Delfines: Detecting Laser Fault Injection Attacks Via Digital Sensors

Mohammad Ebrahimabadi, Suhee Sanjana Mehjabin, Raphael Viera, Sylvain Guilley, Jean-Luc Danger, Jean-Max Dutertre, Naghmeh Karimi

DELFINES: DETECTING LASER FAULT INJECTION ATTACKS VIA DIGITAL SENSORS

Mohammad Ebrahimabadi, *Student Member IEEE*, Suhee Sanjana Mehjabin, Raphael Viera, *Member IEEE*, Sylvain Guilley, *Senior Member IEEE*, Jean-Luc Danger, *Member IEEE*, Jean-Max Dutertre, *Member IEEE* and Naghmeh Karimi, *Senior Member IEEE*

***Abstract*—Laser Fault Injection Attacks (LFIA) are a major concern in physical security of electronic circuits as they allow an attacker to inject a fault with a very high spatial accuracy. They are also often considered by Information Technology Security Evaluation Facilities (ITSEFs) to deliver security certification, as Common Criteria, of embedded systems. Time or spatial redundancy can be foreseen as protection methods but they are costly and do not ensure immunity against multiple laser injections. The detection would be efficient if the detecting sensors meet enough density and sensitivity to cover the functional blocks being protected. Most sensors rely on analog and specific technology. In this paper, we propose a method to detect LFIAs via a fully digital sensor based on a Time to Digital Converter (TDC) and show its efficacy in detecting such faults in various conditions related to the current induced by the laser, the characteristics of the Power Grid Network (PGN) of the circuit and the environmental variables (voltage, temperature). The simulation results obtained using a 45nm Nangate technology confirms the high efficiency of the proposed scheme in detecting LFIAs in a large range of such conditions.**

I. Introduction

Thanks to the optimized performance and reduced power demands in the state-of-the-art electronic devices, billions of transistors can be embedded in a single chip. Such complexity calls for high security and reliability assurance against both unintentional and malicious device perturbations. The problem is exacerbated for the safety and security critical applications such as autonomous vehicles where a single compromise may be life threatening.

Fault Injection Attacks (FIAs), aiming at provoking system malfunction or leak sensitive data, are among the prominent vulnerabilities that threaten the security of devices by imposing voltage or clock glitches [1], [2], temperature change [3], body biasing injection [4], inducing parasitic currents via electromagnetic disturbances or intense light flashes [5], [6], and laser illumination attacks [7], [8]. Among all such attacks, laser attacks have received the lion's share of attention considering their focusable target. Indeed, owing to their high spatial and temporal resolutions, laser-induced FIAs (LFIA) allow to finely control the injected faults. Accordingly, in this paper, we focus on LFIAs and tailor an efficient countermeasure to detect such attacks.

When illuminating a target via laser shots, a parasitic current is generated in the point of interest which results in an undesired transient voltage. The effect of this toggling may propagate through the combinational paths and subsequently be captured by the related sequential elements. In practice, the adversary may benefit from such transient fault in bypassing a security process [9] (e.g., authentication), corrupting the data used to enforce security (e.g., privilege escalation in modern microprocessors), executing targeted operations inside the chip (e.g., skip or replace instructions [10]), toggling the value of a specific signal at runtime resulting an embedded cryptographic module to become compromised, e.g., leaks its encryption/decryption keys [11].

In practice, thanks to the miniaturization of transistors in the state-of-the-art technologies, laser illumination does not only affect the targeted point; rather it also results in a transient drop of supply voltage, the so-called IR drop [12]. Depending on the significance (i.e., magnitude) of the imposed IR drop timing violations may or may not occur in the other paths of the circuit as well [13]. A recent paper by Viera et al. [14] also confirms that the LFIAs manifest as the complex combination of global and local effects across the chip. This effect is referred to as "glocal". Accordingly, to detect the LFIAs, the power source can be monitored during the circuit runtime regarding the occurrence of such IR drops. One such monitoring can be provided with the Time-to-Digital Converters (TDC); the so-called Digital Sensors hereafter.

Being portable among different technologies (due to solely composing of digital standard cells), being devoid of costly calibration requirements, being sensitive to voltage and temperature altogether (not as individual entities), as well as featuring high accuracy and resiliency against removal attacks, make the digital sensors a promising solution over their analog counterparts [15]. In practice, digital sensors have been shown to be highly effective in detecting timing and environmental attacks such as clock skew attacks (ClkScrew [16], Hertzbleed [17]), temperature attacks [18], voltage attacks (PlunderVolt [19], VoltJockey [20]–[22], VoltPillager [23]), mixed timing+temperature [24], and timing+voltage attacks [25].

This paper moves one step further and uses such DSs in detecting LFIAs and *demonstrate their high efficiency in detecting such attacks in different voltage and temperature combinations as well as different characteristics of the PGN.*

M. Ebrahimabadi, S. S. Mehjabin, and N. Karimi are with the Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD 21250, USA (e-mail:{e127, suheesm1, nkarimi}@umbc.edu).

R. Viera and J.-M. Dutertre are with École des Mines de Saint-Étienne, France (e-mail:{raphael.viera, dutertre}@emse.fr).

S. Guilley and J.-L. Danger are with the Think Ahead Business Line of Secure-IC S.A.S. & Institut Polytechnique de Paris, France (e-mail: firstname.lastname@{secure-ic.com, telecom-paris.fr})

Our contributions include:

- A simple model representing the impact of LFIAs in the targeted circuit;
- A methodology to effectively detect the LFIAs during the circuit runtime;
- Extensive HSpice simulations to extract the miss and false alarm rates for the considered FIAs;
- A thorough investigation of how our sensor reacts in different temperature and voltage conditions in presence of an LFIA;
- Studying the impact of characteristics of the power grid network on the attack detection;
- Extracting the sensitivity of the deployed sensor and in turn the proposed methodology to the environmental changes when no attack has been launched.

Please note that digital Sensors, and in particular TDC sensors, have been already used for detecting faults in attacks that have large impacts, e.g., glitches on power supply [26]. However, in this paper we target the laser fault injection attacks where the target point is as small as a logic gate.

Threat Model: We assume that the adversary uses focused laser shots to inject transient faults which toggle the value of the targeted points. We show that such transient faults are detected using the proposed sensor-based countermeasure; thanks to its indirect impact on the Vdd (i.e., laser-induced IR drop).

Even if the sensor components are illuminated unintentionally by the LFIA whose target was the main circuit, our sensor still detects the attack. Thereby, our detection scheme is "glocal" although the fault injection is local (targeted).

Outline: The rest of this paper is structured as follows. Section II discusses the related work on detecting fault injection attacks. Section III presents a preliminary background on laser FIAs and their impacts on the targeted circuit. The deployed sensor and its characterization are also discussed in Section III. Section IV presents the proposed fault detection scheme. Experimental setup and results are presented in Section V. Finally, conclusions and future directions are drawn in Section VI.

II. Related Works

Several sensor-based fault detection schemes have been proposed in the recent literature, e.g., Deshpande et al. [27] presented a sensor based on dual-complementary flip-flops to detect ElectroMagnetic-induced Fault Injection Attacks (EMFI). Although highly accurate, the proposed method suffers from significant hardware overhead as their detector needs to be implemented for every net of the target circuit. El-Baze et al. [28] also proposed a fully digital sensor benefiting from sampling flip-flops to detect EMFIs that change the expected values captured by the sampling flip-flops. To protect the chip, such a sensor is placed in several parts of the chip; thus imposes high area-overhead.

A PLL-based sensor to detect EMFI was proposed in [29]. In this method a number of Ring Oscillators (RO) are embedded in the circuit where their phase is affected by the EMFIs. Such phase change is then captured via an embedded PLL. This method also imposes high hardware and power overhead. A Hogg phase-detector is deployed in [30] to raise an alarm when an EMFI fault is injected in the system. Here the phase of an embedded RO is changed when an EMFI is launched. Although featuring a high detection rate, it unfortunately also suffers from a significant false alarm rate. The authors of [31] replace such a PLL-based sensor with a Ring-Oscillator based counterpart. Although their sensor acquires high fault detection rate but it suffers from high latency in detecting the faults.

To detect probing attacks, [32] presents a resonant-based sensor. Such attack results in a mutual inductance that changes the total inductance of the sensor, and in turn the sensor resonance frequency. This change can be detected by an embedded counter. This sensor has information leakage [33]. Hence by solving one problem, the countermeasure opens another vulnerability.

Bulk Built-In Current Sensor (BBICS [34], [35]) is an analog sensor capable of detecting transient faults. The essential idea of BBICS is the connection of integrated current sensors to the bulks of the target transistors under monitoring. This allows the detection of a broader range of transient faults than conventional built-in current sensors, which are otherwise coupled up to the sources of the monitored transistors. BBICS has a limited area of detection, hence several instances have to be embedded. Analog sensors nevertheless require an accurate trimming strategy, as they might depend on the fabrication process. Moreover, analog sensors might have characteristics which differ from chip to chip. Therefore, maintaining a given detection rate across chips is a challenge.

