

Design Considerations for EM Pulse Fault Injection

Arthur Beckers¹, Masahiro Kinugawa², Yuichi Hayashi³, Daisuke Fujimoto³,
Josep Balasch¹, Benedikt Gierlichs¹, and Ingrid Verbauwhede¹

¹ imec-COSIC KU Leuven, Belgium

² National Institute of Technology (KOSEN), Sendai College, Japan

³ Nara Institute of Science and Technology, Japan

¹{*firstname.lastname*}@esat.kuleuven.be, ²kinugawa@sendai-nct.ac.jp,
³{yu-ichi,fujimoto}@is.naist.jp

Abstract. Electromagnetic-fault injection (EM-FI) setups are appealing since they can be made at a low cost, achieve relatively high spatial resolutions, and avoid the need of tampering with the PCB or packaging of the target. In this paper we first sketch the importance of understanding the pulse characteristics of a pulse injection setup in order to successfully mount an attack. We then look into the different components that make up an EM-pulse setup and demonstrate their impact on the pulse shape. The different components are then assembled to form an EM-pulse injection setup. The effectiveness of the setup and how different design decisions impact the outcome of a fault injection campaign are demonstrated on a 32-bit ARM microcontroller.

Keywords: EM fault attack · probe design · EM-FI setup

1 Introduction

Since the introduction of the Bellcore attack by Boneh et al. [3] many different fault injection methods have been developed [2]. These fault injection methods are often classified according to their invasiveness and locality. Techniques such as clock and voltage glitching introduce global faults into the chip, but do not require tampering with the chip package or the chip itself. Therefore they are labeled as non-invasive and global. On the other side of the spectrum, optical fault injection [12] is a (semi-)invasive technique that requires line of sight to the target IC. In return, it can achieve high locality and potentially affect only a few transistors.

EM-fault injection [11] can be situated somewhere in between. It involves exposing the target IC to a pulsed or continuous E or H-field, or a combination of both. The injected field couples with the wiring of the IC, inducing voltage and current fluctuations inside the device. Since the EM-field can propagate through the package of the IC, the method can be labeled as non invasive. In some situations, however, removing the package might be beneficial. It can increase the resolution of the attack and the field strength received by the IC. This makes

EM-FI applicable also in (semi-)invasive settings. If the spatial dimensions of the injected field are sufficiently small compared to the size of the IC, only a smaller portion of the IC is affected. This gives EM-fault injection a certain degree of locality. Alternatively, EM-FI can achieve global effects by targeting bonding wires or PCB traces. This can be seen as a “contactless” voltage or clock glitching.

Related Work. EM-FI comes in two variants. One can either inject a continuous (harmonic) EM-wave or a single EM pulse. In this work we focus on the latter. More specifically, we investigate how different design decisions impact the pulse shape generated by an EM-pulse generator. In a previous work by R. Omarouayache et al. [9] a detailed study was done on how different probe parameters impact the size and shape of the generated magnetic field. The authors investigated the effect of different parameters by simulating the probes using a 3D EM simulator. In this work, we take their design recommendations into account and perform empirical testing of various probes when integrated into a complete EM-pulse injection setup.

Setups to perform EM-pulse injection have been described in the academic literature [7]. Most works use experimental setups around commercial high-voltage pulse generators, capable of generating pulses up to 500 V and 5 ns width. Using such a setup, Ordas et al. [10] compare different type of handmade injectors (flat, sharp, crescent) when targeting an FPGA platform. Alternative designs include the BADFET by Cui and Housley [4] and the setup designed by Balasch et al. [1]. The former uses a similar circuitry as the one described in this paper, storing the energy released over the EM probe in a capacitor bank, but use rather large probes in the order of centimeters. The latter setup uses a different approach, in which the energy released to the EM probe is stored in a large inductor.

In addition to academic literature, there exist several commercial solutions available for EM-FI such as the NewAE’s ChipSHOUTER ⁴, Riscure’s EM-FI Transient Probe ⁵ or Langer EMV’s ICI Set ⁶. For most of these setups, the circuitry used for pulse generation is not public information. The only commercial solution for which the circuit diagram is available is the ChipSHOUTER, which uses a similar approach to the one we use in this work.

Contributions. The goal of this work is not to propose a new EM-FI setup and compare it to existing solutions. Rather differently, we aim to investigate how different components of an EM-pulse injection setup impact the shape of the generated pulse. We start by studying the impact of the probe design parameters. For this, we propose a measurement method based on a microstrip line to measure spatial and temporal characteristics of the probes. After the different parameters that impact the pulse shape are established, we describe a set of design guidelines by building an EM-pulse fault injection setup and demonstrating its effectiveness on a 32-bit microcontroller.

