EM Fault Injection-Induced Clock Glitches: From Mechanism Analysis to Novel Sensor Design

Roukoz Nabhan, Jean-Max Dutertre, Jean-Baptiste Rigaud, Jean-Luc Danger, Laurent Sauvage

Authors' version
IOLTS 2024
DOI: 10.1109/IOLTS60994.2024.10616074

EM Fault Injection-Induced Clock Glitches: From Mechanism Analysis to Novel Sensor Design

Roukoz Nabhan*, Jean-Max Dutertre*, Jean-Baptiste Rigaud*, Jean-Luc Danger† and Laurent Sauvage†
*Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France
†LTCI, Télécom Paris, Institut Mines-Télécom, 91120 Palaiseau, France
*{roukoz.nabhan, dutertre, rigaud}@emse.fr †{jean-luc.danger, laurent.sauvage}@telecom-paris.fr

***Abstract*—This paper introduces a novel sensor that is capable of detecting faults injected by electromagnetic disturbances. The sensor has been designed with a deep understanding of the physical mechanisms of ElectroMagnetic Fault Injection (EMFI). A recent study has identified an EMFI mechanism based on the timing violation fault model, which highlights the coexistence of two distinct mechanisms: electromagnetic disturbances that are coupled to the target's power distribution network, which can cause timing faults by extending the propagation time beyond the clock period, and disturbances that are coupled to the target's clock distribution network, which can cause timing constraint violations due to EMFI-induced voltage glitches within the target's clock tree. Building on this work, we have investigated the mechanism of EMFI-induced clock glitches, providing useful insights for designing a new sensor. The sensor incorporates two dummy clock paths that are maintained in a frozen state within the circuit, and is capable of detecting both positive and negative EMFI-induced glitches along these paths. The proposed sensor offers significant advantages, including full digitization, ease of implementation, low cost in terms of silicon area, low power consumption, and a high fault detection rate. Accurate design and experimental tests were performed on an FPGA board. Validation experiments were supported by spatial and temporal sensitivity maps covering the full-frequency spectrum of the target, which confirmed the effectiveness of the sensor.**

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

I. Introduction

Securing connected objects remains an ongoing challenge. The confidentiality and integrity of their data can be threatened by hardware attacks, in particular Fault Injection Attacks (FIA), which aim at forcing faults during their computations. Our research focuses on ElectroMagnetic Fault Injection (EMFI) attacks among the various FIA techniques existing in the literature. From an attacker's point of view, EMFI offers attractive advantages. Since it is efficient and local, faults can be injected into a selected part of a target, it does not necessarily require the chip package to be open and it is more affordable than laser FIA [1]. One method of preventing these attacks is to develop sensors that detect abnormal phenomena that can lead to the creation of faults. In order to develop effective on-chip detection sensors as a countermeasure against EMFI attacks, it is crucial to study the mechanisms involved in fault injection due to EM disturbances. There have been numerous state-of-the-art efforts to investigate the origins of EMFI-induced faults [2]–[7] and to explore various approaches to designing dedicated EMFI sensors based on these mechanisms [8]–[12].

Recently, Nabhan et al. [7], [13] have demonstrated that electromagnetic-induced fault can occur through two distinct mechanisms within the timing violations fault model: timing faults, resulting from EM disturbances coupling with the target's Power Distribution Network (PDN), and EMFI-induced clock glitches within the target's Clock Distribution Network (CDN). They performed an in-depth analysis of these models, which were corroborated by rigorous experimentation results tested and validated on an Field-Programmable Gate Array (FPGA) board.

In this work, we have investigated the mechanism of the EMFI-induced clock glitches, providing useful insights for the design of a novel sensor capable of EMFI detection. This sensor basically integrates two dummy clock paths, which are maintained in a frozen state within the circuit and is capable of detecting both positive and negative glitches induced by EMFI along these paths. Through numerous experiments conducted on an FPGA board, we evaluated the spatial and temporal performance over the target's full-frequency range, demonstrating the effectiveness of the sensor in detecting EMFI faults. In addition to its high detection rate, this sensor offers several advantages such as full digitization, ease of implementation, low cost in terms of silicon area, and low power consumption.

