

**THESIS TO OBTAIN THE DEGREE OF DOCTOR
OF THE UNIVERSITY OF MONTPELLIER**

In SyAM - Automatic and Microelectronic Systems

Doctoral school: Information, Structures, and Systems sciences

Research Unit: LIRMM

Body biasing fault injection: modeling

Presented by Geoffrey Chancel

COMPILATION DATE: [2023-10-11 17:01:33+02:00](#)

Under the supervision of TO BE COMPLETED

Thesis Committee:

Philippe Maurine , Associate Professor ?? , University of Montpellier

Thesis Director

Jean-Marc Gallière, Associate Professor ?? , University of Montpellier

Thesis Supervisor



**UNIVERSITÉ DE
MONTPELLIER**

Abstract 2023-10-11 17:01:33+02:00

Résumé de la thèse 2023-10-11 17:01:33+02:00

Acknowledgements 2023-10-11 17:01:33+02:00

The authors acknowledge the support of the French Agence Nationale de la Recherche (ANR), under grant ANR-19-CE39-0008 (project ARCHI-SEC). They also acknowledge the French Ministère des Armées – Agence de l’innovation de défense (AID) under grant ID-UM-2019 65 0036.

Contents

List of Figures	ix
List of Tables	xi
List of algorithms JAAJ	xiii
List of Acronyms	xv
Publications	xvi
General introduction	xvii
1 Introduction and state of the art <small>2023-10-11 17:01:21+02:00</small>	1
1.1 Summary <small>2023-10-11 17:01:21+02:00</small>	2
1.2 Introduction <small>2023-10-11 17:01:21+02:00</small>	2
1.3 Side-channel attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.3.1 Timing attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.3.2 Power analysis and electromagnetic analysis attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.4 Fault-injection attacks <small>2023-10-11 17:01:21+02:00</small>	7
1.4.1 Giraud's differential fault attack <small>2023-10-11 17:01:21+02:00</small>	8
1.5 Fault-injection techniques <small>2023-10-11 17:01:21+02:00</small>	8
1.5.1 Glitch fault injection <small>2023-10-11 17:01:21+02:00</small>	8
1.5.2 Laser fault injection <small>2023-10-11 17:01:21+02:00</small>	8
1.5.3 Electromagnetic fault injection <small>2023-10-11 17:01:21+02:00</small>	9
1.5.4 Body biasing injection <small>2023-10-11 17:01:21+02:00</small>	9
2 Body Biasing Injection platforms and good practices <small>2023-10-11 17:01:21+02:00</small>	11
2.1 Summary <small>NEW 2023-10-11 17:01:21+02:00</small>	13
2.2 Introduction <small>UPDATED 2023-10-11 17:01:21+02:00</small>	13
2.3 BBI platforms in the state-of-the-art <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	14
2.3.1 Initial BBI platforms <small>UPDATED 2023-10-11 17:01:21+02:00</small>	14
2.3.2 C. O'Flynn BBI platform <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	14
2.3.3 Commercial platforms <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	15
2.3.4 An overview about BBI platforms <small>NEW 2023-10-11 17:01:21+02:00</small>	19
2.4 Our BBI platform <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	20
2.4.1 The probe <small>UPDATED 2023-10-11 17:01:21+02:00</small>	20

2.4.2	The generator <small>UPDATED 2023-10-11 17:01:21+02:00</small>	21
2.5	BBI in practice <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.1	Typical BBI platform model <small>UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.2	Platforms evaluation criteria <small>UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.3	Raw results <small>UPDATED 2023-10-11 17:01:21+02:00</small>	23
2.5.4	Analysis conclusions <small>UPDATED 2023-10-11 17:01:21+02:00</small>	23
2.6	Enhanced BBI platform model and simulation <small>2023-10-11 17:01:21+02:00</small>	25
2.6.1	Matching the generator output impedance <small>UPDATED 2023-10-11 17:01:21+02:00</small>	25
2.6.2	Improving the grounding installation <small>UPDATED 2023-10-11 17:01:21+02:00</small>	26
2.6.3	Simulation results <small>UPDATED 2023-10-11 17:01:21+02:00</small>	26
2.6.4	Simulation conclusions <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	27
2.7	Actual enhanced BBI platform <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	27
2.7.1	Generator impedance matching in practice <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.7.2	Grounding installation bypass in practice <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.7.3	Practical analysis <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.8	Enhanced BBI platform in a fault attack context <small>UPDATED 2023-10-11 17:01:21+02:00</small>	30
2.8.1	Giraud's DFA detailed description <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	30
2.8.2	Integrated circuits target characteristics <small>UPDATED 2023-10-11 17:01:21+02:00</small>	32
2.8.3	Preliminary attack experiments <small>UPDATED 2023-10-11 17:01:21+02:00</small>	33
2.8.4	Attack results and analysis <small>NEW 2023-10-11 17:01:21+02:00</small>	34
2.8.5	Giraud's DFA conclusion <small>NEW 2023-10-11 17:01:21+02:00</small>	35
2.9	Conclusion <small>UPDATED 2023-10-11 17:01:21+02:00</small>	35
3	Integrated circuits modeling <small>IN PROGRESS 2023-10-11 17:01:21+02:00</small>	37
3.1	Summary <small>UPDATED 2023-10-11 17:01:21+02:00</small>	38
3.2	Introduction <small>UPDATED 2023-10-11 17:01:21+02:00</small>	38
3.3	Integrated circuits structure <small>NEW 2023-10-11 17:01:21+02:00</small>	39
3.3.1	Power supply rails <small>NEW 2023-10-11 17:01:21+02:00</small>	39
3.3.2	Standard-Cell rows <small>NEW 2023-10-11 17:01:21+02:00</small>	40
3.3.3	Various substrate types <small>NEW 2023-10-11 17:01:21+02:00</small>	41
3.4	Standard-Cell Segment (SCS) and their models <small>NEW 2023-10-11 17:01:21+02:00</small>	42
3.4.1	The case of Dual-Well substrates <small>NEW 2023-10-11 17:01:21+02:00</small>	43
3.4.2	The case of Triple-Well substrates <small>NEW 2023-10-11 17:01:21+02:00</small>	45
3.4.3	Writing the elementary models <small>NEW 2023-10-11 17:01:21+02:00</small>	45
3.5	Integrated circuit modeling: interconnecting Standard-Cell Segments together <small>NEW 2023-10-11 17:01:21+02:00</small>	46
3.6	Preliminary models validation <small>NEW 2023-10-11 17:01:21+02:00</small>	48
4	Substrate thinning analysis <small>2023-10-11 17:01:21+02:00</small>	51
4.1	Summary <small>2023-10-11 17:01:21+02:00</small>	52
4.2	Introduction <small>2023-10-11 17:01:21+02:00</small>	52
4.3	Geometric and electrical modeling <small>2023-10-11 17:01:21+02:00</small>	53

4.3.1	Geometric modeling 2023-10-11 17:01:21+02:00	53
4.3.2	Electrical approach 2023-10-11 17:01:21+02:00	56
4.4	Models validation 2023-10-11 17:01:21+02:00	58
4.4.1	IC substrate thinning quick look 2023-10-11 17:01:21+02:00	58
4.4.2	Experiments with thinned circuits 2023-10-11 17:01:21+02:00	59
4.5	Conclusion 2023-10-11 17:01:21+02:00	60
5	Fault model 2023-10-11 17:01:21+02:00	63
5.1	Summary 2023-10-11 17:01:21+02:00	64
5.2	Introduction 2023-10-11 17:01:21+02:00	64
5.3	Charge extortion 2023-10-11 17:01:21+02:00	64
5.3.1	Sequential logic operation and simple fault model 2023-10-11 17:01:21+02:00	65
5.4	Silicon substrate charges propagation 2023-10-11 17:01:21+02:00	65
5.5	Logic gates simulation under BBI 2023-10-11 17:01:21+02:00	65
6	Conclusion	67
Bibliography		69

List of Figures

2.1	Schematic extracted from C. O'Flynn [1]: BBI injection device proposed by C. O'Flynn [1], using a transformer to produce high voltage pulses from a low voltage power supply.	15
2.2	BBI probe proposed by the company Langer EMV-Technik GmbH.	16
2.3	BBI probe proposed by the company Riscure BV.	17
2.4	Pulse generator for EMFI and BBI proposed by NewAE Technology Inc.	18
2.5	PicoEMP: a low-cost pulse generator from NewAE Technology Inc. It provides much less instantaneous power than a typical generator, has a long recovery time (from 1 to 4 seconds), has a lower maximum amplitude (250 V), is not pre-calibrated, and has no controllable pulse width. However, it costs 94 % less than a typical generator, giving it a considerable advantage when building low-cost BBI platforms.	18
2.6	Custom BBI probes photographs	20
2.7	Front side of the Avtech Electrosystems Ltd. AVRK-4-B High Voltage Pulser, used during all my thesis experiments.	21
2.8	BBI platform electrical model developed for my thesis to quickly evaluate various platform's parameters, alongside the model simulation results.	22
2.9	Platform simulation results with different IC load values.	24
2.10	BBI platform enhanced electrical model developed for my thesis to quickly evaluate various platform parameters, alongside the model simulation results.	25
2.11	Simulation results of the enhanced platform with a 250Ω IC load (2.11a) and a $2 k\Omega$ IC load (2.11b). The current increase in 2.11a is natural due to the load impedance reduction. However, the effective pulse amplitude relative to the set point has only a -7 % error, which is a drastic improvement over the previous -30 %. The set point is met. Then, in 2.11b, the current decrease is logical given the higher impedance value. The effective pulse amplitude relative to the set point has only a 7 % error, which is a drastic improvement over the previous 40 %. The ringing almost disappeared in every case. It is because the generator is not only loaded by the IC, but by the equivalent load composed of the IC and the compensation load, which reduces the effective load variation when changing the IC load value.	27

2.12	BBI platforms comparison: state-of-the-art (S1P and S1G) versus the proposed enhanced platform (S2P and S2G). The ideal voltage pulse is -140 V ample and 20 ns wide, with rise and fall times of 4 ns. S1P shows a -108 % negative percentage overshoot. PW is 275 % too high with a 75 ns value. The fall time is 4 times higher than requested, and the rise time is more than 15 times higher. S1G highlights the ringing, seen on S1P on a lesser extent. On S2P, the voltage set point negative PO measures -31 %. PW now perfectly matches the set point of 20 ns. Rise and fall times are 4 times higher than they should be, despite both being consistent. S2G shows significant ringing reduction, while maintaining the same amount of transferred energy into the IC.	29
2.13	The two last rounds of an AES-128	31
2.14	Fault analysis mapping	33
3.1	Typical integrated circuit power delivery network, with two metal levels, showing standard-cell rows and standard-cell segments (in yellow) sandwiched between GND and VDD power rails.	40
3.2	Front view of an IC with Standard Cell Rows and Standard Cell Segments (SCS) displayed in yellow.	40
3.3	Dual-well (3.3a) and triple-well (3.3b) inverter silicon sectional view.	41
3.4	Substrate subdivision improvement over M. Dumont model for EMFI [20]. The backside is the accessible substrate, and the epitaxy is the highest substrate level, a.k.a. the silicon junction between the P-substrate and the N-well.	43
3.5	3-dimensional Dual-Well and Triple-Well IC comprehensive Standard-Cell Segment electrical models.	44
3.6	Equivalent logic gates models used in the SCS model (3.6a), and a simplified top view of a Standard-Cell with its size (3.6b).	44
3.7	Elementary substrate building block 3D schematic and its SPICE netlist.	45
3.8	SCS substrate layer SPICE netlist	46
3.9	Three-dimensional Standard-Cell Segments interconnection example.	47
4.1	BBI susceptibility area cross-sectional 2D view	54
4.2	Simulated non-thinned IC (140 μm) substrate voltage distribution: peak of the first voltage pulse edge	56
4.3	Simulated thinned IC (60 μm) substrate voltage distribution: peak of the first voltage pulse edge	57
4.4	Fault susceptibility maps	59
4.5	Susceptibility area spreading	59
4.6	Fault susceptibility maps couples	59
5.1	Sequential logic operation and BBI sampling fault susceptibility	65

List of Tables

2.1	FAM faults description	33
2.2	Giraud's DFA results. In yellow are indicated the bytes retrieved with a brute-force method instead of the Giraud's bit fault attack.	35

List of Algorithms

1	Integrated circuit SPICE netlist generation algorithm.	49
---	--	----

List of Acronyms

AES	Advanced Encryption Standard
BBI	Body Biasing Injection
BSIM	Berkeley Short-channel IGFET Model
CPS	Cyber-Physical System
DES	Data Encryption Standard
DoM	Difference of Means
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DW	Dual-Well
ECC	Elliptic-Curve Cryptography
EMFI	Electro-Magnetic Fault Injection
FAM	Fault Analysis Mapping
FIB	Focused Ion Beam
FSA	Fault Sensibility Analysis
FSM	Fault Susceptibility Map
GFI	Glitch Fault Injection
HFI	Hardware Fault Injection
IoT	Internet of Things
LFI	Laser Fault Injection
PCC	Pearson Correlation Coefficient
PLL	Phase Locked Loop
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
SCA	Side Channel Attack
SCS	Standard Cell Segment
SMA	SubMiniature version A
SPA	Simple Power Analysis
TW	Triple-Well
WLCSP	Wafer-Level Chip-Scale Packaging

Publications

2023-10-11 17:01:33+02:00

- [2]

General introduction 2023-10-11 17:01:33+02:00

Over the past years, various fault injection methods, representing a significant threat for secure integrated circuits, have been extensively studied, like laser fault injection (LFI), or more recently electromagnetic fault injection (EMFI). The purpose of these studies is to propose efficient countermeasures to the right cost. They have had multiple objectives, such as understanding the various phenomena at the origin of fault creation, or being able to simulate fault propagation over multiple abstraction levels...

Voltage pulse substrate fault injection, commonly called Body Biasing Injection (BBI), while being contemporary to EMFI, led to very few researches and studies in comparison. Up to the best of our knowledge, three scientific papers existed at the beginning of my thesis, back in 2020.

The LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier: Computer Sciences, Robotics and Microelectronics Laboratory of Montpellier), inventor of this technique in 2011, proposed this thesis to answer various questions such as:

- What are the phenomena at work leading to fault injection?
- What kind of spatial resolution does BBI offer?
- What is the time resolution of this method?
- Is it relevant to thin the silicon substrate of BBI target ICs?
- Can constraining fault attacks be performed with this method?

These questions have guided my thesis work through the last three years. These works have led me to propose CMOS integrated circuits simulation models in a BBI context, in addition to proposing improvements for the practice of BBI. My thesis manuscript is structured in five chapters. Each one of them attempt to provide answers to the preceding interrogations.

The **first chapter** of this manuscript provides an overview of the existing fault injection techniques, with a particular emphasis on BBI.

The **second chapter** describes improvements for the practice of BBI. These improvements have been conceived and obtained through my studies concerning BBI resolution and accuracy, both in time and space. Additionally, this **chapter** describes the practical results of a differential fault attack performed thanks to BBI and requiring single-bit faults.

The **third chapter** is dedicated to CMOS integrated circuits modeling under BBI. It introduces the established simulation models, in addition the designed algorithms allowing to simulate circuits subjected to BBI. The models and methods introduced allow us to simulate circuit behavior in reasonable duration, which allows us to perform parametric analysis of BBI effects.

The **fourth chapter** discusses a common practice in fault injection methods: the thinning of integrated circuits' substrate. While this topic has been extensively addressed concerning LFI, it is not the case for BBI. It relates to studying IC behavioral differences and BBI efficiency on different substrate thicknesses circuits. Various models are introduced to get different approaches, allowing to predict differently electrical and physical phenomena at work. Mathematical models are also derived from the previous models, enabling the calculation of optimal experimental parameters, in addition to predicting circuit behavior.

The **fifth** is dedicated to the understanding of fault creation in circuits subjected to BBI. It allows deriving a fault model from the simulations.

Eventually, the **last chapter** presents a general conclusion of my thesis work. In addition to this, outlooks are provided. The latter are interrogations remaining unanswered by my thesis works, mostly concerning more specific BBI effects on integrated circuits.

I

Introduction and state of the art 2023-10-11

17:01:33+02:00

chap:1_stateOfTheArt

Contents

1.1	Summary <small>2023-10-11 17:01:21+02:00</small>	2
1.2	Introduction <small>2023-10-11 17:01:21+02:00</small>	2
1.3	Side-channel attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.3.1	Timing attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.3.2	Power analysis and electromagnetic analysis attacks <small>2023-10-11 17:01:21+02:00</small>	5
1.4	Fault-injection attacks <small>2023-10-11 17:01:21+02:00</small>	7
1.4.1	Giraud's differential fault attack <small>2023-10-11 17:01:21+02:00</small>	8
1.5	Fault-injection techniques <small>2023-10-11 17:01:21+02:00</small>	8
1.5.1	Glitch fault injection <small>2023-10-11 17:01:21+02:00</small>	8
1.5.2	Laser fault injection <small>2023-10-11 17:01:21+02:00</small>	8
1.5.3	Electromagnetic fault injection <small>2023-10-11 17:01:21+02:00</small>	9
1.5.4	Body biasing injection <small>2023-10-11 17:01:21+02:00</small>	9

1.1 Summary 2023-10-11 17:01:33+02:00

chap:1; sect:summary

This chapter reviews the state-of-the-art concerning fault injection methods. It first defines the interest of studying fault injection and its context. Then, various fault injection techniques are presented and their differences, advantages and disadvantages are analyzed. Specifically, platforms equipment across all methods is described alongside the different techniques employed to perform such fault injection. Eventually, body biasing injection is introduced, and we will study its interests in a fault injection context.

1.2 Introduction 2023-10-11 17:01:33+02:00

chap:1; sect:intro

In our time, almost every business sector and every part of our surroundings, directly or indirectly, use integrated electronics circuits. It ranges from smart-cards to supercomputers, through military devices, cell-phones, Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) objects to name but a few.

Traditionally, integrated circuits design mainly focused on performance upgrades over the generations. Performance was measured thanks to two factors: computation speed and silicon surface. Within this context, power consumption was not a design constraint, therefore, integrated circuits became more and more energy-consuming. However, with the advent of portable devices, power consumption became a predominant design factor over speed, and space and got included into the former design flows. Nevertheless, less space and more speed does not physically equate with less energy. Alongside, new systems have emerged and have massively grown these past decades: IoT and CPS. On one hand, CPS are often systems where hardware and software are interlaced and thought together, and can be drastically different from one application to another. On the other hand, IoT systems have often less coordination between hardware and software, but are commonly more flexible. Whatsoever, both of these systems have something strong in common: their security is fundamental. Therefore, in this context, as it has been proposed in [3], and because security had been adopted as a counter-measure after the design flow, it has to enter as a fourth design rule when creating integrated circuits. This is required because a secure system has to ensure that every data going in and out of it are subject to the following criteria:

- Authenticity: data received have to come from the sender
- Integrity: data cannot be altered in any way
- Confidentiality: data cannot be accessed (read or written) by third-parties

Therefore, it is imperative to study and comprehend the strategies for enhancing IC security in order to develop future integrated circuits that are designed with security in mind from the

initial stages of development to its completion.

Currently, electronic devices implement security in two distinct ways, namely from a software or hardware standpoint. To accomplish this objective, encryption algorithms have been integrated. It is possible to distinguish two distinct categories of encryption algorithms, namely symmetric and asymmetric algorithms.

In short, symmetric cryptographic techniques use a unique key for encrypting and decrypting messages. The most popular algorithms are the AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), RC5 (Rivest Cipher 5), and TDES (Triple DES) not to cite them all. The key must be kept confidential and only shared among parties in order to maintain a confidential connection between them. The requirement for a single key is the main drawback of symmetric encryption methods. As a result, every possible step must be taken to safeguard key secrecy, such as avoiding key exchanges on public networks. However, symmetric encryption has a clear advantage over asymmetric encryption. As a result of utilizing a single key, symmetric algorithms are typically simpler than asymmetric algorithms, resulting in a reduction in computing power required for encryption. It is therefore possible to encrypt a large amount of data in a short amount of time.

In contrast, when it comes to symmetric cryptographic techniques, commonly referred to as public key cryptography techniques, a pair of keys is employed. The keys are usually referred to as public-key and private-key. The public key is used to encrypt a message, and anyone can use it. The private-key is, however, kept confidential to ensure that only authorized parties can decrypt a message that has been encrypted with the public-key. The primary motivation behind having two keys is that it is impracticable to reconstruct the public-key from the private-key. The most commonly employed asymmetric algorithms include the RSA (Rivest–Shamir–Adleman) algorithm, the ElGamal encryption system, the ECC (Elliptic-curve cryptography), and the Cramer-Shoup system, to name a few. The main drawback of symmetrical algorithms is that they involve large mathematical calculations, which implies a higher time complexity. Hence, these techniques are capable of encrypting a limited quantity of data. Therefore, to achieve this objective, in the majority of systems, a hybrid approach is employed to employ both encryption methods, thereby ensuring optimal security and a brief calculation time.

On the one hand, if all the previously mentioned algorithms are mathematically reliable, their reliability will decrease when they are implemented on actual integrated circuits. Indeed, every integrated circuit uses electrical energy to function. Therefore, when an electric current appears in a conductor, there is inevitably an electromagnetic field associated with this current. Moreover, every measurable physical quantity concerning the IC could be a point of information leakage. This is particularly true when considering the fact that these quantities will exhibit varying variations based on the calculations performed by the IC. When evaluating these quantities, it is possible to retrieve confidential information. We described what is called a "**side-channel attack**" (SCA) when considering cybersecurity.

