Enhancing Electromagnetic Attacks using Spectral Coherence based Cartography

Amine Dehbaoui, Victor Lomné, Philippe Maurine, Lionel Torres, Michel Robert

Enhancing Electromagnetic Attacks using Spectral Coherence based Cartography

Amine Dehbaoui, Victor Lomne,
Philippe Maurine, Lionel Torres, Michel Robert

LIRMM, CNRS - University of Montpellier 2
161, rue Ada, 34392 Montpellier, France
{amine.dehbaoui,victor.lomne,pmaurine,
lionel.torres,michel.robert}@lirmm.fr

Abstract. Electromagnetic Aattacks hve been recently identified as an efficient technique to retrieve the secret key of cryptographic algorithms. Although similar mathematically speaking, Power or Electromagnetic Attacks have different advantages in practice. Among the advantages of EM attacks, the feasibility of attacking limited and bounded area of integrated systems is the key one. However, efficient techniques are required to localize hot spots, characterized by partially *data dependent* electromagnetic emissions, at which DEMA may be applied with success. This paper aims at introducing a pragmatic technique to localize quickly and efficiently these points of interest.

Key words: Side-Channel Attacks, EM emissions, Coherence analysis

1 Introduction

In the last century, modern cryptology has mainly focused on defining cryptosystems resistant against theoretical attacks. However, with the increasing use of secure embedded systems like smartcards, researchers focused on exploiting the physical syndromes leaking from secure devices during cryptographic operations to disclose the key. As a result, a new kind of attack called Side-Channel Attacks (SCA) has appeared. Among the known attacks, some exploit the timing behavior of Integrated Circuits (IC) [1], while others exploit the global power consumed by IC such as the well known Differential Power Analysis (DPA) [2]. Recently, the Electro-Magnetic (EM) emanations of embedded systems have been identified as a major threat [3][4].

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 targeting the bounded hardware area integrating the cryptographic algorithm under attack or part of it. This is all the more interesting since it also allows getting round global hardware countermeasures against power attacks such as the use of detached power supplies [5] by focusing the attack on reduced die areas.

However, this requires the use of small magnetic sensors to localize the leaking spots and thus implies a quadratic increase (with the square of the ratio between the length of the measured chip and the size of the sensor) of the number of points to be attacked using Differential Electro-Magnetic Analyses (DEMA) [3][4]. Thus, according to the magnetic sensor size, it could be very long and tedious for an attacker to apply DEMA on each possible position above the package or circuit.

Within this context, our contribution is a practical technique allowing the localization of hardware modules involved in the cryptographic operation, by localizing die areas with partially *data dependent* electromagnetic emanations. The proposed technique has several interesting properties.

Firstly, it requires only few EM measurements to be efficiently applied. Secondly, it remains efficient (a) even in presence of *data independent* EM emanations such as the ones generated by the clock tree or any *always on* analogue blocks but also (b) in presence fully *data independent* parasitic emissions such as noise. Thirdly, it allows finding positions where DEMA might be successful with a reduced set of EM traces. Finally, as last advantage, this non invasive and contactless technique can be applied with success, as demonstrated in section 4, even if the circuit under attack is encapsulated.

The remainder of this paper is organized as follows. Section 2 gives an overview of Differential ElectroMagnetic Analysis and its variants, but also some experimental results related to successful attacks performed on a standard Data Encryption Standard (DES) [13] mapped onto an Field Programmable Gate Array (FPGA). Section 3 introduces theoretical explanations about the proposed localization technique called Weighted Global Magnitude Squared Incoherence technique ($WGMSI$)and how to couple $WGMSI$ technique with EM near field scanning systems. Section 4 presents some concrete results related to the application of $WGMSI$ localization technique to different mappings on a FPGA of a same design. This section also demonstrates the efficiency of $WGMSI$ cartography to guide DEMA. Finally, conclusions are drawn in section 5.

2 DEMA overview and improvements

In this section, we first recall the principles of DEMA and the main known improvements, through a concrete example of a DEMA performed on a naive DES (mapped into a FPGA).

2.1 DEMA overview

Differential Electromagnetic Analysis introduced in [3][4] is based on the fact that EM emissions radiated by a circuit during a cryptographic operation depend strongly on the manipulated data. This attack, like Power Analysis based attack, is usually performed in three steps: data collection, data sorting and data analysis.

- *Data collection* : it consists in sampling and recording, with a sensor, the direct EM emanations radiated by the circuit or part of it depending on the spatial resolution of the sensor. This is typically done for a large number of cryptographic operations leading to an important collection of EM traces.
- *Data sorting* : it consists in extracting from the whole set of EM traces several sub-sets of EM traces accordingly to one selection function. Different selection functions allow predicting, for each possible guess made on a small part of the secret key (denoted by sub-key afterwards), few bits of intermediate words necessarily computed during the algorithm execution. Thus, for each possible guess of the sub-key, a differential curve is computed.
- *Data analysis* : it consists in identifying which guess among all possible guesses of the sub-key is the correct one, by searching the differential curve with the greatest peak.

2.2 A standard DEMA example

DEMA is a known plaintext or known ciphertext attack. The adversary ciphers (resp. deciphers) N PlainText Inputs (PTI) (resp. N CipherText Outputs, CTO) with an unknown key stored in the device, and monitors the ElectroMagnetic (EM) radiations of the device during each ciphering (resp. deciphering). At the end of the first stage, he gets N $PTIs$ (resp. N $CTOs$) and N EM traces. Each EM trace is the evolution versus time of the EM radiations of the chip.

Note that these EM traces have to be well aligned, that means that the time index of the beginning of the ciphering has to be the same for all measurements. If measurements are not well aligned (due for instance to countermeasures like random clock frequency or dummy instructions), different preprocessing techniques allow to re-synchronize EM traces [6][7][8][9][10].

Fig.1 shows several EM traces corresponding to the DES encryption of different $PTIs$ with the same key, called Simple Electro-Magnetic Analysis (SEMA), monitored on an FPGA with the acquisition plateform described in section 4.

The second stage is a statistical processing of the N $PTIs$ (resp. N $CTOs$) with the N EM traces.

In the rest of the article, the DES will be used as example, because of it is the well-known block cipher and principles of SCA stay the same on others cryptographic algorithms as, for example, Advanced Encryption Standard AES) [14]. Moreover, we consider, for convenience, that the adversary is in the case of a known plain-text attack and tries to guess the round-key 1 of the DES (the remaining 8 bits could be found with a brute-force attack). A similar algorithm allows to disclose the round-key 16 in a known cipher-text attack [20].

Because of the set of all possible values for the round-key 1 is too big to test all of them, the adversary divides usually the round-key 1 in 8 parts of 6 bits (called here sub-key) and attacks each sub-key independently and sequentially. Thus, for each sub-key, there is 64 possible values.

