DELFINES: Detecting Laser Fault Injection Attacks via Digital Sensors

Mohammad Ebrahimabadi, *Graduate 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 article, 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.**

***Index Terms*—Fault attack detection, IR drop, laser fault injection attack (LFIA), time to digital converter (TDC).**

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 [9]. Owing to their high spatial and temporal resolutions, laser-induced FIAs (LFIA) allow to finely control the injected faults. Accordingly, in this article, 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 [10] (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 [11]), toggling the value of a specific signal at runtime resulting an embedded cryptographic module to become compromised, e.g., leaks its encryption/decryption keys [12].

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 [13]. 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 [14]. A recent paper by Camponogara Viera et al. [15] 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 (TDCs); the so-called Digital Sensors hereafter.

Being portable among different technologies (due to solely composing of digital standard cells), being devoid of costly

Manuscript received 12 January 2023; revised 3 July 2023; accepted 21 September 2023. Date of publication 6 October 2023; date of current version 21 February 2024. This work was supported in part by the French National Research Agency (ANR) under Grant ANR-20-CYAL-0007 (APRIORI Project), and in part by the National Science Foundation CAREER Award under Grant NSF CNS-1943224. Secure-IC acknowledges partial funding from the European Union's Horizon Europe Research and Innovation Programme through ALLEGRO Project under Grant 101092766. A preliminary version of this paper was presented at the 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) [DOI: 10.1109/HOST54066.2022.9840318]. This article was recommended by Associate Editor Y. Jin. *(Corresponding author: Mohammad Ebrahimabadi.)*

Mohammad Ebrahimabadi, Suhee Sanjana Mehjabin, and Naghmeh Karimi are with the Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD 21250 USA (e-mail: e127@umbc.edu; suheesm1@umbc.edu; nkarimi@umbc.edu).

Raphael Viera and Jean-Max Dutertre are with the Département Systèmes et Architectures Sécurisés, École des Mines de Saint-Étienne, 42100 Saint-Étienne, France (e-mail: raphael.viera@emse.fr; dutertre@emse.fr).

Sylvain Guilley is with Secure-IC S.A.S., Paris, France, and also with Institut Polytechnique de Paris/Telecom-Paris, 91120 Palaiseau, France (e-mail: sylvain.guilley@secure-ic.com).

Jean-Luc Danger is with the Institute Polytechnique de Paris/Telecom-Paris, 91120 Palaiseau, France (e-mail: jean-luc.danger@telecom-paris.fr).

Digital Object Identifier 10.1109/TCAD.2023.3322623

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 [16]. In practice, digital sensors have been shown to be highly effective in detecting timing and environmental attacks, such as clock skew attacks (ClkScrew [17], Hertzbleed [18]), temperature attacks [19], voltage attacks (PlunderVolt [20], VoltJockey [21], [22], [23], VoltPillager [24]), mixed timing+temperature [25], and timing+voltage attacks [26].

This article 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 power grid network (PGN).

Our contributions include:

1) A simple model representing the impact of LFIAs in the targeted circuit;
2) A methodology to effectively detect the LFIAs during the circuit runtime;
3) Extensive HSpice simulations to extract the miss and false alarm rates for the considered FIAs;
4) A thorough investigation of how our sensor reacts in different temperature and voltage conditions in presence of an LFIA;
5) Studying the impact of characteristics of the PGN on the attack detection;
6) 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 [27]. However, in this article we target the laser FIAs 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 remainder of this article is structured as follows. Section II discusses the related work on detecting FIAs. 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.

To enhance readability, Table I provides the definition of the variables used in this study.

Compared to the conference version, this paper includes: (1) Evaluating the efficiency of our LFIA detection scheme in a wide range of operating conditions; (2) A complete discussion on the proposed fault model and its impact on the target chip; (3) An algorithm to fine-tune the minimum current required to inject the fault in all considered operating conditions; (4) An extensive discussion on the impact of circuit layout on FIA, overhead of the proposed method and its detection latency; and (5) Extracting the sensitivity of the digital sensor to the voltage variations.

TABLE I
DEFINITION OF THE ALL VARIABLES USED IN THIS ARTICLE

Variable	Definition
I_{PGN}	Induced transient current from Vdd to GND
I_{gate}	Induced transient current from NMOS drain to GND
N	Ratio of I_{PGN} and I_{gate}
CC	Number of clock cycle (in this paper = 8)
CC_i	i^{th} Clock Cycle
FN_i	Sensor outcome in i^{th} Clock Cycle
AFN	Average of FN_i over a number of CC_i
Vdd	Power supply of the chip
Vdd_b	Effective power supply of the chip
n_0	Number of leading inverters in TDC
n_1	Number of sampling inverters and flip-flops in TDC
V^*	Set of Voltages = {0.65, 0.7, 0.75, ..., 1.4}V
T^*	Set of Temperatures = {-10, -5, 0, 5, ..., 150}$^\circ C$
R^*	Set of Resistors = {1, 10, 20, 30, ..., 100}Ω
C^*	Set of Capacitances = {2, 4, 6, 8, ...,20}pF

II. RELATED WORKS

Several sensor-based fault detection schemes have been proposed in the recent literature, e.g., Deshpande et al. [28] and Guilley and Le Rolland [29] presented a sensor based on dual-complementary flip-flops to detect electromagnetic-induced FIAs (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. [30] 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 [31]. In this method a number of ring oscillators (ROs) 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. He et al. [32] proposed a method to detect LFIA and EM attacks via an RO and a PLL embedded in an FPGA platform. However the availability of PLL is not guaranteed in all chips [33, Sec. 2.4]. A Hogg phase-detector is deployed in [34] 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. He et al. [33] replaced such a PLL-based sensor with a Ring-Oscillator-based counterpart. Although their sensor features a high fault detection rate, it unfortunately suffers from high latency in detecting the faults.

