EM Probes Characterization for Electromagnetic Fault Injection Attacks

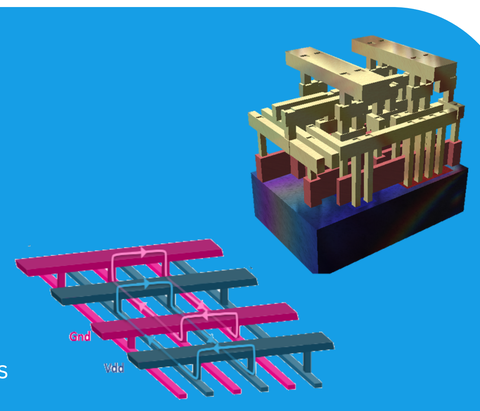
Elie Daher[1,2], Lichao Wu[1], Mathieu Dumont[1], Noemie Beringuier-Boher[1]
[1] : SGS Brightsight ; [2] : Mines Saint-Etienne, ISMIN

Context

Electromagnetic Fault Injection (EMFI) is a well-known attack that induces faults in electronic devices using high-powered EM fields. Our work focuses on evaluating and chatacterizing existing EM coils to optimize their performance *for EMFI*. Varying coil parameters impact fault quality and reliability.

IC Metal layers

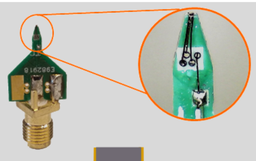
The power (Vdd) and Ground (Gnd) supply rails form two grids which deliver power to the CMOS gates. These grids form numerous **vertical** and **horizontal** loops in the circuit, acting as antennas. Therefore, two different types of antennas are used for the carachterization.

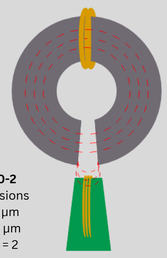


Probe names

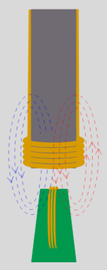
Probe names will be as : Type - dimensions - Nb of loops
Type: Crescent “C”, Flat “F” and Sharp “S”
Dimensions: in µm

Vertical loops

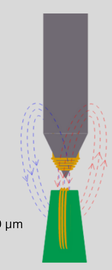




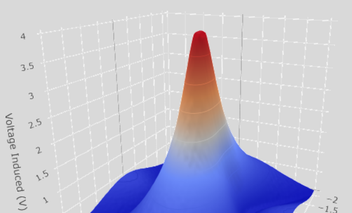
C-1200x750-2
Ferrite dimensions = 1200x750 µm
Φwire = 200 µm
Nb of loops = 2



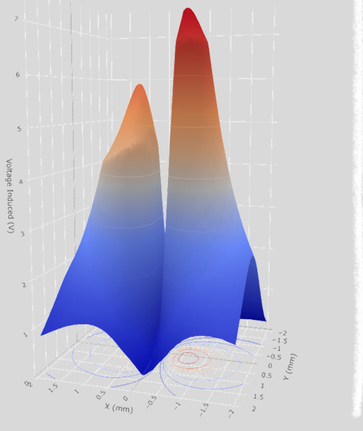
F-760-5
Φferrite = 760 µm
Φwire = 200 µm
Nb of loops = 5



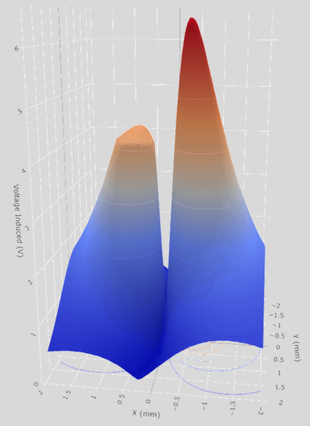
S-1500_330-5
Φferrite = 1500 -> 330 µm
Φwire = 50 µm
Nb of loops = 5



V_max = 3.9 V
Width@80% = **469 µm**.

