Enhanced BBI Techniques for Fault Injection in Hardware Cryptographic Systems

Geoffrey Chancel

***Abstract*—Over the past decades, several fault injection techniques have been investigated, such as Laser Fault Injection (LFI), Electromagnetic Fault Injection (EMFI), or Body Biasing Injection. Each technique manipulates various physical properties to achieve their objectives. EMFI exploits the electromagnetic susceptibility of integrated circuits, LFI uses the photosensitivity of the silicon, and BBI the conductive nature of the silicon substrate in the ICs. Although BBI has gained interest over the past few years, there are still numerous aspects to explore. In this context, this paper presents an enhanced BBI platform, allowing to perform differential fault attacks on a hardware cryptographic co-processor. In addition to this, it also describes a simulation flow devloped to provide inshigts on how BBI induces faults in ICs.**

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

I. Introduction

NOWADAYS, electronic devices are found in every economic sector, and very often manipulate sensitive and confidential data, such as in bank transaction systems, Internet of Things (IoT) devices, smartcards, or smartphones. To ensure data authenticity and confidentiality, these devices embed cryptographic algorithms. While theoretically secure and robust, once implemented on actual devices, these algorithms become fallible by leaking parts of the manipulated data through various physical quantities such as electromagnetic waves, infrared emissions, or sound emissions, not to cite them all. In addition to this, they are sensitive to external disturbances, which, when finely controlled, can lead the circuits to give unwanted information about the manipulated data.

Cybersecurity, and more specifically hardware security, takes place in this context. Commonly, when comes hardware security often comes side-channel attacks and fault injection attacks. On the one hand, side-channel attacks take advantage of the circuit leakage by measuring the various physical quantities available. On the other hand, fault injection aims at inducing controlled physical disturbances into integrated circuits, with methods like Electromagnetic Fault Injection (EMFI) [1], [2], Laser Fault Injection (LFI) [3], or Body Biasing Injection (BBI) [4], not to cite them all. Among these methods, EMFI and LFI are widely studied and well understood. However, despite a resurgence in the past few years, BBI knowledge is still less mature compared to the previously cited methods. Therefore, this article is dedicated in presenting our work on Body Biasing Injection, such as the description of better practices to improve BBI reproducibility, in addition to an entire simulation flow for BBI, designed to understand the underlying mechanisms of BBI.

A. Fault injection objectives

Before going further in the discussion about BBI, let us first outline the main objectives of fault injection methods. Most commonly, fault injection is used 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.

To achieve these objectives, an attacker can use the previously mentioned injection methods, such as EMFI, LFI or BBI. Prior to presenting further our work on BBI, let us analyze the available and existing BBI platforms in the state-of-the-art.

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

When compared to EMFI or LFI, 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 focusing on BBI [4]–[13]. Each one of them made a unique contribution for a better understanding of BBI.

The original works [4], [5] introduced the technique for the first time by applying its principle to an ASIC embedding counter-measures. The researchers performed a Bellcore attack [14], as this attack has weak fault requirements, on a modular exponentiation partially performed by the target thanks to its arithmetic co-processor.

Then, another paper [6] introduced an advanced BBI test bench aiming at performing reproducible attacks. In addition to this, it introduced a dual-well substrate lumped model to analyze and evaluate electrical phenomena occuring during BBI.

Four years later, another work [7] demonstrated that BBI can be performed quite easily using Wafer-Level Chip-Scale Packaging (WLCSP), naturally exposing the backside of ICs and thus reducing the complexity to set up BBI attacks. In addition to this, it introduced a low-cost tool to perform BBI: the Pico-EMP, a cheap and open-source device able to generate high voltage pulse with simple hardware.

Then, quite interestingly, researchers proposed a study of BBI on flip-chip packaging ICs using an ESD gun as a voltage surge generator, but concluded that its accuracy, either spatially or in terms of analytical capabilities was pretty limited [8], [9]. Therefore, the researchers developed a custom tool called a high-voltage pulse injector (HVPI), equipped with

a transformer, controller through a NMOS transistor. They tested their design against DFF registers and observed bit flips in those.

At the same time, the impact of substrate thickness on BBI efficiency has been studied in [10], comparing the effects of BBI on identical ICs with their substrate thinned to various levels, in addition to introducing a simulation flow.

Then, [11] studied the impact of dual-well and triple-well substrate types on BBI induced effects, and observed that BBI destructiveness highly depends on the substrate type and the voltage pulse polarity.

Thereafter, [12] proposed better practices for BBI platform design while studying a logic gate level model of BBI to further study the injection method impact on ICs.

Eventually, one last work proposed a safety-focused low-cost and open-source design for the practice of BBI [13].

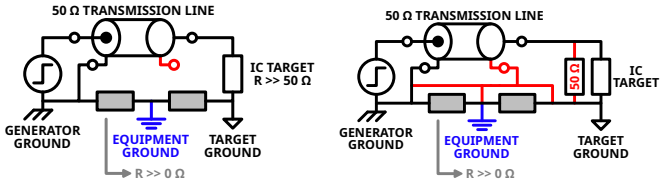
However, despite this extensive work, there are still unanswered questions, and the current works aims at bringing more answers to the underlying mechanisms of BBI.

II. Practicing BBI in a better way

THIS section is dedicated in presenting BBI platforms and the various improvements which can be brought to increase experiments repeatability and reliability.

A. BBI platforms in the state of the art

In the first place, let us analyze, from a theoretical perspective, a typical BBI platform, such as the one found in the state of the art. To do so, we created simple platform models highlighting the major limiting factors of such platforms.



(a) Typical (b) Improved

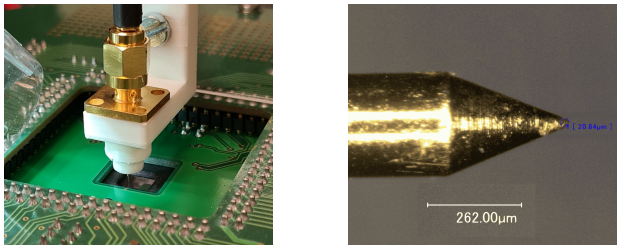
Fig. 1: A typical (a) and an improved (b) BBI setup.

The typical platform model is described in Fig. 1a, and illustrates the main components of a BBI platform, while omitting positioning tables, such as:

- The voltage pulse generator;
- The transmission line;
- The grounding installation;
- The IC target.

In addition to this, the schematic in Fig. 1a shows some important flaws we are going to address.

While this is not always the case, fast and high-voltage pulse generators are typically specified to be loaded with a 50 Ω load, or more generally with a fixed load. When performing BBI, the backside of the IC is electrically connected to the generator output. Therefore, outside of luck alone, it is very rare that the impedance presented by the IC to the generator perfectly matches the required one. It implies that the generator will be, most of the time, out of specifications, and that the conditions will vary depending on the chosen IC, the substrate thickness, and the location of the BBI probe. This can lead to issues such as errors in the set-point voltage and pulse width, in addition to ringing in the transmission line. This represents a first flaw to the typical approach.



(a) Global view (b) Zoomed view

Fig. 2: Our custom BBI probe.

Then, there is the grounding installation. The model presents a non-ideal but simple platform grounding. The reference node, used by the oscilloscope and the main computer, is represented in blue and called ”equipment ground”. Ideally, every ground on the platform is connected to this reference node with a very low impedance interconnection. However, depending on the hardware used, it may greatly vary from one platform to another. In the model, the generator and target grounds are connected to the reference node thanks to vastly imperfect interconnections, whose impedance is significantly greater than zero. This mainly lead to set-point errors due to shifts in the voltage pulse amplitude. Therefore, it limits the inter-platform repeatability and comparison of BBI experiments.

B. Our BBI platform

As most BBI platforms, our platform is focused on three main pieces of equipment: a voltage pulse generator, a metallic probe (Fig. 2), and a positioning table.

The positioning table we use is an OWIS PS 35 control unit, allowing to drive three motors for free movement in three dimensions. The generator model is the AVRK-4-B from the company Avtech Electrosystems Ltd. This model is commonly used for EMFI, but is suitable for BBI or any other application requiring fast voltage pulses, and its specifications are the following:

- Pulse amplitude: ± [150, 750] V;
- Pulse width: [6, 20] ns;
- First edge rise/fall time: 4 ns;
- Second edge rise/fall time: load dependent;
- Recovery time: < 1 ms;
- Propagation delay (PD): 150 ns;
- Jitter: ± 100 ps ± 0.03 % of PD;
- DC-coupled output;
- Loaded with 50 Ω.

