Modeling Time Domain Magnetic Emissions of ICs

Philippe Maurine, Victor Lomné, Lionel Torres, Thomas Ordas, Mathieu Lisart, Jérome Toublanc

Modeling Time Domain Magnetic Emissions of ICs

Victor Lomné[1], Philippe Maurine[1], Lionel Torres[1], Thomas Ordas[1,2], Mathieu Lisart[2], and Jérome Toublanc[3]

[1] LIRMM, UMR 5506
university of Montpellier 2 / CNRS
161, rue Ada
34095 Montpellier, France
{firstname.lastname}@lirmm.fr
[2] STMicroelectronics
190 Avenue Celestin Coq
13106 Rousset, France
{firstname.lastname}@st.com
[3] Apache Design Solutions
300 route des Cretes
06902 Sophia-Antipolis, France
{firstname}@apache-da.com

Abstract. ElectroMagnetic (EM) radiations of Integrated Circuits (IC) is for many years a main problem from an ElectroMagnetic Compatibility (EMC) point-of-view. But with the increasing use of secure embedded systems, and the apparition of new attacks based on the exploitation of physical leakages of such secure ICs, it is now also a critical problem for secure IC designers. Indeed, EM radiations of an IC, and more precisely the magnetic component, can be exploited to retrieve sensible data such as, the secret key of cryptographic algorithms. Within this context, this paper aims at introducing a magnetic field simulation flow allowing predicting, with high spatial and time resolutions, the magnetic radiations of IC cores. Such a flow being mandatory to predict the robustness of secure ICs before fabrication against EM attacks.

1 Introduction

With the ever increasing speed and power consumption of ICs, EM interferences of chips are becoming a more and more challenging issue from an EMC point of view.

To prevent from these problems, designers need to simulate these EM radiations during the IC design flow. Different simulation methods and tools have been developed to ensure that EM radiations emitted by the different parts of an electronic system do not interfere with the others.

Most of these tools model the circuit, and more precisely its pads, its internal Power/Ground network and its digital macro-blocks using passive RLC elements and current sources.

R. van Leuken and G. Sicard (Eds.): PATMOS 2010, LNCS 6448, pp. 238–249, 2011.

If these models (IBIS [1], ICEM [2] or IMIC [3]) and the related tools have been demonstrated efficient to predict the EM radiations of a circuit in its whole (leads, bonding, package and IC core), they are too coarse grain to address problems which are specific to the design of secure circuits.

Other tools, like CST studio [4], allow to compute a complete 3D EM simulation of any electronic device with very high spatial and time resolutions. But this kind of tools need to solve Maxwell equations at lot of positions in the device, and the CPU time necessary to model complex ICs made of several hundred thousand gates, is not reasonnable for a designer.

From a hardware security point-of-view, with the ever increasing use of embedded systems to manage sensible data, a new kind of threats appeared at the end of the 20th century. They are called Side-Channel Attacks (SCA), and exploit physical leakages like power consumption or EM radiations emanated by the IC while it computes a cryptographic operation.

Among these threats, the major ones are the Simple ElectroMagnetic Analysis (SEMA) and the Differential ElectroMagnetic Analysis (DEMA) [5].

The SEMA consists in analysing a single EM trace of a cryptographic operation, measured with the Surface Scan method [6] using a small magnetic probe made of a coiled wire with diameter varying between 50μm and 500μm. The measured trace is the evolution of the magnetic field radiated by the IC versus time.

When applying a SEMA at different positions above the IC, it is thus possible to compute static and dynamic (time domain) EM cartographies [7]. Furthemore, advanced techniques based on signal processing have been proposed to localize the crypto module [8] [9] [10].

The DEMA exploits several EM traces corresponding to several cryptographic operations using the same key. It consists in a statistical processing of these traces in order to guess the key. More precisely, it exploits variation in amplitude of EM traces, which are correlated to the processed data.

Note that, although these methods are called *ElectroMagnetic Analyses*, it is usually the magnetic field which is measured with the Surface Scan method [6] and a magnetic probe.