On the other hand, physical quantity measurement is not the only flaw in actual algorithm implementations. In fact, every physical IC has specifications under which it can execute its functions properly. It includes temperature, clock frequency, power supply voltage, and the electromagnetic environment. When pushed beyond its specifications, any integrated circuit will exhibit unpredictable behavior. However, it is still possible to control an IC's behavior outside its specifications with a certain degree of success. By doing so, it allows running the IC calculation incorrectly by finely controlling how much time and by which amount the IC is outside its specifications, thus enabling, with specific mathematical algorithms, to retrieve hidden data manipulated by the IC. This process is commonly referred to as a "**fault injection attack**".

We have identified two potential attacks on robust algorithms that have been implemented into actual integrated circuits. However, it is customary to categorize cyberattacks into three distinct categories based on their execution methods.

Despite being technically advanced, noninvasive attacks are the most materially trivial. SCA are included in this set, which do not require any hardware modification to the targeted ICs, even if there is no physical contact. It is a delicate task to detect them; hence, they are deemed to be highly dangerous and are commonly considered in the initial stages of designing integrated circuits.

It is then possible to distinguish semi-invasive attacks. Systematically, they are accompanied by device physical preparation, which is entirely devoid of noninvasive attacks, but they are not accompanied by device physical modification. ICs integrity is therefore theoretically preserved. A typical IC modification involves the removal of the chip package. It enables access to either the front or back side of the integrated circuit, thereby facilitating micro-probing, laser injection, or substrate pulse injection. Furthermore, substrate thinning is also commonly considered and used, as it facilitates the fine-tuning of certain fault injection techniques, such as laser fault injection (LFI). These attacks necessitate specialized hardware, tools, and expertise and are frequently challenging to establish and execute.

Eventually, there are invasive attacks. They imply further physical modifications to integrated circuits. For instance, it is common to eliminate the layers of a chip, thereby enabling the photographing of the various layers and the reverse engineering of the target. A focused ion beam (FIB) can also be used to change the IC target internally by making electric connections that did not exist before. Contrary to semi-invasive attacks, invasive attacks frequently involve the definitive destruction of the target, primarily due to the absence of physical integrity during the process.

This doctoral thesis is dedicated to the study of a specific fault injection method: Body Biasing Injection (BBI). In this particular context, we will examine in this chapter the current state of the art in relation to side-channel attacks and fault injection techniques as outlined in the literature. This allows us to explain the interests of the current work regarding hardware

security.

In the first place, we will briefly discuss side-channel attacks. We will then examine the various fault injection platforms commonly described. Eventually, we will ponder the interests of BBI in this context.

1.3 Side-channel attacks 2023-10-11 17:01:33+02:00

chap:1;sect:sca

1.3.1 Timing attacks 2023-10-11 17:01:33+02:00

chap:1;sect:sca;subsect:timingAttacks

The most fundamental side-channel attack was initially introduced in 1996 [4]. This attack involves determining the duration required to execute cryptographic computations. By executing this method, the adversaries were able to obtain a variety of algorithmic keys, specifically for the RSA algorithm. The computation cost of this attack is low, thereby enabling it to execute swift attacks. Indeed, as per the RSA algorithm, as outlined in [5], the encryption of a message necessitates the calculation of the following relationship:

$$C \equiv E(M) \equiv M^e \pmod{n} \quad \text{eqn:rsa (1.1)}$$

M denotes the message to be encrypted, while C is the ciphertext and (e, n) the encryption key pair. The objective of the attack outlined in [4] is to retrieve e. To achieve this objective, the integrated circuit must perform multiple computations of the equation 1.1 for varying values of M, while maintaining identical values of e. Subsequently, the attacker must evaluate the duration of each computation. If the value of e differs for each operation, the attack cannot be executed. After the demonstration of this attack, countermeasures were implemented, including the implementation of constant-time cryptographic algorithms allowing the elimination of leaks through the utilization of timing analysis. More recently, other, more advanced countermeasures have also been proposed [6].

1.3.2 Power analysis and electromagnetic analysis attacks 2023-10-11 17:01:33+02:00

chap:1;sect:sca;subsect:powerAttack

Subsequently, more elaborated side-channel attacks were explained in 1999, as documented in [7]. This paper presents the concepts of simple power analysis (SPA) and differential power analysis (DPA).

On the one hand, SPA entails the measurement and direct interpretation of power consumption traces of a cryptographic integrated circuit. For instance, it enables the counting of DES or AES rounds to gain insights into the utilized implementation. Furthermore, it allows for the observation of power consumption variations depending on the executed instruction. A proposal has been made to prevent the utilization of secret keys or information during conditional

branching logic, with the objective of preventing simple power analysis.

On the other hand, DPA is a more elaborate approach that aims to identify the effects and variations associated with data processed by ICs. The aforementioned variations are more subtle and frequently obscured by noise. Therefore, DPA proposes to use statistics tools to reveal hidden system information, specifically by computing the difference of means (DoM) between traces. Therefore, preventing DPA is more complicated than preventing SPA. One of the simplest methods is to add electrical noise. Another technique is to reduce measurable signal amplitude. It is done first by optimizing code execution, by finely choosing which operation is performed to reduce electromagnetic leakage. Second, it is also possible to shield the device, but it increases the IC's cost significantly.

In addition to these attacks, there is also another attack which is commonly studied: correlation power analysis (CPA) [8]. As well as DPA, CPA uses statistical tools. However, as opposite to computing the difference of means, it involves calculating the Pearson correlation coefficient (PCC), allowing to measure the linear correlation between different power consumption traces.

It is important to note that SPA, DPA and CPA are historically performed using traces directly measured from the ICs power consumption. However, these attacks can also be performed thanks to IC electromagnetic radiation analysis [9]. Because electric charges are circulating into the IC, they inevitably generate electromagnetic waves. Therefore, it is possible to pick up these waves, and similar to power consumption, their shape depends on the data being processed. There has been numerous active research concerning this method for twenty years. It can be explained thanks to its advantages compared to bare power consumption analysis. Indeed, when measuring the entire power consumption of an IC, it is not possible to target a specific area. It leads, especially with complex ICs and countermeasures, to an impossibility to perform such attacks. On the contrary, electromagnetic analysis attacks have multiple advantages over power consumption analysis attacks:

- No sample preparation required
- No physical contact with the target
- It requires only little equipment: probe and voltage amplifier

As we stated previously, power consumption analysis attacks target an entire IC, whereas electromagnetic analysis attacks allow having fine resolutions. Indeed, small probes with a size down to 50 µm have been proposed [10]. Such small probes allow focusing the measurement on the cryptographic area of the IC, while excluding from the measurement, with a certain amount, any undesirable electromagnetic emission which could potentially harm the attack efficiency. In addition to that, electromagnetic probes, depending on their design, can have very high cutoff frequency. Therefore, it allows analyzing ICs running at high frequencies, enabling attacks on recent devices such as smartphones [11].

1.4 Fault-injection attacks 2023-10-11 17:01:33+02:00

chap:1;sect:fattack

Fault injections are widely described in the literature and can be utilized for a variety of purposes. For instance, during integrated circuits testing, it is common to find fault injection susceptibility tests, allowing for engineers to test fault detection circuits, recovery capabilities and reconfiguration possibilities of ICs. In this work, we are going to take a closer look at hardware fault injections (HFI) techniques solely, which fall in two distinct categories, similar to side-channel attacks:

- HFI with physical contact
- Contactless HFI

For each kind of HFI, multiple outcomes are aimed. On the one hand, the HFI can produce, in the targeted IC, branching errors leading secret codes to be revealed or protected rights to be acquired by an attacker. On the other hand, HFI can produce incorrect behaviors, allowing to retrieve hidden and protected data thanks to mathematical tools. In that case, HFI targets are mostly cryptographic algorithms, and can be segmented in non-comprehensive set of categories.

One of the most performed HFI is called differential fault attack/analysis (DFA). The principle of DFA lies in inducing computation errors during the decryption process of cryptographic algorithm thanks to fault injection. Several DFA were proposed on different algorithms [12, 13, 14, 15, 16]. Every DFA implies that the attacker has access to at least two ciphertexts, a correct one, denoted C , and a faulty one, denoted C_F . In addition to that, the attacker must also know the characteristics of the induced faults, such as the amount of faulted bits, in which operation they are faulted, etc. Eventually, it is needed to be able to induce the expected faults depending on the fault model required for the DFA.

Another common HFI is the fault sensitivity analysis (FSA) [17]. As every HFI, it is still required to have physical access to the device. FSA usefulness comes from the fact that alongside fault characteristics, other information can be used by attackers, in that case: the IC sensitivity to faults. As defined in [17], fault sensitivity is a condition where the faulty output begins to show specific characteristics. Specifically, this work defines a critical condition, similar to the PLL capture ranges (lock-in, hold-in, pull-in, etc.), where the IC starts to exhibit a faulty behavior or when it stops this behavior. Then, to perform an attack with this information, the attacker has to know the relationship between the fault sensitivity and the computed data, without knowing the insights of the cryptographic algorithm at work. It states that the algorithm will inevitably exhibit data-dependency of fault sensitivity. Hence, it allows using the IC as an almost black box.

In the next paragraph, we are going to analyze deeper a specific fault attack and its impli-

cations

1.4.1 Giraud's differential fault attack 2023-10-11 17:01:33+02:00

chap:1; sect:fattack; subsect:giraud

1.5 Fault-injection techniques 2023-10-11 17:01:33+02:00

chap:1; sect:fInjTech

1.5.1 Glitch fault injection 2023-10-11 17:01:33+02:00

chap:1; sect:fInjTech; subsect:glitch

Glitch fault injection (GFI) are one of the first historical documented fault injection attacks. They are simple and require little equipment. For the most part, they are non-invasive, which means that they are reversible, physically speaking. Various physical quantities can be disturbed, but the power supply voltages (VDD or GND), and the IC clock are the most common. Each physical quantity can be modified at the attacker's discretion, with a certain amount. However, the disturbances have to be short enough to avoid IC shutdown concerning power supply glitches, but also not powerful enough to avoid the IC destruction. On the one hand, the main advantage of such attack is its easiness to set up compared to other methods. On the other hand, their main disadvantage is the complete lack of locality with the injection effects. Indeed, disturbing IC's macro-parameters interfere with the entire chip and does not guarantee a useful faulty behavior. In addition to that, every modern IC is prepared to detect such attacks and thus protect itself by resetting its electronics.

1.5.2 Laser fault injection 2023-10-11 17:01:33+02:00

chap:1; sect:fInjTech; subsect:lfi

Laser fault injection (LFI), sometimes called optical fault injection, has been introduced in 2002 [18] and is a more complex technique than GFI. However, its precision is immensely better, at the cost of being semi-invasive, and sometimes invasive. LFI consists in targeting specific regions of the IC with laser beams of specific wavelengths. Several other parameters are involved for this method to succeed, such as the light emission duration, the area/volume of the targeted region, the IC substrate thickness, etc. Although LFI requires chip preparation, it is often minimal. LFI works thanks to the fact that every silicon semiconductor device (diode, transistor...) is intrinsically sensitive to light, typically with wavelengths ranging from 400 nm to 1000 nm. Therefore, if the light conveys enough energy, it is possible to change the state of some transistors, thus affecting logical values. The main shortcoming of LFI is the platform price. [Add more details.](#)

1.5.3 Electromagnetic fault injection 2023-10-11 17:01:33+02:00

chap:1; sect:fInjTech; subsect:emfi

Electromagnetic fault injection (EMFI) is a more recent and more studied technique, introduced in 2002 [19]. Its principle is basic: an electric current in a wire (probe) near an IC creates a corresponding electric current in the IC power delivery network, similar to an electric transformer. Similar to GFI, the attack can be non-invasive, although this method yields better results while being semi-invasive. Indeed, the closer the probe to the IC, the better the coupling and the mutual inductance, which often required to remove the IC's plastic package. This injection technique efficiency greatly varies depending on the probe's characteristics, the IC transistors size, the targeted location, the field duration, etc. Over the time, electromagnetic probes were constantly improved, and it is common to find probes with a ferrite core, allowing for better injection locality. In 2020, a modeling workflow was proposed [20], allowing to explain how EM probe can couple to IC power delivery networks. [Add more details.](#)

1.5.4 Body biasing injection 2023-10-11 17:01:33+02:00

chap:1; sect:fInjTech; subsect:bbi

Eventually, there is another fault injection method, less studied and more recent than the others, commonly called Body Biasing Injection (BBI), which is the research topic of this thesis. This technique has been introduced in 2012 [21], and further studied in 2013 [22] and 2016 [23]. At the beginning of this thesis, a fourth article was published [1], studying the interests of BBI concerning Wafer-Level Chip-Scale Packaging (WLCSP). The principle behind BBI is fairly simple: applying voltage pulses directly onto the backside of IC targets, thanks to a metallic probe. On the one hand, despite this simple premise, in the vast majority of cases, BBI is a semi-invasive method. Indeed, as most IC are encapsulated in a ceramic or plastic package, it is required, to access to the substrate, to partially remove a piece of the package. On the other hand, building a BBI platform is not expensive and technically easier when compared to LFI or EMFI. Indeed, a metallic probe with a custom armature costs around 10 euros at worst, and is easy to build at hand, while manufacturing a precise EMFI probe requires more knowledge to achieve good results. Considering that EMFI and BBI both require similar voltage pulse generator, which is often the most expensive piece of equipment, the overall platform cost is lower concerning BBI.

II

Body Biasing Injection platforms and good practices 2023-10-11 17:01:33+02:00

Contents

2.1	Summary <small>NEW 2023-10-11 17:01:21+02:00</small>	13
2.2	Introduction <small>UPDATED 2023-10-11 17:01:21+02:00</small>	13
2.3	BBI platforms in the state-of-the-art <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	14
2.3.1	Initial BBI platforms <small>UPDATED 2023-10-11 17:01:21+02:00</small>	14
2.3.2	C. O'Flynn BBI platform <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	14
2.3.3	Commercial platforms <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	15
2.3.4	An overview about BBI platforms <small>NEW 2023-10-11 17:01:21+02:00</small>	19
2.4	Our BBI platform <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	20
2.4.1	The probe <small>UPDATED 2023-10-11 17:01:21+02:00</small>	20
2.4.2	The generator <small>UPDATED 2023-10-11 17:01:21+02:00</small>	21
2.5	BBI in practice <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.1	Typical BBI platform model <small>UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.2	Platforms evaluation criteria <small>UPDATED 2023-10-11 17:01:21+02:00</small>	22
2.5.3	Raw results <small>UPDATED 2023-10-11 17:01:21+02:00</small>	23
2.5.4	Analysis conclusions <small>UPDATED 2023-10-11 17:01:21+02:00</small>	23
2.6	Enhanced BBI platform model and simulation <small>2023-10-11 17:01:21+02:00</small>	25
2.6.1	Matching the generator output impedance <small>UPDATED 2023-10-11 17:01:21+02:00</small>	25
2.6.2	Improving the grounding installation <small>UPDATED 2023-10-11 17:01:21+02:00</small>	26
2.6.3	Simulation results <small>UPDATED 2023-10-11 17:01:21+02:00</small>	26
2.6.4	Simulation conclusions <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	27
2.7	Actual enhanced BBI platform <small>PARTIALLY UPDATED 2023-10-11 17:01:21+02:00</small>	27
2.7.1	Generator impedance matching in practice <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.7.2	Grounding installation bypass in practice <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.7.3	Practical analysis <small>UPDATED 2023-10-11 17:01:21+02:00</small>	28
2.8	Enhanced BBI platform in a fault attack context <small>UPDATED 2023-10-11 17:01:21+02:00</small>	30
2.8.1	Giraud's DFA detailed description <small>NO CHANGES 2023-10-11 17:01:21+02:00</small>	30
2.8.2	Integrated circuits target characteristics <small>UPDATED 2023-10-11 17:01:21+02:00</small>	32
2.8.3	Preliminary attack experiments <small>UPDATED 2023-10-11 17:01:21+02:00</small>	33
2.8.4	Attack results and analysis <small>NEW 2023-10-11 17:01:21+02:00</small>	34
2.8.5	Giraud's DFA conclusion <small>NEW 2023-10-11 17:01:21+02:00</small>	35
2.9	Conclusion <small>UPDATED 2023-10-11 17:01:21+02:00</small>	35

2.1 Summary NEW 2023-10-11 17:01:33+02:00

This chapter first presents the various existing BBI platforms in the state-of-the-art, in addition to introducing our BBI platform. Then, I introduce improvements over the default platform used, allowing for better reproducibility and control over BBI parameters when compared to state-of-the-art platforms. At the beginning of this work, I was working using a state-of-the-art like platform, which led me to elaborating the enhancements as experiments were not reproducible due to great variations in every platform's parameter. Thanks to these improvements, I was able to draw better experimental results and to compare them to state-of-the-art platforms to verify the soundness of such platform modifications. These results are presented in the last part of this chapter thanks to elementary electrical experiments, followed by a differential fault attack, that I managed to perform thanks to the enhancements on a hardware AES coprocessor. Parts of this work were published in FDTC 2022 [24] and FDTC 2023. ([Add reference, quand on l'aura.](#))

2.2 Introduction UPDATED 2023-10-11 17:01:33+02:00

`chap:2_goodPractices; sect:summaryIntro`

In the first place, we are going to introduce Body Biasing Injection platforms:

- What exists in the state-of-the-art
- What I am using for my experiments

Afterward, I present a general BBI platform with its electrical model, in addition to evaluating the platform characteristics. Thanks to the model, I can perform electric simulations, allowing me to study and highlight its inherent flaws, such as:

- Poor control over the characteristics of the platform
- Obvious ringing leading to poor temporal accuracy
- Platform dependent parameters such as the ground installation quality
- Main physical quantities, such as the voltage and the pulse width, set points not met

Thereafter, I propose enhancements to overcome the previous platform shortcomings, which are:

- Matching the output impedance of the generator to reduce the ringing and bring the measurements closer to the specifications and the set points
- Bypassing the grounding installation to minimize platform dependency

After that, I present a deeper analysis of these enhancements, including ringing, set points accuracy, and load and transmission line dependency. Then, I discuss various techniques allowing to match the generator output impedance, in addition to introducing practical grounding installation bypass. Next, I perform actual experiments with our BBI platform, including measurements of such platform, illustrating the enhancements in practice. Eventually, I introduce a constraining differential fault attack set-up with our platform. It includes the attack description, followed by a thorough description of the IC target, sustained with experiments allowing me to perform the attack with more ease, with a comparison of a state-of-the-art platform with our enhanced platform, ended up by the attack results.

2.3 BBI platforms in the state-of-the-art PARTIALLY UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiPlatforms

2.3.1 Initial BBI platforms UPDATED 2023-10-11 17:01:33+02:00

First introduced in 2012 by P. Maurine et al. [21], further studied in 2013 by K. Tobich et al. [22], the proposed BBI platform in both papers is fairly simple, similar to EMFI platforms, composed of:

- A decapped IC, with its backside accessible;
- An independent voltage pulse generator able to generate positive and negative voltage pulses up to 100 V, with a maximum current of 2 A. The generator is DC-coupled with the load;
- A passive custom-made probe, consisting of an SMA connector and a standard needle soldered to it;
- A positioning system to place the probe precisely onto the IC backside;
- An acquisition system, measuring various voltages.

It is important to remark that the probe is connected through a relatively long interconnection, acting as a transmission line.

2.3.2 C. O'Flynn BBI platform NO CHANGES 2023-10-11 17:01:33+02:00

The original platform had stayed identical in the literature [23], until C. O'Flynn published in 2020 [1] practical examples of BBI attacks on WLCSP integrated circuits. In this work, the platform is structured differently. There are common elements, such as:

- An IC target with an accessible backside, in that case thanks to the WLCSP;
- A positioning system;

- Various acquisition tools.

The structural differences concern the voltage pulse generation. Instead of an independent voltage pulse generator, connected to a passive probe through a transmission line, the proposed solution consists in implementing an active probe with a separate pulse trigger generator.

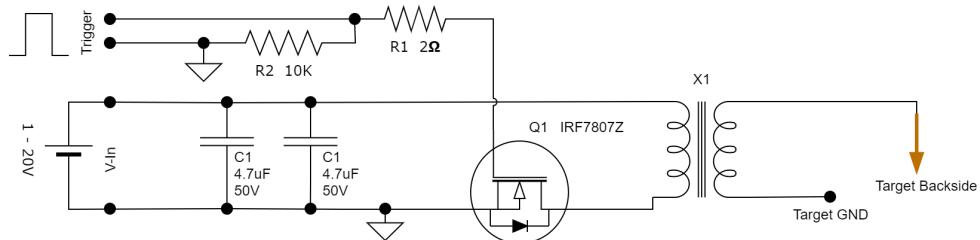


Figure 2.1: Schematic extracted from C. O'Flynn [1]: BBI injection device proposed by C. O'Flynn [1], using a transformer to produce high voltage pulses from a low voltage power supply. Fig: colinBBIsonde

Fig. 2.1 shows the design extracted from C. O'Flynn work [1]. The transformer allows creating high voltage pulses from a low voltage power supply. The transformer is controlled through the transistor Q1. Because the output is the secondary of a transformer, it is AC-coupled to the load, thus, no DC current can be transferred to the load. The transformer is custom-made and allows for ten times voltage multiplication, therefore enabling 300 V pulses with a 30 V power supply unit (PSU), which is fairly common for a lab PSU. The transistor is controlled thanks to an external trigger pulse, generated by another piece of equipment on this platform. It is on this point that O'Flynn's platform greatly differs from Maurine's initial platform.

The pulse generator used in this paper is a ChipWhisperer-Lite, an open-source tool created by NewAE Technology Inc. This tool can perform various tasks, such as pulse generation (as it is currently done), analog signals capture, or clock generation, enabling clock glitch fault injection. In addition to that, it can act as a simultaneous capture and target board, which is of great use in a BBI context.