To detect the voltage glitch attacks, Zussa et al. pair a sampling D flip-flop with a delay element to generate a shifted clock. This shifted clock feeds the clock signal of the sampling flip-flop whose D input is the system clock. The flip-flop output raises an alarm in case of EMFI [36]. Similar to BBICS, a single sensor cannot cover the whole circuit. Thus, several sensors need to be embedded in a regular mesh. In other words, a single sensor covers efficiently a reduced area, and even if several sensors are embedded in the circuit still some faults may escape detection.

A custom-design laser fault detection was proposed in [37]. The method suffers from portability among different technologies and Process Design Kit (PDK) libraries. Moreover, it has not been yet tested experimentally.

Concurrent Error Detection (CED) schemes can be also used to detect LFIAs. Among them, hardware-redundancy based schemes such as Dual Modular- (DMR) and Triple Modular-redundancy (TMR) [38], [39] impose a significant hardware overhead. Time-redundancy based methods (e.g., [40]) perform each operation twice; hence significantly increasing the circuit latency and power consumption. Guo et al. presented a time-redundancy based scheme [41] that computes the operations twice selectively. This imposes less overhead compared to [40] yet may result in higher fault escapes. Information-redundancy schemes (e.g., [42]) either have a low detection rate or impose high overhead. To detect and correct the variation-induced delay errors, the authors of [43] proposed Razor II. This method detects clock glitching but is not detecting LFIAs.

III. Preliminaries

A. Laser-Based Fault Injection Attacks and Their Impact on the Targeted Chip

Integrated Circuits (ICs) are known to be sensitive to laser illumination: a laser beam passing through the device creates electron-hole pairs along the path of the laser beam (due to the so-called photoelectric effect [44]). These charge carriers, when induced in the vicinity of reverse biased PN junctions: the places in an IC where strong electric fields exist, are put into motion by this electric field generating transient currents through the targeted gate (the reverse biased junctions are the most laser-sensitive part of circuits) [45]. The polarity, amplitude, and duration of the induced transient current change based on the laser shot energy and location as well as the device technology, supply voltage, and output load. The nature of these currents was first studied in the case of radioactive particles [46]–[50].

The impact of laser illumination on an inverter is shown in Fig. 1. As depicted, the laser shot generates photocurrents (i.e., I_{gate}) at gate level. Indeed the laser-sensitive part of a gate is the drain of its OFF transistors where there is a reverse biased PN junction between the drain and substrate. Accordingly, if the inverter (depicted in Fig. 1) is fed with '1', an induced transient current (I_{gate}) flows from the substrate of the PMOS (here Vdd) to its drain (i.e., the inverter output). Thereby, the output capacitance is being charged via I_{gate}, resulting in the toggling of the inverter output to '1'; thus a so-called transient voltage-change occurs. Similarly, when the inverter input is low the laser-induced I_{gate} flows between the NMOS transistor's drain and GND (ground) which in turn participates in discharging C_{Load} and switching the output value to '0'.

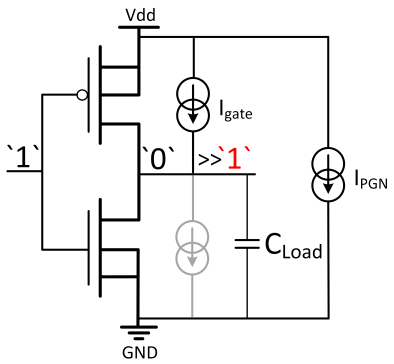


Figure 1. Laser-induced transient fault model (applied to an inverter with input biased at '1'). The model takes into account the supply voltage drop/bounce (IR drop) induced by the I_{PGN} parasitic current [14].

When illuminating with laser, not only the I_{gate} current is induced in the targeted net (as discussed above), but also a transient current (so-called named I_{PGN}) flows directly from Vdd to the ground. This current is induced in the reversed biased $Psub$-$Nwell$ junction that surrounds every $Nwell$. In other words, even if the laser beam is directed toward a sensitive NMOS transistor, it also induces charge carriers that will be sufficiently close to a $Psub$-$Nwell$ junction to induce the transient current I_{PGN}. This current has no direct effect on the gate output as it draws from the gate's power grid network (PGN). As a result, the targeted gate power supply (Vdd) undergoes an IR drop and its ground supply experiences a ground bounce. Furthermore, as neighboring cells are subject to similar transient currents, their effects add up and can propagate to distinct cells via the PGN. Indeed I_{PGN} current can have a significant effect on the fault injection mechanism as by itself it can result in timing errors (timing constraint violations) or even data disruptions leading to sampling erroneous values by D flip-flops. The laser-induced transient fault model used in this work was experimentally validated in a commercial FPGA by Viera [51] (cf. [14] for a shorter version).

If the inverter of Fig. 1 is part of a larger combinational logic block, the voltage drop can propagate through the logic toward the input of memory cells (registers or latches) and flip the correct output of a register.

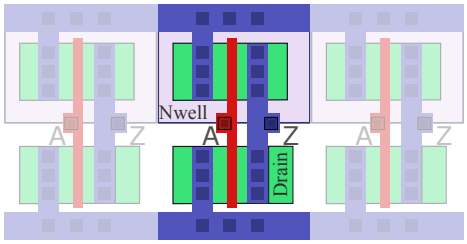


Figure 2. Generic layout of a CMOS inverter showing the size of the PMOS' Nwell layer and the NMOS drain. The inverter is surrounded by other cells that may contribute to the generation of transient currents.

The amplitude of I_{PGN} relates to I_{gate} via $I_{PGN} = N \times I_{gate}$ where N follows Eq. 1. In this equation, $Area_{NWell}$ (related to I_{PGN}) is the total area of the illuminated Nwell PN junctions and $Area_{drain}$ (related to I_{gate}) is the total area of the illuminated NMOS or PMOS drain. In practice, the I_{PGN} current is usually larger (10x or more) than the I_{gate} since the drain area is significantly smaller than the Nwell's area as illustrated in the sample layout in Fig. 2.

$$N = \frac{Area_{Nwell}}{Area_{drain}} \tag{1}$$

B. Time-to-Digital Converter

Time-to-Digital converters (*so-called digital sensors hereafter*), have been used in recent years to sense environmental conditions, e.g., temperature and voltage, in embedded systems [52]. Such sensing is essential for safety and security provision by preventing failures or detect attacks. The FIAs imposed by clock glitching can be also detected by these sensors [53]. In practice, portability among different technologies, low-cost calibration, and high failure-detection rate, make such sensors impressive compared to their analog counterparts.

The TDC-based digital sensors can be realized via inserting artificial critical paths (as simple as delay chains) into the chip logic such that if the chip is operated in abnormal conditions, setup time violations occur on the sensor's intentionally long paths beforehand [54]. In these sensors, instead of quantifying the propagation time, it is checked if the transition feeding the corresponding delay chain manages to propagate to the

end of the delay chain at the considered frequency. As will be discussed later, we use such a sensor for detecting LFIAs in this paper.

The architecture of the digital sensor used in this paper is depicted in Fig. 3. The circuit includes n_0 leading inverters followed by n_1 inverters each feeding a D flip-flop (DFF). The first leading inverter is fed with a Toggle flip-flop. All flip-flops operate under the same clock which feeds the targeted circuit as well. Such strategy allows to minimize the area overhead, as the sensor sensing area is reduced to its minimal structure. Depending on the operating conditions (i.e. voltage, temperature) and system frequency, the setup time violation occurs in a different flip-flop. The index of this flip-flop is used to characterize the sensor as discussed below. In our case, without loss of generality, we consider the S-Box of PRESENT cipher as the circuit targeted by FIA (shown in the upper part of Fig. 3). The role of the sensor is then to monitor any laser-induced current resulting from this FIA, and raise an alarm accordingly.

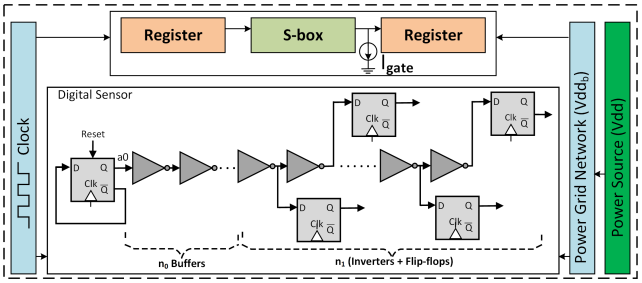
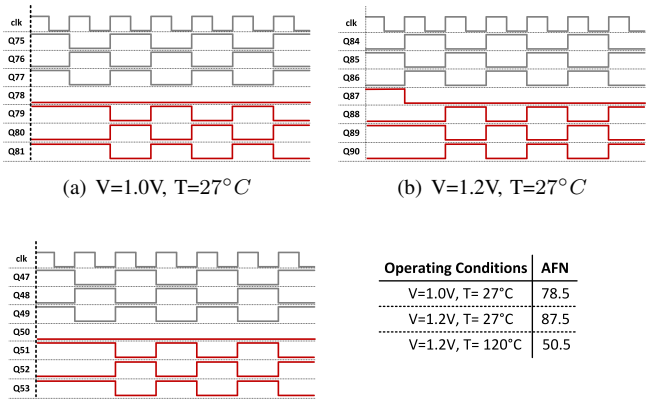


Figure 3. Architecture of the sensor-integrated target system.

