On the Harmonic Locking of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection in FPGAs

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

On the Harmonic Locking of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection in FPGAs

Sami El Amraoui Aghiles Douadi Régis Leveugle Paolo Maistri

Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000, Grenoble, France
{sami.el-amraoui,aghiles.douadi,regis.leveugle,paolo.maistri}@univ-grenoble-alpes.fr

Abstract. ElectroMagnetic Fault Injection (EMFI) attacks have garnered noteworthy attention in the world of embedded secure devices due to the optimal balance between the attack effectiveness and the setup requirements. Since Ring Oscillators (ROs) can be critical components for secure primitives such as True Random Number Generators (TRNGs), Physical Unclonable Functions (PUFs) and on-chip voltage or temperature sensors, their response to this potent threat needs to be fully investigated. In this paper, we contribute to a deeper understanding of EMFI faults by performing single EM pulsed fault injections on ROs implemented in Field-Programmable Gate Arrays (FPGAs). The fault models proposed in the state of the art, such as the Sampling Fault Model and the Timing Fault Model, mainly refer to synchronous logic and are not tuned for asynchronous combinational logic in a loop. Our findings reveal that harmonic locking explains the occurrence of harmonic errors with variable characteristics depending on the different EM pulse settings, the RO placement within the FPGA chip and the manufacturing properties of the FPGA. These findings improve our understanding of EMFI's impact on different architectures and can be leveraged to design more robust hardware implementations against this attack.

Keywords: Ring oscillators, EM Fault Injection, Single pulse injection, Harmonic locking, FPGA security.

1 Introduction

The widespread use of digital systems nowadays led to a massive spread of data in uncontrolled environments where security vulnerabilities expose sensitive data to cybercriminals, allowing them to access personal information or take control of devices. Therefore, to guarantee data protection, designers augmented their devices with optimized hardware implementations of cryptographic features and hashing algorithms. However, physical attacks remain a serious threat to their effectiveness through side-channel and fault attacks. Side-channel attacks exploit unintended information leakage from a system's physical implementation. These attacks gather data such as power consumption, electromagnetic emissions, timing or even temperature and acoustic information, which can then be analyzed to infer sensitive information like cryptographic keys [6]. On the other hand, in the realm of fault attacks, a variety of techniques such as laser [1] or X-ray beams [2], EM emissions [3], power [4] or clock glitches and heat [5] have been applied to devices and have been proven effective in bypassing security

features (e.g., password checks), extracting confidential information and gaining unauthorized access [6]. 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 [7] and no need for chip decapsulation [8] [9]. Thus, designers should very early assess the vulnerability of their devices to EMFI and understand the behavior of the whole system in the presence of faults to define and validate appropriate countermeasures on the hardware and software levels.

In order to choose effective countermeasures, impacting the performance of the system as slightly as possible, 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 for hardware implementations including asynchronous combinational logic. Within this context, this paper aims to enhance the understanding of the harmonic locking impact on ROs with pulsed EMFI in FPGAs. This vulnerability was first introduced in our paper [10] where we demonstrated the locking of the RO frequency into one of its harmonics through a single properly tuned EM pulse. The RO harmonic response was only characterized with respect to its placement in the FPGA chip, to the EM pulse width (PW) and amplitude, and to the position of the probe over the FPGA package.

In this study, we further elaborate on the influence of other parameters related to the EM pulse, the RO layout and the manufacturing or packaging features of the FPGA. Analyses go as far as possible, in spite of the limited visibility into the internal structure of the FPGA's power distribution network (PDN). To go beyond and fully interpret the differences observed in response to the variation of the pulse properties, the experiments reported in this paper should be replicated in further work on a dedicated Application-Specific Integrated Circuit (ASIC), where the PDN architecture would be explicitly known and accessible. At that time, in more detail, the contributions of this paper consist of:

- Demonstrating the impact of pulse polarity on the fault distribution and its magnitude for different RO placements.
- Providing the threshold voltage of the induced faults with both pulse polarities to highlight the different fault susceptibility of the power and ground network in an FPGA.
- Showing how the injection timing of the pulse can enable more control over the range of induced harmonic errors.
- Analyzing the effect of process variation and FPGA packaging technology on the harmonic response of the RO to underline the importance of conducting tests across various FPGAs of similar manufacturing technology.

The remainder of this paper is organized as follows. Section 2 introduces the related works on EMFI as well as the locking phenomenon on ROs. The experimental setup and methodology is described in Section 3. Section 4 reports and analyzes the experimental results. Finally, Section 5 draws conclusions and provides perspectives.

2 Background

2.1 EMFI Mechanism

EMFI was first introduced in a paper dating from 2002 [11], which explains how it corrupts 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 generated by a probe.

EMFI enables an adversary to inject errors on a circuit to gain knowledge of sensitive information or to bypass security features through EM coupling using two different ways: harmonic EMFI and pulsed EMFI. The former consists of exposing the ICs to continuous EM waves to usually target analog blocks of ICs whose operation is not clocked but continuous in time like clock generators or True Random Number Generators (TRNGs) as studied in [12] and [13]. 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 that 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; therefore, our EMFI will be focused on EM pulses.

2.2 Related Works

EM Fault Models. To improve the efficiency of fault injections, many research papers [14] [15] [16] [32] tried to investigate how different components of an EM pulse injection setup and design parameters can affect the final pulse shape and the outcome of the attack. These studies provided guidelines supported by experimental results showing that a good tuning of the EMFI setup to the target device is critical for the success rate of an EM injection campaign. Yet, even after accomplishing that, the number of parameters an evaluator has to tweak to obtain an exploitable fault is too wide knowing that the evaluation is always time-limited. Within this context, a recent paper [34] 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 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.

Considering all these challenges, EM fault modeling is required 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 about pulsed EMFI is largely focused on synchronous logic and highlights that logical faults are either bit-set, bit-reset, bit-flip or no-sampling. They are related to two main fault models: Timing and Sampling.

EMFI can induce timing faults in two ways. First, akin to the under-powering technique that causes setup time violations as introduced in [35], the pulse brings disturbances to the power networks, which may affect the signal propagation delay and lead

to the violation of timing constraints [17]. In the paper by Trabelsi et al. [18] for instance, the authors characterized the impact of EMFI on the propagation delay of a combinational logic path implemented in a Xilinx Virtex-II Pro chip while varying different settings of the EM pulse. Their results showed that a significant acceleration or deceleration impact on the path delay is possible due to EMFI when more than 100 successive pulses are injected. Second, the attack can directly perturb the clock network to generate clock glitches [19]. This first model was not able to explain all the faults obtained by the EMFI. Indeed, bit-set and bit-reset faults can be injected into D-type flip-flops (DFFs) that are not triggered by the clock signal [20]. 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, the authors found that the probability of inducing a fault follows a periodical pattern with a period equal to the clock period. The width of the time window during which faults occur is independent of the clock period but depends on the target circuit. This work was then refined in [21], showing that the pulse applied to the probe generates two EM pulses of opposite polarities. The first one induces a transient reversal of the supply voltage while the second restores it. Therefore, the disruption of clock and logic signals leads to a wrong sampling by the DFF at the phase of the clock signal recovery.