⁴ <http://store.newae.com/chipshouter-kit>

⁵ <https://getquote.riscure.com/en/quote/2101068/em-fi-transient-probe.htm>

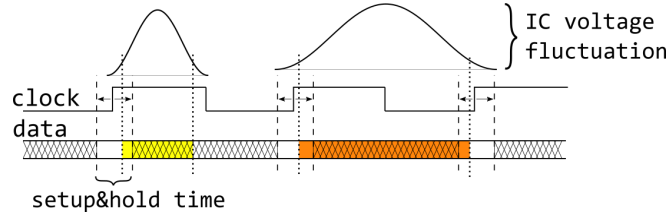
⁶ <https://www.langer-emv.de/en/category/ic-side-channel-analysis/94>

2 Challenge

Building an EM-pulse injection setup is conceptually simple. One needs to interface a pulse generator with an injection probe. Both components are commercially available, or they can be constructed. In any case, the shape of the generated EM pulse is determined by the choice of these components. In turn, the success rate of a fault injection campaign depends strongly on the characteristics of the pulse. Thus correctly tailoring the pulse parameters to the target device might have a significant impact on the outcome of a fault injection campaign. If we have a setup capable of generating small pulse widths, we can for example target individual instructions at high clock frequencies. Or if we have a larger pulse width, we might fault multiple instructions simultaneously.

Fault models for EM-fault injection have been described by Ordas et al. [10] for FPGAs and by Moro et al. [8] for microcontrollers. Both studies conclude that EM-pulse injection causes violations of the setup and hold times of the IC. Therefore pulses must be injected around a clock edge in order to be effective. The voltage and current fluctuations caused by the EM-pulse result in an incorrect sampling of the data at the input of a flip-flop during the setup or hold time. How these induced voltages and currents propagate through a particular IC requires extensive testing or detailed EM-simulations. This aspect has been recently investigated by Dumont et al. [5], which model the interactions between EM probes, EM pulses and ICs to gain understanding on the occurrence of EM faults.

Intuitively, we can abstract the concept to the following: an IC will be faulted if a clock edge occurs when voltage and current fluctuations exceed a certain threshold. The time window ($t_{sensitive}$) during which the induced voltage and current fluctuations persist on the device, depends on a multitude of parameters. $t_{sensitive}$ can, for instance, be enlarged by increasing the pulse width, by injecting multiple pulses in rapid succession, or by increasing the size of the injected field. The ratio between the time window during which we can fault an operation and the clock period (t_{clock}) determines whether we affect one or multiple clock cycles. We call this ratio the fault sensitivity ratio (FSR) expressed as $FSR = t_{sensitive}/t_{clock}$. If the FSR is larger than 1, one can fault multiple clock cycles simultaneously. If the FSR is smaller than 1, one is able to fault a single clock cycle. The time $t_{sensitive}$ is determined by both the target device and the EM-FI pulse characteristics, as illustrated in Figure 1. The value $t_{sensitive}$ equals the sum of the setup and hold time of the device plus the pulse width. This is a simplification of the actual fault mechanism, but it gives a good intuition on how different pulse characteristics influence the outcome of EM-pulse injection. In practice, a per device study should be done to investigate how $t_{sensitive}$ relates to the pulse shape. The value t_{clock} on the other hand is fixed by the clock frequency of the target device, which may not be controllable by an adversary. By changing the pulse characteristics, we can thus tune the FSR depending on the application. A high FSR might for instance be desired when a device is profiled for its sensitivity to EM-pulse injection, while an FSR lower than 1 might be preferable when performing an attack.

Fig. 1: Illustration of the fault sensitivity ratio (FSR).

3 Probe design

In this section we examine the impact different probe parameters have on the pulse characteristics. In what follows we only consider H-field probes, although in theory also E-field probes could be used for performing EM-fault injection. H-field probes are commonly constructed by winding conductive wiring around either an air or ferrite core, thus forming a solenoid. The pulses generated by an EM-FI setup generally have a rise-time in the nanosecond range. We are thus operating in the near-field since the probes are commonly placed within a few centimeters of the target device. Different relations apply when the probes have a higher rise time or are placed further away from the target.

3.1 Near-field coupling

In the near-field region, currents induced into a target device are the result of coupling between probe and device. Generally, the pulse generator can be modeled as a charge capacitor in combination with a switching element. An EM-pulse is generated by discharging the capacitor through the injection probe. This model is equivalent to an RLC circuit if we assume an ideal switch. A diagram of such a circuit can be seen in Figure 2. Before pulse injection, the capacitor is charged to a high DC voltage. Once charged, the switch is closed and current starts flowing through the inductor. Due to coupling between the IC and the probe, a current will be induced in the wiring of the target device. The amount of current will depend on the shape of the H-field pulse and on the wire geometry of the target device. Thus, once placed above an IC, the load seen by the pulse generator will be that of the coupled inductors. The amount of coupling between the probe and device will be frequency dependent. The resistor in the RLC model combines both the parasitic resistance of the probe and resistance added for damping the response.

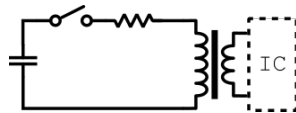


Fig. 2: Model of EM-pulse injection circuit.

