Enhancing Side-Channel Attacks through X-Ray-Induced Leakage Amplification

Nasr-eddine Ouldei Tebina*, Luc Salvo†, Laurent Maingault‡, Nacer-Eddine Zergainoh*,
Guillaume Hubert§ and Paolo Maistri*
Univ Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000 Grenoble, France
†Univ Grenoble Alpes, CNRS, Grenoble INP*, SIMaP, 38000 Grenoble, France
‡CEA-Leti, 17 av. Des Martyrs, 38054 Grenoble, France
§ONERA DPHY, University of Toulouse, 31055 Toulouse, France

***Abstract*—In this paper, we propose a novel approach that utilizes localized X-ray irradiation to amplify data-dependent leakage currents in CMOS-based cryptography circuits. Our proposed technique strategically targets specific regions in a circuit using X-rays, inducing variations in dynamic and static power consumption due to Total Ionizing Dose (TID) effects, which increases or even reveals hidden data leakage. In this work, we present several experimental campaigns highlighting the benefits of our approach to combinational and sequential logic. Our experiments show a significant increase in information leakage in the targeted regions, which improves the signal-to-noise ratio coefficient and thus makes recovering the processed bytes easier. We envision the possibility of using this technique on full cryptographic designs on both FPGA and ASICs.**

***Index Terms*—Leakage, X-Ray, Side-Channel, CPA**

I. Introduction

The widespread need for data processing has led to the proliferation of embedded systems in a wide spectrum of application domains, such as IoT, home automation, and automotive systems. The fact that processed information often needs to be protected against unauthorized use implies the use of cryptographic algorithms in order to provide confidentiality and party authentication, among other features.

When implemented on actual devices, however, cryptographic algorithms may be exposed to physical attacks, passive and/or active, now well known in the literature. They are powerful techniques that severely affect the security of cryptographic implementations: while the former allows extracting sensitive information from the observation of the device, such as by monitoring the power consumption [1] or electromagnetic emissions [2], the latter exploits the altered behaviors in the presence of external perturbations [3].

These attacks are usually exploited independently from each other, due to their large differences in setup and methodology (i.e., passive observation vs. active perturbation). Nonetheless, a few works have explored the feasibility and benefits of combining complementary approaches at the same time. In [4], [5], side channel analysis is used to infer the actual event of faulty values in the absence of outputs, making fault attacks possible even in the presence of hiding countermeasures. On the other hand, Laser Fault Injection (LFI) has been leveraged in [6], where the photocurrent generated by the laser pulse creates a momentary local increase in power consumption, thus increasing information leakage during injection. However, this approach is prone to typical limitations of LFI: the device needs to be prepared beforehand as the injection is performed on the backside, and a time-consuming scan of the region of interest is required to target specific gates. When the layout is unknown to the attacker, these requirements increase the complexity of the attack.

In recent years, an alternative method to inject faults in secure circuits has been identified in X-Rays [7]. Ionizing radiations are well known and have been studied to understand how integrated systems may behave in harsh environments [8], but their application in the security domain is still in an early stage. In [7], the authors have shown how a nanofocused X-ray beam available at a synchrotron facility can be leveraged to target even a single transistor and thus induce a semi-permanent fault, which can be reverted through thermal annealing. Later, it was shown that similar results can be obtained with more affordable laboratory X-ray sources [9], at the expense of a rather limited controllability for the position and effect of the fault.

However, until now, ionizing radiation has been used mainly to perform fault injections and reliability evaluations. Although their effect on power consumption is known [10], [11], their influence on side channel leakage has never been studied so far. In this paper, we propose a first evaluation of the effects of X-Ray ionization when attacking simple cryptographic IPs through Correlation Power Analysis (CPA) [12]. We show how the leakage coefficient can be improved by radiation, under certain circumstances, for combinational and sequential logic. To the best of our knowledge, this is the first work dealing with the application of X-rays in side-channel analysis.

This paper is structured as follows. The next section provides a brief background on the interaction between integrated circuits and ionizing radiation, along with a concise summary of side-channel analysis. Section III describes the experimental irradiation setup and the device used as a target. In Section IV, we describe our experimental campaigns and perform side channel analysis before and after irradiation. Finally, Section V concludes the paper.