During runtime the toggle flip-flop feeds a continuous pulse to the sensor. This pulse feeds each DFF with an image of the clock (or its toggled version) at halved frequency. In each clock cycle i, denoted as CC_i, if there were no setup time violation, each two consecutive DFFs would experience opposite phases, i.e., one of them would be in the phase of A (say '0' $\rightarrow$ '1' $\rightarrow$ '0' $\rightarrow$ ...) and the other in the phase of $\bar{A}$ (say '1' $\rightarrow$ '0' $\rightarrow$ '1' $\rightarrow$ ...). However, owing to the propagation delay through the delay chain, in practice a setup time violation occurs in the delay chain in each CC_i. This results in DFF $K-1$ and DFF K (where K changes based on operating conditions and clock frequency in each clock cycle CC_i) experience the same phase; instead of opposite phases. In this case, K which is the index of the *first* DFF that exhibits the same phase as its predecessor is extracted and used to characterize the sensor outcome. We refer to this index in each clock cycle CC_i as FN_i and the average of all FN_is over a number of clock cycles as AFN. When the circuit operates in slower conditions (e.g., lower voltage, higher temperature), the AFN index is lower, and when it operates in faster conditions the AFN value increases. This qualifies AFN to be used for sensing operating conditions.

Fig. 4 shows sample waveforms for the sensor of Fig. 3 in different (V, T) combinations as well as the related AFN values. The waveforms extracted from the sensor with n_0 =10 leading inverters followed by n_1 =115 buffers and flip-flops. As expected, the slower the circuit (due to voltage and temperature conditions) the lower the AFN.



(a) V=1.0V, T=27°C (b) V=1.2V, T=27°C

(c) V=1.2V, T=120°C

Operating Conditions	AFN
V=1.0V, T= 27°C	78.5
V=1.2V, T= 27°C	87.5
V=1.2V, T= 120°C	50.5

(d) AFN of Fig. 4(a), 4(b), 4(c)

Figure 4. Waveforms of Fig. 3 depicting the output of the embedded flip-flops in different voltage and temperature combinations. In each figure, the X-axis represents the time and the Y-axis shows the voltage of the considered flip-flops.

IV. Proposed LFIA Detection Scheme

To be able to detect LFIAs, the digital sensor discussed in Section III-B is embedded along with the target circuit in the chip as depicted in Fig. 3. In this research, we selected the S-Box module of PRESENT cipher as the target circuitry. As discussed earlier, the outcome of the sensor (FN) is affected when the sensor is operated under different operating conditions, e.g. increasing voltage or decreasing temperature results in increasing FN index. We benefit from this observation to detect laser-induced FIAs as these faults result in the change of the sensor's voltage.

In practice, as mentioned in Section III, when the target circuit is attacked by laser illumination, not only the voltage level of a gate illuminated by the laser spot is changed but also the effect of this change propagates to a broader extent of the circuit as IR drop. This IR drop leads to a droop in the power supply of the target circuitry which in turn is detected by the digital sensor due to the change of its FN value. Accordingly, in our detection scheme, the outcome of the sensor, i.e., FN index, is monitored during runtime of the circuit in each clock cycle, and if the FN change is beyond a specific threshold (will be discussed later), an alarm is raised. *Considering the similarities of the proposed method in detecting faults and the mechanism that dolphins exploit to detect objects in oceans, we name our proposed method as Delfines (the spanish translate of dolphins). Indeed both the proposed method and dolphins detect an object based on its echo, for our case the object is a laser attack and the echo is the change of I_{PGN} due to such an attack.*

The parasite model of Power Grid Network (PGN) is shown in Fig. 5. In this model the effect of laser shot illumination is modeled with the current source I_{PGN} in the power grid network. Here Vdd is the power source of the chip and Vdd_b is the effective power including the effect of the IR drop-induced voltage that the circuit is fed with. During the

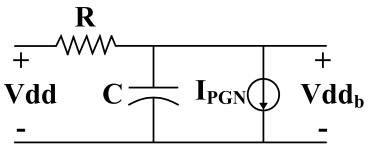


Figure 5. RC circuitry modeling the laser-induced IR drop.

normal operation, i.e., in the absence of any laser illumination, $Vdd_b \approx Vdd$. However, the circuit is experiencing a drop in its effective power supply as a consequence of laser illumination ($Vdd_b < Vdd$). As mentioned in Section III, the laser illumination results in the I_{gate} current in the target point of fault injection, and based on the practical observation in [51] this induced current goes along with a current flowing from Vdd_b to ground through the target Nwell-Psubstrate junction: I_{PGN}. This current downgrades the performance of the PGN and can be modeled by $I_{PGN} = N \times I_{gate}$. In other words, even the portions of the circuit that were not directly under attack are affected by such illumination. Indeed, in the absence of faults $I_{gate} = I_{PGN}$=0.

As long as there is no illumination in the circuit, the IR drop-induced voltage, Vdd_b, is only affected by the PGN and can be assessed based on the Equation 2. However, in the present of LFIAs the $Vdd_b(faulty)$ follows Equation 3.

$$Vdd_b = Vdd \cdot (1 - e^{-\frac{t}{R \times C}}) \approx Vdd \tag{2}$$

$$\begin{aligned} Vdd_{b(faulty)} &= (Vdd - R \times I_{PGN}) \cdot (1 - e^{-\frac{t}{R \times C}}) \\ &\approx Vdd - R \times I_{PGN} \end{aligned} \tag{3}$$

The differences between the above two equations reveal that the voltage drop due to the fault injection attack is $R \times I_{PGN}$. This droop in voltage results in a decrease of FN index in the embedded sensor as the sensor is fed with the same power source. To detect the attack, the FN value is monitored in each clock cycle i to check if $FN_i - FN_{i-1}$ goes beyond a predefined threshold value, and if so an alarm is raised. Following this scheme would result in a high attack detection rate, yet also a high false alarm rate in noisy environments where the voltage may change (even in the absence of LFIA). Thereby, to decrease the false alarm rate while having a high detection rate we use the average FN over a number of clock cycles (say the previous CC clock cycles) instead of FN_{i-1} and followed Equation 4 and Equation 5 to decide about raising alarms when needed. This differential method of fault detection (the differences between FNs over the time) removes the influence of noise induced from other circuits embedded in the System-on-Chip on the targeted circuitry. Being differential allows our sensor framework to be resilient against process variations as we always compare the outcome of the sensor in one clock cycle with the outcome of the same sensor in previous cycles.

$$AFN_{i-1} = \frac{1}{CC} \sum_{j=i-CC-1}^{i-1} FN_j. \tag{4}$$

$$Alarm = \begin{cases} \text{'1'} & \text{when } \lceil FN_i - AFN_{i-1} \rceil \geq TH \\ \text{'0'} & \text{otherwise} \end{cases} \tag{5}$$

Accordingly, In this paper, we consider the average of FN values (called AFN) over the last 8 clock cycles (i.e., $CC = 8$) and the threshold value to raise an alarm as 2 (i.e., $TH = 2$). As will be shown through our experimental results, our configuration results in a very low false alarm and a highly promising rate of fault detection. Note that to compute the running average of the last CC values of FN, we do not need to save them individually.

Also it is noteworthy to mention that some sensor's components may have been located close to the attacker's target point. In this case, there is a possibility of injecting faults in the sensor as well. However, this results in the change of the FN value as a direct consequence of laser illumination. Accordingly, in this scenario the sensor can still detect the fault. This confirms the efficiency of DELFINES schemed.

V. Experimental Results and Discussions

A. Experimental Setup

We targeted the S-Box of the PRESENT cipher, and implemented the sensor and S-Box at transistor level using a 45nm NANGATE technology. We used HSpice for the simulations. Our sensor includes n_0=10 leading inverters and n_1=115 sampling flip-flops and related inverters. The sensor dimensioning (to determine n_0 and n_1 during the design phase based on the device spec and operating range) was performed based on [15]. Please note that we used 45nm NANGATE technology as a proof of concept in this paper. However the proposed LFIA detection method is also applicable on the newer technologies.

We considered the voltage $V^* = [-0.65, 1.4]$V (step 0.05V), temperature $T^* = [-10, 150]$°C (step 5°C), $R^* = [1, 100]\Omega$ (step 10Ω), and $C^* = [2, 20]$ pF (step 2pF). We assume that the adversary insists on inducing a failure in S-Box in each case as otherwise the attack is not successful. Thus we estimate the minimum fault intensity (i.e., the value of I_{gate}) in each (V, T, R, C) $\in V^* \times T^* \times R^* \times C^*$ combination using our Hierarchical Linear Regression (HLR) scheme discussed below.

As mentioned the IR drop induced current (I_{PGN}) is significantly greater than I_{gate}. Thus, to investigate the implemented sensor detection capability in the worst condition, N is considered as 10 (in $I_{PGN} = N \times I_{gate}$) based on [14]. As discussed earlier, N is computed based on the area of Nwells and drains of transistors illuminated by the laser. This ratio can be computed by analyzing standard cells' layouts in the `.lef` format, and the placed and routed netlist.

