# A Simple Protocol to Compare EMFI platforms

Julien Toulemont, Nasr-Eddine Ouldei-Tebina, Jean-Marc J.-M. Galliere, Pascal Nouet, Eric Bourbao, Philippe Maurine

# A Simple Protocol to Compare EMFI platforms

J. Toulemont[1], N. Ouldei-Tebina[1], J. M. Galliere[1], P. Nouet,[1], E. Bourbao[2], P. Maurine[1]

[1] LIRMM,
University of Montpellier
161, rue Ada
34095 Montpellier, France

[2] Thales DIS
La Vigie – Avenue des Jujubiers
Z.I. Athélia IV
13705 La Ciotat Cedex, France

**Abstract.** Several electromagnetic fault injection (EMFI) platforms have been developed these last years. They rely on different technical solutions and figures of merit used in the related datasheets or publications are also different. This renders difficult the comparison of the various EMFI platforms and the choice of the one adapted to its own usage. This paper suggests a characterization protocol which application is fast and requires equipment usually available in labs involved in security characterization. It also introduces an effective solution to enhance (by a factor 5) the timing resolution of EMFI platforms built around a commercial voltage pulse generator designed to drive 50 Ohm termination.

**Keywords:** EM Fault Injection · Secure IC design

## 1 Introduction

Electromagnetic Fault Injection (EMFI) is a quite recent injection technique which is becoming more and more popular. This is probably due to its inherent advantages among which the reduced preparation of samples required for its application. Initially suggested in [13] as a potential threat against secure circuits, it is only in 2007 that first convincing results were reported in [14].

Following these seminal works, numerous papers were published among which some [1–5, 7, 9, 10, 12] describe EMFI platforms. These platforms are usually classified into two categories: harmonic and pulsed. Soon after these publications, three companies started selling EMFI platforms or equipment, namely RISCURE, Langer and NewAE.

Unfortunately, when the time comes for someone to buy or design a pulsed EMFI setup, the choice among the whole available technical solutions is not easy to do. Indeed, solutions can be radically different and above all the characteristics and numbers reported in publications or data sheets differ in nature.

Within this context, the first contribution of this paper is to propose a simple characterization protocol of EMFI platforms which application only requires equipment usually available in all security characterization labs. The second contribution is to share the characterization results obtained following the proposed protocol for the two different EMFI platforms at our disposal : namely an EMFI platform from Langer company and a home made EMFI platform based on an Avtech pulse

generator similar to the one used in [12]. Finally, as a last contribution, this paper introduces a simple system to suppress signal bounces in the EMFI probe when using an Avtech pulse generator or any similar equipment.

## 2 State of the Art

Among all existing technical solutions to develop an EMFI setup, one can identify two main approaches. The first approach, followed by authors of [5, 10, 12], consists in using a commercial pulse generator to inject a high amplitude but short voltage pulse (for example provided by Avtech) into a commercial EM probe or a home made design probe [10, 12]. The main drawback of such an approach is that pulse generators are designed to drive $50\Omega$ loads while EM probes, especially home made probes, have a low impedance (about $1\Omega$). This impedance mismatch forces the voltage pulse in going back and forth between the probe and the generator. This limits the timing resolution of such EMFI platforms as explained in section 5 which also describes a simple solution to overcome this problem.

The second but more challenging approach is to develop its own pulse generator to ensure a perfect matching with the EM probe. This approach was followed by authors of [4] who introduced a low cost EMFI platform and used it to attack an ARM trusted zone. Authors of [1] also developed a low cost EMFI platform generating pulses up to $1.2kV$ and applied it to bypass the firmware protection of an IoT device. Another EMFI platform, called ChipShouter, is described in [8]. The latter was demonstrated efficient on two devices: a Trezor bit-coin wallet and a Solo Key open-source FIDO2 authentication key. Finally, in [2], authors describe another low cost EMFI platform and use it to perform a Piret's differential fault attack on an AES running on an ATmega328P microcontroller. A very interesting aspect in their paper is that they provide characterization results of their platform obtained by delivering EM pulses in a target made up of a flat coil and a $50\Omega$ resistance.

