Magnetic Microprobe Design for EM Fault Attack

R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau
Institut d'Electronique du Sud
IES
Montpellier, France
omarouayache@ies.univ-montp2.fr

P. Maurine
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier
LIRMM
Montpellier, France
Philippe.Maurine@lirmm.fr

***Abstract*— Fault attacks constitute a threat against secure integrated circuits. If they can be conducted by different means, a large attention has recently been paid to the EM side-channel. EM fault attacks are performed through near-field probes. To be efficient, these probes must deliver an intense and localized field. Using 3-D electromagnetic simulations, this paper proposes guidelines for the design of an efficient magnetic probe excited by a pulse signal.**

Keywords—EM fault attack, Magnetic probe, Probe design guidelines, Radiated field simulations

I. INTRODUCTION

Nowadays, the laser is the most effective tool for injecting faults into secure micro-controllers for cryptanalysis purposes. Among the reasons for this success, we can of course mention its main advantages considering both high spatial and temporal resolutions.

However, these benefits are available at the cost of significant investments in time and money. Indeed, the cost of a laser attack platform varies from two to four hundred thousand euros depending on the quality of the laser. Given these costs, and the associated know-how, the number of people likely to conduct laser based attacks is reduced. In addition to these financial aspects that could encourage the development of new fault injection techniques with a moderated cost, the integration by smartcard manufacturers of more and more effective countermeasures [1] has recently led the community to consider alternative techniques for fault injection.

Among these alternative techniques, one may identify electromagnetic (EM) fault injection techniques that allow disrupting the behavior of circuits by the front-side without requiring any preparation stage of the circuit. For example, it was recently demonstrated in [2] that harmonic EM waves can be used to bias the output a True Random Number Generator. More recently, it has been shown in [3] that errors generated by EM pulses can be exploited to carry out the Piret-Quisquater attack [4]. Fault injection using EM means is more and more an active research field and the effectiveness as well as the limitations of these techniques are poorly identified to date.

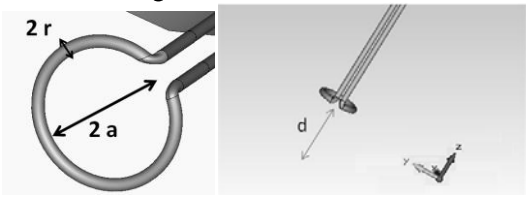
Among the remaining questions related to EM fault injection, one may identify the lack of information about the design of probes delivering an intense and local magnetic pulse. Within this context, the paper investigates the effects of different probe design options on the magnetic pulse characteristics and spatial resolution achievable from such coils. With very simple designs, this is done using analytic rules whereas numerical computations using CST [5] are involved for the analysis of more complex designs.

II. PROBE DESIGN OPTIONS

Pulse excitation signals have recently been demonstrated as being efficient for disrupting the operation of a digital circuit [3]. Moreover integrated circuits are subject to currents induced by magnetic interference attacks. It is for these reasons that we focus on the study of magnetic probes. The coil probes were shown to transfer EM interferences to circuits over a broad frequency band. In practice, the EM signal pulse is injected from a very localised point in the close vicinity of the circuit front side.

To produce a transient fault into a circuit using an EM pulse, one can divert commercial probes [6], initially designed for EM analysis, that can achieve resolution below 1 mm for the smallest ones. There is however no information in datasheets on how optimal would be the energy transfer between the magnetic field and the circuit to attack. In particular, it is well known that current loops are the most interesting targets to look at, so a probe generating a vertical magnetic field must be preferred. The starting point for designing a probe dedicated to injection should thus be close to that of the Langer RF-B above models, but many questions remain considering the coil diameter, wire radius, number of loops in the coil, ratio between the open area to the overall probe dimension including wires, influence of the coil feed wires, and eventually influence of an additional ferrite to concentrate the magnetic field.

This paper provides some answers to these questions owing to electromagnetic simulations conducted with the commercial 3-D electromagnetic simulator CST Microwave Studio [5].



(a) (b)

Fig. 1. Basic probe geometry. (a) close view, (b) general view.

The basic element of the probe considered consists in a copper wire forming a loop as depicted in Fig. 1a. It is electrically excited through a SMA connector placed at the end of the feed wires making a *90°* turn with the loop plan. In the following the radius of the loop will be noted *a* and the wire radius *r*. Calculation results are always recorded at a fixed distance, *d,* from the loop plan.