Considering this threats, the basic design guidelines to increase the robustness of an IC:

- to reduce as far as possible the EM radiations of the cryptographic modules, or
- to hide them within the EM radiations of other blocks, or finally
- to design the circuit such as to obtain inintelligible EM radiations.

However, adopting these basic guidelines requires the development of a flow allowing to predict at the design step, with high time and spatial resolutions, the magnetic field generated by a circuit in the close vicinity of its surface.

Within this context, the main contribution of this paper is the proposal of an industrial flow allowing predicting the time domain evolution of magnetic radiations with high accuracy and with high spatial and time resolutions.

The rest of this paper is organized as follows. Section 2 provides an overview of the simulation flow and then details its main features. Section 3 gives an experimental validation of our flow applied on two complex ICs. Finally, conclusion is drawn section 4.

2 Magnetic Field Simulation Flow

Due to the ever increasing demand of performance, industrial integrated products have moved from simple IC to complex integrated system, known as System-on-Chip (SoC) which consumes a significant amount of power.

To distribute efficiently this power to the basic elements of SoC, more or less complex Power/Ground (P/G) networks are designed according to specific design guidelines addressing different signal integrity problems such as IR drops.

As a result, the current consumed by a circuit typically flows from the top metal layers, characterized by a lower resistivity, down to logic gates regularly and hierarchically in order to minimize static and dynamic IR drops.

2.1 Basic Concept

Consequently, P/G networks of complex SoC, especially the part routed on top level metal wires, constitute the main sources of magnetic emissions, as it has been experimentally observed in [7], since high amplitude currents (several mA) flow within. On the contrary, interconnect wires, which are much more resistive and controlled by simple logic gates, are weaker sources of magnetic emissions.

From these considerations, supported by experimental results, it appears that modeling the magnetic radiations of complex SoC results mainly in modeling the magnetic radiations of its P/G network.

Our magnetic field simulation flow aiming at being as general as possible, the backbone of our modeling approach, which is represented in figure 1, follows these steps:

- cut the P/G network in small pieces of metal, considered as small electrical dipoles, and simulate the current within each of these pieces of wire
- compute the magnetic field generated by each dipole, at several positions on a plane parallel to the IC surface (like a grid), according to Biot-Savart law
- obtain the magnetic emissions of the IC at each coordinates of this plane by summing all the contributions of all these dipoles
- compute what can be seen by measurement, i.e. to take into account the main characteristics of the measurement setup assumed to be used.

If this approach is simple, it requires computing the time domain evolution of the current flowing in each dipole with a high time resolution.

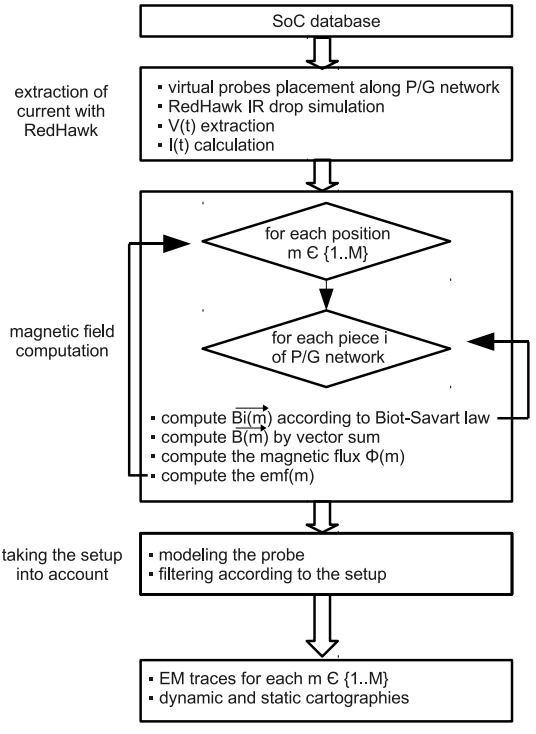

Fig. 1. Overview of the proposed magnetic field simulation flow

2.2 Current Extraction Step

If it is quite standard to compute the current consumed by a small digital block, using for example a SPICE-like tool, it is much more difficult to compute the current flowing along the entire P/G network of a complex SoC made of many digital and analogue blocks and memories.

