Body biasing injection: analysis, modeling and simulation

Geoffrey Chancel

***Abstract*—This is the abstract.**
Orange text is for undecided wording/words.
Red text is for important messages.
Cyan text is for future bib references to add.

***Index Terms*—Article submission, IEEE, IEEEtran, journal, LaTeX, paper, template, typesetting.**

I. Introduction

A. Context

When working with cybersecurity, specifically with hardware security, various fault injection methods are often considered. One can point out Electromagnetic Fault Injection (EMFI) [1], Laser Fault Injection (LFI) [2], or Body Biasing Injection (BBI) [3], not to cite them all. The current work is dedicated in studying Body Biasing Injection.

Nowadays, electronic devices are found in every economic sector, and very often they manipulate sensitive data, such as in bank transactions, Internet of Things (IoT) devices, or smartphones. To ensure data authenticity, these devices embed cryptographic algorithms. While theoretically secure, once implemented on actual devices, these algorithms become fallible, leaking manipulated data, in addition to being sensitive to external disturbances.

B. Fault injection objectives

Fault injection methods are set up to perform various malicious manipulation on integrated circuits, such as:

- Denial of service (DoS) → Stop circuit operation and the related services;
- Verification bypass → Modify data on the fly to fake authenticity (e.g. to bypass bootloader security);
- Confidential data extraction → Modify data to perform differential fault analysis.

C. BBI in the state-of-the-art

When compared to EMFI, BBI has a smaller state-of-the-art, whether in the amount of scientific papers published or in the amount of industrial platforms proposed. Currently, there are ten main works lingering on BBI [3]–[12]. Each one of them made a unique contribution for a better understanding of BBI.

The first one [3] introduced the technique and presented a Bellcore attack on the targeted IC. Then, one year later, another work [4] further studied the method, followed by a third work three years later [5], introducing an advanced test bench to work and perform attacks with BBI.

Fig. 1. Langer and Riscure BBI probes.

However, there are still unanswered questions, and the current works aims at bringing more answers thanks to previous and new data.

Before introducing the present work, let us eventually analyze the industrial platforms proposed by various manufacturers and introduce our own test platform. We can distinguish three major actors proposing BBI related products:

- Langer EMV-Technik;
- Riscure;
- NewAE Technology.

1) Langer EMV-Technik platform: The German society Langer EMV-Technik proposes an all-in-one and ready-to-use BBI platform composed of two hardware tools:

- A current pulse generator with a metal needle, shown in left in Fig. 1;
- A general controller called "Burst Power Station", combining a power supply, control and monitor tool and a software.

D. BBI interrogations

With all the work in the state-of-the-art in mind, there are still remaining questions unanswered about BBI, such as:

- What is the spatial resolution of BBI?
- What is the time resolution of BBI?
- Is thinning the substrate useful in any way?
- How BBI induced faults occur?
- How to properly model BBI?

II. Body biasing injection platforms modeling

THE objective of this first section is to present the work done concerning electrical modeling of integrated circuits in a BBI context. Developing IC models in that specific case is not an easy task. Indeed, modern digital ICs contains billions of transistors, and even considering microcontrollers where the transistor count is less important, with current technologies, it is impossible to evaluate circuits at a transistor level.

A. The hybrid simulation flow: introduction

To tackle these limitations, we decided to adopt an hybrid approach, combining transistor-less models and local logic gates simulations. This approach is a compromise between accuracy and computational cost/time, and allows simulating relatively big circuits under BBI disturbances.

The resulting simulation flow is divided in three consecutive steps:

- The simulation of an IC under BBI using a transistor-less model, allowing for a purely electrical analysis;
- The extraction of significant disturbed signals from the previous simulation;
- The simulation of functional logic gates under BBI thanks to the previously extracted signals.

The first step allows analyzing IC macro-electrical behavior when subject to BBI, and at a lower computational cost compared to a functional model including transistors and internal transmission lines, even if it could be done in a reasonable time constraint for millions of transistors. Then, by extracting useful signals such as the power delivery and the transistor substrate voltages, we can evaluate what would be the behavior of actual logic gates subject to BBI.

B. The hybrid simulation flow : building the models

Building these models requires a correct understanding on integrated circuits internal structures, such as:

- The power supply network, composed of various stacked metal wires;
- The standard-cells, made of logic gates, and thus transistors, being pre-characterized cells used as building blocks;
- The silicon substrate, which can be of various type depending on the technology.

