HAL
open science

Investigation of Near-Field Pulsed EMI at IC Level

Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, Assia Tria

To cite this version:

Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, Assia Tria. Investigation of Near-Field Pulsed EMI at IC Level. Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility, May 2013, Melbourne, Australia. cea-01097120

HAL Id: cea-01097120

https://cea.hal.science/cea-01097120v1

Submitted on 18 Dec 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Investigation of Near-Field Pulsed EMI at IC Level

Amine Dehbaoui*, Jean-Max Dutertre†, Bruno Robisson* and Assia Tria*

*†Département Systèmes et Architectures Sécurisés (SAS)
†École Nationale Supérieure des Mines de Saint-Étienne
*CEA-LETI, France
{Firstname.Lastname}@cea.fr Lastname@emse.fr

***Abstract*—This article describes the use of a near-field electromagnetic pulse EMP injection technique in order to perform a hardware cryptanalysis of the AES algorithm. This characterization technique is based on the fact that conductors, such as the rails of a Power Distribution Network PDN which is one of the primary EMI risk factors, act as antennas for the radiated EMP energy. This energy induces high electrical currents in the PDN responsible for the violation of the integrated circuit's timing constraints. This modification of the chip's behavior is then exploited in order to recover the AES key by using cryptanalysis techniques based on Differential Fault Analysis (DFA).**

I. Introduction

Electromagnetic interferences (EMI) are unwanted disturbances that affect integrated circuits due to electromagnetic conduction or electromagnetic radiation emitted from an internal or external source. From an EM Compatibility (EMC) point-of-view, EMI whether intentional or not, are considered as a source of noise and interferences. Today, electromagnetic susceptibility of integrated circuits represent also vulnerabilities for hardware security modules like smart-cards. Recently, from a security point of view, researchers, industrials and governmental agencies are focusing with strong interest on these electromagnetic disturbances.

The efficiency of the EM channel is mainly due to the inner properties of EM emissions. Their ability to propagate through different materials is the most interesting one since it allows an attacker to bypass the chip package and/or some EM shields implemented as counter-measure. Moreover, the small size of EM probes permits to focus the perturbation into a small area of the targeted device. This is all the more interesting since it also allows getting around global hardware countermeasures against power glitches such as the use of detached power supplies [1] by focusing the EMP injection on reduced die areas.

Two kinds of near-field EM perturbations are usually considered: transient pulses and harmonic emissions. In [2] authors considered the effect of a 1 GHz electric field applied to an IC with an embedded ring oscillator (RO). The main component of that electric field was the transverse one (i.e. parallel to the surface of the chip). The perturbation impacted the output frequency of the RO. Monitoring the effect of that perturbation enabled them to draw a cartography of the sensitive areas of the chip. A cross examination between the layout of the device and the cartography demonstrates that the coupling between the injection antenna and the circuit lies mainly in the Power Distribution Network (PDN). Regarding transient EM pulses, Schmidt et al. reported the use of a spark generator to fault a CRT-based RSA algorithm running on an 8-bits micro-controller [3]. The injected fault leads to a successful attack as it allows them to factorize the RSA modulus. Besides, their experimental setups is characterized by a very large jitter because of the use of the spark-generator.

This article describes the use of the EM channel to carry out attacks against a hardware AES embedded in a FPGA with a good temporal and spacial resolution. Transient electromagnetic pulses (EMPs) are injected with a very low jitter on top of the surface of the targets using a 500 μm-diameter magnetic antenna. By doing so, we intend to analyze firstly, the effect of the EMP's polarity on the target, secondly, whether the effect of the EMP on the target is global or local, and finally, the occurrence and the behavior of the faults induced by a very short EM pulse.

The remainder of this article is organized as follows. We describe the EMP injection bench used to generate EMPs in section II. In sections III we study the effect of a localized EMP injected on top of the surface of an FPGA while executing the Advanced Encryption Standard (AES). As a conclusion, section IV summarizes our findings.

II. Test setup

In this section, the near-field EMP pulse injection bench used to induce transient faults is described.