Our contributions are outlined as follows:

- Designed a novel sensor for EMFI detection that incorporates two dummy clock paths in a frozen state, with advantages including full digitization, ease of implementation, and low cost in terms of silicon area.
- Demonstrated its robust EMFI detection through rigorous experimental results validated on an FPGA board.
- Investigated the mechanism of EMFI-induced clock glitches.

The remainder of this paper is organized as follows: Section II provides a reminder of the principle of EMFI and the related work which that considers various mechanisms of EMFI models and EMFI sensors. Section III outlines the motivation behind the basis of the novel sensor, and describes the architecture. Section IV details our experimental EMFI setup and section V and discusses the implementation of this detector. The experimental results are reported and analyzed in section VI with a focus on the spatial and temporal performance of the sensor over the target's full-frequency range. Finally,

This work was supported by the French National Research Agency (ANR) under grand ANR-20-CYAL-0007

section VII provides the conclusion and our future work.

II. Backgrounds

A. EMFI principle

EMFI attacks are based on the generation of an EM disturbance near an Integrated Circuit (IC). This is achieved by sending a voltage pulse with sharp transitions into an EM probe (made of a few copper wire loops around a ferrite core) located over a chip. EMFI has a local effect [4], [5], [9], [14]. These localized EM disturbances induce a transient voltage within the chip, corrupting its normal operation and causing digital faults.

B. EMFI models

Several fault models have been proposed in the literature, posing a challenge in the research field to clarify the physical mechanisms of EM fault injection. In 2012, Dehbaoui et al. [5] proposed the first explanations of the fault model, attributing the origin of injected faults to the violation of timing constraints. The model, known as the "timing fault model", highlights the increase in propagation time in combinational logic due to the decrease in supply voltage during EMFI attacks. They hypothesized that the EM field generated by the injection probe couples with the target's power distribution network (V_{dd} and Gnd). In contrast to the timing fault model, Ordas et al. [2], [15] introduced the "sampling fault model" in 2017, by observing the effect of EM disturbances on the sampling operation of the D Flip-Flop (DFF) around the clock rising edge which is at a vulnerable moment during an IC operation. In 2018, Ghodrati et al. [4] studied the effect of EMFI on power, clock and reset networks, demonstrating that the clock is the most affected network. They highlighted that faults occur due to EMFI-induced glitches in the clock network.

In 2023, recent publications [13] reveal the coexistence of at least two mechanisms during an EMFI attack, proven by experimental results spanning the full-frequency range of the target. One mechanism involves timing faults resulting from EM disturbances coupling with the target's PDN by extending the propagation time beyond the clock period. The other mechanism involves EMFI-induced voltage glitches on the clock network due to the coupling of EM disturbances with the target's CDN. These two physical mechanisms are regrouped under the timing violation fault model. This is the first study that shows the possibility to isolate the origin of the injected faults, whether arising from either of these mechanisms. It is determined by considering several factors such as the circuit's clock frequency, the EM injection time and the pulse voltage parameters (amplitude and width). The same authors completed their explanation in [7] by elucidating the principle and the characteristics of these mechanisms. These mechanisms are described hereafter.

1) Timing faults mechanism: Dehbaoui et al. [5] suggested that EMFI could induce timing faults. This is caused by a transient decrease in the supply voltage V_{dd}, which induces an increase in the propagation delay t_p of the target's logic gates. At a given level of increasing t_p, a timing constraint violation occurs, and a fault is injected [16]. The experimental results presented in [7], [13] confirm the existence of timing faults mechanisms. They demonstrate that this mechanism occurs consistently, but more readily at high frequencies (close to the maximum clock frequency) due to the short timing slack compared to lower clock frequencies. The timing fault model has four main characteristics suggested in [5] and demonstrated in [7]:

- Faults are injected into the target's critical paths.
- Fault incidents gradually escalate with rising EM stress.
- Faults are contingent on input data given that logic propagation times are data-dependent.
- The faults that arise are 100% reproducible.

2) EMFI-induced clock glitches mechanism: Nabhan et al. [7] demonstrate that EMFI-induced clock glitches in the clock tree due to the coupling of EM disturbances with the CDN. They perform a detailed analysis of EMFI-induced clock glitches characteristics and delineate the conditions for inducing positive or negative clock glitches based on the voltage pulse polarity. Fig.1 depicts three distinct behaviors for each voltage pulse polarity, highlighted in red from left to right.

