Review of: Protecting FPGA-Based Cryptohardware Implementations from Fault Attacks Using ADCs

F. E. Potestad-Ordóñez[1,3,*], A. Casado-Galán[3], E. Tena-Sánchez[1,3], and A. J . Acosta-Jiménez[2,3]
[1]Escuela Politécnica Superior, Universidad de Sevilla
[2]Facultad de Física, Universidad de Sevilla
[3]Instituto de Microelectrónica de Sevilla, IMSE-CNM (Universidad de Sevilla/CSIC)
e-mail:potestad;casado;erica;acojim@imse-cnm.csic.es

***Abstract*—In this paper, we present a review of the work [1]. Some of the most powerful hardware attacks are called fault injection attacks. These attacks involve introducing a malfunction into the normal operation of the device and then analyzing the data obtained by comparing them with the expected behavior, to retrieve secret information. To implement the fault injections it is possible to use the methods of variation of the supply voltage and temperature or the injection of electromagnetic pulses. In this paper, a hardware design methodology using analog-to-digital converters (ADCs) is presented to detect attacks on cryptocircuits. The results obtained demonstrate that, in 100% of the cases the detectors activate an alarm signal when the cryptographic module is attacked.**

***Index Terms*—Hardware Security, Voltage Attack, Temperature Attack, Electromagnetic Attack, Countermeasures, FPGA.**

Tipo de contribución: *Investigación ya publicada*

I. Introduction

The proliferation of the Internet of Things (IoT) has caused a rapid and significant increase in the number of interconnected devices. These interconnected devices process a large amount of data, most of which are sensitive user data. Due to the methods that hackers are constantly developing, like fault injections, to gain access to the secret information of users, protecting sensitive data and countering attacks by third parties has become a constant challenge. Non-invasive attacks are a major concern for the cryptographic community due to their low cost, minimal equipment requirements, and high success rate.

II. Physical Fault Injection Attacks

For non-invasive active attacks based on fault injection, the attacker maliciously aims to cause transitory faults in the operations of cryptographic algorithms. Faults must not be permanent, as this would render the circuit unusable and eliminate the possibility of a differential study. With this in mind, the attacker will try to determine the erroneous behavior under different types of fault, which depends on the algorithm under attack, and compare it with the correct behavior of the circuit. This mathematical comparison is known as Differential Fault Analysis (DFA) [2] and allows one to establish the relationship between the produced faults and the internal information of the cipher.

The most commonly used techniques to inject transient faults are those based on voltage supply glitching, temperature variations, electromagnetic pulse injections, or clock signal manipulations. For the supply voltage, an increase or decrease in the voltage supply to the chip above the tolerance level of the devices (typically 10%) can cause faults in the combinational operations or in the bits stored in the flip-flops (FFs). These faults can affect part of the circuit or cause widespread faults [3]. When considering temperature attacks, exceeding the temperature range specified by chip manufacturers for proper operation can deliberately induce faults in the chip. By configuring the chip temperature to a level at which write operations are functional while reads are not, or vice versa, multiple attacks can be launched.

Electromagnetic Fault Injection (EMFI) attacks are based on the introduction of errors in an integrated circuit using an electromagnetic pulse (EMP). When the electromagnetic field of the EMP penetrates the device, it produces anomalous voltage differences and currents within the components of the circuit. Inducing Foucault currents on the chip surface can cause a fault of up to a single bit [4].

III. Design Methodology to Protect against Attacks

Regarding the attacks mentioned above, the proposed solution uses the Xilinx Analog-to-Digital Converters (XADCs) provided by Xilinx in its Field-Programmable Gate Array (FPGA) devices. The possible applications that can be developed with these components include the reading and monitoring of the analog values of the operating voltages of the device. Therefore, in this work, this component was used to establish operating ranges outside of which the system will understand that the device is being maliciously manipulated. Therefore, an alarm signal is activated allowing the system to detect that it is being attacked and, in this case, giving a zero value as a response. With this response triggered by the alarm, an attacker cannot know whether the attack was effective or not because any data related to the data stored or processed during encryption or decryption are given in the output, completely blocking DFA attacks.

IV. Setups and Results

To test the performance of this protection, a Xilinx Nexys 4 board with an Artix 7 100T FPGA was used. In addition to the board, different tools were used: a Thermonics ATS-505-S-2 temperature control system, a Keysight e36312A power supply, an Agilent InfiniiVision DSO7054A oscilloscope with 4 G/samples and a bandwidth of 500 MHz, and a NewAE EM pulse generator called ChipSHOUTER.

A. Voltage and Temperature Setup and Results

Figure 1 presents the configuration for the manipulation of temperature and voltage ((1) Thermonics, (2) Nexys board, and (3) supply voltage). In the case of the power supply voltage, the main power supply voltage, V_{CCINT}; the memory voltages of Random-Access Memory (RAM), V_{CCBRAM}; and the internal auxiliary power supply voltage of the FPGA itself, V_{CCAUX}, are protected against malicious variations. The values established as performance limits were those established following the manufacturer's characterization tests. Outside of these ranges, the protection scheme considers the device to be under attack. For the voltage case, it is necessary to consider only tools (2) and (3) in Figure 1.

