Figure of merits of 28nm Si technologies for implementing laser attack resistant security dedicated circuits

Stephan De Castro, Jean-Max Dutertre, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

http://dx.doi.org/10.1109/ISVLSI.2015.76
VLSI (ISVLSI), 2015 IEEE Computer Society Annual Symposium on

Figure of merits of 28nm Si technologies for implementing laser attack resistant security dedicated circuits

S. De Castro[1,2], J.-M. Dutertre[1], G. Di Natale[2], M.-L. Flottes[2], B. Rouzeyre[2]
1 : Ecole Nat. Sup. des Mines de St-Etienne, LSAS, CMP, 880 route de Mimet, 13541 Gardanne, France
2 : LIRMM CNRS/Université de Montpellier, Montpellier France

***Abstract*— Among all means to attack a security dedicated circuit, fault injection by means of laser illumination is a very efficient one. The laser beam creates electrons/holes pairs along its way through the silicon. The collection of these charges creates a transient current and thus may induce a fault in the circuit. Nevertheless the collection efficiency depends on various parameters including the technology used to implement the circuit. Here, up-to-date Bulk and Fully Depleted Silicon on Insulator (FD-SOI) 28nm technologies are compared in terms of sensitivity against laser injection. It comes out that FD-SOI structures show less sensitivity to laser injection and thus should be further explored for security dedicated circuits implementations.**

Keywords—hardware security, laser, fault injection, CMOS technology

I. INTRODUCTION

The development of security-dedicated circuits, e.g. smartcards or cryptoprocessors, goes together with the development of hardware attacks intended to retrieve secret information. Laser illumination is one of the means to perform such attacks in particular the so-called "fault attacks" that rely on disrupting the target's normal functional operation (e.g. **[3]**). Indeed, laser is particularly adequate since it offers a good accuracy in time and space to perform a precise disruption of the circuit **[2]**.

When the laser beam goes through the silicon, electron/hole pairs are generated if the energy of the laser's photon is higher than the silicon bandgap. These charges are then put in movement and collected by the transistor.

To describe the mechanisms involved in the collection of these charges, we concentrate on a PN junction in bulk transistors. The charge generation in the silicon along the laser beam is illustrated in Fig.1(a). The two mechanisms that put those charges in movement are illustrated in Fig.1(b) the drift current and in Fig.1(c) diffusion current.. The diffusion current is created by the movement of the charges carriers for maintaining the same carriers' concentration over the substrate. The diffusion current last longer than the drift current but is lower. These two mechanisms create a transient current that flows through the PN junction. The charge space zone of the PN junction amplifies this high current of short duration

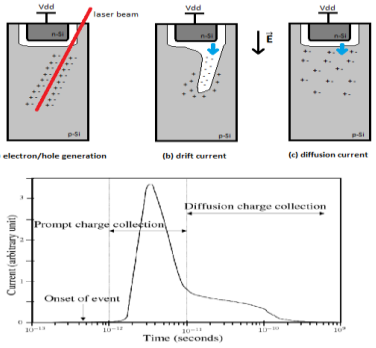

Fig. 1. charge generation and induced currenst due to laser injection on a PN junction [5]

Assuming this PN junction corresponds to the drain of an OFF-state NMOS transistor in an inverter, the induced transient current may discharge the output capacitance of the gate and thus creates a voltage transient on the gate output, which temporarily switches from 1 to 0. If the transient propagates to memory element(s), the transient fault turns into a single or multiple bit errors from which the attacker can retrieve a secret information, e.g. key bits in a crypto-coprocessor **[3][4]**.

As further discussed in section III, sensitivity to laser injection depends on the underlying CMOS technology. An old 90 nm bulk technology with an up to date 28nm FDSOI have been compared in [1], from which it comes out that old technologies are far more sensitive to laser attacks than recent ones. In this paper, we focus our study on the laser injection sensitivity on two up to date technologies, namely 28nm FD-SOI and 28nm bulk from STMicroelectronics.

For that, we illuminated two transistors of the same size, one for each technology, while keeping laser parameters identical. Transistors are illuminated from the backside of the chip, in order to avoid shadowing effects from the upper metal lines. Backside injection means that the laser beam goes through the silicon from the substrate to the metal lines above. An infrared source (1064nm) has been used in order to loose as few energy as possible in the substrate. While this

technique requires mechanical thinning of the substrate, it is generally preferred to "frontside injection" because of the metal lines on front side that act like mirrors, reflect the laser beam and prevent the laser to reach the silicon **[5]**.

