Highlighting Two EM Fault Models while Analyzing a Digital Sensor Limitations

Roukoz Nabhan*, Jean-Max Dutertre*, Jean-Baptiste Rigaud*, Jean-Luc Danger† and Laurent Sauvage†
*Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne, France
†LTCI, Télécom Paris, Institut Mines-Télécom, 91120 Palaiseau, France
*{roukoz.nabhan, dutertre, rigaud}@emse.fr †{jean-luc.danger, laurent.sauvage}@telecom-paris.fr

***Abstract*—Fault injection attacks can be carried out against an operating circuit by exposing it to EM perturbations. These attacks can be detected using embedded digital sensors based on the EM fault injection mechanism, as the one introduced by El Baze et al. [1] which uses the sampling fault model [2], [3]. We tested on an experimental basis the efficiency of this sensor embedded in the AES accelerator of an FPGA. It proved effective when the target was clocked at moderate frequency (the injected faults were consistent with the sampling fault model). As the clock frequency was progressively increased, faults started to escape detection, which raises warnings about possible limitations of the sampling model. Further tests at frequencies close to the target maximal frequency revealed faults injected according to a timing fault model. Both series of experimental results ascertain that EM injection can follow at least two different fault models. Undetected faults and the existence of different fault injection mechanisms cast doubt upon the use of sensors based on a single model.**

***Index Terms*—EMFI, sampling fault model, timing fault model, fully digital sensor.**

I. Introduction

Securing connected objects is an ongoing challenge. To develop effective on-chip detection sensors as countermeasures against ElectroMagnetic Fault Injection (EMFI) attacks, it is crucial to study the mechanism involved in injecting faults due to EM perturbations. In this paper, we test the effectiveness of a fully digital detector design [1] embedded in an FPGA as a countermeasure against EMFI attacks. To investigate the efficiency of the sensors at detecting EMFI, as well as to study further the related mechanisms, the sensors were embedded in an AES accelerator. The full design consisted of a hardware 128-bit AES accelerator, a serial data link, a finite state machine, the Mixed-Mode Clock Manager (MMCM) block and 16 EMFI detection sensors. We used the Nexys Video 7 board, which embeds an Artix-7, XC7A200T.

Our contributions ascertained that EM-induced faults may follow at least two different mechanisms: timing and sampling, characterized the conditions needed to inject timing faults and illustrated the risks of using an EMFI detection sensor based on a single fault model (as the related mechanism has not yet been fully explained).

II. Experimental results and fault model analysis

For the design's logic blocks, the AES blocks are placed away from the MMCM to differentiate their EM perturbation effects. The 16 sensors are regularly distributed in the AES encryption block and triggered an alarm when exposed to EM perturbations. The correspondences between the design logic blocks and its EMFI sensitive areas were rigorously ascertained through testing various logic locations on the FPGA floorplan and observing the effect it had on the sensitive areas location. Previous works from [1] already studied thoroughly the ability of embedded sensors to cover the physical area of a target against EMFI. This research's work aimed at testing the intrinsic detection ability of a sensor built according to the sampling fault model when used over the target's full-frequency range. That is the reason why we located the EM injection probe in the center of the AES accelerator sensitive area (a place where it shall be at its best efficiency) reported after several experiments. According to this methodology, the explored injection parameters were the frequency of the AES and the timing of the applied EM perturbation with respect to (w.r.t.) the clock edges.

For each test series, the obtained results were expressed according to three metrics matching our research objective: *Alarm* raised if one of the 16 sensors was triggered, *Faulted Bits and Bytes (or FBB)* the number of faulted bits and bytes read from the AES ciphertext and *Alarm Failure (or AF)* raised when an undetected fault is observed.

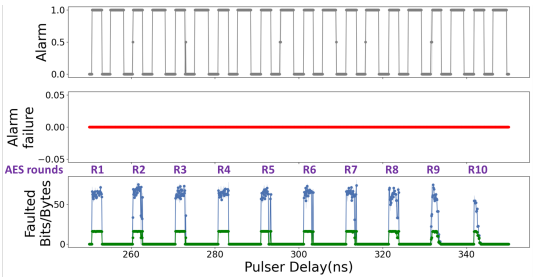

Fig. 1. Project behavior at 100 MHz.

In all our experiments, we set the pulse width to 4.5 ns, and the pulse amplitude to 420 V. Each campaign went through the whole AES rounds with a time step of 0.1 ns. In the following curves, the Alarm, FBB, and AF metrics are drawn as a function of the EM injection timing (expressed as the voltage pulser delay from a trigger signal). The results of 20 tries are averaged at each time position. Fig. 1 presents the results of a campaign launched at 100 MHz. The red curve shows that AF remained null throughout the campaign, indicating that all injected faults were detected. The gray curve shows continuous Detection

This work was supported by the French National Research Agency (ANR) under grand ANR-20-CYAL-0007

Windows (DW) with a width of 2-3 ns, spaced with a half-clock period. The AES computation rounds were identified by Injection Windows (IW) with a periodicity of 10 ns and width of 1.7-2.2 ns. This test series were consistent with the sampling fault model [2], [3]. A same behavior was observed in several campaigns launched by changing the clock frequencies between 10 MHz and 140 MHz while keeping the same parameters.