In this paper, we considered a transient fault model that toggles the targeted signal (to resemble the laser illumination effect in real-silicon experiments). We considered a 8ns duration for laser illumination. Please note that the adversary should inject the fault in the time-frame that the sequential logic captures the output of combinational logic. Without loss of generality, we targeted the Least Significant Bit (LSB) of the S-Box for our fault injection while the S-Box is fed with

the input that results in a '1' in its LSB output in case of no-fault. The other bits of the S-Box will exhibit similar results as well.

Tuning I_{gate}: The I_{gate} current induced due to laser illumination toggles the targeted point if its intensity is high enough. To mimic the attacker's behavior in inducing a laser-induced failure, in our simulation we extract the minimum value of I_{gate} required to toggle the output. Finding the minimum I_{gate} to induce the failure in each (V, T, R, C) $\in V^* \times T^* \times R^* \times C^*$ is not possible via HSpice simulations as we have 58,080 such cases in our experiments. Thus, we deploy the HLR-based scheme shown in Fig. 6 to find minimum I_{gate} in each case.

Step0: V^*= {0.65,0.7,...,1.4}V
C^* = [2,20]pF (step 2pF), C_R = {2}pF
T^* =[−10, 150]°C (step 5 °C), T_R ={−10, 80, 150}°C
R^*= [1,100]Ω (step 10Ω), R_R = {1, 50, 100}Ω,
Step1: Measure I_{gate} in HSpice, for all $(V,T,R,C) \in V^* \times T_R \times R_R \times C_R$
Step2: $T \leftarrow -10$°C, $V \leftarrow 0.65$V, $C \leftarrow 10$pF; Assess I_{gate} for all (V,T,rx,C) using HLR based on I_{gate} for all (V,T,R,C) of Step1 where $rx \in R^* - R_R$
Step3: Repeat Step2 for all $V \in V^*$
Step4: Repeat Step2&3 for T = 80°C and T =150°C
Step5: Repeat Step2&3&4 for all $T \in T^* - T_R$
Step6: Repeat Step1-5 for the other values of $C \in C^* - C_R$

Figure 6. Finding minimum I_{gate} in each (V, T, R, C) point.

- **Step1:** Measure I_{gate}, by using HSpice, for all combinations of (V, T, R, C) where:
  $V \in V* = \{0.65V, 0.7V, ..., 1.4V\}$,
  $T \in T_R = \{-10^oC, 80^oC, 150^oC\}$,
  $R \in R_R = \{1\Omega, 50\Omega, 100\Omega\}$,
  and $C_R \in C* = \{2pF\}$.
  Figure 7(a) shows a snapshot of what needs to be measured for $T = -10^oC$. The same table should be generated for the other two temperatures (here we did not show all voltage steps for the sake of space).
- **Step2:** Set $T = -10^oC$, $V = 0.65V$, $C = 10pF$. Then use HLR to assess I_{gate} for all combinations of (V,T,rx,C) based on the I_{gate} values measured in Step1 where rx includes the resistance values that were not considered in Step1 (e.g., 10Ω, etc.).
- **Step3:** Repeat Step2 for all $V \in V*$ (Figure 7(b) shows the result of the regression in black for the data gathered in this step).
- **Step4:** Repeat Step2 and Step3 for $T = 80^oC$ and $T = 150^oC$.
- **Step5:** Repeat a very similar process to find the I_{gate} in each voltage and resistance combination for the cases whose related temperature is not included in T_R by performing linear regression on the I_{gate} values related to $C1 = 10pF$ and the same voltage and temperature.
- **Step6:** Repeat Step1-Step5 for the other values of C which is not included in C_R.

Our experimental results showed that the minimum I_{gate} values extracted using the above algorithm has enough intensity to toggle the targeted output in all considered (V,T,R,C) combinations. As will be shown in Fig. 12 and Fig. 13, our extensive experiments using 58,080 quadruples of (V,T,R,C) values confirmed that our deployed regression scheme has high accuracy in pinpointing the value of I_{gate} needed to inject a fault. Indeed, in all cases we see that using the I_{gate} value extracted by our regression method, we can successfully inject a fault. Also as we will discuss in Section V, *considering the value of I_{gate} (as we extracted using the above method) is for the benefit of the attacker, i.e., here we considered the best case for the attacker, and the worst case for our defensive fault detection scheme*. However as will be shown through the extracted results in Section V, our detection scheme performs very well even in such a case.

Voltage (V)

Resistance(Ω)	0.65	0.80	0.95	1.10	1.25	1.40
1	130	213	300	390	483	580
10	---	---	---	---	---	---
20	---	---	---	---	---	---
30	---	---	---	---	---	---
40	---	---	---	---	---	---
50	90	160	230	310	380	450
60	---	---	---	---	---	---
70	---	---	---	---	---	---
80	---	---	---	---	---	---
90	---	---	---	---	---	---
100	70	125	181	237	293	350

(a) Collecting I_{gate}

Voltage (V)

Resistance(Ω)	0.65	0.80	0.95	1.10	1.25	1.40
1	130	213	300	390	483	580
10	121	202	285	374	463	553
20	112	190	270	358	441	525
30	103	179	256	341	420	499
40	96	169	242	325	399	473
50	90	160	230	310	380	450
60	84	151	218	294	361	427
70	79	143	207	279	343	406
80	75	136	198	265	325	386
90	72	130	189	251	309	367
100	70	125	181	237	293	350

(b) I_{gate} after regression

Figure 7. Inferring minimum required I_{gate} based on measuring I_{gate} of corner cases. The values have been shown for the temperature of -10°C.

Fig. 8 depicts the values of I_{gate} in different conditions, extracted using the algorithm of Fig. 6. In higher voltages and lower temperatures, the attacker needs to induce a higher I_{gate} to force an output toggling since the ON transistors that set the output voltage of the targeted bit (say Y_0) are capable of driving a higher current (that has to be offset by I_{gate}). Moreover, when the PGN exhibits a lower resistance, there is less IR drop thus higher I_{gate} is needed to induce failure. The capacitance value did not have a visible impact on the required I_{gate} value; not shown here for the sake of clarity.

B. Experimental Results and Discussion

1) Laser Illumination Induced Impacts on the S-Box and Sensor Circuitries: Fig. 9 depicts the impact of LFIA on both the circuit (S-Box) and sensor. As shown, due to the laser illumination (I_{gate} value), the S-Box Least Significant Bit (Y_0) toggles from '1' to '0'. Moreover, Vdd_b experiences a drop that can be sensed by our sensor. As shown, the FN index was 48 before FIA as the 48th Flip-Flop in our sensor named as Q48 experiences a violation (shown in blue), i.e., its output is not the inverse of Q47. However, due to the change of Vdd_b, this index reduces to 44 after the FIA (shown in red). The takeaway from this observation is that our sensor can detect the laser attack by observing the change of its FN.

To show the impact of laser illumination in more detail, Fig. 10 illustrates the magnitude of IR drop ($Vdd - Vdd_b$) in T = 80°C and $Vdd \in \{0.65V, 1.0V, 1.4V\}$ for different combinations of (R, C) when a fault is injected. As shown, for higher values of resistance, the drop is more significant. This is in contrast to the effect of capacitance in the PGN where by increasing C the circuit experiences less IR drop. Another observation that can be made from these heatmaps relates to the IR drop occurring under different voltages. As depicted, the higher the Vdd value, the more the voltage drop. This is due to the increase of I_{PGN} in higher voltages (linked

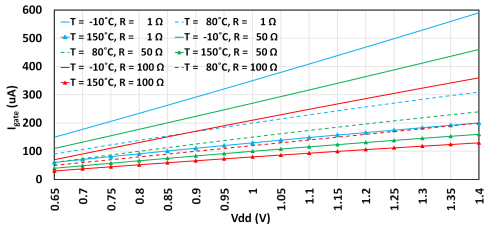


Figure 8. I_{gate} values injected in different (v, t, r). Here c = 10 pF.

to the requirement of using a higher I_{gate} to inject a fault, see Fig. 8). Note that even when no fault is injected (not shown for the sake of space) the circuit experiences an IR drop, yet negligible compared to the cases where a fault is injected. Moreover, the higher the Vdd, the more the voltage drop.

Faulting the S-Box output requires a laser-induced I_{gate}. This in turn is accompanied with a significant I_{PGN} and its related IR drop. The sensor can sense this IR drop and raises an alarm. The minimum intensity of the fault required to launch a successful attack is affected by the PGN factors and circuit's operating conditions.