For the sake of conciseness, we report figure of merits of both 28nm technologies thanks to experiments on PMOS transistors only. Similar experiments on NMOS transistors have been performed and lead to the same conclusion.

This paper is organized as follows. The structures of FD-SOI and bulk PMOS transistors on which experiments are performed are given in section II. Section III deals with the laser induced current model. Section IV describes the experimental setup. Comparative results are given in section V. Section VI concludes the paper.

II. FD-SOI VS BULK STRUCTURE OF A 28NM ST PMOS TRANSISTOR

A. *28nm PMOS FD-SOI and bulk structure*

The structures of the PMOS transistors used here are developed and provided by STMicroelectronics.

A CMOS cross-sectional view of the two structures is given in Fig. 2.

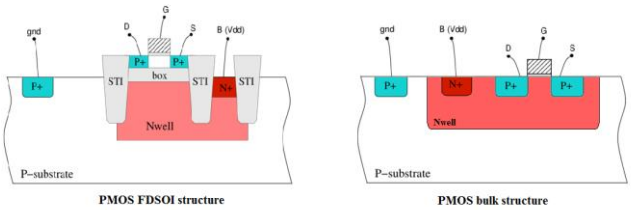

Fig. 2. Cross-sectional views of FD-SOI and bulk 28nm PMOS transistors

In Fig. 2, the red areas represent N doped region (Nwell), the blue areas represent P doped region (drain, source and substrate). The STI and box used in the FD-SOI structure are made of an insulator. The channel in the FD-SOI structure is completely insulated from the substrate conversely to the bulk structure. Moreover, for the FD-SOI structure, the channel is made of intrinsic silicon.

B. *Expected laser injection effects*

In this section we describe from a theoretical point of view the different contributions of charges.

In Fig.3, the induced currents that result from laser illumination are highlighted (green arrows).

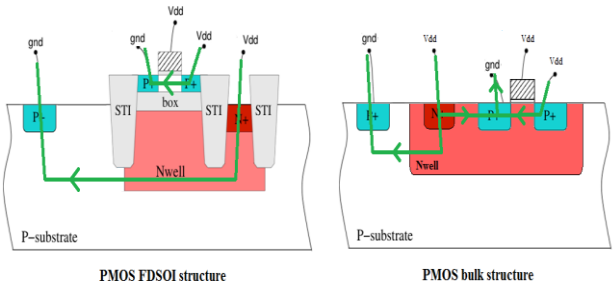

Fig. 3. Induced currents due to laser illumination for both structures

In the FDSOI structure, only two currents can be induced by the laser as illustrated on the left side of the figure. Those two currents are independent. The first one, which goes from the source to the drain, impacts the data path. The second current, which goes from the nwell to the substrate, changes the electric potential of the nwell. This change can alter the transistor function (e.g. threshold voltage). This alteration is not further discussed here.

Conversely, in a bulk structure a laser generates many currents. These currents interact with each other. Thus there is a competition between all these currents. The result of this competition depends on experimental parameters such as the spot size and the distance.

These parameters and the model used to describe the laser-induced currents are detailed in the next section

III. MODELING OF THE LASER INDUCED CURRENT

A laser-induced current model is defined in order to predict the current that flows through each PN junctions constitutive of the transistor. Such a model can be used in a simulator to predict the effect of a laser injection on a circuit **[5]**. The laser-induced current can be modeled by a current source. One current source is used for each charge collection points (drain, source, Nwell, substrate). The equation of the current source I_{ph} is given in equation (1) **[6]**.

$$I_{ph}(t) = \left[a(P).V_r + b(P)\right].A.\alpha_{\text{topology}}\,\omega_{\text{thick}}.\,\Omega_{\text{shape}}(t) \quad (1)$$

All functions except $\Omega_{\text{shape}}(t)$, represent the impact of a parameter on the magnitude of the induced current. Functions a and b represent the laser beam power dependence, V_r the reverse bias voltage of the PN junction, A the surface of the PN junction, α_{topology} the distance of the laser beam to the center of the PN junction, and ω_{thick} the wafer thickness.

All the constant coefficients of these functions depend actually on the technology used to implement the transistor. For instance, those coefficients have been set for 90nm bulk technology in **[5]**.

Finally the function $\Omega_{\text{shape}}(t)$ represents the shape of the induced current over time. It represents the shape of the induced photocurrent. This shape does not depend on the

technology used (FDSOI/bulk) or on the technology node. Fig. 4 shows the induced current measure over time for different illumination duration (from another transistor than the one used here).