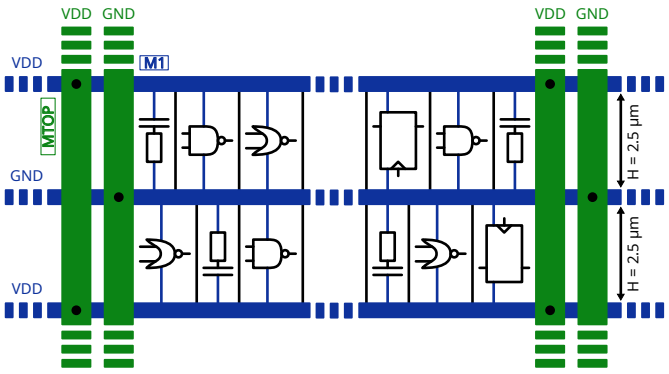

Fig. 2. A Standard-Cell Segment and its power delivery network.

1) Power supply rails and standard-cell segments: The power distribution inside an IC is typically made with a grid-like structure, composed of metal wires stacked on top of each other on planes. The uppermost layer forms a ring surrounding the core. In each layer, the metal wires are equally spaced and have a dedicated width, which becomes thinner the deeper they are. The lowest layer brings the power directly to the transistors.

Within these metal lines are located standard-cell segments (SCS), created by the power planning, as illustrated in Fig. 2. SCS are pre-characterized by foundries and classified according to their performance in timing and power consumption. Their height is fixed, while their width vary depending on their complexity, and are commonly made of logic gates, sequential, and decoupling elements.

2) Silicon substrate structure: Another important element of an IC is the substrate, and most importantly its type. We can mainly distinguish bulk and FD-SOI substrates.

On the one hand, in bulk substrates, the transistor channel forms directly inside the P-substrate, and the depletion layer thickness is difficult to control. On the other hand, in FD-SOI substrates, a silicon oxide layer is created between the channel and the P-substrate, thus constraining the channel thickness.

In this paper, we are focusing only on bulk substrates, and in this family, we can distinguish two substrate types: dual-well (DW) and triple-well (TW). The main difference between DW and TW substrates lies in how are lithographed NMOS transistors. In DW substrates, NMOS are located directly inside the P-doped substrate, and PMOS inside a N-doped well, called the N-well. However, in the case of a TW substrate, the PMOS are still inside the N-well, but the NMOS are located inside an additional P-doped well, made inside the N-well.

These manufacturing differences are illustrated in Fig. 3, representing the cross-sectional view of an inverter made with a bulk technology. The PN and NP diodes formed between the substrate and the wells are represented, and the electrical resistances R_C represent the access resistance of the substrate and the wells.

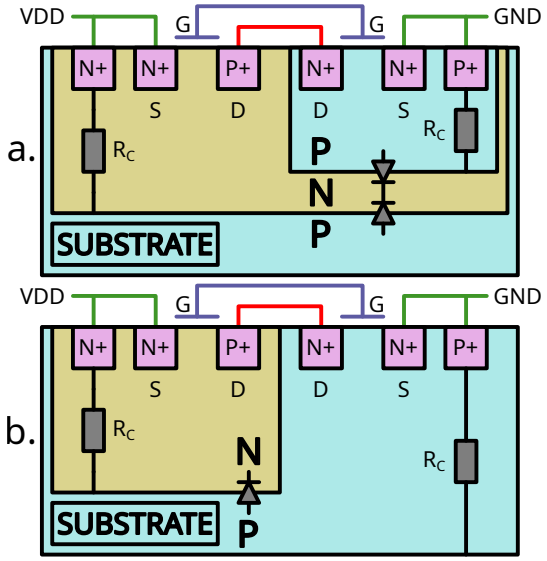

Fig. 3. Triple-well (a.) and Dual-well (b.) inverter cross-sectional view.

Dual-well substrates are found in moderately old ICs, while triple-well ones are common in more recent ICs, often coupled with dual-well substrate on the same die. The combination of both allows for cross-coupling noise reduction, in addition to electrical insulation between transistors located on different domains (DW and TW).

