Choose your Path: Control of Ring Oscillators EMFI Susceptibility through FPGA P&R Constraints

Sami El Amraoui, Régis Leveugle, Paolo Maistri

Choose your Path: Control of Ring Oscillators EMFI Susceptibility through FPGA P&R Constraints

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*— Ring Oscillators (ROs) are widely used in various electronic systems, contributing to their functionality, security, and reliability. Therefore, the characterization of the robustness of RO-based designs against fault attacks such as ElectroMagnetic Fault Injection (EMFI) is a real concern. In this paper, we study the impact of electromagnetic (EM) pulses on ROs implemented in FPGAs. We show that the induced harmonic response depends on the placement and routing of the inverters for different parameters of the pulse. Such a characterization can help developing RO-based structures optimized either for better robustness against attacks or on the opposite for higher sensitivity in order to implement on-chip detectors.**

Keywords*— *Ring oscillators, EMFI, FPGA, routing

I. INTRODUCTION

The security of digital systems is a main concern nowadays as the data passing through devices is susceptible to diverse attacks by malicious entities. The means of attack can target either the hardware or the software layers depending on the detected vulnerabilities of the system. When opting for a hardware attack aiming to disrupt the normal functioning of an Integrated Circuit (IC), fault injection often takes advantage of physical access to influence environmental properties like temperature or functional parameters such as power supply [1] [2]. A less intrusive, more precise and cost-efficient method is ElectroMagnetic Fault Injection (EMFI). EMFI stands out as one of the most effective techniques to inject faults into digital circuits because of its relatively good accuracy compared to the use of lasers that are highly precise (down to the nanometer level) but require specific expertise to avoid damaging the circuit [3] and are much more expensive. Ensuring flawless protection of devices against EMFI requires first to assess their vulnerability to this attack and develop realistic and accurate fault models in order to eventually design effective countermeasures.

EMFI induces parasitic currents in an IC by generating through a magnetic probe an electromagnetic (EM) field that couples with the closed wire loops in the circuit. The EM coupling can be performed through harmonic Fault Injection or pulsed Fault Injection. In this work, we used the second method involving short and highly powerful EM pulses to disrupt the behavior of the FPGA during a few nanoseconds.

ROs are known to be simple circuit structures that are employed particularly in the security field for many applications such as True Random Number Generators (TRNGs) and Physical Unclonable Functions (PUFs). This paper is focused on the impact of pulsed EMFI on ROs made by cascaded inverters and implemented in a Field-Programmable Gate Array (FPGA) chip.

* Institut National Polytechnique Grenoble Alpes

We studied in [4] the magnitude of the harmonic locking impact of a single EM pulse injection on a RO, with respect to the EM pulse amplitude and width, and the position of the probe relative to the FPGA package, for two different RO placements. We investigate here more deeply how the placement and routing (P&R) constraints of both the inverters and the RO input and output (IO) pins influence the sensitivity to the attack. We show that these constraints can be chosen to either minimize or maximize the harmonic response, depending on the designer's goals. We also explore the effect of multiple pulses, in addition to several injection timings and locations.

The remainder of this paper is organized as follows: Section II introduces the state of the art on EM fault models and the harmonic locking phenomenon in ROs. Section III describes the experimental setup and the methodology. Section IV presents and discusses our findings. Finally, Section V draws conclusions and provides perspectives.

II. BACKGROUND

A. EM Fault models

Modeling the EM faults is complex because of the large set of parameters that needs to be properly optimized to obtain exploitable faults. The list of parameters includes: the pulse amplitude, the pulse width (PW), the pulse polarity, the position and height of the EMFI probe above the IC surface, the choice of the probe characteristics and the moment and frequency at which the EM pulse is delivered with respect to the target's operation.

The state of the art findings suggested that the faults induced by EMFI are 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. [5] proved that two distinct underlying mechanisms are involved. At high frequencies, associated with small slack, EM disturbances couple with the power distribution network of the target leading to violations in timing constraints. On the other hand, at low to moderate frequencies, induced faults align more with the Sampling fault model as the EM disturbances perturb the target's clock distribution network and can trigger voltage glitches within the target's clock tree.

