Body biasing injection: analysis, modeling and simulation (MAX 14 PAGES)

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

WHEN working with cybersecurity, specifically with hardware security, various fault injection methods are often considered. One can point out Electromagnetic Fault Injection (EMFI) [1], [13], 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.

A. 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.

B. 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. `riscure_langer`

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.

C. 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. Modeling and simulating BBI

SIMULATING a fault injection method behavior is an important part in understanding its mechanisms. Whether it is EMFI, LFI or BBI, it allows to predict and understand the underlying phenomena at work to set up reliable experiments. In this paper, we are focusing solely on BBI.

Ideally, we would want to directly observe signals inside integrated circuits, allowing for fine measurements of power supply voltages, logic levels and power current not to cite

every physical quantity. However, embedding sensors into an already existing IC is not possible, and doing so on future IC is costly and takes time to fully implement. In addition to this, we do not have any guarantee that these sensors will not be disturbed too much by the fault injection. Therefore, we have decided to take the following approach:

$$\text{Simulation} \rightarrow \text{Conclusions} \rightarrow \text{Verification}$$

By doing so, we have freed ourselves from hardware limitations. However, other limitations remains. Indeed, modern ICs, even the smallest, embed millions of transistors, and with current technologies, it is impossible to evaluate with simulations entire circuits at a transistor level. Therefore, 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 Overall, it is similar to what has been done for EMFI in [1]. 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.

A. An hybrid simulation flow: building the models

Building the correct models for the simulation flow pass through multiple steps. As the goal of the hybrid flow is to reduce the computational power required to evaluate an IC, it is still important to maintain a certain accuracy concerning the IC physical structure. To do so, the models are designed around actual IC implementations. The main building blocks of the models are the power supply network, the standard-cells, and the substrate structure. In this work, we are only focusing on bulk substrates: specifically dual-well and triple-well substrates.

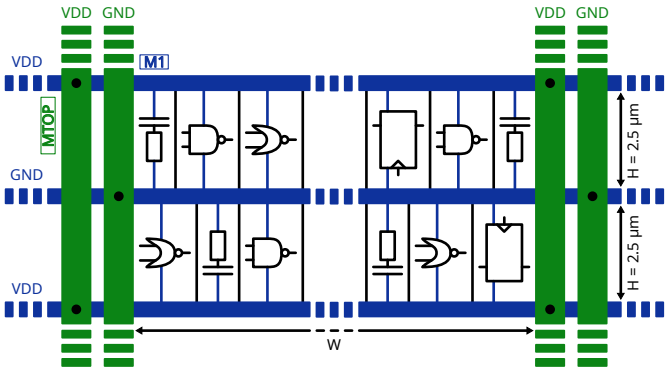

Fig. 2. A Standard-Cell Segment and its power delivery network. fig_alim_std

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. 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. Fig. 2 presents a common power delivery network, designed with two metal levels for simplicity.

Within the metal lines are located standard-cell segments (SCS), composed of decoupling, logic and sequential elements, and are pre-characterized by foundries and categorized depending on their performance (mainly but not exclusively power consumption and speed). As illustrated in Fig. 2, SCS have a constant height, in our case of 2.5 µm, and a variable width depending on how much logic gates each one of them embed. As we have stated previously, the hybrid simulation flow use transistor-less models as basic IC building blocks. Therefore, the transistors, hence the standard-cell segments, are modeled with passive elements such as resistors and capacitors.

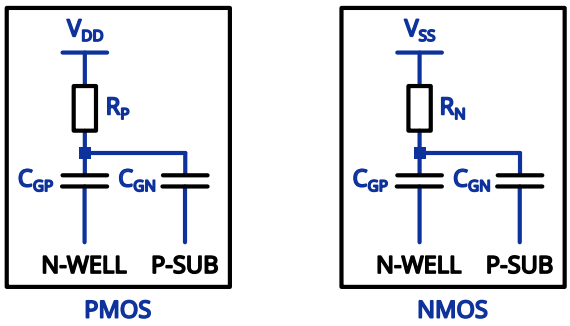

Fig. 3. aaa mos_passive

To that end, the elementary SCS chosen measures 30 µm by 5 µm, representing two rows of logic cells. This represents about a hundred of logic gates, represented with four resistors and two capacitors, as shown in Fig. 3, with half of the transistors conducting, half not conducting. The conducting NMOS transistors, whose source is connected to V_{SS}, are equivalent to the passive resistor R_N. The conducting PMOS transistors, whose source is connected to V_{DD}, are equivalent to the passive resistor R_P. The resistors values depends on the considered technology, as well as the capacitors values, and can be adjusted and calculated according to one needs.

