SPRED: Spatially Distributed Laser Fault Injection Resilient Design

Tasnuva Farheen[1], Shahin Tajik[2], and Domenic Forte[1]
[1]Department of Electrical and Computer Engineering, University of Florida
[2]Department of Electrical and Computer Engineering, Worcester Polytechnic Institute

***Abstract*—Computing systems' hardware implementation is vulnerable to physical attacks. One of the most powerful tools in the arsenal of physical attacks is laser fault injection (LFI), which can successfully compromise an embedded cryptographic implementation even with a single fault. Several countermeasures have been proposed to prevent and detect LFI attacks. However, these schemes cannot protect a multi-spot laser fault injection setup alone. Vulnerabilities can be addressed in such circumstances using a multi-layer or defense-in-depth approach. Defense-in-depth refers to implementing several independent countermeasures within a device to provide aggregated protection against various attack vectors. In this paper, we introduce a multi-layer countermeasure where the proposed approach protects an LFI attack detector against multi-spot LFI attacks. We design and simulate a spatially distributed multi-gate driven design, called SPRED, to prevent single and multi-spot LFI attacks. Simulation results show that the distribution of gates in SPRED forces an attacker to use higher laser power and a thinner wafer to inject a fault.**

***Index Terms*—Laser fault injection, Multi-spot LFI setup, countermeasure, Multi-layer Defense, Detector.**

I. Introduction

There are many fault injection attack variants 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 [1], [2]. The calculation cost of FA can be significantly reduced by precisely controlling the laser's fault injection timing and position. LFI has the highest time and space resolution for the most efficient attack capability compared to the other variants mentioned above. As a result, laser fault injection, initially conceived to mimic radiation effects in space applications, has become a tremendous security threat.

Several countermeasures have been proposed over the years against LFI attacks. One of the most straightforward schemes is computational redundancy [3], [4]. In this scheme, two or more logic copies are integrated, and each output is verified to detect a single fault. This countermeasure, however, is unavoidably burdensome since the power or space overhead is multiplied by the number of copies. Multiple laser injections can also circumvent this countermeasure [5]. Another approach would be a physical-level countermeasure, such as a shield [6]. However, such shields are only effective against front-side LFI, which occurs through upper metal layers. A near-infrared (NIR) laser can penetrate the silicon substrate, enabling back-side LFI to bypass the metal shield [7].

Other countermeasures for front- and back-side LFI include physical sensor-based approaches whereby a detector measures physical disturbances caused by the laser. The challenge is implementing a sensor in a small area and responding immediately after an attack is detected. Typical implementations of photosensors have enormous area penalties since a dense array arrangement is necessary to protect the entire die from focused laser irradiation. Additionally, there has not been much discussion about the response after an attack is detected. Recent work has proposed a compact sense-and-react IC-level countermeasure to LFI. In contrast to the photosensor, an abnormal optoelectric bulk current caused by the laser is detected [8]. However, this sensor can only detect whether the core is being attacked. A new sensor-based countermeasure, extending the sense-and-react strategy, has been published recently [9]. It can detect a partial secret key bit and continue even after the LFI attack for highly available resilient cryptographic systems. However, a multi-spot laser setup [10], where multiple faults are injected simultaneously, can circumvent both of these sensor-based approaches.

In this paper, We propose a spatially distributed multi-gate-driven design called SPRED to address the abovementioned issues. Here, we copy and spread security-critical gates and place them so that the laser effect will be distributed among the logic gates. As a result, there is not enough photocurrent generation to create a fault. Our approach can also be effective against a multi-spot laser setup. As we place the gates at such a distance, it will not be possible for the attacker to affect the design cumulatively with multiple laser spots. Moreover, we propose using our spatially distributed multi-gate driven design and a detector to provide aggregated protection against single and multi-spot laser fault injections.

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

- We propose SPRED, a spatially distributed multi-gate-driven design, to prevent LFI attacks. A single, security-critical net is created by inserting copies of the same logic gates at a distance specified by the user.
- To showcase the strength of our approach, we perform simulation-based analysis on inverters and NAND gates. The simulation considers various laser-sensitive parameters, including laser power, wafer thickness, pulse duration, area, and spatial distribution.
- There are several security metrics we devise: sensitive area, spatial distribution, critical power, and wafer thickness. Based on these metrics, we evaluate SPRED's resilience

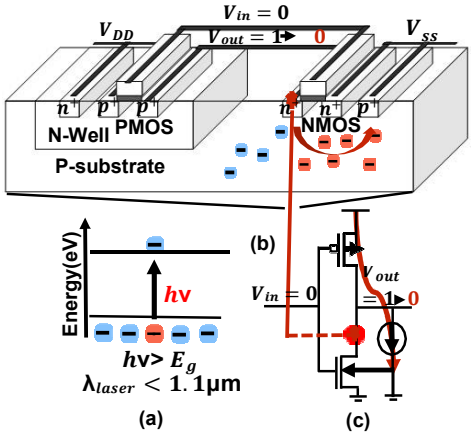

Fig. 1: (a) Physics of photoelectric laser stimulation (b) Laser fault injection mechanism (c) Occurrence of single event error.

against fault occurrence. The analysis shows that proposed approach can increase the protection against LFI with high confidence.

