New probe design for hardware characterization by ElectroMagnetic Fault Injection

Clément Gaine, Jean-Pierre Nikolovski, Driss Aboulkassimi, Jean-Max Dutertre

New Probe Design for Hardware Characterization by ElectroMagnetic Fault Injection

Clément Gaine*, Jean-Pierre Nikolovski*, Driss Aboulkassimi*, Jean-Max Dutertre†
*Univ. Grenoble Alpes, CEA, LETI, MINATEC Campus, F-38054 Grenoble, France
†Mines Saint-Etienne, CEA-Tech, Centre CMP, F-13541 Gardanne France
Email: firstname.lastname@cea.fr, dutertre@emse.fr

***Abstract*—ElectroMagnetic Fault Injection requires two main devices, a pulse generator and an electromagnetic (EM) injection probe. To improve security characterizations, inductive probes need to be optimized as regards the pulse waveform and field distribution. The improvement of these parameters leads to greater electromotive forces generated in the integrated circuits, which reinforces the efficiency of the attacks by fault injections. This paper presents a complete model of the electromagnetic field induced at the target surface according to Biot and Savart's law. This work defines the relevant design parameters of the new probes that are used for hardware characterization of the target components. These new probes reduce the voltage fault threshold required to disturb the execution of a program in the target. This paper also presents results related to the optimization of spatial resolution and inductive power at the target circuit surface. Understanding these phenomena then helps to implement countermeasures and best secure the strategies of the key IC components.**

***Index Terms*—ElectroMagnetic Pulse, Fault Injection, Inductive Probe**

I. Introduction

Integrated circuits (ICs) use cryptographic algorithms to secure their operations and communications. Almost all algorithms implemented in ICs are standardized [9], [8] and are free of mathematical security flaws. However, codes are still vulnerable to physical attacks targeting their implementation on ICs. The voluntary disruption of the operating environment of a target can corrupt the execution of a code, which can create errors (also called faults). An attacker can then bypass security mechanisms, obtaining personal data and the secret keys of encryption algorithms. This disruption is achieved by generating an EM pulse near the processor [3]. EM fault injection is generally performed with a voltage pulse generator, an injection probe placed on a motorized arm (allowing XYZ positioning), and a control computer as shown in Figure 1. The injection probe is usually made up of a few turns of a conductive wire around a ferrite rod. A voltage pulse delivered to the injection probe induces the EM perturbation. This field couples with the power-ground network of the target, causing a variation of its supply voltage and an alteration of its functioning. The design of the injection probe is therefore essential for a successful characterization, as detailed in [4]. To guide this design, a modelling of the probes and a method to compare the probes is proposed. The effect of the various parameters of the probe, including the effect of a ferrite material, is studied here. The dynamic study of the generator/probe combination

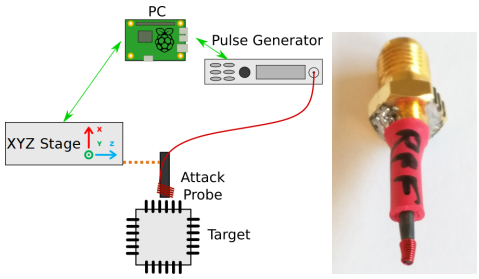


Fig. 1: Electromagnetic fault injection bench **(a)** with a conical probe **(b)**

makes it possible to define the specifications of new probes, which are more efficient than the state-of-the-art.

