Electromagnetic fault injection: the curse of flip-flops

Sébastien Ordas, Ludovic Guillaume-Sage, Philippe Maurine

To cite this version:

Sébastien Ordas, Ludovic Guillaume-Sage, Philippe Maurine. Electromagnetic fault injection: the curse of flip-flops. Journal of Cryptographic Engineering, 2017, 7 (3), pp.183-197. 10.1007/s13389-016-0128-3 . lirmm-01430913

HAL Id: lirmm-01430913
https://hal-lirmm.ccsd.cnrs.fr/lirmm-01430913

Submitted on 25 Jun 2019

Noname manuscript No.
(will be inserted by the editor)

Electromagnetic Fault Injection : the curse of flip-flops

S. Ordas[1] · **L. Guillaume-Sage**[1] · **P. Maurine**[1,2]

the date of receipt and acceptance should be inserted later

Abstract ElectroMagnetic (EM) waves have been recently pointed out as a medium for fault injection within Integrated Circuits (IC). Indeed, it has been experimentally demonstrated that an EM Pulse (EMP), produced with a high voltage pulse generator and an injector similar to that used to perform EM analyses, was susceptible to create faults exploitable from a cryptanalysis viewpoint. An analysis of the induced faults revealed that they originated from timing constraint violations.

In this context, this paper demonstrates that EM injection, performed with enhanced injectors, can produce not only *timing faults* but also bit-set and bit-reset faults on an IC at rest. This first result clearly extends the range of the threats associated with EM fault injection. It then demonstrates, considering two different ICs under operation: an FPGA and a modern microcontroller, that faults produced by EMP injection are not *timing faults* but correspond to a different model which is presented in this paper. This model allows to explain experimental results introduced in all former communications.

Keywords Physical Attacks, Fault Attacks, EM injection, EM Susceptibility, Model

1 Introduction

Besides power and EM analyses [5], fault injection constitutes [4] a serious threat against secure circuits. Among the means used to inject faults within cryptographic circuits, the laser [12] 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 route signals in a chip; this may prevent from the use of laser to inject faults through the frontside. The second difficulty one may point out is the long practice of laser injection and the progressive development of more and more efficient countermeasures like embedded laser shot detectors. It is therefore not surprising that adversaries are looking for new media 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 [13]. The other one is EM injection which, despite the early warning of Quisquater et al. in 2002 [9], 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 gas spark is used to produce faults in a CRT-RSA.

Two types of EM injection platforms can be mounted to induce faults into circuits. 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 [8] to disturb the behavior of an internal clock generator but also to bias a true random number generator in [1].

EMP platform refers to the second type of platform which is detailed in section 2. It produces a single but powerful EMP that creates a sudden current flow in the power/ ground networks of the targeted IC and therefore voltage drops and/or ground bounces. Such type of platform was first reported efficient in [2] to inject faults into a quite old microcontroller (designed with a 350 nm technology). An analysis of the obtained faults was conducted in [3]. This latter paper concludes that EMP injection produces *timing faults* and

[1] LIRMM, Université Montpellier II
161 rue Ada, 34392 Montpellier CEDEX 5, France
[2] CEA Commissariat à l'Énergie Atomique et aux Énergies Alternatives
880 route de Mimet, 13120 Gardanne, France

more precisely setup time constraint violations. Following this observation, a delay-based glitch detector was evaluated against EMP injection in [14] and demonstrated partially efficient.

If the results reported in [2] are convincing, they limit de facto the interest of EMP for injecting faults into smartcards. Indeed, nowadays smartcards are typically designed with the 90 nm process and operate at a reduced clock frequencies (< 40 MHz). 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 EMP 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 the EMP injection.

In this context, the contributions of this paper are numerous although they all aim at broadening the scope of what is possible with EMP injection. The first one is the experimental demonstration that the EMP injection, performed with an enhanced EMP platform, can produce other types of faults that *timing faults*, namely bit-set and bit-reset faults. The second contribution is the demonstration that the EMP injection disrupts the switching process of DFFs leading to what we call *sampling faults*; a type of faults that explains all the observations reported in previous works. Finally, the third contribution is the definition of this *sampling fault model*.

The remainder of this paper is organized as follows. The principles followed to develop the enhanced EMP injection platform, used in all the experiments reported in this paper, are introduced in section 2. Section 3 describes the various mechanisms by which EMP injection could induce faults into a synchronous IC under operation. Some tests to experimentally discriminate which mechanism is the most likely to explain how EMP injection induces faults are then derived. Section 4 experimentally demonstrates EMP injection can produce bit-set and bit-reset faults in an IC at rest, i.e. in a circuit in which the clock signal has been disabled. This experimental demonstration is a first evidence that *timing faults* are not the sole type of faults that can induce EMP injection. Section 5 reports the results of experiments carried out to identify among the failure mechanisms highlighted in section 3 the one explaining at best all the experimental results obtained on an FPGA and a modern micro-controller. This mechanism being identified, a specific EM fault model is defined in section 6 before concluding in section 7.

2 EMP injection platform

Even if harmonic EM injection platforms, as well as EMP injection ones, are briefly described in [6], this section details the EMP injection platform used to obtain the experimental results reported in this paper. Both the setup and EMP injectors are discussed.

2.1 EMP platform description

The goal of an EMP injection platform is to generate, in the close vicinity of the targeted device, an intense and sudden variation of the magnetic field. This variation of the magnetic flow is then captured by some of the metallic loops formed by the power / ground networks or other interconnects. A sudden and intense current variation thus appears in the IC and results in voltage drops and ground bounces. Because, the IC does not operate under its nominal supply voltage, faults are expected to occur.

Our EMP platform is shown in Fig. 1. It features a laptop that controls all equipments through serial ports, a 3-axis positioning system to place the EMP injector with an accuracy of ± 5 μm at the surface of the Devices Under Test (DUT), a 3-axes vision system made of USB microscopes. An Digital Storage Oscilloscope (DSO) is also used to synchronize EMP injections with the operation of the target device. The pulse generator is a main element of the platform. It delivers, to the EMP injector, a voltage pulse of amplitude V_{pulse} as high as 200 V (current 8 A), with a width that ranges between 5 ns and 100 ns. Its settling times are lower than 2 ns. Because an adversary aims at injecting faults in some specific part of the target's computations while letting the other parts (computations) fault free, the EMP should be localized in the smallest possible area. For that, the adversary can design some specific and miniaturized EM injectors.

2.2 EMP injectors

Various EM injectors can be used according to the practical context. Fig. 2 shows three types of injectors we typically use. All are hand made and designed around a ferrite core to guide the magnetic field lines toward the target. All are also designed in different sizes. 'Flat' injectors (see Fig. 2-a) are designed with ferrite diameter ranging between 750 μm and 300 μm. 'Sharp' injectors are designed with tip end as small as 50 μm (see Fig. 2-b). Finally, 'Crescent' injectors are designed with an air gap separation 's' (see Fig. 2-c) between the ends as small as 450 μm.