Eventually, the most distinctive piece of equipment when it comes to BBI is the probe. Some BBI probes can be active, others passive and less expensive. However, it is important to

keep this piece of equipment relatively cheap as it endures most of the physical strain on the setup, and should be easy to replace or repair. Fig. 2 shows two pictures of our probe from different angles. The one we use is custom-made around three parts:

- A spring-loaded metallic tip, with a 20 µm head diameter;
- A SMA connector, where the tip is soldered;
- A custom 3D-printed enclosure holding the pieces together and cheap to replace.

The spring-loaded tip is 17 mm long and has a global diameter of 0.635 mm. It is specified for a 1.5 A nominal current, and its electrical resistance measures around 70 mΩ.

C. The proposed platform enhancements

To address the aforementioned limitations, we propose two modifications to generalize the platform and improve their repeatability.

First, let us talk about the generator impedance mismatch. For this purpose, multiple solutions can be approached. The best solution would be to implement an adaptive impedance matching system with active feedback, able to measure in real-time the impedance seen by the generator. However, adopting such a method is costly and long to set up in comparison to the next solution. Therefore, we propose a much simpler approach. Since, most of the time with our platform and targets, the impedance presented by the IC on its backside is in the order of 1 k Ω [12], approaching the 50 Ω expected by the generator can be done by connecting a 50 Ω resistor in parallel to the IC, as shown in the schematic in Fig. 1b.

Then, concerning the platform grounding, the solution is fairly straightforward. We propose to choose a reference node, such as the equipment ground in our scenario, and bypass every other ground on the platform with low-impedance interconnections from the previously chosen reference node, as proposed in Fig. 1b.

D. Platform enhancement validation

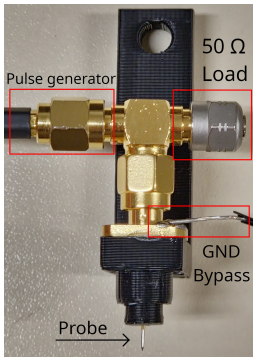


Fig. 3: Impedance matching in practice.

Now that we have outlined the platform improvements theoretically, let us analyze their actual impact on our BBI platform. The proposed solution concerning the approximate impedance matching and ground bypassing is shown in Fig. 3. The picture illustrates the BBI probe with a compensation load connected in parallel. in addition to the probe ground bypass. To highlight the practical benefits of these enhancements, let us analyze measured signals extracted from our platform.

We will compare before and after results and analyze the differences made by these improvements. To that end, we set up simple experiments consisting in injecting a voltage pulse into our IC target, measuring the voltage pulse at the probe and the current in the IC.

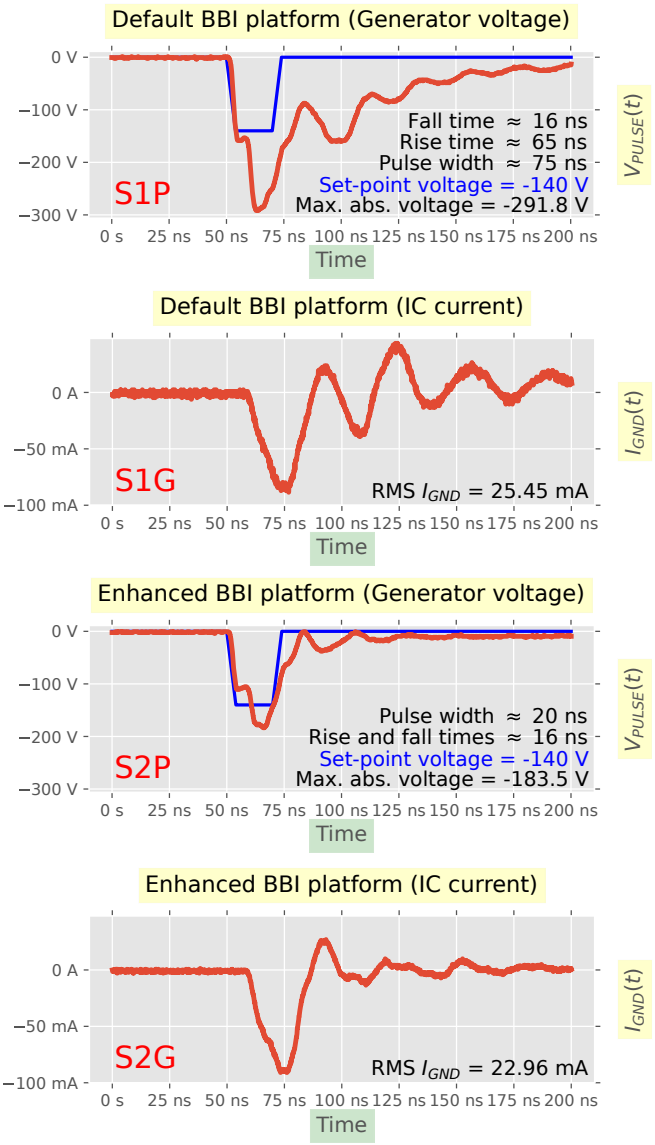


Fig. 4: Platform improvements in practice

Fig. 4 shows the waveform results from these experiments. The figure shows four distinct signals, arranged in the following order:

- S1P: the voltage pulse before improvements;
- S1G: the IC ground current before improvements;
- S2P: the voltage pulse after improvements;
- S2G: the IC ground current after improvements.

The experimental conditions are the following:

- Voltage pulse amplitude = -140 V;
- Voltage pulse width = 20 ns;

- Rise and fall times = 4 ns.

The waveform S1P shows in blue the ideal waveform according to the generator settings and in red the measured waveform. In addition to this are annotated some noteworthy values: such as the set-point voltage of -140 V, the max absolute measured voltage of 292 V, and rise and fall times. The first thing to notice here is the obvious undershoot of about -110 % under the set-point. It is far from being desirable when performing fault injection as the voltage amplitude control is of great importance for precision purposes when considering the method effects on the IC [12]. Furthermore, the pulse width is 275 % higher than the set-point, measuring 75 ns instead of 20 ns. It is an additional issue as it annihilates the accuracy needed in this context, and leads to longer pulses injected into the IC, and therefore energy than required and uncontrollable behavior. Additionally, the rise and fall times are also 4 to 16 times higher than expected. Eventually, we can notice damped oscillations, an observation of ringing in the transmission line.

Then, the waveform S1G, associated with the previous one, shows the IC ground current. Here, the damped oscillations are more clearly visible, in addition to the much longer than expected pulse duration. The RMS value of the injected current measures around 25 mA.

Afterward, the waveform S2P shows the voltage results with the proposed improvements. The voltage pulse amplitude is much closer to the set-point, with an undershoot reduced to -31 %. It is not perfect, but considering the simple nature of the impedance matching method we propose, it was to be expected. On another note, the pulse width set-point is perfectly respected. However, the rise and fall times are still 4 times higher.

Eventually, when looking at the S2G current waveform, we can remark the ringing reduction, while the amount of transferred energy remains approximately the same.

E. Platform enhancement application

To better illustrate the practical benefits of the proposed improvements, not only did we conduct electrical measurements, but also a differential dault attack (DFA). Indeed, performing fault injection is mainly used to conduct attacks, therefore it makes sense to verify the soundness of the improvements in this context. We chose to perform a single bit DFA on our IC target, as the fault criterion is hard to obtain, and therefore it can easily show the interest, or the lack of interest, of performing such improvements to the platform.

The target we used embeds a dedicated cryptographic core, which we set up using an AES on 128 bits. We then decided to perform the Giraud's DFA [15], originally described in 2002. This attack requires creating single bit faults in one or more bytes on the targeted AES. Our target was clocked at 40 MHz thanks to an external 8 MHz crystal, and externally powered with 3.3 V.

1) Preliminary experiments: Prior to performing the attack, we set up preliminary experiments allowing us to identify optimal locations on the IC backside where we could potentially perform the attack. Indeed, many areas and experimental parameters do not allow observing single-bit faults.

To do so, we created what we call Fault Analysis Mappings (FAM). These experiments consist in creating maps of a specific region of the IC, in that case the AES co-processor, and analyzing the IC behavior while performing BBI for a set of various experimental parameters. We categorized the observed behavior into seven cases:

- Correct: the AES responds normally;
- Monobit Monobyte fault: a unique bit faulted on a unique byte;
- Multibit Monobyte faults: multiple bits faulted on a unique byte;
- Monobit Multibyte faults: multiple bytes faulted with a single bit each;
- Multibit Multibyte faults: multiple bytes faulted with multiple bits each;
- Crash: the circuit did not respond correctly;
- Timeout: the circuit did not respond.

