# Simulation Methodology for Assessing X-Ray Effects on Digital Circuits

Nasr-Eddine Ouldei Tebina, Nacer-Eddine Zergainoh, Guillaume Hubert, Paolo Maistri

# Simulation Methodology for Assessing X-Ray Effects on Digital Circuits

Nasr-eddine Ouldei Tebina [1], Nacer-Eddine Zergainoh[1], Guillaume Hubert[2], and Paolo Maistri[1]

[1]Univ Grenoble Alpes, CNRS, Grenoble INP*, TIMA, 38000 Grenoble, France
[2]ONERA DPHY, University of Toulouse, 31055 Toulouse, France

***Abstract*—Recently, X-Rays have proven to be an interesting and feasible mean to perform fault injection attacks against secure implementations. Their wavelength allows targeting single elements even with most recent fabrication technologies, and their high penetration power does not demand to invasively prepare the device for the attack. Unlike operations in harsh environment, a malicious attacker can choose the targeted region at will, from a single cell up to large regions. This aspect forces designers to consider hardening against X-Rays under a different perspective. In this work, we will present a design-time simulation flow, that addresses how the electrical characteristics of the logic are changed when irradiated, from the perspective of injected faults and of biased power consumption.**

***Index Terms*—leakage, TID, Spectre, Secure designs**

## I. Introduction

It is well-known that a huge amount of digital information requires some protection from unauthorized use, either in terms of confidentiality or authentication features. Several cryptographic algorithms have been proposed from the very beginning in order to fulfill these requirements.Nonetheless, algorithms have to be implemented either in software or hardware, which can be vulnerable to physical attacks. Among them, Fault Attacks constitute a powerful and effective way to extract information from a system. These attacks are based on the fact that the device, subject to external perturbations, may exhibit an altered behavior (for example, a corrupted output) that might be leveraged to extract confidential data [1], [2]. Several techniques exist, from perturbation on global inputs (clock or power supply [3]), to more localized ones such as laser [4] or electromagnetic [5] pulses.

Recently, X-Ray illumination has been proposed as a mean to inject calibrated faults into a device as a security threat. Although already known and used in the spatial domain to reproduce harsh environments (eg, natural radiations), their application for physical attacks has been first proposed in [6], where the authors exploited a nanofocused beam available at a synchrotron facility to target a single transistor. Later, the same device was attacked using a laboratory source [7], demonstrating that attacks are possible, at a larger scale, even without very high-end facilities.

The challenges that X-Ray Fault Injection (XRFI) presents to secure designers are different from what they had to deal with so far. Unlike common fault injection techniques, the threat model of X-Rays is completely different on both spatial and temporal scale. Glitches and laser or EM pulses are precisely synchronized in time with the target device, and usually limited to one or very few clock cycles. XRFI, on the other hand, is a slow and continuous process, progressively affecting the characteristics of the circuit. Most importantly, the spatial granularity of XRFI may be completely tunable by the attacker: the first experiments were mostly focused on very few gates, but in principle the attacker can target specific regions or IPs in the design, under the assumption that the layout can be approximately known. As a term of comparison, the attacker has a complete control on the fault location when employing laser or EM pulses, but the targeted region is limited (due to resolution and focusing issues, and to the number of possible spots); no spatial control at all is possible when using glitches, where fault propagation is largely driven by layout and fabrication process. Protecting against XRFI might be achieved through well-known hardening approaches [8], but at a large cost and with little knowledge of new potential vulnerabilities.

For these reasons, it is important for the designer to have the right tools in order to analyse XRFI as soon as possible in the design flow. In this paper, we present a methodology based on Ray-Spect tool [9], targeted at simulating the effects of XRFI with configurable scalability of the targeted region. We will present how the tool can be exploited to simulate, early in the design flow, both the errors induced in the digital logic, as well as the deviations of the electrical characteristics induced by the TID.

The paper is structured as follows. We first introduce in Section II the necessary background on Total Ionizing Radiation (TID) on electronic systems and the state of the art on fault simulation methodologies. In Section III, we describe the simulation model used by the tool and its electrical equivalent. In Section IV, we provide details on the simulation flow used by Ray-Spect. Three use cases of the tool are presented in Section V-A. Finally, in Section VI, we summarize the main ideas discussed in this paper.

