Enhancing Electromagnetic Analysis Using Magnitude Squared Incoherence

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

Enhancing Electromagnetic Analysis Using Magnitude Squared Incoherence

A. Dehbaoui, V. Lomne, T. Ordas, L. Torres, M. Robert, P. Maurine [1]

***Abstract*— This paper demonstrates that Magnitude Squared Incoherence (MSI) analysis is efficient to localize hot spots, i.e. points at which focused Electromagnetic (EM) Analyses can be applied with success. It is also demonstrated that MSI may be applied to enhance Differential EM Analyses (DEMA) based on Difference of Means (DoM).**

***Index Terms*— Side Channel Attacks, EM analysis**

I. Introduction

Among Side-channel attacks some exploit the timing behavior of I [1], while others exploit the power consumption [2] or the EM emissions [3-5].

EM side channel efficiency is due to the inner properties of EM emissions. Their ability to propagate through different materials is the most striking one. Indeed, it allows attackers targeting the bounded hardware area integrating the crypto-module under attack or part of it.

This is all the more interesting because it allows getting round global hardware countermeasures against power analysis [11] by focusing the analysis on reduced silicon die areas thanks to tiny probes. Moreover, replacing the large probe of Fig. 1a by the tiny one shown Fig. 1b allows dividing the number of EM traces required to disclose the key of standard iterative DES (Data Encryption Standard) mapped into a FPGA by 100 to 200. However, this requires localizing beforehand the crypto-module that may occupy only a small fraction of the device area.

However, focusing EM attacks, using small sensors, requires localizing leaking spots to overcome the quadratic increase (with the square of package / probe sizes) of the number of points to be attacked using either Differential EM Analyses (DEMA) [3-4] or Correlation EM Analyses (CEMA).

Within this context, the contribution of this paper is twofold. First, a localization technique based on Spectral Coherence analyses is introduced. It allows finding positions where EM attacks might be successful with a reduced set of traces. The technique, called Weighted Global Magnitude Squared Incoherence (WGMSI) analysis, has several interesting properties. Firstly, it requires only few EM measurements to be efficiently applied. Thirdly, this non invasive and contactless technique can be applied even if the circuit under attack is encapsulated.

Manuscript received September 14, 2010. All Authors are with the Laboratory of Informatics Robotics and Microelectronics of Montpellier, France (email: firstname.name@lirmm.fr)

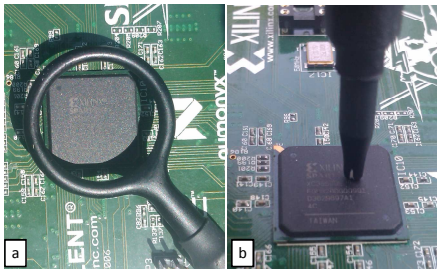

Fig. 1. (a) global EM analysis and (b) focused EM analysis

The second contribution is a Spectral Coherence based technique allowing performing successful DEMA with a reduced set of traces. This technique, which accelerates the convergence of DEMA based on DoM test, is denoted by Differential Global Magnitude Square Incoherence (DGMSI) analysis afterward.

The paper is organized as follows. Section II highlights the localization problem and gives details about the proposed localization technique. This section ends with experimental results demonstrating that WGMSI is efficient to localize the less robust positions against EM attacks. Section III highlights how Spectral Coherence can be further used to enhance DEMA based on DoM by reducing the number of traces to be collected and processed to disclose the secret key. Note that DoM is not the sole statistical test that can be used during an EM attack. Indeed there are many other tests; a classification of test is given in [10]. Conclusion is drawn in section IV.

II. Weighted Global Magnitude Squared Incoherence

Performing a DEMA, requires collecting a large number of traces. It is thus time consuming even if the analysis is done at a single position above the device, with a large probe.

The situation becomes unpractical when tiny sensors are used by an attacker or an evaluator aiming at demonstrating the robustness of a design against EM analyses.

