Non-Invasive Attack on Ring Oscillator-based PUFs through Localized X-Ray Irradiation

Nasr-Eddine Ouldei Tebina, Aghiles Douadi, Luc Salvo, Vincent Beroulle, Nacer-Eddine Zergainoh, Guillaume Hubert, Ioana Vatajelu, Giorgio Di Natale, Paolo Maistri

Non-Invasive Attack on Ring Oscillator-based PUFs through Localized X-Ray Irradiation

Nasr-eddine Ouldei Tebina[1], Aghiles Douadi[1], Luc Salvo[2], Vincent Beroulle[3], Nacer-Eddine Zergainoh[1], Guillaume Hubert[4], Ioana Vatajelu[1], Giorgio Di Natale[1], and Paolo Maistri[1]

[1]Univ Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000 Grenoble, France
[2]Univ Grenoble Alpes, CNRS, Grenoble INP*, SIMaP, 38000 Grenoble, France
[3]Univ. Grenoble Alpes, Grenoble INP*, LCIS, 26000 Valence, France
[4]ONERA DPHY, University of Toulouse, 31055 Toulouse, France

***Abstract*—Physical Unclonable Functions (PUFs) are emerging as a fundamental component of secure architectures that provide services such as authentication and key generation. A specific class of PUF is based on Ring Oscillators (ROs), where minimal behavioral differences due to process variations are harnessed to generate unique responses. The inherent strength of PUFs lies in the fact that it is practically impossible to control these phenomena to forge a specific response from the device. In this paper, we present a novel approach by introducing localized X-Ray attacks on PUFs for the first time. These attacks significantly alter the behavior of a selected RO within the array of oscillators on an FPGA. By biasing the properties of the target block, we demonstrate the feasibility of modifying the response of a specific PUF. In particular, these attacks can be executed when the target is powered off, bypassing several circuit monitoring countermeasures. This capability introduces a new class of attacks that exploit vulnerabilities even in systems with stringent security measures, raising concerns about the robustness of current security frameworks.**

***Index Terms*—PUF, Ring Oscillators, X-Ray, Biasing, Cloning**

I. Introduction

Smart devices are pervasive in current society. The number of devices equipped with integrated circuits and capable of some data processing is constantly increasing [1]. At the same time, the amount and type of information stored and elaborated is steadily broadening, and the most sensitive information needs to be protected against unauthorized access. In general, this can be achieved through cryptographic algorithms and protocols, implemented either in hardware or as embedded software running on CPUs and/or microcontrollers.

In all these scenarios, Physical Unclonable Functions (PUFs) are emerging as a great opportunity to solve one of the major challenges in secure devices, that is, secure and reliable on-chip key generation [2], in order to avoid device cloning or counterfeiting among other threats. PUFs can generate unique values, such as authentication keys, on demand: they exploit the natural variability resulting from fabrication [3], and therefore it is almost impossible to predict or clone the value of the generated key. The generation mechanism is based on a challenge-response protocol: The device is queried by the user with a specific value (Challenge), which is used to create and send back the Response; the set of all these pairs (Challenge-Response Pairs – CRPs) defines the PUF. Several types of PUFs have been proposed in the literature: a complete overview is beyond the scope of this paper. In this work, we will focus mainly on ring oscillator PUFs (RO-PUFs), which exploit random variations of propagation and switching delays in integrated circuits.

A large class of attacks on PUFs is based on modeling and reproducing CRPs without actually going into the lower-level details of how the PUF generates its responses [4] [5]. To respond to these threats, controlled PUF [6] or CRP obfuscation [7] is required to make modeling unfeasible. Nevertheless, PUFs remain dependent on their environment and may therefore be vulnerable to external perturbations, such as changes in temperature or power supply. In order to provide consistent and reliable key extraction even in the presence of these variations or errors in the raw PUF responses, fuzzy extractors can be used [8]. However, these elements are based on the assumption that the errors in PUF responses are random and uniformly distributed. These techniques, in fact, affect the device in its entirety and hence most, if not all, CRPs at the same time. If an attacker can manipulate the errors systematically, it can compromise the security of the system.

More localized attacks, such as Laser Fault Injection [9], can be used to alter the CRPs but require complex preparation of the device (e.g., depackaging and layer removal), and the attack has to be performed when the device is powered on (which may trigger onboard countermeasures). An alternative approach has been presented in [10], where a custom bitstream intentionally creates localized short-circuits in the programmable logic, locally producing heat that increases the temperature in correspondence with the targeted ROs. This heat-induced accelerated aging affects the electrical characteristics of certain ROs with respect to others, allowing the attacker to potentially clone the device on another FPGA. However, note that this approach requires reprogramming the device three times: first the original design for the characterization, then the attack bitstream, and finally the original one again for the attack.

Recently, a novel approach to physical attacks in secure

*Institute of Engineering Univ. Grenoble Alpes

circuits has been identified in X-Rays [11]. Although ionizing radiations are well known and have been thoroughly studied to understand how integrated systems may behave in harsh environments [12], their use to attack secure implementations is still in an early stage. In [11], the authors have demonstrated that a nanofocused X-ray beam (available in a synchrotron facility) could target single transistors in the target device and induce a semi-permanent fault, recoverable by thermal annealing. Subsequently, similar results were obtained with a more affordable laboratory X-ray source [13], with the trade-off of more limited precision in the position and occurrence of the fault. Very recently, a laboratory source has been used to investigate fault injection on a powered off microcontroller [14], highlighting a bit-set fault model when targeting the device memory. However, until now, ionizing radiation has been used mostly as a fault injection technique.

In this paper, we propose to leverage the capability of X-Rays to modify the electrical behavior of the targeted gates. We show that, through a positioning and masking protocol similar to [13], we are able to target a specific Ring-Oscillator among those implemented on our target programmable board, and heavily modify its delay properties. As a consequence, the answers from the attacked PUF are altered when the biased RO is selected. We show and quantify the effects of several dosing sessions both when the device is running, when it is in idle state (i.e., powered on but non oscillating), and when attacked during power off state. We highlight the significant behavioral changes in these scenarios, which constitute a serious threat to the security of ring oscillator structures.

The rest of this paper is structured as follows. In the next section, we present the necessary background on ring oscillators and the effects of ionizing radiations on integrated circuits; we also describe a few monitoring structures that can be used as attack detectors in secure circuits and could be biased by our approach. Section III presents our threat model and potential attack scenarios. In Section IV, we describe the simulation model that introduces the physical phenomena that will be exploited in this work. In Section V and VI we present our experimental setup and the results of our campaigns, which are then further analyzed in Section VII. Finally, Section VIII concludes the paper.

II. Background

In this section, the necessary background is given. We will briefly describe ring oscillators, which are the main primitives used as a target in this work; then, we recall the basic physics concerning the circuit absorption of Total Ionizing Dosing radiations (TID). Finally, we will describe a few monitoring structures that can be used as security countermeasures and that can be biased by X-Ray irradiation.