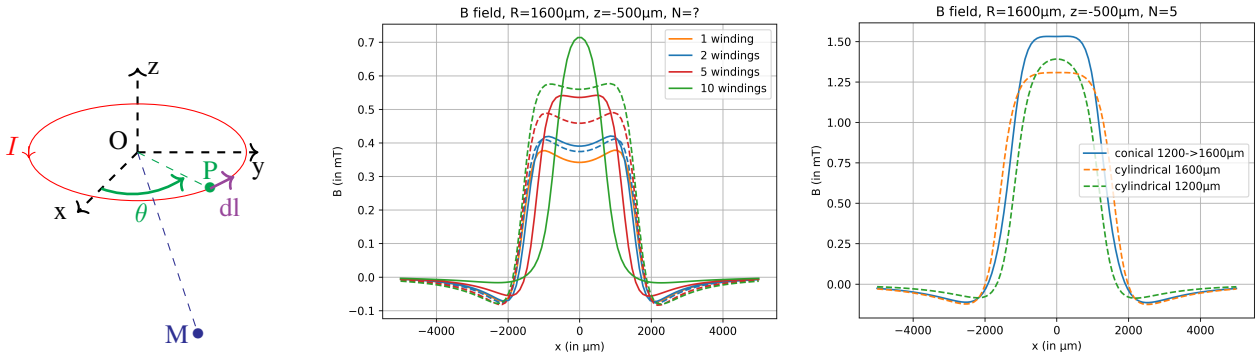
II. State-of-the-Art

Physical attacks are based on observing the operation of software code with and without its disruption. This first type of attack, also called fault injection (FIA), can be done by modifications in the operating environment such as temperature increases [12], changes in supply voltages [13] and clocks [6] generated by laser [15] or electromagnetic pulse disturbances.

The first experimental realization of an EM induced FIA was done by Schmidt and Hutter [11] on an 8-bit microcontroller using sparks induced by a spark gap generator made from a gas lighter. However, this approach suffered from a lack of spatial and timing accuracy which was later improved using voltage pulse generators and coil-shaped EM injection probes. Dehbaoui et al. [3] realized the first fault injection with an electromagnetic pulse on both software and hardware implementation of the AES encryption algorithm. They were able to extract the AES encryption keys. Omarouayache et al. [10] modeled and simulated magnetic probes for fault injection to deduce the effects of different parameters. They showed that the flux intensity depends on the distance between the probe and the circuit. They also suggested that a single wire loop can optimize the flux intensity and that the addition of a tapered ferrite tip improves the magnitude of the magnetic field delivered to the target.

Chusseau et al. [2] demonstrated that several turns allow better coupling between the injection probe and the target at low frequencies and that the addition of a ferrite material improves the intensity of the EM flux.

Beckers et al. [1] showed that an increase in the number of turns decreases the amplitude of applied generator voltage,



a. One loop probe parameters b. B field intensity c. Variation of the angle at the vertex

Fig. 2: Modeling of probes

but this is slightly compensated by an increase in the EM field generated. An increase of the ferrite diameter reduces the amplitude of the disturbance, as the inductance and EM field depend on the radius of the solenoid.

Toulemont et al. [14] presented a protocol for comparing Electromagnetic Fault Injection platforms with a commercial probe. They explained that the use of a Transil diode limits the bounces of the voltage pulse in the probe, thus increasing the timing accuracy.

III. Testing protocol and Methodology

The voltage pulse generators used can deliver pulses up to several hundreds of Volts with currents up to ten Amperes in a 50 Ω load. The rise and fall times are about 2 ns, while the duration of the pulse can be set between 10 ns and 100 ns.

An injection probe consists of a coil made of copper wire (coated with an insulator to avoid short-circuits between adjacent loops) wound around a ferrite rod. It is connected to the voltage pulse generator (as its load) and positioned in the close vicinity of the target. A picture of a state-of-the-art probe is given in Figure 1.b. In order to experimentally compare the properties of the injection probes we studied, we set up a protocol that uses three types of targets: (1) other EM probes used as targets and two ICs: (2) an ATMega328P microcontroller and (3) a Zynq FPGA.

1) Probes used as targets: To measure the EM field induced by a given injection probe, we use two EM probes. The first one is a commercial RF-B probe from Langer with a diameter of 3 mm that makes it possible to record calibrated measurements of the overall intensity of the received EM field. The second one is a precise tiny home-made probe, 250 µm in diameter, considered as almost spot probe for local measurements.

