Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael Viera, Philippe Maurine, Jean-Max Dutertre, Rodrigo Possamai Bastos

Importance of IR Drops on the Modeling of Laser-Induced Transient Faults

Raphael A. Camponogara Viera*†‡, Philippe Maurine*, Jean-Max Dutertre†, and Rodrigo Possamai Bastos‡,
* LIRMM, CNRS, UMR N5506 (Montpellier, France)
† Ecole Nat. Sup. des Mines de St-Etienne (Gardanne, France)
‡ Univ. Grenoble Alpes, CNRS, TIMA (Grenoble, France)
raphael@ieee.org, philippe.maurine@lirmm.fr, dutertre@emse.fr, rodrigo.bastos@imag.fr

***Abstract*—Laser fault injection attacks induce transient faults by locally generating transient currents capable of temporarily flip the outputs of several gates. Many models used to simulate transient faults induced by laser consider several elements to better represent the effects of the laser on ICs. However, a laser-induced current between VDD and GND, which provokes significant IR drops, has been neglected. This paper highlights the importance of the induced IR drops on the modeling of laser-induced transient faults by using IR drop CAD tools. It also shows that laser-induced IR drops can be sufficiently strong to produce alone transient faults. As a result, the number of faults on a case-study circuit is accentuated whether IR drop effects are taken into account.**

I. Introduction

The design of ICs, especially secure circuits, which have to be resistant to laser fault injection, requires mitigating the effects of transient faults at all design stages. This implies the capability of simulating the effect of laser shots. At electrical level, a double exponential current source is usually considered to model the effect of a laser shot in accordance with [1]. These current sources are added to the netlists of cells illuminated by the laser. Then an electrical-level simulation that takes into account the effects of the laser attack can be performed.

The idea commonly accepted, is that a laser shot generates parasitic currents [1]. These currents temporarily flip the output of few gates. This undesired state propagates toward the input of registers (flip-flops or latches) and, if it is still present when the clock edges occurs a soft error appears. However, flipping the output of a gate with a laser source forces it in a state where there is a massive short-circuit between VDD and GND (this current component has been experimentally validated in [2]). The question remains if this massive short-circuit creates significant IR drops and thus can induce transient faults by itself. This is an important question since as technology scales, ICs become increasingly sensitive to IR drops [3], [4].

To the best of our knowledge, there is only one investigation from [5] on the role of the IR drop in the fault injection process related to laser illumination. This paper's authors built the model of the laser illumination of an inverter, in which they consider the vertical parasitic bipolar junction transistors inherent to CMOS bulk devices. Showing that these parasitic transistors also contribute to the injected fault than just the PN junctions of the OFF MOS side. However, they did not study the effect of the IR drop in the fault injection mechanism.

In order to fill this gap, this paper contributions are:

- A transient fault model that takes into account the laser induced IR drop effects in the power and ground rails.
- a methodology, based on standard CAD tools and the proposed model, to simulate with the highest accuracy the effect of laser shots on complex circuits;
- Analysis of the IR drop generation phenomenon providing some highlights if the soft errors are induced by the propagation of a laser-induced perturbation through logic gates, due to IR drop effects or even accentuated when considering both effects.

II. Induced Transient Currents and Classical Transient Fault Model

ICs are sensitive to induced transient currents that may be caused by laser shots passing through the device, thus creating electron-hole pairs along the path of the laser beam. Induced charge carriers recombine without any significant effect, unless they reach the strong electric field found in the vicinity of reverse biased PN junctions. In this case, the electrical field puts these charges in movement and a transient current appears as well as a transient fault. The nature of this fault is similar to the ionization effect generated by energetic particles [6].

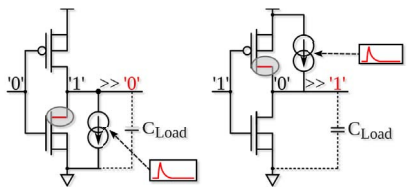


Fig. 1: Classical model: transient current modeled as a current source for: (a) NMOS sensitive drain (b) PMOS sensitive drain.

