Automated experimental setup for EM cartography to enhance EM attacks

1st Erica Tena-Sánchez
Microelectronics Institute of Seville
Dept. of Electronics Technology US
Seville, Spain
erica@imse-cnm.csic.es

2nd Alejandro Casado-Galán
Microelectronics Institute of Seville
Dept. of Electronics and Electromagnetism US
Seville, Spain
alecasgal@alumn.us.es

3rd Virginia Zúñiga-González
Microelectronics Institute of Seville
Dept. of Electronics and Electromagnetism US
Seville, Spain
virginia@imse-cnm.csic.es

4th F. Eugenio Potestad-Ordóñez
Microelectronics Institute of Seville
Dept. of Electronics Technology US
Seville, Spain
potestad@imse-cnm.csic.es

5th Antonio J. Acosta
Microelectronics Institute of Seville
Dept. of Electronics and Electromagnetism US
Seville, Spain
acojim@imse-cnm.csic.es

***Abstract*—Side-channel attacks are a real threat, exploiting and revealing the secret data stored in our electronic devices just analyzing the leaked information of the cryptographic modules during their normal encryption/decryption operations. In this sense, electromagnetic attacks have been posed as one of the most powerful attacks, retrieving the secret information by analyzing the existing relation between the leaked electromagnetic radiation and the data being processed. These attacks are known as ElectroMagnetic (EM) attacks and a extremely critic point for their success is the EM probe positioning. In this paper, an automated experimental setup for EM cartography is described to enhance EM attacks and to help hardware designers to detect the possible information leakage flaws, as well as to determine the security level reached by the hardware implementations against EM attacks.**

***Index Terms*—EM cartography, cryptography, security, side-channel attacks, experimental setup**

I. Introduction

In the current information and communication based world, security in our electronic devices is a must. Electronic devices such as smart phones or smart cards, use cryptography to ensure security. These cryptographic modules are implemented both in software and hardware, but with the current trends in IoT to low power consumption, frequency acceleration and constrained resources, the cryptographic modules are usually implemented in hardware.

The cryptographic modules, due to their physical implementation, leak side-channel information such as power consumption, electromagnetic radiation or different execution times. This leaked information can be used by potential attackers to reveal the secret information stored in the device through the well known Side-Channel Analysis (SCA) attacks [1]–[4]. SCAs exploit the existing correlation between the data being processed and the leaked information to reveal the secret data, for example, the secret key used in a symmetric algorithm for encryption or decryption. One of the most powerful attacks are the electromagnetic (EM) attacks [4]–[7]. These attacks exploit the existing relation between the electromagnetic radiation of the device during its normal operations and secret keys.

To prevent EM attacks, hardware designers are encouraged to include countermeasures in their implementations. Hardware countermeasures, try to break this correlation between the leaked information and the data being processed, making impossible or at least extremely time consuming the recovery of the secret information. To evaluate the level of security of hardware devices, although there exist indirect metrics to evaluate the security without performing a EM attack, the definitive option and the one that will offer us the greatest degree of precision in the determination of the security level of our hardware device is to carry out the attack itself as if it were a hacker attack. In this sense, the designer requires to implement a EM attack to determine the level of security and be able to identify potential information leakage points.

In this paper, an automated experimental setup is presented to improve EM attacks. The complete procedure to determine the best attack point is described, as well as the results derived in our study showing the relationship between time consumption and EM cartography resolution. In this sense, the rest of the paper is organized as follows. In Section II, the state of the art of EM attacks and the experimental attack setups are analyzed. In section III, the proposed experimental setup is described, as well as the EM cartography generation procedure. Section IV show the results of our proposal applied to an Advanced Encryption Standard (AES) block cipher implemented in FPGA. Finally, in Section V, the conclusions are exposed.