2) Microcontroller ATMega328P: This 8-bit RISC microcontroller is present on Arduino Uno prototyping platforms. Its technology is CMOS 0.35 µm. It runs at 16 MHz. It was used to compare the ability of various injection probes to inject faults into a dedicated test code: it writes and reads data into and from the core's registers. We defined a fault threshold as the minimum voltage pulse magnitude that induces an EM perturbation capable of injecting faults into the target's registers. We use it as a metric to compare different designs of EM injection probes.

3) FPGA Zynq-7010: We embedded and targeted a ring-oscillator-based sensor developed by Gravellier [5] in the FPGA target. When exposed to an EM pulse, the supply voltage of the FPGA undergoes variations of its core voltage. Thus, the propagation delays of its logic gates evolve according to the intensity of the disturbance, which generates fluctuations in the output values of the sensor. This provides an image of the voltage variation inside the target. This sensor acts as an internal oscilloscope which measures the variations of voltages induced in the target.

IV. Parameters to consider when designing an EM injection probe

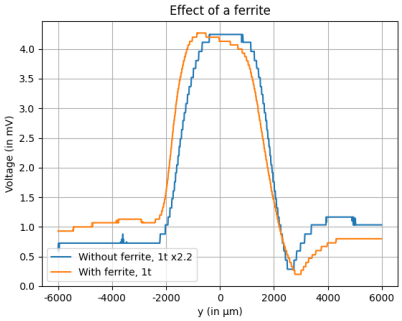
A. Modeling of the magnetic field

Although the disturbance is mostly called electromagnetic, it is only inductive and not capacitive, so we can only consider the B field. The modeling of this field, for a point in space given by its (x,y,z) coordinates, can be calculated using Biot and Savart's law:

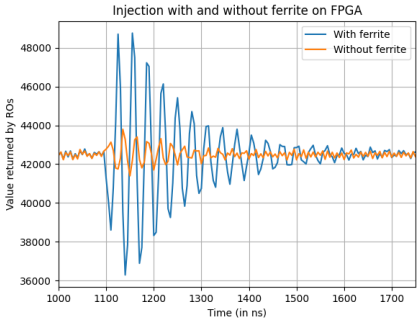
$$B_z(x,y,z) = \frac{\mu_0 I}{4\pi} \sum_{n=0}^{N-1} \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}} \quad (1)$$

ζ and δ represent the vertical and horizontal distance between two turns, R the radius of the coil, Θ the angle between the X axis and an elementary portion of the wire, as shown in Figure 2.a. I is the intensity of the disturbance and N the number of turns.

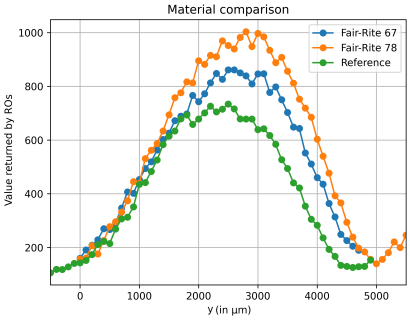
In Figure 2.b, where the field strength is shown as a function of x, it can be seen that an increase in the number of coils raises the strength of the disturbance. The solid lines represent the conical turns and the dotted lines the cylindrical ones, enabling the effect of conical versus cylindrical probes to be compared. A conical probe has a smaller spatial extent and a slightly higher generated field value than a cylindrical one. Therefore, the conical probe with 10 turns seems, on a theoretical basis, the most relevant for our parameters. These studies are done for a constant current I. However, in practice, ohmic law implies that an increase in wire length due to the number of turns or geometry will limit the current I.



a. B-field measured on a 250 µm probe



b. B-field mesured on FPGA



c. Effect of various materials

Fig. 3: Ferrite

Even if it is preferable to have the smallest possible radius, shaping the tip of a probe into a conical shape improves the localization of the flux and the value of the generated field, as presented in Figure 2.c, with 5-turn probes. An angle at the tip is best for maximizing the generated field. However, even if the interdependent relations between the optimal values of radius R, number of turns N, δ, ζ and distance z to optimize the flux have not been clearly established, they can be determined iteratively by simulations as presented in IV-D. An angle of 120° is a first approximation given by the simulation.

