# Incoherence Analysis and its Application to Time Domain EM Analysis of Secure Circuits

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

2010 Asia-Pacific International Symposium on Electromagnetic Compatibility, April 12 - 16, 2010, Beijing, China

# Incoherence Analysis and its Application to Time Domain EM Analysis of Secure Circuits

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

*LIRMM - University Montpellier 2, CNRS*
*161, rue Ada, 34292 Montpellier, France*
dehbaoui@lirmm.fr

***Abstract*— Since several years, Electromagnetic (EM) radiations of ICs are considered as source of noise and interferences from an EM Compatibility (EMC) point-of-view. Electromagnetic interferences (EMI) are unwanted disturbances that affect digital circuits due to electromagnetic conduction or electromagnetic radiation emitted from an internal or external source. Today electromagnetic radiations of ICs also represent vulnerabilities for hardware security modules like smartcards. Recently, from a hardware security point of view, researchers, industrials and governmental agencies are focusing with strong interest on these radiations. This paper aims at introducing a pragmatic technique WGMSI (Weighted Global Magnitude Squared Incoherence) allowing localizing hardware security modules within the whole EM noise generated by the environment or other modules of the circuits.**

## I. 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 a cryptographic operation to disclose the key. As a result, a new kind of attack called Side-Channel Attack (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 to integrate 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 analyses such as the use of detached power supplies [5] by focusing the analysis 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.

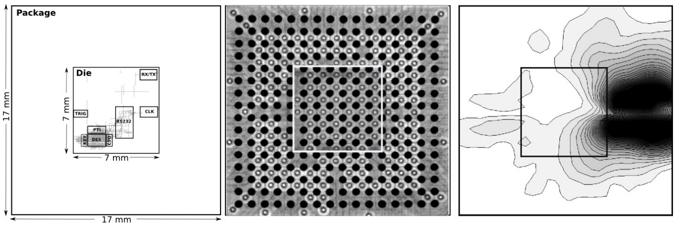


Fig. 1. (a) Design floorplan (b) X-Ray (c) Peak to Peak map

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 3, even if the circuit under attack is encapsulated.

The remainder of this paper is organized as follows. Section 2 introduces theoretical explanations about the proposed localization technique called $Weighted\ Global\ Magnitude\ Squared\ Incoherence$ ($WGMSI$)technique and how to couple $WGMSI$ technique with EM near field scanning systems. Section 3 presents some concrete results related to the application of $WGMSI$ localization technique to different mappings on FPGA of a same design. This section also demonstrates the efficiency of $WGMSI$ cartography to lead a reverse engineering of the IC. Finally, conclusions are drawn in Section 4.

## II. Global Magnitude Squared Incoherence

### A. 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 [6]) and large portion of the emissions of S.
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 close 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.1c 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 3). Fig.1b is an X-Ray photography of the package containing the circuit under attack. Finally, Fig.1a 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.1a with Fig.1c even if the die area is roughly known thanks to the X-Ray photography Fig.1b. 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 CEMA only on the DES module, in order to avoid potential global hardware countermeasures such as [5].

### B. 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 [7].
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 [6][8]. 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 [6][8]. 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 character-ristics completely change (are incoherent). Such a behavior is said partially data-dependent in the rest of the paper, and the proposed $WGMSI$ technique[9] aims at disclosing circuit areas characterized by this behavior.

### C. 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 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.

## III. 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 CEMA.

### A. 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. 4. This was done to definitively validate the efficiency of $WGMSI$ map in disclosing area with partially data-dependent radiations.

### B. $WGMSI$ 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 a 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 500$\mu$m 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 $8mm$ by $8mm$. The whole package was scanned with a displacement step of 500$\mu$m. This resulted in acquiring EM emissions at 1156 coordinates for each mapping. It took 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.3 shows the 3 obtained $WGMSI$ maps. The lower left map of Fig.3 is to be compared to Fig.1c. This comparison demonstrates that $WGMSI$ map provides more valuable information than a maximum time domain amplitude analysis. 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.

