Capture the Pulse: Impact of FPGA Resource Utilization on EM Fault Injection Attacks Detection

Sami El Amraoui, Régis Leveugle, Paolo Maistri

Capture the Pulse: Impact of FPGA Resource Utilization on EM Fault Injection Attacks Detection

Sami El Amraoui, Régis Leveugle, Paolo Maistri
Univ. Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000, Grenoble, France
{sami.el-amraoui,regis.leveugle,paolo.maistri}@univ-grenoble-alpes.fr

Abstract— **With the increasing use of Field-Programmable Gate Arrays (FPGAs) in critical applications, safeguarding against malicious attacks becomes necessary. ElectroMagnetic Fault Injection (EMFI) stands out as a potent threat among localized fault attacks with its optimal compromise between cost and effectiveness, without the risk of damaging the target chip. Among potential targets, Ring Oscillators (ROs) are critical components that can be used in secure primitives, as well as detectors against physical attacks. In this paper, we analyze how the use of FPGA resources affects the outcome of EMFI attacks: we experimentally show with single EM pulse injections on three families of Xilinx FPGAs manufactured in 28nm process technology that the harmonic response of a RO heavily depends on its layout and density within the FPGA die. We also highlight the need of considering both EM pulse polarities when evaluating the efficiency of any proposed countermeasures, as this can reveal different sensitive locations on the chip. These findings can be leveraged for designing architectures that address the EMFI threat more effectively.**

Keywords— Ring oscillators, EMFI, FPGA, P&R, Harmonic error, Hardware security.

I. INTRODUCTION

In today's digital landscape, ensuring the security of electronic systems is paramount, as they can be targeted by malicious entities seeking to compromise data confidentiality and system integrity. To this end, physical attacks and notably fault attacks have become a prevalent method for circumventing the security mechanisms of embedded devices, with a large arsenal of techniques at the attackers' disposal. These techniques range from disrupting clock signals to inducing sudden variations in temperature, supply voltage or substrate bias, along with injecting parasitic currents using powerful electromagnetic (EM) disturbances [1]. Other sophisticated techniques using laser or X-rays can be more efficient but very expensive and risky for the attackers as they can damage the target device. Among these methods, ElectroMagnetic Fault Injection (EMFI) has gained prominence due to the optimal balance between the attack effectiveness and its low cost and device preparation requirements. In a recent paper [2], an open-source design 'PicoEMP' was introduced whereby an EM pulsed fault injection can be mounted for less than 100$. This makes EMFI attacks more accessible in both academia and industry which will help improve our understanding of its fault mechanisms.

EMFI alters the behavior of a target device by inducing ground bounces or voltage drops as a result of the magnetic flux created by the EM probe [3]. The EM coupling can be performed either through harmonic or pulsed Fault Injection. In the context of our study, we are interested in the second method involving powerful EM pulses.

After recognizing the inherent threat of EMFI, extensive research efforts have been targeted in recent years to fully understand and mitigate its impact on diverse devices, ranging from microcontrollers to FPGAs and Application-Specific Integrated Circuits (ASICs). Our focus in this work will be directed towards FPGAs as they represent good candidates for implementing cryptographic algorithms and security primitives such as Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs). Since these primitives employ ROs as an essential building block in their design, assessing their response to EMFI is important to improve their robustness.

Within this context, this paper aims to enhance the understanding of the harmonic locking impact on ROs with pulsed EMFI in FPGAs. This effect was introduced in [4] where the authors were able to lock the RO frequency into one of its harmonics through a single properly tuned EM pulse. The RO harmonic response was characterized as a function of its placement in the FPGA chip, the EM pulse width (PW) and amplitude, and the position of the probe relative to the FPGA package. In [5], the investigation sought to understand how multiple pulses and the placement and routing (P&R) constraints (of both the inverters and the input/output (IO) pins) influence the sensitivity of the ring. In this study, we advance from the groundwork of these papers to explore on different modern FPGA platforms how changing the FPGA structure (Spartan7 vs. Artix7) and its type of packaging (Wire-bond vs. Flip-Chip) can affect the harmonic response of the RO. We also elaborate on the effect of P&R constraints to maximize the harmonic response while varying the density and the layout of the RO with the same number of inverters. Furthermore, unlike many papers in the literature that neglect the impact of EM pulse polarity, here we show the fault distribution for both positive and negative polarities to highlight the importance of this parameter when evaluating the efficiency of EMFI across various FPGAs.