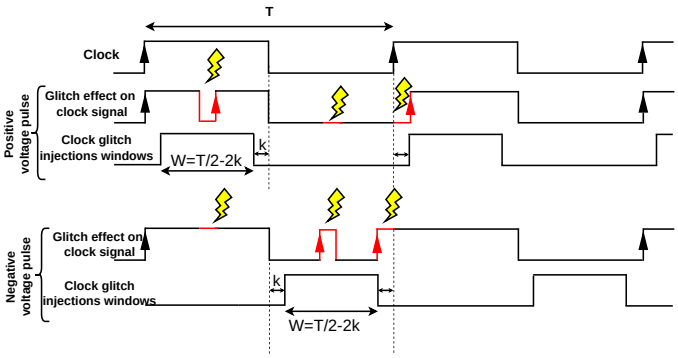


Fig. 1: EMFI-induced clock glitch principle.

In case 1, a positive voltage pulse induces negative glitches: when the EM injection time corresponds to the clock signal at level '1', negative glitches are induced with an additional clock rising edge in the target's clock signal. It has no effect when it corresponds with the clock signal at level '0'. When the EM injection timing is just after the rising clock edges, a shift in the clock signal edge is observed, denoted by a constant margin k. It is related to the induced clock glitch width. This is not an effective glitch, where the clock edges get a small shift. In fact, it extends one clock period and shortens the following one. In case 2, a negative pulse induces positive glitches: when the EM injection time corresponds to the clock signal at level '1', there is no effect. When it corresponds with the clock signal at level '0', positive glitches are induced along with an additional clock rising edge in the target's clock signal. When the EM injection timing is just before the rising clock edge, a shift in the clock signal is observed during a constant margin k. This is not an effective glitch, where the clock edges get a small shift. In fact, it shortens one clock period and extends the following one. Thus, they established that the mechanisms of EMFI-induced clock glitches depend on the clock frequency, and the

susceptibility window for injecting effective glitches (positive or negative) through EMFI attacks is related to T/2. The width of the susceptibility windows caused by clock glitches under EMFI attacks can be calculated in the following eqt. 1, where k is a constant margin where clock edges get a small shift under EMFI attacks.

$$W_{EMFI\ susceptibility\ windows} = T/2 - 2k \quad (1)$$

C. EMFI sensors

The study of fault mechanisms caused by electromagnetic disturbances is essential not only for understanding the physical mechanisms of faults, but also for the development of a sensor based on the identified models. This section provides a brief overview of the main detection sensors available in the state of the art, designed according to different models described in the previous section.

El-Baze et al. [8] designed an efficient embedded digital detector, based on the sampling fault model. Subsequently, Nabhan et al. [7], [13] evaluated the performance of this sensor within an AES accelerator of an FPGA, testing its functionality across the full-frequency range of the target. In this study, they ascertained the validation of the timing violations fault model. However, they observed instances where the sensor turned out to be effective at low or moderate frequencies but proved inadequate against faults injected at high frequencies close to the maximum target frequency, suggesting its limitations beyond its intended design context.

The closest related work to our research is the study conducted by Zussa et al. [9]. They developed a clock glitch detector as an EMFI detection sensor based on the timing violations fault model. Its operation is based on the insertion of a configurable delay block, called the ”guard delay block”, must be greater than the maximum propagation delay of the combinational logic critical path but less than the clock period. In the initial configuration performed by Zussa et al., five of these sensors were evaluated, which was proved to be insufficient to achieve an optimal detection rate. This underscores the need to increase both the number of sensors and their strategic placement at each extremity of the clock tree. Further testing is required to examine and improve the effectiveness of this sensor in detecting localized clock glitches induced by EMFI.

Other sensors exist in the state-of-the-art such as the PLL-based detector [11], which works on the principle that EMFI attacks destabilize the operation of the ring oscillator. Incorporating clock generators may prove impractical for ASIC and FPGA designs. Similarly, Breier et al. [10] use a Hogge-phase detector, which has a good detection rate but may incur a significant power consumption, limiting its application in integrated circuits. In addition, Deshpande et al. [12] introduce a dual complementary flip-flop detector that offers a high detection rate but at a significant increase in area cost.

Upon reviewing the existing sensors in the state of the art, it is evident that there is a need to design novel sensors with improved fault detection rate. Furthermore, to the best of our knowledge, no sensor design has been proposed in the literature that is specifically tailored to detect faults due to the EMFI-induced clock glitch mechanisms [7]. Our study contributes to the design of a novel sensor based on this model, which is discussed in the following sections.