A. Problem

Considering an iterative DES mapped onto a FPGA, one may plan collecting, at 784 (28×28) positions above and around the Spartan3 core (displacement step of 250µm), 20 000 EM traces, using a 500µm diameter magnetic loop, to determine if EM emissions may be exploited or not. However, this would result, in collecting traces during 24 days at first order and with the setup presented in annex A.

This leads to the question: how efficiently and quickly position tiny probes? One may think, to solve this problem, by performing a EM Near Field Scan (NFS) to localize the cryptographic block. However this is often insufficient.

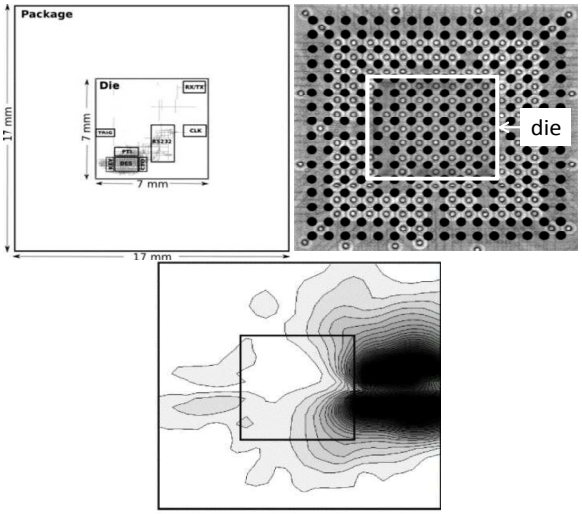

Fig. 2. (a) Design floorplan (b) X-Ray photography of the package (c) measured Peak to Peak EM cartography above the package.

As an illustration, Fig. 2c shows a peak to peak cartography (obtained with the setup introduced in annex A) of the EM emissions measured at several coordinates above the FPGA package during a DES ciphering. Fig. 2b is an X-Ray photography of the package containing the circuit under attack. Finally, Fig.2a discloses the floorplan of the 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. 2a with Fig. 2c even if the die area is known thanks to the X-Ray photography. It appears all the more difficult to localize the DES module and thus decide where to position the magnetic sensor to perform a successful focused DEMA or CEMA to avoid potential global hardware countermeasures.

B. Basics of Global Magnitude Squared Incoherence

DEMA exploits the data dependent behavior of the EM emissions radiated by circuits during cryptographic operations. EM emissions are generated by flows of electrical charges through the wires connecting logic gates but also trough wires supplying the circuit [7]. Since the switching of gates generates a current flow through the circuit interconnect, we may conclude that gates generate some data dependent EM emissions at different points above the circuit according to the power distribution network. These data dependent behaviors is exploited by statistical means [3,4], to retrieve the secret key.

Even if the timing and power characteristics of CMOS gates are known, it is difficult to deduce any characteristic about the EM emissions generated of actual IC due to the complexity of their power distribution grid. Thus, the only conclusion we may consider is that gates generate some EM perturbations i.e. generate 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: considering two successive hardware operations, we are sure that some gates switch during one computation and do 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 characteristics completely change (are incoherent). Such a data dependent behavior is disclosed by the WGMSI technique.

The Magnitude Squared Coherence (MSC) between two signals w1(t) and w2(t) is a real-valued function of frequency with values between 0 and 1. It is defined by:

$$MSC_{w1,w2}(f) = \frac{\left|P_{w1,w2}(f)\right|^2}{P_{w1,w1}(f) \cdot P_{w2,w2}(f)} \quad (1)$$

$$MSI_{w1,w2}(f) = 1 - MSC_{w1,w2}(f) \quad (2)$$

where $P_{w1w1}(f)$, $P_{w2w2}(f)$ are the power spectral density of w1(t), w2(t), and $P_{w1w2}(f)$ is the cross power spectral density of w1(t) and w2(t). At a given frequency *f*, a MSC(*f*) value of 1 indicates that the two spectra are exactly the same while, a value of 0 means that the spectra are different i.e. incoherent. Alternatively, one may compute the Magnitude Squared Incoherence MSI(*f*) (2). This criterion has also its values between 0 and 1 but indicates rigorously the contrary of (1).

