with a Langer ICR HH100 probe (diameter $d = 100\mu m$) parallel to the IC surface were performed. The probe was placed at two different heights, $z = 50\mu m$ and $z = 100\mu m$. Then, Eq. 13 was applied at each position of the scan (thus for each set of traces) and the corresponding maps were drawn.

In parallel, the same scans were performed by simulation. The only difference between experimental scans and simulated ones was the use of the Noise-to-Add concept rather than the correlation.

The first row of Fig. 32 shows the experimental $|\rho^*|$ maps, for both heights. Both maps have the same color scale in order to enhance the effect of the height on results. One can observe that the

height z has an important impact. Indeed, increasing the height decreases the number of coordinates where the $|\rho^*|$ is greater than 0.12. This was expected since increasing the distance between the probe and the IC surface results in reducing the SNR of traces.

The second row of this figure shows the simulated $\sqrt{V^*(\eta)}$, still for $z = 50\mu m$ and $z = 100\mu m$. One can observe that the simulated maps are visually in good agreement with experimental ones. In fact, accordingly to what has been experimentally observed with the correlation coefficient, increasing z causes the diminution of the number of coordinates where $\sqrt{V^*(\eta)}$ is greater than 0.4.

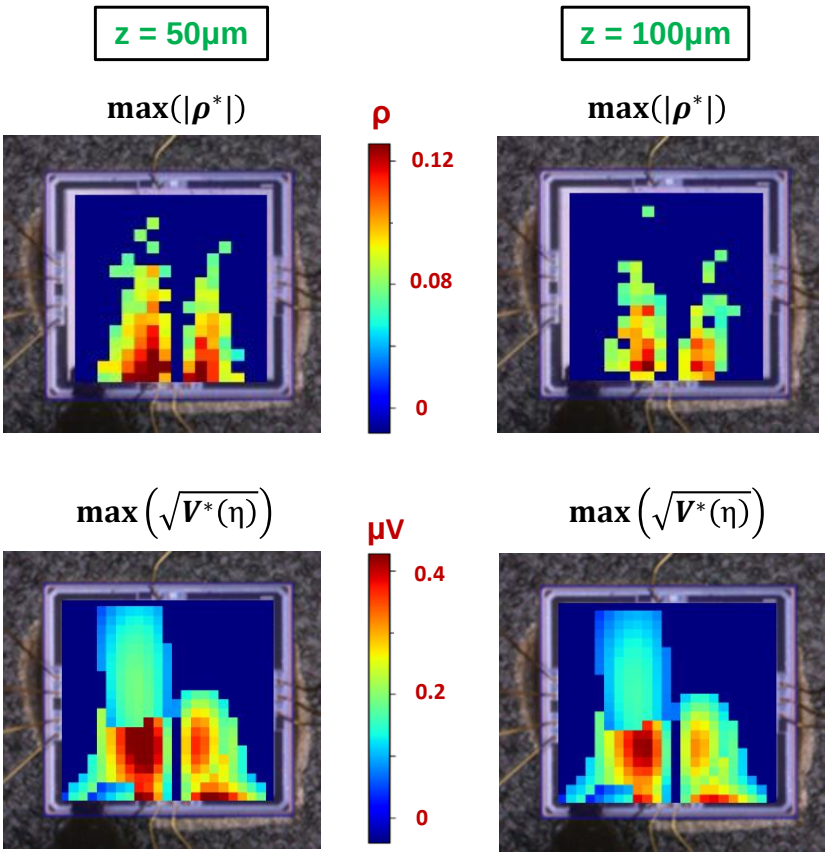

Figure 32: Experimental $|\rho^*|$ maps (first row) and simulated $\sqrt{V^*(\eta)}$ maps (second row) for two different probe heights.

Following these first conclusive results, the impact of the probe diameter was also analysed. To this end, the Langer ICR HH100 was replaced by the Langer ICR HH150 (with a diameter of $150\mu m$) for a scan performed at a height $z = 100\mu m$ from the IC surface. The corresponding scan was simulated with a similar process than that described in the preceding paragraphs. The two resulting maps ($d = 100\mu m$, $d = 150\mu m$ with $z = 100\mu m$), still taking care to set the same color

scales to highlight the effect of the diameter d, are given in Fig. 33.

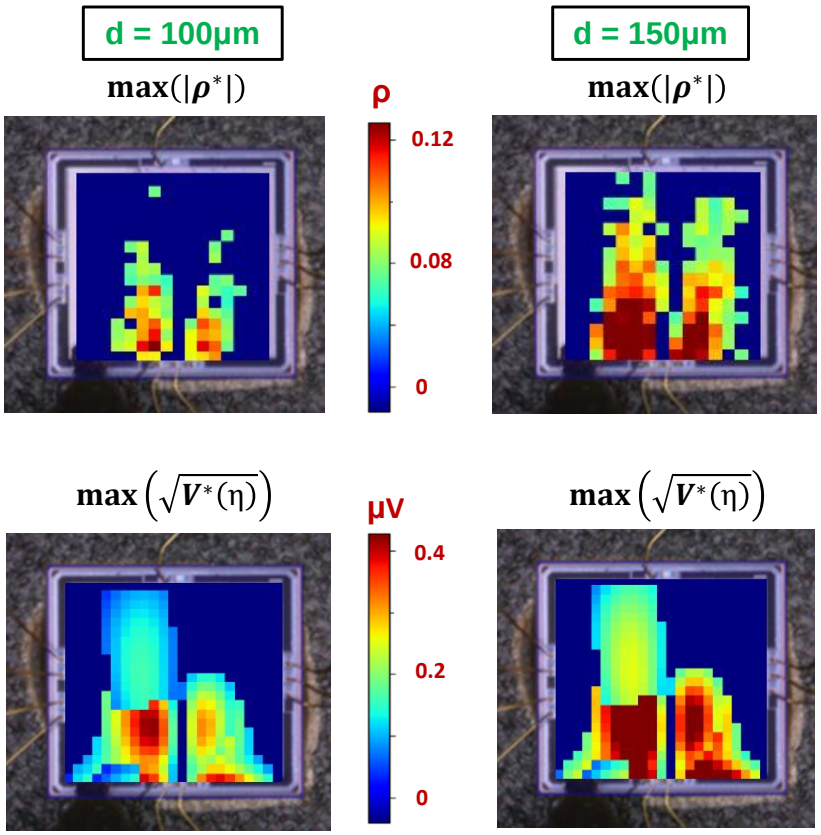

Figure 33: Experimental $|\rho^*|$ maps (first row) and simulated $\sqrt{V^*(\eta)}$ maps (second row) for two different probe diameters.

One can observe the agreement between simulated and experimental maps. Furthermore and as expected, using a probe with a larger diameter increases the amplitude of the collected signals and therefore of $\sqrt{V^*(\eta)}$. This results in a widening of the area where $\sqrt{V^*(\eta)} > 0.4$ in this case. Interestingly, the maps obtained for a probe with diameter $150\mu m$ placed at height $z = 100\mu m$ from the IC surface (right column of Fig. 33) are really similar to that obtained with a probe with diameter $100\mu m$ placed at height $z = 50\mu m$ (left column of Fig. 32). Thus, it seems preferable to use larger probes when performing scans without removing the plastic package. This is a known result from experience which is confirmed by simulation.

These first results are very important. They demonstrate that the simulation flow correctly takes into account changes of the probe height and diameter and it also allows identifying the EM leakages an attacker could find by attacking an IC with different probe configurations.

In the following section, simulated and experimental correlation maps obtained with vertical probes are compared in order to verify if it is sufficient to simulate the current flowing in top metal layers to accurately emulate the magnetic field captured by EM probes.

4.2.3 Vertical probes measuring the x and y component of the magnetic field

Adversaries usually perform near-field scans of the vertical magnetic field using ICR HHXXX (horizontal) probes. Despite this shared preference, two experimental scans with the ICR HV100 probe measuring the horizontal magnetic field were performed. The goal was to provide a first evidence (the second one is given in section 4.2.4) of the soundness of the assumption done in section 3.2.2. The latter consists in assuming that considering upper metal layers is sufficient to accurately reproduce the magnetic field of ICs.

To this aim, two experimental EM scans with a vertical probe, the Langer ICR HV100 (diameter $d = 100\mu m$), at a height $z = 100\mu m$ from TCA were performed. In the first scan the probe was parallel to the y-axis, while in the second it was parallel to the x-axis. Then, $|\rho^*|$ maps were drawn on the collected EM traces.

The simulated $\sqrt{V^*(\eta)}$ maps were drawn as usual by considering only the currents flowing in the topmost metal layer (AluCap) of TCA. The probe being perpendicular to the IC surface, it only measures the x or y components of $\overrightarrow{B}$. Thus, Python scripts were adapted in order to compute the x and y components of the magnetic field measured at each point of a surface S perpendicular the each wire of the PGN.

Fig. 34 shows the results. The similarity between experimental and simulated maps constitutes another proof of the soundness of the flow. Furthermore, this figure provides very useful information.

In fact, when the probe is parallel to the y-axis and thus to the preferred routing direction of the AluCap wires (Fig. 34a), it can capture the force lines of the magnetic field and both correlation and $\sqrt{V^*(\eta)}$ are strong. One can observe that there is now only one wide leakage area, centered on the AES block. This is because the probe captures the x component of the magnetic field.

On the other hand, when the probe is parallel to the x-axis and thus perpendicular to the direction of AluCap wires (Fig. 34b), $|\rho^*|$ and $\sqrt{V^*(\eta)}$ are equal to 0 almost everywhere over the IC surface, except at few positions (due to a large Vdd rail parallel to the orientation of the EM probe).

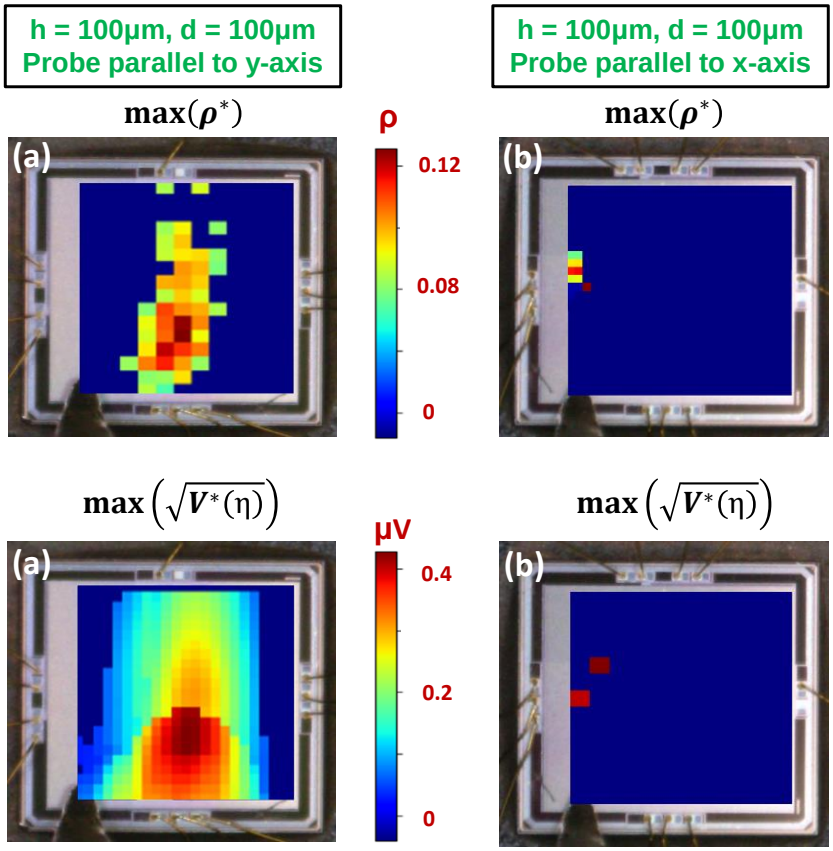

Figure 34: Resulting $|\rho^*|$ and $\sqrt{V^*(\eta)}$ maps obtained with a vertical probe. Probe parallel to y-axis (a) and x-axis (b).

This means that the correct key guess is (almost) never retrieved in this configuration and no EM hotspots were identified.

This observation clearly indicates that EM probes placed close to the IC surface mainly captures the magnetic field radiates by upper metal layers. Finally, one can confirm (what is known from experience) that attacking an IC with horizontal probes is preferable. This avoids having to guess the routing direction of the topmost metal layers.

As a second important evidence of this effect, a comparison between EM analyses performed with *TCA* mounted in front-side and back-side was conducted. Results are given in the next section. When an IC is mounted back-side, the lowest metal layers (usually in Metal1) are the closest to the EM probe. So, theoretically, the magnetic field radiated by the currents flowing in the Metal1 should be the main contributor to the EM radiations captured by EM probes.

4.2.4 Front-side vs back-side: the effect of the substrate

The objective of this section is analysing the differences between EM attacks performed front-side and back-side. In fact, one may wonder in which configuration EM attacks are more effective. Furthermore, this analysis is important because even if attacks are usually carried out on front-side sometimes ICs are only available on back-side. For this reason it is interesting to investigates the impact of the IC orientation on the ease with whom adversaries can perform attacks. Finally, replicating these experiments by simulation allows to obtain a further corroboration of the soundness of the simulation flow.

The first experiment presented below consisted in performing two experimental EM scans with a Langer ICR HH100 probe placed close to the front-side (Fig. 35a) and back-side (Fig. 35b) of *TCA* at $z = 50\mu m$ in both cases. One can observe that back-side map is slightly wider. This is because of the absence of bonding wires that allows to scan a larger part of the IC surface.

Looking at Fig. 35 the first observation one can do is that front-side map shows stronger leaky areas than back-side one. This indicates that in back-side the SNR of the EM traces collected by the probe is lower due to the greater distance between AluCap rails and the probe. In fact, the thickness of the substrate is equal to $180\mu m$ thus the probe is $180\mu m$ further from the AluCap. As a result, this first result suggests that AluCap rails are predominant in contributing to the field captured by the probe.

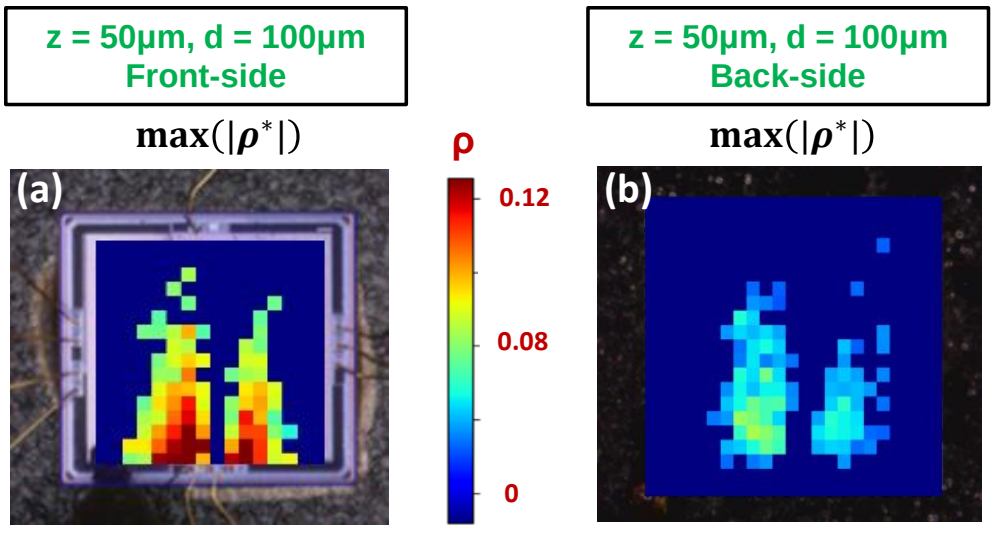

Figure 35: (a) Front-side vs (b) back-side $|\rho^*|$ maps obtained for the testchip *TCA*.

As a further evidence of this assumption and to obtain another corroboration of the effectiveness of the EM simulation flow, two EM scans with a Langer ICR HH100 probe placed close to the front-side and back-side of *TCA* respectively were performed. The thickness of the substrate being equal to $180\mu m$, the probe was placed at $z \sim 180 + 50 = 230\mu m$ during scans of the front-side and at $z = 50\mu m$ during scans performed back-side. In this manner, the probe was at the same distance from the AluCap rails in both front-side and back-side. Corresponding simulated maps were then drawn.

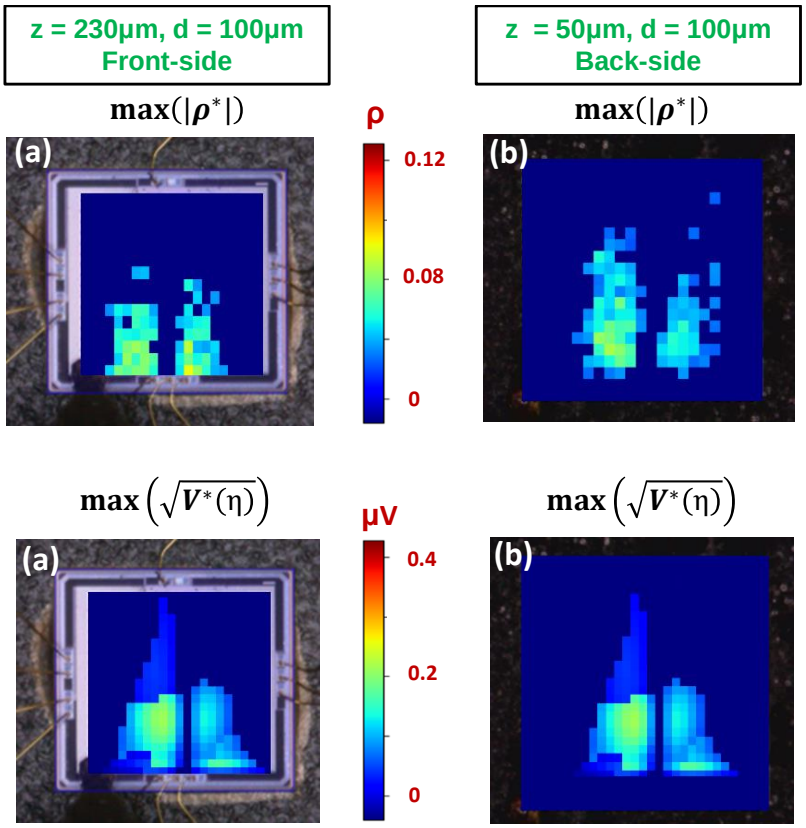

Figure 36: (a) Front-side vs (b) back-side $|\rho^*|$ and $\sqrt{V^*(\eta)}$ maps obtained for the testchip *TCA*.

Observing the maps of Fig. 36, one can state that now there are no significant differences between front-side (Fig. 36a) and back-side (Fig. 36b) results. The first reason is that, as anticipated in section 3.2.2, the currents flowing in the AluCap layer are 38 times stronger in average than those flowing in Metal1. Thus, AluCap is the main contributor to the EM field.