When ROs are implemented in an FPGA design, both fault models may become less accurate since combinational logic in a loop is also susceptible to EMFI. Therefore, achieving a more global and comprehensive fault model for EMFI requires considering the harmonic errors due to EM pulsed injection.

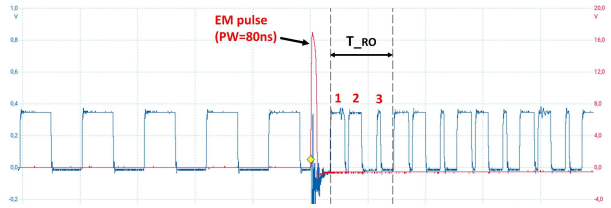
In a previous paper [6], Trabelsi et al. characterized the impact of EMFI on the propagation delay of a combinational logic path implemented in a Xilinx Virtex-II Pro chip

manufactured in 90nm process technology while varying four EM pulse parameters (the injection timing, the number of pulses, the pulse amplitude and its polarity). They reported that a significant acceleration or deceleration impact on the path delay is possible only when more than 100 successive pulses are injected. During their tests, the placement of their design has been constrained to the bottom part of the FPGA to validate the correlation between the position of the EM probe and the impact of the EMFI. However, the effect of different placements and routings was not explored.

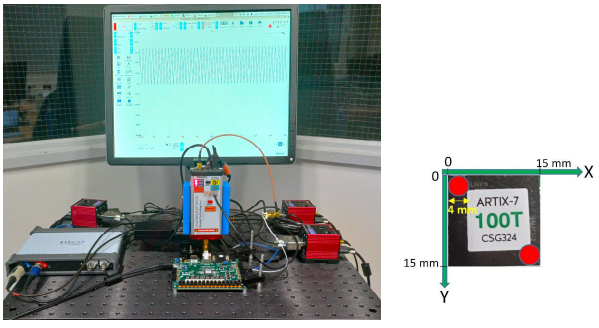
B. *Harmonic Locking of Ring Oscillators*

A RO originally runs at a fundamental frequency that depends mainly on the delay of its stages. We say that a RO is locked when it is forced to oscillate at another frequency. Various studies on ROs presented this phenomenon using radiofrequency interference on the power supply [7], sinusoidal perturbation signals [8] or laser shots [9], that make them lock onto a signal with a frequency close to their natural oscillation frequency or its harmonics (i.e. multiples of the original frequency). This locking phenomenon can help the attacker degrade the randomness of RO-based TRNGs as demonstrated in [10] and [11] through EM harmonic injections.

On the other hand, it was shown in [9] that when one or several Single Event Transients (SETs) with a pulse width smaller than the total loop delay T/2 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 number of extra rising edges induced in one period of oscillation. In [4], we were able to validate for the first time this harmonic vulnerability as shown in Fig. 1(a) by only injecting a single EM pulse with different amplitudes and widths into a RO oscillating at 927KHz and implemented in an Artix7 FPGA (28nm). We concluded that depending on the placement of the RO in the chip and the location of the probe, a minimal amplitude and PW threshold must be reached to induce harmonic errors or bitstream corruptions. Furthermore, we highlighted that forcing higher harmonics (e.g., 19th harmonic) with higher probabilities could be achieved in particular locations by increasing the width and amplitude of the pulse.



(a)



(b)

Fig. 1. (a) 3rd harmonic induced error (b) Experimental setup

III. Experimental Setup & Methodology

A. *EMFI Setup*

To perform the EMFI experiments we used the following setup shown in Fig. 1(b):

1) PC: It controls the whole platform through serial ports.

2) XYZ Motorized Table: It is used to precisely control the position of the EM probe on top of the target.

3) Pulse Generator: We used the ChipShouter pulse generator by NewAE Technology for this work to perform EM pulsed fault injection. This device can generate pulses with amplitudes from 150V up to 500V and variable widths, depending on the probe's diameter and the voltage amplitude as demonstrated in [12]. Properties of the pulse are configured using the RS-232 serial port interface.