At 150 MHz, alarm failures started to emerge (i.e., EMFI that is not detected). The appearing AF windows were progressively increased from 150 MHz to 200 MHz close to the DUT max. frequency. At 200 MHz, the AF windows developed

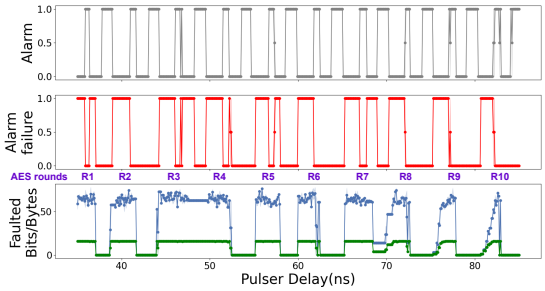

Fig. 2. Project behavior at 200 MHz (420 V voltage pulse).

significantly as shown in Fig. 2: most injected faults escaped the sampling fault-based sensors (the DWs were reduced to less than 1 ns). The AES computation faults were repeatable and consistent with the mechanism of timing faults violation as described in [4]. Most of the injected faults were fitting the timing fault model, but some still were fitting the sampling fault model. Furthermore, a strong EM stress was not required to inject faults during project execution at 200 MHz, as the experiments carried out for a reduced voltage pulse amplitude of 340 V. At this voltage level, faults following the timing fault model were injected and the DWs were reduced to zero. This clearly confirms that EMFI can follow a timing fault model at high clock frequency. Hence, for a higher-voltage pulse (420 V), both injection mechanisms shall interact to explain the faults injected around the clock rising edges and the fact that the IWs widths were found different for clock frequencies on the 100 MHz to 200 MHz range. It contradicts the sampling fault model hypothesis that the IW are constants against frequency variations [2], [3]. It shall be investigated further to reconcile theory and practice.

III. Discussion

EMFI experiments were carried out for clock frequencies ranging from 10 MHz to 200 MHz, it made it possible to record the voltage pulse amplitude thresholds needed to inject faults into the AES computations and to trigger the sensors. These thresholds are drawn in Fig. 3 (respectively in orange and blue) for an injection timing set close to the clock rising edge. The sensors threshold (blue) remained constant at 380 V for all frequencies. Whereas the fault threshold was constant at the same 380 V value up to 150 MHz, before decreasing progressively to 280 V at 200 MHz. Beyond this point, undetected faults started to appear (the orange curve goes below the blue one). We assumed that all the faults injected at clock frequencies less than 150 MHz correspond to the sampling fault model only. Above 150 MHz, timing fault effects started to increase progressively with increasing clock frequencies. For an EM injection timing set between the sensor DWs (i.e., in-between the clock rising and falling edges) a different voltage pulse amplitude threshold is obtained (drawn in green in Fig. 3). It is consistent with a timing fault model: starting at 120 MHz it decreases from approx. 700 V to 450 V at 170 MHz as the timing slack of the AES decreases with increasing the operating frequency. Around 180 MHz, it goes below the detection threshold (blue) to reach 340 V at 200 MHz. These results clearly show that two distinct

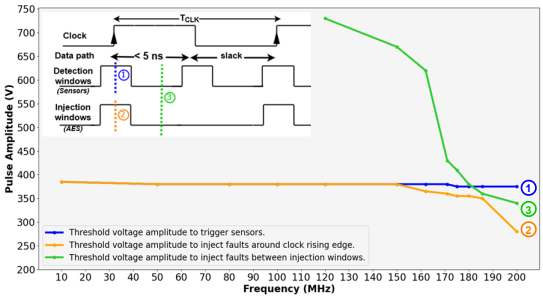

Fig. 3. Evolution of the threshold voltage amplitudes w.r.t the clock frequency.

fault injection mechanisms are at play to explain EMFI. They also blend as the shape of the fault threshold (orange) goes down after 150 MHz when the timing fault mechanism becomes more prevalent (decreasing green curve) while the detection threshold (blue) related to sampling faults stays unmodified.

IV. Conclusion

This paper explored the efficiency of EMFI detection sensors based on the assumption that the sampling fault model can explain EMFI. The sensor efficiency started to fail for operating frequencies above 150 MHz casting doubts upon the model validity. It illustrates the risk taken when basing a sensor on an incomplete fault model. Indeed, we ascertained the ability to inject EM faults in a target according to a timing fault model when its frequency is close to its maximum (these faults escaped detection). It also demonstrates on an experimental basis that EMFI works according to different mechanisms on the very same target for different injection parameters (time of injection and frequency). It may offer an attacker the ability to select a fault model in order to escape any sensor based on another mechanism. It also highlights that EMFI mechanisms are plurals and are still incompletely understood: further analyses and tests are needed.

References

[1] D. El-Baze, J.-B. Rigaud, and P. Maurine, "A fully-digital em pulse detector," in 2016 Design, Automation Test in Europe Conference Exhibition (DATE), 2016, pp. 439–444.

[2] M. Dumont, M. Lisart, and P. Maurine, "Modeling and simulating electromagnetic fault injection," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp. 680–693, 2020.

[3] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 183–197, 2017.

[4] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012, 2012, pp. 7–15.