Design and Evaluation of a Spark Gap Based EM-fault Injection Setup

Arthur Beckers*, Masahiro Kinugawa†, Yuichi Hayashi†, Josep Balasch*, Ingrid Verbauwhede*
†Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma, Nara 630-0192, Japan
*imec-COSIC, KU Leuven Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
*firstname.lastname@esat.kuleuven.be

***Abstract*—The rapid and widespread deployment of electronic devices operating in the field is bringing security issues into the spotlight. Fault injection, for instance, is a class of attacks that allows adversaries to bypass security-related capabilities by tampering with the normal functioning of a device. In this paper we describe a setup capable of faulting integrated circuits by exposing them to a pulsed magnetic field. The magnetic field is generated by discharging a pulse forming network made from a transmission line over an injection probe. The discharge is triggered by a spark gap based switch. We describe the mechanisms behind the different circuit components and evaluate the performance of the setup in practice. To the best of our knowledge, this is the first time a spark gap switch is used to build an electromagnetic (EM) pulse fault injection setup.**

I. Introduction

Breaking the security guarantees provided by a cryptographic algorithm can occur at two different layers. The adversary can either attack the cryptographic algorithm in a mathematical manner or target its actual implementation. Since most standardized cryptographic algorithms are thoroughly peer reviewed, breaking them mathematically is considered unfeasible. This makes attackers shift their focus towards attacking the platform on which the algorithm is implemented, i.e. the Device Under Test (DUT). Attacks which target the implementation are also called physical attacks, as they exploit the interaction of the DUT with its surroundings. Physical attacks can be either passive or active in nature. When an adversary actively tries to manipulate the target device during its operation, the attack gets classified as a fault attack [1].

The first description of a fault attack against a cryptographic implementation was the Bellcore attack introduced by Boneh et al. [2]. This work triggered researchers to investigate different methods for injecting faults into integrated circuits (ICs). Nowadays several faulting mechanisms are described in the literature, including clock glitching [3], voltage glitching [4], laser fault injection [5] and electromagnetic fault injection (EM-FI) [6].

Fault injection attacks are commonly classified according to their invasiveness and locality. The invasiveness level indicates how much an adversary has to modify the DUT before the attack can be performed. For instance, some attacks such as laser fault injection, require the removal of the DUT's package to expose the die. The locality of an attack indicates whether the fault injection mechanism impacts the entire IC (e.g. glitching the supply line) or just a portion of it.

The focus of this work is on a new type of setup for EM-FI. In general an EM-FI setup injects EM-waves into a target IC. The injected EM-waves can be either continuous or pulsed. Our proposed setup belongs to the latter category. EM pulses injected into a DUT introduce voltage fluctuation on the internal wiring of the target IC. These voltage fluctuations can cause setup and hold time violations leading to errors into the target IC [7]. EM-FI can be classified as a local non-invasive fault injection method. It can target specific parts of the DUT while the packaging does not need to be tampered with. This is because EM waves can propagate through the packaging of the DUT.

A. Previous work

Multiple EM-FI setups have been described in literature. These setups are either commercial [8]–[10] or academic in nature [11]–[13]. They all have in common that their construction is centered around a semi-conductor based switching element. The role of the switching element is to release the capacitively or inductively stored energy into the EM-probe.

Currently all energy storage for EM-FI setups is done by using discrete components such as capacitors or inductors. This however gives the user little control over the pulse shape produced by the EM-probe. The EM-probe in an EM-FI setup transforms the current into an EM-field which can fault the target IC. The most commonly used EM-probes are solenoid based H-field probes.

B. Contribution

In this work we describe an EM-FI setup built around a spark gap based switch. Although these type of switches are common in high voltage short pulse width applications such as radar, this is the first time they are applied to the setting of EM-FI. Instead of a discrete energy storage element, our construction uses a continuous pulse forming network in the form of a transmission line as storage element.

