

HEED: A Highly Efficient Electromagnetic Fault Detection Scheme

Roukoz Nabhan^{*}, Mohammad Ebrahimabadi[†], Jean-Luc Danger[‡], Jean-Max Dutertre^{*}, Sylvain Guilley[§],
Naghmeh Karimi[†], Raphael Viera^{*}, and Iyad Zaarour[¶]

^{*}Mines de Saint-Étienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France

[†]University of Maryland Baltimore County, United States

[‡]LTCI, Télécom Paris, Institut Mines-Télécom, 91120 Palaiseau, France

[§]Secure-IC S.A.S., France *and* ENS Information Security Group, 45 rue d'Ulm, 75,005 Paris, France

[¶]R&D Department, Yncréa Méditerranée, Toulon, France

Abstract—ElectroMagnetic Fault Injection (EMFI) is a hardware attack technique that uses EM perturbations to deliberately induce faults in integrated circuits for attack purposes. In this paper, we propose to use a Digital Sensor (DS) based on a Time-to-Digital Converter (TDC) to detect such EMFI attacks. A TDC uses a delay line to sense variations in a device's core voltage at the rate of its clock. Thus, it can detect EMFI attacks involving voltage and clock signal perturbations. The sensor output is expressed as a digital index, FN, which captures EMFI-induced delay variations. We evaluated the sensor's effectiveness on real silicon using an FPGA test vehicle through extensive experiments. The results demonstrate that a single sensor can efficiently detect 100% of faults injected into an AES crypto-accelerator while ensuring wide circuit area coverage, with a highly negligible $\approx 1\%$ false alarms rate thanks to the proposed differential fault detection methodology. To ascertain the sensor's robustness, experiments were conducted under various thermal and noise conditions. Beyond fault detection, the sensor provides insight into the EMFI mechanism. The observed behavior is consistent with a timing constraint violation fault model.

Index Terms—EMFI, timing violations fault model, EMFI-induced clock glitches, timing faults, TDC, digital sensor, FPGA.

I. INTRODUCTION

Integrated Circuits (ICs) use security features, such as cryptographic accelerators, to ensure the confidentiality and integrity of sensitive data. However, they are increasingly susceptible to hardware-based attacks. Among these, Fault Injection Attacks (FIAs) pose a critical threat by deliberately inducing faults in the hardware to compromise secret information [1]–[3]. Our research focuses on the ElectroMagnetic Fault Injection (EMFI) attacks [4], which have recently gained significant attention due to several advantages. EMFI enables a local effect, does not require chip decapsulation, and is more affordable than Laser Fault Injection (LFI) [5]. One way to protect against FIAs is to design sensors that trigger an alarm when the circuit experiences abnormal disturbances that could cause faults. To develop effective on-chip detection sensors as countermeasures against EMFI attacks, it is crucial to study the mechanism involved in injecting faults due to EM disturbances. Recently, Nabhan et al. [6] and Ghodrati et al. [7] studied EMFI mechanisms and determined that they follow a timing violation fault model. This model stems from two distinct mechanisms: timing faults caused by the coupling of the EM probe and the Power Distribution Network (PDN), and EMFI-induced clock glitches within the Clock Distribution Network (CDN).

We deployed a Time-to-Digital Converter (TDC) [8], [9] based on a delay-line to design an embedded digital sensor that can reliably detect EMFI. TDCs have been adopted in the state-of-the-art for various purposes: [10] introduced a TDC reference to compare internal and external EMFI measurements

This work was supported by the National Science Foundation CAREER Award (NSF CNS-1943224).

across different platforms; other works have used TDCs to study FIAs [11], [12] or in side-channel analysis [13]. In particular, the TDC-based sensor design from [14] aligned well with the EMFI timing violation fault model, making it a good match for our purposes (it has notably demonstrated effectiveness in detecting laser-induced fault injections [15]).

This paper reports on the ability of this fully digital sensor to detect EMFI when embedded in an FPGA. We also evaluate the risk of a false alarm, which is defined as an alarm that is raised while no attack is ongoing, under a wide range of thermal and noise conditions. Additionally, a brief analysis of EMFI mechanisms is provided to emphasize the sensor's dual function in detecting and characterizing faults caused by EMFI. Our contributions are as follows:

- Design and validation of a delay-line based TDC sensor for EMFI detection that can achieve a 100% detection rate with almost 1% false alarms demonstrating a wide circuit-level coverage with a single sensor, as validated through extensive experiments in real silicon (i.e., FPGA) via a real EMFI setup.
- Capability for early fault prevention, allowing the detection of EMFI attacks even when no faults are injected.
- Dual functionality of the TDC enabling both reliable fault detection and characterization of EMFI mechanisms.
- Introduction of an alarm triggering methodology that avoids false alarms due to thermal and noise variations.

II. RELATED WORKS

A. EMFI principle

EMFI attacks are based on the generation of a strong EM disturbance near an IC. This is achieved by sending a voltage pulse with sharp transitions into an EM injection probe (made of a few copper wire loops around a ferrite core) located over a chip. EMFI has a local effect [4]. These localized EM disturbances induce transient voltages within the target IC, disrupting its normal operation and leading to digital faults.