Therefore, as we only need single bit faults, only two cases are valid for the Giraud's DFA. To compare the two platforms, we performed a FAM on each one of them, using the following parameters:

- Pulse amplitude: from -150 V to -400 V with -5 V steps;
- Pulse width: 4.5 ns;
- Pulse delay: 150 ns + 553 ns targeting the penultimate AES round;
- Displacement step: 40 mm for the BBI probe over the mapped area.

Depending on the IC behavior, the experiments can take up to 36 hours. The parameters were selected to minimize the maximum energy transferred into the IC to minimize potential irreversible damage.

Fig. 5 presents the FAM results for both a typical (top) and the improved (bottom) platforms. The mapped area encloses a little more than the actual AES location, to be sure to map its entirety.

Let us look at Fig. 5 (top) first. What is interesting here is that we can spot numerous locations where the circuit crashed. More specifically, they represent 70 % of the mapped area. This behavior is problematic in such an experiment as it cannot lead to any useful data for a DFA. Initially, we attributed the experimental parameters to be the issue. Thus, we repeated the experiment with various different set of parameters. However, despite observing a majority of crashed locations, we never observed any single bit fault.

Then, let us discuss Fig. 5 (bottom). The first interesting thing to remark here is the total absence of IC crash. It is a desirable behavior as it indicates that we did not set a too high voltage or a too long pulse. Then, concerning single bit faults, we can spot five locations. It is a good sign for a preliminary experiment as it indicates the feasibility of such faults without much effort. However, it does not mean that we can perform the attack on one location with one set of parameters. It rather means that we can use these locations as good starting points to perform the DFA.

2) DFA results: To perform the DFA, we focused on the five previously found monobit locations above the AES core. Then, for each location, we used the following parameters:

#B	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 I: Giraud DFA

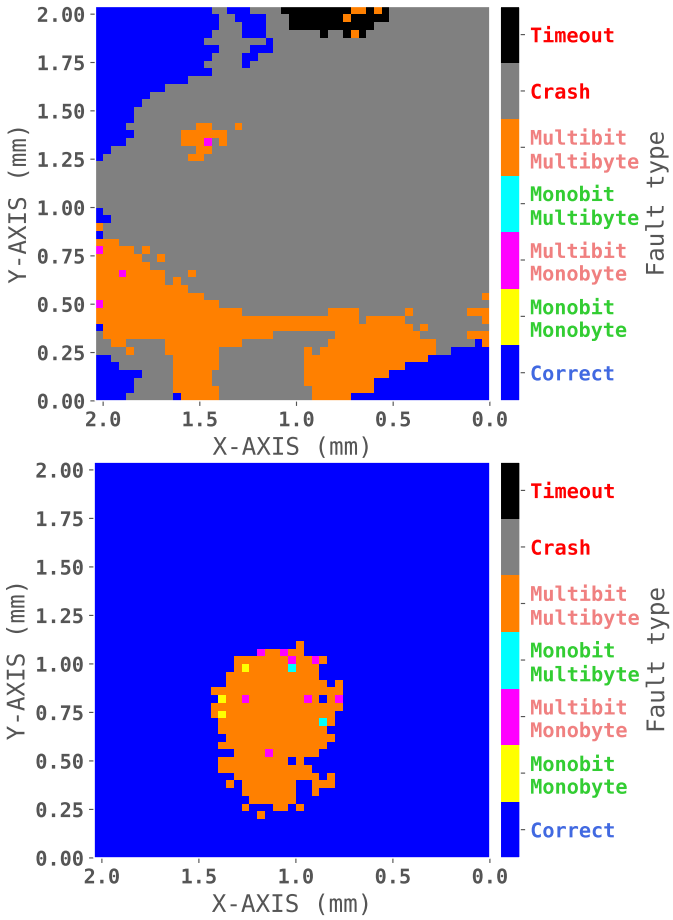


Fig. 5: Giraud's attack preliminary FAM

- Voltage ranging from -300 V to -600 V;
- Pulse width ranging from 4.5 ns to 5.5 ns;
- Injection delay ranging from ±10 ns around the penultimate AES round.

For each set of experimental parameters, we had to set some limits when trying to inject faults. Indeed, it is required to create a finite experiment and of reasonable duration. The first limit consists in trying to retrieve a maximum of 100 single bit faults. We have chosen this value as it is far more than what is suggested by Giraud's DFA [15] description. However, if reaching this limit can be easy on some sets of location and parameters, on others, it is almost impossible. Therefore, we have set another limit of 10000 trials to achieve the previous goal.

Thanks to this experiment, we retrieved, using the five previously identified locations, 14 bytes out of 16 of the AES K10 key, which is directly linked to the secret key in an AES-128 bits implementation, as shown in Table I. We could not retrieve with the Giraud's DFA the bytes number 2 and 5, which are located in the red cells in the previous table. To retrieve the key in its entirety, we performed a brute force method consisting in calculating every possibility for the remaining two bytes. Considering a slow laptop being able to compute approximately $10 \cdot 10^3$ AES encryptions per second, and the 16 remaining bits representing 65536 combinations, we decided to blindly calculate every combination. This calculation represents around 6.5 seconds of total computation time, and the results are shown in Table I. This experiment demonstrates the soundness of the proposed platform enhancements in terms of end user applications, i.e. a differential fault attack.

III. Body Biasing Injection: Disturbances Nature and Propagation

SIMULATING a fault injection method behavior is an important part in understanding its mechanisms. Whether it is EMFI, LFI or BBI, it allows predicting and understanding the underlying phenomena at work to set up reliable experiments, perform predictions and develop countermeasures.

Ideally, we would want to directly observe signals inside integrated circuits, allowing for fine measurements of power supply voltages, currents, and logic levels at a transistor-level. However, embedding sensors into an already existing IC is not possible, and doing so on future IC is costly, takes time to fully implement, and requires the manufacturer to do so. 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:

$$\text{Simulation} \rightarrow \text{Analysis} \rightarrow \text{Hardware Verification}$$

which is flexible and can be used in any existing commercial circuit.

By doing so, we have freed ourselves from hardware limitations. However, other limitations remain. Indeed, modern ICs, even the smallest, embed millions of transistors, and with current technologies, it is impossible to evaluate entire circuits at a transistor level with brute-force simulations. To tackle these limitations, we decided to adopt an hybrid approach, combining transistor-less models and targeted 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 [2]. The resulting simulation flow is then 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 power signals from the previous simulation;
- The simulation of a selection of disturbed logic gates under BBI thanks to the previously extracted signals.

A. Modeling ICs and BBI platforms

Building the correct models for the simulation flow involves multiple steps. If the goal of the hybrid flow is to reduce the computational time 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 addition to this, we are only focusing on bulk substrates: specifically dual-well and triple-well substrates.

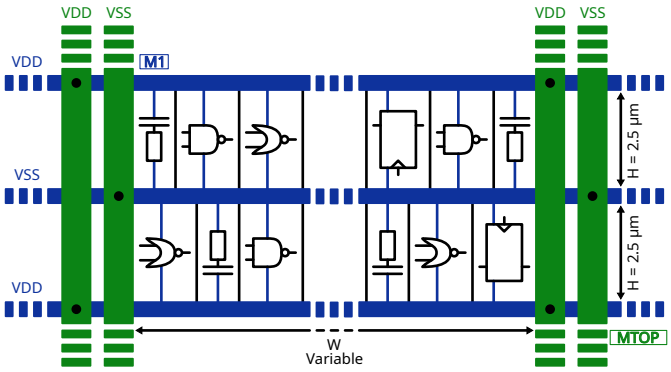


Fig. 6: A Standard-Cell Segment and its power delivery network.

1) Power supply rails and standard-cell segments: The power distribution inside an IC is typically made with a layered grid-like structure, composed of metal wires stacked on top of each other on planes, which results in multiple metal loops. In each layer, the metal wires are equally spaced and have a dedicated width, which becomes thinner the deeper they are. The lowest layer is directly connected to the transistors. Fig. 6 presents a common power delivery network, designed with two metal levels for simplicity (in blue and green).