II. circuit

In general EM-FI circuits are composed of three main components. They require a form of energy storage able to release the stored energy quickly, a switch to release the stored energy and a probe to convert the energy into an EM-pulse. In the following we describe the type of energy storage element and switching component used in our EM-FI setup. The setup is used in combination with a solenoid H-field probe. A detailed discussion on the impact of the probe design on the generated H-field can be found in the work of Omarouayache et al. [14].

A. Energy storage

When building an EM-pulse injection circuit two types of energy storage can be used. One can either store the energy capacitively or inductively. In the literature we can find examples for both cases using discrete components such as capacitors [13] or inductors [12]. In this work however we do not use a discrete component as storage element, but rather a continuous one in the form of a transmission line [15]. When using a transmission line as a storage element it can store energy in a capacitive or inductive manner. For this setup the transmission line was used as a capacitive storage element.

The transmission line acts as a pulse forming network. Once the switch is closed the transmission line starts discharging over the EM-probe. It will continue to discharge until the charge at the end of the transmission line has reached the load. Thus the length of the transmission line will determine the pulse width. When using an open ended transmission line such as a coaxial cable, the cable acts as a pulse forming network and a square pulse is generated. The current and voltage seen by the load, the injection probe, are $I_L = {}^{V_0}\!/_{2Z_0}$ and $V_L = {}^{V_0}\!/_{2}$. The length of the pulse is determined by the length of the cable and is given by:

$$\delta_p = \frac{2l_{T1}}{cV_f},$$

with c the speed of light and V_f the velocity factor of the used transmission line.

The advantage of using a transmission line as a pulse forming network is the fine control the user has over the pulse shape. However, if different pulse widths or a large pulse width is needed, such an approach may become impractical.

B. Switching element

Contrary to previous EM-FI setups, the triggering element in our setup is not semi-conductor based. Instead, we use a triggered high-pressure spark gap. There are different techniques for switching a spark gap. In this work, we use a spark relay mechanism as a trigger [16]. This type of spark gap switch is constructed with three electrodes: the anode electrode (AE), the cathode electrode (CE) and a trigger electrode (TE). The triggering process is illustrated in Figure 1. Upon triggering, a high voltage is placed on the trigger electrode causing a first breakdown between the trigger and the cathode electrode. During this breakdown, UV light is produced which ionizes the air between the anode and cathode electrode (Figure 1a). This ionization causes a reduction in the breakdown voltage between the anode and cathode. If the anode potential is sufficiently high to cause breakdown between the anode and cathode under the reduced breakdown voltage, the energy stored in the pulse forming network is released (Figure 1b).

The breakdown voltage can be tuned by increasing and decreasing the distance between the anode and cathode or by changing the gas pressure. The gas used for our setup is air at 1 atm. The distance between anode and cathode should be taken large enough such that no spontaneous breakdown can occur within the chosen voltage range, but small enough for breakdown to occur upon triggering. The upper and lower pulse voltages are thus determined by the gap distance and trigger combination. Once breakdown occurs, the channel has a residual resistance and inductance which are determined by the geometry of the spark gap. As it is difficult to calculate the spark gap properties analytically, we rely on experimental results to calibrate the spark gap switch. Varying the gas pressure, the distance between anode and cathode or the triggering mechanism will impact the rise time and voltage range of the spark gap based switch. In this work we chose for a configuration which we could easily tune to our needs. An example setup is provide to demonstrate the feasibility of using a spark gap based switch for EM-pulse injection. We stress however that this setup is by no means an optimal one. The tuning of the different switch parameters is left for future work.

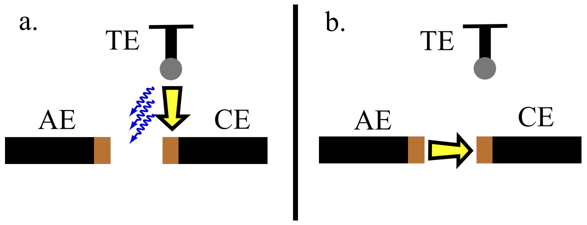

Fig. 1. Spark gap switching mechanism.