B. EMFI models

The root cause considered in our work stems from an EM coupling between the EM probe and two main receiving antennas of the target: its PDN, and its CDN [7]. Several fault models have been proposed in the literature, posing a challenge in the research field to clarify the EMFI physical mechanisms. Dehbaoui et al. [4] proposed the first explanation of the fault model, attributing the origin of injected faults to the violation of timing constraints. Recently, Nabhan et al. [6] highlighted on experimental basis the coexistence of at least two EMFI mechanisms. Both involve fault injection processes related to the timing violation fault model as described hereafter.

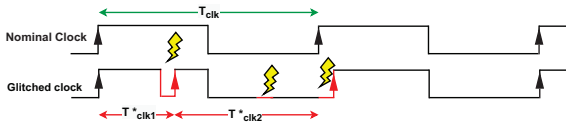


Fig. 1: EMFI-induced negative clock glitch — Principle.

1) *Timing fault mechanism*: According to this fault model [4], EMFI results in a transient decrease in the target’s supply voltage V_{dd} , which increases its gate propagation delays and leads to timing constraint violation faults [16]. The experimental results presented in [6] confirm this mechanism. They demonstrate that it occurs consistently, particularly at high frequencies when the time margin is low.

2) *EMFI-induced clock glitch mechanism*: The other mechanism involves EMFI-induced voltage glitches in the clock network due to the coupling of EM disturbances with the target’s CDN. [6] reports extensively on the conditions for inducing positive or negative clock glitches depending on the injection parameters (whether the voltage pulse is positive or negative w.r.t. the winding direction of the injection probe). Considering induction of a negative clock glitch, three distinct behaviors may happen as illustrated in Fig.1 (from left to right). When the EM injection time corresponds to the clock signal’s positive half, a transient modification of the clock signal to ground occurs. As a result, a nominal clock cycle of period T_{clk} is split into two clock sub-cycles, with periods T_{clk1}^* and T_{clk2}^* , respectively. A timing violation is then usually induced that results in faults. When the negative glitch corresponds with the clock signal’s zero half, it has no effect. When it is aligned with the rising clock edges, a shift in the clock signal edge is observed. This is not an effective glitch, a clock cycle is slightly extended while the following one is shortened. Under nominal conditions, this shift has limited impact (though the risk of timing violations still exists when the time margin is low).

For different experimental conditions (e.g., inverting the voltage pulse polarity), a positive clock glitch may happen with a behavior similar to that displayed in Fig.1, resulting an EMFI if its timing matches that of the zero half of the clock signal.

C. EMFI sensors

The study of fault mechanisms caused by EM disturbances is essential not only for understanding the physical mechanisms of faults, but also for the development of a sensor based on the actual fault model. This section provides a brief overview of the main detection sensors designed to take advantage of EMFI mechanisms. El-Baze et al. [17] designed an efficient embedded digital detector, its efficiency was tested experimentally in [6]. It proved effective at low or moderate frequencies but failed to detect many faults when the target’s clock period was set close to its maximum. Zussa et al. [18] developed a clock glitch detector as an EMFI detection sensor based on the timing fault model. Five of these sensors spread in an FPGA target proved to be insufficient to catch all injected faults (probably because they failed to see clock glitches injected into unmonitored clock paths). Other sensors exist in the state-of-the-art such as the PLL-based detector in [19], which works on the principle that EMFI attacks destabilize the operation of the ring oscillator that produces the PLL input clock. This approach is effective, but it requires the use of a PLL that is both area- and design-intensive. Similarly, Breier et al. [20]

used a Hogge-phase detector, which has a good detection rate but may incur a significant power consumption, limiting its application in ICs. In addition, Deshpande et al. [21] introduce a dual complementary flip-flop detector that offers a high detection rate but at the cost of a significant increase in area cost. Nabhan et al. [22] proposed a sensor based on the EMFI-induced clock glitch mechanism, achieving a high detection rate regardless of the injection timing. However, its activation is inherently local; faults arising from timing faults outside the sensor’s coverage area remain undetected. TDCs have been widely leveraged in hardware security. Several works [23]–[25] employed TDCs for power side-channel attacks, where power variations in cryptographic circuits are reflected as variations in TDC outputs. Hayashi et al. [26], [27] proposed TDC-based laser fault injection detection, exploiting perturbations in delay chains as indicators of laser-induced faults. Muttaki et al. [28] introduced the Fault-Time Converter (FTC) sensor, a TDC-inspired sensor scheme targeting multiple fault injection attacks (LFI, EMFI, voltage, and clock glitches). While comprehensive, their work did not address performance in terms of false and missed alarm rates. Upon reviewing the existing sensors in the state-of-the-art, it is evident that there is a need to design sensors based on the timing violation fault model, which encompasses both underlying mechanisms discussed in Sec. II-B. Such an approach prevents attackers from exploiting one fault model to circumvent another. Building on this idea, we propose a TDC-based digital sensor, whose design and evaluation are presented in the following sections.

III. PROPOSED TDC-BASED EMFI DETECTION SCHEME: HEED

The EMFI detection sensor we introduce is fully digital and has to be embedded alongside the logic it aims to protect (an AES crypto-accelerator in our case) in order to capture FIA attempts. As detailed in Sec. II, EMFI exploits timing violations through two distinct mechanisms. Therefore, we selected a digital sensor based on a TDC, because it can respond to both mechanisms: (1) timing faults caused by prolonged propagation delays, and (2) EMFI-induced clock glitches within the clock network. We present the design of the proposed TDC, along with its implementation on FPGA and basic operation.