Considering the whole spectra of two time domain signals, one may compute the WGMSI coefficients between them according to (3) that consider the signal w2(t) as a reference.

$$WGMSI = \sum_{f \in BW} MSI_{w1,w2}(f) \cdot \frac{A_{w2}(f)}{\underset{f \in BW}{Max}\,(A_{w2}(f))} \quad (3)$$

where *nf* is the number of frequency values at which the MSI(*f*) coefficients are computed, BW is the considered frequency bandwidth and $A_{w2}(f)$ is the power spectrum amplitude at the frequency *f*.

WGMSI has values between 0 and 1. A high value indicates that w1(t) and w2(t) have perfectly incoherent spectra, while a low value indicates the contrary. Note that the second term of (3) is a key term. Indeed, it weights MSI(*f*) values such that incoherent and high amplitude harmonics have more impact on the final WGMSI value than incoherent but low amplitude harmonics. This reduces significantly the impact of noise.

To illustrate these definitions, 5 time domain EM traces were acquired during 5 different data processing of a DES. These traces (Fig. 3) have been collected with a 500µm diameter probe placed respectively above a DES (Fig. 3a) and above a clock wire (Fig. 3b). As a result, one may expect that curves Fig.3a are data dependent traces while, waveforms Fig. 3b are completely data independent. To validate this assumption, MSC(*f*) were computed. Fig. 3c gives the MSC(*f*) evolution with respect to frequency for both 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, validating the above discussion.

The obtained MSC(*f*) values were gathered to compute the WGMSI coefficients. As expected, WGMSI values (Table 1) corresponding to acquisitions above clock nets are two magnitude order lower than those acquired above the DES.

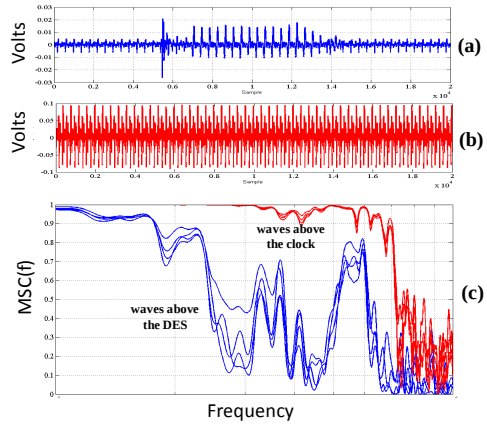

Fig. 3. EM traces collected (a) above the DES (b) above the clock network and (c) MSC(f) versus frequency

TABLE I. WGMSI VALUES

WGMSI between:	Traces collected above a clock net	Traces collected above the DES	Ratio
data1 & data 2	$2.8\ 10^{-5}$	$2.6\ 10^{-3}$	91
data1 & data 3	$2.1\ 10^{-5}$	$2.5\ 10^{-3}$	117
data1 & data 4	$2.4\ 10^{-5}$	$2.4\ 10^{-3}$	101
data1 & data 5	$2.4\ 10^{-5}$	$1.7\ 10^{-3}$	71

Considering these results, one may assume that the WGMSI criterion appears efficient to differentiate a data dependent behavior from a data independent one and may be used during a magnetic NFS to localize area with data dependent EM emissions expected to be hot spots for EM analysis.

C. Coupling WGMSI and EM Near Field Scan

Coupling WGMSI with NFS system to localize points characterized by data-dependent EM emissions is straightforward. The idea is to collect at each (X,Y) coordinates above the IC at least two different time domain traces of the EM field corresponding to two different data processing. Then, WGMSI values are computed for all (X,Y) positions to obtain a WGMSI cartography revealing positions with data-dependent EM emissions. Note that computing WGMSI values for more than 2 data and averaging the results is not mandatory but leads to better results in practice.