From the formula, it can be seen that the space between two turns needs to be minimized to strengthen the field at the point of interest nearby, outside the probe.

B. Effect of a ferrite material

1) Presence of a ferrite material: In the literature, some probes are ferrite-based while others are not. We want to experimentally determine the effect of a ferrite material, and ascertain whether its presence is necessary. Currently, in the production of probes, a parameter limiting the reduction of the diameter of the probes is the presence of ferrite that is too brittle for small diameters. However, the reduction of the diameters of the probes can increase the intensity of the disturbance; we therefore want to verify that we should expect the presence of a ferrite material to enhance the magnetic field and generate faults.

Our first experiment was designed to test whether it is useful to have a ferrite core in an injection probe. We measured the maximum voltage magnitude induced in the 250 µm target probe by 1 loop 3 mm diameter injection probes with or without a ferrite material for the same voltage pulse. Figure 3.a provides the induced voltage magnitude as a function of the off axis distance between both probes. Note that the curve for the ferrite-free probe is normalized (i.e. multiplied by 2.2) w.r.t. the probe with a ferrite core in order to better compare the shapes of their respective field pattern. This practical experiment showed that using a ferrite core improves the induction phenomenon by more than a factor of 2 with no significant effect on the field radiation pattern. It may therefore be necessary to choose a probe adapted to the distance from the target. A probe with a thin diameter, less than 250 μm for example, will have limited disturbance for a target at 500 µm.

Figure 3.b depicts the effect of the 3 mm diameter probes on the FPGA sensor. The induced disturbance on the target core supply appears to be clearly diminished when a ferrite free probe is used. These results prove that the presence of a ferrite material is necessary to maximize the transient magnetic flux and inductive effect on the target.

2) Ferrite material: There are different types of ferrites; in order to maximize the generated fields, we studied 3 different types:

Reference ferrites in common use (as in several publications [7])

Fair-rite 67 ferrites composed of nickel and zinc alloys, with a high quality factor up to 50MHz

Fair-rite 78 ferrites composed of manganese and zinc alloys, for power applications up to 200kHz

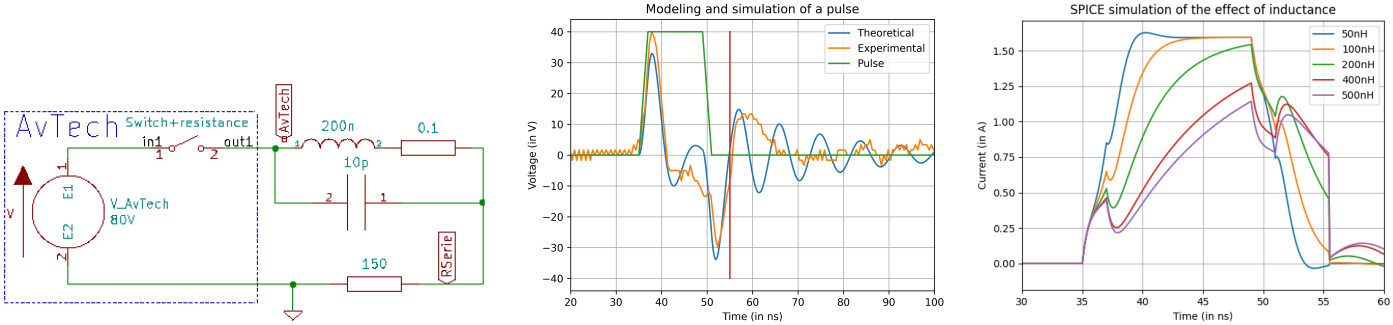
The FPGA-based test circuit is used to compare measurements between ferrite 67, 78 and reference probes for various diameters. The measurements shown in Figure 3.c present the maximum recorded value of Ring Oscillators during a spatial scan. The results for a 1500 µm ferrite diameter are shown, but they are similar for the other diameters. The inductive disturbance is higher with ferrite 78 type probes than with ferrite 67 and reference type probes. The Fair-rite 78 material exhibits the best performance compared with other ferrites.

