Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells

Cyril Roscian, Alexandre Sarafianos, Jean-Max Dutertre, Assia Tria

Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on
http://dx.doi.org/10.1109/FDTC.2013.17

Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells

Cyril Roscian*, Alexandre Sarafianos†, Jean-Max Dutertre* and Assia Tria‡

*†*Département Systèmes et Architectures Sécurisés* (SAS)
**École Nationale Supérieure des Mines de Saint-Étienne*
†CEA-TECH, *Gardanne, France*
{Firstname.Lastname}@cea.fr Lastname@emse.fr

***Abstract*—The use of a laser to inject faults into SRAM memory cells is well known. However, the corresponding fault model is often unknown or misunderstood: the induced faults may be described as *bit-flip* or *bit-set/reset* faults. We have investigated in this paper whether the *bit-set/reset* fault model or *bit-flip* fault model may be encountered in SRAMs. First, the fault model of a standalone SRAM was considered. Experiments revealed that the relevant fault model was the *bit-set/reset*. This result was further investigated through electrical simulations based on the use of an electrical model of MOS transistors under laser illumination. Then, fault injections have been performed on the RAM memory of a micro-controller to check the validity of the previous results based on experiments and simulations.**

***Keywords*-Laser Fault injection, SRAM, Fault model, SPICE Simulation, Bit-flip, Bit-set, Bit-reset.**

I. Introduction

Secure circuits are prone to a wide range of physical attacks. Among them, fault attacks (FA) are based on the disturbance of the chip environmental conditions in order to induce faults into its computations. Fault injection may be achieved by using laser exposure [1], voltage [2] or clock glitches [3], electromagnetic perturbation [4], etc. It exists a very efficient method called Differential Fault Attack (DFA) applied to encryption algorithms that takes advantage of a comparison between correct and faulted ciphertexts to retrieve the secret key used during the ciphering process [5], [6], [7], [8]. In these attacks, the fault model [9] can be very restrictive and is often the base of the attack efficiency. Thus, it is important to know what fault model is relevant or feasible with the targeted chip.

This work reports the study of the fault model of SRAM memory cells when exposed to laser pulses. Transient fault injection in memory elements is often modelled according two fault models: (1) the *bit-set/reset* model and (2) the *bit-flip* model. A data bit suffers from a *bit-set* (resp. a *bit-reset*) fault, if it is changed from 0 to 1 (resp. from 1 to 0), thus creating a calculation error. On the contrary, it remains unfaulted if its logical value was yet a 1 (resp. a 0). This data-dependent fault type is very worrying as it makes it possible to mount safe error attacks against cryptosystems [2], [10], [11]. A data bit suffers from a *bit-flip* fault if it is inverted regardless of its value. This latter fault model is data-independent. The injected faults in SRAMs are often described in research papers according these two fault models [12]. However, to the best of our knowledge, their relevance has never been precisely investigated. Moreover, the *bit-flip* fault model is questionable according a first order analysis of the laser-sensitive zones of an SRAM cell.

Our main contributions to that research field are:

- the identification on experimental basis of the actual fault model of laser-induced faults into SRAM cells,
- the use of electrical simulations that consider the induced photo-currents and the topology of the targeted SRAM cell to assess and further analyse the fault model.

This paper is organized as follows. The first part reminds the effects of laser on silicon and emphasizes the notion of laser-sensitive zones on CMOS circuits. Then, a set of assumptions, derived from this notion, is made and its consequences on the fault model of an SRAM cell are reviewed. The second part reports the experiments we have carried out to find out the right fault model. In the third part, simulations results based on a proper model of laser-induced effects are displayed and commented for deeper analysis purposes. The forth part reports further experiments conducted on a micro-controller's RAM memory. Finally, a conclusion summarizes the different results and some perspectives are given for future works.

II. SEU on SRAM Cell

A. *From* SEE *to* SEU

A photoelectric effect is generated by a laser beam passing through silicon provided that its photons energy is greater than the silicon bandgap [13]. This effect creates electron-hole pairs along the laser path. Generally these pairs recombine and there is no noticeable effect on the IC's behaviour. However, under specific conditions, some undesired effects may appear: the so-called Single Event Effects (SEE). A SEE happens when the charge carriers (i.e. electrons and holes) created by the laser beam are drifted in opposite directions by the electrical field found in the PN-junctions of CMOS transistors instead of recombining. As a consequence a transient current (i.e. moving charge carriers) is generated through the struck junction. This phenomenon is depicted in the left part of Figure 1, where the PN-junction of an NMOS transistor in its turned "*OFF*" state is drawn.

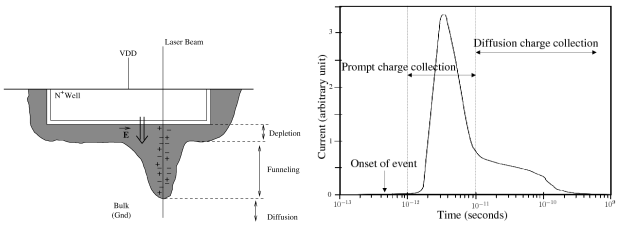

Figure 1. Photoelectric effect of a laser beam through a PN-junction (left) - Transient current resulting from charge collection after a laser shot [14] (right).

This phenomenon can be decomposed in two parts described in [14]. In a first time, the depletion region (hence the electric field) is stretched along the laser beam, the charges nearby are collected in a few picoseconds and gives a current peak, called funneling. In a second time, the remaining charges are collected in a longer phenomenon, called diffusion. The current decreases slowly until all charges are collected. The outline of the corresponding photo-current is displayed on the right part of Figure 1.

It exists a strong electric field, sufficient to create a transient current as explained above, in any PN-junction of the transistors used in CMOS logic regardless of their state (i.e. turned "*ON*" or "*OFF*"). However, such a transient current may, or may not, have an effect on the target's logic signals depending on both its location and the data handled by the logic. These dependencies are usually explained by considering the inverter case (see Figure 2).

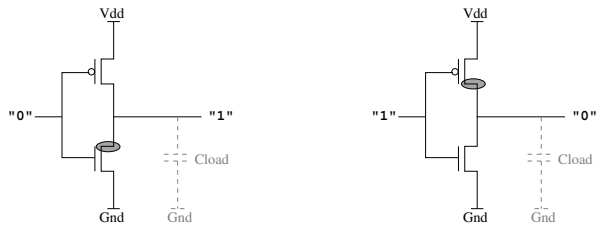

Figure 2. Inverter's schematic with its data-dependent sensitive areas.

