Laser Fault Injection Vulnerability Assessment and Mitigation with Case Study on PG-TVD Logic Cells

Ryan Holzhausen, Tasnuva Farheen, Morgan Thomas, Nima Maghari, Domenic Forte
Department of Electrical and Computer Engineering, University of Florida, Gainesville, Florida
Email: {ryan.holzhausen, tasnuvafarheen, morganana13}@ufl.edu, {maghari, dforte}@ece.ufl.edu

***Abstract*—Physical attacks on secure devices can leak sensitive data and have significant consequences for individuals, companies, and governments. Today, much research is centered around understanding hardware weaknesses and vulnerabilities and, in turn, designing countermeasures to increase system security. One such countermeasure is the implementation of the camouflaging gate called PG-TVD (pass gate-based threshold voltage defined), which ensures protection against reverse engineering and side-channel attacks. However, proper investigation is needed to determine if the countermeasure opens the door to other powerful attacks, such as laser fault injection (LFI) attacks. Identifying the vulnerability against this attack requires a proper assessment. As the first attempt to understand laser sensitivity in PG-TVD, we develop a workflow for assessing a circuit layout's sensitivity to LFI. We use this workflow to analyze the PG-TVD, giving the laser-sensitive areas. A deeper understanding of how to protect devices can be gained from this assessment to keep sensitive data secure. From the information obtained by our workflow, we also propose, design, and simulate a mitigation scheme that mitigates the laser sensitivity in PG-TVD logic cells by approximately 83%.**

***Index Terms*—Laser Fault Injection, Vulnerability Assessment work Flow, PG-TVD, Mitigation scheme, Hardware Security.**

I. Introduction

The growing prevalence of hardware attacks, such as reverse engineering, side-channel, and fault injection attacks, has made integrated circuits(IC) and intellectual property (IP) more vulnerable [1], [2], [3]. Reverse engineering can reveal the design and functionality of the circuit. It can open the door to third parties replicating the IP or finding exploits to extract sensitive data. Various non-invasive and invasive methods can be used by third parties to obtain information about materials, performance, and functionality, including delayering, system-level analysis, product analysis, and circuit extraction [4], [5]. Conversely, side-channel attacks extract design information while the device operates by observing its reaction to user-defined stimuli [6], [7], [8]. Several well-known attacks in this category, including differential power analysis (DPA) [9], extract design characteristics using current consumption measured across different combinations of input signals. Another powerful tool in the arsenal of physical attacks is fault injection, which can successfully compromise an embedded cryptographic implementation even with a single fault. Many fault injection attack variants exist in practice, e.g., laser exposure, voltage or clock glitches, and electromagnetic perturbation. Among these approaches, laser fault injection (LFI) is known as one of the most powerful physical attacks. An LFI attacker injects a temporal fault during a cryptographic operation using a laser module [10], [11]. LFI has the highest time and space resolution for the most efficient attack capability compared to the aforementioned variants. As a result, laser fault injection, initially conceived to mimic radiation effects in space applications, has become a tremendous security threat.

Several countermeasures have emerged to reduce the efficacy of physical attacks. Among those, the camouflaging gate called PG-TVD (pass gate-based threshold voltage defined) is promising as it ensures protection against reverse engineering and side-channel attacks. The PG-TVD logic family is designed in such a way that the logical functionality of the gate cannot be determined through visual inspection, making the design less susceptible to reverse engineering [12]. This is possible because each different logic gate appears identical using optical, electron-based, and ion-based imaging systems. In addition, the logic gates are designed such that they have greater protection against potential side-channel attacks because the HVT and LVT transistors on each side of the circuit are equally matched across different input combinations and Boolean functions [12]. Because of this, current consumption and propagation delays are comparable for the different input and Boolean combinations and side-channel leakage are lower.

However, proper investigation is needed to determine if the countermeasure opens the door to other powerful attacks, such as LFI. Studying them from an LFI perspective to see if there is a security tradeoff is interesting. Identifying the vulnerability against this attack requires a proper assessment. In this paper, a workflow is developed for assessing a circuit layout's sensitivity to LFI to assess laser sensitivity in PG-TVD. This workflow is used to analyze the PG-TVD, showing laser-sensitive areas. From the information obtained by our workflow, we propose, design, and simulate a mitigation scheme that mitigates the laser sensitivity in PG-TVD logic cells. To our knowledge, the security of such gates has never been investigated with respect to fault injection.

Contributions. Our main contributions in this paper are summarized as follows:

- We develop and implement a workflow to analyze the vulnerability of a gate's layout to LFI-based on attack parameters such as laser power, wafer thickness, spot size, spatial distribution, and laser pulse duration. The output of the workflow is a map of the layout that designates which areas of the layout result in LFI faults.

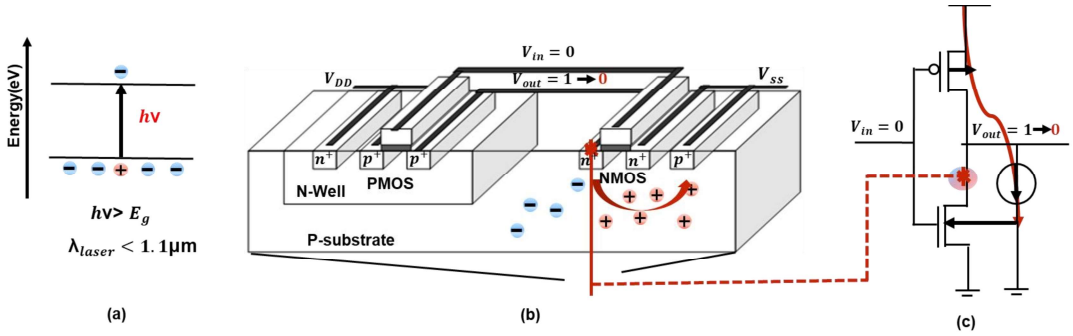

Fig. 1: (a) Physics of photoelectric laser stimulation (b) Laser fault injection mechanism (c) Occurrence of single event error.

- To showcase the strength of our workflow, we use it to perform a case study on three PG-TVD gates (NAND, NOR, and XOR) under varying parameters in 65nm technology node. We find areas in the cells' sense amplifier and core that are sensitive to bit flip, reset, and set faults. The PMOS transistors are identified as the weakest part of the design.
- Based on the LFI results for the baseline PG-TVD design and layout, we propose a modified NMOS-only PG-TVD gate. Further, the gate's layout is modified to decrease LFI sensitivity.
- Upon acceptance of this paper, the scripts and codes corresponding to our LFI mapping workflow will be made publicly available for researchers and practitioners.