*Institute of Engineering Univ. Grenoble Alpes

979-8-3503-4859-0/DATE24/© 2024 EDAA

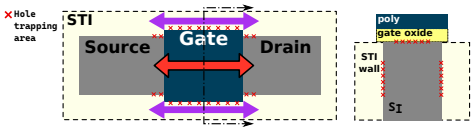


Fig. 1: TID induced leakage paths in a CMOS component on the gate oxide (red) and on the STI oxides (purple)

II. Background

A. Total-Ionizing-Dose Effects

TID radiations, such as X-rays, have a significant impact on the characteristics of MOS transistors, particularly the drain current $I_d(V_G)$ [13]. This impact manifests through three key parametric shifts in the transistor behavior: A shift in the threshold voltage, an increase in leakage current, and transconductance degradation. These effects are mainly attributed to the phenomenon of hole trapping within the oxide material.

Hole trapping occurs in several stages. Initially, electron-hole pairs are generated within the oxide as a result of pair generation mechanisms, with most of these pairs recombining quickly, representing the charge yield. Electrons, being highly mobile, dissipate through the gate when biased positively, whereas the remaining holes migrate toward negative potential and get trapped at defect sites, predominantly oxygen vacancies. Subsequently, interface traps form, whose nature depends on the position of the Fermi level in silicon. These interface traps actively exchange charge carriers with the substrate.

In modern technologies transistors, two types of oxides are the target of these effects: gate oxides and Shallow Trench Isolation (STI) oxides. The major effect in older technology is the shift in threshold voltage that is caused by positive charge traps induced by ionizing radiation in the gate oxides. These traps attract negative charge carriers at the canal level, leading to a decrease in the threshold voltage for N-type MOS and an increase for P-type MOS. Thinner gate oxides have been found to exhibit greater resistance to TID-induced effects, because they offer less volume for X-ray absorption and the generation of oxide traps. However, continuous scaling of CMOS technology has introduced new concerns, particularly related to charges trapped within STI oxides, which contribute to leakage currents in both the intracomponent and intercomponents [11].

As a result, for our concerns about leakage currents induced by X-rays, only the NMOS can be affected. There are two types of TID-induced leakage currents. First, the subthreshold leakage current, which results from lowering the threshold voltage (gate oxide charge traps). This type is static and can occur between the drain and the source at $V_{GS} = 0$. The other component of leakage occurs between the drain and the source through the parasitic paths that have formed on the walls of the STI. The smaller the technology, the more dominant the STI leakage, since they scale less than the gate oxide thickness. Fig. 1 shows the possible path of parasitic leakage that can form on an NMOS structure.

B. Side Channel Attacks

Side Channel Analysis (SCA) is focused on extracting cryptographic keys or other sensitive information by monitoring the physical signals emitted by an IC during its operation. This approach relies on the observation that ICs inadvertently reveal information about their internal states through observable side channels, such as power consumption, electromagnetic emanations, and execution time. These side channels provide adversaries with valuable information about the secret data being processed, potentially compromising the security of the IC and the entire system. For practical reasons, this work targets power consumption leakage, since the irradiation process makes online measurement of EM emissions rather complex.

Kocher et al.'s pioneering paper [1] was instrumental in introducing the concept of power analysis attacks. This work laid the foundation for Differential Power Analysis (DPA), for which power traces are classified according to a target function (such as a specific internal value) and the partitions are screened for statistical differences, revealing the secret. Further improvements of SCA include Correlation Power Analysis (CPA) [12]: this method leverages statistical methods to correlate power consumption measurements with specific intermediate values in cryptographic algorithms, enhancing the precision of key recovery attacks.

Before an actual key recovery attack, an evaluator can assess the circuit leakage with statistical methods. Signal-to-Noise-Ratio (SNR) [14] is the method of choice in the community and is computed as follows: for every EM/power trace is attributed a leakage partition / specific category which depends on the leakage model chosen. The SNR is thus defined as the ratio of the variance of the means of each partition over the mean of the variances of each category. Even tough there now exists a huge literature with more complex and effective attacks or leakage evaluation methods [15], we focus on SNR and CPA to demonstrate the irradiation effect on leakage.