To detect probing attacks, [35] 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. But this sensor offers an information leakage [36]. Hence, by solving one problem, the countermeasure opens

TABLE II
COMPARING DELFINES WITH THE RELATED WORK

Ref.	Methodology	Disadvantage
[28], [29]	Implementing dual-complementary flip-flops to detect EMFI attack	Significant hardware overhead
[30]	Detecting electromagnetic pulse attack sensor realized by preliminary gates	High area overhead
[31]	Detecting EMFI attack via checking the phase of an embedded RO	High area and power overheads
[32]	Sensing frequency ripple by a watchdog RO and PLL in FPGA platform	Having PLL is not always guaranteed in all circuits
[34]	Monitoring frequency turbulence induced by watchdog RO and phase detector	Significant false alarm rate
[33]	Sensing frequency ripple by a high frequency watchdog RO and disturbance capture	High latency in detecting fault
[35]	Detecting probing attack based on the change in the sensor's inductance induced by the attack	Information leakage of sensor [36]
[37]	Detecting fault attacks via a PUF-based physical sensor	High power consumption and high sensitivity to changes in voltage and temperature
[38]	Proposing an RO-PUF based fault injection detector	Cannot detect faults timely; is not proven against local attacks
[39], [40]	Detecting transient faults by connecting an analog sensor to the bulk of transistors being monitored	Requires multiple sensors to detect faults with high coverage
[41]	Detecting the voltage glitch attack by shift phasing the clock signal with some delay elements	Requires multiple sensors to detect faults with high coverage
[42]	Detecting LFIA with a custom design of logic gates	Suffering from portability among different technologies
[43], [44]	Detecting fault by implementing Triple Modular Redundancy	Significant hardware overhead
[45]	Detecting fault via time-redundancy	Increasing the circuit latency and power
[46]	Detecting fault via time-redundancy on selected operations	Resulting in higher fault escapes
[47]	Detecting fault via information-redundancy schemes	Features low detection rate and high overhead
[48]	Detecting clock glitch via delaying the system clock	Unable to detect LFIAs

another vulnerability. Tajik et al. [37] proposed a PUF-based sensor to monitor the circuit operation against laser voltage probing (LVP), clock manipulations and reconfiguration attacks. Although the proposed detection scheme is effective, it suffers from high power consumption as well as high sensitivity to changes in operating conditions [37, Sec. VI-B]. Köylü et al. [38] proposed a fault attack detection method based on RO-PUF. This method stores the PUF response in the early stages of usage. Then, by comparing this response to the PUF response during the runtime, the possible faults can be detected. This way of sensing is smart, but cannot detect timely (measuring the frequency of a RO requires more than one clock period). In addition, it has not be proven yet on local attacks.

Bulk built-in current sensor (BBICS [39], [40]) 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 (DFF) 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 [41]. 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 [42]. 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) [43], [44] impose a significant hardware overhead. Time-redundancy-based methods (e.g., [45]) perform each operation twice; hence significantly increasing the circuit latency and power consumption. Guo and Karri [46] presented a time-redundancy-based scheme that computes the operations twice selectively. This imposes less overhead compared to [45] yet may result in higher fault escapes. Information-redundancy schemes (e.g., [47]) either have a low detection rate or impose high overhead. To detect and correct the variation-induced delay errors, Das et al. [48] proposed Razor II. This method detects clock glitching but is not detecting LFIAs. Table II summarizes the related works discussed above.

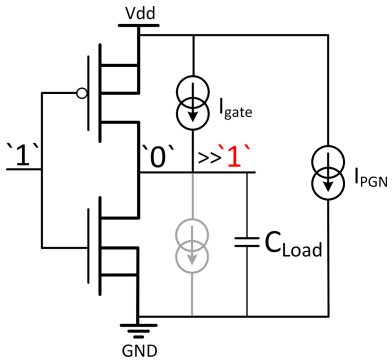


Fig. 1. Laser-induced transient fault model (applied to an inverter with input biased at '1'). The model takes into account the supply voltage drop/bounce (IR drop) induced by the I_{PGN} parasitic current [15].

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 [49]). 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 parts of circuits) [50]. The polarity,

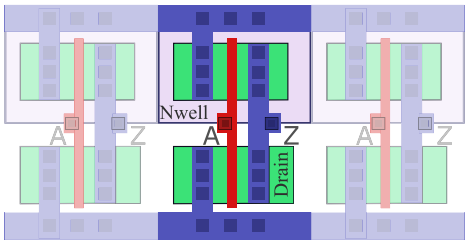


Fig. 2. Generic layout of a CMOS inverter showing the size of the pMOS' Nwell layer and the nMOS drain. The inverter is surrounded by other cells that may contribute to the generation of transient currents.

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 [13], [51], [52], [53], [54].

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'.

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 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 DFFs. The laser-induced transient fault model used in this work was experimentally validated in a commercial FPGA by Camponogara-Viera [55] (cf. [15] 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.

The amplitude of I_{PGN} relates to I_{gate} via $I_{\text{PGN}} = N \times I_{\text{gate}}$ where N follows (1). In this equation, $\text{Area}_{\text{NWell}}$ (related to I_{PGN}) is the total area of the illuminated Nwell PN junctions and $\text{Area}_{\text{drain}}$ (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

$$N = \frac{\text{Area}_{\text{Nwell}}}{\text{Area}_{\text{drain}}}. \tag{1}$$

In this article, the value of N is decided based on a single standard cell (an inverter which is the worst case for our proposed detection scheme and best case for the attacker). By inclusion of dummy cells in the proximity of this standard cell, the area of Nwell is increased while the total area of transistors' drains remains intact. Thus, based on the (1) the effective N value will increase and would be higher than its expected value. This facilitates detecting the LFIA.

B. Time-to-Digital Converter

TDCs (*so-called digital sensors hereafter*), have been used in recent years to sense environmental conditions, e.g., temperature and voltage, in embedded systems [56]. 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 [57]. 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 [58]. 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 article [59].

The architecture of the digital sensor used in this article is depicted in Fig. 3. The circuit includes n_0 leading inverters followed by n_1 inverters each feeding a 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.

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

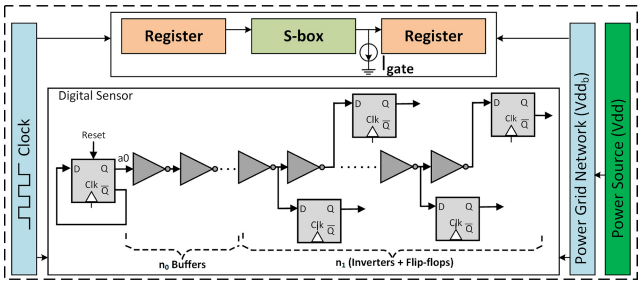


Fig. 3. Architecture of the sensor-integrated target system.