III. THEORETICAL FIELD CALCULATION OF AN IDEAL CURRENT LOOP

In order to validate the correctness of our simulation procedure, it is important to evaluate theoretically the field radiated by a simple current loop. This was done by considering an infinitely thin wire loop fed by a DC current for which the Biot and Savart's law applies. Although in practice we are mainly interested in pulsed operation with this probe, the DC current excitation is however completely representative of what happens during the plateau of the pulsed excitation. Then the magnetic induction element $d\vec{B}$ at a distance *d* from the center of the loop is known to be

$$d\vec{B} = \frac{\mu_0}{4\pi} \frac{I\,\vec{dl} \wedge d'\vec{u}}{|d'\vec{u}|^3} \qquad (1)$$

where $\vec{dl}$ accounts for a small length of wire and observed in the direction of the vector $d'\vec{u}$ and *I* is the current injected into the loop. Integration of (1) is easy along the Oz axis. This axis flows through the middle of the loop in a perpendicular direction to the loop plane. It yields the z component of the magnetic induction at a given height *z*:

$$B_z = \frac{\mu_0}{4\pi} \frac{2\pi a^2 I}{(a^2 + z^2)^{3/2}} \qquad (2)$$

This result shows that the field intensity decreases very quickly according to a $1/z^3$ law when departing from the loop plan. Strong interaction with circuits is thus only expected in the near-field in order to perform attacks with the highest possible magnetic field.

To evaluate the spatial distribution of B_z as a function of distance *d*, (1) is solved numerically for a loop radius of *100* µm. Results are given in Fig. 2 and 3 for the two distances $d = a$ and $d = a/10$.

At the distance $d = a$, B_z exhibits a regular bell-shaped curve with a maximum just at the centre of the loop. At that point, the field intensity is $3.5\ 10^{-4}$ T/A. At the smallest distance, $d = a/10$, the maximum intensity of B_z is located along the perimeter defined by the current loop and its value is significantly bigger: $2.2\ 10^{-3}$ T/A. In contrast to what was observed for $d = a$, B_z presents a local minimum just at the center of the loop, an intrinsic quality of the near-field that was not a priori expected.

Similar theoretical calculations were conducted for the two other components, B_x and B_y, of the magnetic field. The B_x component is depicted Fig. 4 for the two heights considered whereas the B_y component is omitted because it can be deduced owing to the cylindrical symmetry of the loop.

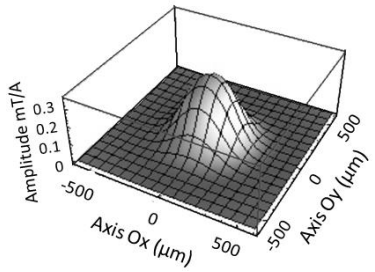


Fig. 2. B_z spatial distribution calculated at the height $d = a = 200$ µm.

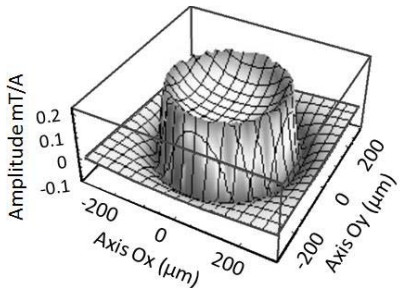


Fig. 3. B_z spatial distribution calculated at the height $d = a/10 = 20$ µm.

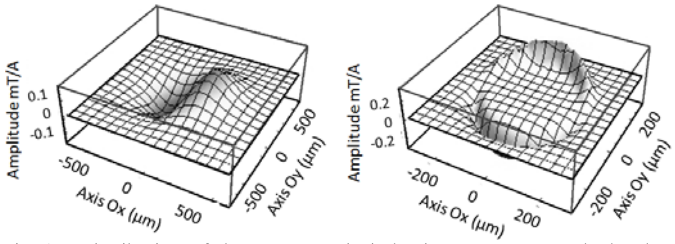


Fig. 4. Distribution of the B_x magnetic induction component calculated at heights (a) $d = a = 200$ µm (b) $d = a/10 = 20$ µm.