However, a detailed overview of the topic is beyond the scope of this work; the interested reader may find more information in [16].

SCA, distinguished by its cost-effectiveness, stands as a formidable menace to security, prompting the formulation of large array of mitigation strategies. In the arsenal of these countermeasures, the reduction of power consumption [17] and the introduction of hardware-based noise [18] assume pivotal roles in thwarting any prospective key recovery. It is within this context that our proposed technique assumes high relevance.

III. Experimental Setup

A. Irradiation Setup

The laboratory setup consists of an EASYTOMXL tomograph manufactured by RX Solution SAS in Chavanod, France. It comprises an X-ray source and a flat panel detector, specifically the Varex 2520DX, for imaging purposes. The X-ray source is a Hamamatsu L10711-03 source, featuring a Lab6 wire at the cathode and equipped with a tungsten (W) target mounted on a diamond substrate.

There are three available modes of focalization, namely, small, medium, and large spot. For our experiments, we used the large-spot mode with a voltage of 60 kV and a current

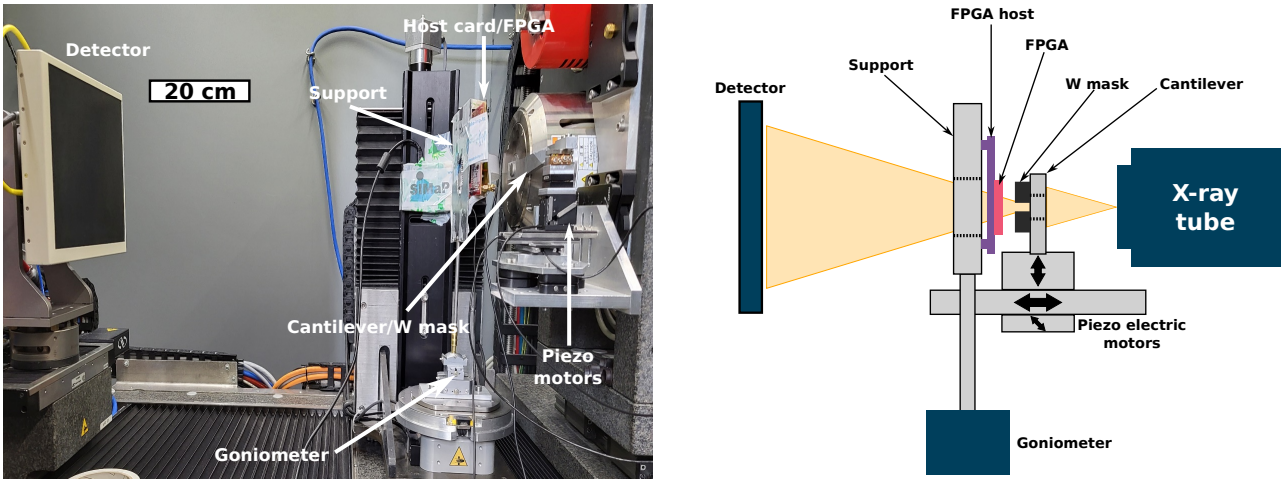


Fig. 2: X-ray irradiation setup which allows for accurate area targeting

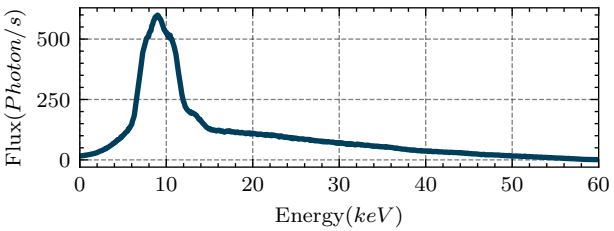


Fig. 3: EASYTOMXL Nano Source spectrum at 60kV 50uA and W target on diamond

of 50 μA. No filter was interposed between the X-ray source and the FPGA component. Under these conditions, the X-ray energy spectrum emitted by the laboratory tomograph onto the sample was measured using an Amptek CdTe spectrometer and is depicted in Fig. 3; the estimated total dose of photons received by the sample is approximately 3800 $photon/s$.