The 'Flat' and 'Sharp' injectors are typically designed to localize the magnetic flow below the ferrite tip end. In that case, sharpening the tip-end of the ferrite (see Fig. 2-b), as proposed in [7], allows to further concentrate the flow into a smaller area and thus to expect a higher spatial resolution. Note however that contrarily to what has been obtained by simulation in [7], practice has shown that 4 to 7 turns around the ferrite provide better results than 1 or 2. Indeed, practice

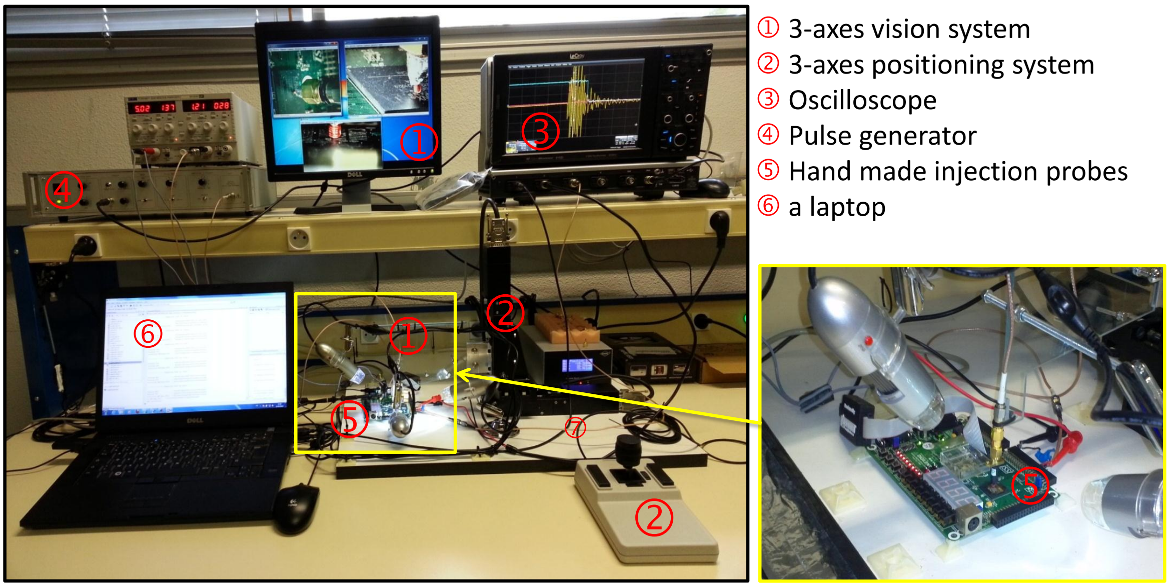

Fig. 1 EMP platform used for all experiments reported in this paper.

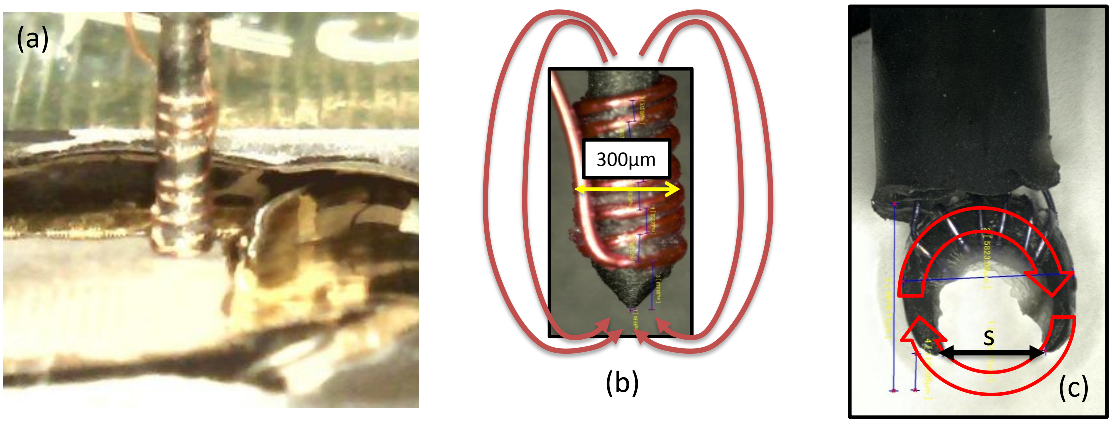

Fig. 2 EM Injectors: (a) 'Flat' Injector (b) 'Sharp' Injector and (c) 'Crescent' Injector

shows that increasing further the number of turns does not help in producing faults and can be counterproductive.

Several reasons could explain this discrepancy between simulation and practice. Among them one may observe that in [7], the recommendation for 1 or 2 loops is done for EM injectors without ferrite core. One can also observe that in [7], the goal is to generate the strongest magnetic field, while for EM injection it is preferable to maximize the magnetic field rate of change at the rising and falling edges of the pulse. Indeed, the main front door for EM injection is a coupling between two antennas.

If both the 'Flat' and 'Sharp' injectors are efficient, they have a same drawback. The magnetic field lines form close loops from one tip end to the other in an ellipsoid shape as roughly represented by red arrows the Fig. 2-b. Therefore, resolution cannot be as high as expected even if the magnetic field is extremely strong below the tip end of the 'Sharp' injectors.

'Crescent' EMP injectors are designed to circumvent this limitation. The idea is to create a circular magnetic field in order to concentrate it between the two ends of the ferrite. This is expected to limit the magnetic pollution all around the space separating the two ends because the magnetic lines should get out from one end, then surround the top layer of the power / ground network before coming back into the ferrite by the other end. Additionally, because of their geometry, 'crescent' EMP injectors have an interesting property: they are directional. If rotated around the z-axis, the field lines direction will also rotate. This modifies the coupling between the injector and the target. This is not the case for the 'Flat' and 'Sharp' injectors because of their cylindrical symmetry.

3 Source of failure of synchronous circuits

Today, the majority of ICs are synchronous circuits i.e. IC whose operations are clocked by a global signal: the clock. This section first reminds what is the structure of these circuits, what are their constituting elements and finally what is their basic operating principle. These reminders are a preamble to the identification, conducted in a second step, of the various mechanisms that may explain the occurrence of faults in circuits subjected to EMP of high amplitude. Finally in a third stage, some tests allowing to experimentally discriminate the different failure mechanisms are defined. These tests are exploited in section 5 to determine which mechanism explains at best the experimental observations.

3.1 Structure and operation of synchronous circuits

A synchronous IC is a circuit in which exchanges of data between its constituting blocks are synchronized by a global signal. This signal, the clock, triggers at regular time intervals the sampling of the calculation results but also their transmission from one block to another.

Calculations are performed by logic gates, usually CMOS combinational gates, interposed between two registers, i.e. D-type Flip-Flops (DFFs), which ensure both the sampling and the transfer of the calculation results between blocks. Given this structure, a synchronous IC can be schematically represented as in Fig. 3 in which the registers are represented by two DFFs (with an active high Set input and an active low Reset input) surrounding a block ('LOGIC') of combinational CMOS logic gates ensuring the calculation.

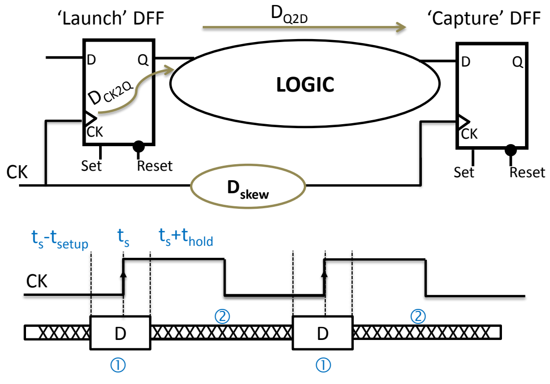

Fig. 3 A simple synchronous IC and some of its timing metrics

3.2 Gate level constraints as a source of failure

If the behavior of the combinational gates used in order to integrate on silicon boolean functions, is quite simple, DFFs have a more complex behavior. Some analogue constraints must be met to ensure a proper operation.

As a reminder, a DFF copies its input signal D, arrived since $D2CK$ ps, on the rising edge of the clock signal, CK, on its output Q. The copy is effective after a delay $CK2Q$. However, as illustrated Fig. 4 for a correct copy of D onto Q, the signal D must be stable t_{setup} ps before the rising edge of CK and remain unchanged t_{hold} ps after. Because $CK2Q$ reaches large values when the data D arrived $t_{setup} + \epsilon$ before the clock edge (ϵ being a small positive delay), it is common to consider a margin during the design of ICs and more precisely to take t^p_{setup} (resp. t^p_{hold}) into account at the design stage, values corresponding to a degradation of 10% of the $CK2D$ delay associated to an early arrival of the data D wrt the clock edge ($D2CK = -\infty$) .