Consider the left part of Figure 2 where the inverter's input is at a low logical level: its PMOS transistor is turned "*ON*" and its NMOS transistor is turned "*OFF*". Hence the inverter's output is at a high logical level and its output's capacitive load (dotted in Figure 2) is charged. The inverter has four PN-junctions which are likely to give rise to a transient current if struck by a laser: the drains and sources of both PMOS and NMOS transistors. Nevertheless only a transient current originated in the NMOS' drain will result in a disturbance of the inverter's output (pointed out by a filled grey ellipse). In that case, the transient current is flowing from the drain to the substrate which is grounded (as drawn in the left part of Figure 1). Hence the capacitive load is discharged provided that the transient current is big enough to overcome a charging current flowing through the "*ON*" PMOS transistor. As a result the output of the inverter passes temporarily to a low logical level. When the transient current vanishes, the capacitive load is charged again via the turned "*ON*" PMOS transistor. Thus, due to the transient current generated in the NMOS' drain, the output voltage of the inverter undergoes a transient voltage inversion. This transient voltage may then propagate through the downstream logic: a so-called Single Event Transient (SET). Any transient current created in the NMOS' source has no effect on the output since it is isolated from the output by the turned "*OFF*" NMOS. Regarding the transient currents created in the PMOS' diffusions, they create a leakage path to the N-well which is biased at the core supply voltage (i.e. Vdd). Hence they have no discharging effect on the output's capacitive load. To sum up, the only laser-sensitive area of an inverter, when its input is in a low logical state, is the drain of the "*OFF*" NMOS transistor.

Likewise, when considering an inverter with its input at high level (right part of Figure 2), a similar reasoning may be conducted. It results that the only laser-sensitive area of an inverter when its input is in a high logical state is the drain of the "*OFF*" PMOS (underlined in grey).

As a conclusion, the laser-sensitive area of a CMOS inverter is the drain of the "*OFF*" transistor, whose location is changing with the logical level of the inverter's input. In a more general way the laser-sensitive areas of CMOS ICs are data-dependent. The occurrence of a laser-induced fault depends on the handled data.

B. The SRAM *circuit*

The SRAM cell used in this study is a configuration SRAM (CSRAM), principally used to store the configuration bitstream in configurable logic (FPGA). It is part of a test chip designed in 0.25 μm CMOS technology with a 2.5 V power supply that embeds several patterns for laser testing. This CSRAM is constituted by five transistors, more precisely, two CMOS inverters and one access transistor. The schematic of the CSRAM is depicted in Figure 3.

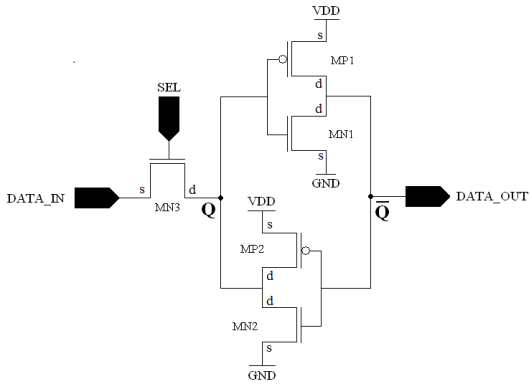

Figure 3. CSRAM's schematic.

This CSRAM is used to store a configuration bit, which is used through the output *DATA_OUT*. In the following we will refer to the CSRAM's state being state "1" as node *DATA_OUT* has a high logical level (i.e. $\overline{Q} = 1$); respectively, we will refer to state "0" as *DATA_OUT* is low (i.e. $\overline{Q} = 0$). The configuration bit is stored by the logical effect of the two cross-coupled inverters (built from the NMOS and PMOS transistors *MN1/MP1* and *MN2/MP2* respectively). It may be updated (from the value of the *DATA_IN* input) through the access NMOS transistor *MN3*, as long as it is in "*ON*" state (for $SEL = 1$). As $SEL = 0$, the access transistor is "*OFF*", thus the CSRAM is in its static mode: it memorizes its configuration bit.

A picture of the whole test chip is given in Figure 4, a zoom highlights the part where the CSRAM is located. The size of the CSRAM memory cell is 9 μm by 4 μm.

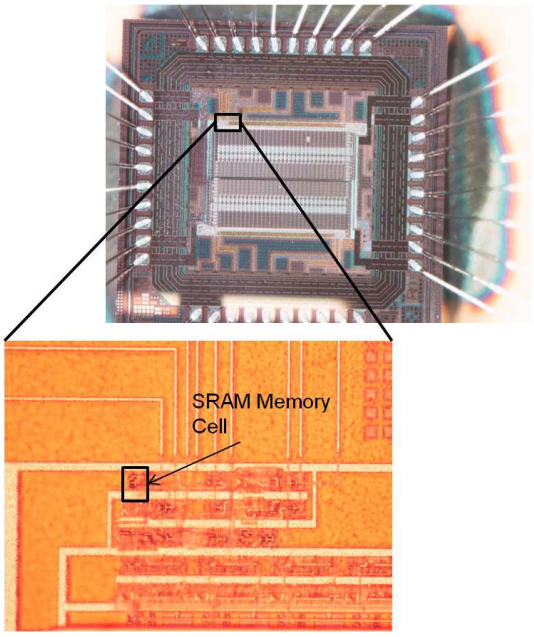

Figure 4. Test chip view, and close-up to the CSRAM cell.

Hereafter, we will rather use the term SRAM as the following results apply equally to standard six transistors SRAM cells.

C. Theoretical analysis of the SRAM's laser-sensitive zones

As presented in II-A, the laser-sensitive zones of a CMOS circuit are data-dependent. The laser-sensitive zones are highlighted on the SRAM's layout in Figure 5. Two zones, drawn in blue for laser-sensitivity in state "1", correspond to the drains of *MP2* and *MN1* (these transistors are turned "*OFF*" in state "1"). The laser-sensitive zones in state "0" are drawn in red. They correspond to the drains of the "*OFF*" transistors *MP1* and *MN2/MN3* (as seen on the layout *MN2* and *MN3* share a common drain diffusion). Thus, the analysis of the layout leads theoretically to the existence of four data-dependent laser-sensitive zones: two in state "1" and two in state "0".