D. WGMSI vs EM cartographies

To validate the effectiveness of the WGMSI analysis, two kinds of validation were performed. One aimed at correlating the obtained WGMSI cartographies with design floorplans while the 2nd aimed at demonstrating that spots with the highest WGMSI values are good candidates for DEMA and CEMA. Results related to the 1st validation step being available in [9] we give here only the results related to the 2nd validation step. Note however, that the 1st validation step allowed us concluding that WGMSI technique is an efficient technique to localize a cryptographic system, and its Power/Ground (P/G) network, within noise.

Note finally that both validation steps have been carried out with the experimental setup described in annex A and were performed considering a design mapped into a FPGA circuit and more precisely a Spartan3 board. The mapped design (50MHz) integrated: a RS232 to communicate with the PC, a finite state machine that manages the communications and the behavior of the chip, and a DES.

To evaluate the efficiency of WGMSI cartographies in disclosing hot spots for EMA, we scanned a 7mm × 7mm area of the package centered on the Spartan core with a 1mm probe displacement step. The core size was estimated to be roughly of 5×5mm² thanks to an X-ray photography, while the package has a size of 17× 17mm².

At each of the 64 resulting positions, 5000 averaged traces (20 trials for each PTI) were collected corresponding to the ciphering of 5000 different PTI. Note that the same 5000 PTI were processed at each position in the same order.

TABLE II. NORMALIZED (%) WGMSI CARTOGRAPHY / [40MHz, 950MHz]

Y/X	1	2	3	4	5	6	7	8
8	33	29	14	5	3	1	1	1
7	53	35	24	10	4	1	1	1
6	85	57	50	33	13	1	1	6
5	90	62	64	63	52	13	20	11
4	83	48	30	16	13	1	1	2
3	100	37	20	12	8	2	1	1
2	75	24	17	12	6	3	2	2
1	40	24	20	12	7	3	2	3

TABLE III. NORMALIZED (%) WGMSI / [40MHz, 200MHz]

Y/X	1	2	3	4	5	6	7	8
8	9	12	14	9	4	1	1	1
7	8	12	23	22	9	1	1	2
6	11	11	26	27	27	1	2	14
5	30	12	33	38	41	6	100	32
4	39	10	21	20	22	2	4	8
3	57	30	8	11	4	4	1	4
2	36	21	5	6	8	6	2	1
1	27	5	1	2	2	3	5	3

Data acquisition achieved, WGMSI cartographies were computed considering two frequency bandwidths, [40-, 950MHz] and [40- 200MHz], and EM traces corresponding to the whole DES course. The 1st bandwidth is the full bandwidth of our acquisition chain, while the 2nd one has been chosen to keep only the emissions of the P/G network according to [7].

Tables II and III give the WGMSI values in both cases after normalization done so that the maximum WGMSI value corresponds to 100% and the minimum one to 0%. Note that black cells point out positions with WGMSI values lower than 20%. As shown, the DES and part of P/G rails in which flows its switching current generate data dependent EM emissions mainly in left side of the cartographies.

In a 2nd stage, 64 DEMA and CEMA, considering the Hamming Distance model were performed; both attacks targeted the last round of the DES. To compare the results obtained at different positions two criteria were considered. Note we performed CEMA using the Pearson's correlation.

The 1st criterion was the Measurements To Disclosure with Stability (MTDwS) adopted during the DPA contest 2009 [8].

Its evaluation resumes in detecting and storing, while the number of processed traces increases, the beginning of the 1st sequence of 100 successive right guesses of the key. Table IV and V show normalized MTDwS values for DEMA and CEMA. The normalization has been done so that a value of 60% means that 60% of EM traces have been processed to reach the 1st sequence of 100 successive right guesses. Black cells indicate positions at which the MTDwS is greater than 50% or positions at which the attack failed.