The decrease of the magnetic field as the distance between the probe and its target increases is similar whatever the type of ferrite. The losses are about 15% for a distance of 200 µm and 30% for a distance of 500 µm with a probe using a ferrite of 1500 µm in diameter.

C. Dynamic study for the probe/generator combination

In our experiments, we used a voltage pulse generator from AvTech, the output impedance of which switches from 50 Ω to 1k Ω about 2 ns after the voltage pulse ends. Fig. 4.a provides the schematic of the SPICE model we used to simulate the voltage pulse generator and the injection probe (the parameters of the injection probe, a 200 nH inductance with a serial 0.1 Ω resistor in parallel with a 10 pF capacitor, were obtained from various measurements). A 150 Ω resistor is added between the probe and the pulse generator in order to easily measure the current across the probe.

The voltages at the probe, obtained with simulations and experimentally are shown in Figure 4.b. The curves have the



a. Electronic circuit diagram b. Voltage across the probe c. Effect of the inductance on current

Fig. 4: Dynamic study of the probe

same tendencies, even if we do not observe as many bounces in practice. The simulation is consistent with the experiment during the pulse; we can therefore consider this model to properly describe the variation of the current according to different parameters. The variation in current will determine the variation in magnetic flux and therefore the electromotive force within the target.

1) Effect of inductance: Since an increase in the number of turns increases the inductance, it is necessary to know how this influences the current variation. The simulation, in Figure 4.c, shows that decreasing the inductance increases the voltage across the probe and shortens the disturbance. Thus, minimizing the number of turns could improve the intensity of the disturbance. However, it has previously been seen that an increase in the number of turns strengthens the intensity of the disturbance. These two factors balance each other, but in order to keep a rise time roughly lower than 2 ns, it is necessary to keep an inductance lower than 100 nH. The best compromise is to stay close to this value.

2) Effect of resistance: Changing the diameter or length of the lead wire affects the resistance. When we simulate the addition of a series resistance, the current variation decreases. However, between 0 and 10 Ω, the fall is limited to 5%. The resistance generated by a wire ranging between 40 µm to 250 µm in diameter varies from 1.38 Ω to 30 mΩ. This parameter is therefore not very relevant and the reduction of the wire diameter and thus the diameter and the length of the solenoid leads to successful optimization.

D. Conclusion

The above results allowed us to understand the mechanisms involved in inductive generation and to define rules for the design of the probes best suited for a given distance from a target:

- Use of a ferrite material, Fair-rite 78 for example
- Maximization of the number of turns keeping an inductance value below 100 nH
- Diameter of the probe chosen according to the distance from the target
- Conical geometry with close-wound turns to improve disturbance locality and intensity
- Wire as thin as possible, 40 µm to 100 µm in diameter

Geometry (9-turn probe)	Simulation (Figure 5.a.)	Langer probe (Figure 5.b)	ATMega328p
Cylindrical	2250 mT	175 mV	80 V
Overlay (5-4)	2930 mT (+30%)	180 mV (+3%)	75 V (-6%)
Double overlay (4-3-2)	3210 mT (+43%)	200 mV (+14%)	60 V (-25%)

TABLE I: Effect of overlaying on different sensors

Now that we have identified the best probe parameters to optimize the energy transferred from the generator, we can use these results to make high-performance probes. We built a utility program tool, based on formula (1), that simulates the magnetic fields generated by the probes. It helps to achieve, by simulation, the best ferrite diameter and vertex, depending on the number of turns and the distance z to the target. This tool makes it possible to imagine and test new probe geometries.

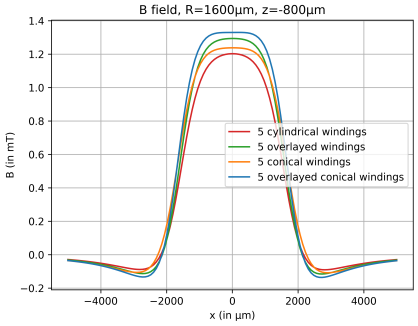
V. New design factors of EM probes

With successive runs of the utility program, probe design alternatives have emerged. A conical geometry is more effective at performing fault injections than a simple cylindrical geometry. We evaluate hereafter the behavior of various alloys of ferrites and coil geometries.