A specific mask is placed between the FPGA and the source. This mask is a 16 mm diameter, 2 mm thick W disk with a 1 mm central hole. It is fixed to a cantilever, which allows for precise alignment of the hole with the X-ray beam, thanks to two attocube piezoelectric motors controlled in a closed loop. The mask position can be fine-tuned in proximity to the FPGA using an additional attocube piezoelectric motor [19].

The FPGA is mounted on an electronic host FPGA card and the entire system, including the X-ray source, is shielded by a 1 mm thick lead sheet with a hole in front of the FPGA device. This configuration ensures the safety and proper functioning of the system. The complete setup is depicted in Fig. 2.

B. Target Device and Positioning

The target chip for the irradiation campaign is a Xilinx Spartan-6 in the TQFP package (XC6SLX9-2TQG144C), mounted on a victim board Chipwhisperer CW308T. This is then mounted on the host board CW308, which facilitates different types of attack on different targets. The FPGA can be programmed through the JTAG interface using the Xilinx JTAG programmer.

Vdd pins are connected to the shunt resistors to retrieve power traces from the victim board. Further more, a 20dB Low-Noise Amplifier (LNA) is used to enhance the signal quality. An external oscilloscope can be used to retrieve power traces or a Chipwhisperer Capture card. In our case, a Chipwhisperer-Lite[1] was used to retrieve the traces using the Simple Serial V1 protocol. A Simple Serial Core has been implemented in the hardware design to load the input vectors serially and read the output vectors in a similar manner.

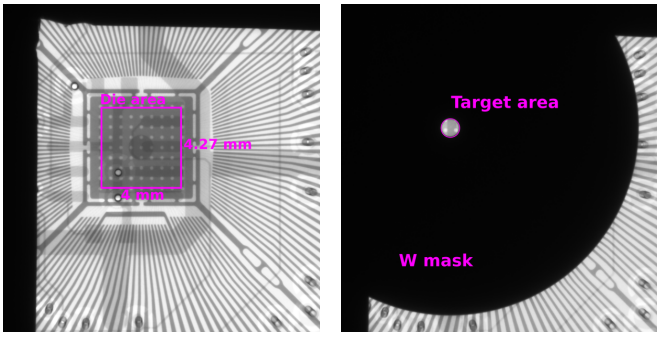
The correct positioning of the pinhole over the target area is of primordial importance. Two conditions are required for this procedure to be successful: noninvasively knowing the orientation of the FPGA chip, and an X-ray image showing the metal bondings surrounding the die area as retrieving an image of the die borders is a challenging task. A relative reference is placed at one of the corners of the die, and the pinhole is then shifted through the XY plane to the correct position. Fig. 4 shows the positioning procedure of the FPGA chip on top of the correct position.

We use an identical spare target FPGA chip to position the mask at the desired location. Taking X-ray snapshots would also generate leakage currents in the totality of the chip, which would then reduce the accuracy of our experiments. Therefore, a fresh FPGA chip is swapped in when the W mask is already locked in position. Due to this methodology, the leakage current is generated only in the exposed area of the mask. The system allows retrieving the desired position on the fresh FGPA with enough precision.

C. Target Architecture

To accurately highlight the localized effects of X-rays, FPGA circuits have been strategically implemented. A subset of the Advanced Encryption Standard (AES) has been implemented in order to demonstrate the effects of X-rays. The design is an XOR operation of a 32-bit plain-text with the key, followed by the Sub-Bytes operation performed by four 8-bit

[1]https://rtfm.newae.com/Capture/ChipWhisperer-Lite/



(a) (b)

Fig. 4: (a) X-ray snapshot of the Spartan6 chip (b) X-ray snapshot of a targeted area after the W mask positioning

AES substitution boxes (S-box), which is a popular leakage target for side channel attacks.