As shown in Fig. 4, the B_x component is radial from the center of this loop. Moreover this field is always maximum just above the wire with a location that becomes more and more precise when the observation distance is shortened. But the amplitude of this radial component is found to be of the same order of magnitude ($\approx$ *2* to $3\ 10^{-4}$ T/A) whatever the height considered, a behavior contrary to that of B_z that what strongly enhanced at shorter distances as discussed previously. At the shortest distance B_z is thus expected an order of magnitude more intense than the radial component. As a consequence attacks are expected more efficient using loops at short distance involving the B_z component, which corresponds to a configuration where supply tracks of the circuit form loops that are thus the main target of EM aggression. All the above explains why all the rest of the paper focuses on the B_z component while simulating more realistic probes, and why, at very close distances from the loop, we were expecting a gradual decrease in the magnitude of the B_z component at the center of the loop together with an increase on its inner edges. Starting from this ideal current loop picture, we will now study the radiation versus different geometrical and excitation parameters using CST simulations.

IV. SIMULATION OF THE MAGNETIC BEHAVIOUR OF A PULSE-EXCITED SINGLE LOOP

A. *Influence of the probe-circuit distance*

From now on, amplitude for the magnetic field $\vec{H}$ will be simulated. Because $\vec{H} = \vec{B}/\mu$ results of section III remain valid. CST Microwave Studio (CST MWS) [3] is a specialized tool for simulating three-dimensional (3D) electromagnetic field (EM) components at high frequencies. The software inputs are the three dimensions of the object: its length, height and depth (x, y, z are the three axes which form the orthonormal basis of the space geometry). The principle of 3D simulation is to use these 3 coordinates for visualization of the EM fields radiated by the object under study.

In this paper, the transient solver with the finite difference in time domain (FDTD) method is used [7]. This method solves Maxwell's equations directly in the time and space domain. Thus, we can get a quick idea of the electromagnetic behavior of our designs at high frequencies.

We choose a simplified system consisting in a single loop without feeding wires, so as to focus only on the magnetic field generated by the loop. In these simulations the wire loop is no more infinitely small, as in section III.

The excitation port is placed on an opening in the loop. This will enable us to refer to the preceding theoretical calculations for the current loop. Loop radius $a = 500$ µm is formed with a wire width $r = 50$ µm. The conductor is considered lossless to highlight the influence of the geometry on the intrinsic radiation of the loop. Field is calculated for different distances d from 20 µm to 1 mm representative of those chosen for attacks on cryptographic circuits [8]. In these simulations the excitation pulse has the following characteristics: rise time (T_{rise}) and fall time (T_{fall}) both equal to 3 ns, and a pulse duration of 100 ns.

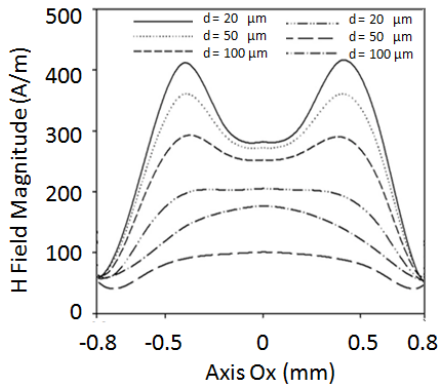


Fig. 5. Magnetic field amplitude of a current loop with radius $a = 500$ µm, wire radius $r = 50$ µm, for different distances d.

Fig. 5 shows that the amplitude of the magnetic field is symmetrical with respect to the Ox axis. This is in agreement with previous analytical calculations given in Figs. 2 and 3. For distances $d < 200$ µm, the magnitude is maximum close to the wire in the inner side of the loop. We calculate a difference in amplitude at $x = 0$ mm and $x = 0.5$ mm of up to 25% for $d = 20$ µm. For $d > 200$ µm, the field amplitude is maximum at the center of the axis of symmetry, as seen in Fig. 2.

One can assume that for a successful localized aggression in terms of quantity of injected signal, it will be better to use the edges of the probe if the distance separating the probe from the circuit is small. It seems more accurate to work with the center of the probe at distances d above 200 µm.

B. *Influence of the loop geometry*

Let us now consider the ratio $R = r/a$ between the radius of the wire and radius of the loop. Fig. 6 shows the system composed of SMA connector, loop and feed wires.