A. PUFs & Ring-Oscillators

With the increase in attacks related to software or hardware, finding a cost-effective and efficient solution to protect circuits and devices has become imperative. Physical Unclonable Functions (PUFs) have emerged as reliable and affordable solutions to build trusted systems [2], [15]. The primary advantage of PUFs is that they operate only when the circuit is powered, thus avoiding the need to store keys in easily compromised memories. In addition, integration into chips is easy and simple, as they use relatively straightforward designs.

Physical Unclonable Functions exploit the natural variability that occurs during the fabrication process to generate a unique key for each electronic component [16]. In fact, during the manufacturing of semiconductors, which form the basis of the majority current circuits, small defects and unintentional imperfections arise, rendering each chip unique. PUFs use these imperfections to generate device-dependent outputs (*Responses*) from user-provided inputs (*Challenges*) and thus identify each component, eliminating any risk of cloning or duplication. However, despite the reliability and affordability of PUFs, they remain sensitive to various environmental factors, such as high temperatures, fluctuations in supply voltage, and natural circuit aging.

Several metrics have been proposed to evaluate PUFs, ensure long-term reliability and increased resistance to different attacks or changes in environmental conditions, thus guaranteeing overall reliability over time [17]. Among these metrics, we have notably the following:

- Reliability: The PUF response needs to be consistently stable over time and under various usage conditions. In essence, when the experiment is conducted multiple times, the response should remain consistent.
- Uniqueness: This property refers to a PUF's ability to differentiate a particular device from a population of devices in a distinctive manner. To assess uniqueness, each device undergoes an initial analysis and a reference sample is obtained. When a new device is introduced into the system, it is compared to every existing device by computing the Hamming distance between their respective reference samples.
- Uniformity: It evaluates the distribution of responses across all instances of a PUF, as reflected in the arrangement of '0's and '1's within the response bits. A uniform distribution of responses is desirable because it ensures that the PUF is equally resilient to attacks, regardless of the particular PUF instance under consideration. The ideal value of uniformity is 50%.
- Bit-aliasing: It refers to the presence of systematic biases in the distribution of binary digits (1s and 0s) in the output of a PUF. Unlike uniformity, bit-aliasing is assessed on a per-challenge basis.

Various types of non-clonable physical functions exist, including Arbiter PUFs, Ring Oscillator-based PUFs, and SRAM-based PUFs [18] [19]. Ring oscillators are particularly studied in the literature [20] due to their straightforward implementation and high performance.

In a PUF based on Ring Oscillators, pairs of rings are selected through the challenge values and their frequencies are compared, as shown in Fig. 1. Due to the variability inherent in the fabrication process, the frequencies of the ring oscillators differ, resulting in a unique response for each device. In this

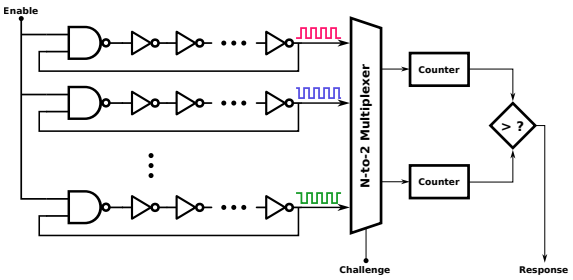


Fig. 1: Ring oscillator PUF

paper, we chose to work with a PUF based on a ring oscillator due to its ease of implementation, particularly on various types of FPGA, and its low requirement in terms of hardware resources. This approach provides a practical and efficient solution for our study, while offering notable advantages in terms of simplicity and resource efficiency.

In the literature, numerous studies have shed light on the vulnerabilities of this structure to various attacks, especially those based on variations in temperature and power supply voltage, as mentioned above. One of the most significant threats that arises from these vulnerabilities is the potential cloning of these structures. Recently, researchers successfully cloned a Ring Oscillator Physical Unclonable Function (PUF) on an FPGA by exploiting factors such as temperature and aging effects, particularly Positive Bias Temperature Instability (PBTI) [10]. Indeed, by deliberately creating short-circuits at specific points in the bitstream used for FPGA programming, they intentionally increased the temperature around specific ring oscillators forming the RO-PUF. As a result, the aging process of PTBI was expedited, leading to changes in the frequencies of these ring oscillators. Despite the non-perfect localized distribution of the temperature generated by the short-circuits, they were able to improve the success rate of the attack by keeping the targeted rings in a freezing state (i.e., in power-on mode but without oscillations); on the contrary, nearby ring oscillators were operating normally. This choice was due to the fact that aging effects have been shown to be more pronounced when transistors are frozen (*i.e.*, deactivated) as opposed to when they oscillate, allowing for a certain degree of recovery [21].

B. TID Effects

TID radiations, exemplified by X-rays, exert a notable influence on MOS transistors, particularly impacting the drain current $I_d(V_G)$ [12]. This influence is characterized by three primary shifts in transistor behavior: a change in threshold voltage, an increase in leakage current, and degradation of transconductance. These effects are predominantly attributed to hole trapping within the oxide material.

The hole-trapping process unfolds in multiple stages. Initially, electron-hole pairs are generated within the oxide as a result of pair generation mechanisms, with most pairs recombining swiftly and representing the charge yield. Electrons, being highly mobile, disperse through the positively biased

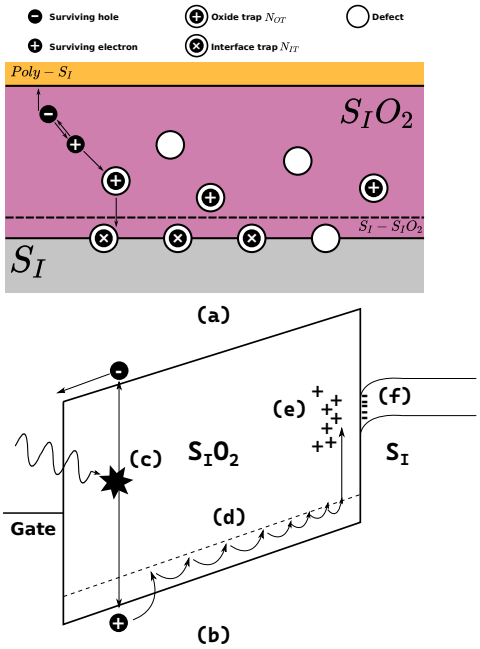
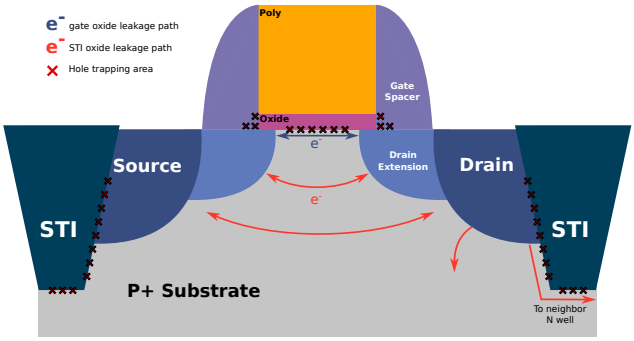


Fig. 2: **(a)** Simplified view of hole-trapping mechanism under ionizing dose. **(b)** Energy band diagram schematic demonstrating different mechanisms in a MOS structure under an ionizing dose **(c)** Pair generation by ionizing radiation **(d)** Transport of positive charge through localised states in oxide bulk **(e)** Hole trapping near S_I/S_IO_2 interface **(f)** Formation of interface traps inducing a threshold shift

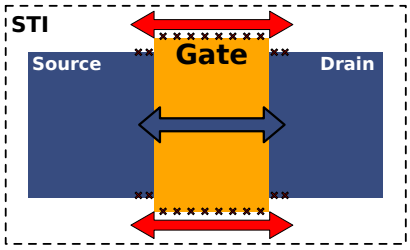
gate, while the remaining holes migrate toward negative potential, getting trapped at defect sites, chiefly oxygen vacancies. Subsequently, interface traps form and their nature hinges on the position of the Fermi level in silicon. These interface traps actively exchange charge carriers with the substrate. The hole trapping process is detailed in Figure 2.