The rest of the paper is organized as follows. In Section II, we introduce the background of the fault injection mechanism, laser-induced faults, and the fundamentals of PG-TVD logic cells. In Section III, we describe the LFI model and associated vulnerability assessment workflow. The assessment results for the original PG-TVD gates are shown in Section IV. Our proposed mitigation scheme modified PG-TVD gates is described in Section V along with the LFI vulnerability reduction evidence. Finally, the conclusion and future work are provided in Section VI.

II. Background and Related Work

Laser fault injection can be carried out in one of two ways: a front-side attack or a back-side attack. In a front-side attack, a laser is directed at the front-side of the wafer and has to pass through the various metal layers before reaching the PN junctions. The metal layers offer a level of protection as it reflects most of the light from the laser. The wavelength of the laser needs to be carefully selected based on the number of metal layers and whether or not the die has any shielding. The wavelength typically chosen for a front-side attack range from about 500nm to 800nm [13].

In a back-side attack, the ion beam is directed at the bulk of the silicon, which offers far less protection than metal layers. The bulk of the die is polished down from 300μm to 30μm so that the light has as little bulk to diffuse through as possible [14]. With the use of an X-ray, the transistors can be observed through the bulk of the die, and a laser with an extremely precise step size can be focused on this location to induce a current in the transistor. The laser wavelength generally chosen for a back-side attack is 1065nm [13]. With flip-chip packaging becoming an industry standard, in which the chip is mounted with its back-side facing up, as well as the ever-growing number of metal layers protecting the front side of the chip, back-side attacks have become the more effective method for inducing faults.

A. Fault Injection Mechanism

Due to their interaction with silicon, lasers can cause faults in ICs by causing a photoelectric effect. When a laser beam with a wavelength corresponding to an energy level higher than the silicon bandgap [15], [16] passes through silicon, as shown in Fig. 1 (a), it creates electron-hole pairs along its path called the *photoelectric effect*. There may be no noticeable effect on this recombination of charge carriers. An exception occurs when the laser beam passes through a transistor's reverse-biased PN junction (drain/bulk or source/bulk) – as shown in Fig. 1 (b) – a place where there exists a strong electric field. Consequently, a current pulse is induced because the charge carriers drift in opposite directions. Upon exhaustion of the charges, this pulse vanishes but may last hundreds of picoseconds after the laser pulse ceases [16]. A transient voltage spike caused by this current pulse induces faults in secure circuits to retrieve confidential data stored in these devices [17], [3].

B. Laser Induced Faults

Fig. 1 (c) illustrates how a transient photocurrent is turned into a single-event error (SEE) [18] for an inverter with input at the low logical level. In this configuration, the sensitive SEE area is the drain of the NMOS transistor (shaded in pink), which is in an OFF state. A current source depicted in Fig. 1 (c) shows how laser-induced photocurrent may be injected into the NMOS through a reverse-biased PN junction connected to the N-type drain of the NMOS (biased at VDD) and the P-type substrate (grounded).). Consequently, the inverter's output voltage may drop from logic '1' to '0', provided that the injected photocurrent exceeds the PMOS transistor's saturation current. Thus, SET (single event transient) voltages may propagate through gates in the fanout of the inverter, leading to a fault. A similar phenomenon may also occur when

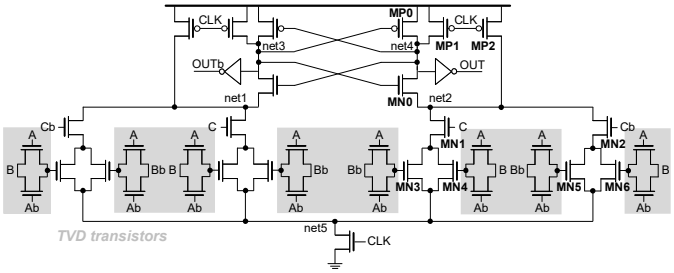

Fig. 2: Schematic Design of PG-TVD Logic cell with two main blocks: the core (lower half) and the sense amplifier (upper half) [12].

the inverter input is at logic high. The laser-sensitive area in this instance is the OFF PMOS drain. Then the photocurrent flows from VDD through the N-well's biasing contact (or tap) (i.e., the PMOS bulk) to the ground. Further, suppose a flip-flop is directly induced with a SET. In that case, the stored data may be flipped, characterizing the so-called SEU (single event upset) [19], i.e., a bit set will cause a stored value of '0' to change to '1' or a bit reset from '1' to '0'.

C. Fundamentals of PG-TVD Logic Cells

Pass Gate-Based Threshold Voltage Defined (PG-TVD) logic cells can be broken down into two main blocks: the *core* and the *sense amplifier*. In the core, shown in the lower half of Fig. 2 provided by Thomas et al. [12], the TVD transistors utilize different threshold voltages to create different logical functions. These different transistors alter the gate voltage of the non-TVD transistors in the core that are connected to the current path. This gate voltage will then set the current going through each respective branch which will set the output of the sense amplifier.

As illustrated in Fig. 2, the output of the core is fed into the sense amplifier, located in the top half of the figure, which compares the current through each branch, and changes the value stored in the cross-coupled inverters. This stored value is updated at every positive clock edge. This process begins with the clock signal at a LOW value. This means that PMOS transistors (MP1 and MP2) and their counterparts in the other branch are 'ON'. These transistors respectively set net4 and net2, as well as the corresponding nets in the other branch, to a HIGH value. When the clock signal goes HIGH, these transistors are turned 'OFF' and these nets are disconnected from VDD. The sense amplifier now responds to the currents being generated in the core. These currents should be slightly different, meaning that the drains of the two NMOSs that make up the cross-coupled inverters are biased differently. In the case where the voltage is higher at net2 than the same point in the other branch, the value at net4 is driven to a HIGH value. This value is connected to the input of the other inverter, so the voltage in the opposite branch is driven LOW. This value is stored until the clock signal is driven LOW again, and net2, net4, and the corresponding nets in the other branch, are reset to a value of '1'. Because the circuit is mirrored, the sense amplifier has two outputs, which, during typical use, are opposite logic values when the clock signal is HIGH.

