HAL open science

(Adversarial) Electromagnetic Disturbance in the Industry

Arthur Beckers, Sylvain Guilley, Philippe Maurine, Colin O'Flynn, Stjepan Picek

▶ **To cite this version:**

Arthur Beckers, Sylvain Guilley, Philippe Maurine, Colin O'Flynn, Stjepan Picek. (Adversarial) Electromagnetic Disturbance in the Industry. IEEE Transactions on Computers, 2023, 72 (2), pp.414-422. 10.1109/TC.2022.3224373 . hal-03874307

HAL Id: hal-03874307

https://telecom-paris.hal.science/hal-03874307v1

Submitted on 27 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

(Adversarial) Electromagnetic Disturbance in the Industry

Arthur Beckers, Sylvain Guilley, *Senior Member, IEEE,* Philippe Maurine, Colin O'Flynn, *Member, IEEE,* and Stjepan Picek, *Senior Member, IEEE*

Abstract—Faults occur naturally and are responsible for reliability concerns. Faults are also an interesting tool for attackers to extract sensitive information from secure chips. In particular, non-invasive fault attacks have received a fair amount of attention. One easy way to perturb a chip without altering it is the so-called Electromagnetic Fault Injection (EMFI). Such attack has been studied in great depth, and nowadays, it is part and parcel of the state-of-the-art. Indeed, new capabilities have emerged where EM experimental benches are used to cryptanalyze chips. The progress of this "field" is fast, in terms of *reproducibility*, *accuracy*, and *number of use-cases*. However, there is too little awareness about such advances.
In this paper, we aim to expose the true harmfulness of EMFI (including reproducibility) to enable reasonable security quotations. We also analyze protections (at hardware/firmware/system levels) in light of their efficiency. We characterize the specificity of EM fault injection compared to other injection means (laser, glitch, probing).

Index Terms—Electromagnetic fault injection (EMFI), test benches, setup calibration, fault parameters identification, effectivity of fault countermeasures.

1 Introduction

Today, embedded security devices are widely used while various threats affect the security and privacy of our data. The attackers often aim at weaknesses in the implementations to obtain secret information, representing the core idea of implementation attacks. The focus is not on the algorithm itself but instead on exploiting some physical effects. Two well-known types of implementation attacks are side-channel attacks (SCAs) and fault injection (FI) attacks. Side-channel attacks are passive, non-invasive attacks where the attacked device operates within specified conditions, and the attacker observes the physical leakages produced by the device. Fault injection attacks are active, potentially invasive attacks where the attacker inserts faults to disrupt the normal behavior of the algorithm. They are considered serious by the industry and are inventoried in the "Common Weaknesses Enumeration" list (as CWE-1247 or CWE-1332 [1]). Fault injection is often possible through a variety of different techniques. Most of the employed techniques induce a current into the target device resulting in faulty behavior. This can, for instance, be achieved by introducing glitches in the clock or power supply rails [2] of the device, by exposing it to *electromagnetic fields* [3], and laser pulses [4].

Electromagnetic (EM) waves are naturally emitted by electronic chips, which can cause interference on other chips in the vicinity. This phenomenon can disrupt transceiver circuits, for instance. If the conducted or radiated emissions are sufficiently high, e.g., fields generated by motor drivers, even digital circuits are no longer immune and can be put into an erroneous state. Integrated circuits (ICs) are not only impacted by unintentional electromagnetic fields but can also be faulted through single event upsets (SEU) [5] caused by radiation. This can occur when chips are operated in harsh conditions like space applications or nuclear power plants.

Context

Attacks have been using these fault mechanisms to induce malevolent errors (see [6], [7]) into ICs. When electromagnetic fields are used as a fault injection mechanism, it is called EM fault injection (or EMFI).

The use of EMFI as a fault injection method is stimulated by various favorable factors, such as:

- the relative easiness and low operating cost of the setup,

- *A. Beckers is with imec-COSIC, KU Leuven, Belgium.*
- *S. Guilley is with Secure-IC and Télécom Paris, Institut Polytechnique de Paris, France.*
- *Ph. Maurine is with LIRMM, France.*
- *C. O'Flynn is with NewAE Technologies Inc. and Dalhousie U., Canada.*
- *S. Picek is with Radboud University, The Netherlands.*

This "position paper" results from a panel organized at the 21st Fault Detection and Tolerance in Cryptography (FDTC) IEEE conference, which has been held (virtually) on September 17th, 2021. The discussions addressed EM fault injection on a specific angle, attracting attention and motivating this article's write-up. The co-authors are the members of the panel.

- the semi-localized nature of the induced faults,
- no modification to the chip package is required, or
- the fact that this perturbation vector does not damage the chip irreversibly.

Thus, evaluation teams and research groups spent a fair amount of time developing EMFI injection setups and often resorted to EMFI when targeting various ICs. Based on the available testimonies [8], [9], [10], these attempts (after sustained efforts) to extract the secret data using EMFI have turned out to be successful in all cases.

The effectiveness of EMFI as a fault injection technique has been well established. There is, however, still a gap between the effectiveness of EMFI and the research done in the area of countermeasures to prevent this powerful attack vector. The gap can stem from the difficulty of implementing and proving the effectiveness of countermeasures, inappropriate assumptions of fault models, and the interaction between the abstraction layers one encounters in a security-centered design, e.g., on the software, firmware, or hardware level. These open questions shall nevertheless not refrain us from making an inventory of today's situation regarding EMFI.

