Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation

Laurent Sauvage [#1], Sylvain Guilley [#1], Jean-Luc Danger [#1], Naofumi Homma [*2], Yu-ichi Hayashi [*2]

[#] *Institut Télécom, Télécom ParisTech, CNRS LTCI*
46 rue Barrault, F-75634, Paris Cedex 13, FRANCE
[1] name.forname@telecom-paristech.fr

[*] *Graduate School of Information Sciences, Tohoku University*
6-6-5 Aoba, Aramaki, Aoba-ku, Sendai 980-8579, Japan
[2] homma@aoki.ecei.tohoku.ac.jp

***Abstract*—Side channel attack is a powerful technique to extracting secret key from cryptographic applications of embedded systems. Best results are obtained by placing a small electromagnetic probe just over areas of an integrated circuit which are leaking the most information. To find such locations, some cartography methods have been proposed in the past, but never used against asymmetric-key cryptosystems. In this paper, we target such cryptosystem, more precisely a FPGA-based RSA hardware implementation. We show that these methods are effective to locate the RSA cryptoprocessor.**

I. Introduction

Side Channel Attack appeared in the late 1990s, and exploited the power consumption [1] of a Device Under Analysis (DUA) to retrieve its secret key. Then, results from [2] have shown that the parasitic electromagnetic (EM) field radiated by the DUA could also be used for key-recovering. With an EM probe well smaller than the DUA and properly positionned, the number of measurements to be succesful could be reduced by a factor from ten to one hundred [3]. Indeed, in this configuration, the EM field acquired is mainly due to the cryptoprocessor activity, whereas a measurement of the power consumption, global, contains the activity of other parts of the DUA such as the microcontroler, the communication interface, *etc*, noise from an attacker-standpoint.

To find areas where the information leakage is maximal, the first step is to define a set of positions over the DUA. Then, for each of them, one or more observations of the EM field are collected. This is typically done with two motorized axes moving the EM probe from a position to another one. The second and final step consists in processing all of the observations to affect a value to each position. The greater this value is, the greater the information leakage at the corresponding position is. In this paper, we survey state-of-the-art processing methods which:

- take avantage of specific characteristics of the EM field temporal variations (Sec. III);
- focus on singular frequencies of the EM field spectrum (Sec. IV);
- assess the similarity level between each observation of the EM field (Sec. V);

to build a cartography of compromising areas. But first of all, we present in the next section the target of the analyses and the experimental setup.

II. Background Material

The practical results of this paper have been obtained by applying our cartography methods against the FPGA-based RSA hardware implementation of [4]. In order to show the consistency of our localization methods, we provide in figure 1 the post-place & route results for the cryptoprocessor main modules (see [4], in particular figure 3). At the very beginning of an encryption, the secret key is loaded in the **shift register K**, whose particular placement forms a kind of capital "C" on the floorplan's left. According to each key bit value, the **sequencer block**, close to the center, runs a specific operation of the **multiplication block**, at the top middle, for instance a modular squaring, followed by a modular multiplication if and only if the current key bit is set. As the multiplication block behaviour directly depends on the secret key, we have to locate this former. Hence, the multiplication block will be our analysis target. The inputs (outputs) of the multiplication block are read from (stored in) two **memories**, distributed around the sequencer and multiplication blocks. The **wrapper** on the

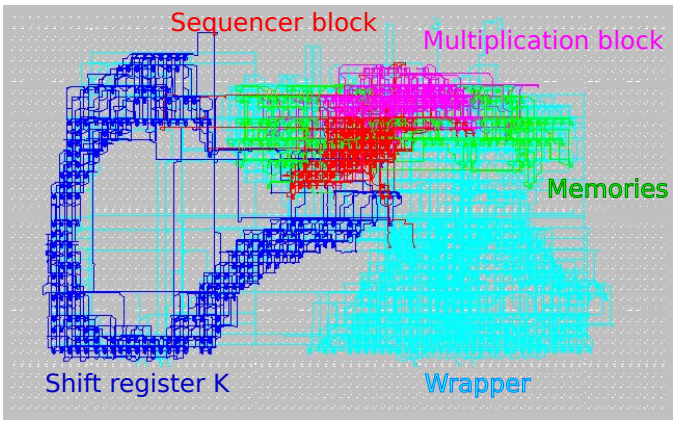


Figure 1. Post-place & route results for the cryptoprocessor main modules.

bottom left is the rest of the design: a top-level state machine and some hardwired constants such as the secret key and the plaintext message, selected via configuration switches.