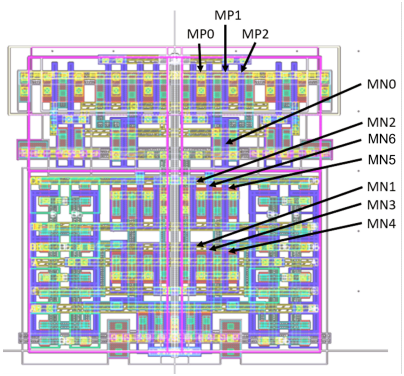

Fig. 3: Layout of PG-TVD Logic cell providing labels for notable transistors [12].

Fig. 3 illustrates the layout of a 3-input PG-TVD cell and provides labels for notable transistors. Our proposed workflow will be used to analyze the LFI sensitivity of this layout.

III. Proposed Workflow for LFI Vulnerability Assessment

An attack model's effectiveness depends on how closely its effects correspond to the real world and how well it is designed. The adversary model might not reflect an adversary's practical realities and capabilities, resulting in inappropriate countermeasures. Physical implementations are still vulnerable to LFI attacks if they fail to provide the desired level of security. It is more reliable to assess the vulnerability of an attack if the effects are close to actual scenarios. In this regard, we propose an LFI vulnerability assessment workflow that incorporates all laser-affecting parameters such as laser power, silicon wafer thickness, pulse duration, and positions of the critical gates in the layout. These parameters are considered in order to set up realistic simulations that would expose all potential vulnerabilities in the circuit.

A. Model Overview

Many parameters had to be considered in order to set up realistic simulations that would expose all potential vulnerabilities in the circuit. For this, a variety of prior studies were analyzed to determine the best model for exposing these vulnerabilities. Most of these studies came to slightly different conclusion as to the best way to model the effect of a laser on a silicon device, but they were based on the same underlying methodology of placing a current source at each PN-junction of the circuit that triggers a pulse of current at the moment of the laser strike. This injected current should accurately model the transient current induced by the photoelectric effect along the path of the laser. This current pulse has a peak current that is dependent on a number of variables that account for laser parameters, laser location, wafer thickness, and circuit topology.

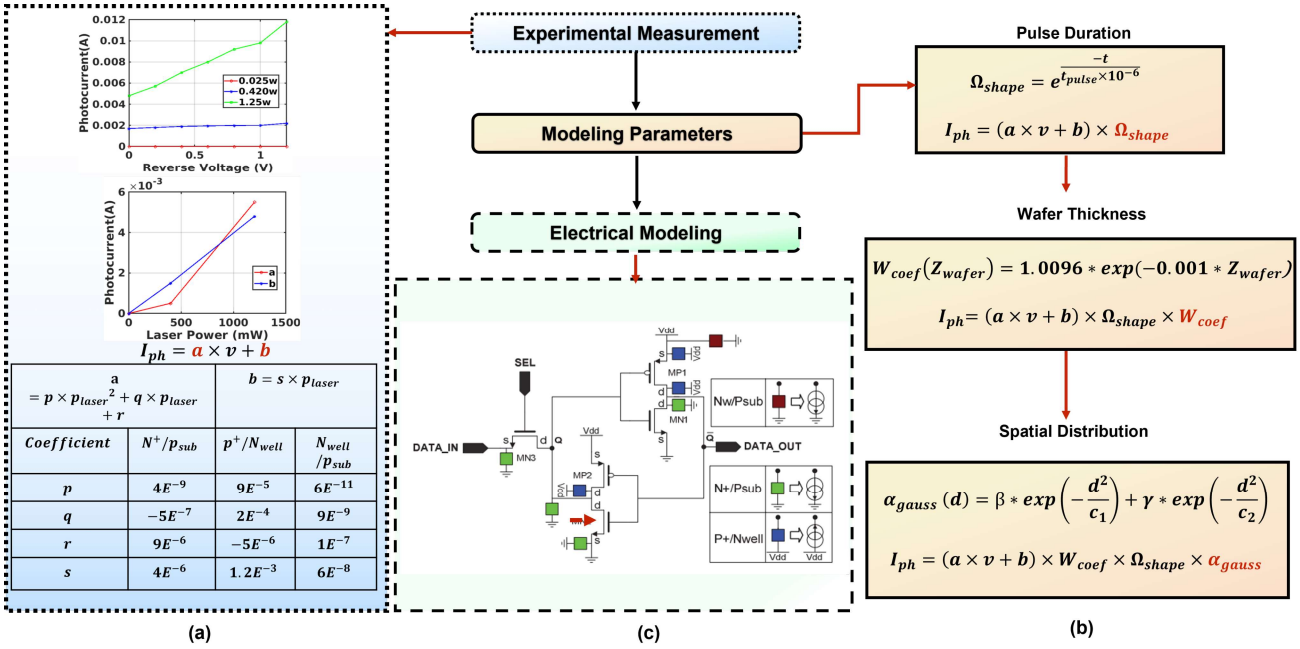

Fig. 4: Modeling of photoelectric laser stimulation (a) Experimental measurement data from literature [20]; (b) Modeling parameters [21]; and (c) An example of electrical modeling of laser attack on SRAM cell.

B. Influential Parameters in LFI Modeling

To delineate the scope of our model, we incorporate experimental measurement data from literature [20], [22], [23] and influential parameters in LFI [21] as shown in Fig. 4. The testbench is set up with the circuit in question having a current source at each PN junction that has these parameters accounted for. At the time of the attack, each PN junction is injected with a current pulse. The equation for determining the transient current as a function of time is

$$I(t) = (a * V + b) * \alpha_{gauss} * W_{coef} * \Omega_{shape}(t).$$

In the above equation, V is the reverse voltage of the junction, expressed in volts.

Laser Power Effect: P_{laser} is the power of the laser expressed in Watts. a and b are coefficients that are related to the parameters of the laser and are determined by the following equations.

$$a = p * P_{laser}^2 + q * P_{laser} + r$$

$$b = s * P_{laser}$$

Investigation of the N+/P substrate (PN) junction under PLS (Photocurrent Laser Stimulation) is a necessary step in the comprehensive study of the phenomena involved when a pulsed laser stimulates the backside of a transistor. In order to model the effect of PLS on a PN junction, the laser spot should be centered in the middle of the junction. For a given laser power, the more the PN junction is reverse biased, the more the electrical field between the two electrodes increases, which induces a higher photoelectric current.

