2025 Design, Automation & Test in Europe Conference (DATE 2025)

Multi-Sensor Data Fusion for Enhanced Detection of Laser Fault Injection Attacks in Cryptographic Hardware: Practical Results

Mohammad Ebrahimabadi*, Raphael Viera†, Sylvain Guilley‡,
Jean-Luc Danger§, Jean-Max Dutertre†, and Naghmeh Karimi*
*University of Maryland Baltimore County, United States
†Mines de Saint-Étienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France
‡Secure-IC S.A.S., France *and* ENS Information Security Group, 45 rue d'Ulm, 75,005 Paris, France
§Telecom Paris, Institut Polytechnique de Paris, France

***Abstract*—Though considered secure the cryptographic hardware can be compromised by fault injection attack, especially laser illumination due to its precision in targeting specific areas and its fine temporal control. To address this threat, this paper presents a low-cost detection scheme that utilizes Time-to-Digital Converters (TDCs) to sense the IR drops induced by laser illumination. To achieve a high detection rate while minimizing false alarms, the proposed approach incorporates multiple sensors, with as few as two sensors demonstrated in the study. The effectiveness of the scheme is validated using a real laser setup to illuminate a targeted AES module implemented on an AMD/Xilinx Artix-7 FPGA.**

I. Introduction

Hardware-based cryptographic devices have been widely adopted to protect sensitive data while offering superior speed and efficiency over software-based solutions. However, Fault Injection Attacks (FIAs) can expose vulnerabilities in these pieces of hardware by enabling adversaries with physical access to these chips to deduce secret keys through exploiting the induced errors [1]. Among fault injection attacks, laser illumination has gained significant attention due to its precise targeting capabilities for inducing faults. Laser-induced FIAs (LFIAs) can compromise devices by introducing transient faults; that are exploited by attackers to extract sensitive data. Although LFIAs are highly precise in altering a signal's value at the targeted point, they can also cause a more critical impact, particularly in advanced technologies. This includes a transient voltage drop, known as an IR drop, which propagates and induces timing variations in the affected area [2]. Thus Monitoring IR drops is a practical method to detect laser illumination attacks. To do so, Ring-Oscillator (RO) sensors have been proposed [3], but they suffer from high detection latency. The Time-To-Digital Converter (TDC), referred to as Digital Sensor (DS) hereafter, offers a promising alternative for on-chip voltage monitoring and IR drop detection [4]. However, while simulations support TDC-based sensors [5], experimental validation with real laser setups remains unexplored. In this paper, we fill the gap by evaluating the capability of TDCs for detecting LFIAs in a real laser setup. We implement a round-based AES architecture with multiple TDCs placed at varying distances from the AES to analyze the impact of LFIA on the sensors.

II. Preliminaries

Time-to-Digital-Converters (TDC): TDCs, aka DSs, have been widely used recently to monitor operating conditions, e.g., temperature, voltage, and clock frequency. A TDC consists of n_0 leading inverters followed by a chain of n_1 inverters, each feeding a flip-flop (Fig. 1). Generally such sensors operate under the same operating condition as the main circuit. This enables the DS to detect LFIAs, as the laser-induced IR drop directly impacts the sensor's outcome.

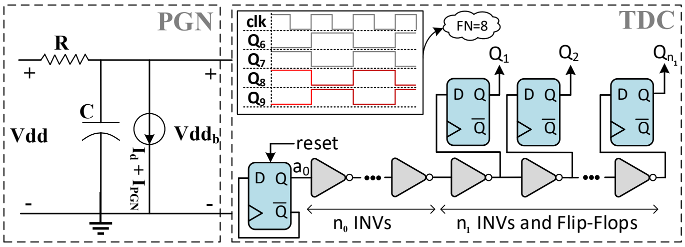
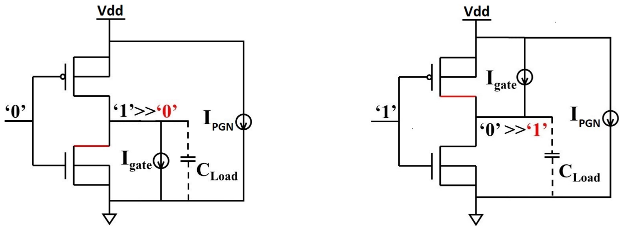


Fig. 1: Parasitic model of Power Grid Network (PGN) of sensor (left) and the architecture of the Digital Sensor (right) used in this study to detect LFIAs. Vdd_b is the effective voltage that feeds the sensor.