II. State of the art

EM attacks retrieve the secret information of a electronic device by analyzing the existing relation between the leaked electromagnetic radiation and the data being processed. In this sense, one of the most powerful EM attack is the Correlation-based Electromagnetic Analysis (CEMA) attacks. This attack

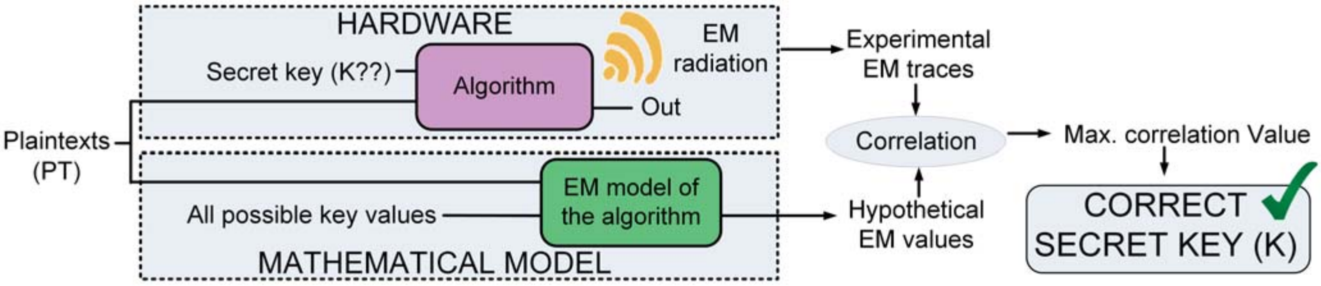

Fig. 1. CEMA attack scheme.

exploits the correlation between the processed data and the electromagnetic radiation following the scheme shown in Fig. 1. As it can be seen in Fig 1, the electromagnetic radiation is measured during encryption or decryption process of the algorithm for a given secret key k stored in the device and a externally fixed plaintexts pt. On the other hand, for the same data-set of plaintexts, through a EM model of the attacked algorithm (mathematical model), the hypothetical electromagnetic values are obtained for all possible key values. After these steps, a correlation is statistically calculated between the measured experimental EM traces and the hypothetical EM values. The correct key will be the one with the maximum correlation value [1].

Unfortunately, although these attacks seem to be easy to carry out, experimental EM attacks in real scenarios are not straightforward. One of the main problems and main success parameter in a experimental CEMA attack is the EM probe positioning. The determination of the point of attack is of vital importance, since the measured EM leakage traces should be those obtained from the execution of the logic implementing the cryptographic algorithm, and not for example from the clock generation logic.

In this sense, several works have been presented since the first SCA appeared in the literature, that propose different techniques to detect these hot points for EM attacks [8]–[10]. In [8] they propose a method to determine EM active regions of FPGAs, being one of main results that it is not necessary the exact location of the cryptographic target. Authors in [9] present different indicators to detect the hot point for the CEMA attack to implement the EM cartography, this is, to show an image of the attacked device with the locations with the highest EM leakages exploitable by CEMA attacks. Finally, in [10] a technique called Weighted Global Magnitude Squared Incoherence is presented to determine the hot spot of a cryptographic module.

As it can be seen in the literature, the probe positioning in EM attacks is a topic of real interest [8]–[10]. However, to carry out practically feasible experimental CEMA attacks, this process must be automated. The EM cartography of the target should be also obtained in the shortest possible time, for these reasons our main contribution in this paper is the proposal of an automated experimental setup for EM cartography to enhance CEMA attacks.

III. Experimental setup and procedure

To perform an EM cartography of the target device to enhance CEMA attacks in the shortest time, an automated experimental setup and procedure are proposed in this paper. As shown in the CEMA attack scheme in Fig 1, the electromagnetic traces have to be measured during encryption/decryption process. This step is the one that must be fully automated and enhanced in the experimental setup. This initial process guarantees you the repetitiveness of the attack, once the point of interest is selected, you go to it to perform the attack. For this reason, it is necessary a first step to determine the location of hot spot in the target device. To carry out this automated setup, the following equipment is needed as shown in Fig 2:

- **Personal computer (PC):** used to control all the instruments and process data.
- **Oscilloscope:** measures the electromagnetic traces from the target device.
- **EM probe:** necessary to measure the electromagnetic radiation from the target device during encryption/decryption.
- **XY-table:** used for precise EM probe positioning.
- **Target:** Field Programmable Gate Array (FPGA) or Application Specific Integration Circuit (ASIC) for the implementation of the cryptographic hardware under test.