Spatial Distribution Effect: The distance between the laser spot and the PN junction has a significant impact on the peak current as well. The term α_{gauss} is used to model the spatial dependency of the laser and is expressed by

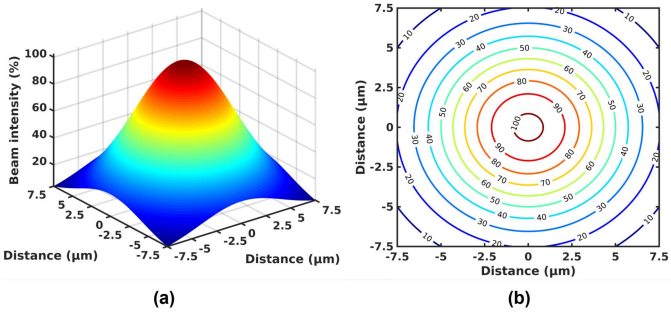

Fig. 5: (a) Laser distribution effect across the distance; (b) Contour lines where 100% of laser beam intensity represents the epicenter of the laser spot.

$$\alpha_{gauss}(d) = \beta * exp\left(-\frac{d^2}{c_1}\right) + \gamma * exp\left(-\frac{d^2}{c_2}\right).$$

This expression equates to a value between 0 and 1 and is derived from a Gaussian equation that is a function of the distance between the junction and the center of the laser beam. β, γ, c_1, and c_2 are determined by the laser equipment being used. These values can vary based on different laser lenses and focus settings, so values that are widely used in prior studies were selected for this experiment. This Gaussian curve to account for the beam's effect as a function of distance becomes increasingly narrower at shorter pulse durations [19]. For the following simulations, a 1μm laser spot size, illustrated

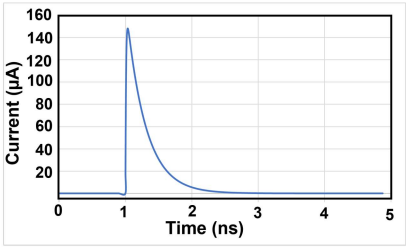

Fig. 6: Laser Pulse Duration Effect with the amount of induced current.

in Fig. 5, is chosen to better observe the effects of a localized, picosecond range pulse width attack. The parameters were chosen such that the peak of the bell curve has a value of 1 and the induced current through a drain with a laser spot 0.5μm away results in half of the current as a laser spot directly on the drain, as shown in Fig. 5.

Wafer Thickness Effect: The thickness of the wafer also has an impact on the photocurrent induced. This is because the light from the laser gets diffused as it travels further through the substrate, lessening the beam's intensity by the time it reaches the PN junction. It was determined experimentally by Sarafianos et al. that the effect of the wafer's thickness z_{wafer} can be modeled by

$$W_{coef}(z_{wafer}) = 1.0096 * exp(-0.001 * z_{wafer}),$$

which decreases exponentially with thicker wafers [22][23].

Pulse Duration Effect: $\Omega_{shape}(t)$ is a double exponent that models the rapid collection of charge and the slower diffusion of electron-hole pairs that would be induced by a laser pulse. A laser with a pulse width in the picosecond range has a smaller, more focused beam, allowing for more localized attacks on a device. Because of this, there are more areas in which an error can potentially be induced, as a smaller beam diameter results in smaller counter-balancing currents from nearby transistors [19]. With feature sizes smaller than 120nm, such as those being tested throughout this paper, it becomes increasingly more difficult to perform a laser attack on a single transistor without a significant disturbance in neighboring transistors. A laser with a pulse in the picosecond range was chosen for this experiment for this reason, as more localized attacks provide the attacker with the greatest amount of information. A graph of the current magnitude as a function of time is provided in Fig. 6. The peak current occurs during the 10ps in which the laser is on. When the laser pulse has turned off, the charges slowly diffuse, and the current tapers off and reaches a value close to 0 in around 1ns.

Finally, a current source with all of these parameters accounted for is placed at each of the PN junctions, and a current pulse is triggered to simulate a laser strike.

C. Effect of LFI on Lower Technology Nodes

D. Applicability of Workflow on Lower Technology Nodes

It is essential to discuss the effect of LFI on lower technology nodes, e.g., FinFETs and Gate-all-around (GAA) devices. They are generally considered less susceptible to LFI than planar FETs. Because of their unique structure, they provide inherent resistance.

The three-dimensional nature of FinFETs means that the active channel region is raised above the substrate and is surrounded by vertical fins on three sides. This configuration makes it more difficult for a laser to directly target the active region than planar FETs where the channel is closer to the substrate. It also adds physical robustness to the transistor, making it harder for laser-induced energy to effectively alter the device's behavior. The fins provide additional layers of material that can dissipate heat and energy, reducing the impact of laser-induced faults. It also results in a more distributed current flow, making them less sensitive to localized energy injection from a laser. In contrast, planar FETs have a more compact structure that can make them more vulnerable to such attacks.

Gate-all-around (GAA) devices, including nanosheet FETs, are even less susceptible to laser fault injection than planar and FinFETs, offering even more resistance to LFI. The channel is surrounded by gate material on all sides, providing unprecedented isolation from external influences like laser-induced energy. This makes it highly challenging for a laser to directly impact the active channel region. Like FinFETs, it exhibits a distributed current flow, reduced area, and improved physical robustness.

It is important to note that while these devices offer increased resistance to laser-induced faults, they are not entirely immune to the attack. So, for security considerations, a comprehensive approach is needed to find the laser-sensitive places in this case as well. That will help later to analyze the feasibility of countermeasures, including hardware layout techniques, cryptographic protections, and other security measures. In this regard, we propose a laser fault injection vulnerability assessment workflow. To clearly explain the flow, we limited our analysis to planar FET only; however, a similar flow should also apply to lower technology nodes.

E. Workflow for LFI Data Collection and Visualization

It is necessary to set up the test bench in a way that the huge amount of data point generation, e.g., 700 points due to simulation, can be easily and repeatably analyzed and summarized. The corresponding workflow for vulnerability assessment of laser fault injection is illustrated in Fig. 7.