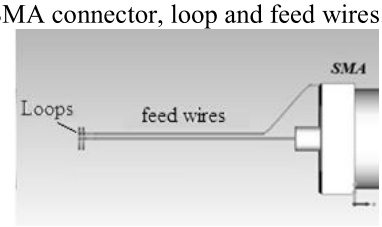


Fig. 6. Complete system probe.

The ratios R considered here are given in Table 1.

TABLE 1: R RATIOS FOR DIFFERENT a AND r VALUES

Loop radius a	**Wire radius r**		
	***r* = 50 µm**	***r* = 75 µm**	***r* = 100 µm**
100 µm	*0.5*	*0.75*	*1*
200 µm	*0.25*	*0.375*	*0.5*
500 µm	*0.1*	*0.15*	*0.2*

Ratio R ranges from 0.1 to 1. In Fig. 7 the magnetic field amplitude is plotted as a function of R for different distances d.

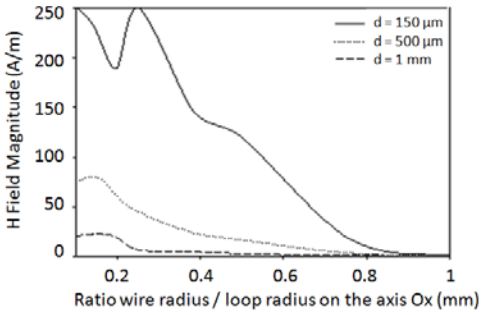


Fig. 7. Magnetic field amplitude as a function of R on the Ox axis for different distances d.

Neglecting the 20% variation for $R = 0.2$ at $d = 150$ µm, the field amplitude can be considered constant at $H = 250$ A/m till $R < 0.3$. When $R > 0.3$, the amplitude decreases quickly.

Depending on the ratio wire radius / loop radius, there are thus two types of evolution for the radiation of the magnetic field.

- In Fig. 8 ratio R is kept constant, with $R < 0.3$. A high magnetic field intensity is radiated, the wire radius has little influence on the amplitude.
- In contrast, Fig. 9 shows that for $R > 0.3$, the loop opening and feeding wires strongly influence the magnetic radiation with a strongly enhanced emission on the right side ($x > 0$) of the loop.

These results were both obtained for $d = 150\ \mu m$, which is a mean value for framing distances chosen for electromagnetic attacks on circuits.

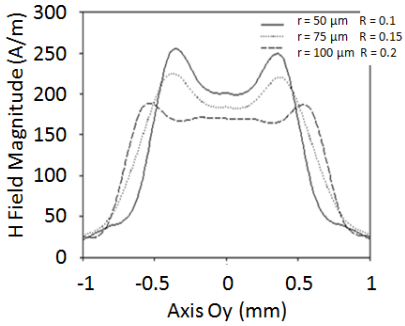


Fig. 8. Distribution of the magnetic field amplitude on the Oy axis for different values of r, loop radius $a = 500$ µm, $d = 150$ µm, $R < 0.3$.

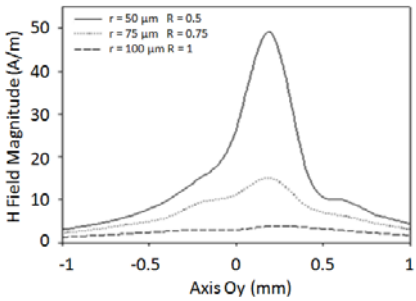
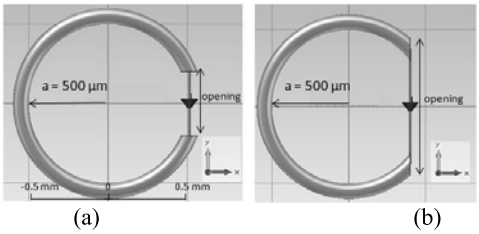


Fig. 9. Distribution of the magnetic field amplitude on the Oy axis for different r values, loop radius $a = 500$ µm, $d = 150\ \mu m$, $R > 0.3$.