Second, the silicon, which is the material the substrate is made of, has a relative magnetic permeability $\mu_r \approx 1$, i.e. close to that of the vacuum. This means that in back-side, when the

probe is close to the substrate, the strong magnetic field radiated by the AluCap layer can easy expand in space, with almost no reflection or absorption effect operated by the substrate. This result constitutes a second evidence that the assumption made in section 3.2.2 is correct.

Another proof of the effectiveness of the Noise-to-Add concept in identifying EM hotspots is given in the next paragraphs. The performed experiment they describe has consisted in analysing the link between the Noise-to-Add maps and the number of experimental traces needed to find a key in practice.

4.2.5 Noise-to-Add and partial Guessing Entropy

To further supports the interest of the Noise-to-Add concept for disclosing EM hotspots by simulation, an additional experiment was performed. Following the procedure exposed in section 4.2.1, 20000 EM traces were acquired at each position with an ICR HH100 probe placed at a height $z = 100\mu m$ over the front-side of TCA.

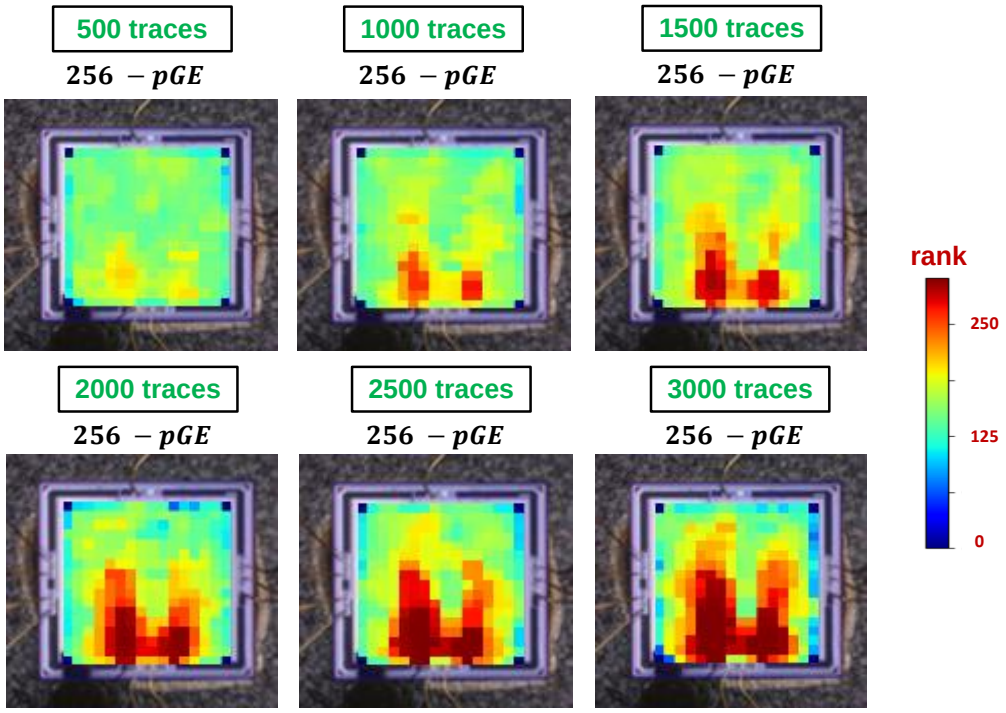

Figure 37: Maps of the $(256 - pGE)$ after the processing of 500, 1000, 1500, 2000, 2500 and 3000 traces.

The acquisition of traces done, ten CPA were successively performed with $n = 500$ traces randomly selected among the 20000 traces after each trial. The average ranking of the key was finally computed after the ten CPA. This procedure was then repeated for $n = 1000, 1500, 2000, 2500, 3000$ to analyse the evolution of the partial Guessing Entropy (pGE) [41].

The evolution of $(256 - pGE)$ is plotted in Fig. 37 (as a reminder, $256 - pGE = 255$ means that the correct key is ranked first in average) and must be compared to the $\sqrt{V^*(\eta)}$ map already showed in Fig. 32 (second row $z = 100\mu m$). This comparison allows concluding that, as soon as the number of processed traces is sufficient (this number depends on the measurement noise and equipment used), $\sqrt{V^*(\eta)}$ maps are similar to $(256 - pGE)$ maps. Thus $\sqrt{V^*(\eta)}$ accurately indicates where to place an EM probe to more easily get the secret when there is a leakage.

4.3 Conclusion

This chapter has been devoted to the validation of the simulation flow. It has been demonstrated, through concrete examples and by providing comparisons between experimental and simulated attack maps, that the flow reproduces the changes of the probe characteristics and localization (height and diameter). Then, the assumption according to which the upper metal layers of ICs are the main contributors to the magnetic field captured by EM probes has been sustained by experiments performed with vertical probes and by comparing front-side and back-side configurations.

Next chapter presents the usefulness of such a flow during the design stage of an IC. In particular, the developed flow could be applied for:

- Leakage verification prior to fabrication: the flow will be firstly used to identify the sources of EM hotspots, i.e. the leakage hotspots, during the design stage. Indeed, the Noise-to-Add concept can be applied on the currents flowing in the lowest metal layers to identify the leaky CMOS gates which are the origins of the EM hotspots identified during EM scans. Identifying these gates during the simulation stage is fundamental to fix errors and design secure ICs.

- Post-silicon leakage analysis: this flow can be also used as “debug” tool when a product shows leakages that have not been detected during the design stage. The flow can be used to

compare leakages found on silicon with those found by simulation. This step is fundamental as it allows to quickly identify leakages, modify the design and re-apply the simulation flow to check if the design still presents weaknesses against EM attacks.

- Evaluation of countermeasures at design stage: the flow can be used to evaluate the effectiveness of countermeasures during the design stage. Three possible hardware countermeasures against EM attacks will be presented. Two of them aim at improving the robustness of ICs against EM attacks by reducing the SNR of the EM radiations captured by EM probes. The third by dynamically changing the value of the supply voltage. Comparisons between experimental and simulated attack maps will be given.

Chapter 5

Usefulness of the simulation flow

Contents

After demonstrating in the previous chapter the soundness and reliability of the simulation flow in disclosing the EM hotspots of an IC, this chapter aims at demonstrating the usefulness of such a flow during the design stage. The integration of this tool in the design flow of secure ICs could be very useful, as it allows to check the presence of leakages before the silicon production, to simulate the effectiveness of countermeasures prior to manufacturing but also to carry out post-silicon analyses on products, already in use, that present weaknesses against EM attacks.

Usefulness of the simulation flow

5.1 Introduction

This chapter can be divided in three main parts. The first part is dedicated to the verification of potential leakages prior to fabrication. It explains how to use the simulation flow to verify and localize any leakage hotspot by simulation prior to fabrication. These hotspots are the leaky CMOS gates that are at the origin of EM hotspots which are the leaky positions of an IC where an attacker can retrieve a secret collecting EM radiations with an EM probe. This part also highlights that, due to the propagation of the currents along the power and ground grids, leakage and EM hotspots are different and constitute different parts of the IC surface.

In the second part, the problem of post-silicon leakage analysis is addressed. It explains how the proposed simulation flow can be used to analyse a leaky product that, for some reasons, presents weaknesses against EM attacks.

In the third part, three countermeasures against EM attacks are proposed and analysed. The first one concerns the power routing strategy of a testchip. It consists in techniques allowing to reduce the EM radiations of ICs and thus reduce the SNR of the collected traces. Two testchips designed with different power routing policies are tested both via experiments and simulations, in order to verify the effectiveness of this countermeasure. This experiment also provides an additional validation about the EM hotspots localization methodology proposed in chapter 3.

The second analysed countermeasure consists in designing lower power chips with reduced supply voltage value and even ICs with varying Vdd. Indeed, lowering Vdd reduces the current flowing in ICs and thus their EM emanations. In addition, varying Vdd is expected to blur these emanations.

The third countermeasure is called EM jamming. It consists in injecting a random noise with jitter in EM traces in order to increase the measurement noise and, thus, decrease the SNR of the EM traces.

5.2 Leakage verification prior to fabrication

5.2.1 Leakage hotspots and current propagation

This section shows how to disclose leakage hotspots during the design stage. All the maps shown below have been obtained on the testchip *TCA* whose characteristics have been presented in section 3.2.1.

In section 3.3.2, it has been demonstrated that Eq. 29 can be applied to disclose not only EM hotspots but also leakage hotspots by simulation. To that aim, Eq. 29 has to be applied on the traces of current flowing in the lowest metal layers of the IC, which are normally in Metal1. 130000 virtual probes were therefore placed with RedHawk on the Metal1 grids supplying the testchip *TCA*. Then, 1000 currents traces were extracted for each probe. Each of these traces corresponds to the ciphering of one plain-text by the AES. This procedure was applied on different time windows in order to highlight the apparition of the leakage and its propagation above the IC surface with that of the currents. Indeed, analysing the evolution of $\sqrt{V^*(\eta)}$ in time is a key advantage to localize hotspots.

Fig. 38 illustrates the obtained result. It shows the progressive apparition of a leakage between time samples n°1 and n°7 (beginning of a clock cycle) and its spreading along the power and ground grids due to the propagation of currents. This results highlights the importance of applying Eq. 29 time sample by time sample to finely localize the root cause of leakages by overcoming the blurring effect due to the propagation of the currents through the power and ground grids.

To better highlight the origin of leakages, zooms on the AES are visible in Fig. 38. Such a series of maps, forming a movie, offers designers the possibility to quickly analyse and fix leakages, with electrical or RTL level simulations, after having identified CMOS gates in the suspect sections of standard cell rows. One can also observe the light blue areas outside the AES placement which are zones from where the AES draws part of the current it consumes. This is a direct evidence of the current propagation which spreads the leakage over a larger area than that it originates.

One can also observe that a leakage occurring at one edge of the clock signal lasts for several nanoseconds due to this propagation effect. This clearly shows the dangerousness of the EM side-channel.

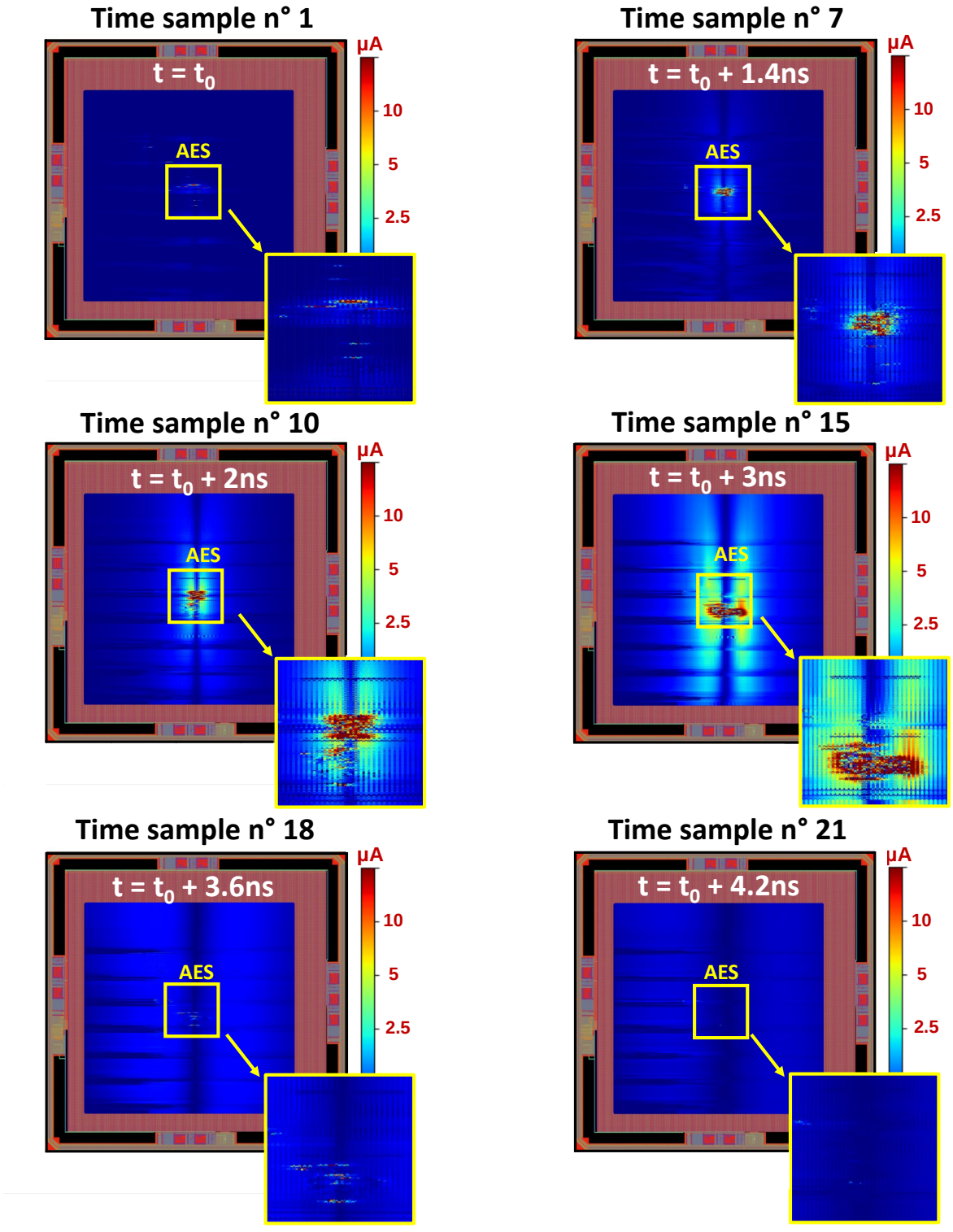

Figure 38: Temporal evolution of the leakage associated to time samples n°1, 7, 10, 15, 18 and 21 disclosing sections of standard cell rows which are leaking.

Next section demonstrates the usefulness of the simulation flow in analysing and disclosing EM hotspots post-silicon.

5.3 Post-silicon leakage analysis

As aforementioned, the flow can be used to analyse products that have been manufactured before its development. Indeed, it could happen that a product presents leakages that were not found at simulation stage or former certification processes. This could happen because, as explained, there was no tool allowing to reproduce EM SCA and disclose EM hotspots prior to fabrication, but also because new attacks appear regularly.

As shown in this manuscript, the effectiveness of the flow has been demonstrated through various examples on different testchips. Of course, firstly testing the flow on a testchip was a fundamental step of the development of the flow to validate the soundness of the approach. Following these encouraging results, the flow could have been applied and tested on a more complex product, called *PA* from now on. It is designed with a $40nm$ low power CMOS technology. It embeds different functional blocks. Among them one can find, as in the testchip TCA, an AES-128 co-processor operating at $50MHz$.

Different experiments were conducted on *PA*. For all ones presented below, all countermeasures of *PA* were disabled. Other details about the IC cannot be given due to confidential constraints.

Experimental EM SCA were performed on *PA* showing many EM hotspots. The flow was thus applied with two objectives. The first one being to obtain another proof of its effectiveness in disclosing EM hotspots and founding the same leaky area than in practice. The second one being to test a new silicon version of *PA*, called *PB*, which was available on silicon and expected to be less leaky than *PB*.

To compare EM hotspots found over *PA* in practice and by simulation, an experimental near-field scan were performed with a Langer ICR HH100 probe (diameter $d = 100\mu m$) parallel to the IC surface and placed at $z < 10\mu m$ over the surface of *PA*. 5000 EM traces were collected at each position. Eq. 13 was thus applied at each position of the scan in order to draw the $|\rho^*|$ map.

In parallel, 1000 traces of current were extracted from the upper metal layer of *PA* with RedHawk and the $\sqrt{V^*(\eta)}$ map was drawn by applying Eq. 29 on the simulated $\varepsilon(t)$ induced in a

probe with $d = 100\mu m$ and placed at $z = 5\mu m$.

Fig. 39 shows maps corresponding to the scanned area of *PA*. The entire layout cannot be shown due to confidential constraints. One can observe that experimental and simulated maps agree well. Both show that this product presents a large area where the leakage is strong.

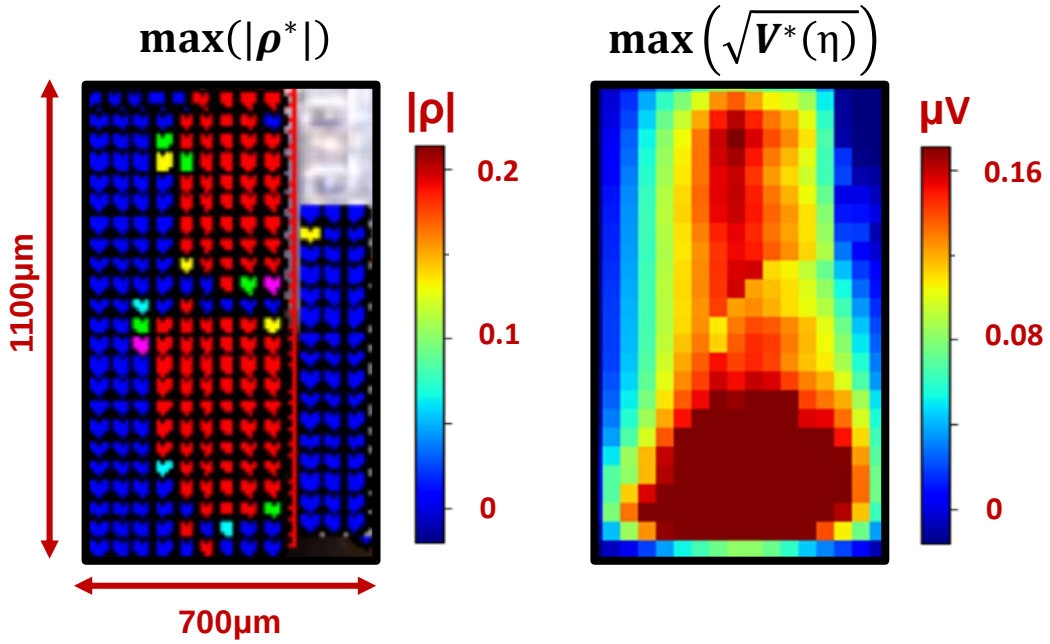

Figure 39: Experimental $|\rho^*|$ and simulated $\sqrt{V^*(\eta)}$ maps for the STMicroelectronics product *PA*.

To remedy this problem, *PA* was redesigned in order to reduce as much as possible the EM hotspot area and strength. The new version of the IC, *PB*, has then also been exposed to the simulation flow. Fig. 40 shows the simulated $\sqrt{V^*(\eta)}$ maps for both *PA* and *PB*. The comparison of both maps clearly shows that *PB* has significantly smaller leaky area; design modifications are therefore effective.