4) EM Probes: We used one of the ChipShouter probes consisting of a 1mm wire coiled clockwise (CW) around a 4mm ferrite core.

5) Target FPGA: The NEXYS A7 development board embedding the AMD-Xilinx Artix-7 XC7A100T-1CSG324 FPGA (technology node 28nm) was used for our EMFI experiments. Enabling or disabling the oscillations of the RO was achieved through a physical switch on the board.

6) Digital Oscilloscope: A Picoscope of 200 MHz bandwidth was used to monitor the RO frequency during tests.

B. *RO Design*

1) *RO Architecture*

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 RO keeps oscillating when the 'Enable' input signal is high otherwise the oscillations stop.

2) *Placement and Routing Constraints*

a) Placement of inverters:

In our FPGA, each Configurable Logic Block (CLB) tile contains two slices. Our RO was formed by configuring one of the 4 Look-Up Tables (LUTs) within each slice as an inverter or a Nand gate. In our experiments, the placement of the 1200 inverters (50 rows of 24 inverters) was constrained either to the top clock region (X0Y3) or to the bottom one (X0Y0) as highlighted with a yellow rectangle in Fig. 3(a), which shows the floorplan of the design extracted from the Vivado tool.

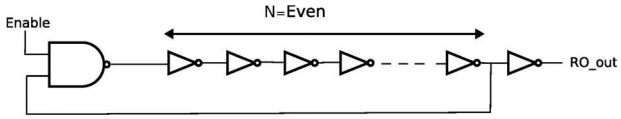


Fig. 2. Architecture of our ring oscillator

b) Placement of IO pins:

Fig. 3(a) also shows the 'Enable' input of the RO that was constrained either to the pin J15 in the left clock region X0Y2 or to the pin H6 in the right clock region X1Y2. The RO output 'RO_out' was constrained to pin C17 in the clock region X0Y2 for both placements of the RO.

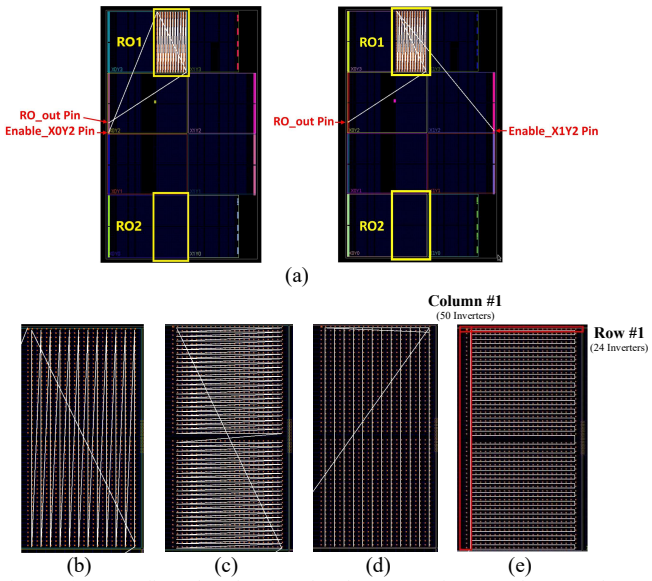


Fig. 3. (a) FPGA floorplan showing the placement of RO1 and RO2 and the input and output pin constraints (b) Vertical routing with long connections 'Zigzag' (c) Horizontal routing with long connections 'Zigzag' (d) Vertical routing with short connections 'Snake' (e) Horizontal routing with short connections 'Snake'

c) Routing of inverters:

Fig. 3(b) to (e) show the four different routings of the rings adopted for both placements. A bitstream was separately generated for each placement and routing of the RO and each 'Enable' placement constraint, resulting in 16 files in total. Table I lists the frequency of the RO depending on its placement and routing. As depicted in this table, keeping the same number of inverters in the RO while changing its placement and routing results in a small difference between the output frequencies: this is mainly due to the use of different connections in the FPGA for each configuration; small differences among same configurations are likely due to process variations within the FPGA fabric.