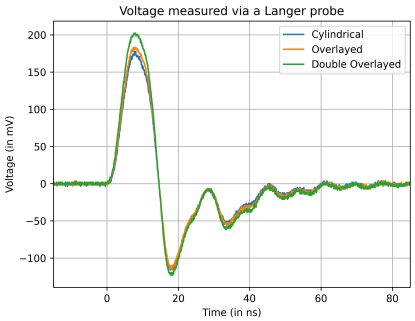
A. Overlaying of coils

One of the limiting parameters of an injection bench is the maximum voltage of the generator. By making the probes more compact, i.e. by reducing the length of the solenoid, it is possible to reinforce the disturbance without increasing the drive voltage. To do this, a possible geometry consists in overlaying several coils, as shown in Figure 6.a (b) and (c). The simulation tools provide, in Figure 5.a, the B fields obtained with different types of probes. We can see that an overlay of the coils increases the intensity of the disturbance.

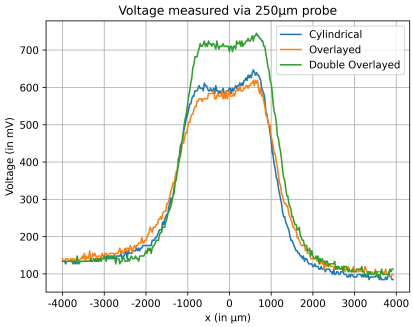
The characteristics of 9-turn cylindrical probes, 5+4 turn (overlay of 4 turns on top of 5 turns) probes and 4+3+2 turn (double overlay of 2 turns on top of a layer of 3 on top of a layer of 4) probes are presented in Table 1. The fault threshold reductions are a little less than expected because such coils are difficult to realize properly. The disturbances were measured with various probes and it can be seen that the temporal (Fig 5.b) and spatial (Fig 5.c) field extensions are not modified, while the intensity of the disturbances is increased. As regards the target microcontroller, the fault threshold is reduced by approximately 25% with the double overlay probe.



a. Simulation

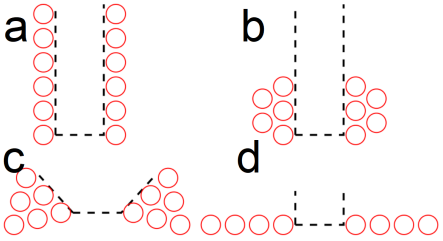


b. Langer probe

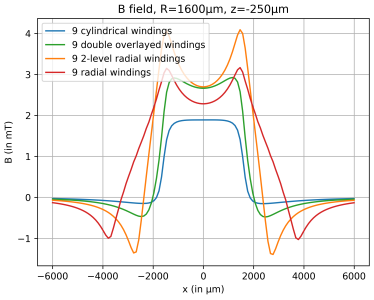


c. Probe 250 µm

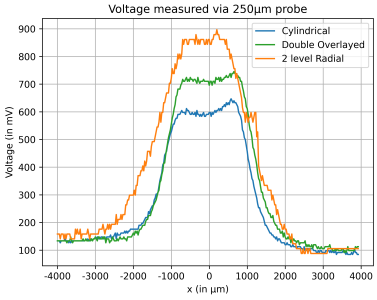
Fig. 5: Overlay of the turns



a. Cylindrical, cylindrical with an overlay, conical with a double overlay and radial probe



b. Simulation of radial probes



c. Effect of radial probes

Fig. 6: Radial probes

This reduction is equivalent to increasing the pulse voltage by 25%, which is not easily available when we are already operating at the highest pulse voltages together with the lowest rise times available on the market.