In contemporary transistor technologies, three oxide types are responsible for these effects: gate oxides , gate spacer oxides, and Shallow Trench Isolation (STI) oxides. In older technologies, the primary effect is the threshold voltage shift caused by positive charge traps induced by ionizing radiation in gate oxides. These traps attract negative charge carriers at the canal level, resulting in a decrease in the threshold voltage for N-type MOS and an increase for P-type MOS. Thinner gate oxides exhibit greater resistance to TID-induced effects, as they provide fewer volumes for X-ray absorption and oxide trap generation. However, the continuous scaling of CMOS technology introduces new concerns, particularly with regard to the charges trapped within STI oxides, which contribute to leakage currents in both the intra-component and inter-component pathways [22].

Therefore, in the context of our concerns about X-ray-induced leakage currents, only NMOS is susceptible. Two types of TID-induced leakage current emerge: subthreshold leakage current, originating from a reduction in threshold voltage (gate oxide charge traps), which is static and can occur between the drain and the source at $V_{GS} = 0$. The other component of leakage occurs between the drain and the source through parasitic pathways formed on the walls of the STI. In



(a)



(b)

Fig. 3: (a) Front view of TID effects and TID induced leakage paths. (b) Top view of TID induced main leakage paths

smaller technologies, STI leakage becomes more dominant, as they scale less than the thickness of the gate oxide. Figure 3 illustrates the potential path of parasitic leakage in an NMOS structure.

C. Circuit Monitoring State of the Art

Specific countermeasures against the attack presented in this document have not yet been developed. However, existing general countermeasures against invasive or non-invasive external disturbance injection methods can be found in the literature. For example, in [23], [24], current sensors are deployed to detect any variation in the bulk current. The usage of Timing-to-Digital (TDC) based delay monitors has also been a popular method to monitor any unexpected voltage or timing variations. The key components of TDC based timing monitors are delay lines. They introduce a delay in a reference signal, usually the system clock, and measure the propagation of this delayed signal as a function of its reference signal. It allows the implementation of a fully digital on-chip perturbation sensor with picometric precision; these solutions are used mainly in FPGA applications because of the versatility it provides, such as in [25] or as detailed in [26]. ASIC solutions have also been deployed and have been known for years, as in [27]. These solutions are designed to monitor a certain data propagation path, usually critical paths, and are calibrated accordingly. The calibration phase consists of adjusting the TDC to ensure its accuracy and reliability in measuring time intervals; it involves typically linearity correction ensuring that the output of the TDC is linearly related to the actual time interval being measured, offset correction in order to sample the correct event and a wide variaty of compensation techniques that might affect the TDC accuracy.

The common property of these countermeasure designs is the necessity for an initial state, and the initial state is usually acquired when the circuit is first powered-on. The delay monitors read a delay value and store it; then the concurrent delay value is constantly compared to the stored reference. If a perturbation occurs and the sampled delay changes, alarm signals are raised. Similarly, in current or photon sensors, a calibration phase is required.

In the scope of this paper, Power-off attacks are first introduced, allowing to bypass most monitoring countermeasures on top of being fully non-invasive and reversible.

III. Threat Model

In this section, we present possible scenarios where modifying the behavior of ROs might constitute a serious security threat. We first discuss the use case of PUF cloning (for instance, in the context of counterfeiting); then, we introduce the scenario of cryptanalytical attacks exploiting biased PUF keys.

A. PUF Cloning

PUFs (Physical Unclonable Functions) enable the identification of devices by generating specific keys directly linked to variations in the manufacturing process of the transistors present in each device, as explained in the preceding sections. However, these devices are not immune to physical attacks, particularly those aimed at cloning the device, which represents one of the greatest dangers a device can face.

In the specific case of ring oscillator PUFs, a key is generated by comparing selected random ring oscillators with a challenge, thereby producing a bit as output, either '1' or '0'. These challenge-response pairs are commonly referred to as CRPs (Challenge-Response Pairs).

In an ideal scenario, when the same challenge is applied to two different PUFs (two devices), half of the response bits should be flipped. Hence, it is necessary to calculate the Hamming distance between the chips (Inter-chip Hamming Distance) and ensure that it remains around 50% or close. In a cloning attack, the attacker aims to make a device generate exactly the same responses to identical challenges for two or more different devices.

The complexity of such an attack is the difficulty for the attacker to bias the behavior in a controlled way, both from a qualitative and quantitative point of view. In this work, we present the methodology and quantify the Total Ionizing Dose required to bias the response of a specific ring.

Moreover, it is important to note that perturbation attacks are usually carried out when the circuit is powered on, in order to leverage the electric fields existing in the working circuit. On the other hand, our approach works in the power-off state as well, though with lesser results. This gives the attacker the opportunity to bias the primitives when the embedded countermeasures are not operational and may thus be bypassed. Likely, if a calibration step is required at power-on, this could be altered as well by the received dose.

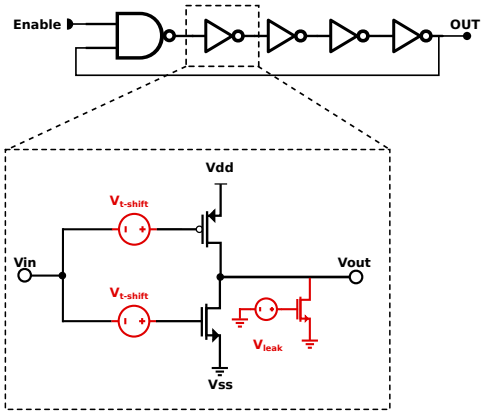


Fig. 4: Electrical model of a ring oscillator under ionizing radiation

B. Cryptanalytical Attacks

A collateral benefit of Physical Unclonable Functions being able to identify a specific instance among a population of devices, is the possibility to be used for key generation. Since PUF's responses can be used to identify and thus authenticate the device, the values can be exploited as initial seeds for a session or private key.

Therefore, the ability to control, even partially, the response value can lead to different scenarios. Biasing the answer of a primitive element can be leveraged from the perspective of bit-set or bit-reset attacks, where the attacker might use differential values to perform differential cryptanalysis that might allow reducing the key search space [28]. Similarly, being able to set part of the response to a known value would allow the attacker to make reasonable guesses on a subset of the key, thus reducing the key search space for other attacks.