## II. Background

### A. TID Effects

It is known that TID radiations such as X-Rays have an impact on the drain current $I_d(V_G)$ characteristic of MOS

*Institute of Engineering Univ. Grenoble Alpes

979-8-3503-1500-4/23/$31.00 ©2023 IEEE

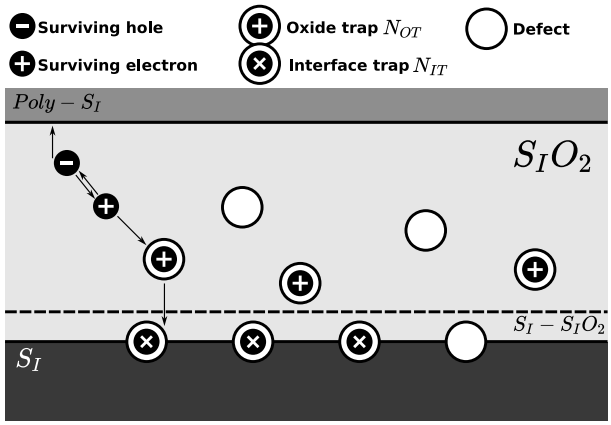



Fig. 1: Hole and interface traps formation in a MOS structure under ionizing radiation

transistors. This impact can be resumed in 3 parametric shifts of the transistor: a shift in the threshold voltage, an increased static leakage current, and a trans-conductance degradation [10]. Hole trapping inside the oxide is the basic mechanism behind these phenomena. Figure 1 shows the basic mechanisms of hole and interface trapping.

The threshold voltage shift effect is a result of positive charge traps induced by the ionizing radiation in the gate oxides. These charges attract negative charge carriers at the canal level leading to lowering the threshold voltage of the N-type MOS, and (negatively) increasing it in case of a P-type MOS. Thus, an NMOS can be made permanently in a conductive state and the PMOS can be made into a permanently blocked state. This is know as the Semi-Permanent Fault Model; the Semi-Permanence property is due to the reversibility of the effect through heat-annealing.

The increased static leakage current effect is due to the TID on the Shallow Trench Isolation (STI) component. It only concerns N-Type transistors since the substrate is P-Type, and N-type parasitic canals can be formed on the STI walls. This leakage can be intra-component, between the source and the drain of the same transistor [11]; it can also be inter-component, as a parasitic path of charge carriers can be formed on the STI connecting two MOS transistors, leading to an increase in the leakage current [12].

The trans-conductance degradation is a result of the buildup of interface traps, which can actively exchange charge carrier with the transistor, and obstruct the movement of charge carriers. Interface traps are much slower to buildup than oxide traps: therefore, this effect is not discussed in this paper since we consider here only freshly irradiated components.

### B. Simulation Tools for Radiation Assessment

Radiation hardening strategies have been developed to overcome single-event transients (SET) and upsets (SEU) triggered in cells, and for mitigating total ionizing dose (TID). Radiation Hardening By Design (RHBD) techniques for TID are only really designed to mitigate effects on parasitic field oxide transistors in the circuit. For SET mitigation, RHBD design techniques can help reduce the probability of SETs being generated and causing errors. Concerning the simulation contribution, development of SEE prediction tools has been a major and growing issue for a few years. The SEMM-2 [13], MRED/RADSAFE [14] and MUSCA SEP3 [15] are some examples of such initiatives. There is no similar approach concerning the TID.

### C. Simulation Approaches for Fault Attacks

With respect to secure implementations, the goal of the designer is to develop countermeasures against known, and possibly unknown, attacks. Several methods exist in the literature exploiting either simulation or emulation approaches for fault injection, with application to evaluating the robustness of designs against defects or natural errors. The major difficulty in this task stems from the fact that fault injection techniques can be varied, as discussed in Section I. Depending on the chosen attack mean, the effects can be therefore different: sampling errors when clock glitching, corrupted signals created by laser pulses, etc. For this reason, one possibility is to abstract and model the effects of the faults at higher level: quite often, for example, fault injection attacks on microcontrollers and CPUs are modeled as instruction skips, replays, or corruptions [16].