2.3.3 Commercial platforms PARTIALLY UPDATED 2023-10-11 17:01:33+02:00

In addition to documented research BBI platforms, there are multiple commercially available solutions. We are going to address the most noteworthy in the current section.

2.3.3.1 Langer EMV-Technik GmbH BBI platform UPDATED 2023-10-11 17:01:33+02:00



Figure 2.2: BBI probe proposed by the company Langer EMV-Technik GmbH. Fig: langerBBI

The German society "Langer EMV-Technik GmbH" proposes a ready-to-use BBI platform. It is composed of two main hardware components:

- A BBI current pulse generator, illustrated in Fig. 2.2;
- A "Burst Power Station", which is the combination of a power supply and a controller allowing to control and monitor every probe sold by the company, with a provided software.

The core design is similar to the state-of-the-art platform, the main difference being that the system commercialized by Langer is marketed as being a current source instead of a voltage source. However, in practical operation, it does not represent a significant difference, since the major difference between a current source and a voltage source is their output impedance. Thus, one can either perform the BBI experiments with both electrical sources without much distinction, as long as the attacker is aware of these characteristics. The probe is specified with the following characteristics:

- A maximum allowable current of 4 A in a 1Ω load;
- A rise time inferior to 2 ns;
- A maximum pulse repetition frequency of 20 kHz;
- Positive and negative polarities;
- The possibility to delay the pulse command thanks to their control module;
- A jitter of ± 1 ns;
- A pulse width of 2 ns at full power, and of 4 ns at minimum power;
- A trigger delay ranging from 70 ns to 420 ns.

According to the product's datasheet, containing actual measurements of the probe, the minimal intensity allows injecting at peak approximately 2.4 A in 1Ω . However, contrary to the

open-source ChipWhisperer-Lite, there is very little official documentation about their products, thus reducing the available knowledge.

2.3.3.2 Riscure BBI platform UPDATED 2023-10-11 17:01:33+02:00

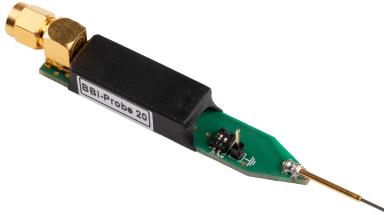


Figure 2.3: BBI probe proposed by the company Riscure BV. fig:riscureBBI

Similar to Ledge, Riscure proposes a quite complete BBI platform. It is composed, as before, of two major tools: a pulse generator and a metal probe. In that case however, the probes are passive ones. The generator, called "EM-FI Transient Probe", originally designed to be used in conjunction with EMFI probes, has the following characteristics:

- A maximum output voltage of $450 \text{ V} \pm 45 \text{ V}$;
- A maximum probe current (with 0 Ohm impedance) of 64 A ;
- A pulse width at half maximum output of 50 ns at full power (there is no mention of a controllable width);
- A trigger latency of 50 ns .

On the other hand, they propose four different BBI probes, one of them being illustrated in 2.3 which, in an odd way, are specified for different polarity and voltage amplitude depending on the model:

- A positive $200 \text{ V} \pm 40 \text{ V}$ with 15 ns pulse width;
- A positive $33 \text{ V} \pm 6.6 \text{ V}$ with 12 ns pulse width;
- A negative $37 \text{ V} \pm 7.4 \text{ V}$ with 20 ns pulse width;
- A negative $200 \text{ V} \pm 40 \text{ V}$ with 23 ns pulse width.

They include an SCS connector and a spring-loaded metal tip to avoid damage to the IC back-side. These BBI probes are meant to be used with the "EM-FI Transient Probe" pulse generator. Eventually, they provide a software to control their equipment.

2.3.3.3 NewAE Technology Inc. generators UPDATED 2023-10-11 17:01:33+02:00



Figure 2.4: Pulse generator for EMFI and BBI proposed by NewAE Technology Inc. fig:chipshouter

Eventually, NewAE Technology Inc. proposes various products for the practice of EMFI and BBI. Most of them can be used with one or the other fault injection method. I am going to cover two of them in this subsection.

The first one being the ChipSHOUTER®, with the pulse generator having the following characteristics:

- A voltage range comprised between 150 V to 500 V;
- A pulse width ranging from 15 ns to 480 ns depending on the connected load;
- A charge rate of 35 V/ms;
- An input jitter of 220 ps;
- A trigger latency of 50 ns;
- Python libraries allowing to interface and control the device;
- Monitor outputs allowing the user to probe internal signals.

This product costs around €4000 and the electrical schematics are available for free. It is a medium cost alternative compared to other equivalent pulse generator suh as the AVTECH AVRZ-5W-B from Avtech Electrosystems Ltd., the base model costing around \$15000.



Figure 2.5: PicoEMP: a low-cost pulse generator from NewAE Technology Inc. It provides much less instantaneous power than a typical generator, has a long recovery time (from 1 to 4 seconds), has a lower maximum amplitude (250 V), is not pre-calibrated, and has no controllable pulse width. However, it costs 94 % less than a typical generator, giving it a considerable advantage when building low-cost BBI platforms. fig:newAeChipShouter

The second product from NewAE is a very low-cost device: the PicoEMP. It is an open-source device, where safety and cost where the two main design rules. The tool is community maintained, and while originally designed for EMFI in mind, it was very recently studied concerning BBI in 2023 [25] by one of its contributors. A photograph of the device is shown in Fig. 2.5. Thanks to the low-cost design approach, the bill-of-materials for this tool is roughly equal to 50 \$., which makes it very accessible for anyone to build it from scratch. Its main characteristics and drawbacks are the following:

- It uses a transformer to generate high voltages, therefore no DC voltage option is available at its output;
- The output transformer is low-power, around up to 200 mW;
- The recovery time is slow, measured between 1 to 4 seconds depending on operating conditions;
- The maximum voltage pulse is of approximately 250 V;
- A pulse width of about 85 ns in $50\ \Omega$;
- There is no pre-calibration;
- It does not allow pulse width control by default. However, it is possible through drive signal control, even though being less accurate.

2.3.4 An overview about BBI platforms NEW 2023-10-11 17:01:33+02:00

From what I described previously, there are many different platforms and tools available for the practice of BBI. Their characteristics greatly vary from one platform to another, but they share a common ground, allowing to distinguish many tools and equipment constituting a typical BBI platform, which are the following:

- A metallic probe, allowing to make an electrical contact with the target backside, preferably spring-loaded;
- A voltage pulse generator capable of generating very high, short and precise pulses;
- A 3D positioning table, with a precision high enough for the application, to move the probe precisely with correct pressure on the backside;
- A preferably vibration-proof table to minimize probe physical jitter due to vibration caused by other equipment or natural vibration;
- A high precision oscilloscope to measure various physical quantities that might help to practice BBI.

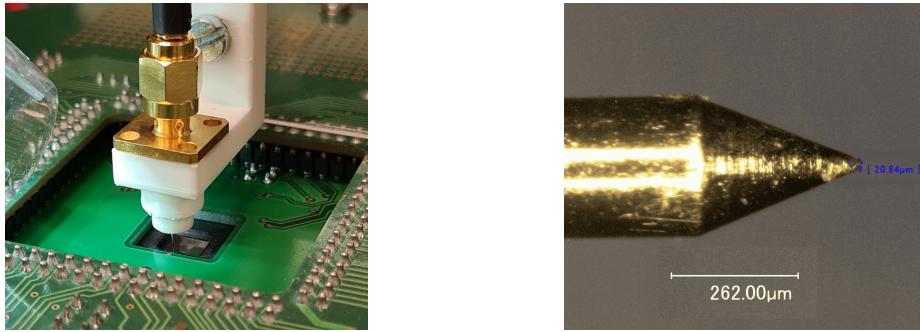
Some of these tools are not necessary to constitute a BBI platform, such as the positioning table, but they greatly simplify the platform reliability and reproducibility.

2.4 Our BBI platform PARTIALLY UPDATED 2023-10-11 17:01:33+02:00

With these tools in mind, we are describing in this section the platform we are using in our lab in detail.

2.4.1 The probe UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiPlatforms; subsect:probes



(a) Custom BBI probe in mechanical contact with the IC backside, seen through the perforated PCB
subfig:sondeBBI

(b) Custom BBI probe microscopy physical measurements
subfig:pointeBBI

Figure 2.6: Custom BBI probes photographs fig:sondePointeBBI

The most distinctive piece of equipment when working with BBI compared to other fault injection methods is the electrical probe. As we have seen before, it is commonly made with a metal tip, a connector of any sort and a mechanical support to hold the structure together. Some can be active, while others are passive, and therefore less expensive. However, it is very easy to build one, and any needle size available on the market can be used depending on the needs. In the case of BBI, the probe is used to establish the electrical contact with the substrate of integrated circuits, the latter being poorly conductive, but not isolating. For this work, we designed a custom probe, allowing us to control its characteristics, around three simple parts:

- An SMA connector, to have a low-cost, small and standard interconnection available with almost every high-speed equipment;
- A spring-loaded metallic tip soldered onto the SMA connector providing a better control over the applied pressure onto the backside;
- A custom 3D-printed support holding the parts together, shaped to fit with our other tools.

Fig. 2.6 shows detailed pictures of the probe we designed, with a photograph in operation in Fig. 2.6a, and a photograph under a microscope of the probe tip-end in Fig. 2.6b, allowing to measure its actual size before its first usage. The metallic probe we had chosen has a 0.635 mm diameter and is 16.35 mm long. The specified maximum nominal current of the probe is of 1.5 A, and the electrical contact resistance measures approximately 70 mΩ. The tip has a diameter

roughly equal to 20 μm , and it is important to note that this value tends to increase when the probe is utilized, due to the physical contact and the pressure with the IC backside. The bill-of-materials cost for our custom probe tool is roughly equal to 20 \$, ignoring manual labor to assemble everything together.

2.4.2 The generator UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiPlatforms; subsect:generator

The other fundamental piece of equipment when practicing BBI is the voltage pulse generator. It is, generally, one of the most expensive platform tool, similar to EMFI. Indeed, because BBI relies on voltage pulses to disturb an IC, it is necessary to provide a precise control over the pulse parameters to the user, such as the voltage set point, the pulse duration, etc.



Figure 2.7: Front side of the Avtech Electrosystems Ltd. AVRK-4-B High Voltage Pulser, used during all my thesis experiments.

fig:avrk4b

For my thesis, I am using a precise high speed and high voltage pulse generator to be able to finely study the voltage pulse characteristics effects on BBI, more specifically the AVRK-4-B from Avtech Electrosystems Ltd. It is shown in Fig. 2.7, and costs around \$14500 in its most basic configuration. Similar to the low-cost generator described previously, it is commonly used for EMFI, but is also suitable for BBI. Its main specifications are the following:

- The voltage pulse amplitude is specified between 150 V and 750 V with positive and negative polarities. The generator can go below and above these thresholds, however, there is no guarantee of the set point value correctness;
- The pulse width is specified between 6 ns and 20 ns. Similar to the voltage, the generator can go down from 4.5 ns, up to 22 ns, but is not specified out of the default range;
- Rise time (resp. fall time) for positive (resp. negative) pulses is specified to be precisely of 4 ns. Fall time (resp. rise time) for positive (resp. negative) pulses is not specified and depends on the generator load characteristics;
- The recovery time is inferior to 1 ms, allowing a pulse repetition frequency up to 1 kHz;
- The minimal propagation delay measures 150 ns, and can be raised up to 1 s;
- The jitter measures $\pm 100 \text{ os} \pm 0.03\%$ of the propagation delay;
- The output is DC-coupled, allowing the generator to continue providing energy to the load (if resistive or inductive) during the pulse plateau;
- All the specifications presuppose that the generator is loaded precisely with 50Ω .

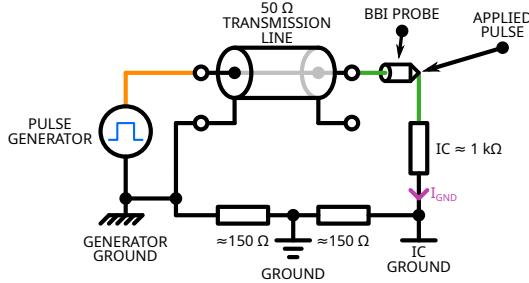
2.5 BBI in practice PARTIALLY UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiInPractice

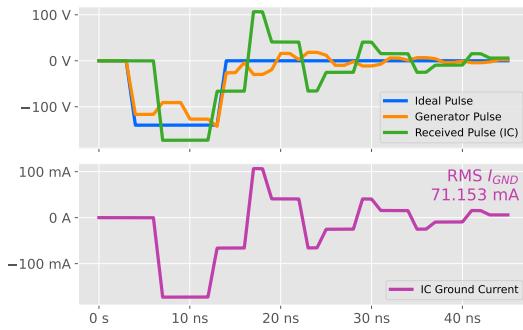
With actual BBI platform in mind, let me introduce a typical BBI platform model that we are going to study in details. These models allow us to concisely understand, evaluate and simulate BBI platforms behavior, limitations and room for improvement. We will therefore analyze the platform's performance and point out its weaknesses.

2.5.1 Typical BBI platform model UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiInPractice; subsect:bbiPlatformModel



(a) Model of a state-of-the-art BBI setup. It consists of the voltage pulse generator, the BBI metal probe, the transmission line, the IC ($1\text{ k}\Omega$ resistor), and the platform grounding (two $150\text{ }\Omega$ resistors). This model allows for fast evaluation and prediction of the BBI platform macro-behavior.



(b) Simulation results of the BBI model. Blue: ideal voltage pulse (-140 V, 10 ns). Green: effective signal applied on the IC backside. Orange: generator output. Purple: IC ground current. These results highlight the platform limitations: ringing (impedance mismatch) and high ground impedance, leading to higher voltage.

Figure 2.8: BBI platform electrical model developed for my thesis to quickly evaluate various platform's parameters, alongside the model simulation results.

fig:bbiBadGndGlobalFig

To be able to quickly predict and analyze BBI platforms, I developed a very simple electrical model, illustrated in Fig. 2.8a. This model represents the key components of a BBI platform, which are:

- The voltage pulse generator;
- The transmission line, used to connect the probe to the generator;
- The BBI probe;
- The targeted IC, modeled by an electrical resistance;
- The grounding installation, consisting of electrical resistances connected between equipment grounding.

2.5.2 Platforms evaluation criteria UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiInPractice; subsect:platformEvalCrit

For the purpose of evaluating BBI platforms, we decided to focus on two important criteria, allowing to represent the platform quality:

- The characteristics of the voltage pulse measured at the generator output, allowing to observe how the generator behave when loaded with the transmission line and the IC;
- The characteristics of the target ground current waveform, allowing to monitor exactly what is actually injected into the IC.

2.5.3 Raw results UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiInPractice; subsect:rawRes

To that end, we will deeply analyze the platform's simulation results shown in Fig. 2.8b. Four signals are displayed, with their colors matching the colors in Fig. 2.8a for greater clarity. There are three voltage waveforms and a current waveform. The blue waveform is the ideal voltage pulse an attacker want to apply to the backside of an IC during a body biasing injection. Its characteristics are the following: a voltage set point of -140 V and a pulse width set point of 10 ns. It is a steep, fast and precise pulse with controlled rise and fall times, pulse width and voltage. However, when performing real experiments, which the model allow us to evaluate, this ideal pulse falls apart. It can be seen thanks to the orange and green waveforms, representing respectively the pulse observer at the generator output and the pulse effectively applied onto the backside of the IC target. There are multiple obvious observations that can be made concerning the received pulse (green) signal:

- The voltage set point is not respected, with a 23.5 % negative percentage overshoot (PO) on the falling edge, and a 107 % positive percentage overshoot (PO);
- There is obvious ringing, causing the pulse width to be longer than expected in addition to damped oscillations

These effects can also be observed on the IC ground current waveform (**purple**), as it is a mirror of the applied pulse due to the pure resistive nature of the IC in that model.

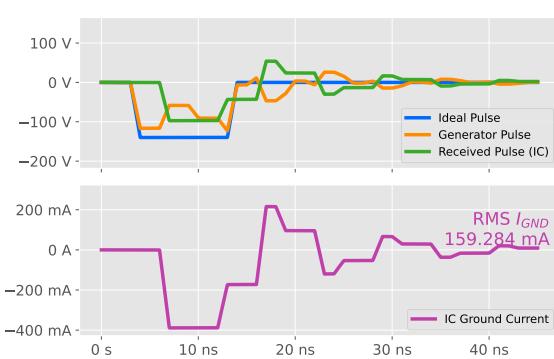
2.5.4 Analysis conclusions UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:bbiInPractice; subsect:analysConcl

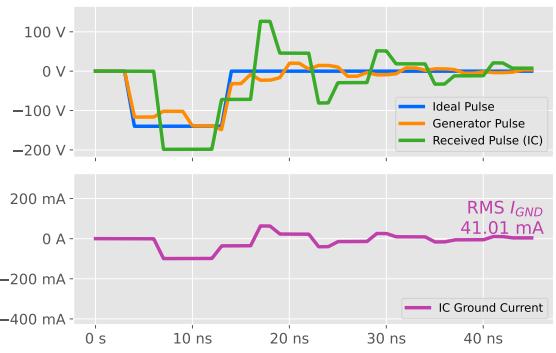
In order to understand the implications of such observations, let us analyze each one of them.

The first important thing to note is that the various model numeric values are extracted from our actual platform. Therefore, the $150\ \Omega$ grounding and the $1\ k\Omega$ IC are average measured values of actual devices. Thus, these parameters, in addition to the transmission line characteristics, will inevitably vary with a certain amount from one platform to another.

Indeed, the backside surface of an IC does not equal to a constant load. In addition to this, if the IC substrate is thinned, these values will change even more. Therefore, depending on the probe location and the IC substrate thickness, the generator might not see the exact same load. To illustrate the induced effects of such differences, I performed simulations with various IC



(a) Simulation result with an IC load equals to 250Ω . The voltage set point is not met, and the amplitude is -30 % lower than requested, with obvious ringing. Due to the lower IC load value, there is more energy injected into the IC. This is mainly caused by the voltage divider formed by the generator output stage and the IC load.



(b) Simulation result with an IC load equals to $2 k\Omega$. The voltage set point is not met once again, and the amplitude is 40 % higher than the requested value, with obvious ringing on all waveforms. Due to the higher IC load value, there is less energy injected into the IC. This is mainly caused by the voltage divider formed by the generator output stage and the IC load.

Figure 2.9: Platform simulation results with different IC load values

values, representing typical measured values for my IC target when thinned down to $50 \mu m$, up to more than $700 \mu m$, and the results are shown in Fig. 2.9, both for a 250Ω load (Fig. 2.9a), and a $2 k\Omega$ load (Fig. 2.9b). In both cases, due to the non-zero generator output impedance, the latter forms a voltage divider with the IC load. On the one hand, with an IC load value one quarter lower, there is more current in it, while the applied pulse amplitude is 30% lower. On the other hand, with an IC load value two times higher, there is less current in it, while the applied pulse amplitude is 40% higher. It represents a 70 % range around the set point value, which is excessively high. However, in both cases, the ringing is still present with the same amount relative to the pulse amplitude.

Eventually, all of these observations allow us to spot three major flaws of such platform:

- The platform parameters are difficult to control, leading to unknown values concerning pulse width, voltage set point, etc.;
- It leads to a poor temporal accuracy, thus minimizing the chances to perform a precise and repeatable fault injection;
- At last, all parameters are platform dependent, leading to a low reproducibility rate, thus lowering the credibility of experiments performed on such platforms.

In this context, I present in the next section various simple improvements to the BBI state-of-the-art platform.

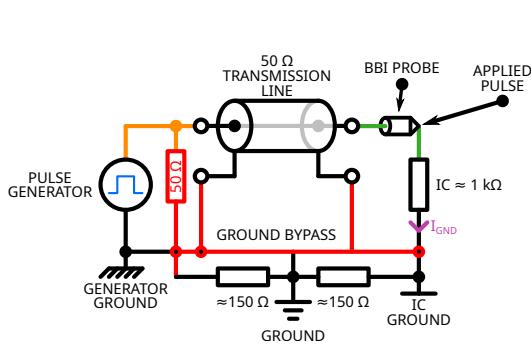
2.6 Enhanced BBI platform model and simulation 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIPlatforms

In this section, I propose platform enhancements over the state-of-the-art BBI platform previously introduced. These improvements aim at being low-cost, fast and easy to set up, to represent an interesting addition without drastically increasing the platform financial cost. Eventually, I am able to draw conclusions on such improvements thanks to simulation results.

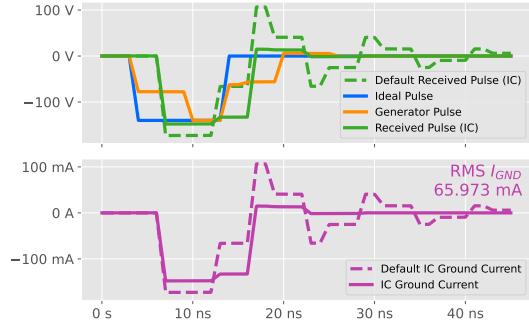
2.6.1 Matching the generator output impedance UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIPlatforms; subsect:bbiGenImpMatch



(a) Enhanced BBI platform model. It describes the generator, the BBI probe, the transmission line, the IC ($1\text{ k}\Omega$ resistor), the default platform grounding (both $150\text{ }\Omega$ resistors), and the enhancements highlighted in red, which are: creating an approximate impedance matching for the generator, and bypassing the poor grounding with low impedance copper wires.

fig:bbiPracticeImpGnd



(b) Simulation results of the enhanced BBI model. Blue: ideal voltage pulse (-140 V, 10 ns). Green: effective signal applied on the IC backside. Orange: generator output. Purple: IC ground current. The dotted waveforms are those observed in Fig. 2.8b. The most obvious observed improvements concern the set points, which are fully respected, in addition to the drastic ringing reduction, leading to better temporal control.

fig:bbiPracticeImpGndSignals

Figure 2.10: BBI platform enhanced electrical model developed for my thesis to quickly evaluate various platform parameters, alongside the model simulation results.

fig:bbiImpGndGlobalFig

The first proposed improvement concerns the generated voltage pulse characteristics. As we observed previously, the various parameters set points were not met. In a fault injection context, it is an undesirable behavior, as it is required to finely control the generated pulse to produce controlled disturbances into ICs. Therefore, and because most high speed high voltage pulse generator are specified to be loaded with a precise impedance, I simply propose to connect a known load directly at the output of the generator model. In my model, a $50\text{ }\Omega$ resistor is loaded at the generator output, as illustrated in red in Fig. 2.10a. Thus, the generator sees the impedance network formed by the compensation load, the IC, the transmission line, and the grounding installation. However, because the grounding installation is platform dependent, it is required, in order to perform a better impedance matching of the generator output, to improve the grounding, which leads to the other platform enhancement described in the following section.

