Harmonic Response of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection

Sami El Amraoui, Aghiles Douadi, Régis Leveugle, Paolo Maistri

Harmonic Response of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection

Sami El Amraoui, Aghiles Douadi, Régis Leveugle, Paolo Maistri
Univ. Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000, Grenoble, France
firstname.lastname@univ-grenoble-alpes.fr

***Abstract*— Ring Oscillators (ROs) are essential building blocks in digital devices used for instance in clock generation, True Random Number Generators (TRNGs), Physical Unclonable Functions (PUFs) or on-chip voltage or temperature sensors. Their response to laser pulses, EM (ElectroMagnetic) harmonic fault injections or radio frequency interferences injected into the power distribution network has already been extensively studied. In this paper, we present experimental characterization results of EM pulsed fault injection performed on ROs implemented in FPGAs. We highlight the occurrence of harmonic responses with variable characteristics depending on several parameters, such as the RO placement within the FPGA chip, the timing and location of the injection and the electromagnetic pulse width and amplitude. We show that the usual fault model based on Single Event Transients (SETs) can only partially explain the faulty behavior, even after a single pulse injection.**

Keywords*— *Ring oscillators, EMFI, Single pulse injection, Harmonic locking, SET, FPGA security

I. INTRODUCTION

Physical attacks and specifically fault attacks have long been a serious threat in the world of embedded secure devices. A variety of techniques, such as laser beams, EM emissions, power or clock glitches and heat have been applied to various devices and have been proven effective in bypassing security features (e.g., password checks), extracting confidential information and gaining unauthorized access [1]. Among these techniques, EM Fault Injection (EMFI) has been pointed out as one of the most effective ways to inject faults into digital circuits because of its relatively good accuracy, reasonable cost and no need for chip decapsulation [2]. Thus, designers should assess the vulnerability of their devices to EMFI very early and understand the behavior of the whole system in the presence of faults to define and validate appropriate countermeasures at the hardware and software levels.

In order to design effective countermeasures, it is necessary to have realistic and precise fault models. Fault models are proposed in the state of the art, but remain to be refined. Within this context, this paper aims to more comprehensively model electromagnetic faults on a cascade of combinational logic gates as previously studied in [3], except that here we focus particularly on the case of Ring Oscillators (ROs) made by cascaded inverters and implemented in a Field-Programmable Gate Array (FPGA) chip.

The main contribution of the study presented in this paper is evaluating the harmonic locking impact of a single EM pulse on the original frequency of a RO when (1) its placement constraints FPGA and (2) the EMFI parameters (the pulse width and amplitude, and the injection timing and location) are defined in different ways. The resulting harmonic errors may lead to system errors and synchronization problems causing unreliable operation of digital devices, which makes the characterization and the hardening of RO designs against them of paramount importance.

The remainder of this paper is organized as follows. In section II, the necessary background on EM fault injection is detailed as well as previous attacks related to the locking phenomenon on ROs. The experimental setup and methodology are described in section III. Section IV discusses the results with respect to the impactful parameters. Finally, section V draws conclusions and provides perspectives.

II. BACKGROUND

EMFI was first introduced in a paper dating from 2002 [4]. It is a direct exploitation of the electromagnetic induction principle stating that a parasitic current is expected to be induced in all wire loops of an integrated circuit (IC) after a sudden variation of the magnetic field.

A. EMFI Mechanism

EMFI enables an adversary to inject errors on a circuit to gain knowledge of sensitive information or to bypass security features. EM coupling can be used in two different ways: harmonic Fault Injection and pulsed Fault Injection. The first one consists in exposing the circuit to continuous EM waves to target analog blocks whose operation is not clocked but continuous in time; examples are clock generators or TRNGs as studied in [5]. On the other hand, pulsed EMFI disrupts the behavior of ICs during a few clock cycles by generating sudden variations of the magnetic field in a reduced volume close to the IC surface. These variations induce parasitic currents in the closed loops of the power and ground networks of the DUT.

In this work, we are mainly interested in single short perturbations and therefore our EMFI will be focused on EM pulses.