The four-S-box design in Fig. 5 (Above) is replicated 13 times to maximize resource usage in the FPGA and thus increase the observable leakage as much as possible, to emphasize and facilitate power analysis. Replicating the S-boxes also has the goal of fitting the pinhole size and thus amplifying the observable X-ray effects, because we provide more surface and more oxide area to irradiate, and the larger surface also provides more room for the pinhole area to target within the same byte. An additional AND layer will add LUTs and Programmable Interconnect Points (PIP), which will add an important contribution to data leakage, since PIPs are widely considered one of the most power-consuming components in FPGAs [20]. Fig. 5 (below) shows the leakages that correlate with the S-box output power model.

As a design strategy for the 32-bit AES S-box, the four bytes of the design have been fenced in specific regions using the placement block (P-block) capability of the Xillinx floor planning tools. The design was synthesized on Xillinx ISE, and the synthesis option of "*Equivalent Register Removal*" was disabled along side enabling the "*Keep Hierarchy*". More importantly, the "*ROM Style*" was set to be *Distributed* to avoid the synthesis of a BRAM-based S-Box. To analyze the localized effects of the proposed experimental flow, the components (LUTs, MUXes, and Flip-Flops) of the four S-boxes are separated into regions. The partitioning of the regions is then chosen according to the effect that we want to highlight. All the bytes are placed into regions containing all their components; LUTs of the substitution operation, registers containing the SubBytes output values, and the LUTs performing the AND operation. The bytes from 0 to 3 in order are placed to be from the furthest to the closest distance to the serial shift core. Byte 0 being the farthest.

IV. Evaluation

In this section, we discuss the results of our irradiation campaigns on a specific S-box of our design (Byte 1, see Fig. 6) after properly positioning the design under the 1 mm pinhole. All the bytes were constrained in placement using

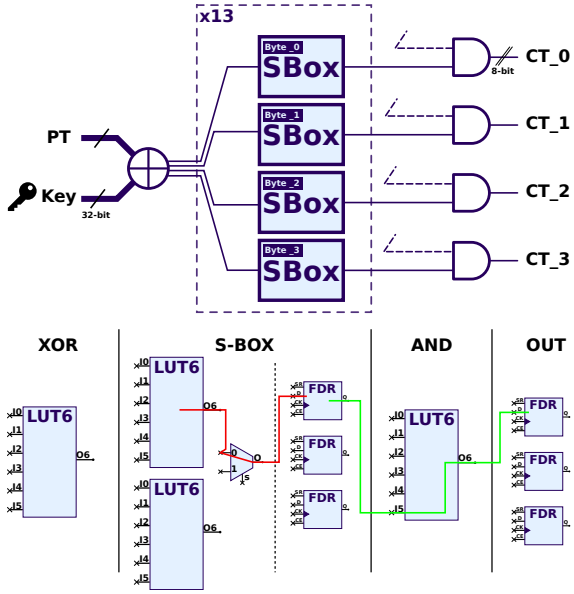


Fig. 5: Target cryptographic design of the attack (above) and its schematic implementation with FPGA resources (below). The red line corresponds to the first leakage path (Only combinational cells), and the green line corresponds to the second leakage path (Combinational and sequential cells)

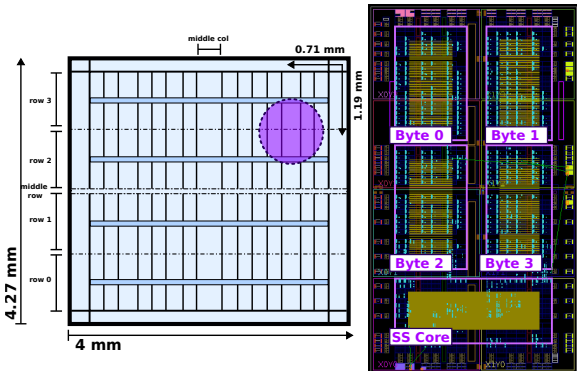


Fig. 6: Simplified view of the target FPGA die and the targeted area of the pinhole (on the left) and Xilinx Plan-ahead view of the defined regions for each byte (on the right)