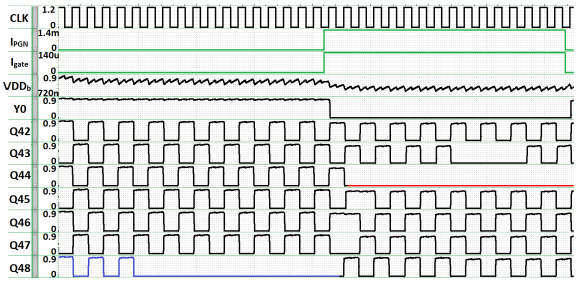
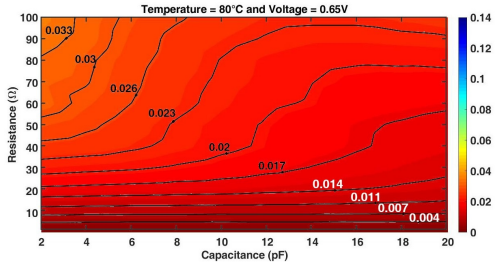


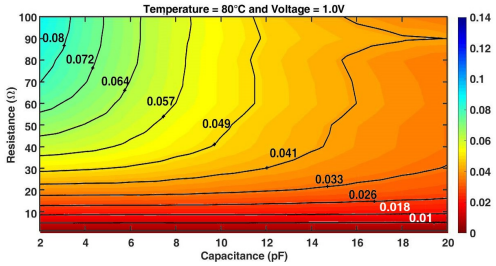
Figure 9. S-Box and Sensor signal waveform for $V = 1V$, $T = 80$°C, $R = 50\Omega$ and $C = 10pF$. In this figure, the X-axis represents the time.

2) The Effect of Environmental Conditions on the Sensor's Outcome: Fig. 11 depicts how the sensor outcome is affected in different operating voltage and temperature. As expected, when the system operates in slower conditions, i.e. in high temperature and low voltage, the AFN is lower than when running in fast conditions. These results confirm that the deployed sensor is simultaneously sensitive to the voltage and temperature. Fig. 11(a) depicts the AFN values when no fault is injected and Fig. 11(b) shows the related AFN values during the fault injection period. Comparing the AFN values in these two figures vis-a-vis confirms that laser illumination on the S-Box affects the sensor outcome. Indeed the laser illumination results in an IR drop causing the system to become slower. Consequently, the AFN value is decreased and such AFN change can be detected by the sensor. For example, in T = 80°C and Vdd 1.05V the AFN value is 51 when no fault is injected while this value decreases to 47 after the fault injection. The takeaway point from these observations is that our sensor outcome is affected by the laser illumination although the adversary does not target the sensor directly and rather he targets the circuitry of interest (S-Box in this paper).

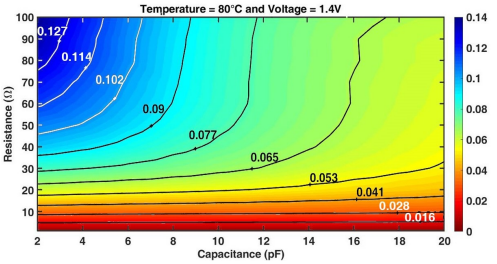
3) Detection Rate of the Laser-induced Faults: This set of results demonstrates the detection rate of our sensor when a laser-based fault injection attack is launched on the targeted S-Box. We have extracted the results for the whole range



(a) Vdd=0.65V



(b) Vdd=1V

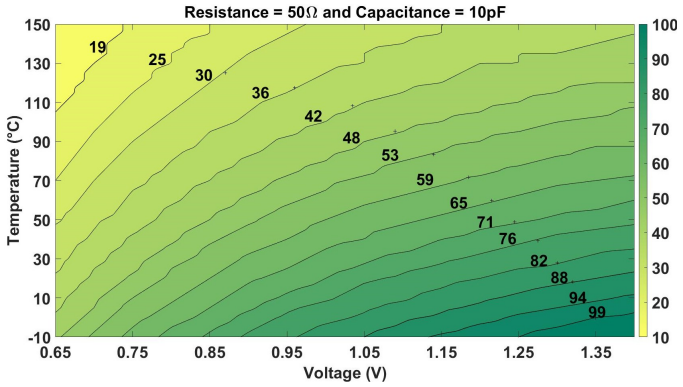


(c) Vdd=1.4V

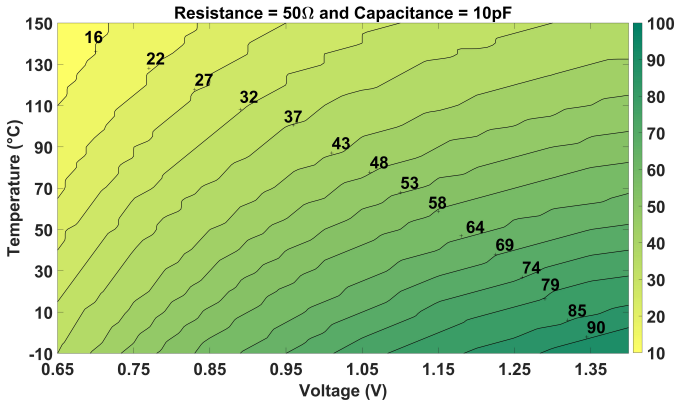
Figure 10. The heatmaps of voltage drop (i.e., $Vdd - Vdd_b$) in different (R, C) combinations and Vdd values. Here $T = 80°C$. The unit for all voltage values shown in these figures is volt.

of (R,C,V,T) discussed in Section V-A; totally 58,080 cases. Figure 12 depicts the cases for the whole considered range of R, C and Vdd when $T \in \{-10, 80, 150\}C$. As shown, the escapes (i.e., missed alarms) are mainly related to the case of R=1Ω. This is due to the low IR drop occurring in very low resistances. Although in the case of R=1Ω, I_{gate} is sufficient to toggle the targeted S-Box output, the induced effect on PGN (i.e. value of I_{PGN}) is not large enough to be sensed by the sensor.

Another observation that can be made from Fig. 12 is that by increasing the temperature, the missed alarm rate increases. For example, at -10°C, the sensor detects $\approx$ 91% of the faults while the detection rate is around 81% at 80°C. This is also due to the fact that in higher temperatures the circuit operates slowly; thus the attacker is able to toggle the targeted point by inducing a lower I_{gate}. Such low I_{gate}, as also mentioned above, results in a lower I_{PGN} and thus the fault can escape being detected by the sensor; resulting in a missed alarm. We can observe the same trend in case of low voltages as again the circuit operates slower in these cases so the attacker can prevent fault being detected by inducing a very low I_{gate} that changes the S-Box output yet cannot be sensed by the sensor. Recall that as mentioned in Section V-A, in this paper we



(a) No fault has been injected



(b) After fault Injection

Figure 11. AFN values without and with laser illumination (so that a fault is injected) in different (V, T) combinations where R=50Ω and C=10pF.

considered the best case for the attacker, i.e., toggling the S-Box output with minimal laser injection effort (i.e., minimum I_{gate}). However, if the attack intensity increases by increasing the illumination, the fault is detected even in the slowest circuit operating conditions. **Thus, here we are showing the Best case for the attacker and the worst case for our defensive fault detection scheme**.

Figure 13 portrays the sensor detection outcome for different combinations of R, T and Vdd where $C{\in}\{2, 10, 20\}pF$. As depicted, the effect of capacitance is peripheral. For $C = 2pF$, the fault detection rate is around 80%. This rate increases to ≈81% when the capacitance is $20pF$. This concludes that the effect of capacitance is marginal in terms of the sensor outcome. **Recall that our sensor does not fire any false alarm related to an insufficient illumination** (i.e., a weak laser attack that does not affect the S-Box output) as in each experiment we induce the minimum I_{gate} (found based on Tuning $\mathbf{I_{gate}}$) that toggles the targeted S-Box output.

4) Impact of Layout on the Attack Detection Rate: As mentioned in Sec. IV, LFIAs result in an IR drop in the power grid network. This is sensed with our sensor. The amount of such side-effect (change of I_{PGN} due to the intensity of fault, i.e., the amount of I_{gate}) depends on the circuit layout, in particular the area of Nwells and the area of drains of transistors illuminated by the laser. In this paper, as pointed out in Sec. V-A, we considered a factor of N=10 between I_{PGN} and I_{gate} (i.e., $I_{PGN} = 10 \times I_{gate}$) based on standard cells that build up our circuit [14]. However, to show the impact for higher/lower N values, we also conducted HSpice simulations for N=8 and N=12. Based on their applications, chips are usually designed in different temperature grades under which the chip is expected to be functional. Tab. I shows our LFIA detection rate for each of these grades, each for three values of N, in particular for T∈[0°C,70°C] in commercial grade, T∈[-10°C,85°C] for Industrial Grade and T∈[-10°C,125°C] for Military Grade.

For the sake of completeness, we considered $R \in [1\Omega, 100\Omega]$, but in real circuits the R value related to the PGN is higher than 1Ω as Viera [51] showed that the minimum value of R is around 10Ω for a typical-sized circuit. Thus, in Table I, we show the FIA detection rate for $10\Omega{\leq}R{\leq}100\Omega$ as well. Note that the lower the R, the less the detection rate. Thus by considering R=1, we targeted a worst case scenario for our detection, yet showed our method still works well in this case. As depicted, for the commercial and industrial grades we detect over 95% and for military grade over 91% of the faults for $10\Omega{\leq}R{\leq}100\Omega$ when N=10. As expected, the detection rate slightly changes for other N values; the higher the N the more IR drop and thus higher detection rate. The takeaway point from these observations is that the deployed sensor can effectively detect the LFIAs.