IV. Simulation Model of Ring Oscillators under Ionizing Radiations

In this section, the behavior of a single ring oscillator is electrically simulated using the ST65nm technology node; the goal is to qualitatively model the behavior of a ring oscillator under ionizing radiation. This model has been recurrent in the literature, as in [29]. The threshold voltage shift effect can be easily simulated by using its electrical equivalent effect: a DC source can be inserted at the gate terminal of the transistors; an increase of this DC voltage signifies gradually opening the NMOS canal, which corresponds to the lowering of the threshold voltage. For PMOS, in contrast, it means further closing of the canal, which corresponds to an increase in the threshold voltage.

Figure 4 describes the electrical simulation model of a ring oscillator under TID effects. The voltage $V_{t-shift}$ corresponds to the change in threshold voltage: it is the dynamic leakage component of TID-induced leakages. On the other hand, V_{leak} corresponds to the increase in static leakage due to parasitic pathways created on the walls of the STI in an NMOS: it is the component of static leakage induced by TID. Figure 5 shows the simulation results of two ring oscillators, made of 11 and 101 inverters, respectively. The graph shows the average

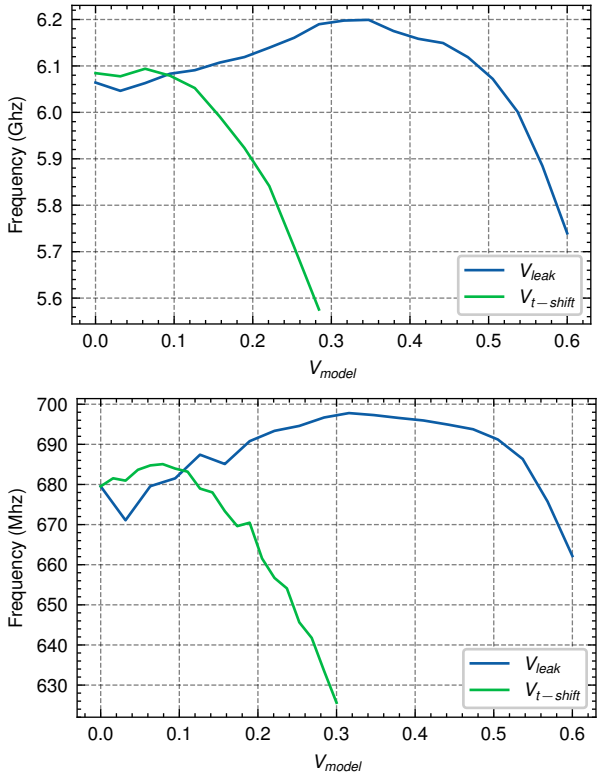


Fig. 5: RO Frequency variation as a function of the simulation leakage parameter (modeled by $V_{t-shift}$ or V_{leak}) for an **11 stage** RO (above) and a **101 stage** RO (below).

oscillation frequency as a function of each leakage component, modeled by $V_{t-shift}$ or V_{leak}. The relationship between the two is not linear since the thickness of the two oxides does not scale in the same manner. In newer technologies, V_{leak} is the most dominant effect, as it is related to STI effects; $V_{t-shift}$ has a minimal impact compared to V_{leak}.

TABLE I: Comparison of the frequency increase after TID effects, for both 11-stage and 101-stage RO

	11-inverter RO	101-inverter RO
$f_0(Ghz)$	6.064	0.6795
f_{MAX}	6.199	0.6977
Δf	+2.23%	+2.68%

The simulation results suggest that, in both leakage components, the oscillation frequency increases (before decreasing). Due to the parasitic leakage paths induced by TID, the N transistors discharge faster, increasing power consumption and switching activity, and thus oscillating at a higher frequency. This increase is less observed in the gate oxide leakage component ($V_{t-shift}$). The component of STI leakage (V_{leak}) has the greatest impact on the increase in the oscillation frequency, as it opens a pathway for the current to discharge faster. This effect persists until a saturation point is reached, and the frequency starts to decrease due to the destruction of the oscillating signal.

It should be noted that increasing the number of inverters used for RO does not lead to more important TID effects on

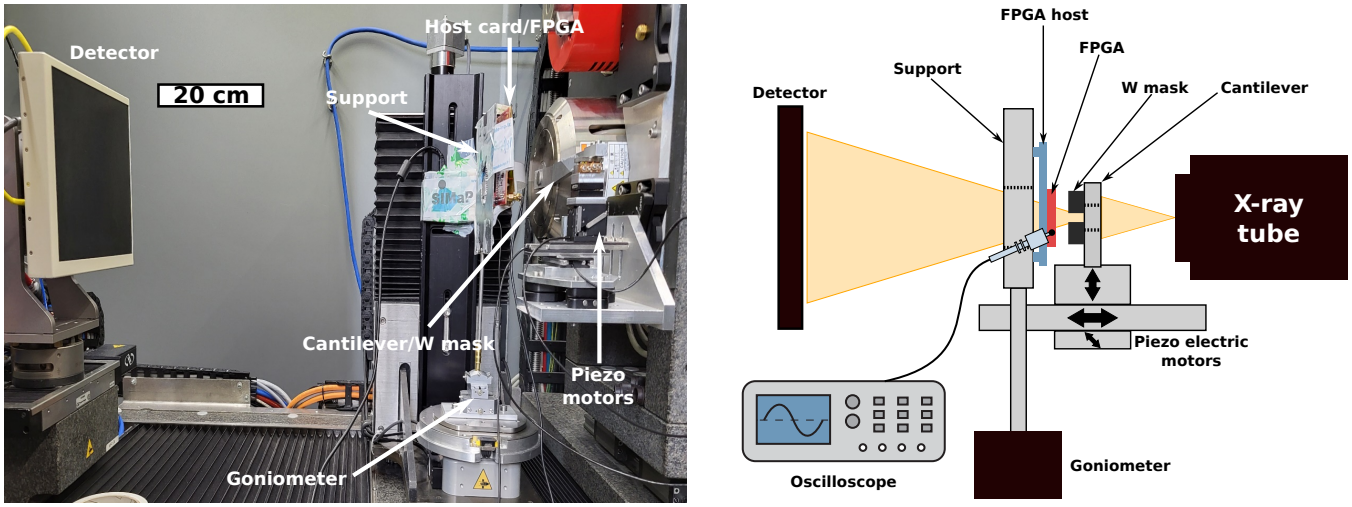


Fig. 6: X-ray irradiation setup which allows for accurate area targeting

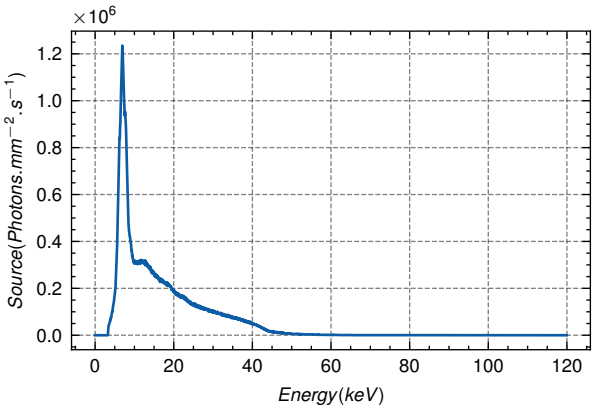


Fig. 7: X-Ray transmitted energy spectrum

the RO; it would be expected that because more cells are being irradiated, the TID effects would be more visible. However, this is not the case: the increase in frequency remains the same and is not dependent on the number of inverters used. Table I compares the simulation results of the initial oscillation frequency of the 11-stage RO and the 101-stage RO with their maximum oscillation frequency reached due to the TID effects of STI.