A. Sensor design

The TDC-based sensor (referred to hereafter as the Digital Sensor, or DS) is a hardware module, which is widely used to monitor operating conditions and clock signals due to its low-cost architecture and portability across various PDKs. Fig. 2 illustrates the architecture of the DS, where a propagation path is constructed using a chain of n_0 inverters followed by a chain of n_1 inverters each driving a flip-flop (DFF). A toggling flip-flop (TFF) feeds the initial chain with the $a0$ signal which oscillates at half the system clock frequency. All flip-flops operate on the system clock, and the DS shares the same power supply and temperature conditions as the main circuit. This makes the DS a suitable solution for detecting voltage and clock glitches, as well as temperature variations [29].

The DS operates by detecting setup time violations along an intentional long critical path. Under different operating conditions or variations in clock frequency, the location of the setup violation shifts to a different flip-flop. The index of

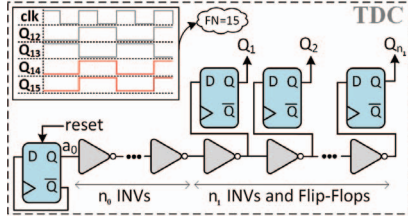


Fig. 2: Architecture of the Digital Sensor used in this study to detect EMFI.

the first flip-flop that captures such a violation is defined as the sensor output, denoted as FN (Flip-Flop Number). At the point of violation, two consecutive DFFs latch the same value, rather than the opposite values that normally result from the inverter between them, indicating the occurrence of the setup time violation at that specific index (the output FN is defined by the index of the second flip-flop in the pair; for instance, Fig. 2 illustrates a case where FN=15).

B. Sensor implementation and modes of operation

To evaluate the proposed scheme, we implemented an AES crypto-accelerator with a round-based architecture on a Xilinx Artix-7 FPGA (Digilent Nexys Video board). We also integrated three DSs (numbered 1 to 3) placed at different physical proximities to the main AES. Each DS consists of 128 inverters, with each inverter driving one DFF, i.e., in this implementation, no n_0 leading inverters are included. To introduce controllable noise, we further implemented eight AES auxiliary cores distributed around the AES and DSs (referred hereafter as noise generators 0 to 7). These noise generators can be selectively enabled to regulate both the number of active cores and their active clock cycles, thereby generating different levels of switching noise around the DSs and the main AES. Fig. 3 displays the FPGA floorplan, showing the placement of the AES, noise generators, and DSs. In our setup, the FPGA operates with a 50 MHz clock, while a UART interface is used to communicate with the FPGA and record the outputs of both the AES core and the sensors. Note that as will be discussed later only one sensor suffices yet we placed three sensors here to show the detectability rate of each sensor separately and to demonstrate that process variation is not a factor in the EMFI detectability, i.e., all three sensors operate almost similarly against EMFI attacks.

Our FPGA target is designed to evaluate the effectiveness of the TDC-based DS under EMFI attacks, to analyze the faults injected into the AES, and to study the impact of internally generated noise. Each experiment involves an AES calculation lasting 11 clock cycles and the recording of the 3 DS outputs

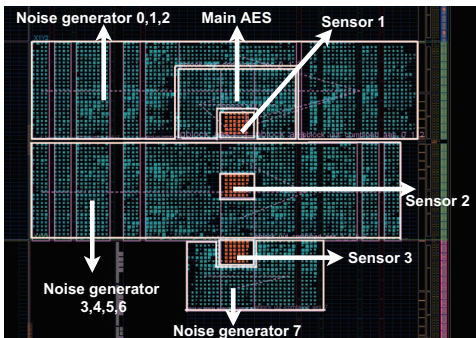


Fig. 3: FPGA floorplan of the implemented logic and DSs.

over 21 cycles (starting 4 cycles before the AES computation, and finishing 6 clock cycles later). A trigger signal is used to synchronize these operations with an applied EM perturbation (some tests did not involve any EMFI). The noise generators are used to analyze the effect of noise on the DS outputs. They are controlled by dedicated enable signals, allowing the production of either static noise (always ON) or dynamic noise (activated at precise times). Each noise generator has its own control signals, allowing it to be set OFF, continuously ON, or ON for a predefined duration, and start and end times. As a result, the noise level is controllable (with a stress level from 0 to 8) and can be applied continuously or dynamically.

C. HEED EMFI detection methodology

As mentioned earlier, the output of a DS is a digital value so called FN that depends on its operating conditions: voltage, clock frequency, and temperature. The variations of FN over time make it possible to track any variation of these parameters through their effect on the TDC. Our proposed HEED scheme operates based on the fact that any voltage shift or clock glitch induced by an EMFI (its very symptoms as reminded in Sec. II) can be detected by monitoring the FN of the embedded sensor.

The DS output (i.e., FN) is also sensitive to temperature and voltage noise (any voltage variation not linked to an attack) which may result in a false alarm if it is solely considered for EMFI detection. In other words, considering FN value thresholds and triggering an alarm when FN values exit a FN nominal range centered on nominal conditions would involve an unwanted false alarm rate caused by temperature variations or voltage legitimate noise (as exposed in the following Sec. IV). Moreover, if such a threshold is set at a high value to avoid false alarms it raises the risk of not detecting a perturbation due to an actual EMFI attack, what is called a missed alarm.