B. Related Works

1) EM Fault Models

To improve the efficiency of fault injections, many research papers [6] [7] tried to investigate how different components of an EM-pulse injection setup and design parameters affect the final pulse shape. These studies provided guidelines supported by experimental results showing that a good tuning of the EM-pulse setup to the target device is critical for the success rate of an EM injection campaign. Yet, even after doing that, the amount of parameters an evaluator has to tweak to obtain a fault is still quite large. In fact, a complex challenge during EM injections is the optimization of the large parameters set to obtain exploitable faults knowing that the evaluation is always time-

* Institute of Engineering Univ. Grenoble Alpes

limited. As a reminder, the list of parameters includes: the pulse amplitude, the pulse width, the pulse polarity that can be either positive or negative, the position of the EMFI probe above the IC surface, the choice of the probe characteristics and the moment at which the EM pulse is delivered with respect to the target's operation.

In previous works, the purpose of EM fault modeling was to describe the type of faults that can be induced and their consequences in integrated circuits. To the best of our knowledge, the state-of-the-art highlights that logical faults induced by EMFI are either bitset, bitreset, bitflip or no-sampling. They are related to two main fault models: Timing and Sampling.

EMFI can induce timing faults in two ways. First, the pulse brings disturbances on the power networks, increasing the signal propagation delay and leading to the violation of timing constraints [8], [9]. Second, the attack can directly perturb the clock network to generate clock glitches [10]. This first model was not able to explain all the faults obtained by EMFI. Indeed, bitset and bitreset faults can be injected into D-type flip-flops (DFFs) that are not triggered by the clock signal [11]. This led to the sampling fault model, validated during injection campaigns on an FPGA target (Xilinx Spartan3-1000) and a 32-bit microcontroller, both integrating a hardware implementation of 128-bit AES. By shifting in time (throughout the encryption) the occurrence of the EM pulse injection, they found that the fault occurrence follows the period of the clock and the width of these sensitivity windows depends on the routing of power and ground networks in the target circuit. This work was then refined in [12], showing that the pulse applied to the probe generates two EM pulses of opposite polarities. The first induces a transient reversal of the supply voltage while the second restores it, which disrupts the clock and logic signals and leads to a wrong sampling by the DFF at the phase of the fast clock signal recovery.

The fault model associated with EMFI remains complex because of the challenges faced by the evaluator during the characterization of different targets using different injection platforms. It has been shown throughout many papers that each of the two models can be more accurate, depending on the clock frequency of the circuit and the strength of the EM coupling within the circuit. For example, when attacking a circuit running at a low clock frequency thus having large timing slacks, the variation in propagation delays will be proportionally small and the sampling model would be able to explain the faults induced. However, if we are interested in higher frequencies, the timing model becomes relevant. This was confirmed in a recent paper by Nabhan et al. [13] where they evaluated the effectiveness of a sampling fault model-based EMFI detection sensor introduced by Elbaze et al. [14]. After performing various experiments on an FPGA-based Advanced Encryption Standard (AES) accelerator accompanied by 16 sensors, they validated the sensor's inefficiency for operating frequencies exceeding 150 MHz. Besides, they highlighted that the power distribution network is the most sensitive on-chip network at high frequencies while at low or moderate frequencies; it is the clock distribution network that is highly susceptible.

In the case of a design implementing ROs, both fault models may become less accurate since combinational logic in a loop is also subject to EMFI. Therefore, it is crucial to consider the resulting harmonic errors of EM pulsed injection

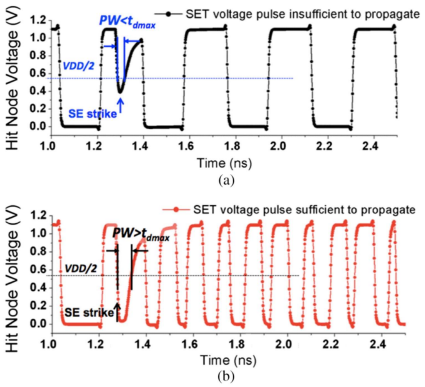


Fig. 1. Case when SET pulse width is (a) insufficient and (b) sufficient to propagate through RO (Figure from [17])

on ROs towards a more global and comprehensive fault model for EMFI on digital circuits.

2) Locking of Ring Oscillators

The term "locking" refers to when the RO originally runs at a fundamental frequency and is then forced to oscillate at another frequency. Previous studies on ROs focused mainly on the locking phenomenon happening due to radio-frequency interference on the power supply [15] or sinusoidal perturbation signals passed across a delay line placed near the RO [16], which makes them lock onto a signal with a frequency close to their natural oscillation frequency or its harmonics which are multiples of the original frequency. This locking phenomenon can render the confidential key generated using RO-based TRNGs partially or even fully deterministic by controlling the bias as demonstrated in [5] through EM harmonic injections.