To determine the location of the EM probe for a successful CEMA attack, the following procedure is proposed. The scheme of the automated EM cartography generation procedure is shown in Fig. 3.

- **Step1:** First, the PC carries out the connection with the rest of the laboratory equipment: oscilloscope, XY-table and target device.
- **Step2:** Then, the laboratory instruments are set into a initial state: the oscilloscope initial configuration is fixed, the EM probe is positioned with the XY-table into its initial position and the target device is reset to start an encryption/decryption process.
- **Step3:** After the initial configuration of all the devices, the PC sends the stimulus to the target device to initiate an encryption/decryption operation. Note that after the initialization, the cryptographic circuit is continuously encrypting/decrypting, since it is not performing an attack, but rather deciding where the attack is to be performed.

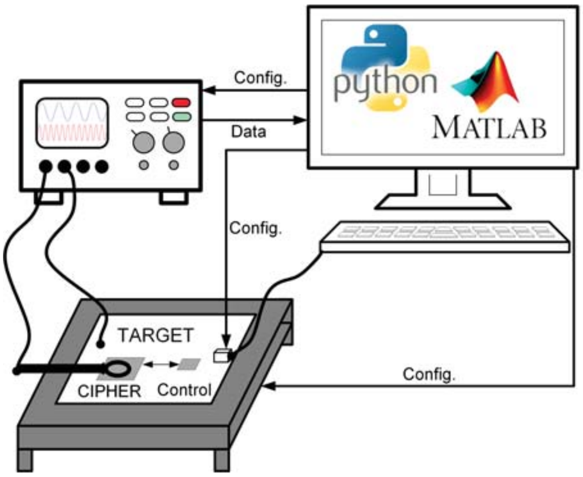

Fig. 2. Setup scheme for EM cartography.

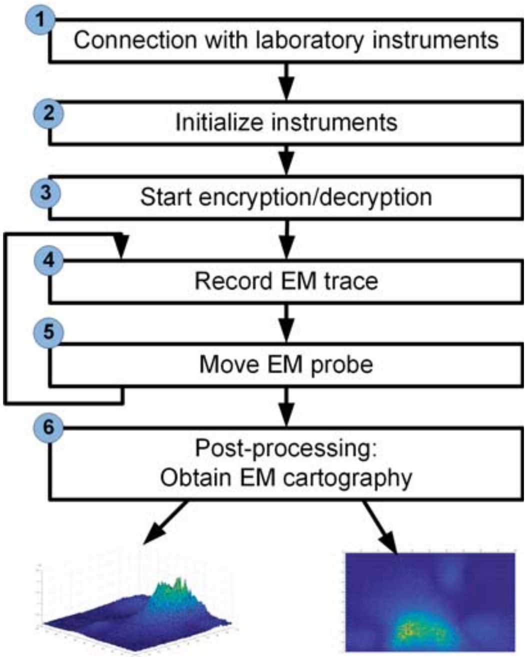
1 Connection with laboratory instruments
2 Initialize instruments
3 Start encryption/decryption
4 Record EM trace
5 Move EM probe
6 Post-processing: Obtain EM cartography

Fig. 3. Steps for the automated EM cartography generation.

- **Step4:** Once the oscilloscope has triggered, the PC records the EM trace from the oscilloscope and store it for post-processing.
- **Step5:** After that, the PC moves the EM probe to its next position and the process is repeated. This measurement process (steps 3 to 5) is repeated as many times as points have been determined on the target device while the encryption/decryption process is iterated endlessly.
- **Step6:** Once all the EM traces are measured, the post-processing is carried out generating the EM cartography of the target device and determining the hot spot to perform the CEMA attack.

