Experimental Evaluation of Delayed-based Detectors against Power-off Attack

Maryam Esmaeilian*, Aghiles Douadi‡, Zahra Kazemi*, Vincent Beroulle*, Amir-Pasha Mirbaha*, Mahdi Fazeli†, Elena Ioana Vatajelu‡, Paolo Maistri‡, Giorgio Di Natale‡
*Univ. Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France
†, School of Information Technology, Halmstad University, Halmstad, Sweden
‡Univ. Grenoble Alpes, CNRS, Grenoble INP1 , TIMA, 38000 Grenoble, France

***Abstract*—Embedded systems are vulnerable to significant security threats from Fault Injection Attacks (FIAs), which allow attackers to gain access to confidential information. While various attack detectors have been proposed in the literature to detect different types of FIAs, these detectors themselves are susceptible to such attacks and can be compromised. Hence, the robustness of these detectors is critical in maintaining the security of embedded systems. The focus of this study is to evaluate the robustness of digital circuits and delay-based digital detectors against a new type of FIA called Power-Off Attack (POA). POA occurs when the power to the chip is turned off, and the detectors are not active. Following a POA attack, the circuit or its detectors may not function properly when the power is turned back on, which can allow other attacks to be applied without being detected if the detectors are less sensitive. This study implements two detectors on Xilinx Artix-7 FPGAs and examines the impact of heating cycles on detector characteristics when the FPGA is in various states, including power-off, power-on, and inactive states (such as clock-freezing mode). Our experiments reveal that heating cycles in power-off mode can alter the FPGA component delays and the accuracy of its detectors, which highlights the vulnerability of these systems to POA and potential issues for embedded system security.**

***Index Terms*—hardware security, fault attack, power-off attack, temperature attack, secure circuit design, delay-based detectors**

I. Introduction

Nowadays, the use of electronic devices in our daily life is growing fast. These devices are employed in security applications, such as authentication applications. One of the most important concerns about such security applications is their existing vulnerabilities against different attacks. Among these attacks, Hardware Attacks (HAs) against embedded devices have attracted a lot of attention. Side Channel Attacks (SCA) [1] and Fault Injection Attacks (FIA) [2] are two types of these attacks. SCAs exploit the leaked information from the devices, such as time and power consumption, to extract sensitive data. On the other hand, FIAs involve the attacker attempting to manipulate the system's input or environmental conditions, such as temperature, to cause unintended behavior and extract confidential information.

The techniques for performing Fault Injection Attacks (FIAs) are becoming increasingly more advanced and powerful. Nevertheless, numerous security experts and designers are actively developing protection and detection mechanisms to mitigate the risks associated with such attacks. For instance, various digital and analog detectors have been proposed to detect the attack before it causes wrong behavior in the devices [3] [4]. The recent works are mostly focused on digital detectors because they can be easily calibrated and placed close to the 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.

Therefore, detectors are used to protect the system from security attacks such as FIA. However, it is critical to ensure the protection of these detectors themselves against potential FIAs. There is a bunch of research work on the vulnerability of detectors [8] [9] to various types of Fault Injection Attacks (FIAs) as well as methods for protecting them. All of them assume that the detector is connected to the power supply, but none of them have been evaluated against FIA when the power is off. This new type of FIA, which we call a Power-Off Attack (POA), 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, when the detectors are off. Such changes can adversely impact the key detector features, such as the detection thresholds, leading to a modification in the false positive and false negative detection rates. Alterations in the rate of false positives can impact the accuracy of the detector, while an increase in the rate of false negatives may lead to security risks and grant unauthorized access to the system to attackers.