By solving the differential equation of the RLC circuit we can get a basic understanding of how different parameters influence the pulse shape. There are three possible solutions to the differential equation depending on the damping of the RLC circuit. Ideally we would like our EM-injection setup to be critically damped. Over-damping would increase our pulse width, while under-damping will result in ringing. The different current equations to resulting from the differential equation can be found in Appendix A. Since the magnetic field generated by the probe is proportional to the current flowing through it, we can derive some of the pulse characteristics from the current equations (Appendix A).

The rise time, peak amplitude and pulse width will be determined by the resistance, the initial voltage over the capacitor and the probe inductance. The resistance and the initial voltage are two parameters which can generally be chosen freely by the designer. The inductance on the other hand is determined by the probe geometry. Equation 1 gives the inductance of an ideal solenoid. Here k is the relative permeability, μ_0 is the permeability of free space, N is the number of windings, A is the loop area and l is the length of the solenoid. The actual probe will have a different inductance because of parasitics, saturation of the ferrite core, etc. but the equation gives us the basic relationship between the different variables that make up the probe inductance.

$$L = \frac{k\mu_0 N^2 A}{l} \quad (1)$$

The size of the magnetic field at the center line of the solenoid resulting from the current flowing through the probe is given by Equation 2. Here r is the radius of the probe and z is the distance along its axis. The bottom of the solenoid is situated at $z = 0$ while the top is located at $z = l$. From Equations 4 and 1 we can see that the size of the magnetic field is inversely proportional to the inductance of the probe. By varying the different parameters we can tune the pulse characteristics to our needs.

$$B = \frac{k\mu_0 N}{2l} I \left[\frac{z}{\sqrt{z^2 + r^2}} - \frac{z - l}{\sqrt{(z - l)^2 + r^2}} \right] \quad (2)$$

Another approach for modeling the impact of different parameters on the generated field is by simulating the RLC circuit in SPICE, which allows for a more accurate modeling of the circuit.

3.2 Experimental validation

In order to confirm that the theoretical relations from the previous section hold, we performed experimental measurements on solenoid probes with different winding geometries. To this end, we built a test setup similar to the circuit in Figure 2. Instead of an ideal switch, we used a gas discharge tube with a breakdown voltage of 370 V. This component is selected because of its high rise time and small parasitics, which makes its behaviour similar to that of

an ideal switch. For our experiments, the capacitor was connected to a 400 V power supply through a current limiting resistor of 1 M Ω . Once the capacitor voltage reaches 370 V, breakdown occurs and a current flows through the probe generating a magnetic pulse. Our test setup is shown in Figure 3.

The evaluated probes were made with ferrite rods produced by Fair-Rite ⁷. The windings around the ferrite core were made using enameled wire with a thickness of 150 μm . We only used rods, and no other special geometries such as sharpened tips were tested. These special geometries could however improve the magnetic field characteristics as observed in [9]. The default configuration of our evaluation board has a 47 pF charge capacitor, a probe with 2 windings and a 2 mm ferrite core.

For the probe evaluation we used a 50 Ω microstrip line to measure the H-field pulse. It was made from a 0.3 mm thick dual sided FR-4 substrate with a copper thickness of 18 μm and dielectric constant of 4.7. The resulting width of the microstrip line was 0.532 mm for a 50 Ω line. At either end, the microstrip line was terminated by a 50 Ω impedance. The PCB dimensions were 14 cm wide and 24 cm long. The board was chosen to be as thin as possible to have a narrow 50 Ω stripline, which is beneficial for measuring the spatial resolution. The length of the board was chosen as large as practically feasible, in order to have a larger temporal separation between the reflection that might occur due to small impedance mismatches and the actual pulse. In order to measure the response of the probe, we mounted the evaluation board on a stepper table with a 15 μm step size. The probe was placed on top of the PCB and moved perpendicular to the microstrip line. The theoretical result of a microstrip line measurement for an H-field pulse are shown in Figure 4. When the centerline of the probe is placed on top of the middle of the microstrip line the measured field will be zero, since the magnetic field to either side of the microstrip line will be equal. Once the probe is moved away from the center of the microstrip line, a net magnetic field will be measured and the peak amplitude of the response will increase up to the point *Re*. At the point *Re*, we measure the maximal peak amplitude response *Am* of the probe. When time domain responses are given for a probe, they are taken at the point *Re*. The distance between the middle of the microstrip line and *Re* is also taken as a measure for the resolution of the probe.

The microstrip line was chosen as measurement method since besides the temporal characteristics of the probe it can also be used to evaluate its spatial resolution. An alternative method is to use loop antennas, but these can not capture the spatial resolution of the probe. In order to determine the minimal field strength required to fault the intended target, it should be mounted on a test board and profiled for its EM-pulse sensitivity. However, this approach has its limitations for probe characterization. First, the result will not only depend on the probe characteristics but also depend heavily on the used target IC. And second, spatial resolution might be hard to establish using an IC as profiling device given that the induced currents might propagate through the entire IC

⁷ <https://www.fair-rite.com/products/engineering-kits/?kit=21558>

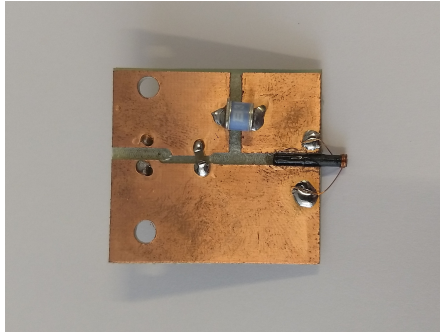


Fig. 3: Gas discharge tube based EM-probe evaluation circuit.