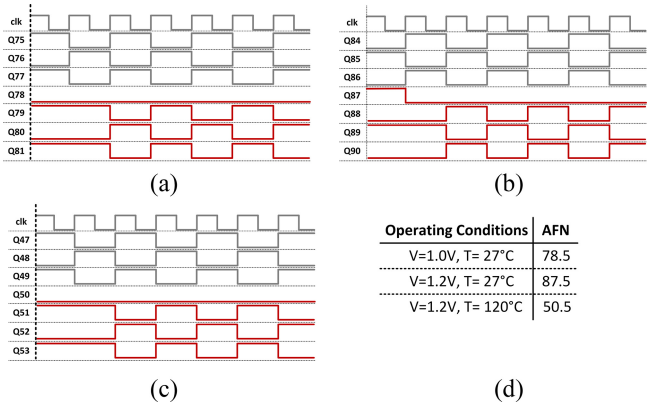


Fig. 4. Waveforms of Fig. 3 depicting the output of the embedded flip-flops in different voltage and temperature combinations. In each figure, the x-axis represents the time and the y-axis shows the voltage of the considered flip-flops. (a) V = 1.0 V, T = 27 °C. (b) V = 1.2 V, T = 27 °C. (c) V = 1.2 V, T = 120 °C. (d) AFN of Fig. 4(a)–(c).

violation, each two consecutive DFFs would experience opposite phases, i.e., one of them would be in the phase of A (say '0' → '1' → '0' → ...) and the other in the phase of $\bar{A}$ (say '1' → '0' → '1' → ...). 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.

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

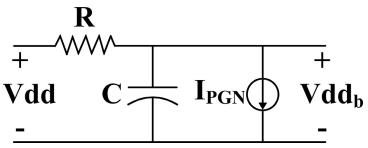


Fig. 5. RC circuitry modeling the laser-induced IR drop.

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 PGN (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 PGN. 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 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 [55] 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 (2). However, in the present of LFIAs the Vdd_b(faulty) follows (3):

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

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

The differences between the above two equations reveal that the voltage drop due to the FIA is $R \times I_{\text{PGN}}$. 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 $\text{FN}_i - \text{FN}_{i-1}$ 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 (4) and (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

$$\text{AFN}_{i-1} = \frac{1}{\text{CC}} \sum_{j=i-\text{CC}-1}^{i-1} \text{FN}_j. \tag{4}$$

$$\text{Alarm} = \begin{cases} \text{'1'} & \text{when } \lceil \text{FN}_i - \text{AFN}_{i-1} \rceil \geq \text{TH} \\ \text{'0'} & \text{otherwise.} \end{cases} \tag{5}$$

Accordingly, In this article, 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 two (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.

A. Hardware Implementation of DELFINES

Fig. 6 shows the proposed hardware used to characterize the sensor by generating the FN_i in each clock cycle CC_i. The top part of this figure relates to the used TDC where only the outputs of the n_1 embedded DFFs have been shown (recall Fig. 3). These outputs (depicted as $O_0, O_2, \ldots, O_{n_1-1}$) feed our "FN calculator" which in turn computes the FN_i in each clock cycle (CC_i) by determining the index of the first flip-flop that experiences a phase similar to its predecessor flip-flop (referring to Section III-B). The "FN calculator" can be as simple as a set of XNORs and a priority encoder. XNORs detect the phase similarity and then the priority encoder extracts the index of the first DFF that experiences such phase similarity. By indexing the DFFs from '0' to '$n_1 - 1$', FN_i would be between 1 and $n_1 - 1$. Thus, the first input of the priority encoder is connected to ground. As mentioned earlier and shown in (5), to remove the effect of short duration abnormal changes in operating conditions (that may result in false alarms), the average of FN values (i.e., AFN) is calculated over the K clock cycles (8 clock cycles in our experiments).

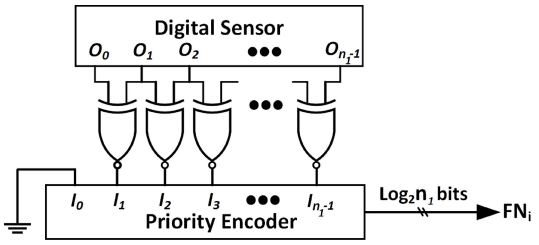


Fig. 6. Hardware implementation of the FN calculator.

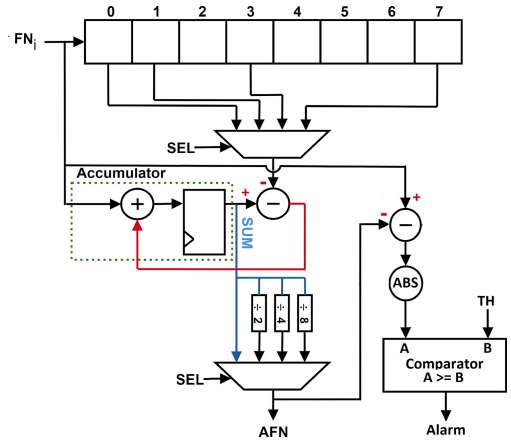


Fig. 7. Hardware implementation of DELFINES. The AFN calculator is shown for the case where SEL is 2 bits (thus $0 \leq \text{SEL} \leq 3$).

As Fig. 7 depicts, the "AFN calculator" includes a buffer (in particular a shift register) that keeps the last K values of *FNs* where $K = 2^{\text{SEL}}$ and SEL is a primary input for the "AFN calculator" module. The value of AFN is evaluated based on these K consecutive FN values resided in the buffer in each clock cycle. Note that the content of this buffer is updated by shifting in the new FN in each clock cycle and shifting out the oldest saved value.

Fig. 7 depicts the "AFN calculator" for the case when SEL is a 2-bit input. Our implementation provides the capability of configuring the AFN assessment during the runtime such that it can be calculated based on the FNs in the last $K = 2^{\text{SEL}}$ cycles where $K \in \{1, 2, 4, 8\}$. The summation of the last K values of FN is then right shifted to find the AFN value. In summary, in our implementation, the sum of the last K consecutive FN_i readings is calculated in each clock cycle by adding the FN_i value to the SUM provided in the previous clock cycle and subtracting the oldest one (FN_{i-N}) from this summation. Consequently, the overhead of our AFN calculation circuitry during runtime is minimal. Deciding about the value of SEL enables the user to determine the number of clock cycles used in AFN computation during the runtime. Note that during the system operation, SEL and consequently K should remain fixed, and updating its values requires resetting the AFN calculation circuitry. After resetting the "AFN

calculator" the buffer shown in Fig. 7 gets reset, therefore for the first K clock cycle the AFN value is not valid.

Finally, as shown in (5), after calculating the differences between the computed AFN (AFN_{i-1}) and the FN_i values, the comparator decides whether an alarm should be raised.

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 45 nm 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 [16]. Please note that we used 45 nm NANGATE technology as a proof of concept in this article. However the proposed LFIA detection method is also applicable on the newer technologies.