Thus, to get this current, we use an efficient IR drop tool allowing computing, with a high time resolution, the voltage evolution along the entire P/G network, called RedHawk (from Apache tools suite) [11]. RedHawk allows designers verifying that their P/G network does not suffer any significant static or dynamic voltage drops before launching the production.

Another key advantage of this tool is its ability in simulating, with a reduced cpu time and a high accuracy (see section 3), SoC integrating many different elements such as digital blocks, co-processors, memories and analogue blocks. More precisely, another tool from Apache tools suite, called Totem [11], allows to characterize the current evolution of analogue blocks and memories, for a usage within RedHawk.

This characterization step achieved, the simulation can be launched, according to a scenario, specifying to the tool kernel, which block is involved. This simulation provides different results such as static and dynamic maps disclosing the IR drops along the P/G network. A map, allowing identifying the areas that have suffered from the most important IR drops during a scenario, is given figure 2. In that case, it corresponds to a memory decoder power rail (red part on the figure 2).

Among all its features, RedHawk offers a key advantage for the modeling of magnetic emissions. Indeed, it allows extracting, by positioning virtual probes (a specific instance of this tool), the time domain evolution of the voltage anywhere along the P/G network, i.e. the ability of computing the evolution of the current flowing in any piece of the P/G network considered as an electrical dipole in our magnetic field simulation flow.

More precisely, for the magnetic field simulation of a given IC, the first step (figure 1) is to place virtual probes regularly (every X μm) along the power and ground rails. The placement policy was to place a virtual probe:

- every X μm along unidirectional wire
- at each intersection of vertical or horizontal wires
- at each intersection of a wire and a *via* in order to warrant that two successive virtual probes are connected by a single and unidirectional wire.

This point is important since it allows computing easily the current flowing between two probes, knowing the resistivity of the considered metal layer and the voltage at both wire ends.

The computation of the currents flowing in all the dipoles achieved, the results are stored in a file gathering, for each dipole, the sampled current waveform (the sampling rate fixes the time domain resolution and the simulation speed) but also the coordinates of the dipole.

2.3 Magnetic Field Calculation Step

The second step of our flow is based on the classical rules of the EM wave theory [12]. As aforementioned, each piece of the P/G network in which a current flows, radiates an EM field according to Maxwell equations.

In our case, considering the distance between the magnetic sensor, the IC surface and the typical frequency bandwidth scanned by a magnetic measurement setup operating in time domain (from $1MHz$ to $1GHz$), we may adopt the quasi-stationary regime approximation. This fact allows using the Biot-Savart law (1) for faster calculations rather than more complex expressions deduced from Maxwell equations.

To get an idea of what can be seen on the scope at a point m of a plane parallel to the IC surface, we first compute the magnetic field at this point.

More precisely, knowing the current $I_{AB}(t)$ that flows in each piece of P/G network represented by a finite wire of length AB, its contribution $B_i(t)$ to the magnetic field $B(t)$ at the position m is first evaluated according to the expression of the Biot-Savart law (1), where μ is the permeability of the considered

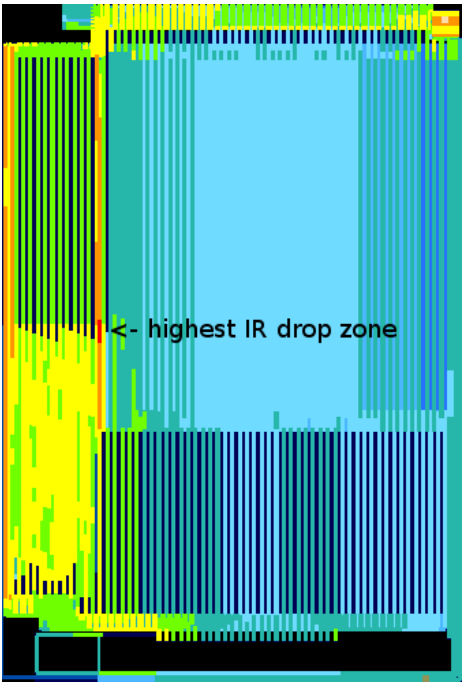

Fig. 2. A static IR drop map obtained with RedHawk

space, and r the distance between the wire AB and the point m. Then, the final value $B(t)$ of the magnetic field at the position m is computed by vectorial sum of magnetic fields radiated by the N pieces of P/G network (2).