The aim of this study is to assess how environmental changes, specifically heating, impact the properties of simple digital detectors when power is not supplied. In order to conduct this experiment, we subjected the chip to varying periods of heating, as certain Fault Injection Attacks (FIAs) like Laser Fault Injection (LFI) can lead to temperature elevation. By applying heat, 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: Section II, we will review state of the art and related to our work. In Section III, the structure and methodology of this study will be explained. Experimental results are presented in section

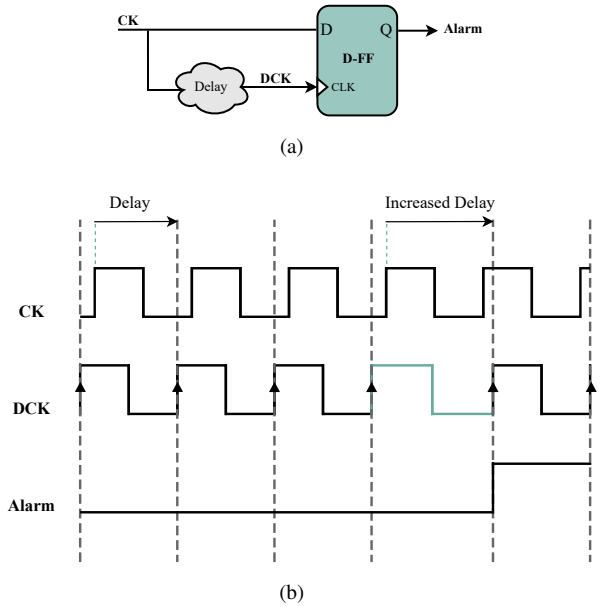

Fig. 1. (a) Schematic diagram and (b) waveforms of the delay-based detector proposed in [10]

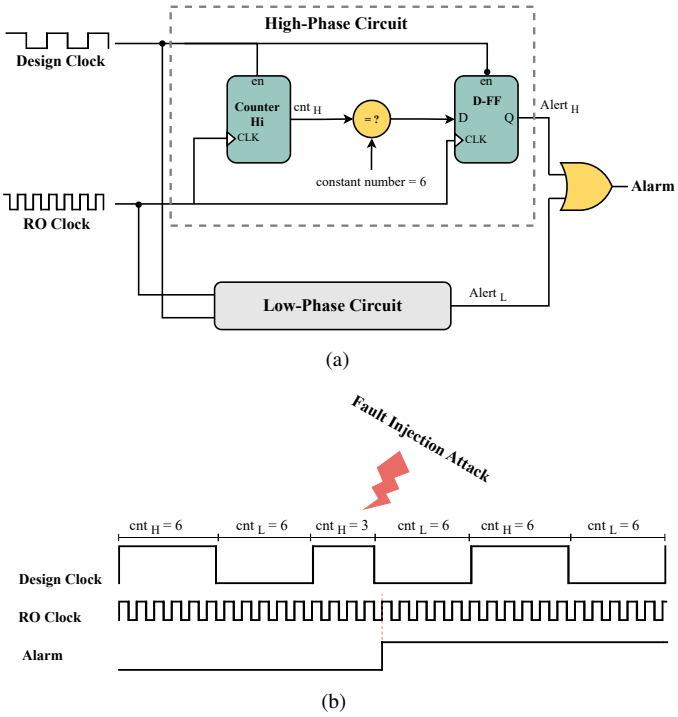

Fig. 2. (a) Schematic diagram and (b) waveforms of the counter-based detector proposed in [18]

IV. In section V, we discuss the results. And at the end of this paper in section VI we conclude and give the perspectives for future works.

II. State-of-the-Art

Several methods have been introduced in the literature to protect devices against FIAs. These techniques can be based on redundancy at different levels or techniques based on the use of sensors. The advantage of using redundancy is that it makes it possible to detect faults independently of the FI technique, but the main disadvantage of this method is that this technique cannot capture all possible faults [11]. The second technique is to use fault detection sensors, also known as detectors. Detectors can be divided into 2 categories, digital detectors, and analog detectors, the analog type as its name suggests, uses analog sources to detect FIA, in [12] a type of analog detector is proposed that uses 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.

