Spatial EM Jamming: a Countermeasure Against EM Analysis ?

François Poucheret, Lyonel Barthe, Pascal Benoit, Lionel Torres, Philippe Maurine, Michel Robert

Spatial EM Jamming: a Countermeasure Against EM Analysis?

Francois Poucheret, Lyonel Barthe, Pascal Benoit, Lionel Torres, Philippe Maurine, Michel Robert
LIRMM UMR 5506-CNRS
161, Rue Ada, 34392 Montpellier, France
E-mail:firstname.lastname@lirmm.fr

Abstract—**Electro-Magnetic Analysis has been identified as an efficient technique to retrieve the secret key of cryptographic algorithms. Although similar mathematically speaking, Power or Electro-Magnetic Analysis have different advantages in practice. Among the advantages of EM Analysis, the feasibility of attacking limited and bounded area of integrated systems is the key one. Within this context, the contribution of this paper is a countermeasure against local EM attack performed with tiny magnetic probes. The basic idea is to design circuits such that all datapaths and D-type Flip-Flops, involved in the computation of intermediate values of cryptographic elements, randomly change within a set of logically equivalent electrical paths that are spatially distributed within the Integrated Circuit (IC) die.**

I. INTRODUCTION

In the last century, modern cryptology was mainly focused on defining crypto-systems resistant against theoretical attacks. However, with the increasing use of secure embedded systems, researchers have 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 of them exploit the timing behavior of Integrated Circuits (IC) [1], while others exploit their global power consumption such that the well known Differential Power Analysis (DPA) [2].

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 striking one. Indeed, it allows an attacker to target the bounded hardware area integrating the cryptographic algorithm under attack or part of it, typically D-type Flip-Flops sampling intermediate values of a given cryptographic module. This is all the more interesting since it also allows to get around global hardware countermeasures against power analysis such that the use of detached power supplies [5] by focusing the analysis on reduced die areas.

Assuming that attackers are able to focus their analysis on a reduced die area implies a main design problem: how to protect critical data from such extremely focused attacks?

The solution proposed in this paper is to design circuits in order to ensure that there is no bounded area of the circuit which is dedicated to a given and clearly identified cryptographic operation. More precisely, the basic idea proposed herein is to design crypto-modules so that all their intermediate values may be computed and sampled by different, but logically equivalent datapaths, and D-type Flip-Flops that are spatially distributed within the IC die.

Note that the idea of randomly changing the location of the functional blocks has been recently proposed in [6] as a countermeasure against Power and Fault attacks. However, [6] exploits the dynamic reconfiguration capabilities of some programmable logic devices and thus the associated solution is not suitable for ASIC design. Furthermore no evaluation of this solution against EM attacks is given.

Note also that the solution proposed herein is not equivalent to the solution consisting in duplicating the considered crypto-module into several, and randomly using one of them to perform the computation. Indeed, it rather consists in designing a single module implemented so that:

- a given functional part of the considered algorithm and its associated registers may randomly compute, and store different intermediate values,
- all parts of the resulting crypto-module are always activated during all cryptographic operations in order to avoid attackers detecting, during a local EM attack, whenever a piece of hardware is in use or not.

Considering the DES algorithm as a case study, which has been widely studied in the literature, we organized the remainder of the paper as follows. A minimal presentation about the DES algorithm is done in Section II. This section also explains the problem linked to Differential and Correlation EM analysis (DEMA & CEMA), and shows several attacks realized on a standard iterative DES. Section III shows how it is possible to transform a standard DES crypto-module [7] according the aforementioned design guidelines to obtain a DES with the proposed spatial jamming countermeasure against local EM analysis. Section IV gives details related to the evaluation of the countermeasure robustness against EM analysis, with concrete results and a related discussion, before to conclude in section VI.

II. ELECTRO-MAGNETIC ANALYSIS ON DES

We introduce the Data Encryption Standard (DES) [7] and its standard iterative implementation, which has been the groundwork of our analysis. DEMA and CEMA are then briefly described. A standard DES, on an FPGA, is then attacked in order to evaluate its robustness and fix a robustness reference.

