An experimentally tuned compact electrical model for laser fault injection simulation

William Souza da Cruz, Raphael Viera, Jean-Baptiste Rigaud, Guillaume Hubert, Jean-Max Dutertre

An Experimentally Tuned Compact Electrical Model for Laser Fault Injection Simulation

William Souza da Cruz*, Raphael Viera*, Jean-Baptiste Rigaud*, Guillaume Hubert† and Jean-Max Dutertre*
*Mines Saint-Étienne, CEA-LETI, Centre CMP, F - 13541 Gardanne France
†French Aerospace Laboratory, ONERA, Toulouse, France
*{w.souza-da-cruz, raphael.viera, rigaud, dutertre}@emse.fr †guillaume.hubert@onera.fr

***Abstract*—This work reports LFI experiments carried out on custom CMOS 65 nm digital test gates, aiming at tuning the parameters of a compact electrical model. Like in previous works, we observed a difference in behavior in the induced faults when using nanosecond and picosecond range laser pulse duration. However, our experimental results showed that the laser-sensitive areas were restricted to the PMOS transistors for ns laser pulses, contrary to what was previously stated in the literature. For ps pulse duration, these works outline the sensitivity of both the NMOS and PMOS of an SRAM cell following the theoretical model of LFI. These experiments help to calibrate the parameters of a compact electrical model, allowing the simulation of LFI attacks (using SPICE-like CAD tools). This compact model is built upon previous works, with simplifications to facilitate its use. Once tuned, simulations using the proposed compact model exhibit a good correlation with the experimental results.**

***Index Terms*—Laser fault injection, Electrical simulation, Electrical model, SRAM, Voltage transient**

I. Introduction

An electronic integrated circuit (IC) can be subjected to two types of faults: those caused by natural disturbances, or intentional faults. While the first type is caused by the environment to which the device is exposed [1], the second is usually caused for a specific purpose, such as a third party seeking to extract secret information [2].

Among the diverse types of physical attacks to which an IC is exposed, there are fault injection attacks (FIA) [3], [4]. This type of attack is based on disturbing the normal operation of the circuit by inducing computational faults inside it [5], [6]. Several techniques for inducing faults in ICs are already known and studied [3], [7]–[9].

In this context, laser pulse sources are used because of their high temporal and spatial resolution [10]. In [11] was shown the possibility of inducing faults in SRAM memory cells. It exposed the need to understand laser fault injection (LFI) attacks to design robust ICs. Since then, models and methodologies for simulating the effects of laser illumination on ICs have started to be developed.

This paper introduces a new model for simulating laser illumination phenomena in ICs at the electrical level. This model follows the methodology of a compact model [12], aiming at using known equations or elaborating new ones that allow performing simulations with a satisfactory level of precision and that are faster than more complex models.

This research has been supported by a PhD grant from the French region PACA (Emplois Jeunes Doctorants).

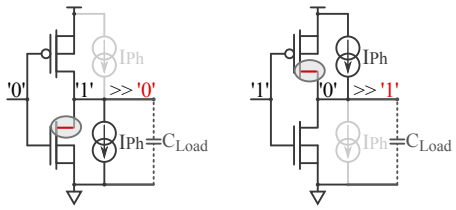
II. State of the Art of Laser Shot Effects on ICs

A. Effects of a Laser Shot on a PN Region

Transient electrical currents can be induced in an IC by its exposure to ionizing radiation or even by laser beams passing through the device [13], [14]. For a fault eventually to occur, this depends on several parameters such as the amplitude of the transient current (or photoelectric current, I_{Ph}, named after the charge generation mechanism), its location in the circuit logic and the handled input data.

B. Effects of a Laser Shot in a CMOS Inverter

A MOS transistor is composed of at least two PN junctions (drain and source), this makes such a device have regions sensitive to photocurrent induction. Fig. 1 shows the currents that can be induced in a CMOS inverter depending on its input.



(a) NMOS sensitive drain. (b) PMOS sensitive drain.

Fig. 1. Electrical model of laser-induced currents applied to a CMOS inverter.