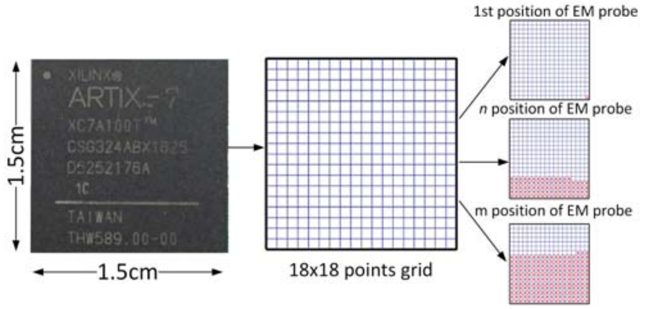

Fig. 4. Target device point selection example: 18x18 grid in FPGA Artix7.

It is important to clarify that, as stated in [8], it is not mandatory to have an extreme precision in the positioning of the EM probe. This means that although the XY-table has a great precision, it must be evaluated the number of points to measure in the target device with the gain in the effectiveness in the CEMA attack and taking into account the time needed for the whole process. In this sense, the number of points into which it will be divided the target device to position the probe will have to be previously evaluated to reach the best trade-off between accuracy and time consumption. See for example Fig 4, where the target (Xilinx Artix 7 FPGA) is divided into a 18x18 grid, having in total 324 measurement points.

The post-processing of the recorded EM traces is another critical point of the procedure. There have been presented several metrics in the literature [8]–[10] and the selection of the best one is not straightforward. In this case, depending on the target the designer/attacker must select the one that better fits the implementation. It should be ensured that the selected metric is the best choice in case the target is an ASIC or FPGA implementation, the implemented cryptographic algorithm or the specific particularities of each implementation. Please note that the main contribution of this paper is the automation of the EM cartography generation and not the proposal of different metrics to determine the best positioning of the EM probe depending on the selected target.

The procedure and experimental setup described in this paper are applicable to any cryptographic circuit and is used to generate an EM signature to determine the optimal positioning of the EM probe for a CEMA attack.

IV. Results

As demonstration vehicle, the NIST standard block cipher AES [11] has been implemented in the Xilinx Artix 7 FPGA (evaluation board Nexys 4 DDR). The AES is a symmetric block cipher that encrypts/decrypts plaintexts of 128-bits (16 bytes) using 128, 192 or 256 bit key sizes. Depending on the input key size, AES transforms the plaintexts over multiple rounds (10, 12 or 14 respectively for different input key sizes). The resulting output data is a ciphertext of 128-bit length. In our example, we implement the AES with a 128 bit key size.

The experimental setup is carried out following the indications explained in Section III. In this sense, we use a Windows 7 PC, i5 processor with 4GB RAM running Matlab to control

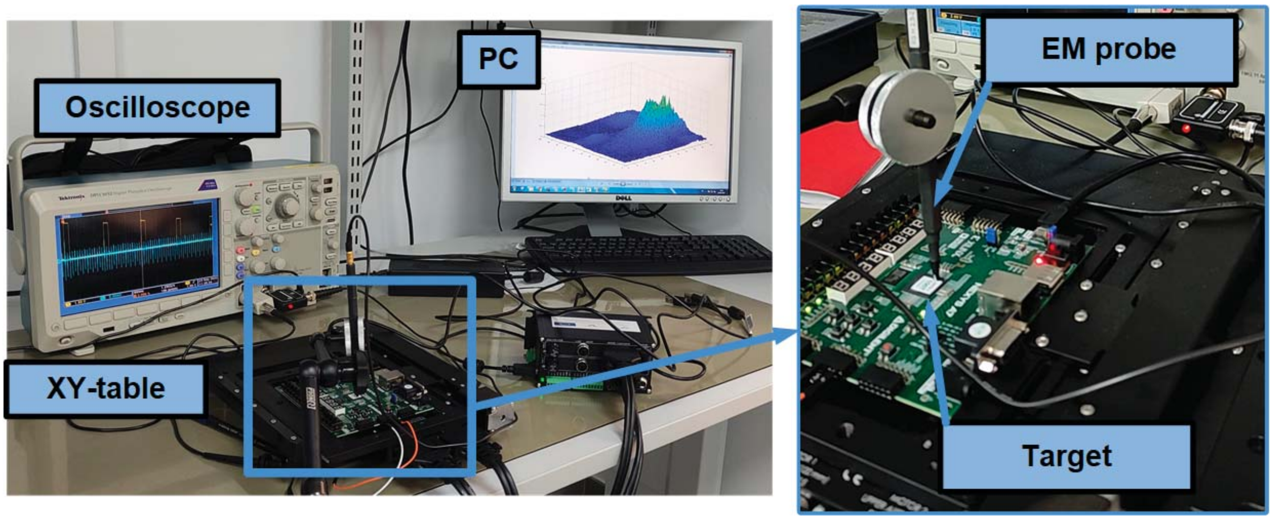

Fig. 5. Experimental setup.

