On Power-Off Temperature Attacks Potential Against Security Sensors

Maryam Esmaeilian, Vincent Beroulle, David Hély

MDPI

Article

On Power-off Temperature Attacks Potential against Security Sensors

Maryam Esmaeilian[1,*,†], Vincent Beroulle[1,†], and David Hély[1,†]

[1] Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France;
Emails: firstname.lastname@lcis.grenoble-inp.fr
* Correspondence: maryam.esmaeilian@lcis.grenoble-inp.fr
† These authors contributed equally to this work.

Abstract: Embedded systems can be targeted by Fault Injection Attacks (FIAs), which enable attackers to alter the system specified behavior, potentially gaining access to confidential information or causing unintended outcomes, among other effects. While numerous security sensors and attack detectors have been proposed in the literature to detect different sources of FIAs, it is crucial to ensure that these mechanisms themselves have not been tampered. Hence, the integrity of these detectors is critical in maintaining the security of embedded systems. The study focuses on evaluating the robustness of delay-based digital detectors against a new type of FIA called Power-Off Temperature Attack (POTA). POTA occurs when the chip power is turned off, rendering the detectors inactive and allowing the attackers to bypass them. After a POTA, the circuit or its detectors may not function properly when the power is restored, potentially allowing other attacks to go undetected if the detectors are less sensitive. This study implements two attack detectors on Xilinx Artix-7 FPGAs and investigates the impact of heating cycles on theses detectors characteristics when the FPGA is in different states, including power-off, power-on, and inactive modes (such as clock-freezing mode). Our experiments reveal that heating cycles in power-off or inactive modes can alter the FPGA component delays and reduce the accuracy of its detectors, which highlights the vulnerability of these systems to POTA and potential risks to embedded system security.

Keywords: hardware security; fault injection attack; power-off attack; temperature attack; secure circuit; delay-based detectors

1. Introduction

Electronic devices are increasingly employed in security applications, such as authentication applications.a consequence, these devices are the target of many different attacks aiming at either modifying their normal behavior or revealing secret data such as cryptographic keys. Due to the nature of their applications, such devices are particularly vulnerable to physical attacks, where the attacker can leverage a physical access to the device and further perform a so-called hardware attacks such as Side Channel Attacks (SCAs) [1] and Fault Injection Attacks (FIA) [2] two popular types of these attacks.

SCAs represent a class of security vulnerabilities that exploit unintended information leakage from a device during its operation. SCAs focus on the physical characteristics of a device, such as its power consumption, execution time, electromagnetic emissions, or even sound emissions. By analyzing these side-channel signals, attackers can glean valuable information about the device's internal processes, leading to the extraction of sensitive data or cryptographic keys. The fundamental premise behind SCA is that the behavior of a device, even one designed securely, can inadvertently reveal subtle clues about the computations it performs. For example, when a device performs cryptographic operations, the electrical power it consumes might vary depending on the specific operations being executed. Similarly, the time it takes to complete certain tasks can also provide hints about the data being processed.

Citation: Esmaeilian, M.; Beroulle, V.; Hély, D. On Power-off Temperature Attacks Potential against Security Sensors. *Journal Not Specified* **2023**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

Unlike SCA, where the attacker does not affect the normal operation of the system, FIA involves intentionally disrupting the normal operation of the system by injecting faults. These faults can stem from various sources, such as altering the system's component electrical parameters. The result is a deviation from expected behavior, potentially granting attackers unauthorized access or exposing vulnerabilities. In this study, our main focus is on these FIAs.

The techniques for FIAs are becoming increasingly advanced and powerful. This development causes an important concern and a threat to systems where security plays a fundamental role. So, numerous security experts and designers are actively developing protection and detection mechanisms to mitigate the risks associated with such attacks. One of these mechanisms is the use of detectors (or sensors) to detect FIAs. These detectors, which can be digital or analog, can detect FIAs[3,4]. Recent works have mostly focused on digital detectors because they can be easily calibrated and placed close to security primitives such as PUFs and encryption cores. For example, in [5] a digital detector is presented to detect FIA based on electromagnetic radiations. Furthermore, digital detectors introduced in [6] and [7] can detect clock glitching and voltage glitching attacks, respectively.

Detectors are used to protect the system from FIA. However, it is crucial to ensure that these detectors themselves are protected against potential FIAs. There is a bunch of research work on the vulnerability of detectors [8][9] to various types of FIAs as well as methods for protecting them. However, all previous studies evaluating detectors against FIAs have assumed that the detectors are connected to the power supply. However, none have assessed their effectiveness against FIA when the power is off.

Recent research has demonstrated that Laser Fault Injection (LFI) can be performed even when a device is not powered [10]. This study targets the Flash memory of a 32-bit microcontrollers, showing that laser exposure can introduce persistent faults without requiring real-time synchronization between the attacker and the system. These findings highlight the increasing sophistication of FIA techniques and their potential impact on security. However, while prior works have investigated attacks on unpowered devices, they have not specifically examined their effects on FIA detectors. Our study addresses this gap by evaluating how Power-Off Temperature Attacks (POTA) impact digital FIA detectors. This new type of FIA, which we call a POTA, is performed when the target device is not connected to any power supply. The characteristics of the detectors can be changed by an attacker without being detected, as the detectors are off. Such changes can adversely affect the key detector features, such as the detection thresholds, leading to a modification in the false-positive and false-negative detection rates. Alterations can affect detector accuracy, while an increase in the false-negative rate may lead to security risks and grant unauthorized access to the system to attackers. Unlike [10], which focuses on modifying stored memory contents, we analyze how temperature-induced variations can alter detection thresholds and compromise the reliability of security mechanisms.

The objective of this work is to evaluate potential attacks on FIA detectors while the system is powered off. Our main contributions are as follows: First, we introduce the concept of POTA and demonstrate its impact on digital FIA detectors. Second, we investigate how high temperatures induced by external heating can alter detector characteristics and compromise detection reliability. Finally, we conduct experimental validation using a Ring Oscillator(RO) and a digital detector to analyze the effects of LFI and aging in power-off. Our study focuses on the detector proposed in [11] and a RO to assess the impact of LFI and aging attacks when the target device is turned off. To simulate these attacks, we use overheating to emulate the effects of LFI and aging, as overheating cycles can induce permanent variations in the detector's characteristics. These persistent changes can be critical, particularly in cases where false negatives occur in FIA detection.

The general aim of this study is how heating when power is not supplied, impacts the properties of simple digital detectors. To conduct this experiment, we subjected the chip to various periods of heating, as certain FIAs like LFI can lead to temperature elevation.

By heating the circuits under study, we were able to evaluate the impact of the FIA on the chip's properties and determine its effects on the detection threshold.

The rest of the paper is organized as follows: In Section 2, we review the state-of-the-art related to our work. In Section 3, the structure and methodology of this study will be explained. Experimental results are presented in section 4. In Section 5, we discuss the results. And at the end of this paper in Section 6 we conclude and give the perspectives for future works.

2. Related work

2.1. Digital and Analog FIAs Detectors

Several methods have been introduced in the literature to protect devices against FIAs. These techniques can be based on redundancy at different levels or on techniques based on sensors' use. The advantage of redundancy is that it allows for faults to be detected independently of the FI technique. However, the main disadvantage of this method is that this method cannot capture all possible faults [12]. The second technique is to use fault detection sensors, also known as detectors. Detectors can be divided into two categories, digital detectors and analog detectors; the analog type, as its name suggests, uses analog sources to detect FIA, in [13] a type of analog detector is proposed that uses a time-to-digital converter to detect FIA. These types of detectors, because they use analog sources, are much more difficult to calibrate than digital ones; on the other hand, they require more power consumption, so digital detectors are widely used today. Different digital FIA detectors are proposed in the literature[14,15]. One of the most popular designs, named Delayed-based detector, has been suggested in [16]. This detector is based on the timing constraints of the synchronous circuits Equation (1). To guarantee that synchronous circuits operate correctly, the clock period (T_{Clock}) must be greater than the sum of the propagation delay ($T_{PropagationDelay}$) and the setup time (T_{Setup}); otherwise, the circuits do not have enough time to perform its operations.

$$T_{\text{Clock}} \geq T_{\text{PropagationDelay}} + T_{\text{Setup}} \tag{1}$$

Delayed-based detectors can detect various FIAs, such as clock glitching, under-powering or overheating [17–19].