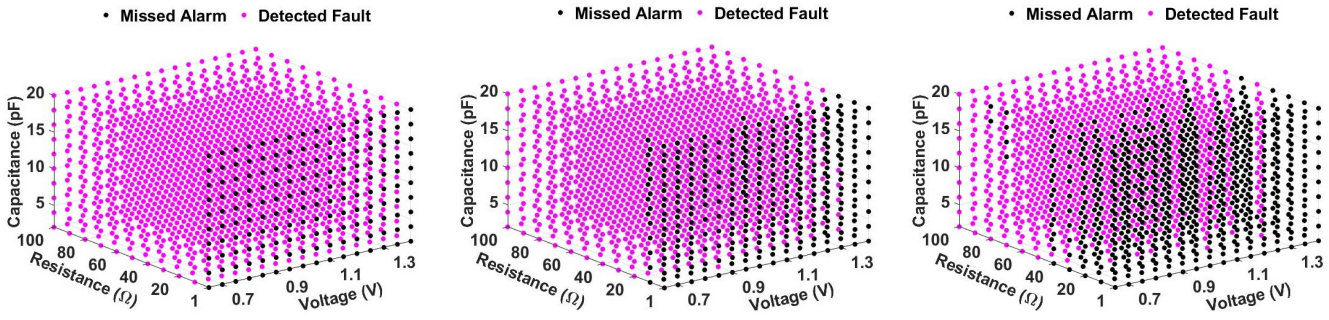
Table I
LASER-INDUCED FIA DETECTION RATE FOR DIFFERENT N FACTORS

	PGN Resistance	N=8	N=10	N=12
Commercial Grade	$1\Omega{\leq}R{\leq}100\Omega$	84.0%	87.1%	88.8%
	$10\Omega{\leq}R{\leq}100\Omega$	92.3%	95.8%	97.7%
Industrial Grade	$1\Omega{\leq}R{\leq}100\Omega$	85.3%	86.5%	89.2%
	$10\Omega{\leq}R{\leq}100\Omega$	93.9%	95.2%	98.1%
Military Grade	$1\Omega{\leq}R{\leq}100\Omega$	81.4%	83.1%	86.8%
	$10\Omega{\leq}R{\leq}100\Omega$	89.5%	91.4%	95.4%

Note that the value of N depends on the technology, and in particular transistors' size. However by changing the technology this value is not changed drastically. Our previous study [51] on a 28nm silicon revealed N between 8-20; thus we considered it as 19 on that research based on the layout of the target chip. However, in this paper, we consider a worst case scenario for our detection scheme by selecting $N = 8, 10, 12$ as the greater the value of N the higher the fault detection rate, yet we showed, through our simulations, that the fault detection rate of our method is very high even in worst case scenarios.

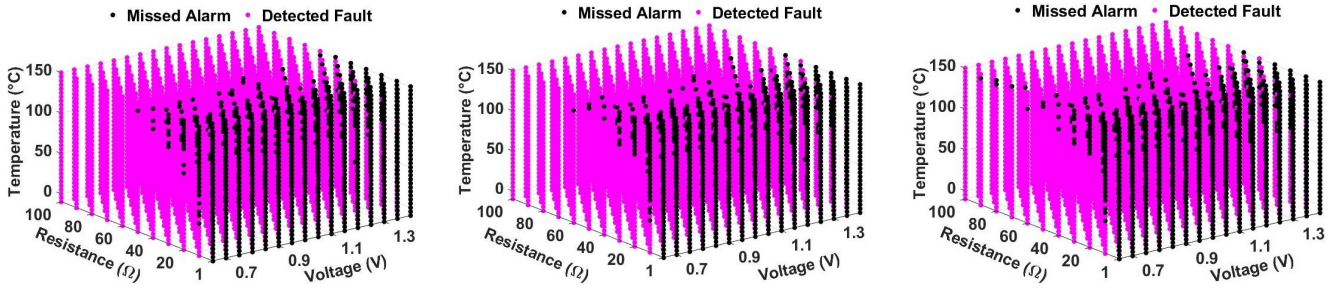
It is noteworthy to mention that N is also affected by placement and routing of the circuitry located around the laser illumination target. This can be interpret by Eq. 1 through area of N_{well} and $drain$. Therefore, we can perform the place and route of the circuit around the critical areas (which will be potential targets by the adversary for laser illumination to leak sensitive data) such that the highest possible value of N is achieved. This helps in increasing the detection rate of the LFIAs as confirmed by Table I in the cost of more area overhead.

As observed with experimental results in Viera [51], IR drops induced by I_{PGN} play an important role in the fault occurrence process by either amplifying the transient voltages generated by I_{gate} or by directly disrupting the behavior of gates or datapaths far from the laser spot location because



(a) T=-10°C (b) T=80°C (c) T=150°C

Figure 12. The sensor's laser attack detection outcome in different (V,R,C) combinations for temperature of -10°C, 80°C, and 150°C.



(a) C=2pF (b) C=10pF (c) C=20pF

Figure 13. The sensor's laser attack detection outcome in different (V,T,R) combinations for C=2pF, 10pF, and 20pF.

IR drops propagate through the PDN. Therefore, depending on how the PDN is laid out, it can affect the sensitivity of the sensor as more or less laser-induced IR drop can be observed by the sensor. In this case it is recommended to glue the sensor to the protected circuit.

5) Device Mismatch: The precision of analog integrated circuit blocks most often depends on the matching of pairs of identically designed devices [55]. For example, the offset of comparators is typically determined by the matching of the gate-source voltage of two nominally identical transistors in a differential input pair; the precision of current-mode digital-to-analog converters depends on the accurate matching of currents in nominally identical transistors biased as current sources; the accuracy of the gain of amplifiers with resistive feedback is set by the matching of resistor ratios, whereas the accuracy of the gain of switched-capacitor based amplifiers relies on the accurate matching of ratioed capacitors. As such, many performance parameters of analog circuits depend on the matching between identically designed components. In this work, even if no physical test was made, we assume that the correlation between simulation and experimental results are high since: 1) the sensor in this work being fully digital, the mismatch problem derived from circuit fabrication is greatly reduced; 2) the comparison between experimental results with simulation results in Viera [51] using the same PDN model applied to a ring oscillator are characterized by a high level of correlation and 3) as already mentioned we used worst case values for N, C and R which give margin for device mismatch.

6) Sensitivity of Digital Sensor: The sensitivity of the sensor to the change of power supply voltage is highly important as in practice the chip power supply may experience some variations and noise even when there is no fault attack. If such voltage change is detected incorrectly by the sensor, it can result in a false alarm. Thereby, we report the voltage-changed induced false alarm rate of the deployed sensor when there is no LFIA.

The sensitivity relates to the minimum variation required in the voltage supply that can be sensed by the sensor to raise an alarm. Indeed the lower the required change of voltage for altering the Sensor's FN index, the higher the sensitivity. As mentioned in Sec. IV, in our system we set to raise an alarm when there is at least two unit changes in the FN output of the sensor. To assess the sensitivity of our sensor, we extracted the FN in different voltages with the step of $0.005V$, and we repeated the experiments for different temperatures. Fig. 14 depicts the sensitivity of our sensor for three temperatures, namely -10°C, 70°C, and 150°C. For example, as depicted (via a black point) in this figure, if the sensor is operated in $(V, T) = (1.15V, 150°C)$, for FN to change 2 units, a $0.094V$ drop is required. Note that for the sake of space, we did not show the sensitivity in all temperatures, and Fig. 14 only depicts the sensitivity for lowest, median, and highest temperatures. As shown, depending on the Vdd value, the sensor demonstrates different sensitivities. The high picks in this figure relate to the voltage values which are less sensitive to the noise-induced voltage change, i.e., the Vdd values which need more noise to result in raising an alarm falsely.

As depicted in Fig. 14, with the increase of temperature, the minimum voltage drop required to be sensed by the sensor increases and thus the sensitivity decreases. We refer to Fig.11(a) to explain this observation. As depicted, in higher temperatures, more voltage change is needed to variate the FN value. In other words, in higher temperatures the sensitivity decreases, e.g., in voltage = $1.15V$, a voltage

drop of $0.036V$, $0.049V$, and $0.094V$ are required to change FN with 2 units when the temperature is $-10°C$, $70°C$, and $150°C$, respectively.

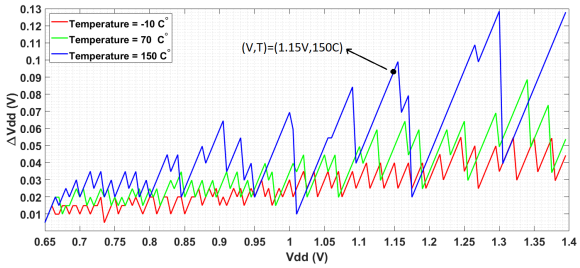


Figure 14. Sensitivity of the digital sensor in three different temperatures.

To extract the rate of the false alarms raised due to the voltage change, we assume that the circuit experiences a $\pm 1\%$ Vdd change *in 1 clock cycle*. In this case, our sensor results in 3.03% false alarms when there is not any LFIA. Please note that this assumption can be too pessimistic as in real applications voltage is not changed sharply just in one clock cycle. Thereby, we also extracted the false alarm rates in case of 0.2%, 0.4%, 0.6%, and 0.8% Vdd change in 1 clock cycle.

