

Impact of Intentional Electromagnetic Interference on Pure Combinational Logic

Oualid Trabelsi, Laurent Sauvage, Jean-Luc Danger

▶ **To cite this version:**

Oualid Trabelsi, Laurent Sauvage, Jean-Luc Danger. Impact of Intentional Electromagnetic Interference on Pure Combinational Logic. 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE, Sep 2019, Barcelone, Spain. pp.398-403. hal-02318731

HAL Id: hal-02318731

https://telecom-paris.hal.science/hal-02318731

Submitted on 17 Oct 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Impact of Intentional Electromagnetic Interference on Pure Combinational Logic

Oualid Trabelsi, Laurent Sauvage and Jean-Luc Danger
LTCI, Télécom ParisTech, Institut Polytechnique de Paris
Saclay, France
Email: name.forname@telecom-paristech.fr

***Abstract*—Electromagnetic fault injection is a growing topic when it is applied to jeopardize the security of integrated circuit. Indeed, if the main part of the process will focus on the hardware efficiency of the near-field probes, tweaking properties of the electromagnetic disturbance can also lead to the success of the attack. In this paper, we are presenting characterization results of intentional electromagnetic interference by measuring its impact within the target, and more precisely on the propagation delay of a combinational logic path. The evaluation of the impact shows that the electromagnetic coupling between the probe and the integrated circuit strongly depends on the characterized properties.**

***Index Terms*—Side-channel attacks, immunity testing, probes, field programmable gate array.**

I. Introduction

Fault injection is a continuous threat for cyber-physical systems, as it permanently improves with new concepts and equipment efficiency. Even if the laser method is still the most effective to accurately inject faults into a circuit, recent research give more interest to less intrusive and cheaper techniques.

Used mainly as a listening tool for side channel attack on retrieving electromagnetic traces, the Electromagnetic fault injection (EMFI) has emerged as an efficient tool for fault attacks. As an alternative for the laser method, it can be used at both front side or back side of a secured integrated circuit. It can also be used without the need of extra chip preparation to remove protection layers. Hence it is one of the attack means which requires a low-cost global setup. To succeed an EMFI, one has to consider the efficiency of the injection bench which largely depends on the probes. In addition to characterization of electric [4] and magnetic probes [5], experimental results show the evolution of the designed probes with different geometries and properties, and point out the differences between commercial and homemade probes. Oumarouayache et al. have presented in [2] a guidance for magnetic probe design using simulation. Further experiments by Ordas et al. [3] show that different properties of the probes (e.g. number of loop) can lead to a better pulse excitation and resulting impact when testing on real target.

The main contribution of the study presented in this paper is to evaluate the impact on the propagation delay of a combinational logic path when the properties of the EMFI are subject to variation. In the experiments we have considered four electromagnetic pulses parameters (the pulse amplitude, the number of pulses, the injection timing and the pulse polarity).

The detailed experimental setup will be described in section II. Section III will present the test results of the characterized EMFI parameters. Finally, section IV draws conclusions and provide perspectives.

This research is financially supported by the "Fonds Unique Interministériel" (FUI, French Government) through the CSAFE+ program.

II. Characterization at Logical Level

Faults in an Integrated circuit (IC) are created by EMFI either directly when the logic state of some storage elements such as flip-flops is inverted, or when the propagation delay of some combinational paths is so increased that their output is stored while the right value is not arrived [3]. These previous works have focused on the impact of EMFI on a large chain of flip-flops.

In a complementary way, our method involves a large cascade of combinational logic gates, whose nominal propagation delay is denoted by t_p. Under EMFI, this delay is subject to variations, and we define its measurements as t'_p. Therefore, at a position (x, y) of the probe, the impact $\Delta t_p(x, y)$ can be evaluated as the difference between $t'_p(x, y)$ and t_p.