- We also discuss the resiliency of SPRED against a multi-spot LFI setup and describe how it can complement sensor-based countermeasures in a multi-layer defense solution.

The rest of the paper is organized as follows. In Section II, we introduce the background of fault injection mechanism, single event error, and influential parameters in LFI. In Section III, we describe an electrical threat model that mimics the photoelectric effect. In Section IV, we propose our LFI resilient spatially distributed design countermeasure SPRED. Afterward, in Section V, we develop security metrics to evaluate our design. In Section VI we discuss the validation of our proposed approach with simulation results. Section VII describes the application of our proposed countermeasure with the detector as multi-layer-defense approach. Finally, the conclusion and future work are provided in Section VIII.

II. Background and Related Work

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 [11], [12] 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 ceased [12]. A transient voltage spike caused by this current pulse induces faults in secure circuits to retrieve confidential data stored in these devices [13], [14].

B. Single Event Error (SEE)

Fig. 1 (c) illustrates how a transient photocurrent is turned into a single-event error (SEE) 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 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), 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. Influential Parameters in Laser Fault Injection

In this section, we discuss the parameters that influence the laser fault injection.

a) Laser Power Effect: Investigation of the N+/P substrate (PN) junction under PLS 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.

The current-voltage (IV) characteristics as shown in Fig. 2 (a) were obtained from [15] by experimental measurement. 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. The photocurrent induced in a reverse biased PN junction by a laser pulse could be approximated by a first order polynomial function [15] :

$$I_{ph}(P_{laser}, V_j) = a(P_{laser}).V_j + b(P_{laser}) \quad (1)$$

where a and b are modeling coefficients, P_{laser} represents power, and V_j is the voltage across the junction.

b) Pulse Duration Effect: In Equation (2) [16], $Pulse_{width}$ considers the laser pulse duration dependency where t_{pulse} is the laser pulse duration in seconds. Equation (3) represents the effect of pulse duration by incorporating $Pulse_{width}$.

$$Pulse_{width} = 1 - \exp^{\frac{-t_{pulse}}{250\times10^{-9}}} \quad (2)$$

$$I_{ph}(P_{laser}, V_j, Pulse_{width}) = (a \times V_j + b) \times Pulse_{width} \quad (3)$$

c) Junctions Area Effect: PN junction area also has a significant effect on the generated photocurrent. Specifically,

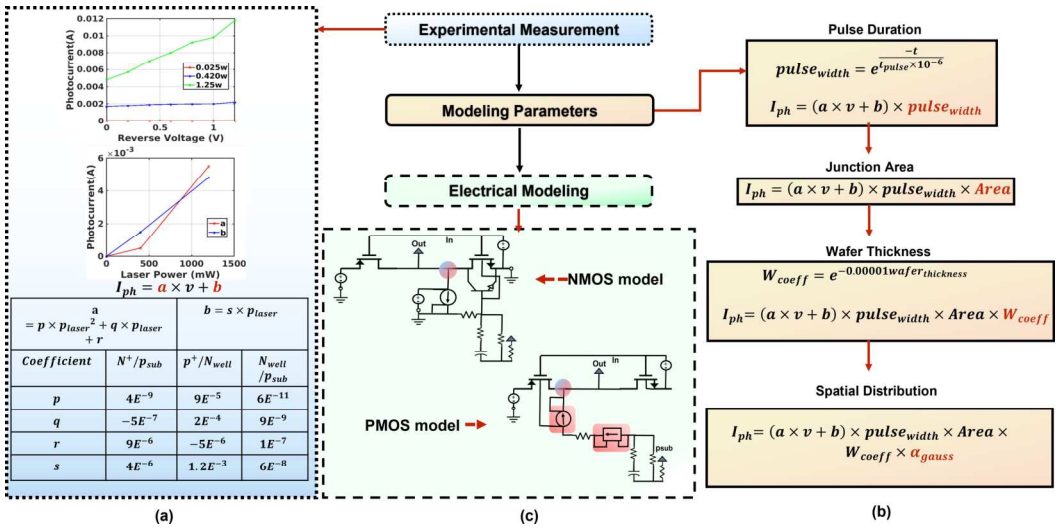

Fig. 2: Threat modeling of photoelectric laser stimulation (a) Experimental measurement data from literature [15] (b) Modeling parameters [16] and (c) Electrical modeling using verilog-A module.

it is directly proportional to the area as one can see from Equation (4) [16].

$$I_{ph} = (a \times V_j + b) \times Pulse_{width} \times Area_{exposed} \quad (4)$$

The larger the area, the larger the interaction of the laser with the silicon and electron-hole pair generation.