The main drawback of such a home made approach is the difficulty and the time required to design such a pulse generator. However this can be achieved as described in [1, 2, 4, 9]. This perfect impedance matching usually forces to have the EM probe very close to the pulse generator which can be viewed as a second drawback for the practice of EMFI. Indeed, drawing EMFI susceptibility maps requires in this case moving the probe and the generator.

Anyway, the above considerations are not sound reasons to choose a solution rather than another. Better reasons related to the performance of platforms are preferable. Analyzing carefully these publications, as well as the datasheets provided by Riscure NewAE and Langer companies, we have set Table 1. It lists different characteristics (among many others) of the available platforms. Among them, some are related to the voltage pulse generator: $V_{pulse}$ is the maximum amplitude of the voltage pulse generated by the platform at the input of the EM probe. It can be viewed as a figure of merit of the platform power. $PW$ is the width of the voltage pulse. It is a rough indicator of the timing resolution of the platform. $L$ is the latency between the triggering event and the deliverance of the EM pulse, a key parameter to perform double shoots on ICs. Other parameters are related to the EM probes among which $\Phi$ is the probe diameter, and core indicates the nature of the coil core. Finally, the last metric is the number of wire turns around the core which is usually a ferrite rod to enhanced the EM coupling with the target IC.

All characteristics reported Table 1 are related either to the pulse generator or to the EM probe. None of them is related to the generated EM pulse, i.e to the effective characteristics of the generated EM pulse. This observation has led us to the following question: what are the performance

Table 1: EMFI platform characteristics extracted from publications and datasheets. An enhanced AVRK4-B pulse voltage generator is considered for the avtech based plateform.

| EMFI plaform | Pulser characteristics | | EM probe characteristics | |
|---|---|---|---|---|
| SiliconToaster [9] | $V_{pulse}$ $(V)$ | 1200 | $\Phi$ $(\mu m)$ | 6600 |
| | $PW$ $(ns)$ | $NA$ | $core$ | $ferrite$ |
| | $L$ | $8ms$ | $\#$ $of$ $turns$ | 9 |
| ChipShouter [8] | $V_{pulse}$ $(V)$ | 500 | $\Phi$ $(\mu m)$ | 1000 |
| | $PW$ $(ns)$ | 20 | $core$ | $ferrite$ |
| | $L$ | $20ns$ | $\#$ $of$ $turns$ | NA |
| [2] | $V_{pulse}$ $(V)$ | 200 | $\Phi$ $(\mu m)$ | 1500 |
| | $PW$ $(ns)$ | $NA$ | $core$ | $ferrite$ |
| | $L$ | $120\mu s$ | $\#$ $of$ $turns$ | 6 |
| Avtech based [11] | $V_{pulse}$ $(V)$ | 750 | $\Phi$ $(\mu m)$ | 300-2000 |
| | $PW$ $(ns)$ | 6 | $core$ | $ferrite$ |
| | $L$ | $100ns$ | $\#$ $of$ $turns$ | 4-6 |
| Riscure | $V_{pulse}$ $(V)$ | 450 | $\Phi$ $(\mu m)$ | 1500-4000 |
| | $PW$ $(ns)$ | 50 | $core$ | $ferrite$ |
| | $L$ | $50ns$ | $\#$ $of$ $turns$ | NA |
| Langer | $V_{pulse}$ $(V)$ | 500 | $\Phi$ $(\mu m)$ | 300 |
| | $PW$ $(ns)$ | 2 | $core$ | $ferrite$ |
| | $L$ | $40ns$ | $\#$ $of$ $turns$ | NA |

metrics of an EMFI platform in view of the end application consisting in injecting reproducible and controllable faults?