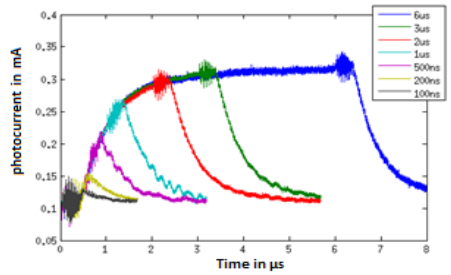

Fig. 4. Laser induced current over time for different illumination durations

IV. MEASUREMENT EQUIPMENT USED

In this section, the measurement methods and parameters are detailed. First, the laser injection parameters and information about the structures are given. Section IV.B deals with the measurement methods used to evaluate the induced current generated flowing through the transistor.

A. Laser and transistor's description

The FD-SOI and bulk transistors used for the experimentations are built using a 28nm CMOS technology developed by ST microelectronics for both technologies. As said before, the experiments results are reported for two PMOS transistors (FD-SOI and bulk). Both transistors have a channel width of 3µm and a channel length of 1µm.

Our laser bench allows performing backside injection with an infrared laser source (λ=1064nm). The laser beam used for the experimentation has a spot size of 1µm*1µm. For the transistors used here, the induced current typically reaches its maximum for laser illumination longer than 500ns (see Fig. 4). In order to be sure to actually measure the maximum current in spite of the jitter between the laser and the oscilloscope and avoid measurements noise, we have illuminated the circuits during 50µs.

B. Measurement circuit

The objective of the experiments was to measure the amplitude of the induced current flowing through the transistor. In order to do so, the transistor is set on "off" mode (the gate is connected to Vdd) and a resistor (1kΩ) is connected to the drain of the transistor. Other experiments have been performed with "on" mode (gate connected to gnd) and also measuring the drain induced current but are not presented in this paper. The results of those experiments lead to the same observations as the one shown here. Fig. 5 depicts the measurement circuit used.

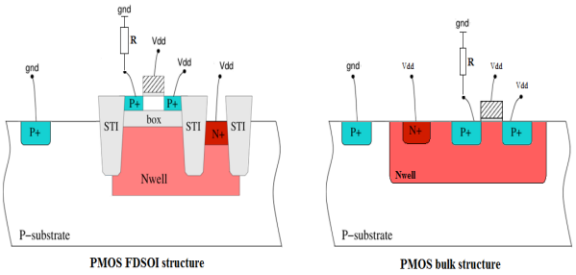

Fig. 5. Current measurement circuit

During the illumination of the transistor, the voltage over the resistance R is measured. The induced current flowing in the transistor is deduced from the Ohm law.

Among all the parameters that impact the induced current (laser energy, duration, supply voltage, etc.), here we focus on the effect of the distance between the laser beam and the transistor (α_{topology} in (1)). All the other parameters were set constant during the experiments.

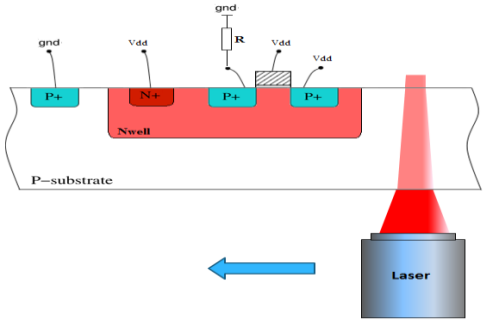

Fig. 6. Experiment to determine the effect of the horizontal distance on induced current (not scaled)

Fig. 6 depicts the performed experiments. The laser scans the transistor by 1µm step (following the two dimensions) in x and y directions. All the others parameters stay the same during the experimentation. Thus, the effect of the horizontal distance on the induced current amplitude is measured.

V. TECHNOLOGY SENSITIVITY TO LASER INDUCED CURRENT

In this section, results of the experimentations are discussed. The maximum amplitude of the induced current pulse as a function of the distance between the laser beam and the transistor's center is compared for both transistor structures. For confidentiality reasons, all the following measures are scaled using an arbitrary unit.

A. 28nm PMOS FDSOI vs 28nm PMOS bulk

Fig. 7 gives the maximum amplitude of the induced current collected by the drain for each laser injection position for both PMOS structures.