This holds for microcontrollers, however, and is not feasible when considering general circuits. In this case, when designing countermeasures it is important to delve deeper into lower abstraction levels, such as RTL. At this level, usual fault models are based on stuck-ats or bit-flips; then, qualification campaigns can be done on the basis of a statistical distribution of fault occurrences [17], or on models based on the specific fault injection technique (such as selection of critical paths for delay faults, or spatial estimation of the targets for LFI [18]). Of course, the lower the abstraction, the more consistent the description will be, but this will also mean that the modeling will be quite tailored to the specific context.

Thus, specific approaches are required for different techniques when working at lower levels of abstraction. In the following, we will present our methodology addressing XRFI through two different approaches, and highlight what are the expected biases when irradiating a secure design.

## III. Simulation Models

### A. Parametric Degradation Model

In this approach, the parameters are injected directly into the SPICE-like netlist and are defined by the compact model of the transistor such as the BSIM3v3 or the BSIM4 models. New parameters can be inserted, and already existing parameters can also be used to emulate the desired effect. In the case of X-Ray effects, an inversion increment $V_{i-pmos}$ or a decrement $V_{i-nmos}$ in the threshold voltage parameter $V_{th}$ can be introduced in the equations of the compact model. This value can then be propagated through the SPICE-like netlist for the transistor level simulation. Fig 2 shows an example of the parameter propagation across different sub-circuits in a Cadence® Spectre netlist.

```
subckt inv_core in out inh_gnd inh_vdd
parameters mnw=0.35u mnl=0.35u vi_nmos=0 vi_pmos=0
   MN1 (out in inh_gnd inh_gnd) modn w=mnw l=mnl  vthadd=vi_nmos
   MP1 (out in inh_vdd inh_vdd) modp w=mnw l=mnl  vthadd=vi_pmos
ends inv_core
```

```
subckt INV3 A Q inh_gnd inh_vdd
   I3 (A Q inh_gnd inh_vdd) inv_core vi_nmos=0.32 vi_pmos=0.2
ends INV3
```

Fig. 2: Spectre sub-circuit parameter inheritance grammar description

### B. Electrical Equivalent Model

Several approaches have been proposed over the years to emulate the effects of TID at the electrical level. Esqueda et al. [19] propose to use a Voltage Controlled Voltage Source (VCVS) connected to the grid of the transistor in order to emulate the threshold voltage shift. On the other hand, static leakage can be modeled as a transistor connected in parallel to the irradiated N-type MOS [20].

Our approach is to emulate both the dynamic leakage (Threshold voltage shift) and the static current leakage $I_{OFF}$ at the same time. The dynamic leakage can be emulated using a VCVS where the positive terminal of the voltage source is connected to the grid of either the N-Type or P-Type MOS. The static leakage can be emulated using an N-Type parasitic transistor connected to an independent VCVS and in parallel to the target NMOS. Figure 3 represents the equivalent schematic of an irradiated CMOS inverter.