C. *Influence of the loop opening*

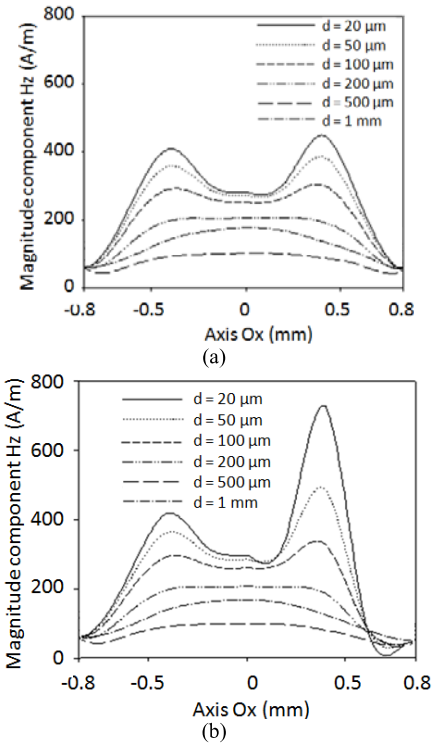
To study the influence of the loop opening on the spatial distribution of the magnetic field, the radiation issued from a single loop, without the feeding wires, is simulated. Characteristics are: loop radius $a = 500$ µm, radius of the wire $r = 50$ µm. The excitation port is directly placed on the opening of the loop. Two opening values are considered (cf. Fig. 10): an opening $O = 18\%$ of the total volume of the loop, and $O = 25\%$.



(a) (b)

Fig. 10. Opening geometry: (a) $O = 18\%$, (b) $O = 25\%$.

The H_z magnetic field component radiated by both opening values is simulated and plotted in Fig. 11.



(a)

(b)

Fig. 11. Distribution of the Hz component for different d, (a) $O = 18\%$, (b) $O = 25\%$.

We recall that the loop radius is $a = 500$ µm, which positions the opening of the loop at $x = 0.5$ mm. Results obtained on Fig. 11b show a strong field asymmetry at $x = 0.5$ mm. Indeed, for distance $d = 20\ \mu m$, amplitude at $x = 0.5$ mm is twice that at $x = -0.5$ mm. Notice that the asymmetry decreases with d. For $d > 200\ \mu m$ the field distribution becomes symmetrical.

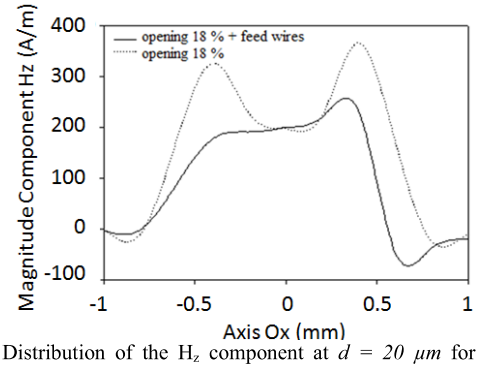


Fig 12. Distribution of the H_z component at $d = 20\ \mu m$ for $O = 18\%$. Continuous line: presence of feeding wires. Dotted loop: no feeding wires.

Fig. 12 illustrates the comparison of the shape of the H_z component for two different feeding schemes. Probe with feeding wires (solid line) is representative of a real probe. It exhibits an asymmetry on the spatial distribution of H_z on the opening side. Looking at Figs. 11 and 12, we then conclude that both the loop opening and the feeding wires play an important role in the distribution of the magnetic field radiation in the near-field. It should thus not be avoided for accurate predictions of the probe behaviour.

D. Influence of the number of loops

Here we evaluate the influence of the number of loops when it is increased from *1* to *4* (cf. Fig. 13).

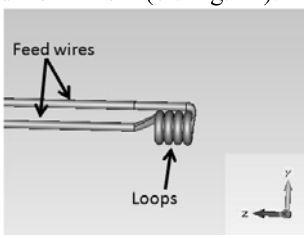


Fig. 13. Magnetic probe with 4 loops.

In a first time the magnetic field distribution is calculated along the Ox and Oy axes at the fixed distance $d = 200$ µm. The Fig. 14 then depicted the evolution of the magnetic near-field when the number of loops is varied from *1* to *4*.