Approach in this paper

This paper intends to explore this gap by understanding how no definite answer to the question of EMFI has emerged. Therefore, we report on a situation of relative failure; maybe the gap will narrow by better and more formal countermeasures, or maybe the gap will enlarge due to the development of a higher attack potential. It is hard to predict the future, but we can account in the article that, contrary to cryptography, whose security can be demonstrated based on hypotheses, the protection against EMFI is a *trade-off* where the goal is not to make attacks provably impossible but sufficiently costly to deter an attacker from investing time &money in this direction.

Contributions

This article aims to account for this state-of-the-art and perform a gap analysis. Our contributions are:

- to iterate that, no matter the target, one can inject faults into an IC with enough time and effort.
- to rate the balance between attacker and defender;
- to compare the strengths of EMFI relative to other fault attack methods.

Outline

In this respect, the rest of this paper is structured as follows. A primer on electromagnetic injection in the context of cyber-physical attacks is given in Sec. 2. The methodology to be deployed to calibrate a fault injection bench is discussed in Sec. 3, both post- and pre-silicon. Other perturbation methods exist. We discuss them in Sec. 4 and analyze their pros and cons. Protections do exist: they are surveyed and analyzed in Sec. 5. Finally, conclusions and perspectives are stated in Sec. 6.

2 EM Injection

A strong electromagnetic field being able to modify memory in a digital device (without permanently damaging the device) has been known since at least 1960s [11], [12]. Such fields may occur when devices are operated near high-power devices, causing random faults that could compromise a critical system, such as the engine controller on an automotive vehicle. From a safety perspective, we can see various countermeasures commonly applied (and often required to be applied by standards), such as error-correcting memory, multi-party voting, and hardening of devices [12].

Subjecting the entire device to electromagnetic fields may cause random errors, but from a security perspective, we often want to limit our errors to only occur in specific areas of the chip (such as an AES engine) or affect certain operations (such as a comparison). EMFI, when used for security analysis, differs in that the tooling allows very specific focusing of the energy in both time and space.

The fundamental objective of an EM injection platform is to generate a changing magnetic field to induce a voltage into structures on the IC surface [13]. Generating a changing magnetic field requires passing a current through a "coil" of wire. This coil has many parameters defining the dimensions, number of turns, and use of core material. The coil also needs a drive circuit capable of generating a suitable change in current within the coil. To understand where suitable parameters come from, we must consider the physical interaction of the various parameters.

These parameters include the voltage injected at nodes of the target device V_{inj}, the magnetic field generated by the coil at the target B_{inj}, the current through the coil I_{coil}, and the drive voltage applied across the coil V_{coil}. We will consider the parameters of the coil to include the number of turns N_{coil} and the inductance of the coil L_{coil}.

Here, we find some trade-offs inherent in the physics of the system. Trying to maximize V_{inj} means a larger magnetic field B_{inj} is required, which can be accomplished by increasing the current through the coil I_{coil}, or increasing the number of turns N_{coil}. Practical drivers cannot switch a current quickly but instead drive a given voltage V_{coil} onto the coil, which conducts a given current I_{coil}. Here, the maximum current I_{coil} is also limited

in practice, as the drive electronics become more complicated if we need to switch higher currents onto the coil. Nevertheless, if we simply try to increase N_{coil} to increase B_{inj} for a given current, we find that this also increases the inductance L_{coil}. Unfortunately, this means the same pulse of V_{coil} will now generate a smaller current I_{coil}, so there is a trade-off between our drive voltage, the number of turns of the coil, what "standard commercial electronics" can accomplish, and the resulting injected voltage V_{inj}.

Practically, the above distills down into a typical voltage in the range of 100 to 1 000 V, with pulse widths in the range of 1 ns to 1 000 ns. Such parameters will routinely appear in the examples of various EMFI tooling to be discussed.

2.1 Drive Architectures

Driving the injection coil can be broken down into two main categories: a *direct-drive* and a *coupled-drive* architecture. In a direct-drive architecture, a switching element (typically MOSFET or IGBT) directly switches a capacitor charged to a high voltage onto the coil. A coupled-drive architecture uses a coupling element such as a capacitor or transformer to couple the voltage pulse from the switching element onto the coil. This has the advantage of being inherently safe for the user since the coupling element prevents the output coil from being continuously energized. The downside is that maximizing the energy transferred to the output coil requires matching the output coil to the coupling mechanism. A detailed evaluation of this is given in [8].

Examples of the architectures and variations can be seen in published and available injection platforms. This includes platforms described in previous work such as [8], [9], [14], [15], [16].

2.2 EM Coils or Probes

The physical size and design of the EM coil (often referred to as a probe) naturally define the characteristic of the EM field injected into the target device [17]. As previously mentioned, this may interact with the driver when it comes to the amplitude and duration of the resulting field.

Typically probes are referred to by their diameter, which is the diameter of the EM coil itself or the core material diameter around which the coil is wrapped. Typically this probe may be in the range of 0.2–4 mm. If we consider that the EM coil is coupling to the power or ground grid of the IC die [13], a smaller diameter probe can be seen to impact a smaller area of the target IC. As it is also known that "ringing" on internal power rails results in faults [18], the link between the coupling on the power rails and the insertion of faults is well established.

Besides the geometry of the probe, the position itself also impacts the resulting waveform inserted onto the IC. Notably, the distance above the die of the IC is connected to the shape of the waveform, as bringing the probe closer to the die results in closer coupling between the EM coil in the probe and the IC [13]. The IC packaging will define the minimum distance if no device preparation is done. This is because, for most devices, the packaging will add some distance in the encapsulation material of the IC, which may be roughly in the range of 0.2–1 mm, depending on the package itself.