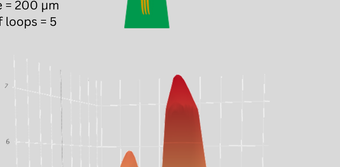


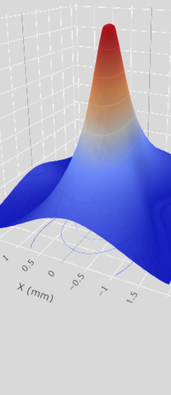
V_max = **7 V**
Width@80% = 786 µm.



V_max = 6.47 V
Width@80% = 665 µm.

Horizontal loops

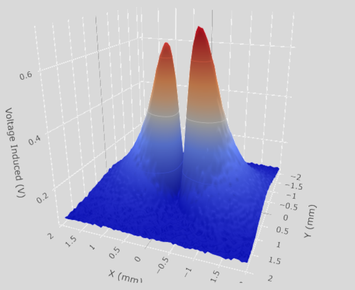




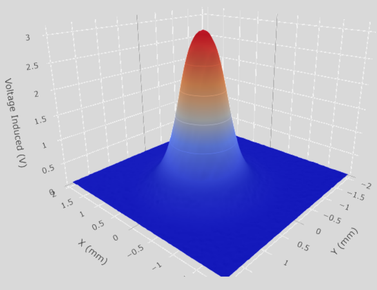
C-1200x750-2
Ferrite dimensions = 1200x750 µm
Φwire = 200 µm
Nb of loops = 2

F-760-5
Φferrite = 760 µm
Φwire = 200 µm
Nb of loops = 5

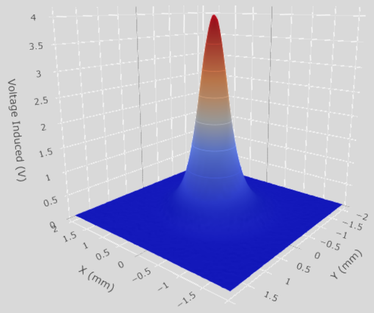
S-1500_330-5
Φferrite = 1500 -> 330 µm
Φwire = 50 µm
Nb of loops = 5



V_max = 0.71 V.
Width@80% = 450 µm.



V_max = 3.3 V.
Width@80% = 590 µm.

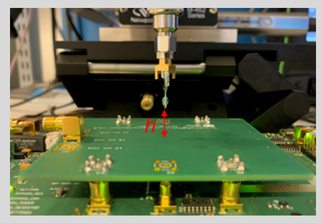


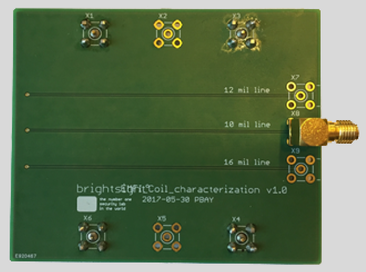
V_max = **4.04V.**
Width@80% = **384 µm**.

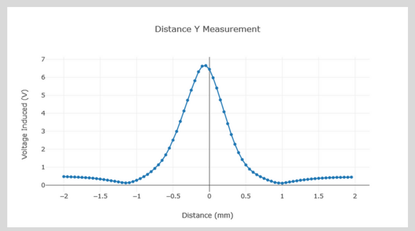
Reference Measurement Card

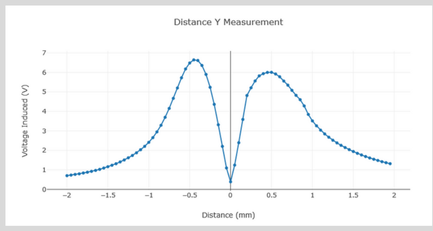
A PCB board with strip-lines that forms loops to measure test the probe characteristics.

- V_induced vs V_input
- V_induced vs Y
- V_induced vs Z

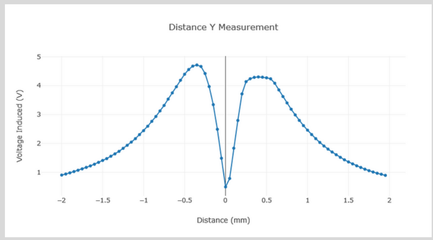








C-1200x750-1
Ferrite dimensions = 1200x750 µm
Φwire = 200 µm
Nb of loops = 1



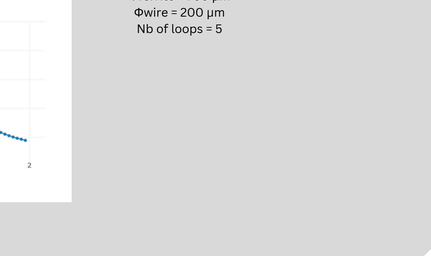
S-1500_330-5
Φferrite = 1500 -> 330 µm
Φwire = 50 µm
Nb of loops = 5

