Physically-aware Laser Fault Injection Assessment

Henian Li, Sukanta Dey, Farimah Farahmandi
Department of Electrical and Computer Engineering
University of Florida, Gainesville, Florida, 32611
Email: {henian.li, sukanta.dey}@ufl.edu, farimah@ece.ufl.edu

***Abstract*—Laser-based fault injection (LFI) attacks are powerful physical attacks with high precision and controllability. Several works in literature attempt to model and simulate the laser effect in pre-silicon digital designs, including RTL, SPICE and TCAD models. However, these fault models are neither scalable nor account for actual laser fault simulation. In this paper, for the first time, we propose a physical layout-level LFI assessment framework to verify the layout's resiliency against LFI. The proposed framework can inject Gaussian laser current profiles of any spot size into the physical layout. To make it scalable, we perform SPICE simulations, and employ machine learning to develop cell-level laser fault models which can capture the current characteristics of every standard cell, under different laser-induced transient current intensities. This laser cell library is then utilized during laser fault simulation. Finally, we demonstrate the effectiveness of the proposed framework by analyzing the fully implemented AES design layout.**

***Index Terms*—design verification; fault simulation; laser fault injection; physical layout security**

I. Introduction

Laser Fault Injection (LFI) attack allows an attacker to have precise spatial and temporal controllability over the fault. For studying the impact of LFI in digital circuits, pre-silicon LFI modeling [1]–[3] can be done at different design abstractions: Logical fault simulation relies on injecting fault during RTL/netlist simulation, thus is fast but cannot account for any physical characteristics. For electrical models, the laser's impact is modeled as current sources at the reverse-biased PN junctions. Device-based (TCAD) models use heavy ions to model the laser impact. However, the electrical and TCAD models are not scalable to large designs due to modeling and simulation complexity. Therefore, a scalable pre-silicon LFI assessment framework that combines different modeling abstractions is needed to allow fast LFI assessment.

Our Contributions: To the best of our knowledge, this is the first work in literature, which addresses physical layout-level LFI assessment. In this paper, we present an LFI assessment framework integrated into a commercial sign-off tool. The proposed framework has two advantages over the other works of literature. Firstly, laser effects on circuits are simulated accurately through our physical layout-level assessment. Secondly, the reduction of potential critical locations and machine learning (ML) laser cell models make the framework scalable for a full-chip laser fault simulation.

The proposed framework consists of two sub-analysis. The first analysis (Criticality Analysis) is driven by security-property checking using logical fault simulations at the gate level to identify the critical locations (gates/flip-flops), which can significantly reduce the assessment's time and complexity at the layout. The second analysis (Feasibility Analysis) is performed at the layout level, accounting for the physical parameters of the laser and layout. We first create a cell-level laser library by performing the SPICE simulation of every standard cell, and a regression-based ML model is built for each cell to capture the trend between current demands on power pins and the laser photocurrent intensity. Further, we perform a full-chip vectorless dynamic power simulation with the cells in the laser spot replaced with those from the cell laser library, and their current profile is scaled as per the photocurrent intensity using the ML models. Dual goals are reached through our assessment: 1) create the Gaussian nature of the laser, and 2) test the chip for different photocurrent intensities without building a new laser library, thus providing a robust sign-off solution.

II. Background

A. Backside Laser Injection

When the laser beam passes through the silicon substrate, it generates electron-hole pairs (EHPs), which under reverse-biased PN junction drift apart to create a photoelectric current. These currents can cause the charging/discharging of capacitive load at the gate's output to cause a single event transient (SET) or flip the value in the memory element to cause a single event upset (SEU). Take an inverter for illustration, if we consider the laser-illuminated on the drain (n+_Psub junction) of NMOS when input is '0', current (I_{ph}) flows from drain to Psub-bias. However, since Nwell and Psub are reverse biased in normal operating conditions, transient current (I_{ph_bias}) also flows from Nwell biasing to Psub biasing. Due to the shrinkage of the technology node, this can add up and cause a significant impact on the IR drop, causing voltage drop and ground bounce on the power grid. The peak magnitude of photocurrents in the model can be computed using the following equation [4]:

$$I_{ph} = (a \times V + b) \times \alpha_{gauss} \times w \times S_{area}, \qquad (1)$$

where V is the reverse biased voltage (in Volts) of the PN junction, a and b are coefficients dependent on laser power (in Watts). α_{gauss} is dependent on the distance (in μm) between

DISTRIBUTION STATEMENT A. Approved for public release: distribution is unlimited.