The remainder of this paper is structured as follows: Section II introduces the related works on EMFI and the harmonic locking of ROs. Section III details the experimental setup and the methodology. Section IV reports and analyzes the obtained results. Finally, Section V draws conclusions and provides perspectives.

II. BACKGROUND

A. Electromagnetic Fault Injection

EMFI can corrupt the normal operation of an integrated circuit (IC) through parasitic currents that are induced in all wire loops of the IC after a sudden variation of the magnetic or electric field.

Mounting a successful EMFI attack includes multiple steps and identifying the optimal sensitive location on the die is the critical one. To achieve that, one can leverage EM side-channel to find the maximum leakage observed on the target

* Institute of Engineering Univ. Grenoble Alpes

chip. Within this context, a recent paper [6] investigated the design optimization of a hybrid EM probe that can efficiently enable both capturing EM emissions and injecting EM perturbations. This can help reduce the time and complexity of the evaluation that still includes other parameters related to the pulse such as the injection timing, and the width, amplitude, and polarity of the pulse.

Considering all these challenges, ensuring full protection of different devices against EMFI requires accurate fault models describing the mechanism involved in EM-induced faults. Several works [7] [8] [9] have been carried out to explain their nature. They suggested that these faults can be explained either by the Timing or by the Sampling fault model, depending on the clock frequency of the target and the strength of the EM coupling within the circuit. A recent study by Nabhan et al. [10] highlighted that two underlying mechanisms are involved within the timing fault model. The first one relates to the target's clock distribution network which becomes highly susceptible to voltage glitches on the clock tree at low or moderate frequencies. However, at high frequencies associated with small slack, the power distribution network (PDN) is the most sensitive on-chip network as EM perturbation leads to violations in timing constraints. In another paper [11] trying to uncover the complexity of the EM injection and its interaction with circuits at a low physical level, the authors conducted EMFI experiments from the substrate backside of a 180 nm CMOS technology equipped with six crypto cores of 128-bit AES and an on-chip voltage waveform monitor. Their results showed a key finding emphasizing that depending on the polarity of the probe, significant negative voltage drops can be induced at specific locations within the PDN originating from injection positions that are not necessarily close to the impacted point.

Previous works studied the implementation of EMFI countermeasures on FPGAs such as [12] and [13]. However, the optimal number and location of the sensors to guarantee security against EM perturbations with the lowest overhead is still an open question. This primarily stems from the fact that the customization of placement and routing is challenging in FPGA design tools as they are designed by default to guarantee the best performance and resource optimization but do not take into account the circuit's EM emissions or susceptibility issues during the P&R process. To this end, our work will try to give more insights into the effects of P&R constraints on EMFI susceptibility to determine the best strategy for implementing detectors in different FPGA platforms.

B. *Harmonic Locking of Ring Oscillators*

A RO is harmonically locked when it is forced to oscillate at a harmonic frequency (i.e., a multiple of the fundamental frequency). This phenomenon was achieved with both laser experiments on a custom-designed 40nm Bulk CMOS ring oscillator, and electrical experiments on a RO constructed with discrete components in [14]. They were able to conclude that when one or several Single Event Transients (SETs) with a pulse width smaller than the total loop delay are induced during one oscillation period T of the RO, it deviates from its fundamental frequency and locks to one of its odd harmonics depending on the induced number of extra rising edges. In [4], the authors were able to validate this behavior through the injection of a single positive EM pulse into a RO composed of 1200 (50 x 24) inverters and implemented in an Artix7 FPGA. In their work, the ring was placed either on the top or bottom clock region and used 1 Look-Up Table (LUT) per Slice. The results showed that the placement of the RO in the chip, and the location and intensity of the injection affect the fault occurrence: when placed on the top clock region, the RO was more vulnerable to harmonic errors. Also, it was shown that in order to force higher harmonics with higher probabilities, one can increase the PW and amplitude of the pulse.

