EM Injection: Fault Model and Locality

Sébastien Ordas, Ludovic Guillaume-Sage, Philippe Maurine

EM Injection: fault model and locality

S. Ordas
LIRMM, Univ. of Montpellier,
France
ordas@lirmm.fr

L. Guillaume-Sage
LIRMM, Univ. of Montpellier,
France
ludovic.guillaume-sage@lirmm.fr

P. Maurine
CEA-TECH/ LIRMM, Univ. of Montpellier
France
philippe.maurine@cea.fr
pmaurine@lirmm.fr

***Abstract*—EM injection recently emerged as an effective medium for fault injection. This paper presents an analysis of the IC susceptibility to EM pulses. It highlights that faults produced by EM pulse injection are not timing faults but correspond to a different model which is presented in this paper. This model also allows to explain experimental results introduced in former communications.**

***Keywords*-EM Fault Injection; EM fault model**

I. Introduction

Besides power and ElectroMagnetic (EM) analyses [6], [5], fault injection constitutes [2] a serious threat against secure circuits. Among the means used to inject faults within cryptographic IC, the laser [11] is undoubtedly the most popular because of its high spatial and temporal resolutions. However, fault injection with laser is facing difficulties. Among them one can identify the increasing number of metal layers (up to 12 levels) used to rout signals in a chip; this may prevent from the use of laser to inject fault through the frontside. The second difficulty one may point out is the long practice of laser injection and the related and progressive development of more and more efficient countermeasures like embedded laser shot detectors. It is therefore not surprising that adversaries are looking for new mediums for injecting faults.

Two fault injection means appeared recently. One of them is the injection of a voltage spike directly into the substrate of the targeted IC to produce ground bounces or voltage drops according to the polarity of the spike [12]. The other is EM injection which, despite the early warning of Quisquater et al. in 2002 [8], did only find recently a larger echo in the scientific bibliography despite its inherent advantages: ability to inject faults through the package and the frontside being the most important as highlighted in [10] in which a high frequency spark gap is used to produce faults in a CRT-RSA .

Two types of EM injection platforms can be mounted to induce faults into IC. Harmonic EM injection platform refers to the first type. It produces sine EM waves, that can be modulated in amplitude or not, to produce faults. Such type of platform has been reported efficient in [7] to disturb the behavior of an internal clock generator and in [1] to bias a true random number generator.

EM Pulse (EMP) platform refers to the second type of platform which is detailed in section II. It produces a single but powerful EMP that creates a sudden current flow in the power/ ground networks of IC and therefore voltage drops and/or ground bounces. Such type of platform was first reported efficient in [3] to inject faults into an old microcontroller designed with a 350nm technology. The analysis of the fault obtained using such a platform was conducted in [4]. This paper concludes that EM injection produces timing faults and more precisely setup time constraint violations. As a result of this observation, a delay-based glitch detector was evaluated against EM injection in [13] and demonstrated partially efficient.

If the results reported in [3] are convincing, they limit de facto the interest of EMP for injecting faults into smartcards. Indeed, nowadays smartcards are typically designed with the 90nm process and operate at a reduced clock frequency ($< 40MHz$). They are therefore characterized by large timing slacks (i.e. time margins between a circuit critical time and the clock period). They are thus quite robust to EM injection (considering the ranges and the slew rates of modern high speed voltage generators) if the latter does only produce timing faults. Indeed, producing timing faults in such circuits requires the use of extremely powerful pulse generator to produce sufficiently intense EMP. Additionally producing such EMP reduces the spatial resolution of EM injections.

To broaden the range of IC on which the EM injection is effective, [9] has shown that with probes focusing the magnetic field on a small part of IC surface it is possible to create bitsets, bitresets, single byte or mylti-bytes faults or even single bit faults. However, for their experimental demonstration, the authors targeted an IC in which the clock is intentionally during EM injections to avert the occurrence of timing faults. If the demonstration that EM injection can produce some bitsets and bitresets is convincing, one question remains. What types of fault appear preferentially when injections are performed while the Device Under Test

978-1-4673-7579-5/15 $31.00 © 2015 European Union
DOI 10.1109/FDTC.2015.9

(DUT) operates: bitsets, bitresets, timing faults or a mixture of all types?

Within this context, this paper aims at contributing to the State of the Art on EM injection by showing that faults produced within an IC while it operates are neither bitsets, nor bitresets or timing faults, but are what we call 'sampling faults'. These errors result from the disturbance of the D-type Flip-Flop (DFF) sampling process. As a second contribution, this paper shows that EM injection is local, much more than expected and reported in former works such as [3], [9].

The remainder of this paper is organized as follows. Section II shows the equipment used to carry out the experimental demonstration that EM injection produces sampling faults. Section III recalls the fundamentals related to synchronous IC, their operation and the associated sources of faults. Section IV defines the experiments as well as their goals and gives the obtained results. Finally, a conclusion is drawn in section V.

II. EM Injection Setup

This section describes the equipments that have been used to perform the experiments detailled in the rest of the paper. It should be noticed the equipements are similar (at some minor differences) to that presented in [9].

A. EMP-Injection platform

The EMP platform used during the experiments described in this paper is shown Fig. 1. It features a laptop that controls the whole platform through serial ports, a 3-axis positioning system to place the EM injector with an accuracy of $\pm 5\mu m$ at the surface of the DUT, a 3-axes vision system made of USB microscopes connected to the laptop. An oscilloscope is also used in order to monitor the synchronization between the EMP and the target's operations. The pulse generator is a main element of the platform. It delivers, to the EM injector, a voltage pulse of amplitude V_{pulse} as high as 400V (current 16A), with a width that ranges between 5ns and 35ns. Its settling times are lower than 2ns.