There are different digital FIA detectors that are proposed in the literature. One of the most popular designs, named Delayed-based detector, has been suggested in [10]. This detector is based on the timing constraints of the synchronous systems equation (1). In order to guarantee that the processors will 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 processor will not have enough time to perform its operations.

$$T_{Clock} \geq T_{propagationDelay} + T_{Setup} \quad (1)$$

Delayed-based detectors can detect various FIAs, such as clock glitching, under-powering or overheating [13]–[15]. Figure 1 illustrates how this detector compares the delayed clock signal (denoted DCK) with the primary clock signal using a D-FF. If there is a malfunction (e.g., delay variations, clk period decrease), the alarm will be activated. Although delayed-based detectors are simple and efficient against some FIAs, they are impractical when dealing with attacks that have a local effect such as laser or electromagnetic FIAs [16]. Accordingly, other designs have been introduced to improve the detection rates against FIAs. The next category of the proposed detectors is the one that is based on the Ring Oscillators (RO). ROs can be implemented using a closed chain of odd-numbered NOT gates [16]. In this structure, RO alternates between zero and one, so it can be a frequency generator, whose output frequency depends on the number of NOT gates and propagation delays.

The other solution to implement the ROs is to utilize Phase Locked Loop (PLL). This idea has been introduced in [17]. However, the primary issue with this approach is that PLLs are only available on modern FPGAs.

The implemented ROs can be used in a detector design. For instance, as shown in Figure 2 from [18], this detector consists of two high-phase and low-phase circuits, which are used for the one and zero levels of the clock signal, respectively. 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 in the case of an attack, the number of RO oscillations changes and is not equal to the constant value.

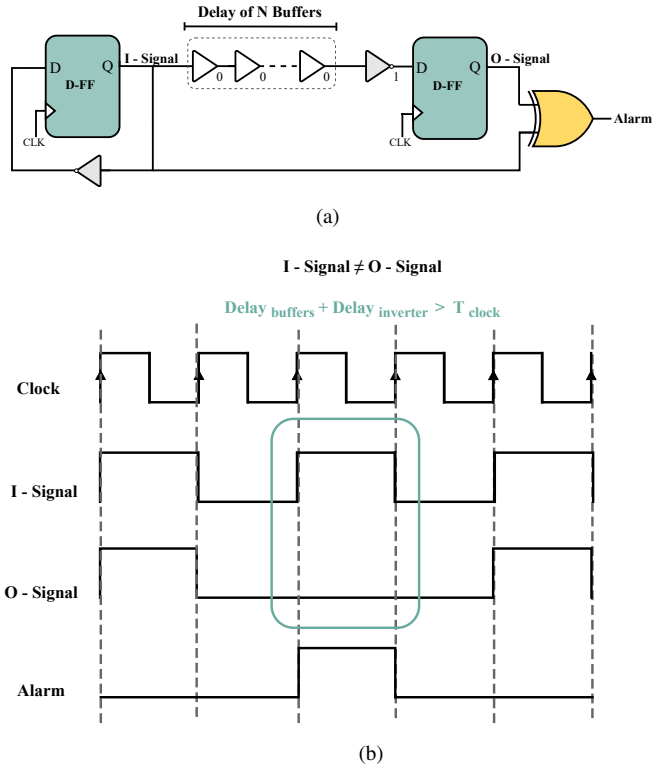

Fig. 3. (a) Schematic and (b) waveforms of the delay-based detector proposed in [19]

As a result, the alarm will be activated. Since this detector uses two separate circuits for the zero level and a clock, it can speed up fault detection, so it will have higher accuracy than delay-based detectors. Hence, it can be used to detect local faults such as lasers and electromagnetic FIAs.

As mentioned in the previous section, the goal of this study is to evaluate how high temperatures, when the power is off, affect the sensitivity of the detectors. In Section III, more details about the implementation and test scenarios are discussed.

III. Our Methodology

In this section, our goal is to explain the details of the Device Under Test (DUT) and the method of our experiment.

The goal of this study is to evaluate how high temperatures when the power is off, affect the sensitivity of the detectors. To achieve this objective, we have selected two main detector designs for our experiment.

We chose to evaluate the delay-based detector proposed in [10] as our first detector design because it is less complex to implement than other types. Figure 3(a) illustrates the delay-based detector, which operates by keeping the alarm inactive while the output of the two flip-flops (represented as the O-signal and I-signal in Figure 3) are equal. But, when these two signals are complementary, the alarm will be activated. However, 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 (2), as long as this equation is true, the alarm is not activated.