Assuming that the input of the inverter is equal to the logical value '0', and the output is '1' (Fig. 1(a)), the equivalent output capacitance (C_{Load}) is fully charged. In this case, the drain of the NMOS is the most laser-sensitive location in the inverter. By illuminating this region with a laser, because there is a reverse biased PN junction, an induced current (I_{Ph}) flows from the drain of the NMOS to the $P_{substrate}$. When the input is '1' (Fig. 1(b)), the susceptible part of the inverter is the drain of the PMOS. In Fig. 1(a) (resp. Fig. 1(b)), a part of the I_{Ph} discharges (resp. charges) C_{Load}. Then, the output switches temporarily to a low voltage (resp. high voltage). This causes what is called Single Event Transient, or SET.

C. Effects of a Laser Shot on an SRAM Memory

The SRAM memory cell has been the subject of many works studying laser attacks [15]–[17]. It is composed of two cross-coupled inverters and two access transistors (Fig. 2).

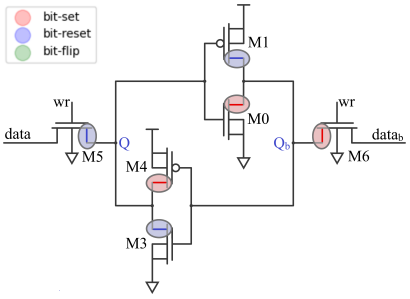


Fig. 2. Schematic of an SRAM cell with its laser-sensitive regions.

The two inverters are formed by transistor pairs $M1/M0$ and $M4/M3$, respectively. Transistors $M5$ and $M6$ are the access transistors. The two inverters operate to store the value of a single bit. If wr (signal to the gate of $M5$ and $M6$) is set to '0', the memory is in a hold state, storing the internal value. If wr is equal to '1', a value can be written in (or read from) the memory through the $data$ and $datab$ lines.

In Fig. 2 four theoretical zones in the inverters are highlighted, two in each of them. An SET induced in one of these sensitive areas will propagate through both inverters, inverting its stored value (a phenomenon called Single Event Upset, SEU). The colors red and blue are used to differentiate the type of fault the SRAM is exposed to in that region. In red are highlighted the zones that are sensitive to a bit-set: i.e. the change of the bit stored from '0' to '1' after a laser shot. In blue, by contrast, the sensitive zones to a bit-reset are highlighted (when a bit '1' stored in memory becomes '0' after a laser shot). In theory, there is also the possibility of bit-flip regions, which are regions sensitive to bit-set and bit-reset faults at the same time [16]. Two other theoretical sensitive zones are associated with the access transistors.

III. Experimental Study of Laser Effects on ICs

Experimental tests were performed to better understand the effects of laser illumination on ICs and to help the development of a compact electrical model for LFI simulations. A test chip containing different SRAM memories and basic gates, such as inverters and buffers, was used. It was manufactured at a 65 nm CMOS technology node, and it has a 1.2 V power supply.

The experimental tests were conducted with laser sources with pulse durations (d_p) in a range of ps and ns, and with wavelengths of 1,030 nm and 1,064 nm, respectively. The spot diameter used in all experiments was set to 1 μm.

A. Experimental Results - LFI on inverters

Our first LFI tests were performed on single inverters. The inverters' output signals pass through buffers and MUX gates before reaching the IC output pin. Hence, to observe SETs, it is necessary for the inverter's output voltage to reach the MOS devices' threshold voltage of the next structure in the circuit. To accomplish this, many tests were performed varying the laser power (P_{laser}) and d_p, as well as the shot coordinates. For this structure, no SET was observed during experiments. This result was expected for a ps range pulse. In fact, ps pulses induce short SETs that are filtered out by the chip output pads limited bandwidth.

B. Experimental Results - LFI on buffers

Further LFI experiments on buffer gates (made of two close inverters connected in serial) revealed the propagation of SETs for laser pulses in the ns range.

By mapping the region where the buffer is located, it was possible to observe SETs, especially in the region where the P-type transistors are located. The location that presented a longer SET duration was chosen for the LFI tests. The tests were carried out for different P_{laser} and d_p.

Fig. 3 provides the waveforms[1] of the induced SETs for P_{laser} = 1.8 W and d_p ranging from 100 ns to 2,000 ns. At 100 ns, no SET is induced. A threshold d_p has to be crossed, then SETs are induced with a duration growing with that of the laser pulse. Using the same experimental settings on single inverters did not produce any SET. This is due to compound effects: the laser shot induces I_{Ph} on the drains of the OFF transistors of the two buffer's inverters (which are both in the laser effect area). A single I_{Ph} is not able to generate an SET, while the addition of their effects on both inverters of a buffer is. This underlines the importance of taking into account all the laser-sensitive areas of a logic gate.