2.6.2 Improving the grounding installation UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIPlatforms; subsect:bbiGndBetter

In many platforms, the grounding installation might be perfectly fine, and the following section may not apply to them. However, with our platform, we quickly observed that the grounding impedance was far from negligible. Indeed, with an average IC impedance around $1\text{ k}\Omega$, and inter-equipment ground impedance around $150\text{ }\Omega$, it represents a 15 % increase in the total impedance seen by the generator. Therefore, in order to transfer a maximum amount of energy into the IC, especially in areas where the IC impedance might be closer to the grounding impedance, it is required to cancel as much as possible the latter.

To that end, I propose a very simple setup modification. It consists in keeping the platform as is, and adding short copper wires between equipment grounds. Therefore, they shunt the platform ground and creates a low-impedance path for electric charges, thus allowing the previous section approximate impedance matching to perform better.

2.6.3 Simulation results UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIPlatforms; subsect:simRes

To verify the soundness of the previously proposed enhancements, I performed simulations thanks to the model presented in Fig. 2.10a. The simulation results are shown in Fig. 2.10b.

In that case, unlike in the state-of-the-art platform, the voltage set point is almost met concerning the received pulse (green waveform), with a slight undershoot of 6%. It is mirrored on the IC ground current waveform, where the ringing is drastically reduced, which leads to a steeper and more accurate pulse. It is especially noticeable when directly comparing the state-of-the-art waveforms in dotted lines. Concerning the generator pulse (orange waveform), it is still distorted as the ringing has not disappeared, but is less of a concern since the waveform of interest is the one effectively applied to the IC backside.

2.6.3.1 Load dependency NO CHANGES 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIPlatforms; subsect:simRes; subsubsect:loadDep

To further analyze the benefits of the proposed improvements, I performed, as for the state-of-the-art platform, additional simulations with various loads. As before, $250\text{ }\Omega$ and $2\text{ k}\Omega$ were chosen to have a common point of comparison. As I stated previously, these values are chosen to match the average typical value of my IC target when thinned down to $50\text{ }\mu\text{m}$, up to $700\text{ }\mu\text{m}$.

Fig. 2.11 presents the simulation results for such loads. For both loads, the measured voltage moves away from the set point by around 7 % in each case. It represents a 14 % range around the -140 V set point, which is immensely better than in the previous platform. It is still not perfect, but the platform is overall less dependent to the IC load, which is desirable in order to have repeatable voltage pulse across the entire IC backside.

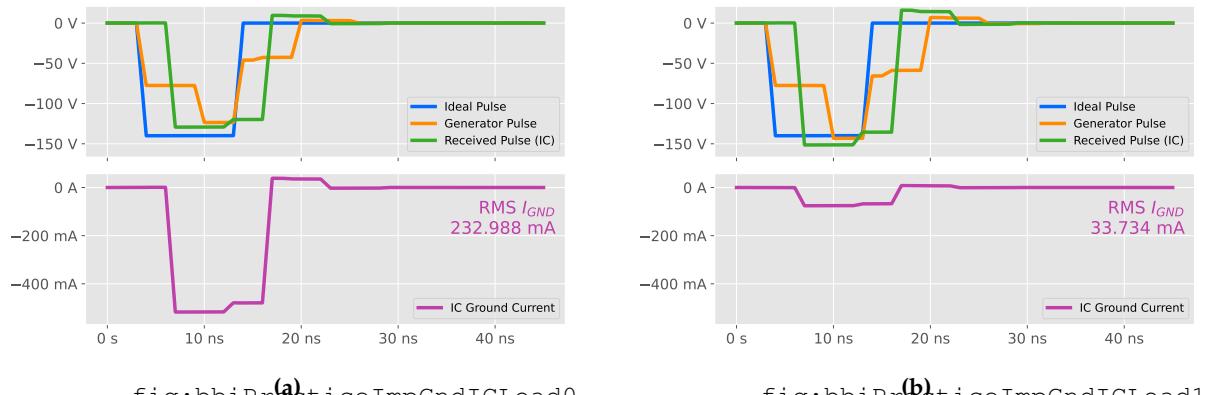


Figure 2.11: Simulation results of the enhanced platform with a 250Ω IC load (2.11a) and a $2 \text{ k}\Omega$ IC load (2.11b). The current increase in 2.11a is natural due to the load impedance reduction. However, the effective pulse amplitude relative to the set point has only a -7 % error, which is a drastic improvement over the previous -30 %. The set point is met. Then, in 2.11b, the current decrease is logical given the higher impedance value. The effective pulse amplitude relative to the set point has only a 7 % error, which is a drastic improvement over the previous 40 %. The ringing almost disappeared in every case. It is because the generator is not only loaded by the IC, but by the equivalent load composed of the IC and the compensation load, which reduces the effective load variation when changing the IC load value.
fig:bbiPracticeImpGndICLoad0 fig:bbiPracticeImpGndICLoad1

Then, quite naturally, for the 250Ω load, the current is higher than for the $1 \text{ k}\Omega$, and with the $2 \text{ k}\Omega$, it is lower. In addition to that, thanks to the 50Ω resistor placed at the generator output, it reduces the range in which the effective load (the compensation load in parallel with the IC) changes. Indeed, it goes from around 42Ω to about 49Ω , instead of going from 250Ω to $2 \text{ k}\Omega$ in the previous case. Eventually, in addition to all of the above, these enhancements have also drastically reduced ringing, which contributes to the applied pulse amplitude being closer to the set point.

2.6.4 Simulation conclusions NO CHANGES 2023-10-11 17:01:33+02:00

All of this leads to better control over the various platform parameters, allowing for more accurate and shorter pulses, closer to the expectations. In addition to that, the platform is less design dependent thanks to the minimization of impedance mismatch and poor grounding installation. It leads to a better time accuracy, enabling potentially more controllable fault injections.

2.7 Actual enhanced BBI platform PARTIALLY UPDATED 2023-10-11 17:01:33+02:00

The previous models being a useful tool to draw quick conclusions and predictions, it does not represent the reality. To that end, I set up the various presented enhancements in an actual BBI platform in order to verify the soundness of all the outcomes. In the first place, we are going to discuss how to perform the approximate impedance matching. Then, I will explain how to set up an efficient grounding bypass. After that, we will take a look at actual measurements

allowing to spot the improvements.

2.7.1 Generator impedance matching in practice UPDATED 2023-10-11 17:01:33+02:00

Add pictures of real platform impedance matching. An ideal impedance matching implementation should be adaptive and vary the impedance seen by the generator to perfectly match 50 Ω in every case. It would require a system with feedback, capable of measuring in real time the impedance presented by the IC target, in addition to the transmission line characteristics, to be able to adapt the compensation load impedance value. However, this is not the approach I have chosen. Indeed, the goal here is to minimize financial cost and platform modification, while allowing for better control over the platform parameters.

Another possibility would be to first measure the average IC backside impedance over its entire area or only the targeted area (such as the cryptographic core for instance). Then, thanks to the average value, the compensation load impedance could be chosen to better match the required 50 Ω .

Eventually, the selected solution is the simplest one. It consists in connecting a compensation load at the generator output, consisting in a 50 Ω SMA terminator. It is far from ideal, as this solution does not consider the transmission line nor the IC effective load nor the capacitive and/or inductive nature of the IC in addition to its resistive nature. However, it is a solution requiring little to no change to an existing platform and has proven to be good enough thanks to the previous models.

2.7.2 Grounding installation bypass in practice UPDATED 2023-10-11 17:01:33+02:00

Add pictures of real GND bypass. As we discussed previously, the grounding installation can drastically vary from one platform to another. Its effective impedance can be very high, such as in our platform, where equipment is grounded thanks to the platform earthing, with inter-equipment ground of around 150 Ω . To alleviate the effects of such ground impedance, I simply decided to shunt the existing earthing with short low-resistance copper wires. To that end, I chose an arbitrary piece of equipment as the reference, and connected every other piece of equipment local ground to the reference. It allowed reducing the effective platform ground impedance to a value close to 0 Ω .

2.7.3 Practical analysis UPDATED 2023-10-11 17:01:33+02:00

Now that I presented how to practically set up the enhancements, let us analyze actual measurements on the platform. We will compare before and after results, allowing us to analyze each evaluation criterion. As it was done for the simulations, we will observe the voltage pulse

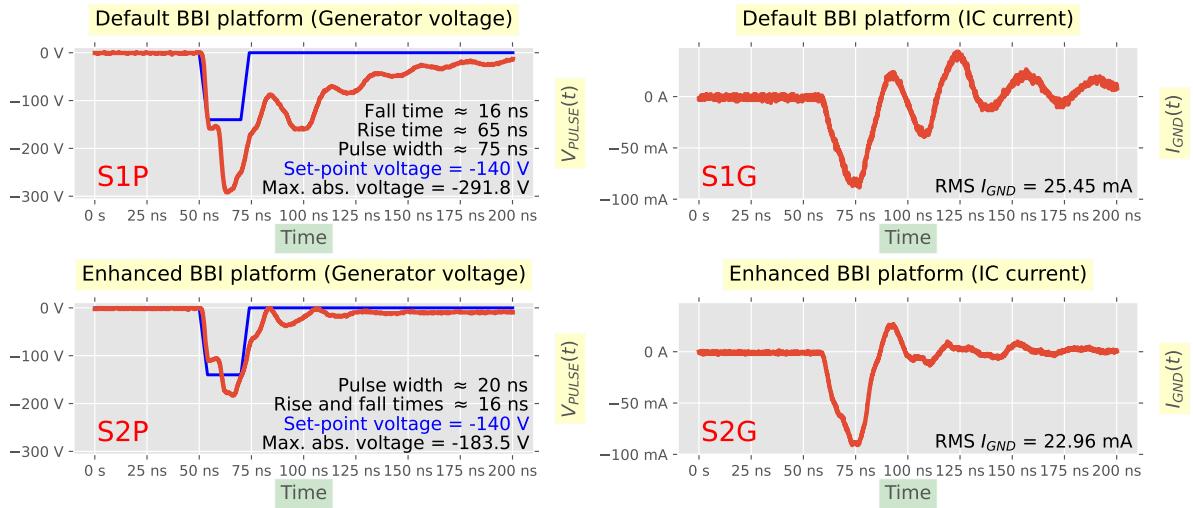


Figure 2.12: BBI platforms comparison: state-of-the-art (S1P and S1G) versus the proposed enhanced platform (S2P and S2G). The ideal voltage pulse is -140 V ample and 20 ns wide, with rise and fall times of 4 ns. S1P shows a -108 % negative percentage overshoot. PW is 275 % too high with a 75 ns value. The fall time is 4 times higher than requested, and the rise time is more than 15 times higher. S1G highlights the ringing, seen on S1P on a lesser extent. On S2P, the voltage set point negative PO measures -31 %. PW now perfectly matches the set point of 20 ns. Rise and fall times are 4 times higher than they should be, despite both being consistent. S2G shows significant ringing reduction, while maintaining the same amount of transferred energy into the IC.

fig:bbiRealXp

and the IC ground current.

Fig. 2.12 presents the various waveform results. The voltage pulse was measured at the IC backside during the injection, and the IC ground current was measured using a current probe thanks to the IC PCB ground interconnection. Therefore, the measured current is precisely the IC ground current, excluding any other equipment. The four waveforms displayed in Fig. 2.12 are code named using three characters for clarity. The first character is common to all waveforms, denoted "S" for "setup". Then, the number indicates which platform is concerned, "1" being the default platform, "2" being the enhanced one. Eventually, the last letter indicates which waveform is observed, "P" being the voltage pulse, "G" being the IC ground current. Therefore, the default platform contains S1P and S1G waveforms, while the enhanced one contains S2P and S2G signals. Fig. 2.12 also displays the waveforms characteristics for more clarity. The ideal voltage pulse applied has a maximum negative amplitude of 140 V, a pulse width of 20 ns, and 4 ns rise and fall times.

S1P shows a clear undershoot of -108 % under the set point. It is a clearly non-negligible value, which is far from desirable when performing fault injection, as most of the time, the voltage value has a great importance concerning efficiency and repeatability. In addition to this, the pulse width is 275 % higher than its set point. It is an additional undesirable behavior, especially when one wants to inject precise disturbances into an IC under test. Then, fall time is four times higher than requested, and rise time is more than fifteen times higher. Put with the longer pulse width, it worsens the pulse accuracy.

S1G brings to light the obvious ringing issue, also observable to a lesser extent on S1P, which leads to longer than expected disturbance inside the IC. Considering that the ringing is mainly caused by impedance mismatch between the generator and the IC, it will drastically change from one location to another, further reducing repeatability.

S2P, on the other hand, shows a better voltage amplitude, with a -31 % undershoot. It is far from perfect, but given the approximate nature of the proposed impedance matching, it was to be expected. Concerning the pulse width, the set point value is perfectly respected, which is very important for precise disturbance duration. However, rise and fall times are now consistent, but still four times higher than requested. It can easily be explained by the fact that the transmission line, the probe, the IC and the power installation are not a purely resistive load. Therefore, any capacitive element in the chain will inevitably reduce the system response time, thus elongating rise and fall times, leading to a shorter pulse plateau.

Concerning S2G, the approximate impedance matching shows a clear ringing reduction, with a steep current pulse, leading to a precise disturbance.

2.8 Enhanced BBI platform in a fault attack context UPDATED 2023-10-11

17:01:33+02:00

chap:2_goodPractices; sect:enhancedBBIGiraudAttack

Now that we have seen with simple actual experiments the benefits of the proposed enhanced BBI platform, let us linger on further experiments to verify more thoroughly the soundness of these enhancements. To that end, I performed a differential fault attack on our IC target. More specifically, a constraining fault attack requiring single bit faults on one or more bytes working on an AES cryptographic core, introduced by C. Giraud [16] in 2002, submitted in April 2002 to CHES'02. In the first place, we are going to discuss in details the core of the attack. Afterward, I will describe the IC target, its characteristics, and its operating conditions for the experiments. Then, I will introduce experiments we developed to perform preliminary measurements to the attack, accelerating the search of points of interests on the IC. Next, we will discuss the practical attack results. Eventually, we will draw conclusions on the various observations.

2.8.1 Giraud's DFA detailed description NO CHANGES 2023-10-11 17:01:33+02:00

When Giraud's paper [16] was published in 2002, no existing DFA was capable of attacking an AES algorithm. In this context, they proposed two types of DFA on AES, in order to cover various fault types one can induce on secured ICs. In this thesis, I focused on the first fault model, consisting in inducing single bit faults, therefore, this is the one we are going to discuss and describe in details in this section. It is interesting to note that Piret and Quisquater published another DFA one year after Giraud to CHES'03 [26], but I focused on Giraud's DFA for my thesis.

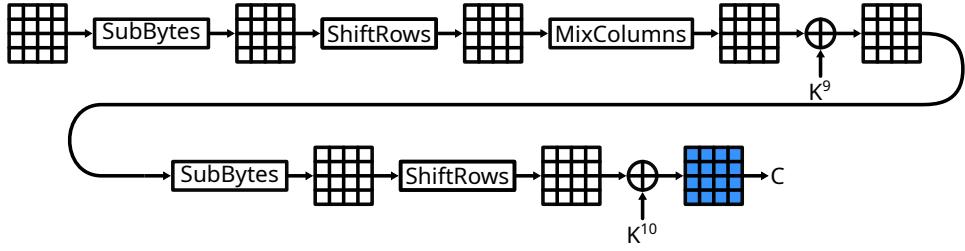


Figure 2.13: The two last rounds of an AES-128 fig:aesLastRounds

As we said before, the attack requires single bit faults on AES computation. More specifically, the fault has to appear at the beginning of the final AES round. Because we are using an AES-128, we will describe everything with this in mind. In addition to this, the various notations we will be using are the following:

- P is the AES plaintext and K the AES secret key
- P^i stands for the intermediate cipher result after the i^{th} AES round
- P_j^i is the j^{th} byte of P^i
- K^i represents the i^{th} AES round key
- As for P , K_j^i is the j^{th} byte of K^i
- C is the correct ciphertext, C_j is the j^{th} byte of C
- Eventually, CF stands for the faulty ciphertext, CF_j is the j^{th} byte of CF

Although the attack requires single bit faults on the final round, the attack is fairly simple and quick to perform with the right data at hand. I will not describe how AES operates, as it is well described in [16, 27]. The final ciphertext is given thanks to the following equation:

$$C = ShiftRows(SubBytes(P^9)) \oplus K^{10} \quad \text{cipherGiraud1} \quad (2.1)$$

With $SubBytes(P_j^i)$ being the substitution table (S-box) result calculated on M_j^i byte, and $ShiftRow(j)$ being the j^{th} byte position of the temporary result of the $ShiftRows$ transform. Thanks to eqn. 2.1, we can then deduce:

$$C_{ShiftRow(i)} = SubByte(P_i^9) \oplus K_{ShiftRow(i)}^{10}, \forall i \in \llbracket 0, 15 \rrbracket \quad \text{cipherGiraud2} \quad (2.2)$$

If an attacker manages to induce a fault e_j on a single bit of the j^{th} byte of the intermediate cipher P^9 before the AES final round, we have the following faulty ciphertext CF :

$$CF_{ShiftRow(j)} = SubByte(P_j^9 \oplus e_j) \oplus K_{ShiftRow(j)}^{10} \quad \text{faultyCipherGiraud1} \quad (2.3)$$

Which then gives us as before:

$$CF_{ShiftRow(i)} = SubByte(P_i^9 \oplus e_i) \oplus K_{ShiftRow(i)}^{10}, \forall i \in \llbracket 0, 15 \rrbracket \quad \text{faultyCipherGiraud2} \quad (2.4)$$

If there is no fault on the i^{th} byte of P^9 , thanks to eqns. 2.2 and 2.4, we have the following relation:

$$C_{ShiftRow(i)} \oplus CF_{ShiftRow(i)} = 0 \quad \text{griaudNoByteFault_ith} \quad (2.5)$$

If there is a fault on P_j^9 , we have, thanks to eqns. 2.2 and 2.3:

$$C_{ShiftRow(j)} \oplus CF_{ShiftRow(j)} = SubByte(P_j^9) \oplus SubByte(P_j^9 \oplus e_j) \quad \text{griaudFault} \quad (2.6)$$

Eventually, we have to first calculate ShiftRow(j), which gives us the location of the only non-zero byte of $C \oplus CF$, which in return gives us j . We then need to find P_j^9 : we look for the single bit fault e_j , and identify an ensemble of values of P_j^9 satisfying eqn. 2.6. For each correct value, we increase a counter by 1. Then, by taking another faulty ciphertext CF , and the correct value for P_j^9 should be counter more often than another incorrect value. Therefore, we can identify the correct value thanks to that affirmation. This process shall be repeated as much as needed to find every bytes of P^9 .

Thanks to eqn. 2.1, it is possible to retrieve the last round key K^{10} , which can be then converted to the AES secret key thanks to the inverse Key Scheduling applied on K^{10} . **To finish.**

2.8.2 Integrated circuits target characteristics UPDATED 2023-10-11 17:01:33+02:00

For the purpose of understanding clearly how we set up the previous attack, it is required to describe thoroughly the integrated circuit targeted. The model is an STM32F439VIT6 32-bits ARM Cortex-M4 microcontroller from STMicroelectronics, available in a LQFP100 package. The IC is manufactured using a 90 nm bulk technology. Its main characteristics are the following:

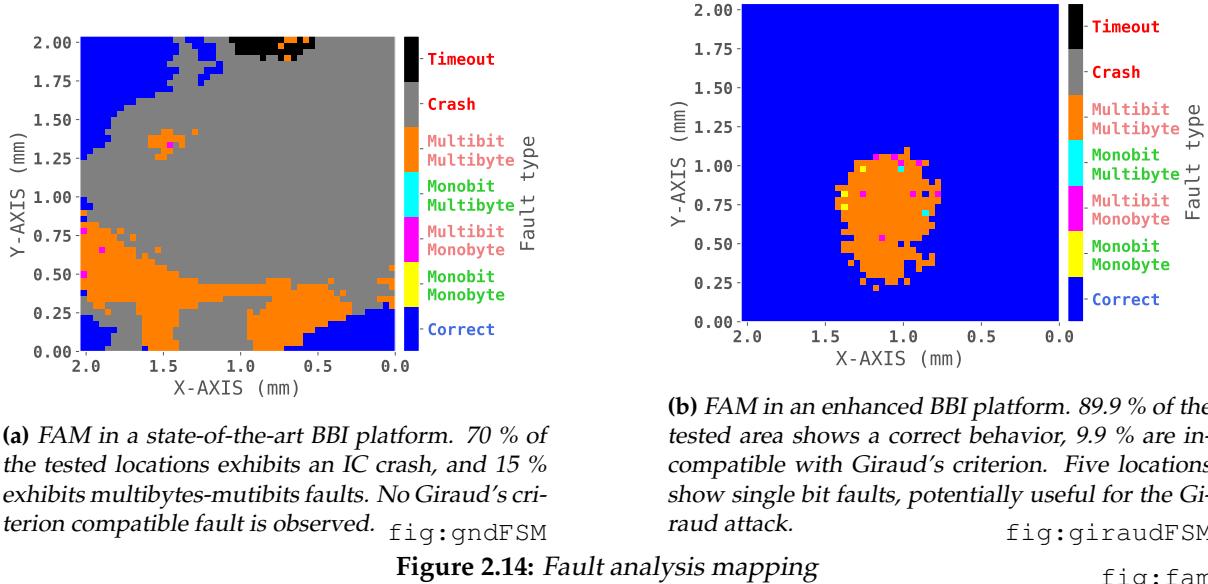
- A core clock up to 180 MHz;
- Two 1 MB FLASH memory banks;
- 256 kB of RAM;
- Voltage supply allowed from 1.7 V to 3.6 V;
- A True Random Number Generator (TRNG);
- A dedicated hardware cryptographic coprocessor, embedding AES (128, 192 and 256 bits), triple DES, and various HASH algorithms;
- A 700 μ m substrate thickness.