## 3 EMFI objectives and figures of merit for EMFI characterization

According to [6], EMFI relies on the principle of EM induction and thus on Faraday's laws. More precisely and as illustrated Figure 1, the EM probe, which is a simple coil of inductance $L_P$, couples with the closed loops (of inductance $L_i^{IC}$) forming the power and ground grids of the target integrated circuits. This EM coupling creates in return several voltage transformers of mutual inductance $M_i \propto \sqrt{L_i^{IC} \cdot L_P}$ (one for each closed loop in the power and ground grid) between the pulse generator and the integrated circuits.

Consequently, applying a pulse at the input of the EM probe induces several (one in each closed loop of the power and ground grid) voltage pulses of lower amplitude in the power and ground grids of the IC. Still according to [6], because of the regular topology of the supply grids, these voltage pulses are of high amplitude only below the edge of the EM probe and of moderated amplitude below its core. Thus the spatial resolution of an EMFI is fixed by the diameter of the probe used. As a result, if the voltage pulse applied to the EM probe is of sufficient amplitude and width, transient faults occur below the edge of the probe. From the above, to be efficient, an EMFI platform must be tunable ($V_{pulse}$ and $PW$ must be finely controllable) and must of course generate:

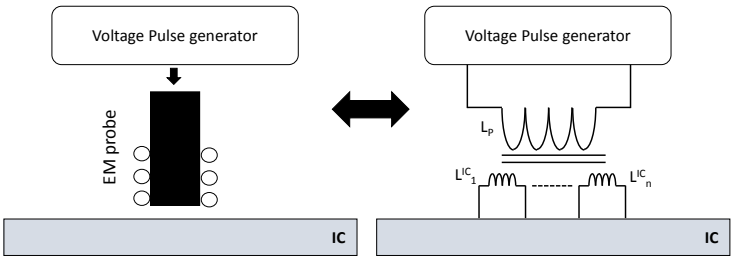


Fig. 1: Principle of EMFI

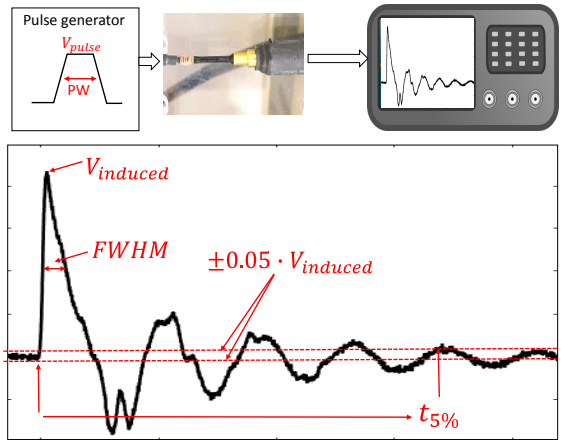


Fig. 2: Experimental setup and figures of merit for EMFI platform characterization or comparison

- the most powerful as possible electromagnetic pulse to inject faults in any device despite the evolution of CMOS technology leading to smaller and smaller closed loops in the power and ground networks,
- the shortest electromagnetic pulse as possible to address devices operating at low ($< 100MHz$) or high operating frequencies ($> 100MHz$) and therefore not corrupting too many instructions (or clock cycles) at a time.

We therefore propose to characterize and compare EMFI platforms by drawing the trends with respect to $V_{pulse}$ and $PW$ of the generated EM pulse and not to limit the characterization at the sole listing of the voltage generator and probe characteristics. This implies providing the trends with $V_{pulse}$ and $PW$ of:

- the maximum amplitude denoted afterward $V_{induced}$,
- the full width at half maximum ($FWHM$),
- and $t_{5\%}$ defined as the time spent to nearly vanish (measured at 5% of the $V_{induced}$)

of the voltage pulse induced in common reference coil, at contact of the EMFI probe, charged by a $50\Omega$ resistance, i.e. the input of a digital sampling scope in $DC50\Omega$ mode as illustrated Figure 2. At that stage, the resulting question is related to the choice of the reference coil. We do suggest to use a RF3mini probe from Langer because it is adapted to $50\Omega$ load, has a really large bandwidth ($30MHz$ to $3GHz$), is robust to high voltage transients, is cheap and available in most labs involved in security characterization.