III. Novel sensor: Frozen dual-clock detector

In this section, we discuss the main idea behind our proposed sensor and its architecture. The timing violations fault model explained in [7], which involves the 2 mechanisms induced by EMFI described in the previous section, provides useful insights for designing a new sensor. The design of this sensor should meet several specifications including full digitization, ease of implementation, low cost in terms of silicon area, low power consumption, and a high fault detection rate.

A. EMFI-induced clock glitches mechanism

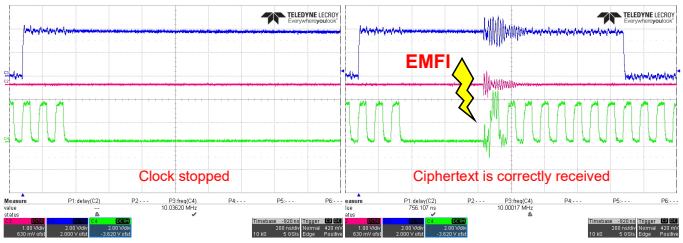


Fig. 2: Freezing the AES clock signal.

To validate the EMFI-induced clock glitch mechanism, Nabhan et al. [7] conducted a test wherein they froze the input clock of the AES computation blocks. The aim was to demonstrate that the glitches induced on the clock signal were effective in replacing a genuine clock rising edge. They used a BUFfer Global (BUFG) with a Clock-Enable (CE) to gate the clock signal. In the unfreeze case, when the CE is asserted, the clock signal passes through the buffer. However, in the freeze case, when the clock has stopped, the output of the buffer is held at logic ‘0’ as the CE is deasserted. An FSM controlled the CE of the buffer. Once the AES counter reached the predefined value, it entered into a closed state, deasserted the CE and the clock signal was held at a low level. This is the freeze case, as shown on the left side of Fig. 2. The clock signal is stopped, blocking the flow of the AES calculations. The FSM was designed in order to automatically exit the freeze state on the next clock cycle, but because the clock signal was stopped in a low state, the FSM remains frozen in a deadlock: it needs a clock rising edge to exit the freeze state and resume the clock signal to normal. The test conclusively demonstrated that a negative pulse induces positive glitches in the clock signal, effectively replacing a genuine clock rising edge as shown on the right side of Fig. 2 under EMFI attacks, where they received an accurate ciphertext. These tests confirm that EMFI does indeed induce clock glitches in the target’s CDN that are capable of replacing genuine clock rising edges. This mechanism is validated in two scenarios: dynamically during normal clock signal operation, and statically when the clock is stopped. Consequently, this test provides a valuable insight into the use of a freezing clock signal as a detector for EMFI-induced clock glitches.

B. Concept and implementation strategy

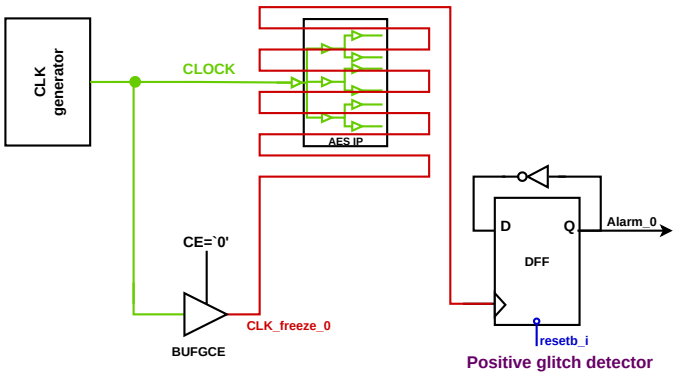


Fig. 3: Concept and implementation strategy of the proposed sensors.

Our approach is grounded in the use of frozen clock signals in a static state capable of detecting any glitches or disturbances induced by EMFI. Extending this concept, we have developed a new sensor based on models of EMFI-induced clock glitches. The concept of the sensor is illustrated in Fig. 3, where a dummy clock is used in a frozen state (shown in red) and the routing path of the clock is distributed in a serpentine form across the sensitive cryptographic blocks (such as AES) to protect them against EMFI. A DFF is clocked by the dummy clock path and its output is inverted and fed back to the input. Under normal conditions, the DFF output remains at a low level because no clocks are present, but it passes to a high level due to the possible glitches induced under EMFI attacks along the path. The proposed routing of the dummy clock paths allows for extensive coverage of injected faults by EMFI, as it is distributed within the target's main clock network.