Finally, the 2nd criterion is the Percentage of Right Guesses (PRG) obtained after the processing of 5000 traces. Tables VI and VII show results. Black cells point out positions with a PRG value lower than 20%.

TABLE IV. NORMALIZED MTDWS (%) VALUES FOR DEMA (5000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	84	58	36	62	fail	fail	fail	fail
7	62	34	98	86	88	fail	fail	fail
6	98	94	86	48	48	fail	fail	52
5	58	82	80	58	34	48	40	34
4	36	56	70	fail	48	fail	fail	80
3	96	94	54	52	98	fail	fail	fail
2	50	74	fail	48	50	fail	84	fail
1	80	fail	fail	70	42	fail	fail	fail

TABLE V. NORMALIZED MTDWS (%) VALUES FOR CEMA (5000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	96	36	38	40	60	fail	fail	72
7	50	35	35	32	39	61	41	81
6	31	38	19	20	38	95	23	35
5	36	53	21	9	38	29	25	12
4	28	79	13	15	41	35	34	21
3	7	40	18	18	16	18	fail	32
2	49	43	63	17	22	24	33	fail
1	23	71	fail	69	30	32	39	fail

TABLE VI. NORMALIZED PRG (%) VALUES FOR DEMA (5000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	40	60	65	39	0	0	0	0
7	38	71	33	40	54	0	0	0
6	33	57	10	69	57	0	0	49
5	11	36	17	35	66	53	64	66
4	66	44	13	0	61	0	0	42
3	65	17	53	60	27	0	0	1
2	51	6	0	69	51	0	6	0
1	46	0	0	19	67	0	2	0

TABLE VII. NORMALIZED PRG (%) VALUES FOR CEMA (5000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	40	71	64	61	50	5	0	43
7	54	70	75	75	72	39	64	32
6	77	72	88	85	62	52	78	65
5	65	62	85	92	63	75	80	89
4	77	41	91	90	61	69	67	85
3	80	62	85	86	84	90	0	82
2	55	67	49	84	85	87	69	0
1	78	21	0	40	70	69	64	0

Comparing these tables highlights of several results. First, Tables II and III indicate that the DES and part of the overall P/G network supplying it are localized mainly on the left of the core as expected from the floorplan.

Second, Tables II to VII show that WGMSI and MTDwS cartographies have similarities. Indeed, most positions with high MTDwS values are mainly on the right part of the cartographies as positions with low WGMSI values. To better support this observation, correlations between WGMSI cartographies and, all other ones have been computed. Table VIII gives the results. Note that to compute the correlations involving MTDwS, we considered MTDwS equal to 100 for positions where attacks were unsuccessful. As shown, there are correlations between these cartographies. This demonstrates the interest of WGMSI to localize hot spots. Note that higher correlation values are obtained for the frequency bandwidth [40MHz - 200MHz]. According to [7], this means that the most leaking points are part of the P/G network.

TABLE VIII. CORRELATIONS BETWEEN WGMSI AND MTDWS, PRG VALUES

Correlation		MTDwS	PRG
DEMA	WGMSI 40 – 950 MHz	-0.33	0.41
	WGMSI 40 – 200 MHz	-0.46	0.49
CEMA	WGMSI 40 – 950 MHz	-0.20	0.20
	WGMSI 40 – 200 MHz	-0.40	0.38

III. DIFFERENTIAL GLOBAL MAGNITUDE SQUARED INCOHERENCE

If the above results have demonstrated the interest of the WGMSI, they also suggest using MSI to enhance DEMA.