The RSA implementation has been programmed on a Xilinx [5] Virtex 5 Field-programmable Gate Array (FPGA). As depicted by figure 2, we have removed its metallic lid with a cutter. This way, not only we can reduce the analysis area strictly to the FPGA silicon die, but the signal to noise ratio is also greatly improved. The measurements have been acquired using a 2 mm diameter EM probe, a 3 GHz bandwidth 30 dB gain preamplifier, and an Agilent [6] Infiniium 54854 oscilloscope, whose bandwidth and sampling rate have been set up to respectively 3 GHz and 10 GSa/s. The EM probe has been moved following a 25×25 points grid, per step of 400 μm along the X-axis, and 480 μm along the Y-axis. The grid is rather rectangular, since we covered the whole silicon die: 10 mm wide and 12 mm long.

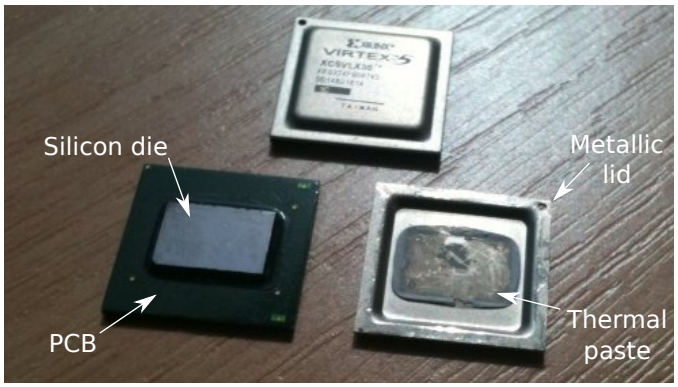


Figure 2. Photograph of the Xilinx Virtex 5 FPGA with metallic lid removed.

III. Temporal EM Cartography

The first SCA-dedicated localization methods have been proposed in [3]. They require a single observation of the EM field per position, on which a "map" function $\mathcal{M}$ is applied to resume the n samples of the temporal observation to a unique scalar. Taking the average value of the observation for the $\mathcal{M}$ function is unsuitable as it physically corresponds to a DC component, not measurable by EM probes. Considering the signal dynamic, i.e. the difference between the maximal and minimal value of the EM probe output voltage, is better but not sufficient: indeed, a high radiation level does not necessary mean a high information leakage. In the experiments of [3], the most radiating parts of the DUA are the 16 MHz and 20 MHz system clocks pins.

To overcome this problem, the authors have proposed to compute the signal dynamic difference depending on the target state: idle or ciphering. More precisely, as our target is the multiplication block, "ciphering" means performing a square or a multiply operation. Applied to our implementation, this leads to the map at the top of figure 3. An area is highlighted in the top middle, with a maximal information leakage located at (X=6.840 mm,Y=9.200 mm). The temporal variations of the