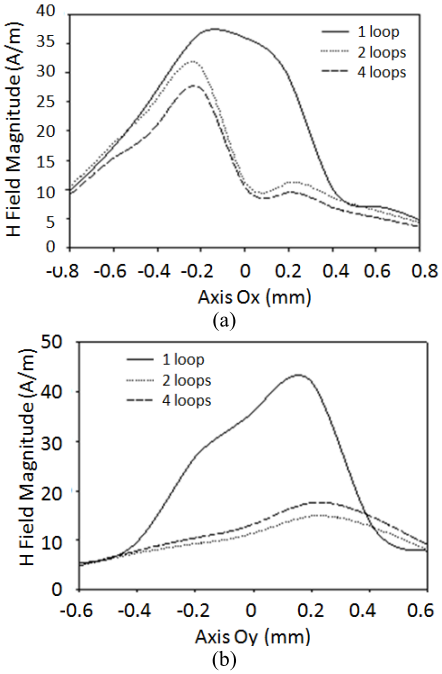


Fig. 14. Distribution of the magnetic field for different number of loops, (a) on the Ox axis, (b) on the Oy axis.

As previously observed the field presents an asymmetry in shape but the most important remark while considering these plots concerns the amplitude. Surprisingly, the maximum amplitude decreases when the number of loops increases. To the contrary of what occurs with DC solenoids, there is no benefit on the near-field magnetic field to multiply the number of loops. It seems therefore optimum to work with a single loop since it achieves the higher magnitude.

Let us now consider the *H* field magnitude as a function of the observation distance *d* along Oz for various loop counts. Results given in Fig. 15 show that the amplitude of the magnetic field decreases with the increasing distance. With one loop the maximum amplitude reaches *60* A/m, while for 4 loops it is only *10* A/m. Again there is no benefit to increase the loop count since field strength is reduced by *85%* in the near-field while going from *1* to *4*. As a major conclusion of this study it is more interesting to work with a single loop for our purpose.

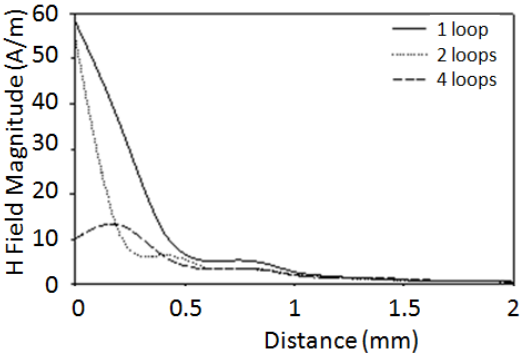


Fig. 15. Distribution of the magnetic field amplitude on the Oz axis as a function of d for different loop counts.

E. Influence of a ferrite core

To localise the magnetic field it is possible to include a ferrite core in the center of the magnetic loop. We choose to use a ferrimagnetic material composed of Nickel-Zinc. This type of ferrite is used for the realization of transformers or inductors for frequencies up to 100 MHz. Based on the datasheet of the ferrite, we established a model taking into account the real permeability and permittivity of the material. Moreover a model of dielectric and magnetic losses as a function of frequency are implemented in CST software for the calculation of EM fields generated by the probe. A ferrite rod with a relative permittivity $\varepsilon_r = 15$ and a relative permeability $\mu_r = 40$ at 50 MHz is modelled in CST.

To further focus the magnetic field, the simulated probe is conceived with a loop including a ferrite core sharpened at one of its ends. The tip diameter is *20* µm (Fig. 16). The probe consists of a single loop whose radius is $a = 750$ µm, the radius of the wire being $r = 50$ µm. The excitation signal is the same as in previous simulations (3 ns rise and fall time and a time duration of *100* ns).

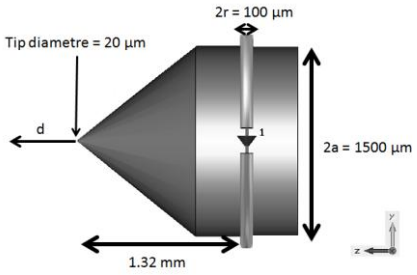


Fig 16. Sharpened ferrite in the loop and geometrical parameters.

The simulation results for H_z in the Oxy plane at different distances from the tip are given in Fig. 17. As expected, the ferrite concentrates the H_z component in the center of the loop for all distances considered here. Moreover, in comparison with results Fig. 12 at $d = 20$ µm (same case without the ferrite), the maximum fields are of the same order of magnitude. Hence the ferrite improves the performance of the probe for a localised magnetic field injection.