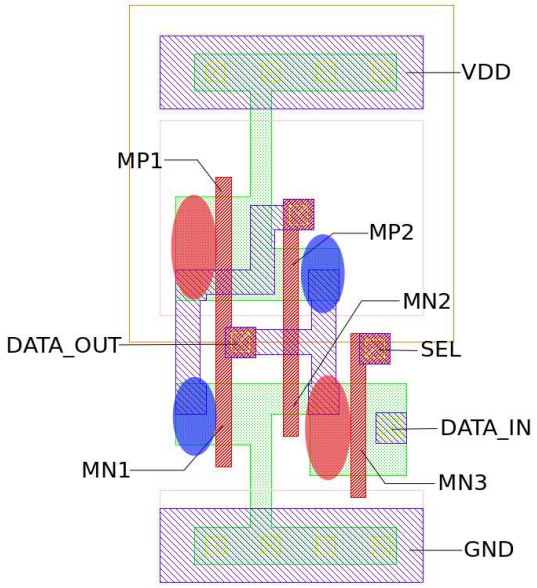

Figure 5. CSRAM layout with theoretical laser-sensitivite zones: blue for state "1", red for state "0".

Such a laser-sensitive zones cartography is consistent with the *bit-set/reset* fault model. For a laser beam directed on a blue zone, a fault may appear provided that the SRAM is in state "1": this would be a *bit-reset* fault. Respectively, for a laser beam directed on a red zone, a fault may appear provided that the SRAM is in state "0": this would be a *bit-set* fault. This cartography excludes the feasibility of a *bit-flip*, for there is no location where a fault may be induced irrespectively of the SRAM's state (there is no overlap between blue and red zones).

However, this behaviour is questionable. Indeed, the previous analysis was made under the assumption that one laser shot will affect only one sensitive zone. Two parameters put this assumption at stake: (1) the SRAM size, which is 4 μm $\times$9 μm; (2) the minimum feasible diameter of a laser spot which is 1 μm given the laws of optic, moreover its effect area may extend far beyond it (depending on the pulse energy) [15]. Thus the laser-sensitive zones shall extend beyond the drains: they may overlap as depicted in Figure 6.

The overlapping of laser-sensitive zones corresponding to *bit-set* and *bit-reset* gives rise to the feasibility of a bit-flip: if a laser shot arises on an overlapping area as depicted in Figure 6, the SRAM's configuration bit will be inverted irrespectively of its state. This correspond to a *bit-flip* fault model.

The next section presents the laser injection experiments carried out on this SRAM cell for the purpose of identifying the actual fault model.

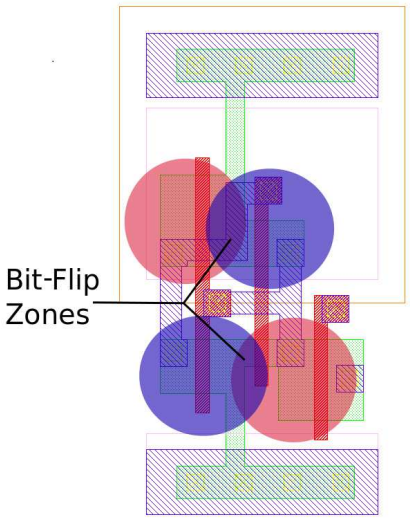

Figure 6. CSRAM layout with bit-flip zones.

III. Experiments

A. Laser Set-up

The experiments reported in this section were performed in front side with a laser source at 1064 nm wavelength. The duration of the laser pulses was set to 50 ns. The laser power range extends from 0 to 3 Watts. The size of the laser spot could be chosen among three values, depending of the optical lenses, let 1 μm, 5 μm and 20 μm. The test chip was mounted on a motorized XYZ stage. It permitted us to draw an experimental cartography of the laser-sensitivity of the SRAM as reported in the following subsection.

B. Laser-sensitivity maps for small and large laser spots

An area of 10x10 μm^2, around the SRAM, was scanned with a resolution step of 0.2 μm. For each scanning point, the SRAM was written either in state "1" or in state "0". Then, the laser was fired. After a few μs the SRAM's state was read back and compared to the state value initially written. In case of fault, the corresponding scanned point was added to the laser-sensitivity cartography. We used the term *bit-set* fault (resp. *bit-reset* fault) for a fault injected as the SRAM was in state "0" (resp. in state "1"). Figure 7 depicts the laser-sensitivity map of the SRAM at 1.6W and 1 μm laser spot diameter. Coordinates corresponding to *bit-set* faults (resp. *bit-reset* faults) are given in red (resp. blue).

In Figure 7, there are two zones corresponding to *bit-set* faults (the drains of *MP1* and *MN2/MN3*) and one zone corresponding to *bit-reset* fault (*MN1*'s drain). The *bit-reset* laser-sensitive zone corresponding to the drain of *MP2* is missing. The hypothesis that this missing sensitivity zones is due to the metal coverage is not relevant here. As it can be observed on the Figure 5, the drain of *MP2* is not covered by metal layer. A similar effect is also reported in section V. However, despite being promising, the analysis of this phenomenon is out of the scope of this paper.

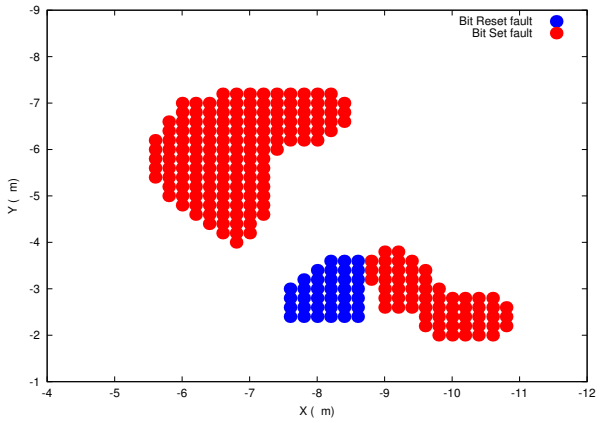

Figure 7. Experimental laser-sensitivity map of the SRAM at 1.6W

The main point with this cartography is that *bit-set* and *bit-reset* sensitive zones do no overlap. Consequently, there is no laser shot location where a fault may be induced whatever is the SRAM's state: the bit-flip fault model proved irrelevant.

Identical results were obtained for other experiment series conducted with laser spot diameters set to 1 μm, 5 μm and 20 μm, and laser power in the 1 W to 2 W range (the SRAM cell is destroyed for a laser power above $2W$, probably because of a latchup and the SRAM's value cannot be read or write). As a conclusion, based on these experimental results we concluded that the fault model of laser-induced faults on this SRAM is the *bit-set/reset* model.