d) Wafer Thickness Effect: The substrate thickness has a significant effect on the photocurrent generation of PN junctions under PLS. The light intensity exponentially decreases throughout the material and so does the photocurrent effect. In other words, the thinner the wafer, the more photocurrent generated on PN junction under PLS. The effect can be modeled by Equation (5) [16].

$$W_{coeff} = \exp^{-0.00001 \times wafer_{thickness}} \quad (5)$$

Here, $wafer_{thickness}$ is the thickness of the wafer expressed in μm. Hence, Equation (6), that incorporates the wafer thickness dependency.

$$I_{ph} = (a \times V_j + b) \times Pulse_{width} \times Area_{exposed} \times W_{coeff} \quad (6)$$

This final equation includes all the parameters discussed above: reverse-biased voltage V_j, a and b that depend on the laser power P_{laser}, $Pulse_{width}$ accounting for the laser pulse duration, W_{coeff} for the wafer thickness effect, and $Area_{exposed}$ is the effective area of the exposed PN junction.

III. Threat Model

To delineate the scope of our threat model, we incorporate experimental measurement data from literature [15] and influential parameters in LFI [16] as shown in Fig. 2. In our threat model, we restrict our analysis to combinational logic, where a fault injection's outcome depends on the logic gates' specific input pattern. We assume that an adversary can accurately inject faults into the logic gates based on the coordinates of the laser beam, laser power, silicon wafer thickness, and positions of the critical gates in the layout through reverse engineering or an insider. For current technology nodes where the laser beam diameter is much larger than the minimum feature size, one laser spot can incur multiple faults if they are close to each other. Further, faults can be increased by incorporating more simultaneous lasers using a multi-spot laser setup [10]. The laser beam diameter can also be increased; however, this lowers the laser power density and thus the probability of occurring faults [17].

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 counter an attack if the effects are close to actual scenarios. Our electrical threat model incorporates all laser-affecting parameters using the Verilog-A module. A general threat model can handle LFI attacks in state-of-the-art setups. Based on this threat model, we propose a countermeasure (SPRED).

IV. SPRED Methodology

In order to improve the circuit resilience to laser-based attacks we propose spatially-aware distributed design with transistor sizing or SPRED.

Photocurrent vs. Laser Position: When a standard logic cell is entirely illuminated, all the laser-induced effects fall on the PN junctions that are laser sensitive. Consider the inverter in Fig. 3(a) as an example. Here, the inverter input is in the low state, so 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. Let us assume the laser only focuses on the drain of the NMOS transistor. So, according to Fig. 3(b), the laser beam intensity will be highest at this point. Due to the laser shot, parasitic current will be generated, causing the bit to reset error at output shown in

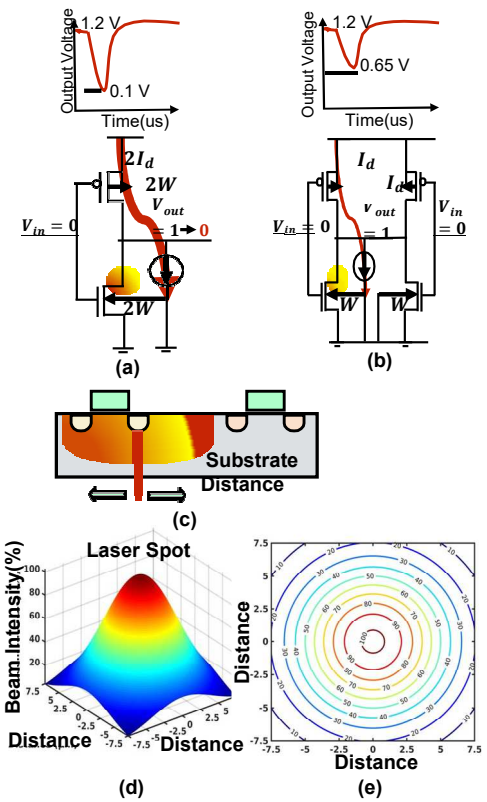

Fig. 3: Voltage level comparison for corresponding designs – (a) regular logic gate; (b) spatially distributed multi-gate design; (c) Laser distribution effect across the distance (d) Laser beam in terms of intensity per area in three dimensional view with the color representation of different laser energy level; (e) Contour lines where 100% of laser beam intensity represents the epicenter of the laser spot.

the output voltage vs. time graph in Fig. 3(a). The generation of this photocurrent and laser effect on the output voltage depends on the laser-sensitive junction area as discussed in Section II-C. We have tweaked this parameter and propose a countermeasure exploiting this.

Placement of the Distributed Gates: The basic concept of our approach is to split the target transistors by placing parallel pull-up and pull-down transistors far enough apart such that the laser intensity will be distributed among the distributed logic gates under the laser spot. We place the distributed logic gates depending on the bivariate normal distribution of the laser intensity as shown in Fig. 3(d),(e). With the increase of the distance from the epicenter of the laser shown in Fig. 3(c), the laser effect gets distributed. As a result, the photocurrent would be too low to trigger a fault.