We considered the voltage $V^* = [0.65, 1.4]$ V (step 0.05 V), temperature $T^* = [-10, 150]$ °C (step 5 °C), $R^* = [1, 100]\Omega$ (step 10 Ω), and $C^* = [2, 20]$ pF (step 2 pF). 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 $I_{\text{PGN}} = N \times I_{\text{gate}}$) based on [15]. 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 article, we considered a transient fault model that toggles the targeted signal (to resemble the laser illumination effect in real-silicon experiments). We considered a 8 ns duration for laser illumination. 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. 8 to find minimum I_{gate} in each case.

1) *Step 1:* Measure I_{gate}, by using HSPICE, for all combinations of (V, T, R, C) where:
   $V \in V* = \{0.65\text{ V}, 0.7\text{ V}, \ldots, 1.4\text{ V}\}$,
   $T \in T_R = \{-10\text{ °C}, 80\text{ °C}, 150\text{ °C},$
   $R \in R_R = \{1\ \Omega, 50\ \Omega, 100\ \Omega\}$,
   and $C_R \in C* = \{2\text{ pF}\}$.
   Fig. 9(a) shows a snapshot of what needs to be measured for $T = -10$ °C. The same table should be generated for the other two temperatures (here we did not show all voltage steps for the sake of space).
2) *Step 2:* Set $T = -10$ °C, $V = 0.65$ V, $C = 10$ pF. 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., 10 Ω, etc.).
3) *Step 3:* Repeat Step2 for all $V \in V*$ [Fig. 9(b) shows the result of the regression in black for the data gathered in this step].
4) *Step4:* Repeat Step2 and Step3 for $T = 80$ °C and $T = 150$ °C.
5) *Step 5:* 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 $C1 = 10$ pF and the same voltage and temperature.
6) *Step 6:* 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 Figs. 14 and 15, 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

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 $C \in C^* - C_R$

Fig. 8. Finding minimum I_{gate} in each (V, T, R, C) point.

Resistance(Ω) \ Voltage (V)	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)

Resistance(Ω) \ Voltage (V)	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)

Fig. 9. Inferring minimum required I_{gate} based on measuring I_{gate} of corner cases. The values have been shown for the temperature of −10 °C. (a) Collecting I_{gate}. (b) I_{gate} after regression.

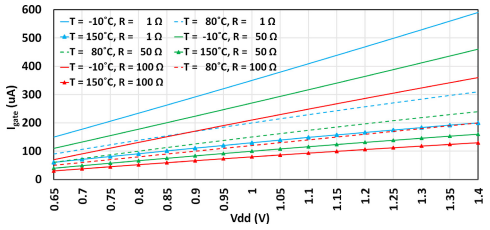


Fig. 10. I_{gate} values injected in different (v, t, r). Here, $c = 10$ pF.

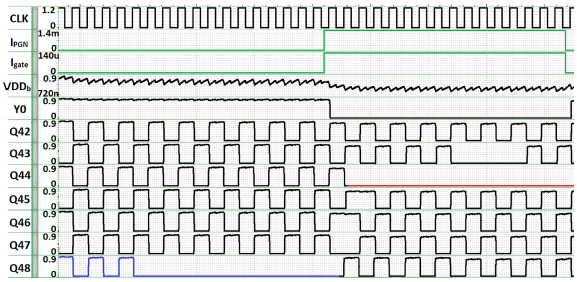


Fig. 11. S-Box and Sensor signal waveform for $V = 1$ V, $T = 80$ °C, $R = 50$ Ω and $C = 10$ pF. In this figure, the x-axis represents the time.

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.

Fig. 10 depicts the values of I_{gate} in different conditions, extracted using the algorithm of Fig. 8. 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. 11 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 LSB (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. 12 illustrates the magnitude of IR drop ($\text{Vdd}–\text{Vdd}_b$) in $T = 80$ °C and $\text{Vdd} \in \{0.65\text{ V}, 1.0\text{ V}, 1.4\text{ V}\}$ 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.

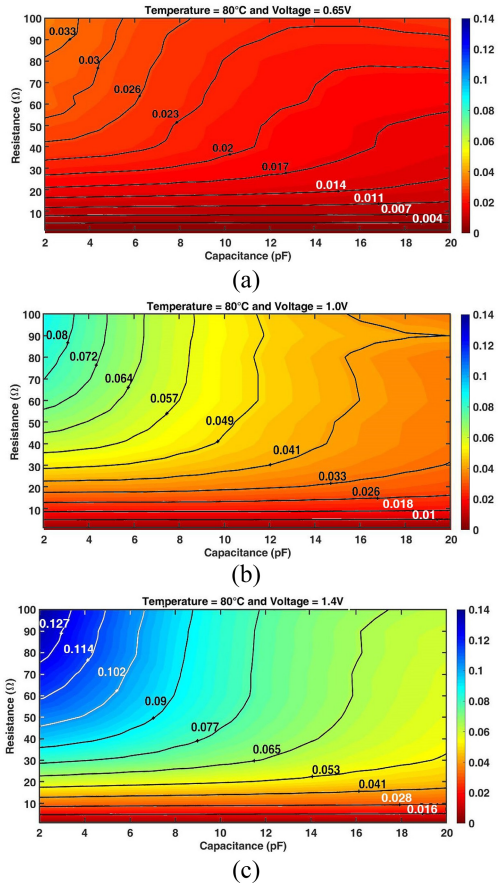
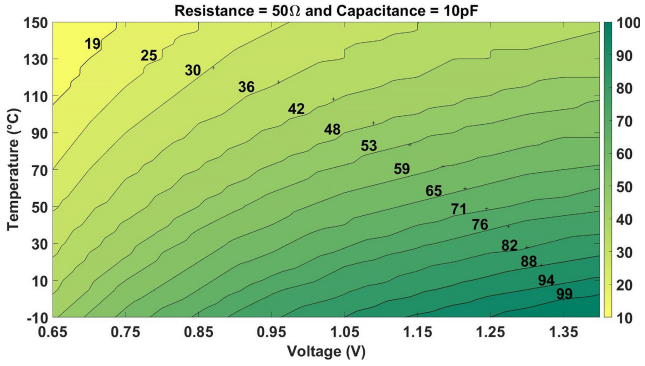


Fig. 12. Heatmaps of voltage drop (i.e., $\text{Vdd} - \text{Vdd}_b$) in different (R, C) combinations and Vdd values. Here, $T = 80$ °C. The unit for all voltage values shown in these figures is volt. (a) $\text{Vdd} = 0.65$ V. (b) $\text{Vdd} = 1$ V. (c) $\text{Vdd} = 1.4$ V.