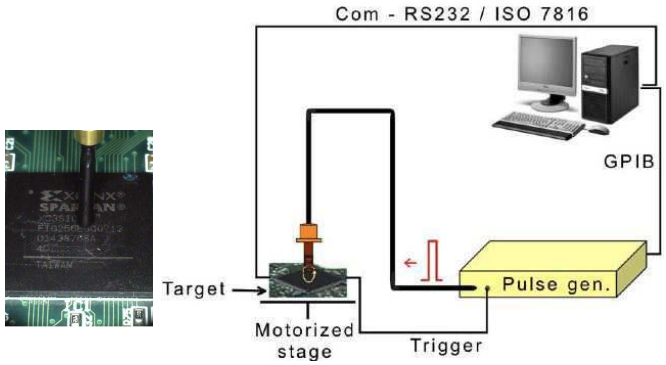

Fig. 1. Near-field EMP injection bench.

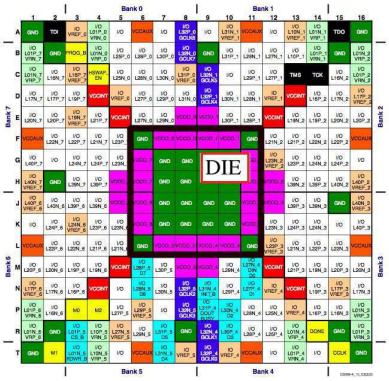

Fig. 2. The FPGA package footprint [4]

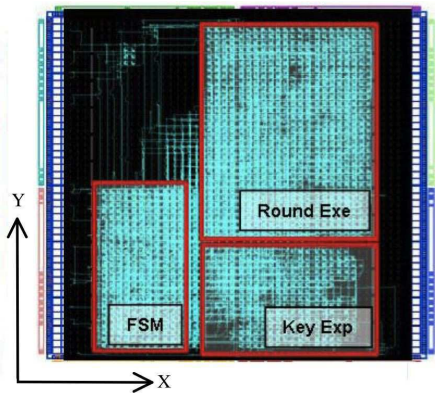

Fig. 3. Floorplan of the device under test

A. Pulsed EMI bench description

The near-field EMP injection bench (Figure 1) is built of a control PC, the device under test (Target), a motorized stage, a pulse generator, and a 500 μm-diameter magnetic antenna. The antenna is moved above the target by means of a high-precision mechanical positioning system (to within $0.01\mu m$ minimum). Every element of the bench is controlled by the control PC, and the communication with the target is established through a serial port or a smart card reader.

The pulse generator is capable of generating 200 V with high current (4 A) directed to a target by the antenna 50 Ω loads (with a very low jitter $< 30ps$), and at repetition rates up to 50 kHz. The output pulse width is variable from 10 to 200 ns. The rise and fall times are 2 ns or less, $20\% - 80\%$.

B. Test chip description

The device under test is a FPGA (Xilinx Spartan 3 family Fig. 2). Internal core logic circuits such as the configurable logic blocks CLB and programmable interconnect operate from the 1.2V VCCINT voltage supply inputs. All VCCINT inputs are connected together and to the +1.2V voltage supply, but in order to guarantee problem-free operation, a supply decoupling is present, as described in [4].

This FPGA implements a hardware 128 bits version of the AES algorithm [5]. This algorithm is used for various security purposes. The design is written in VHDL and synthesized for the FPGA. It is built out of three main blocks: a communication and control module (FSM), a key expansion module and a cipher module (ROUND EXE). A manual Place-and-Route stage is performed in order to distinguish between the impacted logical blocks by a comparison with the Floorplan (Figure 3).

We choose to use a 128 bit-wide data path AES and to execute simultaneously on the chip the key expansion and cipher routines. As a consequence, a complete encryption round takes only one clock period, and the whole encryption process is executed in eleven clock periods.

The key expansion routine generates the round keys "on-the-fly". For each clock cycle, a new round key is obtained from the key expansion module and sent to the cipher module. The cipher module's architecture is divided into five submodules: ADDROUNDKEY, SUBBYTES, SHIFTROWS, MIXCOLUMNS, and Mux. The first four, as their names suggest, correspond to the individual AES transformations. The ADDROUNDKEY module owns a dedicated output to store the ciphertext after the final round. The MIXCOLUMNS module is bypassed during the final round.