Fig. 4 reports the SETs induced for a 2,000 ns laser pulse with P_{laser} ranging from 1.2 W to 2.3 W. At 1.2 W no SET is induced, while at 1.3 W a threshold is reached, and an SET is generated (in red). However, it takes a delay greater than 1,200 ns for the SET to appear as the induced I_{Ph} is relatively low and hence takes time to force the buffer output to a faulty value. The resulting SET lasts less than 800 ns. As P_{laser} is increased, longer SETs are induced.

C. Experimental Results - LFI on SRAM cells

Experimental tests were also conducted on SRAM cells of various dimensions. Fig. 5 depicts the layout of the most compact SRAM, as well as its theoretical laser-sensitive zones.

The SRAM tests are performed by reading the stored data after each laser shot. Fig. 6 depicts a laser fault map obtained for P_{laser} = 2.1 W and a 50 ns laser pulse.

Only two laser-sensitive zones were found instead of the four theoretical zones shown in Fig. 5. In addition, these zones are centered on the two PMOS devices of the cell, as if its NMOS were not sensitive to laser illumination. This phenomenon of missing sensitive zones when targeting an SRAM cell with ns range laser pulses was already reported by [17]. However, contrarily with our results, they identified the PMOS as the non-sensitive transistors. It should be noted, however, that this previous work is based on experimental tests of a commercial CMOS 0.35 μm technology, for which the layout was unknown, hence NMOS may have been confused with PMOS.

Furthermore, confirming the results of [17], we effectively observed the four theoretical SEU-sensitive zones when using d_p = 30 ps, as presented in Fig. 7.

[1]Note that the SET voltage scale is reversed for ease of comparison with the simulations results of section V because the measured waveform is an inverted image of the buffer output while simulation results report directly the buffer output voltage.

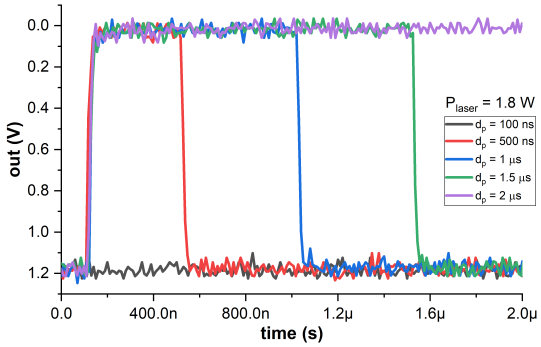


Fig. 3. Experimental results of LFI in a buffer for different pulse durations.

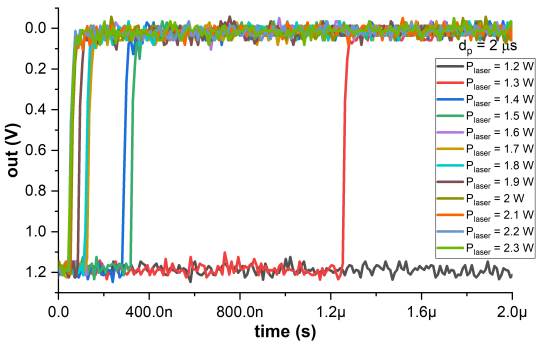


Fig. 4. Experimental results of LFI in a buffer for different laser powers.

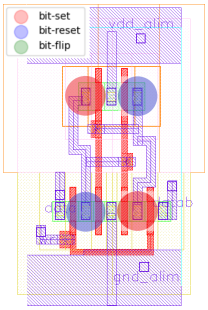


Fig. 5. Layout of the SRAM used for LFI experiments.

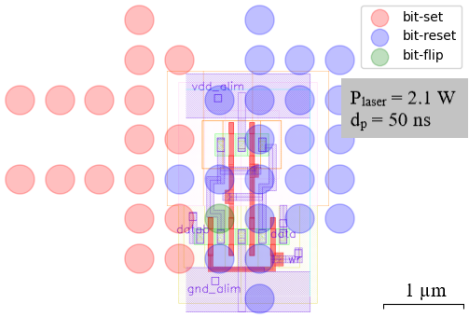


Fig. 6. SRAM LFI map at 2.1 W and 50 ns pulse duration.