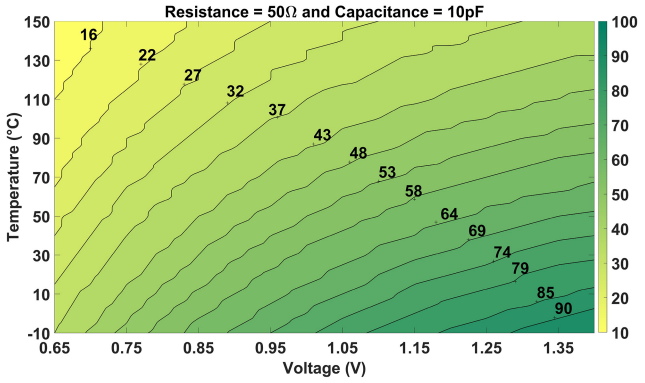
This is due to the increase of I_{PGN} in higher voltages (linked to the requirement of using a higher I_{gate} to inject a fault, see Fig. 10). Note that even when no fault is injected (not shown for the sake of space) the circuit experiences an IR drop, yet negligible compared to the cases where a 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.

2) Effect of Environmental Conditions on the Sensor's Outcome: Fig. 13 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. 13(a) depicts the AFN values when no fault is injected and Fig. 13(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



(a)



(b)

Fig. 13. AFN values without and with laser illumination (so that a fault is injected) in different (V, T) combinations where $R = 50\ \Omega$ and $C = 10$ pF. (a) No fault has been injected. (b) After fault Injection.

$T = 80$ °C and Vdd 1.05 V 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 article).

3) Detection Rate of the Laser-Induced Faults: This set of results demonstrates the detection rate of our sensor when a laser-based FIA is launched on the targeted S-Box. We have extracted the results for the whole range of (R, C, V, T) discussed in Section V-A; totally 58 080 cases. Fig. 14 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 = 1 Ω. This is due to the low IR drop occurring in very low resistances. Although in the case of R = 1 Ω, 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. 14 is that by increasing the temperature, the missed alarm rate increases. For example, at –10 °C, the sensor detects ≈ 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 article we 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.

Fig. 15 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 $C = 2$ pF, the fault detection rate is around 80%. This rate increases to ≈81% when the capacitance is 20 pF. 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 Section IV, LFIAs result in an IR drop in the PGN. 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 article, as pointed out in Section V-A, we considered a factor of $N = 10$ between I_{PGN} and I_{gate} (i.e., $I_{\text{PGN}} = 10 \times I_{\text{gate}}$) based on standard cells that build up our circuit [15]. 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. Table III shows our LFIA detection rate for each of these grades, each for three values of N, in particular for $T \in [0\ °C, 70\ °C]$ in commercial grade, $T \in [-10\ °C, 85\ °C]$ for Industrial Grade, and $T \in [-10\ °C, 125\ °C]$ 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 1 Ω as Camponogara-Viera [55] showed that the minimum value of R is around 10Ω for a typical-sized circuit. Thus, in Table III, 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.

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 [55] on a 28 nm silicon revealed N between 8 and 20; thus we considered it as 19 on that research based on the layout of the target chip. However, in this article, we consider

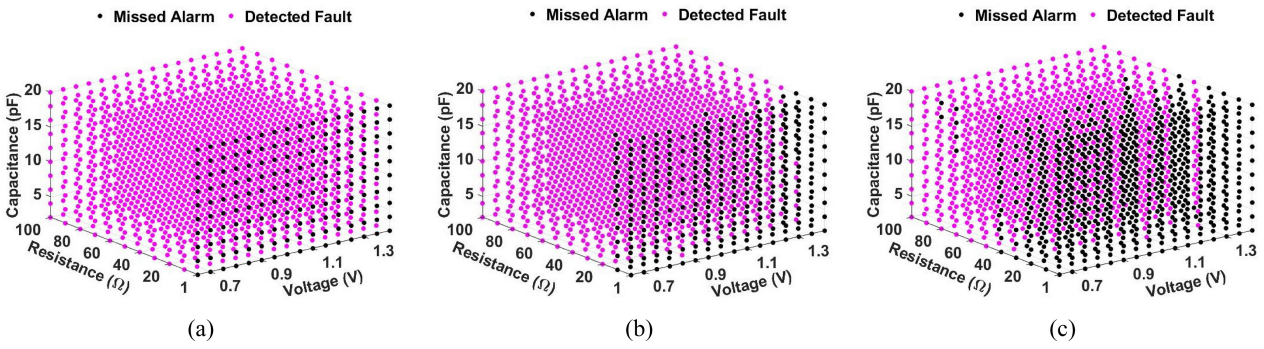


Fig. 14. Sensor's laser attack detection outcome in different (V, R, C) combinations for temperature of -10 °C, 80 °C, and 150 °C. (a) T $= -10$ °C. (b) T $= 80$ °C. (c) T $= 150$ °C.

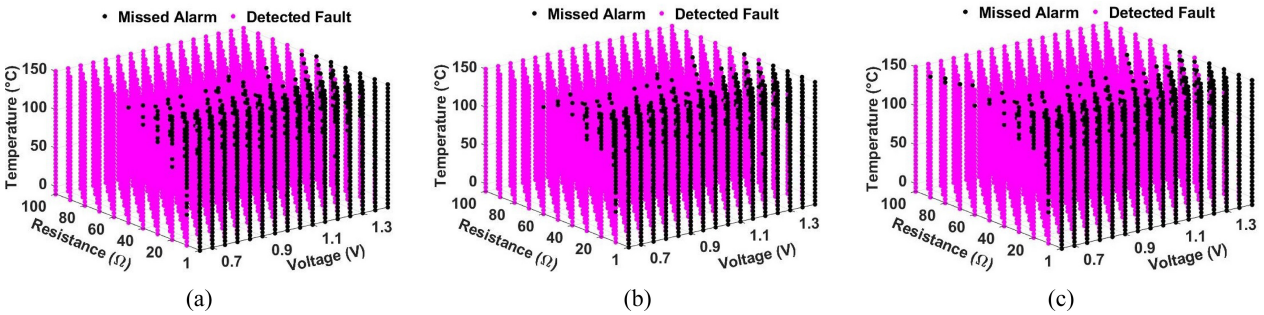


Fig. 15. Sensor's laser attack detection outcome in different (V, T, R) combinations for C $= 2$ pF, 10 pF, and 20 pF. (a) C $= 2$ pF. (b) C $= 10$ pF. (c) C $= 20$ pF.

TABLE III
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%

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 (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 III in the cost of more area overhead.