B. Radial probes

Another way to improve the field intensity is to overlay all the turns, so as to create radial probes, as presented in Figure 6.a (d) and 8.a. Figure 6.b is a cross section view along the X axis, showing that the disturbance generated by a radial probe, in red, has a much larger lateral field extension, meaning poor locality compared to cylindrical probes but with the same intensity. A good compromise is to have probes with an overlay, as shown by the orange curve. The experimental results of a characterization with the 250 µm diameter probe are presented in Figure 6.c and are in good agreement with the simulation. The 2-level radial probe, in orange, generates higher disturbances than a cylindrical probe. Its lateral field extension is slightly worse.
For the ATMega328P target, the fault threshold is close to those of the cylindrical probes with double overlay. The experimental use is more complex because the probe is rather large-sized; it is thus difficult to be in contact with the target.

C. Tape probes

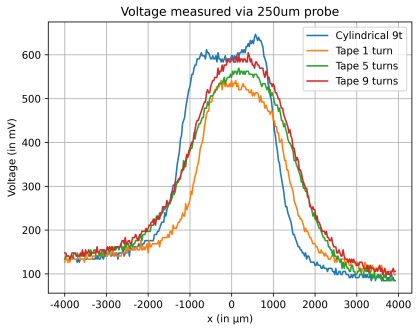
In certain cases, such as small technological nodes, it is useful to improve the locality of the probes while preserving similar disturbance intensities. One solution is to replace the copper wire with a copper tape. Three probes with a diameter of 2 mm and with 1, 5 and 9 turns were made. The experimental results of a characterization by a probe of diameter 250 µm are presented in figure 7.a. The profiles of the tape probes are symmetrical and their lateral spread at 90% of the maximum signal is much reduced compared to a cylindrical probe. The differences in the measured field strengths are less than 15%, which suggests a screening effect of the outer turns from the inner turns. This type of tape probe is also validated on a microcontroller ATMega328p, with a fault threshold of 75 V against 80 V for a cylindrical probe with the same characteristics. An interesting aspect with these probes is that their measured inductances are 20% lower than those of probes made with a copper wire of 200 µm.

D. Wrapped probes

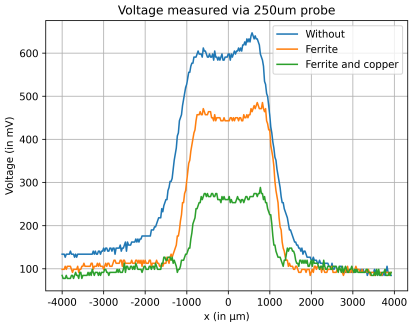
If the magnetic field has to be even more concentrated and a loss of efficiency is acceptable, it is possible to wrap the probe in a ferrite sheet layer and if necessary overlay the wrapped probe with a thin copper sheet, as presented in Figure 8.b. The results of characterization with a 250 µm diameter probe are shown in Figure 7.b. Lateral field extension is reduced, falling sharply to a width of half the maximum value of 2500 µm for the cylindrical probe, 2300 µm for the ferrite-wrapped probe and 2100 µm for the ferrite-copper-wrapped probe.

E. Field projected through the integrated circuit

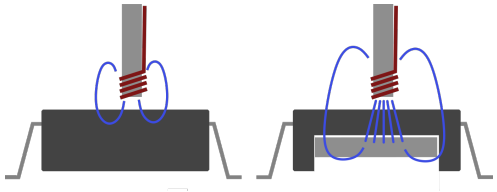
The magnetic field lines must loop back at the ends of the coil. The target positioned at the end of the probe is thus disturbed by a portion of the magnetic flux. In order to maximize the vertical extension of the flux while keeping lateral extension at its minimum, it is conceivable to have the



a. Effect of tabe probes



b. Effect of probes with envelopes



c. Guidance of EM field through the chip

Fig. 7: Others designs

field lines not quickly looping back to the other side of the coil, but through the target, as presented in Figure 7.c. The field intensity at the target is then maximized. This was done for an ATMega328p target where the back side was removed and a ferrite layer sheet introduced. The fault threshold is then reduced from 62 to 57 V with the ferrite sheet. This brings an additional gain of 10% of the threshold voltage and can be combined with the new probe designs.

