Malicious Wave: a Survey on Actively Tampering Using Electromagnetic Glitch

Shivam Bhasin, Telecom ParisTech, Paris, France, shivam.bhasin@telecom-paristech.fr
Paolo Maistri, Univ. Grenoble Alpes - TIMA Laboratory, CNRS - TIMA Laboratory, paolo.maistri@imag.fr
Francesco Regazzoni, ALaRI - USI, Lugano, Switzerland, regazzoni@alari.ch

***Abstract*—Physical attacks are a serious threat for secure embedded devices. Attacks based on analysis of electromagnetic emissions of such devices have proven to be particularly dangerous, more than power-based analyses, as they can target even small and specific portion of the chip. The electromagnetic waves can be used effectively also as an active mean of attack, by perturbing the secure computations. In this paper we report the main results in the area, focusing in particular on active electromagnetic attacks. We conclude the paper reporting the current works in the area of early estimation of EM vulnerabilities and in the area of countermeasures, as example of promising directions for future research.**

I. Introduction

Embedded systems have evolved a long way since their introduction. Modern embedded systems can be seen in wide variety of applications, ranging from simple communication devices, image or digital processing systems to complex systems-on-chip (SoC). When such SoC are used in mission critical applications like medical, automotive, defense etc, a certain security requirement must be fulfilled. To address these security needs, embedded systems use cryptographic-cores implementing strong cryptographic algorithms, which are considered mathematically secure. A possible example of these algorithms is the Advanced Encryption Standard (AES [21]).

However, despite being mathematically secure, these crypto-cores can be compromised by exploiting the weaknesses and the information leakage of their physical implementations. These attacks are called physical attacks and were presented in the past in several variants, ranging from Side-Channel Attacks (SCA) [7] to Fault Attacks (FA) [5]. Both attacks are sufficiently powerful to allow the adversary to gain complete knowledge of the secret key with reasonable time and resources.

SCA are passive attacks that are based on the observation of physical emanations of the system. The channel observed is usually either the power consumed during the computation of the cryptograpic routine (Power Analysis [17]), the electromagnetic field generated during the computation of the cryptographic routine (Electro-Magnetic (EM) Analysis [1]), or the time needed for the computation of the cryptographic routine (Timing Attacks [13]).

These attacks are possible as the target embedded systems are operating in a hostile environment. Thus, an adversary in proximity of the target device can measure one or more of these physical quantities and perform an analysis aimed at exploiting the dependency between the measured quantity and the secret key involved in to computation. During Side Channel Analysis, often the successful attack is determined when the maximum correlation between a predicted value for the secret key and the collected physical quantity allows distinguishing the correct hypothesis from the wrong ones. The correlation is computed using statistical tools like covariance (DPA [17]), correlation (CPA) [7]), and maximum likelihood (Templates [8]).

Fault attacks instead are active attacks. They involve the active tampering with the devices by injecting one or more faults during the execution of a cryptographic algorithm and a post-process analysis of the faulty output of the device. Several techniques were presented in the past to inject the faults, ranging from the variations of supply voltage, clock frequency, temperature variation, to the irradiation of a laser/EM beam. Possible effects are the computation of a wrong results or the skipping of a crucial sanity check. Both the effects can be exploited to compromise the security of the device. For instance, from the knowledge of one or multiple pairs of correct and faulted ciphertext, it is possible to build an attack which exploit the differences between the pairs: this attack is called Differential Fault Analysis [5] (DFA).

Electromagnetic emission can be exploited in both types of attacks: passive side channel as well as active fault attacks. In side channel attacks, EM measures are usually more targeted than the general power supply, thus, for certain devices, EM attacks might be easier to be carried out compared to power analysis. In fact, unlike EM which requires only a careful placement of antenna in proximity of the device, power measurement would often need also modification to the supply line or to the ground line of the device.

Electromagnetic glitches were also demonstrated to be a suitable and reliable way to induce fault into devices. In fact, variation of clock, voltage or temperature, can only create global faults. Laser beams are capable of localized fault injection, but they require the decapsulation of the device which is an expensive and error prone process. Electromagnetic glitches instead can be used to inject both localized and global faults and they generally do not require decapsulation of the target.