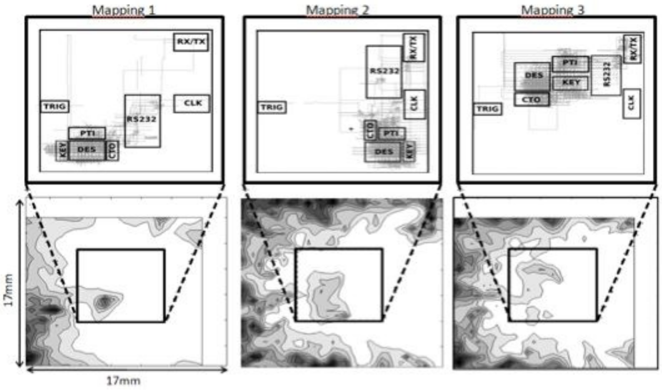


Fig. 2. Circuit floorplans and related full package $WGMSI$ maps obtained for the three considered mappings of the design

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 [6][8].

### C. $WGMSI$ and Frequency Bandwidth

As generally recognized CMOS gate dissipates power, this power dissipation is strongly affected by non-zero input signal transition times $\tau_{in}$. Depending on $Fast$ or $Slow$ input signal settling times [10], and according to the Biot-Savart Law, the gate radiation will be spread in the frequency domain, depending on $\tau_{in}$ (1),(2) :

$$\begin{aligned} |Env_B|^{fast} = \tfrac{\mu_0}{4\pi}.I_{max}^{fast}.\tau_{in}.sinc_a^2(\omega.\tfrac{\tau_{in}}{2}). \\ (1+2.cos(\omega.\tau_{in})).(sin\theta_2 - sin\theta_1) \end{aligned} \quad (1)$$

$$\begin{aligned} |Env_B|^{slow} = \tfrac{\mu_0}{4\pi}.I_{max}^{slow}.\tau_{in}.sinc_a^2(\omega.\tfrac{\tau_{in}}{2}). \\ (sin\theta_2 - sin\theta_1) \end{aligned} \quad (2)$$

Where $\mu_0$, $\tau_{in}$, $\theta_1$ and $\theta_2$, are respectively the permeability of free space, the ramp duration, and angles involved in Biot-Savart law.

As shown in [10], gates obey to two types of switching processes, fast and slow ones. Although both processes may exist within the same circuit, the fast one is much more common within typical circuit [11]. Such switching mechanisms, are characterized at first order by a current consumed taking the shape of a trapezoid for fast processes, and the shape of a triangle for slow ones.

Considering $Fast$ and $Slow$ input signal settling times, Fig. 3 gives the power spectral density of the power radiated by a CMOS inverter, and the measured one using a perfect differentiator (magnetic loop). As observed, for slow switching process, amplitudes measured with a differentiator sensor are more significant at lower frequencies, while, for fast switching process, the highest amplitudes are localized at higher frequencies.

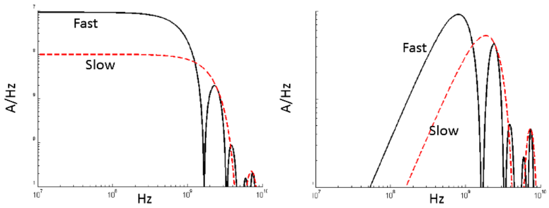


Fig. 3. First-Order Power Spectral Densities a) radiated by a CMOS inverter b) collected with a perfect differentiator

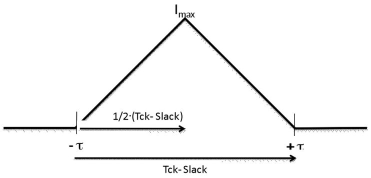


Fig. 4. Simple Consumption Model of combinatory block

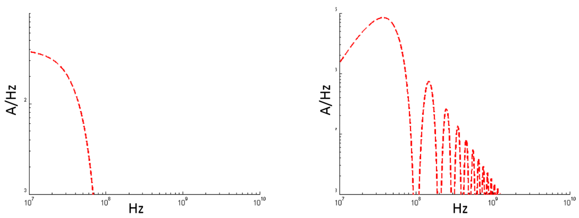


Fig. 5. First-Order Power Spectral Densities a) radiated by a CMOS circuit b) collected with a perfect differentiator