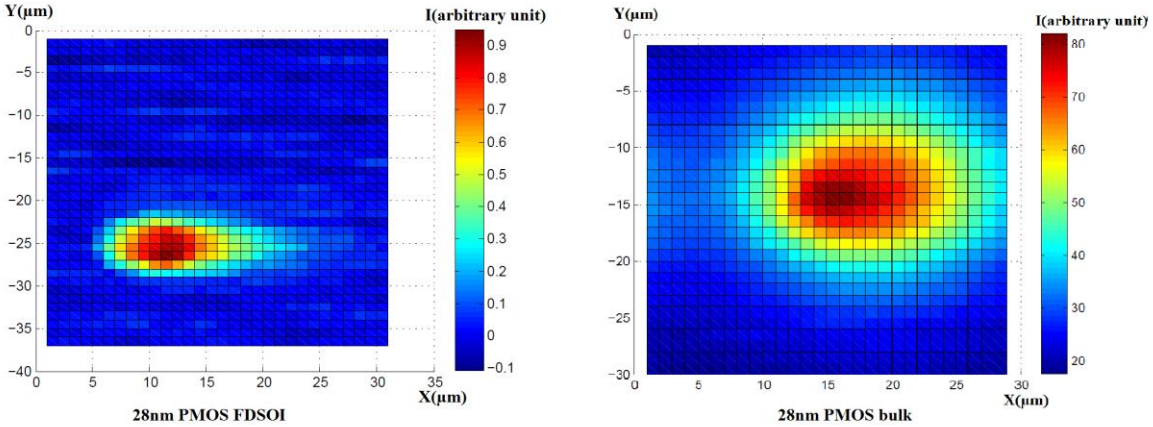

Fig. 7. Induced current amplitude for bulk and FD-SOI 28nm PMOS vs the distance (top view)

The experiment performed here measures the induced current flowing through the drain of the FD-SOI and bulk transistors. Red areas correspond to the more sensitive zones.

One can see in Fig. 7, that the red and yellow area is wider for the bulk structure than for the FDSOI structure (10µm*13µm for bulk against 5µm*7µm for the FDSOI).

These results have to be compared to the PMOS size. Its size is about 3µm*1µm. For FDSOI transistor, as the laser spot is not anymore above the transistor, the induced current maximum amplitude collapses.

The wide red area for the bulk transistor is due to the connection between the Nwell and the drain. Indeed the Nwell is wider than the transistor, thus it extends the area of effect of the laser injection. This shows that the distance sensitivity is less important for FDSOI transistors than for bulk ones.

Fig.8 gives a side view of the previous experimentation. This allows comparing the maximum induced current for the same PMOS transistor in FDSOI and bulk. It comes out that the induced current is much higher for the bulk transistor (1.7µA) than for the FDSOI transistor (20nA).

The explanation of this difference is that for the FDSOI transistor, the charges that are collected at the drain only come from the charges generated in the channel as depict in Fig.3. For the bulk, the current collected comes from the source and the Nwell of the transistor, which represents a wider volume of charges.

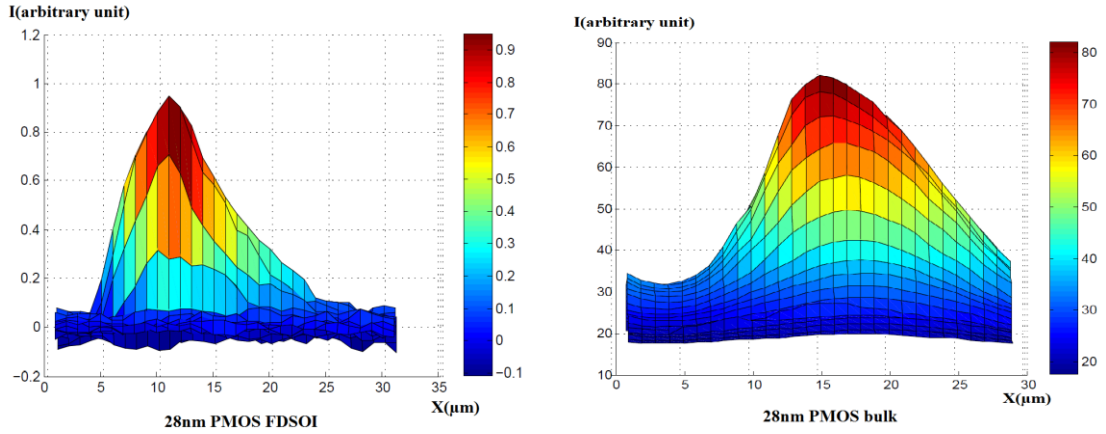

Fig. 8. normalized induced current vs the distance

Nevertheless, in terms of fault effects, these induced currents have to be compared with the current needed to charge (or discharge) the output capacitance (i.e input capacitance of the downstream logic gate) without laser illumination.