B. EMP-Injectors

In [9] three types of EM injectors are introduced: injectors with flat tip end, injectors with a sharpened end, and injectors with crescent shape. Fig. 2 shows the three types of injectors. In the remainder of this paper, we report results obtained with two injectors with: one with a crescent shape and the other with a flathead. They are shown Fig. 2a and c. The flathead injector used during our experiments has 7 loops wound around a ferrite core with a diameter equal to $800\mu m$. The distance, s, between the tips of the crescent-shaped injector we used is equal to $450\mu m$.

III. Source of failure of synchronous circuits

This section recalls the operation principle of synchronous IC, its advantages and drawbacks. These recalls are done to introduce the three main design constraints that must be observed in order to obtain circuits operating correctly, but also in order to list the main sources of potential faults.

A. Synchronous IC operation

A synchronous IC is a circuit in which exchanges of data between the various building blocks are synchronized by a global signal. This signal, the clock, orders the sampling, at regular time intervals, of the calculation results but also their transmission from one block to another. This design approach, as compared to asynchronous IC design, has two main advantages. The first is that data exchanges are performed at regular intervals, making the understanding of how a circuit operates intuitive.

The second is that a synchronous IC can pass through any logic states between sampling times t_s that correspond to the rising edges of the clock, without degradation of its functionality provided the results to be correct and stable at t_s i.e. at the arrival of the next rising edge. Here, a logic state means a vector formed by all the output values of all logic gates at a given time t. This is an important advantage of synchronous IC over asynchronous IC because it is not necessary to check (or even list) the validity of the logic states for the whole continuous time window (time window 2 on Fig. 3) between the sampling times t_s (time window 1 on Fig. 3). Indeed, it is just necessary to check that the IC is in a correct and steady state at t_s. This is usually achieved using Static Timing Analysis tools avalaible in CAD suites.

B. Circuit level timing constraints

However, these advantages are accompanied by some counterparties. All the constituting blocks of a given IC must perform their calculations within one sampling period, i.e. in less than one clock cycle, T_{CK}. Some design efforts are therefore required to integrate blocks performing complex operations under a high clock frequency.

The second issue is that the sampling elements that are currently integrated on silicon, the DFF, are imperfect and are not able to sample and transfer data instantaneously. Consequently, some constraints must be met: data must be stable $T_{setup}\ ps$ before the rising edge of the clock and remain stable $T_{hold}\ ps$ after.

These two constraints coming from the basic operation of DFF are associated, at circuit level, to the so called $Setup$ and $Hold$ time constraints reported in eq. 1 and 2 and illustrated by Fig. 3 in which appears the time window

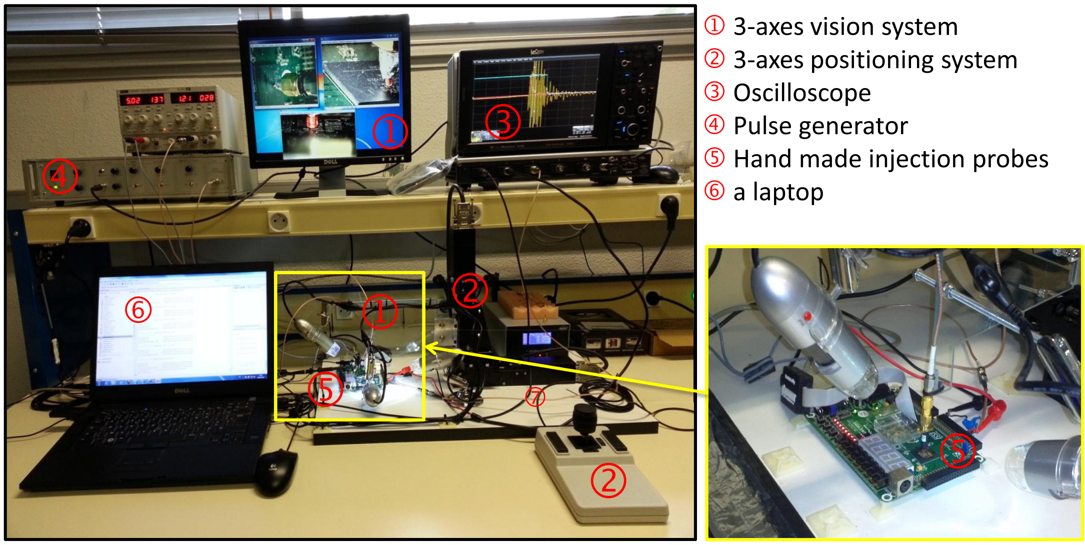

Figure 1. EMP platform used for all experiments reported in this paper.