In the case of an FPGA implementation, the routing of the sensor's dummy clock paths based on the proposed concept is limited to be accomplished on an FPGA board because the clock network is prefabricated as part of the FPGA architecture. However, this challenge is mitigated in the case of an ASIC implementation. We initially planned to validate this sensor using an FPGA board. Confronted with the challenge of routing the sensor's clock signal in a serpentine form to cover the target circuit's clock tree on an FPGA board, we opted to place multiple numbers of the proposed sensor on the circuit's floorplan.

C. Basics of sensor design and operation

The sensor architecture is illustrated in Fig. 4. The clock signal, generated by the clock generator block, is highlighted in green (CLOCK) in Fig. 4. The frozen dual-clock detector consists of two frequency dividers:

- Positive glitch detector: sampled on the rising edge. It is driven by a dummy clock signal in a low-level frozen state, called CLK_FREEZE_0. This signal is output by BUFGCE, which takes the clock signal (in green) as input and delivers CLK_FREEZE_0 as output. It is responsible for detecting positive glitches induced by EMFI.
- Negative glitch detector: sampled on the falling edge. It is driven by a dummy clock signal in a high-level frozen state, called CLK_FREEZE_1. This signal is output by BUFGCE_1, which takes the clock signal (in green) as input and delivers CLK_FREEZE_1 as output. It is responsible for detecting negative glitches induced by EMFI.

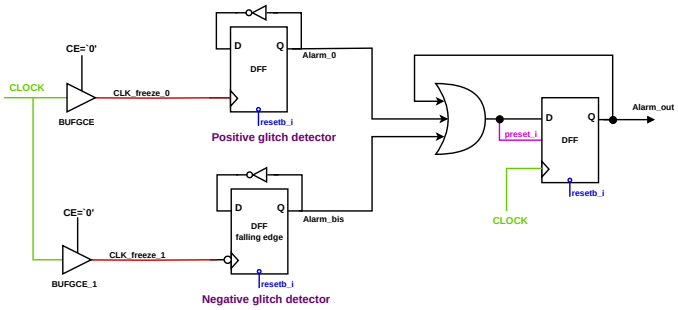


Fig. 4: The architecture of the frozen dual-clock detector.

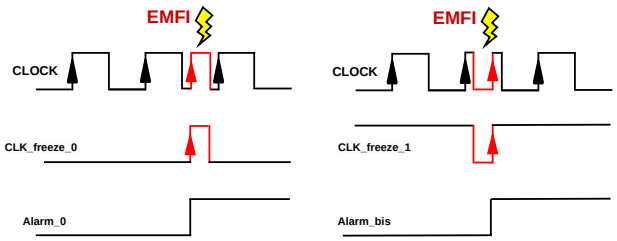


Fig. 5: Animation of the sensor alarm activation for positive (left) and negative (right) glitches induced by EMFI on the clock signals.

Under EMFI attacks, multiple glitches can be induced. An even number of glitches induced on a clock signal can activate the alarm output with one glitch and deactivate it with subsequent glitch. To avoid the possibility of missed detection, we added a DFF fed by the output of the OR gate of ALARM_0 and ALARM_BIS to the asynchronous *preset_i* input. Additionally, a feedback loop was incorporated to maintain the state of the alarm output, which acts as the final output ALARM_OUT of the sensor. An animation of the EMFI-induced clock glitches cases to activate the alarm signal are shown in Fig. 5.

In the following sections, we evaluate the performance of this sensor within an AES accelerator of an FPGA by testing its spatial and temporal functionality over the full-frequency range of the target.

IV. Experimental Setup

Our EMFI experimental 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. For the EM probe, we used a homemade EM probe consisting of a 0.2 mm diameter enameled copper wire wound 4 times around a cylindrical ferrite core with a diameter of 2 mm. For the FPGA target tested under EMFI attacks, we selected a Nexys

Video 7 board, which embeds an Artix-7, XC7A200T FPGA manufactured in a 28 nm CMOS technology.