978-1-4244-6471-5/10/$26.00 ©2010 IEEE

A. DES Implementation

The DES algorithm, depicted in Fig. 1, is basically a 16-round process. As shown in Fig. 2, its standard implementation is iterative and requires 17 clock cycles to cipher (or encipher) a plain text input (PTI). Several functional blocks are necessary to perform the round computation. The Key schedule computes, at each clock cycle, the 48-bit round key from the main 64-bit secret key (KEY). The Feistel function (F) shuffles data and sub-keys using a XOR operator, eight substitution boxes, an expansion function and an internal permutation. Two 32-bit registers, Ln and Rn, allow sampling intermediate 32-bit words, while the PTI and final ciphered text output (CTO) are stored in 64-bit registers. Finally, a cipher manager block ensures the sequencing of all operations.

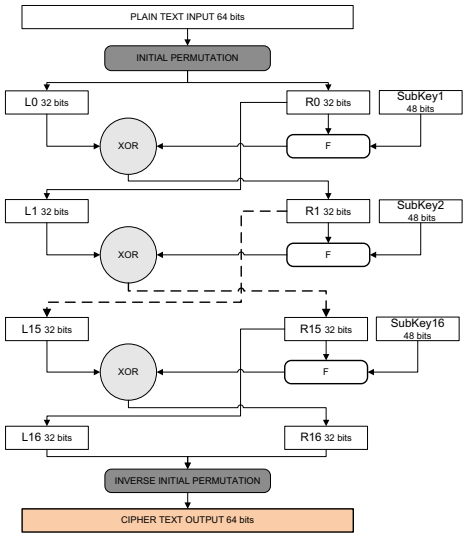

Figure 1. Data Encryption Standard (DES)

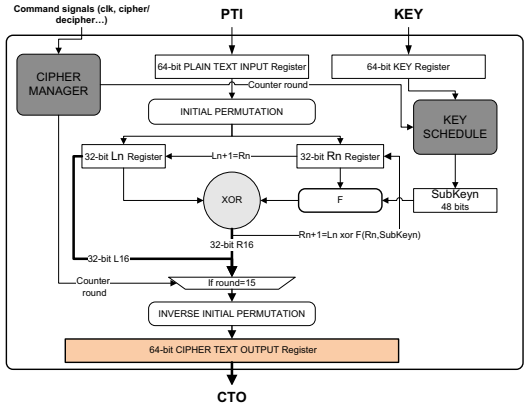

Figure 2. Iterative DES implementation

B. Electromagnetic Analysis

DEMA and CEMA introduced in [3,4,8] are based on the fact that EM emanations during cryptographic operations strongly depend on the handled data. These attacks, like Power Analysis based ones, are usually performed in three steps: *data collection, data sorting and data analysis*.

Data collection consists in sampling and recording the EM emanations with a sensor, 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.

As depicted in Fig. 3, the magnetic probe (a loop with a 500µm diameter, and a bandwidth greater than 1GHz), positioned with accuracy by the motorized stage (along X, Y and Z axes with a resolution of 10µm) just above the FPGA, is linked to a low noise amplifier (48dB with 1GHz bandwidth). The output of the latter is connected to the digital oscilloscope (with a 2.5GHz bandwidth, to sample at 40GS/s the time domain evolutions of measured signals). The crypto-module does the encryption on 64-bit words sent by the computer (via RS232) with the secret key defined by the user and previously stored in the crypto module. Then, the circuit sends back the 64-bit cipher text to the PC. A software DES is carried out simultaneously and processes the same 64-bits words. At the end of the 16th round, both 64-bit are compared in order to detect eventual but rare ciphering mistakes (mainly due to bad communications). Finally, the oscilloscope sends the EM trace, saved during the encryption stage, to the PC.