The obtained cartographies showed no overlap between *bit-set* and *bit-reset* zones. However, these zones can almost touch each others (see the bottom part of Figure 7) suggesting that an overlap is not absolutely impossible. In order to confirm the lack of bit-flip we have further investigated the injection of faults in this location on a simulation basis as reported in the next section. Moreover, additional tests were carried out on the RAM memory of a micro-controller for validation purposes (see section V).

IV. SPICE Simulation

A. Spice model

The simulations presented in this section were based on the SPICE model of MOS transistors under laser illumination introduced in [16]. According to this model, the photo-current induced by the laser beam in any PN junction of the SRAM was simulated by a voltage controlled current source with a current amplitude expressed by:

$$I_{laser} = (a * V + b) * \Omega_{laser} * S \quad (1)$$

where S is the surface of the sensitive zone in μm^2, a and b fitting parameters depending on the laser power (P_{laser} in Watts) and technology parameters, V is the reversed bias voltage of the PN junction under the laser illumination. a and b are expressed as follows (p, q, and s are fitting parameters defined in [16]):

$$a = p * P_{laser}^2 + q * P_{laser} \quad (2)$$

$$b = s * P_{laser} \quad (3)$$

Ω_{laser} is a parameter used to take into account the distance between the PN junction of interest and the laser spot (i.e. this model considers the topology of the target). The equation of Ω_{laser} is :

$$\Omega_{laser} = \beta * \exp(-\frac{d^2}{c_1}) + \gamma * \exp(-\frac{d^2}{c_2}) \quad (4)$$

where d is the distance between the sensitive zone and the center of the laser spot, c_1 and c_2 represents the influence of the optical lens uses to focus the laser beam, β and γ are fitting parameters.

To simulate a laser shoot on the SRAM circuit, each PN junction of the SRAM cell was connected to a current source modelling the laser-induced photo-current. Indeed, as demonstrated in [16], even if the sources and the drains of the "*ON*" transistors were not considered sensitive, a photo-current could be injected by a laser shoot. To simulate this effect, current sources had to be connected to all transistors sources and drains, not only to sensitivity zones. Finally, according to the layout of the memory cell presented in Figure 5 and the different shared diffusions, seven current sources were connected to the different drains and sources of the SRAM cell. The schematic of the final circuit used for simulation is depicted in Figure 8.

The surface of the SRAM was divided into squares of 0.5 μm $\times 0.5$ μm. For each simulated point, the distance between the laser beam and the different sensitive zones of the memory cell were calculated and injected in the I_{laser} expressions of their corresponding current sources. The other parameters have a fixed value.

B. Simulation of laser-sensitivity map

A first set of simulations was performed in order to draw the laser-sensitivity map of the SRAM cell: Figure 9 also depicts the corresponding fault-models (on simulation basis). This map was used for comparison purposes with the experimental results of section III-B. It validates the relevance of the model.

This simulated laser-sensitivity map is very similar to the experimental laser-sensitivity cartography shown in Figure 7. The sensitivity zone corresponding to the drain of *MP2* is well missing and at the bottom of the Figure, the *bit-set* area and *bit-reset* area do not overlap. The model of laser-induced effects has been developed for 90 nm technology,

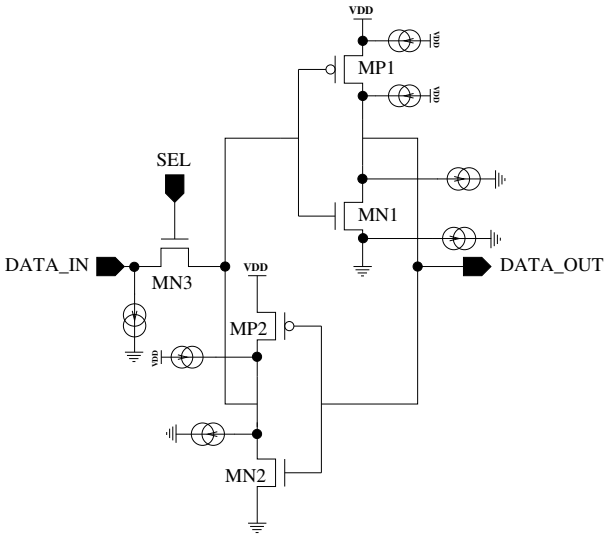

Figure 8. CSRAM schematic with current sources modelling laser-induced photo-currents.

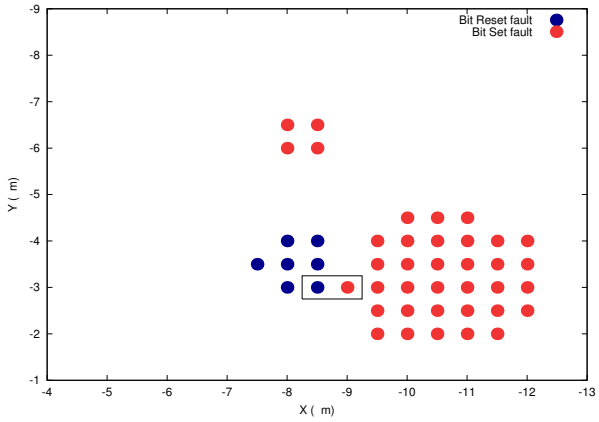

Figure 9. Laser-sensitivity map of the SRAM cell obtained from simulation.

it can explain the slight differences of the sensitivity zones between simulation and experiments performed with a test chip in 0.25 μm. However, the behaviour of the test chip and the simulation model were similar, that's allowed us to use this model to confirm the infeasibility of *bit-flip* fault (see next section). The two possible initial states of the SRAM ("0" or "1") have been simulated.

C. Analysis of laser fault simulation results

In Figure 9, there is only one contact point (with no overlap however) between *bit-set* and *bit-reset* zones: it is highlighted by a rectangle. We report in this subsection simulation results corresponding to laser injection in this area in order to illustrate the lack of *bit-flip* faults.

The first simulation was run for a laser shooting at the left inside part of this rectangle: a *bit-reset* sensitive zone. The SRAM was initialized in state "1", the laser pulse (50 ns

duration) was simulated at 200 ns. As expected, a *bit-reset* fault occurred as illustrated in Figure 10 where the voltages at nodes *Q* and *DATA_OUT* are drawn.