V. Experimental Setup

A. Irradiation Setup

The laboratory configuration features an EASYTOMXL tomograph produced by RX Solution SAS in Chavanod, France. This setup incorporates a Hamamatsu L10711-03 X-ray source with a Lab6 wire at the cathode and a 1 μm tungsten (W) target on a diamond substrate, coupled with a Varex 2520DX flat panel detector for imaging. Focalization options include small, medium, and large spot modes. Our experiments utilized the large-spot mode at $60kV$ and 50 μA without a filter between the X-ray source and the FPGA component in order to obtain the maximum flux.

In the imaging process, a 16 mm diameter, 2 mm thick tungsten (W) disk with a central 1 mm hole serves as a mask between the FPGA and the source. This mask, fixed to a cantilever, enables precise alignment with the X-ray beam using attocube piezoelectric motors controlled in a closed loop. An additional piezoelectric attocube motor allows for fine tuning of the mask position near the FPGA [30].

The FPGA, located on an electronic card, is shielded along with the entire system, including the X-ray source, by a 1 mm thick lead sheet with a hole in front of the FPGA device. This arrangement ensures optimal system functionality and safety. The complete setup is illustrated in Fig. 6. The X-ray energy spectrum emitted by the laboratory tomograph onto the sample was measured using an Amptek CdTe spectrometer, as shown in Fig. 7. Measurements were made with a pinhole of 100 μm with a current of 10 μA at a distance of 58mm and during 100s, which ensures good statistics on the spectrometer.

B. Target Device and Precise Positioning Setup

The focal point of the irradiation campaign is a Xilinx Spartan-6 in the TQFP package (XC6SLX9-2TQG144C), located on a victim board, specifically the Chipwhisperer CW308T. This assembly is then affixed to the host board CW308, enabling various attack methodologies on various targets. The FPGA is programmable through the JTAG interface using the Xilinx JTAG programmer.

The correct placement of the pinhole on the target area is crucial. Two prerequisites for successful execution are the knowledge of the FPGA chip orientation, and an X-ray image displaying metal bondings around the die area; this way, the die borders can be located non-invasively. A relative reference is placed in the corner of the die, and the pinhole is shifted in the XY plane to the correct position, as illustrated in Figure 8.

To precisely irradiate the target area of the die, we use an identical spare target FPGA chip. X-ray snapshots due to the positioning phase may induce leakage currents throughout the

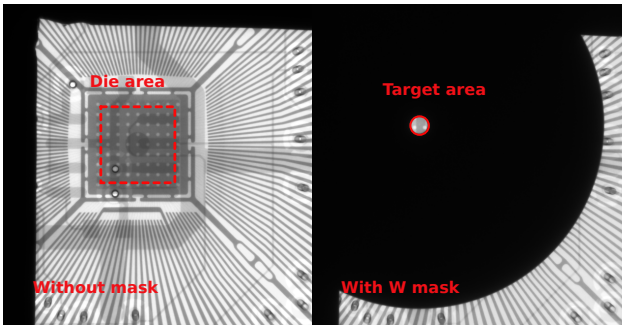


Fig. 8: X-ray snapshot of the Spartan6 chip (On the left) and an X-ray snapshot of a targeted area post W mask positioning (On the right)

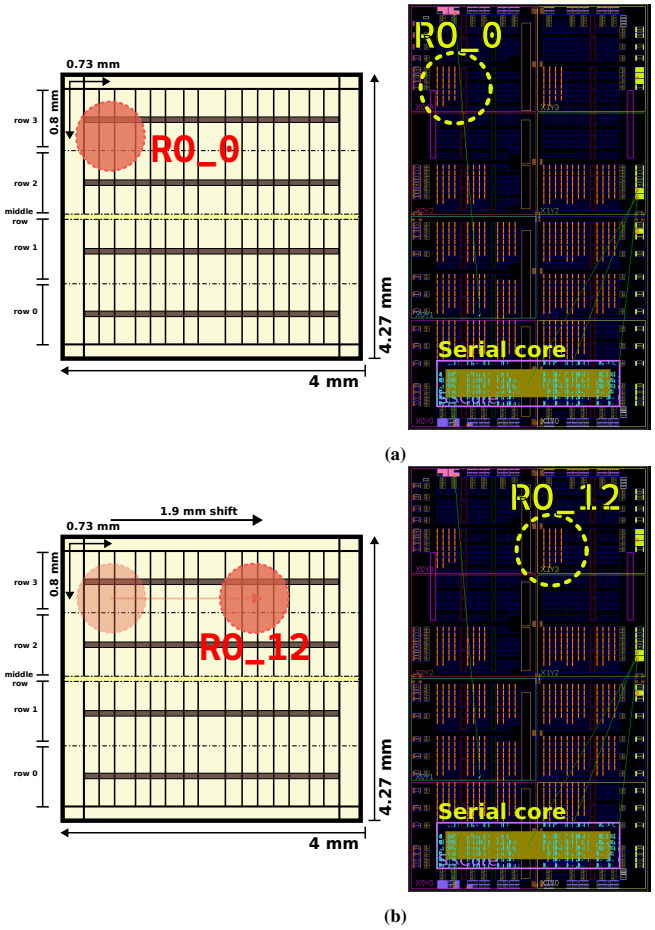


Fig. 9: Upscaled simplified view of the target FPGA die and the targeted area of the pinhole (on the left) and Xilinx Plan-ahead view of the placed cells of each RO (on the right) for both RO targets **(a)** for RO_0 and **(b)** for RO_{12}

entire chip and not just the desired area, compromising experiment accuracy. Consequently, a fresh FPGA chip is swapped in once the mask is securely positioned. This approach confines the leakage current only to the exposed mask area, enabling precise targeting of the desired position on the fresh FPGA.

C. Target RO-PUF Architecture

To accurately identify and highlight the localized effects of the experimental attack, a set of 24 ring oscillators that

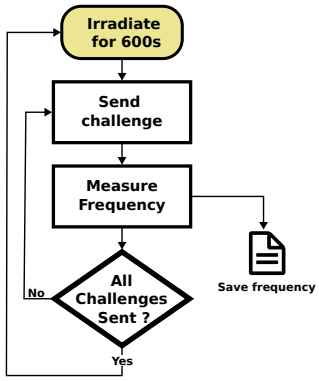


Fig. 10: Frequency measurement automation flow

represent a simple 12-by-12 RO-PUF has been implemented on the Spartan-6 FPGA victim. Each RO consists of 103 inverter stages, in this case, 2-to-1 FPGA LUTs. The number of inverters was chosen arbitrarily to best obtain an easily measurable frequency, and thus quantify the contribution of X-Rays on the frequency as best as possible.