## 4 Characterization results

The proposed characterization protocol was applied to the EMFI platform sold by Langer and to an Avtech based EMFI platform. Figure 3 gives, for both EMFI platforms, the trends of $V_{induced}$, $FWHM$ and $t_{5\%}$ with respect to $V_{pulse}$ for different $PW$ values.

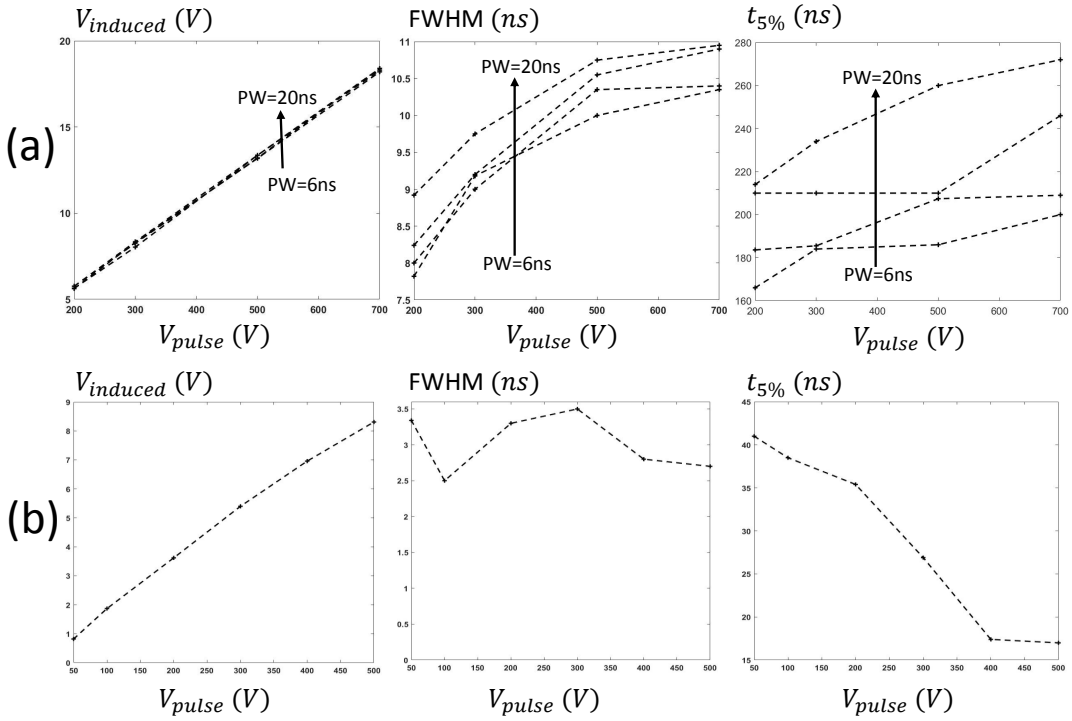


Fig. 3: $V_{induced}$, FWHM and $t_{5\%}$ versus $V_{pulse}$ for $PW \in \{6ns, 8ns, 10ns, 20ns\}$.(a) case of the considered avtech based platform. (b) case of the Langer EMFI platform.

The considered Avtech based EMFI platform features an enhanced AVRK4-B pulse generator generating in a $50\Omega$ resistance voltage pulses of amplitude ranging between $200V$ and $\pm 750V$ and of width ranging between $6ns$ and $20ns$. This enhanced generator also features two external trigger

inputs so that to generate, on the same output, two fully controllable and independent pulses. The delay $D$ between the external triggers and the pulses can be set between $100ns$ and $1s$; the minimal time separating the two pulses being equal to $100ns$. The jitter between the triggers and the pulses is equal to $\pm 100ps + 0.03\% \cdot D$. The EM probe is designed around a ferrite core with a diameter equal to $1000\mu m$. It has 5 spaced turns and a flat end.