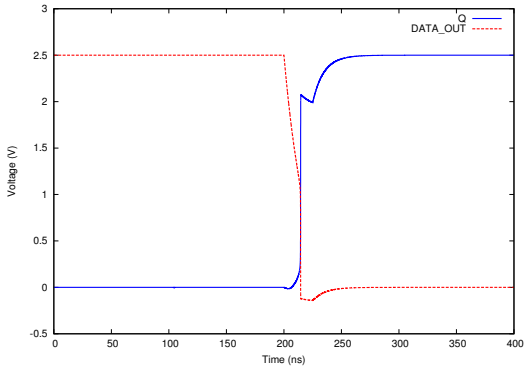

Figure 10. *Bit-reset* simulation: voltages at nodes *Q* and *DATA_OUT*.

The shooting zone is close to the drain of *MN1* which is laser-sensitive in state "1". As a result, a laser-induced photo-current, $I_{laser}(MN1)$, flows from *MN1*'s drain to the substrate which is grounded (see the corresponding current source model in Figure 8). This current has a discharging effect on node *DATA_OUT*. Note that a balancing current, $I_{SD}(MP1)$, flows from Vdd to node *DATA_OUT* through *MP1* (which is in "*ON*" state): it has a charging effect on node *DATA_OUT*. Both currents are depicted in Figure 11.

An SEU actually occurred because *MN1*'s photo-current overcame *MP1*'s balancing current. It is more noticeable by drawing the electrical charge injected by both currents on node *DATA_OUT* as displayed in Figure 12 (its absolute value is drawn).

From 200 ns to 220 ns, *DATA_OUT*'s charge decreases slowly because $I_{laser}(MN1)$ prevails on $I_{SD}(MP1)$ by only 10 μA. It drives progressively *DATA_OUT*'s voltage from 2.5 V to the SRAM's inversion threshold. Then, due to the inversion of the SRAM's state, this phenomenon accelerates as shown by the charge waveform. Finally, the SRAM stabilizes in state "0". A *bit-reset* fault injection has been simulated. There is a second balancing effect which comes from the photo-current induced in *MN2*'s drain: $I_{laser}(MN2)$ displayed in Figure 13. It flows from node *Q* (connected to *MN2*'s drain) to the ground.

Indeed, $I_{laser}(MN2)$ contributes to maintain node *Q* at a low logical level. However, its strength is too weak to avoid the *bit-reset*.

The second simulation was run with the same settings but the SRAM initialized in state "0". As expected for this location, no fault was injected. Figure 14 depicts the simulated voltages of nodes *Q* and *DATA_OUT*.

The laser beam closest laser-sensitive zone likely to induce a *bit-set* is the drain of *MN2*. Indeed the voltage of node *Q* undergoes a transient decrease during the laser shoot (from 200 ns to 250 ns in Figure 14). However, it is insufficient to

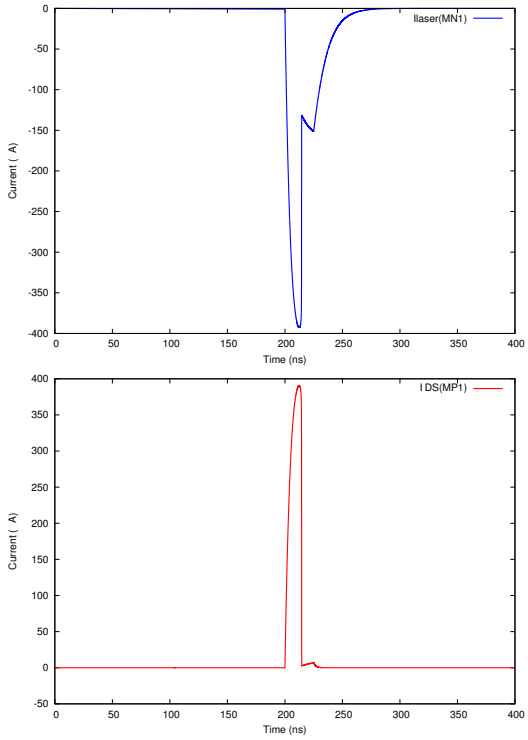

Figure 11. *Bit-reset* simulation: photo-current induced in *MN1*'s drain (upper part) and current flowing through *MP1* (bottom part).

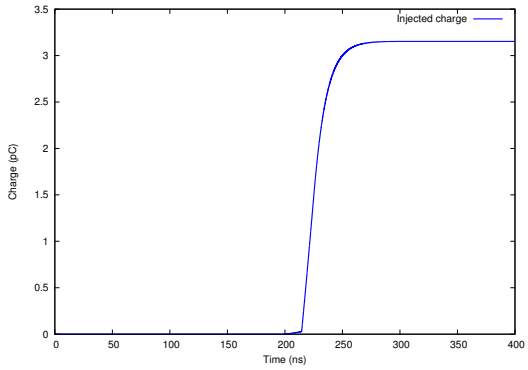

Figure 12. Simulation of the injected charge at node *DATA_OUT*.

change the SRAM's state. The photo-current induced in *MN2*, $I_{laser}(MN2)$, which has a discharging effect on node *Q* is balanced by the current $I_{SD}(MP2)$, flowing through *MP2* (in "*ON*" state). They are both depicted in Figure 15.

This balancing effect is clearly seen in Figure 16 where the electrical charge injected at node *Q* is drawn.

Node *Q* undergoes a discharge of about 0.03 pC, far below the 3.15 pC charge that was necessary to induce a *bit-reset* as illustrated in Figure 12. Note that, $I_{laser}(MN2)$ only grew to a maximum amplitude of 120 μA, whereas $I_{laser}(MN1)$ reached a current amplitude of 400 μA when the SRAM was in state "1" (see upper part of Figure 11). It explains why

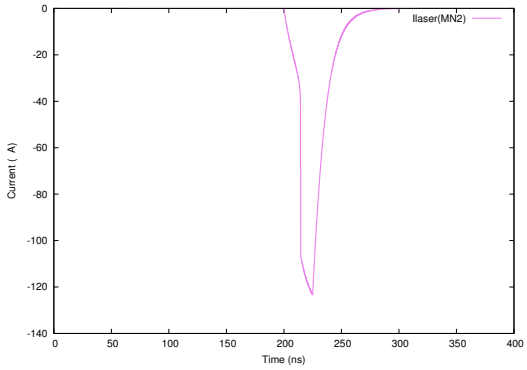

Figure 13. Simulation of the photo-current induced in the drain of *MN2*.