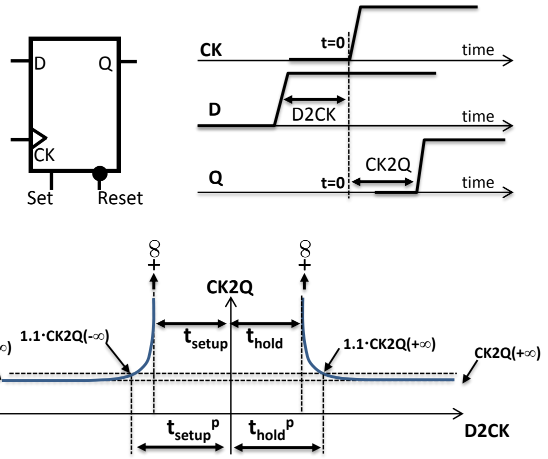

Fig. 4 A DFF, its timing diagram and definitions of setup (t_{setup}, t^p_{setup}) and hold times (t_{hold}, t^p_{hold})

The stability of the signal D during the switching of a DFF is a tight constraint. Not fulfilling this constraint leads to the onset of fault types : bit-set, bit-reset or bit-flip. EMP injection, through the induction of a strong current and thus through the alteration of the power network voltage (or that of the interconnects carrying the signal D), can therefore produce an improper operation of a DFF that will be denoted by *sampling fault* afterward.

Assuming that EMP injection may significantly alter the bias of any signal in an IC, it seems possible that EM injection induces bit-set or bit-reset faults in DFFs by simply modifying the local potentials of 'Set' or 'Reset' signals. This appears feasible even in the absence of commutation of the target DFF if ' Set' and 'Reset' mechanisms have been designed to be asynchronous. If this turns out true, EMP injection could also induce the inadvertent switching of DFFs by generating locally a parasitic rising clock edge, or conversely to prevent the switching of DFFs by inhibiting locally a rising edge.

From all the above, and because of their specific gate level constraints, DFFs appear as a possible EM fault injection path into an IC at rest or not. This later point would be experimentally investigated in section 4.

3.3 Circuit level constraint and source of failure

The gate level constraints associated to the operation of DFFs import timing constraints that have to be met during the design stage, i.e. at circuit level. They are fixed during the design using static timing analysis tools. Among the most demanding constraints one may identify the circuit level hold time and setup time constraints. The latter is known since 2008 [11] and has been highlighted in [3] as the potential EMP fault injection path. Let us remind what is the setup time constraint and why it is a potential EM fault injection path.

The circuit level setup time constraint is defined by the following inequality:

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

where T_{CK} stands for the clock signal period, D_{CK2Q} for the propagation delays of the 'launch DFF' (see Fig. 4), D_{Q2D} for the propagation delay of the combinational block, t_{setup} for the setup time of the 'capture DFF', and D_{Skew} for the clock skew.

At design stage, the Art of Designers is to force all logical paths so that D_{Q2D} satisfies eq. 2 for a given target T_{CK} value. This is done for a temperature range imposed by the application for which the IC is designed (e.g. -40 to $+125^o$C) but also for a reduced voltage range: $0.9 \cdot V_{dd}$ to $1.1 \cdot V_{dd}$; V_{dd} being the nominal supply voltage imposed by the technology which is as low as 1.2V for nowadays technologies. Outside this reduced supply voltage range, the operation of the circuit is not guaranteed.

In [3], the circuit level setup time constraint is highlighted as the potential EMP fault injection path. Indeed, it is suggested that because EMP injection alters locally and temporarily the supply voltage of logic gates, D_{Q2D} delays are increased so that the circuit level setup time constraint is not met and a transient *timing fault* appears. If this is a sound explanation, it is not so clear that EMP injection produces faults by inducing violations of the setup time constraint (or hold time) at gate level or at circuit level. Let us define some tests to determine if EMP injection induces gate level constraint violations or circuit level ones, i.e. some tests to determine if EMP injection induces *sampling faults* (gate level) or *timing faults* (circuit level).

3.4 Discrimination tests

We therefore searched for some tests to check if the *timing fault model* is a better EMP fault injection model than the *sampling fault model*.

According to eq. 2, several criteria or tests can be defined to experimentally determine if EMP injection follows the *timing fault model*. A first test consists 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 consists in producing the same EMP injection during a same clock period but at different times t_{pulse} (within the same clock period) and then in verifying that the occurrence of the fault is independent of that parameter. Indeed, independently to the time at which an increase of D_{Q2D} is produced (the beginning of the clock period, the middle or the end) if the increase is sufficient a fault appears. One may probably define other tests. However, these two tests were considered sufficient for the experimentations detailed in section 5 to verify if EMP injection induces *timing faults* or not.

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 EMP injection produces such faults then these faults can solely appear when an EMP is produced just before the occurrence of a rising clock edge and more precisely during the 'sampling windows' corresponding to the effective switching of DFFs. Additionally, if this EM fault injection model is valid, these time windows (denoted afterward by 'susceptibility windows') during which EMP 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 DFFs (such as schematic, layout, technology or supply voltage ...) and on the transition times of the clock and D signals.
- are necessarily separated by time slots during which the probability to produce a fault is null if the *sampling fault model* is correct; these windows corresponding to EMP injections that do not fall within the EM susceptibility windows of DFFs.

One could be surprised that in the above discussion we have assumed that only rising clock edges are a front door for EMP injection. In fact we did assume that DFFs are highly susceptible to EMP injection during their switching process, i.e. during a rising or a falling edge of the clock. However because of the structure of IC, a disruption of the switching during the falling edge does not disrupt the IC. Indeed, DFFs mainly feature two latches in cascade.

The first stage, the master, collects the incoming data D when the clock signal is low while the second stage, the slave, maintains the output Q. When the clock signal is high, the master, in which D is already present for a while, passes D to the slave. During this time interval, the Master stage is isolated from the logical gate controlling the DFF input. As a result, a disruption of the data D just before the falling edge has no real effect on the IC behavior (except if the perturbation persist up to the next rising edge). Indeed, as soon as the clock signal falls, the correct data D is restored in the master by the logic gate controlling D. This is done in few tens of ps, a delay which is largely lower than the timing slack of IC.

Conversely, an EMP produced before the rising edge alters D just before the master become isolated from the gate controlling the DFF input D; as a result no recovery of the correct value of D is possible. This explains why we stated in the above discussion that the EM susceptibility of DFFs is really high during the rising edge of the clock.

All the above implications of the *sampling fault model* will be used to check if EMP injection induces *sampling faults* during experimentations described in section 5. However, before applying these discrimination tests, let us evaluate if it is possible to induce bit-set or bit-reset faults by disrupting the 'Set' or 'Reset' signals of DFF at rest; a positive answer constituting first evidence in favor of the *sampling fault model*.

4 Evidence of static fault model on an IC at rest

Aiming at demonstrating that EMP injection induces bit-set or bit-reset faults by disrupting the 'Set' or 'Reset' signals, a specific test chip was designed.

4.1 Detecting bit-sets / bit-resets: testchip and experiments

Our intend was to be able to easily write and read the content of DFFs to detect by simple comparison the occurrence of bit-set or bit-reset faults. A large FIFO featuring (640×8) DFFs (640 bytes) was mapped into a Xilinx spartan 3E-1000 (technology node 90nm). Fig. 5 shows the floorplan of this design. A key point for the rest of the paper is to remember that all DFFs were mapped with a Reset (resp. Set) signal active low (resp. high).