Within the metal lines are located standard-cell segments (SCS), composed of decoupling, logic and sequential elements. These SCS are pre-characterized by foundries and categorized depending on their performance (mainly according to, but not exclusively, their power consumption and timing). As illustrated in Fig. 6, SCS have a constant height, in our case of 2.5 µm, and a width depending on the power routing policy (in our case W = 30 µm). 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.

To that end, the elementary SCS chosen measures 30 µm by 5 µm, representing two rows of logic cells. An SCS contains about a hundred of logic gates in a 90 nm bulk technology, which are represented with passive elements, such as four capacitors and two resistors, as shown in Fig. 7. These elementary models consider that half of the transistor are conducting, and half are not, which represents an average behavior. The values of R_P, R_N, C_{GP} and C_{GN} depend on the targeted technology, i.e. the transistor size. The conducting NMOS

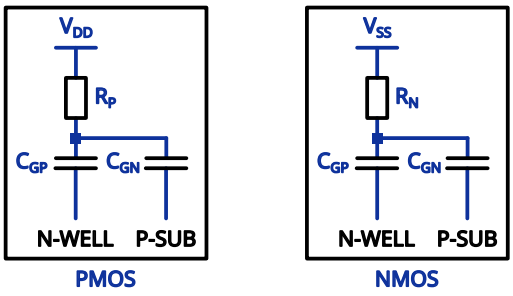


Fig. 7: Transistor-less equivalent model of a set of PMOS and NMOS in a SCS.

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. Eventually, C_{GP} and C_{GN} represent the connected NMOS and PMOS transistor gates.

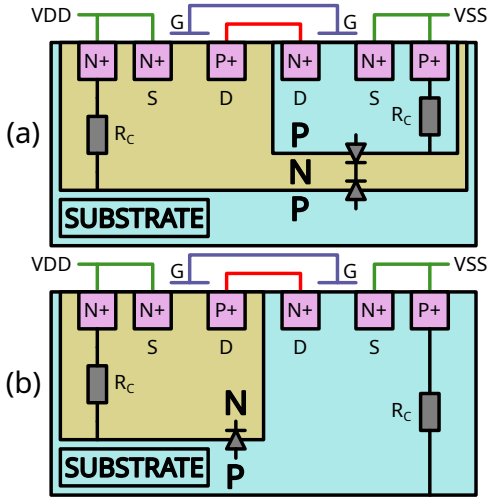


Fig. 8: Triple-well (a) and Dual-well (b) inverter cross-sectional view.

2) The substrate: Because BBI can be performed thanks to the silicon substrate as the main physical environment transferring energy from a generator to the active port of 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, therefore we only considered a P-substrate. There are two typical ways of lithographing the transistors in a bulk substrate, either using dual-well or triple-well structures. Dual-well substrates are commonly found in moderately old circuits, while triple-well substrate is commonly found mixed with dual-well 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. 8a and Fig. 8b:

- In the triple-well substrate, the NMOS transistors

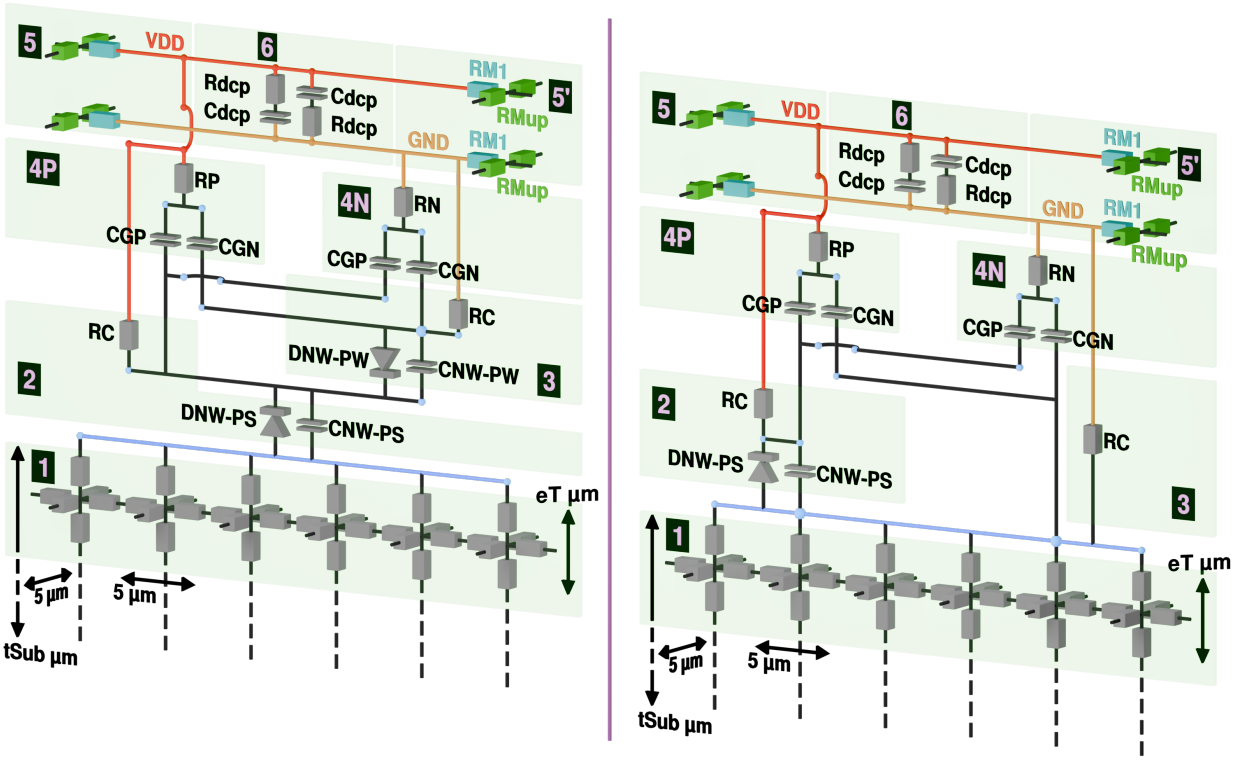


Fig. 9: Triple-well (left) and dual-well (right) Standard-cell Segment elementary models

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 previously introduced, 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 SCS of the simulated IC, measuring 30 µm by 5 µm by t_{Sub} µm, the latter being the substrate thickness, a parameter which may 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. 9. Each model consists in multiplesub-regions, whose descriptions follow:

- [1] is the elementary 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.

In addition to this, the desired substrate thickness can be achieved by instanciating as much as needed the elementary substrate layer inside the model itself, its elementary thickness being eT µm.

As we have stated before, these models only represent a small portion of the modeled IC. To create an entire IC of a defined size, it is required to instantiate and interconnect as much as needed the elementary models. By doing so, we can create a bigger model of virtually any size. The language we have chosen to work with the simulation is the SPICE language. However, we created a custom Python script to interconnect the SCS together, place external power connections, and generate a main SPICE netlist. For the current work, we have chosen to put the external power connections at the top and bottom of the IC (seen from above), and the BBI probe at the center of the IC (on the backside).

B. Simulation results: operating point

Now that we have described the base models and their replication, we can perform BBI simulations using these models. To properly use these models, it is required, in the first place, to validate them through various steps to ensure their reliability. To that end, we generated an IC measuring

550 µm by 450 µm with a 140 µm substrate thickness (tSub), and performed an operating point to verify the correctness of the models for each substrate type. We should expect almost no voltage drop and almost zero current consumption from such a model. Otherwise, it indicates an underlying issue with the model.

Table II shows the operating point results for both a triple-well and a dual-well circuit, and indicates a correct operating point, with idle currents and voltage drops close to zero.

Value	Triple-well	Dual-well
I_{GND}	2.88 nA	2.85 nA
I_{VDD}	-8.64 nA	-2.92 nA
$\overline{GND_{drop}}$	1.83 nV	1.76 nV
$\overline{V_{DD_{drop}}}$	1.2 nV	1 nV

TABLE II: Operating point simulation results.

However, verifying the bias point alone is not sufficient to consider the model validated. As these models are dedicated to be mainly used in transient simulations, it is required to perform one and evaluate the soundness of its results.

Therefore, we performed BBI transient simulations with a triple-well and dual-well IC, with the following parameters:

- A nominal power supply voltage of 1.2 V;
- A voltage pulse amplitude of ± 300 V;
- A voltage pulse width of 15 ns;
- Rise and fall times of 8 ns;
- A simulation duration of 80 ns;
- A simulation time step: of 50 ps.

Analyzing the simulation results involves observing various internal IC signals, for each substrate type, the ones presented in this section being:

- The power supply voltage distribution;
- The epitaxial current;
- The substrate current distribution;
- The substrate per-layer current density.