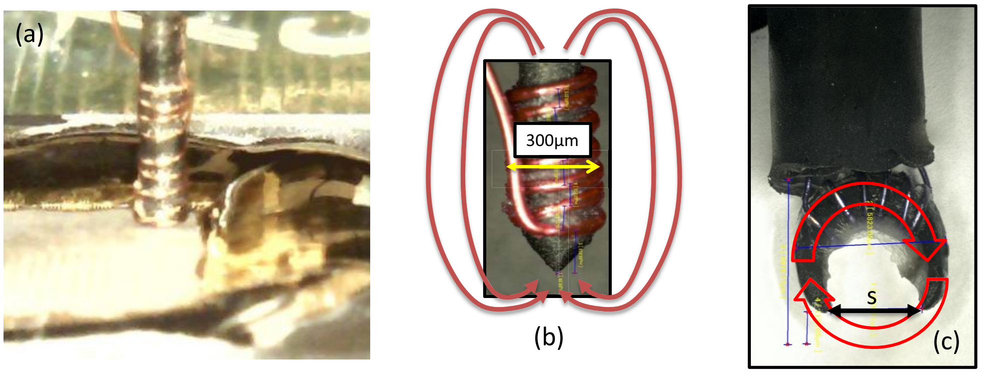

Figure 2. EMP-Injectors: (a) 'Flat' Injector (b) 'Sharp' Injector and (c) 'Crescent' Injector

during which data must be correct and stable (regions 1).

$$T_{CK} > D_{CK2Q} + D_{Q2D} + T_{Setup} + D_{Skew} \quad (1)$$

$$D_{CK2Q} + D_{Q2D} > T_{Hold} + D_{Skew} \quad (2)$$

In these equations, T_{CK} stands for the clock signal period, D_{CK2Q} for the propagation delays of DFF, D_{Q2D} for the delay of the combinational blocks and D_{Skew} for the clock skew.

C. Sources of timing constraint violations

Given these $Setup$ and $Hold$ time constraints, one can define different scenarios leading to the occurrence of a fault produced by an EMP.

1) Timing faults.: Let us start with the one put forward in [4]: the timing fault model. In this model, the EMP induces a voltage drop sufficiently important for increasing the propagation delay of the data, D_{Q2D}, so that a violation of a setup time constraint (eq. 1) occurs.

According to this model and to eq. 1, several criteria or tests can be defined to experimentally determine if EM injection follows the timing fault model or not. Indeed, following eq. 1, a first test could consist in trying to avoid the apparition of a setup constraint violation (being given an EM injection repeated with the same settings) by reducing the clock frequency, i.e. by increasing T_{CK}. A second test could consist in producing at different times t_{pulse} within the same clock period the same EM injection and then in

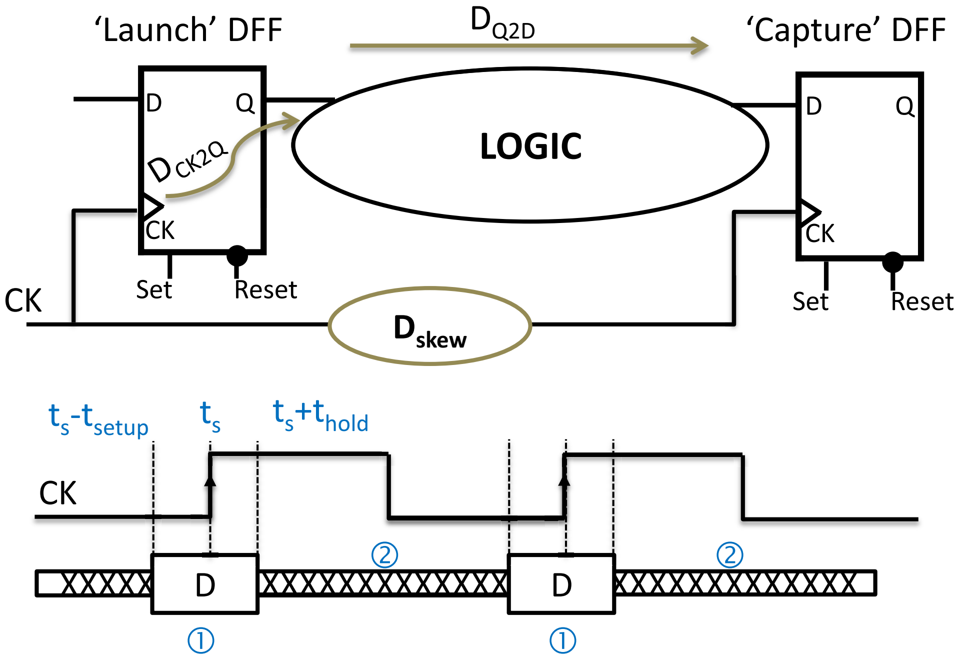

Figure 3. Setup timing constraint in a synchronous IC

verifying that the occurrence of the fault is independent of that parameter. Indeed, independently to the time t_{pulse} at which an increase of D_{Q2D} is produced (the beginning of the clock period, the middle or the end) if the delay increase is sufficient a fault appears.

One may probably define other tests. However, these two tests, denoted by *TFM (Timing Fault Model) tests*, afterward were considered sufficient during the experimentations detailed in section IV-C to verify whetever EM injections induce timing faults or not.

2) Sampling faults: This model relies on the assumption that EM injection is able to sufficiently modify the amplitude of one or several DFF input signals $(D, CK, Set, Reset$ in Fig. 3) during their switching (region 1 on Fig. 3) so that the gate level setup or hold time constraint is violated; violation that results in an erroneous sampling and/or transfer of the input data onto the outputs. It is important to note that violating these gate level constraints is different to violating the related circuit level constraints defined by eq. 1 and 2. Indeed, the propagation delays and other timing figures involved in these equations could still have satisfactory values even if EM injection breaks the data stability just before or during the rising clock edge.