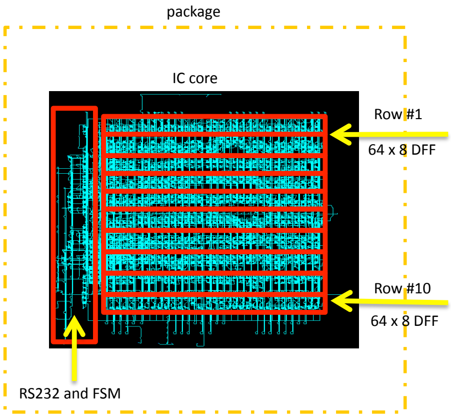

Fig. 5 Large chain of registers (FIFO) designed to demonstrate the occurrence of bit-set and bit-reset faults.

This testchip was exposed to EMPs for the purpose of drawing a fault sensitivity map. The following automated procedure was adopted in order to detect (i.e. experimentally demonstrate) the occurrence of bit-set and bit-reset faults:

- 1^{st} *step*: the EM injector is placed at a given (X, Y) (initial value $(0, 0)$) coordinate above the test chip, in its close vicinity (i.e. close to contact) in order to maximize the spatial resolution of the EM injection,
- 2^{nd} *step*: the content of each byte of the FIFO is set to the hexadecimal value 'AA' ('10101010' in binary),
- 3^{rd} *step*: the clock signal is stopped in order to avoid the occurrence of a *timing fault*,
- 4^{th} *step*: an EMP, with an amplitude V_{pulse} ranging between -200 V and 200 V is delivered to the EM injector,
- 5^{th} *step*: the clock signal is re-activated after a while (several μs) and the content of the FIFO recovered,
- 6^{th} *step*: the initial and final contents are compared (a xor operation) in order to detect the occurrence of bit-set and bit-reset faults, and the result of the comparison is stored in a log file.
- 7^{th} *step*: steps $\#2$ to $\#6$ are repeated 9 times in order to estimate the probabilities to obtain bit-set and bit-reset faults at the current position (X, Y),
- 8^{th} *step*: restart the procedure at step $\#1$ at a new (X, Y) coordinate in order to obtain a fault sensitivity map of the target.

4.2 Occurrence of bit-set and bit-reset faults

Many fault sensitivity maps of the testchip were drawn according to the above procedure. Indeed, different V_{pulse} values were considered in $\{-200\ V, ..., 0, ..., 200\ V\}$. Different EM injectors were also used. However, we report herein only the results obtained with a 'crescent' injector characterized by '$s = 450\ \mu$m' because these results are the best that were obtained with regard to spatial resolution.

During these fault injection campaigns, four different responses from the circuit were observed:

- injection of bit-set faults into one or several DFFs according to the EM injector position and to V_{pulse} value,
- injection of bit-reset faults into one or several DFFs according to the EM injector position and to V_{pulse} value,
- 'Mute' or loss of the communication channel with the circuit,
- fault free.

Fig. 6 shows three fault sensitivity maps obtained with a displacement step of the EM injector equal to 300 μm (< to the air gap of the crescent probe). The whole die surface (5500 μm $\times$ 5000 μm) was scanned resulting in 4500 μm $\times$2400 μm fault sensitivity maps because of the shape of the EM injector and a of guard-banding to avoid any collision of the injector with bondings. These maps were obtained with the following settings: $V_{pulse} = +170$ V and a pulse width $PW = 8$ ns. Fig. 6-a shows the probability to have faults regardless of the type of the obtained faults (either bit-set, bit-reset or Mute). Fig. 6-b reports the probability to have bit-set faults while Fig. 6-c gives the probability to have 'Mutes'. Fig. 6-d shows that no bit-reset fault was induced. Finally, Fig.6-e shows the orientation of the injector above the IC surface, a parameter that will be discussed later.

Two kind of 'Mutes' were observed. The first category is made up by 'no response' from the IC; 'no response' that do not require reprogramming the FPGA to relaunch the cartography procedure. This suggests the occurrence of a fault in one of the DFF of the finite state machine. The second category of 'no response' is more severe. Indeed, relaunching the cartography has required in that case to reprogram the FPGA. This suggests that the bitstream was corrupted by the EMP injection.

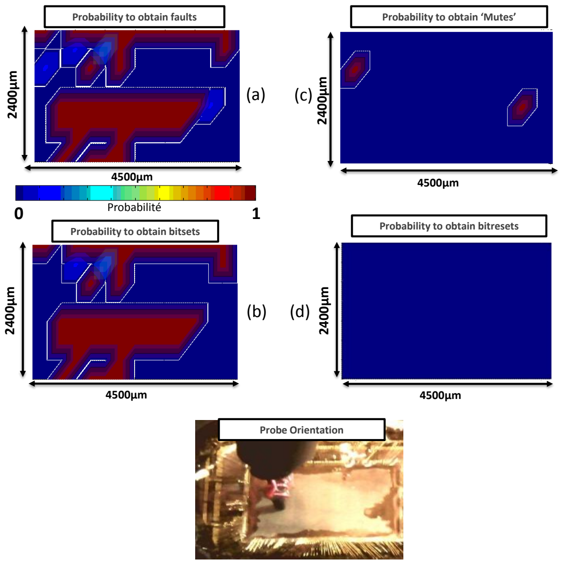

Fig. 6 Probabilities to produce (a) faults regardless of the fault type (b) bit-set faults (c) 'no-response', (d) bit-reset faults and (e) injector orientation (air gap along the y-axis) – (170 V, 8 ns) EMP.

Obtaining these sensitivity maps, especially the one of Fig. 6-b, constitutes an experimental demonstration that EMP injection, performed with enhanced injectors, can induce bit-sets. This was one of our objectives.

Additionally, one may observe once again that EMP injection is reproducible. Indeed, we did verify that the bit-sets obtained at a given coordinate from one injection to another, were exactly the same. This observation is further sustained through the observation that the probability of injecting a fault is either equal to zero or one at most coordinates.

These cartographies also highlight that EMP injection is local. Here the term 'local' means the effect of an injection significantly depends on the positioning of the injector above the testchip. However, it is important to consider that there is no direct link between the EMP injector position and the placement of the faulted DFFs. Faults could be induced in DFFs placed just below the EMP injector or far from it. EMP disturbances seems to propagate across the IC.

4.3 Correlation between the EMP polarity and the occurrence of bit-sets and bit-resets.

Despite being an experimental demonstration that EMP injection induces faults into DFFs, regardless of any timing considerations, the experiments reported in subsection 4.2 never led to a bit-reset fault. Considering that the Set signal of the DFFs is active high and the Reset active low, a similar set of experiments was relaunched: with $V_{pulse} = -140$ V and $+140$ V instead of $+170$ V only. The idea that motivated this experiment was the assumption that an EMP of a given polarity may affect more the ground network than the power network (or vice-versa) or may increase or reduce the bias of an interconnect signal. Therefore, it may be easier to induce bit-set faults than bit-reset faults (or the contrary) depending on the EMP polarity. Note however that the polarity is here an arbitrary notion that depends in our case on both the injector orientation and the sign of the voltage spike. For the sake of simplicity, we choose here to define the polarity as positive when the pulse affects more the Set signal which is active high than the Reset signal which is active low.

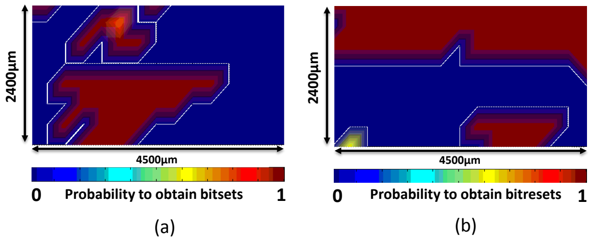

Fig. 7 Probabilities to obtain (a) bit-set faults with $V_{pulse} = +140$ V and (b) bit-reset faults with $V_{pulse} = -140$ V

Fig. 7-a gives the probability to obtain bit-set faults when applying a positive pulse of amplitude +140 V instead of +170 V for Fig. 6-b. Comparing these two figures (Fig. 6-b and 7-a) allows observing that reducing V_{pulse} reduces the size of the fault sensitive areas. Note however, that the two maps remain really similar in shape. This indicates that the magnitude V_{pulse} is an efficient control parameter of the EMP injection power as it was expected.