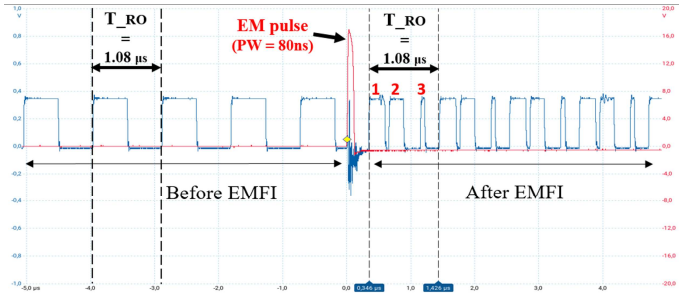
The fault model associated with EMFI remains complex because of the challenges faced by the evaluator during EMFI characterization of different targets using different injection platforms. It has been shown throughout many papers that each of the two models can be more accurate, depending on the clock 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 paper by Nabhan et al. [22] where the authors evaluated the effectiveness of a sampling fault model-based EMFI detection sensor introduced by El-Baze et al. [23]. After performing various experiments on an FPGA-based Advanced Encryption Standard (AES) accelerator implemented in addition to 16 sensors, they validated the sensor's inefficiency for operating frequencies exceeding 150 MHz. Besides, their study highlighted that the power distribution network is the main sensitive on-chip network at high frequencies, while at low or moderate frequencies it is the clock distribution network that is mostly susceptible.

In the case of a design implementing ROs, both fault models may become less accurate since they did not focus on asynchronous combinational logic in a loop that may also be subject to EMFI. Therefore, it is crucial to consider the resulting harmonic errors of EM pulsed injection on ROs towards a more global and comprehensive fault model for EMFI on digital circuits.

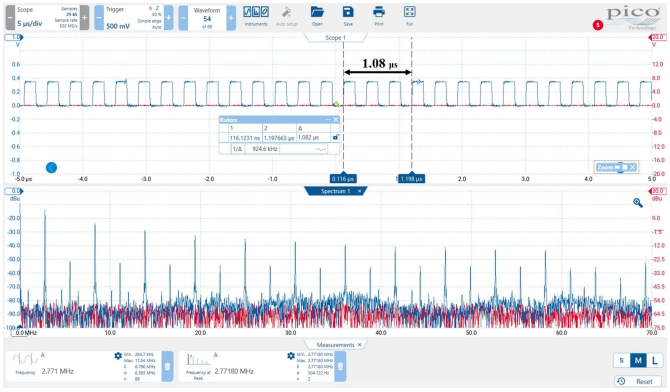
Locking of Ring Oscillators. The term "locking" refers to when the RO originally runs at a fundamental frequency and is forced to oscillate at another frequency. Previous studies on ROs focused mainly on the locking phenomenon happening due to radio-

frequency interference on the power supply [24] or sinusoidal perturbation signals passed across a delay line placed near the RO [25], which makes them lock onto a signal with a frequency close to their natural oscillation frequency or its harmonics. 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 [12] [26] through EM harmonic injections.

Sustained Harmonic Errors. When one or several Single Event Transients (SETs) 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 the period of oscillation. The reason behind inducing only odd harmonics can be explained by the fact that due to the odd symmetry of the RO, one rising/falling edge loops around the ring every half-oscillation period (T/2) leading to the fundamental frequency of operation. However, as we perform the attack, a number "n" of new transitions can be introduced in T/2. Thus, "2n+1" transitions loop around the RO, modulating the frequency to be the odd harmonic "2n+1". The conditions to



(a)



(b)

Fig. 1. (a) RO output response under a single EM pulse injection (b) RO output signal showing the sustained third harmonic error locked with a consistent duty cycle few hundreds of oscillations after EMFI

induce sustained third harmonic errors from a single particle strike at the output of the RO were detailed in [27] as follows:

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

$$t_{SET} > t_{dmax} \tag{1}$$

3. t_{SET} should be smaller than the total loop delay (L=T/2) minus two times t_{dmax}:

$$t_{SET} < L - 2\, t_{dmax} \tag{2}$$

Looking at all the previous fault models in comparison to our study focusing on the susceptibility of ROs to pulsed EMFI, the best fault model that fits our case is the last one defining harmonic errors [27]. Fig. 1(a) shows an example of a RO running originally at 925 kHz targeted by a single EM pulse injection. Since the injection settings led to the satisfaction of the three conditions above, two extra rising edges were induced within one period of oscillation which locked the RO to its third harmonic 2.775 MHz as shown in Fig. 1(b). It is important to note that after a few hundreds of oscillations the original duty cycle is restored and the harmonic error is sustained over time despite variations in temperature and voltage; however, it can be cleared by resetting the ring's oscillations.

3 Experimental Setup and Methodology

3.1 EMFI Setup

We used the following equipment shown in Fig. 2 to perform the EMFI experiments:

- Pulse Generator: We used the ChipShouter pulse generator for this work to perform EM pulsed fault injection. It can generate pulses with amplitudes from 150V up to 500V and variable pulse widths starting at 20ns. Depending on the probe's physical characteristics (e.g., diameter or wrapping direction of coils), the voltage amplitude applied to the probe and its distance from the target, we can indirectly control the strength of the resulting electromagnetic field produced by the probe as demonstrated in Figures 5 and 6 from [28].
- 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 via an RS-232 serial control interface.
- EM Probes: We used two of the EM probes provided with the ChipShouter and consisting of a 1mm wire coiled either clockwise (CW) or counter-clockwise (CCW) around a 4mm ferrite core to induce positive or negative polarity of the pulse respectively.
- Control PC: controls the whole platform through serial ports.