Attacking a DES sub-key by DEMA consists in computing 64 DoM according to (4) and in identifying the one having the sample with the highest amplitude.

$$\Delta_{Ks}[j] = \frac{\sum_{i=1}^{N} D(PTI_i, K_s)\cdot T_i[j]}{\sum_{i=1}^{N} D(PTI_i, K_s)} - \frac{\sum_{i=1}^{N} (1 - D(PTI_i, K_s))\cdot T_i[j]}{\sum_{i=1}^{N} (1 - D(PTI_i, K_s))} \quad (4)$$

In (4), extracted from [6], $\Delta_{Ks}[j]$ is the j^{th} sample of the DoM, N is the number of EM traces used, PTI_i is the i^{th} plaintext, $T_i[j]$ is the j^{th} sample of associated EM trace and D the selection function returning the value of the targeted bit according to the PTI and the sub-key guess.

According to [1], if the sub-key guess is correct the right and left hand terms of (4) correspond to the averaged traces characterized by an effective targeted bit value of 1 and 0, respectively. Thus, the difference of these terms $\Delta_{Ks}[j]$ shows a bounce as illustrated by Fig.4b.

Contrarily, if the sub-key guess is wrong, the left and right terms are undistinguishable, and a smaller bounce appears. Indeed, the selection function D fails in sorting traces according to the targeted bit and these terms are expected to be less incoherent than for the right guess.

Considering this, one may compute, for each sub-key guess Ks, the Global Magnitude Squared Incoherence, $GMSI_{Ks}$, between these two means curves. Then, rather than computing the DoM, one may compute the DoM weighted by the $GMSI_{Ks}$ (5), and search the sample with the highest amplitude:

$$\Delta^{*}_{Ks}[j] = \Delta_{Ks}[j]\cdot GMSI_{Ks} \quad GMSI_{Ks} = \sum_{f\in BW} \frac{MSI(f)}{nf} \quad (5)$$

Let us denote by DGMSI, a DEMA attack considering the four output bits of Sboxes [6] and performed using the proposed weighting strategy.

To evaluate its efficiency, we computed MTDwS and PRG cartographies using only 1000 PTI rather than 5000. Tables IX and X give the results. As shown, a DGMSI performed with 1000 PTI gave results quite similar to that of a DEMA performed with 5000 PTI. One may conclude that DGMSI

allows reducing by ~5, wrt DEMA, the number of PTIs required to disclose the secret key. This demonstrates the interest of MSI to enhance EM analyses.

TABLE IX. NORMALIZED MTDWS (%) VALUES FOR DGMSI (1000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	91	96	48	92	fail	fail	fail	fail
7	fail	71	22	24	60	fail	fail	fail
6	fail	24	29	24	40	fail	fail	25
5	28	60	28	28	28	41	21	26
4	25	fail	28	29	24	fail	fail	60
3	21	43	65	36	26	fail	fail	fail
2	27	39	69	27	42	65	fail	fail
1	41	58	fail	fail	63	fail	fail	fail

TABLE X. NORMALIZED PRG (%) VALUES FOR DGMSI (1000 PTIS)

Y/X	1	2	3	4	5	6	7	8
8	11	12	63	30	0	0	0	0
7	10	72	80	78	46	0	0	0
6	16	76	73	77	69	0	16	75
5	74	62	72	78	76	59	79	75
4	76	9	75	71	76	0	0	33
3	79	60	35	76	74	18	0	0
2	73	68	38	86	62	37	0	0
1	59	44	0	1	42	10	0	0

One may wonder why DGMSI allows reducing MTDwS and increasing the PRG. Practically, the obtained enhancement is explained by the reduction of the set of key candidates during the key search by removing keys related to coherent means in the DoM.