Furthermore, to ensure that the frequency differences among these ring oscillators are exclusively a result of the variability in the transistor process forming the LUTs, rather than internal routing, a Python script has been developed in order to generate deterministic routing constraints (in the Xilinx ISE format) and place the ring oscillators as regularly as possible.

The flow of the experiment consists of targeting two different ROs at two different locations on the chip. The design has been strategically implemented to separate these two target ROs from the others, to better isolate the effects of X-Rays on a single RO. Nevertheless, the other oscillators in the design are active at the same time, emulating the behavior of a real functioning RO-PUF. The target ROs are RO_0, implemented on the top left, and RO_{12}, on the top right, as shown in Fig. 9.

The output of each RO is connected to a 24-to-1 MUX, whose output is connected to an external pin for the frequency measurement. The selection inputs of the MUX are used to provide the module with the challenges (24 in total, corresponding to the number of RO in the design), and hence select a specific RO to measure at the output of the MUX.

A simple serial communication protocol has been implemented in the hardware design in order to use the Python Chipwhisperer API to send challenges. The frequency measurements have been performed using the Picoscope 5000 series, at a sampling rate of 1 GS/s while collecting 50k samples each time. Picoscope Python API has been used to automate the measurement process and to synchronize with the Chipwhisperer scripts that implement the challenge-response exchange. The entire measurement flow is depicted in Figure 10.

The synthesis tools do not provide the real up-to-scale shape of the die; the target region is located on the basis of its relative position. Taking into account the number of rows and columns it occupies and the numbering of these columns and columns, it is possible to estimate the location of the design on the die.

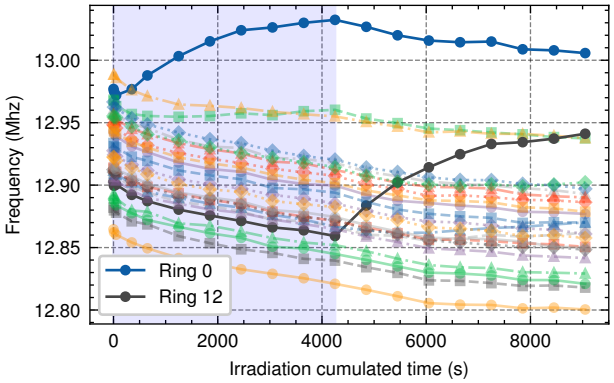


Fig. 11: Evolution of the oscillation frequency of each ring oscillator, during the X-ray irradiation of RO_0 (in light blue section), and RO_{12} (in white section) while **powered ON and oscillating**

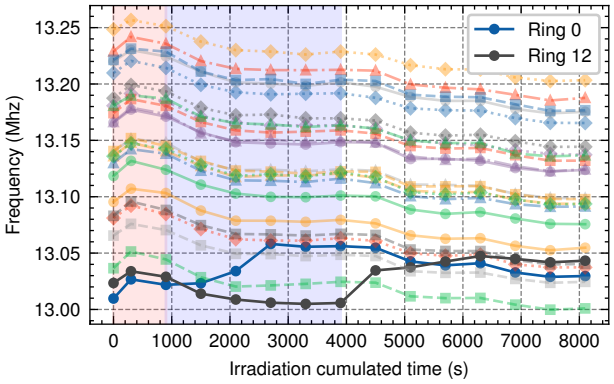


Fig. 12: Evolution of the oscillation frequency of each ring oscillator , during the X-ray irradiation of RO_0 (in light blue section), and RO_{12} (in white section) while **powered OFF completely**, the red section corresponds to the positioning phase inaccuracy

A circular pinhole with diameter of $1mm$ was chosen to best fit the irradiated area. Fig. 9 shows the design of the target area compared to its implementation view on the PlanAhead tool; real measured scale is given as a term for comparison to the relative position in the design tool.

VI. Experimental Results

In this section, we present the experimental results of the irradiation on the two ring oscillators RO_0 and RO_{12}. The setup was designed to perform 600-second irradiation steps each before the frequencies were acquired. Under this configuration, the TID effects were best observable; however, this duration can (and should) be tweaked according to the characteristics of the X-Ray source.

It should be noted that in our experiments, we evaluated two configurations consecutively in order to demonstrate the localized effect. First, RO_0 is irradiated, then the mask is shifted over the next target, which is the RO_{12} area, to start again irradiating. The temporal (X) axis in the figures represents this combined approach, showing the accumulated irradiation time.

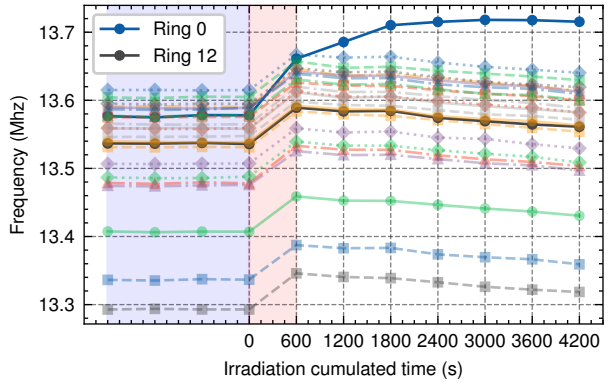


Fig. 13: Evolution of the oscillation frequency of each ring oscillator, during the X-ray irradiation of only RO_0 in the combined red and the white sections while **powered ON and in a frozen state (Not oscillating)**. The red section corresponds to the inaccuracies induced by the hole positioning phase; the blue section corresponds to the pre-radiation phase

In this experimental campaign, three test cases have been evaluated: (1) when the ROs are powered-on and oscillating (the enable signal is asserted); (2) when the ROs are powered-on and are not oscillating (the enable signal is deasserted); and (3) when the ROs are powered off completely. The results of the power-on effects are illustrated in Figure 11, showing the evolution of all ring oscillator frequencies when the ring oscillator RO_0 is targeted for about 4200s; the mask is then shifted to the right and RO_{12} is targeted.

The behavior of the targeted ring oscillators matches the simulation when only static leakage paths are considered, i.e., the STI effects modeled by V_{leak} (see Figure 5) are taken into account. Similarly, in experimental cases, the RO frequency reaches a saturation point, and additional irradiation does not further increase the frequency any more. This indicates that the maximum of $p+$ trapped in transistor oxides is being reached. On the other hand, the other non-targeted ROs witness a steady decrease in their oscillation frequencies, because of the extra power drawn by the irradiated RO (due to the IR drop phenomenon).

Oxides with a thickness of 10 nm or less are known to be almost invulnerable to TID effects, such as gate oxides from technologies of 65 nm or less. It is very difficult to generate electron-hole pairs in such oxides unless highly energetic and focused X-ray beams are used, such as in synchrotron-grade X-ray sources [31], which is considerably more energetic than the source used for this study. Therefore, the effects observed in Figures 11, 12, and 13 are mainly caused by STI related leakage pathways.