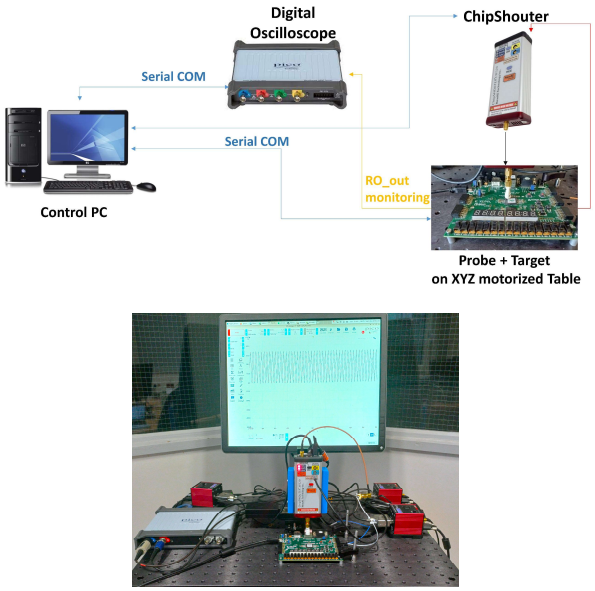


Fig. 2. Experimental setup

- Digital Oscilloscope: A Picoscope of 200 MHz bandwidth monitored the frequency of the RO and the synchronization between its oscillations and the pulse injection.
- Targets: Our characterization has been achieved on two types of Xilinx Artix-7 FPGAs (technology node 28nm). The first one is xc7a100T-1CSG324 embedded in a Nexys-A7 Digilent board shown in Fig. 2 while the second one is xc7a100T-2FTG256 within the CW305 ChipWhisperer board. The main difference between these two FPGAs is their type of packaging making the Nexys-A7 FPGA package size (15mm × 15mm) smaller than the CW305 (17mm × 17mm).

3.2 RO Layout

Ring Oscillator. A ring consists of a number of inverting and activation gates connected in a loop. 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 = 1200 of inverters and a Nand gate used as an activation gate.

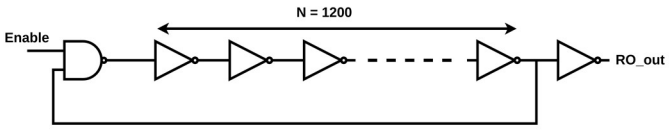


Fig. 3. Architecture of the targeted RO

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

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

where d_{Nand} is the delay of the Nand gate, $d_{Inverter}$ is the mean delay of the inverters and $d_{routing}$ is the average delay related to the routing between inverters.

Placement and Routing Constraints. In our FPGA, each Configurable Logic Block (CLB) tile contains two slices and each slice contains four Look-Up Tables (LUTs) that one of them will be configured later as an inverter gate or Nand gate to form our RO. The implemented RO features a Nand gate connected to 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 showing the extracted floorplan of the design from the Vivado tool. Fig. 4 shows also the vertical routing with long connections between LUTs that was adopted for both ROs. Therefore, a bitstream file was separately generated for each RO placement. Table 1 shows the frequency of the ROs depending on their placement. It should be noted that the FPGA

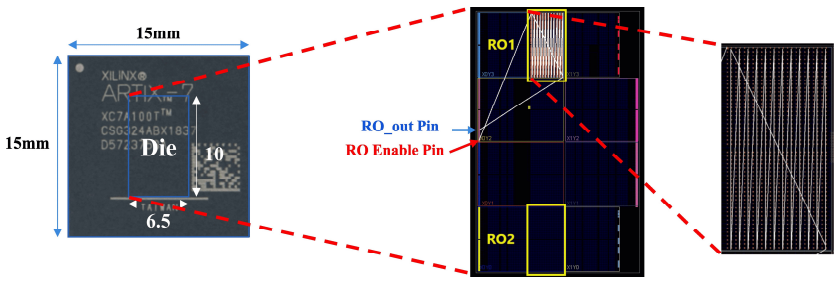


Fig. 4. Nexys-A7 FPGA die floorplan showing the P&R of RO1 and RO2

Table 1. Characteristics of the RO depending on its placement constraint

	Clock region	Frequency (kHz)
RO1	X0Y3	927
RO2	X0Y0	925

die represents only 6.5mm × 10mm of the whole package size (15mm × 15mm) as reported in [29].

3.3 Methodology

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

- **Unchanged frequency:** After the attack, the RO still oscillates at the same fundamental frequency F_{RO}. If we disable the RO (i.e. force the Enable signal from the input of the Nand gate to move low) 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 is locked into one of its odd harmonics (n = 3, n = 5, n = 7…) depending on how many transients were induced within half the oscillation period. If we disable the Enable signal 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.

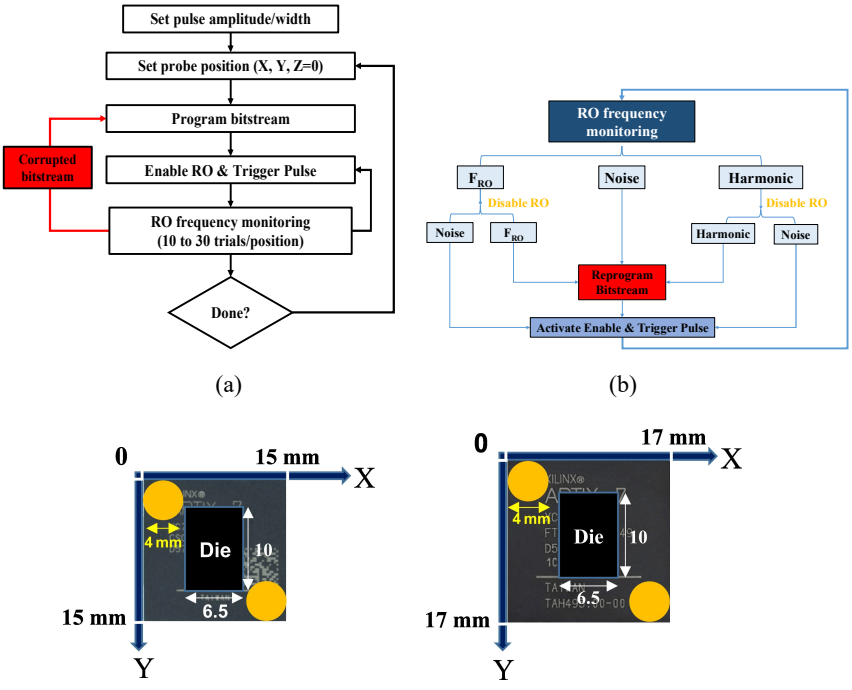


Fig. 5. (a) Flowchart of EMFI on the RO (b) Behavior of RO after EMFI (c) Scan of Nexys-A7 & CW305 FPGA Packages

- **Noise signal:** the attack forces 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. 5(b) 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 4mm CW/CCW probe kept in contact (Z = 0) on top of the FPGA package by steps of 1 mm (due to the probe's resolution) from top left to bottom right as shown in Fig. 5(c):

- **1st step:** Set the initial EM pulse parameters for the test (amplitude = 450V / PW = 80ns). The choice of these values is motivated by the results shown in the next sections 4.3 and 4.5.
- **2nd step:** Place the probe at a given coordinate [initial XY value (0, 0)] above the chip package.
- **3rd step:** Program FPGA with the bitstream.
- **4th step:** Trigger the Enable signal of the RO and the single EM pulse injection.
- **5th step:** Monitor the output RO frequency after injection then reset the RO to clear the occurrence of harmonic induced errors and detect bitstream corruptions.
- **6th step:** Repeat #step4 and #step5 to assess the reproducibility of faults for the same (X, Y) coordinate.
- **7th step:** Restart the procedure at #step3 for a new (X, Y) coordinate with a displacement step of 1mm until the last coordinate (X= 11, Y=11) for Nexys-A7 or (X= 13, Y=13) for CW305 to obtain a fault sensitivity map of the FPGA package.
  Fig. 5(a) represents the flowchart of the described procedure.