We searched for some tests to check if the 'sampling fault' model is a valid EM injection model or not. For that, similarly to what we did for the timing fault model, we analyzed the various implications of the sampling fault model.

Among them, one may observe that if EM injection produces such faults then these faults can solely appear when the EMP is produced just before or after the occurrence of a rising clock edge (i.e. at times t_s) and more precisely during the 'sampling windows' corresponding to the effective switching of DFF. Additionally, if this EM fault model is valid, these time windows (denoted afterward by 'susceptibility windows') during which EM injection is able to produce faults, are :

- periodic with a period equal to T_{CK} and have a width independent of the clock frequency. Indeed, T_{setup} and T_{hold} depend only of intrinsic parameters related to the design of DFF (such as schematic, layout, technology or supply voltage ...).
- are necessarily separated by time slots during which the probability to produce a fault is null if the 'sampling model' is correct; these windows are corresponding to EM injections that do not fall within the EM susceptibility window of DFF.

All these interesting implications of the 'sampling model' define the *SFM (Sampling Fault Model) test* were used to

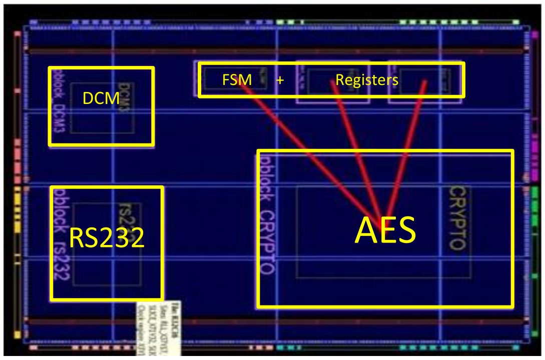

Figure 4. DUT floorplan

check if EM injection produces sampling faults during the experimentations described in section IV.

IV. Objectives and related experimentations

This section describes, first, the DUT used during our experiments. Secondly, it describes the experiments we did to determine which model is valid among the timing fault model and the sampling fault model. Thirdly, the results of these experiments are presented and analyzed.

A. Device Under Test

The DUT adopted to conduct our experiments is an FPGA (xilinx Spartan 3E-1000), designed with a 90nm process, on which four functional blocks have been mapped. The first is a Finite State Machine (FSM) operating at $50MHz$. It controls all the events and contains registers for storing the encryption / decryption result and the ciphering key. The second is a Digital Clock Manager (DCM) providing on command a frequency of $100MHz$, $50MHz$ or $25MHz$ to the third block. The third block is an AES-128bits. It ciphers a plaintext in 10 rounds at either $100MHz$, $50MHz$ or at $25MHz$. Finally, the fourth block is an RS232 enabling communications between the finite state machine and the outside of the circuit. The floorplan of the circuit, which was established under constraint to separate the block is visible Fig. 4. These design constraints were fixed to enable the analysis of EM injection effects spatially.

B. Objectives

If in the previous paragraphs, the focus was put on the various possible fault models, one of the first questions we addressed is the location of faults that are produced, injection being delivered during the ninth round of the AES. Mappings revealing the probability to induce a fault have been therefore established for the DUT described above. The obtained faults were also analyzed to reveal their nature (multi-bits, single bit ...), the number of faulted bytes or again the injector positions leading to disrupt each of the sixteen bytes manipulated by the AES.

Following these preliminary experiments, EM injection campaigns were conducted with the injector placed at selected positions above the DUT. These campaigns aimed at applying the *TFM and SFM tests* defined in section III to identify which model is the most relevant.

C. Experimental results

This section describes the experimental results and the protocols that have been followed to obtain them.

1) Experiment n^o 1: locality of the EMP injection.: The mappings revealing the probability to induce a fault, with both types of injectors, were obtained by performing at each coordinate (x, y) 100 injections with 10 plaintexts randomly selected before launching the experiments. These EMP injections were acheived by providing to the injectors a voltage pulse of amplitude $V_{pulse} = 44V$ and a pulse width $PW = 8ns$. The end(s) of the injectors were in contact with the IC surface. The operating frequency of the AES was fixed at $100MHz$ and the core supply voltage Vdd was set to $1.2V$, the nominal voltage of the DUT.

The mappings performed with the flathead injector were achieved with a displacement step $\delta x = \delta y = 200\mu m$. Those performed with the 'crescent' injector with $\delta x = 100\mu m$ and $\delta y = 100\mu m$. Fig. 5a and b gives the probability of inducing a fault with an EMP. In the case of the flathead injector, two types of faults were observed: some faults were erroneous ciphertexts and other were 'no-response'. The latter case corresponds to the situation in which the FPGA stops operating correctly and does not provide any response either a good one or a wrong one. Fig. 5c shows the coordinates at which 'no-response' were obtained. It should be noticed that only correct or erroneous ciphertexts were obtained with the 'crescent injector'.

As can be seen Fig. 5a, EM injections performed with the 'crescent' injector is local. Indeed, faults are obtained with a high probability level in disjoint areas corresponding roughly to the floorplan adopted during the design of the DUT. These regions correspond respectively with the placement of the AES, the placement of the registers storing the key and the ciphertexts, but also to the placement of the FSM. It is interesting to notice that faults produced with the 'crescent' injector placed above the FSM did not stop the circuit operation but are 'erroneous' ciphering.