Because EMFI-induced variations are sudden, a practical solution is to monitor the absolute differential FN value variations, i.e., the change in FN value across time. This can mitigate the temperature effects on the DS output, as temperature does not change much from one clock cycle to the next, and thereby remove false alarms, defined as alarm triggering by the sensor when no EMFI is applied and the ciphertext remains fault-free. According to our proposed methodology, known as HEED, consecutive FN values are compared, and an alarm is raised when the absolute difference exceeds a threshold. However, based on the DS implementation on FPGA and the nature of analog signals, we observed that the FN values are different in even *versus* odd clock cycles. This difference is usually of ± 1 unit and in some cases ± 2 units. This occurs because the rise and fall propagation time of the signal feeding the delay chain (a_0 in Fig. 2) are different. To account for this, we compare FN in each clock cycle CC_i , denoted as FN_i , with the FN from one clock cycle earlier, FN_{i-1} . Thus, based on Eq. 1, the sensor determines whether to raise an alarm (if a threshold TH is crossed) or not. In this paper, we set $TH = 2$.

$$\text{Alarm} = \begin{cases} 1 & \text{if } |FN_{i-1} - FN_i| > TH \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

IV. EXPERIMENTAL RESULTS

In this section, we investigate the performance of the DS under EMFI attacks and assess its robustness against environmental variations, such as noise and temperature variations.

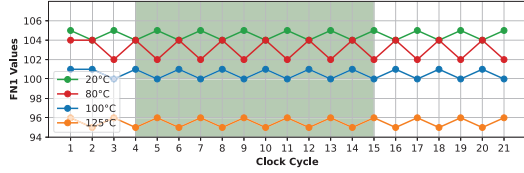


Fig. 4: FN distribution for DS1 at different temperatures (the green area corresponds to the AES computations).

A. EMFI experimental setup

Our EMFI setup includes an AV-Tech voltage pulse generator capable of generating pulses with amplitudes up to ± 750 V and pulse widths ranging from 4.5 ns to 20 ns. Two homemade EM probes were utilized. The first consists of a 0.2 mm diameter enameled copper wire wound 4 times around a 2 mm diameter cylindrical ferrite core. The second probe has a diameter of 750 μm and 5 turns.

B. HEED's sensitivity to temperature variations

For thermal experiments, we used a thermal chamber that allowed us to operate our FPGA board at different temperatures within the range of 20°C to +180°C (in practice, the maximum temperature was limited to 125°C in order to comply with the thermal tolerance of the FPGA board). For each temperature setting, FN values were recorded over 21 clock cycles, as described in Sec. III-B. Fig. 4 displays the distributions of FN values across clock cycles for the first DS sensor (DS1) at various temperatures: shifts in propagation delays, that reflect on the FN values are recorded. Depending on the temperature, DS1 output can hover around 104 – 105 at room temperature (20°C) and down to 95 – 96 when increased to 125°C (a temperature increase induces an increase of the propagation delays which translates in a decrease of FN). At a given temperature, FN hovers from 1 – 2 FN units around a stable value. Similar behavior was observed for DS2 and DS3 during the thermal experiments. This behavior aligns well with HEED's alarm triggering methodology presented in Sec. III-C: the FN variations due to temperature won't trigger false alarms.

C. HEED's sensitivity to noise

To further evaluate the DS sensors against false alarms, we studied their behavior under controlled noise generation using the 8 embedded noise generators to apply different noise levels. Two scenarios were considered: (i) static noise, where the selected noise generators remained continuously active during AES operations, and (ii) dynamic noise, where the generators were toggled ON and OFF at specific times.

1) *Static noise generation:* Fig. 5 displays the effects of different levels of static noise on DS1 (the noise level corresponds to the number of activated noise generators). No significant impact on DS1 was observed (i.e., 0% false alarm rate), thanks to the differential nature of HEED methodology (Sec. III-C). The same behavior was also observed for DS2 and DS3.

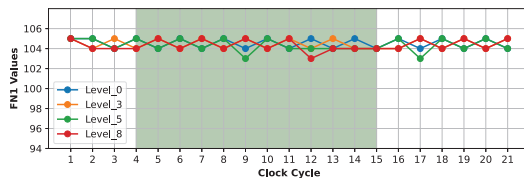


Fig. 5: FN distribution for DS1 under different static noise levels (at room temperature).

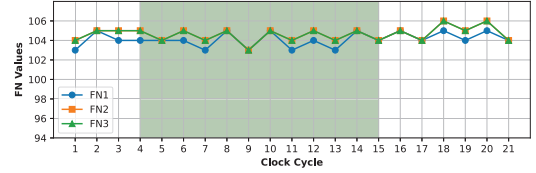


Fig. 6: FN distribution of the 3 DSs under dynamic noise, of 10 clock cycles duration, starting at the 4th clock cycle (at room temperature).

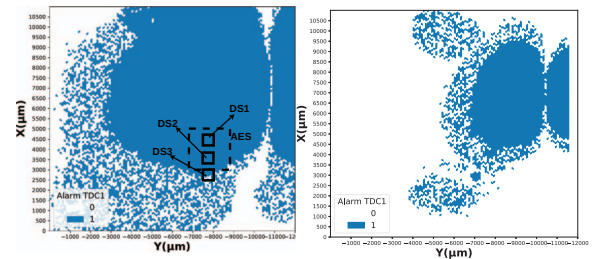
2) *Dynamic noise generation:* Extensive combinations of dynamic noise (defined as a noise dynamically set ON or OFF during to the AES operations) were tested for all levels of noise. Fig. 6 reports on an example of FN variations resulting from a dynamic noise with a level of 3 starting at the 4th clock cycle and lasting for 10 clock cycles. At most, FN experienced a 2-unit change that appeared with a delay of a few clock cycles after both the start and end of dynamic noise generation. The HEED's differential approach effectively ensures a minimal false alarm rate. This conclusion was validated across all tested noise configurations.