$$\overrightarrow{B_i(t)} = \frac{\mu . I_{AB}(t)}{4\pi} \frac{\overrightarrow{AB} \times \overrightarrow{r}}{r^3} \tag{1}$$

$$\overrightarrow{B(t)} = \sum_{i=1}^{N} \overrightarrow{B_i(t)} \tag{2}$$

Thus, we compute the magnetic flux $\phi_B(t)$ flowing through the coiled magnetic sensor, according its diameter giving a surface S (3). This is done, assuming that the surface S is parallel to the IC surface. This assumption is important since it allows computing the magnetic flux by computing the magnetic field at several points inside the surface S and by summing them.

$$\phi_B(t) = \int_S \overrightarrow{B(t)} . \overrightarrow{dS} \tag{3}$$

Finally, we compute the electromotive force $emf(t)$, measured at the pins of the coiled sensor, by a differentiation of the magnetic flux by the time (4).

$$emf(t) = -\frac{d\phi_B(t)}{dt} \tag{4}$$

2.4 Additional Mandatory Steps

If the calculation of the magnetic field at all points of a plane, parallel to the IC surface, is quite standard, it is not sufficient to get an accurate idea of what can be seen by measurement.

Indeed, to obtain, by simulation, a more accurate representation of results provided by a near-field scan of the IC, by simulation, the characteristics of the setup assumed to be used by for measurements have to be considered.

In our simulation flow, three main characteristics of the setup are considered. The probe size assumed to be a small loop, and the overall bandwidth of the acquisition chain. More precisely, to increase the accuracy of the results obtained:

- we take into account the change in direction of a wave due to the refraction involved by the passivation layer. Thus, at a given position m of the sensor, the magnetic field radiated by a piece of the P/G network far from the sensor is not taken into account in the resulting magnetic field measured by the sensor. This characteristic is only estimated, because it is hard to estimate the distance between the passivation layer and the magnetic sensor with a precision $< 5\mu$m.
- we filter (band pass filter) the time domain evolution of the computed emf according to the acquisition chain bandwidth. More precisely, knowing the frequency bandwidth of the sensor, the low-noise amplifier and the oscilloscope, we can estimate the frequency bandwidth of the acquisition chain.
- we take into account the gain (in decibels) of the low-noise amplifier.

3 Validation

To validate the proposed magnetic field simulation flow, static and dynamic cartographies of the magnetic field generated by two circuits have been obtained using:

- a near-field scan setup operating in time domain, composed of a motorized X-Y stage with a minimal displacement step of 1μm, a magnetic sensor made of a coiled metal wire with diameter of 50μm, a low-noise amplifier with a gain of $63dB$, an oscilloscope and a computer controlling the whole setup (figure 3).
- our magnetic field simulation flow, using characteristics of the near-field scan setup, as described in section 2.

The two considered ICs are microcontrollers designed in 130nm CMOS technology. They integrate different macro-bocks such as ROM, RAM, EEPROM, CPU and small analogue blocks.

One processing scenario, previously stored in the RAM memory, is executed on each circuit. It consists in reading data in RAM and passing them to the CPU.

During the execution of this scenario (several clock cycles), we measured the magnetic field radiated by the chips, using a 50μm sensor and a 25μm displacement