Similarly, one may observe Fig. 5b that EM injection conducted with the flathead injector are also local but

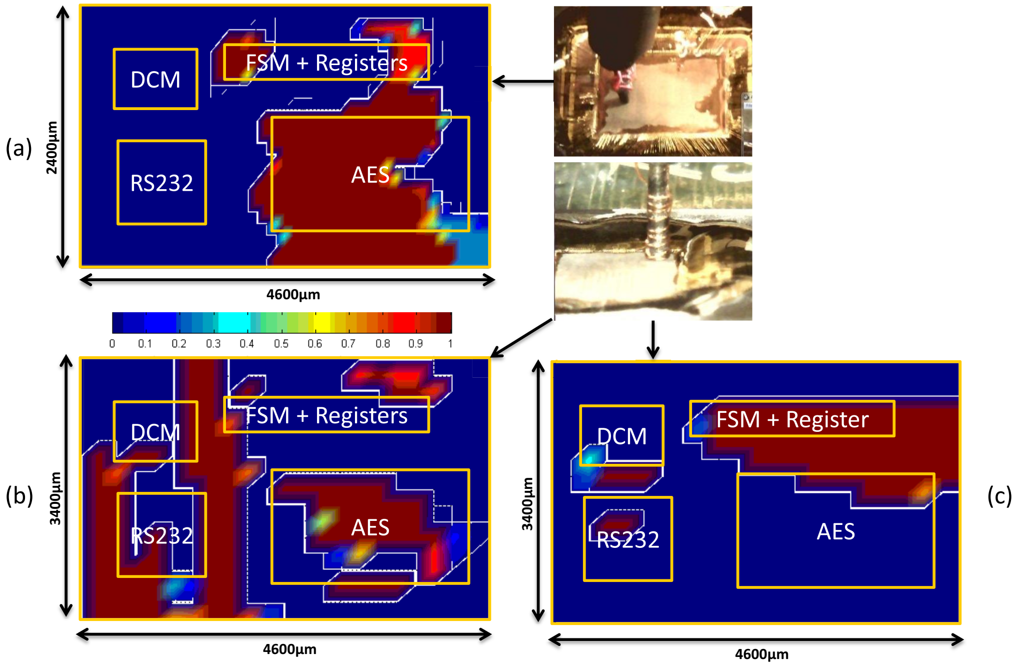

Figure 5. Probability to induce (a) a bad ciphering with the 'crescent injector', (b) a bad ciphering with the flathead injector and (c) a 'no-response' with the flathead injector

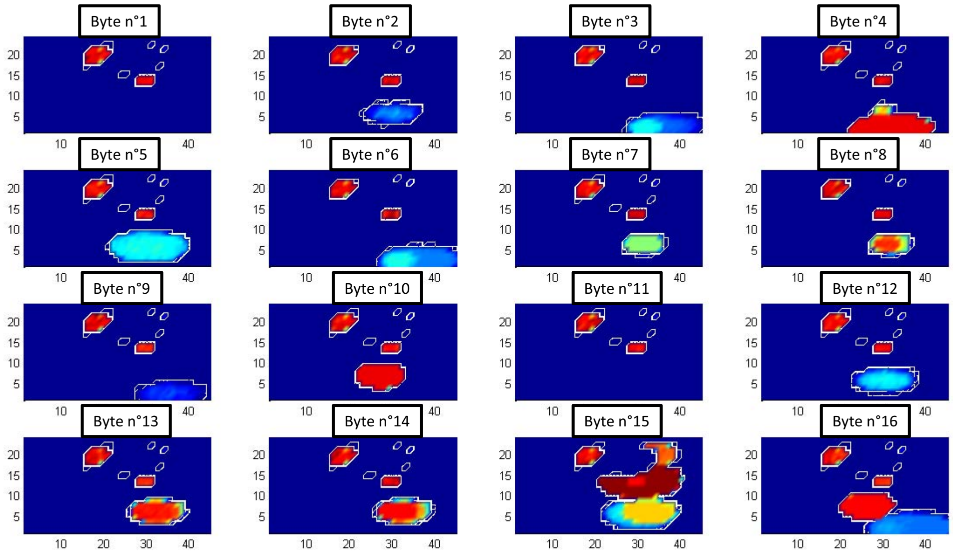

Figure 6. Probability to fault each byte wrt to the positioning of the 'crescent' injector (the color scale is the same than in Fig. 5)

that coordinates with a high level of probability are really different to that of Fig. 5a. Indeed, there are less coordinates on top and around the AES leading to faulty responses and there are much more coordinates in the neighborhood of the FSM and of the DCM leading to faults. In addition to these spatial differences probably explained by the different radiation diagrams of the injectors, the main divergence between the results obtained with the two probes is the appearance of 'no-response'. Many injections performed with the flathead injector produced a 'no response' while there is not with the 'crescent probe'.

If those mappings reveal the local nature of EMP injection, this characteristic appears much more evident when the link between the positioning of the injector and the faulted bytes processed by the AES is analyzed. Fig. 6 gives, in case of the 'crescent injector', the probability to induce a fault in each of the 16 bytes processed by the AES with respect to the positioning of the injector. As can be seen the positioning the injector has an influence on the fault rate at a given byte, and the positions at which it is easy to induce a fault in given byte are different to that of other bytes. They are of course positions at which several bytes are faulted.

The local character of EM injection being highlighted, and the coordinates (x, y) associated with a high probability to induce a fault being known, the experimentations aiming at identifying which model between the *timing fault model* and the *sampling fault model* is the more realistic were conducted.