As observed with experimental results in Camponogara-Viera [55], 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 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 IC blocks most often depends on the matching of pairs of identically designed devices [60]. 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 Camponogara-Viera [55] using the same PDN model applied to a RO 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

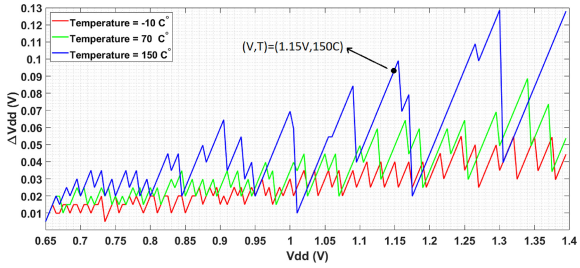


Fig. 16. Sensitivity of the digital sensor in three different temperatures.

result in a false alarm. 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 Section 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 0.005 V, and we repeated the experiments for different temperatures. Fig. 16 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 $(V, T) = (1.15$ V, 150 °C), for FN to change 2 units, a 0.094 V drop is required. Note that for the sake of space, we did not show the sensitivity in all temperatures, and Fig. 16 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. 16, 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. 13(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 $= 1.15$ V, a voltage drop of 0.036 V, 0.049 V, and 0.094 V are required to change FN with 2 units when the temperature is -10 °C, 70 °C, and 150 °C, respectively.

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 IV 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 IV
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. To ensure that the security of the target circuit is not compromised in those rare cases ($\approx 3\%$) that a false alarm is raised, we will implement the following procedure to differentiate between false alarms and real alarms: Whenever the system raises an alarm, the faulty output is prevented to be loaded on the output bus. Then, after 8 clock cycles, we redo the same computation. If the first received alarm was a result of voltage variation, the probability of getting an alarm in the recomputation step is very negligible as the voltage variation is random. The reason to wait for 8 clock cycles for the recomputation step is to let the buffer of the AFN calculator converge to the FN value to prevent getting false alarms consecutively in the computation and recomputation steps as much as possible. In case we get an alarm in the recomputation step as well, we may conclude that a fault attack has happened. However, the system is safe as we did not load the ciphertext to the bus yet.

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 article 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 article is for the sake of illustration and sensors can be deployed within complete security chips.

In this article, 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 statically ineffective fault attack (SIFA). 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 probe 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. Even if the adversary knows the exact location and intensity of the laser shot needed to inject an effective fault, it is still very difficult to target the exact same point in the target chip in one shot of illumination. 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.

9) Discussion on the Resiliency of Our Sensor Against Disabling Attack: An attacker may seek to disable the TDC sensor while carrying out a laser attack on the protected logic. As the TDC proper operations rely on the same clock signal as the protected logic, he/she may target the clock signal. This involves a stronger fault model than the one previously addressed: an attacker that can both conduct a laser attack and also tamper with the TDC clock signal. In case an external clock is used, the fault model seems to be relaxed. However, any glitch on the clock signal will disturb the propagation of the continuous pulse fed to the TDC inverters line (see Section III-B), as a result, an unexpected FN output will be produced and will trigger the alarm. Tampering with the TDC clock signal at one point of its propagation tree inside the circuit could also be done with a second laser beam by a powerful attacker (a few dual-beam laser equipments have been reported). We considered and simulated the case of a laser shot that freezes the TDC clock signal to a low level while a fault is injected on the targeted logic. The attacker's goal would be to freeze the sensor in a no-alarm state. However, as the clock signal is released, similarly to the case of an external clock tampering attack, an unexpected FN output was produced and the alarm was subsequently triggered as illustrated in Fig. 17. In this figure, as depicted the FN and consequently AFN are 46 before and during the FIA. However,

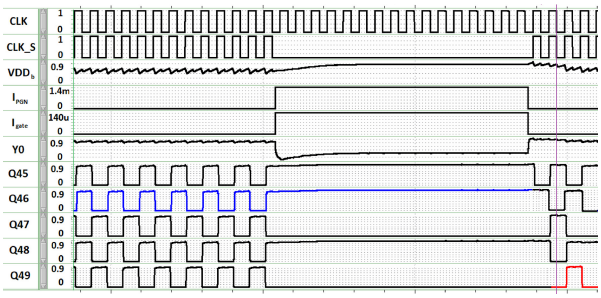


Fig. 17. S-Box and Sensor signal waveform for $V = 1$ V, $T = 90$ °C, $R = 60$ Ω, and $C = 10$ pF while the sensor's clock (*CLK_S*) gets frozen maliciously during the laser illumination. In this figure, the x-axis represents the time.

when the sensor's clock is activated again (after attack) the FN value is increased to 49, and thus attack is detected at that time. Indeed, any deviation of the continuous pulse fed to the TDC inverters line results in a strongly different FN output that triggers the alarm. The TDC sensor is by nature highly sensitive to any perturbation of its clock signal. Note that in case of freezing the clock signal for only 1 clock cycle, again we get the same result, i.e., the fault is detected.

10) Reproducibility of DELFINES With Another PDK: To show that DELFINES works in other technology nodes as well, we targeted the 32 nm SAED PDK (provided by Synopsys). In the new simulations, for the sake of simulation time, we only considered a subset of all (V, T, R, C) combinations discussed above (the corner cases and the median values). We considered voltage $V^* = \{1.05, 1.225, 1.4\}$ V, temperature $T^* = \{-10, 70, 150\}$ °C, resistor $R^* = \{1, 10, 100\}$ Ω, and capacitance $C^* = \{2, 10, 20\}$ pF. Please note that the recommended minimum value for the voltage in the library is 1.05 V. Thereby, we changed the range of voltage accordingly. We simulated the circuit for 81 $(= 3 \times 3 \times 3 \times 3)$ possible configurations. For the new library, we first extracted the value of N based on the layout of the inverter, and it was 9.5. Therefore, we set $N = 9$ in our experiments. Based on our results, the digital sensor is able to detect the faults in all configurations except when the value of $R = 1\Omega$. This is completely similar to the results we had for the 45 nm NANGATE PDK.

VI. Conclusion and Future Directions

Owing to their high spatial accuracy, laser-induced FIAs have received a lot of attention in recent years. In this article, 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 article 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 *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 2010, pp. 182–193.

[2] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," in *Proc. Smartcard*, vol. 99, 1999, pp. 9–20.

[3] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 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 *Proc. Yet Another Conf. Cryptogr. (YACC)*, Sep. 2012, pp. 1–16. [Online]. Available: https://hal-lirmm.ccsd.cnrs.fr/lirmm-00762035

[5] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012.

[6] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of AES," in *Proc. FDTC*, 2012, pp. 7–15.