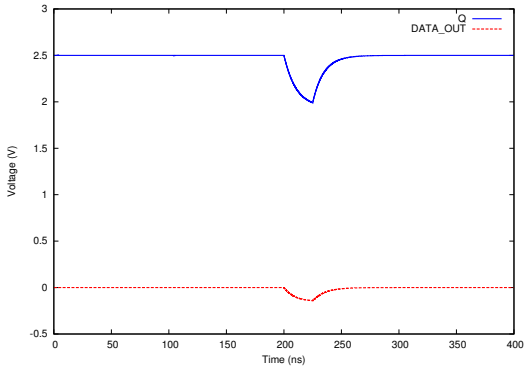

Figure 14. Aborted *bit-set* simulation: voltages at nodes *Q* and *DATA_OUT*.

no *bit-set* fault is induced at this laser location in state "0".

As the simulated laser beam is displaced to the right inside part of the rectangle in Figure 9, it reaches a *bit-set* sensitive zone. The third simulation we report was carried out at this location with an SRAM in state "0". Figure 17 reports the voltage simulations of nodes *Q* and *DATA_OUT* at this position. As expected, a *bit-set* fault occured. The photo-current induced in *MN2*'s drain overcome the *MP2*'s balancing current in the same way as with *bit-reset* fault simulation.

The electrical charge injected by both currents, drawn in Figure 18, has the same behaviour that one displayed in Figure 12. *MN2*'s induced photo-current drives progressively *Q*'s voltage from $2.5V$ to the SRAM's inversion threshold, then the electrical charge injected increases quickly until the SRAM stabilizes in state "1". A *bit-set* fault injection has been simulated. A photo-current is also injected on *MN1*'s drain that contribute to maintain *DATA_ OUT* at a low logical level but its maximum value is too low to avoid the *bit-set*.

The last simulation was carried out at the *bit-set* laser-sensitive zone with the SRAM in state "1". Figure 19 reports the simulation of nodes *Q* and *DATA_ OUT* voltages during laser exposure: no fault was injected.

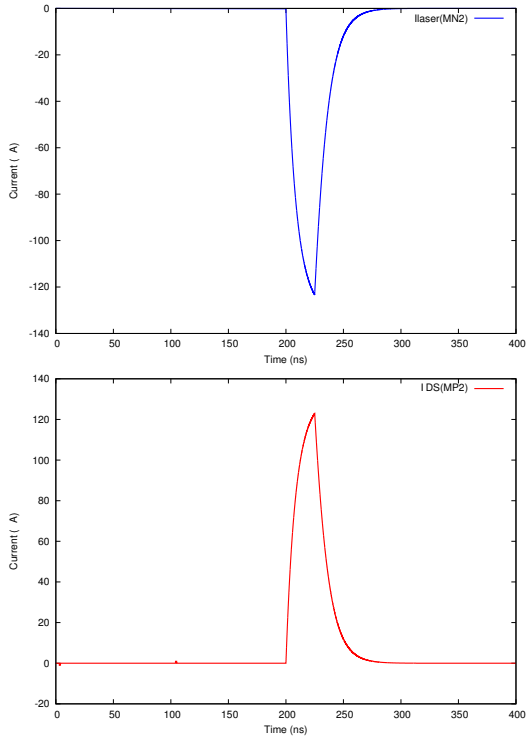

Figure 15. Simulation of *MN2*'s photo-current (upper part) and *MP2*'s current (bottom part) in state "0".

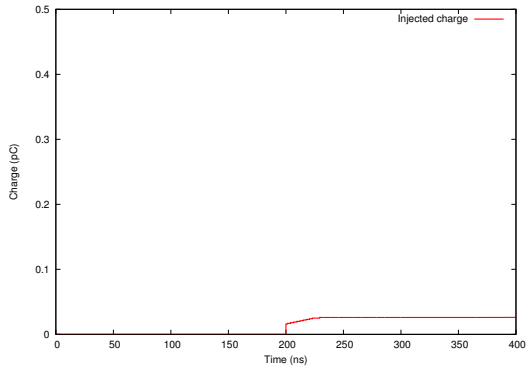

Figure 16. Simulation of the charge injected at node *Q*.

The electrical charge injected at *DATA_ OUT*'s node, depicted in Figure 20, is 0.03 pC which is far below the 0.7 pC charge necessary to change the SRAM state. Thus, a *bit-reset* fault is infeasible at this location.

Considering the two position highlighted on Figure 9 as the most likely position to have *bit-flip* fault, this type of fault is then infeasible on the memory cell.

To confirm the lack of *bit-flip* faults on SRAM cells, laser fault injection experiments have also been made on a micro-controller RAM memory as reported in the next section.

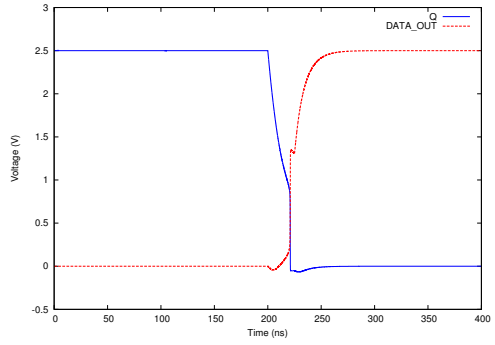

Figure 17. *Bit-set* simulation: voltages at nodes *Q* and *DATA_OUT*.

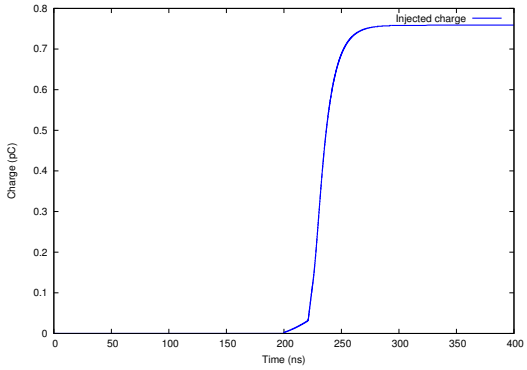

Figure 18. Simulation of the charge injected at node *Q*.

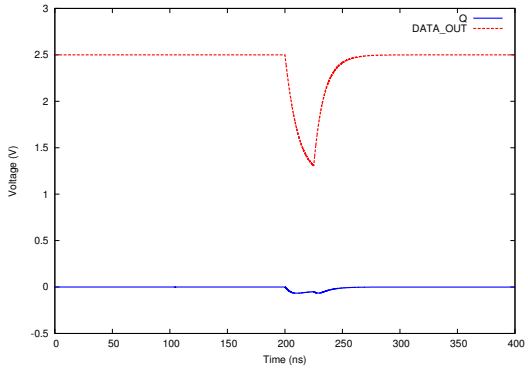

Figure 19. Aborted *bit-reset* simulation: voltages at nodes *Q* and *DATA_OUT*.