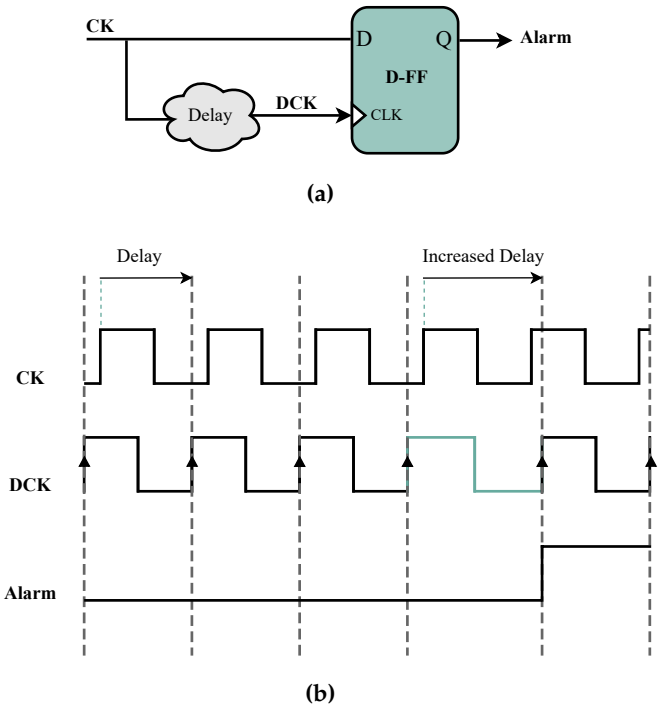


Figure 1. Schematic diagram and waveforms of the delay-based detector proposed in [16]

Figure. 1 illustrates how this detector compares the delayed clock signal (denoted DCK) with the primary clock signal using a D Flip Flop (D-FF). If there is a malfunction (e.g., delay variations or clock period increases), the alarm is activated. While this detector is simple and efficient against certain FIAs, it is less effective for attacks with localized effects, such as laser or electromagnetic FIAs. This limitation exists because detectors can detect violations from global sources. However, using a network of these detectors can improve the detection of localized attacks[20]. Additionally, this type of detector can detect FIAs that increase the clock period or propagation delay but is unable to detect attacks that decrease the clock period [20]. Accordingly, other designs have been introduced to improve the detection rates against FIAs. The next category of the proposed detectors is based on RO. ROs can be implemented using a closed chain of odd-numbered inverters [20]. In this structure, RO alternates between zero and one, so it can be a frequency generator whose output frequency depends on the number of inverters and propagation delays.

The implemented ROs can be used in a detector design. For instance, as shown in Figure. 2 from [21], this detector consists of two high- and low-phase circuits, which are used for the one- and zero levels of the clock signal, respectively.

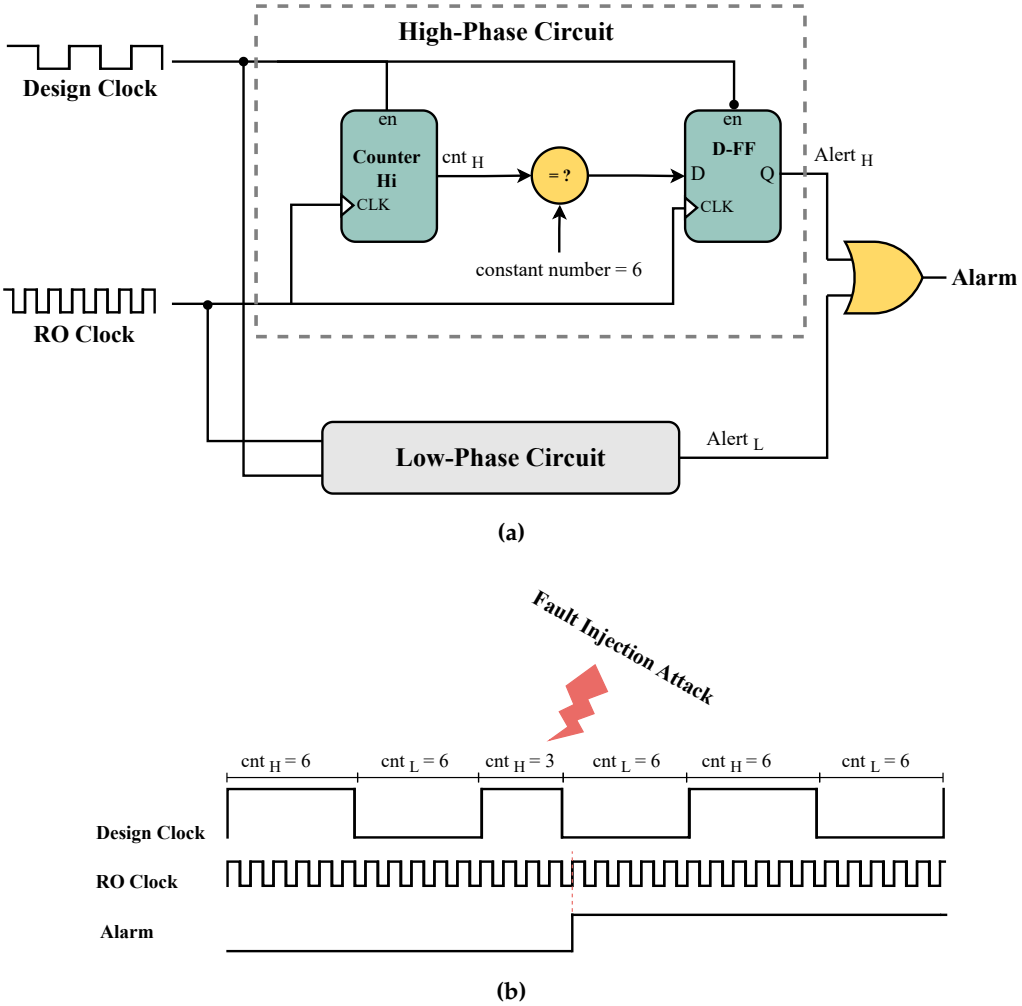


Figure 2. (a) Schematic diagram and (b) waveforms of the counter-based detector proposed in [21]

Each of these circuits counts the number of RO oscillations at each clock level and then compares them with a constant value. In normal mode, the number of RO oscillations is always the same, but when unde attack, the number of RO oscillations changes and is not equal to the constant value which as a consequence triggers the alarm. Since this detector uses two separate circuits for the zero/one levels of the clock, it can detect attack attemps at each level of the clock and thus can speed up the fault detection. Furthermore,

in order to detect an attack it compares with a constant value, so it is capable of detecting attacks that can decrease and increase the clock period, so it exposes a higher accuracy than the delay-based detector that is proposed in [16]. In [22], the authors evaluated glitch detection circuits against FIAs. Their experiments revealed significant weaknesses, as they successfully bypassed the detectors using four distinct glitching attacks. The effectiveness of these detectors was shown to depend heavily on internal parameters and the techniques used to attack the circuit. This suggests that FIA detectors may also be vulnerable to other types of attacks. In our work, we specifically evaluate the robustness of these detectors against power-off temperature attacks, aiming to further investigate their potential weaknesses under varying environmental conditions. In this study, we aim to evaluate the effects of POTA on delay-based detectors. These detection circuits have been extensively studied in the literature and are widely deployed to counter various FIA methods. Indeed, several FIA techniques induce timing violations. Notably, timing-violation detection circuits have been proposed as effective countermeasures against attacks that exploit timing anomalies, including underpowering voltage glitching [23] and electromagnetic FIA [24]. Consequently, any attack detector designed to identify other threats could also be vulnerable to POTA if it relies on delay-based principles. These detectors are widely adopted due to their capability to detect a broad range of FIA techniques. More recently, Intel announced the integration of such detectors into Intel Core processors [25]. Given the growing reliance on these mechanisms, understanding their potential vulnerabilities to POTA is crucial for enhancing security.

2.2. Aging Effects

Aging is a critical factor to consider in our work, as it directly impacts the long-term performance and reliability of FIA detectors. Over time, aging mechanisms can degrade transistors [26,27][28], potentially increasing the vulnerability of these detectors. The following four primary mechanisms of aging are commonly referenced in the literature [29].

2.2.1. Bias Temperature Instability (BTI)

Bias Temperature Instability (BTI) is an aging mechanism that affects the reliability of transistors in integrated circuits. It occurs because of prolonged exposure to electrical stress and elevated temperatures during device operation. BTI leads to a gradual increase in the transistor's threshold voltage and a decrease in its performance. Over time, this degradation can result in reduced speed and power efficiency in electronic devices, affecting their overall lifespan and reliability. BTI consists of two main phases as shown in Figure. 3 :

- **Stress Phase:** BTI begins when a transistor is under constant electrical stress during operation. This stress gradually affects the transistor's performance, mainly by increasing its threshold voltage.
- **Recovery Phase:** When the stress is removed, the transistor might partially recover its original performance, but it may not fully return to its initial state as shown in Figure. 3. The recovery phase follows the stress phase in BTI.

2.2.2. Hot Carrier Injection (HCI)

HCI is another aging effect that affects the reliability of transistors. It occurs when high-energy electrons or holes are injected into the gate oxide of the transistor under high-voltage conditions. This injection can create traps or defects in the oxide layer, which degrades the transistor's performance and can lead to threshold voltage shifts. HCI is more pronounced in transistors with smaller feature sizes, as they are more susceptible to higher electric fields.