C. Methodology

Preliminary tests revealed the following behaviors of the RO output after a single pulse injection:

- **Unchanged frequency:** In that case, after the attack, the RO still oscillates at the same fundamental frequency. If we turn off the Enable signal and the RO keeps oscillating, we know that the Enable configuration was corrupted, and the FPGA must be reprogrammed.
- **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, a nonworking Enable switch means that the board must be reprogrammed for the next test.
- **Noise signal:** the attack can also force the RO output signal to noise, which means the bitstream was corrupted as resetting the Enable signal does not restart the oscillations. Therefore, reprogramming the bitstream is mandatory before the next test.

TABLE I. Characteristics of the RO depending on its placement and routing constraints

	Clock Region	Routing of inverters	Frequency (KHz)	RO Input
RO1	X0Y3	b) Vertical Zigzag	927	J15 Pin (X0Y2) or H6 Pin (X1Y2)
		c) Horizontal Zigzag	1206	
		d) Vertical Snake	1076	
		e) Horizontal Snake	1253	
RO2	X0Y0	b) Vertical Zigzag	925	
		c) Horizontal Zigzag	1204	
		d) Vertical Snake	1075	
		e) Horizontal Snake	1251	

Based on these observed effects, a specific methodology (depicted in Fig. 4) was then adopted to inject a single pulse into the RO. The goal is to detect the occurrence of harmonics while moving the 4mm CW probe over the chip area. The probe tip is kept in contact (Z = 0) on top of the FPGA package (15mm × 15mm) and displaced by steps of 1 mm (due to the probe's resolution) from top left to bottom right as depicted in Fig. 1(b). It should be noted that the FPGA die represents only 6.5mm × 10mm of the whole package size as reported in [13]. The detailed steps are:

1) Set the initial EM pulse parameters for the test (PW = 80ns 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) Trigger the 'Enable' signal of the RO and the delayed 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 50 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 (X = 11, Y = 11) to obtain a fault sensitivity map of the FPGA package with 12 × 12 positions.

We emphasize that each performed injection induces the pulse at a different moment during the low or high level of the clock to enable injections randomly spanning over the oscillation period. The reason behind this type of injection is due to the results of the tests with controlled injection timing which revealed limited sensitive areas to harmonic faults compared to a random injection timing.

IV. EXPERIMENTAL RESULTS

The experimental results reported in this section show the effect of the EM pulsed injection with the different placement and routing constraints and the impact of multiple injected pulses.

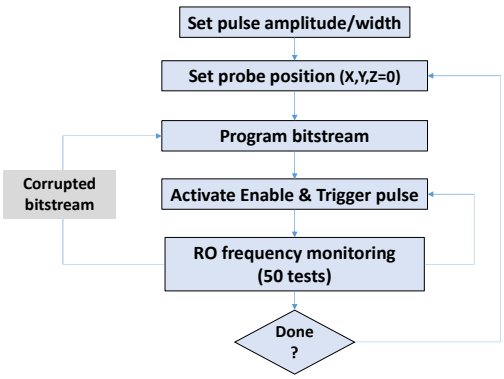


Fig. 4. Flowchart of EMFI on the RO

To improve the readability of the fault sensitivity maps, we assigned a specific color and symbol for each effect. It should be noted also 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:

- **Green:** No faults (Frequency remained the same and the bitstream was not corrupted).
- **Gradient from White to Red:** shows the harmonic error intensity, with 3 being the lowest and 39 being the highest observed. When two numbers are mentioned, they represent the lowest and highest recorded induced odd harmonic frequencies within the 50 conducted tests.
- **Grey with a number:** 'Enable' pin connection is corrupted because the oscillations cannot be disabled; the probability of bitstream corruption is 100%.
- **Grey with an X mark:** Noise signal (due to bitstream corruption); the probability of bitstream corruption is also in this case 100%.