As an approximate rule of thumb, the maximum distance is around the diameter of the EM coil. This means that using very small probes may require thinning of the device package or even a full decapsulation [13], [19], [20]. This also means that larger diameter probes can inject faults without any device preparation at all, and in some cases, even directly through the product package itself [21].

The shape of the core and probes is not limited to simple classic coils or rods as described either. In particular, various more complex designs, including ferrite cores that come to a point [17], [20], crescent-shaped cores [20], and 3D printed structures have been demonstrated [22]. A sample of several probes is presented in Fig. 1.

Characterization of the platforms and probes can be used when comparing various tools [23], but in attack scenarios, a researcher works empirically towards a specific exploitation goal, using some of the techniques to be discussed in Sec. 3.

2.3 From Interference to Exploitation

The EM probe simply creates a large magnetic field around areas of the target, which is several steps removed from the actual goal of causing an unexpected behavior (the fault). As previously mentioned, the field induces voltage perturbations inside of the power nets on the target IC [13], which is known to cause timing violations resulting in faults [24], but it should be noted that EMFI is also capable of directly flipping bits in registers or static memory at rest [25].

The exploitation of the fault is not specific to EM faults, and many comprehensive backgrounds on this topic have been given [7], [26]. The objective of an attacker will vary widely, but real-world demonstrations have shown usage of EMFI to dump secrets from memory [21], bypass password checks in bootloaders [10], bypass code protection mechanisms in microcontrollers [14], and perform differential fault analysis [9], [16], [27]. The insertion of faults with EMFI can even be used to validate safety-critical systems [25].

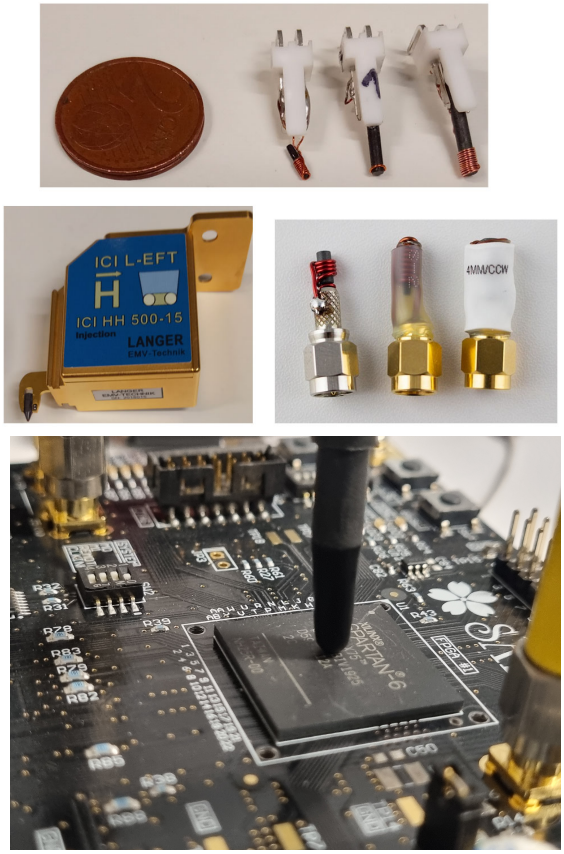

Figure 1. Example EM coils (or 'probes') including commercial & homemade examples (scales differ).

3 Methodology to Search for Effects

3.1 Post-silicon Methodology to Find Faults

Recall a fault injection attack can be considered successful if, after exposing the attacked device to external interference, the device shows an unexpected behavior, i.e., a fault that can be used by an attacker. The goal of an attacker is, therefore, to:

1) perturb any computation, be it data or control flow,
2) while the system does not crash, i.e., licit values can still be read out.

As a prerequisite, the attacker must devise a resilient setup specified to be able to restart afresh in case of a fault that crashes the system. Such a setup enables trial-and-error characterization campaigns. Building such a setup can be achieved by resorting to "off-the-shelf" appliances of dedicated professional sets of equipment.

Then, we can recognize two aspects of a successful fault injection attack. First, the attacker needs to find faults, and second, use those faults to break the system's security. While the latter aspect is application-specific (where sometimes one fault is sufficient [28], while in other settings, multiple faults are required [29]), the former can be considered from the perspective of the glitch source. For each glitch source, various parameters can lead to successful fault injection. For EMFI, commonly considered parameters are 1) the spatial position of the probe tip, 2) the moment when the EM pulse fires, 3) the pulse intensity, 4) the shape of the EM probe and the angle to the target, and 5) the shape of EM pulse concerning time. The process of finding useful faults is summarized in Fig. 2.

Finding faults in this search space can be a very challenging task. Common approaches include random search, grid search (with a specific step and considering a subset of parameters), and metaheuristics like evolutionary algorithms [30]. Unfortunately, an exhaustive search is practically impossible due to the time required to evaluate all options and the chances of breaking the target before the process is done. Interestingly, it can also be recognized that faults appear more often in certain (specific) regions, e.g., on the boundary between where the target responds in a normal way and resets. Additionally, exploitable faults are not necessarily obtained by pushing the parameters to the extreme. Still, we note that faults can manifest as singularities (i.e., separated from other faults, hence casually referred to as "sweet spots") or grouped in specific regions. We depict a target characterization for EMFI in Fig. 3. Thus, this shows that the comprehension of the EMFI phenomena is far from being fully mastered as of today.

Finally, we note that some recent advances suggest analyzing circuits not based on their functionality but based on the structure of their power plan [13]. Indeed, modern circuits are made up of a myriad of loops, each of which can be induced a current through the attacking probe.