In sum, we conducted 1,650 noise experiments using various noise methods, as previously described, and combined with temperature variation scenarios. Across these tests, only 17 false alarms occurred (1%).

D. EMFI detection

This subsection presents our experimental results, focusing on the spatial and temporal evaluation of the sensor's performance in detecting EMFI attacks. We further examine how a DS detection threshold and the AES fault injection threshold depend on the amplitude of the injected voltage pulses.

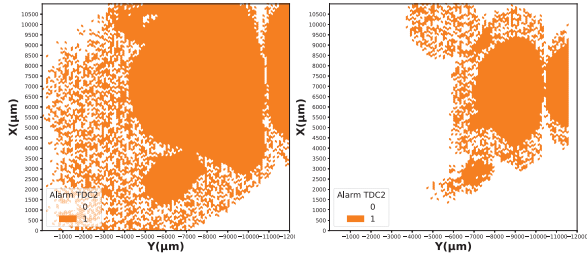
1) *Spatial exploration:* In this set of experiments, we performed spatial exploration test series with a 100 μm displacement step of the injection probe over the FPGA target in both XY directions (starting from a fixed origin, the whole FPGA die was covered). The voltage pulse amplitude threshold required to inject faults in the AES or to trigger the DS sensors depends on the electromagnetic field generated by the injection probe (we use $\varnothing 2$ mm and $\varnothing 750$ μm in our experiments, note that these thresholds increase as the diameter of the injection probe decreases [30], [31]). Fig. 7, Fig. 8, and Fig. 9 provide the sensitivity maps of the three DS sensors obtained with both probes (a color dot is placed on the map at the injection probe coordinates when an alarm is triggered according to the methodology described in subsection III-C).



(a) EM probe: $\varnothing 2$ mm; voltage pulse: (+400 V; 20 ns). (b) EM probe: $\varnothing 750$ μm ; voltage pulse: (+700 V; 20 ns).

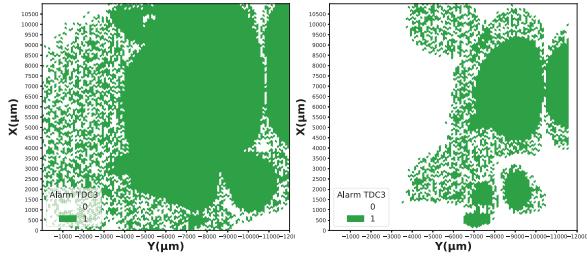
Fig. 7: Alarm sensitivity maps of DS1.

Fig. 7a displays the triggering of DS1 with blue dots when a test series was conducted with a $\varnothing 2$ mm probe, at a voltage pulse amplitude of +400 V, and width of 20 ns (the approximate



(a) EM probe: $\varnothing 2\text{mm}$; voltage pulse: (+400V;20 ns). (b) EM probe: $\varnothing 750\mu\text{m}$; voltage pulse: (+700V;20 ns).

Fig. 8: Alarm sensitivity maps of DS2.



(a) EM probe: $\varnothing 2\text{mm}$; voltage pulse: (+400V;20 ns). (b) EM probe: $\varnothing 750\mu\text{m}$; voltage pulse: (+700V;20 ns).

Fig. 9: Alarm sensitivity maps of DS3.

location of the AES core and DS sensors is highlighted with black boxes). Fig. 7b for its part was obtained for a $\varnothing 750\mu\text{m}$ probe, using a +700 V pulse amplitude and a pulse width of 20 ns. The AES fault sensitivity map is shown in Fig. 11b and discussed further in Sec. V. A comparison of both alarm and fault sensitivity maps reveals that the DS sensors successfully detected all faults injected into the AES: the alarm areas extensively cover the fault areas (the 400 V and 700 V pulse amplitude were chosen to be just above the fault injection thresholds). Comparing the two alarm maps in Fig. 7a and Fig. 7b, we observe that the larger injection probe has a significantly stronger effect on DS1, as it extends on a larger area and is obtained from a lower voltage pulse amplitude.

Fig. 8 and Fig. 9 present the alarm sensitivity maps of DS2 and DS3. In sum, in Fig. 7, Fig. 8, and Fig. 9, the left and right images show different locations where the alarm was raised under each voltage and probe condition. In the right images, the alarm was raised in fewer locations, as faults were injected at fewer locations as well. In practice, our evaluations show a 100% detection rate in all these cases.

These experiments demonstrate three main results: (i) the DSs provide a wide coverage of the EMFI-sensitive areas, (ii) the setup successfully detected 100% of the faults injected into the AES and (iii) a single DS is sufficient to achieve high detection performance. To validate these findings, we conducted multiple campaigns covering a wide range of pulse amplitudes, pulse widths, and both positive and negative polarities, using both EM probes. All experiments consistently confirmed the results described above.