[17] explains this phenomenon by underlying that ps laser pulses have a smaller effect area, hence limiting the compound effects of I_{Ph}. Longer pulses, in the ns range, have a larger effect area that creates compound effects responsible for masking the sensitivity of the SRAM NMOS (a mechanism that can be used to design LFI-hardened SRAMs [18]).

IV. Development of a Compact Model Used for Simulating Laser Beam Effects on ICs

A. Previous Models for Simulating Laser Effects on ICs

Simulation of laser effects on ICs can be considered at three different abstraction levels: physical, analog and logical. In our work, we focused on analog electrical simulation that can provide sufficient accuracy at describing LFI while avoiding the huge computational load of physical simulation. A SPICE model for LFI was introduced in [19], [20]. This model is based on a current source that is defined by the empirical Eq. 1:

$$I_{Ph\_peak} = (a \times V + b) \times \alpha_{gauss(x,y)} \times S \qquad (1)$$

where all parameters were defined experimentally using 90 nm CMOS technology node MOSFETs (cf. [19] for a thorough explanation of each parameter). This model proved to be satisfactory for this technology and d_p in the ns range. In [21], two different electrical models were proposed: one for short laser pulses and another for long pulses. Another approach was presented in [17], also based on Eq. 1 and experimental tests, certain parameters were modified to allow simulating laser effects with d_p of the order of ns and ps.

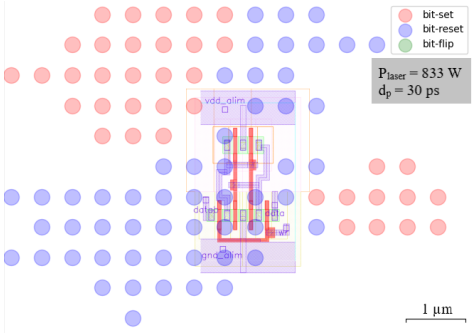


Fig. 7. SRAM LFI map at 25 nJ and 30 ps pulse duration.

B. Proposed Compact Model

This paper introduces a new compact model for LFI electrical simulation. A compact model should, as much as possible, efficiently describe the phenomenon under study while allowing easy implementation in simulators. For this purpose, it was chosen to develop this model in Verilog-A [12].

The model starts from the idea of adding current sources modeling I_{Ph} in each PN region of a circuit exposed to LFI, it is derived from Eq. 1. It is intended to consider the compound effects of the I_{Ph} induced at various sensitive nodes by a single laser shot. To do so, it considers the target topology at the layout level to set the parameters of the I_{Ph} sources.

One of the main additions or changes to Eq. 1 is that parameters a and b are calculated using a new P_{laser_Eff} parameter. P_{laser_Eff} is defined as the effective laser power achieved in the PN region. It is calculated using the spatial extension of the laser effect (parameter α_{gauss} that now models the P_{laser} distribution in space, and no longer the amplitude of I_{Ph}). To model α_{gauss} and add the effect of d_p to the equation, a β_{gauss} parameter was added to the α_{gauss} equation. Fig. 10 graphically presents the equation of I_{Ph} used and the equations of its parameters. r_{spot} is the laser spot radius and d the distance from the spot to the considered PN junction.

In Fig. 10, two curves are given: the first (left) depicts the relation between β_{gauss} and d_p, and the second (right) presents

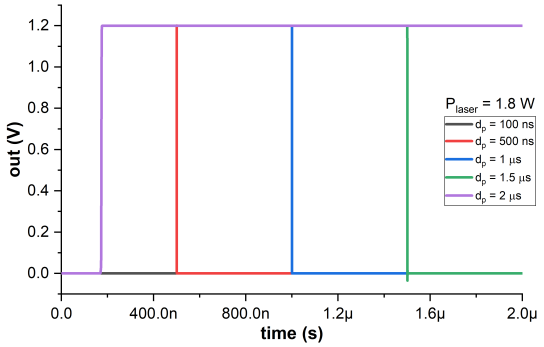


Fig. 8. Simulation results of LFI in a buffer for different pulse durations.

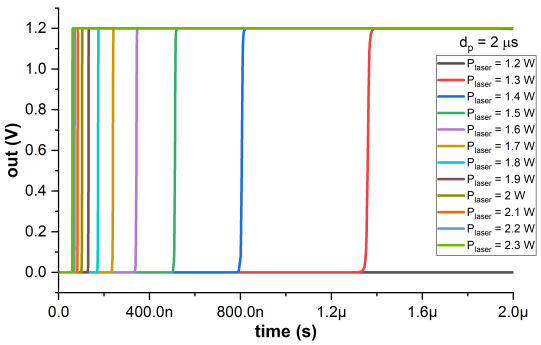


Fig. 9. Simulation results of LFI in a buffer for different laser powers.