The adversary makes an hypothesis on the 6 bits of the attacked sub-key, and for each PTI, he computes the output (4 bits) of the corresponding sbox.

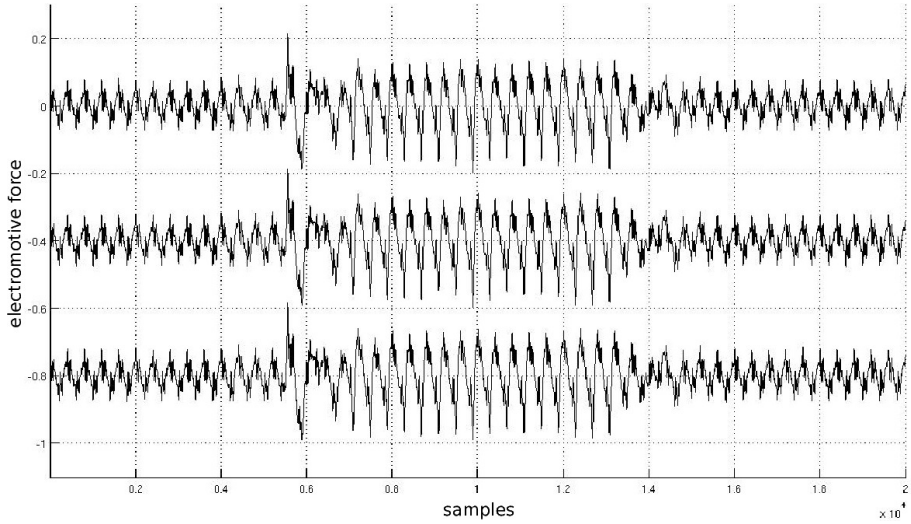

Fig. 1. several SEMA of a DES encryption on FPGA

This value is called the Intermediate Value (IV). In the state-of-the-art mono-bit DPA [2], the adversary targets one bit among the four, for instance the Less Significant Bit (LSB).

If the LSB of IV_1 (corresponding to the first plaintext, PTI_1) is equal to 0, the associated trace (T_1) is ranked in set A.

At the contrary, if the LSB of IV_1 is equal to 1, T_1 is ranked in set B. The adversary ranks all the traces, as explained above, in sets A or B, and then computes the difference of the means of sets A and B. The resulting curve is called a differential curve, and corresponds to an hypothesis of a sub-key.

The adversary computes the 64 differential curves corresponding to the 64 possible values for a given sub-key.

As explained in [2], the differential curve, noted Δ, for a sub-key hypothesis K_s, is calculated following equation 1:

$$\Delta_{K_s}[j] = \frac{\sum_{i=1}^{N} D(PTI_i, K_s)T_i[j]}{\sum_{i=1}^{N} D(PTI_i, K_s)} - \frac{\sum_{i=1}^{N}(1 - D(PTI_i, K_s))T_i[j]}{\sum_{i=1}^{N}(1 - D(PTI_i, K_s))} \quad (1)$$

where $\Delta_{K_s}[j]$ is the j-th sample of the differential curve, N is the number of EM traces used, PTI_i is the i-th plaintext, $T_i[j]$ is the j-th sample of the EM trace and D the decision function ranking EM traces in sets A or B, also called *selection function*.

If the hypothesis on the sub-key is wrong, all the computed intermediate values will be wrong in comparison with the data really processed in the chip. Then EM traces will be randomly classified in sets A and B. The mean curves

of sets A and B will be similar, and the differential curve will look-like to a thick horizontal line (mainly composed of noise).

At the contrary, if the hypothesis on the sub-key is good, all the computed intermediate values will match with the real processed data in the chip, and EM traces in set A will have the same characteristic : at the time index where the intermediate value is computed, the LSB of IV equal to 0 will not lead to an excess of power consumption. Inversely, when the LSB of IV is equal to 1, a bit more energy will be consumed at the same time index and spikes corresponding to the clock cycle where IV is computed will be greater on traces in set B than on traces in set A. When computing the difference of the means of the 2 sets, a spike will appear at the considered time index of the differential curve, which indicates that the sub-key hypothesis is good.

Fig.2 represents the 64 differential curves computed following guesses of the sub-key 1 of the round-key 1 of the DES, using 500 EM traces. Differential curves corresponding to bad guess of the sub-key are drawn in cyan, whereas the curve corresponding to the good guess of the sub-key is drawn in black, and has the greatest peak.

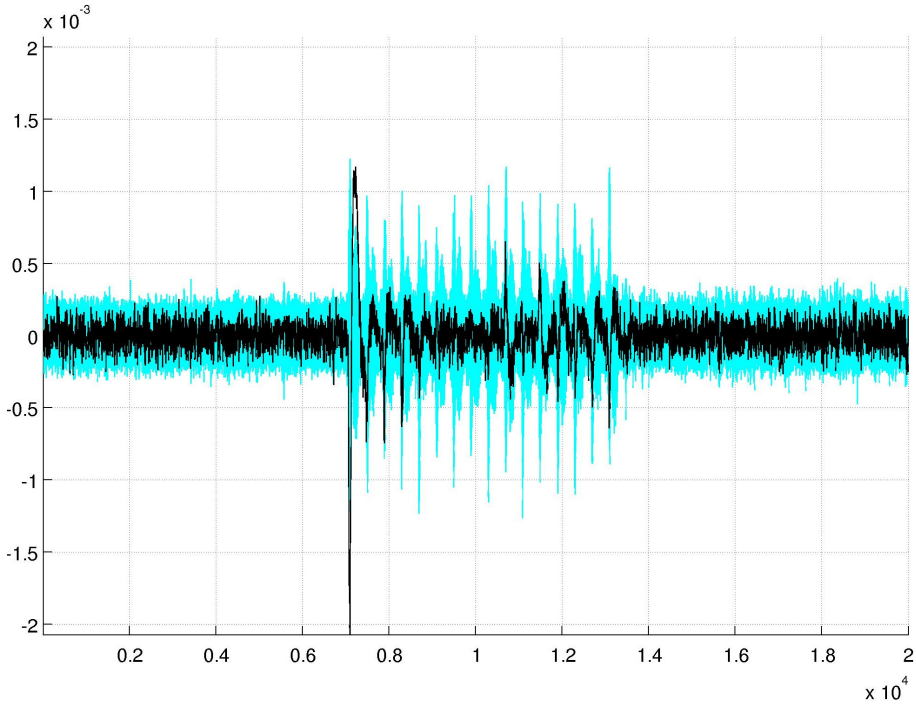

Fig. 2. Example of a successful DEMA: 64 differential curves computed following guesses of the sub-key 1 of the round-key 1 of the DES, using 500 EM traces

This processing is applied on each sub-key to guess the eight parts of the round-key 1.