The test design has been generated as a cascade of buffers and programmed in a reconfigurable IC, namely Field-programmable gate array (FPGA). The presented characterization and measurements in this paper has been achieved using a non decapsulated FPGA FPGAs Xilinx Virtex-II Pro manufactured in 90 nm process technology.

Since the propagation delay of a single buffer depends on the process technology, the propagation delay of the whole cascade is a multiple of the number of buffers. With the use of 5888 buffers within the implemented design, the corresponding delay value t_p is about 2.23 µs The placement of the design has been constrained to the bottom part of the FPGA, as visible in the floorplans of fig. 1. In this way, it is possible to check whether there is a correlation between the impact of an EMFI and the position of the injection probe.

Figure 2 is the timings diagram of the EMFI: At t_{in}, the input signal of the test design is flipped to the high logic state. The signal arrives at the output at time t_{out}, or at t'_{out} when an EMFI impacts the nominal propagation delay t_p by Δt_p. The figure illustrates a positive impact, which corresponds to a deceleration of the propagation, but experiment also shows that the impact can be negative ($t'_{out} < t_{out}$), meaning an

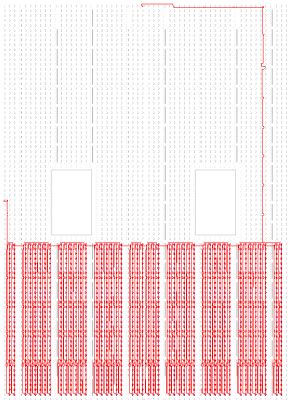


Figure 1. Floorplan of bigDelay for Xilinx Virtex-II Pro.

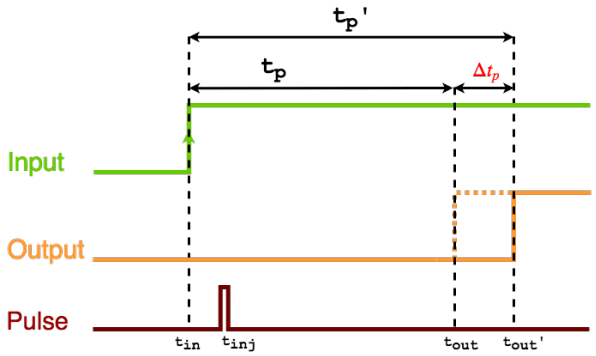


Figure 2. EMFI timings diagram.

acceleration of the propagation. In both cases, the EMFI has to occur during the propagation, i.e. between t_{in} and t'_{out}. Indeed, a modification of the propagation delay while the output has been updated is unobservable.

The propagation delay between the rising edge of the input signal and that of the output signal is measured using an internal function of an oscilloscope. EMFI is proceeded by generating a single pulse with a rising and falling edge of 1 ns, hence a width of 1.5 ns. The rest of the EMFI test bench is very similar to that of [1, fig. 1]: A 330 MHz pulse generator, whose output amplitude is set up to 0 dBm, driving a 10 kHz to 400 MHz 260 W class A broadband amplifier. The magnetic probe is connected to its output, and moved over a FPGA using a 4-axis positioning system (fig. 3).

The probe used for the experiment, Arelis N1 (fig. 4), is an handmade prototype developed by the french company Arelis. It is built from a ferrite core whose shape is that of a circular truncated cone. The top diameter is about 1.5 mm and the bottom diameter equals 0.80 mm. The probe is designed with four turns of a 150 µm wire.