1) Testbench: To generate a fault map, a simulation was run in which the x- and y-coordinates of the laser were swept to provide total coverage of the logic cell. The simulated laser was set up to sweep all x-values from -3.5μm to 3.5μm and all y-values from -0.5μm to 5.5μm in 0.25μm steps. The current sources and laser parameters are set up as described in Section III. The laser was triggered at $t = 10$ns, at the moment the clock edge is rising. This was done to reveal as many potential faults as possible, as attacks on certain transistors will only result in a fault if targeted at the positive edge of the clock. At $t = 13\mu$s, the value of the logic cell's output is compared against the expected value for the given input combination.

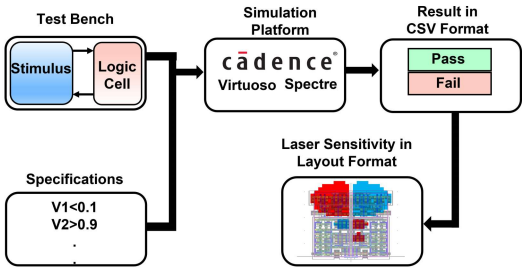

Fig. 7: Workflow for generating LFI fault maps.

Evaluating the voltage at this time will only reveal faults that resulted in the stored value being changed. This simulation is separately run for each of the three logic gates being tested: a NAND gate, NOR gate, and XNOR gate.

2) Specifications: Specifications can be set within Cadence to compare the simulation results against an expected value easily. The voltage at the output of each logic gate is extracted 2ns after the injected current. This voltage is compared against the expected voltage for the given input combination with a 10% margin of error. If the extracted voltage falls outside the spec limits, a "fail" is returned, and that logic block is determined to have faulted at that laser location.

3) Result in CSV Format: After the simulation, a CSV file is generated that summarizes the extracted values and the results of the spec comparisons. The results are displayed in a tabular format, with one row for each spec measured. Each row contains the measured value, the defined spec, and whether the extracted value passed or failed.

4) Laser Sensitivity Fault Mapping: The data from the CSV file is then copied and pasted into an Excel sheet designed to parse the data and generate a fault map. A fault map summarizes the types of faults induced in a cell and where they occurred. Each input combination's pass/fail results are passed into an Excel equation that determines if a bit-set, bit-reset, bit-flip, or no fault occurred. Next, a grid is set up with each cell having a VLOOKUP equation to find the type of error for that xy-coordinate. With the type of error displayed in the grid, conditional formatting can be applied to change the cell color based on the type of fault that occurred at that point. Finally, a screenshot of the relevant area of the cell can be superimposed over this grid to illustrate the vulnerable points of the cell clearly.

IV. Simulation Results and Discussion on Vulnerability Assessment of PG-TVD Logic Cells

The simulations presented are run using Cadence Virtuoso with the ADEXL simulation tool. The PG-TVD schematics analyzed for this study use a commercial 65nm library.

A. Transient Response

The first simulation is intended to provide a deeper understanding of how a fault is induced in the PG-TVD logic cell by analyzing the transient response of the cell to an induced photocurrent.

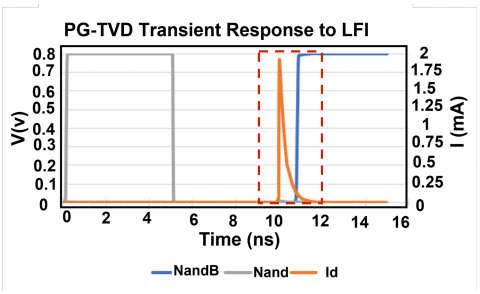

Fig. 8: Waveform of simulated fault in the logic cell, inducing laser-induced current at 10 ns showing the created fault in red dashed line box.

1) Simulation Setup: In order to analyze the laser fault injection vulnerabilities of the circuit, a current source was connected to each reverse biased PN junction in a NAND gate with input '000', as described in Section III. A simulation was run with the laser location being set to target transistor MP0. We would expect an attack on this transistor to force the value at net4 to go HIGH, and therefore force the output of the logic cell LOW.

2) Simulation Results: Fig. 8 shows the waveforms of the logic cell's positive and negative outputs, as well as the induced current through the bulk of the transistor.

For the first 10ns, the circuit demonstrates normal behavior as the positive output is HIGH and the negative output is LOW before they are reset at $t = 5$ns. It can be seen in the figure that the current source is triggered at $t = 10$ns. There is a negligible voltage change in the positive output of the logic block at the time of the induced current, but the voltage fails to transition to a HIGH value, resulting in a forced LOW fault. Shortly after this, the inverse output of the logic block faults to a HIGH value, as the value stored in the cross-coupled transistors has been forced to a logic '0' creating a fault.

B. Fault Map

Once it is determined that a fault can be induced in the logic cell, the testbench is expanded to find all possible fault locations on the cell. To do this, a fault map is generated, which summarizes the effect of a laser attack at each location in the cell. The areas marked with blue are locations where a laser simulation resulted in the output of the cell being forced LOW. The red areas are where the output was forced HIGH. The purple areas are where the output of the cell was flipped, regardless of the original output.

Table I(left) summarizes the number of simulations for each type of logic gate that resulted in each type of error. This data will be used for reference in Section IV-C in which the effect of varying the simulation parameters is analyzed. Because the XNOR logic gate reveals the most laser-sensitive regions, it is used for the remaining simulations.

The workflow described in Section III-E is implemented to generate the fault maps shown in Fig. 9. Because there is only one input combination for a NAND gate that results in a LOW output, it can be seen that only one of the NMOS groupings is

TABLE I: Number of locations where various faults can be induced at various conditions.

Fault Type	Number of Locations Where Various Faults can be Induced								
	Various PG-TVD Logic Gates			PG-TVD XNOR Gates with Varying Laser Spot Size			PG-TVD NAND Gates with Varying Induced Current		
	NAND	NOR	XNOR	$5\mu m$	$1\mu m$	$0.5\mu m$	$0.5x$	$1x$	$10x$
Bit-set	96	106	106	262	106	50	78	106	162
Bit-reset	105	99	106	262	106	50	78	106	162
Bit-flip	0	0	0	0	0	0	0	0	0
None	533	549	542	230	542	654	598	542	420

able to force a HIGH value. Similarly, for the NOR gate, there is only one input combination that results in a HIGH output, so only one of the NMOS groupings is able to force a LOW value. With a few exceptions, the sensitive areas found through simulation match very well with the expected vulnerable areas. As expected, an attack on the PMOS transistors on the right half of the sense amplifier force the output to a logic '0', and an attack on the PMOS transistors on the left half of the sense amplifier forces the output to a logic '1'. In addition, attacks on transistors MN1-MN6 result in the output of the logic cell being forced HIGH, as was predicted, and attacks on these transistors on the other branch result in the output being forced LOW.