2.3 Improvements of DEMA

From this first idea, different improvements have been proposed.

Hamming Weight vs Hamming Distance power model

In the original DPA algorithm and as explained above, the selection function follows the Hamming Weight (HW) power consumption model. Actually this model does not match exactly with the reality. Indeed, the power consumption of devices built in CMOS technology is generally considered in terms of two components [11]:

- *Switching power component* : related to the charging and discharging of the load capacitance at the gate output.
- *Short circuit power component* : during the transition of the input line from one voltage level to the other, there is a period of time when both the PMOS and the NMOS transistors are on, thus creating a path from VDD to VSS.
- *Static power component* : due to leakage, that is present even when the circuit is not switching. This, in turn, is mainly composed of two components - gate to source leakage, which is directly though the gate insulator, mostly by tunneling, and source-drain leakage attributed to both tunneling and sub-threshold conduction.

The two first components are related to the processed data, and in case of an inverter, it is not its output state that leaks through its power consumption, but its switching from one state to another.

So the Hamming Weight power model could be improved by considering the switching rather than the output state [12] (the Hamming Distance (HD) between the previous and the new state) :

- transitions 0 to 0 and 1 to 1 do not lead to an excess of power consumption. So, in the example of part 1, if the value of the LSB does not change, EM trace associated to the considered IV has to be ranked in set A.
- transitions 0 to 1 and 1 to 0 involve an excess of power consumption and the corresponding EM trace has to be ranked in set B.

Moreover, rather than considering an output bit of a sbox, one can consider the bit linked to the previous one in R1 [13]. Thus, as the adversary knows the value of this bit in R0 (because he knows the PTI), and assuming that R0 and R1 are stored in the same register which is updated at each round, one can compute the hamming distance between the value of the targeted bit in RO and R1. In this case, it is not the power consumption of an inverter which is estimated, but the power consumption of a flip-flop.

Multi-bit DEMA

Another way to improve DEMA attacks consists in considering the four bits linked to the output of the sbox rather than one. One can, as proposed in [15], compute the differential curve for each bit among the four of the output of the sbox, and sum the four differential curves.

One can also rank traces following another criterion [16]: we add the number of switching bits among the four considered, and if this sum is smaller than 2, we rank the associated trace in set A, and if the sum is greater than 2, the trace is ranked in set B.

Correlation ElectroMagnetic Analysis (CEMA)

The first class of *selection function* (also called *distinguisher*) described before, is called *Difference of Means*. But the main idea of the DEMA is to find which hypothesis of the sub-key is the most correlated to the EM radiations of the chip. From this idea, Brier and al. have proposed in [12] to use a well-known statistical tool, the Pearson correlation.

Considering that the adversary has ciphered N $PTIs$, and has obtained N EM traces, he can compute, for each sub-key hypothesis, the N IVs. Thus, for each time index j of the EM traces, he computes the Pearson correlation between the row-vector composed of the N IVs and the row-vector of the EM radiations of the N EM traces at time index j. Doing this computation for each j will give a differential curve as in the case of a DEMA.

3 Global Magnitude Squared Incoherence

As demonstrated in section 2, performing even a simple EM attack, requires collecting a significant number of EM traces, and thus could be time consuming even if the latter analysis is done at only one position above the attacked cryptographic modules.

The situation becomes much more critical or even unpractical, as discussed in section 1, if an adversary uses tiny sensors to attack a circuit or equivalently if a circuit provider aims at demonstrating the robustness of its designs against EM attacks performed with such tiny probes.

Considering our previous example, one may to plan collecting, at 71x71 positions above the Spartan3 core (displacement step of 100μm), 10000 EM traces, using a magnetic loop with a 100μm diameter, in order to determine if EM emissions may be exploited or not by an adversary. However, this would result, in our example, in collecting EM traces during approximately 70 days.

This situation leads to the following question: how efficiently and quickly position tiny probes ? One may naturally think, to solve this problem, in performing a standard EM near field scan of the surface in order to localize the cryptographic modules. However, as explain below, this is often insufficient.

3.1 Problem definition

Let us consider, for simplicity, that there are only two local sources of EM emissions within the chip: the source CB (corresponding to the cryptographic block) which is *data dependent*, and a source S (such as clock, or an *always on* analogue block), which is *data independent*.

In that case, if a probe placed close to the IC surface but far from CB and close to S collects: only a small fraction of the *data dependent* emissions radiated by CB (since the magnetic field amplitude decreases rapidly as the square or the cube of the distance [18]) and large portion of the emissions of S.

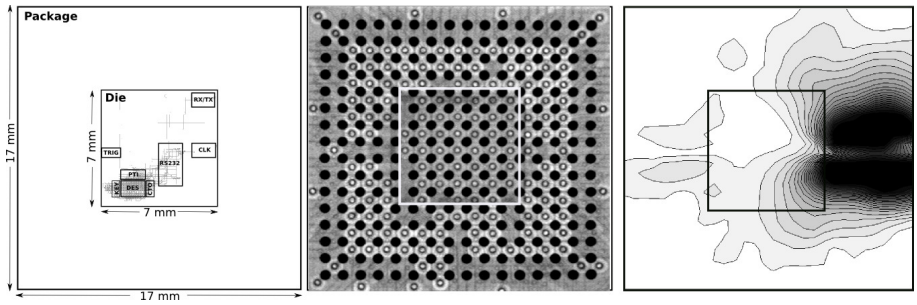

Fig. 3. (a) Design floor plan (b) X-Ray photography (c) Peak to Peak EM amplitude map

On the contrary, if the probe is placed really close to CB, the probe collects a large fraction of the *data dependent* emissions radiated by CB during its operation and a small portion of the emissions of S. From the considerations above, one may conclude that positioning the probe closed to the co-processor CB, results in collecting time domain traces differing significantly one from another, and therefore that it is easy to localize the cryptographic module. However, these last claims do not hold !

Indeed, if the EM emissions radiated by the source S are significantly greater than the emissions of the CB or, if S and CB sources are really close one from the other, it is still extremely difficult to localize CB, even if the probe is placed just above, since most of the signal collected by the probe is generated by S.

As a result, any localization technique based on time domain amplitude analyses may not work in presence of large EM *data independent* emanations sources such as clock generators, PLL or I/O interfaces, or even in presence of large environmental electromagnetic noise sources.

As an illustration, Fig.3c shows a map revealing the maximum amplitude of the EM emissions measured at several coordinates of the FPGA package surface during a DES ciphering (this EM emission maps has been obtained with the experimental setup introduced section 4). Fig.3b is an X-Ray photography of the package containing the circuit under attack. Finally, Fig.3a discloses the

routing (obtained with Xilinx ISE tool suite) of the considered circuit, running at 50MHz and integrating a DES module, a finite state machine and a RS232 interface for communication purpose.