These results have represented an important achievement during this thesis. First, they allowed to state that the flow is effective not only for testchips but also for real products. Second, they confirmed that the flow can be used for post-silicon verification of formerly designed and manufactured ICs.

Next section focuses on the use of the flow to evaluate the soundness of countermeasures at design stage.

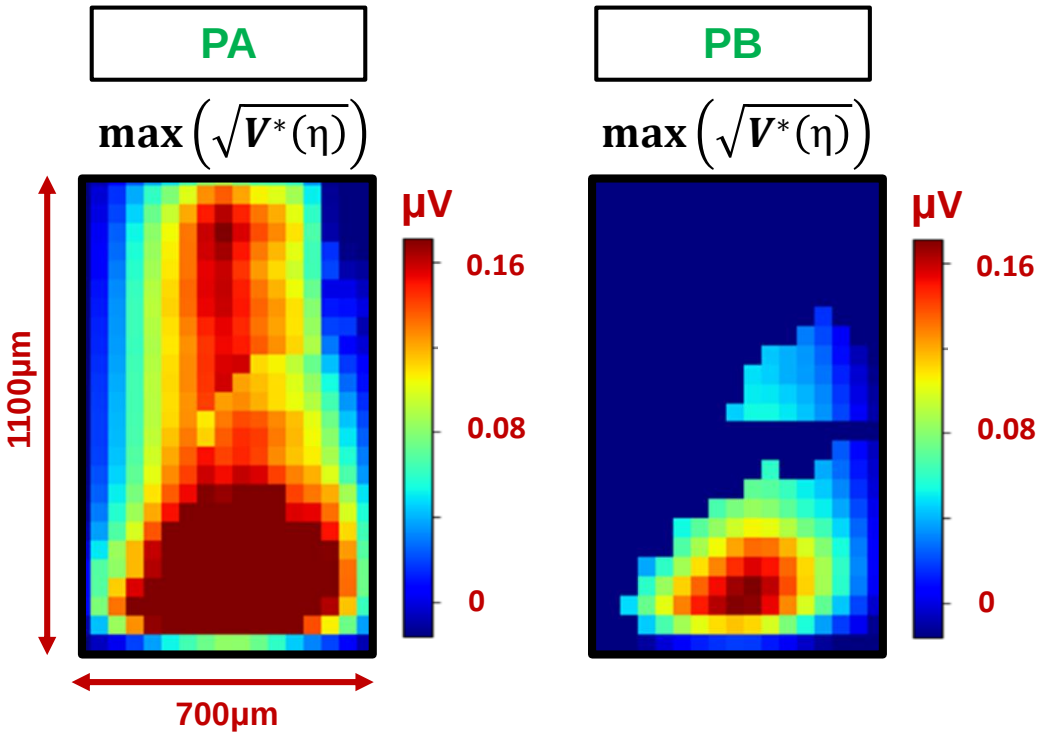

Figure 40: Simulated $\sqrt{V^*(\eta)}$ maps for *PA* (left) and *PB* (right).

5.4 Evaluation of countermeasures at design stage

As aforementioned, the threat represented by EM SCA is increasing the more and more in the last decades. Indeed, adversaries regularly find new solutions to break the security of ICs and retrieve sensitive data. Hence the need for developing countermeasures which make these attacks harder to put into practice, knowing that it is impossible, at the moment, to assure that a single given countermeasure makes impossible for adversaries to identify the secret key.

Many smart and efficient countermeasures have been proposed in the literature. The most popular [42], [43], [44] randomize the course of algorithms and thus physical leakages such as EM radiations. However, when it comes to integrating them, all benefits of such countermeasures can sometimes vanish because of physical effects in devices or some negligence during the design stage. When this occurs, this causes a huge loss of time and money. Hence the need for verification tools and methodologies prior to fabrication (and hence the need for the simulation flow introduced in this thesis). In this context, being able to test the effectiveness of a countermeasure against EM

attacks at design stage would be an important added value for secure IC designers. This flow can be used for this purpose. In the following paragraphs three countermeasures are tested with the simulation flow and comparisons with experiments conducted when the silicon was available.

5.4.1 Choosing between power routing strategies

The first countermeasure involves the power routing strategy. It has been anticipated in previous sections that the power routing structure of ICs can have a great impact on its robustness against EM attacks. Thus, designing the PGN so as to minimize their EM radiations is very important. Indeed, the greater is the amplitude of EM radiations, the greater is the SNR of the traces collected by EM probes and thus the less measures are polluted by the measurement noise.

As shown previously, the magnetic field radiated by an IC directly depends on the current flowing in the power (Vdd) and ground (Gnd) rails of the PGN. If the current flows in the same direction in both rails, the magnetic fields radiated by these rails have the same direction and thus pile up.

One possible countermeasure to reduce the SNR is thus to design the PGN so that the current in the power and ground rails flows in opposite directions [23]. In this way, the magnetic fields radiated have an opposite direction and, thus, compensate each other (at least in part). Fig. 41 shows this compensation effect caused by two wires crossed by currents flowing in opposite directions.

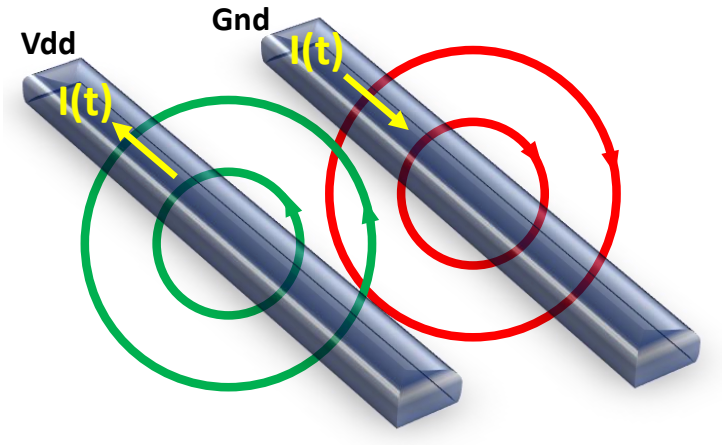

Figure 41: Compensation on the magnetic field radiated by Vdd and Gnd wires in which the currents flow in opposite directions.

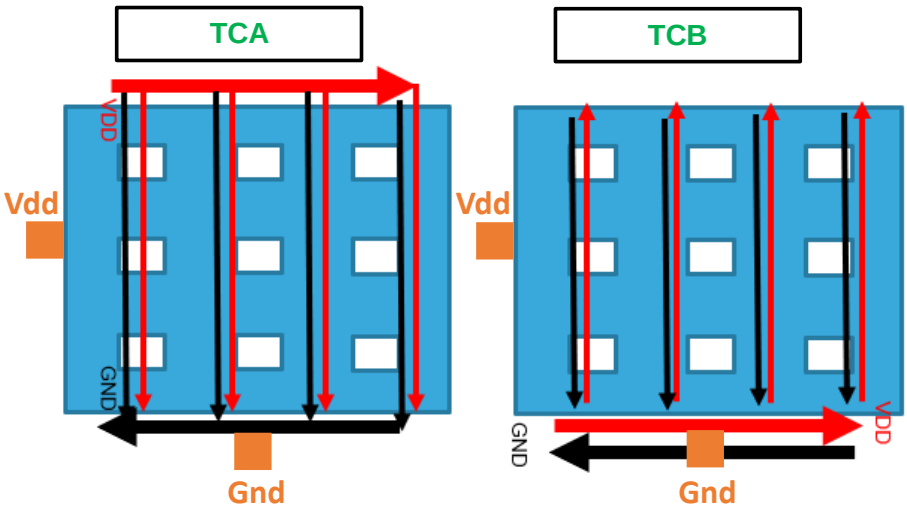

Figure 42: Routing policies of the upper level metal lines of Vdd and Gnd for TCA and TCB.

This countermeasure was implemented in one testchip: TCB. TCA and TCB are quasi-identical. The only difference is the routing strategy of the PGN (Fig. 42). As shown, in TCA the currents flow in the same directions, while in TCB in opposite directions. As a consequence, TCB should present lower EM radiations and a better robustness against EM attacks.

Using the simulation flow and the Noise-to-Add concept, one can test by simulation if the countermeasure implemented on TCB is effective in reducing its EM radiations and thus its leaky areas.

These two testchips being also available on silicon, the simulations results were compared with experimental ones. To that aim, two experimental near-field scans on both TCA and TCB were performed with a Langer ICR HH100 probe (diameter $d = 100\mu m$) parallel to the IC surface and placed at $z = 100\mu m$. Then, Eq. 13 was applied at each position of the scan and the $|\rho^*|$ maps were drawn.

The corresponding $\sqrt{V^*(\eta)}$ maps were drawn by applying Eq. 29 on the simulated $\varepsilon(t)$ induced in a probe with $d = 100\mu m$ and placed at $z = 100\mu m$, starting from the current traces extracted with RedHawk from the upper metal layer (AluCap) of both testchips. The maps were drawn to have the same color scale in order to highlight the differences between the two testchips.

Fig. 43 shows the comparison between TCA and TCB. The first observation one can do is that experimental $|\rho^*|$ and simulated $\sqrt{V^*(\eta)}$ maps are in good agreement. This constitutes another proof of the soundness of the approach. Secondly, one can observe that the countermeasure seems

to work. In fact, *TCB* shows weaker leakages with respect to *TCA*. This is an important confirmation that the flow is effective in testing a countermeasure by simulation. In this example the silicon was available and making comparisons was possible, but of course this approach can (and should) be used even with new products which are not available on silicon yet and which are still in the design stage.

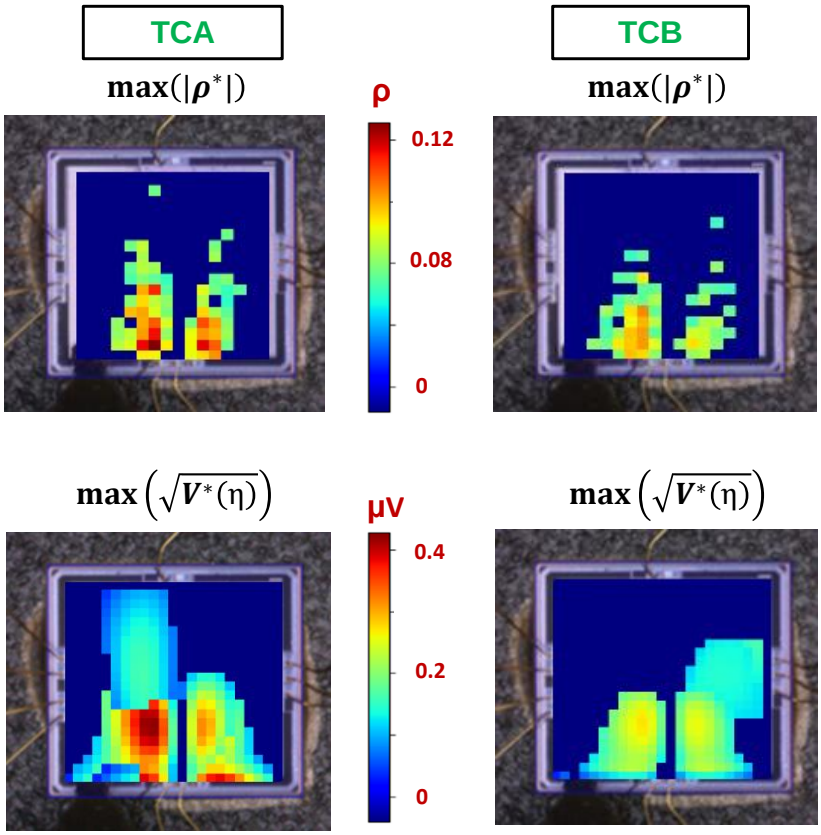

Figure 43: Experimental $|\rho^*|$ and simulated $\sqrt{V^*(\eta)}$ maps for *TCA* and *TCB*.

This was a simple countermeasure that designers can implement to improve the robustness of ICs against EM attacks. Following this idea, other routing policies for the PGN can be imagined. Indeed, it is possible to design structures allowing to further reduce the EM radiations.

A possible improvement of *TCB* has been simulated. Fig. 44 shows the power routing of a testchip *TCC* (which is not available on silicon) which should radiate a magnetic field even lower than *TCB*. As shown, the currents flow in opposite directions, both along the horizontal and vertical directions.

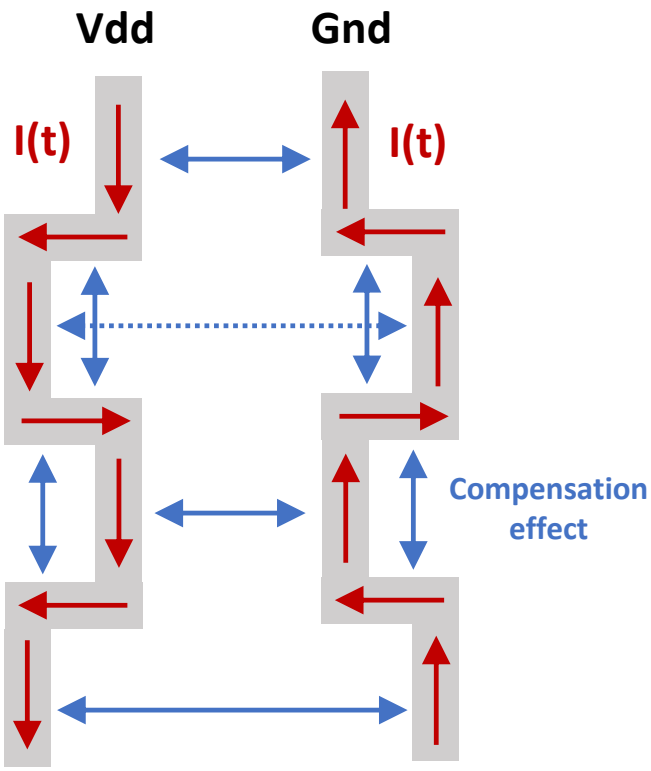

Figure 44: Power routing strategy of the testchip *TCC*.

Vdd and *Gnd* rails of *TCC* are designed so that to form a kind of "serpentine". This structure introduces another compensation effect. In fact, as shown in Fig. 44, a loop is formed along each *Vdd* and *Gnd* rail. In this manner, the magnetic field radiated by each horizontal piece of the rail is compensated by that radiated by another horizontal piece in which the current flows in an opposite direction. Thus, this countermeasure should be more effective because it combines two compensation effects. The first one is due to the opposite direction of the current flowing in the *Vdd* and *Gnd* rails. The second is due to the loops formed on the same rail which contribute to reduce the magnetic field radiated by each rail.

Fig. 45 shows the resulting simulated $\sqrt{V^*(\eta)}$ maps for *TCA*, *TCB* and *TCC*. As aforementioned, *TCC* is not available on silicon, so the comparison between experiments and simulations was not possible. Be that as it may, the countermeasure implemented on *TCC* significantly reduces the magnetic field radiated by the circuit and *TCC* should be more robust against EM SCA than *TCA* and *TCB*.

These examples are of prime importance. Indeed, they show that a countermeasure can be

tested prior to fabrication and thus before having the silicon at disposal. This is an enormous added value for secure IC designers.

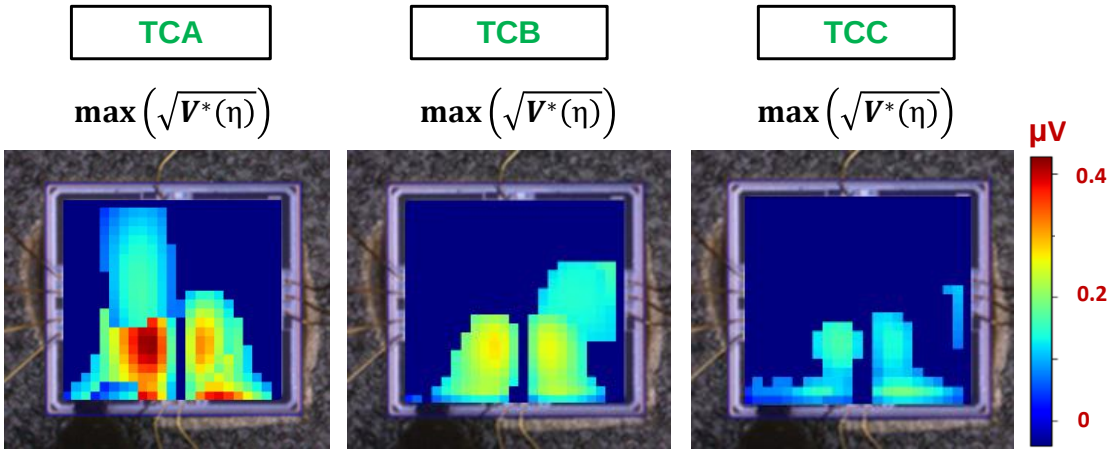

Figure 45: Simulated $\sqrt{V^*(\eta)}$ maps for TCA, TCB and TCC.

In next section the simulation flow is used to test another countermeasure prior to fabrication.

5.4.2 Impact of the the supply voltage

In this section, at first, the effect of decreasing or increasing the supply voltage of an IC on its robustness against EM attacks is investigated. Varying the supply voltage could be an effective countermeasure because the voltage supplying CMOS gates has an impact on their speed and power consumption.

Following Eq. 1, Fig. 46 shows the relation between the power consumption and the supply voltage of CMOS gates for Vdd ranging between $0.8V$ and $1.4V$, $C_L = 10fF$, $f_{clk} = 50MHz$ and $\alpha = 0.5$. One can observe that the power consumption quadratically varies with respect to Vdd. Furthermore, reducing Vdd by $\sqrt{2}$ divide roughly by 2 the power consumption of ICs. It follows that also the magnetic field radiated should be impacted by changes of the supply voltage.

On the other hand, the speed of CMOS gates is directly proportional to Vdd. It follows that CMOS gates supplied with higher Vdd produce a faster output ramp and then a steeper $dI(t)/dt$. Fig. 47 shows this effect. To obtain this figure, an analog simulation of a CMOS inverter was launched. The figure shows the gate output current required to charge a load capacitor $C_L = 50fF$

with two different Vdd values ($1.8V$ and $3.3V$). As shown, the output ramp is greatly steeper with $Vdd = 3.3V$ than with $Vdd = 1.8V$. More sudden changes in the current flowing in CMOS gates make these current easier to be exploited with an EM probe.