3) Sustained Harmonic Errors

When one or several SETs are induced during one oscillation period T of the RO, it deviates from its fundamental frequency and locks to one of its harmonics depending on the number of extra rising edges induced in the period of oscillation.

The conditions to induce sustained third harmonic errors from a single particle strike at the output of the RO were detailed in [17] as follows:

- The SET must introduce one rising edge and one falling edge transition within half the oscillation period.
- The pulse width of the SET (t_{SET}) should be greater than the largest gate propagation delay in the ring (t_{dmax}):

$$\mathbf{t_{SET} > t_{dmax}} \quad (1)$$

- t_{SET} should be smaller than the total loop delay (L = T/2) minus $2t_{dmax}$:

$$\mathbf{t_{SET} < L - 2\ t_{dmax}} \quad (2)$$

Fig. 1 [17] shows two cases when the SET pulse width is either insufficient or sufficient to propagate in the RO and possibly force it into the third harmonic. The authors of the paper were able to validate the harmonic vulnerability with both laser experiments on a custom-designed 40nm Bulk CMOS ring oscillator and electrical experiments on a RO constructed with discrete components.

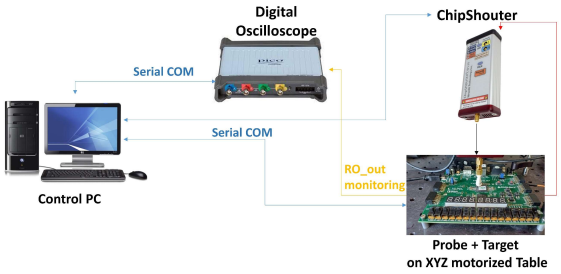


Fig. 2. Experimental setup

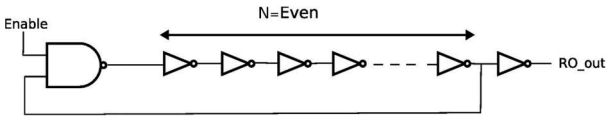


Fig. 3. Architecture of a ring oscillator

III. EXPERIMENTAL SETUP & METHODOLOGY

A. EMFI Setup

We use the following equipment for performing the EMFI experiments as shown in Fig. 2:

1) Target FPGA: We used the NEXYS A7 board, which is equipped with a Xilinx Artix-7 FPGA (technology node 28nm). The major components of the FPGA bitstream are the ROs and the state machine for the EM pulse trigger. To enable or disable the oscillations of the RO, we used a physical switch on the board. When the switch is enabled, the RO starts oscillating and the FPGA outputs a trigger signal forcing the pulse generator to inject an EM pulse. When the switch is disabled, the RO stops oscillating.

2) Pulse Generator: We used the ChipShouter pulse generator for this work to perform EM pulsed fault injection. This device can generate pulses with amplitudes from 150V up to 500V and pulse widths ranging from 20ns to 300ns. Properties of the pulse are configured using the RS-232 serial port interface.

3) XYZ Motorized Table: The motors are used to precisely control the position of the EM probe. They can set the X, Y, and Z positions with 7µm accuracy via an RS-232 serial control interface.

4) EM Probe: We used one of the ChipShouter probes consisting of a 1mm wire coiled clockwise (CW) around a 4mm ferrite core to create and guide the magnetic field lines toward the target.

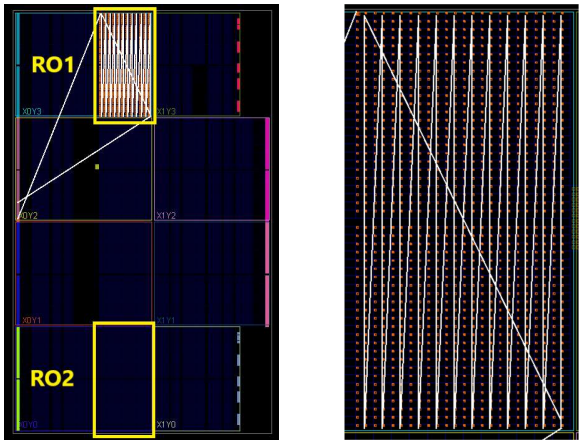
5) Control PC: It controls the whole platform through serial ports.