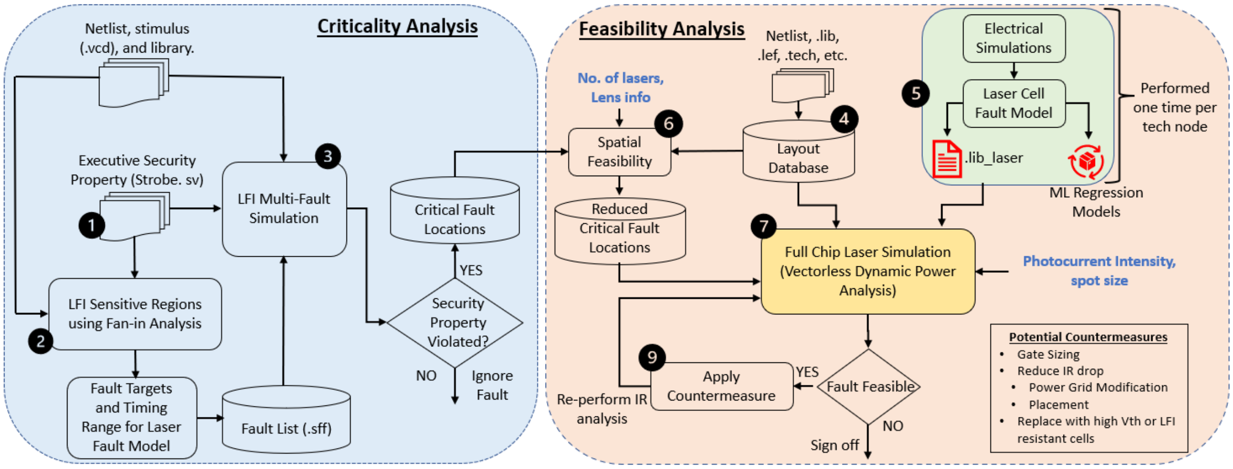

Criticality Analysis
Netlist, stimulus (.vcd), and library.
Executive Security Property (Strobe. sv)
1
2
3
LFI Multi-Fault Simulation
LFI Sensitive Regions using Fan-in Analysis
Fault Targets and Timing Range for Laser Fault Model
Fault List (.sff)
Critical Fault Locations
YES
Security Property Violated?
NO
Ignore Fault
Feasibility Analysis
No. of lasers, Lens info
Netlist, .lib, .lef, .tech, etc.
6
Spatial Feasibility
4
Layout Database
Reduced Critical Fault Locations
5
Electrical Simulations
Laser Cell Fault Model
.lib_laser
Performed one time per tech node
ML Regression Models
7
Full Chip Laser Simulation (Vectorless Dynamic Power Analysis)
Photocurrent Intensity, spot size
9
Apply Countermeasures
Re-perform IR analysis
YES
Fault Feasible
NO
Sign off
Potential Countermeasures
Gate Sizing
Reduce IR drop
Power Grid Modification
Placement
Replace with high Vth or LFI resistant cells

Fig. 1: Proposed framework for fast and scalable pre-silicon LFI assessment.

the laser spot and PN junction and the properties of the optical lens. In addition, w is a normalization factor if the pulse duration is lower than $1\mu s$, and S_{area} is the active junction area (in μm^2).

B. Frontside Laser Injection

The effect of frontside laser injection is similar to that of backside laser injection if the laser manages to reach the active PN junctions. Otherwise, the laser gets reflected, refracted, or absorbed by the metal layers. In modern ICs, the metal layer density is too high with generally more than 10 metal layers [5]. Therefore, it's almost impossible for the laser to reach the desired cells to cause the required faults for fault analysis.

For the metal layers illuminated by the laser, it causes a local increase of the temperature, thus impacting the resistivity of the metal as:

$$\delta\rho = \rho_0 \times \alpha \times \delta T \tag{2}$$

where ρ_0 is the metal resistivity, α is the thermal coefficient of resistance, and δT is temperature change. This change in resistivity causes a change in current or voltage depending on the different TLS techniques.

For optical beam-induced resistivity change (OBRICH), the change in current due to the change in resistance across the metal line held across constant voltage is given by equation 2. For thermally induced voltage alteration (TIVA), the change in voltage due to resistance change across the metal line having constant current is given by.

$$\delta I = -(\frac{\delta R}{R^2}) \times V_s \tag{3}$$

$$\delta V = \delta R \times I_s \tag{4}$$

where V_s and I_s are constant voltage and current sources, δR is the change in resistance, and R is the resistance.