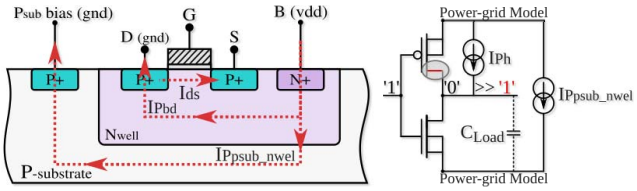
Fig. 1 illustrates the classical model explaining where laser shots generate a parasitic current. In the case the inverter input is in low state the most laser-sensitive part of the inverter is the drain of the NMOS transistor since there is a reverse biased PN junction between the drain and the P substrate. The effect of a laser is thus modeled by a double exponential current

source (Fig. 1(a)) placed between the drain and the source of the NMOS transistor. In the case of Fig. 1(a) (resp. Fig. 1(b)), a part of the induced current discharges (resp. charges) the output of the inverter and the other part is drawn from the VDD (resp. GND). A laser shot thus generates a short circuit and a transient voltage.

III. Proposed Model

According to the the classical fault model, the induced transient voltage propagates through the logic and eventually produces a soft error if latched by a flip-flop at the next rising clock edge. However, in advanced technologies this model is questionable. Indeed, for such technologies, a laser shot simultaneously illuminates several gates at a time and not only a PN junction. As a result, a direct and significant short circuit current flows directly from VDD (resp. GND) as shown by the component $I_{P_{sub\_nwell}}$ in Fig. 2(a). This current, which can produce significant IR drops, is neglected in the classical fault model. Fig. 2(b) presents the proposed model which takes into account the $I_{P_{sub\_nwell}}$ current as well as a non ideal power-grid model generated by a standard CAD tool.

This observation highlights the importance of considering the spatial distribution of the laser beam energy on the IC surface. It also highlights the importance of accurately modeling the power/ground network when one aims at simulating laser effects on ICs. Next sections address these points.



(a) (b)

Fig. 2: Laser-induced current component. (a) Cross-section of a PMOS transistor. (b) proposed model.

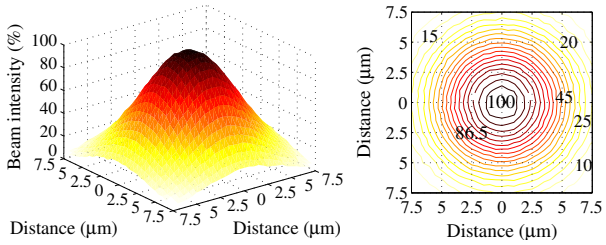
IV. Spatial Distribution of Laser Beam Energy

The beam diameter is the most important propagation attribute of a laser beam in a class of commonly measured parameters (beam diameter, spatial intensity distribution, beam quality factor etc.). A commonly used definition of the laser beam diameter is derived from the bivariate normal distribution of its intensity leading to measure the beam diameter at 86.5% of its maximum value [8], or a drop of $\frac{1}{e^2}$ from its peak value.

The effects of a Near Infra-Red laser beam have been modeled in [1] and later in [7]. In the latter work, it is shown that the induced photocurrent, which is spatially distributed as a bivariate normal distribution, has a peak amplitude I_{ph} that follows the empirical equation:

$$I_{ph} = (a \times V + b) \times \alpha_{gauss(x,y)} \times Pulse_w \times S \quad (1)$$

where V is the reverse-biased voltage, a and b are constants that depend on the laser power, $\alpha_{gauss(x,y)}$ is a term related to the bivariate distribution of the laser beam amplitude in space, $Pulse_w$ is a term allowing to take into account the laser pulse duration and S is the the area of the exposed PN junction. Refer to [7] for additional details of the above parameters.



(a) (b)

Fig. 3: Laser beam in terms of intensity per area. 100% of laser beam intensity represents the epicenter of the laser spot: (a) Three-dimensional view (b) contour lines.

By way of illustration, Fig. 3(a) shows a three-dimensional view of the normalized amplitude of a laser spot. Beam intensity at a given coordinate (x,y) represents the amount of power delivered by the laser source at this specific point. Fig. 3(b) presents the contour lines of Fig. 3(a) in order to provide a topographic view of the laser beam intensity.