6) Digital Oscilloscope: A Picoscope with 200 MHz bandwidth was used to monitor the frequency of the RO and the synchronization between its oscillations and the EM pulse.

B. RO Layout

1) Ring Oscillator

A ring consists of a number of inverting and activation gates connected in series to form a ring. This number depends on the type of ring and its expected behavior. Fig. 3 shows the architecture of our implemented RO with an even number N of inverters and a Nand gate used as an activation gate.



(a) (b)

Fig. 4. (a) FPGA floorplan showing the placement of RO1 and RO2 (b) Vertical routing of the inverters

After the Enable signal moves from a low to a high level, oscillations start; if we force the Enable signal to low, the oscillations stop. At any time, only the rising or falling edge is propagating across the RO and after a full lap, the rising edge is transformed into a falling edge or vice versa. The oscillation frequency of the RO depends on many parameters and it can be simplified in the following equation:

$$\mathbf{F_{RO}} = \frac{1}{2\,(\mathbf{d_{Nand}} + \mathbf{N}\,\mathbf{d_{Inverter}})} \qquad (3)$$

where d_{Nand} is the delay of the Nand gate, $d_{Inverter}$ is the average delay of an inverter and N is the number of inverters.

2) Placement and Routing Constraints

In our FPGA, each Configurable Logic Block (CLB) tile contains two slices and each slice contains 4 Look-Up Tables (LUTs): each is configured as an inverter or a Nand gate to form our RO. In our experiments, N = 1200 (24 × 50) inverters. The placement of the inverters was constrained either to the top clock region (X0Y3) or to the bottom one (X0Y0) as highlighted with a yellow rectangle in Fig. 4(a) showing the extracted floorplan of the design from the Vivado tool. Fig. 4(b) shows the vertical routing of the inverters adopted for both ROs. A bitstream file was separately generated for each RO placement. Table I lists the frequency of the ROs depending on their placement.

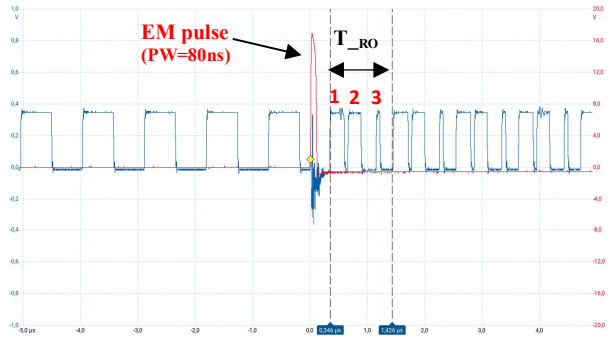
C. Methodology

Initial tests with different EM pulse parameters enabled us to observe the following behaviors of the RO output after a single pulse injection:

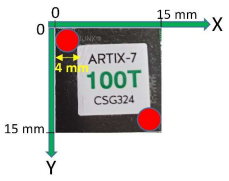
- **Unchanged frequency:** In that case, after the attack, the RO still oscillates at the same fundamental frequency $F_{\_RO}$. If we turn off the Enable signal and the RO keeps oscillating, we know that the bitstream was corrupted and we need to reprogram it.

TABLE I. CHARACTERISTICS OF THE TWO SEPARATELY IMPLEMENTED ROS

	Clock region	Frequency
RO1	X0Y3	927 KHz
RO2	X0Y0	925 KHz



(a)



(b)

Fig. 5. (a) 3rd harmonic induced error (b) Initial & Final probe position

- **Harmonic locked frequency:** After the attack, the RO frequency can be locked into one of its odd harmonics (3, 5, 7….). If we disable the oscillations and the monitored output signal of the RO still shows the same harmonic frequency it means that the bitstream was corrupted and we need to reprogram it for the next test. Fig. 5(a) shows the case where an EM pulse injection induced three rising edges within a single period of oscillation, which locked the RO to its third harmonic.
- **Noise signal:** the attack can also force the RO output signal to noise, which means the bitstream was corrupted as resetting the enable signal doesn't restart oscillations. Therefore, reprogramming the bitstream is always mandatory before the next test.

Fig. 6 gives an overview of all the observed behaviors after the single pulsed injection.