It also appears that the inverters at the output of the cell are not contributing to any additional fault locations. This is because an attack on these transistors doesn't propagate to the memory of the cell and alter the stored value. Attacking the output inverter simply results in a temporary fault in the output that doesn't last much longer than the laser pulse duration.

There were a number of areas in which the discovered sensitivity did not match what would be expected for an attack on that transistor. First, an attack on transistor MN0 was expected to drive net4 LOW and force the output of the cell to be HIGH. The reason that the cell is not forced HIGH with a laser attack on this transistor is that the current induced in the PMOS of this inverter, transistor MP0, is so large that it overpowers the effects of the NMOS current. Despite this explainable difference, the fault map looks as expected.

C. Varying Simulation Parameters

With a clear understanding of how this particular laser attack affects this logic cell, we wish to observe the effect of changing the parameters described in Section III-B on the fault-sensitive regions. The selected parameters were based on information provided in prior works, but these numbers can vary greatly based on the equipment being used and the laser parameters. In this section, an analysis is provided as to how changing these simulation variables affects the obtained results.

1) Laser Spot Size: The laser spot size is dependent on a number of laser and lens parameters as well as the amount of diffusion through silicon before the light is incident on the PN junctions. In previous simulations, a laser spot of 1μm was selected to provide the most localized attacks possible with modern equipment, but this may not expose all possible vulnerabilities. Lasers with a spot size of 5μm are widely available and were previously used for laser attacks in larger technology nodes. The fault injection simulation was rerun with the spot size parameter changed to 5μm in order to see how the resulting fault map changes with a larger laser spot size. The left image in Fig. 10 summarizes the induced faults.

Table I(middle) summarizes the number of simulations for the various laser spot sizes that resulted in each type of error. The larger number of faults induced by using the larger laser size suggests that the larger laser can induce faults from attacks that are further away from the cell.

Again, the areas marked with blue are locations where a laser simulation resulted in the output of the cell being forced LOW. The red areas are where the output was forced HIGH. The purple areas are where the output of the cell was flipped, regardless of the original output. When compared against Fig. 9, which contains the results from the same simulation with a 1μm spot size, it can be seen that the increased spot size resulted in significantly reduced localization of the attack. The vertical line down the middle of the cell, where faults were not induced, widens with the larger spot size. This is because in this area, all transistors in the sense amplifier have a large current induced, and the effects are canceled out.

Although a laser spot size of less than 1μm is uncommon for laser fault injections, future technological advances may make this attack possible. A simulation was run in which the spot size was set to 0.5μm in order to see how the simulated fault map changes with a smaller laser spot size. The same simulation was rerun, and the right image in Fig. 10 summarizes the fault locations. When compared against Fig. 10 from the previous simulation and Fig. 11 with the 5μm and 1μm spot sizes, respectively, it is clear that using a smaller spot size results in more localized attacks, but fewer areas in which a fault can be induced. This means very precise positioning equipment would have to be used for attacking with the smaller spot size. With the more localized attack, the currents induced in the NMOSs of the sense amplifier are no longer overpowered by the PMOS currents, and the missing NMOS faults become visible in the fault map.

2) Induced Current: Next, the effect of the peak transient current on the simulated fault map was observed by analyzing the fault map at different current amplitudes. The use of FDSOI can reportedly reduce the peak transient current of a laser attack by a factor of 2 [24]. The testbench was adjusted such that the peak current of each of the current sources at the PN junctions was reduced by a factor of 2 to provide a rough estimation of how the simulated fault areas would

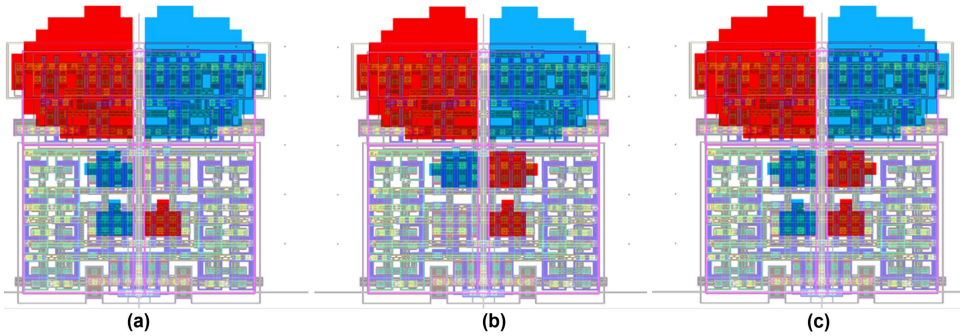

Fig. 9: Map of simulated faults in PG-TVD (a) NAND (b) NOR (c) XNOR logic gates.

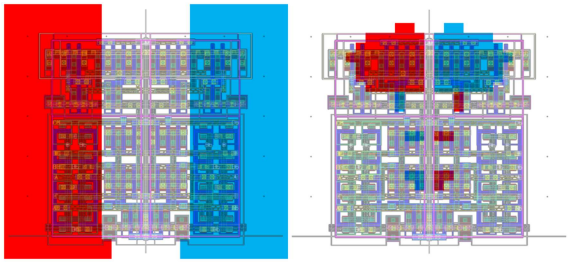

Fig. 10: Map of simulated faults (left) with $5\mu m$ laser spot size and (right) with $0.5\mu m$ laser spot size.

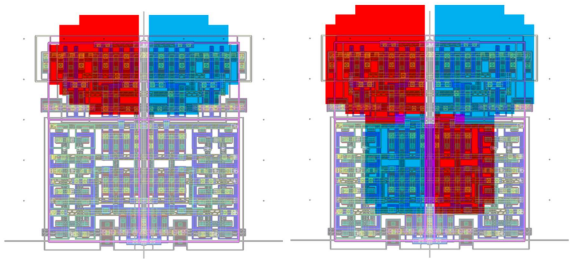

Fig. 11: Map of simulated faults (left) with induced current decreased by a factor of 2 and (right) with induced current increased by a factor of 10.

change with the use of FDSOI. The simulation was rerun with the decreased currents, and the resulting fault map is displayed in the left image in Fig. 11.