2) The substrate: Because BBI can be performed thanks to the silicon substrate as the main physical environment transferring energy from a generator to an IC, it is fundamental to elaborate a proper substrate model to precisely represent the various involved phenomena. As stated previously, our work focuses on bulk substrates, and in most cases, the substrate silicon is P-doped. There are two typical ways of lithographing the transistors in a bulk substrate, using dual-well or triple-well structures. Dual-well substrates are commonly found in moderately old circuits, while triple-well substrates are found in more recent circuits, while not bleeding-edge.

To properly understand how the differences between dual-well and triple-well substrates change the resulting model, let us analyze the cross-sectional schematics of an inverter created respectively in a triple-well and a dual-well substrate, as shown respectively in Fig. 4.a and Fig. 4.b:

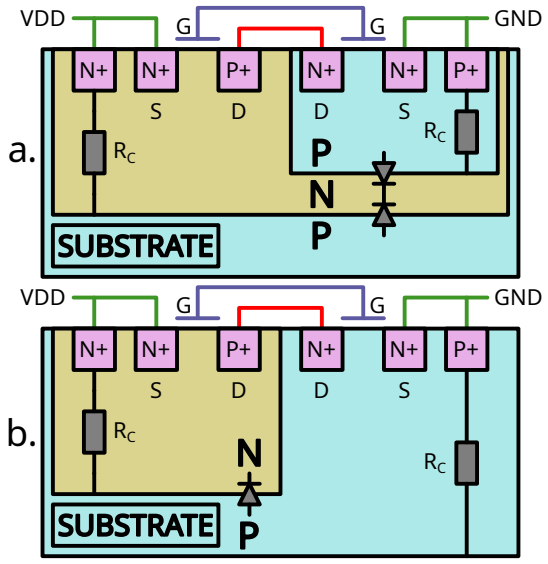

Fig. 4. Triple-well (a.) and Dual-well (b.) inverter cross-sectional view. `fig_sub`

- In the triple-well substrate, the NMOS transistors are lithographed into a P-doped silicon well, itself lithographed inside a N-doped well, buried inside the P-doped substrate. The PMOS transistors are located inside the N-doped well;
- In the dual-well substrate, the PMOS transistors are still located inside the N-doped well, however, the NMOS are lithographed directly inside the P-doped substrate.

On the one hand, the triple-well substrate reveals two diodes:

- One formed between the P-well and the N-well;
- Another formed between the N-well and the P-substrate.

On the other hand, the dual-well substrate only reveals one diode between the N-well and the P-substrate.

3) The resulting model: Thanks to what we have introduced previously, we can now build the elementary building blocks for our hybrid simulation flow. It combines the power delivery network architecture, the equivalent logic gates models, and the substrate structure, all in an embedded model. This model represents an elementary section of the simulated IC, measuring 30 µm by 5 µm by t_{Sub} µm, the latter being the substrate thickness, a parameter which will vary depending on each considered IC.

As we consider both triple-well and dual-well substrate, there are two resulting elementary models, shown in Fig. 5. Each model is composed of various sub-regions, whose descriptions follow:

- 1 is the substrate network, divided into six sub-networks of six resistors for finer details;
- 2 is the first P-N silicon junction, common to both models;
- 3 is the access resistor (DW) or the second junction (TW);
- 4P is the PMOS equivalent section;
- 4N is the NMOS equivalent section;
- 5, 5' are the power supply metal layers (upper metal in green, first level in blue);
- 6 is the power supply decoupling.