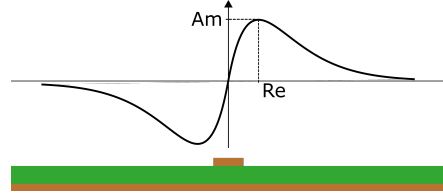


Fig. 4: Microstrip line response.

depending on the internal routing. Therefore we opted to use a microstrip line as evaluation method. It should be noted however, that when an IC is targeted the frequency dependency of the coupling between probe and IC might give significant performance differences between different probes. Ideally, the transfer characteristic of an IC should first be measured and the probe should be designed accordingly. This is however outside the scope of this work.

3.3 Results

In what follows we experimentally analyze the influence several parameters in the design have on the pulse shape. All measurements are done using a Tektronix DPO7040C scope with 25 GS/s sample rate and a 6 GHz bandwidth. The input impedance of the scope is set to 50 Ohm.

Ferrite material. When large magnetic fields are induced into ferrite materials they will saturate. This saturation causes them to behave non-linearly, which makes simulating the impact of the chosen ferrite on the pulse shape difficult unless exact data is delivered by the manufacturer. The pulse shape was measured using three different ferrite materials made by the same manufacturer. They are all marketed for RF applications. The three materials have a different frequency rating and permeability. The permeability of the first ferrite material, material 78 is 2000 H/m and has its pole at 1 MHz. The second material, material 61 has a permeability of 110 H/m and has its pole at 20 MHz. Lastly, material 67 has a permeability of 40 H/m and a pole at 100 MHz. The probe responses for each material are depicted in Figure 5. The plot clearly shows that the used ferrite material has a significant impact on the pulse response, e.g. the pulse magnitude of material 61 is more than 50% larger than material 67. In the rest of our experiments we use material 67. Although the pulse has the smallest amplitude response, the material is designed to operate at high frequencies making it unlikely to be the limiting factor for the rise time of our probe.

Number of windings. The inductance is expected to rise quadratically with the number of windings. Thus according to Equation 5, we expect the pulse amplitude to decrease with the number of windings. Since also the damping of the circuit depends on the inductance, we further expect the pulse width to increase with the number of windings. The magnetic field however linearly increases with the number of windings and thus compensates slightly for the decrease in current amplitude. Figure 6 shows the pulse response measured at position Re for variations in the number of windings. It behaves as expected.

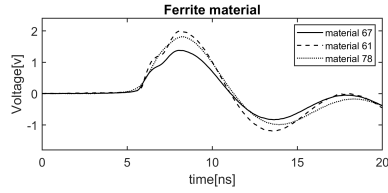


Fig. 5: Pulse response for different ferrite materials.

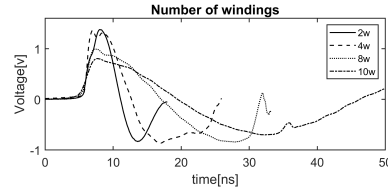


Fig. 6: Pulse response for different number of windings.

Core diameter. Increasing the core diameter will reduce the amplitude of the pulse, since both the inductance (Equation 1) and magnetic field (Equation 2) depend on the solenoid radius. In this experiment we are however more interested in the probe resolution. We varied the probe diameter and measured the spatial characteristics of the probe. The results can be seen in Figure 7. As shown in the plot, the distance between the peak amplitudes Re varies linearly with the probe diameter. Note that for our experiments we used rather large probe diameters, ranging from 1 to 4 mm. These diameters were chosen out of practical considerations, being one of the few sets commercially available. Using a probe with a large diameter to target an IC might not be ideal, since the current induced in the IC is proportional to the magnetic field difference around the wiring.

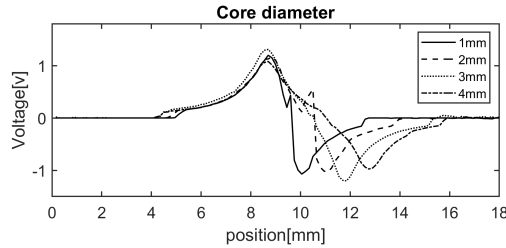


Fig. 7: Pulse response for different solenoid diameters.

Winding geometry. A final probe parameter which can be varied is the length of the solenoid. There are two strategies which can be employed. Either the wire thickness can be reduced or windings can be overlapped. Reducing the wire thickness increases the resistance of the wire. The increased resistance usually does not pose a problem since some resistance is needed to dampen the pulse. The increased resistance however increases the risk of burning through the wiring due to the high current flowing through it. Figure 8 shows the response for a probe with 10 windings placed next to each other, and that of a probe with two layers of 5 windings. It shows that an increase in pulse magnitude can be achieved by altering the winding configuration.