2.2.3. Time-Dependent Dielectric Breakdown (TDDB)

Time-Dependent Dielectric Breakdown (TDDB) refers to the gradual weakening of the insulating material in electronic devices over time due to sustained electrical stress

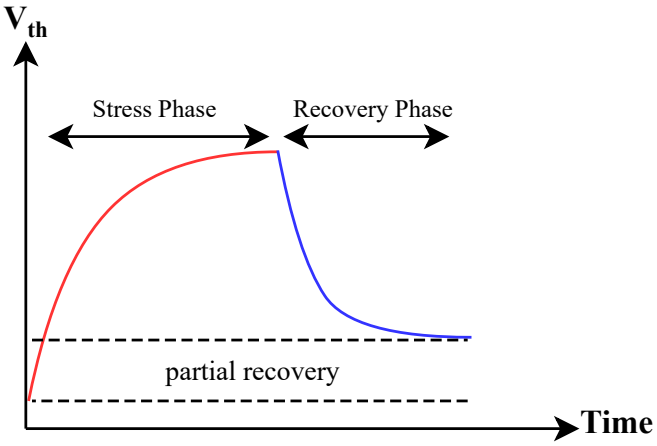


Figure 3. BTI has two phases: the stress phase and the recovery phase.

and voltage. This degradation can lead to the formation of microscopic defects, which may result in electrical leakage or short circuits, ultimately reducing the reliability and operational lifespan of the device.

2.2.4. Electromigration

Electromigration occurs when metal atoms in electronic components gradually move due to high current and heat. Over time, this can weaken connections and lead to electrical failures, affecting the reliability of the device.

The aging effects on transistors can result in a variety of issues, such as increased power consumption, reduced switching speed, and diminished overall circuit reliability. Between all aging mechanisms, BTI and HCI have a greater effect on the performance of the transistor[30].

In this section, we discussed previous works related to countermeasures against FIA, particularly focusing on digital detectors. Additionally, We discussed aging and its effects. The two main factors contributing to aging in transistors are temperature and electrical stress. As explained earlier, our project aims to assess the impact of LFI and aging attacks on FIA detectors and a basic RO. One of the effects of LFI is an increase in temperature at the targeted location of the chips. High temperature is also a method to accelerate aging, so in our evaluation, we use high temperature to simulate the effects of LFI and aging attacks.

3. Methodology

In this section, our goal is to explain the detection principles of the two Device Under Test (DUT) and the method of our experiment. As explained in the previous section, our goal in this study is to evaluate the effect of LFI on the sensitivity of the detector when the power of the device is off. As recalled earlier, heating (due to several possible sources) is a major source of aging for integrated circuits; in the rest of the study, we consider heating (without considering the source, which can be a laser or simply an oven) as a characterization means to analyze the effect of power-off attacks.

3.1. Device Under Test (DUT)

In this case study we choose two DUTs for our experiment: delay-based detector and RO based detector.

3.1.1. Delay-based detector

For the first DUT, we selected the delay-based detector that was proposed in [16] because this type of detector is less complex to implement than other types. Figure. 4a illustrates the delay-based detector, which operates by keeping the alarm inactive while

the output of the two flip-flops (represented as the I-Signal and O-Signal in Figure. 4a) are equal. But, when these two signals are complementary, the alarm will be activated. In fact, if the delay of the buffer chain exceeds the clock period, the I-Signal may not arrive at the second flip-flop input in time, causing the outputs of the two flip-flops to differ and trigger the alarm. The number of buffers should be selected carefully to ensure that their delay is sufficiently close to the clock period. This will ensure that the alarm remains inactive in normal operation but becomes active in the event of an attack on the circuit. As shown in Equation 2, as long as this equation is true, the alarm is not activated.

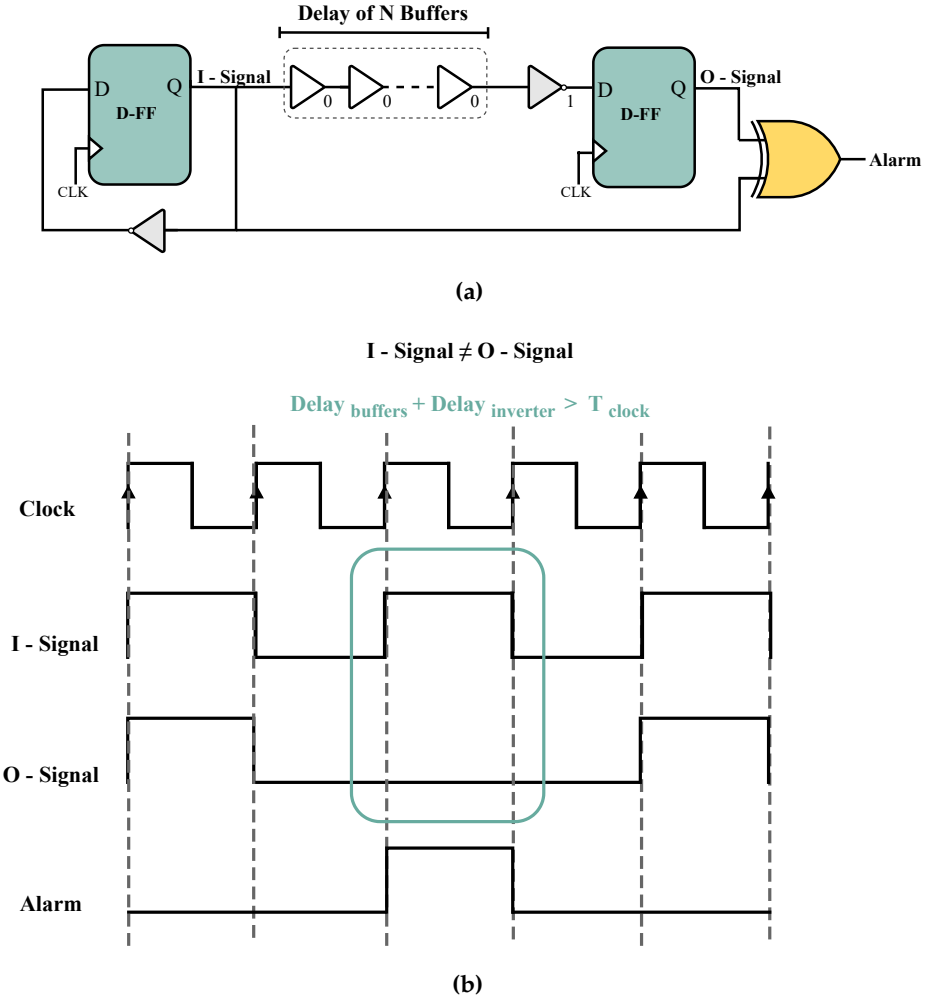


Figure 4. (a) Schematic and (b) waveforms of the delay-based detector proposed in [11]

FIAs, such as heating and laser, can increase the delay of logic gates, thereby modifying Equation 2 and triggering this detector. The sensitivity of the detector increases as the delay caused by the buffers approaches the clock period. However, this also increases the likelihood of false positives. Therefore, there is a trade-off between improving the accuracy of the detector and increasing the number of false positives. As mentioned earlier, selecting the optimal number of buffers is critical to implment this detector. Since we need to choose the number of buffers whose delay is close to the clock period.

$$T_{clock} \geq Delay_{(buffers+inverter)} + T_{setup} \tag{2}$$

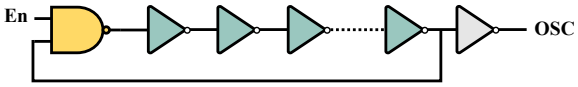


Figure 5. Ring Oscillator (RO)

3.1.2. Ring Oscillator (RO)

As many detectors rely on RO, the second Device Under Test (DUT) is a basic RO design. Furthermore, compared to delay-based detectors, RO-based detectors offer a better understanding of how power-off attacks function. as shown in Figure. 5.

3.2. Our Test Scenarios

To improve the precision of assessing the impact of POTA on our DUTs, it is necessary to define several test scenarios. Hence, we incorporate a condition on power and an additional condition on temperature. In the subsequent section, we will examine the aforementioned conditions and their potential contribution to our evaluation process.

3.2.1. **Temperature Condition**

To have a comprehensive comparison to evaluate the effect of heating, we have three temperature conditions.

1. **First condition:** Constant Temperature

   In this condition, we keep the DUTs warm for certain periods, for example, the temperature of the test is the same for one week.

2. **Second condition:** Temperature cycling

   Unlike the previous condition where the DUTs were kept warm continuously for a certain period, in this condition, the DUTs will be heated cyclically for a certain period. In other words, in one week, we cool the DUTs daily and then bring them back to a high temperature. So far, no work has been found to compare the effects of cyclic temperature heating and constant temperature heating, so in this study, we will also compare the effects of these two types of heating.

3. **Third condition:** Room Temperature

   To evaluate the effects of heating, we have to compare with a reference chip, turned on permanently (during the test time) and at room temperature; so we added the third condition.

3.2.2. **Power Conditions**

To conduct our experiment, we will focus on three main scenarios for power, which are described in the following.

1. **First condition:** power-off

   Here, the DUTs are not connected to any power source. Evaluating this condition is the main goal of our study.

2. **Second condition:** power-on

   All of the DUTs in this condition are powered on. We use this condition as a reference, which means that the power-on condition can help us compare the results of this condition with the power-off condition.