C. EM-FI circuit

A complete overview of the EM-FI circuit can be seen in Figure 2. For our experiments we use a transmission line based pulse-forming network T1. The line is precharged to a high DC voltage over the current limiting resistor Z_S. The pulse is propagated towards the injection probe Z_L through the transmission line T2.

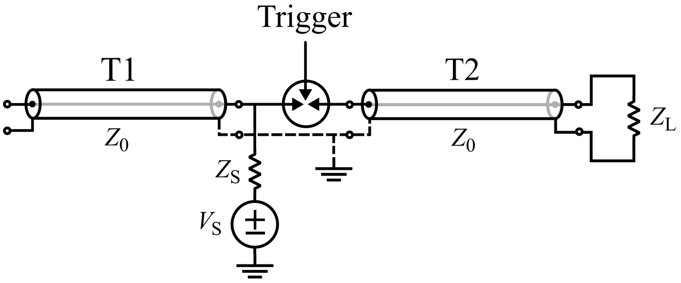

Fig. 2. EM-pulse injection circuit.

Any impedance mismatch between the load and transmission lines causes reflections and hence ringing on the emitted pulse. With this type of pulser it is thus important to match the different components of the circuit, however in some cases the ringing might be a desired side effect.

III. Experimental setup

In this section we describe our complete EM-FI setup based on the circuit from Figure 2. The resulting PCB can be seen in Figure 4. In the center of the PCB the spark gap switch is situated. The electrodes of the spark gap switch are constructed from a copper rod layed with tungsten. For our setup, we use a power supply capable of delivering up to 1000V DC. No spontaneous breakdown of the spark gap should occur when the maximal voltage is applied. Therefore the anode and cathode electrode are placed at approximately 1 mm distance from each other. The appropriate distance between the rods was determined in an empirical manner.

The spark gap breakdown between the anode and cathode is triggered by the trigger electrode. This electrode is made by placing a wire loop around the cathode electrode. By discharging a 40 nF capacitor bank over a step up transformer a high enough voltage is produced to cause breakdown between the cathode and trigger electrode. The discharge is triggered by an IGBT which in turn is driven by a signal generator.

The spark gap switch is connected to the EM-FI injection probe using a 10 Ω transmission line T2 made up of 5 parallel 50 Ω coaxial cables. The 10 Ω transmission line T1 used for the charge storage is made up from 5 parallel 50 Ω coaxial cables. The selection for 50 ohm cables was done based on availability. The transmission line length was taken to be 1 m, but any length of cable could be used.

In order to measure the pulse generated by the injection setup we employed a 50 Ω microstripline as depicted in Figure 3. The microstripline is 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 width of the microstripline measures 0.532 mm. The PCB dimensions are 14 cm wide and 24 cm long. The microstripline is on one end terminated by a 50 Ω impedance and on the other end by the 50 Ω input of the oscilloscope. The scope we used for our measurements is a Tektronix DPO70404C with a sample rate of 25 Gs/s. The probe was positioned such that a maximal amplitude was measured by the microstripline.

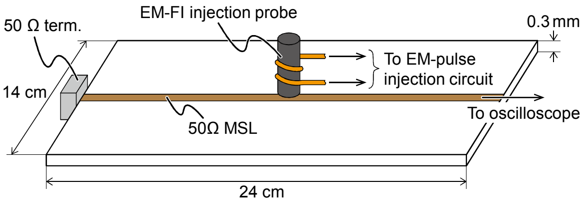

Fig. 3. Measurement setup based on microstripline.

The probe used during our experiments was impedance matched to the 10 ohm transmission wired T1 and T2. Due to the high voltages and currents, a simple wire generates a sufficiently large field to be captured by the 50 Ω microstripline. The entire setup was placed in a protective casing shielding the user from the high DC-voltage.