III. INJECTING DELAY USING PULSED EMI

This section first reviews the principles of digital circuits synchronous operation in order to introduce DFA. From this, a susceptibility criterion is defined in order to perform a near field EMP injection cartography.

A. Timing design considerations

In this subsection we review shortly the principle of the synchronous behavior of digital ICs. In broad outline, synchronous digital circuits execute digital calculation synchronized by a common clock. They could be described as blocks of combinatorial logic separated with register banks of D flip-flop sharing the same clock as figure 4 shows. The data are generally latched by the registers on the positive edge of the clock. Between two successive clock positive edges, the computed data have to travel from one register to the next. The time needed by the data to propagate through combinatorial logic is called the propagation delay. This delay and an other

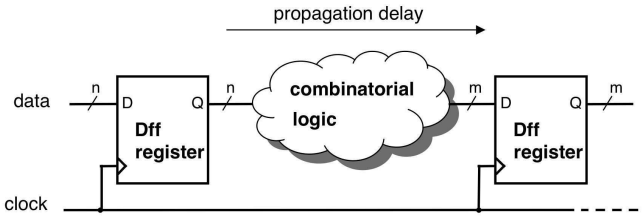

Fig. 4. Synchronous Representation of Digital ICs

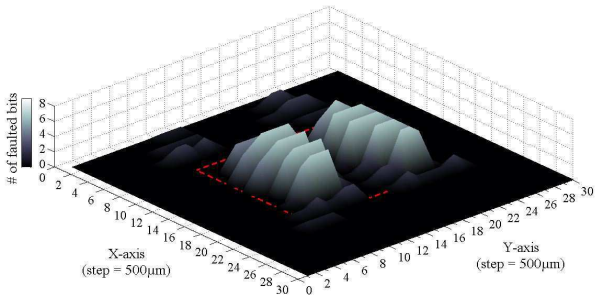

Fig. 5. Faults cartography for a Positive EMP

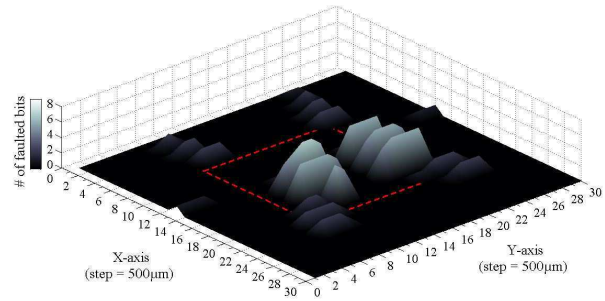

Fig. 6. Faults cartography for a Negative EMP

delay inherent to the use of D flip-flop, called the setup time, affect the choice of the nominal circuit period. Indeed, to ensure a correct computation of the circuit, the clock period must be chosen strictly greater than the critical delay path plus the setup time of the registers, where the critical delay path is the biggest combinatorial logic propagation delay between two registers found in the considered circuit. Equation 1 sums up this constraint:

$$T_{clock} > t_{critical} + t_{setup} \quad (1)$$

Each data bit at the input of a register possesses its own logical cones from the previous register bank associated with its own propagation time. Furthermore, this propagation time is not a constant; it depends highly on the data handled across the logic and the circuit's power supply voltage.

A transient glitch in the power supply voltage, induced by an EMP, will modify the integrated circuit timings. As the master clock frequency remains the same, faults occur in the circuit. These faults may be exploited by an attacker to break a cipher like the AES [6], [7], [8]. The attack of Piret et al. [7] is one of the most powerful. It allows to retrieve an AES key with only one pair of correct/faulty ciphertexts when a fault is induced on a single byte of the state before the penultimate MixColumn.

B. Near field susceptibility cartography

In this test, the susceptibility criterion is a timing violation of the AES design constraints. A high susceptibility value refers to a large number of violated paths, while a low susceptibility value refers to an execution without any timing violation. The pulse width value is chosen to match the clock period (TCLK = $10ns$), with an amplitude of 100 Volts.