SPRED is depicted more clearly in Fig. 4. In a typical inverter, as shown in Fig. 4(a), the laser hits only the pull-down transistor with the larger width, and the generated photocurrent is higher than the drain current I_d of the PMOS. Thus, there is enough photocurrent to reset the output of the inverter, in Fig. 4(b), (c), and (d), the logic gate is distributed as a multi-gate driven design. Let us compare them with a single inverter design. We can see that the laser energy is distributed among

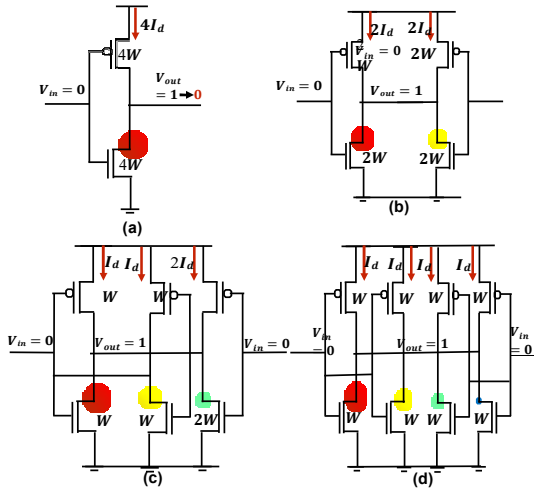

Fig. 4: Transistor sizing with spatial distribution of laser effect in (a) typical inverter, (b) double inverter, (c) triple inverter, and (d) quadruple inverter. Here, W represents the width of the transistor and the colors represent various laser energy level from Fig. 3(d,e) .

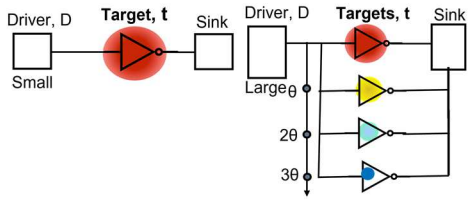

Fig. 5: (left) Original inverter; (right) Placement of the multiple inverter standard cells sharing same input and output with the distribution of laser energy varying by distance ϑ. Note that a larger driver might be needed to accommodate the additional standard cells.

the gates and the photocurrent generation also decreases due to the distribution of sensitive areas.

A similar effect can also be achieved if we replace the larger width standard cell with multiple smaller width standard cells sharing same input and output, and spread them apart in the layout. This is more practical than transistor sizing and spreading since we can rely on standard cells. During the placement as shown in Fig. 5, we make sure that the cells are placed in such a distance that the distribution of the laser effect is maximum. It also complies with the Gaussian distribution of laser energy shown in Fig. 4(c,d).

Algorithm 1 is also presented as a pseudo code to portray the placement methodology leveraging metrics sensitive area/ transistor width and spatial distribution. At first, the target gate is identified as t (line 1). Then, we get the target gate's location along with its width (lines 3,4). After that, we specify the spatial distance ϑ for the placement of multiple standard cells as shown in Fig. 5 (line 5). We identify the minimum transistor width for specific technology and get the footprint of the target transistor (lines 6,7). The metric fault occurrence is defined as the function of transistor width (line 8). After getting all the parameters, our algorithm calculates the fault occurrence

Algorithm 1 Spatial Distribution of Multi-Gate-Driven Design

1: **Input:** t *(target gate)*
2: **Output:** *spatially distributed gates*
3: $x_t, y_t \leftarrow$ *get location of* t
4: $g_{width} \leftarrow$*get the width of target transistor,* t
5: $\vartheta \leftarrow$spatial distance in μm
6: $w \leftarrow$*minimum transistor width of specific technology*
7: $g_{fp} \leftarrow$*get footprint of* t
8: f(W) $\leftarrow$ *faultoccurrence* $= \frac{W}{\theta}$
9: **for** $(i = w, i \leq g_{width}, i++)$
10: *calculate fault occurrence,* $f(i)$
11: **if** $(f(i) < f)$
12: $\gamma = i$ // the size of multi-gates
13: $\delta = \lceil \frac{g_{width}}{i} \rceil$ // the number of multi-gates to add
14: $f \leftarrow f(i)$
15: *downsize* $t \rightarrow \gamma$
16: **for** $(i = 1, i < \delta, i++)$
17: $y_i = y_t \pm \vartheta * i$
18: *Insert* t_i *of lib* g_{fp}*, size* γ *at* $\{x_t, y_i\}$
19: *set dont_touch* t_i
20: **return** *Spatially Distributed Gates*

of the target transistor with width g_{width} and a standard cell of footprint g_{fp} with minimum width w (line 10). According to our proposed approach, SPREAD, we replace the larger width target standard cell with multiple smaller width standard cells and then spread them out. In our algorithm, we use fault occurrence based metric to find out the size of the multi gates. For example, a 4x target gate can be replaced with two 2x or four 1x standard cells. For various combinations, we calculate the fault occurrence; the one with the least fault occurrence value is the chosen one. This design is specified as the size of the multi gates, and then the number of multi-gates needed to add is calculated from this (line 12,13) with the downsizing of t to γ. Next, our algorithm takes care of the placement of the multi-gates confirming the spatial distribution of laser energy varying by distance ϑ (lines 16,17,18). In our work, we set the *dont_touch* (line 19) attribute so that the tool (Synopsys ICC2) can not automatically remove the multiple copies of the standard cells for optimization. In Section VI, a comprehensive simulation analysis of our proposed approach is presented.

