A Frequency Leakage Model and its application to CPA and DPA

S. Tiran[1], S. Ordas[1], Y. Teglia[2], M. Agoyan[2], and P. Maurine[2]

[1] LIRMM, Université Montpellier II
161 rue Ada, 34392 Montpellier CEDEX 5, France
[2] STMicroelectronics, Advanced System Technology (AST)
190 Avenue Célestin Coq, Z.I. Peynier-Rousset, 13106 Rousset CEDEX, France

Abstract. This paper introduces a leakage model in the frequency domain to enhance the efficiency of Side Channel Attacks of CMOS circuits. While usual techniques are focused on noise removal around clock harmonics, we show that the actual leakage is not necessary located in those expected bandwidths as experimentally observed by E. Mateos and C.H. Gebotys in 2010. We start by building a theoretical modeling of power consumption and electromagnetic emanations before deriving from it a criterion to guide standard attacks. This criterion is then validated on real experiments, both on FPGA and ASIC, that show an impressive increase of the yield of SCA.

Keywords: SCA, DPA, CPA; Leakage Model, Frequency Domain

1 Introduction

Since the publication by P. Kocher, J. Jaffe and B. Jun of the [11], new analyses, or techniques to enhance Side Channel Analyses (SCA), have been proposed in the literature. The first improvements consisted in the use of better statistical tools to compare populations distributions. Hence Correlation Power Analysis (CPA) has been proposed in 2004 [5] to replace the difference of means by the Pearson coefficient. Then the Mutual Information Analysis [10] has been proposed in order to capture higher order dependencies and enhanced in [27] [12].

A second category of improvements consisted in the proposal of several solutions for increasing the quality of the measurements. Among the possible improvements of SCA, any technique allowing to increase artificially the Signal to Noise Ratio (SNR) of traces after their acquisition is obviously interesting. An approach lies of course in the use of the average mode of oscilloscopes. However this is not always feasible because of the timing jitter characterizing the circuits operations. Another solution lies in the characterization of the noise usually considered Gaussian to limit its effects or remove it from the signal using a pre-processing technique [6] [13].

More recently, attacks working in the frequency domain have been proposed as a promising alternative to usual time domain attacks because of their potential robustness to noise and to jitter of acquisitions [17]. First, it was suggested in [4], [20], [9] and [17] to transpose well-known CPA and DPA in the frequency domain by using the Fourier Transform (FT). All these works highlighted the efficiency of attacks in the

frequency domain and [17] has experimentally observed that the distribution of the leakage in the frequency domain was independent of the clock signal. Second, but still by working in the frequency domain, it was proposed in [7] and [25] to exploit the shape of traces rather than their amplitude solely. Simultaneously, authors of [2] and [3] have attempted to enhance CPA or DPA by filtering traces around the clock signal frequency or its harmonics. They also have presented a method for finding the frequency bands containing more leakage. It aims at calculating frequency templates for each value of the key assuming the adversary has the full control of an equivalent circuit. In the same vein, adaptive filters were applied in [21] to identify, during the course of SCA, where in the frequency domain, the leakage is the most important.

The getting of traces with little background noise, or the improvements post acquisition of noisy traces, are important topics as evidenced by the state of the art. If most existing solutions consist in the application of signal processing techniques or statistical tools, no work has attempted to address this problem through the analytical modeling of the leakage in the frequency domain; knowing that even a rough model may efficiently drive statistical tools. This is the approach we propose to pursue in this paper.

More specifically, from the study of the operation of synchronous CMOS circuits, we propose in Section 2, a model of their power consumption and of their Electro-Magnetic (EM) emanations. From this first-order model, a model of the leakage in the frequency domain is established in Section 3, before extricating from its implications a simple and efficient method to identify, from few raw traces, the frequencies on which the leakage is a priori greater. Then in Section 4, to validate the correctness of the model in an indirect way, the method is applied to various sets (current or EM) of traces, characterized by different levels of noise. Finally, a conclusion is drawn in Section 5.

2 Leakage Model in the Frequency Domain

This section is intended to establish, from the analysis of the operation of synchronous circuits, a modeling of the leakage in the frequency domain.

2.1 Operation of CMOS circuits

Current cryptographic circuits are, with few exceptions, synchronous. Their electrical activity, and their resulting EM emanations, are thus clocked by a global signal. This clock signal is propagated across the whole circuit, through a network of logic gates and interconnects, called clock tree, to reach the input of all registers (DFF) at the same time.

Fig. 1 gives a simple and generic representation of a synchronous circuit. It is made of two sets of registers (D-type Flip Flop) to sample regularly the output of the logic block (Glue Logic) which realizes some cryptographic calculi or not, and of a clock tree whose activity is independent of data processed by the logic block. [14] show different methods to extract the clock tree activity from traces. Given this description, the modeling of the current consumed by a circuit, or the modeling of its EM emissions, leads to define traces, T, as the sum of different contributions :