V. Simulation Methodology

With all former considerations, a simulation methodology allowing to analyze the impact of IR drops induced by laser shots on complex circuits, has been set up and applied to a test case. This section describes the considered test case, the simulation flow and the simulation scenarios.

A. Device Under Test

The device under test (DUT) is an ARM 7 processor with 5k+ cells designed in a 28 nm technology with core voltage of 1.0 V. The core circuit area is $110\mu m$ x $70\mu m$.

B. Considered Laser Spot

Typical laser sources used to inject faults are characterized by a beam diameter equal to 1μm, 5μm or 20μm and a wavelength of $1064nm$. Although the minimum diameter of a laser spot is 1μm, given the laws of optic its effect area extends far beyond it [9], [10]. Consequently, a laser spot does not induce a single transient current but several transient currents at different sensitive nodes of the target. With this in mind, a spot diameter of 5μm was chosen for this experiment.

C. Design and Simulation Flow

The following steps constitute the design and simulation flow that has been followed in order to obtain the results presented in the next section; results aiming at highlighting the role of IR drops in the fault induction by laser.

- *step 1:* a typical IR drop analysis using an IR drop CAD tool is run;

- *step 2:* equation 1 is used to set the amplitude of the double exponential current source for each cell in the design illuminated by the laser according to the considered laser spot location. Then, a dynamic IR drop analysis is performed to estimate the impact of laser shot on the supply voltage distribution;
- *step 3:* step 2 is performed several times for different laser spot locations while keeping all other simulation parameters constant (spot diameter, intensity, etc.). For each iteration of step 2, a table containing the evolution in time of the supply voltage of each cell in the circuit is saved for future analyses. All these simulations allow to draw several IR-drop fault maps. Some are given later in the paper;
- *step 4:* all voltage waveforms generated by the IR drop CAD tool are injected in the netlist of the original design in order to successively perform a simulation considering the voltage drop of each cell for each considered laser spot location.
- *step 5:* for each considered laser spot location, a second simulation is performed. In the latter only the classical current sources with a double exponential shape are injected in illuminated gates to simulate the effects of the laser. Therefore, all cells in the design are considered supplied with the nominal VDD;
- *step 6:* at this step, both the voltage drops and the classical current sources with a double exponential shape are considered in the electrical simulation to get an insight of the overall effect of laser shots.

D. Simulated Scenarios

We report a total of 3 scenarios among the studied. They are illustrated in Fig. 4. In the first quadrant the clock signal waveform is used as a time reference. The three other quadrants give the typical evolutions observed during our simulations, of the signal Q_x, the output of the cell 'x' of the design under illumination, in three different situations. These situations represent the behavior when a laser pulse with 250 ps of duration starting at 1.7 ns (this time is more or less close to the next rising clock edge) strike a region of the circuit.

The 2^{nd} quadrant of Fig. 4 shows when only the classical current sources with a double exponential shape are considered to model the laser effects. The 3^{rd} quadrant shows when only the IR-drops are considered. The 4^{th} quadrant shows when both the current sources and the IR drops are considered.

In the 2^{nd} quadrant, the curve has a double exponential waveform. In the 3^{rd} quadrant, the curve has also a double exponential waveform, however, with a smoother profile. This is due to the filtering effect (RC effect) of the supply voltage network that also reduces its amplitude with respect to quadrant 2. The shape of the curve is similar in the 4^{th} quadrant to that of quadrants 2 and 3. However its amplitude is much more important and even greater than the sum of the amplitude of the corresponding curves in quadrants 2 and 3. Therefore, a simple superposition of the IR drop and current source effects cannot explain this result.

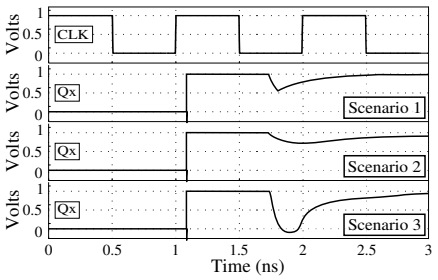


Fig. 4: Typical waveforms observed during simulations at the output of gates illuminated by a laser beam.