V. Proposed Security Metrics

We have developed the following security metrics for evaluating a gate's resistance to LFI. During the evaluation of the proposed approach, we have considered these metrics and presented the results based on these.

a) Sensitive Area: Sensitive area is the PN junction area of OFF transistors under the laser spot. The area has a significant effect on the photocurrent with proportional relationship.

b) Spatial Distribution: The distance between the laser spot and the PN junction has a substantial impact on the beam intensity distribution, thus impacting the value of the generated photocurrent and fault occurrence.

c) Critical Power: Critical power is the maximum power up to which a gate is resistant to fault injection. For various logic gate designs, the values of this security metric vary.

d) Critical Wafer Thickness: Critical wafer thickness is the minimum thickness up to which a gate is resistant to fault injection. This metric also varies for various logic gate designs.

$$f \propto \frac{Area_{exposed} * w_{critical}}{Distance * P_{critical}}$$

Here,$Area_{exposed}$ is the sensitive area, e.g., the NMOS drain area. With the decrease of the sensitive area under the laser spot, photocurrent decreases so does the fault occurrence, f, thereby increasing the security against laser fault injection. With the increase of the distance from the laser spot, the laser effect gradually decreases. As a result, the probability of fault occurrence is also reduced. The higher the critical power for a particular design is, the higher the resistance to fault occurrence. The lower the critical wafer thickness for a particular design, the higher the resistance to fault occurrence. In the two critical security metrics presented above, no fixed threshold characteristics (power, wafer thickness) indicate when a fault occurs or not. The occurrence of a fault depends on the cell illuminated by the laser beam.

VI. Simulation Results and Discussion

A. Simulation Setup

Simulation results in Cadence Spectre evaluate the attack resiliency of the proposed countermeasure against laser fault injection. As mentioned in Section IV and shown in Fig. 3(c,d,e), the applied spacing among distributed logic gates is dependent on the area affected by the laser spot, which itself depends on several factors, such as laser power, wafer thickness, etc. To investigate the impact of our approach, as a function of applied spacing constraints, we tested four different spacing in the range [0, 7.5] µm. This range is based on the 5 µm laser spot with Gaussian distribution effect shown in Fig. 3(d), where the affected areas for laser power in the range [0,2] W. We also collect the varying laser power and wafer thickness results for various multi-gate-driven designs and determine the critical parameters.

B. Simulation Flow

Fig. 6 proposes a non-exhaustive step by step simulation methodology. This methodology, which is based on standard CAD tools, – IC compiler II for placement and routing, StarRC for parasitic extraction to incorporate RC delay, PrimeTime to analyze the impact on timing critical paths, Cadence Spectre for the simulation –allows to investigate the resiliency of the proposed spatially distributed LFI resilient design.

C. Proof-of-Concept Logic Gates Implementation

We have implemented two Proof-of-concept (PoC) logic gates in the electrical threat model to generate our experimental results. The target gates are inverter and NAND in The PoC circuit with different input combinations. We implemented two input combinations for the inverter and four input combinations for the NAND gate. Then we generated the simulation results for various LFI attack critical parameters and spatial distribution effects.

D. Simulation Results and Discussion

A fault probability is evaluated in the LFI electrical threat model for preliminary analysis. In this analysis, 'fault' means temporal output bit flip by the laser irradiation, and 'fault probability' means the probability of this temporary bit flip occurring. We have taken the inverter as our sample structure

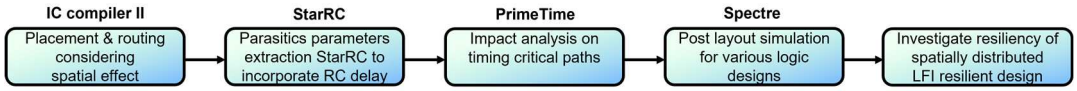

Fig. 6: Experimental validation simulation flow.