4 Experimental Results and Discussion

In this section, we show harmonic locking errors detected after single pulsed injections and how the fault locations correlate with different parameters related to the RO placement within the chip, the EM pulse polarity, amplitude, width, and timing. Furthermore, we show how process variation and the type of packaging can affect the occurrence of these faults for the same Artix-7 FPGA family.

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 the following maps refer to the ratio between the monitored frequency after EM injection and the fundamental frequency of the targeted RO:

- **Green box**: No faults (Unaffected frequency and the bitstream was not corrupted).
- **Grey box with X**: represents mutes where reprogramming the bitstream was mandatory; Probability of bitstream corruption is 100% in this case.
- **Gradient white to red box:** shows the odd harmonic intensity with 3 being the lowest (In case two numbers are mentioned, they represent the lowest and highest recorded induced odd harmonic frequency within 30 tests).

4.1 RO Placement Effect

Following the preliminary experiments, EM injection campaigns were conducted using the procedure described in Section 3.3 while targeting separately the RO1 and RO2 positions, running respectively at F_{RO1}= 927 kHz and F_{RO2}= 925 kHz with a positive pulse polarity of voltage amplitude = 450V and PW = 80ns.

Examination of fault sensitivity maps in Fig. 6(a) and Fig. 6(b) demonstrates that placing ROs with the same number of stages in different parts of the FPGA chip may exhibit different responses under a 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 the top clock region is more vulnerable to harmonic errors than the RO2, as the highest induced harmonic error for RO1 was 19 while it was only 5 for RO2 in only one coordinate. Additionally, the extension of the sensitive regions differs significantly, as RO2 shows only one exclusive sensitive spot, whereas several exist in the RO1 configuration. Upon this observation, one may conclude that placing the RO in the bottom clock region can harden it against harmonic errors. However, to be able to draw this conclusion, further tests (namely, with the opposite pulse polarity) are required.

4.2 Pulse Polarity Effect

Since the effect of RO placement on the fault sensitivity was accomplished only using the positive pulse polarity, we now investigate how the negative pulse polarity can affect the fault distribution while following the same methodology.

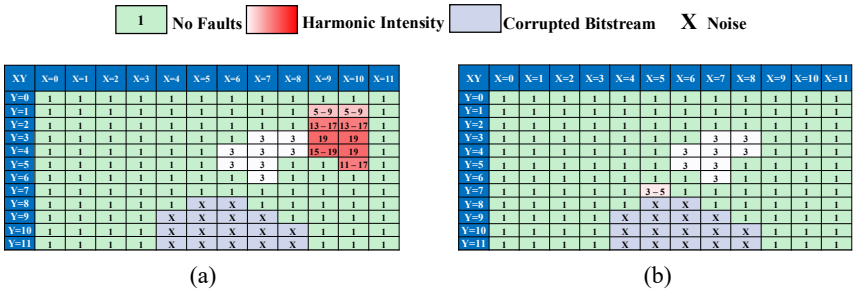


Fig. 6. Fault sensitivity maps with positive pulse polarity (a) RO1 (b) RO2

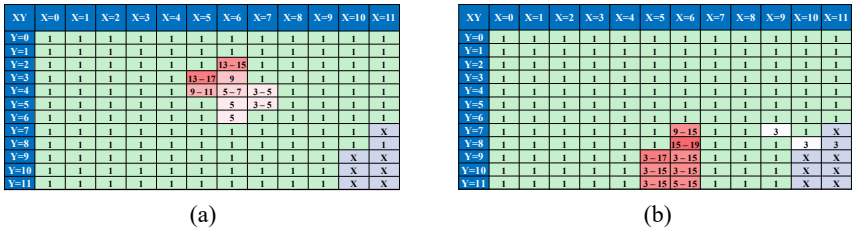


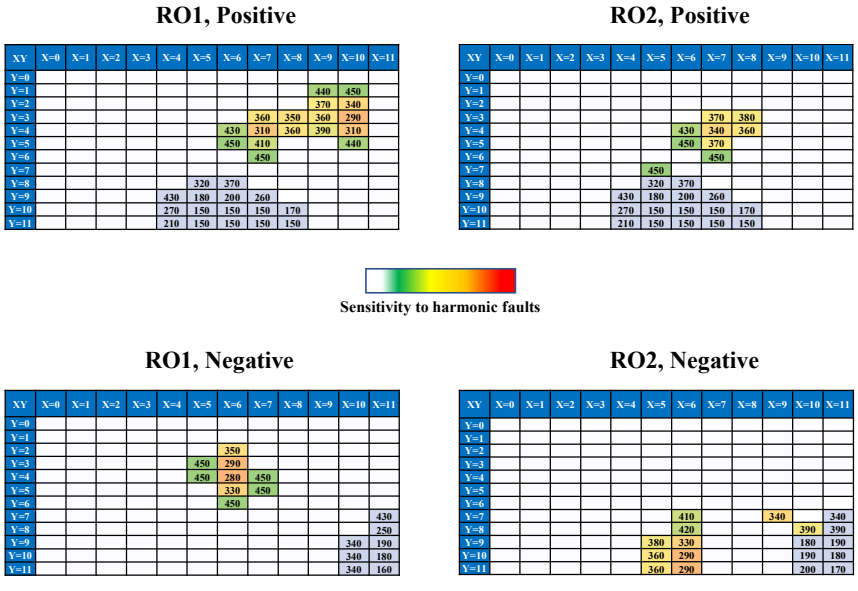
Fig. 7. Fault sensitivity maps with negative pulse polarity (a) RO1 (b) RO2

The results depicted in Fig. 7 reveal new fault locations in the FPGA package that seem to be complementary to the previous ones in Fig. 6. Let us notice first that similar to Fig. 6, both ROs share again similar fault locations in the bottom right of the FPGA package. This likely indicates that these faults are independent from the physical placement of the ring and suggests that they can be related to the FPGA's configuration memory. Furthermore, RO1 is no longer the most sensitive to harmonic errors, as high values of harmonic errors were also obtained for RO2. Therefore, claiming that a particular location in the FPGA is optimal for a design to harden it against EMFI can only be valid when tests are conducted using both pulse polarities. Similarly, the results suggest a different susceptibility of the power and the ground networks to the polarity of the EM pulse injection; it is therefore important to also explore this parameter's effect when assessing a detection mechanism against this attack.