In [5], the characterization included a first analysis of the impact of routing constraints on the harmonic response of the RO. The findings suggested that for the same placement of the ring, favoring short vertical connections (called 'vertical snake') between LUTs results in higher harmonic sensitivity, while the lowest vulnerability was reported with long horizontal connections. Conducting similar tests on Spartan7 and Kintex7 FPGAs enabled us to confirm this conclusion. Therefore in this work, we will adopt the most sensitive routing 'vertical snake' to investigate further parameters: how the negative pulse polarity, the density, and the layout of the RO impact the fault distribution and intensity on different FPGAs.

III. Experimental Setup & Methodology

A. *EMFI Setup*

The setup illustrated in Fig. 1 was used to perform the EMFI experiments. A commercial pulse generator, ChipShouter by NewAE Technology was used to perform EM pulsed fault injection. It generates pulses with amplitudes from 150V up to 500V and variable widths, depending on the probe's diameter and the voltage amplitude. We used two of the EM probes provided with ChipShouter, consisting of a 1mm wire coiled either clockwise (CW) or counter-clockwise (CCW) around a 4mm ferrite core, to induce a positive or negative polarity of the pulse respectively. An XYZ motorized table precisely controls the position of the EM probe on top of the FPGA package in order to perform a full fault cartography. A digital oscilloscope of 200 MHz bandwidth was used to monitor the RO frequency during tests. A PC controls the whole platform through serial ports. The characterization has been achieved on three AMD-Xilinx FPGAs, all manufactured in 28nm process technology: a Spartan7 (xc7s25-1CSGA225) in a Cmod-S7 board; an Artix7 (xc7a100T-1CSG324) within Nexys-A7 board and a Kintex7 (xc7k160T-1FBG676) embedded in a SAKURA-X board. Their characteristics are given in Table I.

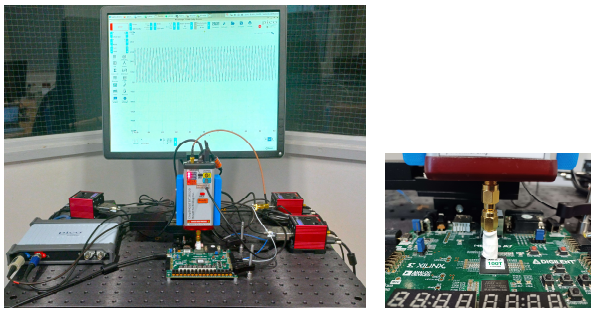


Fig. 1. Experimental setup

Table I. Characteristics of the targeted FPGAs

FPGA	Packaging	Package Size (mm²)	Die Size (mm²)	Logic Slices
Spartan7	Wire-bond chip-scale	13 x 13	5 x 5.1	3650
Artix7	Wire-bond chip-scale	15 x 15	6.5 x 10	15850
Kintex7	Flip-Chip lidless	27 x 27	9 x 12	25350

It should be noted that each FPGA die covers only a portion of the package. The die size of Kintex7 was measured since it is decapsulated in the board. For Spartan7, this information was revealed through X-ray imaging while it was reported in [15] for Artix7. Both Spartan7 and Artix7 use a wire-bond packaging technology, where the die is attached to the substrate face up and the connections are made with wires. On the other hand, the Kintex7 die is flipped over and placed face down, which eliminates wire bonds and results in lower inductance and better thermal performance. All these differences will be leveraged to explore how they will affect the outcome of EMFI.

B. RO Design

1) RO Architecture

The frequency of a RO depends on various parameters but it can be simplified as in the following formula, where D_i is the propagation delay of each delay element in the RO, D_r is the average delay related to the routing between them, and N is the number of these elements:

$$F = \frac{1}{2 \times (D_i + D_r) \times N}$$

Fig. 2 shows the architecture of our implemented RO with an even number N = 1200 of inverters and a Nand gate used as an activation gate. The control of the RO oscillations was achieved through serial communication.

2) Placement and Routing Constraints

In all targeted FPGAs, the Configurable Logic Block (CLB) tile contains two slices. Each slice includes 4 LUTs and 8 flip-flops. Depending on the density that we want to achieve, our RO was formed by configuring either one or all of the 4 LUTs within each slice as an inverter. This makes the ring more or less compact in the FPGA.

Also, to explore the effect of different RO layouts, we customized the placement and routing of the LUTs in Vivado tool to enable either a horizontal, vertical, or square shape. It should be noted that in all our experiments, we used the same number of inverters (N=1200) for each different P&R implementation of the RO in all three FPGAs.