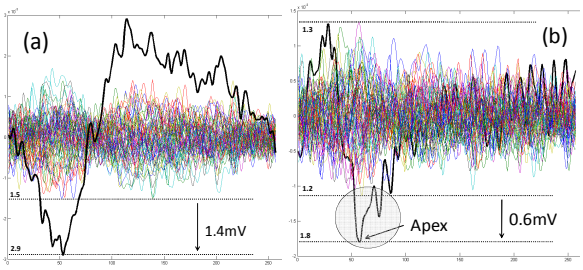

Fig. 4. DoM obtained with (a) DGMSI and (b) DEMA

Fig. 4 shows the DoM obtained with DGMSI and DEMA after the processing of the 1000 PTI. As shown, the right key appears more clearly with DGMSI than for DEMA: the margin between the right and wrong keys is 2 times greater with DGMSI than with DEMA. This is due to the low values of $GMSI_{Ks}$ that flatten the DoM of wrong keys.

TABLE XI. COMPARING DGMSI WITH DEMA AND CEMA (5000 PTI)

	DGMSI		DEMA		CEMA	
	MTDwS	PRG	MTDwS	PRG	MTDwS	PRG
μ	43%	58%	68%	33%	73%	26%
σ	11%	10%	17%	17%	19%	20%

In the previous section, the weighting strategy of DoM has been demonstrated efficient to reduce the number of EM traces required to disclose the secret key. However, during this experiment, we considered averaged EM traces. One may wonder if results hold in presence of noise.

5000 one shot EM traces, were thus acquired and processed using DEMA, CEMA and DGMSI. Note that 10 successive attacks were done; each one differing from the other by the order considered to process data. Table XI gives the results. In this table, μ and σ denotes the mean and the standard deviation obtained considering the 10 processing orders.

As shown, with one shot EM traces, DGMSI allows disclosing the right key with less PTI than with DEMA. Indeed, only 43% of the traces are processed in average to reach for the first time the sequence of 100 successive right guesses of the full key with DGMSI while 68% and 73% are needed with DEMA and CEMA respectively. Moreover the PRG of DGMSI is nearly twice the ones of DEMA and CEMA.

IV. CONCLUSION

The interest of Magnitude Squared Incoherence processing technique for EM analyses has been demonstrated through two applications. One tackles the identification of hot spots to be attacked using tiny probes while the other is an improvement of DEMA based on DoM.

Annex A

All results were obtained with a measurement platform composed of:

– an oscilloscope, with a 3.5 GHz bandwidth, to sample at 40 GS/s the time domain evolutions of the EM signals,
– a low noise 63 dB amplifier with a 1GHz bandwidth,
– a 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 control the whole measurement setup, i.e. to provide data to the DES (50 MHz) through an RS232 module and store the EM traces collected by the scope.

REFERENCES

[1] P. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Proc. of the 16th International Conference on Cryptology, pp 104-113 (1996)
[2] P. Kocher and J. Jaffe and B. Jun: Differential Power Analysis, Proc. of the 19th International Conference on Cryptology, 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, pp. 251-261 (2001)
[4] E. Peeters and F.X. Standaert, J. J. Quisquater: Power and electromagnetic analysis: Improved model consequences and comparisons, Integration, the VLSI Journal, Volume 40, Issue 1, pp 52-60 (2007)
[5] D. Agrawal, B. Archambeault, J. R. Rao and P. Rohatgi. The EM Side—Channel(s). Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, pp. 29-45 (2002)
[6] R. Bevan and E. Knudsen: Ways to Enhance Differential Power Analysis, Proc. 5th International Conference on Information Security and Cryptology, pp 327-342 (2002)
[7] 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, pp 229-236 (2008)
[8] DPAcontest 2008/2009 http://www.dpa-contest.org
[9] A. Dehbaoui, V. Lomne, P. Maurine, L. Torres, M. Robert: Enhancing Electromagnetic Attacks using Spectral Coherence based Cartography. International Conference on VLSI (VLSI-SoC 2009)
[10] F.-X. Standaert, B. Gierlichs, I. Verbauwhede: Partition vs. Comparison Side-Channel Distinguishers: an Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two CMOS Devices. Lecture Notes in Computer Science, vol 5461, pp 253-267, (2008)
[11] 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, pp 121-132 (2000)