For the purpose of every other experiment, the IC is clocked at 40 MHz thanks to an external 8 MHz crystal oscillator.

2.8.3 Preliminary attack experiments UPDATED 2023-10-11 17:01:33+02:00

2.8.3.1 Fault analysis mapping description UPDATED 2023-10-11 17:01:33+02:00

For the purpose of accelerating and simplifying the attack process, especially because creating single bit faults is a troublesome process, I designed experiments to be conducted on the IC target, allowing me to spot interesting IC areas to perform the attack on. Because the attack targets the AES coprocessor, all the experiments described here are performed specifically on the AES core area.



These experiments are called "Fault Analysis Mapping" (FAM), and two results are shown in Fig.2.14. An FAM consists in performing BBI on the cryptographic core of the IC and trying to inject faults while identifying its behavior. We separated seven fault cases, described in Table 2.1.

Fault type	Description
Correct	The AES outputs a correct result
Monobit Monobyte	The fault is located on a single bit on a single byte
Multibit Monobyte	The faults are located multiple bits on a single byte
Monobit Multibyte	The faults are located multiple bytes and are single bit
Multibit Multibyte	The faults are located multiple bytes and multiple bits
Crash	The microcontroller did not respond correctly
Timeout	The microcontroller was unresponsive

Table 2.1: FAM faults description

table:faultType

Over the seven outcomes, only two of them can lead to potential exploitable fault according to Giraud's criterion: Monobit Monobyte and Monobit Multibyte. We performed these exper-

iments on a state-of-the-art (default) platform and on our enhanced platform, with the exact same equipment on both platforms.

2.8.3.2 Fault analysis mapping comparison NEW 2023-10-11 17:01:33+02:00

The FAMs I performed have the following parameters:

- A voltage pulse amplitude ranging from -150 V to -400 V with -5 V steps;
- A fixed pulse width of 4.5 ns;
- A fixed pulse delay of 150 ns + 553 ns allowing to target the penultimate AES round;
- The mapping measures 2 mm by 2 mm, with an isotropic displacement step of 40 μm .

These experiments take from 16 hours at best, up to 36 hours at worst to perform. It is quite long, however, compared to blindly looking for the correct location to perform the Giraud's attack, it is statistically much faster, especially when the AES approximate location is known to the user. I performed two FAMs, on the same IC target, for a state-of-the-art platform and for the proposed enhanced platform. FAM results are shown for the default platform in Fig. 2.14a and for the enhanced platform in Fig. 2.14b.

On the one hand, concerning the state-of-the-art platform, where the FAM is shown in Fig. 2.14a, we can spot numerous locations where a microcontroller crash was observed, more specifically 70 % of the tested locations. It is problematic as this behavior cannot lead to any meaningful data to perform a fault attack. Despite trying numerous experiment parameters, I was never able to obtain a single bit fault on any physical location on the AES core, even considering the ringing and reducing the voltage down to -20 V, to a point where the generator is not specified anymore to deliver consistent amplitudes.

On the other hand, without any tweaking, the FAM results show five single-bit faults. In addition to this, the IC did not crash at any given moment, and eight multi-bit faults can be spotted. It gives valuable information related to potentially interesting areas where the Giraud's DFA could be performed. It does not mean that the attack can be performed entirely on a single location, but it is a great way to guide the attack process, knowing that the set of parameters used is sound.

2.8.4 Attack results and analysis NEW 2023-10-11 17:01:33+02:00

Thanks to the previous FAM results, I decided to perform the attack on every location candidate using the enhanced platform. For each location above the AES core, a parameter sweep was performed, consisting in finding for each set of parameters, as much single bit faults as possible. The test settings are the following:

- The voltage pulse set point ranging from -300 V to -600 V;
- The pulse width ranging from 4.5 ns to 5.5 ns;
- The injection delay ranging from ± 10 ns around the penultimate AES round.

For each set of parameter, I set a limit of 100 single bit faults. However, this is an optimistic goal which, in some cases, can take a very long time to be achieved, and in other cases, cannot be achieved at all. Therefore, I decided to limit the number of trials to 10000, allowing the test algorithm to be finite and quick to perform. Then, with these results, I was able to perform the attack, where the result are shown in Table 2.2.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K10	0xFF	0x1F	0x42	0xE8	0xEF	0x44	0xA5	0x6A	0xCA	0xE7	0x55	0x3C	0xFD	0x65	0x39	0x26
KEY	0x01	0x23	0x45	0x67	0x89	0xAB	0xCD	0xEF	0xDE	0xAD	0xBE	0xEF	0x12	0x34	0x43	0x21

Table 2.2: Giraud's DFA results. In yellow are indicated the bytes retrieved with a brute-force method instead of the Giraud's bit fault attack.

table:dfaResults

What is obvious at first glance is that I was not able to retrieve the 16 bytes of K^{10} . Indeed, without further search for valid locations above the AES core, I was able to retrieve 14 out of 16 bytes. It is a great result, as the attack took about 20 hours to perform, including the FAM, which was the longest experiment to set up the attack. However, to retrieve the secret key, it is required to find all 16 bytes of K^{10} . Because there are 16 bits left, it is not particularly relevant to try to find interesting locations to perform Giraud's DFA, as there are only 65536 combinations to blindly test at worst to find the correct last round key. Considering the platform computer is able to perform approximately $188 \cdot 10^3$ encryptions per second, it would take $\frac{2^{16}}{188 \cdot 10^3} \cong 349 \cdot 10^{-3}$ seconds to perform the required calculation in the worst scenario. I then blindly tested every possibility to find the last two bytes, and I was able to retrieve them, thus allowing me to retrieve the AES secret key. These brute-forced bytes are shown in yellow in Table 2.2.

2.8.5 Giraud's DFA conclusion NEW 2023-10-11 17:01:33+02:00

To finish.

2.9 Conclusion UPDATED 2023-10-11 17:01:33+02:00

chap:2_goodPractices; sect:conclusion

In this chapter, I first introduced existing BBI platforms both in the state-of-the-art and commercially available. We have seen that multiples solutions ranging from low prices to very high prices exist, each one having its own advantages and disadvantages concerning their characteristics. Thanks to this platform overview, I was able to enumerate the fundamental building block of a typical BBI platform. After that, I presented the platform used during my thesis experiments, from the custom probe to the generator. Afterward, I introduced electrical models I

designed to quickly compare and evaluate BBI platforms. We studied the simulation results of such models, which allowed me to introduce enhancements to existing BBI platforms, allowing for better accuracy and reproducibility. Thereafter, I presented experiments performed to verify the soundness of such models, comparing state-of-the-art platforms to the enhanced platform I propose. Eventually, to go further in the model validation, I described and performed a constraining differential fault attack on a hardware AES coprocessor, sustaining the usefulness of the proposed enhancements.

III

Integrated circuits modeling IN PROGRESS 2023-10-11

17:01:33+02:00

Contents

3.1	Summary <small>UPDATED 2023-10-11 17:01:21+02:00</small>	38
3.2	Introduction <small>UPDATED 2023-10-11 17:01:21+02:00</small>	38
3.3	Integrated circuits structure <small>NEW 2023-10-11 17:01:21+02:00</small>	39
3.3.1	Power supply rails <small>NEW 2023-10-11 17:01:21+02:00</small>	39 <small>chap : 3-icModeling</small>
3.3.2	Standard-Cell rows <small>NEW 2023-10-11 17:01:21+02:00</small>	40
3.3.3	Various substrate types <small>NEW 2023-10-11 17:01:21+02:00</small>	41
3.4	Standard-Cell Segment (SCS) and their models <small>NEW 2023-10-11 17:01:21+02:00</small>	42
3.4.1	The case of Dual-Well substrates <small>NEW 2023-10-11 17:01:21+02:00</small>	43
3.4.2	The case of Triple-Well substrates <small>NEW 2023-10-11 17:01:21+02:00</small>	45
3.4.3	Writing the elementary models <small>NEW 2023-10-11 17:01:21+02:00</small>	45
3.5	Integrated circuit modeling: interconnecting Standard-Cell Segments together <small>NEW 2023-10-11 17:01:21+02:00</small>	46
3.6	Preliminary models validation <small>NEW 2023-10-11 17:01:21+02:00</small>	48

3.1 Summary UPDATED 2023-10-11 17:01:33+02:00

This chapter introduces and develops the work carried out concerning the integrated circuit modeling in a BBI context. It begins with an introduction of the various aspects on how ICs are manufactured, including power delivery networks and silicon substrate types, depicting the main aspects of their structure. Afterward, it introduces electrical models allowing to simulate integrated circuits under BBI. Then, it focuses on how to properly model the voltage pulse generator and the electrical probe, which are the main tools for performing BBI. Eventually, it shows the study of how actual logic gates react to BBI disturbances and the implications of such results. Parts of this work have been published both in [2] and [24].

3.2 Introduction UPDATED 2023-10-11 17:01:33+02:00

When evaluating and studying ICs under BBI, it is important to be able to fully predict and understand the underlying mechanisms at work in order to set up reproducible and reliable experiments, as well as being able to set up efficient countermeasures. However, modeling and simulating integrated circuit behavior subject to fault injection is not an easy task. More specifically, simulating an entire IC at a transistor level under fault injection is unrealistic with current resources and technology. It is especially true when considering time cost, as most modern digital ICs are composed of billions of transistors. However, when considering microcontrollers, the transistor count is sensibly lower, in the order of the million of transistors. As no software nor algorithm is currently dedicated to simulate the functional, electrical behavior of millions of transistors at the same time while some of them are disrupted by strong and transient disturbances, I had to overcome this limitation. In addition to that, to be able to set up a reliable model, it is required to have knowledge relative to the detailed architecture of the considered IC, which is impossible in most cases, as the vast majority of digital IC architectures are proprietary and closed-source. Therefore, it is required to find alternative workarounds in order to be able to study IC behavior and their various responses to fault injection techniques.

One of the first techniques allowing to simulate entire ICs behavior under fault injection has been first proposed in 2019 concerning Electromagnetic Fault Injection (EMFI) [28], and further extended in 2021 [20]. More specifically in the latest work [20], the proposed solution consists in establishing an equivalent non-logical model of an elementary section of the considered IC. Instead of modeling each logic gate with as many transistors as required to form a logic function, it was chosen to represent a hundred of logic gates in an average way, solely with a few resistors and capacitors, in addition to the power delivery network and the silicon substrate. It results in a transistor-less model, achieved using manufacturing data for the studied IC. The authors assumed that the first half of the transistors are conducting while the other half are blocking. Then, by repeating the model and interconnecting the various instances to one another, the authors managed to evaluate the IC power delivery network behavior under EMFI. This clever

design allows to drastically reduce the computing work required to analyze and predict behaviors of ICs subject to EMFI. Indeed, simulating the average behavior of a hundred of logic gates only with four resistors and four capacitors is immensely lighter and faster than simulating the equivalent with BSIM (Berkeley Short-channel IGFET Model) transistors. However, the main shortcoming being the lack of functionality with the produced ICs, it is therefore impossible to evaluate the consequences of EMFI concerning their functional behavior.

Body biasing injection being less documented than EMFI, no distributed model has yet been proposed to simulate ICs under BBI. In this context, my motivations were to set up and evaluate electrical models being able to reliably predict both in time and space IC behavior in order to understand how BBI induced disturbances propagate and create faults inside ICs. To that end, I chose to use the previous paper [20] model as a strong basis, while completing the model and providing improvements to properly consider the unique aspects of BBI. Then, and because such model cannot allow me to evaluate the consequences of BBI disturbances on the logic gates behavior, I completed the simulation flow to consider this aspect.

This chapter begins with a presentation of typical integrated circuits structure, including the power delivery networks and the logic gates layout, arranged in elementary blocks called Standard-Cell Segments (SCS). Afterward, I introduce the electrical models allowing me to simulate ICs under BBI, while verifying their soundness. Then, I present the importance of properly modeling the voltage generator when working with BBI simulations. Eventually, I introduce the new workflow I designed, expected to be used in conjunction with the previous models, allowing me to evaluate the functional consequences of BBI on integrated circuits.

3.3 Integrated circuits structure NEW 2023-10-11 17:01:33+02:00

For the purpose of properly introducing the electrical models I developed for BBI, it is required, in the first place, to linger on how integrated circuits are structured. It involves analyzing the main structures composing an IC, such as:

- Its power supply network, consisting in various metal levels stacked one on top of the others;
- The standard-cells: pre-characterized logic cells used as elementary building blocks;
- The various substrate types, such as Dual-Well and Triple-Well that I considered in my work, not to cite them all.

3.3.1 Power supply rails NEW 2023-10-11 17:01:33+02:00

In most modern integrated circuits, power is brought to the transistors through various metal layers organized as meshes. In digital ICs, there is typically two power delivery signals, com-

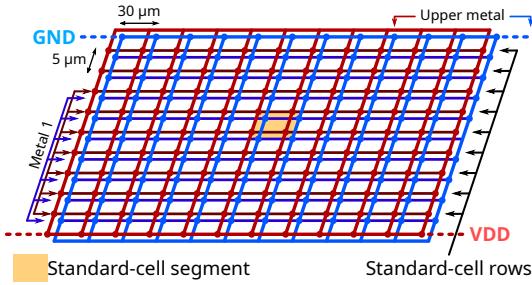


Figure 3.1: Typical integrated circuit power delivery network, with two metal levels, showing standard-cell rows and standard-cell segments (in yellow) sandwiched between GND and V_{DD} power rails.

monly called VDD and GND, GND being the ground reference of the IC. There are one or more pads for each power signal, connecting to power rings, surrounding the IC silicon die, as shown in Fig. 3.1. Then, power straps are created to mesh the rings and distribute evenly the power to the transistors. After that, rails are drawn to connect the power to the standard-cell segments, and vias are placed between rails and straps to wire them together.

3.3.2 Standard-Cell rows NEW 2023-10-11 17:01:33+02:00

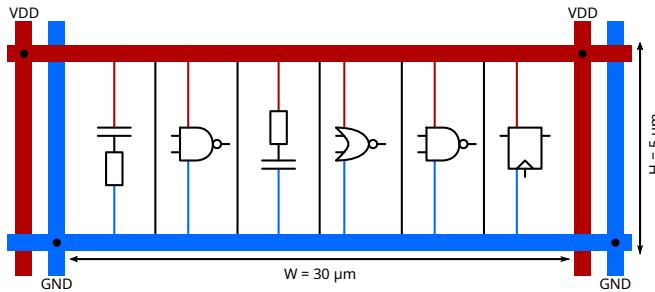


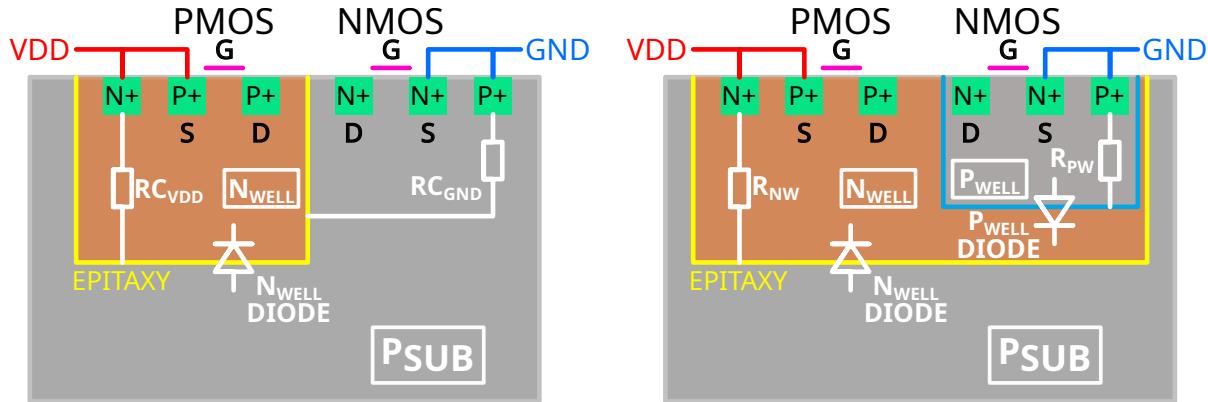
Figure 3.2: Front view of an IC with Standard Cell Rows and Standard Cell Segments (SCS) displayed in yellow.

As previously mentioned, Standard-Cells are the elementary building blocks used to design ICs. They are pre-defined logic cells, fulfilling a specific logic function. Standard-Cells can then be connected together to form a complete logic function. They are usually organized in rows, with a fixed height and variable width depending on the function. This allows simple power connection to each Standard-Cell. Fig. 3.2 illustrates how Standard-Cells are connected to the power supply network in an IC design. At the top of the Standard-Cells is the VDD power input, and at the bottom the GND power input. Typically, without considering various technologies, between the power rails are trapped three main regions:

- A N-doped silicon area, called the N-well, where the PMOS transistors are lithographed;
- A metal area where the transistor gates are accessible;
- A P-doped silicon area, called the P-well, where the NMOS transistors are lithographed.

Therefore, NMOS transistors are located in the bottom half of the standard-cell, and the PMOS are located in the top half.

3.3.3 Various substrate types NEW 2023-10-11 17:01:33+02:00



(a) CMOS inverter in a dual-well silicon substrate sectional view. The epitaxy is the junction between the P-substrate and the N-well. RC_{GND} is the access resistance from the epitaxy to the NMOS through the P-substrate. RC_{VDD} is the access resistance from the epitaxy to the PMOS through the N-well.

(b) CMOS inverter in a triple-well silicon substrate sectional view. The epitaxy is the junction between the P-substrate and the N-well. R_{NW} is the access resistance from the epitaxy to the PMOS through the N-well. Inside the N-well is created the P-well. R_{PW} is the access resistance from the N-well/P-well junction to the NMOS.

Figure 3.3: Dual-well (3.3a) and triple-well (3.3b) inverter silicon sectional view.

Because there are various ways to lithograph transistors for a given technology, I decided to linger and analyze the differences of two substrate types commonly found in bulk technologies:

- Dual-Well substrates, where NMOS transistors are lithographed directly into the P-doped silicon substrate;
- Triple-Well substrates, where the NMOS transistors are lithographed into a buried P-well inside the N-well where the PMOS are lithographed.

For the purpose of illustrating the structural differences between those substrate types, I am going to use the schematics displayed in Fig. 3.3 as a guide, illustrating the cross-sectional view of a logic inverter created in both a Dual-Well and a Triple-Well substrate.

3.3.3.1 Dual-Well substrates NEW 2023-10-11 17:01:33+02:00

To begin with, let us focus on Dual-Well substrates. A schematic sectional view of a CMOS inverter manufactured in a Dual-Well substrate is shown in Fig. 3.3a. Among moderately old ICs, it was common to find Dual-Well substrates. In these substrates, NMOS transistors are lithographed directly into the P-doped silicon substrate, as we can see in Fig. 3.3a. In addition to this, a N-doped silicon area is created inside the P-substrate, called the N-well, to lithograph the PMOS transistors. This results in a silicon junction, electrically represented by the N-well diode on the schematic, and called the epitaxy, highlighted in saturated blue. Because doped silicon does have a non-zero resistivity, electrical resistances are represented to demonstrate this:

- RC_{VDD} represents the access resistance measured between the epitaxy and the PMOS transistor through the N-well;
- RC_{GND} is the access resistance measured between the epitaxy and the NMOS transistor through the P-substrate.

3.3.3.2 Triple-Well substrates NEW 2023-10-11 17:01:33+02:00

TW helps to reduce crosstalk noise. On the other hand, Triple-Well substrates are also commonly used, often in combination with Dual-Well on the same die, to provide an electrical isolation between NMOS and PMOS transistors. It is achieved by creating inside the N-well, another doped silicon area, inversely doped, called the P-well. Inside the latter are then lithographed the NMOS transistors, while the PMOS transistors are still lithographed inside the N-well.

3.4 Standard-Cell Segment (SCS) and their models NEW 2023-10-11 17:01:33+02:00

Thanks to what I have introduced in the previous section, that is, the Standard-Cell arrangement used to create IC architectures, alongside the two identified substrate types of interest: Dual-Well and Triple-Well, it is now possible to elaborate an electrical model for such integrated circuits. Because I am differentiating Dual-Well and Triple-Well substrates, I am introducing two separate models, even though they show some similarities.