VI. Conclusion

The combined characterization work with a custom made probe, a microcontroller and a ring oscillator implemented in FPGA enabled the analysis, understanding and improvement of the radiating pattern of the inductive probes from the point of view of both their spatial and temporal response and the intensity of the generated disturbing magnetic fields.

New test protocols were presented to compare the effects of different probes. This helped improve iteratively the probe specifications as regards the field spatial distribution as well as its disturbing efficiency. The presence of soft high permeability ferrite was proven to limit the requirement of high voltages. A small diameter ferrite material will limit the magnetic field generated by the probe and for a given distance z, the radius R can be chosen to optimize the generated field. The ferrite can be tapered at a certain angle, 120° for example, to concentrate the magnetic flux. The probe coils are preferably composed of several compact overlays, with the constraint that their inductance should remain lower than 100 nH in order to keep a short impulse response or temporal locality. The coils must be close-wound and placed at the tip of the ferrite rod to maximize the projected field intensity. Field projection can also be enhanced with soft ferrite material placed below the target component. All these adjustments add up to about 30% more efficiency in fault thresholds.

This work has been done to improve the efficiency of fault injections. It also proved to be valid in the context of side-channel acquisitions. Tests have shown that bandwidth and signal to noise ratio of traces needed to recover encryption keys are similar to those of commercial probes.

References

[1] A. Beckers, M. Kinugawa, Y. I. Hayashi, D. Fujimoto, J. Balasch, B. Gierlichs, and I. Verbauwhede. Design Considerations for EM Pulse Fault Injection. *Smart Card Research and Advanced Aplications-CARDIS 2019*, pages 1–16, 2019.

[2] L. Chusseau, R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Boyer, B. Vrignon, J. Shepherd, T. H. Le, M. Berthier, L. Riviere, B. Robisson, and A.-L. Ribotta. Electromagnetic analysis, deciphering and reverse engineering of integrated circuits. *IEEE/IFIP International Conference on VLSI and System-on-Chip, VLSI-SoC*, 2015.

[3] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria. Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES. *Fault Diagnosis and Tolerance in Cryptography*, 2012.

[4] C. Gaine, D. Aboulkassimi, S. Pontié, J.-P. Nikolovski, and J.-M. Dutertre. Electromagnetic Fault Injection as a New Forensic Approach for SoCs. *Workshop on Information Forensics and Security*, 2020.

[5] J. Gravellier, J.-M. Dutertre, Y. Teglia, P. Loubet-Moundi, P. Loubet, and M. High. High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs. *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, 2019.

[6] T. Korak and M. Hoefler. On the effects of clock and power supply tampering on two microcontroller platforms. *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014*, 2014.

[7] A. Menu, J.-M. Dutertre, O. Potin, J.-B. Rigaud, and J.-L. Danger. Experimental analysis of the Electromagnetic instruction Skip Fault Model. *Design Technology of Integrated Systems in Nanoscale Era (DTIS)*, 2020.

[8] NIST. Advanced Encryption Standard (AES) FIPS197, 2001.

[9] NIST. Digital Signature Standard (DSS) FIPS186, 7 2013.

[10] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine. Magnetic Microprobe Design for EM Fault Attack. *International Symposium on Electromagnetic Compatibility*, 2013.

[11] J.-M. Schmidt and M. Hutter. Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results. *Proceedings of the Austrochip*, 2007.

[12] S. P. Skorobogatov. Local heating attacks on flash memory devices. *Hardware-Oriented Security and Trust, HOST 2009*, 2009.

[13] N. Timmers and C. Mune. Escalating Privileges in Linux Using Voltage Fault Injection. *Fault Diagnosis and Tolerance in Cryptography*, 2017.

[14] J. Toulemont, J. M. Galliere, P. Nouet, E. Bourbao, and P. Maurine. A Simple Protocol to Compare EMFI platforms. *IACR Cryptol. ePrint Arch.*, pages 1–9, 2020.

[15] A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, and S. Ermeneux. Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot. *Fault Diagnosis and Tolerance in Cryptography*, 2017.

a. Radial probe b. Probes with envelopes

Fig. 8: Probes