While it is difficult to obtain accurate analytical model of consumption of a block taking into account all parameters involved, we can nevertheless estimate the spectral density of a combinatory block based on the empirical model illustrated in Fig. 4, where $Tck$, $Slack$ and $I_{max}^{block}$ are respectively the clock period, the timing margin design and the maximum switching current consumed by the block. The resulting spectral density is given by (3) and represented in Fig. 5.

$$|Env_B|^{block} = \frac{\mu_0}{4\pi}.I_{max}^{block}.\tau.sinc_a^2(\omega.\frac{\tau}{2}).(sin\theta_2 - sin\theta_1) \quad (3)$$

However, the values involved in this expression are very different from those considered for a gate. Indeed, for a combinational block $I_{max}$ and $\tau$ are much greater. So to go further in our reverse engineering analysis, we performed static WGMSI maps for different frequency bandwidths. Fig.6 shows the considered design placement and the corresponding peak to peak map.$WGMSI$ maps for the considered bandwidths ([200MHz - 400MHz] and [800MHz - 900MHz]) are shown in Fig. 7.
As expected, supply rails and pads appear clearly in the frequency bandwidth [200MHz - 400MHz], while, logical blocks appear in the frequency bandwidth [800MHz - 900MHz].

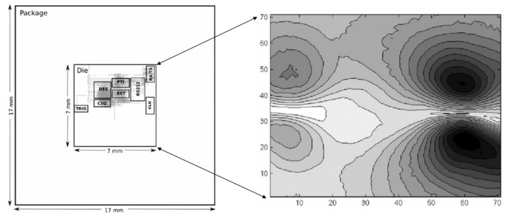


Fig. 6. a) Design Placement b) Peak to Peak map

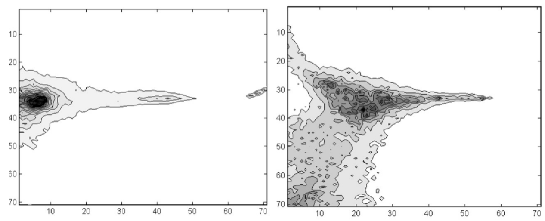

Fig. 7. WGMSI maps a) [200MHz 400MHz] b) [800MHz - 900MHz]

## IV. Conclusion

A new technique to localize Electro-Magnetic hot-spots in hardware cryptographic module was presented in this paper. It is based on the assumption according to which: from a data processing to another one, EM emissions 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," in *CRYPTO*, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. 19th International Conference on Cryptology (CRYPTO)*, 1999, pp. 388–397.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. 3rd Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2001, pp. 251–261.

[4] J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and countermeasures for smart cards," in *Proc. International Conference on Research in Smart Cards (E-SMART)*, 2001, pp. 200–210.

[5] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proc. 2nd Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2000, pp. 71–77.

[6] S. Dhia, M. Ramdani, and E. Sicard, *Electromagnetic Compatibility of Integrated Circuits: Techniques for low emission and susceptibility*. Springer-Verlag, 2005.

[7] G. Yeap, *Practical Low Power Digital VLSI Design*. Springer-Verlag, 1997.

[8] T. Ordas, M. Lisart, E. Sicard, P. Maurine, and L. Torres, "Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits," in *Proc. 18th International Workshop on Power and Timing Modeling Optimization and Simulation (PATMOS)*, 2008, pp. 229–236.

[9] A. Dehbaoui, V. Lomne, P. Maurine, L. Torres, and M. Robert, *Enhancing Electromagnetic Attacks using Spectral Coherence based Cartography*. Springer, 2009.

[10] P. Maurine, M. Rezzoug, N. Azemard, and D. Auvergne, "Transition time modeling in deep submicron cmos," 2002, pp. 1352–1363.

[11] B. Lasbouygues, S. Engels, R. Wilson, P. Maurine, N. Azemard, and D. Auvergne, "Logical effort model extension to propagation delay representation," in *Proc. 7th Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2006, pp. 1677–1684.