Fig. 7-b gives the probability to obtain bit-resets when applying a negative pulse of amplitude -140 V; during this set of experiments no bit-set fault was induced. One may observed that the two cartographies are completely different indicating that the susceptibility of an IC to a positive or a negative pulse may be radically different.

Nevertheless, the main conclusion that can be drawn from these experiments is that the pulse polarity (and therefore the injector orientation) is a key factor in controlling the type of EMP induced faults. It seems to allow targeting more the ground network than the power network according to the topology of the IC or to target more a signal polarized at Vdd or at the 0. These results also suggest that according to their occurrence, bit-set and bit-reset faults are related to the way DFFs are designed (set / reset signals active low or high). However, further investigations are mandatory to sustain this assumption.

5 Evidence of a specific fault model on an operating ICs

At this stage of the paper, it was shown that EMP injection has a local character but above all that it can produce bit-set or bit-reset faults in a circuit at rest. This result suggests that EMP injection follows the *sampling fault model* rather than the *timing fault model*. However, fault attacks are conducted on IC in operation and not at rest.Therefore the goal of this section is to identify on a circuit in operation the most likely fault model between the *sampling fault model* model and the *timing fault* one. For this purpose a new testchip was designed.

5.1 Second testchip

The second testchip adopted to conduct our experiments is an FPGA (xilinx Spartan 3-1000), designed with a 90nm process, on which four functional blocks have been mapped. The first is a Finite State Machine (FSM) clocked at 50 MHz . It controls all events and contains registers for storing the encryption / decryption result and the ciphering key. The second is a Digital Clock Manager providing on command a frequency of 100, 50 or 25 MHz to the third block. The third block is a fully numeric (no BRAM was used) AES-128bits. It ciphers a plaintext in 10 rounds at either 100 , 50 or 25 MHz. 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. 8. These design constraints were fixed to enable the analysis of EMP injection effects spatially.

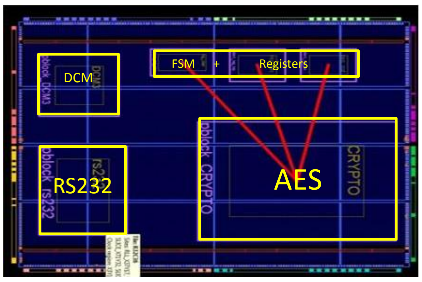

Fig. 8 Floorplan of the testchip

5.2 Objectives

If in the preceding paragraphs, the focus was put on the various possible fault models, one of the first question we adressed is the location of faults that are produced, injection being delivered during the ninth round of the AES. To answer this question, cartographies revealing the probability to induce a fault in the second testchip were drawn. The obtained faults were also analyzed to disclose 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, 100 injections were performed at several positions (at which faults were observed) and for several values of t_{pulse} allowing to cover the complete execution of the AES encryption with a time step Δt_{pulse} equal to 1ns. This was done for the three different values of the clock frequency delivered by the DCM. During these injections the AES was ciphering 100 random plaintexts. These last experiments were conducted to determine if the obtained faults are *timing faults* or *sampling faults* according to the discrimination tests introduced in section 3.4.

5.3 Experimental results

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

5.3.1 Fault cartographies and locality of EM injection.

The cartographies 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. During these injections, the voltage pulse supplied to the injector has an amplitude V_{pulse}= 44 V and a width PW= 8 ns. The end(s) of the two injectors were in contact with the IC surface. The operating frequency of the AES was fixed at 100 MHz and the core supply voltage Vdd was set to 1.2 V.

The cartographies performed with the flathead injector were achieved with a displacement step $\delta x = \delta y = 200$ μm. Those performed with the 'crescent' injector with $\delta x = 100$ μm and $\delta y = 100$ μm. Fig. 9a 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 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. 9c shows the coordinates at which 'no-response' were obtained. It should be observed that only correct or erroneous ciphertexts were obtained with the 'crescent injector'.

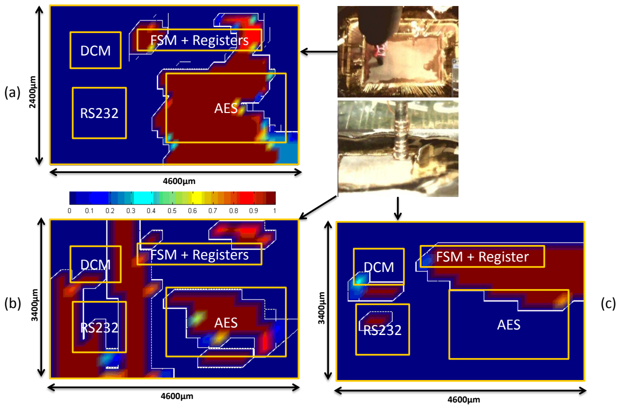

Fig. 9 Probability to induce (a) a bad ciphering with the 'crescent injector', (b) a bad ciphering with the flathead injector and (c) a 'no-response' with the flathead injector

As shown Fig. 9a, EMP injections performed with the 'crescent' injector is local. Indeed, faults are obtained with a high probability level in disjoint areas corresponding roughly to the testchip floorplan. These regions correspond respectively with the AES placement, the placement of the registers storing the key and the ciphertexts, but also to the FSM placement. 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. 9b that EMP injections conducted with the flathead injector are also local but that coordinates with a high level of probability are really different to that of Fig. 9a. 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 EM injectors is the appearance of 'no-response'. Many injections performed with the flathead injector induced a 'no response' while there is not with the 'crescent probe'.

If those cartographies disclose 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. 10 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 a 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 once again 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 performed.

5.3.2 *EM Fault model:* timing or sampling faults *?*

More particularly, several EMP injection campaigns were conducted with the crescent-shaped injector positioned at three distinct coordinates characterized by a high probability of to produce faults (Fig. 9). 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} = 25 MHz, 50 MHz and 100 MHz. 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 noticed that during these experimental campaigns, other injection parameters were kept constant to the following values $V_{pulse} = 44$ V and $PW = 8$ ns.

Fig. 11 reports the evolution of the number of faulted bytes wrt t_{Pulse}, i.e. wrt time for F_{AES} = 100 MHz. Time slots during which it is possible to induce faults appear. These are periodically spaced by 10 ns, value that corresponds to the clock period T_{AES}. These slots of a duration equal to 6 ns are denoted by susceptibility windows in the rest of the paper. They are separated by time slots during which the susceptibility to EMP injection is null.