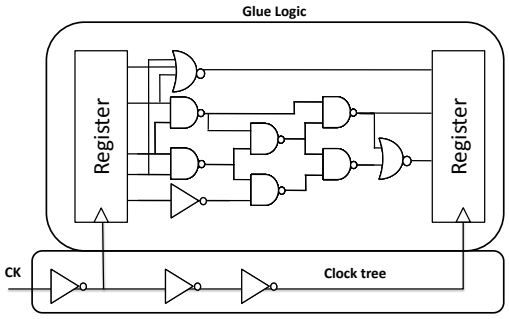

Fig. 1. A simple CMOS circuit

$$T = T_{GlueLogic} + T_{CK-Tree} + \eta_{env} + \eta_{intra} \tag{1}$$

where $T_{GlueLogic}$ is the power consumed by the Glue Logic (or its EM emanations), $T_{CK-Tree}$ the one of the clock tree, η_{env} a noise, assumed Gaussian, produced by the environment but also due to the quantification noise of the oscilloscope and η_{intra} the noise produced by the other elements of the circuit called algorithmic noise [19]. Assuming CMOS gates (including DFF) are the only source of leakage because they are the only elements involved in cryptographic computations, we analyzed owing to electrical simulations [1], the power consumption of the Glue Logic of various circuits. From this study, carried out by varying various design parameters, we defined a first order model of the switching current consumed by a clocked logic block during one clock cycle.

This time dependent model is represented in Fig. 2. It first gives the clock signal that launches a new calculus at each rising edge and therefore produces a current inrush. The simulated waveform of this current as well as its modeling is given Fig. 2b. This current inrush is the source of EM emanations proportional to its amplitude. However, because coils used to measure these emanations have a differentiator behavior, we adopted the modeling of EM emanations represented in Fig. 2c. It should be noted that in Fig. 2, the timing slack is the design margin introduced by designers so that to achieve a high manufacturing yield. It results from the worst case design approach followed by designers to take process manufacturing variations into account but also voltage and temperature variations experienced by Integrated Systems.

2.2 Leakage Model in the frequency domain

From these models, it seems possible to study the spreading in the frequency domain of the leakage starting by the calculation of the Fourier Transforms of the power consumption, $POW(f)$, and of EM emanations, $EM(f)$, of the Glue Logic. These calculations lead to (see Appendix A) :

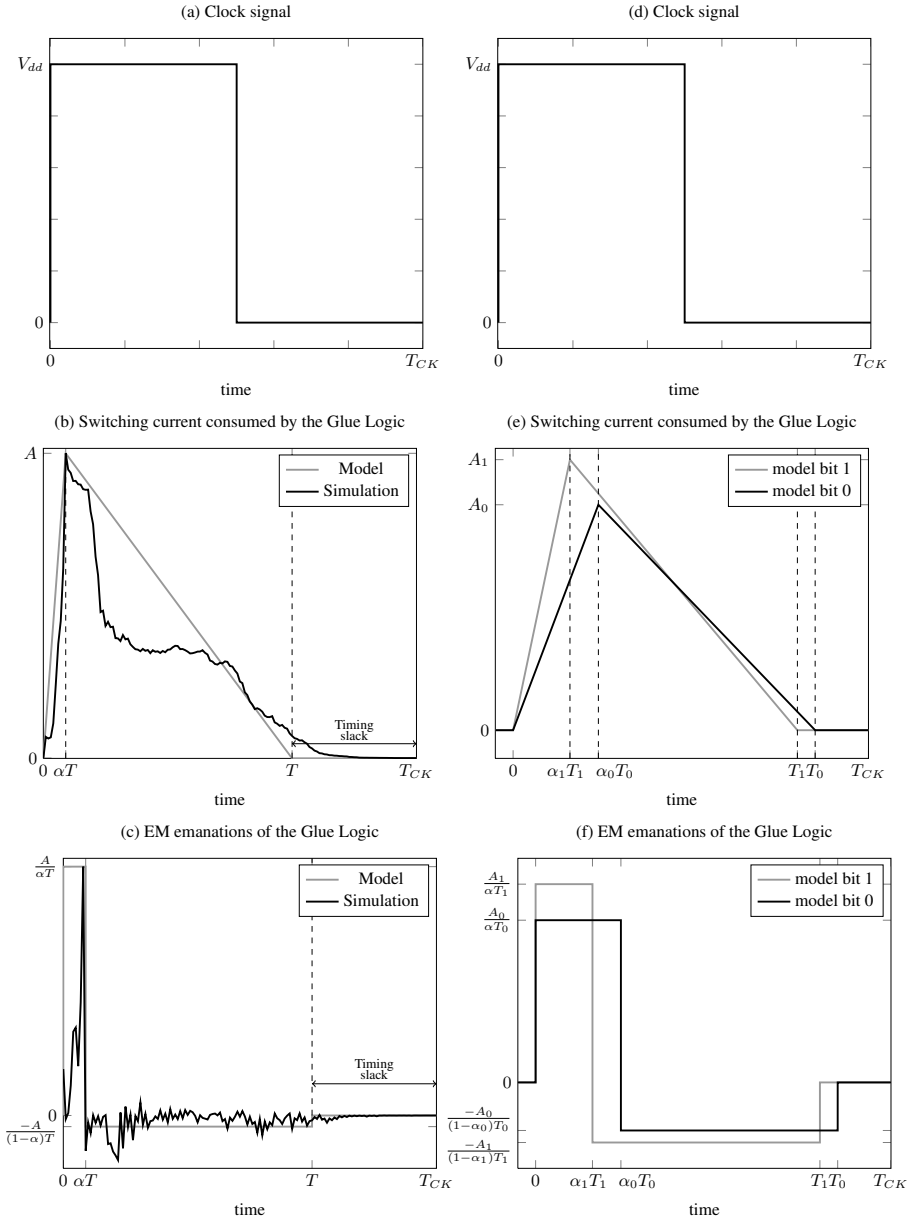

Fig. 2. Models of the switching current consumed (b) by the Glue Logic and of its EM emanations (c); Models of the current and EM leakages (e and f respectively)