Due to the lack of detailed knowledge about the chip's layout, it remains challenging to fully explain the observed variations of the pulse polarity effects. However, deeper insights could be gained in the future by performing similar campaigns on an ASIC chip, where the underlying architecture and characteristics of the PDN would be well known.

4.3 Threshold Voltage of Faults

Our campaigns reveal that different spots show different maximum values for harmonics, which might suggest different sensitivities. However, to reveal the most sensitive coordinates in the FPGA package for both RO placements, we conducted other tests



XY	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												
Y=1										440	450	
Y=2										370	340	
Y=3								360	350	360	290	
Y=4							430	310	360	390	310	
Y=5							450	410			440	
Y=6								450				
Y=7												
Y=8						320	370					
Y=9					430	180	200	260				
Y=10					270	150	150	150	170			
Y=11					210	150	150	150	150			

XY	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												
Y=1												
Y=2												
Y=3								370	380			
Y=4							430	340	360			
Y=5							450	370				
Y=6								450				
Y=7						450						
Y=8						320	370					
Y=9					430	180	200	260				
Y=10					270	150	150	150	170			
Y=11					210	150	150	150	150			

XY	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												
Y=1												
Y=2							350					
Y=3						450	290					
Y=4						450	280	450				
Y=5							330	450				
Y=6							450					
Y=7												430
Y=8												250
Y=9											340	190
Y=10											340	180
Y=11											340	160

XY	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												
Y=1												
Y=2												
Y=3												
Y=4												
Y=5												
Y=6												
Y=7							410			340		340
Y=8							420				390	390
Y=9						380	330				180	190
Y=10						360	290				190	180
Y=11						360	290				200	170

Fig. 8. Voltage threshold of faults for RO1 and RO2 under positive and negative polarities

using both pulse polarities while increasing the voltage amplitude from 150V to 500V by steps of 10V with the PW fixed at 80ns. The same methodology in Section 3.3 was followed to obtain the minimum voltage amplitude required to induce the harmonic or bitstream corruption faults in Fig. 7 and Fig. 6. A specific color was assigned for each scenario:

- **White box**: represents a coordinate where no faults were induced after sweeping the whole range of amplitudes.
- **Grey box**: shows the minimum voltage amplitude to induce a bitstream corruption.
- **Gradient Green to Red box:** shows the minimum voltage amplitude to induce the harmonic error with 500 representing the lowest sensitivity and 150 being the highest one.

The results shown in Fig. 8 demonstrate distinct fault patterns and threshold differences between the two ROs under different polarities of the pulse. However, we notice that 450V was the minimum voltage amplitude in our setup that could reveal all the fault locations on the FPGA package regardless of the RO placement and the chosen pulse polarity. Furthermore, it seems that RO1 is more prone to harmonic errors at lower voltages when subjected to positive polarity while RO2 is highly sensitive when exposed to negative polarity.

Looking more carefully at the threshold voltage maps, we notice clear hotspots where the circuit is most vulnerable such as X10Y3 for the RO1 placement when targeted by a positive pulse and X6Y4 when targeted by a negative pulse. These core weak points are particularly important because they represent efficient attack vectors. An attack targeting these specific coordinates would require less energy to succeed; therefore, designers can leverage this insight to enhance the efficiency of their countermeasure designs and strategies.

4.4 Injection Timing Effect

In the previous tests published in [10], each performed injection induced the pulse at a different moment during the low or high level of the clock to enable injections randomly spanning over the oscillation period. However, to reveal the impact of the injection timing on faults, a state machine using UART communication was implemented to control the RO oscillations and trigger a delayed EM pulse injection. When the RO oscillations are enabled, the FPGA outputs a trigger signal forcing the ChipShouter to precisely inject an EM pulse at the 10^{th} oscillation with a delay of 35ns, 610ns or 1000ns with respect to the rising edge of the oscillation. It should be noted that this delay is set with respect to the start signal that enables oscillations at the beginning of the ring, but the actual phase between the EM pulse and the ring oscillations strongly depends also on the probe position over the ring, i.e. within the sequence of inverters.

Fig. 9 depicts the fault sensitivity maps of the RO2 when targeted by a negative pulse of 450V and PW = 80ns to compare between random injections shown in the top left of Fig. 9 and the three scenarios of delayed injections. As a reminder, the original frequency of the ring in this position is 925 kHz corresponding to a period of 1081ns.

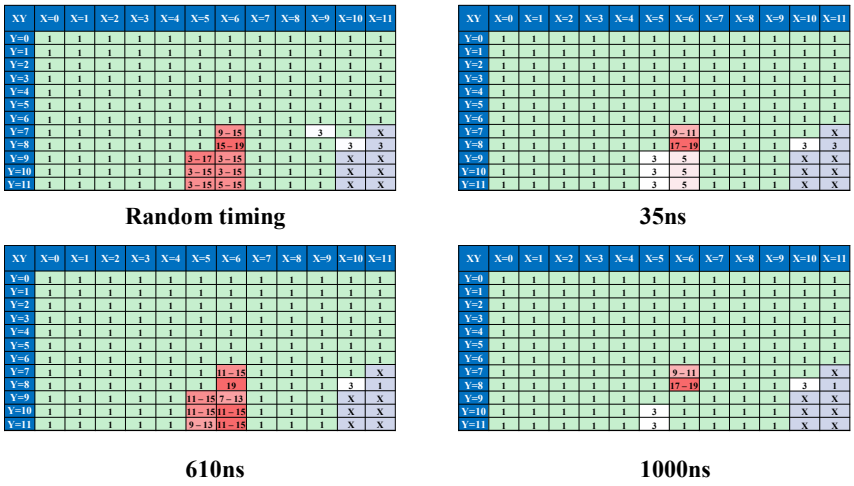


Fig. 9. Injection timing impact on RO2

From the figure, we observe that by selecting a specific timing of the injection, we can change the vulnerability of the RO2 by either suppressing the harmonic response or narrowing down the range of the harmonic errors, as it is the case for the X5Y9 and X6Y9 coordinates for instance. The revealed fault locations for each specific delay (35ns, 610ns and 1000ns) represent subsets of those obtained with a randomized timing. Therefore, we can deduce that tuning the injection timing parameter can be very efficient in controlling the outcome of an EMFI attack. This can be potentially leveraged, for example, to bias the response of Physical Unclonable Functions (PUFs) in FPGAs.