3. **Third condition:** clock freezing

   In this condition, we connect our DUTs to power, but the clock signal of the delay-based detector is frozen (i.e., does not have any edge in clock), also, for RO, the enable signal is equal to zero (i.e., the RO is inactive). We use this condition because the aging

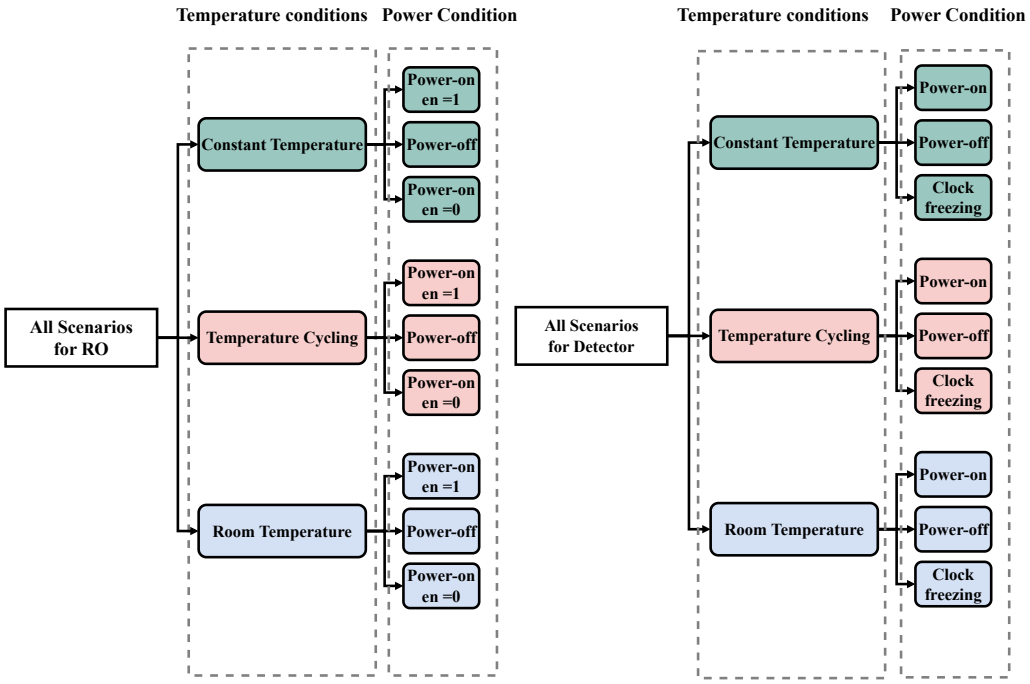


Figure 6. All of the scenarios for our experiment for DUTs (RO and Detector)

effect is sensitive to electrical stress. When there is no clock or an enable inactive, then the detector is unable to detect an attack.

Therefore, we have three temperature conditions for each detector and RO, then for each condition we have three power conditions, which are shown in Figure. 6

3.3. Attacker Model

In this work, we consider an attacker who manipulates the circuit while it is powered-off to alter the intrinsic characteristics of security sensors or attack detectors. The attacker could then successfully carry out a FIA when the circuit is powered-on, exploiting the attack without detection by the compromised fault attack detector. Integrated circuits are particularly sensitive to heat, which alters the intrinsic electrical properties of transistors. Heating accelerates the aging of the circuit. It can be achieved with an oven, but local heating can also result from a laser attack.

For the scenarios outlined in Section 3.2, the attacker must physically access the target system to induce heating and disconnect its power supply to execute the powered-off attack. Additionally, for clock freezing, the attacker needs to freeze the clock of the detector to disable its oscillation.

4. Experiments

In this section, we present experiments conducted on actual devices to evaluate the impact of heating on the scenarios described in the previous section. We begin by describing the experimental setup, followed by the presentation of the experimental results for heating effects. Then, in the next section, these results will be discussed.

4.1. Experimental Setup

As mentioned in the previous sections, our objective is to evaluate the impact of overheating on the performance of the delay-based detector and the frequency of the RO in various power and temperature conditions. For each DUT (RO and delay-based detector), we examined nine scenarios: three temperature conditions and three power conditions. We implemented each scenario on a separate BASYS-3 board with an Xilinx Artix-7 FPGA, for a total of 18 boards.

4.1.1. Measurement setup

To evaluate the detector response time, we utilized an oscilloscope to measure the alarm signal's activation time. For the RO, we measured the period with a 100 ps time resolution. It is important to mention that to determine the detection threshold accurately, we performed 10 successive measurements on each detector before averaging the results.

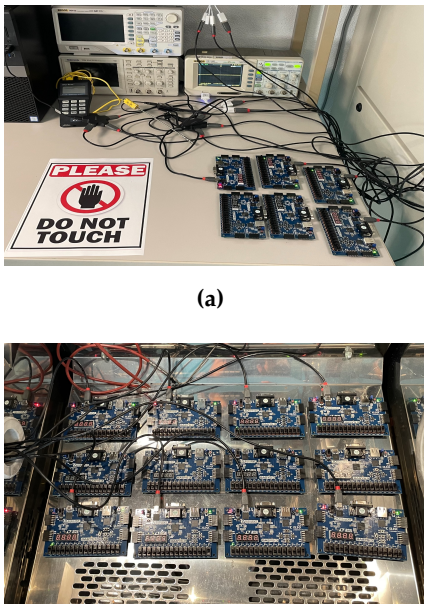
All measurements were taken with the chips at the same temperature, specifically normal room temperature. This requires removing the FPGAs from the climate test chamber and waiting for them to return to room temperature. Removing the DUT every day reduces the duration of exposure (about 8 hours per day) and produces temperature cycles, with temperature rises and falls. However, the state of the art does not mention any particular effects in terms of aging caused by these cycles. Indeed, only the duration during which the components are exposed to high temperatures is known to produce aging effects. In addition to the experiments mentioned above, we conducted two additional tests to increase measurement accuracy: first, we evaluated the internal temperature of the chip and its effects on the RO frequency. This test helps determine if measurements need to be taken at a specific time after the chip is turned on. Secondly, we assessed how increasing internal temperature affects the RO frequency. Understanding this impact helps us gauge the importance of temperature on the detector threshold and identify potential measurement errors. To perform these tests, we accessed the internal temperature of the chips using the built-in temperature detectors in the Artix-7 FPGA.

4.1.2. Delay-based Detector setup

First, we implemented the delay-based detector as shown in 4 using HDL. To evaluate delay-based detectors against power-off attacks, it is first crucial to ensure that the detector works correctly when the device is powered on. To achieve this, we performed an over-clocking attack on the sensor while it was powered on. To perform an overclocking attack, we first changed the clock source from internal to external so that we could manipulate the clock frequency using a pulse generator. We used a Rigol DG4102 Waveform Generator to increase the circuit's frequency. In normal mode, the detector's operating frequency was 10MHz, and when we increased the frequency from 10 MHz to 17.2 MHz, the alarm was triggered. This allowed us to validate the correct operation of the detector and determine its initial threshold detection frequency. To measure the thresholds of the alarm activation, we performed overclocking attacks on each detector and then measured the alarm activation signal with an oscilloscope.

As explained in the previous chapter, we have to evaluate three temperature conditions and three power conditions. Thus, for detector evaluation, we implemented each scenario with one BASYS-3; resulting in the use of nine boards in this study to assess detectors against POTA. To ensure a comprehensive evaluation, it was important to obtain a large number of results for each scenario, enhancing the reliability and accuracy of our tests. Therefore, rather than implementing just one detector per chip, we placed 27 detectors on each chip. This significantly increased the accuracy of our results. We implemented 27 detectors (RO) in each BASYS-3 due to the limitation in the number of Pmod pins on the BASYS-3 board and also because we aimed to realize this test manually. Since we have 27 detectors in each chip, each detector (RO) uses a different clock frequency. This approach is based on literature showing different effects of heating on different RO frequencies [31]. Therefore, we can also evaluate the effects of heat and POTA on different alarm frequencies. For this purpose, we implemented the detectors of each chip in three groups:

- **First Group:**
  Clock source: 25Mhz (T=40ns) Alarm activation with overclocking = 38-39 Mhz
- **Second group:**
  Clock source: 10Mhz (T=100ns) Alarm activation with overclocking = 19-21 Mhz
- **Third Group:**
  Clock source: 2Mhz (T=500ns) Alarm activation with overclocking = 3-4 Mhz



(a)

(b)

Figure 7. All our scenarios include temperature conditions (Room Temperature, Temperature Cycling, Constant Temperature) and power conditions (power-on, power-off, clock freezing)(a) Outside climatic room and (b) Inside climatic room

Since in each chip, we have 3 different groups of detectors with different clock frequencies, hence we need 3 clock sources with different frequencies. For this, we used the Mixed-Mode Clock Management (MMCM) module which is available on Artix-7 FPGA.

4.2. Ring Oscillator (RO) setup

Our second DUT is the RO, as mentioned earlier. Therefore, like the detector, we also implemented it using HDL. To increase the number of results and ensure a comprehensive test, we implemented each scenario on an Artix-7 FPGA with 30 ROs per FPGA. We divided 30 RO into three groups with different frequencies:

- **First Group:** Frequency = 4Mhz
- **Second group:** Frequency = 16Mhz
- **Third Group:** Frequency = 60Mhz

To perform the practical evaluation, we used the Votsch VC 0018 climate test chamber, which can produce heat up to +95°C, as shown in the figure. We subjected the delay-based detector and RO to various time cycles within the thermal chamber to examine the impact of heat on their performance. Figure. 7 shows the general setup of our experiment, the chips that are inside the climate test chamber correspond to the constant temperature and temperature cycling scenarios, and the chips outside the room correspond to the room temperature scenario.