$$POW(f) = \frac{-jA}{2\pi^2 f^2 T} \left\{ \frac{1}{\alpha} \sin(\alpha \pi f T)\, e^{-j\pi f \alpha T} - \frac{1}{1-\alpha} \sin\big((1-\alpha)\pi f T\big)\, e^{-j\pi f \left((\alpha+1)T\right)} \right\} \tag{2}$$

$$EM(f) = \frac{A}{\pi f T}\Big\{ \frac{1}{\alpha}\sin(\alpha\pi f T)\, e^{-j\pi f \alpha T} - \frac{1}{1-\alpha}\sin\big((1-\alpha)\pi f T\big)\, e^{-j\pi f\left((\alpha+1)T\right)}\Big\} \tag{3}$$

where α is a parameter, related to the transition time of clock edges but also to the clock skew [22]; it sets the rise time of the current. T is the effective duration of the calculation which is independent of the clock signal period T_{CK}. However, it depends on the processed data but also on the Glue Logic structure as well as the supply voltage and temperature values. A is the maximum amplitude of the current.

SCA, like DPA and CPA, consist in the comparison of statistical populations with specific criteria [11] [5]. One of them is the adopted power consumption model. Hence in CPA for instance, the attacker performs a correlation between a set of measurements and a set of computed internal variables of the algorithm which is built according to the way the underlying hardware is expected to consume power or generate an EM field. In DPA, the two subsets of curves that will be compared are generated according to the same hypothesis. So far, two models have been proven efficient: the Hamming Weight model (HWM) and the Hamming Distance Model (HDM). According to the first one, the consumption of Glue Logic is greater when the target bit is equal to '1', while according to the second model, the consumption is higher when the bit changes state during the calculation. The CPA is based on the same principle, but works on the linear trend of the power consumption at increasing or at decreasing according to the values of several bits [16].

HDM or HWM are time independent and thus do not allow the establishment of a leakage model in the frequency domain. In order to establish a time dependent model, or at least a model allowing estimating the leakage distribution in the frequency domain, let us assume in accordance with the HD model (HW model), that if the value of the target bit is switched during the calculus (is equal to '1' at the end of the calculus), the current waveform is altered (is different) both in amplitude and duration compared to the case in which the bit remains stable (is equal to '0' at the end of the calculus). This is what shows Fig. 2. These assumptions are justified in that the switching (or not) of a bit stored in a register forces the switching (or not) of a number of CMOS gates in the logic block which depends in turn of the other bits of the register. The amplitude of the current, and hence EM emanations, are therefore altered over a time interval longer than the propagation delay of D-type Flip Flop.

At this point, it should be noticed that without knowing in detail the physical structure of the circuit (except if you are designing a secure product), it appears impossible to finely predict how the current waveform is altered. This explains why in Fig. 2, we drawn the waveform associated to 'HD / HW ='0' with a longer duration (and a higher amplitude at the end of the calculus) than the one associated to 'HD / HW ='1'. We could have represented the opposite situation without being wrong. In fact, the only characteristics of the waveforms of Fig. 2 that remain valid in all cases are:

- their shapes which are representative of current and EM waveforms respectively,
- higher amplitudes in absolute value at $t = \alpha_1 T_1$ than at $t = \alpha_0 T_0$ in accordance with the HD or HW models.

Assuming this model is sufficiently realistic (HW and HD models are currently considered representative) to capture the overall behavior of the leakage, it seems possible

to derive from it a modeling of the leakage in the frequency domain using the Fourier transform. This leads (see Appendix A), respectively, for the current and the EM emanations to:

$$L_{POW}(f) = \frac{-jA_1}{2\pi^2 f^2 T_1}\left\{\frac{1}{\alpha_1}\sin(\alpha_1\pi f T_1)\, e^{-j\pi f\alpha_1 T_1} - \frac{1}{1-\alpha_1}\sin\big((1-\alpha_1)\pi f T_1\big)\, e^{-j\pi f\left((\alpha_1+1)T_1\right)}\right\} - \frac{-jA_0}{2\pi^2 f^2 T_0}\left\{\frac{1}{\alpha_0}\sin(\alpha_0\pi f T_0)\, e^{-j\pi f\alpha_0 T_0} - \frac{1}{1-\alpha_0}\sin\big((1-\alpha_0)\pi f T_0\big)\, e^{-j\pi f\left((\alpha_0+1)T_0\right)}\right\} \quad (4)$$

$$L_{EM}(f) = \frac{A_1}{\pi f T_1}\left\{\frac{1}{\alpha_1}\sin(\alpha_1\pi f T_1)\, e^{-j\pi f\alpha_1 T_1} - \frac{1}{1-\alpha_1}\sin\big((1-\alpha_1)\pi f T_1\big)\, e^{-j\pi f\left((\alpha_1+1)T_1\right)}\right\} - \frac{A_0}{\pi f T_0}\left\{\frac{1}{\alpha_0}\sin(\alpha_0\pi f T_0)\, e^{-j\pi f\alpha_0 T_0} - \frac{1}{1-\alpha_0}\sin\big((1-\alpha_0)\pi f T_0\big)\, e^{-j\pi f\left((\alpha_0+1)T_0\right)}\right\} \quad (5)$$

These equations show that the calculus of the leakage distribution in the frequency domain requires the knowledge of some variables, such as :

- the timing slack to estimate at first order T/T_{CK}, i.e. T, T_1 and T_0,
- the skew and the transition times of the clock signal for estimating α, i.e. to estimate when the maximum current consumption occurs,
- and many other parameters (quality of the process, effective supply voltage, temperature, ...) affecting the propagation delays and the current consumed by the CMOS logic gates.