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

Fault Injection Attacks (FIAs), such as heating and laser, can increase the delay of logic gates, thereby modifying Equation (2) and triggering this detector. The accuracy of the detector increases as the delay caused by the buffers approaches the clock period. However, this also increases the detector's sensitivity and 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 for implementing this detector. Since the normal period is 100 ns, we need to choose the number of buffers whose delay is close to this value. To determine this, we conducted post-implementation simulations using Vivado software and found that the delay of a single buffer was 0.450 ns. We then gradually increased the number of buffers until their total delay reached 100 ns. The delay increases linearly with each additional buffer. After extensive testing, we discovered that 194 buffers are required to achieve a delay of 97.89 ns, which is very close to the normal period. This ensures that the detector remains inactive during normal operation but can detect any attacks that modify the delay of the logic gates. This detector was synthesized using a VHDL RTL description in the Xilinx Vivado design suite and implemented on a Xilinx Artix-7 FPGA using a BASYS-3 board. We determined that the threshold detection frequency of this detector is 17.2 MHz.

As many detectors rely on Ring Oscillators (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. To conduct our experiment, we will focus on three main scenarios, which are described in detail in the following sections.

- *First scenario: power-off*

  DUTs are switched off and not connected to any power source.
- *Second scenario: power-on*

  DUTs are on. This scenario helps us to compare the results of this scenario with the power-off scenario.
- *Third scenario: clock freezing*

  The delay-based detector clock signal is frozen (i.e., does not have any edge). The RO enable signal is zeroed (i.e., the RO is inactive).

In the next section, the experimental setup will be explained in detail.

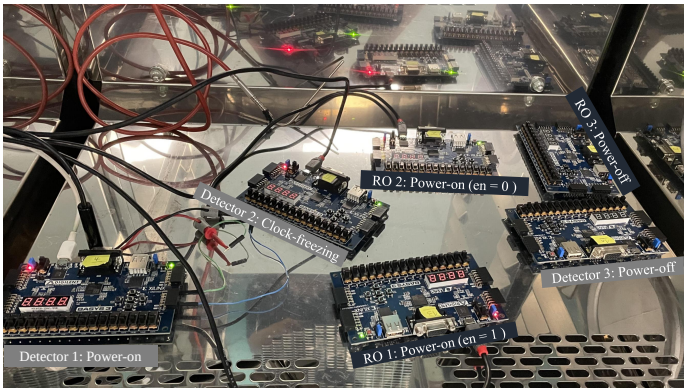

Fig. 4. Experimental setup in the climatic chamber: 3 FPGAs with detectors and 3 FPGAs with ROs using 3 different power states; power-on, clock-freezing (or enable=0) and power-off.

IV. Experiments and Results

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.

A. 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 simple Ring Oscillator (RO) when the power is off. For each DUT, we examined the three previous scenarios. We implemented each scenario on a separate BASYS-3 board, as shown in Figure 4, which contains a Xilinx Artix-7 chip.

To evaluate the DUTs against power-off attacks, it is crucial to ensure that the detector operates correctly when the device is powered on. To achieve this, we conducted an overclocking 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 conduct the practical evaluation, we utilized the Votsch VC 0018 climate test system chamber, capable of producing heat up to +95°C. 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. To evaluate the detector's response time, we utilized a simple LED to measure the alarm signal's activation time, while for the RO, we used a frequency meter. It is important to mention that in order to determine the detection threshold accurately, we performed 10 successive measurements on each detector (in the different FPGAs) before averaging the results.

TABLE I
Results of a heating delay based detector

Percent change of Alarm activation (%)			
Time under test	power-on	clock-freezing	power-off
Initial value	0	0	0
After 1-day	0	0	-0.3
After 2-day	-1.7	-3.2	-0.2
After 7-day	-6.4	-4.2	-1.3

TABLE II
Results of a heating RO

Percent change of Ring Oscillator(RO) frequency (%)			
Time under test	power-on (en=1)	clock-freezing (en=0)	power-off
Initial value	0	0	0
After 1-day	0.2	-0.5	0
After 2-day	-1.0	-0.5	0
After 7-day	-1.0	-0.9	-0.7