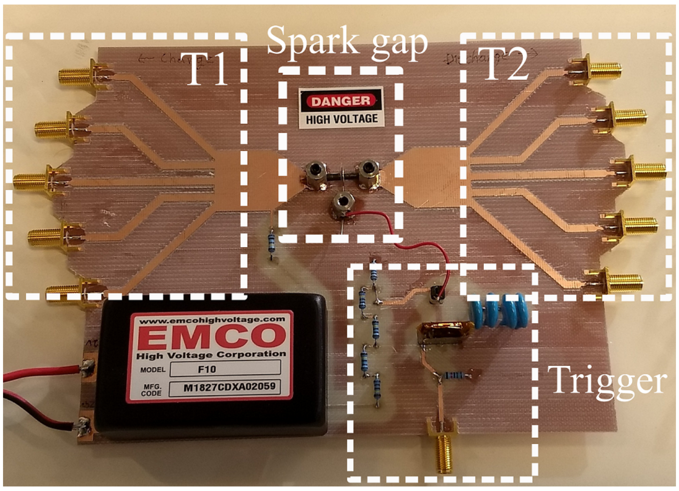

Fig. 4. EM-pulse injection PCB.

IV. Experimental results

In this section we summarize the results of evaluating our experimental setup. Since we measure the magnetic field generated by the probe, we measure the derivative of the current pulse flowing through it. Given that the pulse forming network of our circuit produces square pulses, we expect the measurements to show a positive and negative peak corresponding to the rising and falling edge of the pulse. The distance between these two peaks allow us to measure the width of the square pulse.

Figure 5 shows the measured fields for a transmission line length of 1 m and 2 m, respectively. Using a 1 m transmission line results in a pulse width of 12 ns, while the 2 m transmission line produces a 24 ns pulse width. Thus, as expected per the theory, doubling of the transmission line length results in a doubling of the pulse width.

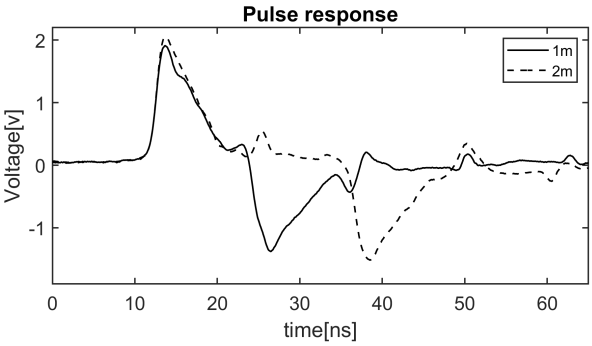

Fig. 5. EM-pulse for a 1m and 2m transmission line.

When using an EM-FI setup, the amplitude of the emitted field needs to be tuned to the target device. Too large of an amplitude might cause damage to the DUT, while too low an amplitude may not fault the device. The amplitude of the pulse can be tuned by varying the DC voltage placed over T1. Figure 6 shows the pulse measured by the microstripline for a voltage of 1000 V and 900 V across the spark gap made by the anode and cathode electrode. The plot clearly shows one can tune the pulse amplitude by varying the voltage across the spark gap. There is however an upper and lower limit to the applied voltage range, as explained in Section II-B. One of the main advantages of using a spark gap based switch are the high voltages the switch can tolerate. Contrary to semiconductor based switches, spark gaps can effortlessly switch thousands of Volts through the injection probe.

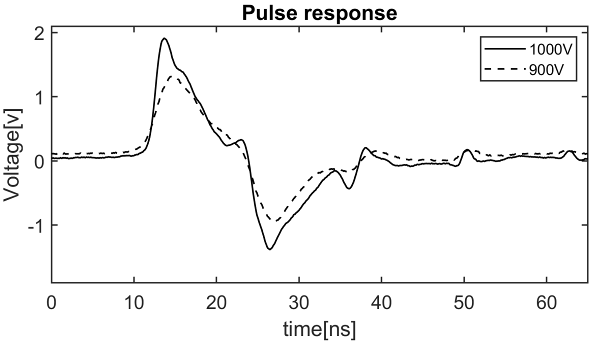

Fig. 6. EM-pulse for 1000V and 900V.