2) *Fault injection and sensor detection*: Identifying the thresholds for sensor triggering and AES fault injection is crucial to selecting an optimal DS. Ideally, the sensor should trigger before a fault is induced in the AES operations. To evaluate this, we positioned the EM injection probe above the AES logic (red area in Fig. 11b). Using a 20 ns voltage pulse width, we explored a large range of voltage pulse amplitudes and identified 3 distinct behaviors as shown in Fig. 10a:

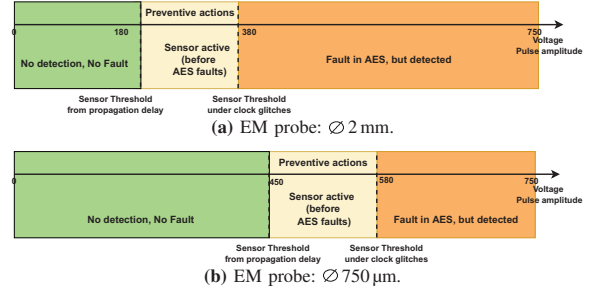


Fig. 10: Fault injection and DS1 sensor detection thresholds vs. voltage pulse amplitude.

- **Green zone (amplitude <180 V)**: No fault is injected, and the sensor is not triggered.
- **Yellow zone (amplitude 180–380 V)**: The sensor is triggered, but no fault is injected into the AES. This represents a preventive action zone, indicating that an EMFI attack is underway but has not been successful thus far.
- **Orange zone (amplitude > 380 V)**: AES faults are injected and the sensor triggers an alarm.

Since all injected faults were detected, there is 0% missed alarm and thus there are only 3 zones in Fig. 10. A similar voltage amplitude scan was conducted using a $\varnothing 750\mu\text{m}$ EM probe (Fig. 10b). The results showed three corresponding zones, comparable to those obtained with the 2 mm probe, confirming the consistency of the threshold behavior. Note that these zones are defined under normal operating conditions, i.e., room temperature and nominal power supply. Under other operating conditions, the ranges of the FNs vary accordingly yet still the missed alarm rate is 0%. The sensor outcome under other operating conditions are not shown due to space. It should be noted that the FN ranges differ across silicon setups, such as other FPGAs, as well as ASICs fabricated with different PDKs.

E. Discussion

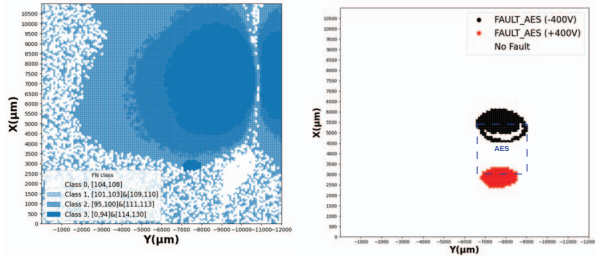
During EMFI experiments, each individual DS achieved a 100% detection rate of the injected faults. They exhibited large detection areas extending over hundreds of μm . As a result the missed alarm rate was 0%. This also means that embedding one DS is enough for highly efficient fault detection.

Noise and temperature experiments were carried out to assess the risk of false alarms (i.e. alarms triggered by legitimate conditions that do not lead to fault injection). The choice of a differential evaluation of FN values (as described in Sec.III-C) mitigates these effects and reduces the false alarm rate (1%).

The experiments reported in Sec. IV involved 13,431 EMFI attempts: 144 resulted in successful fault injection into the AES, 10,326 triggered DS1¹, and 3,105 add no noticeable effect (i.e. they did not succeed in causing a fault, nor were they detected by DS1). All the 144 injected faults were detected, yielding a 100% detection rate and zero missed alarm. DS1 was triggered 10,326 times due to actual EMFI attacks while no fault was injected: these events constitute preventive detections of an ongoing attack, they are not false alarms.

In addition, we evaluated the detection latency of HEED to be of only a few clock cycles (<3 cycles); and the hardware footprint of our TDC to be minimal, making its area overhead negligible (almost 0%).

¹This analysis focuses on a single sensor: DS1. Considering DS2 or DS3 provides the same results.



(a) EM probe: $\varnothing 2$ mm; Voltage pulse: (+400 V, 20 ns). (b) EM probe: $\varnothing 2$ mm; Voltage pulse: (+/-400 V, 20 ns).

Fig. 11: DS1 outputs map for Classes 1 to 3 (left) and fault sensitivity map (right) for a pulse set either at +400 V (red) or at -400 V (black).

V. TDC-BASED ANALYSIS OF EMFI MECHANISMS

A TDC-based sensor can serve a dual purpose: (1) detecting EMFI attacks and (2) analyzing the underlying fault injection mechanism. In this context, [6] observed a timing violation fault model based on two mechanisms: propagation delay faults and EMFI-induced clock glitches. Hence, our DS sensors are of interest to study EMFI both from the detection point and from a characterization perspective. For characterization purposes, we classified the sensor outputs into four categories depending on the FN variation range in response to an EM disturbance:

- **Class 0** ($104 \leq FN \leq 108$): Normal operating conditions of the sensor.
- **Class 1** ($101 \leq FN \leq 103$ or $109 \leq FN \leq 110$): Small variations in propagation delay.
- **Class 2** ($95 \leq FN \leq 100$ or $111 \leq FN \leq 113$): Significant variations caused by a significant propagation delay shift.
- **Class 3** ($FN \leq 94$ or $FN \geq 114$): Strong variations, corresponding to EMFI-induced clock glitches.