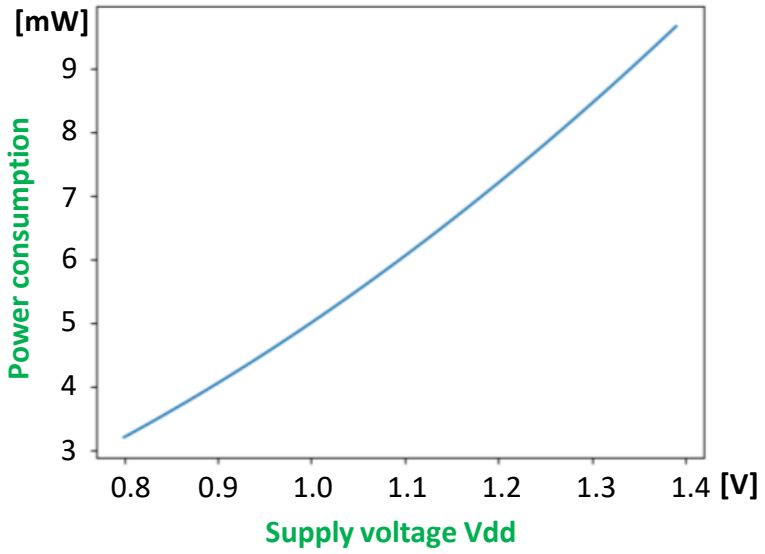

Figure 46: Relation between dynamic power consumption and supply voltage Vdd of CMOS gates.

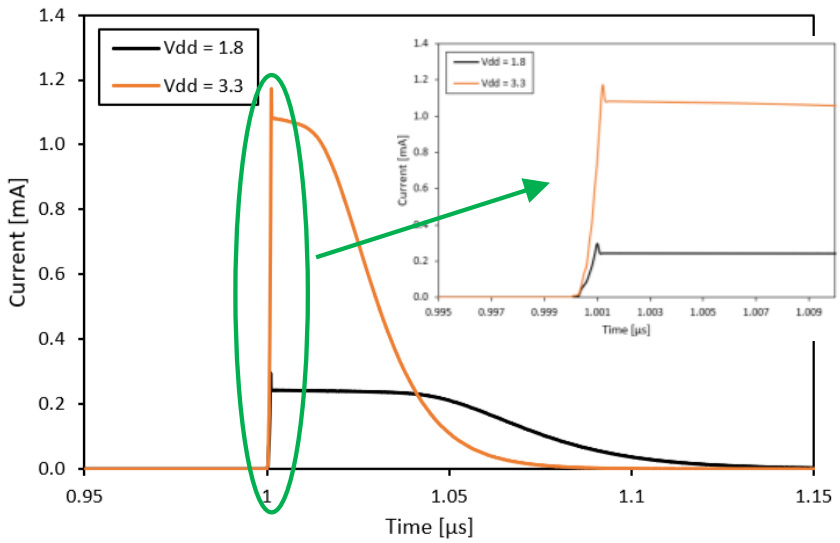

Figure 47: Output ramp of a CMOS inverter supplied with $Vdd = 1.8V$ (black) and $3.3V$ (orange).

This effect is evaluated both by simulation and through experiments. Experimental $|\rho^*|$ maps

were performed for TCA for supply voltage values equal to $1.08V$, $1.2V$ and $1.32V$, i.e. the three Vdd corner values. 5000 EM traces at each position of TCA were acquired. In parallel, 1000 electromotive force traces per virtual probe were simulated with the flow to get the respective $\sqrt{V^*(\eta)}$ maps. These simulations and experiments were done with a Langer ICR HH100 probe (diameter $d = 100\mu m$) parallel to the IC surface and placed at $z = 100\mu m$.

Fig. 48 allows comparing the experimental maps with the simulated ones. One can observe that increasing the supply voltage value by more than $200mV$ (16% of the nominal voltage value) does not drastically change the $|\rho^*|$ and $\sqrt{V^*(\eta)}$ maps which are in good agreement. Indeed, one can only observe, both in simulation and in practice, a slight widening of the areas where $|\rho^*|$ and $\sqrt{V^*(\eta)}$ are greater than 0.10 and 0.3 respectively.

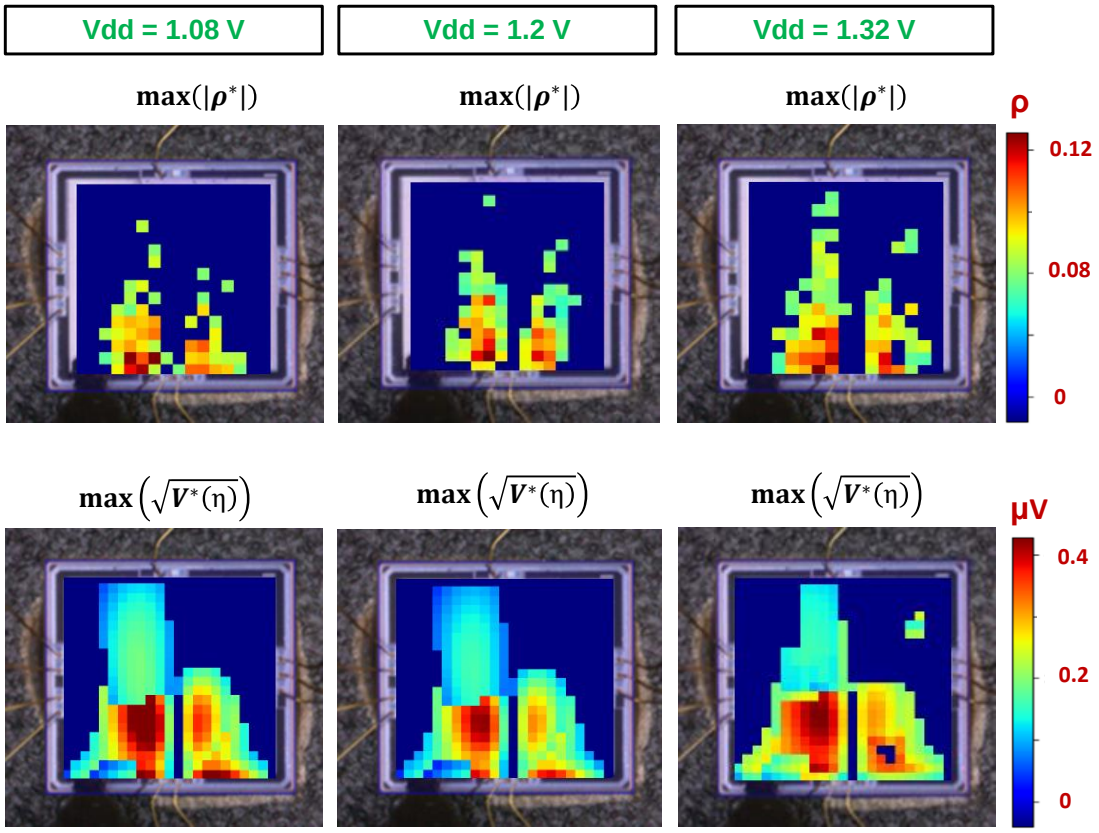

Figure 48: Experimental $|\rho^*|$ and simulated $\sqrt{V^*(\eta)}$ maps for $Vdd \in \{1.08V, 1.2V, 1.32V\}$.

One could find this result surprising since the dynamic power consumption of ICs quadratically depends on Vdd as shown in Fig. 46. However, this can be explained by observing that the electromotive force $\varepsilon(t)$ induced in the EM probe does not depend on the power consumption but

on the derivative of the current consumed by transistors which is proportional to $(Vdd - V_{th})^2$, with V_{th} the threshold voltage of transistors (assumed equal for P and N transistors for the sake of simplicity). As a result, the derivative of $\varepsilon(t)$ with Vdd is proportional to $2 \cdot (Vdd - V_{th})$ and is thus fairly low for low power technologies for which $Vdd \gtrsim 2 \cdot V_{th}$. This also explains why the EM radiations of an IC designed with 350nm CMOS technology with a nominal voltage equal to $3.3V$ and those of a design in a 40nm technology with a nominal voltage equal to $1.2V$ remain measurable with the same equipment.

Even if CMOS gates are theoretically impacted by changes of their supply voltage, these experiments indicate that simply decreasing the supply voltage of ICs in order to reduce their power consumption and then the magnetic field radiated is not enough to improve the robustness of ICs against EM SCA.

One possible improvement of this countermeasure consists in dynamically and regularly changing the Vdd/Gnd. The goal of this countermeasure is adding random shifts in the clock edges with continuous changes of the supply voltage so that the power consumption does not follow the HW model.

The impact of this countermeasure on the number of traces required to get the secret key was analysed experimentally and by simulation. To that aim, one leaky position, shown in Fig. 49, was considered. 10000 traces were measured above this position for three different Vdd values: $1.08V$, $1.2V$ and $1.32V$. This provided three sets of traces: $S^{meas}_{1.08}$, $S^{meas}_{1.2}$ and $S^{meas}_{1.32}$.

Similarly, 1000 traces above this position were obtained by simulation. This provided $S^{sim}_{1.08}$, $S^{sim}_{1.2}$ and $S^{sim}_{1.32}$. Measured and simulated traces acquired, two experiments were performed.

First, ten CPA were performed on sets $S^{meas}_{1.2}$ and $S^{sim}_{1.2}$ with $n \in \{500, 1000, ..., 10000\}$ and $n \in \{100, 200, ..., 500\}$ traces, respectively. The average correlation after the processing of n traces was computed and recorded.

Second, ten CPA were performed on sets:

$$S^{meas} = S^{meas}_{1.08} \cup S^{meas}_{1.2} \cup S^{meas}_{1.32} \tag{30}$$

and:

$$S^{sim} = S^{sim}_{1.08} \cup S^{sim}_{1.2} \cup S^{sim}_{1.32} \tag{31}$$

with $n \in \{500, 1000, ..., 10000\}$ and $n \in \{100, 200, ..., 500\}$ traces randomly selected.

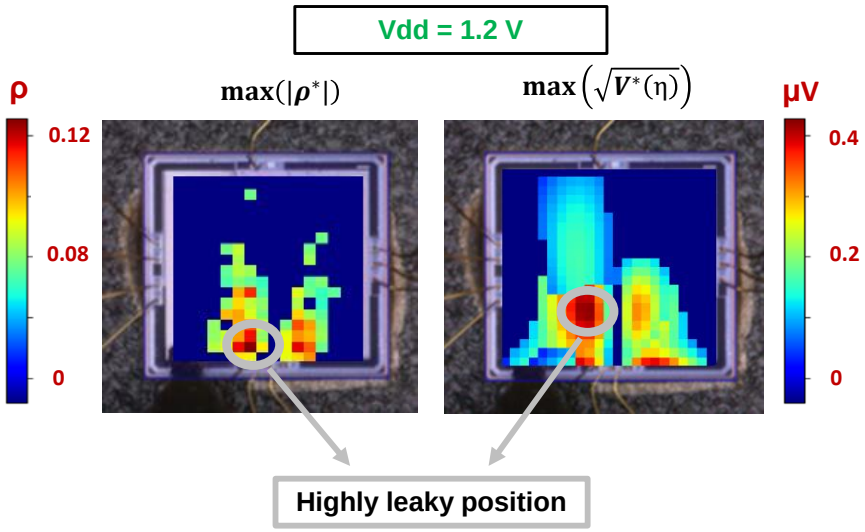

Figure 49: Leaking position of TCA presenting high $|\rho^*|$ and $\sqrt{V^*(\eta)}$ values.

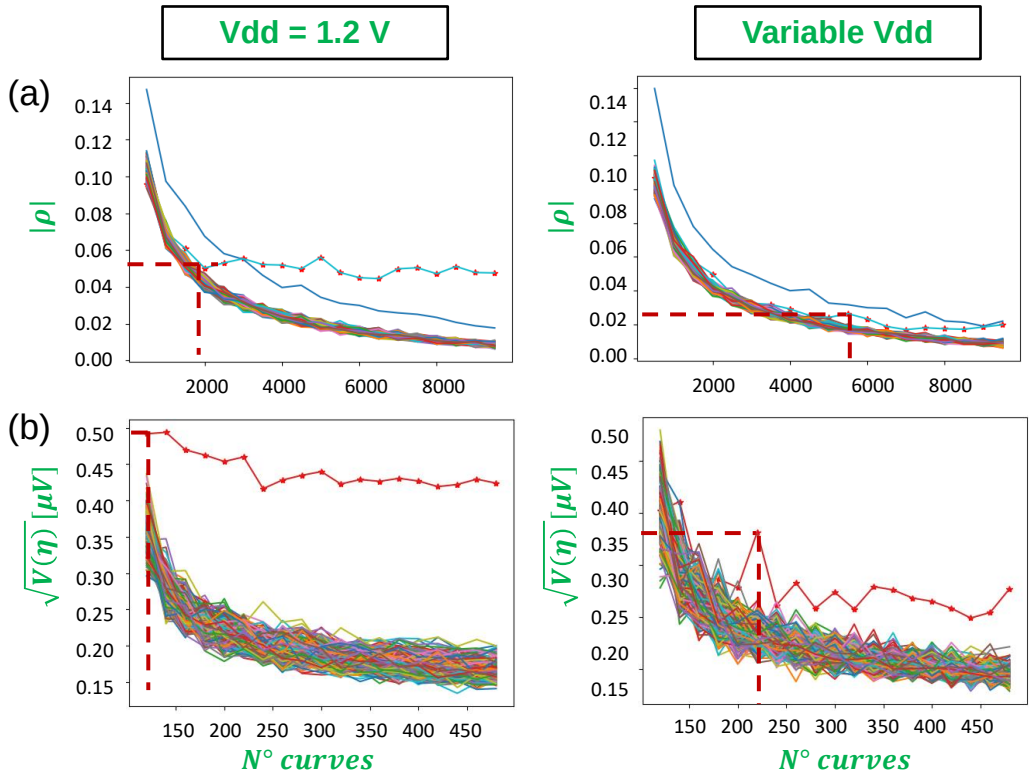

Figure 50: Evolution of $|\rho^*|$ and $\sqrt{V^*(\eta)}$ with the number of processed traces for (a) fixed supply voltage ($1.2V$) and (b) supply voltage randomly changing $Vdd \in \{1.08V, 1.2V, 1.32V\}$.

Then the evolution of the correlation with the number of processed traces was plotted for both experiments. Fig. 50 shows the obtained results. One can observe that for a fixed supply voltage

equal to $1.2V$, 2000 and 100 traces are required in average to get the key experimentally and by simulation, respectively.

One can also observe in Fig. 50 that the number of traces required to get the key increases up to 5800 (+190%) and 225 (+125%) when Vdd is randomly chosen in $\{1.08V, 1.2V, 1.3V\}$ experimentally and by simulation, respectively.

This countermeasure showed to be effective by simulation and experimentally. This demonstrates the interest of the flow for evaluating countermeasures prior to fabrication.

Next section analyses a third countermeasure experimentally and by simulation.

5.4.3 EM jamming: injecting random noise in EM traces

The objective of the EM jamming countermeasure is to add a random jittering noise in order to reduce the SNR of the collected EM traces and thus the statistical link between these traces and the data processed by the IC.

There are two main solutions to reduce the SNR: reducing the amplitude of the signal which carries sensitive information or increasing the noise amplitude. The proposed countermeasure follows the second option. In particular, the noise is increased thanks to a specific device connected to embedded antennas. These antennas create a noisy magnetic field which perturbs the EM leakage acquisition above the crypto-processor (AES). This magnetic field has the same magnitude than the field generated by the IC and it is randomly active when EM leakages occur. The resulting total EM activity is thus different at each execution. Fig. 51 shows a sketch of the EM jamming principle.

As described in previous chapters, SCA exploit consumption differences of same sequences of data in order to retrieve secrets by ICs. Fig. 52 shows the difference of the EM activity related to 2 different executions.

The EM jamming IP is implemented close to a block to protect in order to hide its sensitive EM field. The delay and amplitude of the noise perturbation can be randomly changed at each cycle. Without activation of the EM jamming, adversaries can retrieve sensitive data by exploiting EM activity differences when the crypto-processor executes the same sequence. The differences of each sequence are linked to the data processed by the IC.

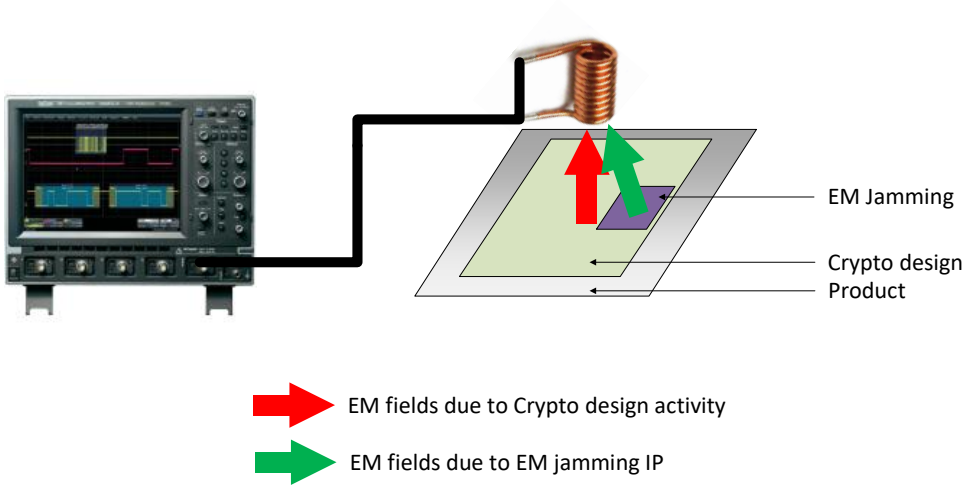

Figure 51: Schematic of the EM jamming concept.

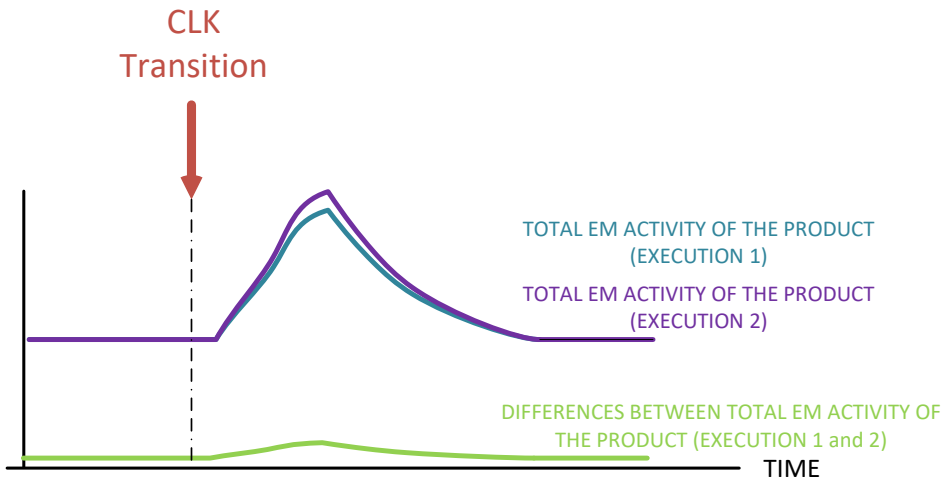

Figure 52: Consumption comparison between 2 different executions.