III. Experimental Results

The experimental results reported in this section correspond to the spatial distribution of Δt_p. For a given position (x, y), the propagation delay, with or without EMFI, is evaluated as

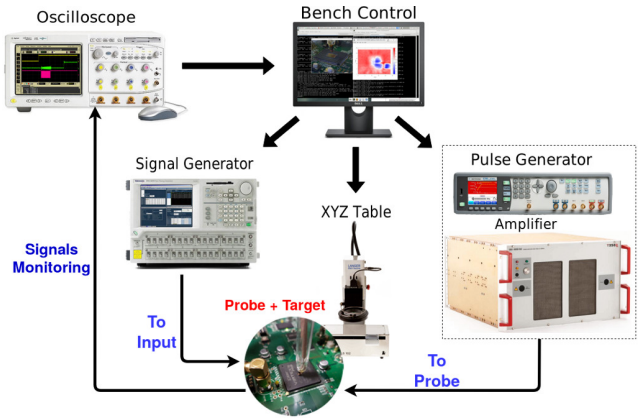
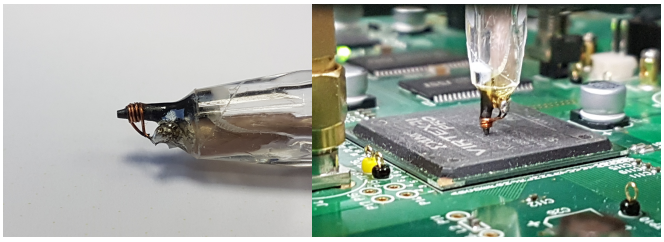


Figure 3. EMFI test bench.



(a) (b)

Figure 4. Photographs of the magnetic probe Arelis N1: (a) Head and (b) when scanning Xilinx Virtex-II Pro.

the arithmetic mean of ten measurements. The EMFI scan of the Xilinx Virtex-II Pro represents a square area of $24.0\,\mathrm{mm} \times 24.0\,\mathrm{mm}$ and obtained over 40×40 positions at a distance (z-axis) of 50 µm from the package.

Injecting only *one* pulse as defined in fig. 2 did not report major variation of $\Delta t_p(x, y)$ over the target. We evolved the EMFI as per the timing diagram described in fig. 5. A burst of 100 successive pulses distant from 3 ns with amplitude configured to 0 dBm is then injected. The starting time of the injection t_{inj} is equal the rising edge of the input t_{in}.

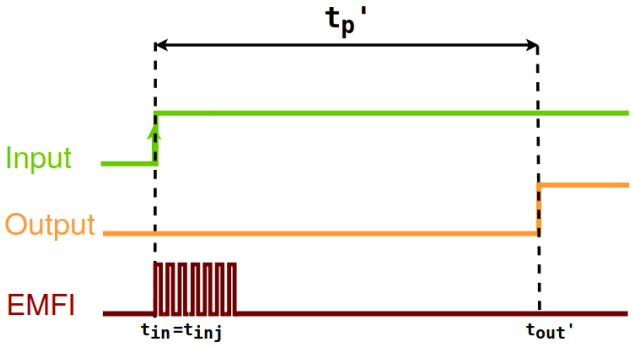


Figure 5. Injection model diagram with a burst of pulses.

The spatial distribution of Δt_p when injecting 100 pulses is presented in fig. 6. It shows as expected that the impact $\Delta t_p(x, y)$ can be either positive (**deceleration**) in red, or negative (**acceleration**) with the blue color. At least, three

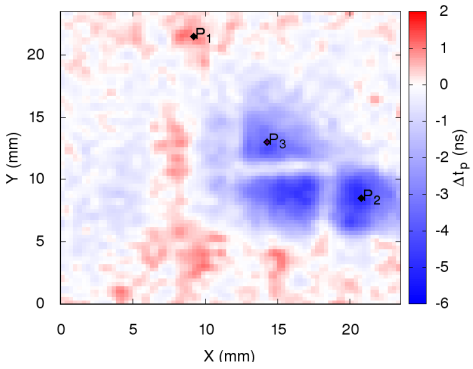


Figure 6. Spatial distribution of Δt_p when injecting 100 pulses.

separated zones of impact, following an acceleration behavior, can be clearly identified by their delimited areas. For the sake of clarity, three positions are considered in the following characterizations as shown by fig. 6. We will denote by **P1** the position for maximum impact resulting of the deceleration behavior and **P2** as the position for maximum impact resulting of the acceleration behavior. **P3** is a position from the center of the FPGA where we assume the die's location.