Change in resistance across the metal line can be computed from the average temperature across the metal line at a given time t.

$$\delta R(t) = \rho_0 \times \alpha \times \frac{L}{S} \times (T_{avg}(t) - T_0) \tag{5}$$

where L is length of metal, S is its cross-section, and T_0 is the initial temperature.

III. Methodology

The overall flow of our proposed framework is shown in Fig. 1. The framework consists of two steps, 1) Criticality Analysis and 2) Feasibility Analysis.

A. Criticality Analysis

Firstly, we define executable security properties. Violations of security properties indicate a successful security attack, causing confidentiality and integrity violation. In this paper, we focus on the following:

Security Property: *Register $K^9_{0,0}$ or $K^9_{1,0}$ or $K^9_{2,0}$ or $K^9_{3,0}$ of AES should not be faulty.*

$K^9_{0,0}$ to $K^9_{3,0}$ stand for the first column of 9^{th} round key of AES, violations to this property allow a differential fault analysis (DFA) attack [6] to leak the key. Note that a design can be tested for multiple security properties as per the verification engineer's requirements.

Using a laser, an attacker can either directly inject faults at registers in the security property or gates/flops on their fan-in cones, which get propagated to these registers. The location of these instances and flops in the design's layout is classified as LFI-sensitive regions. For example, for the

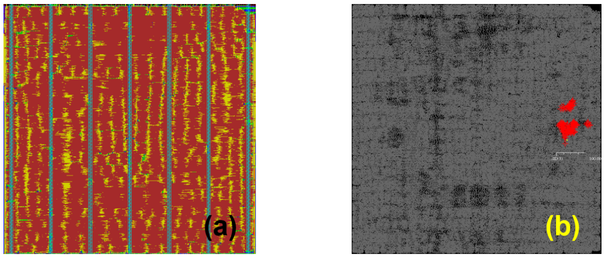
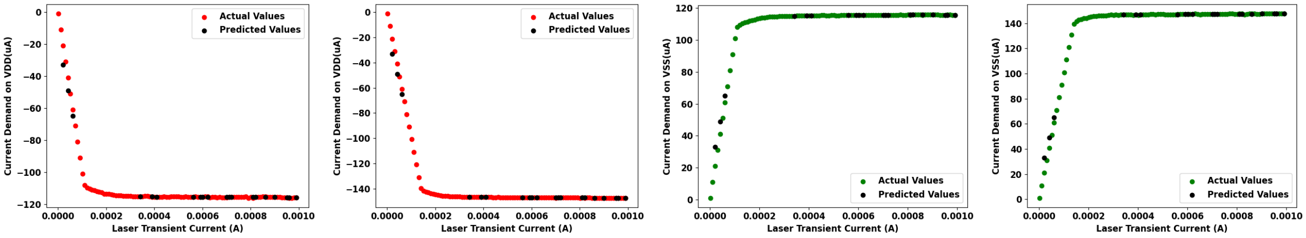


Fig. 2: (a) Layout of tinyAES and (b) critical locations from the security property marked on it.



(a) Pin VDD: Laser State0 (b) Pin VDD: Laser State1 (c) Pin VSS: Laser State0 (d) Pin VSS: Laser State1

Fig. 3: KNN Regression model results for INVX1 cell for different laser states.

security property defined for tinyAES above, we identify the security property registers and then perform the fan-in analysis to identify the LFI critical instances. Fig. 2 shows all these LFI critical instance locations on the layout.

Next, the identified fan-in cells are exploited to generate a fault list for the fault simulation. Each fault in the list could be single-location, or multi-location, considering that a single laser spot can inject multiple faults. Further, the fault is modeled as a transient fault and simulated. The fault simulator performs security property-checking when comparing the good and faulty simulations. Any fault causing security property violations is labeled as a critical location.