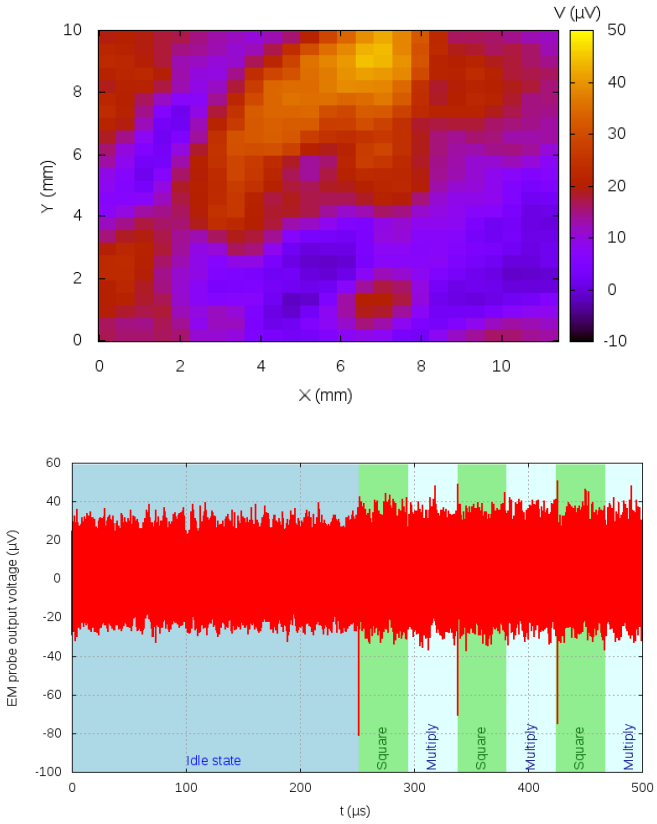


Figure 3. Map of the signal dynamic difference (*top*) and the corresponding observation for the maximal difference (*bottom*).

EM probe output voltage collected at this point are reported at the bottom of figure 3. The timeline is the following: during the first half of the temporal window, from 0 μs to 250 μs, the multiplication block is idle. Then, it switches to ciphering state, always alternating square-and-multiply operations[1] from 250 μs to 500 μs. Each peak at 250.00 μs, 337.72 μs and 425.44 μs indicates the beginning of a square-and-multiply sequence. It is incredibly hard to compare the map and the floorplan of figure 1, but as there is no remarquable activity difference between the idle and ciphering time-slots as well as between the square-and-multiply operations, we think that the EM radiation at this point are rather due to the sequencer block and writing in the memories than to the multiplication block.

We now consider another $\mathcal{M}$ function: the difference between the Root Mean Square (RMS, quadratic mean) value of the observation during the idle state, and during the ciphering state. Note that in this case, the information on the EM field sign is no more available. The resulting map is presented at the top of figure 4. The pinpointed area follows the capital

[1]The modular exponentiation is based on the left-to-right with dummy operation algorithm, a countermeasure to some attacks (see implementation details and explanation in [4].

"C" shape of the key shift register, and the point leaking the most information is at (X=3.192 mm,Y=5.200 mm). This time, the temporal variations of the EM probe output voltage, at the bottom of figure 4, distinctly show a difference between the idle and ciphering states. However, it is very surprising as the key shift register is expected to be active only at the end of each square-and-multiply sequence. We plan to explain this surprising phenomenon by further experiments.

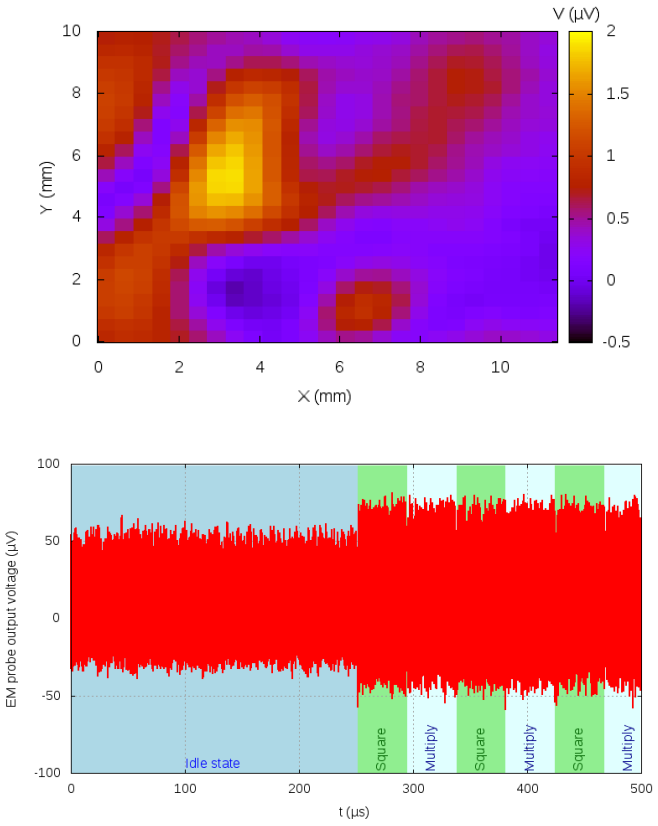


Figure 4. Map of the signal RMS value difference (*top*) and the corresponding observation for the maximal difference (*bottom*).