V. Sensors Implementation

To investigate sensor efficiency, our device under test (DUT) design assembles sensors distributed in an AES accelerator. It consists of a hardware 128-bit AES accelerator that executes a full encryption in 11 clock cycles and 32 sensor blocks. In addition, a clock generator block is integrated to generate clock signals, allowing remote control of the target by dynamically changing the target's clock frequency without modifying the bitstream file. A serial data link (UART) for communication purposes and a finite state machine block to manage the execution flow are added, which both operating by a distinct and fixed clock frequency of 100 MHz. The max. DUT clock frequency was measured above 200 MHz ($t_{critical} \approx 4.5$ ns as clock period).

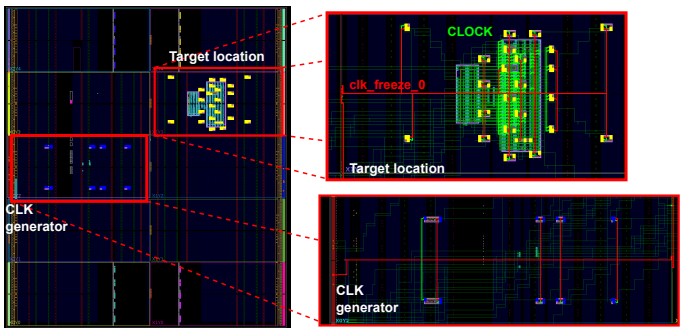


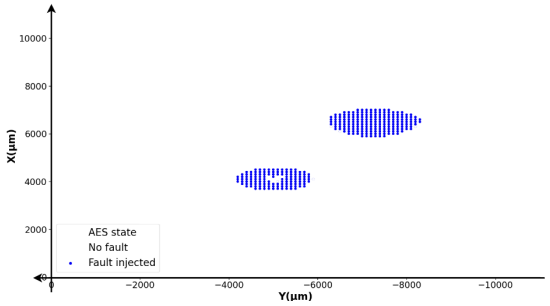
Fig. 6: Target's floorplan from Vivado showing the sensor's distribution within the design logic blocks.

Fig. 6 provides the floorplan of the design, extracted from the Vivado tool. On the left side of Fig. 6, the AES blocks (target location) are placed away from the clock generator to differentiate the effects of the EM disturbance on it from those on the clock generation block (CLK generator). The 32 sensor blocks are distributed in the floorplan. 24 sensors highlighted in yellow located within the AES blocks, while others are positioned around the AES blocks in the target location region. The remaining sensors are distributed in the clock generator region, highlighted in blue. A close-up view (top right) shows the routing of the clock signal (CLOCK), highlighted in green, generated by the clock generator fitted to the AES computations block. The routing of the low-level frozen clock signal (CLK_FREEZE_0) for these sensors is shown in red, while the high-level frozen clock signal (CLK_FREEZE_1) is routed alongside, requiring increased zooming to distinguish them by color. The location of these sensor blocks is fixed to ensure that the sensor's dummy clock paths are routed within the main clock signal (CLOCK) according to the sensor's specifications. Similarly, the close-up view (lower right) shows the clock signals for the sensors distributed in the clock generator region.

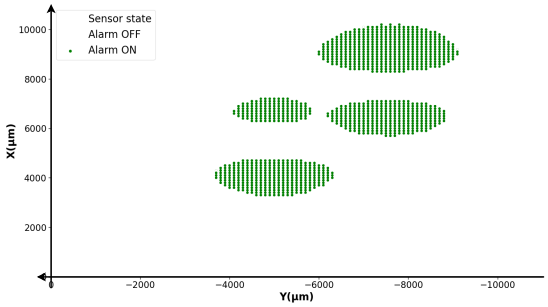
VI. Experimental Results

In this section, we present the experimental results from our campaigns, which aimed at testing the spatial and temporal exploration of the sensor's performance in detecting EMFI attacks across the full-frequency range from low frequencies up to the target's max clock frequency of 200MHz.

A. Spatial exploration of sensor performance



(a) EMFI sensitivity maps for faults injected into AES.



(b) EMFI sensitivity maps for triggering sensors.

Fig. 7: EMFI sensitivity maps launched at 100 MHz (pulse width=4.5 ns, pulse amplitude= +420 V).