A. *RO Placement Effect*

Following the procedure shown in Fig. 4, EM injection campaigns were conducted while targeting separately the two ROs: $RO1_{VerticalZigzag}$ and $RO2_{VerticalZigzag}$, originally running at 927 KHz and 925 KHz respectively. Their 'Enable' input was constrained to the pin J15 in the left clock region X0Y2 as illustrated in Fig. 3(a).

Fig. 5 represents the fault sensitivity maps of RO1 and RO2 and shows that changing the placement of the RO in the FPGA chip leads to different responses under a single pulse injection. The RO1 placed on the top clock region of the FPGA is more sensitive to induced harmonic errors than the RO2, as the highest harmonic error for RO1 is 19 and only 7 for RO2. On the other hand, we observe that both ROs share a similar fault sensitivity when targeting the bottom (leading to bitstream corruptions) and upper center (leading to 3rd harmonic errors) of the FPGA package. Also, a single pulse injection in the coordinate X9Y3 forces the corruption of the 'Enable' signal regardless of the placement of the RO.

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	7 – 9	1
Y=2	1	1	1	1	1	1	1	1	1	13 – 19	11 – 17	1
Y=3	1	1	1	1	1	1	1	3	3	19	19	1
Y=4	1	1	1	1	1	1	3	3	3	1	17 – 19	1
Y=5	1	1	1	1	1	1	3	3	1	1	11 – 17	1
Y=6	1	1	1	1	1	1	1	3	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(a)

1 No faults **X** Noise Corrupted bitstream Harmonic intensity

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	3	3	1	1	1
Y=4	1	1	1	1	1	1	3	3	3	1	1	1
Y=5	1	1	1	1	1	1	3	3	1	1	1	1
Y=6	1	1	1	1	1	1	1	3	1	1	1	1
Y=7	1	1	1	1	1	3 – 7	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(b)

Fig. 5. Fault sensitivity maps with 'Enable' input pin constrained to J15 in X0Y2 clock region. (a) $RO1_{VerticalZigzag}$ (b) $RO2_{VerticalZigzag}$

To see the potential effects of manufacturing or experimental variations, we applied the same analysis on two other identical Artix7 FPGAs programmed with the same bitstream. The results for both RO1 and RO2 changed only slightly in terms of harmonic error intensity. To further investigate these similarities, we decided to conduct new experiments on RO1 and RO2 while changing the placement constraint of the IO pins.

B. *IO Pin Placement Constraint Effect*

To explore the influence of this parameter on the fault sensitivity of the RO, we first changed the constraint of the 'Enable' input pin from J15 in the left clock region X0Y2 to H6 in the right clock region X1Y2 for both RO1 and RO2 as shown in Fig. 3(a). The results of the conducted experiments are shown in Fig. 6, which depicts the changes in the harmonic fault sensitivity. In particular, in the upper center coordinates, the third harmonic errors are no longer induced for both placements of the RO. Another main difference between Fig. 5 and Fig. 6 lies in the coordinate X9Y3 where the change of 'Enable' pin constraints likely led to suppressing the corruption of its connection. Additionally, for RO1, the locations of harmonic sensitivity remained the same but with a higher intensity in some cases. On the other hand, it is important to highlight the similar positions linked with bitstream corruption faults in the bottom part of the FPGA package for both ROs in these figures.

Similar tests were also conducted to investigate the effect of changing the constraint of the RO output pin from C17 in the X0Y2 clock region to K1 in the X1Y2 clock region while keeping the 'Enable' input at J15. The results showed that this change did not have a noticeable impact compared to the results in Fig. 5 as the fault sensitivity remained the same except that a higher harmonic intensity was induced for RO1 in some X9 and X10 coordinates.