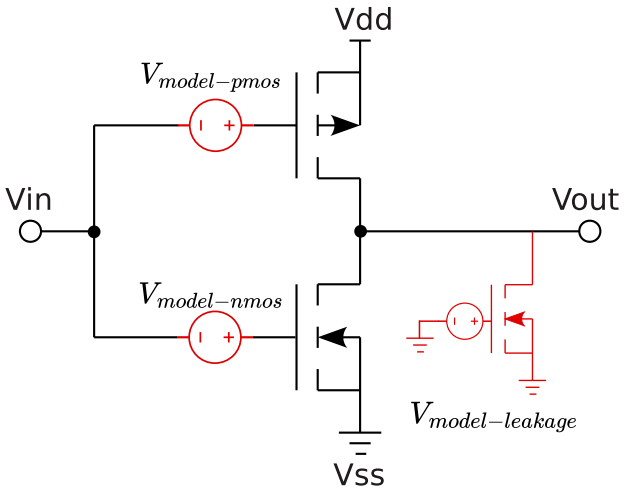



Fig. 3: Schematic representation of the TID leakage model

## IV. Simulation Flow

### A. Ray-Spect

Ray-Spect [9] is a Python framework designed specifically for assessing the sensitivity of secure designs against fault attacks and side channel attacks. It enables the simulation of localized parametric degradation in secure circuits. The simulation framework provided by Ray-Spect aims to capture the impact of these attacks on circuit performance, with a particular emphasis on localized degradation. Ray-Spect is best suited for modifying a few to several instances at a time, such as in X-ray attacks using laboratory sources.

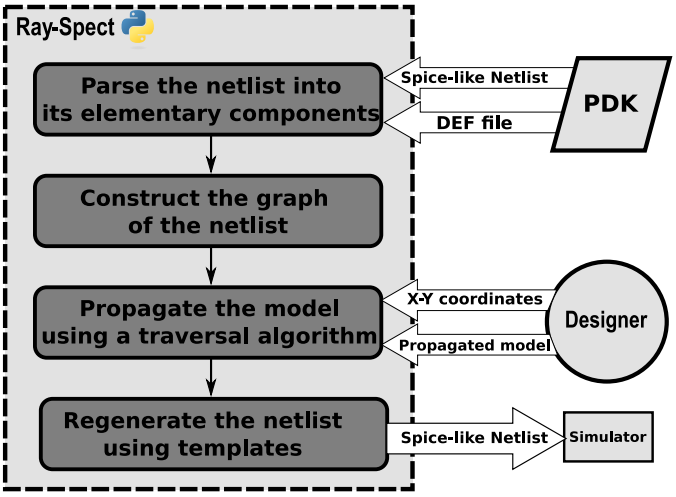



Fig. 4: Overview of the simulation flow using Ray-Spect

In this paper, the tool is used to assess the sensitivity of a secure design against X-Ray attacks. Firstly, from a fault injection perspective. Secondly, from a side channel attacks perspective, where X-Rays can be used not to fault an output, but to amplify the information leakage observed through the power consumption.

The simulation flow of Ray-Spect consists of several key steps:

*1) Parsing:* Ray-Spect starts by parsing a Cadence Spectre netlist using a netlist parser. The parsed netlist is organized into a class called NetlistElement, which represents different types of network elements in the netlist, such as sub-circuits, top instances, and comments.

*2) Graph Generation:* The tool generates a directed graph representing the netlist structure, starting from a given list of instances. The graph is constructed based on the connections between different components in the netlist, such as sub-circuits and top instances. The graph generation algorithm defines the edges of the graph based on the grammar of the Spectre netlist components.

*3) Model Propagation:* Whether it is parameter-based or equivalent circuit, Ray-Spect propagates the desired model through the netlist using a traversal algorithm, such as Breadth First Search (BFS). The paths from the fetched instances to the base FET components are identified, and the modified values are injected into the netlist buffer based on the parameter inheritance grammar in the Spectre netlist. The propagation algorithm loops over all the fetched instances and modifies the netlist buffer accordingly.

*4) Netlist Generation:* Once the desired parameters have been propagated throughout the netlist, Ray-Spect can generate a new netlist using templates. The tool utilizes a Spectre component template to generate the Spectre netlist, providing

flexibility and high rendering speed. Figure 4 provides a global overview of the Ray-Spect simulation flow.

### B. Fault injection use

Fault injection occurrences can be simulated by propagating the fault model into the netlist and sweeping its values until observing faulted outputs. In the case of TID effects, the propagated model can be purely parametric, meaning that we propagate an increment $V_{i-pmos}$ or a decrement $V_{i-nmos}$ to the threshold voltage of the transistor model until obtaining the inversion threshold voltage $V_{thi-nmos}$ (where the N-MOS becomes permanently conductive), and the inversion threshold voltage $V_{thi-pmos}$ (where the P-MOS becomes permanently blocked). Equations 1 and 2 describe the relationship between the inversion threshold voltage and the inversion voltage, where $V_{th}$ is the original threshold voltage of the transistor model:

$$V_{thi-nmos} = V_{th} - V_{i-nmos} \tag{1}$$

$$V_{thi-pmos} = V_{th} + V_{i-pmos} \tag{2}$$

The propagated model can be the electrical equivalent of the TID effect. The object-oriented design of the tool makes it easy to insert additional components: we can for example insert instances of DC voltage sources in a certain "sub-circuit" and modify the nets so that they are connected to the grid of the target transistors. A sweep can be performed on the values of the DC voltages until observing faulty outputs.