These parameters are not known a priori by the opponent, it is therefore difficult for an attacker, with no collusion, to directly exploit this modeling. From the designer standpoint, this is a powerful tool allowing to deeply characterize the security blocks while providing him a competitive advantage over the attacker. Indeed, the designers may now know which frequencies should be blurred by adding noise or reduced in amplitude.

2.3 Model Implications

If it is difficult and even impossible except for the designer to predict with accuracy the values of all terms involved in the two leakage models, the analysis of these equations indicates that the frequency distribution of the leakage:

- extends in a domain ranging between 0 Hz and $+\infty$, and more pragmatically up to the cut-off frequency of the acquisition system, contrarily to what was observed in [17],
- is independent of the clock frequency at which the circuit works as experimentally observed by [17], although indirectly linked to the maximum frequency, $F_{CKmax} = 1/T$, at which the circuit can operate,
- results from the difference of two *sinc* functions, and is therefore essentially distributed at low frequencies with an amplitude bounded above by the function $\frac{1}{f}$ (or $\frac{1}{f^2}$) for the EM leakage (for the current leakage respectively).

These indications can be leveraged to enhance the efficiency of DPA and CPA analyses. This is what is highlighted by the rest of the paper in order to support the validity of this leakage modeling in the frequency domain. Indeed, the main implications of these models indicate a way to increase the SNR of traces before application of a CPA or a DPA analysis. Indeed, because the leakage is mainly located on the lower frequencies (ie bounded by the function $\frac{1}{f}$ or $\frac{1}{f^2}$), it seems possible to improve the signal to noise ratio of traces by pre-processing.

More specifically, two scenarii emerge. The first one is related to the analysis of traces characterized by a small background noise such as traces obtained using the average mode of oscilloscopes. In that case, the model suggests that it is better not to filter the traces and even encourages the use of equipments with the highest bandwidth possible.

The second case, which is more realistic, is related to the analysis of noisy traces. In that case, the model suggests to improve the signal to noise ratio by filtering or removing high frequencies carrying only a small part of the leakage. We consider these two cases in the next section.

2.4 Model exploitation

The choice of frequencies that must be kept or removed from traces prior to application of a CPA or DPA analysis seems difficult. However considering the lessons provided by the model the choice appears easier. Indeed, even if the opponent has only raw traces given by Eq. 1, he can easily calculate the signal to noise ratio at each frequency, f, of the raw signal spectrum and multiply the result by $\frac{1}{f}$ or $\frac{1}{f^2}$ as he manipulates EM or current traces respectively; this latter multiplication being sufficient to take into account the main lesson of the model according to which most of the leakage is in low frequency. The signal to noise ratio definition used here corresponds to the mean divided by the standard deviation. A definition widely used in image processing.[26] This results in the definition of two criteria, expressed from the usual Signal to Noise Ratio ($SNR(f)$). The first one is for power consumption (eq.4) and the second one is for EM emanations (eq.5). Both are denoted by Leakage to Noise Ratio and allow identifying harmonics where the leakage is a priori the most important.

$$LNR_{POW}(f) = \frac{1}{f^2} \frac{< A_{RawSig}(f) >}{\sigma_{A_{RawSig}}(f)} = \frac{1}{f^2} SNR(f) \tag{6}$$

$$LNR_{EM}(f) = \frac{1}{f} \frac{< A_{RawSig}(f) >}{\sigma_{A_{RawSig}}(f)} = \frac{1}{f} SNR(f) \tag{7}$$

where $A_{RawSig}(f)$ is the power spectral density at f of the mean signal and $\sigma_{RawSig}(f)$ its standard deviation, both computed with at least one hundred traces to be statistically significant. It is to notice that these criteria are not perfect, they just give an order of idea of the frequencies leaking the most.

3 Indirect Validation of the leakage Model

To validate the leakage models in the frequency domain, we studied the frequency distribution of the leakage on several sets of traces and we also investigated the relevance of the LNR criteria. Finally, other implications of the models were verified.

3.1 Traces with a little background noise

These experiments were first conducted on EM traces with a little background noise that were collected above an unprotected AES hardware mapped onto a FPGA platform. Only a RS232 unit and a finite state machine were jointly embedded in the FPGA with the AES to limit the noise. The acquisition chain used to retrieve these 5000 traces of 10000 points consists of an EM probe with a $300\mu m$ diameter, a low noise amplifier with a 40db gain and a Lecroy oscilloscope. The bandwidths of these equipments are respectively: $[30MHz, 3.5GHz]$, $[100MHz, 1GHz]$ and $[0Hz, 3.5GHz]$. During the acquisition, the sampling rate of the oscilloscope was set to 20GS/s and each collected traces was the averaging of 20 trials to reduce the noise. These EM traces collected, CPA and Absolute Sum DPA [8] have been carried out in the time domain without application of any pre-processing to estimate the robustness level of this unprotected design. We then re-applied the same analyses on the same traces but by keeping successively the frequency bands $[0; F_{lim}]$ or $[F_{lim}; F_{sample}/2]$ with F_{lim} a variable of experiment and F_{sample} the sampling frequency used during acquisitions. The evolution of the Success Rate [23] with F_{lim} was then analyzed.