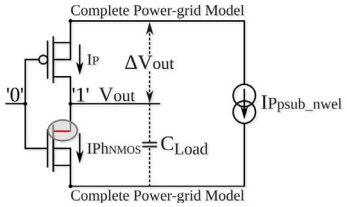


Fig. 5: Inverter with a low input signal under laser illumination

To explain this result, consider an inverter with its input signal at 0 in Fig. 5. In normal operation the current flowing in the PMOS transistor, which is in the linear operation, is equal to zero. Now, if the inverter is submitted to a constant laser illumination, the PMOS must let flow the photocurrent $I_{Ph_{NMOS}}$. This implies a fall of the inverter output equal to:

$$\Delta V_{out}(withoutIR) = \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - V_T)}, \quad (2)$$

in which $I_{Ph_{NMOS}}$ is the photocurrent amplitude as described in (1), W and L the width and the length of the PMOS transistor, μ the hole mobility and C_{ox} the oxide thickness.

In the above simple calculation, the supply voltage was considered unaffected by the laser shot and thus equal to VDD. Considering now that the laser shot generates an IR drop of amplitude ΔV_{drop}, the fall of the inverter output increases to:

$$\Delta V_{out}(withIR) = \frac{I_{Ph_{NMOS}}}{\frac{\mu \cdot C_{ox} \cdot W}{L}(V_{DD} - \Delta V_{drop} - V_T)}, \quad (3)$$

As shown by (3), the effect of the IR drop on the ΔV_{out} is hyperbolic. Voltage drops induced by laser shots have thus an important effect and cannot be neglected. This is especially true for IC designed in advanced technologies for which the supply voltage is low as shown by:

$$\frac{\Delta V_{out}(withIR)}{\Delta V_{out}(withoutIR)} = \frac{1}{1 - \frac{\Delta V_{drop}}{V_{DD} - V_T}} \quad (4)$$

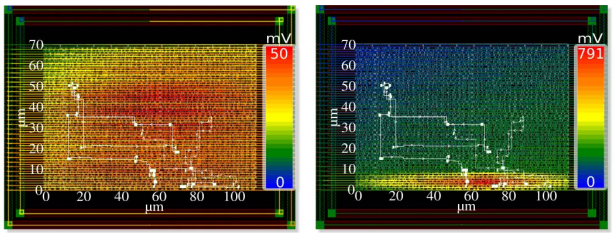
that gives the amplification by the IR drop of the laser induced perturbation at the gate output.

VI. Simulation Results

A. Voltage Drop Propagation

To illustrate how the IR drop propagates in the circuit, refer to Fig. 6. In Fig. 6(a), for which no laser effect is

considered, the IR drop across the rails reach the maximum of 50 mV. In this figure, the voltage drop is uniquely due to normal switching activity. Now refer to Fig. 6(b) in which the laser shot is considered. The effect area of the 5 μm laser spot has a shape that is stretched horizontally along the power supply rails: they provide propagation paths to the laser-induced IR drop and ground bounce. The diameter of the laser spot appears vertically. Fig. 6(b) reports the IR drop at its apex: an amplitude of 791 mV is observed. At this time, the voltage swing is reduced to only 209 mV, far below the nominal voltage of 1 V.



(a) (b)

Fig. 6: ARM 7 Layout with 5k+ instances (critical-path with 38 instances in evidence): (a) Maximum voltage drop (IR-Drop + Bounce) in normal operation condition. (b) Maximum voltage drop in presence of a laser shot characterized with laser spot diameter equal to 5μm.