A susceptibility cartography of the design is performed during the last round of the AES. It aims at disclosing the (X,Y) coordinates where the EMP induces a timing violation (i.e faulty computation). The whole surface of the package is exposed to a localized EMP with a displacement step of 500μm (which is also the antenna diameter). The relative distance between the antenna and the surface of the package is set to 500μm. At each location, an EMP is injected during the last round of the AES and the corresponding faulted ciphertext (if any) is retrieved. This process is done for 1,000 encryptions of the same plaintext input, and for every of the 30x30 different locations of the injection antenna on top of the FPGA package.

1) Positive EMP*:* In this test, and according to the polarity of the EMP, only a coupling between the antenna and the ground network of the circuit will vary the susceptibility criterion. Figure 5 reports the resulting susceptibility cartography for a positive EMP with an amplitude of +100 Volts. In this figure, the red square in the center corresponds to the FPGA die position. At each location, the number of faulted bits are reported.

Considering Figure 5, we observe that the targeted chip is very sensitive to the positive EMP. In fact, a large number of locations over the surface of the package seems more sensitive to a positive EMP than a negative one. This high susceptibility is due to a low resistivity of the ground network in comparison with a decoupled power network.

2) Negative EMP*:* Figure 6 reports the resulting susceptibility cartography for a negative EMP with an amplitude of -100 Volts. In this figure, the red square in the center corresponds to the FPGA die position. At each location, the number of most frequent faulted bits are reported.

Considering Figure 6, we observe that the effect of the EMP is clearly localized in space. Some locations above the surface of the circuit are more sensitive to the EMP than others. When the EMP is localized in the region near the block cipher, the number of faulted data paths increases. Moreover, we observe a good correlation between the most sensitive coordinates and the position of the ROUNDEXE in Figure 3. This logical block is the place where the critical delay path is located.

Figure 7 shows the behavior of the induced faults for a first random position (X_1,Y_1,Z) on top of the die's surface (7x7mm^2) right in the ROUNDEXE area (the cipher module). 1,000 encryptions were done with random plaintexts and a constant key while injecting EMPs during the last round of the AES calculations. The occurrence rates of both single-bit (i.e. fault affecting a single bit) and multi-bits faults are given.

The path corresponding to the 15th byte appears to be the most sensitive to the EMP at coordinates (X_1,Y_1,Z). For this

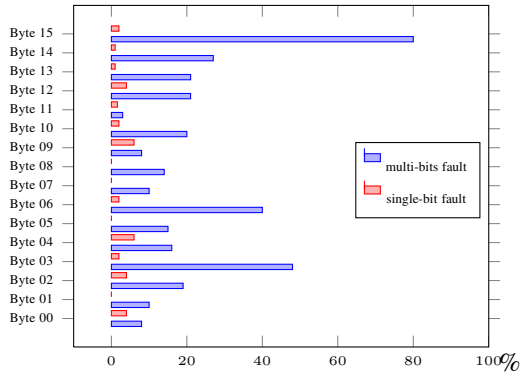

Fig. 7. Fault occurrence at coordinates (X_1,Y_1,Z)

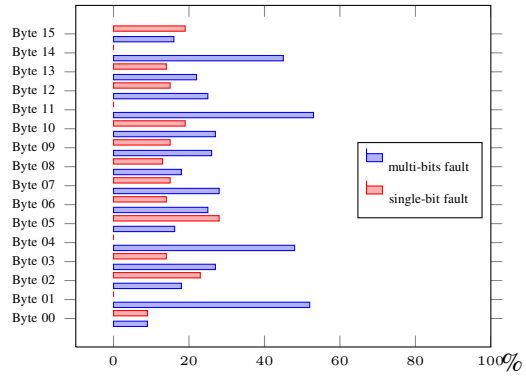

Fig. 8. Fault occurrence at coordinates (X_2,Y_2,Z)