### C. Side channel use

Optically induced static leakages are a recent technique that was introduced in [21], where a laser transient pulse is injected in a combinational gate in the moment of switching in order to amplify its data dependant leakage. However, this technique is very expensive in terms of spatial and temporal accuracy. In this paper, we describe a novel technique to amplify the data dependency of the leakages. A certain area of the circuit can be targeted by X-Rays in order to increase its dynamic and static power consumption due to effects of TID radiations (detailed in Section II-A). The collection of power traces from the Spectre simulator is facilitated using Monaco [22], a tool designed to automate the simulation of multiple netlists.

Side channel leakage assessment, most notably power analysis, can be performed in Ray-Spect using a similar approach to fault injection, by sweeping the parameters in a range that does not induce faulty behaviour. The higher abstraction level of Ray-Spect provides a mean to assess the contribution of each component. For example, we can propagate the parametric degradation over a specific type of standard-cells to evaluate if certain logic gates are more leaky than others. In another scenario, one can also assess which transistor type is more prominent to target, by propagating the model over only a certain transistor type. Additionally, the assessment can be area dependent, by sweeping over chosen areas of a circuit to identify the most sensitive spots to attack.

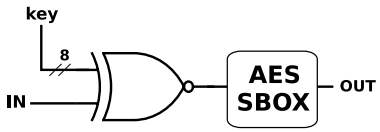
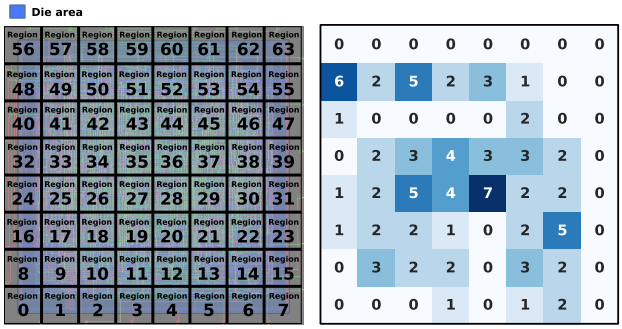



Fig. 5: Schematic view of the implemented S-Box design




(a) (b)

Fig. 6: (a) $8 \times 8$ grid representing the 64 region definition (b) Number of flipped bits in the output text

## V. Case studies

In this section, we will discuss three different use cases for our flow: the first concerning TID fault emulation, whereas the second and the third address side channel leakage variations.

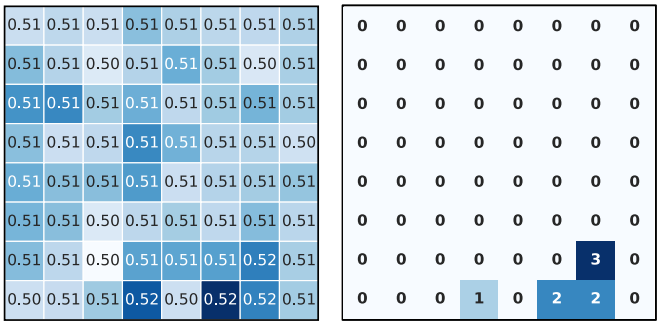
### A. Fault Injection on AES S-Box

For this case, a simple 8-bit Rijndael Substitution Box (S-Box) circuit for the Advanced Encryption Standard (AES) has been implemented (see figure 5). The goal in this case is to reach the inversion threshold voltage and observe flipped bit values at the output, when propagating the changes throughout selected regions of the circuit. The inversion voltage depends on the technology used; in our case, the circuit has been implemented with the AMS 350nm technology, but the methodology applies to any process. A simple threshold voltage sweep simulation can be performed in order to estimate the suitable values. Table I details different values extracted from the simulation.