At this point, it should be noticed that no filtering tool has been used. Indeed, instead of filtering these harmonics, they were replaced in each trace by the corresponding harmonics of the mean signal calculated by averaging 150 raw traces. The adopted procedure consists therefore in applying a FT to the whole trace, in replacing undesired harmonics by the corresponding harmonics of the mean signal, and finally in applying the inverse FT to get back in the time domain. It is also possible to replace the undesired harmonics by zeros in the results of the FT, but this does not preserve the original shape of the signal, this explains our choice mainly motivated by the visual comfort! Whatever is the chosen solution, these approaches, compared to the use of filters, allow replacing unwanted varying harmonics by constants that allow ensuring a complete removal of noise on these harmonics and not only its reduction.

Tables 1 gives the number of traces for reaching a Success Rate equal to 20% or 80% with respect to the frequency bands retained during the analyses. The results are consistent with the predictions of the EM leakage model. Indeed, as shown in Table 1, removing low frequencies leads to a rapid increase in the number of curves and eventually a failure to achieve the targeted SR values. In addition, the model also predicts that the suppressing of high frequencies does not significantly modifies the efficiency of CPA and DPA analyses because most of the leakage energy is spread on low frequencies. This is what can be effectively observed in Table 1, removing harmonics between 70MHz and 10GHz (i.e. 4966 harmonics over a set of 5001) does not modify significantly the results provided by CPA and DPA. It should be noted that we conducted the same experiments on traces from the DPA contest v1 and v2 [24] and got similar results.

All above results confirm the main prediction of the leakage model according to which the leakage is spread over all frequencies but with the majority of its energy in a narrow band of low frequencies. In addition, and as expected, removing high frequencies within traces with little noise, can only offer a slight improvement of the attacks. What happens in case of really noisy curves?

Table 1. Number of EM traces processed to reach a Success Rate of 20% or 80% with CPA and DPA with respect to the considered frequency bandwidth

	CPA		AbsSum DPA	
Freq \ SR	20%	80%	20%	80%
0 Hz-10 GHz	530	980	1260	2540
100 MHz -10 GHz	1940	4070	2430	3600
200 MHz -10 GHz	4310	Fail	3610	4560
500 MHz -10 GHz	Fail	Fail	Fail	Fail
1 GHz -10 GHz	Fail	Fail	Fail	Fail
2 GHz -10 GHz	Fail	Fail	Fail	Fail
3 GHz -10 GHz	Fail	Fail	Fail	Fail
4 GHz -10 GHz	Fail	Fail	Fail	Fail
5 GHz -10 GHz	Fail	Fail	Fail	Fail
7 GHz -10 GHz	Fail	Fail	Fail	Fail
8 GHz -10 GHz	Fail	Fail	Fail	Fail

	CPA		AbsSum DPA	
Freq \ SR	20%	80%	20%	80%
0-70MHz	520	820	840	1200
0-100MHz	500	1060	1010	1810
0-200MHz	480	850	1650	2610
0-300MHz	500	860	1310	2450
0-400MHz	520	870	1290	2460
0-500MHz	540	860	1390	2590
0-800MHz	510	910	1320	2610
0-1GHz	510	940	1320	2610
0-2GHz	510	970	1310	2610
0-5GHz	540	970	1320	2630
0-10GHz	530	970	1360	2610

3.2 Noisy traces

EM emissions, of an AES hardware embedded within a cortex M3 processor designed with a 90nm technology, were collected with exactly the same equipment as before without removing the package protecting the circuit. The EM probe was placed on top of the AES to not collect too much EM emanations from other operating block. Despite this precaution and the use of average mode of the oscilloscope (10 trials for one trace), the collected traces remained noisy because of the impulsive noises of other operational blocks (pump charge, counters, ...) embedded in the micro-controller and working simultaneously (and not necessarily synchronously) with the AES. As a result, a CPA applied on a set of 54000 traces (540000 measurements) did not succeed in disclosing the full key.

We therefore applied the $LNR_{EM}(f)$ on this set of traces in order to identify the frequencies likely to carry more leakage than noise but also in order to suppress (with our previously described 'filtering' procedure) harmonics carrying more noise than leakage. To do this, the Fourier transform of the mean signal as well as the standard deviations of each harmonic, were calculated with 150 traces. Fig. 3 gives the evolutions of the $LNR_{EM}(f)$ and of the $SNR(f)$ for a frequency band ranging between 0Hz and 450MHz. The $LNR_{EM}(f)$ criterion clearly points the frequency band $BW1 = [4, 48]MHz$ as the main source of leakage while $SNR(f)$ points the band

$BW3 = [83, 160]MHz$. The $SNR(f)$ is here misled by the algorithmic noise identified as particularly important around the harmonics of the clock signal (in our case the AES operates at 120 MHz) in [18]. Finally, we also observe that $LNR_{EM}(f)$ is almost zero between $160MHz$ and $450MHz$ while the $SNR(f)$ has oscillations reaching the value 0.3 in this frequency range.