As Table II shows our results are highly promising; the false alarm rate is only 1.32% for the $\pm 0.8\%$ Vdd. Note that in real silicon, the circuit may experience even 5% voltage variation yet not in 1 clock cycle as power supplies are highly capacitive, hence react slowly. Thus, our false alarm results are valid. Recall that we do not have any false alarms in case of laser illumination as based on our threat model, the adversary insists in imposing a toggle in the targeted point thus increases the fault intensity till achieving the goal.

Table II
FALSE ALARM RATE OF OUR LFIA DETECTION METHOD FOR DIFFERENT VARIATIONS OF Vdd OCCURRING IN 1 CLOCK CYCLE. THE NUMBERS SHOW THE AVERAGE RATES ASSESSED ON DIFFERENT TEMPERATURES.

Voltage Variation (%)	0.2	0.4	0.6	0.8	1.0
False Alarm (%)	0.00	0.06	0.37	1.32	3.03

We investigated the sensitivity of the sensor to the temperature change when no fault has been injected, i.e., if our sensor raises any false alarm in this case. Indeed, we argue that the temperature change is not abrupt and occurs through several clock cycles. Thereby, our sensor would not experience a change of two units (or more) in the FN value in two consecutive clock cycles. Our analysis shows that our sensor results in 0% false alarm due to the temperature change. The takeaway point is that our sensor is highly efficient in detecting LFIAs while very robust against the environmental changes; resulting in no temperature-induced false alarms and as low as $\approx 3\%$ rate of voltage-induced false alarms.

7) Discussion On Sensor Multiplicity and Overhead: The detection rate can be increased even more by instantiating multiple sensors (to benefit from the glocal impact of our detection scheme) though one can detect the injected faults (with a high detection rate as shown earlier) even if the laser shot spot is targeting a remote point from the sensor location. When deploying multiple sensors, we need to implement an aggregation function to make a decision based on outcome of the sensors altogether. On the other hand, we may also have one sensor to protect multiple circuitries embedded in the same chip. Such investigations are out of the scope of this paper and sensor multiplicity is treated in our future research. Indeed the concept of multiplicity of sensors will be applied to the larger circuits with multiple critical parts where we want that at least one sensor monitors the IR drop occurred around the critical part. Therefore our proposed method is scalable for any circuit. It is also noteworthy to mention that using PRESENT S-Box in this paper is for the sake of illustration and sensors can be deployed within complete security chips.

In this paper, as mentioned earlier, the sensor include 115 flip-flops and 125 Inverters. This is equivalent to 876 2-input Nand gates. Note that the area overhead for a round-based architecture of PRESENT cipher is around 2748 2-input Nand gates in the same technology (based on our implementation and estimation). At the first glance, it may seem that the overhead of our detection method is high compared to the encryption core. However, it is important to consider that the sensors are utilized to detect attacks and/or malfunctions in System-on-Chips and a cipher is only a portion of such a system. Therefore, the logic overhead of the deployed sensor is negligible compared to the area of the whole system.

8) Discussion On Detection latency: In the proposed LFIA detection scheme, as soon as an alarm signal is raised, the circuit's controller sends out a random value to the output port (or even reset the output data) to protect the circuit against SIFA (Statically Ineffective Fault Attack). Note that the detection circuitry has 1 clock cycle latency as the FN value is monitored in each clock cycle to decide about raising an alarm if needed. At the first glance it seems that if the fault is injected in the last clock cycle of the encryption process, the faulty output will be on the bus before the alarm is raised and the protection mechanism is activated. However, the laser fault injection requires iterative adjustment of laser prob to target the point of interest. However, when the probe's location is changed, the circuit experiences an IR drop. Therefore, even in the case of injecting Laser-based faults in the last clock cycle of the encryption, the alarm mechanism is activated even before the fault is really injected. Also, in LFIAs the laser intensity is increased gradually. This may be detected by the TDC before the laser shot becomes strong enough to toggle the target point. Finally, in order to prevent the adversary from getting access to the faulty output on the bus, the designer can force 1 clock latency to send out the output (after it is generated) to buy some time to activate the protection mechanism.

VI. CONCLUSION AND FUTURE DIRECTIONS

Owing to their high spatial accuracy, laser-induced fault injection attacks have received a lot of attention in recent years. In this paper, we deployed time-to-digital sensors to detect such attacks. The proposed methodology is based on monitoring the IR drop induced via the current component that flows directly from V_{dd} to ground due to laser illumination. Our low-cost detection scheme demonstrates a very high fault detection rate in different environmental conditions and various power distribution network specifications, while incurs

a very low false alarm rate occurring due to the supply voltage noise. We will extend this paper by considering the impact of device aging on the proposed detection scheme. We will also investigate our findings on real-silicon.

REFERENCES

[1] M. Agoyan, J.-M. Dutertre, D. Naccache, B. Robisson, and A. Tria, "When clocks fail: On critical paths and clock faults," in *International conference on smart card research and advanced applications*. Springer, 2010, pp. 182–193.

[2] O. Kömmerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," *Smartcard*, vol. 99, pp. 9–20, 1999.

[3] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *Int'l Conf.e on Smart Card Research and Advanced Applications*, 2013, pp. 219–235.

[4] P. Maurine, K. Tobich, T. Ordas, and P. Y. Liardet, "Yet another fault injection technique: by forward body biasing injection," in *Yet Another Conference on Cryptography (YACC)*, 2012.

[5] 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.

[6] A. Dehbaoui et al., "Electromagnetic transient faults injection on a hardware and a software implementatation of AES," in *FDTC*, 2012, pp. 7–15.

[7] J. Rodriguez, A. Baldomero, V. Montilla, and J. Mujal, "LLFI: Lateral laser fault injection attack," in *FDTC*, 2019, pp. 41–47.

[8] P.-L. Cayrel et al., "Message-recovery laser fault injection attack on the Classic McEliece cryptosystem," in *EuroCrypt*, 2021, pp. 438–467.

[9] L. Claudepierre et al., "Traitor: a low-cost evaluation platform for multifault injection," in *ASSS*, 2021, pp. 51–56.

[10] E. Dottax, C. Giraud, M. Rivain, and Y. Sierra, "On second-order fault analysis resistance for crt-rsa implementations," in *IFIP International Workshop on Information Security Theory and Practices*. Springer, 2009, pp. 68–83.

[11] R. Shrivastwa et al., "Multi-source fault injection detection using machine learning and sensor fusion," in *S&P*. Springer, 2021, pp. 93–107.

[12] L. Hériveaux et al., "Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design," in *ISTFA*, 2013, pp. 361–368.

[13] S.-Y. Lin et al., "IR drop prediction of ECO-revised circuits using machine learning," in *VTS*, 2018, pp. 1–6.

[14] R. Viera et al., "Simulation and experimental demonstration of the importance of ir-drops during laser fault injection," *IEEE TCAD*, vol. 39, no. 6, pp. 1231–1244, 2019.

[15] M. T. H. e. a. Anik, "Detecting failures and attacks via digital sensors," *IEEE TCAD*, vol. 40, no. 7, pp. 1315–1326, 2020.

[16] A. Tang et al., "CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management," in *USENIX Sec.*, 2017, pp. 1057–1074.

[17] Y. Wang, R. Paccagnella, E. T. He, H. Shacham, C. Fletcher, and D. Kohlbrenner, "Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on `x86`," 2022.

[18] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *IEEE Symposium on Security and Privacy (S & P)*, vol. 7, no. 2, pp. 79–82, 2009.

[19] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based fault injection attacks against intel sgx," in *Symp. on Security and Privacy (S & P)*, 2020, pp. 1466–1482.

[20] P. Qiu et al., "Voltjockey: Breaking sgx by software-controlled voltage-induced hardware faults," in *AsianHOST*, 2019, pp. 1–6.

[21] ——, "Voltjockey: Breaching trustzone by software-controlled voltage manipulation over multi-core frequencies," in *CCS*, 2019.

[22] Z. Kenjar et al., "V0LTpwn: Attacking x86 Processor Integrity from Software," in *USENIX Security Symp.*, 2020, pp. 1445–1461.

[23] Z. Chen et al, "VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface," in *USENIX Security Symp.*, 2021.

[24] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2014, pp. 104–114.

[25] T. Korak and M. Hoefler, "On the effects of clock and power supply tampering on two microcontroller platforms," in *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2014, pp. 8–17.

[26] L. Zussa, J.-M. Dutertre, J. Clédière, and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter," in *Int'l Symp. on Hardware-Oriented Security and Trust (HOST)*, 2014, pp. 130–135.

[27] C. Deshpande et al., "Employing dual-complementary flip-flops to detect EMFI attacks," in *AsianHOST*, 2017, pp. 109–114.

[28] D. El-Baze et al., "A fully-digital EM pulse detector," in *DATE*, 2016, pp. 439–444.

[29] N. Miura et al., "PLL to the rescue: a novel EM fault countermeasure," in *DAC*, 2016, pp. 1–6.