A. *Impact of injection timing*

Figure 7 shows the impact on Δt_p when a burst of successive pulses is injected during three different t_{inj} time chosen within an injection window i_w equal to the path delay t_p. The burst is set up with 100 of successive pulses distant from 3 ns, while the pulse amplitude is configured to −6 dBm.

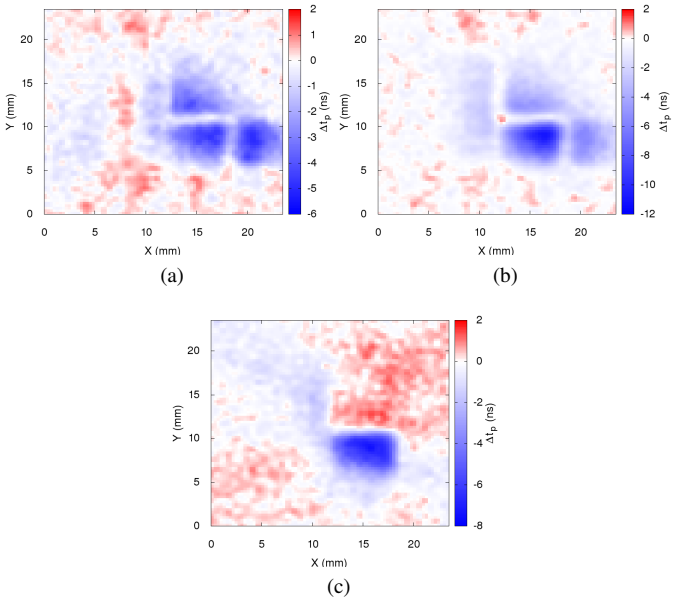


Figure 7. Spatial distribution of Δt_p when 100 pulses are injected (a) at the beginning ($t_{inj} = t_{in}$) of the computation, (b) in the middle ($t_{inj} = \frac{i_w}{2}$) and (c) later ($\frac{i_w}{2} < t_{inj} < t_{out}$).

Whatever the injection time t_{inj}, all results report a maximal positive impact of 2 ns. However, a maximum negative impact of −12 dBm is reported when the burst is injected at $t_{inj} = \frac{i_w}{2}$ as per fig. 7b. It is basically the double of the generated acceleration when $t_{inj} = t_{in}$ fig. 7a. While this impact is about −8 ns when t_{inj} is configured between $\frac{i_w}{2}$ and t'_{out} fig. 7c, the spacial distribution of the resulted impact is different from the previous t_{inj} values and present less delimited areas.

For a better analysis of this behavior, a more elaborated test is proceeded and we focused on the results from positions P1, P2 and P3. The injection window i_w is expanded to cover out the time before and after the path delay t_p. It is set up to start 3 µs before t_{in}, and set to end 950 ns after t_{out}. The injection time t_{inj} will move through a step of 100 ns within this configuration of i_w. The timing diagram of this test is described in fig. 8.

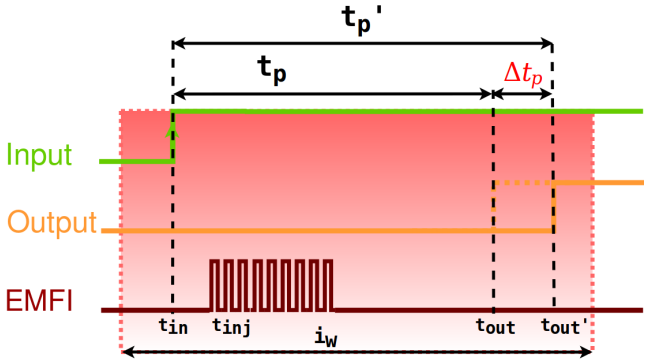


Figure 8. Injection model diagram for a burst during $i_w > t_p$.