As shown, it appears impossible to correlate Fig.3a with Fig.3c even if the die area is roughly known thanks to the X-Ray photography Fig.3b. It thus appears all the more difficult to identify the DES module on this kind of EM cartography and thus to decide where to position the magnetic sensors above the package to perform a successful DEMA only on the DES module, in order to avoid potential global hardware countermeasures such as [5].

3.2 Fundamentals of Global Magnitude Squared Incoherence

About the behavior of EM emissions of IC

DPA exploits by statistical means the *data dependent* behavior of the switching current consumed by circuits during a computation of a cryptographic module. This behavior is due to inner properties of the CMOS logic which consumes energy (much more than in the idle state) only to switch from one logical state to another [17].

EM emissions of a circuit are mainly generated by flows of electrical charges through the different metal wires connecting logic gates but also trough wires supplying the circuit [18][19]. Since the switching of gates generates a current flow through the circuit interconnect, we may conclude that these switching generate some *data dependent* EM emissions at different points in the circuit according to the power distribution network [18][19]. These *data dependent* behaviors may be exploited by statistical means, using for example DEMA [3][4], to retrieve the secret key.

Even if the magnitudes of both power consumption and computation time of logic cells are roughly known, it is extremely difficult to deduce any characteristic about the EM emissions generated by gates due to the complexity of the power distribution grid of actual IC. As a result, the only conclusion we may draw and consider in the remainder of the paper is that gates generates some EM perturbations and more precisely generates some *data dependent* harmonics located somewhere in the whole EM emission spectrum.

Within this context, the proposed technique allows disclosing the *data dependent* behavior of EM emissions in the frequency domain without making any assumption on the EM emission characteristics. It is based on spectral incoherence analysis of two time domain signals as detailed below. The only observation on which is based the method is the following: considering two successive hardware operations, we are sure that some gates switch during one computation and does not switch during the other, while some gates switch during both operations. This leads to the following intuitive conclusion that guides the development of our proposal: between two cryptographic operations some characteristics of the EM emissions remain constant (coherent) from one operation to another, while some characterristics completely change (are incoherent). Such

a behavior is said partially *data dependent* in the rest of the paper and the proposed $WGMSI$ technique aims at disclosing circuit areas characterized by this behavior.

Weighted Global Magnitude Squared Incoherence

The Magnitude Squared Coherence (MSC) between two signals $w_1(t)$ and $w_2(t)$ is a real-valued function of frequency with values between 0 and 1. It is defined by the following expression:

$$MSC_{w_1,w_2}(f) = \frac{P_{w_1,w_2}(f)^2}{P_{w_1,w_1}(f).P_{w_2,w_2}(f)} \tag{2}$$

where $P_{w_1,w_1}(f)$, $P_{w_2,w_2}(f)$ are respectively the power spectral density of $w_1(t)$, $w_2(t)$, and $P_{w_1,w_2}(f)$ is the cross power spectral density of $w_1(t)$ and $w_2(t)$. At a given frequency f, a $MSC(f)$ value of 1 indicates that the two signal spectra have exactly the same amplitude i.e. are coherent while a value of 0 means that the signal spectra are different i.e. incoherent. Alternatively, one may compute the Mean Squared Incoherence $MSI(f)$ defined by (2). This criterion has also its values between 0 and 1 but indicates rigorously the contrary of (1).

$$MSI_{w_1,w_2}(f) = 1 - MSC_{w_1,w_2}(f) \tag{3}$$

Considering the whole spectra of two sampled time domain signals, one may compute respectively the Weighted Global Magnitude Squared Coherence or Incoherence coefficients ($WGMSC$ and $WGMSI$ factors) between two time domain signals according to the definitions (3,4) that consider the signal $w_2(t)$ as a reference. In these definitions, nf is the number of frequency values at which the $MSC(f)$ and $MSI(f)$ coefficients are computed, BW is the considered frequency bandwidth and $A_{w_2(t)}$ is the power spectrum amplitude at the f frequency.

$$WGMSC = \sum_{f \in BW} \frac{MSC_{w_1,w_2}(f)}{nf} . \frac{A_{w_2}(f)}{\max\limits_{f \in BW}(A_{w_2}(f))} \tag{4}$$

$$WGMSI = \sum_{f \in BW} \frac{MSI_{w_1,w_2}(f)}{nf} . \frac{A_{w_2}(f)}{\max\limits_{f \in BW}(A_{w_2}(f))} \tag{5}$$

$WGMSI$ and $WGMSC$ have values ranging between 0 and 1. Considering the $WGMSI$, a high value indicates that $w_1(t)$ and $w_2(t)$ have perfectly incoherent spectra, while a low value indicates the contrary. It is to be noted that the right hand term of (4) is a key term. Indeed, it weights $MSI(f)$ value such that fully incoherent and high amplitude harmonics have more impact on the final $WGMSI$ value than fully incoherent but low amplitude harmonics.

Table 1. $WGMSI$ values

WGMSI values calculated between :	traces collected above clock nets	traces collected above the DES module	Ratio
data1 & data1	0	0	NaN
data1 & data2	2.8 10^{-5}	2.6 10^{-3}	90.9
data1 & data3	2.1 10^{-5}	2.5 10^{-3}	116.8
data1 & data4	2.4 10^{-5}	2.4 10^{-3}	100.4
data1 & data5	2.4 10^{-5}	1.7 10^{-3}	70.5

Illustrations

To illustrate the proposed definitions, 5 time domain EM traces were acquired during 5 different ciphering of a DES module ($50MHz$). These traces, shown in Fig.4, have been collected with 500μm diameter probe placed respectively above a DES module (Fig.4a) and above some nets distributing the clock signal (Fig.4b). As a result, one may expect that curves Fig.4a are partially *data dependent* traces while, waveforms Fig.4b are completely *data independent*. To validate this assumption, $MSC(f)$ were computed.

Fig.4c gives the $MSC(f)$ evolution with respect to frequency for both partially *data dependent* and fully *data independent* traces. As shown, the $MSC(f)$ values obtained considering traces collected above some clock nets have, as expected, values closer to 1 over a wider frequency range than the $MSC(f)$ values computed with traces collected above the DES module, validating the above discussion.

The obtained $MSC(f)$ values were gathered to compute the $WGMSI$ coefficients. As expected again, $WGMSI$ values (Table 1) corresponding to acquisitions above the clock nets are two magnitude order lower than that corresponding to acquisitions above the DES. However, the latter values remain low meaning that only few harmonics are incoherent or that the amplitudes of those harmonics is significantly lower than those of coherent harmonics. Hence, the used term of partially *data dependent* EM emission.