The S-Box layout measures $400.4 \times 400.4 \mu m$. We divided the area into an $8 \times 8$ grid, with each square measuring $50 \times 50 \mu m$ and matching a simulated X-Ray beam. The chosen size is configurable and is based on our threat model, which considers the possibility of an attacker targeting an area of interest rather than just a single transistor. It is worth noting that this choice does not take into account the recent advancements in laboratory X-Ray targeted beams, which can reach sizes of approximately $1 \mu m$. Figure 6a shows the

TABLE I: Simulation results of the threshold voltage sweep

| Technology node | vdd (V) | $W/L$ (um) | $V_{th}$ (mV) | $V_{i-nmos}$ (V) |
|---|---|---|---|---|
| AMS 350 nm | 3.3 | 0.35/10 | 567 | 1.54 |




(a) (b)

Fig. 7: (a) CPA correlations coefficients after each region irradiation (b) Number of Flip-Flop instances existing in each region

definition of each region to be targeted by the parameter injection flow in Ray-Spect. Each square represents a netlist generated after the parameter propagation within the square, that is then simulated using Spectre. Figure 6b represents the number of flipped bits in the output cipher text after targeting the corresponding region.

### *B. Side Channel Analysis on an AES S-Box*

For the following case study, the threat model considers that an attacker may be able to bias the power consumption in a certain area of the circuit and thus amplify the information leakage. Power analysis methods such as the Correlation Power Analysis (CPA) and Differential Power Analysis (DPA) are applied to our design in order to assess potential information leakages. A shunt resistor is connected in series with the power distribution pin (vdd) in order to observe the simulated power traces.

*1) Correlation Power Analysis:* A CPA attack has been conducted on the 64 generated 8-bit S-Box netlists. A set of 70 random plaintexts among the possible 256 have been fed to the inputs of the circuit. If the key guess equals the correct encryption key, the Pearson Correlation Coefficient is stored.

For each netlist, CPA is performed 1000 times with 70 plaintexts and the correlation coefficient is averaged for statistical accuracy. Figure 7a shows the result of CPA after the irradiation of each region, whereas Figure 7b depicts the number of flip-flops contained in the region. The pre-rad coefficient was uniformly equal to 0.50, but after irradiation the behavior is region-dependent: these results suggest that Flip-Flops containing the current state and the key are the most sensitive components when targeted with radiations.

*2) Differential Power Analysis:* A DPA analysis was performed on two netlists: under the normal behaviour (figure 8a), and after irradiating the most sensitive spot discovered in the previous scenario (Figure 8b). The DPA was performed on several selection bits. For specific bits, the difference between the power consumption of the logical state '0' and the logical state '1' increases, thus resulting in a higher differential leakage. Figure 8 shows the difference between the