The impact is at its maximum during an injection window which seems to have the same duration of the initial path delay t_p, and identified in fig. 9 by the two vertical red lines. Outside this window, the impact is at its minimum.

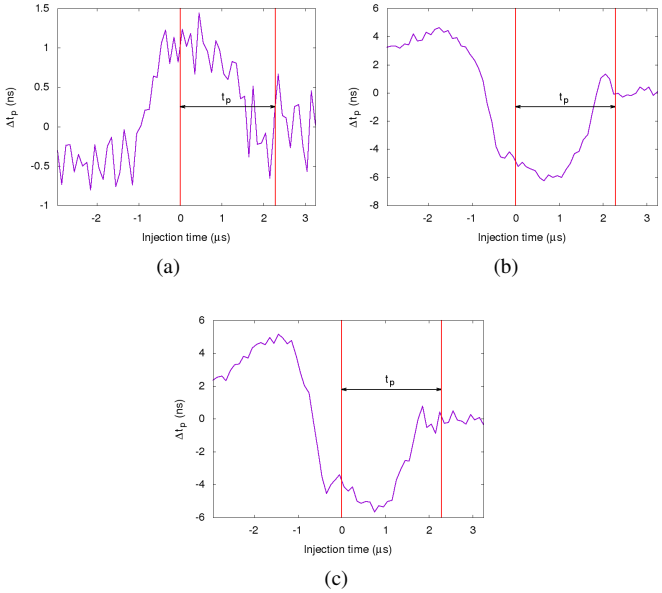
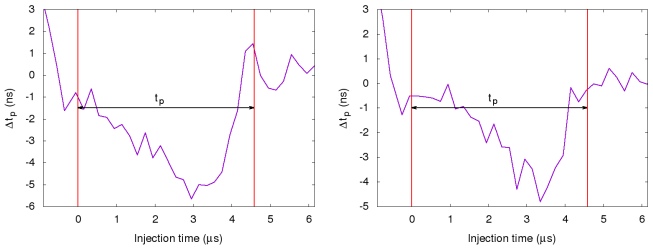


Figure 9. Variation of Δt_p according to the injection timing t_{inj}, for bigDelay and positions (a) P1, (b) P2 and (c) P3.

To validate this hypothesis, we implement a new design bigDelay Double with twice the number of buffers (11 776 of logical blocks) in order to double the path delay. Measurement of the path delay t_p from this new design report 4.57 µs. Depicted by fig. 10, the tests done at the positions P2 and P3 confirm that the impact window is in turn doubled and that impact follow the same behavior as for the first bigDelay design.

In the end, those results are not really surprising, since no impact on the output should be reported before the input is flipped to the high logic state. In the other hand, for any EMFI that came after the output, it will no longer have impact since the logic gate has already updated its output.



(a) (b)

Figure 10. Variation of Δt_p according to the injection timing t_{inj}, for bigDelay Double and positions (a) P2 and (b) P3.