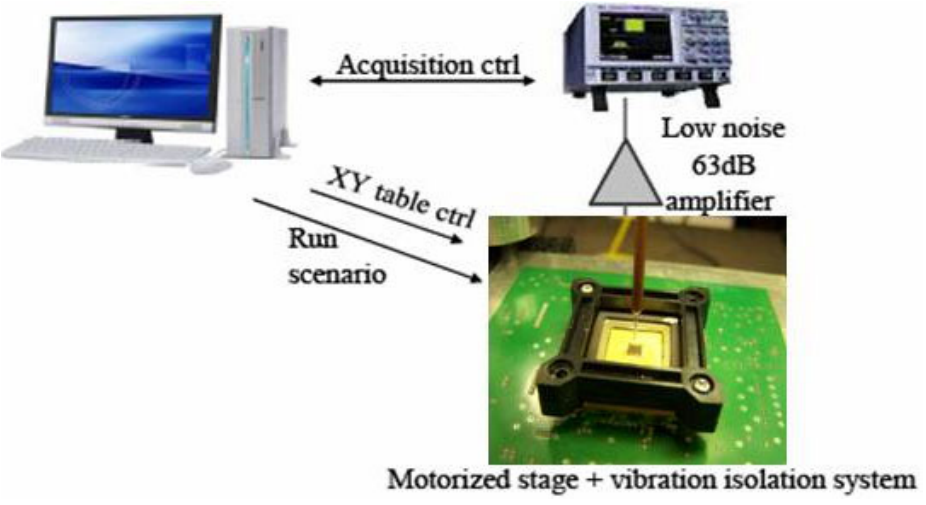

Fig. 3. Near-field scan setup used for experimental validation

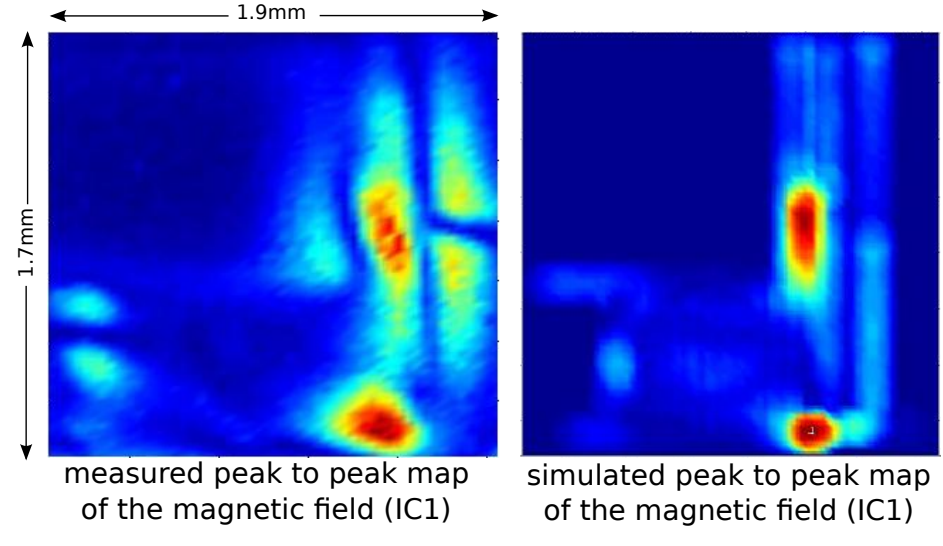

Fig. 4. Measured and simulated maps disclosing the peak to peak amplitude of the magnetic field in the close vicinity of IC1 surface

step. The scenario was repeated 100 times for each position of the scanned surface in order to increase the signal to noise ratio.

Figures 4 and 5 show the cartographies (revealing the peak to peak amplitude of the magnetic field) obtained respectively using the aforementioned near-field scan setup and the proposed magnetic field simulation flow.

Note that data acquisition with the near-field scan setup takes 3 hours while simulation runs in 5 hours. Note also that these simulations have been launched to obtain an emf value every 25μm. During these simulations the probe diameter and the frequency bandwidth were fixed respectively to 50μm and 1GHz accordingly to characteristics of our near-field scan setup. The simulation time step was chosen accordingly to the sampling rate of our scope. The distance separating the sensor from the IC surface was estimated to be roughly 30μm, using a small micro camera with a zoom x100.