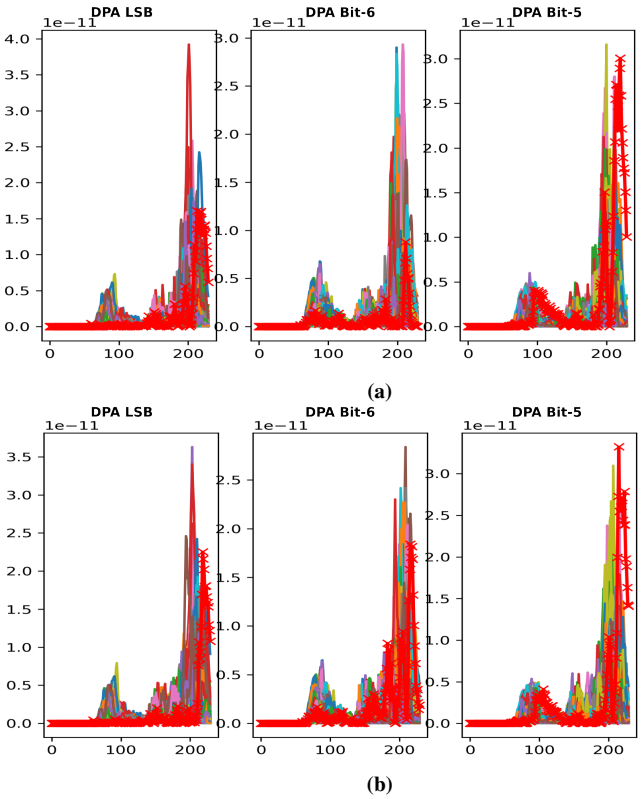



Fig. 8: DPA analysis on the selection bits 0, 5 and 6 of: (a) the original circuit; and (b) when region 5 is irradiated.

two behaviours: the '+' waveform is the correct key guess. In the selection bit 5, the correct guess could not be retrieved in normal operation, but became identifiable after irradiation due to the leakage amplification caused by X-Rays. In the other two cases, the correct key is still hidden, but its differential feature is largely improved.

### *C. Side Channel Analysis on 32-bit AES SubBytes*

In this scenario, a design with four AES S-Boxes is implemented (S-Box(0-3)). An arbitrary region in S-Box(2) is targeted by X-Ray irradiation. A set of fixed 500 plaintexts are used to attack the design in both cases, before and after the attack. Figure 9 shows the location of the 4 S-Box circuits and the targeted area in the S-Box(2).

The results of the CPA attack before and after radiation are shown in Table II. The same 500 plaintexts were applied in both cases. Byte 3 was not retrievable initially, but was successfully found after the irradiation. While the TID effects introduced in Byte 2 actually reduced the corresponding

TABLE II: CPA attack results on the quadruple S-Box

| Actual key | 0x0A | 0x0D | 0x82 | 0x80 |
|---|---|---|---|---|
| Key guess pre-rad | 0x0A | 0x2D | 0x82 | 0x24 |
| Coefficients pre-rad | 0.23 | 0.21 | 0.24 | 0.22 |
| Key guess post-rad | 0x0A | 0xAB | 0x82 | 0x80 |
| Coefficients post-rad | 0.23 | 0.22 | 0.23 | 0.21 |

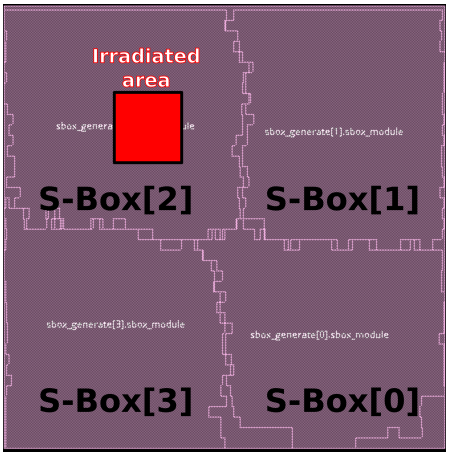



Fig. 9: Quadruple S-Box and targeted region area distribution

correlation coefficient, this highlighted the leakage of the byte 3 in the power trace, which allowed us to retrieve the key successfully.

## VI. Conclusion

Ray-Spect is a Python framework designed specifically for assessing the sensitivity of secure designs against fault attacks and side channel attacks. It provides a simulation flow that captures the impact of these attacks on circuit performance, with a focus on localized parametric degradation. The framework offers capabilities specifically targeted at X-Ray attacks.

Three case studies were presented to demonstrate the capabilities of Ray-Spect. In the first case study, the sensitivity of an AES S-Box circuit against fault injection was assessed. The inversion threshold voltage was propagated throughout selected regions of the circuit to observe flipped bit values at the output. The second and third cases studies are focused on side channel attacks, where power analysis methods were applied to assess information leakages. CPA and DPA attacks were conducted, and the effects of X-Ray irradiation on power consumption and leakage amplification were analyzed.

## Acknowledgment

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

## References

[1] D. Boneh et al. On the importance of checking cryptographic protocols for faults (extended abstract). In W. Fumy, editor, *International Conference on the Theory and Application of Cryptographic Techniques*, volume 1233 of *Lecture Notes in Computer Science*, pp. 37–51, Konstanz, Germany, 1997. Springer.