[30] J. Breier et al., "An electromagnetic fault injection sensor using Hogge phase-detector," in *ISQED*, 2017, pp. 307–312.

[31] W. He et al., "Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks," in *SPACE*, 2016, pp. 27–46.

[32] N. Homma, Y.-i. Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki, "EM attack is non-invasive? design methodology and validity verification of EM attack sensor," in *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2014, pp. 1–16.

[33] J. Shiomi et al., "Tamper-Resistant Optical Logic Circuits Based on Integrated Nanophotonics," in *Design Automation Conference (DAC)*, 2021, pp. 139–144.

[34] E. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. Kastensmidt, "Using Bulk Built-in Current Sensors to Detect Soft Errors," *Micro, IEEE*, vol. 26, no. 5, pp. 10–18, Sept 2006.

[35] A. Simionovski et al., "Simulation Evaluation of an Implemented Set of Complementary Bulk Built-In Current Sensors With Dynamic Storage Cell," *IEEE Trans. on TDMR*, vol. 14, no. 1, pp. 255–261, 2014.

[36] L. Zussa et al., "Efficiency of a glitch detector against electromagnetic fault injection," in *DATE*, 2014, pp. 1–6.

[37] F. Lu et al., "Customized cell detector for laser-induced-fault detection," in *Int'l On-Line Testing Symp. (IOLTS)*, 2014, pp. 37–42.

[38] R. Vadlamani et al., "Multicore soft error rate stabilization using adaptive dual modular redundancy," in *DATE*, 2010, pp. 27–32.

[39] C. Carmichael, "Triple module redundancy design techniques for virtex fpgas," *Xilinx Application Note XAPP197*, vol. 1, 2001.

[40] M. Nicolaidis, "Time redundancy based soft-error tolerance to rescue nanometer technologies," in *VLSI Test Symp.*, 1999, pp. 86–94.

[41] X. Guo and R. Karri, "Recomputing with permuted operands: A concurrent error detection approach," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, vol. 32, no. 10, pp. 1595–1608, 2013.

[42] K. Wu et al., "Low cost concurrent error detection for the advanced encryption standard," in *Int'l Test Conf. (ITC)*, 2004, pp. 1242–1248.

[43] S. Das et al., "RazorII: In situ error detection and correction for PVT and SER tolerance," *IEEE J. of Solid-State Circuits*, vol. 44, no. 1, 2008.

[44] A. H. Johnston, "Charge generation and collection in PN junctions excited with pulsed infrared lasers," *IEEE Transactions on Nuclear Science*, vol. 40, no. 6, pp. 1694–1702, 1993.

[45] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," *IEEE Transactions on Device and materials reliability*, vol. 5, no. 3, pp. 305–316, 2005.

[46] 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.

[47] T. C. May and M. H. Woods, "Alpha-particle-induced soft errors in dynamic memories," *IEEE transactions on Electron devices*, vol. 26, no. 1, pp. 2–9, 1979.

[48] C. Hsieh, P. C. Murley, and R. O'Brien, "A field-funneling effect on the collection of alpha-particle-generated carriers in silicon devices," *IEEE electron device letters*, vol. 2, no. 4, pp. 103–105, 1981.

[49] L. Hériveaux, J. Clédière, and S. Anceau, "Electrical modeling of the effect of photoelectric laser fault injection on bulk cmos design," in *ISTFA*. ASM International, 2013, pp. 361–368.

[50] F. Wang and V. Agrawal, "Single event upset: An embedded tutorial," in *Int'l Conf. on VLSI Design (VLSID)*, 2008, pp. 429–434.

[51] R. A. Camponogara-Viera, "Simulating and modeling the effects of laser fault injection on integrated circuits," Ph.D. dissertation, Université Montpellier, Oct. 2018. [Online]. Available: https://tel.archives-ouvertes.fr/tel-02150306

[52] M. T. H. Anik, M. Ebrahimabadi, H. Pirsiavash, J.-L. Danger, S. Guilley, and N. Karimi, "On-chip voltage and temperature digital sensor for security, reliability, and portability," in *Int'l Conf. on Computer Design (ICCD)*, 2020, pp. 506–509.

[53] N. Selmane, S. Bhasin, S. Guilley, and J.-L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET information security*, vol. 5, no. 4, pp. 181–190, 2011.

[54] M. Ebrahimabadi, M. T. H. Anik, J.-L. Danger, S. Guilley, and N. Karimi, "Using digital sensors to leverage chips' security," in *Physical Assurance and Inspection of Electronics (PAINE)*, 2020, pp. 1–6.
[55] R. Baker, *CMOS: Circuit Design, Layout, and Simulation*, ser. IEEE Press Series on Microelectronic Systems. Wiley, 2019. [Online]. Available: https://books.google.fr/books?id=payXDwAAQBAJ

Mohammad Ebrahimabadi (GSM'21) received the B.Sc. degree in electrical engineering from Zanjan University, Zanjan, Iran, in 2008, and the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2011. He is working towards the Ph.D. degree in the Department of Computer Science and Electrical Engineering at the University of Maryland Baltimore County, MD, USA since 2019. He is a member of the SECure, REliable and Trusted Systems (SECRETS) research lab. His current research focus is on hardware security, and in particular side-channel analysis and fault injection attacks and countermeasures, sensor-assisted secure and reliable design, as well as developing PUF-based authentication and secure communication protocols in IoT frameworks. He has published 20 papers in referred conference proceedings and journal manuscripts

Suhee Sanjana Mehjabin received the B.Sc. degree in electrical engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, in 2020. She is working towards the Ph.D. degree in the Department of Computer Science and Electrical Engineering at the University of Maryland Baltimore County, MD, USA since 2021.

Raphael Viera is an Associate Professor at Mines Saint-Étienne. His main research interests include performing the evaluation of secure IPs resistant to laser attacks; hardening by design of IPs against radiation and laser fault injection and modeling the effects of laser fault injection on ICs. He received his Ph.D. degree in Microelectronics from the University of Montpellier, France, in 2018.

Sylvain Guilley (SM'21) is General Manager and Chief Technology Officer at Secure-IC, a company offering security for embedded systems. Secure-IC's flagship technology is the multi-certified SECURYZR® integrated Secure Element (iSE). Within Secure-IC, he is also director of "Threat Analysis" and "Think Ahead" business lines, which develop respectively security evaluation tools and advanced research. Sylvain is also professor at TELECOM-Paris, associate research at École Normale Supérieure (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS). His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods. Since 2012, he organizes the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. He is also lead editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of non-invasive testing tools), ISO/IEC 24485 (White Box Cryptography), and ISO/IEC 17825 (detection of side-channel leakage). He is "High Level Principles for Design/Architecture" team leader for the drafting of Singapore TR68-3 standard on Cyber-Security of Autonomous Vehicles. Sylvain is associate editor of the Journal of Cryptography Engineering (JCEN, Springer). He has coauthored 300+ research papers and filed 40+ patents. He is member of the IACR and senior member of the IEEE and of the CryptArchi club. He is an alumni of Ecole Polytechnique and TELECOM-ParisTech.

Jean-Luc Danger (M'96) is full Professor at TELECOM Paris. He is the head of the digital electronic system research team involved in Research in security/safety of embedded systems, configurable architectures, and implementation of complex algorithms in ASICs or FPGAs. He authored more than 250+ scientific publications and patents in architectures of embedded systems and security. He received his engineering degree in Electrical Engineering from École Supérieure d'Électricité in 1981. After 12 years in industrial laboratories (namely PHILIPS, NOKIA), he joined TELECOM Paris in 1993 where he became full professor in 2002. He is a co-founder of Secure-IC. His personal research interests are trusted computing in embedded systems, random number generation, and protected implementations in novel technologies.

Jean-Max Dutertre is professor at Mines Saint-Etienne (MSE), he is the head of MSE Secure Architectures and Systems department. He works in the field of hardware security since 2008 with a focus on laser fault injection (LFI). He is the author or co-author of more than 50 LFI papers addressing this threat from modeling and simulation, to countermeasures design. He received his Ph.D. degree in Microelectronics from the University of Montpellier, France, in 2002.

Naghmeh Karimi (SM'22) received the B.Sc., M.Sc., and Ph.D. degrees in Computer Engineering from the University of Tehran, Iran in 1997, 2002, and 2010, respectively. She was a visiting researcher at Yale University, USA between 2007 and 2009, and a post-doctoral researcher at Duke University, USA during 2011-2012. She has been a visiting assistant professor at New York University and Rutgers University between 2012 and 2016. She joined University of Maryland Baltimore County as an assistant professor in 2017 where she leads the SECure, REliable and Trusted Systems (SECRETS) research lab. She has published three book chapters and authored/co-authored over 80 papers in referred conference proceedings and journal manuscripts. She serves as an Associate Editor of the Springer Journal of Electronic Testing: Theory and Applications (JETTA) and IEEE Design & Test Journal. She has been the corresponding guest editor of the Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS); special issue in Hardware Security in Emerging Technologies in 2021. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability. She is a recipient of the National Science Foundation CAREER Award in 2020. She is a senior member of IEEE.