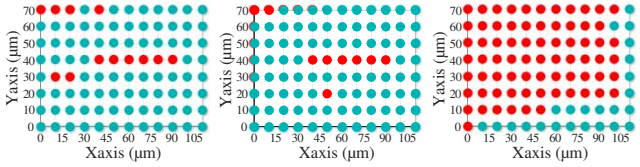
B. Fault Injection Maps

For the purpose of having an overview of this phenomenon at chip level, we drew maps of the injected faults on simulation basis for three different cases: 1^{st} by considering only the laser-induced transient currents between the drains and the substrates of the sensitive transistors, 2^{nd} by considering only the laser-induced IR-drop, and 3^{rd} by considering both phenomenons. These simulations were ran for locations of the laser spot sweeping the whole circuit area (110μm x 70μm) with a X and Y displacement step of 10 μm. For each location, the various scenarios of Fig. 4 were used. Fig. 7 reports the obtained fault maps, where red dots correspond to the occurrence of a fault and green dots the absence of faults (each dot location is that of a simulated laser shot). Note that we considered only bit-flip faults, i.e., if the output of a flip-flop changed its state from 1 to 0 or vice-versa for at least 1 clock cycle.

Fig. 7(a) represents the simulations performed considering only the classical model of laser illumination (i.e. laser-induced IR-drop is ignored). Since the transient current profile has a width of 250 ps, when this current is applied closer to the flip-flop sampling window, more faults are observed.

In Fig. 7(b), only the IR-drop effects are taken into account. One may observe that laser induced IR-drop can cause by itself faults in the circuit due to many factors such as timing failure or even data disruption.

Fig. 7(c), reports the fault map for which both the classical model of laser fault injection and the laser-induced IR-drop are considered. By comparison to Fig. 7(a), it reveals that the fault areas are larger than expected at any time of laser injection. It also unveiled an extension of the laser sensitivity in time. This demonstrates that IR drops induced by laser shots play an important role in the occurrence of faults.



(a) (b) (c)

Fig. 7: Maps of laser-induced faults for laser shot at 1.7 ns: (a) Only classical model. (b) Only IR drops. (c) Complete model (classical model + laser-induced IR drops).

VII. Conclusion

This paper highlighted how laser-induced IR drop effects significantly contribute to fault injection. A model that takes into account the voltage drop effects in the power and ground rails has been presented. The model was used in a methodology which allows the simulation of laser-induced IR drop at circuit scale. This methodology was applied to a test-chip to demonstrate how the IR drop contribution resulted in a massive increase in the number of faults. Both the areas sensitive to laser-fault injection and the time span of laser sensitivity are increased. These results reveal, for the first time, that laser-induced IR drop has to be considered in order not to underestimate fault sensitivity to a laser shot since IR drop is a strong contributor to the fault injection process.

A test chip designed with the same technology is to be tested under laser illumination to corroborate our simulation based results with experiments.

References

[1] G. C. Messenger, "Collection of charge on junction nodes from ion tracks," *IEEE Transactions on Nuclear Science*, Dec 1982.

[2] J.-M. Dutertre *et al.*, "Laser attacks on integrated circuits: From cmos to fd-soi," in *DTIS, 9th IEEE International Conference On*, May 2014.

[3] J. Ma *et al.*, "Identification of ir-drop hot-spots in defective power distribution network using tdf atpg," in *2010 5th International Design and Test Workshop*, Dec 2010, pp. 122–127.

[4] S. Zhao and K. Roy, "Estimation of switching noise on power supply lines in deep sub-micron cmos circuits," in *VLSI Design, 2000. Thirteenth International Conference on*, 2000, pp. 168–173.

[5] L. Hériveaux *et al.*, "Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design," in *39th ISTFA*, Nov 2013.

[6] 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, Oct 1965.

[7] A. Sarafianos *et al.*, "Building the electrical model of the pulsed photoelectric laser stimulation of an nmos transistor in 90nm technology," in *IRPS, 2013 IEEE International*, April 2013, pp. 5B.5.1–5B.5.9.

[8] S. Buchner *et al.*, "Pulsed-laser testing for single-event effects investigations," *Nuclear Science, IEEE Transactions on*, vol. 60, no. 3, pp. 1852–1875, June 2013.

[9] F. Darracq *et al.*, "Backside seu laser testing for commercial off-the-shelf srams," *IEEE Transactions on Nuclear Science*, vol. 49, no. 6, pp. 2977–2983, Dec 2002.

[10] C. Roscian *et al.*, "Fault model analysis of laser-induced faults in sram memory cells," in *FDTC, 2013 Workshop on*, Aug 2013, pp. 89–98.