C. Methodology

After a single EM pulse injection, the RO frequency may change or not, as follows:

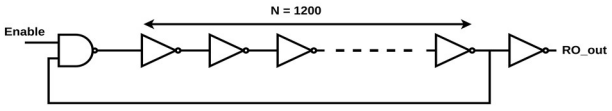
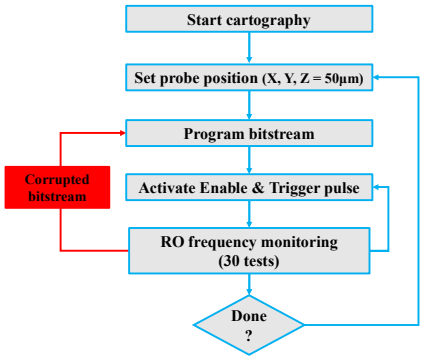


Fig. 2. Architecture of the ring oscillator

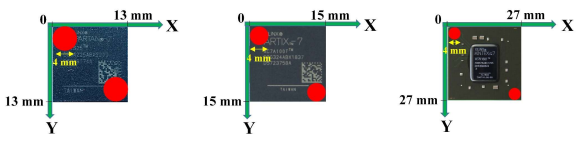
- **Unchanged frequency:** In that case, after the attack, the RO still oscillates at the same fundamental frequency. If we disable the RO and it keeps oscillating, we know that the 'Enable' configuration was corrupted, and the FPGA must be reprogrammed for the next test.
- **Harmonic locked frequency:** After the attack, the RO frequency can be locked into one of its odd harmonics (3, 5, 7….). As in the previous case, lack of control over the 'Enable' means that the board must be reprogrammed.
- **Noise signal:** the attack can also force the RO output signal to noise, which means the bitstream was corrupted, and re-setting the Enable signal does not restart the oscillations. Therefore, reprogramming the bitstream is mandatory before the next test.

Based on these effects, a specific methodology, depicted in Fig. 3(a), was adopted to inject and observe a single pulse into the RO. The goal is to detect the occurrence of harmonics while scanning over the FPGA package with the 4mm CW or CCW probe. The probe tip is kept 50µm on top of the package and displaced by steps of 1 mm (due to the probe's size and resolution) from the top left to bottom right corner as depicted in Fig. 3(b). The detailed steps are:

1) Set the initial EM pulse parameters for the test (PW = 100ns and amplitude = 450V). The choice of these values was motivated by the results reported in [4].
2) Place the probe at the initial coordinate (X = 0, Y = 0) above the chip package.
3) Program the FPGA with the bitstream.
4) Enable the RO and trigger the EM pulse injection.
5) Monitor the output RO frequency after injection then disable the RO, to detect the occurrence of harmonic induced frequencies and bitstream corruptions.
6) Repeat 30 times steps 4 and 5 to assess the reproducibility rate for the given (X, Y) coordinate.
7) Move the probe to a new position and repeat from step 3 until the last coordinate to obtain a fault sensitivity map of the FPGA package.



(a)



(b)

Fig. 3. (a) RO faults evaluation flow (b) FPGA Package Scan

IV. EXPERIMENTAL RESULTS

The experimental results reported in this section show the effect of EM pulsed injection with both polarities on the 3 targeted FPGAs along with the impact of different RO layouts on faults.

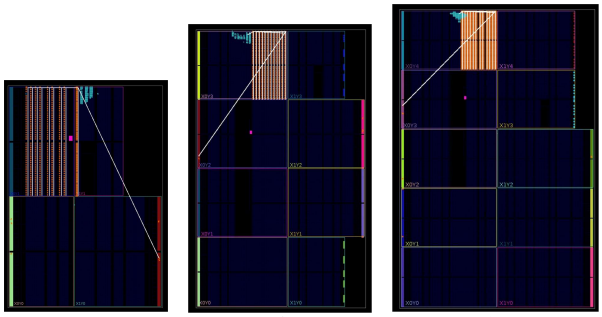
To improve the readability of the fault sensitivity maps, we assigned a specific color for each effect. It should be noted that the numbers in these maps refer to the ratio between the monitored frequency after EM injection and the fundamental frequency of the targeted RO:

- **White:** No faults (Frequency remained the same and the bitstream was not corrupted).
- **Gradient from Yellow to Red:** shows the highest harmonic error that was monitored within 30 conducted tests.
- **Black:** represents mutes where reprogramming the bitstream was mandatory; the probability of bitstream corruption in this case is 100%.