Despite this amount of previous works, several research problems are still open, ranging from tools for early assessment of EM resistance, to more effective countermeasures and improved attack techniques. This paper focuses on active electromagnetic attacks and aims at providing an overview of the main research topic carried out in the area.

The rest of the paper is organized as follows. Section II introduces the EM attacks. Section III and Section IV details the state of the art of fault attacks using EM as a single pulse

and harmonics respectively. Countermeasures proposed so far are discussed in Section V.

II. Overview of Electromagnetic Attacks

Each movement of an electric charge produces an electromagnetic field. Also, any electromagnetic field interacts with surrounding charges. These effects can be exploited maliciously to attack electronic devices which are computing cryptographic algorithms mainly in two ways. The first malicious exploitation is passive and it is based on the fact that the characteristics of the electromagnetic field generated by the current flowing in an electronic device depend on the computation being carried out. Thanks to this, the electromagnetic field can be analyzed and exploited to gain information on the secret key, as it is done in other side channel attacks. These attacks passively exploit electromagnetic emanations and are called Electro Magnetic Analysis (EMA) [22], [14], [1]. They are more powerful compared to power analysis attacks as they can target specific and tiny areas of the chip, and because electromagnetic emissions are usually carrying more than one exploitable information. However, the equipment used for mounting EMA can be much more expensive than the one usually used to carry out attacks based on power consumption; in particular, the probe plays a fundamental role in the success of the attack. Similarly to power analysis, the most popular attacks which passively exploit the emission of electromagnetic waves are SEMA (Simple EMA), in which the adversary attempts to extract secret information from a single EM sample, and DEMA (Differential EMA), in which statistical tools are used to analyze and correlate multiple traces with the secret information.

The second malicious exploitation is active and requires to generate an electromagnetic field capable of interacting with the currents flowing in the target electronic devices, being it an embedded processor, an ASIC or an FPGA. The sensitivity of integrated circuits to near field injection has been largely discussed in literature, showing, for instance, that dies and bonding wires can be sensitive to both magnetic and electric field [2]. In this case, near field electromagnetic radiations are generated by an adversary to actively tamper with the circuit to violate its correct operation conditions.

Depending on the type of the electromagnetic perturbation which is generated, active EM attack can be divided into transient pulses and harmonic emissions [11] attacks. Usually, in the transient pulse attacks, the adversary inject a transient and fast pulse which changes the signal or the power input and produces a glitch with the goal of inducing a fault. During the harmonic emission attacks instead, the adversary generates a magnetic filed capable of directly affecting and controlling the output of the circuits in order to reduce the security of the target device. Successful attacks based on both the generation of transient pulses and harmonics will be discussed in the next session.

Figure. 1 depicts an example of a working EM attacks station. The figure shows an electromagnetic probe placed over a chip. The placement was carefully done after the most suitable point of attack has been identified. In this example, the point is the power distribution line, near a crypto-core which computes the sensitive data.

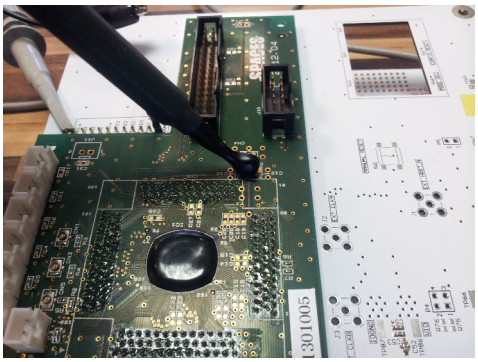

Fig. 1. Side Channel Measurement using an EM probe for a crypto-core.

III. Transient Pulse Attack

In a transient pulse attack, the attacker aims at inducing a fault or a misbehavior of the integrated circuit by generating an electromagnetic pulse. An idealized setup for this attack is depicted in Figure 2. The setup is composed by: a personal computer, which controls the overall system and collects the output of the chip; a pulse generator, which produces the pulse which will be injected into the target chip; an electromagnetic probe mounted on top of an X Y Z stage, which, in order to allow an easy positioning of the probe is usually motorized; and, finally, by the chip under attack, which will produce a faulty output after the injection of the proper pulse. Transient pulse attacks were used in the past to successfully attack software and hardware implementations of the Advanced Encryption Standard [12], [9], [11], as well as of software implementations of the RSA algorithm based on the Chinese Reminder Theorem [24].