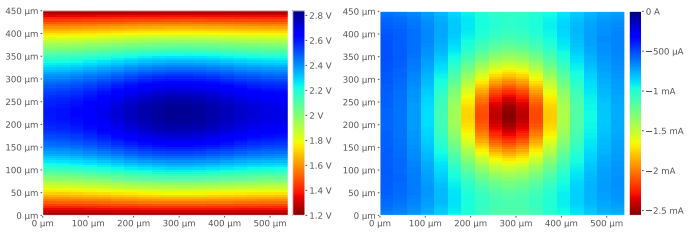
The observed signals are displayed in two dimensions and at the apex of the BBI disturbance. Each signal brings some insights on what happens inside the circuits during a BBI pulse. We will first analyze the dual-well, then the triple-well results, to finally conclude with a comparison of both.

C. Simulation results: dual-well negative pulse

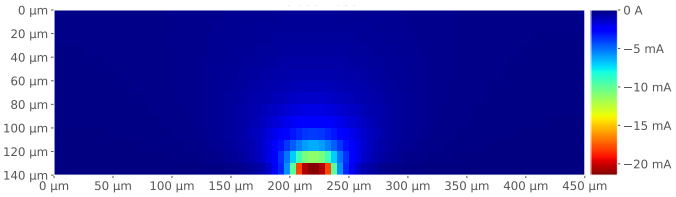
Fig. 10 shows the simulation results for a negative pulse applied to a dual-well IC

Sub-fig. 10a left represents the power delivery network (PDN) voltage distribution across the entire simulated IC, seen from above. In other words, it is the supply voltage of the transistors. Expectedly, far from the external power connections, we observe some deviation from the nominal 1.2 V power supply voltage. However, at the center of the circuit, in other words under the BBI probe, the voltage goes up to 2.8 V, being a 133 % increase from the nominal value.

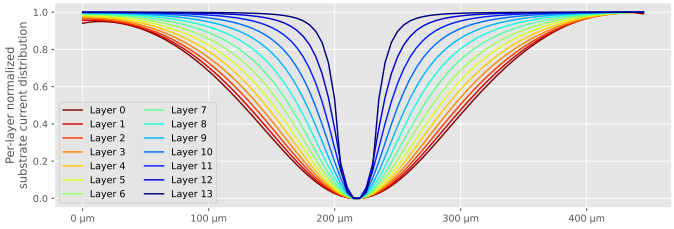
To put these values into perspective, let us look at sub-fig. 10a right, showing the epitaxial current distribution, representing the charges going from the substrate to the top of the SCS. According to these results, most of the charges are



(a) Power delivery network voltage distribution (left), epitaxial current distribution (right)

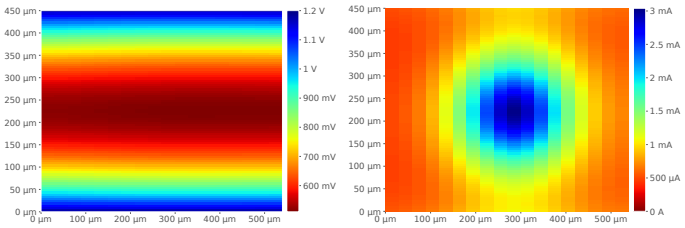


(b) Substrate cross-sectional view current distribution

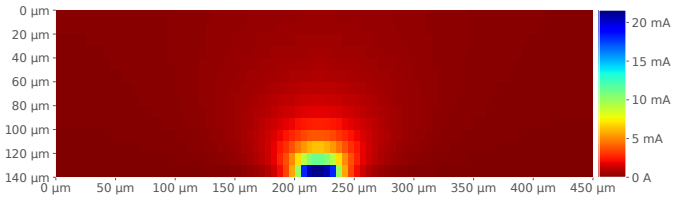


(c) Substrate per-layer normalized current density

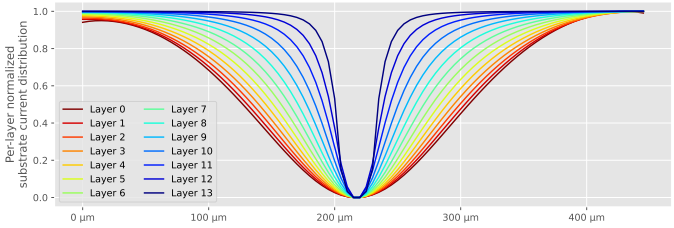
Fig. 10: Dual-well IC negative pulse simulation results.



(a) Power delivery network voltage distribution (left), epitaxial current distribution (right)

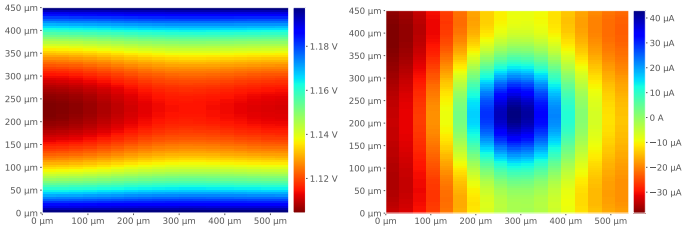


(b) Substrate cross-sectional view current distribution

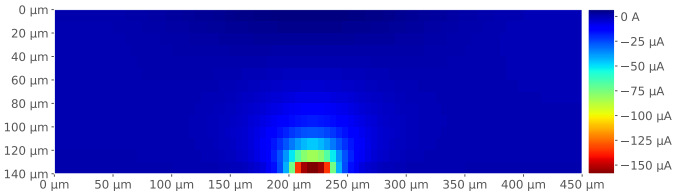


(c) Substrate per-layer normalized current density

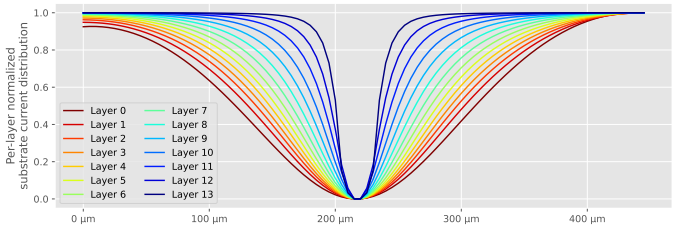
Fig. 11: Dual-well IC positive pulse simulation results.



(a) Power delivery network voltage distribution (left), epitaxial current distribution (right)

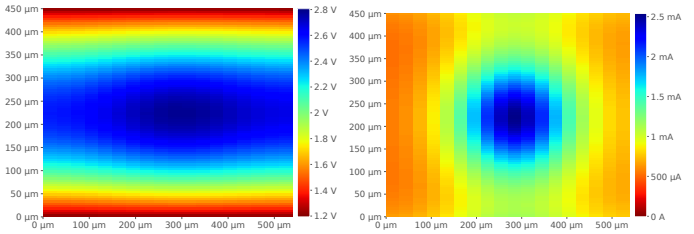


(b) Substrate cross-sectional view current distribution

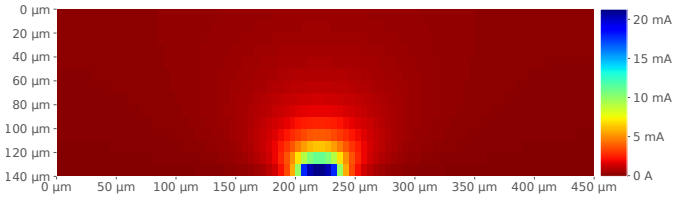


(c) Substrate per-layer normalized current density

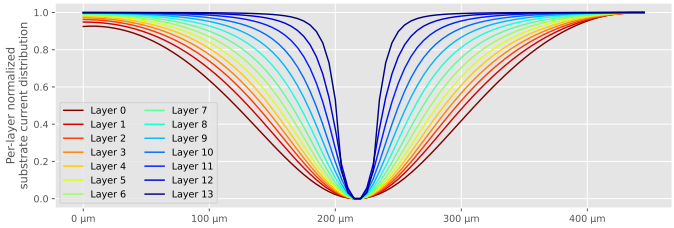
Fig. 12: Triple-well IC negative pulse simulation results.



(a) Power delivery network voltage distribution (left), epitaxial current distribution (right)



(b) Substrate cross-sectional view current distribution



(c) Substrate per-layer normalized current density

Fig. 13: Triple-well IC positive pulse simulation results.

passing through at the center of the IC (under the BBI probe), as the current is the highest in that location. It is sound when comparing left and right sub-fig. 10a, as the voltage difference from the nominal value is higher where the epitaxial current is higher.