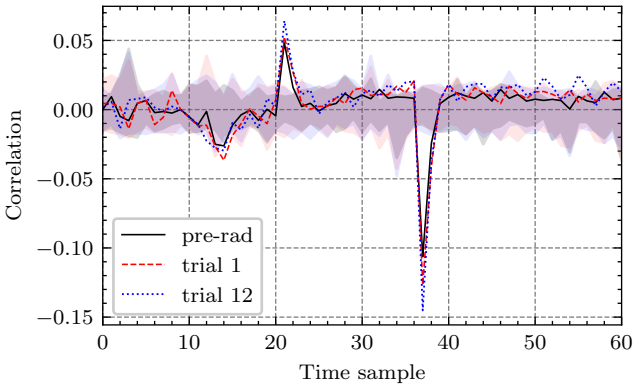


Fig. 7: Comparison of CPA attacks on Byte 1: before irradiation, after 10 minutes irradiation, after 120 minutes irradiation

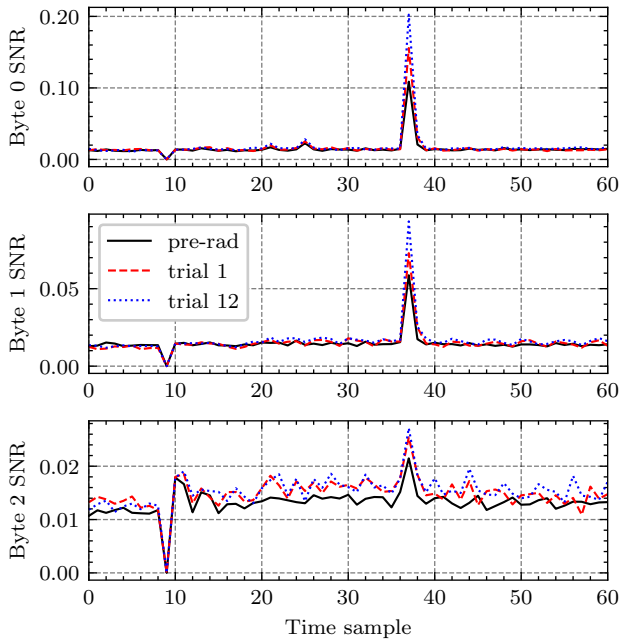


Fig. 8: Comparison of the SNR of Bytes 0, 1 and 2, before and after irradiation (10 and 120 minutes).

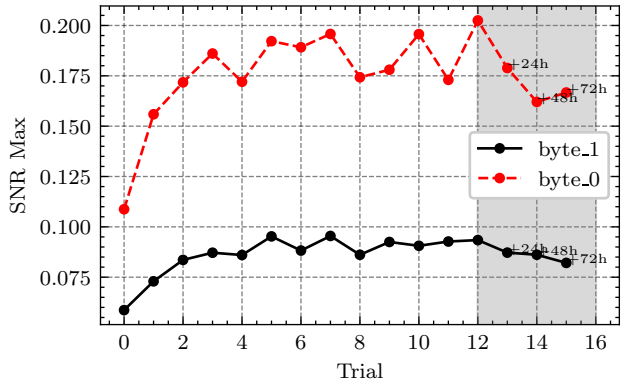


Fig. 9: Evolution of the SNR of Byte 0 and Byte 1 after irradiation of Byte 1 every 10 minutes of irradiation

P-blocks: Byte 1 is placed at the upper right corner of the FPGA. Consider that the synthesis tools do not provide the real up-to-scale shape of the die; the target region is located on the basis of its relative position. The circular pinhole was chosen to best fit the irradiated area. Fig. 6 shows the target area compared to its implementation view on the PlanAhead tool.

The target area was irradiated 12 times, for 10 minutes each. After each step, 20k traces were acquired using a precomputed set of random plaintexts through the ChipWhisperer environment. Each trace is made of 100 samples; using the same set of texts after each experiment allows comparing the results from one campaign to the other. Three additional captures were made at 24 h intervals after the last irradiation, to measure the impact of the annealing process.