4.3. Experimental Results

In this section, the results of the tests described in the previous section will be presented. Table 1 shows how the RO frequency changes after it is turned on. These findings help us determine the optimal time to measure the RO frequency after activation. This matters because the frequency can vary after activation, affecting the accuracy of our main results.

Table 2 illustrates how varying the chip's internal temperature affects different RO frequencies, each operating at a unique frequency. As mentioned in the previous section, we measured the internal temperature using the temperature sensor available in the Artix-7 FPGA.

Table 1. Percentage of RO Frequency Changes Over Time After Activation.

Percentage of RO Frequency Changes After Activation(%)			
Description of RO	**After 30 min**	**After 60 min**	**After 180 min**
RO1 (59.17 Mhz)	-0.04 %	-0.05 %	-0.05 %
RO2 (18.93 Mhz)	-0.02 %	-0.04 %	-0.04 %
RO3 (4.68 Mhz)	0 %	0 %	0 %

Table 2. Effects of Internal Temperature on ROs with Different Frequencies.

Impact of Internal Temperature Changes on RO Frequencies(%)				
Description of RO	**38°C**	**41°C**	**71°C**	**96°C**
RO1 (59.17 Mhz)	0 %	-0.88 %	-3.46 %	-7.98 %
RO2 (18.93 Mhz)	0 %	-0.29 %	-2.87 %	-3.26 %
RO3 (4.68 Mhz)	0 %	-0.41 %	-2.53 %	-3.01 %

Tables 3 and 4 display the results of the tests carried out over 21 days, with all measurements taken while chips were kept at room temperature. In these two tables, the variations in activation thresholds of the detectors and RO frequency are represented. As outlined in Table 3, the degradation in alarm activation showed notable variation across different temperature and power conditions. Under the power-on condition, the most significant degradation was recorded during the temperature cycling scenario, with a reduction of -1.98%. In contrast, under power-off conditions, the degradation rates for temperature cycling and constant temperature were comparable, showing slight increases of +0.36% and +0.31%, respectively. The most substantial overall degradation was observed under the clock-freezing with temperature cycling condition, where the degradation reached -2.53%, the highest among all scenarios evaluated. Similarly, the results presented in Table 4 highlight the degradation in RO frequency across the same set of conditions. In the power-on state with en=1, the temperature cycling condition once again resulted in a considerable degradation, with a reduction of -1.75%. Under power-off conditions, both temperature cycling and constant temperature showed nearly identical degradation rates, with slight increases of +0.26% and +0.29%, respectively. Consistent with the trends observed for alarm activation. However, the most pronounced degradation in RO frequency was recorded in the power-on state with en=0, where a substantial reduction of -2.03% was observed. It is necessary to mention that all of the results obtained from the average of 27 detector activation threshold frequencies are the same for RO. For in-depth analysis, it is better to evaluate each group of frequencies separately.

+95°C is the maximum temperature that the climate test chamber can deliver. It is lower than the temperature that a laser could locally achieve. However, in the context of this study, we want to see if we observe a temperature attack effect when the circuit's power is off. If we observe an effect by immersing the entire circuit in the climatic test chamber, a laser could certainly create the same variations, perhaps more quickly by applying higher temperatures.

In this section, we have detailed the complete setup process to be applied for our DUT, its implementation on the FPGA, and the specific details of the experimental arrangement. Additionally, we presented the results of two tests conducted to validate our measurements, in the first test, we measured the changes in RO frequency from the moment it was activated up to 180 minutes later. This was done to determine whether the frequency remained stable over time. Our results showed that the frequency exhibited only minimal variations, which were negligible and had no significant impact on our overall findings. In our second test, we temporarily increased the internal temperature of the chip to ensure that temperature rise could indeed affect the RO frequency. This was done to validate whether a temperature change directly impacts the frequency of the ROs. Along with the results of our experiment

Table 3. Results of a heating Delay-based detector.

Percent change of Alarm activation(%)			
Temperature Condition	**After 7 days**	**After 14 days**	**After 21 days**
Power Condition: Power-on			
Temperature Cycling	-0.73 %	-1.04 %	**-1.98** %
Constant Temperature	-0.61 %	-0.98 %	**-1.27** %
Room Temperature	+0.10 %	+0.08 %	**+0.12** %
Power Condition: Power-off			
Temperature Cycling	+0.10 %	+0.23 %	**+0.31** %
Constant Temperature	+0.22 %	+0.30 %	**+0.36** %
Room Temperature	+0.019 %	+0.018 %	**+0.015** %
Power Condition: Clock-freezing			
Temperature Cycling	-1.52 %	-1.61 %	**-2.53** %
Constant Temperature	-1.01 %	-1.31 %	**-1.79** %
Room Temperature	-0.18 %	-0.07 %	**-0.11** %

Table 4. Results of a Heating RO.

Percent change of Ring Oscillator(RO) frequency (%)			
Temperature Condition	**After 7 days**	**After 14 days**	**After 21 days**
Power Condition: Power-on, enable=1			
Temperature Cycling	-0.43 %	-0.78 %	**-1.75** %
Constant Temperature	-0.78 %	-0.88 %	**-1.21** %
Room Temperature	-0.127 %	-0.214 %	**-0.22** %
Power Condition: Power-off			
Temperature Cycling	+0.138 %	+0.193 %	**+0.26** %
Constant Temperature	+0.156 %	+0.185 %	**+0.29** %
Room Temperature	+0.07 %	+0.12 %	**+0.10** %
Power Condition: Power-on, enable=0			
Temperature Cycling	-0.55 %	-0.84 %	**-2.03** %
Constant Temperature	-0.56 %	-0.80 %	**-1.47** %
Room Temperature	-0.01 %	-0.02 %	**-0.07** %

on ROs and detectors, including the POTA outcomes, we will provide a comprehensive discussion and analysis of all the findings in the next section.

5. Discussion

The main goal of this chapter is to discuss all the results presented in the previous chapter. To make understanding easier, we've divided these results into three groups:

The first group presents the results of measurement verification. This group comprises two evaluations: the first evaluates the percentage of changes in RO frequency after RO activation, and the second examines the effect of increasing internal temperature on various RO frequencies. The second group presents the results of the delay-based detectors, while the final group displays RO outcomes. In the following sections, detailed explanations and insights into each category are provided.

5.1. Measurement Verification

5.1.1. Percentage of RO frequency changes over time after activation

The objective of this evaluation is to determine the optimal timing for measuring the frequency of the RO after activation. The goal is to assess frequency variations within a specific time window after activation. By doing so, we aim to understand how the RO

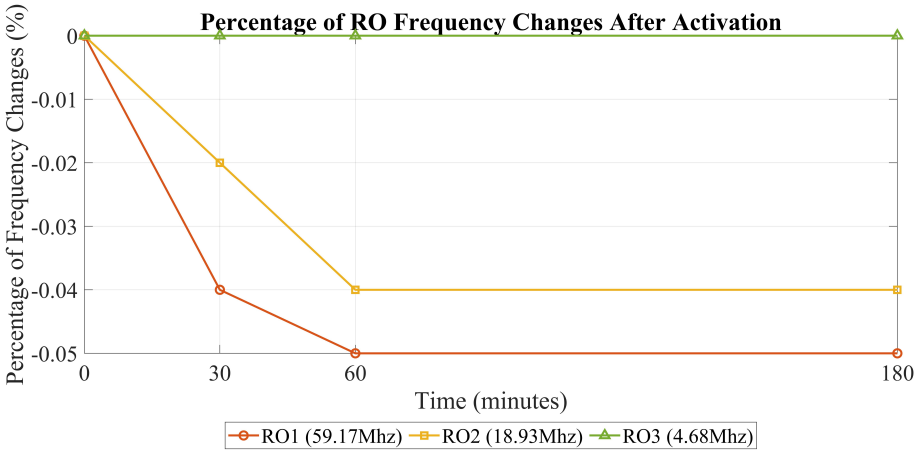


Figure 8. Percentage of RO Frequency Changes After Activation

frequency stabilizes or changes over this period. This evaluation involves measuring the RO's frequency repeatedly within the defined time frame to capture any trends or patterns that emerge. Ultimately, this analysis helps us pinpoint the most suitable moment for accurate frequency measurement after the RO's activation, contributing to a better understanding of its behavior and performance characteristics.

In Figure. 8, the degradation of the RO frequency is depicted from the moment of activation up to 180 minutes later. From this illustration, it becomes evident that the maximum degradation observed is smaller compared to the degradation observed in all heating scenarios. In simpler terms, this evaluation confirms the precision of our measurement.

Among all the heating scenarios (temperature cycling and constant temperature), the power-off scenario has the smallest effect on the RO, with a value of 0.26% in temperature cycling. The most substantial degradation after RO activation was 0.05%. This result indicates that the degradation resulting from the heating is greater than the measurement's accuracy, reinforcing the reliability of this heating evaluation.

The results of this experiment help us determine whether the RO frequency remains stable after activation. This is crucial in understanding the optimal timing for our measurements. Our findings showed that the frequency remains consistent and does not change significantly, regardless of when we perform the measurements after the RO is activated. Therefore, the timing of our measurements does not impact the results.