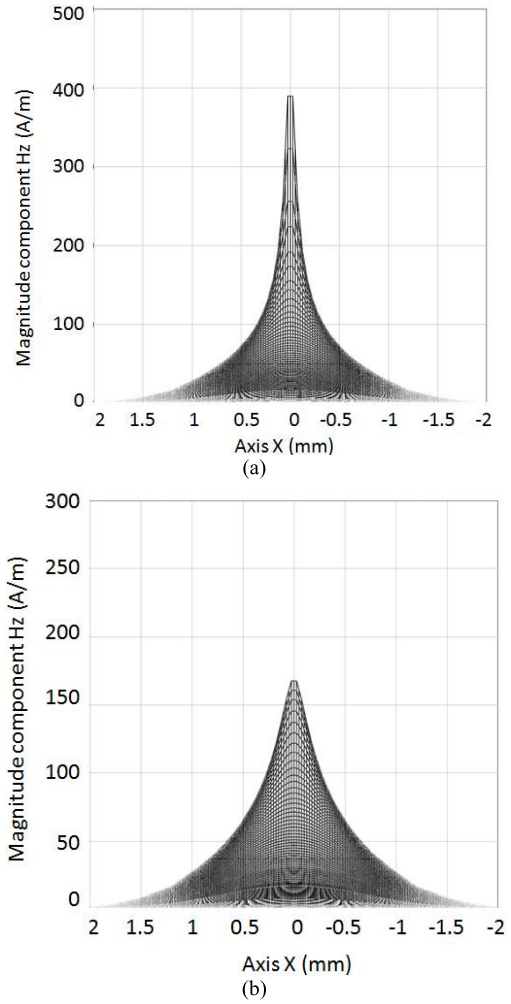


Fig 17. Distribution of the magnetic Hz component. (a) d = 20 µm, (b) d = 100 µm.

V. PROBE DESIGN GUIDELINES

In the framework of EM fault attacks on cryptographic circuits, we have studied magnetic probes built on the basis of small wire loops for the purpose of near-field injection. The goal is to perform intense and localized magnetic field aggressions from a small distance just above the circuits. Several probe design rules satisfying these constraints have been investigated. These investigations have lead to the following guidelines useful for future probe optimisation:

- Pulsed excitations are known to produce largest dysfunctional operations of circuits: probes must be designed as wideband components to transfer the EM power with the best efficiency.
- Considering injection, this paper has highlighted the fact that the field intensity greatly depends on the distance probe-circuit: one should then preferentially inject above the circuit for distances d smaller than the loop diameter for which it was shown that the field intensity is not a simple bell-shape transfer function.
- To the contrary of what was expected at first glance, a single loop must be used for optimized field intensity.
- Also considering field intensity, the wire radius should be smaller than the loop radius by a factor of *10*.
- The loop is supplied through feed wires connected on an opening of the loop. This opening must be of about 18% of the total volume of the loop to avoid field asymmetry.
- The introduction of a point-sharpened ferrite in the middle of the loop concentrates efficiently the field for near-field operation.

In a next future, experiments with these probes will be undertaken to refine the preceding design guidelines. Also the coupling with an integrated circuit under test will be studied by simulation.

REFERENCES

[1] R. Bekkeers and H. König. "Fault injection, a fast moving Target in evaluations", Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Delft, Netherlands, 2011, p. 65.

[2] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator", 3rd International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE Darmstadt, Germany, 2012, pp. 151-166.

[3] A. Dehbaoui, J.M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria., "Injection of transient faults using electromagnetic pulses-Practical results on a cryptographic system", IACR Cryptology ePrint Archive, 2012, p. 123.

[4] G. Piret and J.J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with application to the AES and Khazard", Conference on Hardware and Embedded Systems, CHES 03, Cologne (Germany), 2003, pp. 77-88.

[5] CST Website: http://www.cst.com

[6] Probe Langer website: http://www.langer-emv.de

[7] K.S. Yee, “Numerical solution of initial boundary value problems involving Maxwell”, IEEE Trans. on Microwave Theory and Tech.”, vol. 14, 1966, pp. 302-307.

[8] F. Poucheret, K. Tobisch, M. Lisart, B. Robisson, L. Chusseau, and P. Maurine, "Local and direct EM injection of power into CMOS integrated circuits" FDTC 2011, Fault Diagnosis and Tolerance in Cryptography, Nara, Japan, 28 Sept. 2011.