Fig. 7 shows the CPA analysis after the first and the last irradiation test. The figure confirms the leakage paths shown in Fig. 5: the first correlation spike corresponds to the leakage of the combinational and interconnect components, whereas the second spike corresponds to the contribution of the combinational, sequential, and a much larger interconnect due to the unconstrained AND network. This is due to the fact that PIPs are largely the main contributor to the dynamic power consumption and leakage power of the FPGA [20].

Fig. 8 shows the complete SNR trace for three S-boxes, namely bytes 0, 1, and 2. First, the sharp increase in the second spike in the SNR and CPA confirms that PIPs are the leakage source most sensitive to X-rays. In a second observation, the information leakage increases in both observable information paths: the increase in the first spike corresponds to the combinational parts of the target area, as indicated in Fig. 7. We would expect the same increase in SNR at the same time sample in the targeted byte in Fig. 8 (Byte 1): this is not the case, however, since the power consumption of the interconnects hides the combinational power.

It is interesting to note that, by irradiating Byte 1 PIPs, the whole interconnect network is impacted by the increased power consumption. Since Byte 1 and Byte 0 are routed the furthest from the Simple Serial Core (SSCore), the interconnects carrying the data are longer, hence more power drawing and more information leaking into the power trace.

The increase in the SNR of Byte 0 at the same rate as Byte 1 in Fig. 8 further justifies that the main target for amplification of X-ray leakage was PIPs. The increase is even sharper than in the target area, since the SNR in Byte 0 was initially higher, indicating a higher contribution of the interconnect in the data leakage. This increase is not shared with Byte 2 in Fig. 8, as it is the closest to the SSCore and has the lowest contribution of PIPs to data leakage compared to the other bytes.

There is a direct correlation between the initial SNR maximum of each byte (PIP contribution) and the difference of the SNR induced by X-rays. Table I resumes this effect. Fig. 9 shows the evolution of the SNR after each trial. It can be seen that after an initial increase, the SNR becomes rather stable, and a higher TID does not systematically increase the leakage. With annealing, the device appears to partially recover, but no conclusions can be drawn given the limited horizon.

Fig. 10 shows the progression of the key guessing score of Byte 1 (target) and Byte 0. The results show an enhancement in the score of the targeted Byte, the number of traces being reduced from about 1300 to 700. Byte 0 did not witness such an enhancement, even though its SNR was amplified more than the target Byte, because the leakage components of Byte 0 are only the irradiated interconnects of Byte 1. For Byte 1, LUTs, registers, and interconnects are all leakage amplification sources due to the TID effect. LUTs and registers, despite

TABLE I: Variation of the SNR as a function of the initial SNR maximum value

	Byte 0	Byte 1	Byte 2
SNR_{MAX}	0.1088	0.0587	0.02147
ΔSNR_{MAX}	+0.0937	+0.0348	+0.0057

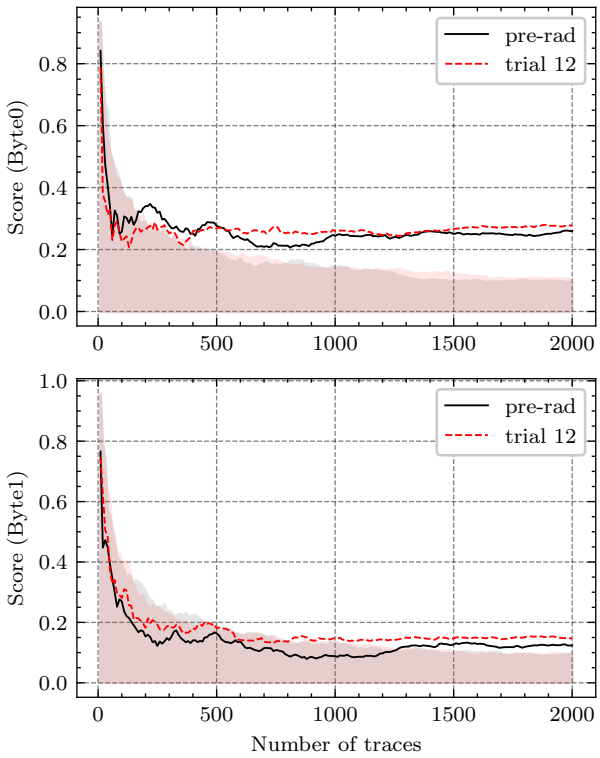


Fig. 10: Score of the correct key guesses versus all 255 key candidates for bytes 0 (above) and byte 1 (below)

their weak signal compared to the interconnects, contribute the most to data-dependent leakage amplification, whereas PIPs contribute the most to signal amplification.