This classification was used to draw a map of DS1 outputs, shown in Fig. 11a for Classes 0 to 3. It provides a map of the strength of the coupling between the injection probe and the target. Note that this classification can be done for other technologies as well, yet the limits used for FN values in each class changes from one technology to another.

Fig. 12 provides examples of FN values sampled for Classes 1 to 3 (obtained for 3 different probe locations that resulted in

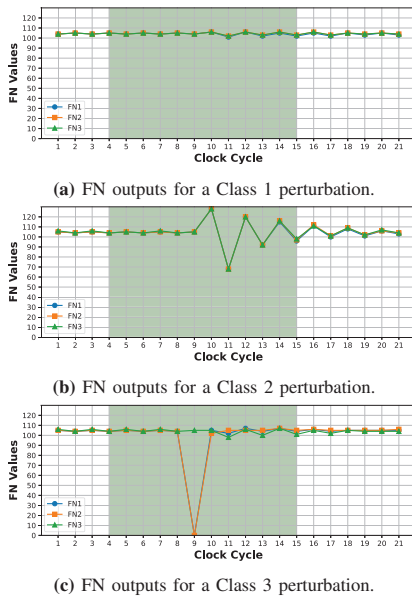


Fig. 12: FN outputs as a function of time for Classes 1 to 3 perturbations.

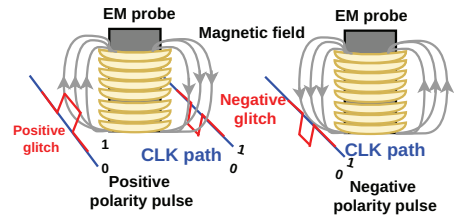


Fig. 13: Effect of EM probe positioning on glitch polarity induced in the clock network under both positive and negative voltage pulse polarities.

the injection of actual AES faults). Classes 1 and 2 correspond to timing faults arising from propagation delay variations due to the coupling of the EM injection probe with the PDN (increasing disturbances of the FN output can be observed from Fig.12a to Fig.12b). Class 3 corresponds to an EMFI-induced clock glitch, resulting from the EM probe coupling with the CDN: it introduces an additional clock edge (as illustrated in Fig. 1) resulting in a strongly reduced FN output. Fig.12c displays the effect of an EMFI-induced clock glitch on DS1 and DS2. The differences in the induced effects (which resulted in the injection of faults in the three reported cases) are an illustration of the spatial locality of EMFI. The obtained results further reinforce the validity of the dual timing violation fault model. We completed Fig.10 by including the min. voltage needed to induce propagation delay increase (Class 1), as well as the min. voltage required for inducing clock glitches (Class 3). Note that such effects occur in both sensors and AES circuitry.

Fig.11b displays the fault sensitivity map obtained with the $\varnothing 2$ mm EM probe for a pulse set either at +400 V (in red) or at -400 V (in black) and a 20 ns width, targeting the AES. We observed two distinct fault-sensitivity regions when applying voltage pulses of inverted polarities (but identical amplitude) to the upper and lower sides of the AES core. This shows that identical clock glitches (both positive clock glitches in the reported case) can be induced by voltage pulses that differ by the injection probe location and their voltage polarities (while maintaining the same injection timing).

This behavior is illustrated in Fig. 13: changing only the voltage pulse polarity for a given location inverts the resulting clock glitch polarity (as a consequence, injecting a fault would require to shift the injection time by half a clock period), while also changing the probe location can compensate for the change in voltage pulse polarity resulting in a clock glitch of the same polarity. In the latter, an EMFI is obtained for the same timing.

VI. CONCLUSION

In this paper, we developed a TDC-based digital sensor framework to detect EMFI attacks and evaluated its efficiency in real silicon (an FPGA target) under real EMFI attacks. The sensor achieved a 100% fault detection rate with large spatial coverage, as demonstrated by extensive experiments involving two EM probes and a wide range of pulse amplitudes and pulse widths. A single sensor proved to be sufficient to detect all injected faults. The proposed HEED methodology, realized based on a differential approach, was instrumental in reducing the false alarm rate to less than 1% (unwanted alarms caused by legitimate temperature variations and voltage noise) while achieving a 0% missed alarm rate. We also highlighted that the DS sensor can serve a dual purpose: detecting EMFI attacks, and characterizing the involved mechanism. The observed results were consistent with an EMFI timing violation fault model caused by both propagation delay variations and clock glitches.