IV. Frequencial EM Cartography

The previous method has two main drawbacks:

- it is very sensible to noise, thus it requires a good Signal-to-Noise Ratio (SNR);
- the idle and ciphering time-slots have to be known, either by implementation (VHDL code) analysis or Simple Power / ElectroMagnetic Analysis (SPA/SEMA) [1].

One solution, presented in [3], is to turn the study into the frequential domain, by calculating the Discrete Fourier Transform (DFT) of each observation, then focusing on singular frequencies. For instance, the maps of figure 6 correspond to the EM field distribution for the odd[2] harmonics of the 50 MHz system clock. On the map for the fundamental frequency, figure 6.a, two areas are standing out: a first one at the bottom, in the middle, and a second one at the top left-hand quarter, which fades out in the map for the next odd harmonic, figure 6.b, then completely disappears in the maps for the upper odd harmonics, as in the maps of figures 6.c and 6.d. The first area is thus clearly related to the system clock. In [3], this method had enabled the authors to locate the 16 MHz and 20 MHz system clocks pins. But here, after comparison with the pinout, it appears that it is strangely not the case. Once again, working with commercial FPGAs whose details on the manufacturing process are unavailable limits the analyses.

Now, to locate the cryptoprocessor, we have to find its singular frequencies. As an observation is a serie of peaks whose amplitude varies according to the data processed by the DUA, its spectrum is that of an Amplitude Modulated (AM) signal, depicted by the following figure 5. It is made of:

1) components at multiples of the system clock frequency F_C, in blue in figure 5;
2) components at multiples of the modulating signal frequency F_M, in green in figure 5;
3) components distributed around each multiple of the system clock frequency F_C, at distances which are multiples of the modulating signal frequency F_M, in red in figure 5.

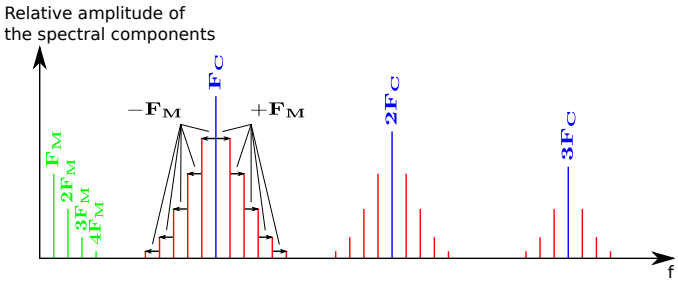
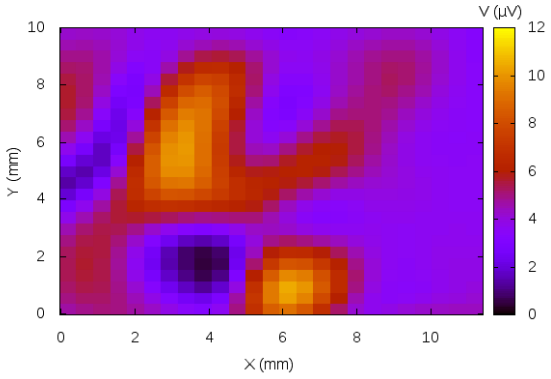


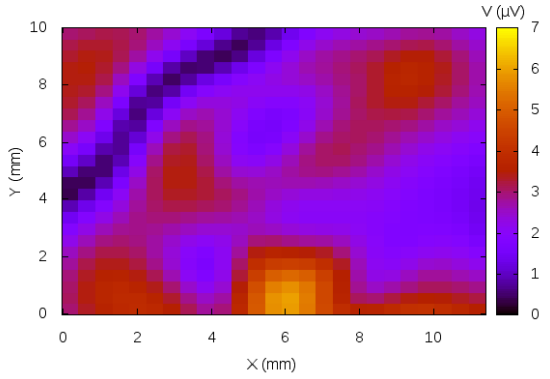
Figure 5. Frequency spectrum of an amplitude modulated signal.