With activation of the EM jamming, differences between 2 executions are not directly linked to the data and SCA are more difficult to put in practice, especially if the EM jamming generates a magnetic field with random behavior. Fig. 53 shows an example of random noisy magnetic field added to the EM radiations of the chip.

What is important to hold back is the fact that the noisy field generated by the EM jamming IP must be inserted during the time interval in which the leakage occur in order to reduce the correlation between EM traces and data manipulated by the IC.

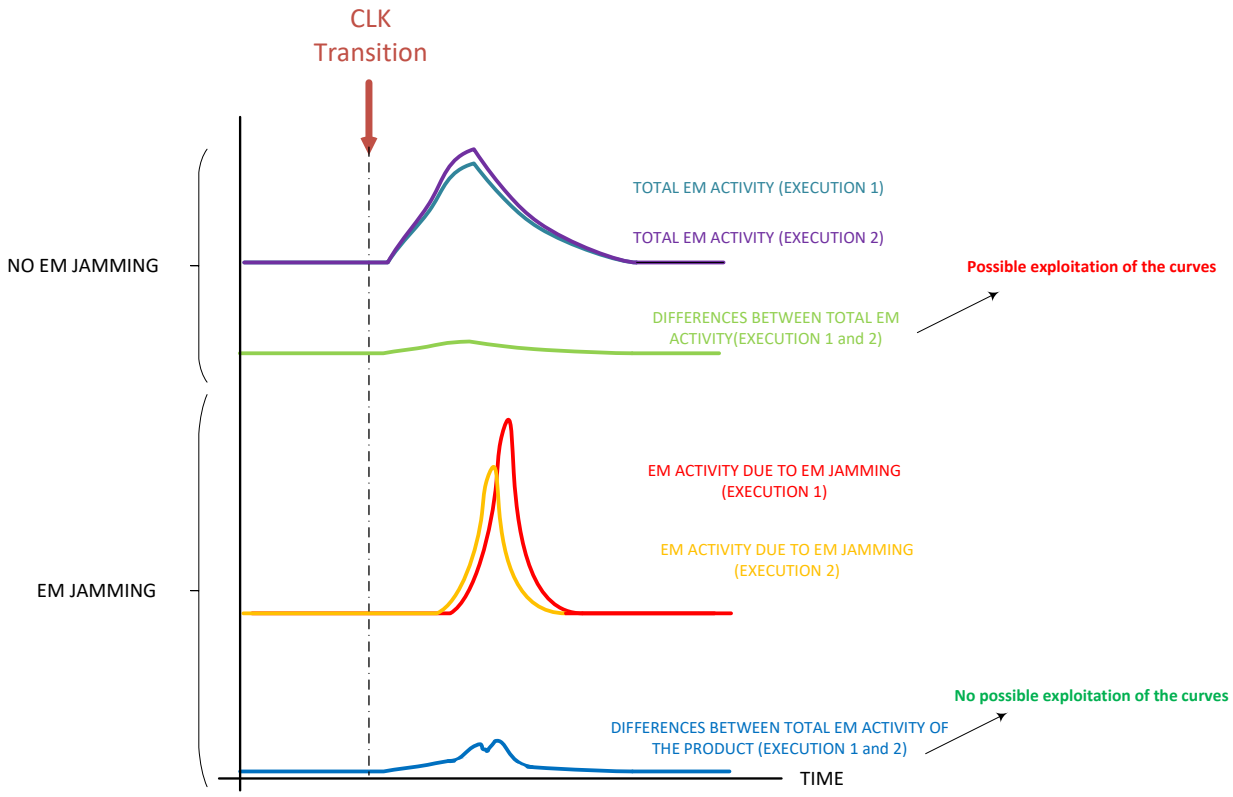

Figure 53: Example of random noise added to the EM emissions due to the chip activity.

Next analyses focus on this aspect. As a first experiment, a leaky position of TCA was targeted. At this position, a Langer ICR HH100 probe (diameter $d = 100\mu m$) was placed parallel to the IC surface at $z = 100\mu m$ in order to collect 3 sets $S1$, $S2$ and $S3$ of 10000 EM traces:

- $S1$ is a set of traces with the countermeasure deactivated.
- $S2$ is a set of traces with the countermeasure activated but not centered on the leakage.
- $S3$ is a set of traces with the countermeasure activated and centered on the leakage.

The sampling rate of the digital oscilloscope was set to $10GS/s$ in order to have the best possible resolution.

Fig. 54a shows the vertical variances associated to $S1$ (blue) and $S2$ (green) and Fig. 54b highlights the correct sub-key guess ($|\rho^*|$) among all the hypotheses for the same sets. As shown, the noise generated by the countermeasure has a high variance but it is only partially centered on the window where the leakage occurs (and thus where the correlation is strong). As a consequence, its effectiveness is almost null and the correlation remains strong in both cases.

Fig. 55 proposes the same experiment associated to $S1$ and $S3$. One can observe that now the noisy field is correctly centered on the leakage and the correlation associated to $S3$ is weaker than that obtained on $S1$ (even if this effect remains weak). This demonstrates the complexity of this countermeasures as it needs to be finely set in order to produce some effects.

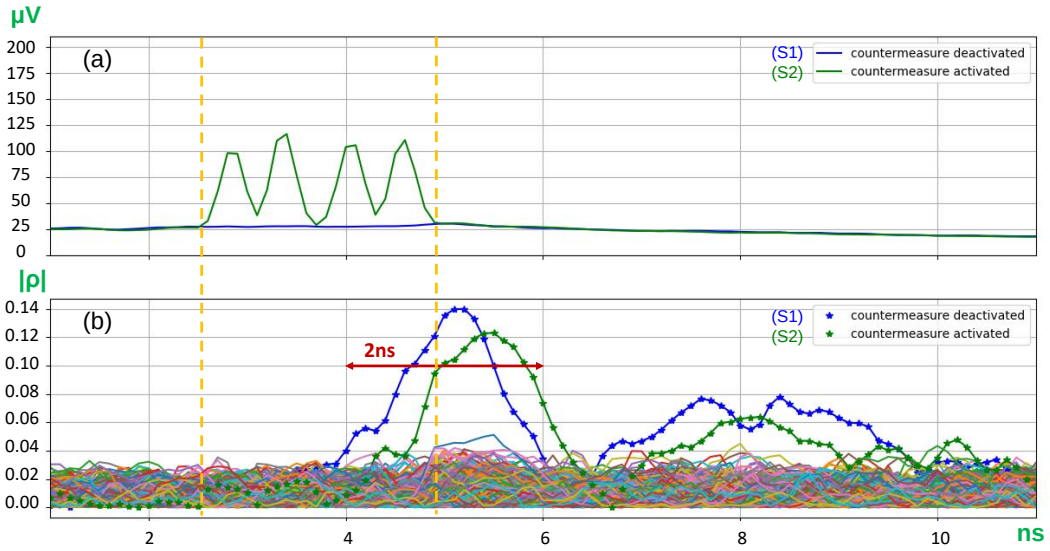

Figure 54: (a) Vertical variances and (b) correlations associated to sets $S1$ and $S2$.

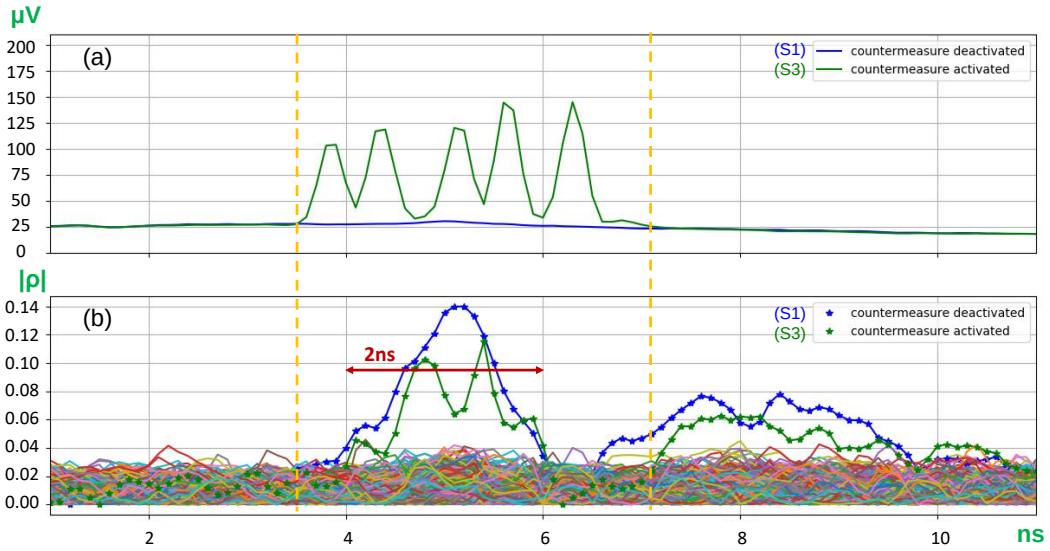

Figure 55: (a) Vertical variances and (b) correlations associated to sets $S1$ and $S3$.

To further sustain the (slight) effect of the countermeasure and following the procedure exposed in section 5.4.2, ten CPA were performed on sets $S1$, $S2$ and $S3$ with $n \in \{200, 400, ..., 3000\}$ traces

randomly selected. The average correlation after the processing of n traces was computed and recorded.

Fig. 56 shows the evolution of the correlations with the number of processed traces and highlights the correlation obtained with the correct sub-key guess ($|\rho^*|$) for the 3 sets of traces. One can observe that without countermeasure (Fig. 56a) the secret sub-key is disclosed after the processing of 750 curves. With countermeasure this number increases up to 1200 (+50%) and 1000 (+25%) when it is centered (Fig. 56c) or not (Fig. 56b) on the leakage.

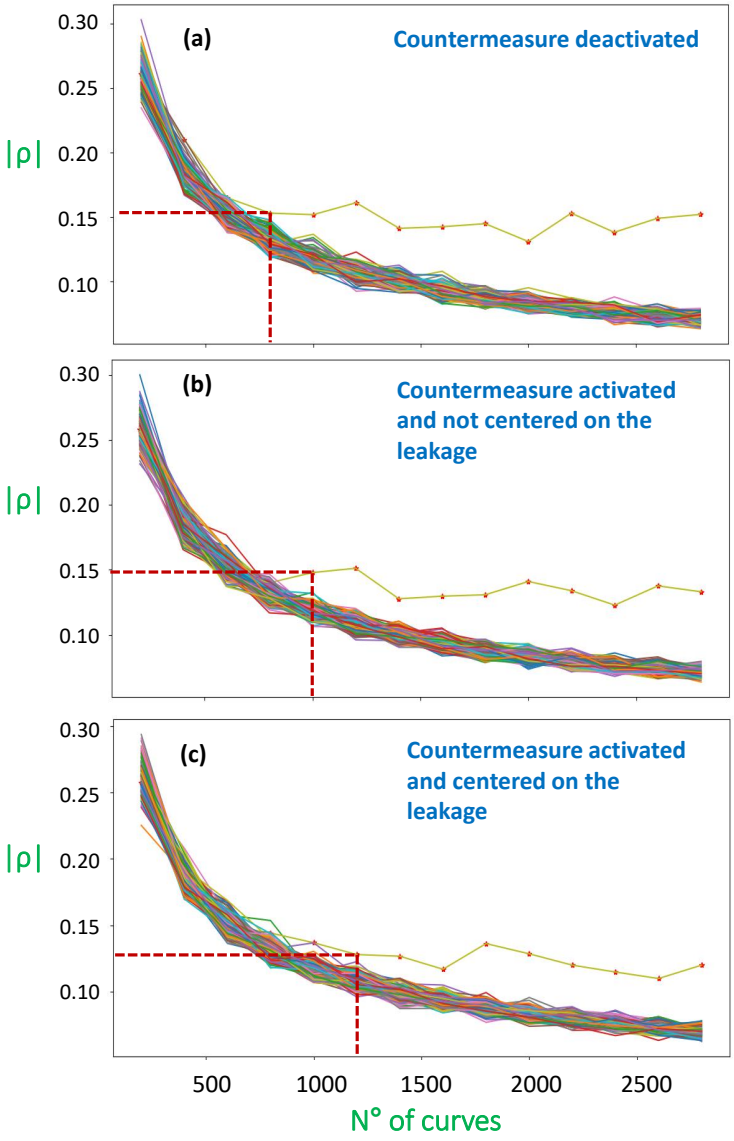

Figure 56: Evolution of $|\rho^*|$ associated to sets (a) $S1$, (b) $S2$ and (c) $S3$.

This countermeasure was also tested by simulation with the developed flow. The goal was to show, even by simulation, that the EM jamming perturbation needs to be correctly inserted when the leakage occurs in order to be effective. 1000 simulations were run with RedHawk and the electromotive force induced in a probe with diameter $d = 100\mu m$ and placed at $z = 100\mu m$ from TCA was computed. In parallel, the noisy magnetic field radiated by the EM jamming IP was reproduced by designing an analog schematic in the Cadence Virtuoso environment. The currents flowing in the 6 antennas composing the IP were simulated and collected. Then, the electromotive force induced in the probe by the magnetic field radiated by each segment of length $20\mu m$ of the antennas was simulated. These contributions were finally added, at the correct position, to the B_Z matrix representing the magnetic field radiated by TCA. This analog simulation was necessary because RedHawk only allows to collect the currents flowing in the power and ground grids but not those flowing in the wires interconnecting logic gates.

Fig. 57 presents three $\sqrt{V^*(\eta)}$ maps obtained at the same time sample $t = t_n$. This latter corresponds to the instant of time where $\sqrt{V^*(\eta)}$ is maximum with no countermeasure activated. Fig. 57a shows the $\sqrt{V^*(\eta)}$ map obtained without EM jamming. In Fig. 57b the countermeasure is activated but the antennas generate a perturbation only in the first time interval in which the leakage is strong. As a result, Fig. 57a and 57b are practically identical. Finally, in Fig. 57c the perturbation covers the entire leakage window. As a consequence, Fig. 57c shows a lower level of noise that has to be added to hide the leakage than Fig. 57a. Even by simulation this effect is pretty slight, but this example showed again a good agreement between experiments performed in practice and by simulation.

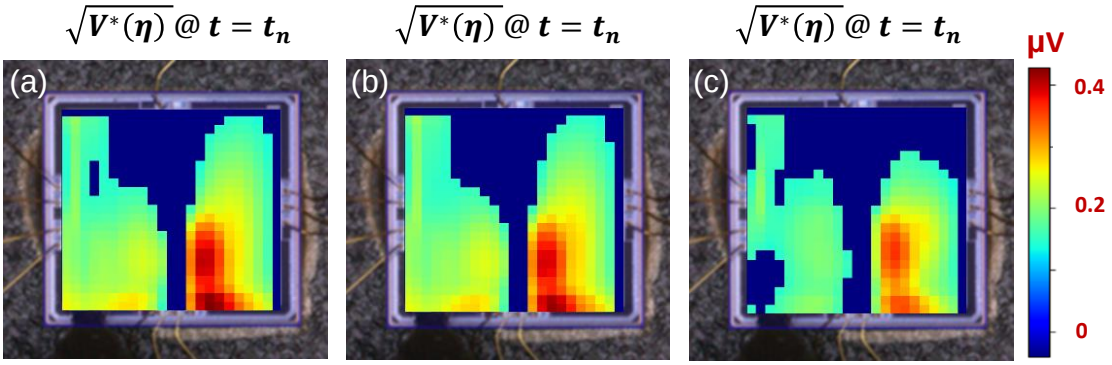

Figure 57: $\sqrt{V^*(\eta)}$ maps with (a) and without (b) and (c) EM jamming.

These experiments allowed to test another countermeasure by simulation. Even if the EM jamming IP needs to be improved and further tested, the developed flow resulted again to be effective in evaluating a countermeasure at design stage. In fact, the flow allowed to explain the poor results obtained in practice. Furthermore, it provided guidelines to enhance the EM jamming IP.

Next section sums up the concepts exposed in the previous paragraphs and concludes the chapter.

5.5 Conclusion

In this chapter the usefulness of the developed simulation flow at design stage has been presented.

In the first part, the flow has been used to identify leakage hotspots, i.e. the sources of EM hotspots. The temporal evolution of leakage hotspots has been analysed time sample by time sample. This procedure allows visualizing the apparition of leakages and their propagation over the IC surface.

In the second part of this chapter, the flow has been used to analyse a real STMicroelectronics product which was manufactured before the development of this flow. EM leaky areas found by simulation were in good agreement with experimental ones, demonstrating that the flow is effective in disclosing EM hotspots not only on testchips but even in real and complex ICs. A new version of the product has been tested and analysed with the flow showing weaker leaky areas.

In the third part of the chapter it has been shown that the flow can be used to evaluate the effectiveness of countermeasures at design stage. Three countermeasures have been tested. Agreements between experimental and simulated results have demonstrated the soundness of the approach.

Next chapter summarizes all the researches carried out during this thesis and highlights the main aspects on which it would be most necessary to work.

Chapter 6

Conclusion and perspectives

Contents

Conclusion and perspectives

This chapter sums up all the researches and works that have been presented in this manuscript. The impact of the obtained results on the state of the Art and on the industrial community is also introduced. Then, the potential perspectives that this work has open and the main aspects that should be studied in order to add other important results to this thesis is discussed.

6.1 Principal results and achievements

The principal objective of this thesis was to develop a tool allowing to perform EM SCA by simulation and to test the robustness of ICs against these attacks prior to fabrication. The importance of identifying hotspots during the design stage of a device and how expensive and tedious is to apply countermeasure to leaky products post-silicon has been illustrated.

Two types of hotspots have been defined: leakage and EM hotspots. The first ones are the source of EM hotspots and are caused by leaking CMOS gates, due to their switching activity during the functioning of the circuit. EM hotspots are instead the positions of the IC where attackers can retrieve sensitive data by placing an EM probe capturing the vertical magnetic field radiated by the circuit.

In the state of the Art (chapter 2), it has been highlighted the lack of such a simulation tool in the scientific community and presented why this lack constitutes a serious problem for secure IC manufacturers. Indeed, only few works in the literature deal with identifying EM leakages at simulation stage, and there is no work proposing comparisons between experimental and simulated EM attack maps. This thesis aimed precisely at filling this gap and proposing a solution to draw attack maps by simulation and compare the results with experimental ones.

The researches presented in chapter 3 have led to two principal contributions. The first one is a simulation flow allowing to emulate all the electromagnetic phenomena triggered in practice

when EM SCA are performed. The flow is primarily based on the use of an IR drop tool from the ANSYS company, RedHawk. Among other functionalities, RedHawk allows to extract the temporal evolution of the currents flowing in the PGN of ICs. It has been made an assumption (then verified) that upper metal layers are the main contributors to the magnetic field captured by EM probes, because the currents flowing in these layers are several orders of magnitude more intense than those flowing in lower metal layers and, in addition, upper layers are the closest to EM probes when EM attacks are performed front-side.