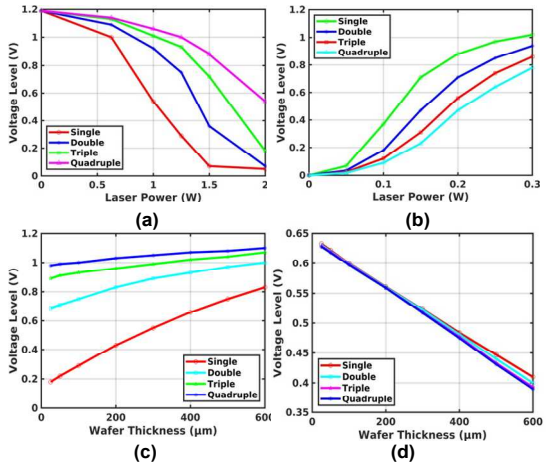

Fig. 7: Level of voltages at various laser power and wafer thickness in (a), (c) for NMOS and in (b), (d) for PMOS respectively at various multi-gate designs. Quadruple design shows the highest resiliency against the fault occurrence with the increase of laser power and decrease of wafer thickness.

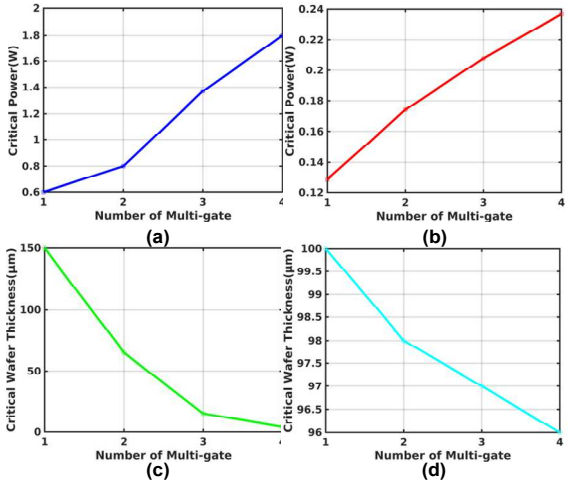

Fig. 8: With the increase of logic gates distribution and spatial distance, the resiliency against the fault occurrence increases due to increase of critical power. Further, the resiliency against the fault occurrence increases with the decrease of critical wafer thickness. This is shown in (a), (c) for NMOS and (b), **(d)** for PMOS, respectively.

to test our proposed approach. We considered two cases: input at '0' referring to the NMOS model, and input at '1' referring to the PMOS model. For the typical scenario at the no-fault condition, with the input at '0', the output should be '1,' or in the bit-set state, and with the input '1', the output should be '0' or in bit-reset state. However, a generation of photocurrent with the laser effect forces the output voltage to drop below 0.6 V, causing the bit to reset fault and increase above 0.6 V, causing the bit to set fault. Here, for a supply voltage of 1.2 V, we can take 0.6 V as the threshold voltage. This section will investigate the resiliency of our proposed approach, up to which level it can prevent the laser fault injection while keeping the voltage level as intended.

Laser Power Effect. To study the PN junction area effect on the generated photocurrent, we significantly distribute the gate size and reduce the laser effect. We have investigated the voltage level with laser power and wafer thickness variation on inverter under laser effect at single gate design and multi-gate driven designs where we split the sensitive gates into multiple gates: double, triple, quadruple, reducing the effective area of photocurrent generation. In Fig. 7(a), we can see that for single gate design, when the laser power is at 1W and above, the voltage level continuously drops, causing a bit-reset fault. With the decreasing area in double, triple, and quadruple designs, the sensitivity of voltage level to laser power decreases. As a result, rather than incurring a bit reset fault at 1W as a single inverter design, the resiliency threshold against laser power increases to 1.25, 1.5, and 1.8 W, respectively, for double, triple, and quadruple designs. Similarly, in the case of a single gate design with input '1', when the laser power is at 130 mW and above, the voltage level continuously increases, causing a bit-set fault as depicted in Fig. 7(b). With the decreasing area in double, triple, and quadruple designs, the sensitivity of voltage level to laser power decreases. As a result, rather than incurring a bit-set error at 130 mW as a single inverter design, the resiliency threshold against laser power increases to 150, 200, and 240 mW, respectively.

Wafer Thickness Effect. The substrate thickness also significantly affects the photocurrent generation of PN junctions under photoelectric laser stimulation (PLS). The light intensity exponentially decreases throughout the material, and so does the photocurrent effect. The variation of voltage level with wafer thickness effects is shown in Fig. 7(c),(d). For a single inverter design with input '0', if the wafer thickness is less than 400 μm, the generated photocurrent will be enough to occur bit-reset fault. Our multi-gate-driven design shows strong resiliency in this case. The wafer thickness should be less than $40\mu m$ for double gate design and less than $10\mu m$ for triple and quadruple configurations to cause bit set-reset errors. In the case of a single inverter design with input '1', if the wafer thickness is less than 100 μm, the generated photocurrent will be enough to occur bit-set error. For our multi-gate driven design, we do not notice a significant effect on the wafer thickness, as shown in Fig. 7(d).