Based on these observed effects, the following procedure was then adopted to inject a single pulse into the RO. The goal is to detect the occurrence of harmonic induced faults and bitstream corruptions over repeated measurements while moving the 4 mm CW probe kept in contact (Z = 0) on top of the FPGA package (15mm x 15mm) by steps of 1 mm (due to the probe's resolution) from top left to bottom right as shown in Fig. 5(b):

1st step: Set the initial EM pulse parameters for the test (amplitude = 450V / PW = 80ns)
2nd step: Place the probe at a given coordinate above the chip package (initial XY value (0, 0))
3rd step: Program FPGA with the bitstream
4th step: Trigger the enable signal of the RO and the delayed EM pulse injection
5th step: Monitor the output RO frequency after injection then disable the RO to detect the occurrence of harmonic induced frequencies and bitstream corruptions
6th step: Repeat ten times step 4 and step 5 to assess the reproducibility rate for the given (X, Y) coordinates
7th step: 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

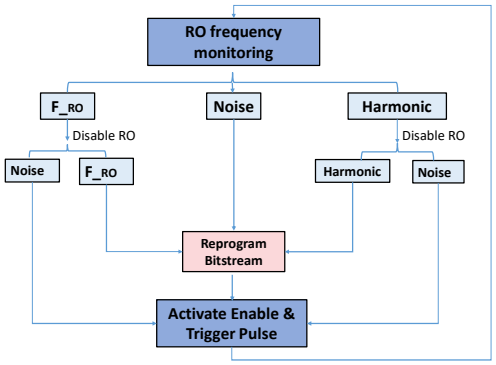


Fig. 6. Behavior of RO after EMFI

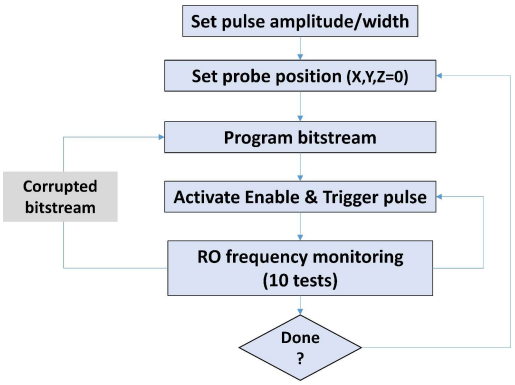


Fig. 7. Flowchart of EMFI on the RO

Fig. 7 represents the flowchart of the described procedure.

IV. EXPERIMENTAL RESULTS

In this section, we show harmonic locking errors detected after single pulsed injections and how the fault locations correlate with the different parameters related to placement within the chip and the EM pulse amplitude and width.
We emphasize that the timing of the injection was not controlled during these tests. 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.

A. RO Placement Effect

Following the preliminary experiments, EM injection campaigns were conducted using the procedure mentioned in section III-C while targeting separately the two ROs RO1 and RO2 running at F_{RO1} = 927 KHz and F_{RO2} = 925 KHz with a pulse of voltage amplitude = 450V and PW = 80ns. The numbers in Fig. 8(a) and Fig. 9(a) refer to the ratio between the monitored frequency after EM injection and the fundamental frequency of the targeted RO (F_{RO1} or F_{RO2}) while Fig. 8(b) and Fig. 9(b) provide the probability of inducing the harmonics in the corresponding (a) figures.

To improve the readability of the fault sensitivity maps, we assigned a specific color and symbol for each effect:

- **Green:** No faults (Frequency remained the same and the bitstream was not corrupted).
- **Grey (with X mark):** Noise signal (due to bitstream corruption) => Probability of bitstream corruption = 100%.

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	5 – 9	5 – 9	1
Y=2	1	1	1	1	1	1	1	1	1	13 – 17	13 – 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	15 – 19	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

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

(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	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Y=1	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	100%	0%
Y=2	0%	0%	0%	0%	0%	0%	0%	0%	0%	100%	100%	0%
Y=3	0%	0%	0%	0%	0%	0%	0%	70%	90%	100%	100%	0%
Y=4	0%	0%	0%	0%	0%	0%	70%	60%	50%	100%	100%	0%
Y=5	0%	0%	0%	0%	0%	0%	70%	60%	0%	0%	100%	0%
Y=6	0%	0%	0%	0%	0%	0%	0%	30%	0%	0%	0%	0%
Y=7	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Y=8	0%	0%	0%	0%	0%	X	X	0%	0%	0%	0%	0%
Y=9	0%	0%	0%	0%	X	X	X	X	0%	0%	0%	0%
Y=10	0%	0%	0%	0%	X	X	X	X	X	0%	0%	0%
Y=11	0%	0%	0%	0%	X	X	X	X	X	0%	0%	0%