3.2 Pre-silicon Fault Exploration

When occurring within the circuit, the fault behavior can be modeled abstractly. It is, therefore, possible to simulate or analyze the effect of different kinds of perturbations statically. The level of modeling shall be adapted to the threat. Let us give two extreme examples: high-level modeling of faults on RSA (for the Bellcore attack, [28]), medium level (which captures the pipeline of a processor), and accurate modelization faithful to physical phenomena (see [13]).

3.2.1 *Bellcore Attack*

The Bellcore attack refers to a Differential Fault Analysis (DFA), which is very specific to RSA [31]. When RSA uses its private key (e.g., while generating a digital signature), then the Chinese Remainder Theorem (abridged CRT) can be leveraged to expedite the computation. The first exponentiation uses the modulus p, while the second uses the

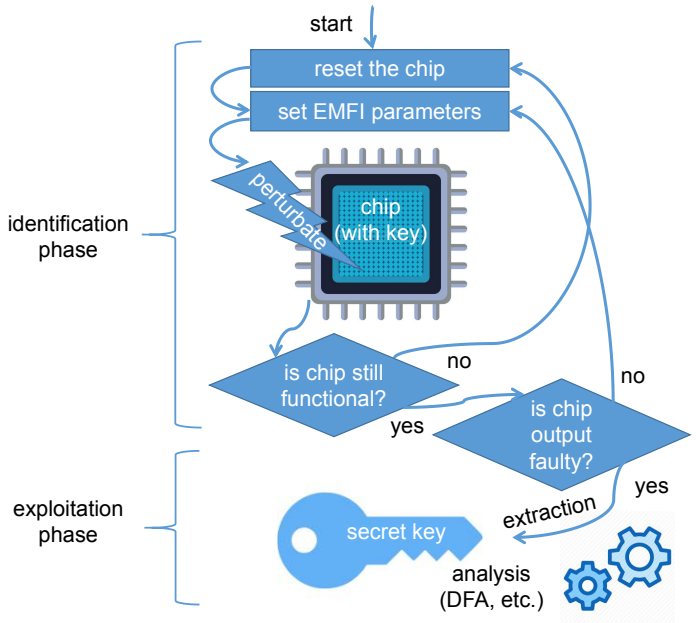

Figure 2. Process for useful faults *identification* and subsequent *exploitation*, during an EMFI campaign.

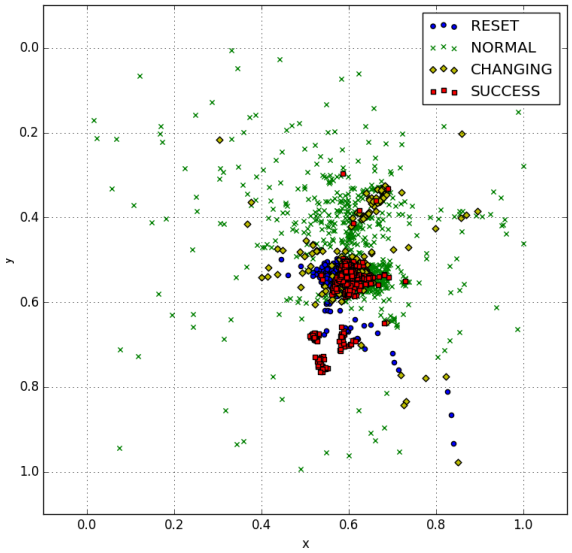

Figure 3. EMFI characterization example [30]. The experiment considers two parameters: x and y position (i.e., the spatial position of the probe). Note that the target can give four different responses once a perturbation is injected: 1) RESET - the target does not reply, requiring a reset, 2) NORMAL - the target responds normally, 3) CHANGING - repeating measurements give different responses, and 4) SUCCESS - the target response is faulty.

modulus q. D. Boneh, R.A. DeMillo, and R.J. Lipton (all three affiliated with the Bell Communications Research, nicknamed "Bellcore") show easy cryptanalysis consisting in recovering either prime factor p or q of $N = pq$ by collecting a valid signature and an erroneous one, obtained by the perturbation of one exponentiation. The attack consists in returning the greatest common divisor between the difference between correct and faulty signatures. Here, the exact nature of the fault does not matter as long as it does not affect both exponentiations simultaneously. Therefore, countermeasures have been designed and tested only by assuming a fault model, where a perturbation can either replace a value with a random one or by the constant zero. This simple and high-level method allowed to formally prove countermeasures as correct or as insufficient [32], [33].

3.2.2 Coarse Attack

A very simple example of a coarse attack is the corruption of solely one part of a CPU. For instance, the CPU can be forced to skip instructions, as discussed in [27]. The level of this model is "intermediate" in that the instructions to execute are now well known, though they must be evaluated timely.

3.2.3 Accurate Attacks on Sensors

Attacks can also be modeled at a very "low level". The rationale is to implement compact and stealthy sensors and model the EM field injected to bypass a multiplicity of randomly placed sensors. For in-

stance, such a setup is presented in the following attack paper [34].

4 Comparison between EM Injection and Other Injection Means

4.1 Other Fault Injection Means

We list here alternative fault injection means, which can compete with EM injection (see also [35]).

Glitches

It has been noted very early [7, §2] that perturbation of global signals, such as power, clock, or reset, could move the system into an unspecified state. Glitching stations generate inputs that violate the nominal operating conditions:

1) Power glitches cause a brownout;
2) Clock glitches result in overclocking;
3) Reset glitches, if fast enough, clear only some bits in the register states.

Laser fault injection

Laser fault has been pioneered by S. Skorobogatov [4]. Intense, focused light can accurately flip bits in registers or RAM cells. Access to the chip surface is required, however. Some chemical preparation is thus usually required to open the package and sometimes to polish or thin the chip (if attacked from the backside).