Considering these results, one may consider that the $WGMSI$ criterion appears efficient enough to differentiate a partially *data dependent* behavior from a *data independent* one and may be used during a magnetic near field scan of a circuit to localize area with partially *data dependent* EM emissions.

3.3 Coupling $WGMSI$ criterion with EM near field scanning

Coupling $WGMSI$ analysis with near field scanning system to localize the points characterized by partially *data dependent* EM emissions and thus leaking spots is straightforward. The basic idea is to collect for each (X,Y) coordinates above

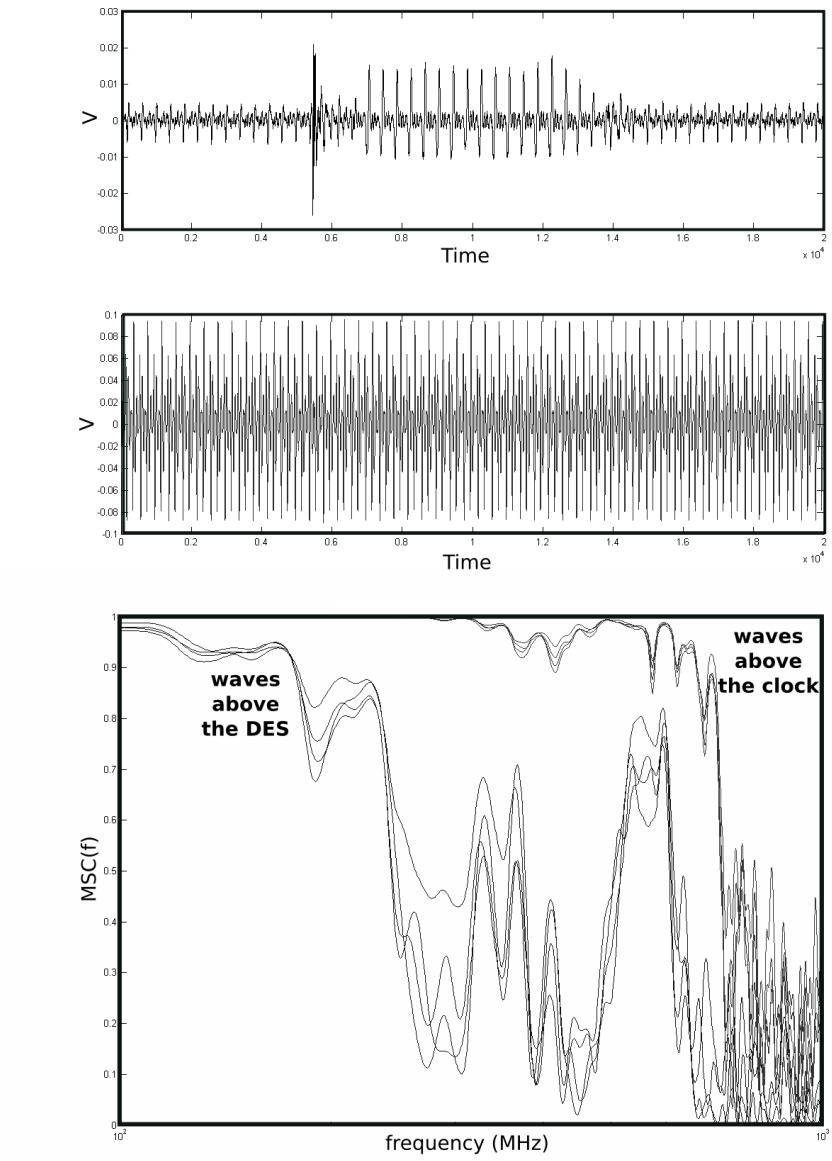

Fig. 4. (a) EM traces collected above the DES (b) EM traces collected above clock nets (c) Evolution with frequency of the corresponding MSC coefficients

the integrated circuit at least two different time domain traces of the magnetic field corresponding to two different data processing. Finally, $WGMSI$ values are computed for all (X,Y) positions. This provides $WGMSI$ cartographies revealing positions characterized by partially *data dependent* EM emissions.

Note however, that computing $WGMSI$ values for more than two data and averaging the results is not theoretically required but may lead to better results in practice.

4 Experimental Results

To validate the effectiveness of the $WGMSI$ analysis in localizing spots with partially *data dependent* EM emissions, 2 kinds of validation were performed. The one aimed at correlating the obtained $WGMSI$ cartographies with the design floorplans while the second aimed at demonstrating that spots characterized by the highest $WGMSI$ values are good candidates for DEMA.

4.1 Experimental setup

These two experimental validation campaigns were achieved with the measurement platform showed Fig.5. It is composed of:

- an oscilloscope, with a 2.5GHz bandwidth, to sample at 40GS/s the time domain evolutions of the measured signals,
- a low noise 63dB amplifier with a 1GHz bandwidth,
- an handmade magnetic loop with a 500μm diameter, and a bandwidth greater than 1GHz,
- a motorized stage allowing positioning along X, Y and Z axes the probe with a resolution of 10μm,
- a PC to controls the whole measurement setup, i.e. provides data to the DES module through an on chip RS232 module and store the measured EM traces from the scope, and controls the motorized stage.

4.2 Analyzed Design

The two aforementioned validation steps were performed considering a design mapped onto a FPGA circuit and more precisely a Spartan3-1000 Digilent board. Note the Spartan die is encapsulated in a cavity-up Ball Grid Array (BGA) package. The mapped design integrates a RS232 block to communicate with the PC, a finite state machine that manages the communications and the behavior of the chip. Three different floorplans of this design were elaborated with ISE tool suite as shown Fig. 6. This was done to definitively validate the efficiency of $WGMSI$ map in disclosing area with partially *data dependent* radiations.