As shown, considering the IC1, the agreement between simulations and measures is satisfactory even if some discrepancies still exist. These discrepancies

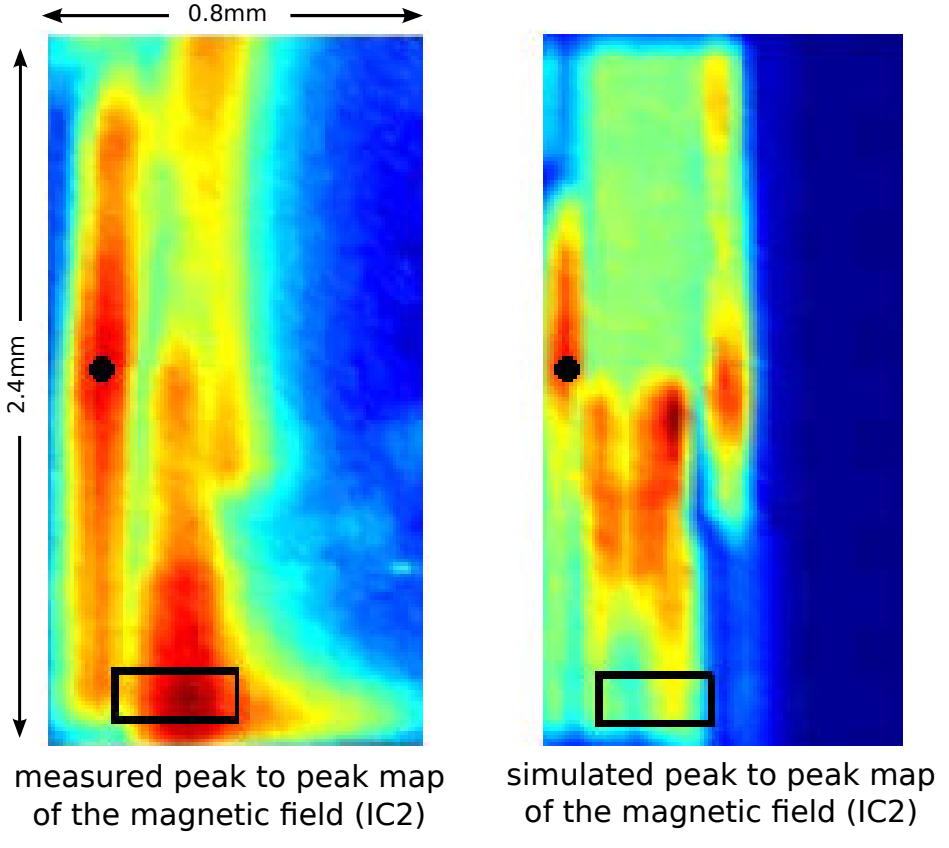

Fig. 5. Measured and simulated maps disclosing the peak to peak amplitude of the magnetic field in the close vicinity of IC2 surface

may be due to several factors. Among them, some may be due to the modeling of the sensor. Indeed it is assumed that:

- the sensor is perfectly horizontal
- the sensor has a perfect circular shape
- the distance between the sensor and the IC is perfectly known

This latter point is critical. It is extremely difficult in practice, even with a micro camera, to measure the distance separating the sensor from the IC with a high accuracy ($< 5\mu$m) due the package shape.

Note also that a fabricated chip does not necessarily have typical characteristics due to process variations.

Concerning IC2, one observe a significant difference (around the rectangles on figure 5) between the measured and the calculated maps. However, this difference was expected since the marked positions are above the clock generator, that was not considered during the simulation (our database related to this design being incomplete).

If these maps demonstrate the interest of the proposed magnetic field simulation flow to compare the efficiency of different P/G network routing strategies in terms of emissions before fabrication, they do not provide any information related to the accuracy of the simulator with respect to time.

To fill this lack, figure 6 gives the measured and simulated time domain evolutions of the magnetic field at a position marked by dots in figure 5. As shown, the wavefroms are quite similar (without application of any filtering solution to model the bandwidth of the near-field scan setup) demonstrating the interest of the magnetic simulation tool.