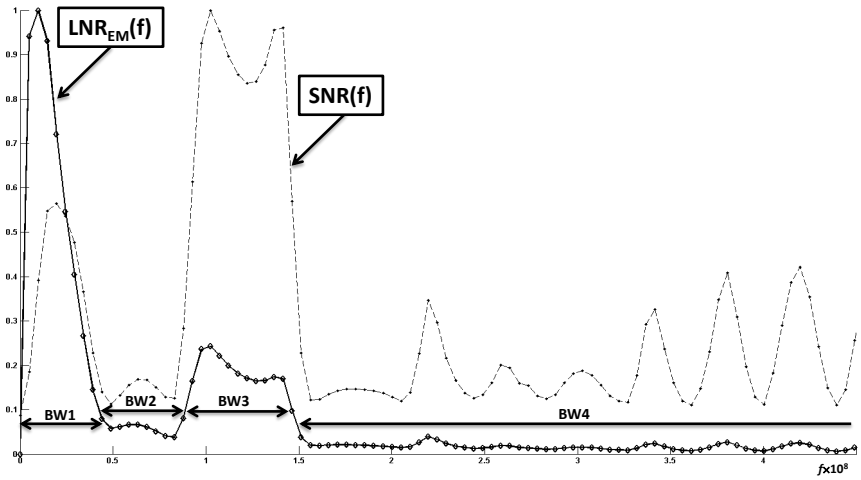

Fig. 3. Normalized evolutions of $LNR_{EM}(f)$ and $SNR(f)$

Table 2 shows that a CPA done while keeping all harmonics or only the harmonics in the frequency range $[1, 200]MHz$ does not succeed in identifying the 16 sub-keys. However, keeping one of the two lobes seen in Fig. 3, allows CPA to recover the 16 sub-keys. Indeed, 28 900 curves are sufficient to find the key with a CPA conducted on $BW1$, while 49 900 (resp. 22 100) are necessary while keeping frequency band $BW3$ (resp. $BW1 \cup BW3$), i.e. by keeping only 78 (resp. 123) harmonics among 10001 in the last case.

All these experimental results clearly demonstrate the effectiveness of the criterion $LNR_{EM}(f)$ and demonstrate indirectly the validity of the leakage model in the frequency domain.

3.3 Current vs EM leakages

The above results were obtained on EM traces. If they, indirectly validate the leakage model in the frequency domain, they do not highlight the difference between the current and EM leakages, and particularly the $\frac{1}{f^2}$ dependency of the current leakage while the EM leakage is related to $\frac{1}{f}$.

In order to highlight this behavioral difference, EM and current traces of an AES mapped into a FPGA were simultaneously collected with the same acquisition chain.

Table 2. Results of CPA attacks on EM traces collected during the course of an AES

f-band	# traces	# subkeys	# harmonics
Full band	Fail	11	10001
1-200 MHz	Fail	12	200
4-160 MHz	27700	16	157
BW1	28900	16	45
BW3	49900	16	78
BW2	Fail	3	36
BW4	Fail	0	9841
BW1 $\cup$ BW3	22100	16	123

Table 3. Results of CPA attacks on 10k current and EM traces collected during the course of an AES

Current / EM	# traces	# subkeys
Full band	2400 / 640	16 / 16
20MHz-10GHz	3910 / 600	16 / 16
50MHz-10GHz	Fail / 1080	13 / 16
70MHz-10GHz	Fail / 2120	10 / 16
100MHz-10GHz	Fail / 4100	7 / 16
130MHz-10GHz	Fail / 5450	5 / 16
160MHz-10GHz	Fail / Fail	7 / 15
200MHz-10GHz	Fail / Fail	3 / 13
400MHz-10GHz	Fail / Fail	1 / 4
800MHz-10GHz	Fail / Fail	0 / 1
1GHz-10GHz	Fail / Fail	0 / 0

The low noise amplifier used to collect EM traces was used to measure the supply voltage variations thanks to a SMA-T connector interconnecting the IC core, the voltage generator and the amplifier input. Then, following the same approach than before, the evolutions of the leakages with f were analysed by evaluating the number of traces that have to be processed by an adversary (using CPA) in order to get the key, results are shown in Table 3. As predicted by the model, the frequency range on which extends the current leakage is narrower than the one of the EM leakage. These bands are respectively for the current and EM leakages: $[0, 40]MHz$ and $[0, 130]MHz$. It should be noted that the frequency range on which extends the current leakage is far below the cut-off frequency of the supply pads. In addition, this comparison confirms that EM traces contain more information than current traces; wealth due to the derivative behavior of EM probes commonly used and of course to the locality of the measure.

3.4 Leakage vs Clock frequency

The models in section 3 indicate that the leakage distribution in the frequency domain does not depend on the clock frequency at which the circuit works but is linked to the maximum frequency at which it can operate. To assess whether this indication of the model is correct, measurements on a AES hardware embedded within a cortex M3 processor were performed for three different operating frequencies: 60, 90 and 120 MHz keeping the EM probe at the same position. Then, using a narrow sliding window of frequencies, we launched many CPA to observe the evolutions of the mean guessing entropies. It was expected to observe the same evolutions for all sets of traces if the clock frequency does not affect the leakage distribution in the frequency domain. This is what can be observed Fig. 4 that has been obtained after the processing of 60000 traces. As predicted by the model, the leakage distribution in the frequency domain does not rely on the operating frequency. However, it depends on the maximum operating frequency F_{CKmax} for which the circuit has been designed (that fixes the propagation delay of critical paths and therefore T), a design objective that can be kept secret !