A. *Impact of the FPGA Structure and Packaging*

To explore the influence of the FPGA structure and packaging on the fault sensitivity of the RO, we followed the methodology shown in Fig. 3(a) by conducting EM injection campaigns targeting the same RO implemented in the three FPGAs; 1 LUT/Slice and a vertical routing with short connections, as illustrated in Fig. 4, were used. It should be noted that even if the same P&R of the RO was adopted, its frequency slightly varied between them because of the difference in their internal structure and the output pin connection. The RO was originally running at 1250 KHz in Spartan7, at 1075 KHz in Artix7, and at 1417 KHz in Kintex7.

Fig. 5 represents the fault sensitivity maps with the positive polarity of the three FPGAs and shows that changing the FPGA family and packaging, even within the same process technology, can effectively influence the intensity and the location of the induced faults. The maximum impact was achieved in Artix7 with a harmonic error of 43, twice



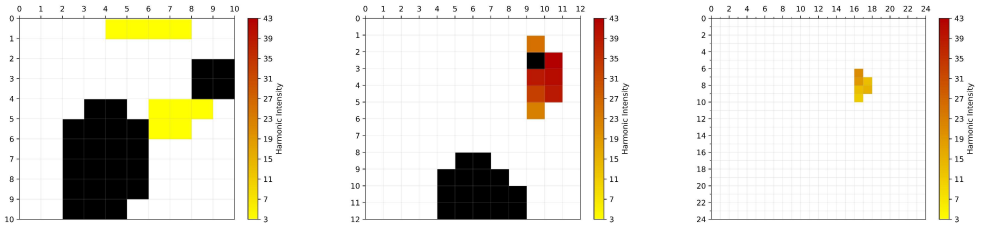
(a) (b) (c)

Fig. 4. FPGA floorplan from Vivado showing the implemented RO in (a) Spartan7 (b) Artix7 (c) Kintex7

larger than the impact on Kintex7. Additionally, Spartan7 was the most sensitive to bitstream corruptions, as opposed to Kintex7 with no recorded vulnerability to this type of faults. This shows how Flip-Chip packaging, usually dedicated to high-performance FPGA, can reduce the fault sensitivity compared to wire-bond packaging. On another hand, if we focus on this later technology used for Spartan7 and Artix7, by comparing Fig. 5(a) and Fig. 5(b) we notice some similarities in the location of faults especially in the bottom center coordinates. However, only third harmonic errors were induced for Spartan7, likely because it includes less programmable logic, hence a lower coupling between the probe and its PDN.

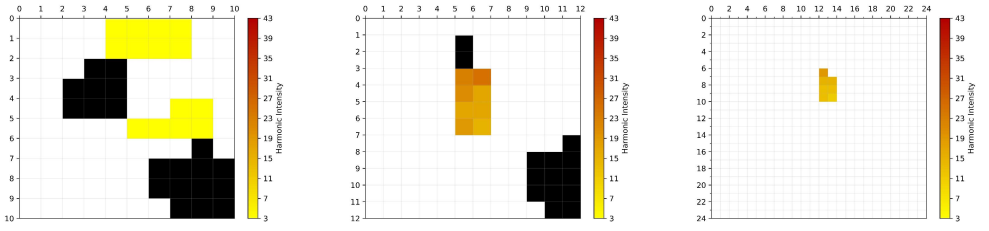
B. *Impact of the Pulse Polarity*

Similar tests were conducted to investigate the effect of changing the pulse polarity and the results are depicted in Fig. 6, showing the new fault locations in the three FPGAs. Upon an initial examination of the three cartographies, one may observe a similar trend compared to the positive polarity with Artix7 being the most vulnerable to harmonics and Spartan7 being the least. However, comparing Fig. 5 and Fig. 6 highlights that the negative polarity reveals complementary fault locations in the FPGA package. This indicates a different susceptibility of the power and the ground network