the experiment and process all the data; a Tektronik DPO3032 with 2.5 GS/s and a bandwidth of 300 MHz to acquire the EM traces; Rohde&Schwarz near field EM probe and a XY-table ZABER ASR100B120B with a movement precision of 156nm in both X and Y axis. The complete setup is shown in Fig. 5 left, where a zoomed image with the positioning of the EM probe is shown in the right.

To follow the steps proposed in Section III, the automated control of the experimental setup is performed with an script in Matlab. This script, first makes the connection with each one of the instruments, oscilloscope and XY-table, and the sends the required commands to the instruments to configure them to their initial starting states. The implemented AES cipher has been designed in such a way that from a fixed key and an initial input pattern, it performs encryptions in a loop. Once the first ciphertext is generated, it will be used as a new input pattern for the next encryption. Please, note that this procedure is the initial step to obtain the best location of the EM probe to obtain the EM cartography, the CEMA attack is not performed in this step. Once the instruments are ready and the cryptographic module is encrypting, the Matlab script starts recording the EM trace for the first position. After storing the EM trace measured from the oscilloscope, the Matlab script automatically sends to the XY-table the new position for the EM probe. The EM trace for the new position is then measured. These two last steps (EM trace recording and EM probe positioning) are repeated as many times as points we have obtained in the division of the area of the FPGA.

As stated in the previous section, a critical point in the EM cartography is the selection of the number of points. This parameter will determine the precision of the location of the hot spot in the FPGA and the time consumed to perform the EM cartography. In this sense, in our experiment we have carried out 5 different grid options. In the first case both the X and Y axis of the FPGA are divided by a resolution factor of n=5, this is 25 points. In the other cases we have a grid of n=10 (100 points), n=20 (400 points), n=40 (1600 points), and n=100 (10000 points).

The time consumed to obtain the EM cartography for each case is shown in Table I. As it can be seen from Table I, the time consumption increases with the resolution factor n. This factor can be as high as the precision of the XY-table (150nm) and the area of the target device (1.5cmx1.5). However, despite being able to position the probe with maximum precision, it is necessary to evaluate whether the measurements taken at each point due to the characteristics of the near field EM probe are sufficiently decisive in improving the resulting EM cartography generation, and thus in the success of the CEMA attack.

TABLE I
TIME CONSUMPTION IN THE EM CARTOGRAPHY GENERATION PROCESS

Resolution (n)	5	10	20	40	100
# of points	25	100	400	1600	10000
Time (s)	14.28	48.16	170.86	604.32	3643.00

The metric used for the post processing of the EM traces has been selected according to the specific characteristics of the target device, in this case, the AES-128 is implemented in the Xilinx Artix-7 FPGA. The AES performs its transformation in 10 encryption rounds. Between one encryption and the following, as our implementation performs infinite looping encryptions, there are several clock cycles used to store the provided ciphertext and to send it as the new plaintext for the next encryption. Therefore we will have 10 clock cycles corresponding to the encryption phase and other clock cycles between one encryption and another considered as dummy operations, as they are not related with the encryption process. In a CEMA attack, an attacker will exploit the EM leaked information corresponding to the encryption process and only the one provided by the logic that performs the encryption.