REFERENCES

- [1] Q. Wang, A. Wang, L. Wu, G. Qu, and G. Zhang, "Template attack on masking AES based on fault sensitivity analysis," in *International Symposium on Hardware Oriented Security and Trust*, 2015, pp. 96–99.
- [2] X. Wang et al., "A Correlation fault attack on rotating S-Box masking AES," in *Asian HOST*, 2021, pp. 1–6.
- [3] F. Zhang, Y. Zhang, H. Jiang, X. Zhu, S. Bhasin, X. Zhao, Z. Liu, D. Gu, and K. Ren, "Persistent fault attack in practice," *Transactions on Cryptographic Hardware and Embedded Systems*, pp. 172–195, 2020.
- [4] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, 2012, pp. 7–15.
- [5] M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "How to flip a bit?" in *On-Line Testing Symposium (IOLTS), 2010 IEEE 16th International*, July 2010, pp. 235–239.
- [6] R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "A tale of two models: Discussing the timing and sampling em fault injection models," in *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, 2023, pp. 1–12.
- [7] M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, and P. Schaumont, "Inducing local timing fault through em injection," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, 2018, pp. 1–6.
- [8] D. G. Mahmoud, O. Glamočanin, F. Regazzoni, and M. Stojilović, "Practical implementations of remote power side-channel and fault-injection attacks on multitenant FPGAs," 2023, pp. 101–135.
- [9] M. T. Hasan Anik, M. Ebrahimabadi, H. Pirsivavash, J.-L. Danger, S. Guilley, and N. Karimi, "On-chip voltage and temperature digital sensor for security, reliability, and portability," in *2020 IEEE 38th International Conference on Computer Design (ICCD)*, 2020, pp. 506–509.
- [10] C. O'Flynn, "Picoemp: A low-cost emfi platform compared to bbi and voltage fault injection using tdc & external vcc measurements," in *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, 2023, pp. 60–71.
- [11] L. Zussa, J.-M. Dutertre, J. Clédière, and A. Tria, "Power supply glitch induced faults on fpga: An in-depth analysis of the injection mechanism," in *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*, 2013, pp. 110–115.
- [12] M. Paquette, B. Marquis, R. Bainbridge, and J. Chapman, "Visualizing electromagnetic fault injection with timing sensors," in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2021, pp. 1–8.
- [13] J. Gravellier, J.-M. Dutertre, Y. Teglia, and P. Loubet-Moundi, "High-speed ring oscillator based sensors for remote side-channel attacks on fpgas," in *2019 International Conference on ReConfigurable Computing and FPGAs (ReConFig)*, 2019, pp. 1–8.
- [14] M. Ebrahimabadi et al., "DELFINES: Detecting laser fault injection attacks via digital sensors," *TCAD*, vol. 43, no. 3, pp. 774–787, 2023.
- [15] M. Ebrahimabadi, R. Viera, S. Guilley, J.-L. Danger, J.-M. Dutertre, and N. Karimi, "Multi-sensor data fusion for enhanced detection of laser fault injection attacks in cryptographic hardware: Practical results," in *2025 Design, Automation & Test in Europe Conference (DATE)*, 2025, pp. 1–2.
- [16] L. Zussa, J.-M. Dutertre, J. Clédière, B. Robisson, A. Tria et al., "Investigation of timing constraints violation as a fault injection means," in *27th Conference on Design of Circuits and Integrated Systems (DCIS), Avignon, France, 2012*, 2012, pp. 1–6.
- [17] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital EM pulse detector," in *Design, Automation & Test in Europe Conference & Exhibition*, 2016, pp. 439–444.
- [18] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clédière, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.
- [19] N. Miura, Z. Najm, W. He, S. Bhasin, X. T. Ngo, M. Nagata, and J.-L. Danger, "PLL to the rescue: A novel EM fault countermeasure," in *Design Automation Conference*, 2016, pp. 1–6.
- [20] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using Hogge phase-detector," in *International Symposium on Quality Electronic Design*, 2017, pp. 307–312.
- [21] C. Deshpande, B. Yuce, L. Nazhandali, and P. Schaumont, "Employing dual-complementary flip-flops to detect EMFI attacks," in *Asian Hardware Oriented Security and Trust Symposium*, 2017, pp. 109–114.
- [22] R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "Em fault injection-induced clock glitches: From mechanism analysis to novel sensor design," in *2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2024, pp. 1–7.
- [23] N. G. Jayasankaran, H. Guo, S. Patnaik, J. Hu et al., "Securing cloud fpgas against power side-channel attacks: A case study on iterative aes," *arXiv preprint arXiv:2307.02569*, 2023.
- [24] D. R. Gnad, V. Meyers, N. M. Dang, F. Schellenberg, A. Moradi, and M. B. Tahoori, "Stealthy logic misuse for power analysis attacks in multitenant fpgas," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2021, pp. 1012–1015.
- [25] M. Probst, L. Tebelmann, M. Wettermann, and M. Pehl, "Remote side-channel analysis of the loop puf using a tdc-based voltage sensor," *Journal of Cryptographic Engineering*, vol. 15, no. 1, p. 1, 2025.
- [26] S. Hayashi, J. Sakamoto, and T. Matsumoto, "Design methodology of digital sensors for detecting laser fault injection attacks in fpgas: S. hayashi et al." *Journal of Cryptographic Engineering*, vol. 15, no. 2, p. 12, 2025.
- [27] S. Hayashi, J. Sakamoto, M. Chikano, and T. Matsumoto, "Effective layout design for laser fault sensor on fpga," in *Proceedings of the 2023 Workshop on Attacks and Solutions in Hardware Security*, 2023, pp. 103–112.
- [28] M. R. Muttaki, T. Zhang, M. Tehranipoor, and F. Farahmandi, "Ftc: A universal sensor for fault injection attack detection," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022, pp. 117–120.
- [29] C.-C. Chen, C.-L. Chen, W. Fang, and Y.-C. Chu, "All-digital cmos time-to-digital converter with temperature-measuring capability," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 9, pp. 2079–2083, 2020.
- [30] A. Beckers, M. Kinugawa, Y. Hayashi, D. Fujimoto, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Design considerations for em pulse fault injection," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2019, pp. 176–192.
- [31] J. Toulemont, G. Chancel, J. M. Gallière, F. Mailly, P. Nouet, and P. Maurine, "On the scaling of emfi probes," in *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE, 2021, pp. 67–73.