# Physically-aware Laser Fault Injection Assessment

Henian Li, Sukanta Dey, Farimah Farahmandi
Department of Electrical and Computer Engineering, University of Florida

*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 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 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, 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 physical parameters of 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 Gaussian nature of the laser, and 2) test chip for different photocurrent intensities without building new laser library, thus providing a robust sign-off solution.

## II. BACKGROUND

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 photoelectric current. These currents can cause charging/discharging of capacitive load at the gate's output to cause single event transient (SET) or flip the value in memory element to cause 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 significant impact on the IR drop, causing voltage drop and ground bounce on power grid. The peak magnitude of photocurrents in the model can be computed using the following equation [1]:

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

where the notations represent parameters as mentioned in [1].

## 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 $K_{0,0}^9$ or $K_{1,0}^9$ or $K_{2,0}^9$ or $K_{3,0}^9$ of AES should not be faulty.*

$K_{0,0}^9$ to $K_{3,0}^9$ stand for the first column of $9^{th}$ round key of AES, violations to this property allow a differential fault analysis (DFA) attack [2] to leak the key.

Next, we perform the fan-in analysis for the given attack window to identify other gates/flops from where faults can propagate to the critical registers involved in security properties. The identified fan-in cells contribute to generating 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 critical locations.

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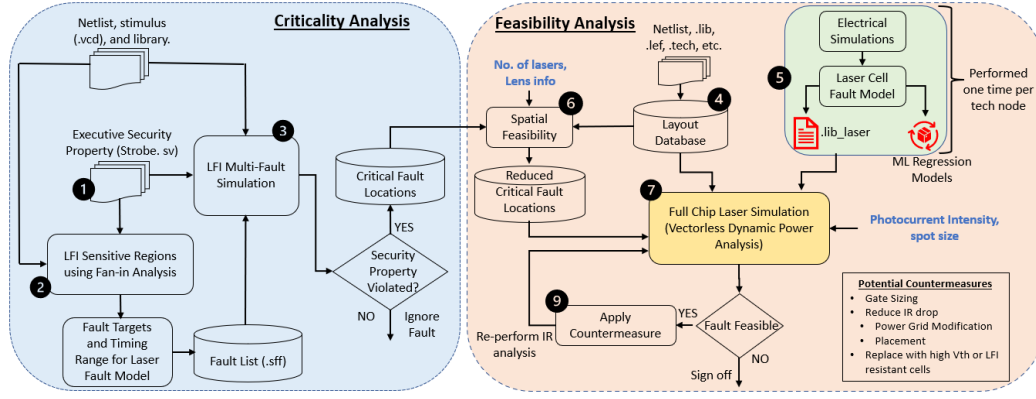
Fig. 1: Proposed framework for fast and scalable pre-silicon LFI assessment.

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 [3] 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 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. Fig. 2 shows an example of these LFI critical instance locations on the layout.

For feasibility analysis, the current demand on different instances illuminated by the laser is shown in Fig. 3. In this single-spot experiment, 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 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 with any other critical cell centered and any laser parameters configured by users. For another experiment applying multi-spot, Fig. 4 shows the results when the laser is
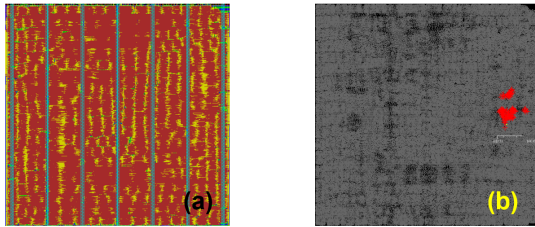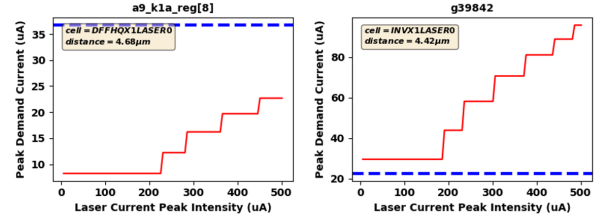


Fig. 3: Current demand on VDD of different cells in a laser spot for varying laser intensity.
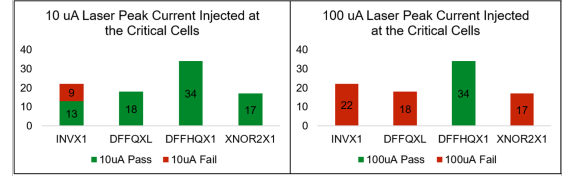


Fig. 4: Number of critical cells failing for two laser intensities.

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 inject Gaussian laser current profiles of any spot size into the physical layout, and analyze 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, reduction of potential critical locations and ML laser cell models make the framework scalable for a full-chip laser fault simulation.

## REFERENCES

[1] 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.

[2] 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.

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

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