Sub-fig. 10b and sub-fig. 10c both represent the same physical quantity in two different ways. We have chosen this approach to extract as much information as possible from these models and simulations. Sub-fig. 10b shows the cross-sectional view (from the Y-axis) of the current distribution inside the substrate. The substrate being an isotropic environment, in other words, its resistivity is homogeneous in every spatial directions, we can observe a hemispheric current distribution in it. However, due to the large difference between the first layer (the farthest to the probe) and the last layer (the closest to the probe), it is difficult to do more observations. Therefore, we can look at sub-fig. 10c, which represents the same data in a different perspective. To better illustrate the inter-layer differences, we have chosen to normalize the data in a per-layer basis. Thus, it allows us to compare the current density between layers. It is important to note that the normalized values are calculated in a way that the closer they are to zero, the denser the current is, and vice-versa. The layer 0 is the closest to the logic gates, while the layer 13 is the closest to the backside (the probe). What is interesting to note here is that for each substrate layer, the current is focused where the probe is located. It is to be expected, as the substrate is isotropic. However, the deeper (starting from the backside) we are into the substrate, the less focused the current is. Once again, it is quite logical as the charges diffuse homogeneously inside the substrate.

D. Simulation results: dual-well positive pulse

Concerning the positive pulse dual-well results, let us look at Fig. 11. Compared to the previous results, sub-fig. 11a left shows that the PDN voltage exhibits not a voltage increase, but rather a voltage drop. Indeed, under the probe, the PDN voltage drops to 500 mV from 1.2 V. This is a substantial difference, which could lead, if applied to actual transistors, a significant change in behavior such as an incorrect biasing and a temporary halt of operations.

Concerning the epitaxial current, shown in sub-fig. 11a right, we can notice two key changes. First, the current polarity has changed, from a negative to a positive one. Once again, it was to be expected, as the voltage pulse polarity has changed. Then, in absolute value, the maximal current is 500 µA higher than previously, which indicates that more energy has been injected into the circuit. Eventually, regarding the substrate current, there are no major differences compared to the previous scenario, except the current polarity, both for sub-fig. 11b and sub-fig. 11c.

E. Simulation results: triple-well negative pulse

Let us take a closer look at Fig. 12. These results stand out all of the others, in many ways. First, if we take a look at sub-fig. 12a left regarding the PDN voltage, we can see that there are very little variations from the nominal voltage.

Indeed, the voltage drops only to 1.1 V. Then, concerning the epitaxial current shown in sub-fig. 12a right, we can see that it is almost a hundred times lower than on other results. It is then confirmed in sub-fig. 12c and sub-fig. 12d with the substrate current distribution. Before analyzing further these results and explaining them, let us analyze the last case.

F. Simulation results: triple-well positive pulse

Interestingly, using a triple-well substrate and a positive voltage pulse, as displayed in Fig. 13, we observe very similar results to those of the dual-well negative case (Fig. 10), whether on the PDN voltage or on the epitaxial current. Indeed, the PDN voltage disturbance is almost identical to sub-fig. 10a left, with an increase in voltage from 1.2 V to 2.8 V. Then, the epitaxial and substrate current maps looks like a mirrored copy (in polarity) of sub-fig. 10a left and 10c. Eventually, the current density graph is very close to the other results.

G. Simulations results: summary and conclusions

As we have seen through this section, we have four possible scenarios:

- A dual-well substrate and a negative voltage pulse;
- A dual-well substrate and a positive voltage pulse;
- A triple-well substrate and a negative voltage pulse;
- A triple-well substrate and a positive voltage pulse.

Each scenario behave differently from the others due to one main reason: the electric coupling between the probe (substrate) and the SCS (logic). These differences in coupling are due to the substrate structure we encounter in dual-well and triple-well circuits.

As we have described before, the dual-well substrate embeds a P-N diode between the P-substrate and the N-well, and depending on the voltage pulse polarity, this diode is either blocking or conducting. This diode is interspersed between the substrate and the PMOS section. On the one hand, concerning the negative pulse scenario, the diode is blocking, thus creating an AC-coupling between the probe and the PMOS. On the other hand, the NMOS are DC-coupled to the probe as they are connected through a resistive path. Therefore, the circuit is globally DC-coupled to the probe, allowing the charges to flow all the time during the pulse. Then, concerning the positive pulse scenario, the diode conducts, creating another DC path to the transistors, reducing the effective circuit impedance seen by the probe. It explains the greater observed currents, as the charges have an additional DC path to follow.

On the triple-well side, the top of the SCS is barred with a first P-N diode (P-substrate N-well), and the NMOS are behind another diode. When using negative pulses, the first diode is blocking, therefore creating a pure AC-coupling between the probe and the circuit. It means that the charges are able to flow in and out of the SCS only on the pulse edges. Consequently, for a given voltage pulse, less energy is transferred into the IC in that case.

Then, regarding the triple-well positive scenario, the first diode become conducting, while the second stays blocking.

Substrate	Polarity	Coupling NMOS	Coupling PMOS	Circuit	Danger
Dual-well	Negative	DC	AC	DC	☠☠☠
Dual-well	Positive	DC	DC	DC	☠☠☠☠
Triple-well	Negative	AC	AC	AC	☠
Triple-well	Positive	AC	DC	DC	☠☠☠

TABLE III: BBI probe and IC coupling.

Therefore, the PMOS are DC-coupled, while the NMOS stay AC-coupled. We come back to a scenario similar to dual-well negative.

Eventually, the main outcomes these simulation results show are in Table III, alongside a qualitative dangerousness appreciation of each scenario. In that case, what we mean by dangerousness is how quickly we have observed a complete circuit destruction according to the voltage pulse polarity and the substrate type.

H. Validating the models

With the aim of verifying the soundness of the previous conclusions, we set up experiments using an actual IC composed of both triple-well and dual-well substrate within a monolithic die. These experiments consist in verifying if the difference in injected energy depending on the substrate type is actually significant or not, as predicted by the simulations.

The target used is a STM32F439 microcontroller, alongside the platform presented in the first chapter. The IC die measures approximately 5.5 mm × 4.5 mm. We call these experiments ”IC ground current mapping”, and quite naturally, they consist in measuring in specific conditions the current at the target circuit external ground connection. The entirety of the IC is mapped, and a voltage pulse is injected at each location. Then, we measure the current at the circuit ground and calculate its RMS value to represent it into a two-dimensional cartography.

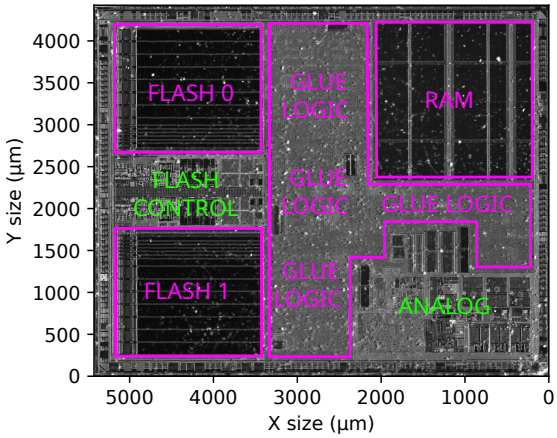


Fig. 14: IR photograph of our target IC

Knowing the coarse structure of the considered IC, in addition to having insights on the substrate type, we could draw the coarse structure picture shown in Fig. 14. The ”glue logic” regions are known to be made with triple-well substrates, while the ”flash control” and ”analog” regions are made with dual-well substrates.