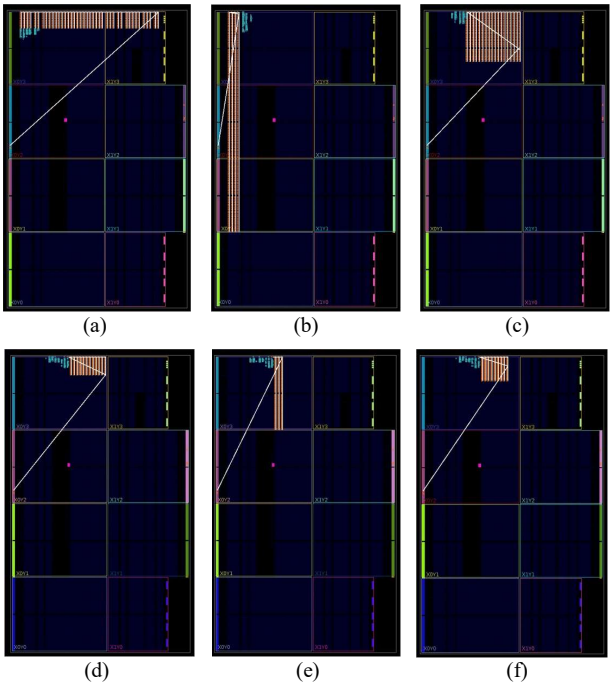
(a) (b) (c)

Fig. 5. Fault sensitivity maps with positive pulse polarity (a) Spartan7 (b) Artix7 (c) Kintex7



(a) (b) (c)

Fig. 6. Fault sensitivity maps with negative pulse polarity (a) Spartan7 (b) Artix7 (c) Kintex7



(a) (b) (c)

(d) (e) (f)

Fig. 7. Different layouts of the RO implemented in Artix7 FPGA using (above) 1LUT/Slice (a) Horizontal (b) Vertical (c) Square and (below) 4LUTs/Slice (d) Horizontal (e) Vertical (f) Square

within FPGAs to the polarity of EMFI, which underlines the importance of this parameter when assessing the robustness of a design against this attack.

C. *Impact of the RO Layout*

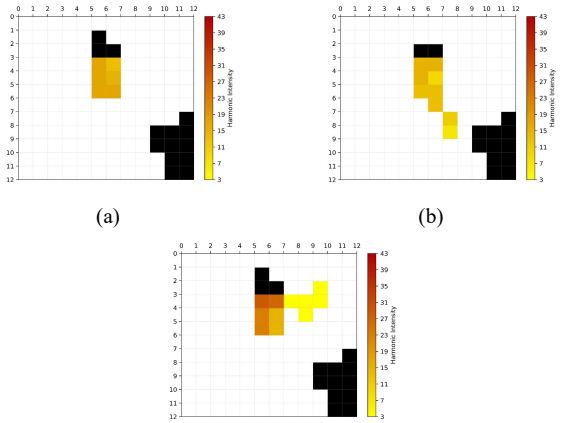
To further investigate the effect of changing the RO layout within the die, we performed new experiments while changing the placement constraints of the LUTs to enable different shapes of the RO. The intended goal is to obtain further insights into the impact that density and connections have on the ring sensitivity. Fig. 7(a) to (c) show the three obtained RO shapes (horizontal, vertical and square) achieved through the use of 1 LUT/Slice. For the sake of conciseness, although tests were conducted on the three FPGAs using positive and negative pulse polarities, we will here present only the results related to the Artix7 FPGA with negative polarity and then compare and discuss the other cases.

Table II lists the frequency of the RO depending on its layout. As shown in this table, changing the layout results in a difference of less than 1% between the output frequencies: this is mainly due to the different use of horizontal and vertical connections.