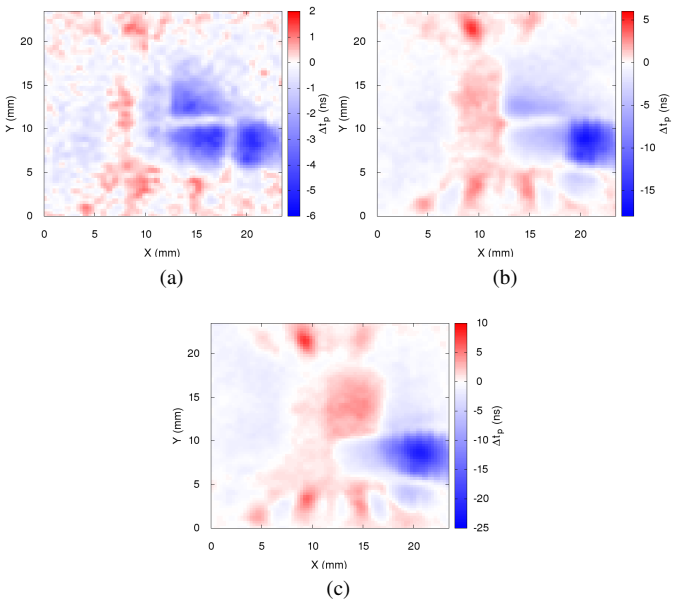
B. Impact of EMFI pulse number

Figure 11 shows the impact on Δt_p for different numbers of successive injected pulses. The burst is set up with successive pulses distant from 3 ns and the pulse amplitude configured to −6 dBm. From the resulted EMFI scan, the maximum impact is reported when using 650 pulses (fig. 11c), with a maximal value of 10 ns as positive impact and −25 ns for the negative impact. From the shape of the impact areas at the borders of the target, we assume that we are facing a coupling with the FPGA bonding or the capacitors. We observe also that the central zone of the FPGA between fig. 11a and fig. 11b is switching in impact polarity when we reach an amount of pulses number.

We studied this behavior by checking the impact on Δt_p (fig. 12) for positions P1, P2 and P3 when the number of pulses ranges from 1 to 650 with a step of 5. There is a clear linear evolution of the impact regarding the increase of the pulse number for positions P1 (fig. 12a) and P2 (fig. 12b). For those positions, we observe a short period of saturation when we are close to the maximum number of injected pulses (i.e close to the end of the the propagation time t_p). Above 600 pulses, there is no more impact induced on the FPGA.

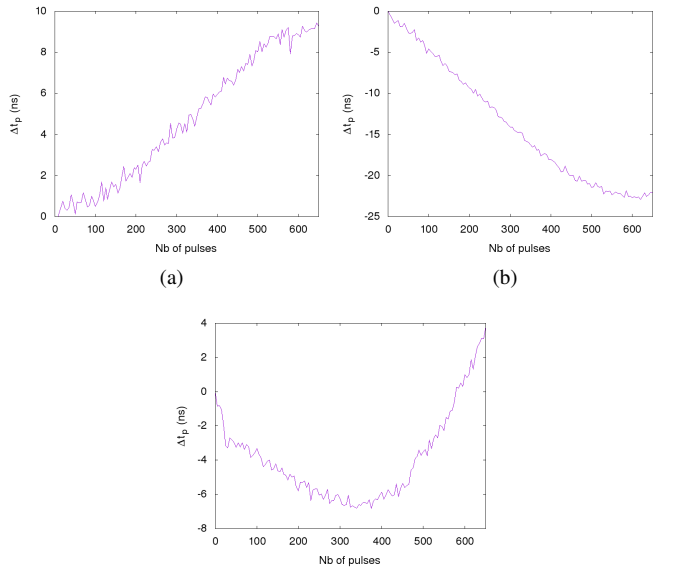
When the probe is above the FPGA's die at position P3, the impact follow a different behavior. Figure 12c shows a linear increase of the impact until a number 400 of pulses, then an opposite linear effect of the impact to reach Δt_p near 0 ns.

We repeated the same test using the design bigDelay Double and fig. 13 shows the induced impact for positions P1, P2



(a) (b) (c)

Figure 11. Spatial distribution of Δt_p when injecting (a) 100, (b) 350 and (c) 650 pulses.



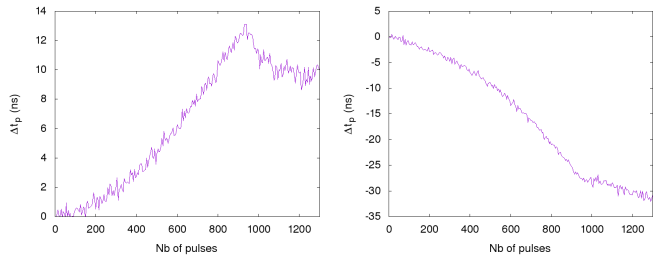
(a) (b) (c)

Figure 12. Variation of Δt_p according to the pulse number, for bigDelay and positions (a) P1, (b) P2 and (c) P3.

and P3. Results confirm that we still have similarity of the IC behavior under EMFI. The one major conclusion from those results that the increase of the number of pulses do not impact in the same way the FPGA's die and the edges of its package.