Another important factor when injecting faults into a DUT is the repeatability of a particular fault injection. This aspect is strongly influenced by the timing jitter between consecutive pulse injections. For our setup, we measured the timing jitter to be 10 ns on average. This timing jitter is caused by both the jitter on the switching of the IGBT as well as the jitter of the spark gap switch.

V. Conclusion

In this work we demonstrated the feasibility of constructing an EM-FI centred around a spark gap based switching element. This type of switch allows the use of almost arbitrarily high voltages for the generation of EM-pulses. Using this type of switch in combination with a pulse forming network gives the user excellent control over the EM-field injected into the DUT. The current setup however has a significant amount of jitter on the generated pulse which might be unacceptable in some scenarios. This issue could be addressed by using a different type of spark gap switch or by varying the switch parameters. An improvement could for instance be achieved by applying a higher voltage to the trigger electrode or switching out the IGBT for a low jitter mosfet. This however is left for future work.

References

[1] 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, 2006.

[2] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," in *EUROCRYPT '97*, ser. LNCS, vol. 1233. Springer, 1997, pp. 37–51.

[3] J. Balasch, B. Gierlichs, and I. Verbauwhede, "An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs," in *FDTC 2011*, L. Breveglieri, S. Guilley, I. Koren, D. Naccache, and J. Takahashi, Eds. IEEE Computer Society, 2011, pp. 105–114.

[4] C. H. Kim and J. Quisquater, "Fault attacks for CRT based RSA: new attacks, new results, and new countermeasures," in *Information Security Theory and Practices - WISTP 2007*, ser. LNCS, D. Sauveron, C. Markantonakis, A. Bilas, and J. Quisquater, Eds., vol. 4462. Springer, 2007, pp. 215–228.

[5] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," in *CHES 2002*, ser. LNCS, B. S. K. Jr., Ç. K. Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 2–12.

[6] J.-J. Quisquater and D. Samyde, "Eddy current for Magnetic Analysis with Active Sensor," in *Esmart 2002*, 2002.

[7] S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M. Dutertre, and P. Maurine, "Evidence of a larger em-induced fault model," in *CARDIS*, M. Joye and A. Moradi, Eds. Cham: Springer International Publishing, 2015, pp. 245–259.

[8] NEWAE, "NEWAE chipshouter," http://store.newae.com/chipshouter-kit/, June 2019.

[9] Riscure, "Riscure EM-FI transient probe," https://getquote.riscure.com/en/quote/2101068/em-fi-transient-probe.htm, June 2019.

[10] Langer EMV, "ICI 01 L-EFT set," https://www.langer-emv.de/en/product/ic-side-channel-analysis/94/ici-01-l-eft-set-ic-em-pulse-injection-langer-pulse/821, July 2019.

[11] 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.

[12] J. Balasch, D. Arumi, and S. Manich, "Design and validation of a platform for electromagnetic fault injection," in *DCIS 2017*. IEEE, 2017, pp. 1–6.

[13] A. Beckers, M. Kinugawa, D. Fujimoto, Y. Hayashi, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Design considerations for em pulse fault injection," in *CARDIS 2019*. Prague: Springer, 2019.

[14] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine, "Magnetic microprobe design for em fault attack," in *EMC2013*, J. Catrysse and D. Pissoort, Eds. Brugge: IEEE Computer Society, 2013, pp. 949–954.

[15] G. N. Glasoe and J. V. Lebacqz, Eds., *Pulse Generators*. McGraw-hill book company Inc., 1948.

[16] G. A. Mesyats, *Pulsed Power*. Springer, Boston, MA, 2005.