Table I(right) summarizes the number of simulations for various induced currents that resulted in each type of error. The data shows a larger number of vulnerable locations when stronger currents are induced by the laser.

From the figure, it is clear that decreasing the peak current reduced the area of the PMOS-sensitive regions and eliminated the NMOS-sensitive regions altogether. These results suggest that FDSOI could provide protection against laser fault attacks assuming the thin intrinsic layer is capable of reducing the induced photocurrent significantly.

Using a laser with different parameters may be able to provide greater transient currents than those used for the simulations in Section IV. Larger induced currents could

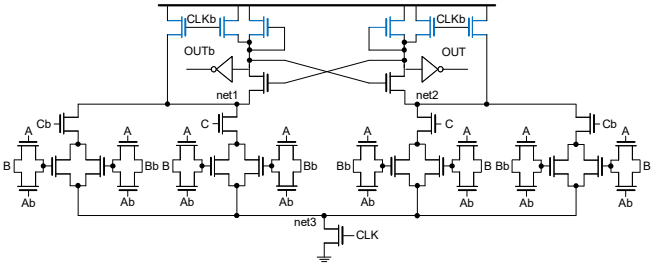

Fig. 12: Mitigation scheme with the PG-TVD cell redesigned with only NMOS devices showing the changes in blue.

potentially result in a larger number of vulnerable transistors. For this reason, the test bench was altered to increase the induced current by a factor of 10. The simulation was rerun, and the results are summarized in the right image in Fig. 11.

From the figure, it is clear that increasing the peak current caused the fault-sensitive regions to increase in area. This is because attacks further away from the PN junction now induce a current strong enough to change the output. In addition, a bit-flip-sensitive region is now present down the center of the logic gate's core. The selection of parameter values described in Section III-B is centered around simulating an attack with the most advanced laser technology available today that would result in the most precise laser attacks possible. By varying these parameters in both directions, we better understand their effect on the circuit and the resulting fault map. Depending on that, we propose a mitigation scheme by changing the layout of the existing PG-TVD logic cells resulting in less sensitivity to laser fault injection. In the next section, we portray the mitigation scheme and the associated results using the proposed vulnerability assessment workflow.

V. Workflow Informed Mitigation Scheme Design and Associated Results

A. Layout Changes

From an analysis of the fault maps, a number of schematic and layout changes that could partially mitigate laser fault injections become apparent. Table II summarizes the number of simulations that resulted in each type of error with the changed layout.

TABLE II: Number of locations where various faults can be induced in NMOS-only PG-TVD logic gates redesigned sense amp and core.

Fault Type	Count		
	NMOS only PG-TVD	Redesigned	
		Sense AMP	Core
Two Output Bit-set	18	20	15
Two Output Bit-reset	18	20	15
Two Output Bit-flip	0	0	0
One Output Bit-set	56	59	48
One Output Bit-reset	56	59	52
One Output Bit-flip	4	0	0
None	602	596	624

1) Sense Amplifier: The fault maps show that the sense amplifier is the most vulnerable section of the logic cell. This is because, using this LFI model, the current induced in a PMOS is about 200 times larger than the induced current in an NMOS. To reduce the sensitivity of the PG-TVD cell to laser-induced faults, the circuit was redesigned using only NMOS transistors. The new schematic is shown in Fig. 12.

The PMOSs in the main branch of the amplifier are replaced with NMOSs with their gates connected to their source. The PMOSs that were used to reset the amplifier, and were driven by the clock signal, were replaced with NMOSs driven by the inverse of the clock signal. With all PMOSs removed from the circuit, the model was updated, and a simulation was run to generate a new fault map. The results of the simulation are shown in Fig. 13.

The new schematic, timing, and power measurements for three logic gates are comparable with the existing design ensuring similar protection against side-channel attacks. Compared to the original PG-TVD schematic, the new schematic has an increase in delay of about 25%. The dynamic and static power is increased by approximately 20%. Despite these significant reductions in performance, it seems to be a good first step for reducing LFI vulnerabilities. Note also that such changes only need to be made sparingly – that is, to the cells where faults would result in critical vulnerabilities rather than all the cells in a design.

The behavior of the new schematic during a laser attack has some interesting differences compared to the original behavior. Many laser attacks resulted in only a single output failing. Given that the two outputs should always be opposite logic values after evaluating the inputs, a simple way of detecting this type of error is to monitor the outputs with an XNOR gate that goes HIGH when the outputs are the same.

Another difference is that some laser attacks resulted in faults that didn't go to strong logic values, but rather, some intermediate voltage. Because subsequent logic blocks would interpret that output somewhat randomly, the resulting output would be randomized, making it more difficult for an attacker to extract relevant information from a laser attack.

When compared against Fig. 9, it is clear that the NMOS transistors significantly reduce the sensitivity of the sense amp to laser fault injections. The total number of laser locations that result in both outputs faulting reduced from 212 to 36, suggesting a significant decrease in LFI sensitivity of the cell.

It can also be noticed that there are a number of parallel transistors placed very close to each other, so a laser attack has the ability to induce much larger currents at these locations. For this reason, a layout change was considered in which the NMOSs MP0, MP1, and MP2 were separated and placed further apart, such that a laser attack on any one would have an insignificant effect on the others. The results of the simulation are shown in Fig. 13(b). With this layout change, the sense amp looks to be much less vulnerable, especially compared to the original CMOS fault map. In addition, the bit-flip sensitive region in the middle of the core is gone. By using an NMOS-only circuit with the sense amp transistors spread further apart, the cell's sensitivity to LFI is greatly reduced.

2) Core: There are a number of transistors in the core of the PG-TVD cell that run in series and are in close proximity in the layout. This allows an attacker to induce greater currents with a laser attack, making the device more vulnerable. Vulnerable transistors in close proximity were separated and placed further apart as with the sense amplifier. A simulation was run with the new setup, and the resulting fault map is shown in Fig. 13(c). With this layout change, the number of attack locations that result in both outputs faulting is reduced even further, down to 30. The spreading apart of transistors results in a sizable increase in the cell's area, with relatively small improvements to the LFI sensitivity. Because of this, the designer would determine what balance of size and protection is best for their given circuit.