In our initial experiments, we conducted a spatial mapping campaign launched with a 1 µm step, operating the circuit at 100 MHz. We configured the pulse amplitude to +420 V, the pulse width to 4.5 ns and the EM injection delay time is fixed to coincide with the clock signal at a high-level, as we anticipated to test the induction of negative glitches due to the positive voltage pulse. Fig. 7a depicts the sensitivity map for injected faults into the AES computations: for a position (X,Y) of the EM probe, points are shown in blue if the ciphertext is faulted, and in white otherwise, resulting in two distinct blue areas. Fig. 7b shows the sensitivity map for triggering sensors, where the green points represent the triggering for at least one of the 32 sensors, resulting in 4 different green areas.

Note that we rigorously ascertained the correspondence between the design logic blocks and the EM sensitive areas by testing several different locations of the logic (AES and/or CLK generator) on the FPGA floorplan and observing the effect on the location of the sensitive areas. The blue area on the right in Fig. 7a corresponds to the location of the AES block, while the other blue area corresponds to the location of the clock generator block. The validation of the correlation was based on analyzing the results of the spatial mapping of the sensor triggering. To gain a deeper understanding of this correlation between the green areas and the triggering sensors, we distinguish the sensor alarm output to ALARM_0 and ALARM_BIS in order to identify the origin of the alarm triggering and determine whether they were caused by negative

or positive glitches induced by EMFI. The two green areas on the right side of Fig. 7b correspond to the triggering of the 24 sensors located in the AES blocks region, as shown in Fig. 6, while the other two areas correspond to the 8 sensors located in the clock generator region.

Therefore, the EM sensitivity map of the triggering sensors ascertains a high detection rate, since all the faults injected into the AES computations are detected. We also emphasized the importance of spatially distributing the sensors within and around the cryptographic blocks with ensuring a high sensor density to guarantee the efficiency of the sensor. Several spatial mapping campaigns were carried out, wherein the clock frequency was varied from 10 MHz to 170 MHz, keeping the same parameters and the same implementation of these 32 sensors. All the results of these campaigns show the high detection rate for this proposed sensor.

B. Temporal exploration of sensor performance

In this section, we conduct a temporal exploration of the sensor's effectiveness in detecting EMFI attacks at both low and high frequencies. Based on the spatial mapping of Fig. 7a, we positioned the EM injection probe in the center of the AES accelerator sensitive area. Fig. 8 shows the results of the

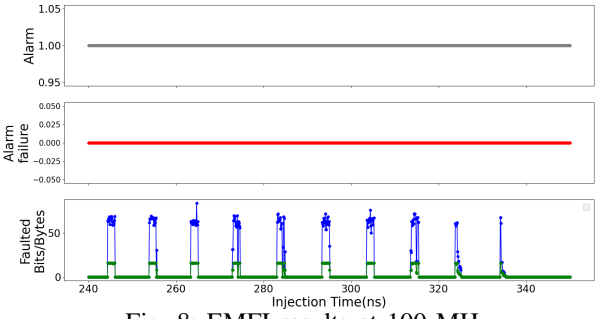


Fig. 8: EMFI results at 100 MHz

campaign launched at 100 MHz with the pulse amplitude set to +420V and a pulse width of 4.5 ns. The gray curve Alarm, representing the alarm state, changes to '1' when one of these 32 sensors is triggered. It shows that it remains at logic state '1' throughout this campaign. The green and blue curves represent the number of faulted bits and bytes (FBB) read from the AES ciphertext, reflecting the same behavior observed in [7]. The red curve, Alarm Failure (AF), remains zero throughout the experiment, proving that all injected faults were detected. Thus, the sensor demonstrates a high detection rate for experiments performed at low frequencies. The same behavior is observed with increasing circuit frequency at high frequencies, reaching up to 200 MHz, close to the circuit's max. frequency. Fig. 9 shows the temporal mapping of the campaign conducted at 200 MHz with a voltage pulse amplitude of +420 V and a width of 4.5 ns. The sensor maintains a 100% fault detection rate throughout the experiments, confirming its effectiveness in detecting any form of glitch, regardless of the EM injection time. To evaluate the effectiveness of this sensor against faults injected according to the timing fault model, we repeat the same campaign at 200 MHz but with a reduced voltage pulse amplitude to +300V.