Body Biasing Injection

Similar transient or semi-persistent faults that are obtained with Electromagnetic interference perturbations can also be induced by a direct (adversarial) contact with a chip backside [36]. Indeed, the rearside (also known as "substrate") of chips is rarely protected, though they are naturally part of the attack surface. Body biasing injection (BBI) exploits this access without any need for an efficient EM coupling between a coil and the target IC thanks to direct electrical contact between a needle and the IC substrate. One may wonder if thinning the substrate is of interest. From an efficiency point of view, BBI does not necessarily require thinning the substrate to inject faults with a high spatial resolution since the latter depends both on the substrate thickness and the amplitude of the applied perturbation. However, thinning the substrate helps to mount more stealthy attacks by lowering the amplitude of voltage pulses required to induce exploitable faults.

4.2 Comparison

A comparison between EM fault injection and aforementioned perturbation techniques is carried out in Tab. 1.

The entries in this table are commented on below.

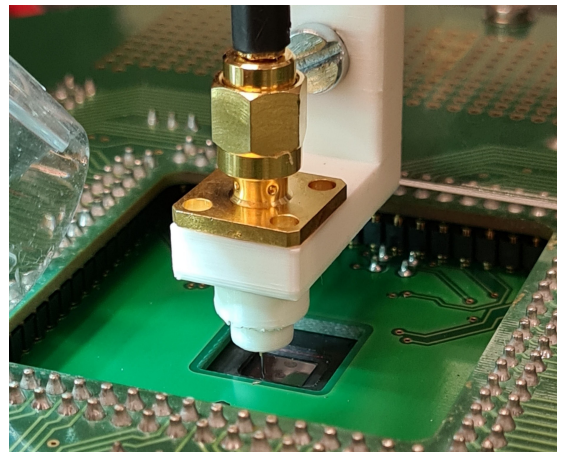

Figure 4. BBI needle at the contact of the substrate.

Equipment Cost

The cost comparison shows that EM falls somewhere between clock/voltage glitching and laser glitching. A wide range of equipment with different capabilities is possible, but if we assume equipment capable of accepting an input trigger (not just a simple spark-gap type pulse generator), the EM system requires more design effort than voltage or clock glitching.

Categorisation of Tools

The European Common Criteria (EUCC) scheme introduces a notion of equipment category, rated as either *standard*, *specialized*, or *bespoke*. This distinguisher gives the best practical approach considering the equipment availability (respectively procurement). It is highly correlated with the equipment cost.

Target Preparation

EM glitching is unique as it can be applied directly to a target system, including examples of EM glitching without opening the enclosure of a product [15], [21]. Clock, reset, and voltage fault injections require modification to the target PCB to connect the glitch apparatus. When using a very small coil or with BBI injection, some level of die thinning or decapping may be needed.

Tuning Parameters

The number of parameters to tune means an increased search space. An EM glitcher mounted on an XYZ stage presents five parameters to tune (glitch power, glitch width, and each X/Y/Z location). This search space is larger than with clock, reset, and voltage glitching. Then comes laser and BBI, which can be tuned with the same parameters except for the Z axis (hence a total of 4 tuning parameters). Voltage glitches have three parameters,

Table 1
Comparison between EMFI and other fault injection techniques.

Characteristic \ Medium	EM	Clock / reset glitch	Voltage glitch	Laser	BBI
Equipment Cost	\$100 – \$50 000	\$50 – \$5 000	\$5 – \$5 000	\$5 000 +	\$20 – \$5 000
EUCC Category	Specialized	Standard	Standard	Specialized	Specialized
Target Preparation	None to Medium	Low	Low	High	Low to Medium
Tuning Parameters	5	2	3	4	4
Spatial Precision	µm – mm	None	Discrete (power pins)	nm – µm	µm – mm
Temporal Precision	ns – µs	ns	ns – µs	ps	ns – µs

namely position in time, duration, and amplitude. Eventually, clock/reset glitches are only characterized by position in time and duration, because the amplitude is fixed by the core voltage.

Spatial Precision

The spatial precision of the EM glitch depends greatly on the physical coil used. This would not be expected to reach the same level as laser glitching, and performing operations such as glitching two locations on the same die may be difficult due to the physical size of the EM probes. BBI is typically mounted on the same XY table (no Z, since the probe is contacting the substrate) as EMFI. Hence, the spatial resolution is comparable, but the "conducted" effect of BBI is more localized than the "radiated" stress conveyed by EMFI.

Temporal Precision

Fundamentally, the EM injection can have high temporal precision depending on the actual injector design. Due to the magnetic coupling limiting the actual rate of change, generally, this will still be more limited than with laser fault injection.

5 Protections

5.1 Survey

Fault countermeasures can be implemented at different abstraction levels within a device. Classic redundancy-based countermeasures can be employed, which protect the program flow and guarantee data integrity [37]. These countermeasures can be employed at higher protocol levels or even at the logic level. Using a redundancy-based approach has the advantage of being effective against every fault injection method independent of the fault injection mechanism. The downside of this approach is that one has to ensure the implemented countermeasure captures all potential faults introduced into the system. Advanced attacks such as safe error attacks (SEA) [38] will, therefore, not always be detected or prevented by redundancy-based countermeasures.

EM fault injection can, however, also be detected by using a dedicated sensor-based approach. Here, two avenues can be taken. The first approach is integrating a magnetic field detector such as a sensor coil [39] into the IC. There, a coil is designed into the metal layers of the IC forming an LC circuit inside the IC. If the self-inductance of the coil is changed by the mutual inductance with the EM probe, an alarm is raised.