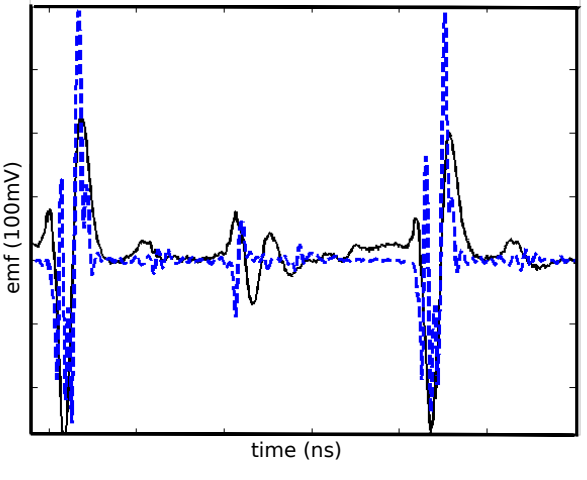

Fig. 6. Measured (continous line) and simulated (dashed line) time domain waveforms of the electromotive force above a supply rail of the IC2 RAM

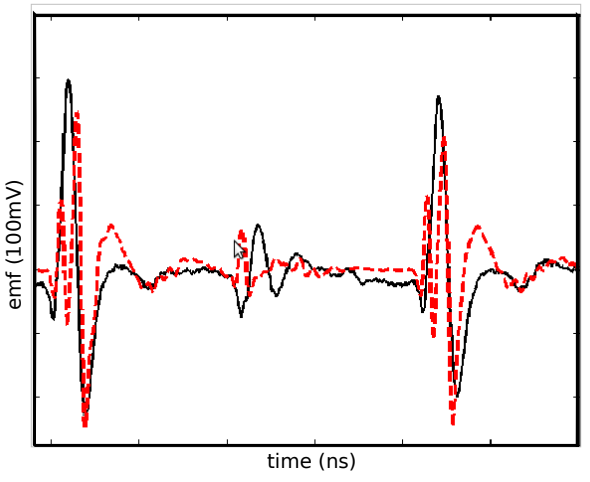

Fig. 7. Measured (continous line) and simulated (dashed line) time domain waveforms (with filtering) of the electromotive force above a supply rail of the IC2 RAM

The figure 7 shows the same results than those represented figure 6, except that the simulated average emf trace has been filtered accordingly to the frequency bandwidth of the acquisition chain. The comparison of Fig. 6 and 7 demonstrates the interest of the considering the acquisition chain impact.

4 Conclusion

In this paper, we have introduced an industrial flow allowing simulating the time domain evolutions of the magnetic emissions of an IC in the close vicinity of its surface. The main ideas on which is based this flow are:

- the use of a dynamic IR drop simulator, RedHawk, that quickly provides the current flowing in all parts of the Power/Ground network
- the use of Biot-Savarts law for fast calculations
- the modeling of the magnetic sensor and, the consideration of the near-field scan setup bandwidth

This flow has been validated by comparing the predicted emissions of two ICs designed in a 130 nm technology with measured emissions. This comparison has demonstrated the efficiency of the proposed flow even if there is room for further improvements.

References

1. Technical Specification IEC 62014-1 (2001)
2. Technical Specification IEC 62014-3 (2002)
3. Technical Specification IEC 62404 (2007)

4. CST Studio suite, http://www.cst.com
5. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis, Concrete Results. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001)
6. Technical Specification IEC 61967-3
7. Ordas, T., Lisart, M., Sicard, E., Maurine, P., Torres, L.: Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits. In: Svensson, L., Monteiro, J. (eds.) PATMOS 2008. LNCS, vol. 5349, pp. 229–236. Springer, Heidelberg (2009)
8. Sauvage, L., Guilley, S., Mathieu, Y.: Electromagnetic Radiations of FPGAs, High Spatial Resolution Cartography and Attack on a Cryptographic Module. ACM Transactions on Reconfigurable Technology and Systems (TRETS) 2(1) (2009)
9. Real, D., Valette, F., Drissi, M.: Enhancing correlation electromagnetic attack using planar near-field cartography. In: International Conference on Design, Automation and Test in Europe (DATE), pp. 628–633 (2009)
10. Dehbaoui, A., Lomne, V., Maurine, P., Torres, L., Robert, M.: Enhancing Electromagnetic Attacks using Spectral Coherence based Cartography. In: International Conference on Very Large Scale Integration, VLSI-SoC (2009)
11. Apache Design Solutions, http://www.apache-da.com
12. Ben Dhia, S., Randani, M., Sicard, E.: Electromagnetic Compatibilty of Integrated Circuits: Techniques for Low Emissions and Susceptibility. Springer Science, Heidelberg (2006)