So, two inverters are connected together, with the PMOS transistor sized as the one used for the experimental measurements. The current needed to change the logic output of the second inverter is computed thanks to electrical simulation. For the FDSOI structure, the necessary current is about 0.2u. For the Bulk structure, this current is about 9u.

	FDSOI	Bulk
Maximal laser induced current	1u	80u
Necessary current to charge the	0.2u	9u

output capacitance		

Table 1: Current induced vs necessary current

It comes out that, even if the FDSOI is less sensitive than the bulk, fault injection can be performed in a secure dedicated circuit using 28nm FDSOI technology. Nevertheless, the parameters used in the reported experiments do not reflect parameters used to perform a fault injection used for an attack, in particular the duration of the laser illumination.

Indeed, in the previous experiments, the illumination time (50µs) is long enough to obtain the highest induced current amplitude but certainly would overlap several clock periods of the circuit, leading to unusable errors (for an attacker perspective). To perform fault injection, the illumination time has to be of the same range of the clock period (range of ns). If the illumination last shorter, the amplitude of the induced current decreases too.

So as the illumination time becomes shorter, the transistor becomes less sensitive to laser injection.

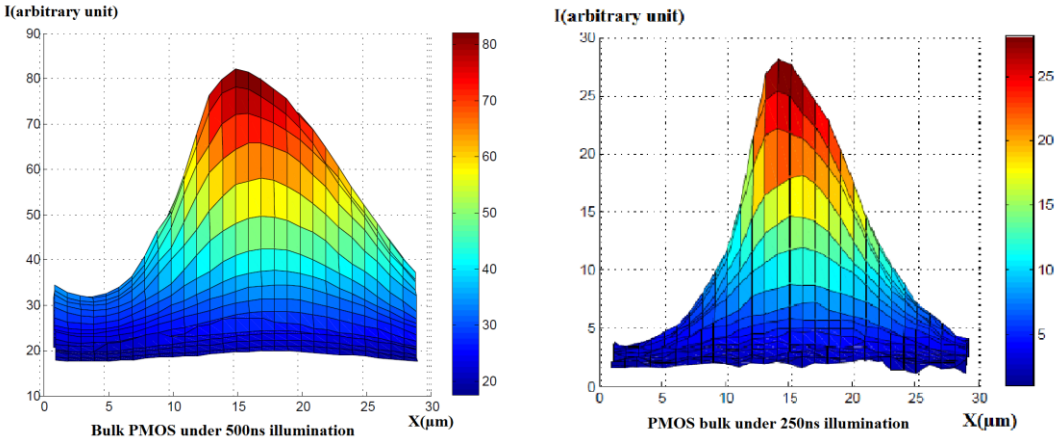

Figure 9: Induced current of 28nm bulk PMOS under illumination of 500ns and 250ns

So, the amplitude of the induced current decreases by 3 when the illumination time goes from 500ns to 250ns for the 28nm PMOS bulk transistors as depicted in Fig.9. This result is the same for bulk and FDSOI transistors.

B. 28nm NMOS FDSOI vs 28nm PMOS FDSOI

In this subsection, a comparison is made between a NMOS and PMOS in 28nm technology. The size and the experimental parameters are set as the previous experiments.

Fig.10 presents the induced current's maximum amplitude depending on the distance of the laser spot.