Given these results and the discrimination tests defined in section 3.4, 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*, the probability to inject a fault would have been constant and equal to one for all t_{pulse} values. This is 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 support this result, these experiments were repeated over the last three rounds of the AES suc-

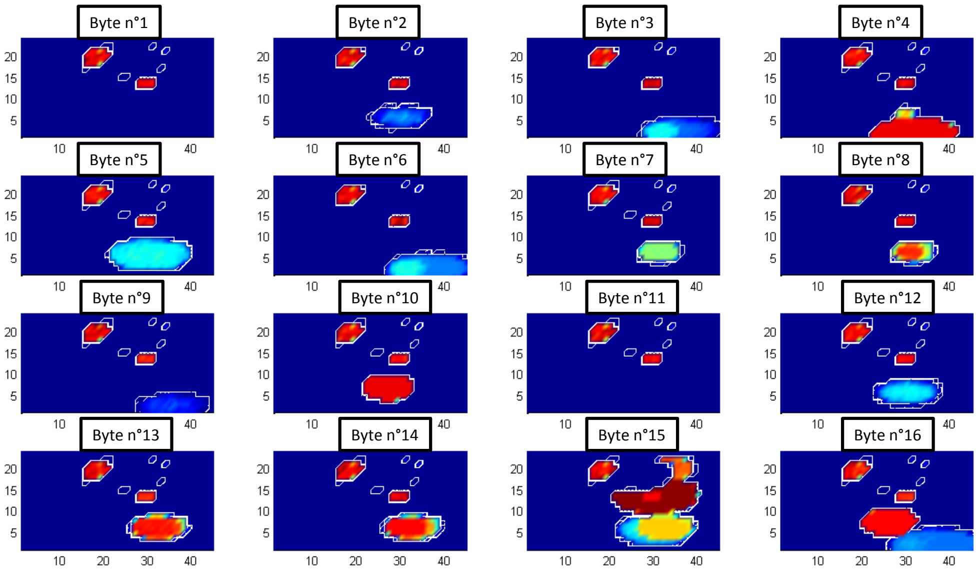

Fig. 10 Probability to fault each byte wrt to the positioning of the 'crescent' injector (the color scale is the same than in Fig. 9)

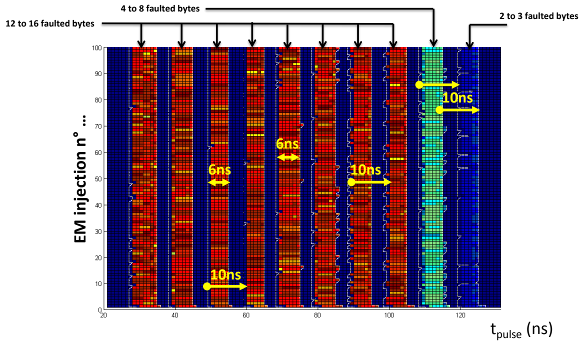

Fig. 11 Number of faulted bytes wrt to t_{Pulse} for the 100 plaintexts processed by the AES

cessively clocked at F_{AES} = 100, 50 and finally 25 MHz. Fig. 12 shows the evolutions of the probability to induce a fault for the three clock frequency values. Observing these three evolutions clearly shows that the apparition of the susceptibility windows is independent of clock period value. It also indicates that the width of these windows is constant and equal to 6 ns. Additionally, one may observe that the time slots duration during which no fault is induced increases linearly with the clock period: the duration of these time slots moving from 34 ns at F_{AES}=25 MHz to 4 ns at F_{AES}=100 MHz. These observations confirm that the more realistic fault model for EMP injection is the *sampling fault model*.

If these experiments are sufficient to demonstrate (see. aslo section 6.3 that obtained faults are *sampling faults*, 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 90 nm process, features an internal voltage regulator to maintain the core supply voltage at 1.2 V. Its main constituting block is an ARM cortex M4 processor clocked at 30 MHz. This micro-controller also embeds a hardware AES-128bits, clocked at 120 MHz (T_{CK} = 8.33 ns). Its architecture is the same than that mapped into the FPGA.

Fig. 13 gives the probability to induce a fault for the three following values of V_{pulse}: 120, 160 and 190V. The time window on which the EMP injections have been performed corresponds to three rounds of the AES. The EMP injector was placed above the AES during these experiments. 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} = 8.3 ns are clearly visible, indeed. However, their duration varies from 2.9 ns to 4.25 ns with V_{pulse}. These values are lower than in the case of the FPGA (6 ns). A likely explanation may be the typical value of the DFF propagation delay (D_{CK2Q}) which is significantly shorter in the case of the ASIC (350 ps) that in the case of FPGA (1 ns). Finally, these windows are more rounded than in the case of AES mapped onto the FPGA.

6 The *sampling fault model*

Given the experiments and observations described in this paper, it seems that the fault model associated with the EM injection (performed with moderate power) is the *sampling fault model*, i.e. the disruption of the switching process of DFFs, an event that can be induced at every rising clock

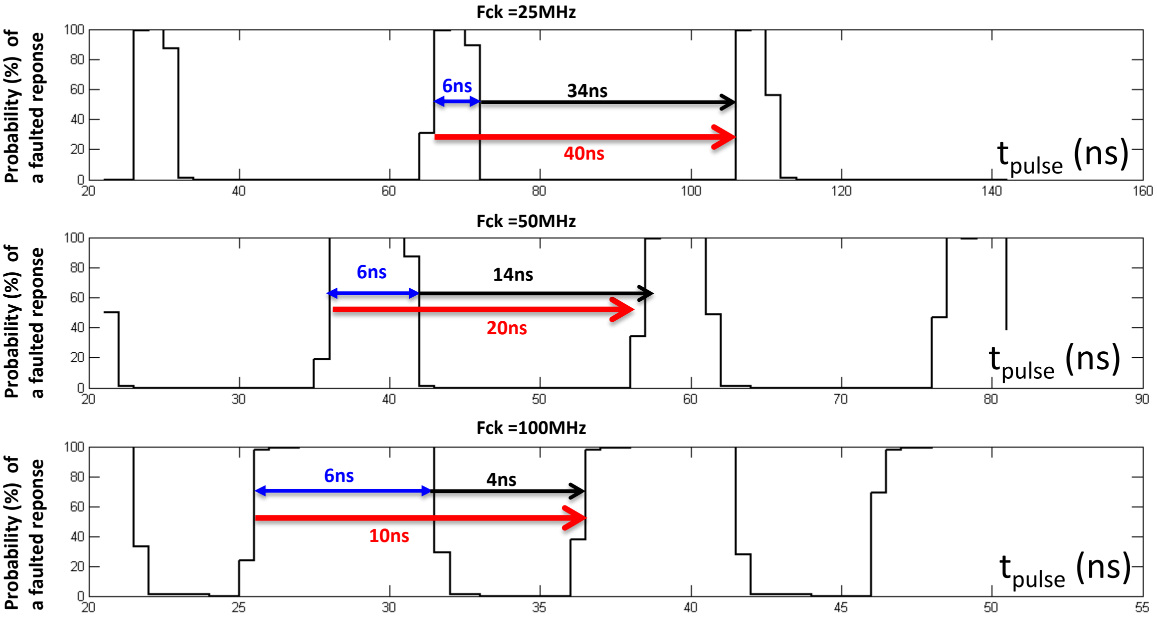

Fig. 12 Evolution of the probability to induce a fault into the hardware AES mapped onto a spartan3-1000 wrt t_{Pulse}

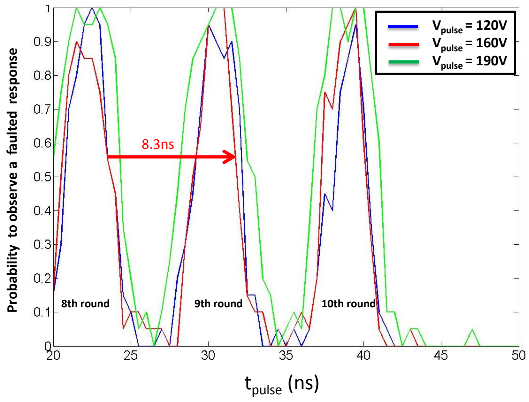

Fig. 13 Evolution of the probability to inject a fault into the hardware AES embedded in the 32bit micro controller wrt t_{pulse}

edge, or at any time if DFFs feature asynchronous 'Set' and 'Reset' inputs. However, it appears more difficult to disrupt the 'Set' and 'Reset' signals of DFFs at rest as indicated by the EMP amplitudes considered in section 4 (more than 100 V to produce bit-set or bit-resets) and in section 5 (44 V to induce faults during the switching of DFFs). This section therefore proposes a description of what is the *sampling fault model*, which appears the more realistic for EM injection. In addition, a last experimental result validating definitively our proposal is also given.