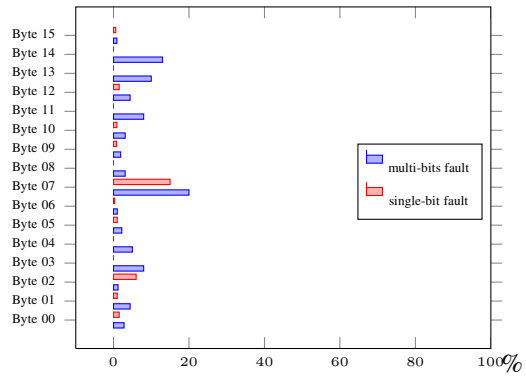

Fig. 9. Fault occurrence at coordinates (X_3,Y_3,Z)

byte, 3% of the faults were single-bit, and 80% of the faults were multi-bits faults. It also reveals a data-dependence of the injected faults to the data handled by the target. This behavior was corroborated by an inspection of the faults. In fact different faults values ('0' or '1') were obtained for different plaintexts with the same experimental settings. This behavior is as well a feature of faults induced by timing constraints violation (its origin lies in the data-dependence of the data propagation time through combinatorial logic). This is another sign that reinforces the assumption that the fault injection mechanism by means of EMP is related to timing constraints violation.

The same experiment was carried out for two other locations (X_2,Y_2,Z) and (X_3,Y_3,Z) on top of the die with the same 1,000 plaintexts used previously. Figures 8 and 9 report the corresponding single-bit and multi-bits fault occurrence rates. These three figures (7, 8 and 9) exhibit different occurrence rates: the injection antenna location has an effect on the induced faults and on their related properties. In fact, at coordinates (X_1,Y_1,Z), the 15th byte is the most sensitive to the EMP. Whereas, at coordinates (X_2,Y_2,Z) and (X_3,Y_3,Z) the most sensitive paths correspond to the 11th byte and to the 7th byte respectively. We observed that the faulted paths were different for different locations of the injection antenna.

The evidence of a local effect (i.e. restricted to a part of the device's area) of the EMPs, demonstrates the ability to fault sub-critical paths. In some locations, the most critical one is never faulted. This is a very interesting property (for an attacker) since it is possible to select the disturbed path without always affecting the most critical ones as it is the case for direct power injection techniques.

IV. Conclusion

The reported fault injection experiment reveals the ability to inject single-bit and multi-bits faults into the calculations of the AES. These faults were found data dependent. Moreover, a local effect of EMPs was underlined: the injected faults (if any) are modified when the injection antenna location is changed. According to the experiments, EMP injection mechanism may lie in a coupling between the EMP and the internal PDN of the targeted chip. This coupling induces a transient decrease of the voltage applied to the logic of the target. As a consequence, the propagation delays through the logic are increased until faults are induced by the violation of the chip's timing constraints. This property of EMP fault injection is particularly worrying. Indeed, it may allow to bypass many countermeasures intended to prevent direct power injection (e.g. power supply low-pass filtering, use of internal supply monitoring, etc.).

Acknowledgment

This work was funded by the EMAISECI project (ANR-10-SEGI-0012)

.

References

[1] A. Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies," in *Proc. 2nd Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2000, pp. 71–77.

[2] F. Poucheret, K. Tobich, M. Lisart, B. Robisson, L. Chusseau, and P. Maurine, "Local and Direct EM Injection of Power into CMOS Integrated Circuits," in *FDTC*, 2011.

[3] J.-M. Schmidt and M. Hutter, "Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results," in *Austrochip*, 2007, pp. 61–67.

[4] Xilinx, "Spartan-3 fpga family: Complete data sheet," 2004.

[5] NIST, "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication, n. 197, Nov. 26, 2001.

[6] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *CRYPTO*, 1997, pp. 513–525.

[7] G. Piret and J.-J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD." in *CHES*, 2003, pp. 77–88.

[8] C. Giraud, "DFA on AES Advanced Encryption Standard – AES," ser. Lecture Notes in Computer Science, H. Dobbertin, V. Rijmen, and A. Sowa, Eds., vol. 3373. Springer Berlin / Heidelberg, 2004, p. 571.