The results are represented in Fig. 8, showing how the fault sensitivity varies with the layout strategy. The most vulnerable layout was the square one with more sensitive

Table II. Frequency of the RO with different layouts in the FPGAs

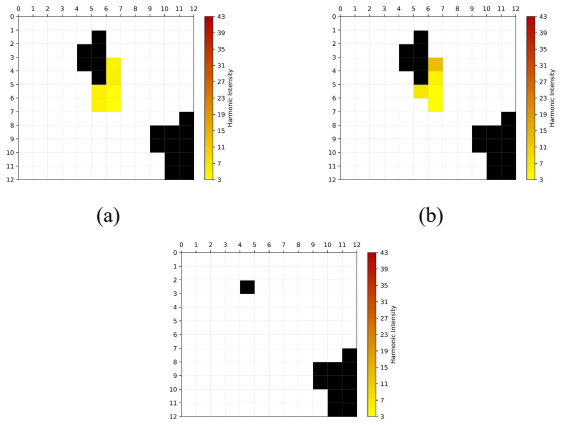
FPGA	Density	Layout	Frequency (KHz)
Artix7	1 LUT/Slice	(a)	1086
		(b)	1076
		(c)	1078
	4 LUTs/Slice	(d)	1550
		(e)	1540
		(f)	1546



(a) (b)

(c)

Fig. 8. Fault sensitivity maps with a negative polarity using 1LUT/Slice configuration (a) Horizontal (b) Vertical (c) Square



(a) (b)

(c)

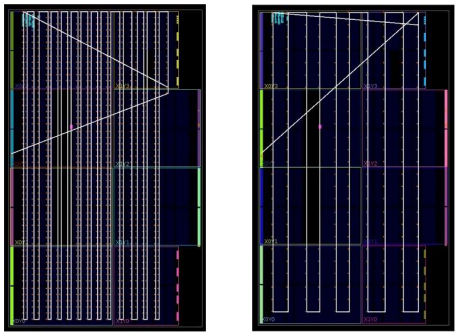
Fig. 9. Fault sensitivity maps with negative polarity using 4LUTs/Slice configuration (a) Horizontal (b) Vertical (c) Square

locations and a harmonic error of 29. This indicates a better coupling between the probe and the FPGA when the RO is more compact within a single clock region, with few horizontal connections between the slices. This is likely due to the optimal density of inverters within the EM pulse. Similar tests on Spartan7 and Kintex7 enabled us to draw the same conclusion for both pulse polarities.

D. *Impact of the RO Density*

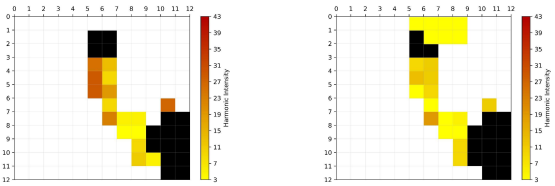
After showing that choices in the RO distribution within the chip lead to consistent differences in the experimental results between the three FPGAs, we aimed to highlight the impact of the RO density on the observed faults. To this end, we implemented similar configurations but using 4LUTs/Slice instead of only one as illustrated in Fig. 7(d) to (f). Their corresponding frequencies are detailed in Table II.

The results reported in Fig. 9 show how minimizing the use of Slices (from 1200 down to 300) had a noticeable impact on the harmonics intensity compared to the results in Fig. 8, especially for the square layout where the harmonic sensitivity was completely suppressed. This was mainly caused by the low spatial resolution of the 4mm probe that cannot couple with elements of a small size, which indicates the likely need for a more advanced setup to induce harmonic errors. The same result was obtained for the two other



(a) (b)

Fig. 10. RO implemented using 1LUT/Slice (a) N=1200 inverters, F=850KHz (b) N=228 inverters, F=4065KHz



(a) (b)

Fig. 11. Fault sensitivity maps with negative polarity (a) N=1200 inverters (b) N=228 inverters

FPGAs, which suggests that if we seek a minimal harmonic response of the RO, then adopting a square layout using 4LUTs/Slice along with horizontal routing as reported in [5] remains the best option. This key finding is important for the robustness of RO-based PUFs and TRNGs against EMFI.

In the opposite direction, we tried to investigate the impact of making the RO layout less compact compared to the previous configurations while distributing the inverters all around the chip using 1LUT/Slice as depicted in Fig. 10(a), with 1200 inverters, and in Fig. 10(b) with only 228 inverters. The fault maps shown in Fig. 11 demonstrate a higher number of impacted locations compared to previous results, even when we reduced the number of LUTs by a factor of 6. This indicates the importance of an optimal utilization of the Programmable Interconnect Points (PIPs) in FPGAs for EMFI detection.