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

[8] P.-L. Cayrel, B. Colombier, V.-F. Dragoi, A. Menu, and L. Bossuet, "Message-recovery laser fault injection attack on the classic McEliece cryptosystem," in *Proc. EuroCrypt*, 2021, pp. 438–467.

[9] M. Ebrahimabadi et al., "Detecting laser fault injection attacks via time-to-digital converter sensors," in *Proc. HOST*, 2022, pp. 97–100.

[10] L. Claudepierre, P.-Y. Péneau, D. Hardy, and E. Rohou, "TRAITOR: A low-cost evaluation platform for multifault injection," in *Proc. ASSS*, 2021, pp. 51–56.

[11] E. Dottax, C. Giraud, M. Rivain, and Y. Sierra, "On second-order fault analysis resistance for CRT-RSA implementations," in *Proc. IFIP Int. Workshop Inf. Security Theory Pract.*, 2009, pp. 68–83.

[12] R.-R. Shrivastwa, S. Guilley, and J.-L. Danger, "Multi-source fault injection detection using machine learning and sensor fusion," in *Proc. Int. Conf. Security Privacy*, 2021, pp. 93–107. [Online]. Available: https://doi.org/10.1007/978--3-030--90553-8_7

[13] L. Hériveaux, J. Clédière, and S. Anceau, "Electrical modeling of the effect of photoelectric laser fault injection on bulk CMOS design," in *Proc. ISTFA*, 2013, pp. 361–368, doi: 10.31399/asm.cp.istfa2013p0361.

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

[15] R. A. Camponogara Viera, P. Maurine, J.-M. Dutertre, and R. P. Bastos, "Simulation and experimental demonstration of the importance of IR-drops during laser fault injection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 6, pp. 1231–1244, Jun. 2020.

[16] Md T. Hasan Anik, J.-L. Danger, S. Guilley, and N. Karimi, "Detecting failures and attacks via digital sensors," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1315–1326, Jul. 2021.

[17] A. Tang, S. Sethumadhavan, and S. J. Stolfo, "CLKSCREW: Exposing the perils of security-oblivious energy management," in *Proc. USENIX Security*, 2017, pp. 1057–1074.

[18] Y. Wang et al., "Hertzbleed: Turning power side-channel attacks into remote timing attacks on x86," *IEEE Micro*, vol. 43, no. 4, pp. 19–27, Jul./Aug. 2023.

[19] J. Brouchier, T. Kean, C. Marsh, and D. Naccache, "Temperature attacks," *IEEE Security Privacy*, vol. 7, no. 2, pp. 79–82, Mar./Apr. 2009.

[20] K. Murdock, D. F. Oswald, F. D. Garcia, J. V. Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based fault injection attacks against intel SGX," in *Proc. IEEE S&P*, 2020, pp. 1466–1482.

[21] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "VoltJockey: Breaking SGX by software-controlled voltage-induced hardware faults," in *Proc. AsianHOST*, 2019, pp. 1–6.

[22] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "VoltJockey: Breaching TrustZone by software-controlled voltage manipulation over multi-core frequencies," in *Proc. CCS*, 2019, pp. 195–209.

[23] Z. Kenjar, T. Frassetto, D. Gens, M. Franz, and A.-R. Sadeghi, "V0LTpwn: Attacking x86 processor integrity from software," in *Proc. USENIX Security Symp.*, 2020, pp. 1445–1461.

[24] Z. Chen, G. Vasilakis, K. Murdock, E. Dean, D. F. Oswald, and F. D. Garcia, "VoltPillager: Hardware-based fault injection attacks against intel SGX enclaves using the SVID voltage scaling interface," in *Proc. USENIX Security Symp.*, 2021, pp. 699–716.

[25] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *Proc. FDTC*, 2014, pp. 104–114.

[26] T. Korak and M. Hoefler, "On the effects of clock and power supply tampering on two microcontroller platforms," in *Proc. FDTC*, 2014, pp. 8–17.

[27] 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 *Proc. IEEE HOST*, 2014, pp. 130–135.

[28] C. Deshpande, B. Yuce, L. Nazhandali, and P. Schaumont, "Employing dual-complementary flip-flops to detect EMFI attacks," in *Proc. AsianHOST*, 2017, pp. 109–114.

[29] S. Guilley and M. Le Rolland, "Improved detection of laser fault injection attacks on cryptographic devices," U.S. Patent 11 546 132 B2, 2019.

[30] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital EM pulse detector," in *Proc. DATE*, 2016, pp. 439–444.

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

[32] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata, "Ring oscillator under laser: Potential of PLL-based countermeasure against laser fault injection," in *Proc. Workshop FDTC*, 2016, pp. 102–113.

[33] W. He, J. Breier, and S. Bhasin, "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks," in *Proc. SPACE*, 2016, pp. 27–46.

[34] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using Hogge phase-detector," in *Proc. ISQED*, 2017, pp. 307–312.

[35] N. Homma et al., "EM attack is non-invasive? design methodology and validity verification of EM attack sensor," in *Proc. CHES*, 2014, pp. 1–16.

[36] J. Shiomi et al., "Tamper-resistant optical logic circuits based on integrated nanophotonics," in *Proc. DAC*, 2021, pp. 139–144.

[37] S. Tajik, J. Fietkau, H. Lohrke, J.-P. Seifert, and C. Boit, "PUFMon: Security monitoring of FPGAs using physically unclonable functions," in *Proc. IOLTS*, 2017, pp. 186–191.

[38] T. Köylü, L. C. Garaffa, C. Reinbrecht, M. Zahedi, S. Hamdioui, and M. Taouil, "Exploiting PUF variation to detect fault injection attacks," in *Proc. DDECS*, 2022, pp. 74–79.

[39] E. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. Kastensmidt, "Using bulk built-in current sensors to detect soft errors," *IEEE Micro*, vol. 26, no. 5, pp. 10–18, Sep./Oct. 2006.

[40] A. Simionovski and G. Wirth, "Simulation evaluation of an implemented set of complementary bulk built-in current sensors with dynamic storage cell," *IEEE Trans. Device Mater. Rel.*, vol. 14, no. 1, pp. 255–261, Mar. 2014.

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

[42] F. Lu, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Customized cell detector for laser-induced-fault detection," in *Proc. Int. On-Line Test. Symp. (IOLTS)*, 2014, pp. 37–42.

[43] R. Vadlamani, J. Zhao, W. P. Burleson, and R. Tessier, "Multicore soft error rate stabilization using adaptive dual modular redundancy," in *Proc. DATE*, 2010, pp. 27–32.