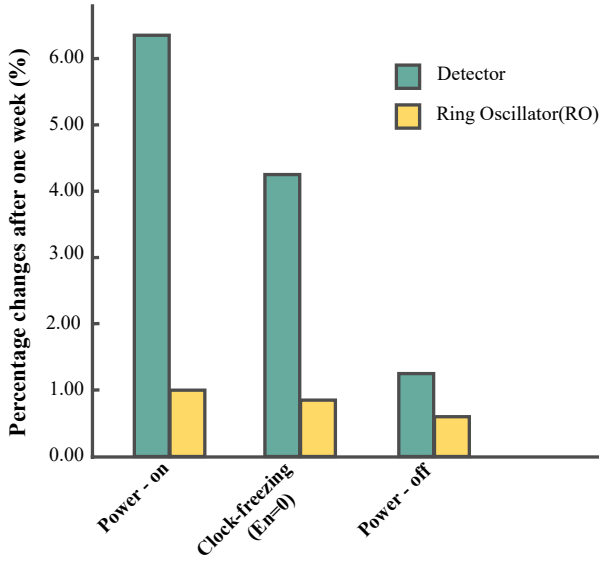

Fig. 5. Percentages decrease of ROs frequency and alarm activation threshold after one week of heating

All measurements were taken with the chips held at the same temperature, namely normal room temperature. This requires removing the FPGAs from the environmental chamber and waiting long enough for the FPGA temperature to return to the normal temperature. The temperature is checked using an infrared thermometer that measures the temperature at the surface of the FPGA packages. Additionally, as a precautionary measure, we waited for an extra hour after returning to the normal temperature measured by the thermometer to allow the internal temperature of the FPGAs to return to normal. Removing the DUT every day reduces the duration of exposure (about 2 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.

B. Experimental Results

Table I and Table II display the results of the test conducted for a period of one week, where all measurements were taken with the chips held at the same temperature, namely room temperature. In these two tables, the variations in activation thresholds of the two preceding detectors are represented. These variations are expressed as a percentage and are given after 1 day, 2 days, and 7 days in the climatic chamber. The 3 previously presented scenarios are used (power-on, clock-freezing, and power-off). 3 FPGAs are used for each type of detector in these 3 scenarios. This temperature is the maximum temperature that the climatic 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 chamber, a laser could certainly create the same variations, perhaps more quickly by applying higher temperatures.

V. DISCUSSION

Heating cycles are effective in reducing both the delay-based detector's threshold detection frequency and the ring oscillator's frequency for all the scenarios including the power-off mode. But, for all scenarios, the ring oscillator design is less affected than the delay-based detector. For instance, in power-on mode after seven days, the threshold detection decrease is 6.4% rather than the ring oscillator frequency decrease is 1%. In power-off mode after seven days, the threshold detection decrease is only 1.3% rather than the ring oscillator frequency decrease is 0.7%. Figure 5 illustrates that even if the power-on mode causes the most damage compared to other scenarios, the power-off mode has also effects. Finally, the clock-freezing mode has a lesser effect than the power-on mode and a higher effect than the power-off mode. We believe that, in clock-freezing mode, as transistors remain stable (i.e., permanently open or close), this implies a Negative Bias Temperature Instability (NBTI) [20] affecting only a part of the PMOS transistors (the always opened transistors). As the effect of NBTI is non-linear with the duration, this makes the aging effects lesser in this mode than in the power-on state (with a living clock) where all the PMOS transistors are then impacted by NBTI. Note that we do not know which effect is observed during the power-off mode where NBTI can not be responsible as no power is applied. As far as we know, no paper has described the effect of heating on power-off circuits.

In general, this type of attack can affect the detectors in two ways, by either increasing false negatives or false positives. But, on our two delay-based detectors, we only observe an increase in false positives. Of course, an attacker's primary goal is most often to increase false negatives to access the system without triggering the alarm.