Data sorting consists in extracting several sub-sets of EM traces according to one selection function from the whole set of traces. For each possible guess made on a small part of the secret key (denoted *sub-key* in the following), different selection functions allow predicting few bits of intermediate words. Then, as an example, according to a guessed intermediate bit values, differential curves may be computed to achieve a single bit DEMA [2]. Without loss of generality, it was considered, in the rest of the paper, that an adversary tries first to guess the round-key 1, and in a second step the remaining bits of the secret key by a brute force attack or a EM attack on the second round (case of a known plain-text attack).

Data analysis consists in identifying which guess among all possible guesses of the sub-key is the correct one. This may be done according to several key search criteria leading to attack with different names [2,3,8]. Among all known attacks, we considered in this paper Differential Electro-Magnetic Analysis (DEMA) as proposed in [2,3] and Correlation Electro-Magnetic Analysis (CEMA) as defined in [8]. Note that all these attacks were done considering both Hamming Weight (HW) and Hamming Distance (HD) models. Since HD model gave better results from an attacker's point of view, only results related to this model are reported afterward.

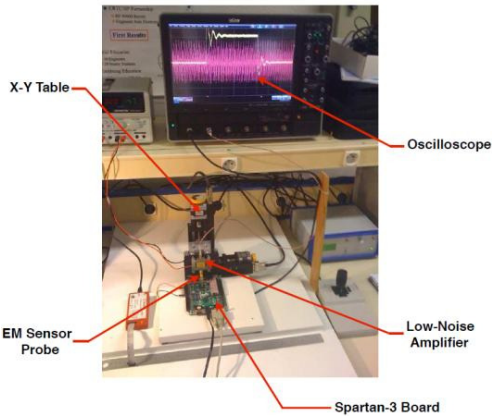

Figure 3. EM measurement platform

Both *DEMA_Sum* and *CEMA* [8] were carried out to evaluate our standard DES design.

The *DEMA_Sum*, consists in: performing for each sub-key four single bit DEMA [2,3], summing the four sets of 64 differential traces (one for each possible guess) and finally in identifying the trace with the greatest amplitude assumed to be the right sub-key by the attacker.

The CEMA of Brier [8] consists, for each sub-key, in computing the HD value for each possible guess of the sub-key, and then in computing, for each time sample of the EM traces, the Pearson's correlation value between the EM amplitude, and the HD value associated to each guess. Finally, the attacker identifies the right guess as the guess with the highest correlation value.

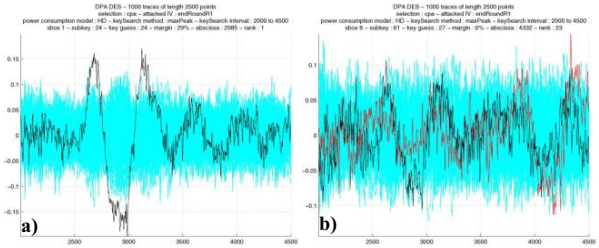

Figure 4. Examples of CEMA curves (HD model, sbox1 (a) and sbox8 (b)).

In Fig. 4, the 64 CEMA traces obtained for the first round key are depicted in two cases. In the first case (a), the *CEMA* is successful: the right sub-key (sub-key 1) corresponds to the curve with the highest amplitude; sufficient traces have been processed to ensure the statistical convergence. On the contrary (case (b)) the correct sub-key (sub-key 8) is not disclosed; more traces have to be processed to ensure the convergence. In this example, it appears that sub-key 1 is less robust against CEMA than sub-key 8. Indeed, for the same number of traces, the same CEMA successfully discloses sub-key 1, and not sub-key 8.

C. *Attacks realized on a standard DES*

Two experimental validation campaigns were achieved with the measurement platform showed in Fig. 3:

- 100 000 EM traces were collected, during this encryption campaign, with a 500µm probe placed at the center of the die,
- 100 000 EM traces were collected, during this encryption campaign, with a 500µm probe placed at a position where the DES was clearly observable by Simple EM analysis [9]; i.e. a position with a high SNR value.