(b)

Fig. 8. (a) RO1 fault sensitivity map (b) Probability of inducing harmonics

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 – 5	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

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

(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	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Y=1	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Y=2	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Y=3	0%	0%	0%	0%	0%	0%	0%	80%	70%	0%	0%	0%
Y=4	0%	0%	0%	0%	0%	0%	40%	90%	50%	0%	0%	0%
Y=5	0%	0%	0%	0%	0%	0%	30%	70%	0%	0%	0%	0%
Y=6	0%	0%	0%	0%	0%	0%	0%	50%	0%	0%	0%	0%
Y=7	0%	0%	0%	0%	0%	70%	0%	0%	0%	0%	0%	0%
Y=8	0%	0%	0%	0%	0%	X	X	0%	0%	0%	0%	0%
Y=9	0%	0%	0%	0%	X	X	X	X	0%	0%	0%	0%
Y=10	0%	0%	0%	0%	X	X	X	X	X	0%	0%	0%
Y=11	0%	0%	0%	0%	X	X	X	X	X	0%	0%	0%

(b)

Fig. 9. (a) RO2 fault sensitivity map (b) Probability of inducing harmonics

- **Gradient White to Red box:** shows in Fig. 8(a) and Fig. 9(a) the harmonic intensity with 3 being the lowest and 19 being the highest observed (in case two numbers are mentioned, they represent the lowest and highest recorded induced odd harmonic frequency within the 10 tests). In Fig. 8(b) and Fig. 9(b), the gradient shows the level of reproducibility.

Examination of fault sensitivity maps in Fig. 8(a) and Fig. 9(a) demonstrates that placing ROs with a similar number of stages in different parts on the FPGA chip may exhibit different responses under single pulse injection. Although both ROs share a similar fault sensitivity when targeting the bottom and upper center of the FPGA package, it is clear that the RO1 placed on top of the design is more vulnerable to induced harmonic errors than the RO2 since the highest forced harmonic error for RO1 is 19 while it is only 5 for RO2 in one specific coordinate.

Further experiments were conducted on two other similar Artix7 FPGAs and the results revealed an identical fault distribution for both RO1 and RO2 with only a small variation in the intensity of harmonic errors.

B. *Pulse Width Effect*

In order to highlight the impact of the Pulse Width (PW) on harmonic errors, we focused on a sensitive coordinate (X10Y5) and we conducted tests on RO1 with a single pulse of 450V while varying the PW from 60ns to 140ns by steps of 20ns. Ten tests were performed for each PW value to characterize the impact on the harmonic response. As shown in Table II, the output of RO1 exhibits a higher harmonic vulnerability as the PW increases. In fact, when performing EMFI with PW = 60ns, the single pulse injection did not affect the RO meaning that in our setup 80ns is the minimum PW that can lead to harmonic errors in that coordinate. Moreover, the harmonic response increased from (11-17) for PW = 80ns to (13-19) for PW = 100ns, finally locking with a 100% probability on the 19th harmonic for PW = 120ns and PW = 140ns. Let us notice that for this position, a small increase of the pulse width from 60 ns to 80 ns quickly leads to high harmonics, while similar increments over 80 ns do not exhibit the same type of consequence.

C. *Pulse Amplitude Effect*

To explore the influence of the pulse amplitude on the harmonic vulnerability of the RO, we conducted other tests. RO1 was targeted at the same coordinate X10Y5, with a fixed PW = 80ns while increasing the amplitude from 150V to 500V by steps of 10V and recording the harmonic response. When generating pulses with amplitudes ranging from 150V to 430V, no harmonic response was induced; therefore, only the limited range of amplitudes (430V – 500V) is shown in Fig. 10. As illustrated in the figure, increasing the voltage amplitude of the pulse did not necessarily lead to inducing higher harmonics but rather increased their occurrence. The

TABLE II. PULSE WIDTH IMPACT ON HARMONICS INTENSITY (RO1 – 450 V – COORDINATE X10Y5)

	PW (ns)				
Test	60	80	100	120	140
1	1	13	15	19	19
2	1	17	15	19	19
3	1	15	13	19	19
4	1	13	17	19	19
5	1	11	17	19	19
6	1	13	13	19	19
7	1	15	15	19	19
8	1	13	15	19	19
9	1	15	15	19	19
10	1	13	19	19	19