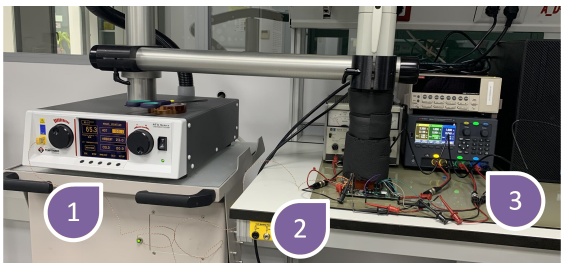

Fig. 1. Experimental setup for testing voltage and temperature schemes.

For the case of temperature variations, the XADC was configured to obtain the operating temperature values of the device and to check if the device was outside the normal operating ranges. The temperature range considered as normal operation is between 0 °C and 60 °C. For this test, the Xilinx Nexys 4 board (2), a Thermonics ATS-505-S-2 temperature control system (1), a supply voltage (3), and a computer with Xilinx Vivado software were used to monitor the results (see Figure 1).

In this case, only the temperature above the normal operating range could be tested, since subjecting the system to temperatures that were too low could produce small frozen water spots and irreversibly damage the device. The temperature was modified to obtain a temperature outside the range, which was the maximum value at 65.5 °C. The test again corroborated that the error signal was correctly triggered by turning on an LED on the board when the temperature was out of range.

B. Electromagnetic Setup and Results

In Figure 2 the EM fault attack setup is shown: (1) a Rohde&Schwarz HZ-15 EM probe for measuring the magnetic field, (2) the probe tip of the ChipSHOUTER EMP tool, and (3) the Nexys 4 board. The main objective was to test whether inserting an EMP into the FPGA would detect a voltage rise (or fall) that could be detected by the XADC. For this, a 4 mm ChipSHOUTER probe tip (diameter of the ferrite core) was used directly above the FPGA encapsulation (approximately 1 mm). The magnetic field probe surrounding the probe tip of the ChipSHOUTER was used to measure the injected magnetic field.

The success of an attack depended on the intensity of the pulse and the position along the XY plane of the FPGA of the ChipSHOUTER probe tip. There were some areas where

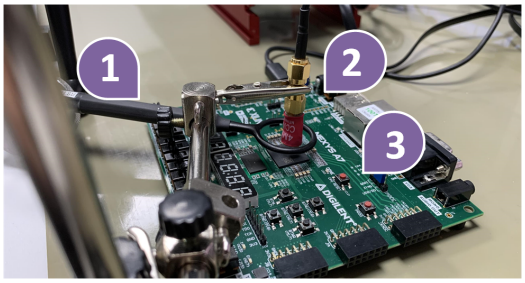

Fig. 2. Details of experimental setup for testing electromagnetic scheme: (1) near-field magnetic probe, (2) probe tip of the ChipSHOUTER directly pointing at the Artix-7 FPGA, (3) Nexys A7 board.

only one pulse was needed to detect an anomalous voltage change in the FPGA by the XADC, while in other areas the injection of an EMP would reset and clear the whole FPGA.

To ascertain whether the EMP produced a voltage change outside of the typical values, circuitry was placed at the ADC output to sample its value each clock cycle (the clock frequency was 100 MHz). If a voltage rise or fall was detected, then the alarm was triggered. As a result, pulse injection was detected in the tests, allowing us to determine that the EM pulses altered the internal voltage and therefore were detectable by the proposed scheme. In these cases, the output of the criptocircuit was zero. The efficiency of the proposed protection scheme was 100% (all effective attacks were detected) in those cases where the injected fault caused no clearing or resetting of the FPGA.

V. Conclusions

In this paper, we presented a design methodology that uses XADCs in the FPGA as a countermeasure to detect and thwart non-invasive active attacks, in particular those based on the supply voltage, temperature, and electromagnetic pulses. The proposed solution offers the possibility of using FPGA resources for protection with minimal resource cost.

Several temperature, voltage, and EM tests were performed, and the results show that once the ranges of temperature and voltage were defined, the scheme was able to detect any variation when the circuit was outside of its operating ranges.

Acknowledgments

Thanks to SPIRS Project Grant Agreement No. 952622; Programa Operativo FEDER 2014-2020 and Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía under project US-1380823; and project grant PID2020-116664RB-I00 funded by MCIN/AEI/10.13039/501100011033.

References

[1] F.E. Potestad-Ordóñez, A. Casado-Galán and E. Tena-Sánchez "Protecting FPGA-Based Cryptohardware Implementations from Fault Attacks Using ADCs," *Sensors*, vol. 24, num. 1598, 2024.

[2] Biham, E.; Shamir, A.: "Differential fault analysis of secret key cryptosystems." *Lect. Notes Comput. Sci. Adv. Cryptol.*, pp. 513-525, 1997.

[3] Barenghi, A.; Bertoni, G.M.; Breveglieri, L.; Pellicioli, M.; Pelosi, G.: "Low voltage fault attacks to AES". In Proceedings of the *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'10)*, Anaheim, CA, USA, pp. 7-12., 2010.

[4] Quisquater, J.J.; Samyde, D.: " Eddy current for magnetic analysis with active sensor". In Proceedings of the *eSMART, San Jose, CA, USA,*, pp. 185-194, 2002.