V. Conclusion

This paper introduces a novel and promising approach that leverages localized X-ray irradiation to enhance data-dependent leakage currents in CMOS-based cryptography using affordable laboratory X-ray systems. The experimental campaigns demonstrate a significant increase in information leakage in the targeted regions up to a factor of 2, improving the signal-to-noise ratio coefficient and facilitating the recovery of processed bytes. This research opens new possibilities for enhancing the security analysis of cryptographic implementations, particularly in the context of side-channel attacks. While traditional side-channel analysis focuses on passive observation, this paper introduces an active approach using X-rays to amplify leakage, making it a novel contribution to the field. In the future, we will analyze different leakage sources and address the potential application of this technique to full cryptographic designs on both FPGAs and ASICs.

Acknowledgment

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

References

[1] P. Kocher et al. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pp. 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[2] K. Gandolfi et al. Electromagnetic analysis: Concrete results. In Ç. K. Koç et al., editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, pp. 251–261, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[3] 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 *LNCS*, pp. 37–51, Konstanz, Germany, 1997. Springer.

[4] T. Roche et al. Combined fault and side-channel attack on protected implementations of aes. In E. Prouff, editor, *Smart Card Research and Advanced Applications*, pp. 65–83, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[5] S. Patranabis et al. One plus one is more than two: A practical combination of power and fault analysis attacks on present and present-like block ciphers. In *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 25–32, 2017.

[6] J. Di-Battista et al. When failure analysis meets side-channel attacks. In S. Mangard and F.-X. Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010*, pp. 188–202, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[7] 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, Proceedings*, volume 10529 of *LNCS*, pp. 175–188. Springer, 2017.

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

[9] 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*, volume 13173 of *LNCS*, pp. 139–150. Springer, 2021.

[10] G. I. Zebrev and M. S. Gorbunov. Modeling of radiation-induced leakage and low dose-rate effects in thick edge isolation of modern mosfets. *IEEE Transactions on Nuclear Science*, 56(4):2230–2236, 2009.

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

[12] E. Brier et al. Correlation power analysis with a leakage model. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pp. 16–29, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

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

[14] S. Mangard. Hardware countermeasures against dpa – a statistical analysis of their effectiveness. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, pp. 222–235, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[15] T. Schneider and A. Moradi. Leakage assessment methodology. In *Cryptographic Hardware and Embedded Systems – CHES 2015*, pp. 495–513, Berlin, Heidelberg, 2022. Springer-Verlag.

[16] S. Mangard et al. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.

[17] D. Das et al. EM and Power SCA-Resilient AES-256 Through >350× Current-Domain Signature Attenuation and Local Lower Metal Routing. *IEEE Journal of Solid-State Circuits*, 56(1):136–150, January 2021. Conference Name: IEEE Journal of Solid-State Circuits.

[18] S. Kotipalli et al. Asynchronous Advanced Encryption Standard Hardware with Random Noise Injection for Improved Side-Channel Attack Resistance. *Journal of Electrical and Computer Engineering*, 2014:e837572, July 2014. Publisher: Hindawi.

[19] H. Murtaza et al. Air-drying of 3d printed part made of lignocellulosic fibres: 3d real-time monitoring combining sub-minute laboratory x-ray microtomography and digital volume correlation. *Cellulose*, 30(10):6173–6185, Jul 2023.

[20] L. Shang et al. Dynamic power consumption in virtex™-ii fpga family. In *Proceedings of the 2002 ACM/SIGDA Tenth International Symposium on Field-Programmable Gate Arrays*, FPGA '02, pp. 157–164, New York, NY, USA, 2002. Association for Computing Machinery.