Another approach uses logic-based countermeasures, which detect the interaction between the EM-pulse and circuit-level components. In the literature, we can find several circuit-level detection strategies dedicated to protecting the IC against EMFI. N. Selmane et al. [40, Fig. 14, page 189], suggested inserting an artificial critical path that raises the alarm when violated (before the user logic gets faulty). Such digital sensors are refined by T. Anik et al. [41] to measure the amount of perturbation injected into the chip (an approach known as *time to digital conversion (TDC)*). The merit of TDC is that they can be implemented as register transfer level (RTL) with standard delay constraints (SDC), hence their great portability amongst various targets (FPGA or ASIC) and technology nodes. L. Zussa et al. [19] used glitch detectors to detect a phase difference and a guarding delay. When faulted, the phase shift between the clock period and the guarding delay element will cause an alarm to be raised. D. EL-Baze et al. [42] used self looped D-flip flops to detect setup and hold time violations. Four flip flops in different configurations are used in a single sensor to detect fault injections at different timings. The feedback loop of a phase-locked loop (PLL) is used by N. Miura et al. [43]. The PLL is routed such that it unlocks when targeted by EMFI. When unlocking of the PLL is detected, an alarm is raised. C. Deshpande et al. [44] used a redundancy-based approach where critical flip flops were duplicated to detect incorrect data being latched into the flip flop. J. Breier et al. [45] used a Hogge phase detector to detect phase errors in a ring oscillator as an EMFI detector.

5.2 Analysis

All sensor-based countermeasures discussed above can be implemented in standard Complementary Metal-Oxide-Semiconductor (CMOS) technology. Due to the locality of EMFI, some manual placement and routing will be required for all countermeasures. The most noticeable distinctions between the sensor-based countermeasures are the need for calibration, the area overhead, and whether or not they can detect other fault injection methods.

The listed sensors have all proven their effectiveness through experimental verification. It is, however, difficult to compare the effectiveness of one sensor approach to another because they were not evaluated using the same EMFI setup on the same target board or in the same CMOS technology. It is, therefore, nearly impossible to claim/prove one approach is more effective than another *per se*. This makes it difficult to compare the area of different sensor designs as one design might have a low area overhead for a single sensor cell but has a lower overall sensitivity and therefore requires significantly more sensor cells to be placed around the to-be-protected design. Our overview will therefore focus on whether or not the sensor requires calibration and the multi-functionality of the proposed sensor.

Three out of the seven discussed sensor designs do not require any tuning. These are the self looped D-flip flop based design [42], the design centered around the Hogge phase detector [45], and the flip flop duplication based approach [44]. Only the D-flip flop-based design advertises to be capable of detecting another fault injection method, namely BBI.

The other four sensor designs included in this overview must be tuned whenever implemented in new technology. However, all these sensors are capable to detect other physical attacks besides EMFI. The sensor coil-based approach [39] requires semi-automated routing of the sensor coil and tuning of the LC circuit. This sensor design can also detect local EM-measurement probes when they are placed near the IC. The time to digital detector [40] also allows to detect the targeted laser shots and can be used in *safety* applications. The glitch detector [19] approach requires the delay chain to be tuned for each technology and operating voltage. It is, however, also capable of detecting voltage and clock glitches. The PLL-based approach [43] requires, besides tuning, also a careful layout of the PLL routing. The approach is only evaluated for EMFI fault attacks but is likely to cover clock and voltage glitching besides EMFI. The sensor design characteristics are also listed in Table 2.

6 Conclusions and Perspectives

This work discusses electromagnetic fault injection (EMFI) as a real-world threat to the security of modern systems. First, we discuss electromagnetic injection principles, followed by examining different approaches to calibrating fault injection benches. We provide a comparison of EMFI and other fault injection techniques, emphasizing how realistic and expensive different fault injection attacks are. Finally, we discuss various countermeasures against such attacks.

As a perspective, we underline the need for pre-silicon fault verification. Indeed, finding out that a (produced) device is vulnerable to a fault injection attack is expensive as the device is already manufactured. Understanding what would be the influence of a perturbation on a device before it is produced could shorten the time between the design and release of the secure devices. Finally, we observe that artificial intelligence techniques are used in the FI domain, but much less than in some related domains like the side-channel analysis. In side-channel analysis, using machine learning has already become the de facto standard when deploying the most powerful attacks. There, the researchers investigate various techniques and constantly manage to improve state-of-the-art attacks. When considering fault injection, the results are much more sparse. As already discussed, there are some results with metaheuristics to characterize the target behavior. Additionally, we are aware of one work that uses deep learning for target characterization but with optical fault injection. Considering that the search space size one commonly encounters when using EMFI is huge, any speed-up would be significant. As the industry still commonly resorts to the random search for this task, more advanced (intelligent) techniques seem to be a natural approach to be investigated. Finally, since the target characterization is independent of the fault injection attack used, any improvements should be generic and applicable to fault injection techniques.

References

[1] MITRE, "2021 CWE Most Important Hardware Weaknesses," 2021, https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html.

[2] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," in *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, ser. WOST'99. USA: USENIX Association, 1999, p. 2.

[3] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES," in *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2012, p. 7–15. [Online]. Available: https://doi.org/10.1109/FDTC.2012.15

Table 2
Mainstream sensors design characteristics.