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	5 – 7	1
Y=2	1	1	1	1	1	1	1	1	1	5 – 13	9 – 13	1
Y=3	1	1	1	1	1	1	1	1	1	19 – 31	19 – 31	1
Y=4	1	1	1	1	1	1	1	1	1	1	27 – 37	1
Y=5	1	1	1	1	1	1	1	1	1	1	15 – 27	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(a)

1 No faults **X** Noise Corrupted bitstream Harmonic intensity

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	1	1	1	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	1	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	3 – 7	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(b)

Fig. 6. Fault sensitivity maps with 'Enable' input pin constrained to H6 in X1Y2 clock region. (a) $RO1_{VerticalZigzag}$ (b) $RO2_{VerticalZigzag}$

C. *RO Routing Effect*

After showing that choices in IO placement (and routing) lead to consistent differences in the experimental results, we aim to highlight the impact of routing between the LUTs on the observed faults. We implemented 4 types of routings as shown in Fig. 3(b) 3(c) 3(d) and 3(e) for both RO1 and RO2 with the 'Enable' input constrained to H6 in the right clock region X1Y2. The results are represented in Fig. 7 and Fig. 8, which show how the fault sensitivity varies with the type of routing for RO1 and RO2 respectively.

From both figures, we can deduce that adopting a horizontal routing with long connections (Zigzag) is optimal for low harmonic sensitivity, while the vertical routing with short connections (Snake) is more suitable if we are interested in a high harmonic sensitivity; this could be exploited, for instance, to implement RO-based detectors. The reason why the vertical routing is more vulnerable to higher harmonic errors may be related to the higher vulnerability of vertical connections in the FPGA and the fact that we placed more inverters vertically (i.e. 50 inverters in each column) than horizontally in our RO design. In addition, comparing Fig. 7(a) and 8(a) with Fig. 7(b) and 8(b) respectively shows that short connections lead to higher harmonics as the EM coupling between the probe and this type of connections is stronger.

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	5 – 7	1
Y=2	1	1	1	1	1	1	1	1	1	5 – 13	9 – 13	1
Y=3	1	1	1	1	1	1	1	1	1	19 – 31	19 – 31	1
Y=4	1	1	1	1	1	1	1	1	1	1	27 – 37	1
Y=5	1	1	1	1	1	1	1	1	1	1	15 – 27	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(a)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	29 – 39	1
Y=2	1	1	1	1	1	1	1	1	1	25 – 35	21 – 35	1
Y=3	1	1	1	1	1	1	1	1	1	21 – 37	29 – 39	1
Y=4	1	1	1	1	1	1	1	1	1	1	29 – 35	1
Y=5	1	1	1	1	1	1	1	1	1	1	19 – 31	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(b)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	3	1	1
Y=3	1	1	1	1	1	1	1	1	1	3 – 5	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	3	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(c)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	3 – 5	1
Y=2	1	1	1	1	1	1	1	1	1	3 – 7	3	1
Y=3	1	1	1	1	1	1	1	1	1	5 – 7	3	1
Y=4	1	1	1	1	1	1	1	1	1	1	3	1
Y=5	1	1	1	1	1	1	1	1	1	1	3 – 5	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(d)

Fig. 7. Routing effect on **RO1**. (a) Vertical Zigzag (b) Vertical Snake (c) Horizontal Zigzag (d) Horizontal Snake

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	1	1	1	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	1	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	3 – 7	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(a)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	1	1	1	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	1	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	15 – 25	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(b)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	1	1	1	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	1	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(c)

XY (mm)	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11
Y=0	1	1	1	1	1	1	1	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	1	1	1	1	1
Y=2	1	1	1	1	1	1	1	1	1	1	1	1
Y=3	1	1	1	1	1	1	1	1	1	1	1	1
Y=4	1	1	1	1	1	1	1	1	1	1	1	1
Y=5	1	1	1	1	1	1	1	1	1	1	1	1
Y=6	1	1	1	1	1	1	1	1	1	1	1	1
Y=7	1	1	1	1	1	1	1	1	1	1	1	1
Y=8	1	1	1	1	1	X	X	1	1	1	1	1
Y=9	1	1	1	1	X	X	X	X	1	1	1	1
Y=10	1	1	1	1	X	X	X	X	X	1	1	1
Y=11	1	1	1	1	X	X	X	X	X	1	1	1

(d)

Fig. 8. Routing effect on **RO2**. (a) Vertical Zigzag (b) Vertical Snake (c) Horizontal Zigzag (d) Horizontal Snake

D. Multiple Injections Effect

In all the previous experiments, we performed only one pulse injection on the RO after which we monitor its frequency and then reset the oscillations for the next test. In this paragraph, we will present how successive EM injections can impact the RO faults. To explore the impact of this parameter, we injected 10 successive EM pulses of amplitude = 450V and PW = 80ns to $RO1_{VerticalZigzag}$ with the 'Enable' pin constrained to J15 and output pin constrained to C17 and monitored the result of each injection without resetting its oscillations.