The Langer platform generates voltage pulse of ampltude ranging between $50V$ and $500V$ to a EM probe also designed around a ferrite core. The pulse width can not be tuned and has fixed value equal to $2ns$. The jitter of the voltage generator is equal to $\pm 1ns$. Contrarily to our probe, it has a sharp end with a diameter equal to $500\mu m$ and the number of turns is not given in the datasheet.

Figure 3a, one can observe that the amplitude $V_{induced}$ of the perturbation induced in the Langer probe is independent of $PW$ and reaches $18V$ at $700V$. The induced current has thus a maximal amplitude of 0.36A since the input of the scope is set in $50\Omega$ mode. Contrarily to $V_{induced}$, the full width at half maximum varies from $7.8ns$ to $11ns$ with $PW$. This last observation holds for $t_{5\%}$. However, the values range from $160ns$ to $240ns$. This indicates a poor timing resolution of the EMFI platform which is due to the presence of bounces in the injected perturbation and thus to the aforementioned impedance mismatch between the generator and the probe. Figure 3b shows the same trends for the Langer EMFI platform except that there is only one curve by figure because the voltage pulse width is fixed. One can observe that the $V_{induced}$ ranges between $0.8V$ and $8.31V$. This is less than for the Avtech based platform. The full width at half maximum keep quite constant at a value close to $3n$ for all considered values of $V_{pulse}$. Concerning $t_{5\%}$, it decreases from 41ns downto 17ns when $V_{pulse}$ is increased.

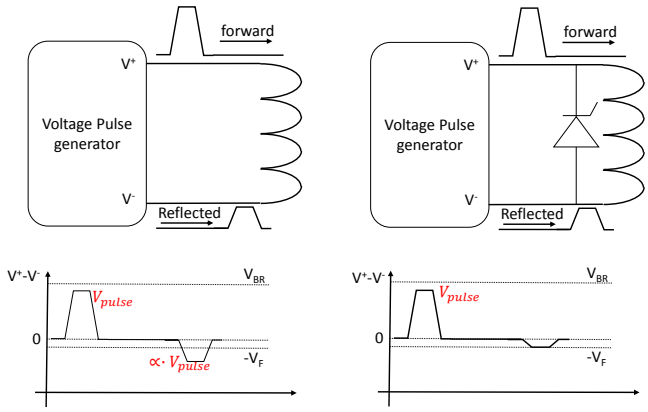


Fig. 4: Anti-bounces system based on a unidirectional transil diode

## 5 Anti-bounces system for EMFI platforms

To enhance the timing resolution of the Avtech based EMFI platform one can think of inserting a voltage transformer between the EM probe and the voltage generator. This is a classical solution

to solve impedance matching problems. Besides, this solution is proposed by Avtech. It consists in inserting the AVX-M4-H voltage transformer to adapt loads about $3\Omega$. However, even if this approach slightly reduces the number of significant bounces, it is not perfectly adapted since EM probes has an impedance below $1\Omega$. In addition, this transformer divides the amplitude of voltage pulse at the probe input by a factor two.

To solve this problem and consequently improve the timing resolution, we do propose to use a high speed unidirectional transil diode with high breakdown and clamping voltages ($V_{BR}$ and $V_{clamp}$ respectively) and a low forward threshold voltage $V_F$. This solution, which is not limited to Avtech voltage generators, allows suppressing all bounces between the voltage generator and the EM probe. It works as described by Figure 4.

As illustrated, when the triggering event occurs, a voltage pulse is generated on the $V^+$. This pulse propagates forward, goes through the EM probe and finally reaches $V^-$. Arrived at $V^-$ a fraction of the pulse is absorbed by the voltage generator and the remainder is reflected. This attenuated and reflected pulse goes through the EM probe and generates a bounce in the EM signal radiated by the probe which limits the timing resolution of the EMFI platform.