F-760-5
Φferrite = 760 µm
Φwire = 200 µm
Nb of loops = 5

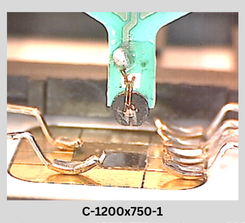
Validation Sample

The validation involves attempting to bypass a secret code and retrieve the secret message from the ATMEL card, which contains an ATmega8515 microcontroller running a test program.
This attack helps us analyze probes’ behaviour on a target device.
This table display the minimum voltage needed to induce faults with a height of z=0 (contact) and the maximum height z for a maximum voltage of 500V:

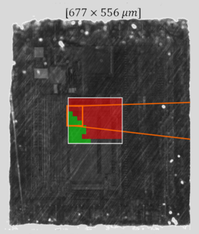
	F-760-1	F-760-5	C-1200x750-2	S-1500_330-5
V_{min}	30V	20V	120V	28V
Z_{max}	1.54mm	3.76mm	1mm	1.93mm

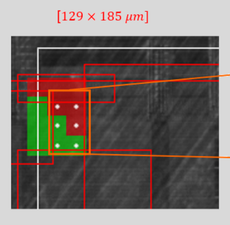


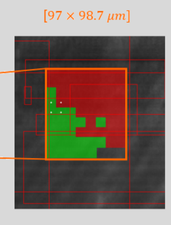
F-760-5
Φferrite = 760 µm ; Φwire = 200 µm
Nb of loops = 5

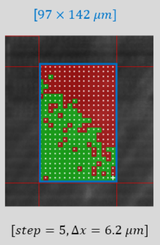


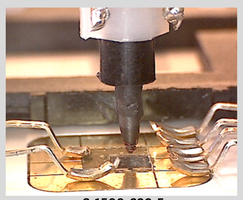
C-1200x750-1
Ferrite dimensions = 1200x750 µm; Φwire = 200 µm
Nb of loops = 1



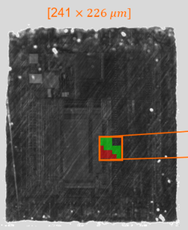


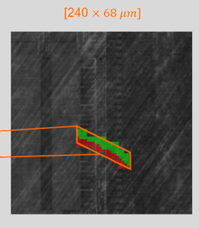


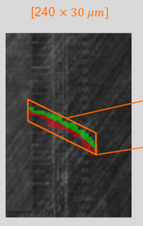


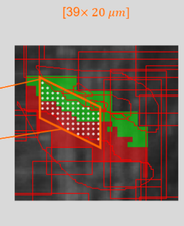


S-1500_330-5
Φferrite = 1500 -> 330 µm ; Φwire = 50 µm
Nb of loops = 5









Results

Three main probe types (flat, sharp, crescent) with different characteristics are used for EMFI, and we characterized them and analyzed their impact on different targets devices. Our results show significant performance improvements through design optimization. We can see that the sharp probe have the best resolution while keeping a high induced voltage. However, this probe is difficult to build. However the crescent probe is easier to do and show high resolution also while the induced voltage is low. Flat probes on the other hand are the easiest to do and have a very high induced voltage with higher penetration effect which can be useful for closed IC with higher thickness. We can see that each probe has its advantages and drawbacks and should be chosen according to the target device . Our research enhances EM coil design for more effective EMFI attacks, strengthening IC security with optimized design guidelines.

References:

[1] Mathieu Dumont. Modélisation de l’injection de faute électromagnétique sur circuits intégrés sécurisés et contre-mesures. Autre. Université Montpellier, 2020.
[2] Clément Gaine. Évaluation et mitigation du risque d'attaque par injection de fautes électromagnétiques sur plateformes mobiles. Autre. Université de Lyon, 2022.