2) Experiment n^o 2: EM Injection Fault model: More particularly, several EM injection campaigns were conducted with the crescent-shaped injector positioned at three distinct coordinates characterized by a high probability to produce faults (Fig. 5). During these injection campaigns two experimental variables were considered.

The first one is the operating frequency of the AES that can be fixed to three values by the DCM: F_{AES} = $25MHz$, $50MHz$ and $100MHz$. The second experimental variable is t_{pulse}, i.e. the time at which the 100 EM injections are produced (still with the same random plaintexts). The range of t_{pulse} values was chosen according to F_{AES} so that to sweep the whole execution of the AES algorithm (11 clock cycles). It should be noted that during these experimental campaigns, other injection parameters were kept constant to the following values $V_{pulse} = 44V$ and $PW = 8ns$.

The obtained results allowed to draw Fig. 7 which reports the evolution of the number of faulted bytes with respect to t_{Pulse}, i.e. wrt time for F_{AES} = $100MHz$. As can be seen, time slots during which it is possible to induce a fault appeared. These are periodically spaced by $10ns$, value that corresponds to the clock period T_{AES}. These slots of a duration equal to $6ns$ are denoted by susceptibility windows in the rest of the paper. They are separated by time slots during which the susceptibility to EM injection is null.

Given these results and the two fault models established in section III, it seems that the more realistic EM injection model is the sampling fault model and not the *timing fault model*. Indeed, if observed faults were timing faults, there would not be time slots during which no fault is induced because the time at which the increase in delay caused by the EM injection begins does not condition the occurrence of a fault.

However, to better sustain this result, these experiments were repeated over the last three rounds of the AES successively clocked at F_{AES} = $100MHz$, $50MHz$ and finally $25MHz$. Fig. 8 shows, for the three clock frequency values, the evolutions of the probability to induce a fault. Observing these evolutions shows that the apparition of the susceptibility windows is independent of clock period and that the width of this window is constant and equal to $6ns$. Additionally, one may observe that the duration of the time slots during which no fault is produced increases linearly with the clock period: the duration of these time slots moving from $34ns$ at $F_{AES} = 25MHz$ to $4ns$ at $F_{AES} = 100MHz$. These observations confirm that the more realistic fault model for EM injection is the *sampling fault model*.

If these experiments are sufficient to demonstrate that obtained faults are of type 'sampling fault', in the case of the AES mapped onto an FPGA, similar experiments were performed on a modern 32-bit micro controller. The aim was to verify that the sampling fault model is not specific to the FPGA. This micro-controller is designed in a $90nm$ process, features an internal voltage regulator to maintain the core supply voltage at $1.2V$. Its main constituting block is an ARM cortex M4 processor clocked at $30MHz$. This micro-controller also embeds a hardware AES-128bits clocked at $120MHz$ ($T_{CK} = 8.33ns$).

Fig. 9 gives the probability to induce a fault for three values of V_{pulse}: $120V$, $160V$ et $190V$. The time slot on which the EM injections have been performed corresponds to three rounds of the AES. As can be seen, the observed behavior is similar to that found in the case of the FPGA. Three susceptibility windows, spaced by $T_{AES} = 8.3ns$ are clearly visible, indeed. However, they are of a duration that varies from $2.9ns$ to $4.25ns$ with V_{pulse}. These durations are lower than in the case of the FPGA ($6ns$). A likely explanation may be the typical value of the propagation

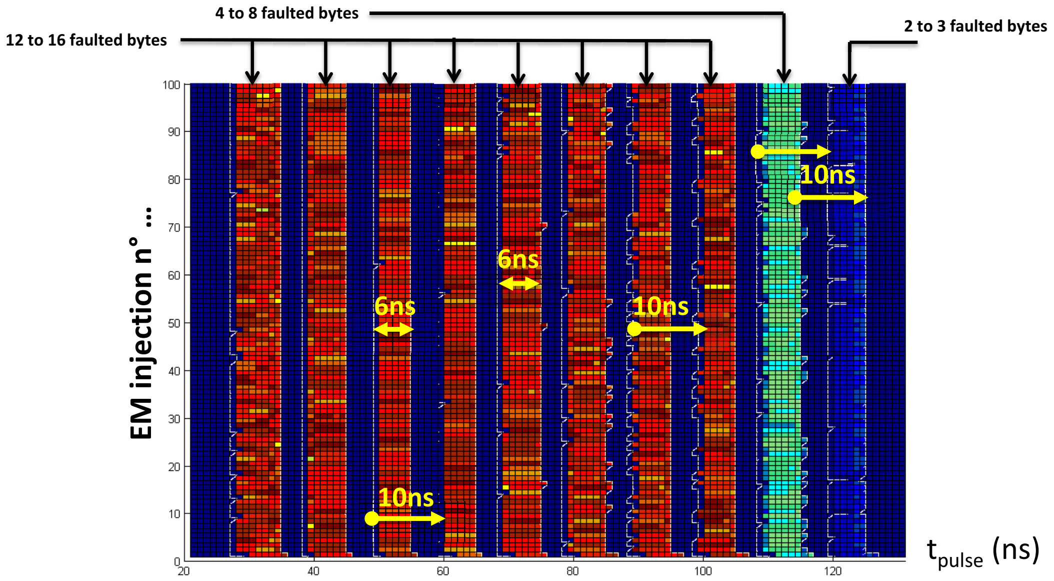

Figure 7. Number of faulted bytes wrt to t_{pulse} for the 100 plaintexts processed by the AES