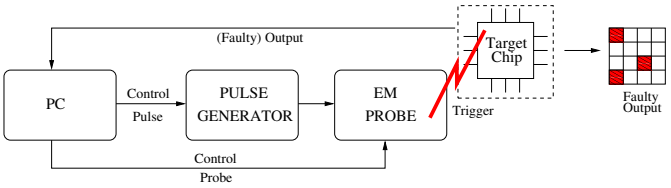

Fig. 2. Idealized setup of a Transient Pulse Attack comprising a personal computer, a pulse generator, an electromagnetic probe, an X Y Z stage, and the chip target of the attack.

An 8-bits AVR Atmega 128 micro-controller running the AES algorithm was attacked by Dehbaoui et al. [11]. The generator used to perform the attack is capable of producing a pulse with a jitter lower than $50ps$, a rising and falling transition time of $5ns$, and an amplitude of the pulses ranging from $1V$ to $100V$. The attack was carried out with a probe capable of targeting very small parts of the target microcontroller. The authors observed two possible faulty outputs: data dependent (which change when the input given to the microcontoller changes) and constant (the ones which, regardless of the input given to the microcontroller, produce always the same faulty output). The authors conclude the analysis showing the suitability of the approach for inducing faults.

The same experimental setup was used for attacking a 128-bit wide datapath AES accelerator implemented on an Xilinx Spartan 3 FPGA [11]. In this case, the authors run several

attacks on different areas of the chip and construct its fault cartography, which report the number of most frequent faulted bytes for each location. The authors support the hypothesis that the faults induced by the pulse are timing violations. This is explained by the fact that the EM pulse couples with the supply and ground lines of the device, which lowers locally the differential voltage supply, thus resulting in slower performance of the logic gates.

Several experiments were also carried out on an ARM Cortex processor, with the goal of characterizing the type of faults which can be injected using electromagnetic pulses [20]. After a large campaign during which they varied the pulse width and voltage, the authors showed that two types of faults can be successfully injected into the microcontroller under study: one instruction can be changed into another, and, when loaded from the flash memory, a value of a data can be changed into another. The reported experiments showed also that some instructions or some registers are more vulnerable than others to EM pulses. It is however important to underline that these results are very dependent on the specific target device.

Also, Schmidt and Hutter [24] showed that is possible to change both the program flow and the SRAM content on the 8-bit microcontroller. The faults were injected while the microcontroller was running a CRT-based RSA algorithm. The EM pulse has been injected during the computation the S_q, while the S_p stayed untouched. Nevertheless, even this single fault was sufficient to successfully factorize the signature computation.

IV. Harmonic Emission Attack

In a harmonic emission attack, the attacker aims at making the device producing a controlled or biased output by injecting a specific electromagnetic wave. An idealized setup is depicted in Figure 3, and it is similar to the one previously discussed for the transient pulse attack. Also in this case, the setup is composed by a personal computer, which controls the overall system and collects the output of the chip, an electromagnetic probe mounted on top of a motorized X Y Z stage, and, finally by the chip under attack. However, in this setup, the pulse generator is replaced by an harmonic generator, which produces the waves needed to bias the output of the device, and the output of the target chip, in this case, will not be faulty but biased according to the intentions of the attacker.

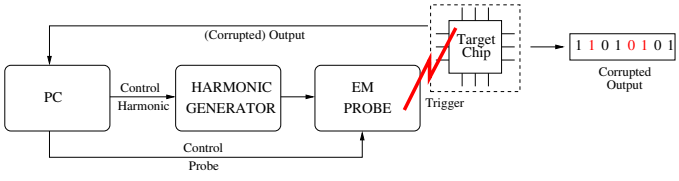

Fig. 3. Idealized setup of an Harmonic Emission Attack comprising a personal computer, a harmonic generator, an electromagnetic probe, an X Y Z stage, and the chip target of the attack.