The traces collecting, sorting and analysis steps were performed on one shot traces (no average). Then, *DEMA_Sum* and CEMA were launched on the first round.

Fig. 5 and 6 sum up the main results. More precisely, these figures give, with respect to the number of processed traces, the number of sub-keys correctly disclosed by CEMA, and *DEMA_Sum* while, considering the HD Model.

Fig. 5 demonstrates that *DEMA_Sum* allows disclosing with 11 000 and 60 000 traces the full round key at the two considered positions.

Similarly, as shown Fig. 6, for both positions, after the processing of only 3000 EM traces, all sub-key are disclosed by the CEMA. These results highlight once again the superiority of CEMA compared to DEMA.

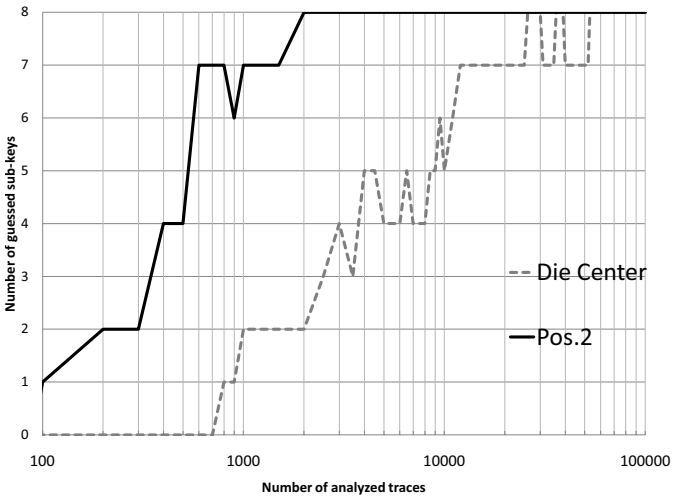

Figure 5. Number of disclosed sub-keys with *DEMA_sum* (HD model) wrt the number of processed traces

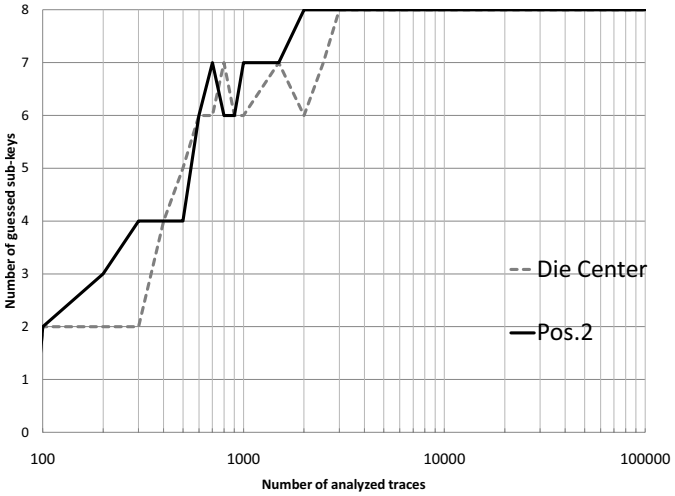

Figure 6. Number of disclosed sub-keys with CEMA (HD model) wrt the number of processed traces

TABLE I. ATTACK RESULTS ON A STANDARD ITERATIVE DES

	Attack	*Model*	*First right guess of the round key*	*Stability reached at*	*% of right round Key guesses*
Die center	CEMA	HD	795	2633	**97.38**
	DEMA	HD	11 134	11 431	**57.36**
Position 2	CEMA	HD	1872	1966	**98.12**
	DEMA	HD	1583	1715	**98.29**

Table I gives additional results related to the attacks performed on the standard iterative DES. More precisely:

- the fourth column gives the number of traces required to disclose for the first time the right round-key,
- the fifth one gives the number of traces required to reach the statisctical convergence according to DPA contest rules [10],
- the last one gives the percentage of correct guesses of the round key after the processing of 100 000 traces.

As shown by this table a standard iterative and unprotected DES implementation is susceptible to EM analysis.