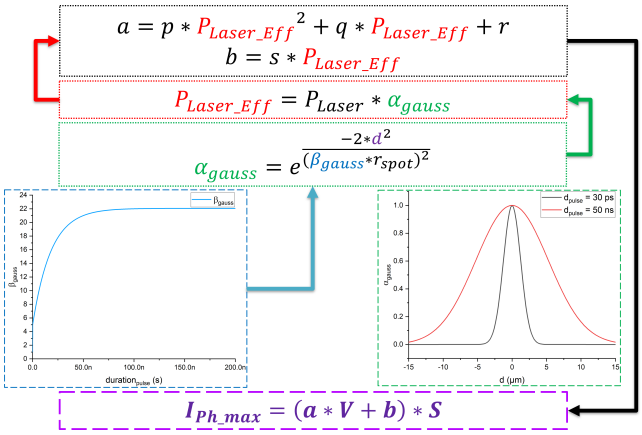


Fig. 10. Main parameters that compose the proposed compact model.

two examples of α_{gauss} as a function of the distance from the PN region to the laser shot location (for d_p = 30 ps and d_p = 50 ns). All the compact model parameters were calibrated from the experiments reported in section III. The compact model parameters are tuned progressively and iteratively by this fitting process. One aim of our approach was to demonstrate that it can be done from experiments carried out on digital gates (i.e. without the need for analog measures on dedicated test elements [20]).

Another addition to the proposed model was a parameter $tc1$ that controls the rise time of the I_{Ph}, depending on the P_{laser_Eff}. It is added separately from the main equation of the proposed model, and it is a novelty regarding previous models.

V. Simulation Results with the Compact Model

This section reports the simulation results with the proposed compact model. They were performed for the buffer of section III. Fig. 8 and Fig. 9 depict the output voltage of the simulated buffer. They can be directly compared to the waveforms in Fig. 3 and Fig. 4 to ascertain the quality of the compact model.

Fig. 8 depicts the simulated LFI at 1.8 W for different d_p. As for the practical experiments, no SET was induced for d_p = 100 ns. Simulations with longer duration pulses generated SETs results similar to the experimental ones (see Fig. 3).

Fig. 9 illustrates the effect of P_{laser} on the induced SET for d_p = 2,000 ns. The same power threshold of 1.3 W is observed. It also shows a decreasing delay in generating an SET as P_{laser} is increased. These results are similar to what was observed experimentally (see Fig. 4).

Though accurate, the obtained compact model can still be improved using the experiments carried out on the SRAM cell, especially to tune the parameters used for ps range laser pulse duration. As the SRAM is a more complex structure with more sensitive zones and an internal feedback loop, it may further improve the model's accuracy (despite a more difficult fitting process).

VI. Conclusions

This work extends and confirms some aspects of previous LFI works. Among them, it experimentally showed the phenomenon of sensitive zones of an SRAM memory being hidden using laser pulses with duration in the ns range. This phenomenon had already been observed for older technologies [17]. However, we highlight that the hidden zones are related to NMOS transistors (not to PMOS as previously assumed). These results underline the importance of considering the duration of the laser pulses in LFI attack, as different sensitive zones were revealed for ns and ps range pulses. This shows that the currents induced in the P-type regions may be more relevant in the process of inducing faults (it may be related to the IR-drop effects induced by laser illumination [22]).

The main goal of our wok was to introduce a new compact model for simulating the effects of LFI on ICs. This new compact model exhibits accurate results between experiments and simulation for ns range laser pulses (on a buffer manufactured in 65 nm CMOS technology). The modeling of the rise slope of the induced I_{Ph} current is a key point, being something not seen in previous models or discussed in previous works about laser fault injections. The compact model parameters were tuned thank to LFI experiments carried out on simple logic gate of the targeted technology.

The next steps regarding the proposed compact model is to refine its parameters through additional experimental results with SRAM memories and conduct new simulations with different structures in order to evaluate its overall accuracy. If validated with satisfactory results, this model can be implemented in an IC design flow aiming at manufacturing robust devices when facing laser illumination.