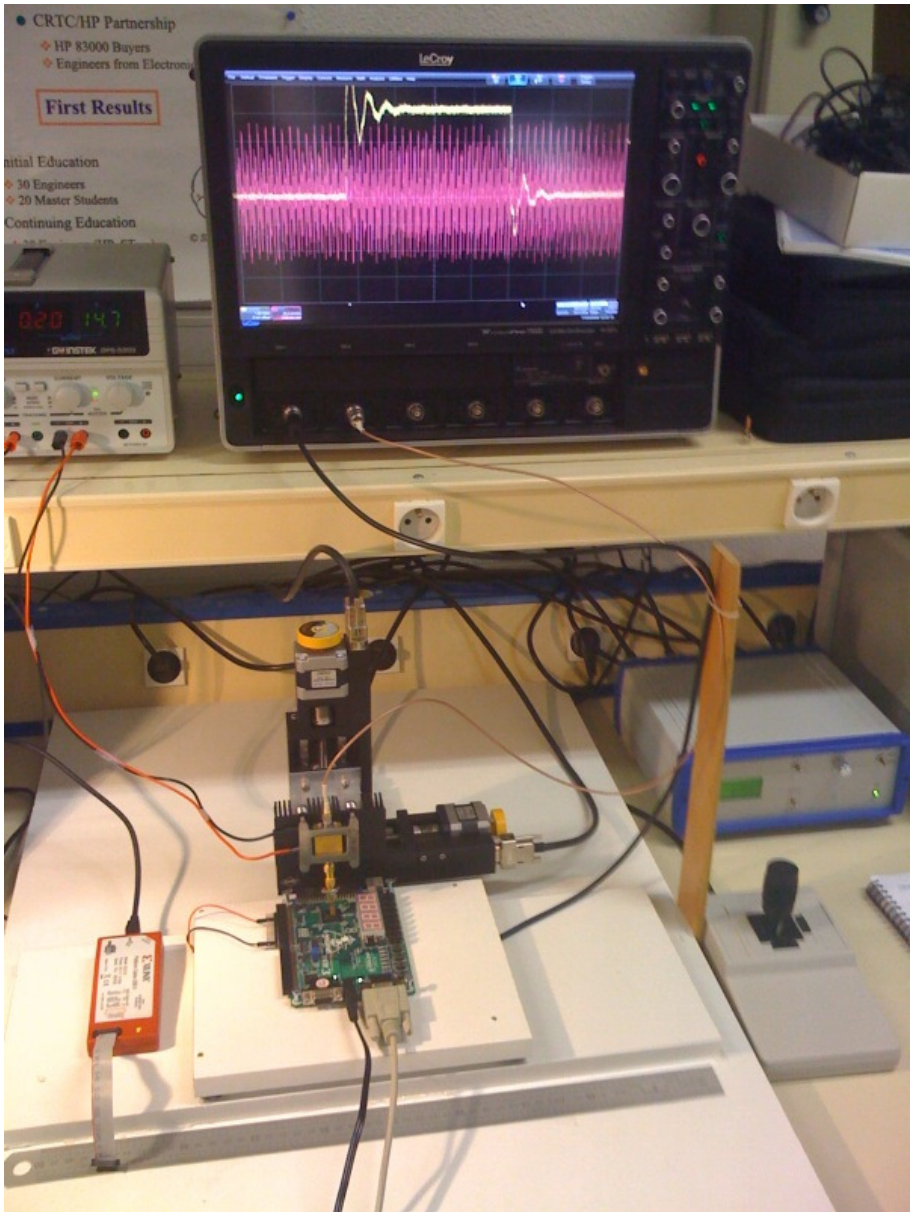

Fig. 5. near field scan and DEMA attack platform

4.3 *WGMSI* maps vs. design floorplans

WGMSI maps aim at disclosing (X,Y) coordinates at which the EM emissions captured by the probes are partially *data dependent*. As a first validation, we therefore scanned the whole package surface during DES ciphering operations and computed the *WGMSI* maps for the 3 considered mappings. The expected result was, at least, to localize the DES module and more precisely to define an area (characterized by higher *WGMSI* values) containing the DES module or part of it since (a) the probe was placed at roughly 500μm from the die and (b) since EM waves are dispersive. Note that the distance from the probe to the die was estimated by removing the package of an identical FPGA and measuring the package thickness. This procedure also allowed measuring the die dimensions (incorporating the IO pads): roughly 7mm by 7mm.

The whole package was scanned with a displacement step of 500μm. This resulted in acquiring EM emissions at 1225 coordinates for each mapping. It tooks 2 hours, for one mapping, to collect the EM emissions corresponding to 5 different encryptions. Note that to increase the Signal to Noise Ratio, each ciphering was performed 20 times and the average computed.

Fig.6 shows the 3 obtained *WGMSI* maps. The lower left map of Fig.6 is to be compared to Fig.3c. This comparison demonstrates that *WGMSI* map provides more valuable information than a maximum time domain amplitude analysis.

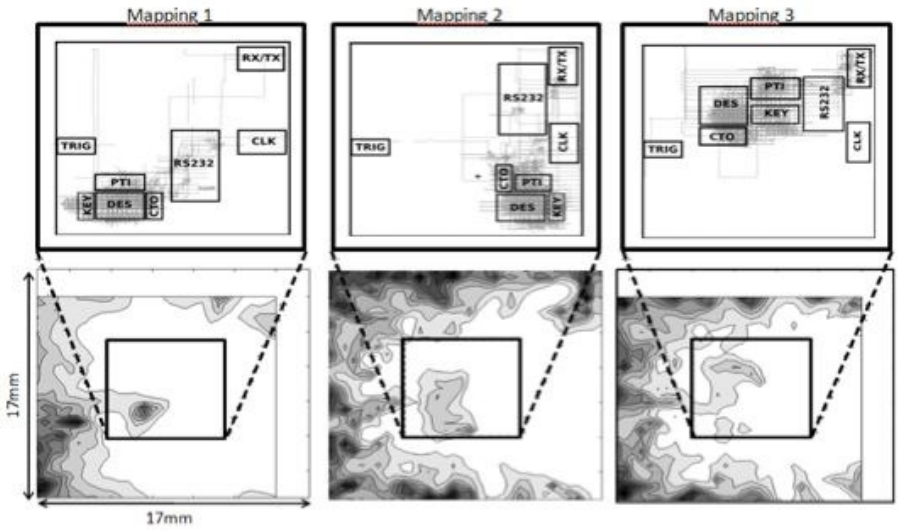

Fig. 6. circuit oorplans and related full package *WGMSI* maps obtained for the three considered mappings of the design

Moreover and as expected the comparison of these maps with the corresponding floorplans demonstrates, considering the accuracy of the die size measure ($0.5mm$), that $WGMSI$ criterion allows disclosing the hardware area corresponding to the DES module. One surprising point is that areas with partially *data dependent* EM emissions have different size even if the DES module occupied roughly the same number of slices.

This is especially true for $WGMSI$ maps corresponding to mappings 1 and 2 that disclose significantly larger and smaller areas than that effectively occupied by the DES module. This is probably due to the power/ground network specificities effectively involved in the supply of the DES module in each mapping; supply rails being recognized as important sources of EM emanations [18][19].

Nevertheless, as illustrated by Fig.7, $WGMSI$ cartographies allow selecting rationally a small number of points (typically 20 to 30 in our testcases) above the die among 225 as interesting candidates for DEMA. Next paragraph aims at evaluating if these points are effectively good candidates for EM attacks.

4.4 *WGMSI* and DEMA attacks

In order to further evaluate the efficiency of the $WGMSI$ criterion, a last validation step has consisted in elaborating a DEMA map of the mapping 3. Several EM attacks were thus performed at different positions of a package area above the die.