V. Conclusion and Future Work

In this paper, we discussed the varying EMFI susceptibility of an FPGA while using various layouts of the RO. The evaluation on three FPGAs of different packaging and internal structures gave us valuable insights to consider for designing countermeasures that can effectively mitigate the EMFI threat in critical applications. By carefully analyzing the effect of pulse polarity on the harmonic response of the RO, we showed its significance when evaluating a detection mechanism to achieve an ideal behavior. Based on our analysis, we concluded that adopting a low compactness strategy when implementing the design of EMFI sensors is advantageous for optimal detection.

As future work, we will explore the possibility to leverage the key findings of this paper to propose a new RO-based countermeasure to detect EMFI and different fault attacks.

Acknowledgment

This work is supported by the “France 2030” government investment plan managed by the French National Research Agency (ANR-22-PECY-0004) in the frame of ARSENE project, and co-funded by the Cybersecurity Institute of Grenoble Alpes (ANR-15-IDEX-02).

References

[1] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures,” *Proceedings of the IEEE*, vol. 100, no. 11.

[2] O'Flynn, Colin. “PicoEMP: A Low-Cost EMFI Platform Compared to BBI and Voltage Fault Injection using TDC & External VCC Measurements.” 2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) (2023): 60-71.

[3] J.-J. Quisquater and D. Samyde, “Eddy current for magnetic analysis with active sensor,” in Proc. Smart Card Programming and Security (E-smart), pages 185–194, 2002.

[4] S. El Amraoui, A. Douadi, R. Leveugle, and P. Maistri, “Harmonic Response of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection,” in 2024 25th Latin American Test Symposium (LATS). [Online]. Available: https://hal.science/hal-04513585

[5] S. El Amraoui, R. Leveugle, and P. Maistri, “Choose your Path: Control of Ring Oscillators EMFI Susceptibility through FPGA P&R Constraints,” in 2024 27th International Symposium on Design & Diagnostics of Electronic Circuits & Systems (DDECS), IEEE, Apr. 2024, pp. 118–123. doi: 10.1109/DDECS60919.2024.10508906.

[6] F. Marrucco, M. Ahmed, B. Bouali, and A. Mady, “EMplifier: Hybrid Electromagnetic Probe for Side Channel and Fault Injection Analysis,” in Proceedings of the 10th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications, Mar. 2024, pp. 815–822.

[7] M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, and P. Schaumont, “Inducing local timing fault through EM injection,” in Proceedings of the 55th Annual Design Automation Conference, New York, NY, USA: ACM, pp. 1–6, Jun. 2018.

[8] 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, IEEE, pp. 7–15, Sep. 2012.

[9] M. Dumont, M. Lisart, and P. Maurine, “Modeling and Simulating Electromagnetic Fault Injection,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 4, pp. 680–693, Apr. 2021.

[10] R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, L. Sauvage, and L. A. Sauvage, “A Tale of Two Models: Discussing the Timing and Sampling EM Fault Injection Models,” in FDTC, Sep. 2023.

[11] Hasegawa, R., Monta, K., Wadatsumi, T., Miki, T., Nagata, M. On-Chip Evaluation of Voltage Drops and Fault Occurrence Induced by Si Backside EM Injection. In: Wacquez, R., Homma, N. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2024. Lecture Notes in Computer Science, vol 14595. Springer, Cham.

[12] D. El-Baze, J. -B. Rigaud and P. Maurine, "A fully-digital EM pulse detector," in Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, pp. 439-444, Mar. 2016.

[13] S. S. Gujar and L. Nazhandali, “Detecting Electromagnetic Injection Attack on FPGAs Using In-situ Timing Sensors,” Journal of Hardware and Systems Security, vol. 4, no. 3, pp. 196–207, Sep. 2020, doi: 10.1007/s41635-020-00096-9.

[14] Y. P. Chen *et al.*, “Single-Event Transient Induced Harmonic Errors in Digitally Controlled Ring Oscillators,” *IEEE Trans Nucl Sci*, vol. 61, no. 6, pp. 3163–3170, Dec. 2014.

[15] M. Paquette, B. Marquis, R. Bainbridge, and J. Chapman, “Visualizing Electromagnetic Fault Injection with Timing Sensors,” in Proceedings of the 2021 IEEE International Conference on Physical Assurance and Inspection on Electronics, PAINE 2021.