The models I developed are an improvement over the electrical models proposed by M. Dumont for EMFI [20]. Similar to [20] and to VLSI design, I am using the Standard-Cells as a basic building block. However, in my model is not represented the logic function of a Standard-Cell, rather its electrical behavior. More specifically, the elementary building block of the proposed electrical model represents the average electrical behavior of several Standard-Cells, called Standard-Cell Segment (SCS).

Because I based my work on M. Dumont model [20], there is a common base to which I have made modifications. The major one consists in improving the model geometric accuracy in the case of BBI studies. In M. Dumont model, the silicon P-substrate is represented solely thanks to a network of 6 resistors, 30 μm wide, 5 μm long, and t_{Sub} deep, t_{Sub} being the entire modeled IC substrate thickness. However, when performing BBI, the substrate is the main physical environment where the electric charges travel. Therefore, as I describe in more details further, it is required to improve the spatial resolution of the model concerning the substrate, as shown in Fig. 3.4. This is done by splitting the substrate electric model in several 6-resistors elementary networks interconnected with each other. It allows representing the same substrate with more resistors, thus enabling more precise analysis of the substrate charges distribution during BBI.

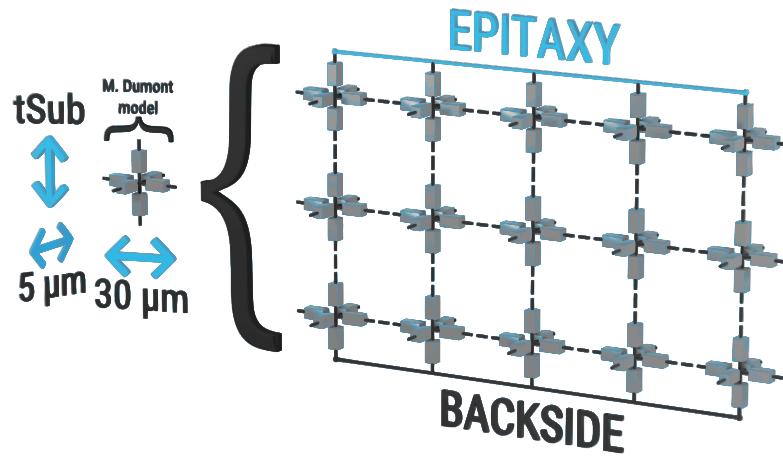


Figure 3.4: Substrate subdivision improvement over M. Dumont model for EMFI [20]. The backside is the accessible substrate, and the epitaxy is the highest substrate level, a.k.a. the silicon junction between the P-substrate and the N-well.

fig:surfaceSubDivid

Fig. 3.5 shows the complete 3-dimensional schematics of the developed models for my thesis. An analog simplified schematic representing the top view of a Standard-Cell is shown in Fig. 3.6b for understanding and clarity purposes. It describes the two levels of metal considered in my modeling (in orange and red), alongside the internal Standard-Cell interconnections in blue, with its size annotated.

The next subsections are dedicated to describing these models both for Dual-Well and Triple-Well substrates. Each SCS is 30 μm wide, 5 μm long and t_{Sub} deep, the thickness of the power delivery network and the logic gates being ignored, as the substrate thickness is often big in front of the latter. In my models, an SCS represents about a hundred of logic gates, where half of their transistors are conducting.

3.4.1 The case of Dual-Well substrates NEW 2023-10-11 17:01:33+02:00

Fig. 3.5a shows the electrical model of an SCS for Dual-Well substrates. Each SCS is delimited by the P-substrate at its bottom (1) and by the power rails at its top (5, 5'). The dotted wires at the bottom of the substrate indicates that each substrate layer can be repeated as required to form the correct t_{Sub} thickness. Dual-Well SCS are composed of six main regions, each one describing a part of an IC core sampling:

- Region 1 is the substrate resistive network, composed of several resistors, and being an isotropic environment;
- Region 2 is the P-substrate/N-well junction, modeled by a diode (DNW-PS) and its capacitance (CNW-PS), and is called the epitaxy, represented thanks to the blue net on the schematic. In addition to this, there is an access resistance from the epitaxy to the top of the N-well (VDD), representing the non-zero electrical resistance of N-doped silicon;

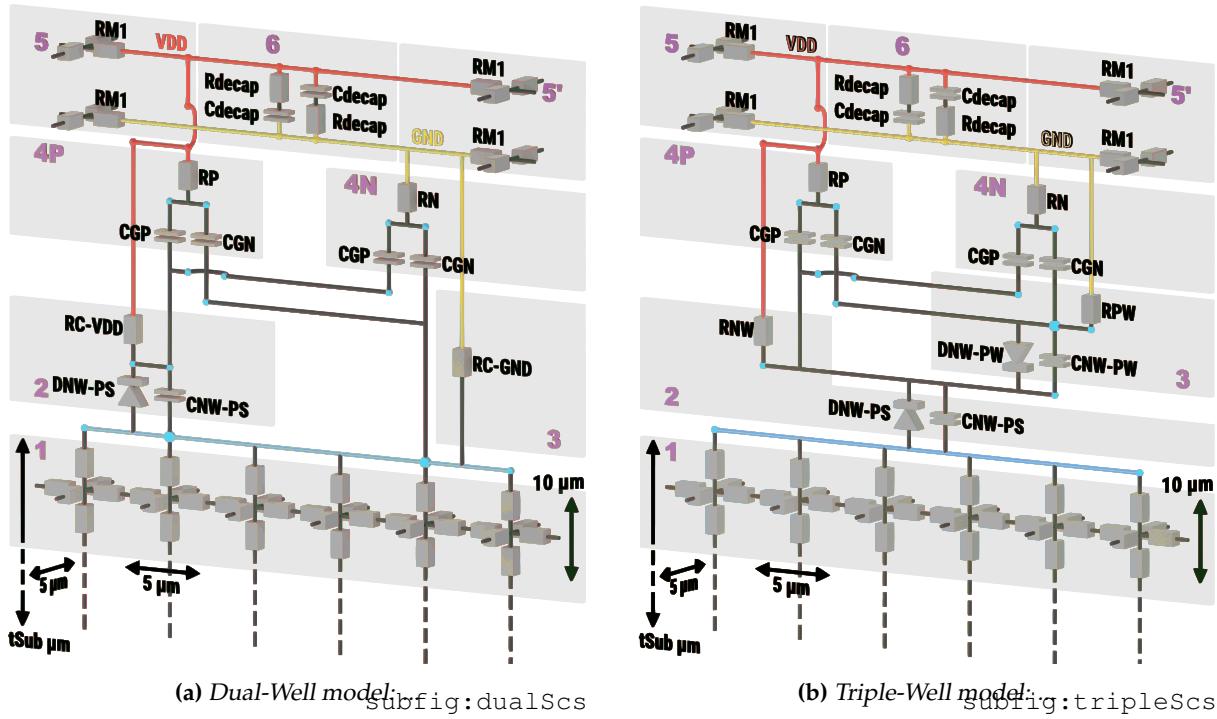
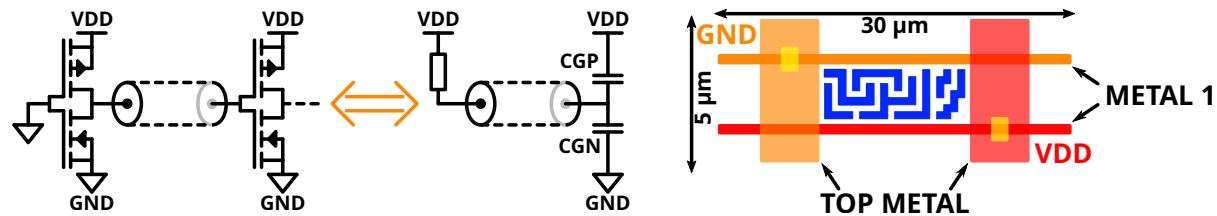


Figure 3.5: 3-dimensional Dual-Well and Triple-Well IC comprehensive Standard-Cell Segment electrical models.



- Region 3 is the access resistance from the epitaxy up to the GND power rail, representing the non-zero electrical resistance of the P-doped substrate;
- Region 4P is the model of the PMOS transistors, half of them being conducting. It consists in an access resistance RP from the VDD power-rail to the PMOS, and two capacitances, CGP being the load formed by the PMOS input capacitances, CGN the load formed by the NMOS input capacitances. Fig. 3.6a shows the model principle;
- Region 4N is similar to 4P: it is the model of the NMOS transistors, half of them being conducting. It consists in an access resistance RN from the GND power-rail to the NMOS, and two capacitances, CGP being the load formed by the PMOS input capacitances, CGN the load formed by the NMOS input capacitances. Fig. 3.6a shows the model principle;
- Region 5 and 5' are the power network interconnections, represented on two metal levels, the colored ones being the first metal levels, the gray being the top metal level.
- Eventually, region 6 is simply the decoupling existing between both GND and VDD

power rails.

3.4.2 The case of Triple-Well substrates NEW 2023-10-11 17:01:33+02:00

Fig. 3.5b illustrates the SCS model for Triple-Well substrates. The SCS are delimited, as before, by the P-substrate at their bottom and the power delivery network at their top. As for the Dual-Well model, the bottom dotted wires indicate that each substrate layer is repeated as needed to create the correct thickness required. The main difference between Dual-Well and Triple-Well SCS models lies in the region 3. First, let me describe every region:

- As for the previous model, region 1 is the silicon P-doped substrate;
- Region 2 is the N-well, created inside the P-substrate, with the junction (epitaxy) represented by a blue wire. It is composed of the diode DNW-PS, and its capacitance CNW-PS, alongside the N-well access resistance RNW from the epitaxy up to the VDD network;
- Region 3 is where the Triple-Well model drastically differ from the Dual-Well one. As I have explained before, in Triple-Well substrates, the NMOS transistors are lithographed inside an isolated P-doped region called the P-well. Therefore, region 3 describes the P-well, with an additional silicon junction modeled with the diode DNW-PW connected backward compared to DNW-PS, its capacitance CNW-PW, and the P-well access resistance RPW to GND;
- The three other regions are identical to the previous Dual-Well model.

3.4.3 Writing the elementary models NEW 2023-10-11 17:01:33+02:00

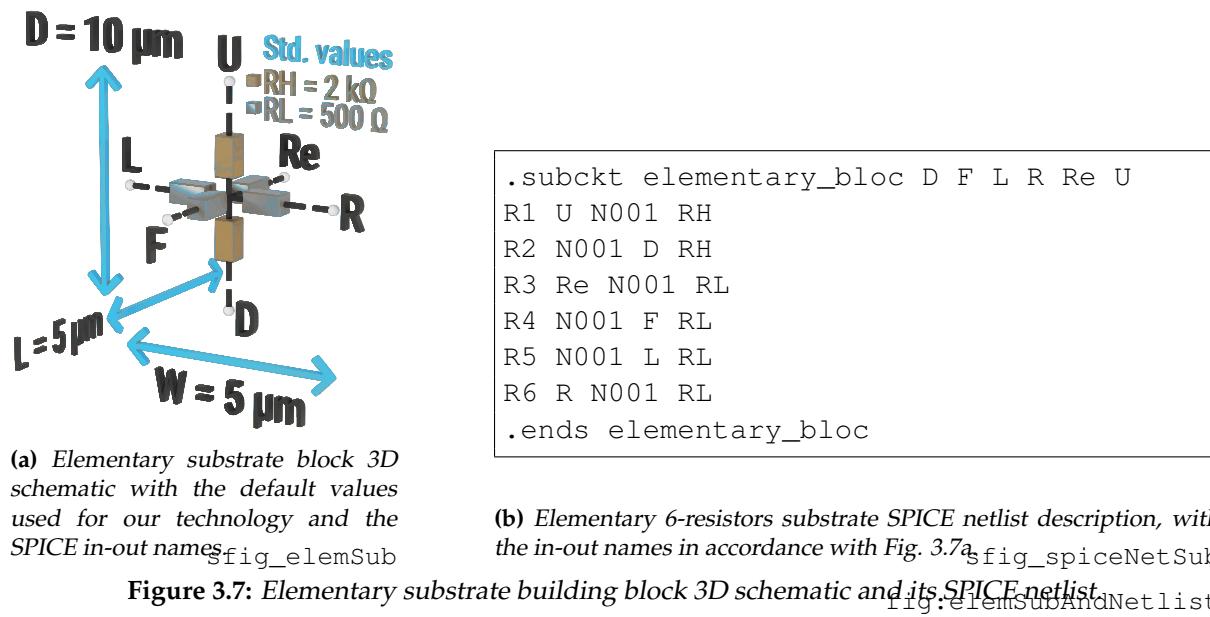


Figure 3.7: Elementary substrate building block 3D schematic and its SPICE netlist

After having abstractly created the models, I decided to write them using SPICE (Simulation Program with Integrated Circuit Emphasis) language. In addition to writing them, I calculated,

thanks to the technology values of our IC targets, to calculate the substrate resistor values. Considering the substrate resistivity being $\rho = 0.01 \Omega \cdot m$, and the elementary block size being $W = 5 \mu m$; $L = 5 \mu m$; $D = 10 \mu m$, it is trivial to calculate each resistance value R_i thanks to the following equation:

$$R_i = \frac{\rho \cdot l}{S} \quad \text{eqn_resistivity (3.1)}$$

Knowing that $L = W \equiv LW$ and that $D = LW$, we can first write that the vertical resistances will be four times the horizontal ones. Therefore, calculating one value of them gives the six values. Let us calculate the vertical resistances, which I will call RH :

$$RH = \frac{\rho \cdot \frac{D}{2}}{L \cdot W} = 2000 \Omega \quad (3.2)$$

Therefore, the horizontal resistances are equal to $RL = 500 \Omega$. These calculations can be adapted as needed depending on the technology used. In addition to that, a substrate with a given thickness t_{Sub} can be represented with virtually any number of layers. For example, one can reduce the number of layer by ten by adjusting the resistor values. It has the advantage to provide a lighter simulation, which will be faster to perform, at the cost of less accuracy.

Previously, I have stated that an SCS is $30 \mu m$ wide. However, the elementary block I described is $5 \mu m$ wide. To achieve a $30 \mu m$ wide SCS, it is simply required to connect six of these blocks together to form a $W = 30 \mu m \cdot L = 5 \mu m \cdot D = 10 \mu m$ substrate, as it can be seen in Fig. 3.5 models. The resulting netlist is shown in Fig. 3.8, and naturally instantiate six times

```
.subckt elementary_blocx6 D1 D2 D3 D4 D5 D6
+F1 F2 F3 F4 F5 F6 L R RE1 RE2 RE3 RE4 RE5 RE6
+U1 U2 U3 U4 U5 U6 VSUBCintC
XX1 D1 F1 L VSUBCintL2 RE1 U1 elementary_bloc
XX2 D2 F2 VSUBCintL2 VSUBCintL1 RE2 U2 elementary_bloc
XX3 D3 F3 VSUBCintL1 VSUBCintC RE3 U3 elementary_bloc
XX4 D4 F4 VSUBCintC VSUBCintR1 RE4 U4 elementary_bloc
XX5 D5 F5 VSUBCintR1 VSUBCintR2 RE5 U5 elementary_bloc
XX6 D6 F6 VSUBCintR2 R RE6 U6 elementary_bloc
.ends elementary_blocx6
```

Figure 3.8: SCS substrate layer SPICE netlist

fig_elemBlocX6

the previous netlist shown in Fig. 3.7b.

3.5 Integrated circuit modeling: interconnecting Standard-Cell Segments together NEW 2023-10-11 17:01:33+02:00

Because the SCS I previously introduced only describe a portion of an integrated circuit, in order to model a complete one, it is required to instantiate several SCS and to connect them with each other in a mesh grid. Fig. 3.9 is a coarse illustration of what is done. SCS are writ-

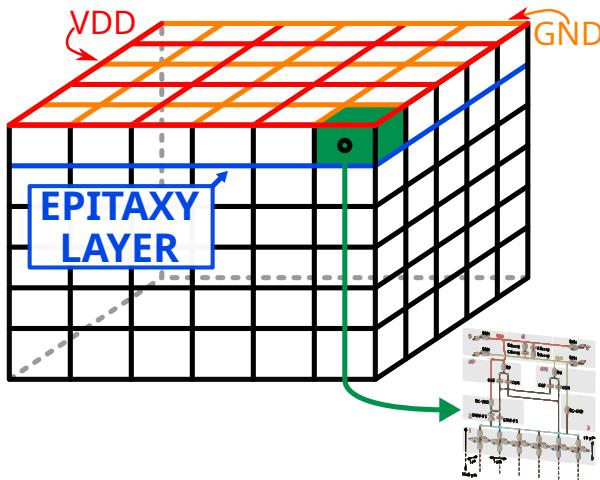


Figure 3.9: Three-dimensional Standard-Cell Segments interconnection example.

ten, as the elementary substrate building blocks, in SPICE. The SCS elementary models were automatically generated instead of being written manually, to avoid errors and enabling fast modifications to the models when required. In addition to this, I decided to create an algorithm to connect as much SCS as needed to create a resulting IC. By doing so, the interconnection process is once again automated and free from human errors. A simple description of the algorithm is depicted in Alg. 1 Because I have designed two separate models, one for Dual-Well and another for Triple-Well substrate types, in addition to the various dynamic parameters which are useful when modeling an IC, the algorithm offers a certain degree of flexibility. The actual program was written and implemented using Python, implementing procedural generation of integrated circuits according to the input parameters. Next is the list of user-modifiable input parameters of the algorithm:

- The resulting IC size;
- The BBI probe location;
- The IC global substrate thickness;
- The substrate sub-model thickness;
- The substrate type: Dual-Well, Triple-Well, or a mix of both, allowing to replicate actual IC architectures;
- The voltage pulse amplitude, width, and rise and fall times;
- Various SPICE simulation settings.

Eventually, the program incorporates a visual inspection tool in order to provide a quick verification of the generated IC structure to the end-user.

3.6 Preliminary models validation NEW 2023-10-11 17:01:33+02:00

Designing and creating the models I previously described is the first step in practically implementing them. Afterward comes various validation to verify the soundness of such models. To that end, using the generation algorithm, I created various ICs with the following measurements: a width of $550 \mu m$, a depth of $450 \mu m$, and a substrate thickness of $140 \mu m$. It is, according to our platform computational power, a reasonable size/calculation time ratio. Three ICs are generated:

- An exclusive Dual-Well circuit, to isolate the Dual-Well specific BBI effects with further simulations;
- An exclusive Triple-Well circuit, to isolate the Triple-Well specific effects under BBI;
- Eventually, a mixed substrate IC, comprising at the same time Dual-Well and Triple-Well SCS, to mimic a real IC, more specifically our platform microcontroller.

For each preliminary validation, the IC is simply powered thanks to its power inputs, and no BBI probe is connected to any of them.

Then, for each generated IC, I defined validation criteria, consisting in:

- Measuring the global IC quiescent leakage current to verify any inconsistencies. Indeed, a steady should draw a reasonable amount of power. Therefore, verifying this criterion allows verifying if the model is flawed, specifically concerning the substrate blocks interconnections and the substrate connection to the top of the SCS;
- Measuring the power network IR drop. It is complementary to the previous measurement and allows spotting any inconsistencies in the power delivery network design or generation.

Algorithm 1 Integrated circuit SPICE netlist generation algorithm.

Require: SUBTYPE ▷ IC substrate type: Dual-well, Triple-well, Mixed
Require: TSUB ▷ IC substrate thickness
Require: ESUB ▷ Elementary substrate block thickness
Require: VPUU ▷ Voltage pulse amplitude
Require: PW ▷ Voltage pulse width
Require: TFR ▷ Voltage pulse rise and fall times
Require: SIMTIME ▷ Simulation duration
Require: SIMSTEP ▷ Simulation time step
Require: TEX ▷ Desired X size (μm)
Require: TEY ▷ Desired Y size (μm)
Require: prbX ▷ BBI probe X coordinate
Require: prbY ▷ BBI probe Y coordinate

$RH \leftarrow 2000$ ▷ Elementary substrate up-down/front-rear resistor value
 $RL \leftarrow 500$ ▷ Elementary substrate left-right resistor value
 $WSEG \leftarrow 30$
 $HSEG \leftarrow 5$
 $W6SEG \leftarrow 30 \div 6$
 $nC \leftarrow TEX \div WSEG$ ▷ Number of column
 $nL \leftarrow TEY \div HSEG$ ▷ Number of lines
 $nH \leftarrow TSUB \div ESUB$ ▷ Number of substrate layers

Ensure: nC, nL and nH are integers

var SCS[nL, nH] ▷ Array containing each standard-cell properties

$RH \leftarrow RH \times (ESUB \div 10)$ ▷ Adjust RH value according to user defined variable
 $RL \leftarrow RL \times (ESUB \div 10)$ ▷ Adjust RL value according to user defined variable

for all cY in $\llbracket 0 ; nL \rrbracket$ **do**

for all cX in $\llbracket 0 ; nH \rrbracket$ **do**

$\vec{X} \leftarrow \begin{bmatrix} cX \times WSEG \\ cX \times WSEG + 1 \times (W6SEG \div 2) \\ cX \times WSEG + 3 \times (W6SEG \div 2) \\ cX \times WSEG + 5 \times (W6SEG \div 2) \\ cX \times WSEG + 7 \times (W6SEG \div 2) \\ cX \times WSEG + 9 \times (W6SEG \div 2) \\ cX \times WSEG + 11 \times (W6SEG \div 2) \\ cX \times WSEG + 12 \times (W6SEG \div 2) \end{bmatrix}$; $\vec{Y} \leftarrow \begin{bmatrix} cY \times HSEG \\ (cY + \frac{1}{2}) \times HSEG \\ (cY + 1) \times HSEG \end{bmatrix}$

if $\vec{Y}[0] = 0 \vee \vec{Y}[0] = TEY$ **then** ▷ Determines if SCS has external power

SCS[cY, cX].power = True

else

SCS[cY, cX].power = False

end if

if $\vec{X}[0] = prbX \wedge \vec{X}[2] = prbX \wedge \vec{Y}[0] \leqslant (prbY + 15) \wedge \vec{Y}[0] \geqslant (prbY - 15)$ **then**

SCS[cY, cX].probe = True

else

SCS[cY, cX].probe = False

end if

end for

end for

IV

Substrate thinning analysis 2023-10-11 17:01:33+02:00

chap:4thinning

Contents

4.1	Summary <small>2023-10-11 17:01:21+02:00</small>	52
4.2	Introduction <small>2023-10-11 17:01:21+02:00</small>	52
4.3	Geometric and electrical modeling <small>2023-10-11 17:01:21+02:00</small>	53
4.3.1	Geometric modeling <small>2023-10-11 17:01:21+02:00</small>	53
4.3.2	Electrical approach <small>2023-10-11 17:01:21+02:00</small>	56
4.4	Models validation <small>2023-10-11 17:01:21+02:00</small>	58
4.4.1	IC substrate thinning quick look <small>2023-10-11 17:01:21+02:00</small>	58
4.4.2	Experiments with thinned circuits <small>2023-10-11 17:01:21+02:00</small>	59
4.5	Conclusion <small>2023-10-11 17:01:21+02:00</small>	60

4.1 Summary 2023-10-11 17:01:33+02:00

This chapter proposes to study the interests of thinning the substrate of integrated circuits with the aim to enhance Body Biasing Injection efficiency. First, we are going to present a geometrical approach in order to appreciate with a certain abstraction from electronics the effects of substrate thinning on ICs behaviors. Second, thanks to the models presented in Chapter 3, in addition to the geometrical approach, we are going to theoretically analyze the effects of substrate thinning from an electrical point of view. Eventually, in order to verify the soundness of the geometric approach and the simulation results, experiments are going to be studied thanks to an actual analysis of substrate thinning on identical IC targets behavior.