To conclude, the Leakage model and the reported results herein confirm the experimental observation of [17] under which the leakage is independent of the clock and occupies a really reduced number of frequency harmonics.

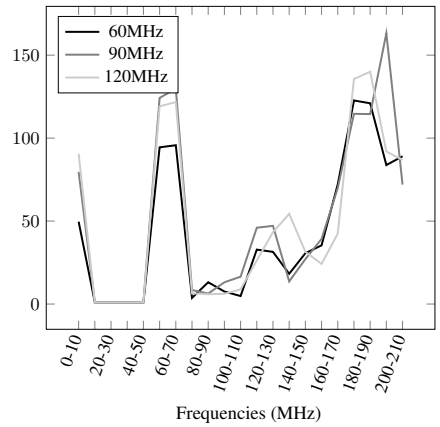

Fig. 4. Evolutions of the Mean Guessing Entropy on the frequency range: $[0; 210MHz]$ after the processing of 60000 traces. The target design has been successively clocked at 60 MHz, 90 MHz and 120 MHz.

4 Conclusion

Starting from a first order modeling of CMOS circuits behavior, we derived leakage models of the current and of EM emanations in the frequency domain. These models highlight the impossibility of predicting the frequency distribution of the leakage without collusion with the designers of targeted circuit. However, these models highlight a specific behavior of the leakage in the frequency domain; behavior that can be exploited to improve the efficiency of DPA and CPA. So, beyond a new way of attacking devices, this model can also be seen as a tool for security teams to assess the resistance of their devices in a worst case situation through of internal evaluations targeting the harmonics leaking the most; the knowledge of all design parameters and thus of these frequencies providing a competitive advantage over an attacker.

To do this, two criteria called leakage to noise ratios (LNR) have been derived from the model, one for power consumption and one for EM emanations. They allow identifying harmonics of the spectrum likely to contain leakage. Compared to the SNR criterion, and with respect of noise, they quantify the importance of the leakage instead of the signal amplitude. With such criteria, one can easily select the frequency to be kept, or rejected, during DPA or CPA analyses using the direct and inverse Fast Fourier Transforms.

Despite the proposal of this efficient pre-processing technique allowing increasing the Leakage to Noise Ratio (and not only the Signal to Noise Ratio) of traces during

SCA; the proposed models encourage to use an amplifier with a low noise figure and with a frequency range from the lowest possible frequency to high frequencies instead of a wide band pass amplifier with a lesser noise figure and a greater low cut-off frequency. Indeed, low frequencies must be favored !

References

1. Nanosim User Guide, tld-2001.06. Document Order Number: 376418-000 JB, 2001.
2. Alessandro Barenghi, Gerardo Pelosi, and Yannick Teglia. Improving first order differential power attacks through digital signal processing. In Oleg B. Makarevich, Atilla Elçi, Mehmet A. Orgun, Sorin A. Huss, Ludmila K. Babenko, Alexander G. Chefranov, and Vijay Varadharajan, editors, *SIN*, pages 124–133. ACM, 2010.
3. Alessandro Barenghi, Gerardo Pelosi, and Yannick Teglia. Information Leakage Discovery Techniques to Enhance Secure Chip Design. In Claudio Agostino Ardagna and Jianying Zhou, editors, *WISTP*, volume 6633 of *Lecture Notes in Computer Science*, pages 128–143. Springer, 2011.
4. E. Bohl, J. Hayek, O. Schimmel, P. Duplys, and W. Rosenstiel. Correlation power analysis in frequency domain. In *COSADE, Darmstadt, Germany*, pages 1–3, 2010.
5. Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In Marc Joye and Jean-Jacques Quisquater, editors, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.
6. Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template Attacks. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *CHES*, volume 2523 of *Lecture Notes in Computer Science*, pages 13–28. Springer, 2002.
7. Amine Dehbaoui, Sebastien Tiran, Philippe Maurine, FranÃğois-Xavier Standaert, and Nicolas Veyrat-Charvillon. Spectral Coherence Analysis - First Experimental Results -. Cryptology ePrint Archive, Report 2011/056, 2011. `http://eprint.iacr.org/`.
8. Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate side channel attacks and leakage modeling. *J. Cryptographic Engineering*, 1(2):123–144, 2011.
9. Catherine H. Gebotys, Simon Ho, and C. C. Tiu. EM Analysis of Rijndael and ECC on a Wireless Java-Based pda. In Josyula R. Rao and Berk Sunar, editors, *CHES*, volume 3659 of *Lecture Notes in Computer Science*, pages 250–264. Springer, 2005.
10. Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual Information Analysis. In Elisabeth Oswald and Pankaj Rohatgi, editors, *CHES*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, 2008.
11. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.
12. Thanh-Ha Le and Maël Berthier. Mutual Information Analysis under the View of Higher-Order Statistics. In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC*, volume 6434 of *Lecture Notes in Computer Science*, pages 285–300. Springer, 2010.
13. Thanh-Ha Le, Jessy Clédière, Christine Servière, and Jean-Louis Lacoume. Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant. *IEEE Transactions on Information Forensics and Security*, 2(4):710–720, 2007.
14. Hongying Liu, Xin Jin, Yukiyasu Tsunoo, and Satoshi Goto. Correlated Noise Reduction for Electromagnetic Analysis. *IEICE Transactions*, 96-A(1):185–195, 2013.
15. Stefan Mangard, editor. *Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers*, volume 7771 of *Lecture Notes in Computer Science*. Springer, 2013.