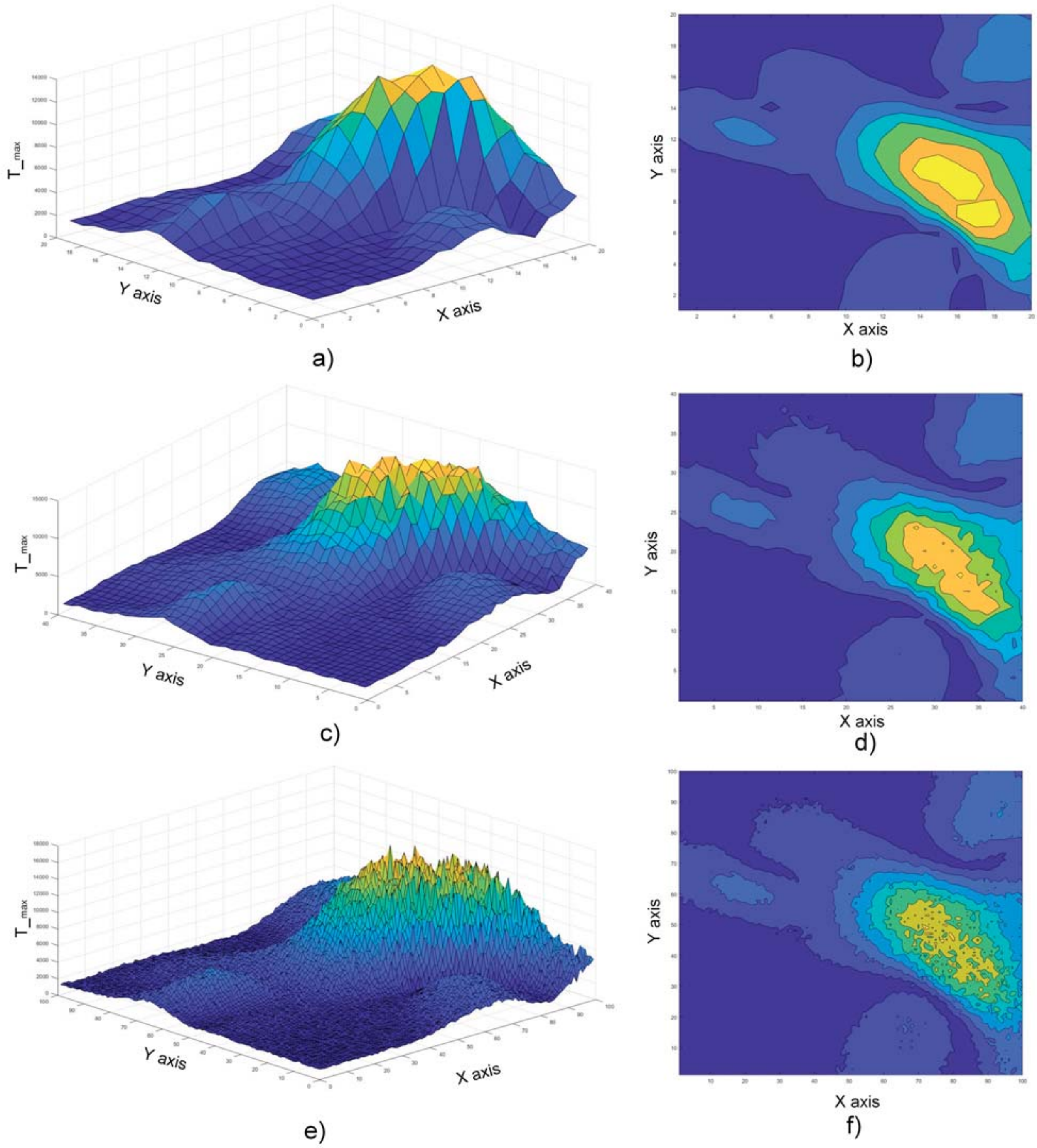

Fig. 6. EM cartography results for different resolutions: a/b) 20x20 grid, c/d) 40x40 grid and e/f) 100x100 grid.

For this reason, the selected metric in our experimental setup calculates the maximum value existing between the difference of the maximum value of the peaks in the encryption rounds with respect to the maximum value of the peaks of the dummy operations. This will determine if the logic implementing the cryptographic algorithm is active or not during encryption, thus locating the exact point for the EM probe positioning. The post-processing is carried out also in a script in Matlab, having both the automatic control of the experiment and the EM cartography generation in the same platform.