5.1.2. Effects of internal temperature on ROs with different frequencies

This evaluation was conducted to validate the impact of heating on our measurement approach by examining frequency degradation in relation to temperature increases. Our findings show a clear correlation between rising internal temperatures and frequency degradation. Specifically, the variations of 2–3% after heating (aging) are comparable to the effects of a +70°C temperature increase. By allowing several hours to pass before taking measurements, we ensured that the observed degradation was not solely due to temporary internal temperature changes. Notably, the highest degradation observed was 7.98%, which exceeds all degradation values recorded for both the detector and RO under normal conditions. This discrepancy arises because our measurements were taken while the chip was still in its heated state, whereas previous evaluations of heating on the detector and RO were performed under normal conditions.

This distinction is critical for two reasons. First, if no degradation is observed while the chip is hot, we can reasonably assume that no degradation will occur once it cools down. However, in our case, significant variations were detected, confirming the presence of a

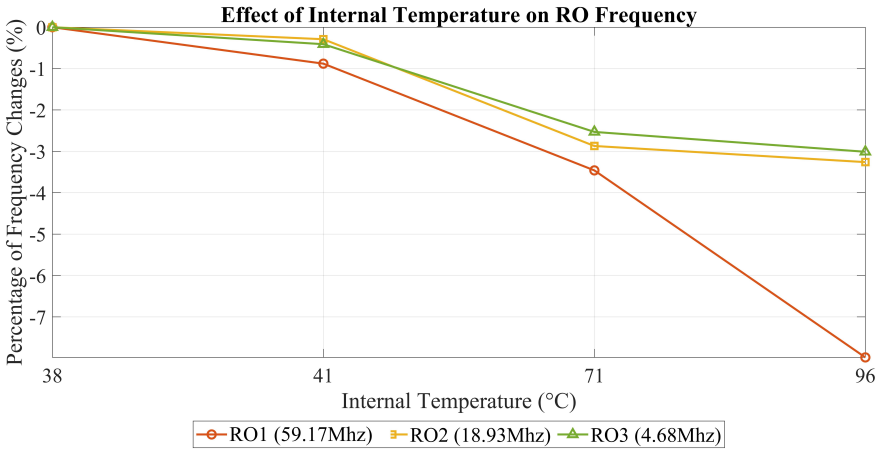


Figure 9. Impact of Internal Temperature Changes on RO Frequencies

heating effect. This evaluation improves our understanding of the relationship between temperature and frequency degradation in our measurement system.

Additionally, Figure. 9 illustrates the differential impact of heating on ROs operating at different frequencies. Three ROs are represented: the red RO at 59.17 MHz, the yellow RO at 18.93 MHz, and the green RO at 4.68 MHz.

In our experiment, we intentionally raised the internal temperature to +96°C. At this elevated temperature, the red RO, operating at the highest frequency, experienced more degradation than the other two ROs. This visually confirms our earlier observation that heating affects ROs more significantly at higher frequencies than at lower ones.

5.2. Delay-based detector analysis against heating

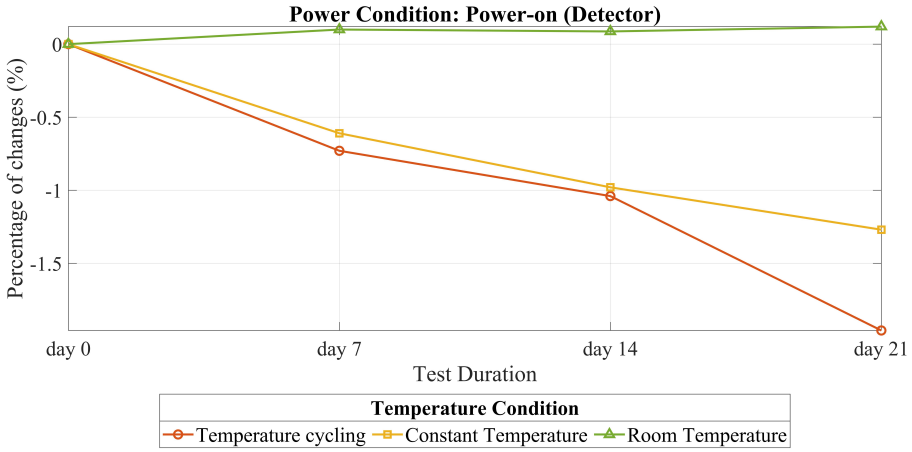
As we explained earlier, we considered three different temperature conditions and three power conditions for the detector. Figure. 10 shows all these scenarios for our detector. In part 10a of the figure, we can see the scenario where the detector is powered on under the three temperature conditions. Similarly, parts 10b and 10c demonstrate the scenarios in which the detector is powered off and the clock is freezing, respectively.

In all power scenarios, room temperature serves as a useful reference point to compare the the results of heating and non-heating conditions. As depicted in Figure. 10b, when the circuit's power is off, both the constant temperature and temperature cycling have a small impact. However, a comparison with the reference (room temperature) reveals an observable effect in the power-off scenario with constant and cycling temperatures. In the power-off attack scenario, **the constant temperature has a greater impact than temperature cycling due to its sustained influence on the system**. Constant temperature maintains a stable condition that can cause more pronounced and consistent changes in the circuit's behavior during the power-off attack. And since no study has been done on POTA, this issue may be related to the physical characteristics of the chip, which are out of the scope of this study. But for other scenarios (i.e., power on and clock freezing), temperature cycling has more effect than constant temperature.

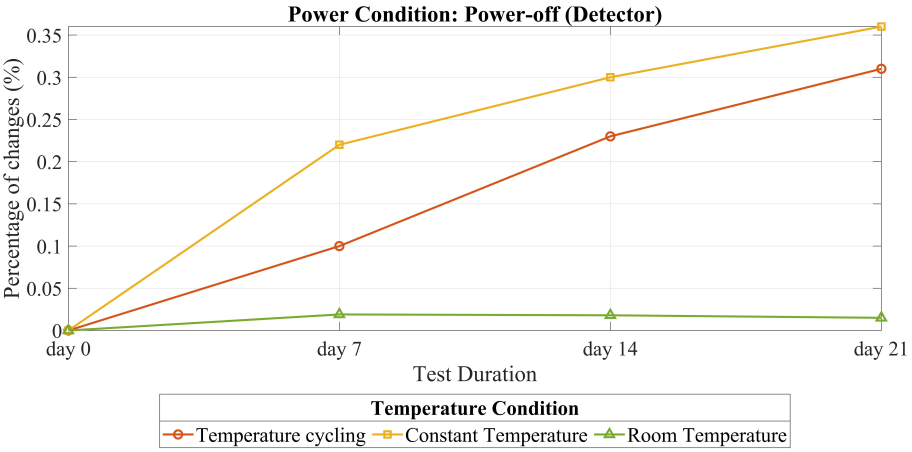
As indicated in Table 3, implementing clock freezing across three temperature scenarios (room temperature, constant temperature, and temperature cycling) has a greater impact on the activation of the detector alarm compared to power-off and power-on power conditions.

It appears logical and normal that the impact of heating during the power-off state is less than that of clock freezing. As explained earlier, we can simulate the heating effect through aging. The primary aging factor is electrical stress on the transistor, Since there is no electrical stress on the transistor in the power-off state, this observation is expected.

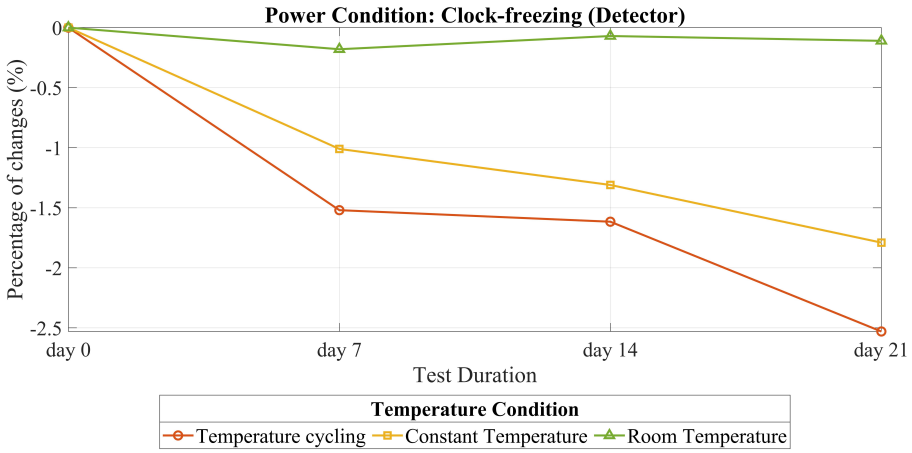
In comparison to the power-on state, clock freezing has a more pronounced effect. This concept can be modeled using Bias Temperature Instability (BTI) effects. As depicted