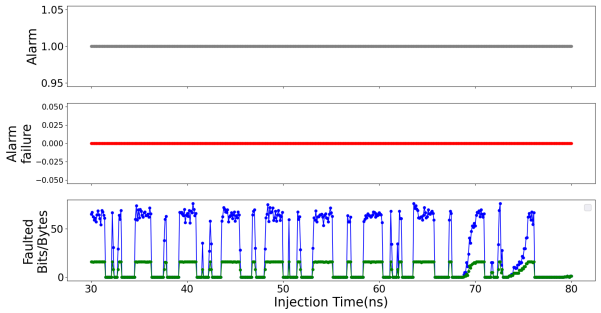


Fig. 9: EMFI results at 200 MHz (+420 V voltage pulse).

The results, shown in Fig. 10, highlight the effectiveness in detecting faults according to the timing fault model obtained at high frequencies, thanks to the adequate distribution with high density of the sensors around the AES computation block. Therefore, the sensor exhibits a high efficiency in detecting induced glitches, positive or negative, as well as injected faults according to the timing fault model.

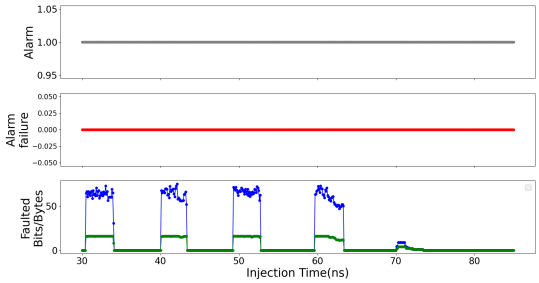


Fig. 10: EMFI results at 200 MHz (+300 V voltage pulse).

VII. Conclusion

This paper explores a novel EMFI detection sensor characterized by full digitization, low-cost at silicon area and low power consumption. The sensor's architecture is based on routing two dummy clock paths in a frozen state at low and high levels to respectively detect positive and negative glitches induced by EMFI along these paths. The use of these dummy clock paths alleviates temporal constraints and avoids the risk of undetected injected fault windows depending on the EM injection time. Experimental results validate the sensor's effectiveness, demonstrating a high fault detection rate tested and proven through spatial and temporal performance exploration over the target's full-frequency range. Furthermore, it is established that the routing of the dummy clock paths within the clock network is crucial for ensuring spatial coverage for EMFI detection, with a dense distribution of sensors across logic design blocks. Further works are still needed to consolidate these findings through additional experiments and to investigate the optimal sensor spacing to maintain a high fault detection rate.

REFERENCES

[1] M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "How to flip a bit?" in 2010 IEEE 16th International On-Line Testing Symposium. IEEE, 2010, pp. 235–239.

[2] M. Dumont, M. Lisart, and P. Maurine, "Modeling and simulating electromagnetic fault injection," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp. 680–693, 2020.

[3] S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine, "Evidence of a larger em-induced fault model," in International Conference on Smart Card Research and Advanced Applications. Springer, 2014, pp. 245–259.

[4] 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). IEEE, 2018, pp. 1–6.

[5] 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.

[6] M. Zhang, H. Li, and Q. Liu, "Deep exploration on fault model of electromagnetic pulse attack," IEEE Transactions on Nanotechnology, vol. 21, pp. 598–605, 2022.

[7] 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 FDTC 2023–Twentieth Workshop on Fault Diagnosis and Tolerance in Cryptography, 2023.

[8] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital em pulse detector," in 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 2016, pp. 439–444.

[9] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, 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.

[10] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using hogge phase-detector," in 2017 18th International Symposium on Quality Electronic Design (ISQED). IEEE, 2017, pp. 307–312.

[11] 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 Proceedings of the 53rd Annual Design Automation Conference, 2016, pp. 1–6.

[12] C. Deshpande, B. Yuce, L. Nazhandali, and P. Schaumont, "Employing dual-complementary flip-flops to detect emfi attacks," in 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST). IEEE, 2017, pp. 109–114.

[13] R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "Highlighting two em fault models while analyzing a digital sensor limitations," in 2023 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2023, pp. 1–2.

[14] F. Poucheret, L. Chusseau, B. Robisson, and P. Maurine, "Local electromagnetic coupling with CMOS integrated circuits," in Proceedings of the International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMC COMPO), pp. 137–141.

[15] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 183–197, 2017.

[16] L. Zussa, J.-M. Dutertre, J. Clédiere, 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, pp. 1–6.