Charge capacitor. In our evaluation board we can also vary the size of the charge capacitor. Varying the charge capacitor emulates a change in the pulse generator design. In Figure 9 the measured pulses for a varying capacitance can be seen.

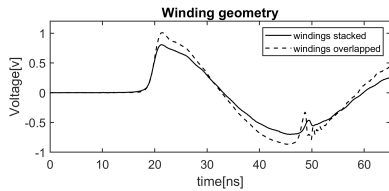


Fig. 8: Pulse response for different winding geometries.

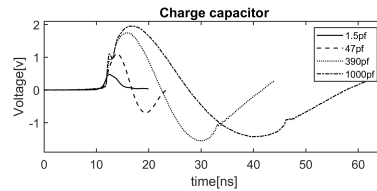


Fig. 9: Pulse response for different charge capacitors.

4 Pulse generator

The main requirement for an EM-FI pulse generator is to produce a large current pulse with a fast rise time. Currents flowing through the probe are usually in the tens of amperes. In order to obtain a good temporal resolution, the rise time should be in the nanoseconds range. In the remainder of the paper we will restrict ourselves to a pulse generator design based on the RLC-circuit introduced in Figure 2. Some adaptations to the circuit have to be made for it to become a functional EM-pulse generator. For instance, the ideal switch will have to be replaced and a power supply will have to be added to the design. Since the pulses needed for EM-pulse injection are generally in the nanoseconds range, the parasitics of the different discrete components can start dominating. Therefore components with good high frequency characteristics should be selected. Components with long lead wires should for instance be avoided, since the parasitic inductance of the leads will reduce the bandwidth of the pulse.

Note that off-the-shelf components such as RF power amplifiers or high voltage pulse generators are usually designed to drive a resistive 50 Ohm load. EM-probes however have a different impedance which might result in a reduced

efficiency of the amplifier or pulse generator. Therefore extra matching circuitry might have to be added to prevent damage to the equipment or to make sure the generated pulse matches the expectations.

4.1 Switching element

When designing an RLC-based pulse generator different switching elements can be used. The most common switching element is a MOSFET, but also other semiconductor devices such as IGBTs or bipolar transistors in regular operation or in avalanche mode could be used. Besides semiconductor devices, one could also use dielectric breakdown devices such as a spark gap based switch. MOSFETs, and to a lesser extent IGBTs, are the preferred switching elements for EM-pulse setups. They tolerate high voltages and currents while providing a reasonable switching speed. One of the major drawbacks are the large parasitic capacitances of these components. A faster switching element, such as a bipolar transistor, could be used for better rise times. However, bipolar transistors can usually not tolerate the high currents and voltages required to generate a sufficiently large magnetic field. Biasing a bipolar transistor into its avalanche breakdown region might give us the best of both worlds: fast switching speeds and low parasitics, while being able to tolerate high voltages and currents. The drawback however is that we can only operate in this avalanche region for a small voltage window.

When selecting the switching component care has to be taken that the parasitics do not start dominating the setup. For instance it is not uncommon for MOSFETs and IGBTs to have an output capacitance which is larger than 1000 pf. These devices do not only have large output capacitances, but also have significant input capacitance. Therefore a good input driving circuit is required to have a good turn on characteristics.

4.2 Pulse delay and jitter

Fault injection inherently requires a delay element in order to time the attack properly. From previous work [10,8] we know that often devices can only be faulted with EM-FI when the injected pulse causes a violation of either the setup or hold time. If we have a narrow pulse width and a low clock frequency, it might occur that we only have a 10 ns window ($t_{sensitive}$) around the clock edge during which we can inject faults. This puts a lower bound on the resolution of our delay element. Too much jitter will reduce the success rate of the pulse injection campaign. Even if the delay is set properly, a portion of the injected pulses will fall outside $t_{sensitive}$. With a large $t_{sensitive}$ the jitter and delay requirements can be relaxed. For our experiments in Section 5 we use an Agilent 33250A signal generator as delay element. An alternative would be to use an FPGA development board as a triggering device.

4.3 Power supply

The power supply needs to be able to provide a sufficiently high DC voltage. From Equation 4 we can see that the current through the probe relates linearly to the voltage across the charge capacitor. The amount of current the power supply can deliver in combination with the size of the charge capacitor will determine the period between consecutive EM-pulse injections. High voltage DC power supplies can be purchased or build for around 20 Euros in the form of a Cockcroft—Walton generator. As a last remark, note that a good decoupling between the EM-FI setup and the rest of the environment is required. Otherwise, coupling between the EM-pulses might interfere with sensitive auxiliary equipment such as oscilloscopes. The decoupling can be achieved by minimizing the parasitic EM emissions from the EM-injection setup by placing decoupling capacitors on the different power supply rails, placing bulk capacitors close to the MOSFET and MOSFET driver and using shielded cables or twisted wire pairs to connect the different components. On the target side, coupling can be minimized by reducing the overall wire length and by using shielded cables, where possible.