The components enumerated in (2) and (3) are the singular frequencies of the cryptoprocessor. During the DFT computation, the observation is made as a periodic signal, i.e. as if the analysed cryptographic operation was repeated to infinity. In our situation, according to figure 3 (or 4), we can therefore consider that we have an idle state, followed by three square-and-multiply sequences, then again an idle state, three square-and-multiply sequences, etc. Also the length of the analysis window, 500 μs, is directly equivalent to the period of the modulating signal. Its frequency equals 2 kHz, and the singular frequencies of the cryptoprocessor are: 2 kHz, 4 kHz, 6 kHz...49.994 MHz, 49.996 MHz, 49.998 MHz, 50.002 MHz, 50.004 MHz, 50.006 MHz...The map of figure 7 is the EM field distribution at 50.006 MHz. The point leaking the most information is at (X=3.192 mm,Y=4.800 mm). With a difference of only one mecanical step on the Y-axis, this point is the same as the one found with the RMS temporal method.

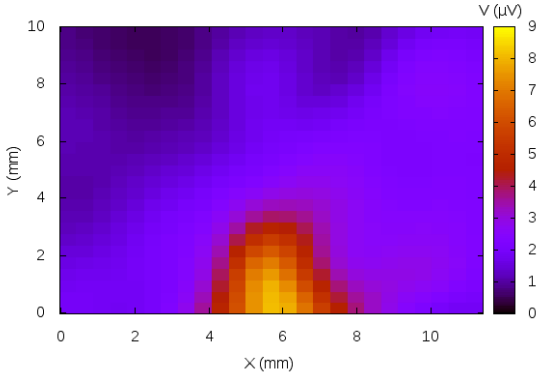
[2]As we deal with digital systems, the signals shapes are rather rectangular, thus their even harmonics are quasi null.



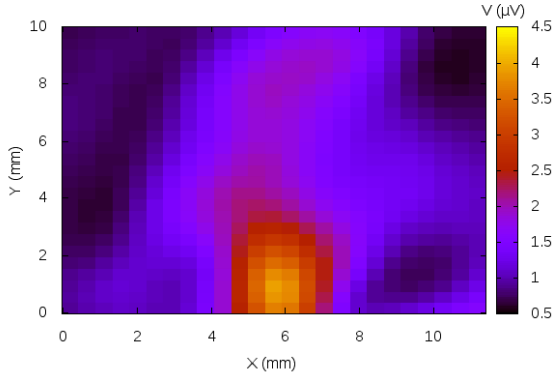
(a) 50 MHz



(b) 150 MHz



(c) 250 MHz



(d) 350 MHz

Figure 6. Maps of the EM field distribution for the firsts odd harmonics of the system clock.

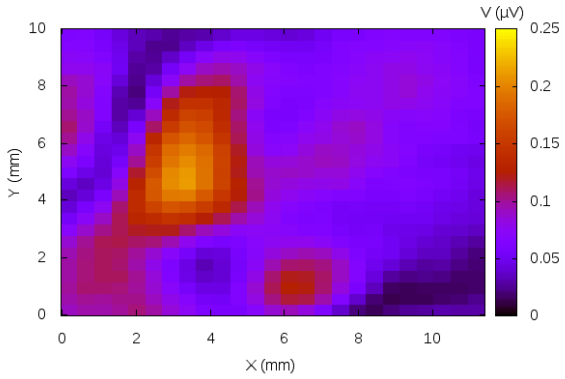


Figure 7. Map of the EM field distribution at 50.006 MHz.

V. Cross-correlation EM Cartography

Although effective, both previous methods not only need to identify the idle and chipering time-slots, but focus also on a single cryptoprocessor. In [7], a zero-knowledge method has been introduced, which provides the exhaustive list of areas of interest. This method is based on the fact that observations acquired on positions close to a same EM source have very similar shapes, whereas those on positions far each one from the others look completely different. In a first step, each position is taken as a reference, and the corresponding observation is compared with all of the others observations, using the cross-correlation function. We get as many correlation maps as positions. Hence, in the second step, the maps highlighting the same area are grouped together in a partition. Once again we use the cross-correlation function, but this time according to two dimensions. Maps are considered the sames if their correlation factor is above a certain threshold, for instance 95 %. Lastly, depending on a selection criterion, one map is extracted from each partition to build the final list. The selection criterion could be that the map to be extracted is the one with the smallest area.