6.1 Definition

The *sampling fault model* is illustrated Fig. 16. It is a time based model. More precisely, all possible effects of an EMP are linked to the clock signal which appears on the top of Fig. 16. As indicated by this figure, the EM susceptibility of an IC, assumed to be equivalent to that of DFFs in our model, also evolves in time. It has a low value when the clock signal is high or low and a high value around the rising edges of the clock. This means that to induce a fault within an IC there are two EM power thresholds.

Assuming for sake of simplicity the EMP power is directly link to V_{pulse}, the first threshold is V_{Low}. It corresponds to the minimum EMP power required to disrupt the switching process of one or several DFFs in the target IC. Crossing this threshold power therefore allows inducing a *sampling fault* marked by a "B" in Fig. 16. However, to that end, the EMP should be delivered just before or during a rising clock edge, i.e. during time intervals marked by a (1). Of course if an EMP with a power lower than V_{Low} is delivered in the close vicinity of the IC, no fault is induced.

The second threshold is V_{High}. Producing an EMP with a power greater or equal to V_{high} allows inducing bit-set or bit-reset faults marked by a "A" in Fig.16), and this according to the pulse polarity. Contrarily to the preceding case, the EMP can be delivered at any time (i.e. during time intervals (1) and (2)) and therefore regardless of the clock signal state.

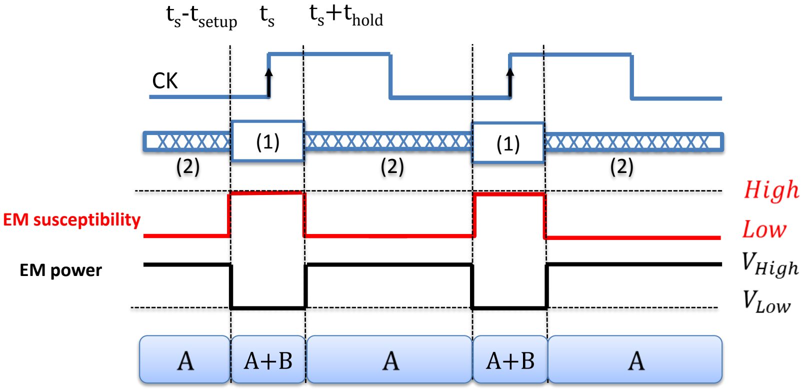

Fig. 14 The *sampling fault model*

This *sampling fault model* defined, one must also consider that the EMP energy delivered by the EM injector is not directly the energy received by the target IC. The power transfer rate depends on the quality of the coupling between the EM injector and the IC. Therefore, for a given injector, the two thresholds depend on many parameters. Among them, two are really important. The first one is of course the positioning of the EM injector above the IC. The second one is the IC itself; according to how the routing of power/ground network is done, the coupling is more or less effective.

Such a model allows explaining the experimental observations done in section 4 but also in section 5. However, those observations have been done separately. Consequently, at that point in the paper, there is no experimental proofs that the increase the EMP power from 0 towards really high values leads to cross two power thresholds. A final validation is therefore proposed section 6.4 to verify this last point.

6.2 Comparing *timing faults* and *sampling faults*

In order to better illustrate the difference between *sampling faults* and *timing faults*, and thus explain the experimental results obtained reported Fig. 12, Fig. 15 was drawn.

The upper part of this figure shows the effect of a fault injection at the times t_1, t_2 and t_3 which induces an delay increase greater than the timing slack of the considered combinational block. Because the delay is an additive quantity, regardless of the moment the fault is injected during the clock cycle, a *timing fault* will a appear if the delay is increased by a value greater or equal to the timing slack. As a result, in this latter case, the probability to induce a fault is constant all over the clock cycle. This is not what has been observed during the experiments that have conduct to Fig. 12.

The lower part of this figure shows the effect of a fault injection attempt (assuming a *sampling fault model*) at the times t_1, t_2 and t_3. If we now consider that the fault injection attempt alters temporarily the voltage of many nodes within the circuit during Dn ps, and that after this time interval, the IC quickly recovers its original state, two cases should be distinguished.

The first case (EMP delivered at times t_1 and t_2) corresponds to fault injection attempts delivered sufficiently close to the next rising clock edge so that the voltage of one (or several) input of DFFs are not at their correct value. In that case a *sampling fault* occurs.

The second case corresponds to a fault injection attempt occurring too early in the on-going clock cycle (EMP delivered at times t_3). In that case, the voltage of many internal nodes is also disrupted for a duration equal to Dn ps that corresponds to the duration of the local perturbation plus the time spent by the IC for recovering its original state i.e. to evacuate the perturbation towards the power and ground IOs. In that case, because the injection occurs too early in the clock cycle, the correct values are recovered before the next rising clock edge and no fault appears.

Considering these two cases, it appears that the probability of inducing a *sampling fault* during a clock cycle is therefore equal to zero at the beginning of the clock cycle and equal to 1 during a short time interval including the next rising clock edge. This behavior corresponds to what have been observed during the experiments that have conducted to Fig. 12.

6.3 Final proof in favor of *sampling faults*

The experimentations aiming at deciding if faults are *sampling fault* or *timing fault* have consisted in reducing the clock frequency from $100MHz$ to $25MHz$ (keeping all other parameters constant) and in verifying

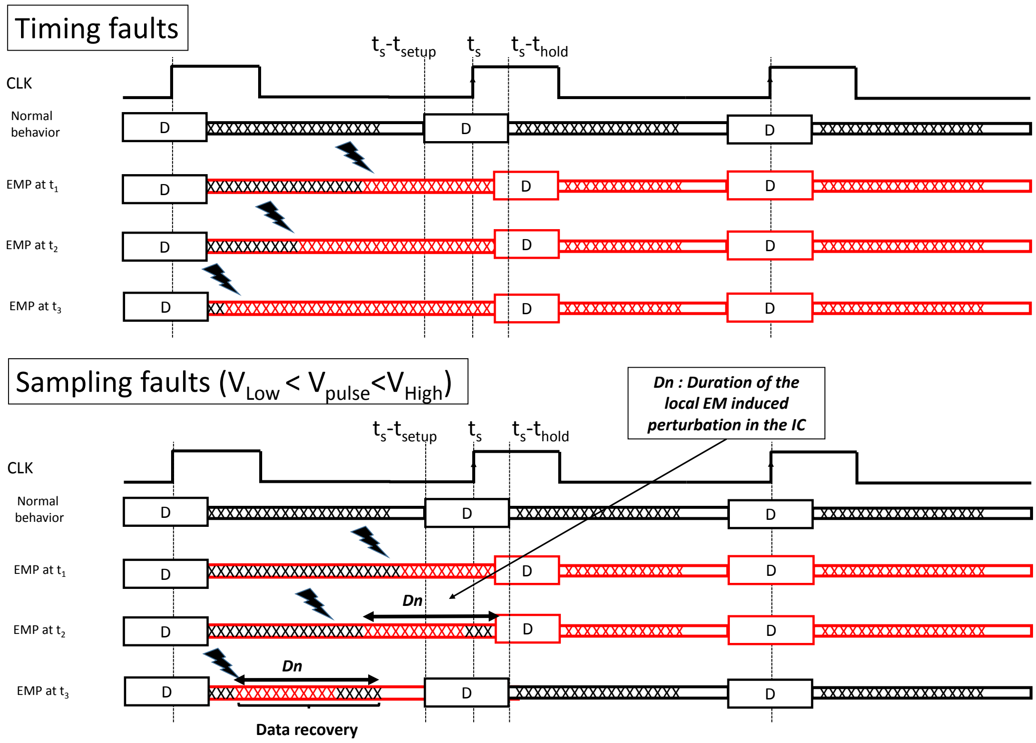

Fig. 15 The *Comparison of* timing faults *and* sampling faults

- that the probability to induce a fault is not constant over a clock cycle and,
- that the evolution of this probability with respect to t_{pulse} is independent of the clock frequency.