B. Feasibility Analysis

With the identified critical locations, feasibility analysis aims to assess whether it is possible to inject laser faults for the given laser specifications and layout parameters. First, we reduce critical faults to those that are spatially feasible for the given laser and placement constraints. Subsequently, we draw an approximate laser spot covering the critical cells' list. For each cell, we approximate the I_{ph_bias} current, based on Equation (1). Next, to prepare for full-chip laser simulation, we extract the SPICE model for each standard cell and perform the electrical simulation by adding the laser transient current. Depending on the distance of the cell from the laser spot center, the induced photocurrent should vary. However, this laser-induced current can be impacted by various factors. It is not feasible to calculate the current demand on power pins based on all these arbitrary currents. Therefore, we built machine learning regression models to create a mapping between different photocurrent intensities and the current demand on power pins. Thus, created a laser cell library, which can scale the current up or down for the impacted cells during laser simulations. Finally, for each critical location, we place a laser spot and substitute the impacted cells with those from the laser cell library. The vectorless dynamic power simulation is performed for varying photocurrent intensities, which can capture the demand current and IR drop at the cell instances under laser illumination.

IV. Experimental Results

This section provides the results for verifying the layout of the opensource tinyAES [7] design using the proposed framework. We used Synopsys Z01X as a netlist fault simulator, Ansys Redhawk-SC to perform full-chip simulations, and Cadence Spectre to perform SPICE simulations.

The design is synthesized for 45nm CMOS technology, one-time cell-level laser library and machine learning regression models were built for 73 different cells. For developing regression models, each cell netlist was simulated for varying laser current intensity and current profiles are captured on the VDD and VSS pins for both laser state0 and state1. Then we used different regression models, i.e., Ridge, K-nearest Neighbors (KNN), Bayesian, Decision Tree, and State Vector Machine. Since the relationship between laser current intensity and current on VDD/VSS pins is of exponential nature, the KNN regression model worked best with an average accuracy of 98% on 20% test size. Fig. 3 shows the example regression results for INVX1 cell for different laser states. The black dots are the predicted current demand by the model for the corresponding laser intensity.

A. Criticality Analysis Results

For criticality analysis, from 1 to 3 concurrent-fault scenarios are considered, identifying 160, 483, and 837 critical locations from a total cell list of 183881 cells, respectively. Table I shows the verification results for tinyAES design for the security property demonstrated in Section III-A for lenses of 50x and 100x objectives, assuming a laser spot size of $9\mu m$ and $2\mu m$, respectively. In Table I, column "Critical Faults" represent the single critical instances or combinations of critical instances that violate the security property.

B. Feasibility Analysis Results

The first step in the feasibility analysis is spatial feasibility, which ensures that the placement of the critical faults is such that they could be simultaneously illuminated by the laser. Table I shows the spatial feasibility results for the given properties. It can be seen that the spatially feasible faults remain the same for 3 simultaneous fault scenarios due to spot size limitation (as seen in the 100x lens case). The important thing to note from the table is that the number of spatially feasible faults for the given laser and lens parameter are very few compared to the total instances in the design. Thus, we need to inject the laser at only those fault locations instead of exhaustively illuminating the entire chip.

The current demand on different instances illuminated by the laser is shown in Fig. 4. In this single-spot experiment,

TABLE I: Criticality and spatial feasibility results on tinyAES benchmark.

Property	Cell Type	Multi-Fault Scenario	Total Instances	Fault List	Fault Sim. Time (s)	Critical Faults (% of Fault List)	Spatial Feasibility (% of Fault List)	
							50x lens	100x lens
							(9um spot)	(2um spot)
One	Seq. only	1 Fault	183881	192	25	160 (83.3%)	160 (83.3%)	160 (83.3%)
		2 Faults		9312	47	3728 (40%)	483 (5.2%)	185 (2%)
		3 Faults		295072	735	63984 (21.6%)	837 (0.3%)	185 (˜0%)
	Seq. + Comb.	1 Fault		320	25	224 (70%)	224 (70%)	224 (70%)
		2 Faults		25760	65	9904 (38%)	1071 (4.1%)	281 (1%)
		3 Faults		1365600	5543	391888 (28%)	2735 (0.2%)	283 (˜0%)

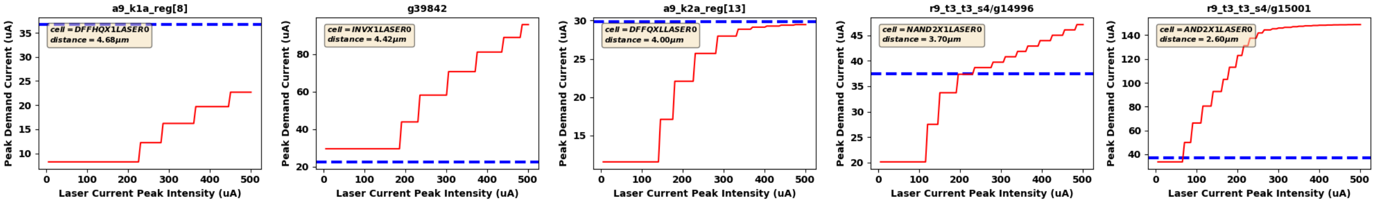


Fig. 4: Current demand on VDD pin of different cells in a laser spot for varying laser intensity.