As we have stated before, these models only represent a small portion of a simulable IC. To create an entire IC of a defined size, it is required to instantiate and multiply as much as needed the elementary models. By doing so, we can create a bigger model of virtually any size.

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.

[13] 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.

[14] Raphael A. Camponogara Viera, Philippe Maurine, Jean-Max Dutertre, and Rodrigo Possamai Bastos. Simulation and experimental demonstration of the importance of ir-drops during laser fault injection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(6):1231–1244, 2020.

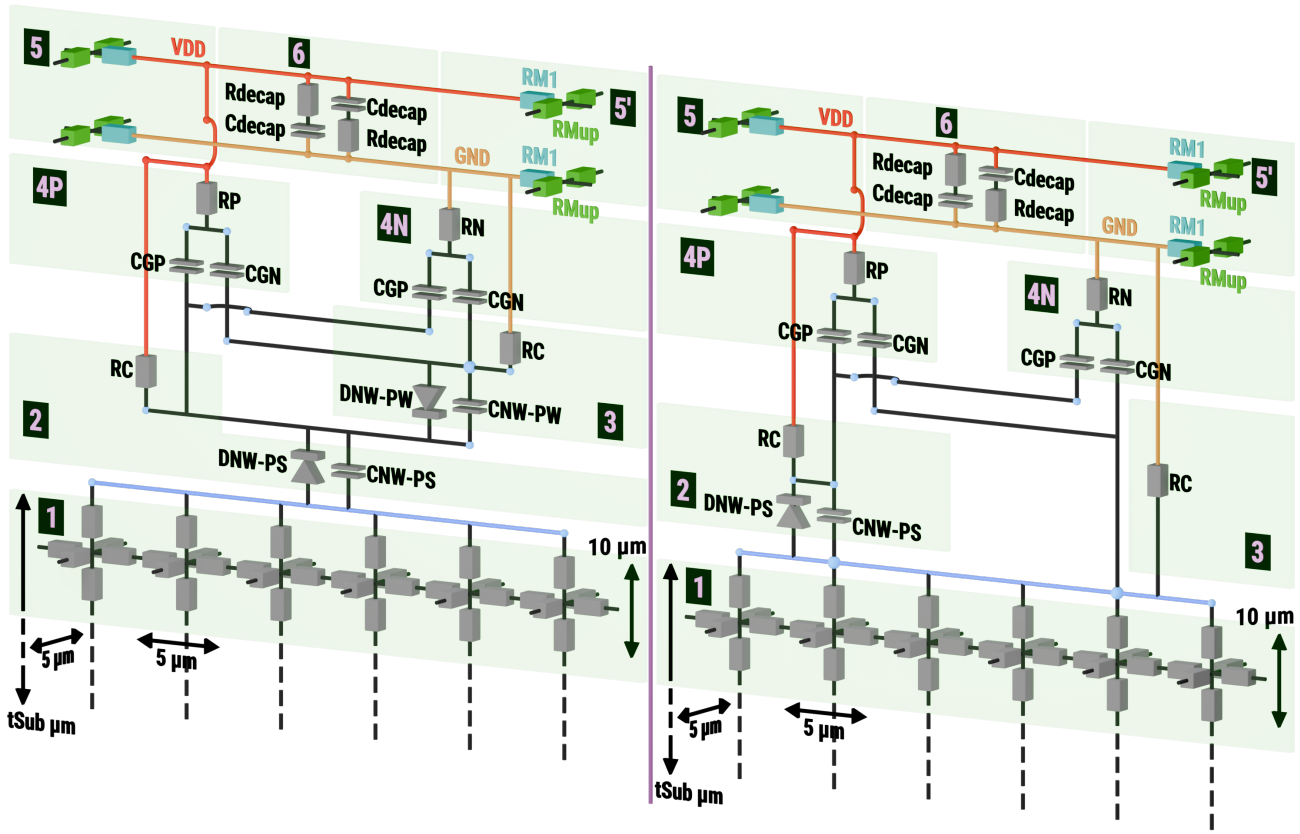

Fig. 5. Triple well (left) and dual well (right) std cell (PEUT ETRE FAIRE DES SOUS-FIGURES)

fig_triplewellstdcell