The PGN of ICs has been modeled as a set of finite length wires and the Biot-Savart law has been applied to each of these wires to reproduce the magnetic field radiated by entire circuits. A focus on the vertical component of the magnetic field has been done, as adversaries usually perform EM attacks by using horizontal probes (parallel to the IC surface) capturing this component. Then, the magnetic flux captured by an EM probe as well as the electromotive force induced in it by variations of the flux have been modeled.

The first validation of this simulation flow has showed to be unsuccessful. Indeed, obtained experimental and simulated CPA maps were totally different. Two main reasons explaining these differences were found: the insensitivity of the correlation coefficient (involved in the significance test for a correlation coefficient [11], [12]) and the absence of noise in simulated traces. It has been shown, through a concrete example on a simple wire, that correlation maps are ineffective in identifying EM hotspots by simulation.

An innovative solution, called Noise-to-Add and representing the second and main contribution of this thesis, has thus been presented. It consists in computing the level of noise that has to be added to the simulated traces in order to hide a potential leakage. This solution is simple and very effective. In fact one can replace the correlation with the Noise-to-Add during an attack without loss of efficiency because the ranking of the Noise-to-Add is the same as that of the correlation. The effectiveness of the Noise-to-Add approach has been validated on a simple wire. From this interesting concept, an important link with the notion of SNR has been done. The notion of SNR is very familiar to designers and allows them to evaluate the dangerousness of a leakage prior to fabrication and eventually modify the design to eliminate the errors.

In chapter 4 the magnetic simulation flow and the Noise-to-Add concept have been validated

on a testchip manufactured by STMicroelectronics, designed in 40*nm* CMOS technology and embedding an AES-128 block cipher. The flow showed to be effective in identifying EM hotspots by simulation. Moreover, the flow reproduced the variations of the probe characteristics and localization (height and diameter) used to perform EM attacks. Experiments with vertical probes (capturing the horizontal magnetic field) as well as comparisons between front-side and back-side analyses have been proposed in order to demonstrate that extracting the currents flowing in top metal layers is sufficient to accurately emulate the magnetic field captured by EM probes.

Another corroboration of the flow in disclosing EM hotspots has been given by proposing a comparison between the simulated Noise-to-Add maps and the experimental partial Guessing Entropy (*pGE*). This experiment has shown that when the number of curves collected is sufficient, simulated and experimental maps show the same leaking coordinates where an EM probe can capture a leakage.

After all these validations, the usefulness of the developed flow at design stage has been presented in chapter 5. In particular, the flow can be used to verify the presence of both leakage and EM hotspots prior to fabrication, to perform post-silicon leakage analyses and to evaluate the effectiveness of countermeasures.

Leakage hotspots can be disclosed by analyzing the current flowing in lowest metal layers of ICs. Once suspects sections of standard cell rows are identified, designers can easily localize leaking CMOS gates through electrical or RTL simulations. In particular, it has been shown the evolution in the time domain of leakage hotspots and illustrated their propagation through the PGN network due to the spreading of the current. This approach has demonstrated the importance of disclosing not only EM hotspots but also leakage hotspots by simulation, and how these leakages are different.

The flow has been used on products that were manufactured before the developing of this flow. The flow showed to be effective in finding, by simulation, the same leaking areas observed in practice.

Finally, three countermeasures have been tested by simulation, the first involving the power routing strategy of ICs, the second involving changes of the supply voltage and the third involving the injection of random noise into the collected EM traces. Comparisons between experimental and

simulated maps were done, showing again the soundness of the proposed approach.

Next section investigates the perspectives that have been opened during this thesis.

6.2 Perspectives and future works

During this thesis, a simulation tool able to reproduce EM SCA and test the robustness of ICs against these attacks prior to fabrication has been proposed. This flow is effective and precise, however improvements can obviously be done. The entire Python flow on which the tool is based could be replaced by proper C codes to reduce simulation times.

Another interesting perspective is the study of the impact of process variations on EM SCA. Authors of [45] demonstrated that the power-attack tolerance (PAT) of embedded crypto-systems is deeply impacted by process variations. Following this work, it would be very interesting to explore the impact of such variations on the robustness of ICs against EM SCA.

Following the methodology presented in section 5.2, one more step may be to add a feature to the simulation flow so that it can directly identify leaky CMOS gates that are the sources of EM hotspots. In fact, the presented methodology allows to disclose leaky standard cells prior to fabrication, but designers still need to run electrical or RTL simulations in order to identify which gates are leaking. This would be an important added value to the flow.

Finally, in the last years the ANSYS company has developed a new version of RedHawk. This new version, called RedHawk SeaScape (RH-SC), also has a new functionality which is expected to disclose EM hotspots by simulation. One of the background tasks of this thesis has been working with the ANSYS support team in order to compare the developed simulation flow with the solution they offer. This track will be surely investigated in the next months and it could be an important validation of the researches carried out during this thesis. Maybe ANSYS will integrate the Noise-to-Add concept in RH-SC.

References

[1] F. Beck, "Integrated circuit failure analysis : A guide to preparation techniques," 1998.

[2] T. W. Lee and S. V. Pabbisetty, "Microelectronic failure analysis : Desk reference," 1993.

[3] S. Skorobogatov and R. Anderson, "Optical fault induction attacks," vol. 2523, Aug. 2002, pp. 2–12, ISBN: 978-3-540-00409-7. DOI: 10.1007/3-540-36400-5_2.

[4] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *Advances in Cryptology — EUROCRYPT '97*, W. Fumy, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51, ISBN: 978-3-540-69053-5.

[5] E. Biham and A. Shamir, Differential cryptanalysis of des-like cryptosystems, *Journal of Cryptology*, vol. 4 2004, pp. 3–72, 2004.

[6] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, M. J. Wiener, Ed., ser. Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25. available from: https://doi.org/10.1007/3-540-48405-1%5C_25.

[7] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," in *2017 IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2017, Irvine, CA, USA, November 13-16, 2017*, S. Parameswaran, Ed., IEEE, 2017, pp. 123–130. DOI: 10.1109/ICCAD.2017.8203769. available from: https://doi.org/10.1109/ICCAD.2017.8203769.

[8] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113, ISBN: 978-3-540-68697-2.

[9] M. Hutter and J.-M. Schmidt, "The temperature side-channel and heating fault attacks," English, in *Smart Card Research and Advanced Applications - CARDIS 2013, 12th International Conference, Berlin, Germany, November 27-29, 2013, Proceedings.*, ser. Lecture Notes in Computer Science, International Conference on Smart Card Research and Advanced Applications ; Conference date: 27-11-2013 Through 29-11-2013, ., 2013.

[10] D. Yucebas Ayaz and H. Yuksel, Power analysis based side-channel attack on visible light communication, *Physical Communication* [online], vol. 31 Apr. 2018, Apr. 2018. DOI: 10.1016/j.phycom.2018.04.013.

[11] R. Artusi, P. Verderio, and E. Marubini, Bravais-pearson and spearman correlation coefficients: Meaning, test of hypothesis and confidence interval, *The International Journal of Biological Markers* [online], vol. 17, no. 2 2002, pp. 148–151, 2002, PMID: 12113584. DOI: 10.1177/172460080201700213. eprint: https://doi.org/10.1177/172460080201700213. available from: https://doi.org/10.1177/172460080201700213.

[12] P. Bobko, *Correlation and regression : applications for industrial organizational psychology and management*, eng, 2nd ed. Thousand Oaks, [Calif.]: Sage Publications, 2001, ISBN: 0761923039.

[13] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, M. Joye and J. Quisquater, Eds., ser. Lecture Notes in Computer Science, vol. 3156, Springer, 2004, pp. 16–29. DOI: 10.1007/978-3-540-28632-5_2. available from: https://doi.org/10.1007/978-3-540-28632-5%5C_2.

[14] A. Vasselle, P. Maurine, and M. Cozzi, "Breaking mobile firmware encryption through near-field side-channel analysis," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES@CCS 2019, London, UK, November 15, 2019*, C. Chang, U. Rührmair, D. E. Holcomb, and P. Schaumont, Eds., ACM, 2019, pp. 23–32. DOI: 10.1145/3338508.3359571. available from: https://doi.org/10.1145/3338508.3359571.

[15] K. Tiri and I. Verbauwhede, A digital design flow for secure integrated circuits, *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* [online], vol. 25, no. 7 2006, pp. 1197–1208, 2006. DOI: 10.1109/TCAD.2005.855939. available from: https://doi.org/10.1109/TCAD.2005.855939.

[16] F. Regazzoni, A. Cevrero, F. Standaert, *et al.*, "A design flow and evaluation framework for dpa-resistant instruction set extensions," in *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, C. Clavier and K. Gaj, Eds., ser. Lecture Notes in Computer Science, vol. 5747, Springer, 2009, pp. 205–219. DOI: 10.1007/978-3-642-04138-9_15. available from: https://doi.org/10.1007/978-3-642-04138-9%5C_15.

[17] F. Regazzoni, S. Badel, T. Eisenbarth, *et al.*, "A simulation-based methodology for evaluating the dpa-resistance of cryptographic functional units with application to CMOS and MCML technologies," in *Proceedings of the 2007 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (IC-SAMOS 2007), Samos, Greece, July 16-19, 2007*, H. Blume, G. Gaydadjiev, C. J. Glossner, and P. M. W. Knijnenburg, Eds., IEEE, 2007, pp. 209–214. DOI: 10.1109/ICSAMOS.2007.4285753. available from: https://doi.org/10.1109/ICSAMOS.2007.4285753.

[18] F. Menichelli, R. Menicocci, M. Olivieri, and A. Trifiletti, High-level side-channel attack modeling and simulation for security-critical systems on chips, *IEEE Trans. Dependable Secur. Comput.* [online], vol. 5, no. 3 2008, pp. 164–176, 2008. DOI: 10.1109/TDSC.2007.70234. available from: https://doi.org/10.1109/TDSC.2007.70234.

[19] V. Lomné, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toublanc, "Modeling time domain magnetic emissions of ics," in *Integrated Circuit and System Design. Power and Timing Modeling, Optimization, and Simulation - 20th International Workshop, PATMOS 2010, Grenoble, France, September 7-10, 2010, Revised Selected Papers*, R. van Leuken and G. Sicard, Eds., ser. Lecture Notes in Computer Science, vol. 6448, Springer, 2010, pp. 238–249. DOI: 10.1007/978-3-642-17752-1_24. available from: https://doi.org/10.1007/978-3-642-17752-1%5C_24.

[20] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, Checking Robustness Against EM Side-Channel Attacks Prior to Manufacturing, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* [online] Jun. 2021, Jun. 2021. DOI: 10.1109/TCAD.2021.3092297. available from: https://hal-lirmm.ccsd.cnrs.fr/lirmm-03278781.

[21] A. Chatzigeorgiou, S. Nikolaidis, and I. Tsoukalas, A modeling technique for CMOS gates, *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* [online], vol. 18, no. 5 1999, pp. 557–575, 1999. DOI: 10.1109/43.759070. available from: https://doi.org/10.1109/43.759070.

[22] P. Maurine, M. Rezzoug, N. Azémard, and D. Auvergne, Transition time modeling in deep submicron CMOS, *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* [online], vol. 21, no. 11 2002, pp. 1352–1363, 2002. DOI: 10.1109/TCAD.2002.804088. available from: https://doi.org/10.1109/TCAD.2002.804088.

[23] A. Razafindraibe, "Analyse et amélioration de la logique double rail pour la conception de circuits sécurisés," Theses, Université Montpellier II - Sciences et Techniques du Languedoc, Nov. 2006. available from: https://tel.archives-ouvertes.fr/tel-00282762.

[24] R. W. Hamming, "Coding and information theory," 1980.

[25] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," in *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, Ç. K. Koç and C. Paar, Eds., ser. Lecture Notes in Computer Science, vol. 1717, Springer, 1999, pp. 144–157. DOI: 10.1007/3-540-48059-5_14. available from: https://doi.org/10.1007/3-540-48059-5%5C_14.

[26] R. L. Rivest, A. Shamir, and L. M. Adleman, A method for obtaining digital signatures and public-key cryptosystems (reprint), *Commun. ACM* [online], vol. 26, no. 1 1983, pp. 96–99, 1983. DOI: 10.1145/357980.358017. available from: https://doi.org/10.1145/357980.358017.

[27] D. Kalpić, N. Hlupić, and M. Lovrić, Student's t-tests, in *International Encyclopedia of Statistical Science*, M. Lovric, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011,

pp. 1559–1563, ISBN: 978-3-642-04898-2. DOI: 10.1007/978-3-642-04898-2_641. available from: https://doi.org/10.1007/978-3-642-04898-2_641.

[28] T. Ordas, M. Lisart, E. Sicard, P. Maurine, and L. Torres, "Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits," in *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, 18th International Workshop, PATMOS 2008, Lisbon, Portugal, September 10-12, 2008. Revised Selected Papers*, L. Svensson and J. Monteiro, Eds., ser. Lecture Notes in Computer Science, vol. 5349, Springer, 2008, pp. 229–236. DOI: 10.1007/978-3-540-95948-9_23. available from: https://doi.org/10.1007/978-3-540-95948-9%5C_23.

[29] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, Ç. K. Koç, D. Naccache, and C. Paar, Eds., ser. Lecture Notes in Computer Science, vol. 2162, Springer, 2001, pp. 251–261. DOI: 10.1007/3-540-44709-1_21. available from: https://doi.org/10.1007/3-540-44709-1%5C_21.

[30] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*, E. Oswald and P. Rohatgi, Eds., ser. Lecture Notes in Computer Science, vol. 5154, Springer, 2008, pp. 426–442. DOI: 10.1007/978-3-540-85053-3_27. available from: https://doi.org/10.1007/978-3-540-85053-3%5C_27.

[31] L. Wei, B. Luo, Y. Li, Y. Liu, and Q. Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators," in *Proceedings of the 34th Annual Computer Security Applications Conference, ACSAC 2018, San Juan, PR, USA, December 03-07, 2018*, ACM, 2018, pp. 393–406. DOI: 10.1145/3274694.3274696. available from: https://doi.org/10.1145/3274694.3274696.

[32] "Technical specification iec 62014-1," 2001.

[33] "Technical specification iec 62014-3," 2002.

[34] "Technical specification iec 62404," 2007.

[35] https://www.ansys.com/products/semiconductors/ansys-redhawk-sc.

[36] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, B. S. K. Jr., Ç. K. Koç, and C. Paar, Eds., ser. Lecture Notes in Computer Science, vol. 2523, Springer, 2002, pp. 29–45. DOI: 10.1007/3-540-36400-5_4. available from: https://doi.org/10.1007/3-540-36400-5%5C_4.

[37] D. Halliday, R. Resnick, and J. Walker, *Fundamentals of Physics*, ser. Halliday & Resnick Fundamentals of Physics. John Wiley & Sons Canada, Limited, 2010, ISBN: 9780470547939. available from: http://books.google.co.uk/books?id=49h2cgAACAAJ.

[38] I. of Electrical, E. Engineers, I. C. S. D. A. S. Subcommittee, I. S. Association, and I. S. Board, *IEEE Standard Verilog Hardware Description Language*, ser. IEEE (std). IEEE, 2001, ISBN: 9780738128269. available from: https://books.google.fr/books?id=oYXxGAAACAAJ.

[39] I. Diop, M. Carbone, S. Ordas, Y. Linge, P. Liardet, and P. Maurine, "Collision for estimating SCA measurement quality and related applications," in *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*, N. Homma and M. Medwed, Eds., ser. Lecture Notes in Computer Science, vol. 9514, Springer, 2015, pp. 143–157. DOI: 10.1007/978-3-319-31271-2_9. available from: https://doi.org/10.1007/978-3-319-31271-2%5C_9.

[40] D. Poggi, P. Maurine, T. Ordas, and A. Sarafianos, "Protecting secure ics against side-channel attacks by identifying and quantifying potential EM and leakage hotspots at simulation stage," in *Constructive Side-Channel Analysis and Secure Design - 12th International Workshop, COSADE 2021, Lugano, Switzerland, October 25-27, 2021, Proceedings*, S. Bhasin and F. D. Santis, Eds., ser. Lecture Notes in Computer Science, vol. 12910, Springer, 2021, pp. 129–147. DOI: 10.1007/978-3-030-89915-8_6. available from: https://doi.org/10.1007/978-3-030-89915-8%5C_6.

[41] F.-X. Standaert, T. G. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology - EUROCRYPT 2009*, A. Joux,

Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 443–461, ISBN: 978-3-642-01001-9.

[42] C. Herbst, E. Oswald, and S. Mangard, "An AES smart card implementation resistant to power analysis attacks," in *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*, J. Zhou, M. Yung, and F. Bao, Eds., ser. Lecture Notes in Computer Science, vol. 3989, 2006, pp. 239–252. DOI: 10.1007/11767480_16. available from: https://doi.org/10.1007/11767480%5C_16.

[43] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, Ç. K. Koç and C. Paar, Eds., ser. Lecture Notes in Computer Science, vol. 1717, Springer, 1999, pp. 292–302. DOI: 10.1007/3-540-48059-5_25. available from: https://doi.org/10.1007/3-540-48059-5%5C_25.

[44] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., Plenum Press, New York, 1982, pp. 199–203. DOI: 10.1007/978-1-4757-0602-4_18. available from: https://doi.org/10.1007/978-1-4757-0602-4%5C_18.

[45] L. Lin and W. P. Burleson, "Analysis and mitigation of process variation impacts on power-attack tolerance," in *Proceedings of the 46th Design Automation Conference, DAC 2009, San Francisco, CA, USA, July 26-31, 2009*, ACM, 2009, pp. 238–243. DOI: 10.1145/1629911.1629977. available from: https://doi.org/10.1145/1629911.1629977.

Publications and Webinars

- **Journal:**

    1. Checking Robustness Against EM Side-Channel Attacks Prior to Manufacturing [20]. Davide Poggi, Philippe Maurine, Thomas Ordas, Alexandre Sarafianos. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE.

- **Papers:**

    1. Protecting secure ICs against side-channel attacks by identifying and quantifying potential EM and leakage hotspots at simulation stage [40]. Davide Poggi, Philippe Maurine, Thomas Ordas, Alexandre Sarafianos, COSADE 2021.
    2. EM emission modeling for secure IC design. Davide Poggi, Philippe Maurine, Thomas Ordas, Alexandre Sarafianos, Jérémy Raoult. EMC Compo 2021.

- **Webinar:**

    1. How to perform electromagnetic side-channel analysis by simulation, Hardwear.io Webinars (https://www.youtube.com/watch?v=h8N5s-dfv6Q&t=1724s).