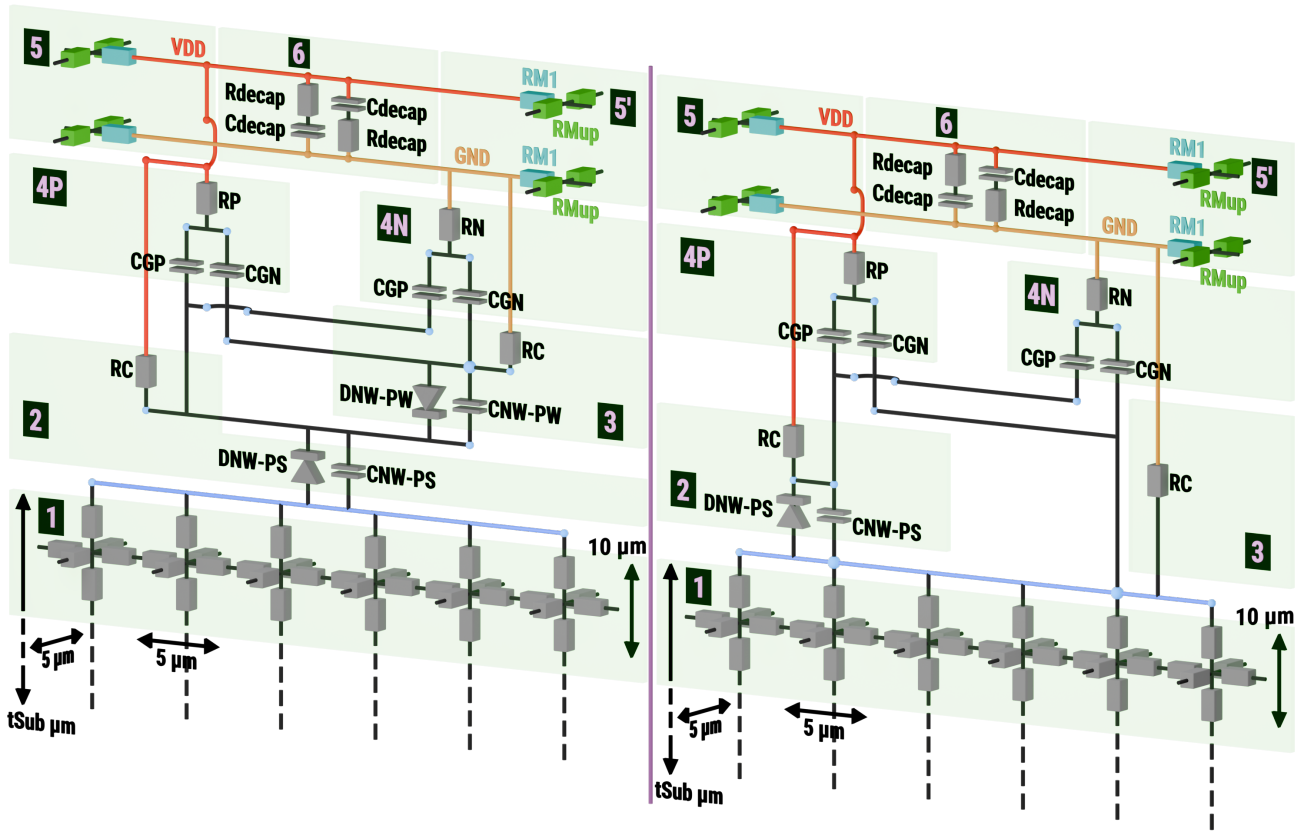

Fig. 4. Triple well (left) and dual well (right) std cell (PEUT ETRE FAIRE DES SOUS-FIGURES)

3) Designing an elementary building-block for mass simulation: Thanks to the previously analyzed elements and models, we can now design elementary standard-cell blocks composed of the power delivery, the logic gates and the substrate, for each substrate type. As it has been said before, we are developing an hybrid simulation flow, therefore the designed elementary block is transistor-less. Eventually, our work is based on previous works on the subject [mathieuEMFI, FDTC2022, FDTC2023].

The model we propose is shown in Fig. II-B3 both for a triple-well and a dual-well substrate. The models are extremely similar, but their difference is what is important. It represents an entire standard-cell segment, including a two levels power delivery network, average models of a hundred of logic gates, silicon junctions, and the silicon substrate. For better clarity, we divided the model into 6 sections, each representing a specific building block:

- 1 The substrate: modeled with 6 blocks of 6 resistors;
- 2 The P-N substrate-well silicon junction;
- 3 The N-P well-well silicon junction (TW), or the substrate access resistance (DW);
- 4N 4P The MOS average electrical model;
- 5 5' The power distribution metals;
- 6 The power supply decoupling.