When an unidirectional transil diode is placed as shown Figure 4, the pulse propagating from $V^+$ to $V^-$ still gets across the EM probe if $V_{pulse} = (V^+ - V^-) < V_{BR}$ and an EM pulse is still emitted by the EM probe. However, the reflected pulse does not go across the probe and is dissipated by the transil diode if $\alpha \cdot V_{pulse} = (V^- - V^+) > V_F$. Indeed, in this case the diode starts conducting and thus shorts the EM probe. As a result, there is no bounce in the EM signal generated by the probe.

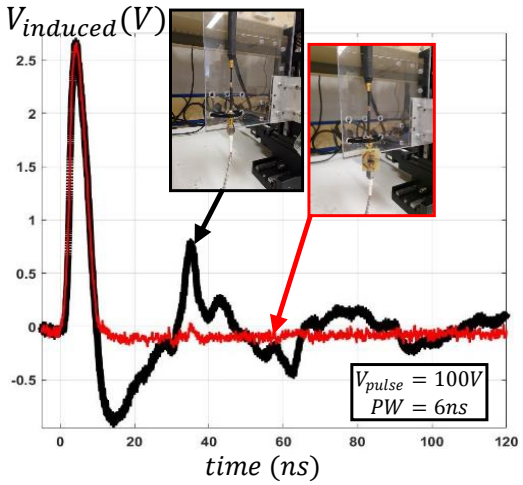


Fig. 5: Voltage induced in a RF3mini with and without the transil diode for a voltage pulse of amplitude and width equal to $100V$ and $6ns$ respectively.

We implemented this solution in a small PCB ($3cm \times 2cm$) that has to be placed at the input of the EM probe. The transil diode we used is an unidirectional $1.5KE600A$ from Littelfuse. Its characteristics are $V_{BR} = 570V$, $V_{clamp} = 860V$ and $V_F = 1V$. It can dissipate a pulse of power up to $1500W$ and has a fast response time equal to $1ps$. Figure 5 demonstrates the efficiency of this

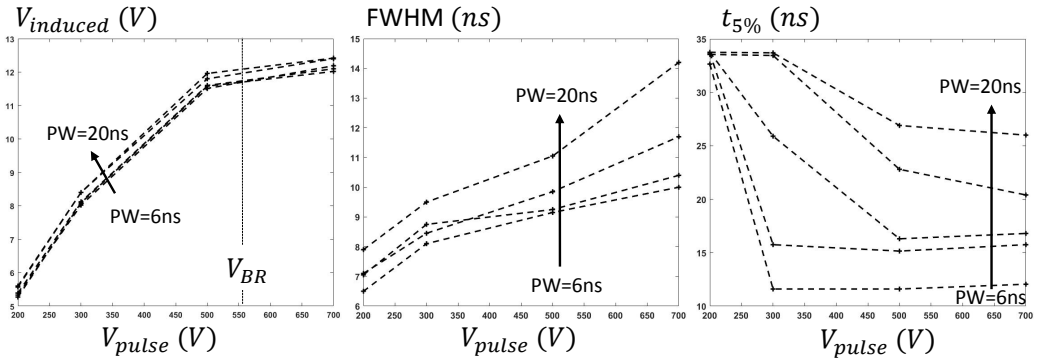


Fig. 6: $V_{induced}$, FWHM and $t_{5\%}$ versus $V_{pulse}$ for $PW \in \{6ns, 8ns, 10ns, 20ns\}$ for the Avtech based platform with the anti-bounced system.

solution by showing the voltage induced in an RF3mini probe with and without this anti-bounces system. One can observe the first pulse is fully transmitted whereas the followings are completely suppressed.