Critical Parameters. From the above analysis and corresponding Fig. 7, we find out the 'critical power' and 'critical wafer thickness' for various designs as shown in Fig. 8. As discussed in Section V, critical power is the power above which there will be a generation of enough photocurrent,

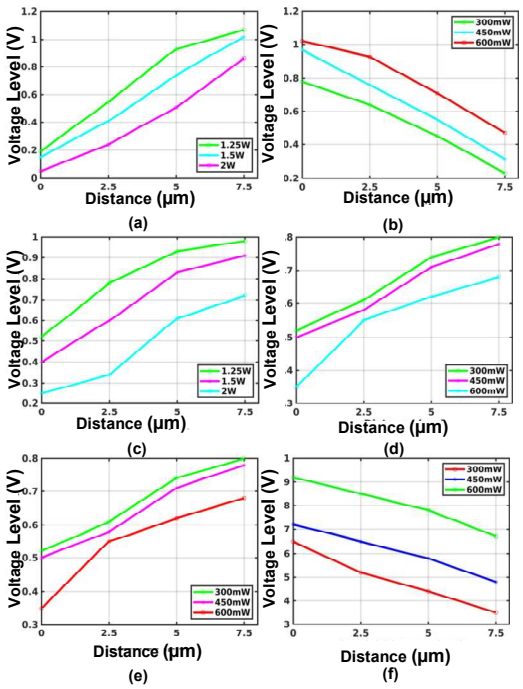

Fig. 9: At various laser power, with the increase of spatial distance in various logic gate designs of different inputs the resiliency against the fault occurrence increases; NOT gate input (a) 0 , (b) 1; and NAND gate inputs (c) (0,0) , (d) (0,1) , (e) (1,0) and (f) (1,1), respectively.

which will cause a bit of set-reset fault. Critical thickness is the thickness below which the induced photocurrent causes bit set-reset errors. The values of these two metrics vary from design to design. However, they provide a concise idea of a particular design's resistance to fault occurrence. The higher the laser power and lower the critical wafer thickness for a particular design, the higher the resistance to fault occurrence is. From Figure 8(a) and (c), the critical power and thickness for single, double, triple, and quadruple designs with input '0' are respectively 1.03, 1.37, 1.63, 1.93 *watt* and 150, 65, 5, 4 μm. The corresponding values for multi-gate designs with input '1' are 0.129, 0.174, 0.208, 0.237 *watt* and 100, 98, 97, 96 μm, respectively.

Spatial Distribution Effect. The above analysis delineates that the quadruple design shows the best resiliency against fault occurrence under the laser spot among all the distributed designs. We do further analysis to show that our approach is resistant to multi-bit faults and multi-spot laser setup. We have taken the inverter and NAND gate as our sample structure to test the spatial distribution effect and perform the post-layout simulation to investigate the voltage level at corresponding distances. The results are shown in Fig. 9. With the increase of the spatial distance for different inputs at various logic gate designs, the resiliency against the fault occurrence increases. To place the gates of the quadruple design at various distances apart, we use IC Compiler II, as shown in Fig. 10.

Impact on Timing Critical Paths. The target gate replaced by SPRED can be a critical path component. We must check whether our design meets critical timing requirements as we

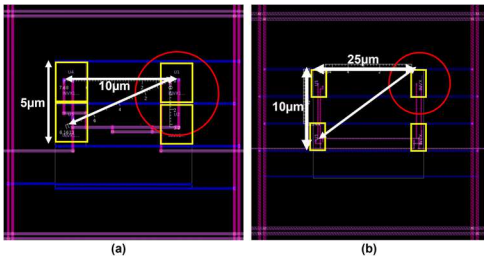

Fig. 10: Placement of logic gates using ICC2. Laser (a) effects two gates close to each other where as at (b) only effects one gate. Here, SPRED ensures certain arrangements comply with security requirements.

are changing the transistor width and playing with the spatial distance. Using Synopsys PrimeTime, we analyze the timing behavior of the gates along the critical path placed at the same interval. The analysis indicates that as we do not modify the total critical path delay and place the gates in this path at a certain distance such that they work as repeaters and do not cause any timing failure.

Resiliency Against Multi-spot LFI Setup. In [10], a multi-spot laser fault injection setup is introduced. A laser spot can be positioned independently on the die by triggering each laser source separately. The four-spot laser fault injection setup may seem similar to four single-spot laser fault injection setups, but this is not the case. A laser spot on the die cannot be separated from another by more than the field of view of the objective lens since all laser beams must pass through it. Laser spot distance depends on the objective lens magnification and the minimal laser spot diameter. For instance, with a 20x magnification, the laser spots cannot be more than 500 μm apart. Therefore, if we place the targeted distributed logic elements further apart than this limit, they cannot be targeted simultaneously, thereby protecting against LFI.

VII. Defense-in-Depth Application

In this section, SPRED is used in a defense-in-depth application. The proposed spatially-distributed design can be combined with a detector to provide aggregated protection against single and multi-spot laser fault injections. In [8], [9], a compact sense-and-react IC-level detection-based countermeasure has been proposed. This sensor converts the laser-induced bulk current into voltage, raising the alarm on LFI detection. As shown in Fig. 11, the sensor comprises two parts: the front-end for current-to-voltage conversion and the back-end for the generation of digital alarm signals since the front-end input is connected to the bulk of the transistors.