For a deeper understanding of the timing effect, further tests with finer steps may be conducted in future work for specific vulnerable locations.

4.5 Pulse Width and Amplitude Effect

To highlight the impact of the PW on harmonic errors, we focused on the X10Y5 coordinate and we conducted tests on RO1 with a single pulse of 450V while varying the PW from 60ns to 140ns by steps of 20ns due to the limitation of the pulse generator. Ten tests were performed for each PW value to characterize how it influences the range of the harmonic response.

As shown in Table 2, 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 80ns is the minimum PW that can lead to harmonic errors. Moreover, the harmonic window increased from (11-17) for PW=80ns to (13-19) for PW=100ns and finally to the 19th harmonic for PW=120ns and PW=140ns with a 100% probability during all 10 tests. This confirms the fact that harmonic errors can be induced only if enough energy is delivered through the EM pulse.

To explore if the pulse amplitude can also have a similar impact on the harmonic vulnerability of the RO as the pulse width, we conducted other tests on RO1 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 performing pulses with amplitudes ranging from 150V to 430V, no harmonic response was induced, therefore Fig. 10 shows the results obtained for 10 tests with a limited range of significant amplitudes (430V – 500V). As illustrated in Fig. 10, increasing the voltage amplitude of the pulse did not necessarily lead to inducing higher harmonics but rather increased the probability of obtaining higher harmonics. The range of harmonic errors remained at (11-17) throughout the entire campaign with random injection timing.

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

Table 2. Pulse width impact on harmonics intensity of RO1 under a 450V pulse targeting the X10Y5 coordinate

	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**

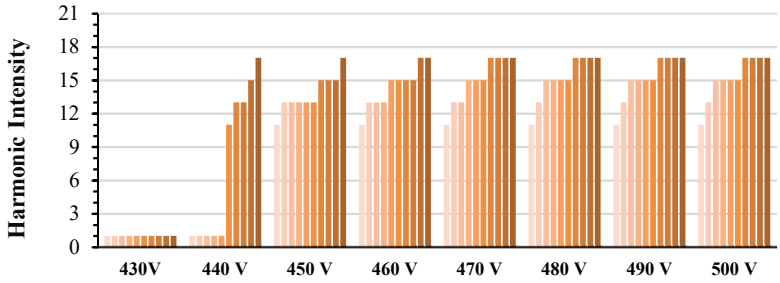


Fig. 10. Pulse amplitude impact on harmonics occurrence (RO1 - PW = 80ns - X10Y5)

respectively. As the amplitude increases further 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 certain voltage and PW threshold must be applied to induce harmonic errors or bitstream corruptions. Furthermore, forcing higher harmonics with higher probabilities could only be achieved in particular locations in the FPGA by increasing the width and the amplitude of the pulse. This is likely related to the structure of the underlying FPGA fabric; however, the precise details of the layout are unknown, and further information could be deduced by attacking a dedicated ASIC chip.

4.6 Process Variation Effect

To explore the potential impact of manufacturing and experimental variations, we performed similar tests to the ones conducted in Section 4.1 on two other identical Nexys-A7 boards both programmed with the same previous RO1 and RO2 bitstreams.

Table 3 shows the impact of process variation on the frequency of the two ROs. The obtained cartographies of RO1 and RO2 targeted with a positive pulse of 450V and 80ns for the three FPGAs are shown in Fig. 11. Comparing Fig. 11(a) with Fig. 11(b)

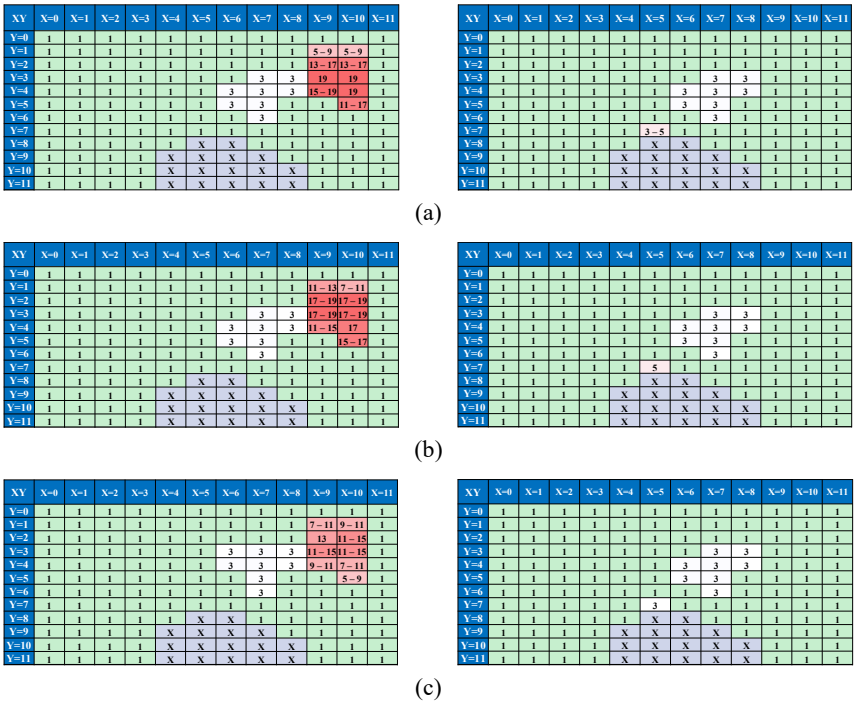


Fig. 11. Fault sensitivity maps of RO1 on the left and RO2 on the right for (a) 1st Nexys-A7 board (b) 2nd Nexys-A7 board (c) 3rd Nexys-A7 board

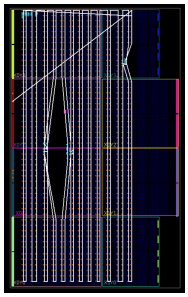
Table 3. Process variation effect on the RO1 and RO2 frequencies

Board	RO1 Frequency (kHz)	RO2 Frequency (kHz)
1	927	925
2	905	918
3	969	970

and Fig. 11(c) shows that potential differences resulting from the manufacturing process variations do not affect the fault distribution of the ROs under EMFI. However, if we focus on the intensity of harmonics, we can observe that the third board was the least sensitive. This can be due to the higher frequency characterizing both RO1 and RO2 in this FPGA, which poses stricter constraints on SET injections as described in Section 2.2.