C. Impact of EMFI pulse amplitude and polarity

Figure 14 shows the impact on Δt_p when the output amplitude A_{dBm} of the pulse generator is set to −19 dBm, −12 dBm and −6 dBm. We used the same burst configuration with pulses separated from −6 ns and the number of pulses is



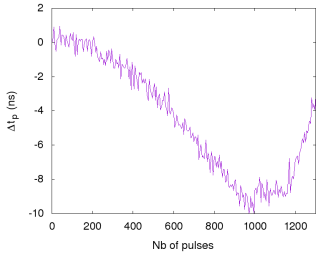
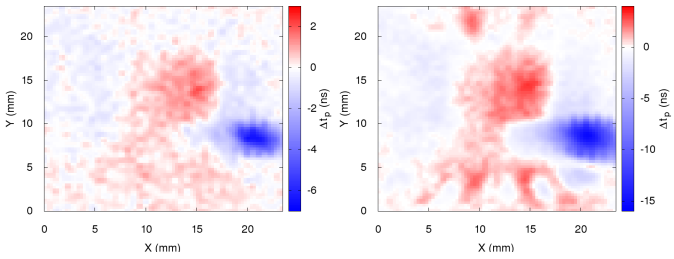


Figure 13. Variation of Δt_p according to the pulse number, for bigDelay Double and positions (a) P1, (b) P2 and (c) P3.



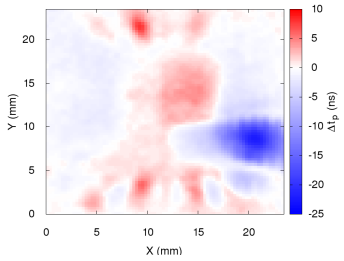
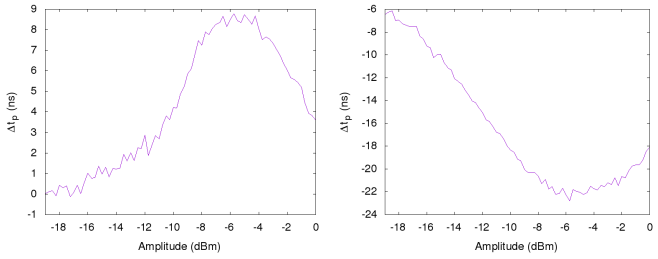


Figure 14. Spatial distribution of Δt_p for a pulse amplitude of (a) −19 dBm, (b) −12 dBm and (c) −6 dBm.

set to 650. From fig. 14a to fig. 14c, we have a clear evolution of the impact in term of value and of spacial resolution. The sharpness of the spacial distribution came also with more details about the impacted areas by the EMFI, located at the top and bottom of the package. however, the spatial distribution of the impact is basically the same for the all tested amplitude.

Figure 15 show the resulted impact for the selected positions P1, P2 and P3 when the configured pulse amplitude ranges from −19 dBm to 0 dBm with a step of 0.25 dBm. As long as A_{dBm} increases, t'_p increases in turn, following a linear function. There is even an impact of −6 ns at the minimal value of A for the position P2. To note that there's a decrease of the impact starting from −6 dBm to 0 dBm for positions P1 (fig. 15a) and P2 (fig. 15b). Unlike this behavior, the one reported from position P3 (fig. 15c) is following a continuous linear increase from −19 dBm to 0 dBm. similarly to the results for the increase of the number of used pulses during the EMFI, The FPGA's central area report a different sensitivity regarding the pulse amplitude increase than for the other areas (i.e. FPGA border).