(a) Power-On

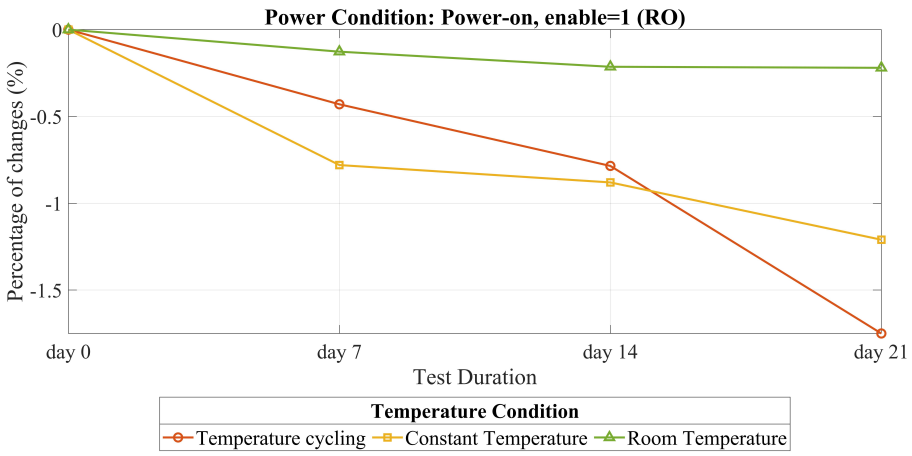


(b) Power-Off

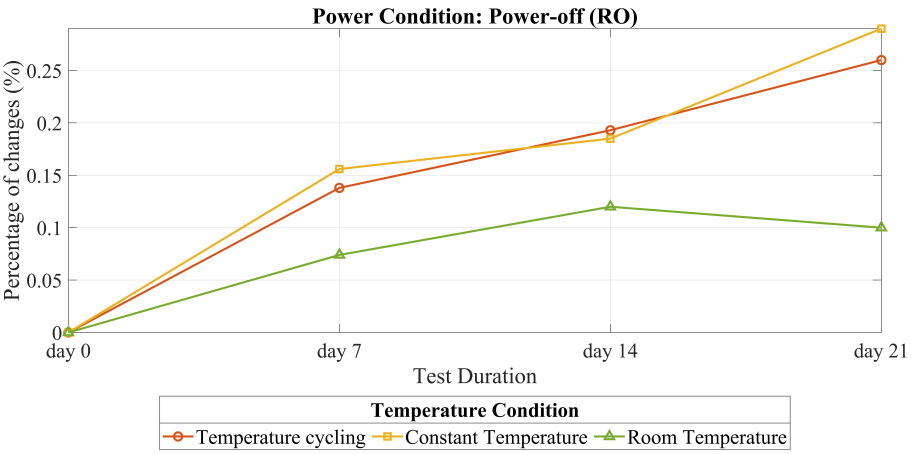


(c) Clock-freezing

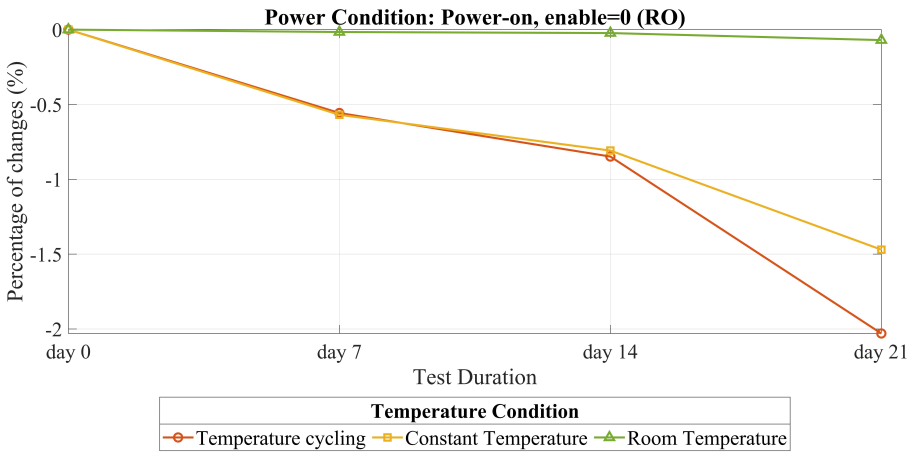
Figure 10. All of the Temperature and Power conditions for the delay-based detector



(a) Power-On, enable = 1



(b) Power-Off



(c) power-on, enable = 0

Figure 11. All of the Temperature and Power conditions for the RO

in Figure. 3, BTI involves two phases: stress and recovery. In the recovery phase, some of the degradation that occurred during the stress phase is recovered. In clock freezing, our clock remains constant, eliminating any clock edges and preventing oscillation between zero and one. Consequently, there is no switching for certain transistors. Therefore, we can conclude that aging in clock freezing results in more degradation compared to power-on. Additionally, in the context of heating, it is observed that clock freezing has a more substantial effect than power-on. This concept is shown in Figures 10a, 10b and10c.

5.3. Ring Oscillator (RO) analysis against heating

Figure. 11 displays how heating over 21 days affects RO. Notably, the figure reveals that the impact on POTA on RO is small but observable, similar to the detector. An important observation here is that **clock freezing has a more significant impact on both the RO and detector compared to other scenarios.** This is because when transistors remain in the same state for extended periods without switching between on and off, they become more susceptible to aging, which can accelerate aging effects such as BTI. Consequently, we anticipate that clock freezing would have a greater effect on aging than scenarios involving power-on (en = 1 in RO). In simpler terms, the freezing of the clock can intensify the aging process, leading to increased degradation compared to other power scenarios. Temperature cycling also leads to greater degradation in this context, mirroring the effects observed in the detector. This similarity in degradation could be attributed to the same underlying reasons observed in the case of the detector. As shown in [32] at a temperature of 90°C (under DC stress and a 1.3Vnom supply voltage), the RO frequency variation is around -3% after one year. Remarkably, after just one month, this variation is approximately -1.5%, which closely corresponds with our findings, despite the authors employing a higher power supply. In this section, we talked about what we found in our experiments. We see that has a very small effect but an observable effect on RO and detector, this type of attack can affect the characteristics of the chip, We can not find any previous works showing this effect. We also noticed something important about freezing the clock signal. Among all the situations we tested, freezing had the biggest effect. This was mainly because of some aging effects, such as BTI. Another thing we found is that when we heat the RO, the ones with higher frequencies get affected more compared to those with lower frequencies. And it's interesting that whether we measure the RO's frequency right after we start it or after 180 minutes, the results are pretty similar. This means the effects are consistent over time.

According to our result and attack model described in Section 3.3, Table 5 presents a comprehensive overview of our attack model from the perspective of the attacker. It outlines three key attack scenarios: Power-on, Power-off, and Clock-freezing, detailing the capabilities required by the attacker for each scenario, along with the corresponding setup procedures. Additionally, the table examines the effects of these attacks on the detector and RO, providing insights into potential security threats posed by each attack type. Through meticulous analysis, the table underscores the critical importance of understanding and mitigating vulnerabilities in integrated circuits to safeguard against malicious exploits.

6. Conclusion

The objective of our study was to evaluate the effects of heating and POTA on digital circuits and the susceptibility of delay-based and RO detectors. These types of attacks can jeopardize chip security since POTAs cannot be detected by active mechanisms.

In the case of a detector safeguarding a secure component, an attacker can manipulate either the circuits or the detector's features by injecting faults (on permanent electrical parameters: for instance, delay modifications) when the chip is turned off. if the detectors are altered, then the attacker can perform other attacks undetected. Our investigation has demonstrated that POTAs can impact circuitry and detectors, leading to an increase in false negatives.

Table 5. Summary of Our Attack Model from the Attacker's Perspective.

	Attacker Perspective		
	Power-on	**Power-off**	**Clock-freezing**
Capabilities	Requires physical access to the target and ability to heat it at constant or cycling temperatures.	Requires physical access to the target, disconnect the power supply, and ability to apply constant or cycling temperature.	Requires physical access to the target, the ability to freeze the clock, and the ability to apply constant or cycling temperature
Attack Setup	Heating entire chip space, either maintaining a constant temperature of 96°C or cycling between 0°C and 96°C over 21 days.	Heating entire chip space, either maintaining a constant temperature of 96°C or cycling between 0°C and 96°C over 21 days. Turn off the target system.	Heating entire chip space, either maintaining a constant temperature of 96°C or cycling between 0°C and 96°C over 21 days. Freeze the clock signal for the detector and disable oscillation for RO.
Effect on detector	For temperature cycling and constant temperature, the alarm activation changes by **-1.98%** and **-1.27%**, respectively.	For temperature cycling and constant temperature, the alarm activation changes by **+0.31%** and **+0.36%**, respectively.	For temperature cycling and constant temperature, the alarm activation changes by **-2.53%** and **-1.79%**, respectively.
Effect on RO	Cycling and maintaining constant temperature can reduce the RO frequency by **-1.75%** and **-1.21%**, respectively.	Cycling and maintaining constant temperature can lead to an increase in the RO frequency by **+0.26%** and **+0.29%**, respectively.	Cycling and maintaining constant temperature can reduce the RO frequency by **-2.03%** and **-1.47%**, respectively.
Security Threats	This type of attack has the potential to increase false positives in delay-based detectors, resulting in early activation in comparison to normal functioning and increasing false alarms. The RO frequency decreases; for detectors that are based on the RO, it may cause security concerns.	This type of attack can **increase false negatives**, which means that the alarm can be active later than in normal mode, which is useful from the attacker's point of view. The RO frequency decreases; for detectors that are based on the RO, it may cause security concerns.	This type of attack has the potential to increase false positives in delay-based detectors, resulting in early activation in comparison to normal functioning and increasing false alarms. The RO frequency decreases; for detectors that are based on the RO, it may cause security concerns.