4.7 FPGA Packaging Effect

After showing that process variations do not lead to significant differences in the experimental results of fault distribution between the three FPGAs, we aimed to highlight the impact of FPGA packaging on the fault sensitivity of the RO. To this end, we chose to target the Artix-7 FPGA embedded in the CW305 Chipwhisperer board because it



(a)

XY	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	9 – 11	9 – 11	1
Y=2	1	1	1	1	1	3	1	1	1	X	X	1
Y=3	1	1	1	1	1	3	3	1	1	13	5 – 9	1
Y=4	1	1	1	1	1	1	1	1	1	21 – 27	9 – 21	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	17 – 21	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	X=0	X=1	X=2	X=3	X=4	X=5	X=6	X=7	X=8	X=9	X=10	X=11	X=12	X=13
Y=0	1	1	1	1	1	1	1	3	3 – 5	1	1	1	1	1
Y=1	1	1	1	1	1	1	1	X	3	1	3 – 7	5 – 11	1	1
Y=2	1	1	1	1	1	3	3 – 5	1	1	3 – 9	5 – 7	X	X	1
Y=3	1	1	1	1	1	3	3 – 7	3	1	1	3 – 11	X	X	1
Y=4	1	1	1	1	1	1	5 – 13	3 – 7	3	1	1	X	X	1
Y=5	1	1	1	1	1	1	1	3	1	1	1	X	X	1
Y=6	1	1	1	1	1	1	3	3 – 7	X	1	X	X	X	1
Y=7	1	1	1	1	1	X	X	X	X	X	X	X	X	1
Y=8	1	1	1	X	X	X	X	X	X	X	X	X	1	1
Y=9	1	1	1	X	X	X	X	X	X	X	X	X	X	1
Y=10	1	1	1	X	X	X	X	X	X	1	X	X	X	1
Y=11	1	1	1	X	X	X	X	X	X	X	1	X	1	1
Y=12	1	1	1	X	X	X	X	X	X	1	X	1	1	1
Y=13	1	1	1	X	X	X	X	X	X	1	X	1	1	1

(c)

Fig. 12. (a) FPGA floorplan showing the RO layout in both FPGAs (b) Nexys-A7 cartography (c) CW305 cartography

has the same structure and number of logic cells as the one embedded in Nexys-A7 (7A100T). However, their main difference is that CW305 (17mm × 17mm) has a wire-bond fine-pitch packaging with 256 pins and a higher speed grade compared to Nexys-A7 (15mm × 15mm) that uses a wire-bond chip-scale technology with 324 pins [33].

In this test, the implementation of our RO consisted of placing the 1200 LUTs across the whole FPGA instead of constraining their placement into one clock region as shown in Fig. 12(a). We adopted this new configuration because other experiments from [30] and [31] revealed that making the RO layout less compact with vertical short connections is optimal for a higher number of impacted locations and harmonics. Therefore, after programming the two FPGAs each with its dedicated bitstream file, the RO was originally running at 850 kHz in Nexys-A7 and at 897 kHz in CW305. This difference mainly stems from the higher speed grade of the CW305 FPGA compared to the other board, which eventually influences the frequency of the ring.

Fig. 12(b) and Fig. 12(c) represent the fault sensitivity maps of both FPGAs targeted with a positive pulse of 450V and PW = 80ns. They demonstrate that changing the FPGA packaging within the same process technology can effectively influence the coupling strength within the FPGA, which in turn affects the intensity and the location of faults. The maximum impact was achieved in the FPGA package within Nexys-A7 with a harmonic error of 27, twice larger than the impact on CW305. However, keeping in mind that they have a similar die size but different package sizes, we can state that the overall fault susceptibility is higher for the wire-bond fine-pitch packaging compared to the wire-bond chip-scale as the CW305 cartography displays more sensitive spots of both harmonic errors and bitstream corruptions. On the other hand, we underline a similar trend of the fault distribution between both FPGA packages regarding the harmonic error distribution.

With the impact of packaging being established, further experiments could be conducted in order to validate these results for other packaging technologies and FPGA families.

5 Conclusion

In this paper, we presented the harmonic locking phenomenon occurring in ring oscillators under different parameters of a single EM pulsed fault injection. The study covers an extended set of parameters compared to our previous work, where the pulsed EMFI vulnerability of two ROs implemented with the same number of stages in an Artix7 FPGA (28nm) was only characterized as a function of the RO placement in the FPGA chip, the probe position and the EM pulse width and amplitude. This work analyses the impact of the pulse polarity on the distribution and magnitude of faults across different RO placements. It also provides the threshold voltage for induced faults with both positive and negative pulse polarities, highlighting the different fault susceptibility of the power and ground networks within an FPGA. Additionally, our findings show how the control over the timing of pulse injection can extend or reduce the range of induced faults, which is critical for RO-based PUF implementations. Finally, further tests analyzing the effects of process variation and FPGA packaging technology on the RO's

harmonic response emphasize the paramount importance of testing across multiple FPGA versions even under a similar manufacturing technology. All these parameters have a noticeable impact on the evaluation and protection efficiency against EMFI attacks.

Considering all the presented experimental results, a key question that emerges is how can we potentially leverage the findings to guide the protection methodologies against the EMFI attack? This will be addressed in future works to investigate the placement and routing strategies tailored to the intended use of ROs; either as components of a detection mechanism or a standalone security primitive. Our future work will also aim at leveraging our current results to evaluate the effectiveness of a RO-based EMFI detector to protect a hardware implementation of a cryptographic algorithm or a RO-based-PUF in several FPGA platforms or dedicated ASIC chips.

Declarations

Funding This work is partially 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, by the Cybersecurity Institute of Grenoble Alpes (ANR-15-IDEX-02) and by the Chips JU European Project: 101112282 — Resilient Trust.

Conflicts of Interests The authors have no competing interests to declare that are relevant to the content of this article.

Data Availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

1. B. Colombier, A. Menu, J.-M. Dutertre, P.-A. Moëllic, J.-B. Rigaud and J.-L. Danger, "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller", in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, USA, 2019, pp. 1-10, https://doi.org/10.1109/HST.2019.8741030
2. N.-E. O. Tebina *et al*., "Non-Invasive Attack on Ring Oscillator-Based PUFs Through Localized X-Ray Irradiation", in *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Tysons Corner, VA, USA, 2024, pp. 01-11, https://doi.org/10.1109/HOST55342.2024.10545397
3. F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson et P. Maurine. "Local and direct EM injection of power into CMOS integrated circuits", in Proceedings of the International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). Nara, Japan, 2011, p. 100-104, https://doi.org/10.1109/FDTC.2011.18
4. L. Zussa, J.-M. Dutertre, J. Clediere and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter", in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Arlington, VA, USA, 2014, pp. 130-135, https://doi.org/10.1109/HST.2014.6855583