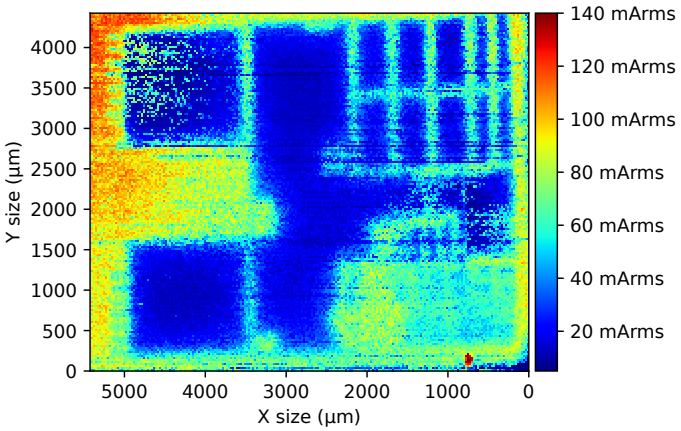
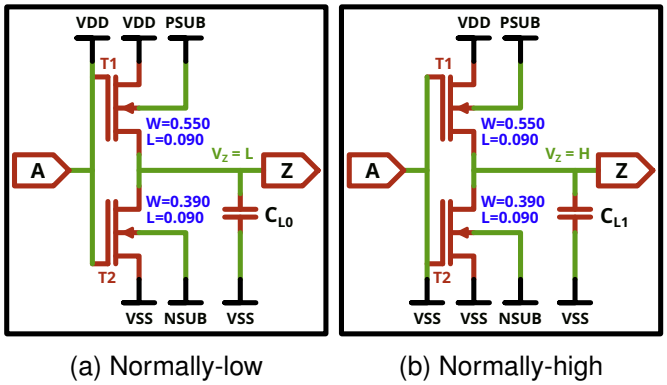


Fig. 15: Ground current mapping of our target IC



(a) Normally-low (b) Normally-high

Fig. 16: Inverter schematic netlists

The experimental results are shown in Fig. 15, and the experimental parameters are the following:

- Negative voltage pulse of 70 V amplitude;
- Pulse width of 20 ns;
- IC substrate thickness of 50 µm.

The voltage pulse used is of negative polarity as we have observed a very fast degradation of IC exposed to positive voltage pulses, therefore, we opted to avoid them entirely. When analyzing the results, we can notice significant differences in the measured current depending on various regions, and the IC floorplan seems to draw itself on the current map. The measured RMS current ranges from 10 mArms to 140 mArms, and as predicted by the simulation results, in the regions where the substrate is of dual-well type, the current is higher than on regions where the substrate is of triple-well type, such as the analog block or the flash control region.

These observations confirm the accuracy of the proposed models. However, as we have seen previously, these models do not consider the functional nature of the considered ICs: their logic behavior. To address this limitation, we chose to enhance the initial simulation flow by introducing what we call a ”hybrid simulation flow”.

IV. Effects of BBI on IC operation

A. Extending the models: logic gates simulation

As we have stated previously, it is required, to complete the models, to properly consider the logical behavior of the considered circuits, which allows for a better appreciation of BBI induced effects and their consequences. These additional steps consist in modeling actual logic and sequential elements in the same or in a close technology as the considered IC, while extracting the significant disturbed signals from the SCS simulation and injecting them into these logic devices. For this purpose, we have divided this section into two subsections:

- A first section dedicated to studying a static logic gate: the classical inverter;
- A second section dedicated to studying an essential sequential element: the DFF.

B. BBI effects on static logic gates: inverters

Because inverters can have two stable output states, we will consider two cases for each substrate scenario: a normally high inverter (Fig. 16.a) and a normally low inverter (Fig. 16.b). The inverters are connected to four external signals which are extracted from the previous SCS simulation:

- VDD: the power supply voltage;
- VSS: the power supply reference voltage;
- PSUB: the bulk voltage of the PMOS transistors;
- NSUB: the bulk voltage of the NMOS transistors.

The voltages PSUB and NSUB are different according to the substrate type. On the one hand, in the dual-well scenario, NSUB is connected to the epitaxial layer, while PSUB is connected to the N-well. On the other hand, in the triple-well scenario, NSUB is connected to the P-well and PSUB to the N-well.

All of this gives us four scenarios to study. For clarity and because two of the four scenarios are less noteworthy, we will only talk about two of them:

- The triple-well substrate and the normally high inverter;
- The dual-well substrate and the normally low inverter.

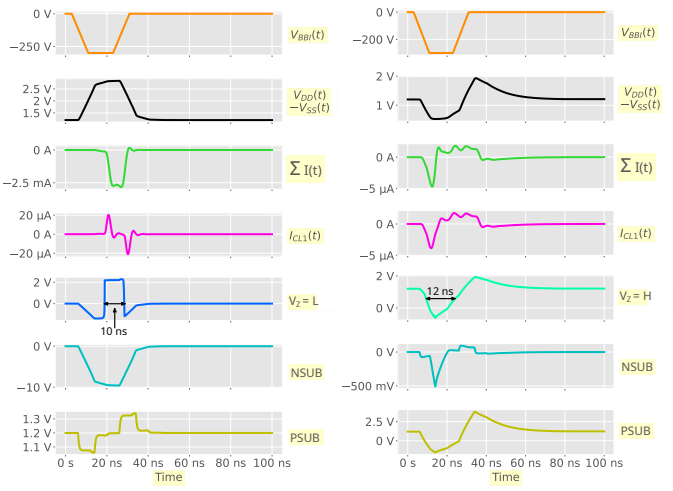
Then, for each scenario, we will analyze seven signals of interest:

- The backside voltage pulse, for reference purposes;
- The local differential power supply voltage (VDD - VSS);
- The current sum of the inverter ($I_{DS}^{T1} + I_{DS}^{T2}$);
- The inverter load current, a.k.a. the current flowing through the capacitive output load;
- The inverter output voltage;
- The NSUB voltage (NMOS bulk voltage);
- the PSUB voltage (PMOS bulk voltage).

The signals extracted from the SCS simulations come from the standard-cell located directly below the BBI probe, a.k.a the cell targeted by the injection.

Fig. 17 presents the inverter simulation results for both considered scenarios.

First, let us focus on the dual-well inverter. The corresponding schematic is shown in Fig. 16b, and the simulation results are shown in Fig. 17a. In that case, as we have seen before, the global IC coupling is resistive, with a discrepancy



(a) Dual-well (b) Triple-well

Fig. 17: Inverters simulation results

between VSS and VDD: VSS being purely resistive, and VDD being purely capacitive. Therefore, the inverter current sum (green) follows a DC-response, similar to the differential power delivery voltage (black). The inverter output follows the current sum curve, and its output goes from a low to a high logic value during 10 ns, then back to its original state. It is further corroborated by looking at the load current, which is charged on the first pulse edge, then discharged on the second one.

Second, concerning the triple-well inverter, where the results are shown in Fig. 17b and the schematic in Fig. 16a, the substrate is globally AC-coupled. It can be seen on the current sum curve, which follows almost exactly the capacitive load current curve. The inverter output, for its part, is discharged like the load, and goes from a high logic value to a low value during 12 ns before returning to its original value.

These observations are of great value because we can discuss a fault model for BBI, similar to what has been studied for EMFI and LFI. The previous results seem to indicate that the faults created using BBI are data-dependent. Indeed, if we lower the voltage of an inverter outputting a low value, or the opposite, it has theoretically no direct effect on the logic value. However, we have seen that it is possible, depending on the substrate type, to temporarily flip the value of a bit for the same amount of time than the pule width duration. Eventually, thanks to these results and the previous ones regarding current density in the substrate in Fig. 10, 11, 12 and 13, it seems that BBI effects are local.

C. BBI effects on dynamic logic gates: DFF

Now that we have analyzed the behavior of static inverters, it is important to consider studying the behavior of sequential elements such as a very common one: the D Flip-Flop. To test the DFF behavior under BBI, we placed it in the middle of a logic path and buffered its clock. The goal of this simulation is to mix the behavior of a disturbed logic path outputting to a disturbed DFF, outputting to a non-disturbed logic path. The

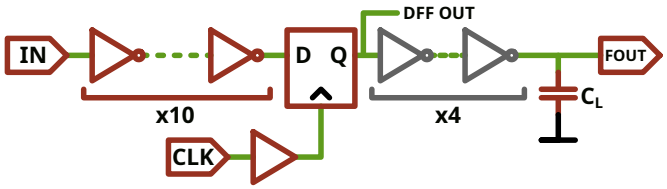


Fig. 18: DFF netlist with its combinatorial logic chain and load

non-disturbed path is here to mimic the behavior of far away logic gates receiving disturbed data while having a correct power supply.

Similar to what we have done in the previous section, we will extract signals from the SCS simulation and inject them into this test circuit. The simplified schematic of this circuit is shown in Fig. 18. The first ten inverters, the buffer and the DFF are disturbed, while the four last inverters are not disturbed. The load C_L mimics another set of logic gates which are loaded into the four inverters. As we did with the inverters, we will only consider negative pulses, both for a dual-well and a triple-well substrate.