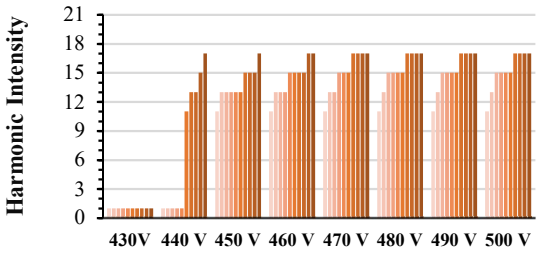


Fig. 10. Pulse amplitude impact on harmonics occurrence (RO1 – PW = 80ns – X10Y5 Coordinate)

range of harmonic errors remained at (11-17) throughout the entire campaign.

This observation suggests that for each coordinate a certain threshold of EM stress should be applied to start inducing harmonic errors within a specific range. To confirm this assumption, we conducted the same tests in the other coordinates with high susceptibility to harmonic errors and we validated that depending on the location, after a threshold voltage only the harmonic occurrence can change and not the range of harmonic response. Furthermore, when conducting similar tests on the X7Y4 and X7Y3 coordinates on which we were only able to force the third harmonic with a pulse of 450V and PW = 80ns, we observed through increasing the amplitude from 150V by steps of 5V that the voltage threshold to induce the third harmonic was 310V and 360V respectively. As the amplitude increases and we reach 460V for X7Y4 and 490V for X7Y3, the bitstream corruption becomes inevitable.

Given the experiments and observations described in this section, we conclude that a minimal voltage and PW threshold must be applied to induce harmonic errors or bitstream corruptions. Furthermore, forcing higher harmonics with higher probabilities could be achieved in particular locations in the FPGA just by increasing the width and the amplitude of the pulse.

V. Conclusion and Future Work

In this paper, we presented the harmonic locking phenomenon occurring in ring oscillators under different parameters of a single EM pulsed fault injection. We showed for the first time that locking the RO frequency into one of its harmonics could be achieved without the use of continuous EM waves or laser fault injection but rather with a single EM pulse properly tuned. The effects were characterized for two ROs implemented with the same number of stages in an Artix7 FPGA (28nm). Specifically, we characterized the magnitude of the harmonic response as a function of the RO placement in the FPGA chip, the electromagnetic pulse width, the pulse amplitude, and the position of the probe relative to the FPGA package.

In our future work, the harmonic locking phenomenon will be studied on other FPGAs to explore the effect on a different internal FPGA structure (28nm) or technology (45nm). On the other hand, it is important to point out that during other experiments, we noticed that the pulse polarity and multiple injections with controlled timing affect the location and the intensity of the faults. Thus, future work will also include experiments with these parameters to characterize, analyze and eventually be able to forecast the effect of EMFI on RO-based digital circuits.

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] C. Shepherd et al., “Physicals fault injection and side-channel attacks on mobile devices: A comprehensive analysis,” Comput Secur, vol. 111, p. 102471, Dec. 2021.

[2] A. Beckers, S. Guilley, P. Maurine, C. O’Flynn, and S. Picek, “(Adversarial) Electromagnetic Disturbance in the Industry,” *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 414–422, Feb. 2023.

[3] 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.

[4] 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.

[5] 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.

[6] J. Toulemont, F. Mailly, P. Maurine, and P. Nouet, “Exploring flexible and 3D printing technologies for the design of high spatial resolution EM probes,” in *2021 19th IEEE International New Circuits and Systems Conference (NEWCAS)*, IEEE, pp. 1–4, Jun. 2021.

[7] A. Beckers *et al.*, “Design Considerations for EM Pulse Fault Injection” in Smart Card Research and Advanced Applications: 18th International Conference, CARDIS 2019, Nov 2019.

[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] O. Trabelsi, L. Sauvage, and J.-L. Danger, “Characterization at logical level of magnetic injection probes”, in Joint Int, Symp. Electromagn. Compat. Sapporo Asia-Pacific Int. Symp. Electromagn. Compat., 2019

[10] 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.

[11] S. Ordas, L. Guillaume-Sage, and P. Maurine, “Electromagnetic fault injection: the curse of flip-flops,” *J Cryptogr Eng*, vol. 7, no. 3, pp. 183–197, Sep. 2017.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.