5. T. Korak, M. Hutter, B. Ege, and L. Batina, “Clock glitch attacks in the presence of heating”, in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Busan, Korea (South), 2014, pp. 104-114, https://doi.org/10.1109/FDTC.2014.20
6. C. Shepherd et al., “Physicals fault injection and side-channel attacks on mobile devices: A comprehensive analysis”, in Computers & Security, vol. 111, p. 102471, Dec. 2021. https://doi.org/10.1016/j.cose.2021.102471
7. O'Flynn, Colin. “PicoEMP: A Low-Cost EMFI Platform Compared to BBI and Voltage Fault Injection using TDC & External VCC Measurements”, in *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, Prague, Czech Republic, 2023, pp. 60-71, https://doi.org/10.1109/FDTC60478.2023.00015
8. J. Breier and X. Hou, “How Practical Are Fault Injection Attacks, Really?”, in *IEEE Access*, vol. 10, pp. 113122–113130, 2022, https://doi.org/10.1109/ACCESS.2022.3217212
9. A. Beckers, S. Guilley, P. Maurine, C. O'Flynn and S. Picek, “(Adversarial) Electromagnetic Disturbance in the Industry”, in *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 414-422, 1 Feb. 2023, https://doi.org/10.1109/TC.2022.3224373
10. S. E. Amraoui, A. Douadi, R. Leveugle, and P. Maistri, “Harmonic Response of Ring Oscillators under Single ElectroMagnetic Pulsed Fault Injection”, in *2024 IEEE 25th Latin American Test Symposium (LATS)*, Maceio, Brazil, 2024, pp. 1-6, https://doi.org/10.1109/LATS62223.2024.10534602
11. 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.
12. P. Bayon et al., “Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator”, in: Schindler, W., Huss, S.A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2012. Lecture Notes in Computer Science, vol 7275. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29912-4_12
13. F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx and P. Maurine, “Local and Direct EM Injection of Power Into CMOS Integrated Circuits”, in *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Nara, Japan, 2011, pp. 100-104, https://doi.org/10.1109/FDTC.2011.18
14. J. Toulemont et al., “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)*, Toulon, France, 2021, pp. 1-4, https://doi.org/10.1109/NEWCAS50681.2021.9462763
15. A. Beckers et al., “Design considerations for EM pulse fault injection”, in Belaïd, S., Güneysu, T. (eds) Smart Card Research and Advanced Applications. CARDIS 2019. Lecture Notes in Computer Science(), vol 11833. Springer, Cham, https://doi.org/10.1007/978-3-030-42068-0_11
16. J. Toulemont, G. Chancel, J. M. Galliere, F. Mailly, P. Nouet, and P. Maurine, “On the scaling of EMFI probes”, in *2021 Workshop on Fault Detection and Tolerance in Cryptography*, IEEE, Sep. 2021, pp. 67–73, https://doi.org/10.1109/FDTC53659.2021.00019
17. A. Dehbaoui, J. Dutertre, B. Robisson, A. Tria, “Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES”, in *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Leuven, Belgium, 2012, pp. 7-15, https://doi.org/10.1109/FDTC.2012.15
18. 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*, Barcelona, Spain, 2019, pp. 398-403, https://doi.org/10.1109/EMCEurope.2019.8871909

19. M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, P. Schaumont, “Inducing Local Timing Fault Through EM Injection”, In 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC). IEEE Press, 1–6, https://doi.org/10.1109/DAC.2018.8465836
20. S. Ordas, L. Guillaume-Sage, P. Maurine, “Electromagnetic fault injection: the curse of flip-flops”, in Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 183–197, 2017, https://doi.org/10.1007/s13389-016-0128-3
21. M. Dumont, M. Lisart, P. Maurine, “Modeling and simulating electromagnetic fault injection”, in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 4, pp. 680-693, April 2021, https://doi.org/10.1109/TCAD.2020.3003287
22. R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger and L. Sauvage, “A Tale of Two Models: Discussing the Timing and Sampling EM Fault Injection Models”, in *2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC),* Prague, Czech Republic, 2023, pp. 1-12, https://doi.org/10.1109/FDTC60478.2023.00010
23. D. El-Baze, J.-B. Rigaud, and P. Maurine, “A fully-digital em pulse detector”, in 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 2016, pp. 439–444.
24. Z. Zhang, S. Yang, and T. Su, “The behavior of frequency locking of ring oscillators with RF interference on the supply”, in *Microelectronics J*, vol. 116, p. 105247, Oct. 2021, https://doi.org/10.1016/j.mejo.2021.105247
25. U. Mureddu, N. Bochard, L. Bossuet and V. Fischer, “Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices”, in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 7, pp. 2560-2571, July 2019, https://doi.org/10.1109/TCSI.2019.2900017
26. S. Osuka *et al.*, “EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage”, in *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1122-1128, Aug. 2019, https://doi.org/10.1109/TEMC.2018.2844027
27. Chen, Y. P. et al, “Single-event transient induced harmonic errors in digitally controlled ring oscillators”, in *IEEE Transactions on Nuclear Science*, vol. 61, no. 6, pp. 3163-3170, Dec. 2014, https://doi.org/10.1109/TNS.2014.2364813
28. 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),* Huntsville, AL, USA, 2023, pp. 1-7, https://doi.org/10.1109/PAINE58317.2023.10317982
29. M. Paquette, B. Marquis, R. Bainbridge, and J. Chapman, “Visualizing Electromagnetic Fault Injection with Timing Sensors”, in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, Washington, DC, USA, 2021, pp. 1-8, https://doi.org/10.1109/PAINE54418.2021.9707696
30. S. E. 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, https://doi.org/10.1109/DDECS60919.2024.10508906
31. S. E. Amraoui, R. Leveugle and P. Maistri, "Capture the Pulse: Impact of FPGA Resource Utilization on EM Fault Injection Attacks Detection," *2024 IFIP/IEEE 32nd International Conference on Very Large Scale Integration (VLSI-SoC)*, Tanger, Morocco, 2024, pp. 1-6, doi: 10.1109/VLSI-SoC62099.2024.10767826.
32. O. Trabelsi, L. Sauvage and J.-L. Danger, “Characterization at Logical Level of Magnetic Injection Probes”, in 2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility

(EMC Sapporo/APEMC), Sapporo, Japan, 2019, pp. 625-628, https://doi.org/10.23919/EMCTokyo.2019.8893692
33. AMD, “7 Series FPGAs Data Sheet: Overview”. Available: https://docs.amd.com/v/u/en-US/ds180_7Series_Overview
34. 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, https://doi.org/10.5220/0012431800003648
35. N. Selmane, S. Guilley and J.-L. Danger, "Practical Setup Time Violation Attacks on AES," *2008 Seventh European Dependable Computing Conference*, Kaunas, Lithuania, 2008, pp. 91-96, doi: 10.1109/EDCC-7.2008.11