[2] G. Piret and J. Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In C. D. Walter et al., editors, *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pp. 77–88. Springer, 2003.

[3] T. Korak and M. Hoefler. On the effects of clock and power supply tampering on two microcontroller platforms. In *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 8–17, 2014.

[4] J.-M. Dutertre et al. Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 1–6, 2018.

[5] A. Dehbaoui et al. Electromagnetic transient faults injection on a hardware and a software implementations of AES. In G. Bertoni and B. Gierlichs, editors, *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, pp. 7–15. IEEE Computer Society, 2012.

[6] S. Anceau et al. Nanofocused x-ray beam to reprogram secure circuits. In W. Fischer and N. Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pp. 175–188. Springer, 2017.

[7] L. Maingault et al. Laboratory x-rays operando single bit attacks on flash memory cells. In V. Grosso and T. Pöppelmann, editors, *Smart Card Research and Advanced Applications - 20th International Conference, CARDIS 2021, Lübeck, Germany, November 11-12, 2021, Revised Selected Papers*, volume 13173 of *Lecture Notes in Computer Science*, pp. 139–150. Springer, 2021.

[8] N. O. Tebina et al. X-ray fault injection: Reviewing defensive approaches from a security perspective. In L. Cassano et al., editors, *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT 2022, Austin, TX, USA, October 19-21, 2022*, pp. 1–4. IEEE, 2022.

[9] N. O. Tebina et al. Ray-spect: Local parametric degradation for secure designs. In *29th IEEE International Symposium on On-Line Testing and Robust System Design, IOLTS 2023, Platanias, Greece, July 3-5, 2023*, pp. 1–7. IEEE, 2023.

[10] B. M. . G. S. *Ionizing Radiation Effects in Electronics: From Memories to Imagers*. CRC Press., 1 edition, 2016.

[11] I. Sanchez Esqueda et al. Modeling inter-device leakage in 90 nm bulk cmos devices. *IEEE Transactions on Nuclear Science*, 58(3):793–799, 2011.

[12] G. I. Zebrev et al. Physics-based modeling of tid induced global static leakage in different cmos circuits. *Microelectronics Reliability*, 84:181–186, 2018.

[13] H. Tang and E. Cannon. Semm-2: a modeling system for single event upset analysis. *IEEE Transactions on Nuclear Science*, 51(6):3342–3348, 2004.

[14] R. A. Weller et al. General framework for single event effects rate prediction in microelectronics. *IEEE Transactions on Nuclear Science*, 56(6):3098–3108, 2009.

[15] G. Hubert et al. Operational ser calculations on the sac-c orbit using the multi-scales single event phenomena predictive platform (musca $\mathrm{sep}^3$). *IEEE Transactions on Nuclear Science*, 56(6):3032–3042, 2009.

[16] L. Rivière et al. High precision fault injections on the instruction cache of armv7-m architectures. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 62–67, 2015.

[17] R. Leveugle et al. Statistical fault injection: Quantified error and confidence. In L. Benini et al., editors, *Design, Automation and Test in Europe, DATE 2009, Nice, France, April 20-24, 2009*, pp. 502–506. IEEE, 2009.

[18] A. Papadimitriou et al. Analysis of laser-induced errors: RTL fault models versus layout locality characteristics. *Microprocess. Microsystems*, 47:64–73, 2016.

[19] I. Sanchez Esqueda et al. Compact modeling of total ionizing dose and aging effects in mos technologies. *IEEE Transactions on Nuclear Science*, 62(4):1501–1515, 2015.

[20] I. Esqueda et al. Two-dimensional methodology for modeling radiation-induced off-state leakage in cmos technologies. *IEEE Transactions on Nuclear Science*, 52(6):2259–2264, 2005.

[21] J. Bělohoubek et al. Optically induced static power in combinational logic: Vulnerabilities and countermeasures. *Microelectronics Reliability*, 124:114281, 2021.

[22] S. V. Gutiérrez et al. Open automation framework for complex parametric electrical simulations. In *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, pp. 132–135, 2023.