Summary

In the last decades, side-channel attacks (SCA) have demonstrated their dangerousness in retrieving sensitive data from ICs. Among these attacks, those exploiting EM radiations of ICs are particularly efficient. Indeed, adversaries need to find only one hotspot (position of the EM probe over the IC surface) where there is an exploitable leakage to compromise the security of the circuit. As a result, designing secure ICs robust against these attacks is incredibly difficult because designers must warrant there is no hotspot over the whole IC surface. This task is all the more difficult as there is no CAD tool allowing to verify the robustness of ICs against EM SCA at the design stage, i.e. prior to fabrication. In this thesis a simulation flow allowing to reproduce EM SCA by simulation is proposed. The Biot-Savart law is used to model the magnetic field radiated by entire ICs and an innovative methodology, called Noise-to-Add, is introduced. This latter allows to overcome the absence of noise in simulations and correctly interpret simulation correlation attacks results.

Résumé en français

Abstract

Parmi les différents canaux auxiliaires, le champ magnétique généré par les circuits intégrés est couramment utilisé et exploité par les adversaires pour récupérer des informations secrètes manipulées par des circuits intégrés. En raison de la résolution et de l'efficacité croissantes des équipements EM utilisés pour effectuer ces attaques, il devient de plus en plus difficile de concevoir des circuits sécurisés suffisamment robustes pour résister à ces attaques. Ce manuscrit apporte différentes contributions. Tout d'abord, il décrit un flot de simulation du champ magnétique rayonné par les circuits intégrés. Le flot introduit est basé sur un outil industriel de chute de tension: ANSYS RedHawk. Deuxièmement, il introduit une méthodologie pour localiser la cause première des fuites dans les circuits intégrés ainsi que les points de fuite EM, c'est-à-dire les positions au-dessus de la surface du circuit intégré où un adversaire peut placer une sonde EM pour tenter de retrouver des données sensibles manipulées par celui-ci. Cette dernière contribution repose sur la notion de bruit à ajouter qui est introduite dans cette thèse afin de pallier l'absence de bruit dans les simulations (bruit omniprésent en pratique) qui limite leur interprétabilité. Enfin, le manuscrit démontre le bien-fondé de la solution proposée en confrontant les résultats de simulation aux mesures expérimentales.

Introduction

Les attaques par canaux auxiliaires (SCA), ont démontré leur potentiel à révéler les secrets des circuits intégrés, que ce soit dans les microcontrôleurs ou même les cartes à puce [14]. Beaucoup de ces attaques sont maintenant publiques [6], [29], [13], [30] et la menace est toujours croissante avec l'émergence de techniques basées sur l'apprentissage en profondeur [31].

A la différence des attaques SCA et des propositions de contre-mesures, seulement quelques travaux ont proposé des techniques de vérification de la robustesse des circuits intégrés face aux SCA. Cela est particulièrement vrai pour les attaques exploitant le canal électromagnétique (EM). Cela constitue un manque surprenant mais sérieux si l'on considère le coût de fabrication des circuits intégrés. Etant donné que le coût d'une modification physique d'un composant (pour corriger un problème de sécurité) est souvent prohibitif, des correctifs logiciels sont souvent appliqués pour supprimer ou limiter les risques. Cependant, cette solution dégrade généralement les performances du système.

Parmi les premières publications proposant une solution pour évaluer la robustesse des circuits face aux SCA, on peut trouver [15]. Ici, les auteurs utilisent des simulations Hspice pour évaluer l'efficacité d'une contre-mesure par rapport aux attaques de type DPA (analyse de la consommation de courant). Un inconvénient majeur d'une telle approche est le coût en temps des simulations Hspice et donc sa limitation à des circuits ou des blocs logiques de petite taille. Pour pallier cette limitation, il a été proposé dans [17], [16] d'utiliser Synopsys Nanosim plutôt que Hspice. Malgré cette amélioration, une telle approche reste limitée aux circuits de faible complexité tels que les crypto-processeurs (AES, DES, etc...).

Avec cette approche limitée aux dispositifs de faible complexité, les auteurs de [18] ont suggéré l'utilisation de simulateurs SystemC pour évaluer la robustesse des codes embarqués tournant sur microcontrôleurs. Cependant, cela s'est fait au détriment de la précision de simulation. En effet, appliquer cette approche nécessite de remplacer les modèles de simulation Hspice par un modèle de puissance plus simple, à savoir le poids de Hamming des données traitées. De tels simulateurs doivent donc être considérés comme une technique de détection des failles de sécurité dans des

codes embarqués plutôt que dans des implémentations physiques.

Suite à ces travaux, les auteurs de [19] ont introduit une solution permettant de simuler le champ électromagnétique rayonné par les microcontrôleurs modernes. La technique proposée consiste à utiliser des outils d'analyse de chute de tension, utilisés lors de la vérification finale, pour dériver, avec une grande résolution temporelle et une grande précision, les courants circulant dans tous les segments de fils constituant le réseau d'alimentation (Vdd et Gnd). Avec de telles données, les auteurs ont démontré qu'en utilisant la loi de Biot-Savart on peut reconstituer des cartographies du champ magnétique rayonné par des circuits intégrés. Cependant, ils n'ont proposé aucun résultat d'attaque comme c'est le cas dans [7]. Les auteurs de cette publication ont suivi la même approche que [19] et des gpus pour accélérer les calculs de champs magnétiques. En conséquence, ils ont pu effectuer, par simulation, des attaques par corrélation (CPA). Ces dernières ont été introduites pour la première fois dans [13] et sont depuis devenues les SCA les plus courantes.

Dans ce contexte, cette thèse s'inscrit dans la continuité de [19] et [7]. Le premier apport est un flot de simulation capable de reproduire avec une grande précision le champ magnétique émis par un circuit intégré.

Le deuxième et principal apport est une technique rationnelle pour interpréter les résultats obtenus avec l'approche de simulation proposés dans ces travaux.

La troisième contribution est une méthode pour identifier les sources des fuites électromagnétiques dans les circuits intégrés. Ces sources sont différentes des fuites EM qui permettend de déterminer les coordonnées où les sondes EM doivent être placées pour effectuer des analyses side-channel.

Ce résumé est organisé comme suit. Dans une première partie, un rappel sur les cartes à puces et les attaques par corrélation exploitant les radiations EM est décrit. Puis, la méthode pour obtenir des cartographies montrant les zones de fuites EM d'un circuit intégré est présentée.

Dans une deuxième partie, quelques informations de base sur les champs magnétiques sont données. Puis, le flot de simulation qui a été développé, basé sur l'outil ANSYS RedHawk et sur la loi de Biot-Savart, est présenté. De plus, une solution pour interpréter les résultats de simulation obtenus avec le flot de simulation sera introduite, ainsi qu'une méthode pour localiser les fuites EM d'un circuit intégré.

Dans la troisième partie, le flot de simulation est validé en proposant quelques exemples pra-

tiques.

Dans la quatrième partie, le flot est utilisé pour localiser les origines des fuites EM et pour évaluer l'efficacité des contre-mesures avant la fabrication d'un circuit intégré.

Attaques par canaux auxiliaires expérimentales

Une carte à puce est un dispositif embarquant un circuit intégré comportant en général un microprocesseur et une mémoire. Les cartes à puce sont donc capables de stocker et de manipuler des données mais aussi d'interagir avec le monde extérieur en recevant et en échangeant des informations.

Une carte à puce ressemble à un appareil inattaquable, conçu pour résister à tout type d'attaque. Malheureusement, la réalité est différente. Des nouvelles attaques sont continuellement développées et celles existantes sont améliorées. Des entreprises telles que STMicroelectronics investissent d'énormes ressources dans le développement de contre-mesures de plus en plus fiables et robustes. Néanmoins, il est toujours possible de trouver un moyen de briser la sécurité d'une carte à puce. Pour cela, il faut disposer de la carte, connaître la structure et le fonctionnement des crypto-processeurs embarqués, et disposer du matériel nécessaire pour mener des attaques.

Parmi les attaques les plus dangereux on trouve les attaques par canaux auxiliaires. L'objectif de celles-ci est de récupérer différents signaux compromettants émis par le circuit, dont les plus fréquents sont la consommation de puissance ou les radiations EM, pour révéler les secrets cachés à l'intérieur du circuit. En particulier, ces attaques cherchent un lien statistique entre ces signaux et les données manipulées par le circuit pendant l'exécution d'une opération cryptographique. En effet, les crypto-processeurs intégrés dans les cartes à puce exécutent des crypto-algorithmes, dont l'un des plus connus est l'Advanced Encryption Standard (AES), qui est un algorithme à clé symmétrique.

Il est possible de rompre la sécurité d'un produit sécurisé en observant les signaux émis par le circuit. Ces signaux sont appelés fuites. Il est donc possible de modéliser ces fuites avec des modèles, comme par exemple le modèle du poids de Hamming. Une fois les traces de mesure collectées et les modèles construits, il est possible de calculer le lien statistiques entre les deux. Une des attaques le plus utilisé est l'attaque par corrélation (CPA) basé sur le coefficient de Bravais-

Pearson.

Pour réaliser une attaque EM, une sonde électromagnétique est placée sur la surface du circuit intégré. Le but est de collecter un grand nombre de traces de radiation EM émises par le circuit lors de la réalisation d'opérations cryptographiques. Lors de la caractérisation d'un produit sécurisé, l'objectif est de valider sa sécurité face aux SCA. Pour ce faire, la sonde est déplacée sur la surface du circuit. Un ensemble de courbes EM est collecté à chaque position et la corrélation entre ces rayonnements et les données secrètes manipulées par le circuit est calculée. Enfin, il est possible de dessiner une carte montrant les zones de fuite d'information du circuit. La figure 1 montre une cartographie obtenue en attaquant une puce de test, dénotée *TCA*, fabriquée par STMicroelectronics.

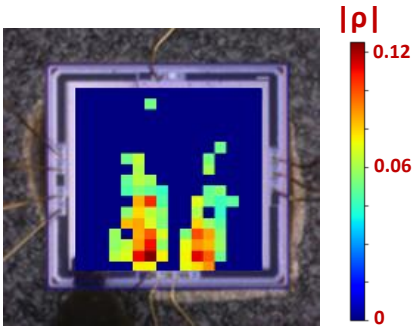

Figure 1: Zone de fuite de la puce de test *TCA* après une attaque EM par correlation.

La reproduction de cette méthodologie en simulation est l'objectif principal de la thèse. Un flot de simulation capable d'effectuer cette tâche est décrit ci-dessous.

Attaques par canaux auxiliaires en simulation

Les leçons de l'expérience pratique

En effectuant réellement des analyses et des balayages électromagnétiques en champ proche (ainsi qu'en lisant des publications connexes), il a été déterminé que les adversaires utilisent généralement des sondes EM de diamètre compris entre $50\mu m$ [28] et $500\mu m$. La sonde EM est alors placée à une faible distance (qui varie entre $10\mu m$ et $200\mu m$) de la surface du circuit intégré et parallèlement

à celle-ci afin de collecter des traces EM avec un rapport signal sur bruit (SNR) élevé, ce dernier défini comme le rapport entre la variance du signal et celle du bruit.

En parallèle, l'observation de différents aménagements conjointement avec les simulations électriques montrent que les courants les plus forts circulent dans les barreaux supérieurs du réseau d'alimentation; les barreaux les plus proches de la sonde EM. Ces barreaux ont une largeur comprise entre $1\mu m$ et $5\mu m$. Comparant l'ordre de grandeur des dimensions des barreaux et la distance qui les sépare avec le diamètre typique des sondes EM, on peut donc les considérer comme des barreaux de longueur finie avec largeur négligeable et on peut donc utiliser la loi de Biot-Savart pour calculer le champ magnétique rayonné par les circuits intégrés. Dans certains cas, on peut trouver des barreaux métalliques plus gros (largeur supérieure à $10\mu m$). Dans ce cas, il est préférable de scinder ces gros barreaux en un nombre n de petits barreaux parcourus chacun par un courant n fois plus faible.

Enfin, l'hypothèse faite dans cette thèse est qu'il suffit de considérer les courants circulant dans les niveaux métalliques supérieurs d'un circuit intégré pour modéliser avec précision le champ magnétique d'un circuit entier. Cette hypothèse sera vérifiée à l'aide d'analyses expérimintales.

Champ magnétique rayonné par un fil de longueur finie

Le réseau d'alimentation d'un circuit peut être modélisé comme un ensemble de fils de longueur finie, chacun parcouru par un courant. La première étape pour modéliser le champ magnétique émis par un circuit intégré est de définir comme modèle de fil de longueur finie. Pour ce faire la loi de Biot-Savart est utilisée pour obtenir la composante verticale du champ magnétique (composante z) qui est capturée par une sonde EM quand cette dernière est placée parallèle à la surface du circuit. L'expression du champ vertical, B_z est donnée ci-dessous:

$$|\overrightarrow{B_{z,v}}(x,y,z,t)| = \frac{\mu_0 \cdot I(t)}{4\pi} \cdot \frac{x^2}{x^2+z^2} \left[\frac{1}{\sqrt{(x-x_A)^2+(y-y_A)^2}} + \frac{1}{\sqrt{(x-x_B)^2+(y-y_B)^2}} \right]$$

Cette équation permet d'obtenir la distribution spatiale du champ magnétique généré par un fil sur une surface rectangulaire placé au-dessus. En appliquant cette distribution à chaque barreau du circuit, il est donc possible d'obtenir le champ magnétique émis par le circuit entier.

Les sondes EM mesurent le champ magnétique rayonné par les circuits intégrés mais délivrent une tension proportionnelle à la force électromotrice (ε) induite par des changements du flux magnétique (ϕ_z) traversant la bobine qui les constitue. C'est ainsi obligatoire de calculer ces deux grandeurs. Les équations suivantes donnent l'expression de ϕ_z et ε.

$$\phi_z(l,c,t) = \sum_{\substack{i\in[l-d,l+d] \\ j\in[c-d,c+d]}} B_Z(i,j,t)$$

$$\varepsilon(l,c,t) = -\frac{\partial \phi_z(l,c,t)}{\partial t}$$

Collecter les traces de courant avec RedHawk

Les équations précédentes indiquent clairement le besoin de connaître les coordonnées de tous les segments de fil et le courant les traversant afin de pouvoir calculer le champ magnétique vertical rayonné par un circuit intégré. L'outil utilisé a été Redhawk, fourni par la société ANSYS. RedHawk permet de reproduire des cartographies de chute de tension statique et dynamique. Les cartographies obtenues sont dépendantes des données car des fichiers VCD (Value Change Dump [38]) doivent être fournis à RedHawk. Il offre également la possibilité d'observer, à l'aide de sondes de courant virtuelles, le courant transitoire traversant n'importe quel point du réseau d'alimentation.

Pour extraire les courants circulant dans le circuit, RedHawk permet de placer les sondes virtuelles sur le réseau d'alimentation. De cette façon, il est possible d'obtenir une matrice contenant tous les barreaux (un barreau est défini comme la distance entre deux vias consecutives) du circuit et le courant circulant dans ces derniers. Une fois que tous les barreux ont été construits et les traces de courant ont été récupérées, il est possible d'appliquer la distribution du champ magnétique calculée précédemment et modéliser le champ magnétique de chaque barreau et, donc, du circuit entier.

Identifier des fuites EM en simulation

Afin de valider le flot de simulation décrit dans la section précédente, il a été appliqué sur le circuit *TCA*, qui est une puce de test conçue en technologie 40*nm* et embarquant, entre autre, un

crypto-processeur AES non protégé. L'intention était de comparer les cartographies de corrélation expérimentales et simulées obtenues en exécutant des analyses par corrélation avec la sonde EM placée à de nombreuses coordonnées au-dessus de la surface de TCA. Les résultats obtenus ont été décevants. En effet, les cartographies expérimentales ont révélé des zones réduites (fuites EM) où la sonde EM peut être placée pour récupérer la clé secrète tandis que les cartographies simulées ont montré que la CPA retrouve la clé presque partout sur la quasi totalité de la surface de TCA.

Pour comprendre le problème, une simulation spécifique a été effectuée. L'objecif était de calculer le champ magnétique vertical à $50\mu m$ d'un circuit intégré n'embarquant qu'un fil de $20\mu m$ de long placé au centre.

Pour cette simulation, le courant traversant le fil a été construit pour porter une fuite importante par rapport au poids de Hamming du secret. L'expérience a montré que la corrélation entre le poids de Hamming et le courant est forte autour du fil et est bien sûr nulle partout ailleurs. Par contre, la corrélation entre le champ magnétique et le poinds de Hamming était forte sur toute la surface (sauf le long de la verticale ligne supportant le fil) quelle que soit la répartition du amplitude du champ magnétique. Ceci est une illustration directe de la inefficacité des attaques par corrélation simulées pour identifier des fuites EM.

La principale raison expliquant l'inefficacité des simulations en champ proche est l'absence de bruit de mesure dans les simulations qui peut être supposé constant sur la surface du circuit intégré en pratique. Ce bruit, qui est absent dans la simulation, réduit ou efface complètement les corrélations où le signal EM rayonné par le circuit a une faible amplitude.

La solution proposée dans ce manuscrit est de calculer le niveau de bruit qu'il faut ajouter aux traces simulées pour rendre la corrélation insignifiante. L'expression est donnée ci-dessous:

$$V(\eta) = V(S) \cdot \left[\frac{\rho^2}{\rho_{crit}^2} - 1 \right]$$

Cette expression dépend de la variable ρ_{crit} qui indique la valeur de corrélation au-delà de laquelle la corrélation doit être considérée comme significative.

De l'équation précédente et dans le cadre de la continuité de [39], il est possible de déterminer une information importante qui est le signal sur bruit minimal, SNR_{min}, qu'il faut observer en simulation pour pouvoir récupérer, à une coordonnée donnée du circuit, une fuite EM. Le calcul de

SNR_{min} est simple à partir de l'équation du bruit à ajouter $V(\eta)$.

$$SNR_{min} = \frac{V(S)}{V(\eta)} = \frac{\rho_{crit}^2}{\rho^2 - \rho_{crit}^2}$$

Le bruit à ajouter ne donne qu'une information sur la signification d'une corrélation et quel niveau de bruit est suffisant pour la rendre insignifiante. Même si c'est une information intéressante, cela ne suffit pas pour décider s'il existe une fuite EM exploitable à une coordonnée donnée au-dessus d'un circuit.

En effet, la CPA classe toutes les hypothèses clés. Ce classement est fait selon la valeur absolue de la corrélation entre le signal et le poids de Hamming de la valeur intermédiaire traitée par le circuit. S'il y a une fuite, la clé correcte est classée en première position (avec la plus grande valeur de corrélation absolue). S'il n'y a pas de fuite son rang est compris entre 2 et 256 dans le cas d'une valeur intermédiaire de 8 bits. Ainsi, pour affirmer qu'il y a une fuite exploitable la valeur de corrélation absolue obtenue pour la bonne estimation de clé doit être supérieure à celle obtenue pour toutes les hypothèses erronées.