Most of the previous successful attacks based on harmonic emission target random number generators based on ring oscillators [18], [19], [4]. The goal, in this case, is either to bias the source, or to reduce the entropy of the generated random bit stream. Unlike pulsed attacks, harmonic injections provide an additional amount of energy, which alters the behavior of the targeted device; in order for the attack to be effective, the target is usually analog logic, which explains why most reported experiments target True Random Number Generators (TRNG).

Markettos at al. [18], [19] attacked a TRNG based on two ring oscillators by injecting a sine wave signal onto the power pads of the integrated circuit. The wave was capable of reducing the number of possible random values from 2^{32} to 255.

Also Bayon at al. [4] focused on TRNGs based on ring oscillators. They presented an attack which does not require contact with the device, nor physical access to it. The output of the TRNG is biased by injecting the electromagnetic signal into the device itself rather than into the power supply pins. The authors carries out experiments on TRNGs implemented on FPGAs and they demonstrated the effectiveness of the generated electromagnetic wave in controlling the behavior of the ring oscillators. Exploiting this fact, they were capable of biasing the output of a RNG composed of up to 50 ring oscillators.

Sauvage et al. [23] demonstarted practical attacks on a ASIC implementation of DES using EM harmonic injection. Authors presented a methodology to charaterize and find the optimal frequency for fault injections. Intentional electromagnetic interference (IEMI) was also used to injection faults in hardware implementation of block ciphers [16].

V. Early Estimation of Vulnerabilities and Countermeasures against EMA

In this section we discuss the previous works on early estimation of vulnerability of integrated circuits against EM attacks and on countermeasures against EM attacks.

One of the main strength of EM-based attacks, in particular the ones which aim at injecting a fault, was the lack of methodologies and support to localize and identify vulnerable parts of a chip before production, and thus apply the proper countermeasures. To date in fact, the vulnerability analysis is carried out after the chip has been fabricated, by repeatedly injecting faults into the device by means of EM pulses. For this reason, addressing the vulnerabilities of integrated circuits against EM attacks is an expensive, tedious, and difficult task.

An interesting research direction for the early estimation of vulnerabilities was presented by Alberto *et al.* [3]. The estimation is carried out at design-phase and exploits the potentialities of the CAD tools like Synopsis PrimeRail or Magma BlastRail which are designed to carry out the IR drop analysis. IR drop analysis allows to build a detailed cartography in which the local voltage drop is estimated when a certain switching activity of the device is assumed. The dynamic IR drop analysis will then give the designer a margin of tolerance, which indicates the minimum intensity of an EM pulsed injection needed to successfully inject a fault into a computation. This methodology, however, is not targeted at harmonic injections.

Researchers also attempted to counteract EM attacks. As the EM injection can easily bypass the metallic shield, countermeasures are usually difficult to be implemented. An

interesting countermeasure which offers resistance to EM-based fault injection is random active shields [6]. Random active shields circulate data on a shield of wires routed above the circuit to be protected. The data are randomly generated, and produced on the one side of the chip and read as well as verified on the other. When a EM wave/pulse is inject into the integrated circuit with the goal of producing a fault, it will also affect the data traversing the shield. This, in turn will trigger an alarm and start a recovery procedure. Another countermeasure is based on the fact that pulsed EM injections can be modeled as transient delay faults: the proposed countermeasure [10] is based on configurable delay structures that would detect any perturbation of the regular operating frequency.

As far as passive attacks are concerned, traditional power attack countermeasures like masking [15] and dual-rail logic [25] are often considered enough to counteract EMA. However, this assumption has not yet carefully evaluated, and might lead to security risks. In fact, although never been demonstrated in practice, a careful and localized EM measurements can distinguish masked data from mask computation (when masking is used) or true network from false network (when dual rail logic is used), leading to a successful attack.

VI. Conclusion

In this paper, we introduced active electromagnetic attacks. We reported previous works which demonstrated how EM pulses can be used to inject faults in embedded processors and cryptographic cores, and we discussed the most recent results obtained attacking ring oscillators. Finally, we highlighted the current research efforts regarding early estimations of EM vulnerabilities and the countermeasures against them. We believe that these last two research directions are very promising and thus need to be further explored in the near future.