VI. Conclusion and Future Work

In this paper, we analyze the effects of laser fault injection at the electrical, transistor, and logic levels. We first establish a clear understanding of how current is induced in a transistor, by means of the photoelectric effect, in the presence of a significant level of radiation. Then, we propose a laser fault injection vulnerability assessment workflow. Using this knowledge, an analysis of the potential laser vulnerabilities that are present in the PG-TVD logic cell is then provided. Through simulation, a map of the cell's vulnerabilities is created in which a number of vulnerable transistors are identified and compared against the expected behavior. It is found that a few transistors in the core of the logic cell are vulnerable, and almost any laser attack on the sense amplifier would result in a fault. The simulation parameters, including laser spot size and peak transient current, are then varied in order to understand their impact on the results and how attacks with different lasers can expose different vulnerabilities. From the analysis, we propose a mitigation scheme that mitigates the laser sensitivity in PG-TVD logic cells by approximately 83%.

All of the results presented in this paper are gathered through simulation, without being tested experimentally. In the future, we want to implement this work in silicon, with proper probing equipment, and an advanced laser setup, in order to

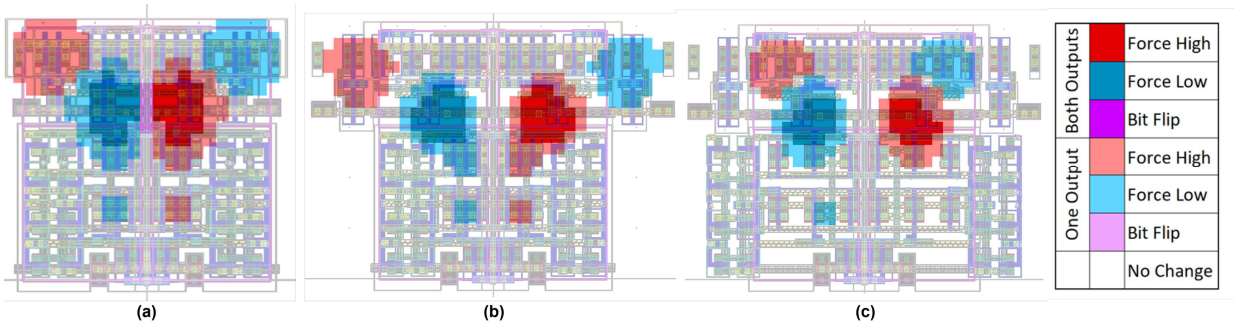

Fig. 13: Map of simulated faults with (a) NMOS-only design; (b) change to sense amp layout; (c) change to the core layout.

validate the laser fault injection model used for this study. With experimental data, adjustments can be made to provide a more accurate model of the induced photocurrent and its effect on the circuit. However, with a model based on information gathered through prior studies, these simulations serve as a valid basis for identifying vulnerabilities and analyzing the feasibility of different countermeasures.

VII. Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. CCF-2221742.

References

[1] S. P. Skorobogatov, "Semi-invasive attacks: a new approach to hardware security analysis," Ph.D. dissertation, Citeseer, 2005.

[2] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, p. 1661.

[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] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai, "A secure camouflaged threshold voltage defined logic family," in *2016 IEEE International symposium on hardware oriented security and trust (HOST)*. IEEE, 2016, pp. 229–235.

[5] T. Farheen, U. Botero, N. Varshney, D. L. Woodard, M. Tehranipoor, D. Forte, and H. Shen, "Proof of reverse engineering barrier: Sem image analysis on covert gates," 2021.

[6] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure integrated circuits and systems*. Springer, 2010.

[7] T. Farheen, S. Roy, S. Tajik, and D. Forte, "A twofold clock and voltage-based detection method for laser logic state imaging attack," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 31, no. 1, pp. 65–78, 2022.

[8] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 1. IEEE, 2004, pp. 246–251.

[9] I. Verbauwhede, K. Tiri, D. Hwang, and P. Schaumont, "Circuits and design techniques for secure ics resistant to side-channel attacks," in *2006 IEEE International Conference on IC Design and Technology*. IEEE, 2006, pp. 1–4.

[10] J. Blömer and J.-P. Seifert, "Fault based cryptanalysis of the advanced encryption standard (aes)," in *International Conference on Financial Cryptography*. Springer, 2003, pp. 162–181.

[11] T. Farheen, S. Tajik, and D. Forte, "Spred: Spatially distributed laser fault injection resilient design."

[12] M. Thomas, B. Park, and N. Maghari, "Pass gate based threshold voltage defined logic family with resilience against hardware attacks," 2023.

[13] N. A. Anagnostopoulos, "Optical fault injection attacks in smart card chips and an evaluation of countermeasures against them," 9 2014.

[14] S. Manich, D. Arumi, R. Rodríguez-Montañés, J. Mujal, and D. Hernandez, "Backside polishing detector: a new protection against backside attacks," in *DCIS - Conference on Design of Circuits and Integrated Systems*, 11 2015.

[15] 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.

[16] S. P. Buchner, F. Miller, V. Pouget, and D. P. McMorrow, "Pulsed-laser testing for single-event effects investigations," *IEEE Transactions on Nuclear Science*, vol. 60, no. 3, pp. 1852–1875, 2013.

[17] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[18] R. Leveugle, P. Maistri, P. Vanhauwaert, F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre, A. Papadimitriou, D. Hély, V. Beroulle, G. Hubert, S. De Castro, J.-M. Dutertre, A. Sarafianos, N. Boher, M. Lisart, J. Damiens, P. Candelier, and C. Tavernier, "Laser-induced fault effects in security-dedicated circuits," in *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, 2014, pp. 1–6.

[19] 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.

[20] 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)*. IEEE, 2013, pp. 5B–5.

[21] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Seu sensitivity and modeling using pico-second pulsed laser stimulation of a d flip-flop in 40 nm cmos technology," in *2015 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFTS)*. IEEE, 2015, pp. 177–182.

[22] 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.

[23] 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.

[24] J.-M. Dutertre, V. Beroulle, P. Candelier, S. De Castro, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hély, R. Leveugle, P. Maistri, G. Di Natale, A. Papadimitriou, and B. Rouzeyre, "Sensitivity to laser fault injection: Cmos fd-soi vs. cmos bulk," *IEEE Transactions on Device and Materials Reliability*, vol. 19, no. 1, pp. 6–15, 2019.