Transistors provide bulk bias to logic when they are always on. An always-on transistor acts as a resistor to convert laser-induced current to voltage. The sensor's back end is driven by a common-source amplifier. An inverter latch produces the digital alarm signal upon activation of the front end. However, a multi-spot laser setup [10] can circumvent this sensor-based approach, as shown in Fig. 11 with the red laser spot. If an attacker has the capability of a multi-spot laser setup, she can attack both places simultaneously, forcing the alarm to give a false signal from high to low.

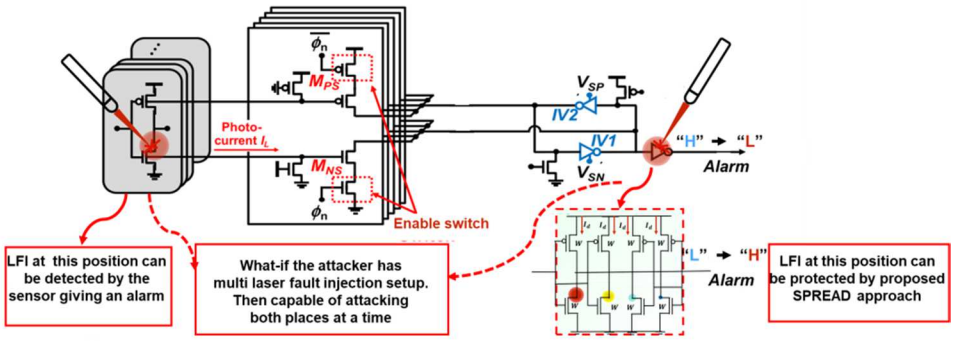

Fig. 11: Two-fold protection with SPRED safeguarding the sense-react detector [8], [9] in a multilayer-defense approach.

Our approach can help prevent an attack in this case. As we discussed in Section VI, we place the targeted logic gates (here, the alarm signal generator gate) further apart so that they cannot be targeted at the same time providing multi-layer protection against LFI. Thus, in a low-cost manner, we can prevent attacks on the detector circuit. In turn, the detector circuit will reliably send an alarm to trigger the zeroization of sensitive assets or self-destruction of the chip.

VIII. Conclusion and Future Work

In this paper, we presented a spatially-aware, multi-gate design methodology to implement a laser fault injection resistant design and evaluated its effectiveness using multiple security metrics. Based on simulations, we have concluded that the proposed countermeasure is effective. We also show that our approach is resistant to multi-bit faults and a multi-spot laser setup. In the near future, we will investigate the IR drop effect in the fault injection process, incorporating it into our threat model and verifying the resiliency of our proposed approach. We will examine the reduction in faults at the circuit level rather than the gate level for a more comprehensive analysis.

IX. Acknowledgements

This effort was sponsored in part by NSF under grant number 2117349. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

We also thank Minyan Gao and Md. Sazadur Rahman for their valuable advice in the implementation of this work using ICC2 and PrimeTime tools.

References

[1] 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.

[2] P. Loubet-Moundi, D. Vigilant, and F. Olivier, "Static fault attacks on hardware des registers," *Cryptology ePrint Archive*, 2011.

[3] M. Doulcier-Verdier, J.-M. Dutertre, J. Fournier, J.-B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant aes circuit working on duplicated complemented values," in *2011 IEEE International Solid-State Circuits Conference*. IEEE, 2011, pp. 274–276.

[4] T. G. Malkin, F.-X. Standaert, and M. Yung, "A comparative cost/security analysis of fault attack countermeasures," in *International Workshop on Fault Diagnosis and Tolerance in Cryptography*. Springer, 2006, pp. 159–172.

[5] E. Trichina and R. Korkikyan, "Multi fault laser attacks on protected crt-rsa," in *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2010, pp. 75–86.

[6] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic processors-a survey," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 357–369, 2006.

[7] J. G. Van Woudenberg, M. F. Witteman, and F. Menarini, "Practical optical fault injection on secure microcontrollers," in *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2011, pp. 91–99.

[8] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Experimental validation of a bulk built-in current sensor for detecting laser-induced currents," in *2015 IEEE 21st International On-Line Testing Symposium (IOLTS)*. IEEE, 2015, pp. 150–155.

[9] K. Matsuda, S. Tada, M. Nagata, Y. Komano, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, "An ic-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density," *Japanese Journal of Applied Physics*, vol. 59, no. SG, p. SGGL02, 2020.

[10] B. Colombier, P. Grandamme, J. Vernay, É. Chanavat, L. Bossuet, L. de Laulanié, and B. Chassagne, "Multi-spot laser fault injection setup: New possibilities for fault injection attacks," in *20th Smart Card Research and Advanced Application Conference-CARDIS 2021*, 2021.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] F. Schellenberg, M. Finkeldey, N. Gerhardt, M. Hofmann, A. Moradi, and C. Paar, "Large laser spots and fault sensitivity analysis," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2016, pp. 203–208.