III. DES WITH SPATIAL JAMMING

One approach to increase the robustness of a chip against DEMA and CEMA is to minimize or reduce the correlation between processed data and measured EM radiations. Emission characteristics depend on many topological and physical parameters such as to the sensor used to collect them, the emitting wire orientations, and of course the amplitude of the current flowing in these wires. Considering these dependencies, the spatial jamming countermeasure aims at changing the positions and the orientations of the wires supplying the current to sensitive pieces of hardware associated to intermediate value computations. Expected effects of this countermeasure are thus: (a) to prevent an attacker from performing a focused EM attack and (b) to jam the EM emissions of the hardware.

The following section describes how to transform an iterative and unprotected DES implementation into one integrating the proposed spatial jamming countermeasure.

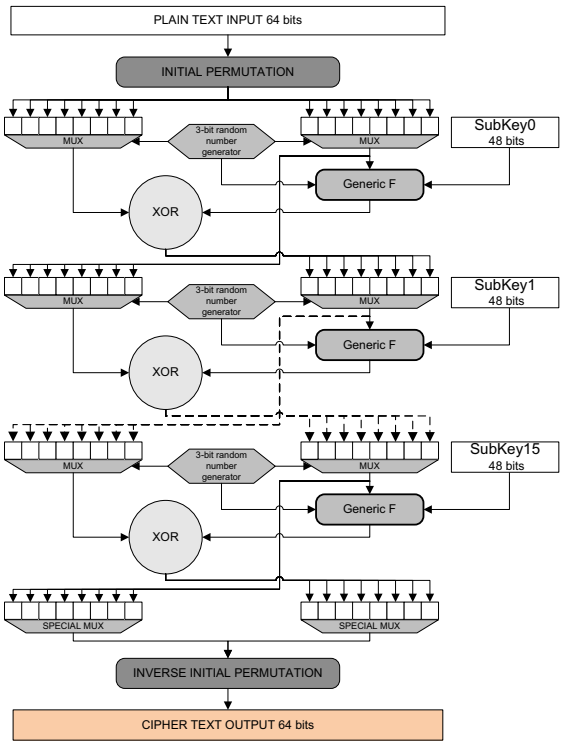

Figure 7. DES with spatial jamming countermeasure

A. Global Modifications

Fig. 7 describes the DES with spatial jamming. The registers Ln and Rn are divided in eight parts submitted to a random cyclic permutation (Fig. 8). With respect to the initial DES algorithm and to be able to decrypt the cipher word, the F function is substituted by a generic F function. The aim of the Generic F is to adapt the 32-bit word stored in Rn, previously mixed by the Mux entity. At the end of DES jamming encryption, the CTO must be the same CTO provided by the standard iterative DES.

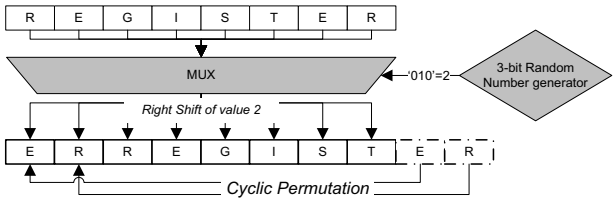

Figure 8. Example of 4-bit word cyclic permutation within Ln or Rn 32-bit register of Fig.7

B. Data multiplexing

Mux functions (Fig. 7 and 8) are the key modifications on which the spatial jamming countermeasure is based. Indeed, these functional blocks ensure that DES intermediate values (the ones obtained at the end of each round), to be stored in Ln and Rn registers at each clock cycle, are computed and sampled by a set of physical instances randomly picked up among a set of available and dedicated resources. More precisely, each bit of the 64 bits to be stored in Ln and Rn registers at the end of each round is physically sampled by a single D-Flip-Flop selected among a set of possible D-Flip-Flops (in our experiment 8) according to a random number RN (3 bits in our experiment); the latter being provided by an on-chip random number generator. In other words, each intermediate bit may be sampled and stored at 8 different places in our design according to a cyclic permutation fixed by RN at each round. As an example: the LSB of Rn at the 5^{th} round may be stored in the 1^{st}, 5^{th}, 9^{th}, 13^{th}, 17^{th}, 21^{th}, 25^{th}, 29^{th} DFF of Rn register.