Acknowledgments

This research is partly supported by project SPACES (Security evaluation of Physically Attacked Cryptoprocessors in Embedded Systems), project EMAISeCi (ElectroMagnetic Analysis and Injection of Secure Circuits, act ANR-2010-SEGI-012-03), and project TRASP.CH (CTI no. 12079.1 PFES-ES).

References

[1] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The em side-channel(s). In B. S. K. Jr., Çetin Kaya Koç, and C. Paar, editors, *CHES*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer, 2002.

[2] A. Alaeldine, T. Ordas, R. Perdriau, P. Maurine, M. Ramdani, L. Torres, and M. Drissi. Assessment of the immunity of unshielded multi-core integrated circuits to near-field injection. In *Electromagnetic Compatibility, 2009 20th International Zurich Symposium on*, pages 361–364. IEEE, 2009.

[3] D. Alberto, P. Maistri, and R. Leveugle. Investigation of electromagnetic fault injection effects on embedded cryptosystems. In *TRUDEVICE*, 2013.

[4] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *Constructive Side-Channel Analysis and Secure Design*, pages 151–166. Springer, 2012.

[5] E. Biham and A. Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In *CRYPTO*, volume 1294 of *LNCS*, pages 513–525. Springer, August 1997. Santa Barbara, California, USA. DOI: 10.1007/BFb0052259.

[6] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf. Random active shield. In *Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium*, pages 103–113, 2012.

[7] É. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.

[8] S. Chari, J. R. Rao, and P. Rohatgi. Template Attacks. In *CHES*, volume 2523 of *LNCS*, pages 13–28. Springer, August 2002. San Francisco Bay (Redwood City), USA.

[9] A. Dehbaoui, J. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses - practical results on a cryptographic system-. Cryptology ePrint Archive, Report 2012/123, 2012. http://eprint.iacr.org/.

[10] A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses - practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012:123, 2012.

[11] 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, Leuven, Belgium*, pages 7–15, 2012.

[12] A. Dehbaoui, A.-P. Mirbaha, N. Moro, J.-M. Dutertre, and A. Tria. Electromagnetic glitch on the aes round counter. In E. Prouff, editor, *COSADE*, volume 7864 of *Lecture Notes in Computer Science*, pages 17–31. Springer, 2013.

[13] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater, and J.-L. Willems. A practical implementation of the timing attack. In *Smart Card Research and Applications*, pages 167–182. Springer, 2000.

[14] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Çetin Kaya Koç, D. Naccache, and C. Paar, editors, *CHES*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer, 2001.

[15] L. Goubin and J. Patarin. DES and Differential Power Analysis. The "Duplication" Method. In *CHES*, LNCS, pages 158–172. Springer, Aug 1999. Worcester, MA, USA.

[16] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone. Transient iemi threats for cryptographic devices. *IEEE Transactions on Electromagnetic Compatibility*, 55(1):140–148, 2013.

[17] P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Proceedings of CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.

[18] A. T. Markettos. Active electromagnetic attacks on secure hardware. In *Technical Report*. University of Cambridge, Computer Laboratory, 2011.

[19] A. T. Markettos and S. W. Moore. The frequency injection attack on ring-oscillator-based true random number generators. In C. Clavier and K. Gaj, editors, *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 317–331. Springer, 2009.

[20] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller. In W. Fischer and J.-M. Schmidt, editors, *FDTC*, pages 77–88. IEEE, 2013.

[21] NIST/ITL/CSD. Advanced Encryption Standard (AES). FIPS PUB 197, Nov 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[22] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In I. Attali and T. P. Jensen, editors, *E-smart*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer, 2001.

[23] L. Sauvage, J.-L. Danger, S. Guilley, N. Homma, and Y.-I. Hayashi. Advanced Analysis of Faults Injected Through Conducted Intentional Electromagnetic Interferences. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):589–596, 2013. Sponsored by the IEEE Electromagnetic Compatibility Society.

[24] J.-M. Schmidt and M. Hutter. Optical and em fault-attacks on crt-based rsa: Concrete results. In *Proceedings of the Austrochip*, pages 61–67. Citeseer, 2007.

[25] K. Tiri and I. Verbauwhede. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In *DATE'04*, pages 246–251. IEEE Computer Society, February 2004. Paris, France. DOI: 10.1109/DATE.2004.1268856.