16. Stefan Mangard, Elisabeth Oswald, and François-Xavier Standaert. One for all - all for one: unifying standard differential power analysis attacks. *IET Information Security*, 5(2):100–110, 2011.
17. Edgar Mateos and Catherine H. Gebotys. A new correlation frequency analysis of the side channel. In *WESS*, page 4. ACM, 2010.
18. Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Examining Smart-Card Security under the Threat of Power Analysis Attacks. *IEEE Trans. Computers*, 51(5):541–552, 2002.
19. Olivier Meynard, Denis Real, Florent Flament, Sylvain Guilley, Naofumi Homma, and Jean-Luc Danger. Quantifying the Quality of Side-Channel Acquisitions. In *COSADE*, pages 16–28, 2011.
20. Olivier Meynard, Denis Real, Sylvain Guilley, Florent Flament, Jean-Luc Danger, and Frédéric Valette. Characterization of the Electromagnetic Side Channel in Frequency Domain. In Xuejia Lai, Moti Yung, and Dongdai Lin, editors, *Inscrypt*, volume 6584 of *Lecture Notes in Computer Science*, pages 471–486. Springer, 2010.
21. David Oswald and Christof Paar. Improving Side-Channel Analysis with Optimal Linear Transforms. In Mangard [15], pages 219–233.
22. Davide Pandini, Guido A. Repetto, and Vincenzo Sinisi. Clock Distribution Techniques for Low-EMI Design. In Nadine Azémard and Lars J. Svensson, editors, *PATMOS*, volume 4644 of *Lecture Notes in Computer Science*, pages 201–210. Springer, 2007.
23. François-Xavier Standaert, Tal Malkin, and Moti Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In Antoine Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, 2009.
24. TELECOM'PARIS. Dpa Contest, 2008-2013. .http://www.dpacontest.org/home/.
25. Sébastien Tiran and Philippe Maurine. SCA with Magnitude Squared Coherence. In Mangard [15], pages 234–247.
26. F. van der Meer and S.M. de Jong. *Imaging Spectrometry: Basic Principles and Prospective Applications*. Remote sensing and digital image processing. Kluwer Academic Publishers, 2006.
27. Alexandre Venelli. Efficient Entropy Estimation for Mutual Information Analysis Using B-Splines. In Pierangela Samarati, Michael Tunstall, Joachim Posegga, Konstantinos Markantonakis, and Damien Sauveron, editors, *WISTP*, volume 6033 of *Lecture Notes in Computer Science*, pages 17–30. Springer, 2010.

A Fourier Transform

For a square signal with an amplitude A such as :

$$rect_T(t) = \begin{cases} A\ if\ t \in [-T/2, T/2] \\ else\ 0 \end{cases} \tag{8}$$

its Fourier transform is equal to

$$FT\left\{rect_T(t)\right\}(f) = AT\mathrm{sinc}(fT) = AT\frac{\sin(\pi fT)}{\pi fT} \tag{9}$$

Moreover, the Fourier transform of a delay t_0 is

$$\begin{array}{l} FT\left\{x(t)\right\}(f) = X(f) \\ FT\left\{x(t-t_0)\right\}(f) = X(f)e^{-j2\pi ft_0} \end{array} \tag{10}$$

$X(f)$ being the Fourier transform of $x(t)$. From Figure 2.c we can see that the EM signal is equal to the sum of two squares, one of amplitude $\frac{A}{\alpha T}$ with a delay $\frac{\alpha T}{2}$ and a period αT and one of amplitude $\frac{-A}{(1-\alpha)T}$ with a delay $\alpha T + \frac{(1-\alpha)T}{2}$ and a period $(1-\alpha)T$. Thus, from Equations 9 and 10 we can deduce that the Fourier transform of the EM model is equal to Equation 3 :

$$EM(f) = \frac{A}{\pi f T}\{\ \frac{1}{\alpha}\sin(\alpha\pi f T)\ e^{-j\pi f \alpha T} - \ \frac{1}{1-\alpha}\sin\big((1-\alpha)\pi f T\big)\ e^{-j\pi f\left((\alpha+1)T\right)}\}$$

For a function g and its derivative $\frac{d}{dt}g$ we have

$$TF\left\{g\right\}(f) = \frac{TF\left\{\frac{d}{dt}g\right\}(f)}{j2\pi f} \tag{11}$$

Knowing that the EM signal is the derivative of the current signal we can deduce Equation 2 :

$$POW(f) = \frac{-jA}{2\pi^2 f^2 T}\ \{\frac{1}{\alpha}\sin(\alpha\pi f T)\ e^{-j\pi f \alpha T} - \frac{1}{1-\alpha}\sin\big((1-\alpha)\pi f T\big)\ e^{-j\pi f\left((\alpha+1)T\right)}\}$$