Figure 12 describes the frequency evolution of the oscillating frequencies of the RO-PUF after targeting RO_0 and RO_{12}, in the OFF state. The frequency increase saturates at almost the same time, which suggests that the number of electron-hole pairs generated is almost the same. However, the increase in the oscillation frequency is less important than in the case where RO is activated. This suggests that the presence of an electric field affects the trapping position of these holes,

TABLE II: Comparison of the frequency increase after TID effects, for power-on, power-off, and power-on frozen ring oscillators

	RO_0	RO_{12}
	Oscillating Powered-ON RO	
$f_0(Mhz)$	12.98	12.86
f_{MAX}	13.03	12.94
Δf	+0.43%	+0.64%
	Powered-OFF RO	
$f_0(Mhz)$	13.01	13.01
f_{MAX}	13.06	13.05
Δf	+0.37%	+0.32%
	Frozen Powered-ON RO	
$f_0(Mhz)$	13.58	-
f_{MAX}	13.72	-
Δf	+1.03%	-

and the closer they are to the transistor canal, the higher the number of charge carriers they will attract from the S_I canal. As a consequence, larger leakage paths are created, leading to a higher frequency increase.

This effect is further demonstrated in Figure 13 where the ring oscillators are powered ON and kept in a frozen state (not oscillating). This implies that the electric field applied to the N-MOS gate of half of the RO inverters is kept constant instead of oscillating between the logical states '0' and '1'. In this case, the hole-directing effect is maximized. When the target RO_0 is irradiated, it undergoes the same saturation effect as the previous experiments in almost the same time, as shown in Figure 13. However, it is interesting to note that the increase in frequency is the largest among all previous cases. A comparison of the results is given in Table II.

VII. Discussion

The preceding sections have illustrated the feasibility of manipulating ring oscillators with X-rays when they are powered and oscillating (Power-on) and when they are powered and frozen (Power-on Frozen). However, the effectiveness of these two attacks may be reduced if a design is equipped with a countermeasure, such as propagation delay watchdogs, perturbation monitors, or physical sensors such as photon detectors. In this paper, a third attack scenario is proposed, where we directly target the structure when the chip is not powered (Power-Off). In such a scenario, any potential active countermeasures in place may be circumvented. This approach improves the versatility of our attack strategies, allowing a wider range of scenarios to be considered in the evaluation of security vulnerabilities.

The downside of power-off attacks is the loss in intensity of the TID effect, as a result of the missing guiding electrical fields. The electrical field acts as a separation medium for the e-p pairs and as a hole-guiding medium for the $p+$ charges as explained in Section II-B. The closer these charges are to the $e-$ canal, the more charge carriers they will attract and the more leakage will occur due to these parasitic canals.

Under current conditions, for this attack to be successful, the frequency shift induced by the X-rays needs to be greater than half of the standard deviation of the measured frequencies. The slowest oscillation frequency needs to be able to reach only half of the standard deviation due to the energy starvation effect, which leads to the lowering of the oscillation frequencies uniformly and with almost the same rate as the increase of the target. In this manner, it is possible to flip the response of every possible bit in the PUF, depending on the target RO.

The design of a RO-PUF forces constraints to achieve oscillation frequencies that are very close to each other. A frequency that is an outlier, that is abnormally far from the distribution of other frequencies is usually filtered out by the PUF design itself. As a result, the attack method presented in this paper scales positively with a robust RO-PUF design: the closer the frequencies are to each other, the more efficient the X-ray attack. A frequency shift of about 1%, as found in our experiments, is usually more than enough to exceed the frequency shift induced by the design process variation in a selection of ring oscillators that are used in a PUF design.

In our setup, the Ring Oscillators were deliberately placed in order to facilitate the experimental campaigns and the analysis of the results. In particular, each RO was distinct from the others and the two targets were placed farther away to minimize the effects of the border on the neighbors. In a real design, we expect the attacker to face several additional difficulties related to the implementation. The actual placement of the PUF, or more specifically of the ROs, should be known by the attacker for an improved success rate. This could be done by either reverse engineering the layout of a sample device or by performing a cartography using differential analysis on several samples. However, identifying the rings to target remains a complex task, and the quantification of border effects or starving of neighbors should also be studied further.

An additional layer of complexity is provided by the spatial resolution of this attack. Although synchrotron sources allow targeting single transistors even on recent technology nodes, laboratory sources are less powerful and less precise, and thus require tungsten masks. Studies are ongoing in order to improve the mask resolution: the current state of the art allows for under $1\mu m$ holes thanks to conic design [31], but correct mask placement also poses a challenge.

To our knowledge, no dedicated countermeasures have been proposed in the literature so far. Ionizing radiations are well known and several techniques for hardening exist: at the process level, oxide hardening [32] or SOI process [33] can improve robustness, as well as design solutions at layout level [34], [35]. However, these approaches may be too expensive and not adapted to localized attacks.

VIII. Conclusion

Physical Unclonable Functions are important building blocks in the root of trust. In this paper, we have shown an attack that can bias the behavior of Ring Oscillator structures, which can be used as basic blocks for PUFs. To achieve this result, we leverage localized ionizing radiations, thanks to a laboratory X-Ray source and a shielding approach based on tungsten masks. We have shown for the first time that this approach allows selected modifications of the electrical

characteristics of the integrated circuit. As a consequence, the attacker may be able to control specific bits of the PUF response.

However, it is crucial to acknowledge the practical challenges and limitations associated with these attacks. The necessity of knowledge of PUF layout, constraints in spatial resolution with laboratory X-ray sources, correct mask placement, and potential border effects introduces complexity to the attack process. Despite these challenges, the noteworthy advantage lies in the exploitability of these attacks in power-off conditions non-invasively which is a unique ability of TID type radiation, allowing for potential circumvention of existing countermeasures effective when the circuit is operational.

In the future, our aim will be to assess the actual threat of this scenario in more realistic use cases and countermeasures, as well as to propose possible solutions.

ACKNOWLEDGMENT

This work has been partially funded by the French National Research Agency in the frame of the ANR project MITIX (ANR-20-CE39-0012) and POP (ANR-21-CE39-0004). TIMA Laboratory is part of the Grenoble Alpes Cybersecurity Institute (ANR-15-IDEX-02).

REFERENCES

[1] Satyajit Sinha. State of iot 2023. https://iot-analytics.com/number-connected-iot-devices/, 2023. Accessed: (2023-12-12).

[2] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th Annual Design Automation Conference*, DAC '07, page 9–14, New York, NY, USA, 2007. Association for Computing Machinery.

[3] Daihyun Lim, Jae W. Lee, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas. Extracting secret keys from integrated circuits. *IEEE Trans. Very Large Scale Integr. Syst.*, 13(10):1200–1205, oct 2005.

[4] Amir Ali-Pour, David Hely, Vincent Beroulle, and Giorgio Di Natale. An efficient approach to model strong puf with multi-layer perceptron using transfer learning. In *2022 23rd International Symposium on Quality Electronic Design (ISQED)*, pages 1–6, 2022.

[5] Ulrich Rührmair and Jan Sölter. Puf modeling attacks: An introduction and overview. In *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1–6, 2014.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Controlled physical random functions. In *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, pages 149–160, 2002.