4.2 Introduction 2023-10-11 17:01:33+02:00

When working with integrated circuits in a fault injection context, several physical parameters of the considered IC are of great importance. For example, as we have seen in the previous Chapter, the type of substrate used to manufacture the IC has a significant impact on BBI efficiency and behavior. In addition to this, the transistors' size, power supply voltage, the IC package or the IC substrate thickness can drastically change fault injections results. Among these examples, one of great interest for body biasing injection is the substrate thickness.

Indeed, as there are different manufacturing processes depending on the purpose of each manufactured IC, it is common to find various substrate thicknesses depending on the IC targeted application. On one hand, it is not rare to find 700 μm thick wafers with 300 mm diameters for generic applications. On the other hand, in other specific applications like SoCs, where vertical stacking is commonly used, or in Smart-cards and ID cards, the typical substrate thickness value is lower, around 200 μm . In addition to these differences one can find in commercial products, the practice of thinning the substrate of ICs is not uncommon in a context of fault injection. More specifically, substrate thinning has been thoroughly studied concerning Laser Fault Injection (LFI) [32, 33], and has proven to greatly enhance LFI efficiency, in addition to drastically reducing the power required to create faults. However, it had not been studied for Body Biasing Injection at the beginning of this work.

In this context, this work was first done in order to assess whether substrate thinning has similar effects on BBI as it has on LFI. Second, because thin ICs commonly found in smart-cards have unavoidable security constraints, third because BBI is performed using the silicon substrate as the physical environment to carry energy through electrical charges. Therefore, this Chapter will evaluate the interests of substrate thinning on BBI efficiency. In other words, we will analyze the electrical and behavioral differences between identical ICs with different substrate thicknesses. This analysis will take place using multiple approaches. In the first place, we will address the question using a geometric approach to appreciate the effects of substrate

thinning on voltage propagation inside the substrate while taking a step back from electrical modeling. Then, the geometric approach will be completed with an electrical simulation analysis of two identical ICs with different substrate thicknesses, created thanks to the models proposed in Chapter 3. Eventually, experimental results will be analyzed in order to verify the correctness of the previous approaches, in addition to studying the actual effects of substrate thinning concerning faults creation.

4.3 Geometric and electrical modeling 2023-10-11 17:01:33+02:00

chap4 : sect : geomModel

To begin with, we will address the geometric approach. It has been chosen thanks to the advantages it brings forward, such as the abstraction from electronics it enables, thus allowing easier and faster modeling. However, because this approach alone is insufficient, we will then study an analogous electrical one.

4.3.1 Geometric modeling 2023-10-11 17:01:33+02:00

chap4 : sect : geomModel : subsect : geomModel

For the purpose of geometric modeling, let us consider two identical ICs. A commercial one, with an arbitrary standard substrate thickness, and another one with its substrate thinned by a certain amount in order to perform fault injection. Fig. 4.1 illustrates the two-dimensional cross-sectional views of the considered ICs substrates during an arbitrary BBI voltage pulse. The silicon substrate being an isotropic resistive environment, it is quite natural to expect the electrical charges to flow and spread evenly when injected into it at any given time. Therefore, equipotentials form half-sphere surfaces inside the substrate volume. These surfaces are highlighted in two-dimensions as green half-circles in Fig. 4.1.

In this scenario, an attacker wants to induce a fault in the logic gates, located at the top of each IC. To that end, they need to change the voltage enough at point P , called V_P , in order to disturb the transistors and change the logic gates behavior. In addition to that, and for the sake of simplicity, let us assume that P is the only location in the considered IC where faults can be injected. However, in order to observe faults at point P , V_P needs to reach a minimal threshold voltage, called V_F . Because the attacker is working with BBI, a metallic probe is connected onto the backside of the IC, at point P_U , in order to inject energy into the IC. Depending on the amount of injected energy, in other words, the maximum amplitude of the voltage pulse because the substrate effective resistance is static, the voltage at P might never reach V_F , therefore, no faults will be observed. Let us consider that the attacker chose an amplitude V_{PU} big enough such that at a moment in the injection, V_P reaches V_F or more in each considered IC. In that scenario, the area on the IC front side where $V > V_F$ is a disk of radius ϕ , centered in P , called the BBI susceptibility area radius. It means that the attacker can position the probe anywhere on the backside within this disk to reach V_F at P , and therefore induce a fault at P .

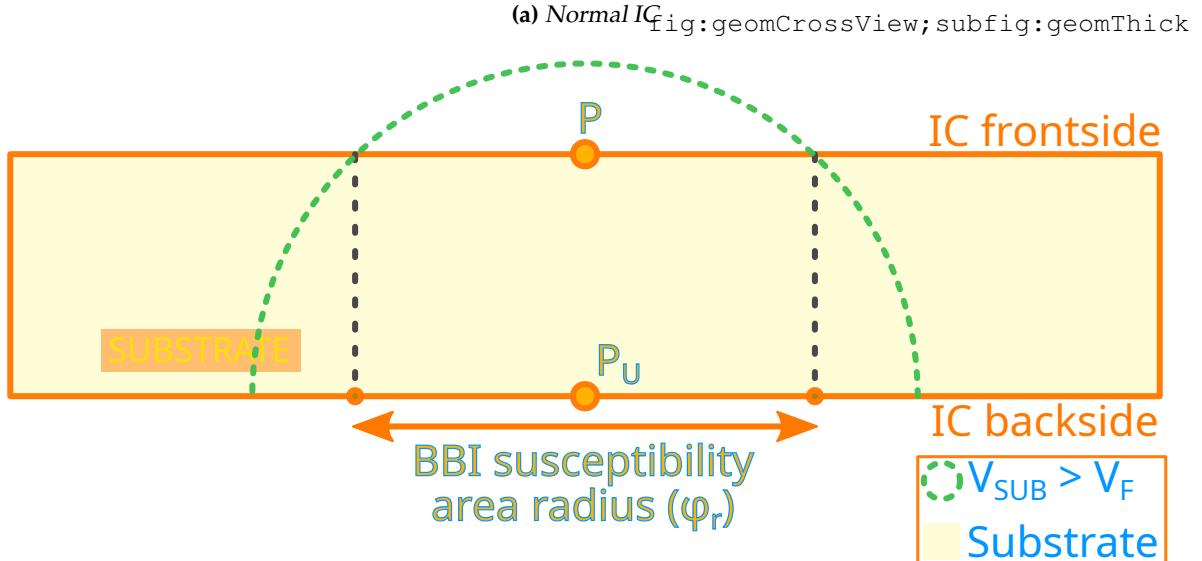
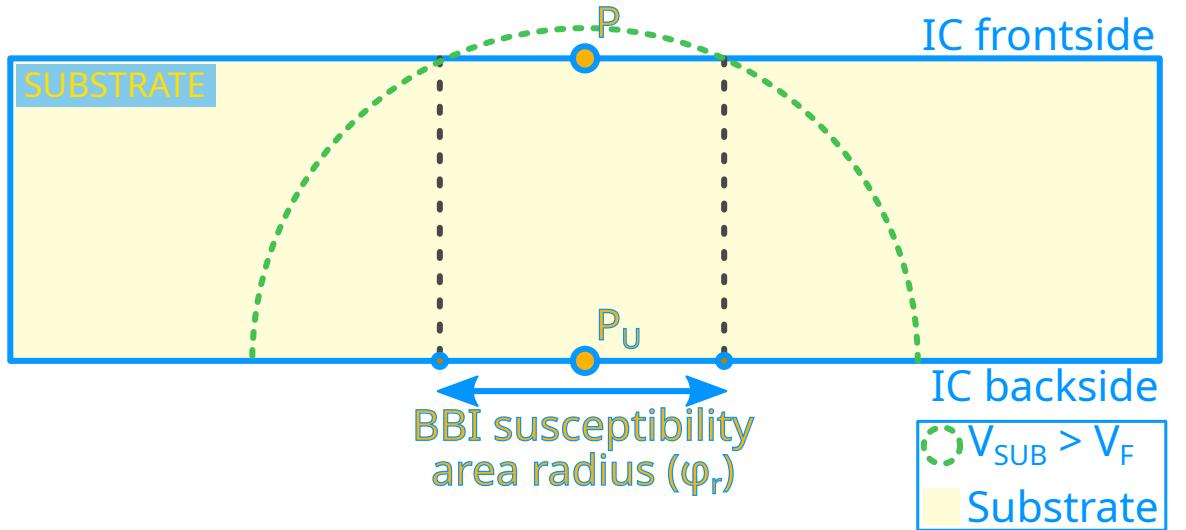


Figure 4.1: BBI susceptibility area cross-sectional 2D view fig:geomCrossView

The half-sphere equipotential radius relative to time can be determined thanks to the following formula:

$$r(t) = \frac{\rho_{SUB}}{\sqrt{2}} \cdot \frac{|I_G(t)|}{|V_{PU}(t) + V_F|} \quad (4.1)$$

with ρ_{SUB} the resistivity of the silicon substrate, $I_G(t)$ the instantaneous sum of the current distribution contained in the half-sphere, and $V_{PU}(t)$ the instantaneous voltage pulse applied on the backside of the IC. Then, logically, the BBI susceptibility area radius, denoted ϕ_r , is described by:

$$\phi_r(t) = 2 \cdot \sqrt{r(t)^2 - t_{SUB}^2} \quad (4.2)$$

with t_{SUB} being the IC substrate thickness.

As it is illustrated in Fig. 4.1, thinning the substrate inevitably increases the size of the susceptibility area if the experimental conditions are constant. It means that the susceptibility

evolution ratio is always greater than 1 when thinning the substrate:

$$\frac{\phi_r^{THIN}}{\phi_r^{THICK}} = \sqrt{\frac{r^2 - t_{THIN}^2}{r^2 - t_{THICK}^2}} > 1 \quad (4.3)$$

Therefore, in order to obtain the same susceptibility area with a thinner IC, it is required to reduce the voltage pulse amplitude, thanks to the following relation:

$$V_{PU}^* = \frac{t_{THIN}}{t_{THICK}} \cdot V_{PU} + V_F \cdot \left(1 - \frac{d_{gap4:\text{sect:geomModel:eqnVpu*}}}{t_{THICK}}\right) \quad (4.4)$$

Eventually, this geometrical approach allows deducing three conclusions:

1. Thinning the substrate allows reducing the minimal voltage pulse amplitude required to induce a fault while keeping a constant susceptibility area.
2. The BBI susceptibility area increases while the substrate thickness decreases while working at a constant voltage pulse V_{PU} .
3. Thinning the substrate alone does not have an influence on BBI spatial resolution, as the susceptibility area depends on the couple (t_{SUB}, V_{PU}) . Thus, similar spatial resolution could be obtained with different substrate thicknesses by changing V_{PU} .

4.3.2 Electrical approach 2023-10-11 17:01:33+02:00

chap4:sect:geomModel:subsect:elecApproach

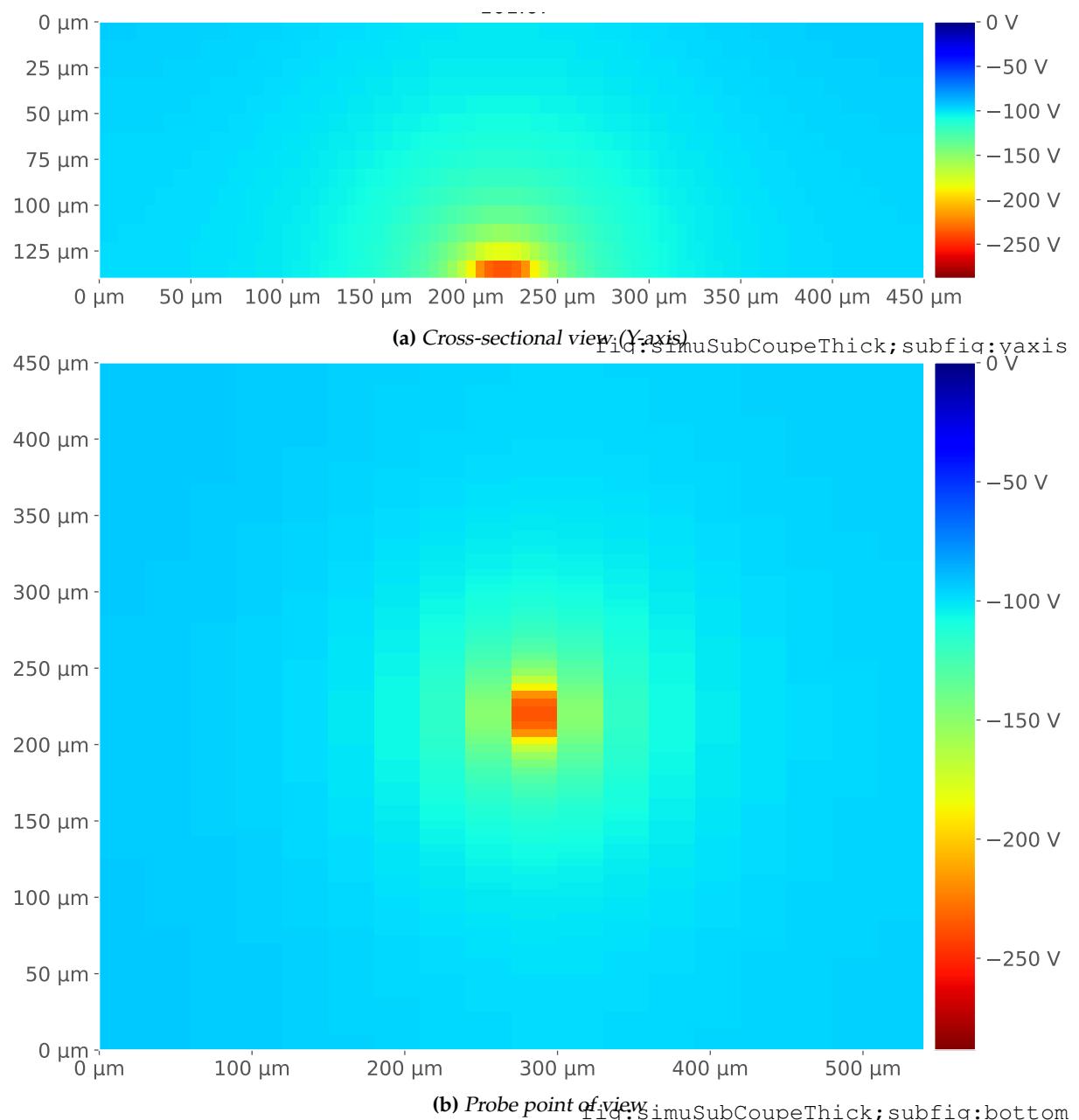


Figure 4.2: Simulated non-thinned IC (140 μm) substrate voltage distribution: peak of the first voltage pulse edge

fig:simuSubCoupeThick

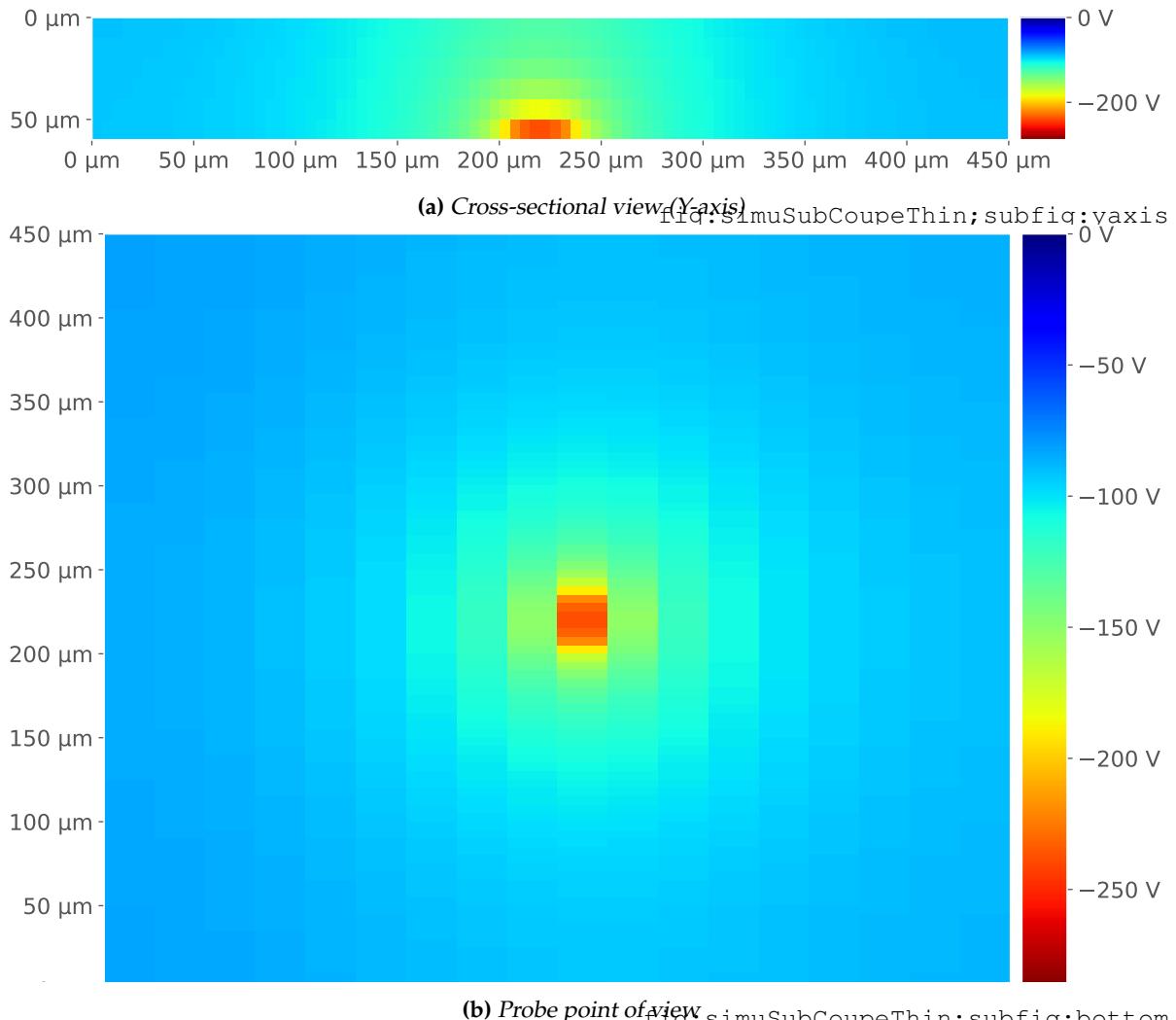


Figure 4.3: Simulated thinned IC (60 μm) substrate voltage distribution: peak of the first voltage pulse edge
fig: simuSubCoupeThin

As stated previously, in order to verify the meaningfulness of the geometrical approach, we will complete it with an electrical modeling approach. For this purpose, the models introduced in Chapter 3 are reused. The electrical approach consists in generating ICs with different substrate thicknesses and simulating them during BBI. The considered ICs are 550 μm wide and 450 μm deep. Two substrate thicknesses are analyzed, 60 μm and 140 μm . The simulation parameters are the following:

- Triple-well substrate
- Required voltage pulse: -300 V
- Required pulse width: 20 ns
- Required rise and fall times: 8 ns

Fig. 4.2 and Fig. 4.3 show, for each simulated IC, the voltage bias across the substrate through different point of view at the apex of the voltage pulse first edge. For simplicity, results

are shown in two dimensions and from two point of views: a cross-sectional view and a bottom view. The first interesting thing to note is that, as predicted thanks to the geometric model and as shown in Fig. 4.2 and 4.3, equipotentials effectively form half-circles into the substrate (half-spheres in 3D). They can be first observed from the bottom, where the voltage is spreading across the backside surface of the IC. Second, in the cross-sectional view, as it was illustrated previously with the geometrical model..... **IL Y A BEAUCOUP DE CHOSES À DIRE MAIS JE MANQUE D'INSPIRATION POUR CETTE PARTIE, JE REVIENDRAI PLUS TARD DESSUS.**

4.4 Models validation 2023-10-11 17:01:33+02:00

chap4:sect:modelValid

This section presents the conducted experiments allowing to validate the previously presented models.