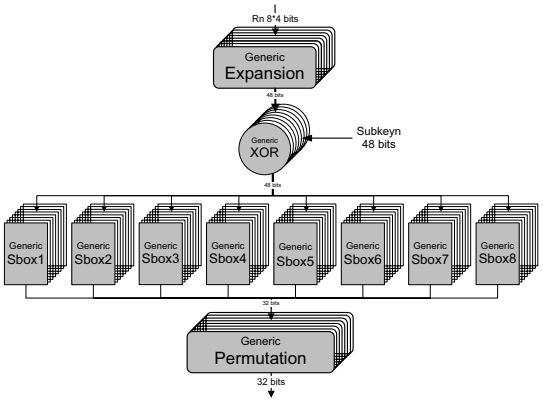

Figure 9. Modified Feistel block (Generic F in Fig.7)

C. Modified Feistel block (Generic F)

Randomly allocating, at each clock cycle, each intermediate bit to a given DFF requires modifying the F function as shown in Fig. 9. Indeed, the eight substitution boxes (s-boxes) enclosed in the F function are non-linear functions and permute a bit with another bit result in a wrong output result. Similarly, the expansion function, the xor, and the permutation, required to integrate the F function, have to be modified in order to preserve theirs functionalities according the 3-bit word cyclic permutation fixed by the random generator.

To overcome this problem, each of the 8 s-boxes is replaced by a generic s-box as illustrated in Fig. 9. This generic s-box takes, as usual, 6 round-key bits and 6 bits of data, but also the random number RN in order to be able to perform the right substitution among the eight ones defined by the Data Encryption Standard, according to RN value. Similarly, expansion and permutation have to be performed during each round according to the RN value. Finally, the xor is modified to be able to add the right round-key bits with the right bits provided by the expansion function.

D. Special Muxes

As shown in Fig. 7, special muxes are used after the sixteenth round in order to recover the right bit arrangement before the reversal of the initial permutation. An ad-hoc small structure is therefore integrated to count the overall number of cyclic permutations realized during each DES algorithm course. More precisely, at each round n (n=0…15) this structure computes the sum SSn of right-shifts done at the considered round with the sum SSn-1 previously obtained. Note that this sum is done modulus 8 since these shifts are done cyclically.

IV. SPATIAL JAMMING ROBUSTNESS AGAINST EM ANALYSIS

The objective of this section is to evaluate the robustness against EM attacks of the proposed countermeasure. This is achieved by comparing attack reports obtained for the DES with spatial jamming with those obtained for the standard iterative DES. Actually note that the experimental results presented in the section II were obtained with a DES with spatial jamming in which a little piece of hardware allows activating or not the countermeasure by forcing the random number RN to zero or not. This choice was done to be sure to evaluate the efficiency of the spatial jamming with strictly the same hardware (same routing, same placement, same clock tree, … and thus the same bitstream).

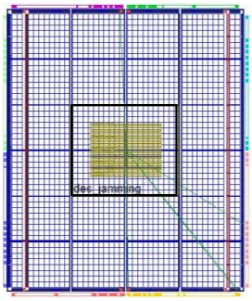

Figure 10. DES jamming Floorplan on a FPGA XC3S1000

A. Prototyping on FPGA

The DES with spatial jamming was implemented into a Xilinx FPGA XC3S 1000 board. The implementation was done in order to (a) place the design in the center of die, and (b) to minimize its area. Fig. 10 gives the resulting floorplan. Note that a RS-232 communication module was also embedded in the core in order to exchange 64-bit data blocks with the PC.

The clock signal used to cadence all data processing elements is the internal 50 MHz clock signal available in the considered Spartan board. Note that a trigger signal is also output by the final design on a circuit pad to synchronize EM measurements.