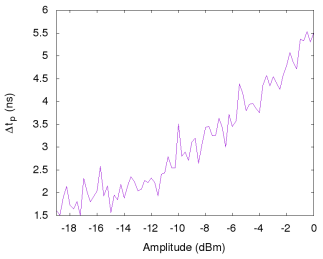


Figure 15. Variation of Δt_p according to the pulse amplitude for positions (a) P1, (b) P2 and (c) P3.

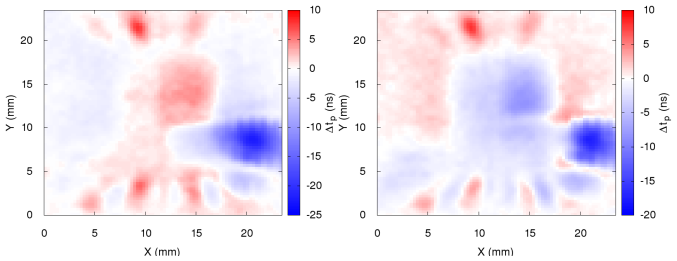


Figure 16. Spatial distribution of Δt_p for (a) positive and (b) negative pulse polarity.

Figure 16 show the impact Δt_p for both positive and negative polarity of the EMFI. We kept the setup configuration with amplitude −6 dBm and a burst of 650 successive pulses separated from 3 ns. both results fig. 16a and fig. 16b report the same spatial distribution of the impact at the top and bottom borders of the FPGA. Means that switching the pulse polarity do not seems to have a different impact on the bonding. However, some zones turn from red to blue and vice versa, especially in the center of the package where we suppose the

FPGA's die location. We thus conclude that pulse polarity can have a direct impact at the logic level and further tests are planned to study this behavior.

IV. Conclusions & Perspectives

By proceeding with an EMFI on a combinational logic based design implemented into a 90 nm FPGA process technologies, this paper presents a characterization study of the EMFI parameters as the pulse amplitude, the number of pulses, the injection timing and the pulse polarity. First, we note that there's a need for more than one pulse to lead to a significant impact on the path delay of our pure combinational logic design bigDelay. In addition, the experiments highlighted that the impact is different for each position of the FPGA package. However, regarding the generated EMFI amplitude, it presents the same spatial distribution. We also observed that, the use of the burst mode and the increase of the pulse number can lead to a better impact intensity. To note that this increase of the number of pulses do not impact in the same way the FPGA's die and the edges of the package.

In future work, we will investigate if different design layouts, i.e. placed at the opposite half-part of the FPGA, will induce a different impact. Another part of future studies is to undertake the same tests on other FPGA technology, and also to characterize further parameters of the generated electromagnetic pulse (i.e. pulse width, harmonic pulse ...).

References

[1] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria. Electromagnetic transient faults injection on a hardware and a software implementations of AES. In Guido Bertoni and Benedikt Gierlichs, editors, *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, pages 7–15. IEEE Computer Society, 2012.

[2] Rachid Omarouayache, Jérémy Raoult, Sylvie Jarrix, Laurent Chusseau, and Philippe Maurine. Magnetic microprobe design for em fault attack. In *2013 International Symposium on Electromagnetic Compatibility*, pages 949–954. IEEE, 2013.

[3] Sébastien Ordas, Ludovic Guillaume-Sage, Karim Tobich, Jean-Max Dutertre, and Philippe Maurine. Evidence of a Larger EM-Induced Fault Model. In Marc Joye and Amir Moradi, editors, *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*, volume 8968 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 2014.

[4] Laurent Sauvage. Electric probes for fault injection attack. In *Electromagnetic Compatibility (APEMC), 2013 Asia-Pacific Symposium on*, pages 1–4. IEEE, 2013.

[5] Christian Wittke, Zoya Dyka, and Peter Langendoerfer. Comparison of em probes using sema of an ecc design. In *New Technologies, Mobility and Security (NTMS), 2016 8th IFIP International Conference on*, pages 1–5. IEEE, 2016.