5 Example Design

In this section we describe an example setup for EM pulse injection based on an RLC circuit with a MOSFET as switching element. This is by no means an optimal setup, but rather a use case tailored to the principles described in the paper. Our goal is to build a platform capable of generating 10 ns pulses, with the goal of targeting individual clock cycles in microcontrollers running at a frequency of 100 MHz.

5.1 EM Pulse Injection Platform

A circuit diagram of the EM-FI setup, including both pulse generator and probe, is shown in Figure 10. As switching element (M1), we select an IPA80R280P7 MOSFET from Infineon Technologies. This is an n-channel MOSFET with a fast rise-time and relatively low output capacitance. It can tolerate a V_{ds} up to 800 V and a maximal pulsed drain current of 45 A. The MOSFET also has integrated ESD protection in the form of a Zener diode which is crucial in order to prevent damage to the MOSFET. Once the capacitor is discharged through L1 there will be a flyback voltage across the inductor. The flyback voltage will result in a negative V_{DS} , which has to be protected against. We opted to not put a flyback diode directly across L1 but instead to rely on the build in Zener diode of the MOSFET.

The IPA80R280P7 is driven by a Microchip MIC4422 low side MOSFET driver (X1). The jitter introduced by the MOSFET and driver combination amounts to 0.43 ns. The delay between the rising edge of the TRIG signal and pulse generation is 56 ns. A current limiting resistor (R2) is inserted at the source terminal of the MOSFET. This resistor serves as a safety mechanism to ensure

the current never exceeds the maximal current rating of the MOSFET. In our case, the gate voltage during the *on* state is fixed to 12 V and the $V_{GS(th)}$ of the MOSFET is 3 V. Choosing the resistor to be 0.22 Ohm, the current through the MOSFET will not exceed 40 A since the voltage across R2 will reduce V_{GS} , turning off the MOSFET if the current exceeds 40 A. Increasing the value of R2 and thus limiting the current through the MOSFET would also allow us to generate square pulses. The PCB design for the EM-pulse generator is shown in Figure 11 and its corresponding schematic in Appendix B. The layout of the PCB is important not only to reduce the parasitics, but also to prevent undesired coupling or hotspots due to excessive heat generation. The main focus during PCB layout should be the high current RLC loop, which should be kept as small as possible. The cost of assembling the entire design is around 40 Euro.

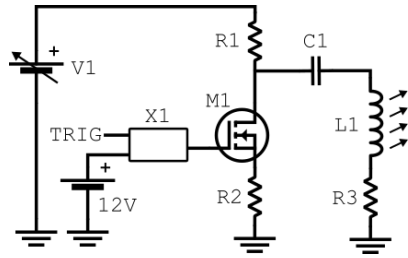


Fig. 10: Circuit diagram of EM Pulse injection setup.

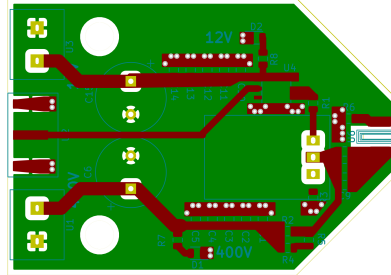


Fig. 11: EM-pulse injector PCB.

The second component in our example design is the probe. In order to obtain a good spatial resolution, we select a ferrite rod with a 750 μm diameter and 4 windings. The number of windings could be reduced in case the setup does not achieve the desired 10 ns pulse width. The inductance L1 of the probe can be estimated using Equation 1, or directly measured using an impedance meter. Knowing the inductance of the probe helps us with the choice of capacitor C1. Since we opt to build a setup that is slightly overdamped, the choice of capacitor size impacts the pulse width and amplitude. By modeling the circuit in SPICE, we estimated that a 1000 pF capacitor for C1 would yield the desired 10 ns pulse width. With these parameters, however, the circuit turns out to be underdamped. Therefore we add a 10 Ohm resistor R3 in order to achieve a slight overdamped response. After assembling the setup a pulse width of 12 ns was measured. Lowering the capacitance C1 and adjusting R3 finally enabled us to obtain the desired 10 ns pulse width.

5.2 Experimental Results

We target an STM32F411 from ST Microelectronics mounted on a NUCLEO-F411RE development board. This is a 32-bit ARM Cortex-M4 microcontroller

featuring a three-stage pipeline. Its maximal frequency of 100 MHz makes it perfectly suitable for our experiments. The board is positioned on an XYZ stepper table such that the EM probe can be placed on top of the IC. Our experiments are performed in a non-invasive setting, e.g. without exposing the die of the chip.

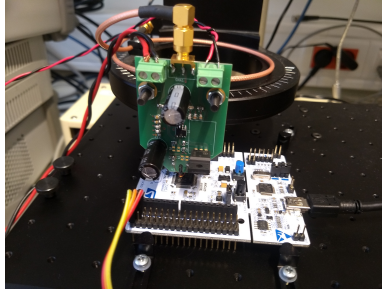
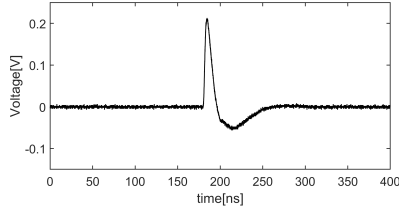


Fig. 12: EM-fault injection setup with STM32F411 target board.