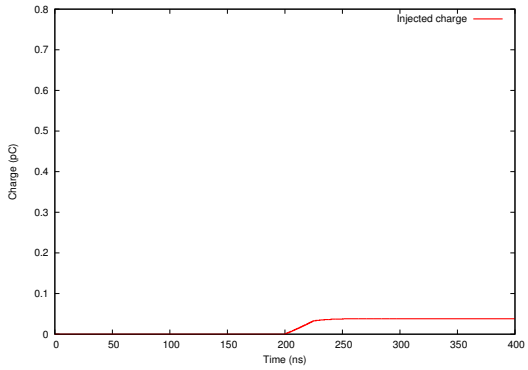

Figure 20. Simulation of the charge injected at the node *DATA_ OUT*.

V. Experiments on micro-controller RAM cells

A. Chip description

The test chip is an 8-bit micro-controller (0.35 μm CMOS process). The RAM of the chip is depicted in Figure 21. Its capacity is 4 kB divided in eight parts, each part contains two blocks of 256 kB. It can be assumed that each SRAM memory cell is constructed with six transistors (two cross coupled inverters and two access transistors). According the hypothesis made in part II-C, each cell should have four data-dependent laser-sensitive zones (two in state "1", two in state "0").

The fault injection experiments have been focused on few bytes of the memory, i.e. a zone of 40 μm $\times$ 40 μm with displacement steps of 0.5 μm. Laser injection was performed through the backside of the chip, with spot sizes of 1 μm and 5 μm. For each fault injection, the protocol was the same as described in section III-B. After the laser shoot, a block size of 256 kB, containing the targeted bytes, was read back and compared with the initially stored values.

B. Sensitivity of the RAM memory

Figure 22 shows the sensitivity map of the RAM memory with a spot size of 1 μm and a power of 1.1 W.

Twelve SRAM cells are clearly distinguishable in this Figure: for each of them a *bit-set* zone (in red) and a *bit-reset* zone (in blue) were revealed. No *bit-flip* was obtained. As with the experiments reported in part III-B, the *bit-set* zone and *bit-reset* zone do not overlap. For each SRAM cell, among the four theoretical sensitivity zones, two were not sensitive (this result is consistent with the experimental results of Figure 7, however, the analysis of this phenomenon is out of scope of this work). We were able to conclude on the absence of two laser-sensitive zones because we knew what bit of what byte was faulted. In addition, this methodology allowed us to draw a map of the memory (i.e. the location of every bit). In Figure 22, the size of an SRAM cell is highlighted by a square: it is about 5 μm $\times$ 5 μm. Note that we have induced single-bit faults (i.e. faults restricted to only one bit of the entire RAM memory) with a success rate close to 99 % during these experiments.

Some additional experiments have been conducted on this test chip at higher laser power and with a larger spot size. Figure 23 displays the result of the experiment at 1.2 W. More SRAM cells were sensitive but similarly to the previous experiments, *bit-set* zones and *bit-reset* zones do not overlap. Thus, increasing the power of laser has no effect on the feasibility of *bit-flip* fault injection.

The last experiment has been done at 1.1 W with a spot size of 5 μm. This time, the different memory cells were

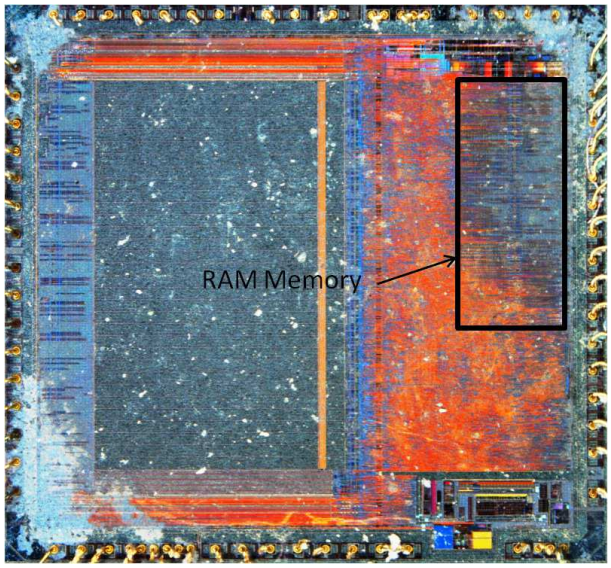

Figure 21. View of the micro-controller with its RAM memory area

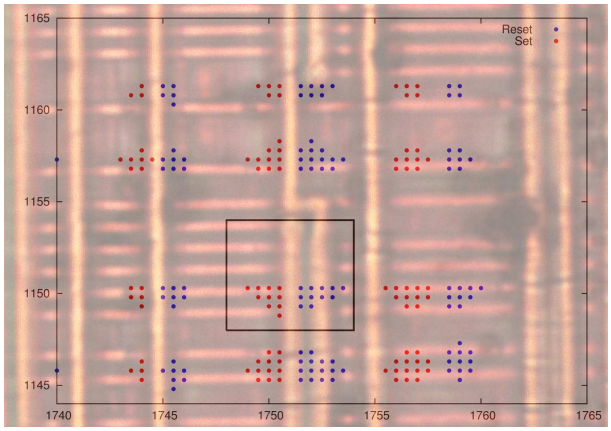

Figure 22. Laser-sensitivity map of the RAM memory at 1.1 W.

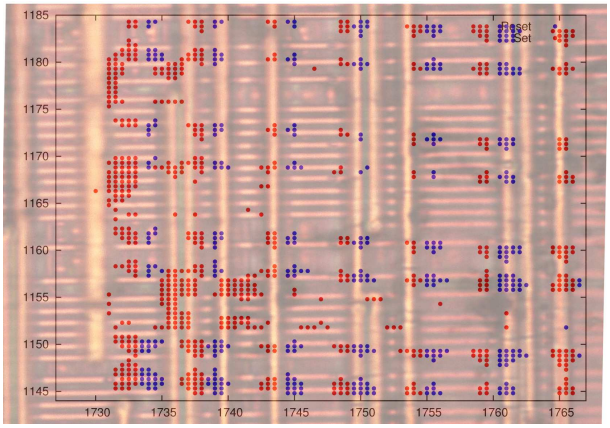

Figure 23. Laser-sensitivity map of the RAM memory at 1.2 W and with a spot size of 1 μm.