Pour ces raisons, la méthode définitive pour identifier des fuites EM en simulation consiste à calculer le niveau de bruit à ajouter seulement si la corrélation absolue obtenue pour la bonne estimation de clé est supérieure à celle obtenue pour toutes les hypothèses erronées:

$$\sqrt{V^*(\eta)} = \begin{cases} \sqrt{V^{k^*}(\eta)} & \text{if } \ |\rho^{k^*}| \geq |\rho^k|, \quad \forall k \in K \\ 0 & \text{otherwise} \end{cases}$$

Validation du flot de simulation

L'efficacité du flot de simulation est validée en proposant quelques exemples pratiques réalisés sur la puce de test TCA. L'objectif est de comparer les cartographies d'attaques de corrélation obtenues expérimentalement avec celles simulées obtenues en appliquant le concept de bruit à ajouter.

Les cartographies expérimentales montrées dans les paragraphes suivants ont été obtenues en collectant des traces EM à chaque coordonnée (x,y) de TCA et en appliquant le critère suivant:

$$|\rho^*| = \begin{cases} |\rho^{k^*}| \quad \text{if} \quad |\rho^{k^*}| \geq |\rho^k|, \quad \forall k \in K \\ 0 \quad \text{otherwise} \end{cases} \tag{32}$$

Les cartographies simulées ont été obtenues en appliquant la formule du bruit à ajouter vue dans la section précédente.

La première expérience implique des variations dans la hauteur et le diamètre de la sonde utilisée pour effectuer une attaque EM SCA.

Les figures suivantes montrent les comparaisons entre les cartographies expérimentales et simulées.

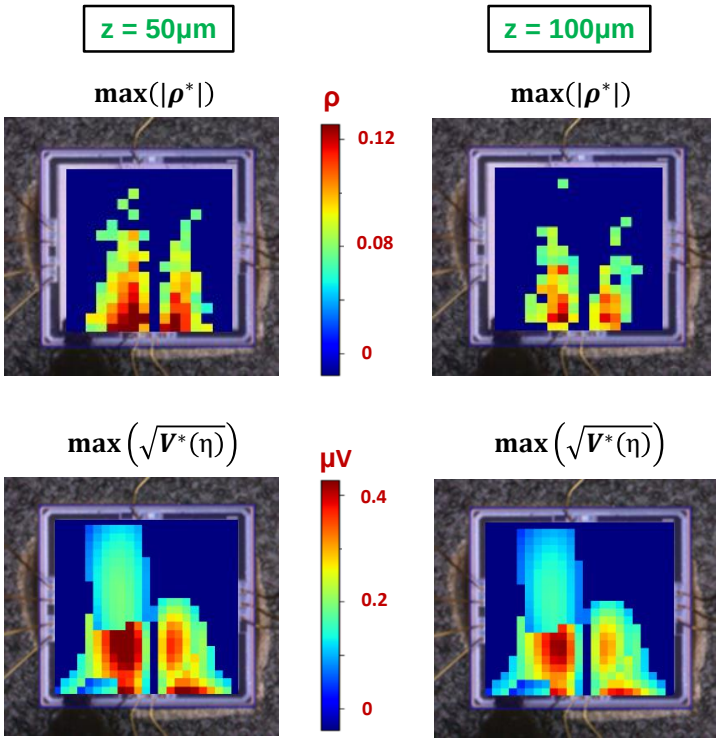

Figure 2: Cartographies expérimentales (ρ) (première ligne) et simulées $\sqrt{V^*(\eta)}$ (deuxième ligne) pour deux différentes hauteurs.

Comme montré, les cartographies simulées et expérimentales sont corrélées, et le flot de simulation peut reproduire correctement les changements de hauteur et de diamètre de la sonde.

Deux autres expériences ont été effectuées. La première avec une sonde verticale, qui capture les champs magnétiques B_x et B_y. La deuxième permet de comparer les cartographies obtenue avec TCA en face arrière et face avant.

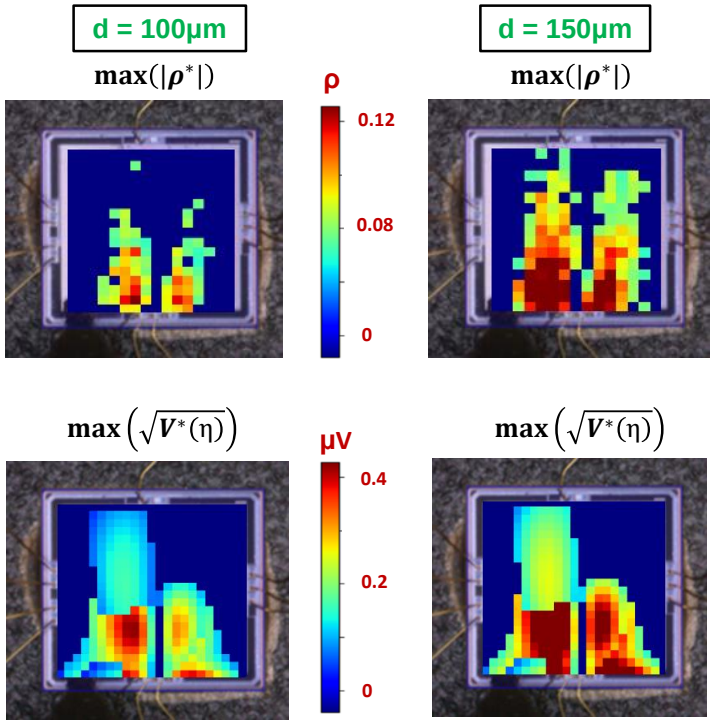

Figure 3: Cartographies expérimentales (ρ) (première ligne) et simulées $\sqrt{V^*(\eta)}$ (deuxième ligne) pour deux différentes diamètres.

Ces deux expériences ont permis d'obtenir deux résultats importants. Le premier est une confirmation de l'efficacité du flot de simulation, qui est capable de reproduire le changement d'orientation de la sonde (sonde horizontale et verticale) et la configuration du produit (face arrière et avant).

Le deuxième résultat est la confirmation que modèliser seulement le courant circulant dans les couches supérieures du circuit est suffisant pour reproduire le champ d'un circuit intégré. En effet, quand une sonde verticale est placée sur le circuit parallèlement à la direction des barreaux supérieurs du circuit, on observe de fortes fuites. D'autre part, quand la sonde est perpendiculaire, aucune fuite n'est observée.

En outre, les cartographies obtenues en face arrière et avant présentent des zones de fuite et une intensité de ces dernières très similaire.

Ces deux expériences montrent que les barreaux supérieurs du réseau d'alimentation sont effectivement les contributeurs principaux au champ magnétique.

Application du flot de simulation pendant la phase de conception d'un produit sécurisé

A ce stade du manuscrit, des expériences concernant la géométrie, l'orientation et la taille de la sonde ont démontré la solidité du flot de simulation. Maintenant, on peut le considérer valide et donner deux exemples de son utilité.

Le premier exemple traite de la localisation des origines des fuites EM avant la fabrication d'un produit. Cet exemple fournit également une validation de la procédure de localisation des fuites par simulation.

Le deuxième exemple concerne l'évaluation de l'efficacité des contremesures pendant la phase de conception d'un circuit.

Orgines de fuites avant fabrication

La méthode permettant d'identifier les orgines des fuites en simulation (et donc pendant la phase de conception) consiste à appliquer le concept de bruit à ajouter aux courants circulant dans les couches du réseau d'alimentation acheminés en métal1 (niveau de métal le plus bas). L'évolution temporelle des fuites liées au champ magnétique sur la puce de test *TCA* est présentée sur la figure ci-dessous.

Cette figure montre l'apparition progressive d'une fuite entre les échantillons temporels n°1 et n°7 (début de cycle d'horloge) et son étalement le long des réseaux d'alimentation en raison de la propagation des courants. Il faut noter que ce résultat a été obtenu par la mise en place de 120000 sondes de courant avec RedHawk le long du réseau d'alimentation sur le métal1.

Calculer le bruit à ajouter échantillon de temps par échantillon de temps est important. En effet, il permet de localiser finement la cause première de fuite et surmonter l'effet de flou dû à la propagation des courants le long du réseau d'alimentation.

Pour mieux mettre en évidence l'origine des fuites, un zoom sur l'AES est visible sur la figure. Une telle série de cartographies offrent aux concepteurs la possibilité d'analyser et de corriger rapidement les fuites, avec des simulations électriques ou de niveau RTL, après avoir identifié des portes CMOS dans les sections suspectes de rangées de cellules standard. On peut aussi observer

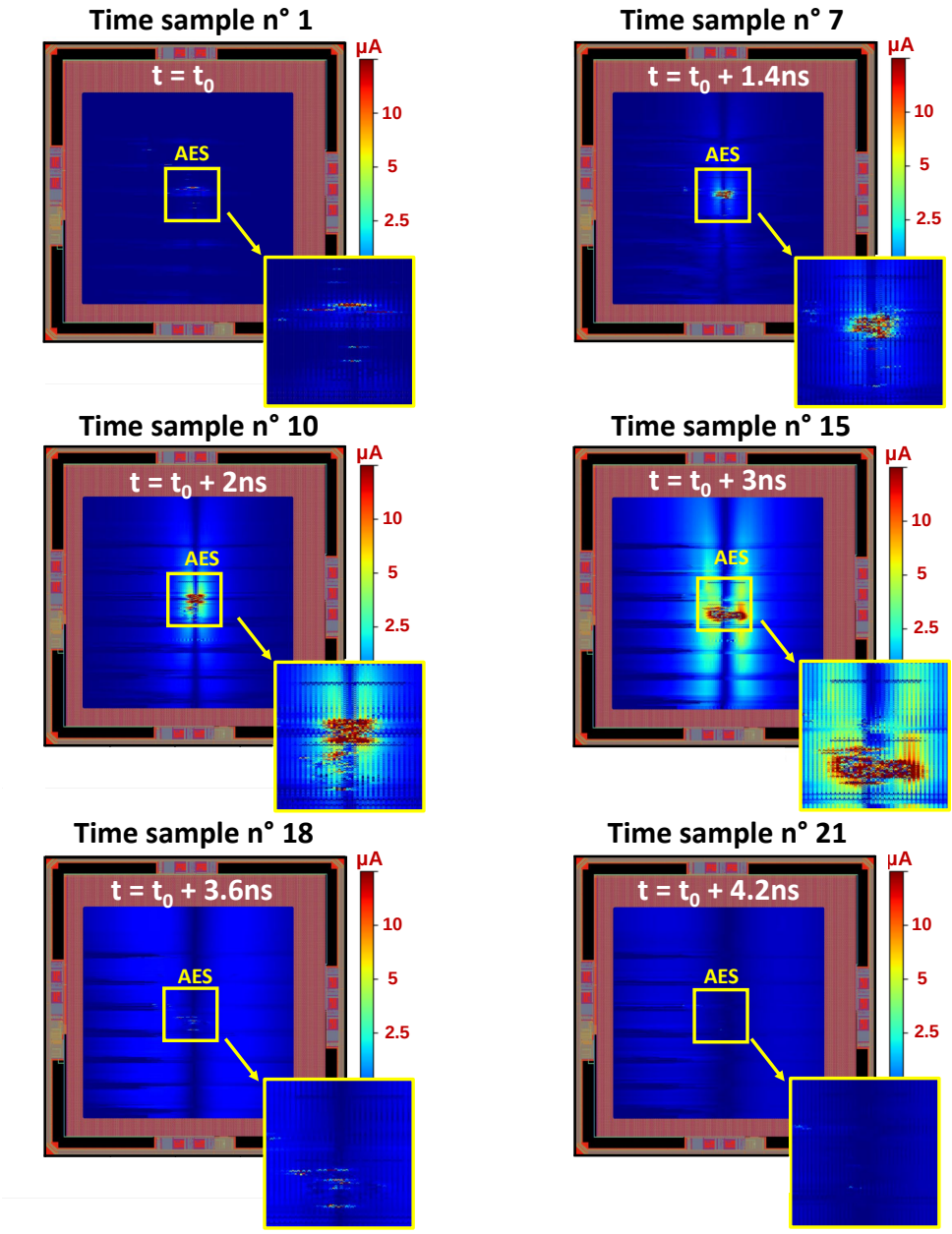

Figure 4: Évolution temporelle des fuites associées aux échantillons temporels n°1, 7, 10, 15, 18 et 21 révélant des sections de rangées de cellules standard qui fuient.

en bleu clair des zones en dehors de la localisation de l'AES qui sont des zones où les cellules de l'AES tire une partie du courant qu'il consomme. Ceci est une preuve directe de la propagation du courant qui propage la fuite sur une surface plus grande que celle dont elle est à l'origine.

Evaluation de l'efficacité des contremesures pendant la phase de conception d'un circuit

Le flot de simulation et la méthode proposée pour localiser les fuites EM et leurs origines peuvent bien sûr être utilisés pour valider contre-mesures logicielles ou matérielles. Ils peuvent aussi être appliquée pour choisir rationnellement entre des alternatives de conception.

Pour illustrer le potentiel de ces solutions, le flot est appliqué à deux puces de test. En effet, on s'attendait à ce que les zones de fuite EM de la puce de test *TCB* soient plus petites que celles de *TCA* à cause de la compensation partielle (le courant circule en sens opposé dans les barreaux verticales de puissance et terre) du champ magnétique généré par les deux barreaux (Vdd et Gnd).

La figure suivante compare les cartographies de corrélation et bruit à ajouter obtenues pour *TCA* et *TCB*.

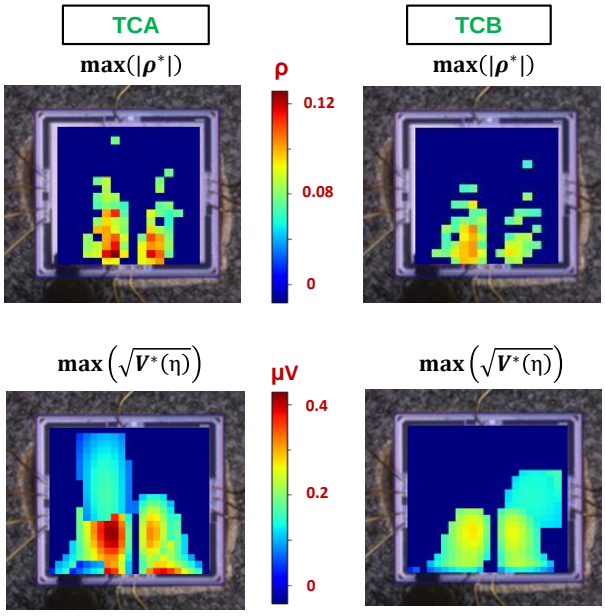

Figure 5: Cartographies expérimentales (en haut) et simulées (en bas) pour *TCA* et *TCB*.

Le premier constat que l'on peut faire est que les cartographies expérimentales et simulées sont

corrélées.

Deuxièmement, on peut observer que la contre-mesure semble être efficace. En fait, *TCB* présente des fuites plus faibles par rapport à *TCA*. C'est une confirmation importante que le flot est efficace pour tester une contre-mesure par simulation. Dans cet exemple, le silicium était disponible et il était possible de faire des comparaisons, mais bien sûr cette approche peut (et devrait) être utilisé même avec de nouveaux produits qui ne sont pas encore disponibles sur silicium et qui sont encore en phase de conception.

Conclusions

L'objectif principal de cette thèse était de développer un outil permettant d'effectuer la simulation des émissions EM afin de pouvoir réaliser des attaques SCA et ainsi de tester la robustesse des circuits intégrés avant la fabrication. L'importance d'identifier les zones de fuite lors de la phase de conception d'un produit sécurisé été illustrée. Deux types de fuites ont été définies: les fuites EM et leur origines.

Dans un premier temps, il a été mis en évidence l'absence d'un tel outil de simulation dans la communauté scientifique et pourquoi ce manque constitue un problème sérieux pour la sécurité des circuits intégrés. En effet, seulement quelques travaux dans la littérature traitent de l'identification des fuites EM à l'aide de simulation, et il n'y a pas de travaux proposant des comparaisons entre cartographies expérimentales et simulées. Cette thèse visait précisément à combler cette lacune et à proposer une solution pour mener des attaques par simulation et comparer les résultats avec des résultats expérimentaux.

Les recherches présentées ont conduit à deux contributions principales. La première est un flot de simulation permettant d'émuler tous les phénomènes électromagnétiques en pratique lorsque des analyses EM SCA sont effectués. Le flot est principalement basé sur l'utilisation de l'outil RedHawk de la société ANSYS. Une hypothèse a été faite (vérifiée ensuite) selon laquelle les couches métalliques supérieures sont les principaux contributeurs au champ magnétique capté par des sondes EM. Les courants circulant dans ces couches sont de plusieurs ordres de grandeur plus intenses que ceux circulant dans les couches métalliques inférieures et, de plus, les couches supérieures sont les plus proches de l'EM sondes lorsque les attaques EM sont effectuées en face avant.

Le réseau d'alimentation d'un circuit a été modélisé comme un ensemble de fils de longueur finie et la loi de Biot-Savart a été appliquée à chacun de ces fils pour reproduire le champ magnétique rayonné par des circuits intégrés. Le flux magnétique capté par une sonde EM ainsi que la force électromotrice qui y est induite par les variations du flux ont été modélisées.

La première validation de ce flot de simulation s'est révélée infructueuse du fait de l'absence de bruit en simulation qui rend inexploitable les cartographies de corrélation.

Une solution innovante, le concept de bruit à ajouter, et représentant le deuxième et principal apport de cette thèse, a ainsi été présenté. Il consiste à calculer le niveau de bruit qu'il faut ajouter aux traces simulées afin de masquer une fuite potentielle.

Le concept de bruit à ajouter a été validée sur un simple barreau de longueur finie. Un lien important avec la notion de signal sur bruit a été fait.

Ensuite, le flot de simulation magnétique et le concept de bruit à ajouter ont été validés sur une puce de test fabriquée par STMicroelectronics, conçue en technologie CMOS 40*nm* et embarquant un crypto-processeur AES. Le flot s'est avéré efficace pour identifier les fuites EM par simulation. De plus, le flot reproduit les variations des caractéristiques et de la localisation de la sonde (hauteur et diamètre) utilisée pour effectuer des attaques EM.

Des expériences avec des sondes verticales (capture du champ magnétique horizontal) ainsi que des comparaisons entre des analyses effectuées avec le circuit en face avant et face arrière ont été proposées afin de démontrer que l'extraction des courants circulant dans les couches métalliques supérieures est suffisante pour émuler avec précision le champ magnétique capturé par les sondes EM.

Après toutes ces validations, l'utilité du flot développé au stade de la conception a été présentée dans la dernière section. En particulier, il a été demontré que le flot peut être utilisé pour identifier les sources des fuites EM pendant la phase de conception d'un produit et pour évaluer l'efficacité des contre-mesures avant la fabrication.