In a detector, if we can activate the alarm earlier than normal, it means that we increase false positives, and when we activate the alarm after normal activation, it means that we increase false negatives. Increasing false negative expansion, unlike increasing false positives, can cause security threats and attackers to enter the system; therefore, it is very important and fundamental to consider this type of attack. Our result shows that with clock freezing and power on, unlike POTA, with heating, we can increase the false positive

of delay-based detectors. This effect on delayed-based detectors will not create any security threat and can only increase false alarms with clock freezing and power on. In our future research, we intend to assess this type of attack for an extended period and on a wider variety of detectors. In particular, we will look for detectors impacted by POTAs and clock-freezing attacks to create false negatives.

Another potential future work for this study is the implementation of self-testing mechanisms. We have seen that POTA has an effect, so we should protect our system against this type of attack by incorporating a dedicated circuitry to check the inetrgity of the sensor after power-up. One way to do this is to use self-testing in our chip to check the characteristic variation every time after activation.

More specifically, within the context of the POP project, our plan is to use a laser and produce a dedicated test chip to conduct comparable experiments. These experiments will involve localized temperature attacks on various digital and analog circuits, including detectors.

7. Acknowledgement

This work was supported by a research grant from the French Agence Nationale de la Recherche (POP project, ANR-21-CE39-0004).

References

1. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the Annual international cryptology conference. Springer, 1999, pp. 388–397.
2. Boneh, D.; DeMillo, R.A.; Lipton, R.J. On the importance of checking cryptographic protocols for faults. In Proceedings of the International conference on the theory and applications of cryptographic techniques. Springer, 1997, pp. 37–51.
3. Breier, J.; Bhasin, S.; He, W. An electromagnetic fault injection sensor using Hogge phase-detector. In Proceedings of the 2017 18th International Symposium on Quality Electronic Design (ISQED), 2017, pp. 307–312. https://doi.org/10.1109/ISQED.2017.7918333.
4. Muttaki, M.R.; Zhang, T.; Tehranipoor, M.; Farahmandi, F. FTC: A Universal Sensor for Fault Injection Attack Detection. In Proceedings of the 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2022, pp. 117–120. https://doi.org/10.1109/HOST54066.2022.9840177.
5. El-Baze, D.; Rigaud, J.B.; Maurine, P. An embedded digital sensor against EM and BB fault injection. In Proceedings of the 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE, 2016, pp. 78–86.
6. Igarashi, H.; Shi, Y.; Yanagisawa, M.; Togawa, N. Concurrent faulty clock detection for crypto circuits against clock glitch based DFA. In Proceedings of the 2013 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2013, pp. 1432–1435.
7. Yanci, A.G.; Pickles, S.; Arslan, T. Characterization of a voltage glitch attack detector for secure devices. In Proceedings of the 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security. IEEE, 2009, pp. 91–96.
8. Richter-Brockmann, J.; Shahmirzadi, A.R.; Sasdrich, P.; Moradi, A.; Güneysu, T. Fiver–robust verification of countermeasures against fault injections. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2021**, pp. 447–473.
9. Selmane, N.; Bhasin, S.; Guilley, S.; Danger, J.L. Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks. *IET information security* **2011**, *5*, 181–190.
10. Grandamme, P.; Tissot, P.A.; Bossuet, L.; Dutertre, J.M.; Colombier, B.; Grosso, V. Switching Off your Device Does Not Protect Against Fault Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2024**, *2024*, 425–450. https://doi.org/10.46586/tches.v2024.i4.425-450.
11. Selmane, N.; Bhasin, S.; Guilley, S.; Danger, J.L. Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks. *IET information security* **2011**, *5*, 181–190.
12. Beckers, A.; Guilley, S.; Maurine, P.; O'Flynn, C.; Picek, S. (Adversarial) Electromagnetic Disturbance in the Industry. *IEEE Transactions on Computers* **2023**, *72*, 414–422. https://doi.org/10.1109/TC.2022.3224373.
13. Anik, M.T.H.; Danger, J.L.; Guilley, S.; Karimi, N. Detecting Failures and Attacks via Digital Sensors. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **2021**, *40*, 1315–1326. https://doi.org/10.1109/TCAD.2020.3020921.
14. Nabhan, R.; Dutertre, J.M.; Rigaud, J.B.; Danger, J.L.; Sauvage, L. EM Fault Injection-Induced Clock Glitches: From Mechanism Analysis to Novel Sensor Design. In Proceedings of the 2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS). IEEE, 2024, pp. 1–7.
15. Askeland, A.; Nikova, S.; Nikov, V. Who Watches the Watchers: Attacking Glitch Detection Circuits. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2024**, *2024*, 157–179.
16. Zussa, L.; Dehbaoui, A.; Tobich, K.; Dutertre, J.M.; Maurine, P.; Guillaume-Sage, L.; Clediere, J.; Tria, A. Efficiency of a glitch detector against electromagnetic fault injection. In Proceedings of the 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2014, pp. 1–6.

17. Zhang, M.; Liu, Q. A Digital and Lightweight Delay-Based Detector against Fault Injection Attacks. In Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2021, pp. 1–5.
18. Endo, S.; Li, Y.; Homma, N.; Sakiyama, K.; Ohta, K.; Fujimoto, D.; Nagata, M.; Katashita, T.; Danger, J.L.; Aoki, T. A silicon-level countermeasure against fault sensitivity analysis and its evaluation. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* **2014**, *23*, 1429–1438.
19. Endo, S.; Li, Y.; Homma, N.; Sakiyama, K.; Ohta, K.; Aoki, T. An efficient countermeasure against fault sensitivity analysis using configurable delay blocks. In Proceedings of the 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography. IEEE, 2012, pp. 95–102.
20. He, W.; Breier, J.; Bhasin, S. Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks. In Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, 2016, pp. 27–46.
21. Deshpande, C.; Yuce, B.; Ghalaty, N.F.; Ganta, D.; Schaumont, P.; Nazhandali, L. A configurable and lightweight timing monitor for fault attack detection. In Proceedings of the 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2016, pp. 461–466.
22. Askeland, A.; Nikova, S.; Nikov, V. Who Watches the Watchers: Attacking Glitch Detection Circuits. Cryptology ePrint Archive, Paper 2023/1647, 2023. https://eprint.iacr.org/2023/1647.
23. Power supply glitch induced faults on FPGA: An in-depth analysis of the injection mechanism.
24. Zussa, L.; Dehbaoui, A.; Tobich, K.; Dutertre, J.M.; Maurine, P.; Guillaume-Sage, L.; Clediere, J.; Tria, A. Efficiency of a glitch detector against electromagnetic fault injection. In Proceedings of the 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2014, pp. 1–6.
25. Nemiroff, D.; Tokunaga, C. Fault-Injection Countermeasures, Deployed at Scale. In Proceedings of the 2024 IEEE Physical Assurance and Inspection of Electronics (PAINE). IEEE, 2024, pp. 1–7.
26. Ghaderi, Z.; Ebrahimi, M.; Navabi, Z.; Bozorgzadeh, E.; Bagherzadeh, N. SENSIBle: A Highly Scalable SENsor DeSIgn for Path-Based Age Monitoring in FPGAs. *IEEE Transactions on Computers* **2017**, *66*, 919–926. https://doi.org/10.1109/TC.2016.2622688.
27. Ghaderi, Z.; Bagherzadeh, N.; Albaqsami, A. STABLE: Stress-Aware Boolean Matching to Mitigate BTI-Induced SNM Reduction in SRAM-Based FPGAs. *IEEE Transactions on Computers* **2018**, *67*, 102–114. https://doi.org/10.1109/TC.2017.2725952.
28. Kraak, D.; Taouil, M.; Hamdioui, S.; Weckx, P.; Catthoor, F.; Chatterjee, A.; Singh, A.; Wunderlich, H.J.; Karimi, N. Device aging: A reliability and security concern. In Proceedings of the 2018 IEEE 23rd European Test Symposium (ETS), 2018, pp. 1–10. https://doi.org/10.1109/ETS.2018.8400702.
29. Douadi, A.; Di Natale, G.; Maistri, P.; Vatajelu, I.; Beroulle, V. A Study of High Temperature Effects on Ring Oscillator based Physical Unclonable Functions. In Proceedings of the 29th IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS 2023), Chania, Greece, 2023.
30. Keane, J.; Wang, X.; Persaud, D.; Kim, C.H. An all-in-one silicon odometer for separately monitoring HCI, BTI, and TDDB. *IEEE Journal of Solid-State Circuits* **2010**, *45*, 817–829.
31. Zhong, J.; Wang, J.; Ding, H. Temperature-variation-based hardware Trojan detection through ring oscillator. *Electronics Letters* **2016**, *52*, 1302–1304.
32. Coutet, J. Étude de la fiabilité et des mécanismes de dégradation dans les composants numériques de dernière génération. Theses, Université de Bordeaux, 2020.