[44] C. Carmichael, "Triple module redundancy design techniques for virtex FPGAs," Application Note XAPP197, Xilinx, San Jose, CA, USA, 2001.

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

[46] X. Guo and R. Karri, "Recomputing with permuted operands: A concurrent error detection approach," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 32, no. 10, pp. 1595–1608, Oct. 2013.

[47] K. Wu, R. Karri, G. Kuznetsov, and M. Gössel, "Low cost concurrent error detection for the advanced encryption standard," in *Proc. Int. Test Conf. (ITC)*, 2004, pp. 1242–1248.

[48] S. Das et al., "RazorII: In situ error detection and correction for PVT and SER tolerance," *IEEE J. Solid-State Circuits*, vol. 44, no. 1, pp. 32–48, Jan. 2009.

[49] A. H. Johnston, "Charge generation and collection in p-n junctions excited with pulsed infrared lasers," *IEEE Trans. Nucl. Sci.*, vol. 40, no. 6, pp. 1694–1702, Dec. 1993.

[50] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," *IEEE Trans. Device Mater. Rel.*, vol. 5, no. 3, pp. 305–316, Sep. 2005.

[51] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Trans. Nucl. Sci.*, vol. 12, no. 5, pp. 91–100, Oct. 1965.

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

[53] 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 Lett.*, vol. 2, no. 4, pp. 103–105, Apr. 1981.

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

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

[56] 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 *Proc. ICCD*, 2020, pp. 506–509.
[57] 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 Inf. Security*, vol. 5, no. 4, pp. 181–190, 2011.
[58] M. Ebrahimabadi, Md. T. Hasan Anik, J.-L. Danger, S. Guilley, and N. Karimi, "Using digital sensors to leverage chips' security," in *Proc. PAINE*, 2020, Washington, DC, USA, pp. 1–6, doi: 10.1109/PAINE49178.2020.9337730.
[59] M. T. H. Anik, M. Ebrahimabadi, J.-L. Danger, S. Guilley, and N. Karimi, "Reducing aging impacts in digital sensors via run-time calibration," *J. Electron. Test.*, vol. 37, nos. 5–6, pp. 653–673, 2021.
[60] R. Baker, *CMOS: Circuit Design, Layout, and Simulation* (IEEE Press Series on Microelectronic Systems). New York, NY, USA: Wiley, 2019. [Online]. Available: https://books.google.fr/books?id=payXDwAAQBAJ

Mohammad Ebrahimabadi (Graduate Student Member, IEEE) 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 currently pursuing the Ph.D. degree with the Department of Computer Science and Electrical Engineering, the University of Maryland Baltimore County, Baltimore, MD, USA since 2019.

He is a member of the SECure, REliable and Trusted Systems research lab. He has published 22 papers in referred conference proceedings and journal manuscripts. 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.

Suhee Sanjana Mehjabin received the B.Sc. degree in electrical and electronic engineering from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2021. She is currently pursuing the Ph.D. degree in computer engineering with the department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD, USA.

She is a member of the Embedded Systems and Networks Laboratory. Her research focuses on cyber–physical security and secure and trusted communication with hardware in the loop.

Raphael Viera (Member, IEEE) received the Ph.D. degree in microelectronics from the University of Montpellier, Montpellier, France, in 2018.

He is an Associate Professor with Mines Saint-Étienne, Saint-Étienne, France. 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.

Sylvain Guilley (Senior Member, IEEE) received the B.Sc. degree from Ecole Polytechnique, Palaiseau, France, in 1997, the M.Sc. degree in quantum physics from Ecole Normale Supérieure, Paris, France, in 2002, and the M.Sc. degree in digital electronics and the Ph.D. degree from TELECOM-ParisTech, Paris, in 2002 and 2007, respectively.

He is currently a General Manager and Chief Technology Officer with Secure-IC, Cesson-Sévigné, France, a company offering security for embedded systems. Secure-IC's flagship product is the multicertified SECURYZR® integrated Secure Element. He is also a Professor with Télécom-Paris, Palaiseau, France, and an Associate Researcher with École Normale Supérieure, Paris, France. He is an alumni of École Polytechnique and Télécom-Paris. 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 has coauthored 350+ research papers and filed 40+ patent families. His research interests are trusted computing, cyber–physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods.

Prof. Guilley is the Lead Editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of noninvasive testing tools), ISO/IEC TR 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. He is an Associate Editor of the *Journal of Cryptography Engineering* (Springer Nature). He is a member of the IACR, the French *Bureau National de l'Automobile*, and a senior member of the CryptArchi club.

Jean-Luc Danger (Member, IEEE) received the Engineering degree in electrical engineering from École Supérieure d'Électricité, Gif-sur-Yvette, France, in 1981.

After 12 years in industrial laboratories (namely, PHILIPS and NOKIA), he joined Télécom-Paris, Palaiseau, France, in 1993, where he became a Full Professor in 2002. He is the Co-Founder of Secure-IC, Cesson-Sévigné, France. 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. His personal research interests are trusted computing in embedded systems, random number generation, and protected implementations in novel technologies.

Jean-Max Dutertre (Member, IEEE) received the Ph.D. degree in microelectronics from the University of Montpellier, Montpellier, France, in 2002.

He is a Professor with Mines Saint-Étienne (MSE), Saint-Étienne, France, where he is the Head of MSE Secure Architectures and Systems department. He works in the field of hardware security since 2008. He is the author or co-author of more than 50 laser fault injection (LFI) papers addressing this threat from modeling and simulation, to countermeasures design. He focus on LFI.

Naghmeh Karimi (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from the University of Tehran, Tehran, Iran, in 1997, 2002, and 2010, respectively.

She was a Visiting Researcher with Yale University, New Haven, CT, USA, between 2007 and 2009, and a Postdoctoral Researcher with Duke University, Durham, NC, USA, during 2011–2012. She has been a Visiting Assistant Professor with New York University, New York, NY, USA and Rutgers University, Piscataway, NJ, USA, between 2012 and 2016. She joined with the University of Maryland Baltimore County, Baltimore, MD, USA, in 2017 where she is currently an Associate Professor. She leads the SECure, REliable and Trusted Systems research lab and has published four book chapters and authored/co-authored over 80 papers in referred conference proceedings and journal manuscripts. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability.

Prof. Karimi is a recipient of the National Science Foundation CAREER Award in 2020. She serves as an Associate Editor for the Springer *Journal of Electronic Testing: Theory and Applications* and IEEE DESIGN AND TEST JOURNAL. She has been the Corresponding Guest Editor of the *Journal on Emerging and Selected Topics in Circuits and Systems*; special issue in Hardware Security in Emerging Technologies in 2021.