The architecture of the DES co-processor being iterative with a fully parallel computation of a round in a clock period, it was therefore possible to use the Hamming distance model, considered as the most efficient when applicable.

For each attacked position, 5000 EM traces were acquired; each trace was obtained by averaging 20 times the signal to increase the Signal to Noise Ratio. Then, we launched on each selected position CEMA attacks on first and sixteenth rounds, following the original CPA attack from Brier and al. [12]. More precisely, a correlation coefficient was computed, for each time sample, every time a new trace was collected. This was done to check the key guess stability by fixing an arbitrary threshold at 100 iterations with the good key to decide that CEMA has definitely found the key accordingly to the DPA contest rules [20].

Following this protocol, several maps were obtained; Fig.7 groups some of them. Fig.7a gives the percentages of correct guesses (among 4900 guesses done during the CEMA), of the sub-key provided to Sbox1 during round 1. On this map, darkest areas correspond to highest percentages of correct guesses while (a) the black curve represents the boundary of the design 3 and (b) black rings correspond to the 25 highest $WGMSI$ points (among 225 values computed). It is to be noted that most of these points coincide with coordinates at which the percentage of right sub-key guesses is greater than 45%, which is a sufficiently high threshold to consider CEMA as successful.

Fig.7b reveals areas at which the full key is obtained with the lowest number of traces. This map must be interpreted according to the following criterion: the darkest the area is, the lower is the number of traces required to disclose the full key. Note that white areas correspond to coordinates at which the CEMA failed.

Once again, the right hand darkest areas coincide with some high $WGMSI$ points.

The above results partially demonstrate the efficiency of the $WGMSI$ criterion in selecting rationally few points to be attacked. Indeed, some coordinates at which an attacker may obtain a high percentage of correct guesses or the full key are not detected by $WGMSI$ cartographies. To our opinion, these points correspond to a Gnd or Vdd rail close to the clock pad. This close vicinity with the clock pad reduces the weights involved in (4) due to high amplitude harmonics generated by the clock. As a result, the rank of these coordinates is lowered. There is thus room to improve the weighting policy of the MSI coefficients.

To definitively demonstrate the interest of the $WGMSI$ criterion as defined in this paper, we computed the percentage of points falling into $WGMSI$ bins. This binning of the whole population done, we computed the percentage of successful CEMA attack in each bin. Fig.8 gives the results. As shown, the percentage of successful CEMA by bin increases with the $WGMSI$ value validating the interest our proposal, while the percentage of points falling into the corresponding bins decreases with the $WGMSI$ value.

4.5 WGMSI vs EM analysis maps

If the above results demonstrate the efficiency of the $WGMSI$ technique in disclosing some of the main hot spots from an attack point of view, they do not allow quantifying what could be the benefits in term of data collecting time reduction. This paragraph aims at providing a first order evaluation of this time reduction considering our DES implementation (design 3). In order to quantify the time cost of elaborating a $WGMSI$ map, Tables 2 and 3 report respectively the time required to collect:

- 10000 different EM traces (corresponding at 10000 data ciphering) to elaborate an attack cartography, i.e. map disclosing the leaking points of the package surface,
- 3 averaged EM traces corresponding to 3 different data ciphering (repeated 20 times) to obtain a WGMSI map.

As shown, the time required, to obtain a $WGMSI$ map, represents less than 3% of the time spent to collect EM traces for attacks at all positions. This definitively demonstrated the interest of the $WGMSI$ technique to guide the EM analysis by ranking the positions to be attacked. Note that the values reported in tables 2 and 3 were extrapolated from the measurement of the time spent to collected 10000 data at a given position.

5 Conclusion

In this paper, a new technique has been introduced. It is based on the assumption according to which: from a data processing to another one, EM emissions

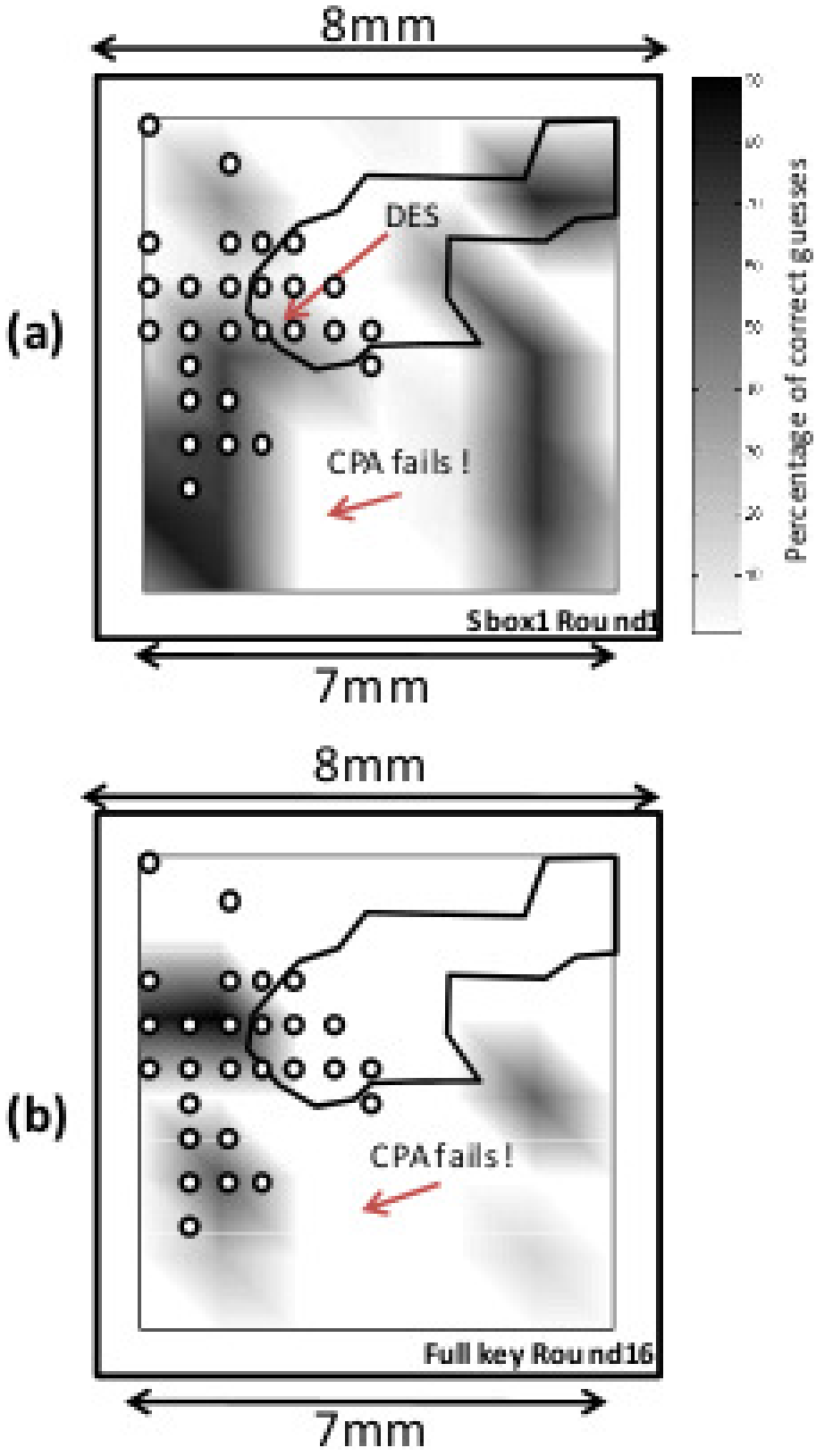

Fig. 7. Percentage of the successful CEMA by WGMSI bin and Percentage of the whole population by bin