To characterize the sensor outcome, we use an index called FN which refers to the index of the 1st DFF in the sensor chain that records the timing violation occurring intentionally thanks to the DS design. At runtime, the sensor is fed with the continuous pulse generated by the initial TFF. Thus, each DFF receives an image of the clock at halved frequency ideally. However, setup time violations occur in some flip-flops, depending on the inverters' delays, which are directly influenced by voltage and temperature. When a violation occurs, at one location (specific index) in the DS, two consecutive DFFs will capture the same value (instead of opposite values related to the inverter in between). The index of the 2nd DFF in this pair is identified as the FN. For example, in the sample waveform of Fig. 1, $FN = 8 \in \{1, \ldots, n_1\}$.

Laser Fault Injection Attack: Laser illumination results in generating electron-hole pairs along illumination path due to the photoelectric effect, potentially causing transient polarity changes in target nodes depending on laser power, duration, location, and device technology [6]. As Fig. 2a shows, this induces a photocurrent (I_{gate}) in the nMOS or pMOS drains, discharging or charging the output load capacitance, thus toggling the inverter output. Laser illumination also induces a transient current (I_{PGN}) in the Power Grid Network (PGN) from V_{dd} to GND (Fig. 2), caused by reverse-biased PN junctions between N-wells and the P-substrate. I_{PGN} does not directly alter gate's output but creates an IR drop in the PGN of the targeted gate, resulting in voltage drops in the neighboring gates [7]. We exploit this IR drop propagation to detect LFIAs.



(a) Inverter fed with logic '0'

(b) Inverter fed with logic '1'

Fig. 2: Laser-induced transient currents model on a CMOS inverter.

978-3-9826741-0-0/DATE25/© 2025 EDAA

III. Methodology

To detect LFIAs, we utilize digital sensors embedded near the protected circuitry (AES in this paper) on the chip. Laser illumination alters the voltage level of the targeted gate and propagates an IR drop in the surrounding area. This IR drop, caused by I_{PGN}, reduces the voltage level near the laser target, as modeled in the RC circuitry shown in Fig. 1. In the absence of a laser attack, the effective voltage supplied to the circuit is approximately $Vdd_b \approx Vdd$, neglecting I_d from circuit activity for simplicity. However, under laser illumination, this voltage decreases to $Vdd_{b(faulty)} \approx Vdd - R \times I_{PGN}$. Indeed by leveraging digital sensors, this IR drop can be detected as it induces a voltage drop ($R \times I_{PGN}$) in the circuit's power supply. To ensure effective detection, the DS should be placed close to the laser impact area, i.e., near the AES core. This voltage drop lowers the DS voltage and causes variations in its FN value.

To design an LFIA detector resilient to temperature changes, we monitor the differential FN values across consecutive clock cycles. If this difference exceeds a threshold TH, an alarm is raised. However, due to the FPGA implementation of DS and the nature of analog signals, FN values differ between even and odd clock cycles because of variations in the rise and fall propagation times of the delay chain input (a_0 in Fig. 1). To address this, FN in each clock cycle CC_i (FN_i) is compared to FN_{i-2}. Using Eq. (1), the sensor raises an alarm at time i if the threshold TH is crossed. Namely:

$$Alarm = \begin{cases} 1 & \text{when } FN_{i-2} - FN_i \geq TH, \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

In this paper, we implemented three sensors alongside the AES module on the Digilent Nexys Video board and used a real laser setup to inject faults into the AES hardware core. To demonstrate that laser illumination generates a propagated IR drop, the first sensor, $S1$, was placed and routed within the AES logic, the second, $S2$, was positioned moderately far from the AES, and the third, $S3$, was placed completely away from the laser shot spot in another zone of the target FPGA while the sensor threshold TH for detecting fault is set to $TH = 2$.

IV. Experimental Results

A. The Effect of Laser Illumination on Sensors

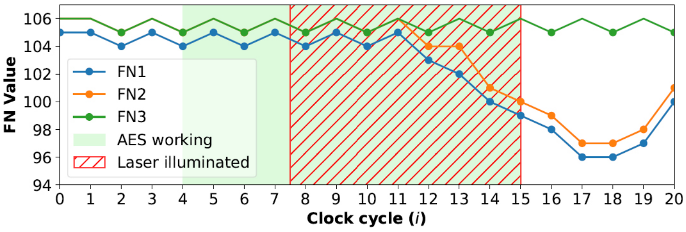


Fig. 3: Variation of *FN* over time for a laser illumination with 150 ns duration and 1,632 mW power when targeting AES core.