Countermeasure	Requires tuning	Also detects
Self looped D-flip flop based design [42]	×	–
Hogge phase detector [45] design	×	–
Flip flop duplication based approach [44]	×	BBI
Sensor coil-based approach [39]	✓	EM-measurement probes
Time to Digital Conversion (TDC) [40]	✓	Laser shots (See HOST'22 paper by Ebrahimabadi et al.)
Glitch detector [19]	✓	Voltage and clock glitches
PLL-based approach [43]	✓	Clock and voltage glitching

[4] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Ç. K. Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 2–12. [Online]. Available: https://doi.org/10.1007/3-540-36400-5_2

[5] T. May and M. Woods, "Alpha-particle-induced soft errors in dynamic memories," *IEEE Transactions on Electron Devices*, vol. 26, no. 1, pp. 2–9, 1979.

[6] J. A. Clark and D. K. Pradhan, "Fault injection: A method for validating computer-system dependability," *Computer*, vol. 28, no. 6, pp. 47–56, 1995. [Online]. Available: https://doi.org/10.1109/2.386985

[7] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370 –382, February 2006.

[8] A. Beckers, M. Kinugawa, Y. Hayashi, D. Fujimoto, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Design Considerations for EM Pulse Fault Injection," in *Smart Card Research and Advanced Applications - 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11-13, 2019, Revised Selected Papers*, ser. Lecture Notes in Computer Science, S. Belaïd and T. Güneysu, Eds., vol. 11833. Springer, 2019, pp. 176–192. [Online]. Available: https://doi.org/10.1007/978-3-030-42068-0_11

[9] M. Dumont, M. Lisart, and P. Maurine, "Electromagnetic Fault Injection : How Faults Occur," in *2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2019, pp. 9–16. [Online]. Available: https://doi.org/10.1109/FDTC.2019.00010

[10] C. O'Flynn, "BAM bam!! on reliability of EMFI for in-situ automotive ECU attacks," *IACR Cryptol. ePrint Arch.*, p. 937, 2020. [Online]. Available: https://eprint.iacr.org/2020/937

[11] J. D. Sabo and J. A. Karp, "Radiation circumvention technique," US Patent US4 413 327A, Nov., 1983. [Online]. Available: https://patents.google.com/patent/US4413327A/en

[12] A. Avižienis, "Design of fault-tolerant computers," in *Proceedings of the November 14-16, 1967, fall joint computer conference*, 1967, pp. 733–743.

[13] M. Dumont, M. Lisart, and P. Maurine, "Modeling and simulating electromagnetic fault injection," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 40, no. 4, pp. 680–693, 2021. [Online]. Available: https://doi.org/10.1109/TCAD.2020.3003287

[14] K. M. Abdellatif and O. Hériveaux, "SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets," in *2020 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2020, pp. 35–40.

[15] A. Cui and R. Housley, "BADFET: Defeating modern secure boot using second-order pulsed electromagnetic fault injection," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. Vancouver, BC: USENIX Association, 2017.

[16] 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)*, 2017, pp. 1–6.

[17] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine, "Magnetic microprobe design for em fault attack," in *2013 International Symposium on Electromagnetic Compatibility*, 2013, pp. 949–954.

[18] L. Zussa, J.-M. Dutertre, J. Clediere, and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2014, pp. 130–135.

[19] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria, "Efficiency of a glitch detector against electromagnetic fault injection," in *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2014, pp. 1–6.

[20] S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine, "Evidence of a larger em-induced fault model," in *CARDIS*, 2014.

[21] C. O'Flynn, "MIN()imum failure: EMFI attacks against USB stacks," in *13th USENIX Workshop on Offensive Technologies (WOOT 19)*. Santa Clara, CA: USENIX Association, aug 2019.

[22] J. Toulemont, G. Chancel, J. M. Galliere, F. Mailly, P. Nouet, and P. Maurine, "On the scaling of EMFI probes," in *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2021, pp. 67–73.

[23] O. Trabelsi, L. Sauvage, and J.-L. Danger, "Characterization at logical level of magnetic injection probes," in *2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility (EMC Sapporo/APEMC)*, 2019, pp. 625–628.

[24] L. Zussa, J.-M. Dutertre, J. Clédiere, B. Robisson, A. Tria *et al.*, "Investigation of timing constraints violation as a fault injection means," in *27th Conference on Design of Circuits and Integrated Systems (DCIS), Avignon, France*. Citeseer, 2012, pp. 1–6.

[25] C. O'Flynn, "EMFI for Safety-Critical Testing of Automotive Systems," in *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2021, pp. 61–66.

[26] M. Joye and M. Tunstall, Eds., *Fault Analysis in Cryptography*, ser. Information Security and Cryptography. Springer, 2012, ISBN: 978-3-642-29655-0; DOI: 10.1007/978-3-642-29656-7. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-29656-7

[27] L. Rivière, Z. Najm, P. Rauzy, J.-L. Danger, J. Bringer, and L. Sauvage, "High precision fault injections on the instruction cache of armv7-m architectures," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2015, pp. 62–67.

[28] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for

Faults," in *Advances in Cryptology — EUROCRYPT '97*, W. Fumy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51.

[29] N. Bagheri, N. Ghaedi, and S. K. Sanadhya, "Differential Fault Analysis of SHA-3," in *Progress in Cryptology – INDOCRYPT 2015*, A. Biryukov and V. Goyal, Eds. Cham: Springer International Publishing, 2015, pp. 253–269.