These design guidelines were applied to facilitate the EM attacks by (a) easing the probe positioning above the package and (b) by limiting the EM noise generated by the pads.

B. Spatial jamming overhead

Table II presents the main design characteristics of (a) the standard iterative DES without any countermeasure and (b) the DES with spatial jamming, both mapped onto the same FPGA. Note again, that all data reported in this paper are related to the DES with spatial jamming except some of Table II that are related to the mapping of a standard iterative DES. This has been done to quantify the area overhead and the performance penalty.

As shown, the number of slices, slices flips-flops and LUTS required to integrate both solutions are reported. Note that these values do not include the extra-hardware required to map the RS232 module. Maximal operating frequencies values are also reported Table II. These latter values have been obtained from post Place and Route timing analysis.

TABLE II. STANDARD DES VS DES JAMMING

Designs	*Slices*	*Flips flops*	*4 inputs LUTs*	*Max.freq (MHz)*
Without jamming	294	125	558	108.1
With jamming	1105	146	2140	50.4
Ratio	**3.75**	**1.17**	**3.83**	**0.47**

In the table II, the number of Flip-flops increases from 125 to 146. This is mainly due to the integration of a 16-bits pseudo-random generator and its associated DFF to sample a new RN value at each clock cycle. As shown, row 2 and 4, the number of slices and the number of LUTs is nearly tripled. This is mainly due to the integration of the multiplexers, and to the generalization of F function. Indeed, the key schedule block does not change, and the number of DFF in the DES module is kept constant.

The maximal frequency, after Place and Route stage, is equivalent to 50.4 MHz. It is divided by 2 compared to the standard DES version. Note however that the synthesis was done to meet the smallest die area (no timing optimization was done). Note also that this value, obtained on FPGA, remains higher than that observed on smartcards.

C. *Robustness of the DES with spatial jamming*

Three experimental validation campaigns were performed with the measurement platform showed in Fig. 3:

- 500 000 traces were collected, during this encryption campaign, with a 500µm probe, positioned at the center of the die,
- 500 000 traces were collected, during this encryption campaign, with the same 500µm probe placed at a position where the DES was clearly observable by Simple EM Analysis (SEMA),

Fig. 11 and 12 show the evolution of the number of correct sub-key guesses according to the number of analyzed traces, at the two different positions for *DEMA_Sum* and CEMA respectively.

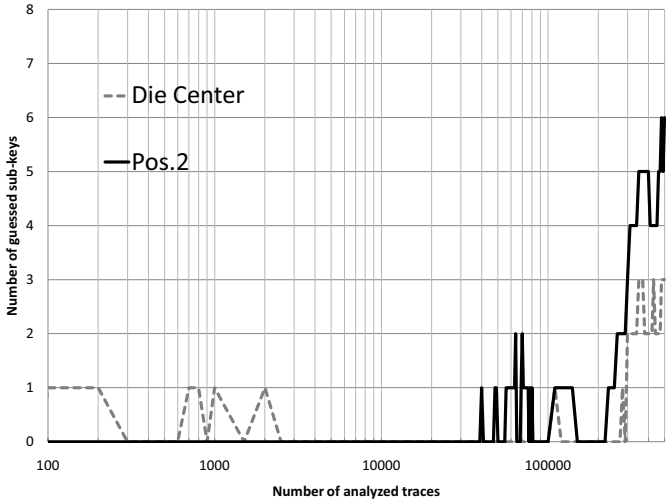

Figure 11. Number of disclosed sub-keys with *DEMA_Sum* (HD model) wrt the number of processed traces