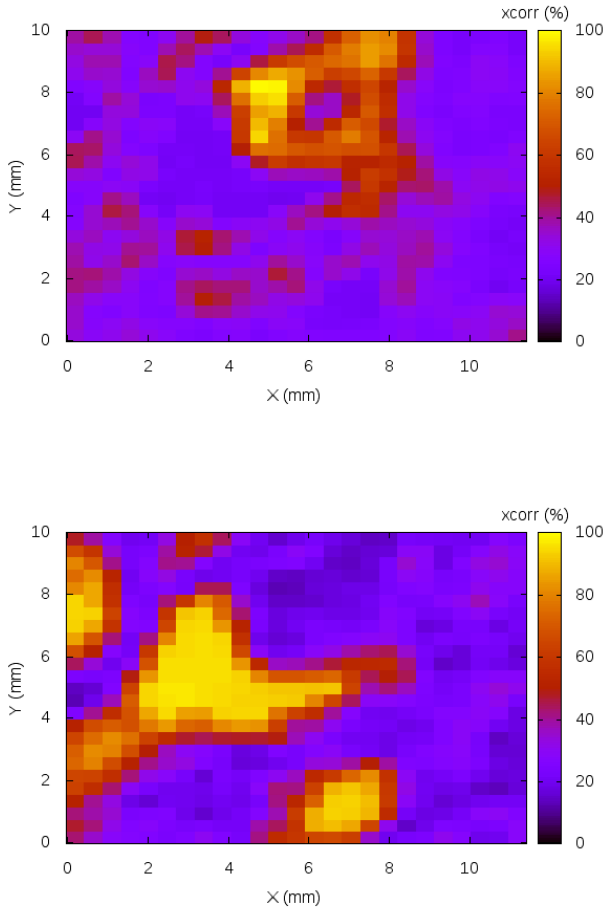


Figure 8. Cross-correlation maps.

For our RSA implementation, only two areas of interest have been found, shown in figure 8. The area identified by the bottom map is strictly the same as the one found with the RMS temporal and frequency methods, while the area pinpointed by the upper map is very close to the one found with the "signal dynamic difference" temporal method.

VI. Conclusion

In this paper, we have successfully used state-of-the-art localization methods against a FPGA-based RSA hardware implementation. Two others techniques exists [8], [9], but we have discarded them as they are data-dependant. Indeed, to be optimal, secret parameters should be known: the key, but also mask values when dealing with a protected implementation, which appears to be really difficult...

Acknowledgment

This research was supported by the Strategic International Cooperative Program SPACES (Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems), funded by the ANR (french national research agency) and the JST (Japan Science and Technology agency).

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 388–397. [Online]. Available: http://www.cryptography.com/resources/whitepapers/DPA.pdf

[2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," in *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, ser. Lecture Notes in Computer Science, Ç. K. Koç, D. Naccache, and C. Paar, Eds., vol. 2162. Springer, May 2001, pp. 251–261. [Online]. Available: http://link.springer.de/link/service/series/0558/bibs/2162/21620251.htm

[3] L. Sauvage, S. Guilley, and Y. Mathieu, "ElectroMagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack of a Cryptographic Module," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 2, no. 1, pp. 1–24, March 2009.

[4] A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, "Chosen-message spa attacks against fpga-based rsa hardware implementations," in *FPL 2008, International Conference on Field Programmable Logic and Applications, Heidelberg, Germany, 8-10 September 2008*. IEEE, 2008, pp. 35–40.

[5] Xilinx FPGA designer, "http://www.xilinx.com/."

[6] Agilent Technologies, "http://www.home.agilent.com."

[7] L. Sauvage, S. Guilley, F. Flament, J.-L. Danger, and Y. Mathieu, "Cross-correlation cartography," in *ReConFig'10: 2010 International Conference on Reconfigurable Computing and FPGAs, Cancun, Quintana Roo, Mexico, 13-15 December 2010, Proceedings*. IEEE Computer Society, 2010, pp. 268–273.

[8] D. Réal, F. Valette, and M. Drissi, "Enhancing correlation electromagnetic attack using planar near-field cartography," in *Design, Automation and Test in Europe, DATE 2009, Nice, France, April 20-24, 2009*. IEEE, 2009, pp. 628–633.

[9] A. Dehbaoui, V. Lomné, P. Maurine, and L. Torres, "Magnitude squared incoherence em analysis for integrated cryptographic module localisation," in *Electronics Letters*, vol. 45 – 15. IEEE, 2009, pp. 778–780.