The results obtained after the post-processing stage are shown in Fig. 6. In this case, the results corresponding to a resolution of n equal to 20, 40 and 100 are shown respectively in Fig. 6-a/b, Fig. 6-c/d and Fig. 6-e/f. Both the X axis and Y axis are divided into n points, the EM probe is positioned up in each position, the EM trace is recorded, and then the post-processing is applied calculating the proposed metric defined as T_{max} value in Fig. 6. The T_{max} value in Fig. 6-b, Fig. 6-d and Fig. 6-f can be determined by the color, where the darkest colors correspond to a lower T_{max} value and the brightest colors to the highest T_{max} values. The best location for the EM probe is the one with the brightest yellow color in the figures.

As a result, it can be seen how our EM cartography generation procedure gives in a short time excellent results to determine the hot spot for EM probe positioning to enhance CEMA attacks. EM cartography or EM signature generation of the hardware implementation of cryptographic devices is extremely useful to obtain successful CEMA attack results. Both the resolution n and the metric used to generate the EM mapping are factors of enormous importance as they will fix the trade-off between successful attacks and time resource consumption.

V. Conclusions

One of the most critical points for a successful EM attack is the probe positioning. In this paper, an automated experimental setup for EM cartography generation to enhance EM attacks has been proposed.

To carry out the experimental automated EM cartography generation setup, the following equipment is needed: PC, oscilloscope, EM probe, XY-table and a target device. To validate our proposal, an experimental EM cartography has been generated over an AES implementation in a Xilinx Artix 7 FPGA. It has been shown that the selection of the number of points for the EM measurements is a critical point. The trade-off between the number of points and time consumption needs to be evaluated in order to have enough accuracy in the attack and obtain the best results.

Acknowledgment

This work has been funded by project SCAROT 1380823-US/JUNTA/FEDER, UE. Thanks to SPIRS Project with Grant Agreement No. 952622 under the European Union's Horizon 2020 programme and Grant PID2020-116664RB-I00 funded by MCIN/AEI/10.13039/501100011033.

References

[1] S. Mangard, E. Oswald, and T. Popp, ”Power Analysis Attacks: Revealing the Secrets of Smart Cards”, Springer, 2007.

[2] P. Kocher, J. Jaffe, and B. Jun, ”Differential Power Analysis”, in Proc. of International Cryptology Conference (CRYPTO'99), pp. 388-397, 1999.

[3] P. Kocher, ”Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, Other Systems”, in Proc. of International Cryptology Conference (CRYPTO'96), pp. 104-113, 1996.

[4] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.L. Danger, ”Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures”, IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 571-580, Jun. 2013.

[5] K. Gandolfi, C. Mourtel, and F. Olivier, ”Electromagnetic Analysis: Concrete Results,” in International Workshop on Cryptographic Hardware and Embedded Systems (CHES'01), vol. 2162, pp.251–261, 2001.

[6] E. Peeters, F.X. Standaert, and J.J. Quisquater, ”Power and electromagnetic analysis:Improved model consequences and comparisons,” in Integration, the VLSI Journal, Special Issue: Embedded Cryptographic Hardware, vol. 40, no. 1, pp. 52–60, 2007.

[7] J.J. Quisquater and D. Samyde, ”Electromagnetic attack,” In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security, 2011.

[8] L. Sauvage, S. Guilley, and Y. Mathieu, ”Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module,” in ACM Transactions on Reconfigurable Technology and Systems (TRETS'09), vol. 2, no 1, pp. 1-24, 2009.

[9] D. Réal, F. Valette, and M. Drissi, ”Enhancing correlation electromagnetic attack using planar near-field cartography,” in Design, Automation & Test in Europe Conference & Exhibition (DATE'09), pp. 628-633, April 2009.

[10] A. Dehbaoui, V. Lomne, P. Maurine, L. Torres, and M. Robert, ”Enhancing electromagnetic attacks using spectral coherence based cartography,” in IFIP/IEEE International Conference on Very Large Scale Integration-System on a Chip, pp. 135-155, October 2009.

[11] Pub, NIST FIPS. ”197: Advanced encryption standard (AES).” Federal information processing standards publication 197.441 (2001): 0311.