The proposed compact model, being experimentally calibrated, will allow satisfactory results in this technology, but will eventually have to be recalibrated when applied to different technologies. The calibration can be done through digital cells, which makes this process straightforward.

REFERENCES

[1] J. F. Ziegler and W. A. Lanford, "Effect of cosmic rays on computer memories," Science, vol. 206, no. 4420, pp. 776–788, 1979. [Online]. Available: http://www.jstor.org/stable/1749072

[2] C. H. Kim and J.-J. Quisquater, "Faults, injection methods, and fault attacks," IEEE Design & Test of Computers, vol. 24, no. 6, pp. 544–545, 2007.

[3] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," Proceedings of the IEEE, vol. 100, no. 11, pp. 3056–3076, 2012.

[4] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," Proceedings of the IEEE, vol. 94, no. 2, pp. 370–382, 2006.

[5] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques, ser. EUROCRYPT'97. Berlin, Heidelberg: Springer-Verlag, 1997, p. 37–51.

[6] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '97. Berlin, Heidelberg: Springer-Verlag, 1997, p. 513–525.

[7] M. Agoyan, J.-M. Dutertre, D. Naccache, B. Robisson, and A. Tria, "When clocks fail: On critical paths and clock faults," vol. 6035, 04 2010, pp. 182–193.

[8] R. Ahmadi and F. Najm, "Timing analysis in presence of power supply and ground voltage variations," in ICCAD-2003. International Conference on Computer Aided Design (IEEE Cat. No.03CH37486), 2003, pp. 176–183.

[9] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2012, pp. 7–15.

[10] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, ser. CHES '02. Berlin, Heidelberg: Springer-Verlag, 2002, p. 2–12.

[11] 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 2008 14th IEEE International On-Line Testing Symposium, 2008, pp. 295–301.

[12] C. C. McAndrew, G. J. Coram, K. K. Gullapalli, J. R. Jones, L. W. Nagel, A. S. Roy, J. Roychowdhury, A. J. Scholten, G. D. J. Smit, X. Wang, and S. Yoshitomi, "Best practices for compact modeling in verilog-a," IEEE Journal of the Electron Devices Society, vol. 3, no. 5, pp. 383–396, 2015.

[13] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," IEEE Transactions on Nuclear Science, vol. 12, no. 5, pp. 91–100, 1965.

[14] A. Johnston, "Charge generation and collection in p-n junctions excited with pulsed infrared lasers," IEEE Transactions on Nuclear Science, vol. 40, no. 6, pp. 1694–1702, 1993.

[15] A. Sarafianos, C. Roscian, J.-M. DUTERTRE, M. Lisart, and A. Tria, "Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell," Microelectronics Reliability, vol. 53, no. 9-11, pp. 1300 – 1305, Sep. 2013. [Online]. Available: https://hal-emse.ccsd.cnrs.fr/emse-01100724

[16] C. Roscian, A. Sarafianos, J.-M. Dutertre, and A. Tria, "Fault model analysis of laser-induced faults in sram memory cells," in 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2013, pp. 89–98.

[17] M. Lacruche, N. Borrel, C. Champeix, C. Roscian, A. Sarafianos, J.-B. Rigaud, J.-M. Dutertre, and E. Kussener, "Laser fault injection into sram cells: Picosecond versus nanosecond pulses," in 2015 IEEE 21st International On-Line Testing Symposium (IOLTS), 2015, pp. 13–18.

[18] A. Sarafianos, M. Lisart, O. Gagliano, V. Serradeil, C. Roscian, J.-M. Dutertre, and A. Tria, "Robustness improvement of an sram cell against laser-induced fault injection," in 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2013, pp. 149–154.

[19] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J.-M. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology," in 2013 IEEE International Reliability Physics Symposium (IRPS), 2013, pp. 5B.5.1–5B.5.9.

[20] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J.-M. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of a pmos transistor in 90nm technology," in Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), 2013, pp. 22–27.

[21] A. Douin, V. Pouget, F. Darracq, D. Lewis, P. Fouillat, and P. Perdu, "Influence of laser pulse duration in single event upset testing," IEEE Transactions on Nuclear Science, vol. 53, no. 4, pp. 1799–1805, 2006.

[22] R. A. C. Viera, P. Maurine, J.-M. Dutertre, and R. Possamai Bastos, "Simulation and experimental demonstration of the importance of ir-drops during laser fault injection," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 6, pp. 1231–1244, 2020.