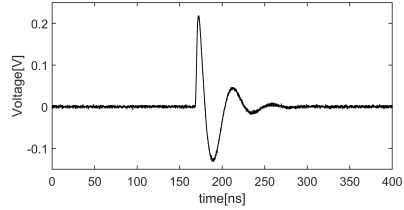
We select the store multiple (STM) instruction as target operation. We write a simple target routine that writes the values of 10 working registers ($r0$ to $r9$) to memory. The values are fixed to $0x55555555$. This alternating string of ones and zeros is chosen to accommodate for the occurrence of bit set, bit reset or bit flip faults. Using a GPIO trigger for synchronization, we inject EM pulses during the writing stage of STM. Two sets of experiments are performed with different damping ratios. For the first experiment, a 10 Ohm resistor is chosen for R3 making the EM-pulse critically damped. For the second experiment, R3 contains a 1 Ohm resistor that makes the EM-pulse underdamped. All other parameters such as the probe, power supply voltage, injection location and timing are kept constant for both sets of experiments. The resulting pulse shapes for both the critically damped and underdamped case can be seen in Figures 13a and 13b. After scanning the entire chip surface for sensitive areas, we selected a location with a high success rate. EM-pulses were injected in this region over a time period of 100 ns, with 1 ns steps.

When injecting pulses with the critically damped setup, we can fault individual writes to memory as can be seen in Figure 13c. The X-axis corresponds to the register written to memory, while the Y-axis corresponds to the timing. An orange square indicates a fault was injected into the STM instruction while storing a particular register. At every step in time, 100 pulses were injected into the target. The plot clearly shows that the critically damped configuration of the setup allows to target individual writes to memory. Converting the setup to an underdamped configuration results in the fault map from Figure 13d. We can still in some occasions target individual instructions, but also multiple instruction faults occur. This effect can be linked to the *FSR* described in Section 2. In the critically damped case, we have a single pulse with a 10 ns pulse width. It is likely that the voltage and current fluctuations only persist for a portion of this pulse width, and therefore we can target individual clock cycles. In the under-

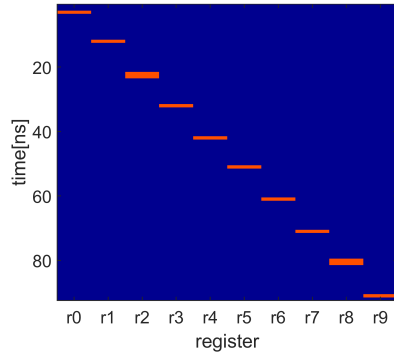
damped case however, we have multiple harmonic oscillations after the first pulse increasing the $t_{sensitive}$ and thus faulting multiple instructions simultaneously.



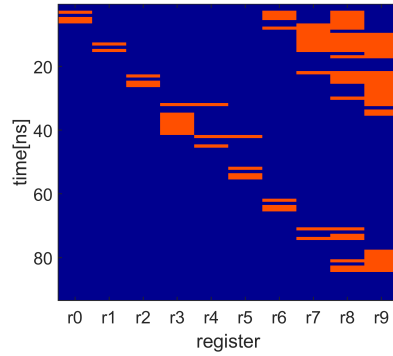
(a) Critically damped probe response



(b) Underdamped probe response



(c) Fault map critically damped probe



(d) Fault map underdamped probe

Fig. 13: EM-pulse injection results on the STM32F411 processor

Note that our experimental evaluation considers only the injection of a single pulse per campaign, which models an adversary capable of injecting one fault per cryptographic execution. If an adversary aims to inject multiple faults per execution, then the pulse frequency becomes a relevant design aspect. The time between consecutive pulses in our setup can be approximated by $4R1(C1 + C_{parasitic})$. The size of $R1$ is dependent on the drive strength of $V1$. The more current that can be supplied by $V1$, the lower we can set $R1$.

6 Conclusions

In this work we show that no special circuitry or equipment is needed to build a quality EM-pulse injection setup. However, a good understanding on how the different building blocks and design parameters impact the final pulse shape is important and not often discussed in the literature. Our study provides some guidelines supported by experimental results, and shows that a good tuning of the EM-pulse setup to the target device is critical for the success rate of an EM-pulse injection campaign.

Acknowledgment

This work was supported in part by the Research Council KU Leuven C1 on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058 and through the Horizon 2020 research and innovation programme under Cathedral ERC Advanced Grant 695305. Additionally this work has been partially supported by FWO project VS06717N in collaboration with JSPS.