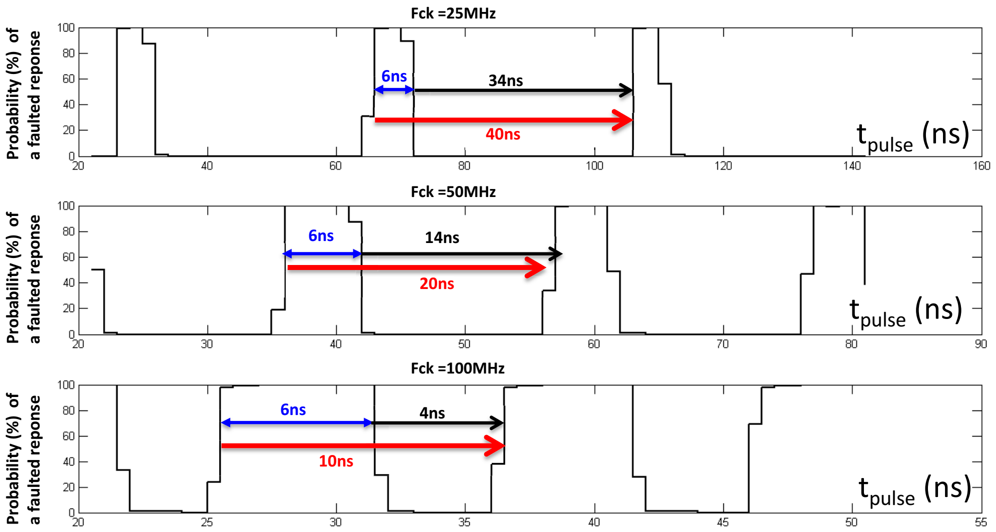

Figure 8. Evolution of the probability to induce a fault into the hardware AES mapped onto a spartan3-1000 wrt t_{pulse}

delay of D_{CK2Q} of the DFF which is significantly shorter in the case of the ASIC ($350ps$) that in the case of FPGA ($1ns$). More detail is given in the following paragraphs. Finally, these windows are more rounded than in the case of AES mapped onto the FPGA. This is mainly explained by a small timing jitter observed on the actual value of t_{pulse}; the injection timing being less reliable than in the case of the FPGA for which the clock signal is constructed from is an external clock source (a quartz) and not a PLL as for the micro-controller.

D. *Synthesizing results related to the EMP Injection Model*

Given the experiments and observations described in this paper, it seems that the fault model associated with the injection is the 'sampling fault' model, i.e. the disruption of the switching process of DFF, an event that can be induced at every rising clock edge. However, the authors of [9] postponed the possibility of inducing bitsets and bitresets on a circuit for which the clock signal is turned off, i.e. when DFF are at rest.

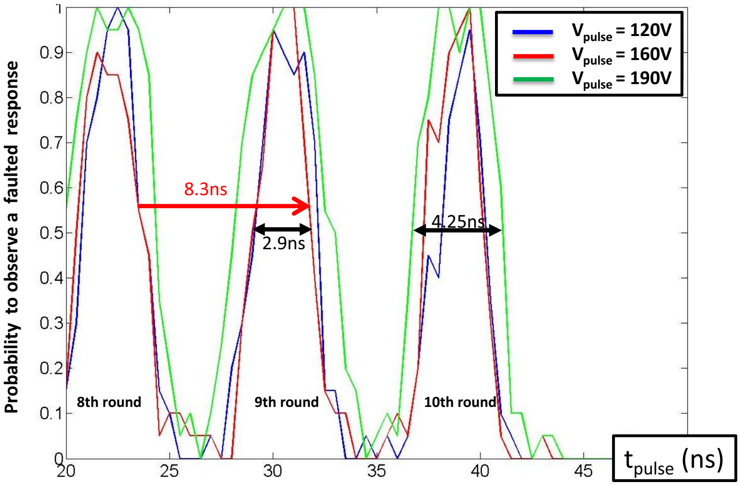

Figure 9. Evolution of the probability to inject a fault into the hardware AES embedded in the 32bit micro controller wrt t_{Pulse}

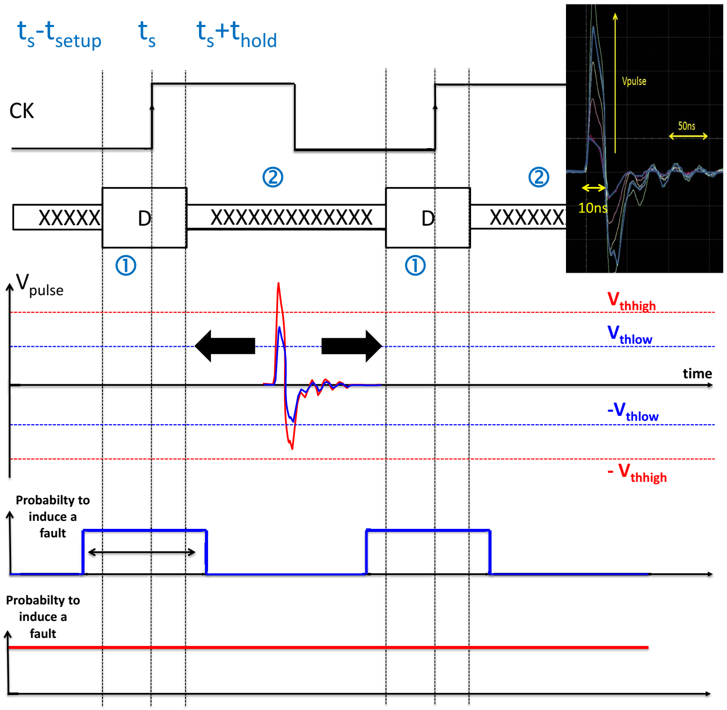

Figure 10. The sampling fault model

Given these two observations on the same type of circuit (xilinx Spartan3-1000) and with the same equipment but with different pulse amplitudes ($44V$ in this paper and more than $100V$ in [9]), we propose in this section a description of what could be the 'sampling' fault model, which appears the more realistic for EM injection. The latter is illustrated Fig. 10.