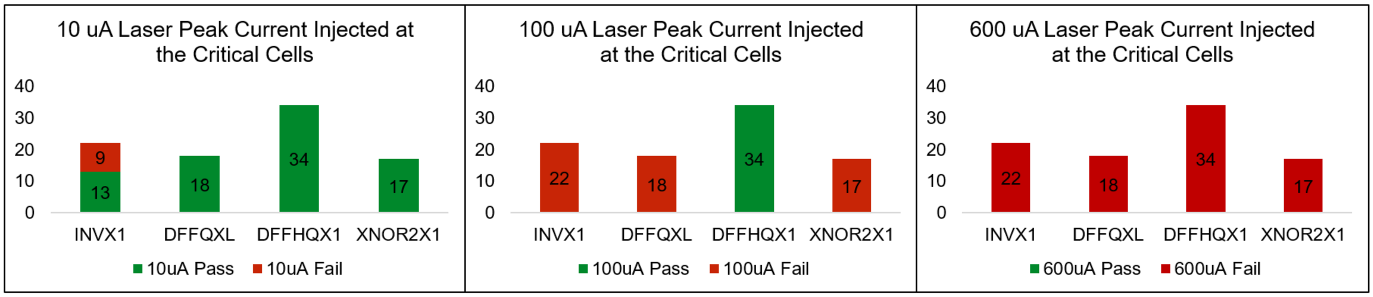


Fig. 5: Number of critical cells failing for different laser current intensities.

the laser is centered at one example critical flip-flop, and all cells covered in the spot are simulated with varying laser intensities. The blue dotted line represents the current demand on the VDD pin of the cell without the laser's impact, thus, if the laser-impacted current demand (red) goes above the blue line, it can be assumed that the cell has experienced a fault (output flipped). Note that this experiment can be repeated by centering any other critical cells and any laser parameters configured by users. For another experiment applying multi-spot, Fig. 5 shows the results when the laser is centered at every critical instance for two different peak laser intensities for $9\mu m$ spot size. Finally, from our experiments, we concluded two observations: 1) Type of nearby cells and their switching activity can impact the critical cell's resiliency against laser injection. 2) Bulky cells require higher laser intensities to inject fault.

V. Conclusion

In this paper, we successfully integrated a pre-silicon LFI assessment framework into a commercial sign-off tool, which allows verification engineers to analyze the impact of laser fault simulation on the layout of a chip. The proposed framework uses machine learning (ML) and security property violation approach to identify LFI critical locations. It also injects Gaussian laser current profiles of any spot size into the physical layout, and analyzes if a laser fault is feasible at the cell instances for the given laser specification. The proposed framework has two advantages over the other works of literature. Firstly, laser effects on circuits are simulated accurately through our layout-level assessment. Secondly, the reduction of potential critical locations and ML laser cell models make the framework scalable for a full-chip laser fault simulation.

References

[1] R. L. Wadsack, "Fault modeling and logic simulation of cmos and mos integrated circuits," *Bell System Technical Journal*, vol. 57, no. 5, pp. 1449–1474, 1978.

[2] C. Godlewski, V. Pouget, D. Lewis, and M. Lisart, "Electrical modeling of the effect of beam profile for pulsed laser fault injection," *Microelectronics Reliability*, vol. 49, no. 9-11, pp. 1143–1147, 2009.

[3] 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.

[4] 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, 2013.

[5] S. D. Castro, J.-M. Dutertre, B. Rouzeyre, G. D. Natale, and M.-L. Flottes, "Frontside versus backside laser injection: a comparative study," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 1, pp. 1–15, 2016.

[6] C. H. Kim and J.-J. Quisquater, "New differential fault analysis on aes key schedule: Two faults are enough," in *Smart Card Research and Advanced Applications*, G. Grimaud and F.-X. Standaert, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 48–60.

[7] OpenCores, "Tinyaes," https://opencores.org/projects/tiny_aes.