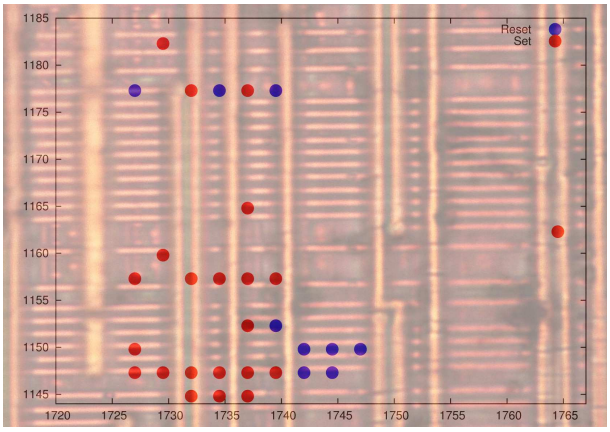

Figure 24. Laser-sensitivity map of the RAM memory at 1.1 W and with a spot size of 5 μm.

not distinguishable as depicted in Figure 23, yet the goal of this experiment was to verify the lack of *bit-flip* fault. It is clearly visible on Figure 24 that there is no overlapping of the *bit-set* and *bit-reset* zones.

Despite the use of different spot size or power for the laser, these fault injections on several SRAM cells confirm the lack of *bit-flip* faults on SRAM cells.

VI. Conclusion

In this paper, we have first reported laser fault injection experiments on a configuration SRAM cell (CSRAM) similar to those used to store the configuration bitstream of FPGAs. Different laser powers and spot sizes were used in order to investigate the corresponding fault model. The results of the experiments showed that the *bit-flip* fault model is not relevant for laser-induced fault in this memory cell. Only *bit-set* (or *bit-reset*) faults are feasible, contrarily to assumptions that may be drawn based on the fact that a laser spot may cover several sensitive zones. Additional SPICE simulations demonstrated and confirmed the infeasibility of *bit-flip* fault on the memory cell under laser illumination. It also provides a detailed understanding of the transition between *bit-set* and *bi-reset* zones as the laser beam location is changed.

Because these results were obtained with a particular SRAM, laser fault injection have been conducted on the RAM memory of a micro-controller for validation purposes. The results are in accordance with those obtained previously: no *bit-flip* has been injected on an area of 40×40 μm^2 gathering several SRAMs cell. Moreover, during these experiment series, almost all the injected faults were single-bit faults.

The *bit-set/reset* fault model related to laser-induced faults in SRAMs is very worrying. It makes it possible to mount relatively easily safe error attacks ([2], [10]) against cryptosystems. Moreover, even if some *bit-flips* are obtained on a given device, the occurrence rate of *bit-set/reset* faults will be much higher than that of *bit-flip*. Such a bias in the fault

statistics will still permit to perform attacks like a differential behavioural analysis [17].

Nevertheless, the analysis of the missing sensitivity zones as reported in sections III and V could bring some interesting elements to improve the security of SRAM memory elements against laser fault injection.

ACKNOWLEDGMENT

The research work of Cyril Roscian was partly funded by the "Conseil Regional PACA". The authors also would like to thank Ronan Lashermes for his help and his support.

REFERENCES

[1] S. Skorobogatov and R. Anderson, "Optical Fault Induction Attacks," in Cryptographic Hardware and Embedded Systems - CHES 2002, ser. Lecture Notes in Computer Science, vol. 2523, 2002, pp. p2–12.

[2] J. Blömer and J. Seifert, "Fault Based Cryptanalysis of the Advanced Encryption Standard (AES)," in Computer Aided Verification, ser. Lecture Notes in Computer Science, vol. 2742, 2003, pp. 162–181.

[3] M. Agoyan, J. Dutertre, D. Naccache, B. Robisson, and A. Tria, "When clocks fail: On critical paths and clock faults," Smart Card Research and Advanced Application, pp. 182–193, 2010.

[4] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic Transient Faults Injection on a Hardware and Software Implementation of AES," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on, 2012, pp. 7–15.

[5] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults," in EUROCRYPT '97, ser. Lecture Notes in Computer Science, vol. 1233, 1997, pp. 37–51.

[6] A. Biham, E.and Shamir, "Differential fault analysis of secret key cryptosystems," in Advances in Cryptology — CRYPTO '97, ser. Lecture Notes in Computer Science, vol. 1294, 1997, pp. 513–525.

[7] C. Giraud, "DFA on AES," in Advanced Encryption Standard – AES, ser. Lecture Notes in Computer Science, vol. 3373, 2005, pp. 571–571.

[8] G. Piret and J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad," in Cryptographic Hardware and Embedded Systems - CHES 2003, ser. Lecture Notes in Computer Science, vol. 2779, 2003, pp. 77–88.

[9] D. Otto, "Fault Attacks and Countermeasures," Ph.D. dissertation, Paderborn University (Germany), 2004.

[10] S. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," IEEE Transactions on Computers, vol. 49, pp. 967–970, 2000.

[11] P. Loubet-Moundi, D. Vigilant, and F. Olivier, "Static Fault Attacks on Hardware DES Registers," Cryptology ePrint Archive, Report 2011/531, 2011.

[12] V. Pouget, A. Douin, G. Foucard, P. Peronnard, D. Lewis, P. Fouillat, and R. Velazco, "Dynamic Testing of an SRAM-based FPGA by Time-Resolved Laser Fault Injection," in 14th IEEE International On-Line Testing Symposium (IOLTS), 2008.

[13] D. H. Habing, "The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits," in Nuclear Science, IEEE Transactions on, vol. 12, 1965, pp. 91 –100.

[14] F. Wang and V. Agrawal, "Single Event Upset: An Embedded Tutorial," in Proc. of 21st International Conference on VLSI Design, 2008, pp. pp. 429–434.

[15] F. Darracq, H. Lapuyade, N. Buard, F. Mounsi, B. Foucher, P. Fouillat, M.-C. Calvet, and R. Dufayel, "Backside SEU Laser Testing for Commercial Off-The-Shelf SRAMs," IEEE TRANSACTIONS ON NUCLEAR SCIENCE, vol. 49, no. 6, pp. 2977–2983, December 2002.

[16] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J. Dutertre, and A. Tria, "Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an NMOS transistor," in IEEE International Reliability Physics Symposium (IRPS), 2013.

[17] B. Robisson and P. Manet, "Differential Behavioral Analysis," in Cryptographic Hardware and Embedded Systems - CHES 2007, ser. Lecture Notes in Computer Science, 2007, pp. p413–426.