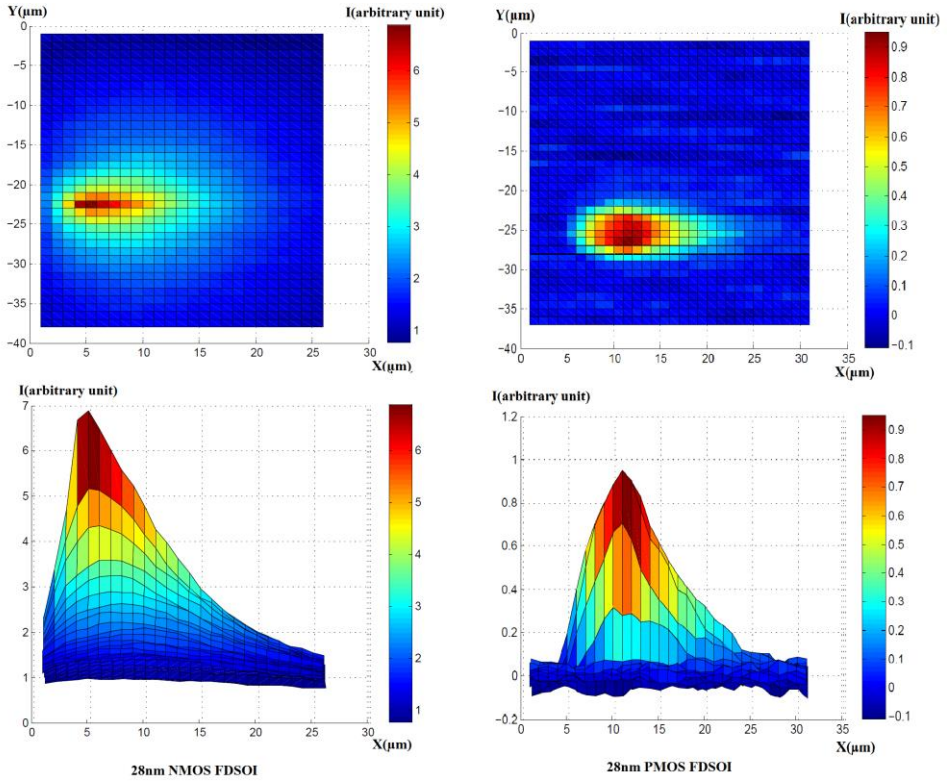

Figure 10: 28nm FDSOI NMOS and PMOS comparison

This experiment confirms that the 28nm FDSOI NMOS has the same "sensitivity features" as the 28nm FDSOI PMOS.

The difference of the induced current's maximum amplitude value between those transistors can be explained by the fact that they have the same size (3µm*1µm). However, in order to drive the same current, the PMOS has to be at least 3 times wider than the NMOS.

In spite of this difference, one can see that these "sensitivity features" comes from the FDSOI technology and are not a bound to the 28nm FDSOI PMOS.

VI. CONCLUSION

In this paper, results about the laser injection sensitivity for FD-SOI and bulk 28nm transistors are given. These results tend to prove that the 28nm ST FD-SOI technology is less sensitive than 28nm bulk technology to laser injection.

This result in favor of FD-SOI technology is due on one hand to the presence of the insulator surrounding the channel. One of the insulator's effect is to limit the volume of charges, thus reducing the induced current that flows through the drain. The other one is that when the laser spot is not above the FDSOI transistor the transistor is no more disturbed.

All these results tend to confirm that the ST FD-SOI technology is a better option to implement security dedicated circuits than bulk technology.

Acknowledgments

This work has been supported by the French "Agence Nationale de la Recherche" under contract ANR LIESSE (ANR-12-INSE-0008-01)

References

[1] Dutertre, Jean-Max, et al. "Laser attacks on integrated circuits: from CMOS to FD-SOI." Design & Technology of Integrated Systems In Nanoscale Era (DTIS), 2014 9th IEEE International Conference On. IEEE, 2014.

[2] C. Roscian, J.-M. Dutertre, A. Tria. Frontside Laser Fault Injection on Cryptosystems Application to the AES' last round. Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on, Jun 2013, Austin, United States.

[3] S. Skorobogatov and R. J Anderson. Optical fault induction attacks.In Cryptographic Hardware and Embedded Systems – CHES 2002.

[4] C. Giraud. dfa on aes. In Advanced Encryption Standard – Proceedings of aes 2004, volume 3373 of lncs, pages 27–41. Springer-Verlag, 2005.

[5] Feng Lu; Di Natale, G.; Flottes, M.-L.; Rouzeyre, B.; Hubert, G., "Layout-aware laser fault injection simulation and modeling: From physical level to gate level," Design & Technology of Integrated Systems In Nanoscale Era (DTIS), 2014.

[6] A. Sarafianos, ph.D Thesis, ENSMSE, "injection de fautes par impulsion laser dans les circuits sécurisés", 2013.

[7] Regis Leveugle, Paolo Maistri, Feng Lu, Giorgio Di Natale, Marie-Lise Flottes, et al.. Laser-induced Fault Effects in Security-dedicated Circuits. International Conference on Very Large Scale Integration (VLSI-SoC), Oct2014, Mexico, Mexico.

[8] Feng Lu; Di Natale, G.; Flottes, M.-L.; Rouzeyre, B., "Laser-Induced Fault Simulation," Digital System Design (DSD), 2013.