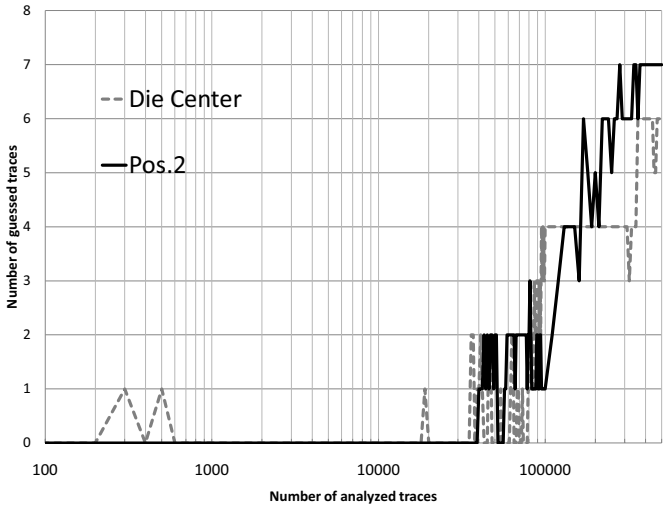

Figure 12. Number of disclosed sub-keys with CEMA (HD model) wrt the number of processed traces

As shown in Fig. 11, only 6 sub-keys are disclosed by DEMA_Sum after the processing of all traces. This number is to be compared with those reported Table I showing that all sub-keys are disclosed with less than 2000 traces for probe position 2. Fig. 12 reports similar results than that of Fig. 11 but for a CEMA launched with the HD model. As shown, CEMA allows an attacker disclosing up to 7 sub-keys by processing 500 000 traces.

As a result, it indisputably appears that the spatial jamming countermeasure increases the security of the DES against DEMA and CEMA. Indeed, with 500 000 traces such attacks were unsuccessful in disclosing the full round key. Compared to the original implementation, experimental results show that the proposed countermeasure has improved the robustness of the DES by a factor of at least 50.

V. CONCLUSION

In this paper, evidences of the efficiency of the spatial jamming countermeasure against local EM attacks have been given. Indeed, it has been experimentally demonstrated that this countermeasure is sufficient to protect a DES implemented into a FPGA against CEMA and DEMA attacks performed with 500 000 traces. Such robustness is obtained for an area overhead of 3.5, i.e. with a lower or equivalent overhead than those obtained with countermeasures based on dual rail encoding [11]. Among future works, we intend to investigate whether the spatial jamming countermeasure can be applied to the AES. We also plan to explore the efficiency of the proposed solution against fault attacks.

REFERENCES

[1] Paul C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996: 104–113

[2] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. Published in Advances in Cryptology - Crypto 99 Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener, ed., Springer-Verlag, 1999.

[3] K.Gandolfi, C. Mourtel, F. Olivier: Electromagnetic Analysis: Concrete Results. Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes In Computer Science; Vol. 2162 archive, pp. 251 – 261, 2001

[4] E. Peeters, F. X. Standaert, J. J. Quisquater: Power and electromagnetic analysis: Improved model consequences and comparisons. Integration, the VLSI Journal, Volume 40, Issue 1 (January 2007), Special issue: Embedded cryptographic hardware, Pages: 52 – 60, 2007.

[5] A. Shamir: Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies. Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems (200), Lecture Notes in Computer Science, Volume 1965/2000.

[6] N. Mentens, B. Gierlichs, and I. Verbauwhede, "Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration," In Cryptographic Hardware and Embedded Systems - CHES 2008, pp. 346-362, 2008.

[7] Data Encryption Standard, FIPS PUB 46-3.

[8] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in: M. Joye, J. J. Quisquater (Eds.), Cryptographic Hardware Embedded System--CHES 2004, Lecture Notes in Computer Science, vol. 3156, Springer, Berlin, 2004, pp. 16-29.

[9] S. Mangard, A Simple Power-Analysis (SPA) attack on implementations of the AES key expansion, ICISC 2002, Lecture Notes in Comput. Sci. vol. 2587, Springer-Verlag, Berlin (2002), pp. 343–358.

[10] http://www.dpacontest.org/v2/rules.php

[11] K. Tiri: Side-Channel Attack Pitfalls, Proc. of the ACM-IEEE Design Automation Conference (DAC 2007), 15-20, ACM-IEEE, 2007