VI. CONCLUSION AND PERSPECTIVES

The objective of our study was to evaluate the effects of power-off attacks on digital circuits and the susceptibility of delay-based detectors. These types of attacks can jeopardize chip security since POAs 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 power-off attacks can impact circuitry and detectors, leading to false alarms, but they do not compromise the security of the system as no false negatives are created. However, it is possible that on other detectors with different structures, this attack could produce false negatives and thus create a security threat for embedded systems. 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 POAs to create false negatives.

More specifically, within the context of the POP project (mentioned in the acknowledgment section), 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.

VII. ACKNOWLEDGEMENT

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

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.

[2] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *International conference on the theory and applications of cryptographic techniques*. Springer, 1997, pp. 37–51.

[3] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using hogge phase-detector," in *2017 18th International Symposium on Quality Electronic Design (ISQED)*, 2017, pp. 307–312.

[4] M. R. Muttaki, T. Zhang, M. Tehranipoor, and F. Farahmandi, "Ftc: A universal sensor for fault injection attack detection," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2022, pp. 117–120.

[5] D. El-Baze, J.-B. Rigaud, and P. Maurine, "An embedded digital sensor against em and bb fault injection," in *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2016, pp. 78–86.

[6] H. Igarashi, Y. Shi, M. Yanagisawa, and N. Togawa, "Concurrent faulty clock detection for crypto circuits against clock glitch based dfa," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2013, pp. 1432–1435.

[7] A. G. Yanci, S. Pickles, and T. Arslan, "Characterization of a voltage glitch attack detector for secure devices," in *2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security*. IEEE, 2009, pp. 91–96.

[8] J. Richter-Brockmann, A. R. Shahmirzadi, P. Sasdrich, A. Moradi, and T. Güneysu, "Fiver–robust verification of countermeasures against fault injections," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 447–473, 2021.

[9] N. Selmane, S. Bhasin, S. Guilley, and J.-L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET information security*, vol. 5, no. 4, pp. 181–190, 2011.

[10] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[11] A. Beckers, S. Guilley, P. Maurine, C. O'Flynn, and S. Picek, "(adversarial) electromagnetic disturbance in the industry," *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 414–422, 2023.

[12] M. T. H. Anik, J.-L. Danger, S. Guilley, and N. Karimi, "Detecting failures and attacks via digital sensors," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 7, pp. 1315–1326, 2021.

[13] M. Zhang and Q. Liu, "A digital and lightweight delay-based detector against fault injection attacks," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[14] S. Endo, Y. Li, N. Homma, K. Sakiyama, K. Ohta, D. Fujimoto, M. Nagata, T. Katashita, J.-L. Danger, and T. Aoki, "A silicon-level countermeasure against fault sensitivity analysis and its evaluation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 8, pp. 1429–1438, 2014.

[15] S. Endo, Y. Li, N. Homma, K. Sakiyama, K. Ohta, and T. Aoki, "An efficient countermeasure against fault sensitivity analysis using configurable delay blocks," in *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2012, pp. 95–102.

[16] W. He, J. Breier, and S. Bhasin, "Cheap and cheerful: A low-cost digital sensor for detecting laser fault injection attacks," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, 2016, pp. 27–46.

[17] N. Miura, Z. Najm, W. He, S. Bhasin, X. T. Ngo, M. Nagata, and J.-L. Danger, "Pll to the rescue: a novel em fault countermeasure," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. IEEE, 2016, pp. 1–6.

[18] C. Deshpande, B. Yuce, N. F. Ghalaty, D. Ganta, P. Schaumont, and L. Nazhandali, "A configurable and lightweight timing monitor for fault attack detection," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2016, pp. 461–466.

[19] N. Selmane, S. Bhasin, S. Guilley, and J.-L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET information security*, vol. 5, no. 4, pp. 181–190, 2011.

[20] Z. Ghaderi, *Aging-induced Performance Degradation: Monitoring and Mitigation*. University of California, Irvine, 2017.

[21] V. Beroulle, B. colombie, G. Natale, P. Maistri, and I. Vatajelu, "Design and evaluation of countermeasures against power-o laser fault injection attacks," https://tima.univ-grenoble-alpes.fr/sites/tima/files/Mediatheque/Jobs/PhD/sujet$_t hese_p op.pdf$, $May 2022$.