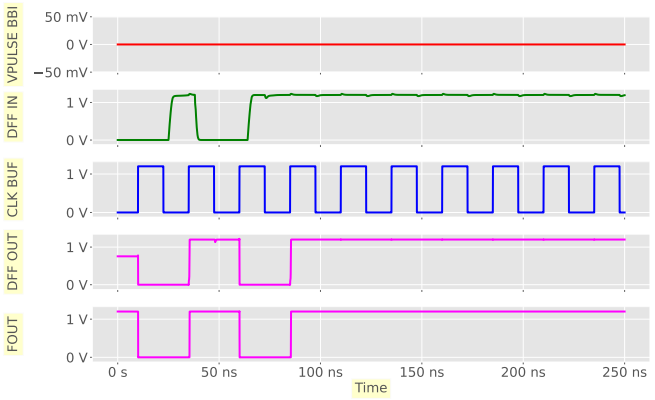


Fig. 19: DFF path: idling

Before diving into the simulation results, let us analyze what would be the normal behavior of the considered DFF. Fig. 19 presents the normal behavior of the modeled DFF path. The flip-flop is governed by a 40 MHz clock, similar to what we have used on our target, and we perform three data input sampling operations with alternating logic levels (High → Low → High), to finally let it rest at the last logic level. Because a DFF is a dynamic device, there are many interesting moments to observe depending on when the voltage pulse is injected. Therefore, we cannot represent every noteworthy moment, so we have chosen the most interesting. First, we will analyze results where the injections are performed during the steady state of the DFF chain, Then, we will analyze the DFF behavior during the write operations.

1) Dual-well substrate, negative pulse: Fig. 20 shows the simulation results for a dual-well negative pulse for a steady state disturbed DFF. Five signals are represented in this order, allowing us to get insights on the circuit behavior:

- The BBI voltage pulse for reference;

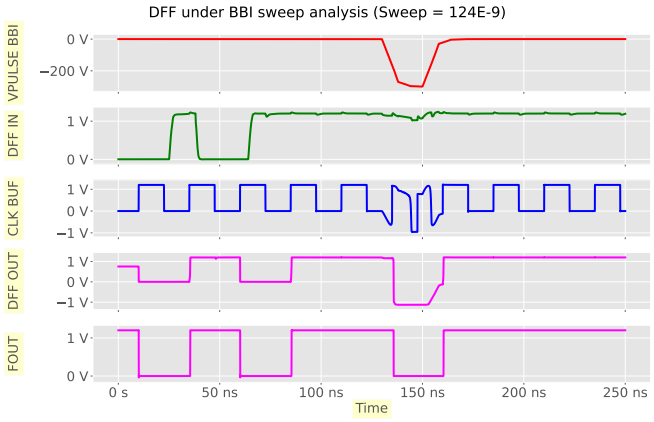


Fig. 20: DFF path: static dual-well

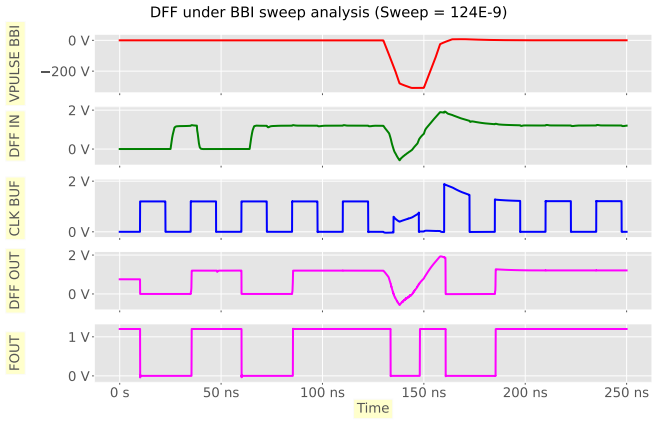


Fig. 22: DFF path: static triple-well

- The DFF input signal (DFF IN), being the output of the first ten inverters;
- The buffered DFF clock (CLK BUF), the clock fed to the DFF after the buffer;
- The DFF output;
- The four last inverters output;

The results show that the DFF input is not disturbed enough to trigger a logic value change. However, the DFF output drops down to -1 V, similar to its own buffered clock. This voltage drop, lasting for 25 ns, reverberates on the clean inverters output, resulting in a low logical value being output. In addition to this, the disturbances on the clock shows the creation of two parasitic clock pulses, replacing a normal one during the injection.

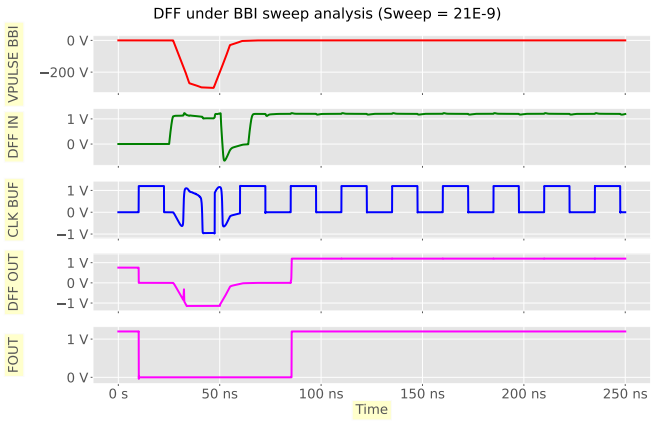


Fig. 21: DFF path: dynamic dual-well

Then, Fig. 21 shows the exact same scenario with a different injection time, performed during the first write operations. These results show that the disturbances prevent the second write operation, supposed to write a high logic value in the DFF. Therefore, this data will never be sampled by the DFF and therefore will never propagate to the output of the circuit.

2) Triple-well substrate, negative pulse: Fig. 22 shows the simulation results for a triple-well negative pulse for a steady state disturbed DFF. In that case, the DFF input is disturbed, similarly to its output, by the BBI pulse. This causes a voltage drop significant enough to create a parasitic low logical value at the net FOUT. Concerning the clock, its maximum voltage is damped by the BBI pulse down 700 mV for one period.

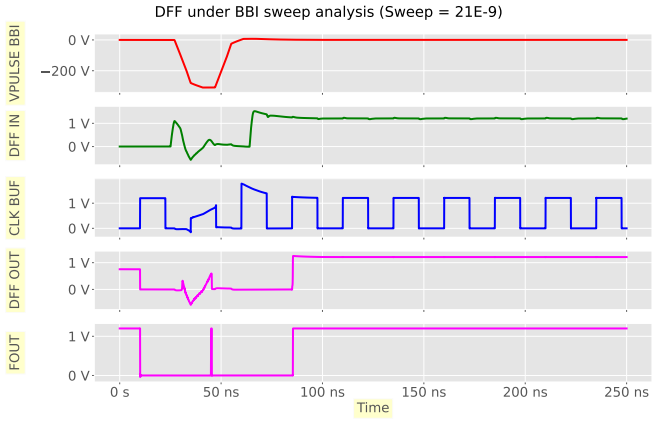


Fig. 23: DFF path: dynamic triple-well

Eventually, Fig. 23 shows the results for a dynamic BBI in a triple-well under a negative pulse. Similar to the steady state result, the clock voltage is damped down to 800 mV. The DFF input is clearly disturbed and the disturbance follows the BBI pulse, which is similar on the DFF output. These disturbances then cause an error during the sampling of the high logic value, which reverberates on the net FOUT, which shows a short pulse instead of a plateau, around 50 ns.

V. Conclusion: to re-write

BODY biasing injection has seen a re-emergence since 2020 [7], and various works have brought more and more knowledge throughout the years [4]–[13]. BBI, contrary to EMFI or LFI, uses the silicon substrate of integrated circuits as the main physical medium to interact, transfer energy, and disturb these circuits. We introduced, through this work, the cumulative knowledge we gathered concerning BBI. This involves various aspects of the subjects.

First, we studied better platforms aiming at improving BBI experiments repeatability and reliability through low-cost enhancements such as impedance matching and proper

grounding. We supported these results with actual experiments such as Fault Analysis Mappings and a Differential Fault Attack.

Then, we introduced large-scale IC modeling thanks to the use of transistor-less models allowing to reduce the computational power required to simulate BBI.

Eventually, we extended this "transistor-less models" simulation flow to consider the logic functions of integrated circuits under BBI. This allowed us to understand the mechanisms at work during fault creation in integrated circuits under BBI, such as data-dependent bit set/reset faults, in addition to understanding the locality of BBI effects.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Colin O'Flynn. Low-cost body biasing injection (BBI) attacks on WLCSP devices. In *Smart Card Research and Advanced Applications*, pages 166–180, Cham, 2020. Springer International Publishing.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.