[7] Elena Ioana Vatajelu, Giorgio Di Natale, Mohd Syafiq Mispan, and Basel Halak. On the encryption of the challenge in physically unclonable functions. In *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 115–120, 2019.

[8] Georg T. Becker. Robust fuzzy extractors and helper data manipulation attacks revisited: Theory versus practice. *IEEE Transactions on Dependable and Secure Computing*, 16(5):783–795, 2019.

[9] Shahin Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert, and Christian Boit. Laser fault attack on physically unclonable functions. In *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pages 85–96, 2015.

[10] Hayden Cook, Jonathan Thompson, Zephram Tripp, Brad Hutchings, and Jeffrey Goeders. Cloning the unclonable: Physically cloning an fpga ring-oscillator puf. In *2022 International Conference on Field-Programmable Technology (ICFPT)*, pages 1–10, 2022.

[11] Stéphanie Anceau, Pierre Bleuet, Jessy Clédière, Laurent Maingault, Jean-Luc Rainard, and Rémi Tucoulou. Nanofocused x-ray beam to reprogram secure circuits. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Proceedings*, volume 10529 of *LNCS*, pages 175–188. Springer, 2017.

[12] H. J. Barnaby. Total-ionizing-dose effects in modern cmos technologies. *IEEE Transactions on Nuclear Science*, 53(6):3103–3121, 2006.

[13] Laurent Maingault, Stéphanie Anceau, Manuel Sulmont, Luc Salvo, Jessy Clédière, Pierre Lhuissier, 9897448 Emrick Beliard, and Jean-Luc Rainard. Laboratory x-rays operando single bit attacks on flash memory cells. In Vincent Grosso and Thomas Pöppelmann, editors, *Smart Card Research and Advanced Applications - 20th International Conference, CARDIS 2021*, volume 13173 of *LNCS*, pages 139–150. Springer, 2021.

[14] Paul Grandamme, Lilian Bossuet, and Jean-Max Dutertre. X-ray fault injection in non-volatile memories on power off devices. In *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pages 1–7, 2023.

[15] J.W. Lee, Daihyun Lim, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, pages 176–179, 2004.

[16] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[17] Abdulaziz Al-Meer and Saif Al-Kuwari. Physical unclonable functions (puf) for iot devices. *ACM Comput. Surv.*, 55(14s), jul 2023.

[18] Huansheng Ning, Fadi Farha, Ata Ullah, and Lingfeng Mao. Physical unclonable function: Architectures, applications and challenges for dependable security. *IET Circuits, Devices & Systems*, 14(4):407–424, 2020.

[19] Sudhanya P and P. Muthu Krishnammal. Study of different silicon physical unclonable functions. In *2016 International Conference on Wireless Communications, Signal Processing and Networking(WiSPNET)*, pages 81–85, 2016.

[20] Abhranil Maiti and Patrick Schaumont. Improving the quality of a physical unclonable function using configurable ring oscillators. In *2009 International Conference on Field Programmable Logic and Applications*, pages 703–707, 2009.

[21] Hans Reisinger, Tibor Grasser, Karsten Ermisch, Heiko Nielen, Wolfgang Gustin, and Christian Schlünder. Understanding and modeling ac bti. In *2011 International Reliability Physics Symposium*, pages 6A.1.1–6A.1.8, 2011.

[22] Hugh J. Barnaby, Michael L. McLain, Ivan Sanchez Esqueda, and Xiao Jie Chen. Modeling ionizing radiation effects in solid state materials and cmos devices. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 56(8):1870–1883, 2009.

[23] E.H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F.L. Kastensmidt. Using bulk built-in current sensors to detect soft errors. *IEEE Micro*, 26(5):10–18, 2006.

[24] Kohei Matsuda, Sho Tada, Makoto Nagata, Yuichi Komano, Yang Li, Takeshi Sugawara, Mitsugu Iwamoto, Kazuo Ohta, Kazuo Sakiyama, and Noriyuki Miura. An ic-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density. *Japanese Journal of Applied Physics*, 59(SG):SGGL02, feb 2020.

[25] David Spielmann, Ognjen Glamočanin, and Mirjana Stojilović. RDS: FPGA Routing Delay Sensors for Effective Remote Power Analysis Attacks. *TCHES*, pages 543–567, March 2023.

[26] Fabio Garzetti, Nicola Corna, Nicola Lusardi, and Angelo Geraci. Time-to-Digital Converter IP-Core for FPGA at State of the Art. *IEEE Access*, 9:85515–85528, 2021.

[27] Alan Drake, Robert Senger, Harmander Deogun, Gary Carpenter, Soraya Ghiasi, Tuyet Nguyen, Norman James, Michael Floyd, and Vikas Pokala. A distributed critical-path timing monitor for a 65nm high-performance microprocessor. In *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, pages 398–399, 2007.

[28] Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round des. In Ernest F. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, pages 487–496, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[29] Nasr-Eddine Ouldei Tebina, Nacer-Eddine Zergainoh, Guillaume Hubert, and Paolo Maistri. Simulation methodology for assessing x-ray effects on digital circuits. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6, 2023.

[30] H. Murtaza, S. Rolland du Roscoat, P. Lhuissier, L. Salvo, L. Orgéas, C. Thibaut, A. Denneulin, D. Chaussy, and D. Beneventi. Air-drying of

3d printed part made of ligno-cellulosic fibres: 3d real-time monitoring combining sub-minute laboratory x-ray microtomography and digital volume correlation. *Cellulose*, 30(10):6173–6185, Jul 2023.

[31] S. Bouat, S. Anceau, L. Maingault, J. Clédière, L. Salvo, and R. Tucoulou. X ray nanoprobe for fault attacks and circuit edits on 28-nm integrated circuits. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6, 2023.

[32] Chao Peng, Zhiyuan Hu, Yunfei En, Yiqiang Chen, Zhifeng Lei, Zhangang Zhang, Zhengxuan Zhang, and Bin Li. Radiation hardening by the modification of shallow trench isolation process in partially depleted soi mosfets. *IEEE Transactions on Nuclear Science*, 65:877–883, 2018.

[33] Yang Huang, Binhong Li, Xing Zhao, Zhongshan Zheng, Jiantou Gao, Gang Zhang, Bo Li, Guohe Zhang, Kai Tang, Zhengsheng Han, and Jiajun Luo. An effective method to compensate total ionizing dose-induced degradation on double-soi structure. *IEEE Transactions on Nuclear Science*, 65(8):1532–1539, 2018.

[34] G. Anelli, M. Campbell, M. Delmastro, F. Faccio, S. Floria, A. Giraldo, E. Heijne, P. Jarron, K. Kloukinas, A. Marchioro, P. Moreira, and W. Snoeys. Radiation tolerant vlsi circuits in standard deep submicron cmos technologies for the lhc experiments: practical design aspects. *IEEE Transactions on Nuclear Science*, 46(6):1690–1696, 1999.

[35] Jie Liu, Jicheng Zhou, Hongwei Luo, Xuedong Kong, Yunfei En, Qian Shi, and Yujuan He. Total-dose-induced edge effect in soi nmos transistors with different layouts. *Microelectronics Reliability*, 50(1):45–47, 2010.