The characterization of the Avtech based platform with the proposed anti-bounces system was performed similarly to the previously described one. Figure 6 reports the trends of $V_{induced}$, $FWHM$ and $t_{5\%}$ with respect to $V_{pulse}$ for different $PW$ values. Comparing these results to those reported in Figure 3a, one can conclude that:

- the timing resolution ($t_{5\%}$) is enhanced by a factor about $\simeq 5$,
- the full width at half maximum remains nearly unchanged,
- there is no degradation of the EM pulse power for $V_{pulse} < V_{BR} = 560V$. However, there is a linearly (proportional to $V_{pulse} - V_{BR}$) increasing loss of power as soon as $V_{pulse}$ becomes greater than $V_{BR}$. However, this limited loss of power can be reduced or even suppressed using a transil diode with a higher breakdown voltage if it exists.

## 6 Conclusion

Several EMFI platforms are now available in the literature or as COTS equipment. Because characteristics reported in datasheets or publications are different in nature, this paper has suggested, as a first contribution, a characterization protocol which can be applied with cheap equipment usually available in labs involved in security characterization. Its originality consisting in characterizing platforms with attributes related to the EM induced perturbation rather than attributes of the equipment used to generate it. Its main advantages are its fast application and simplicity. The second contribution of this paper is an anti-bounces system. It allows increasing the timing resolution of EMFI platforms developed around COTS voltage generators (such as Avtech voltage pulse generators) by a factor about 5 according to our experiments. The last contribution is the sharing of performance metrics of two platforms. One of them is the EMFI platform sold by Langer company.

## References


1. Karim M. Abdellatif and Olivier Hériveaux. Silicontoaster: A cheap and programmable em injector for extracting secrets. Cryptology ePrint Archive, Report 2020/1115, 2020. https://eprint.iacr.org/2020/1115.
2. J. Balasch, D. Arumí, and S. Manich. Design and validation of a platform for electromagnetic fault injection. In 2017 32nd Conference on Design of Circuits and Integrated Systems (DCIS), pages 1–6, 2017.
3. Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In COSADE, pages 151–166, 2012.
4. Ang Cui and Rick Housley. BADFET: Defeating modern secure boot using second-order pulsed electromagnetic fault injection. In 11th USENIX Workshop on Offensive Technologies (WOOT 17), 2017.
5. Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, P. Orsatelli, Philippe Maurine, and Assia Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. IACR Cryptology ePrint Archive, 2012:123, 2012.
6. M. Dumont, M. Lisart, and P. Maurine. Modeling and simulating electromagnetic fault injection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pages 1–1, 2020.
7. Philippe Maurine. Techniques for em fault injection: Equipments and experimental results. In FDTC, pages 3–4, 2012.
8. Colin O'Flynn. Min()imum failure: EMFI attacks against USB stacks. In 13th USENIX Workshop on Offensive Technologies, WOOT 2019, Santa Clara, CA, USA, August 12-13, 2019, 2019.
9. Colin O'Flynn and Alex Dewar. On-device power analysis across hardware security domains. stop hitting yourself. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2019(4):126–153, 2019.
10. R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine. Magnetic microprobe design for em fault attackmagnetic microprobe design for em fault attack. In emceurope, 2013.
11. Sébastien Ordas, Ludovic Guillaume-Sage, and Philippe Maurine. EM injection: Fault model and locality. In 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2015, Saint Malo, France, September 13, 2015, pages 3–13, 2015.
12. Sébastien Ordas, Ludovic Guillaume-Sage, Karim Tobich, Jean-Max Dutertre, and Philippe Maurine. Evidence of a larger em-induced fault model. In Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers, pages 245–259, 2014.
13. David Samyde, Sergei P. Skorobogatov, Ross J. Anderson, and Jean-Jacques Quisquater. On a new way to read data from memory. In Proceedings of the First International IEEE Security in Storage Workshop, SISW 2002, Greenbelt, Maryland, USA, December 11, 2002, pages 65–69, 2002.
14. Jörn-Marc Schmidt and Michael Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results. In Johannes Wolkerstorfer Karl C. Posch, editor, Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings, pages 61 – 67. Verlag der Technischen Universität Graz, 2007.