For the coordinates with no induced faults, multiple injections do not have any impact. However, in the coordinates where the harmonic faults were induced, multiple injections enabled to either force higher harmonics or switch between the harmonics within the range shown in Fig. 5(a). For instance, in the X7Y3 coordinate linked with the 3rd harmonic fault, injecting the 10 pulses induced the harmonic 17 as follows:

- 3 => 5 => 7 => 9 => 11 => 13 => 13 => 13 => 15 => 17.

While in the X10Y5 coordinate, the 10 injections resulted in a sweep between the harmonics 11, 13, 15 and 17 as follows:

- 15 => 11 => 13 => 17 => 17 => 17 => 15 => 17 => 15 => 13.

V. Conclusion and Future Work

This paper characterized the harmonic locking phenomenon occurring in a ring oscillator implemented in an Artix7 FPGA (28nm) under positive EM pulsed fault injection for different parameters related to the placement and routing of the inverters in the RO or of the IO control, and with respect to the number of pulse injections. We have shown that with specific configurations, we can tune the response of the RO to EMFI in order to either be able to harden, or detect, EM fault attacks.

During other tests, we tried to conduct the same experiments presented above with a negative EM pulse polarity and the preliminary results revealed that this parameter changes the location of faults. Thus, future works will also include experiments with this parameter to characterize, analyze, and eventually be able to forecast the effect of EMFIs on RO-based digital circuits. Lastly, these effects will be studied on other FPGAs to explore the effect on different manufacturing technologies, packaging, and structures of the programmable fabric.

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] T. Korak, M. Hutter, B. Ege, and L. Batina. Clock glitch attacks in the presence of heating. In Workshop on Fault Diagnosis and Tolerance in Cryptography, pages 104–114, 2014.

[2] T. Korak and M. Hoefler, "On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, IEEE, Sep. 2014, pp. 8–17.

[3] J. Breier and X. Hou, "How Practical Are Fault Injection Attacks, Really?," *IEEE Access*, vol. 10, pp. 113122–113130, 2022.

[4] S. El Amraoui, A. Douadi, R. Leveugle, P. Maistri, "Harmonic response of ring oscillators under single electromagnetic pulsed fault injection", accepted at IEEE 25th Latin American Test Symposium, Maceió, Brazil, April 9-12, 2024.

[5] 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.

[6] O. Trabelsi, L. Sauvage, and J.-L. Danger, "Impact of Intentional Electromagnetic Interference on Pure Combinational Logic," in *2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, IEEE, pp. 398–403, Sep. 2019.

[7] Z. Zhang, S. Yang, and T. Su, "The behavior of frequency locking of ring oscillators with RF interference on the supply," *Microelectronics J*, vol. 116, p. 105247, Oct. 2021.

[8] U. Mureddu, N. Bochard, L. Bossuet, and V. Fischer, "Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 7, pp. 2560–2571, Jul. 2019.

[9] 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.

[10] S. Osuka *et al.*, "EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and em Information Leakage," *IEEE Trans Electromagn Compat*, vol. 61, no. 4, pp. 1122–1128, Aug. 2019.

[11] P. Bayon et al., "Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator," in Constructive Side-Channel Analysis and Secure Design: Third International Workshop, COSADE 2012, May 2012.

[12] A. Proulx, J. Thibodeau, B. Bourgault, J.-Y. Chouinard, A. Miled, and P. Fortier, "Investigating the Effect of Electromagnetic Fault Injections on the Configuration Memory of SRAM-Based FPGA Devices," in *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, IEEE, Oct. 2023, pp. 1–7.

[13] 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*.