The component values are calculated according to the target technology, in our case 90 nm, and are shown in Table I.

4) Effectively using these building-blocks: Because the SCS models we previously presented do not represent an entire IC, rather a column portion of one, it is needed, to use them, to replicate and interconnect them as much as needed to model an entire IC. All the models were written in the SPICE language, and simulated using HSPICE. Interconnecting each model instance was done using an automated script. It allowed us to reduce human errors by validating the generation process rather than the netlists themselves. Our generation script allows us to set the following parameters:

- The final IC size;
- The BBI probe size and location;
- The substrate thickness;
- The substrate type (TW or DW);
- The backside voltage pulse characteristics.

This flexibility allows us to quickly create various circuits for our simulation needs.

5) Validating the generated circuits: Validating the models requires at least two steps: a DC operating points verification and a transient analysis. We created a 550 µm wide, 450 µm deep and 150 µm thick IC. As the elementary building blocks measure 30 × 5 × 150 µm³, the resulting IC consists of 1620 SCS blocks. The effective power supply $V_{DD} - GND$ measures 1.2 V.

Component	Rmup	RM1	Cdecap	Rdecap	CGP	CGN	ρ_{SUB}	RP	RN	CNW	RC
Description	Metal top Resistance	Metal 1 Resistance	Power Decoupling Capacitance	Power Decoupling Resistance	Equivalent PMOS Gate capacitance	Equivalent NMOS Gate capacitance	Silicon Substrate Resistivity	PMOS Channel Resistance	NMOS Channel Resistance	Wells Diode Capacitance	Substrate/wells Access Resistance
Value	26 Ω	5 Ω	2.25 fF	2 Ω	35.2 fF	25.2 fF	0.01 Ω·m	9.57 Ω	5.3 Ω	20 fF	3.1 kΩ

TABLE I
STANDARD-CELL MODEL PASSIVE COMPONENT VALUES.

Value	Triple-well	Dual-well
I_{GND}	???	???
I_{VDD}	???	???
$\overline{GND}_{drop}$	???	???
$\overline{V}_{DD_{drop}}$	???	???

TABLE II
OP POINT

Concerning the operating point, we should expect an ideal current consumption of 0 A, and power supply voltage drops of 0 V on both power rails. Otherwise, we should /textcol-ororangereconsider the model and check for any errors or bad interconnections. Table II-B5, showing operating points for both triple-well and dual-well ICs, allows us to see that, as it was expected, the model do not consume static energy nor causes voltage drop on the power delivery network.

Now that we have verified the bias point, let us analyze a first transient simulation. The initial conditions are those of the previous operating point, the difference being the presence of a probe connected to the IC backside, and therefore a voltage pulse generator. To that end, the generator is configured as follows:

- Vpulse = -300 V;
- Vpw = 20 ns;
- Rise and fall times of 8 ns.

Then, we will observe various signals in the IC volume from a 2D perspective, for simplicity:

- The power supply voltage distribution (2D-view);
- The epitaxy current distribution (2D-view);
- The substrate voltage distribution centered around the probe (X-view and Y-view);
- The substrate current distribution centered around the probe (X-view and Y-view);
- The per-layer normalized substrate current density, centered around the probe (X-view and Y-view).

The simulations are conducted for both a dual-well and a triple-well IC.

III. HYBRID SIMULATION RESULTS

REFERENCES

[1] 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.

[2] Jean-Max Dutertre, Vincent Beroulle, Philippe Candelier, Stephan De Castro, Louis-Barthelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hély, Regis Leveugle, Paolo Maistri, Giorgio Di Natale, Athanasios Papadimitriou, and Bruno Rouzeyre. Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 1–6, 2018.

[3] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre-Yvan Liardet. Yet another fault injection technique : by forward body biasing injection. *"Yet Another Conference on Cryptography France (2012)"*, 09 2012.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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 2IRPS)*, pages 1–6, 2023.

[9] 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.

[10] G. Chancel, Jean-Marc Gallière, and P. Maurine. Body biasing injection: Impact of substrate types on the induced disturbances$f$. In *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 50–60, 2022.

[11] G. Chancel, J.-M. Galliere, and P. Maurine. A better practice for body biasing injection. In *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 48–59, 2023.

[12] 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.