4.4.1 IC substrate thinning quick look 2023-10-11 17:01:33+02:00

chap4:sect:modelValid:subsect:thinQuick

As substrate thinning is quite widespread when performing fault injection, let us have a quick look on how it is performed. Commonly, It is done using Selected Area Preparation (SAP) or Focused Ion Beams (FIB) milling. SAP milling consists in a very precise mechanical milling tool, generally able to remove material with a precision down to a few micrometers. However, it can often lead to uneven surfaces. FIB milling consists in a physical milling which does not imply a mechanical contact with the material to be removed, and allows nanometer-level precision. For that purpose, FIB is commonly used in combination with SAP [34] to produce even substrate surfaces. In addition to substrate thinning, SAP milling machines allow removing the plastic package and eventual internal metallic heat-sinks of ICs prior to substrate thinning. It has the advantage of providing low damage to thinned ICs, thanks to low spindle speed and low temperature rise compared to traditional high speed milling.

4.4.2 Experiments with thinned circuits 2023-10-11 17:01:33+02:00

chap4:sect:modelValid:subsect:XPthinning

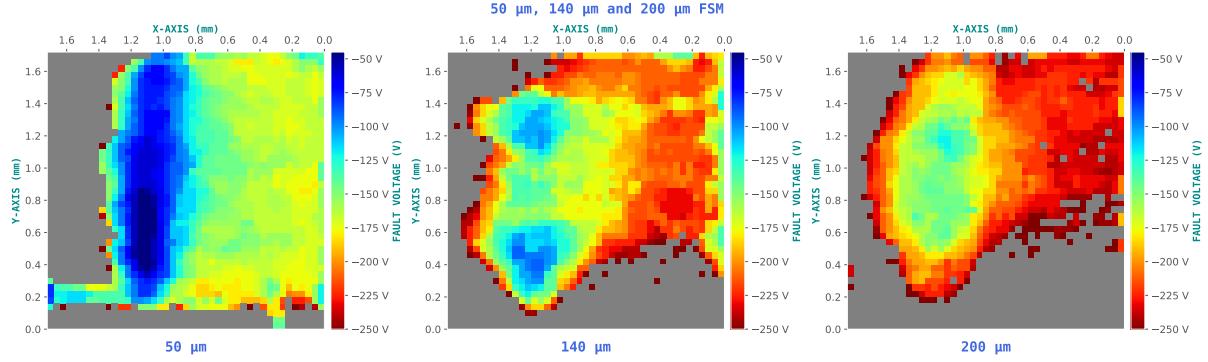


Figure 4.4: Fault susceptibility maps

fig:fsml

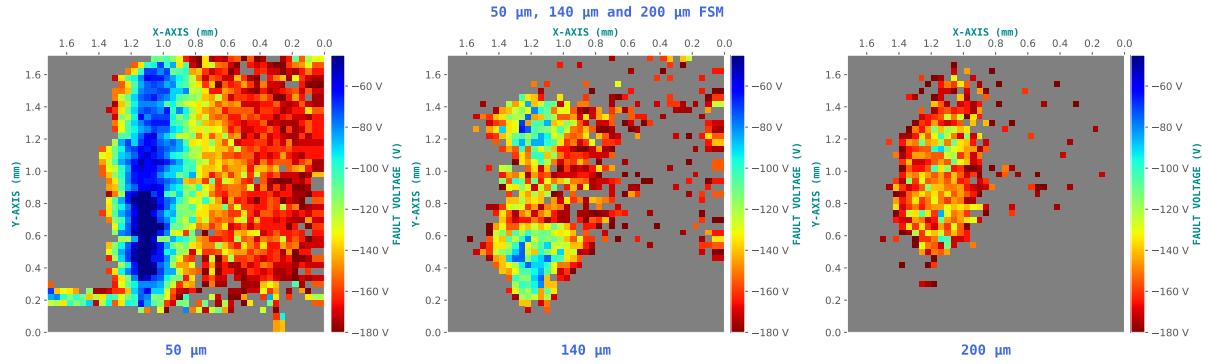


Figure 4.5: Susceptibility area spreading

fig:fsmlspread

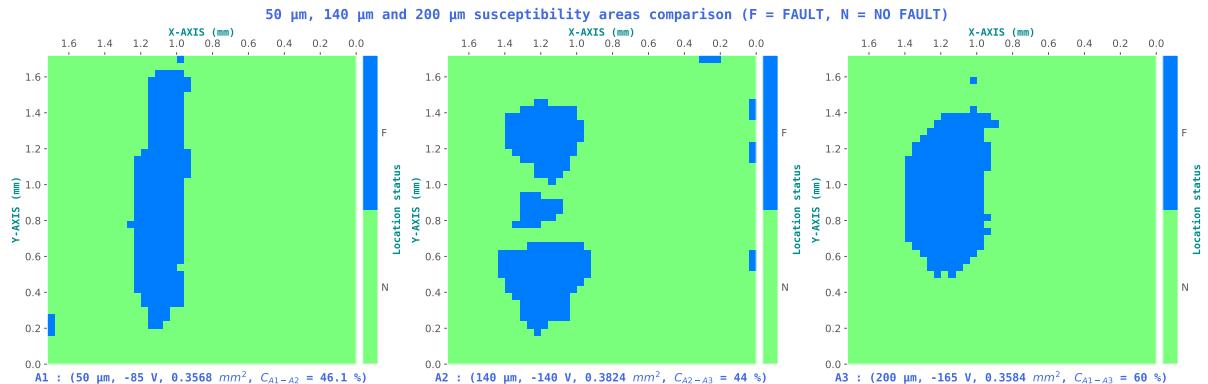


Figure 4.6: Fault susceptibility maps couples

fig:fsmlcouple

With geometric and electrical modeling complete, it is now possible to conduct actual experiments in order to verify the meaningfulness of the previous approaches. In this context, three identical targets were thinned to three different levels, from 750 μm to respectively 200 μm , 140 μm and 50 μm , respectively named ST200, ST140 and ST50 for the rest of this Chapter. In order to verify the three conclusions extracted from the modeling section, three experiments are conducted for each target.

The first experiment aims at measuring the minimal voltage pulse amplitude V_{PU}^{MIN} re-

quired to induce a faulty behavior on an IC performing computations. These experiments are called Fault Susceptibility Maps (FSM). They allow spotting the region where the IC is sensitive to BBI, no matter which type of induced fault. Therefore, when mapping an entire IC, it is common to spot various areas not directly involved in the targeted calculation, like the analog voltage regulator or the FLASH memory logic control logic not to cite them all. As a result, and because in a fault injection context the cryptographic core is very often targeted, it was decided to focus the maps above the STM32 AES core only. Fig. 4.4 presents the three performed FSM. From left to right, t_{SUB} goes from 50 μm , then to 140 μm , finally to 200 μm . As stated before, the maps are performed above the hardware AES core of the IC, temporally aiming the penultimate AES round. The scanned area measures 1.7 mm by 1.7 mm, with a displacement step of 40 μm between each point. V_{PU} was limited to the following range: [30 V ; 280 V], with 5 V steps and a negative polarity. The pulse width was fixed at 6 ns. The first important thing to note here is that, as predicted with the geometric and electrical modelings, a thinner substrate allows a lower fault induction threshold. It is mainly shown thanks to the measurement of the average voltage required to induce a fault across the entire map, annotated at the top of each map. All of this sustains the first conclusion made in section 4.3.

Then, the second experiment, whose results are shown in Fig. 4.5, consist in analyzing the spreading of the BBI susceptibility area. The core of the experiment is identical as before. However, in order to highlight the spreading effect, it was required to set a lower maximum voltage amplitude (in absolute value). The value of 180 V was chosen as it is the average voltage of the medium-thinned IC. What is interesting here is that, for the ST200 target, because the voltage at the epitaxy level cannot reach the threshold value V_F in most cases, the fault area is tiny compared to the other targets, and focused on the AES core. Then, concerning the ST140 target, thanks to the thinner substrate, the voltage at the epitaxy level can reach a higher value, and thus can cause more logic gates or further logic gates from the probe to have a faulty behavior. Eventually, the ST50 target shows the largest fault area. These experiments help to sustain the second conclusion of section 4.3.

Eventually, the last experiment consisted in finding, whenever possible, (t_{SUB}, V_{PU}) couples for which the susceptibility area is identical across all targets. The search for the couples of values was done by first choosing an arbitrary couple for ST200 target, and then calculating the correlation for each couple between the other two susceptibility areas and finding the highest correlation. Then, to confront the geometric modeling predictions, we calculated, thanks to equation 4.4, couples corresponding to

4.5 Conclusion 2023-10-11 17:01:33+02:00

This chapter introduced the interest of thinning the substrate of integrated circuits on Body Biasing Injection efficiency. In the first place, we studied thanks to a geometrical approach the potential benefits of this practice, further completed with electrical simulations. The geomet-

ric approach brought mathematical relations allowing to evaluate preliminary the effects of thinning the substrate of a target IC.

À FINIR.

V

Fault model 2023-10-11 17:01:33+02:00

chap:5faultModel

Contents

5.1	Summary <small>2023-10-11 17:01:21+02:00</small>	64
5.2	Introduction <small>2023-10-11 17:01:21+02:00</small>	64
5.3	Charge extortion <small>2023-10-11 17:01:21+02:00</small>	64
5.3.1	Sequential logic operation and simple fault model <small>2023-10-11 17:01:21+02:00</small>	65
5.4	Silicon substrate charges propagation <small>2023-10-11 17:01:21+02:00</small>	65
5.5	Logic gates simulation under BBI <small>2023-10-11 17:01:21+02:00</small>	65

5.1 Summary 2023-10-11 17:01:33+02:00

chap5:sect:summary

In this chapter, we present a fault model for BBI, extrapolated from a fault model used for EMFI. The objective of this chapter is to provide an explanation of the mechanisms and causes of faults in integrated circuits that are subjected to body biasing injection. Electrical models presented in the chapter 3 can be used to explain how electrical charge displacement in the IC during a BBI pulse allows changing some logic gates output values. Targeting an IC via BBI forces electric charges to be injected (resp. absorbed) with positive pulses (resp. negative). Therefore, it is possible to target a critical time in the IC calculation thanks to the ability to finely control the induced disturbances. Eventually, to verify the correctness of the proposed analysis, both substrate charge propagation and logic gate behavior studies will be conducted in parallel.

5.2 Introduction 2023-10-11 17:01:33+02:00

chap5:sect:intro

To further complete the understanding of BBI, in addition to having a reliable model to predict IC behavior, it is of great importance of having a precise fault model, in order to be able to set up countermeasures. Indeed, the main objective of studying fault injection techniques is to protect further secured ICs in order to consider during the design of new ICs, the implications and impacts of such countermeasures on the design. As it has been said in Chapter 3, simulating at a transistor level an entire IC is unrealistic, at least computationally speaking. Therefore, and because the previous models do not represent the logical functions of the considered ICs, we propose an additional step to the simulation workflow proposed in Chapter 3. This addition consists in extracting the propagated disturbances from standard-cell segments models, and injecting them into functioning logic gates. This method allows appreciating logic gates behavior under BBI in order to get a deeper and more precise understanding of both electrical and functional fault creation mechanisms. All of this is part of the required steps to set up efficient countermeasures, as we need to understand precisely the insights of fault creation.

5.3 Charge extortion 2023-10-11 17:01:33+02:00

chap5:sect:chargeExtortion

This section explains the charge extortion mechanism at work during BBI which allows fault creation. The voltage pulse generator, at each edge of its pulse, injects and then extorts electrical charges into and out of the IC.

5.3.1 Sequential logic operation and simple fault model 2023-10-11 17:01:33+02:00

chap5:sect:chargeExtortion:subsect:seqLogic

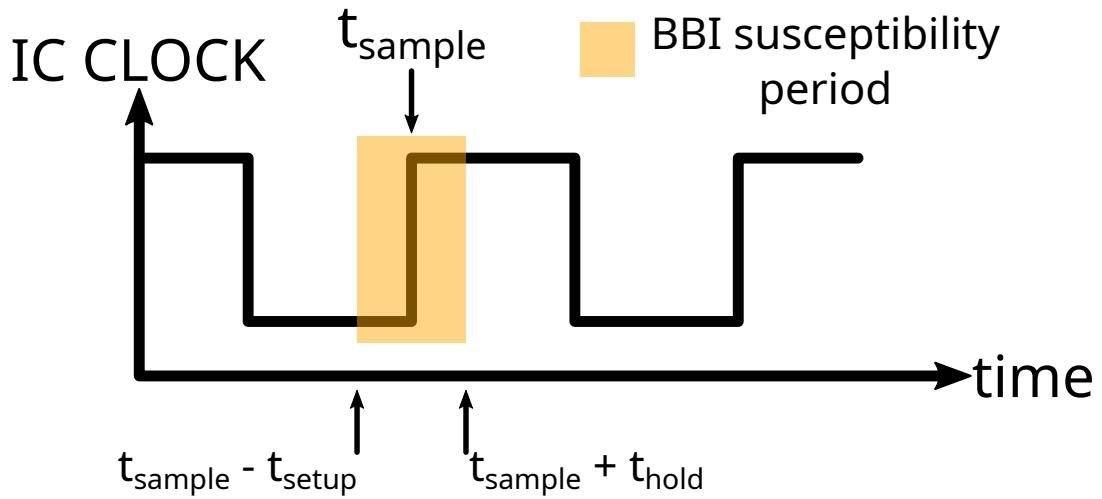


Figure 5.1: Sequential logic operation and BBI sampling fault susceptibility
chap5:fig:bbisusc

As sequential logic is ubiquitous in contemporary integrated circuits, we shall examine its fundamental workings in greater detail. Sequential logic relies on a core element: the edge-triggered D flip-flop (DFF). They are a memory component that is governed by a clock. At each rising-edge or falling-edge (depending on the design) of the clock, DFFs sample their input and replicate it at their output. Between DFFs are placed the logic gates, which fulfill a specific logical function. Because of this, values in sequential logic circuits can only be changed at the clock edges. Hence, in the event that an adversary is able to alter a logical value for an extended period of time at the input of a DFF, the subsequent combinatorial logic will yield an incorrect value, which will propagate to the subsequent DFFs.

We are going to use this fault model, depicted in short in Fig. 5.1, for the rest of this chapter. It is important to note that this model was first introduced for EMFI [35].

5.4 Silicon substrate charges propagation 2023-10-11 17:01:33+02:00

chap5:sect:subEpiCurr

On a déjà montré ces cartes dans des parties précédentes.

5.5 Logic gates simulation under BBI 2023-10-11 17:01:33+02:00

chap5:sect:simuLogic

VI

Conclusion

chap:6conclusion

Bibliography

- [1] Colin O’Flynn. Low-cost body biasing injection (BBI) attacks on WLCSP devices. In Pierre-Yvan Liardet and Nele Mentens, editors, *Smart Card Research and Advanced Applications*, pages 166–180, Cham, 2021. Springer International Publishing. ix, 9, 14, 15
- [2] G. Chancel, J.-M. Galliere, and P. Maurine. Body biasing injection: To thin or not to thin the substrate? In Josep Balasch and Colin O’Flynn, editors, *Constructive Side-Channel Analysis and Secure Design*, pages 125–139, Cham, 2022. Springer International Publishing. xvii, 38
- [3] Prasanna Ravi, Zakaria Najm, Shivam Bhasin, Mustafa Khairallah, Sourav Sen Gupta, and Anupam Chattopadhyay. Security is an architectural design constraint. *Microprocessors and Microsystems*, 68:17–27, 2019. 2
- [4] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO ’96*, pages 104–113, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg. 5
- [5] A. Shamir R.L. Rivest and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In *Communications of the ACM*, volume 21, pages 120–126, 1978. 5
- [6] Boris Köpf and Markus Dürmuth. A provably secure and efficient countermeasure against timing attacks. In *2009 22nd IEEE Computer Security Foundations Symposium*, pages 324–335, 2009. 5
- [7] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO’ 99*, pages 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg. 5
- [8] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 16–29, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg. 6
- [9] Vincent Carlier, Hervé Chabanne, Emmanuelle Dottax, and Hervé Pelletier. Electromagnetic side channels of an fpga implementation of aes. *Cryptology ePrint Archive*, Paper 2004/145, 2004. <https://eprint.iacr.org/2004/145>. 6

- [10] Thomas Ordas, Mathieu Lisart, Etienne Sicard, Philippe Maurine, and Lionel Torres. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. In Lars Svensson and José Monteiro, editors, *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, pages 229–236, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. 6
- [11] Aurélien Vasselle, Philippe Maurine, and Maxime 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’19*, page 23–32, New York, NY, USA, 2019. Association for Computing Machinery. 6
- [12] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In *Annual International Cryptology Conference*, 1997. 7
- [13] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Walter Fumy, editor, *Advances in Cryptology — EUROCRYPT ’97*, pages 37–51, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg. 7
- [14] Mathieu Ciet and Marc Joye. Elliptic curve cryptosystems in the presence of permanent and transient faults. *Designs, Codes and Cryptography*, 36(1):33–43, July 2005. 7
- [15] Ingrid Biehl, Bernd Meyer, and Volker Müller. Differential fault attacks on elliptic curve cryptosystems. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 131–146, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg. 7
- [16] Christophe Giraud. Dfa on aes. In Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors, *Advanced Encryption Standard – AES*, pages 27–41, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. 7, 30, 31
- [17] Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta. Fault sensitivity analysis. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010*, pages 320–334, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. 7
- [18] Sergei Skorobogatov and Ross Anderson. Optical fault induction attacks. volume 2523, pages 2–12, 08 2002. 8
- [19] David Samyde, Sergei P. Skorobogatov, Ross J. Anderson, and Jean-Jacques Quisquater. On a new way to read data from memory. *First International IEEE Security in Storage Workshop, 2002. Proceedings.*, pages 65–69, 2002. 9
- [20] M. Lisart M. Dumont and P. Maurine. Modeling and simulating electromagnetic fault injection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(4):680–693, 2021. x, 9, 38, 39, 42, 43
- [21] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre-Yvan Liardet. Yet another fault injection technique : by forward body biasing injection. 09 2012. 9, 14

- [22] K. Tobich, P. Maurine, P.-Y. Liardet, M. Lisart, and T. Ordas. Voltage spikes on the substrate to obtain timing faults. In *2013 Euromicro Conference on Digital System Design*, pages 483–486, 2013. 9, 14
- [23] Noemie Beringuier-Boher, Marc Lacruche, David El-Baze, Jean-Max Dutertre, Jean-Baptiste Rigaud, and Philippe Maurine. Body biasing injection attacks in practice. In *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems, CS2 '16*, page 49–54, New York, NY, USA, 2016. Association for Computing Machinery. 9, 14
- [24] G. Chancel, Jean-Marc Gallière, and P. Maurine. Body biasing injection: Impact of substrate types on the induced disturbances. In *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 50–60, 2022. 13, 38
- [25] Colin O'Flynn. Picoemp: A low-cost emfi platform compared to bbi and voltage fault injection using tdc and external vcc measurements. Cryptology ePrint Archive, Paper 2023/1195, 2023. <https://eprint.iacr.org/2023/1195>. 19
- [26] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against spn structures, with application to the aes and khazad. In Colin D. Walter, Çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003*, pages 77–88, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. 30
- [27] C. Sanchez-Avila and R. Sanchez-Reillo. The rijndael block cipher (aes proposal) : a comparison with des. In *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186)*, pages 229–234, 2001. 31
- [28] Mathieu Dumont, Philippe Maurine, and Mathieu Lisart. Modeling of electromagnetic fault injection. In *2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, pages 246–248, 2019. 38
- [29] Yasuhiro Ogasahara, Masanori Hashimoto, Toshiki Kanamoto, and Takao Onoye. Supply noise suppression by triple-well structure. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 21(4):781–785, 2013.
- [30] Takuya Wadatsumi, Kohei Kawai, Rikuu Hasegawa, Takuji Miki, Makoto Nagata, Kikuo Muramatsu, Hiromu Hasegawa, Takuya Sawada, Takahito Fukushima, and Hisashi Kondo. Voltage surges by backside esd impacts on ic chip in flip chip packaging. In *2022 IEEE International Reliability Physics Symposium (IRPS)*, pages P14–1–P14–6, 2022.
- [31] Takuya Wadatsumi, Kohei Kawai, Rikuu Hasegawa, Kazuki Monta, Takuji Miki, and Makoto Nagata. Characterization of backside esd impacts on integrated circuits. In *2023 IEEE International Reliability Physics Symposium (IRPS)*, pages 1–6, 2023.
- [32] Breier et al. Extensive laser fault injection profiling of 65 nm fpga. *J Hardw Syst Secur* 1, pages 237–251, 2017. 52

- [33] Jakub Breier and Chien-Ning Chen. On determining optimal parameters for testing devices against laser fault attacks. In *2016 International Symposium on Integrated Circuits (ISIC)*, pages 1–4, 2016. 52
- [34] C. Boit, R. Schlangen, A. Glowacki, U. Kindereit, T. Kiyan, U. Kerst, T. Lundquist, S. Kasapi, and H. Suzuki. Physical ic debug and - backside approach and nanoscale challenge. *Advances in Radio Science*, 6:265–272, 2008. 58
- [35] S. Ordas, L. Guillaume-Sage, and P. Maurine. Electromagnetic fault injection: the curse of flip-flops. *Journal of Cryptographic Engineering*, 7(3):183–197, Sep 2017. 65