References

1. Balasch, J., Arumi, D., Manich, S.: Design and validation of a platform for electromagnetic fault injection. In: DCIS 2017. pp. 1–6. IEEE (2017)
2. Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The Sorcerer’s Apprentice Guide to Fault Attacks. *Proceedings of the IEEE* **94**(2), 370–382 (2006)
3. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the Importance of Checking Cryptographic Protocols for Faults. In: EUROCRYPT ’97. LNCS, vol. 1233, pp. 37–51. Springer (1997)
4. Cui, A., Housley, R.: BADFET: Defeating modern secure boot using second-order pulsed electromagnetic fault injection. In: 11th USENIX Workshop on Offensive Technologies (WOOT 17). USENIX Association, Vancouver, BC (2017)
5. Dumont, M., Lisart, M., Maurine, P.: Electromagnetic Fault Injection : How Faults Occur. In: FDTC 2019. pp. 9–16. IEEE (2019)
6. Giancoli, D.C.: *Physics: Principles with Applications*. Pearson (2014)
7. Maurine, P.: Techniques for EM Fault Injection: Equipments and Experimental Results. In: FDTC 2012. pp. 3–4 (Sept 2012)
8. Moro, N., Dehbaoui, A., Heydemann, K., Robisson, B., Encrenaz, E.: Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller. In: Fischer, W., Schmidt, J. (eds.) FDTC 2013. pp. 77–88. IEEE (2013)
9. Omarouayache, R., Raoult, J., Jarrix, S., Chusseau, L., Maurine, P.: Magnetic microprobe design for em fault attack. In: Catrysse, J., Pissoort, D. (eds.) EMC2013. pp. 949–954. IEEE Computer Society, Brugge (2013)
10. Ordas, S., Guillaume-Sage, L., Tobich, K., Dutertre, J.M., Maurine, P.: Evidence of a larger em-induced fault model. In: Joye, M., Moradi, A. (eds.) CARDIS. pp. 245–259. Springer International Publishing, Cham (2015)
11. Quisquater, J.J., Samyde, D.: Eddy current for Magnetic Analysis with Active Sensor. In: Esmart 2002 (2002)
12. Skorobogatov, S.P., Anderson, R.J.: Optical Fault Induction Attacks. In: Jr., B.S.K., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 2–12. Springer (2002)

A The RLC circuit

By applying Kirchhoff’s law to the RLC loop from Figure 2 we obtain the following equation:

$$\frac{d^2 I}{dt^2} + \frac{R}{L} \frac{dI}{dt} + \frac{I}{LC} = 0, \quad (3)$$

Solving this equation yields three possible solutions depending on whether the circuit is critically damped (Eq. 4), underdamped (Eq. 5) or overdamped (Eq 7 and 8).

$$I = \frac{V_0}{L} t \exp\left(-\frac{R}{2L} t\right) \tag{4}$$

$$I = \frac{V_0}{L\omega_d} \sin(\omega_d t) \exp\left(-\frac{R}{2L} t\right) \tag{5}$$

$$\omega_d = \sqrt{\frac{1}{LC} - \frac{R^2}{4L^2}} \tag{6}$$

$$I = \frac{V_0}{(s_1 - s_2)L} [\exp(s_1 t) - \exp(s_2 t)] \tag{7}$$

$$s_1, s_2 = -\frac{R}{2L} \pm \sqrt{\left(\frac{R}{2L}\right)^2 - \frac{1}{LC}} \tag{8}$$

The solutions to the simple series RLC circuit can be found in nearly every physics textbook, see for instance [6].

B EM-pulse injection circuit - Schematic

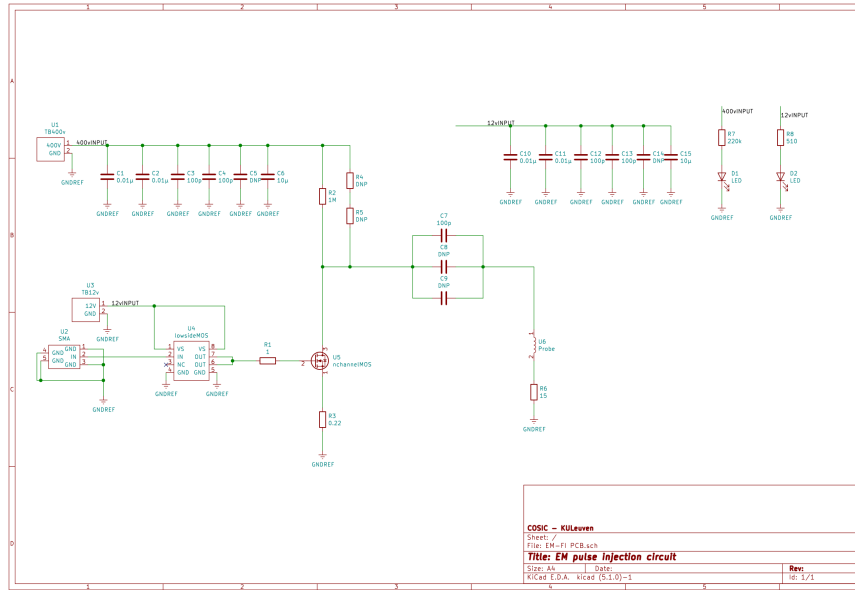


Fig. 14: EM-pulse injector schematic.