The first set of results shows the variation in the outcomes of the three embedded sensors ($FN1$, $FN2$, and $FN3$) over time when the AES core is active, and laser illumination is applied. As shown in Fig. 3, the green area (clock cycles 4 to 15) indicates AES activity, while the red-striped area (clock cycles 7.5 to 15, $7.5 \times 20\,\text{ns} = 150\,\text{ns}$) represents laser illumination. Before the laser illumination, $FN1$ fluctuates between 104 and 105, while $FN2$ and $FN3$ remain 1 unit higher due to $S1$'s closer proximity to AES. This fluctuation is due to slight propagation delay differences along the sensor line. During laser illumination, a significant IR drop causes $FN1$ and $FN2$ to decrease, while $FN3$, located in a different FPGA region, remains unaffected. Although $S2$ is farther than S1 from the laser spot, it is still influenced by the induced IR drop unlike $S3$ which experiences negligible impact.

B. Detectability with Multi Sensor Integration

In this analysis, we assess the detectability of three embedded sensors under laser attacks (with pulse duration of 150 ns, power of 1632 mW, and at 1,064 nm wavelength). Fault injection tests on the FPGA AES module yielded 1155 faults.

Table I highlights the detection rate of the sensors. Sensor $S1$ achieves an overall detection rate of 87.27%. Sensor $S2$ performs similarly but slightly lower detection rate (85.88%) due to its farther proximity to the target. Sensor $S3$, being farthest, has minimal detectability (1.12%) as it cannot sense the propagated IR drop. We conclude from these experiments that combining $S1$ and $S3$ effectively detects faults while minimizing false alarms caused by noise, such as voltage fluctuations, as faults affect only one sensor while noise alters both. We will dig into such details in our future work.

TABLE I: Fault Detection and Detection Rates by all sensors

Total Faults	Detected Faults			Detection Rate (%)		
	S1	S2	S3	S1	S2	S3
1155	1008	992	13	87.27	85.88	1.12

V. Conclusion and Future Directions

We proposed a lightweight TDC-based scheme to detect LFIAs by sensing laser-induced IR drops. Testing on a AMD/Xilinx Artix-7 FPGA showed that the IR drop propagates to neighboring circuits and decreases with distance from the laser spot. Thus, TDCs should be placed near areas likely targeted by adversaries. Meanwhile to decrease the false alarm rate we also benefit from the sensors placed far from the target. Our results demonstrate a detectability rate of 87%. The method is portable to other FPGAs, ASICs, and PDKs, and is robust against temperature and voltage changes thanks to its differential design. Future work will explore the impact of device aging and noise from neighboring logic, as well as examine quantitatively whether employing multi-sensor systems can enhance fault detection performance by reducing both false alarms and missed detections.

Acknowledgements

This work was supported by the National Science Foundation CAREER Award (NSF CNS-1943224). This work has partly benefited from the bilateral MESRI-BMBF project "APRIORI" from the ANR cybersecurity 2020 call.

References

[1] X. Wang et al., "A Correlation fault attack on rotating S-Box masking AES," in *Asian HOST*, 2021, pp. 1–6.

[2] S. Guilley and J.-L. Danger, "Global faults on cryptographic circuits," in *Fault Analysis in Cryptography*. Springer, 2012, pp. 295–311.

[3] H. Wei et al., "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks," in *SPACE*, 2016, pp. 27–46.

[4] M. Anik et al., "On-Chip Voltage and Temperature Digital Sensor for Security, Reliability, and Portability," in *ICCD*, 2020, Hartford, CT, USA.

[5] M. Ebrahimabadi et al., "DELFINES: Detecting laser fault injection attacks via digital sensors," *TCAD*, vol. 43, no. 3, pp. 774–787, 2023.

[6] A. H. Johnston, "Charge generation and collection in PN junctions excited with pulsed infrared lasers," *Trans. Nucl. Sci.*, vol. 40, pp. 1694–1702, 1993.

[7] R. A. C. Viera, "Simulating and Modeling the Effects of Laser Fault Injection on Integrated Circuits," Theses, Université Montpellier, Oct 2018.