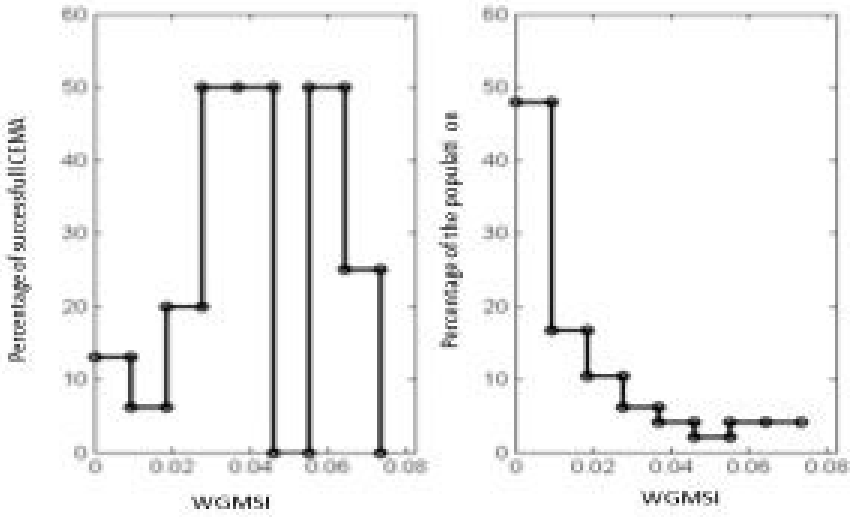

Fig. 8. Percentage of the successful CEMA by $WGMSI$ bin and Percentage of the whole population by bin

Table 2. Data collecting time to obtain attack cartographies

probe size attacked area	1mm	500μm	100μm
1x1mm	20 min	3 hours	1.5 day
7x7mm	21 hours	3 days	70 days
17x17mm	4.5 days	17 days	406 days

Table 3. Data collecting time to obtain $WGMSI$ cartographies

probe size attacked area	1mm	500μm	100μm
1x1mm	1 min	9 min	121 min
7x7mm	64 min	4 hours	3.5 days
17x17mm	5.5 hours	20 hours	20 days

radiated by an integrated circuit have some coherent characteristics and some incoherent characteristics. This claimed property, called partially data-dependence of EM emissions, has been first validated experimentally by verifying its correctness with some measured traces. Then, we deduced from this observation, a localization technique. This technique allows (a) localizing cryptographic modules and more precisely leaking points thanks to EM near field mapping and

(b) selecting rationally a reduced set of points of interests for electromagnetic analyses. Finally, concrete results have been given on an iterative DES mapped on a FPGA. These results have demonstrated the interest of using incoherence analysis of EM emissions.

References

1. P. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Proc. of the 16th International Conference on Cryptology (CRYPTO), pp 104-113 (1996)
2. P. Kocher and J. Jaffe and B. Jun: Differential Power Analysis, Proc. of the 19th International Conference on Cryptology (CRYPTO), pp 388-397 (1999)
3. K. Gandolfi and C. Mourtel and F. Olivier: Electromagnetic Analysis: Concrete Results, Proc. of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp 251-261 (2001)
4. E. Peeters and FX. Standaert and JJ. Quisquater: Power and electromagnetic analysis: Improved model consequences and comparisons, Integration, the VLSI Journal, Volume 40, Issue 1, Special issue: Embedded cryptographic hardware, pp 52-60 (2007)
5. A.Shamir: Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies, Proc. of the 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp 121-132 (2000)
6. C. Clavier and J.S. Coron and N. Dabbous: Differential Power Analysis in the Presence of Hardware Countermeasures, Proc. of the Second International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp 252-263 (2000)
7. HD. Moyart and R. Bevan: A Method for Resynchronizing a random clock on smartcards, Eurosmart, `http://www.nmda.or.jp/nmda/ic-card/proceedings/30-1440-DMoyart.pdf` (2001)
8. H. Pelletier and X Charvet: Improving the DPA attack using wavelet transform, NISTs Physical Security Testing Workshop, `http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper14.pdf` (2005)
9. N. Homma and S. Nagashima and Y. Imai and T. Aoki and A. Satoh: High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching, Proc. of the 8th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp 187-200 (2006)
10. M. Kafi and S. Guilley and S. Marcello and D. Naccache: Deconvolving Protected Signals, Proc. of the International Conference on Availability, Reliability and Security (ARES), pp 687-694 (2009)
11. J.S. Coron and D. Naccache and P. Kocher: Statistics and secret leakage, ACM Transactions on Embedded Computer Systems, Volume 3, pp 492-508 (2004)
12. E. Brier and C. Clavier and F. Olivier: Correlation Power Analysis with a Leakage Model, Proc. of the 7th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), pp 16-29 (2004)
13. Data Encryption Standard, FIPS PUB 46-3
14. Advanced Encryption Standard, FIPS 197
15. R. Bevan and E. Knudsen: Ways to Enhance Differential Power Analysis, Proc. 5th International Conference on Information Security and Cryptology (ICISC), pp 327-342 (2002)

16. T. Messerges and E. Dabbish and R. Sloan: Investigations of power analysis attacks on smartcards, Proc. of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology (WOST), pp 17-17 (1999)
17. G. Yeap: Practical Low Power Digital VLSI Design, Springer-Verlag (1997)
18. S. Dhia and M. Ramdani and E. Sicard: Electromagnetic Compatibility of Integrated Circuits: Techniques for low emission and susceptibility, Springer-Verlag (2005)
19. T. Ordas and M. Lisart and E. Sicard and P. Maurine and L. Torres: Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits, Proc. of the 18th International Workshop on Power and Timing Modeling Optimization and Simulation (PATMOS), pp 229-236 (2008)
20. DPA contest 2008/2009 `http://www.dpacontest.org`