In this Fig. 10 appears in the upper right corner a picture of EMP generated with the system described in section II for increasing V_{pulse} values; these EMP were measured with a Langer probe. As shown, a voltage pulse produces two EMP: one positive and one negative associated to the rising and falling edges of the voltage pulse. The first one has typically a higher amplitude (in absolute value) than the first one. One may also observe that increasing V_{pulse} is equivalent to increase the amplitude of the EMP without increasing their width. It is assumed for shake of simplicity hereafter, that V_{pulse} is a direct measure of the EMP amplitude. This is equivalent to consider an ideal EM coupling between the injector and the DUT.

In Fig. 10, are also reported two threshold voltage values, V_{thhigh} et V_{thlow}, associated to the EM sucsceptibility of a DFF. V_{thhigh} is the minimum amplitude of the EMP that must be produced to induce a fault, i.e. a bitset or bitreset, in DFF at rest. V_{thlow} represents the minimum amplitude of the EMP that must be produced to induce a fault during the switching of a DFF. Of course, these threshold voltage values depend on many design parameters of the considered DFF but also of the Device Under Test that is defining the quality of the EM coupling between the injector and the DUT. It is also obvious that $V_{thhigh} > V_{thlow}$.

As illustrated, Fig. 10, such considerations are sufficient to explain the apparition of susceptibility windows when EM injections are performed with moderated values ($V_{thhigh} > V_{pulse} > V_{thlow}$) of V_{pulse}. Indeed, if the EMP are falling out of the time slot during which the DFF are switching, no fault is induced. Contrarily, for EMP falling within this time slot, there is a high probability to induce a fault. This is illustrated Fig. 10 in which appears a susceptibility window of width $\Delta t = 10ns$, the time during which the first (positive) EMP is greater than V_{thlow} neglecting the switching time of the DFF ($350ps$).

Now, if EM injections are performed with high enough values of V_{pulse} ($V_{pulse} > V_{thhigh}$), fault appear independently of the t_{pulse} value, i.e. even if the clock signal is disabled as in [9]. In that case, the probability to induce a fault is constant over time and depends, in practice, only on the existence of a sufficient EM coupling between the EM injector and the DUT. This is illustrated Fig. 10 by the red line.

V. Conclusion

Several EM injection campaigns were performed on an FPGA and a modern 32bit micro controller, both embedding a hardware AES-128bits. If these experiments have shown that EM injection is local, they have mainly contributed to highlight that the EM injections performed with a moderated power do not produce timing faults but disrupt the switching process of DFF. These observations, together with those described in [9], postponing the possibility of producing and bitsets or bitresets in DFF at rest, led to propose a specific EM fault model: the sampling fault model.

VI. Acknowlegdement

Authors would like to thanks the French Agence Nationale de la Recherche that supported this work through the contract ANR-12-INSE-005 E-Mata-Hari.

References

[1] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *COSADE*, pages 151–166, 2012.

[2] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In *EUROCRYPT*, pages 37–51, 1997.

[3] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, P. Orsatelli, Philippe Maurine, and Assia Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012:123, 2012.

[4] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *FDTC*, pages 7–15, 2012.

[5] Karine Gandolfi, Karine G, Christophe Mourtel, and Franncis Olivier. Electromagnetic analysis: Concrete results, 2001.

[6] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, pages 104–113, London, UK, 1996. Springer-Verlag.

[7] François Poucheret, Karim Tobich, Mathieu Lisart, Laurent Chusseau, Bruno Robisson, and Philippe Maurine. Local and direct em injection of power into cmos integrated circuits. In *FDTC*, pages 100–104, 2011.

[8] JJ Quisquater and D Samyde. Eddy current for magnetic analysis with active sensor. In *Proceedings of ESmart 2002*, page pp 185194. Eurosmart, 2002.

[9] K. Tobich J.-M.Dutertre P. Maurine S. Ordas, L. Guillaume-Sage. Evidence of a larger em-induced fault model. In *Proceedings of the 13th Smart Card Research and Advanced Application Conference*, 2014.

[10] Jörn-Marc Schmidt and Michael Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results. In Johannes Wolkerstorfer Karl C. Posch, editor, *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61 – 67. Verlag der Technischen Universität Graz, 2007.

[11] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. pages 2–12. Springer-Verlag, 2002.

[12] Karim Tobich, Philippe Maurine, Pierre-Yvan Liardet, Mathieu Lisart, and Thomas Ordas. Voltage spikes on the substrate to obtain timing faults. In *DSD*, pages 483–486, 2013.

[13] Loic Zussa, Amine Dehbaoui, Karim Tobich, Jean-Max Dutertre, Philippe Maurine, Ludovic Guillaume-Sage, Jessy Clédière, and Assia Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *DATE*, pages 1–6, 2014.