One could think these experimentations are not sufficient to rigorously demonstrate that obtained faults are not *timing faults*, and that additional experiments with lower clock frequencies are mandatory. This is not the case, and there is no need for additional experiments at $1MHz$ or lower. Let us explain why.

If the obtained faults at F_{CK}= 25 MHz and F_{CK}= 100 MHz are *timing faults*, the delay increase ΔD (that remains the same all along the experiments because injection settings are kept constant) induced by the EMP is therefore, according to 2, such as:

$$\Delta D \geq t_{slack}^{25MHz} - t_{slack}^{100MHz} = 30ns \geq T_{CK}^{100MHz} \qquad (2)$$

where t_{slack}^{100MHz} and t_{slack}^{100MHz} stand for the timing slacks at the 25 and 100MHz respectively.

One can observe that the delay increase ΔD induced by the EMP is therefore necessarily greater than T_{CK}^{100MHz} =10 ns, the period of the clock signal at F_{CK}= 100 MHz. If this is true, this would mean that, regardless of the time t_{pulse} at which the EMP is delivered within a $10ns$ clock period, a fault would appear. This is not what has been observed during experimentations. Faults only appear during what has been formerly defined as susceptibility windows. Hence, this reductio ad absurdum demonstrates that obtained faults are not *timing faults*, and thus that they are *sampling faults* .

6.4 Final validation of the *sampling fault model*

To definitively validate the EM *sampling fault model*, a final experiment was conducted. It has consisted in delivering EMPs with different power (i.e. V_{pulse}) above the FPGA and this all along the course the AES. The FPGA board was changed and the EM injector placed at a different position than the one considered in the experiments of section 5. This choice was done for the purpose of generality. Then the evolution of the probability to inject a fault was computed for all considered V_{pulse} values.

Fig. 16 gives these evolutions for V_{pulse} = 50, 100, 150 V. Because no fault were observed for V_{pulse} values lower than 40 V, and because faults were obtained for V_{pulse} = 50 V, we can conclude that V_{Low} is between 40 V and 50 V. In addition, as shown, for V_{pulse} values equal to 50 V and 100 V, EM susceptibility windows appear. Their duration is of 9 ns. Furthermore, as expected from the *sampling fault model*, there are equally spaced by 20 ns; the clock period value.

Still in accordance with the *sampling fault model*, for this EM injector positioning, as soon as V_{pulse} crosses 140 V bit-set faults appear and the probability to induce faults during time intervals marked by (2) in Fig. 16 increases quickly.

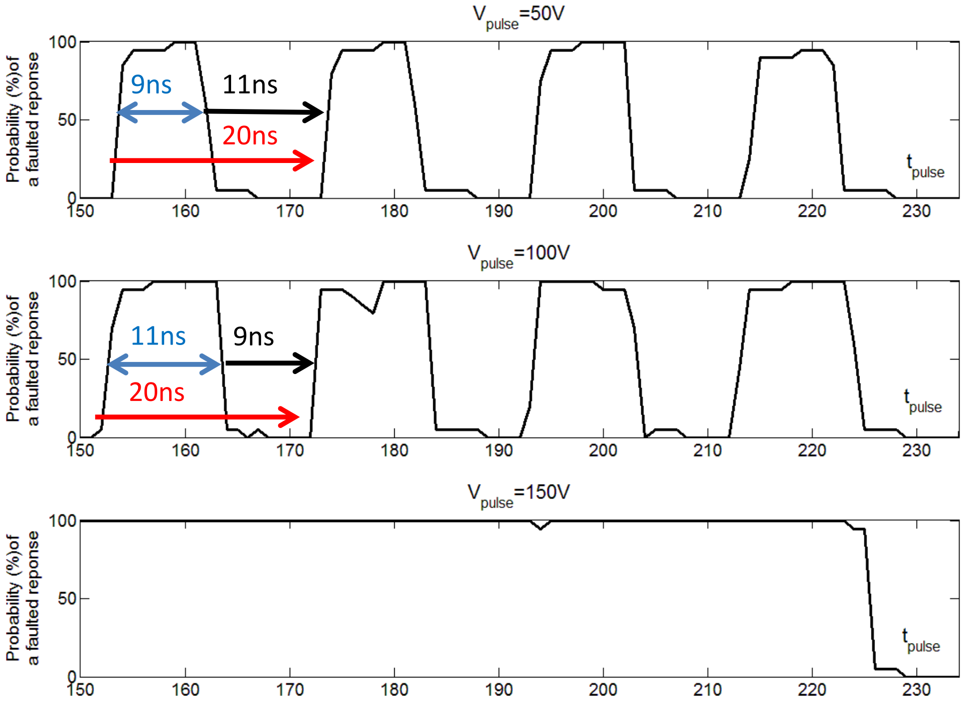

Fig. 16 Evolution of the probability to inject a fault wrt t_{pulse} for V_{pulse} (a) =50 V, (b) = 100 V and (c) =150 V

For $V_{pulse} = 150$ V, the probability to inject of fault at any time during the course of the AES is equal to 1.

These experimental results definitively validate the *sampling fault model* and indicate, that for this injector positioning, $V_{Low} \simeq 45$ V and $V_{High} \simeq 145$ V.

7 Conclusion

In this paper, we have described an EM pulse platform and many experiments conducted on an FPGA and a modern micro-controller. If these experiments have highlighted the locality of EM injection, they were mainly conducted to identify the phenomenon explaining at best the obtained faults. A special care was devoted to *timing faults* that were suggested as the more realistic explanation in former publications.

After an analysis of the different probable failure sources of IC in presence of EM pulses, some experimental tests were defined and exploited in order to identify the more realistic EM fault injection model. Experimental results have shown that the *timing fault model* does not explain all experimental observations while the *sampling fault model* introduced in this paper does. This model suggests that EMP conducted with enhanced EM injectors are sufficiently powerful to disrupt the switching process of DFFs and even to trigger the set or reset of these DFFs by producing even more powerful EM pulses.

Finally, from the point of view of IC designers, this work highlights that DFFs are key elements and therefore renews the interest for DFFs with reduced EM and light (laser) susceptibilities. In addition, it points out that the challenge of increasing the IC robustness to EMP injection does not reduce to increasing the timing margins.

References

1. P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *COSADE*, pages 151–166, 2012.
2. A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012:123, 2012.
3. A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *FDTC*, pages 7–15, 2012.
4. M. Joye and M. Tunstall. *Fault Analysis in Cryptography*. 2012.
5. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.
6. P. Maurine. Techniques for em fault injection: Equipments and experimental results. In *FDTC*, pages 3–4, 2012.
7. R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine. Magnetic microprobe design for em fault attackmagnetic microprobe design for em fault attack. In *emceurope*, 2013.
8. F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, and P. Maurine. Local and direct em injection of power into cmos integrated circuits. In *FDTC*, pages 100–104, 2011.

9. J. Quisquater and D. Samyde. Eddy current for magnetic analysis with active sensor. In *Proceedings of ESmart 2002*, page pp 185âĂŞ194, 2002.
10. J.-M. Schmidt and M. Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results. In J. W. Karl C. Posch, editor, *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61 – 67, 2007.
11. N. Selmane, S. Guilley, and J.-L. Danger. Practical setup time violation attacks on aes. In *Dependable Computing Conference, 2008. EDCC 2008. Seventh European*, pages 91–96, 2008.
12. S. P. Skorobogatov and R. J. Anderson. Optical fault induction attacks. pages 2–12, 2002.
13. K. Tobich, P. Maurine, P.-Y. Liardet, M. Lisart, and T. Ordas. Voltage spikes on the substrate to obtain timing faults. In *DSD*, pages 483–486, 2013.
14. L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clédière, and A. Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *DATE*, pages 1–6, 2014.