[30] A. Maldini, N. Samwel, S. Picek, and L. Batina, "Genetic algorithm-based electromagnetic fault injection," in *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 2018, pp. 35–42. [Online]. Available: https://doi.org/10.1109/FDTC.2018.00014

[31] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, feb 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[32] P. Rauzy, M. Moreau, S. Guilley, and Z. Najm, "A Generic Countermeasure Against Fault Injection Attacks on Asymmetric Cryptography," *IACR Cryptology ePrint Archive*, vol. 2015, p. 882, 2015. [Online]. Available: http://eprint.iacr.org/2015/882

[33] M. Dugardin, S. Guilley, M. Moreau, Z. Najm, and P. Rauzy, "Using modular extension to provably protect Edwards curves against fault attacks," *J. Cryptographic Engineering*, vol. 7, no. 4, pp. 321–330, 2017. [Online]. Available: https://doi.org/10.1007/s13389-017-0167-4

[34] D. Poggi, P. Maurine, T. Ordas, and A. Sarafianos, "Protecting Secure ICs Against Side-Channel Attacks by Identifying and Quantifying Potential EM and Leakage Hotspots at Simulation Stage," in *Constructive Side-Channel Analysis and Secure Design - 12th International Workshop, COSADE 2021, Lugano, Switzerland, October 25-27, 2021, Proceedings*, ser. Lecture Notes in Computer Science, S. Bhasin and F. D. Santis, Eds., vol. 12910. Springer, 2021, pp. 129–147. [Online]. Available: https://doi.org/10.1007/978-3-030-89915-8_6

[35] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012. [Online]. Available: https://doi.org/10.1109/JPROC.2012.2188769

[36] P. Maurine, K. Tobich, T. Ordas, and P. Y. Liardet, "Yet Another Fault Injection Technique : by Forward Body Biasing Injection," in *YACC'2012: Yet Another Conference on Cryptography*, Porquerolles Island, France, Sep. 2012. [Online]. Available: https://hal-lirmm.ccsd.cnrs.fr/lirmm-00762035

[37] N. Theißing, D. Merli, M. Smola, F. Stumpf, and G. Sigl, "Comprehensive analysis of software countermeasures against fault attacks," in *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2013, pp. 404–409.

[38] S.-M. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," *IEEE Transactions on Computers*, vol. 49, no. 9, pp. 967–970, Sep 2000.

[39] N. Miura, D. Fujimoto, M. Nagata, N. Homma, Y. Hayashi, and T. Aoki, "EM attack sensor: Concept, circuit, and design-automation methodology," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1–6.

[40] N. Selmane, S. Bhasin, S. Guilley, and J.-L. Danger, "Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks," *IET Information Security*, vol. 5, no. 4, pp. 181–190, December 2011, DOI: 10.1049/iet-ifs.2010.0238.

[41] M. T. H. Anik, J.-L. D. Danger, S. Guilley, and N. Karimi, "Detecting Failures and Attacks via Digital Sensors," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1315–1326, 2021. [Online]. Available: https://doi.org/10.1109/TCAD.2020.3020921

[42] D. Elbaze, J.-B. Rigaud, and P. Maurine, "An Embedded Digital Sensor against EM and BB Fault Injection," in *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE Computer Society, 08 2016, pp. 78–86.

[43] N. Miura, Z. Najm, W. He, S. Bhasin, X. T. Ngo, M. Nagata, and J.-L. Danger, "PLL to the Rescue: A Novel EM Fault Countermeasure," in *Proceedings of the 53rd Annual Design Automation Conference*, ser. DAC '16. New York, NY, USA: Association for Computing Machinery, 2016. [Online]. Available: https://doi.org/10.1145/2897937.2898065

[44] C. Deshpande, B. Yuce, L. Nazhandali, and P. Schaumont, "Employing dual-complementary flip-flops to detect EMFI attacks," in *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2017, pp. 109–114.

[45] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using Hogge phase-detector," in *2017 18th International Symposium on Quality Electronic Design (ISQED)*, 2017, pp. 307–312.

Arthur Beckers received his PhD in 2021 at the COSIC (Computer security and industrial cryptography) research group of the department of Electrical Engineering within the KU Leuven, Begium, under the supervision of prof. Ingrid Verbauwhede. His research interests are fault attacks on cryptographic implementations and side-channel analysis.

Sylvain Guilley is General Manager and CTO at Secure-IC, a French company offering security for embedded systems. Sylvain is also an adjunct professor at Télćom-Paris and a research associate at École Normale Supérieure (ENS). Sylvain received his M.Sc. from École Polytechnique and his Ph.D. from Télécom-Paris. His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal / mathematical methods.

Sylvain is also lead editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of non-invasive testing tools), and ISO/IEC TR 24485 (White Box Cryptography). Sylvain is associate editor of the Springer Journal of Cryptography Engineering (JCEN). He has co-authored 350+ research papers and filed 40+ invention patents. He is a member of the IACR, a senior member of the IEEE, and the CryptArchi club.

Philippe Maurine received the M.Sc. and Ph.D. degrees in electronics from the University of Montpellier, Montpellier, France, in 1998 and 2001, respectively. Since 2003, he has been an Associate Professor with the Laboratory of Informatics, Robotics, and Microelectronics, University of Montpellier, developing microelectronics in the engineering program of the University. His current research interests include adaptive system-on-chip design, secure IC design, secure embedded software, side-channel analysis, and fault injection techniques.

Colin O'Flynn is CTO at NewAE Technology Inc, along with an adjunct professor at Dalhousie University in Halifax, Canada. He received his PhD in 2017, and from 2018 to 2021, was an assistant professor at Dalhousie University before shifting to industry. He started the ChipWhisperer project, which brings accessible tooling for side-channel power analysis and fault injection to a wide variety of users, including those in both academia and industry.

Stjepan Picek is an associate professor at Radboud University, The Netherlands. He received his PhD in 2015. From 2015 to 2017, he was a postdoctoral researcher at KU Leuven, Belgium and MIT, USA, and from 2017 until 2021, an assistant professor at the Delft University of Technology, The Netherlands. His research interests include security, machine learning, and evolutionary algorithms.