SCA Test Results Depend on the Measurement Equipment: Riscure vs. Teledyne LeCroy

Dmytro Petryk[1], Zoya Dyka[1,2], Peter Langendoerfer[1,2] and Ievgen Kabin[1]
[1] *IHP – Leibniz-Institut für innovative Mikroelektronik,* Frankfurt (Oder), Germany
[2] *BTU Cottbus-Senftenberg,* Cottbus, Germany
{petryk, dyka, langendoerfer, kabin}@ihp-microelectronics.com

***Abstract*— Devices employing cryptographic approaches have to be resistant to physical attacks which are effective means to reveal cryptographic keys. In this paper, we discuss results of a horizontal power analysis attack. We illuminated a decapsulated cryptographic accelerator attacked using a laser, while measuring dynamic power consumption. The SCA was performed with different probes, a current probe from Riscure and a differential probe from Teledyne LeCroy. The quality of measured traces strongly depends on the measurement equipment and due to that the success rate of performed SCA attacks also depends on the measurement equipment. Laser illumination affects the power consumption of the chip, but its influence on the success of the attacks was insignificant.**

Keywords*— *Security, Side-Channel Analysis (SCA), laser illumination, power consumption, current probe, laser, fault injection.

I. INTRODUCTION

Physical attacks pose a great threat for today's semiconductor devices, where cryptographic approaches are frequently used to ensure security requirements. The strength of cryptographic approaches is based on the secrecy of the key(s) used, where their length depends on the applied algorithm and security requirements. Using keys of recommended lengths, the algorithms cannot be compromised by cryptanalysis nor brute-force attacks in a reasonable time. The issue is that in real world scenarios the devices can be stolen and attacked in a lab. Side-Channel Analysis (SCA) as well as Fault Injection (FI) attacks are frequently used to breach the device's protection. SCA is based on the analysis of the device's physical emissions. Analysis of the measured emissions can be done using many traces (vertical attack) or using a single measured trace (horizontal attack). FI attacks aim at manipulating the device's normal operation by inducing a fault while the device is in operation. Faults can be injected by perturbing different environmental and operating parameters using different external sources of perturbation. Attacks using lasers are frequently used due to their localized area of influence and accurate timing. Due to the diffraction limited spot size precise laser-based attacks are frequently performed against chips manufactured in "old" technologies, i.e. technologies with large node size. E.g, in [1], it was feasible to manipulate a single transistor, because the illuminated microcontroller was manufactured in a 1.2 µm technology while the laser beam spot size was 1 µm, i.e. the length of transistor gate is comparable to the laser beam spot size. As technology advances, precision of laser-based attacks is decreasing due to the fact that many cells are illuminated simultaneously even when applying state-of-the-art laser with diffraction-limited spot size. At the same time technology downscaling offers reduced power consumption that means the circuit can be more vulnerable to laser illumination, i.e. the gap between no fault and permanent fault can be so small that untraceable transient faults can be infeasible. Due to these facts, precise single bit faults are expected to be unfeasible in future. We expect that, in future, the main focus will be on illuminating a critical block with the goal to improve SCA by increasing its power consumption without injecting a fault. In such an attack the contribution of the illuminated block in the measured power trace will be "more visible", i.e. it can improve extraction of a secret key processed.

In this work, we present the evolvement of laser-based attacks from FI towards their future evolution into SCA under laser illumination attacks against IHP's Elliptic Curve Cryptography (ECC) accelerator. Opposite to attacks published in the past we try to increase the area illuminated by the laser to estimate the feasibility of such attacks using a single laser.

II. SCA UNDER LASER ILLUMINATION

SCA attacks under laser illumination are rare in the literature. Only few works were published in the past. Authors in [2] used a laser beam to increase the power consumption of a circuit by illuminating an SBOX block. As a result, the authors were able to perform successful DPA attacks with a reduced number of power traces as well as to recover a sub-key, which was unfeasible without laser illumination. In [3], the author used laser illumination to detect access events of SRAM memory. In [4], the authors used laser illumination to extract data stored in EEPROM. While illuminating the EEPROM's sense amplifiers, it was possible to retrieve the program stored in the memory.

III. ECC ACCELERATOR AND ATTACK SETUP

IHP's ECC chip i.e. the attacked ASIC was manufactured at IHP in a 250 nm technology. It is designed to perform Elliptic Curve (EC) point (P) multiplication with a scalar (k), i.e. the kP operation, where P is a point on the EC and k is the private key. The operation is performed using a classical partial multiplier over a standardised NIST EC *B-233*. Additional details about IHP's ECC chip can be found in [5]. To perform the attacks the chip was bonded to printed circuit board without any packaging. kP operations were executed with a frequency of 4 MHz. The duration of a kP execution is about 3 ms.

The Attack setup consists of: an oscilloscope and two different commercially available probes from Riscure [8] and Teledyne LeCroy [9], a stable power supply and a modified laser station [6] using a single-mode laser [7]. Details about the laser station and the single-mode laser as well as the evaluation of its parameters can be found in [10].

IV. Preliminary Results and Future Work

In our experiments, measurements were done with a current probe from Riscure[1] [8] and a differential probe from Teledyne LeCroy [2] [9]. The traces were captured with the same oscilloscope applying the same sampling rate of 5GS/s. The analysis of the measured traces in this work was performed using the IHP SCA tool described in [5].

To compare the quality of the traces measured using the Riscure and the LeCroy probe we measured two reference traces, i.e. traces without laser illumination during the execution of the *kP* operation. **Fig. 1** shows the measured traces. Both traces in **Fig. 1** demonstrate clearly that signal/noise ratio of the trace which was measured with the LeCroy differential probe is significantly better than for trace measured with the Riscure current probe. According to our analysis using the same analysis method the correctness of the best key candidate[3] is 70 % and 86 % for measurements done with the Riscure and the LeCroy probe, respectively.

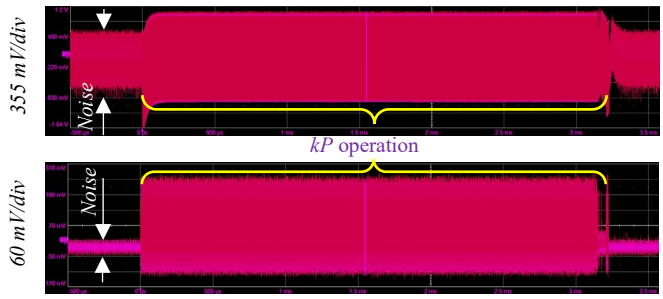

Fig. 1. Measured traces using the current probe from Riscure (top) and differential probe from Teledyne LeCroy (bottom).

To estimate the influence of the laser illumination on the measured trace as well as on the success of the attack we selected the LeCroy differential probe for measurements. We illuminated the partial multiplier of the *kP* accelerator during the measurement. It was expected that illuminating the partial multiplier deteriorates the key extraction because the multiplier is not an SCA leakage source and increasing its contribution to the total power consumption hides the contribution of the other design blocks. We applied different laser beam power and laser beam spots. The influence of the laser illumination on the dynamic power consumption of the cryptographic accelerator was insignificant but the static power consumption was visibly increased. We observed an offset of the measured trace of about 17 mV in comparison to the reference trace. This corroborates with results given in [12], where authors report a significant increase in the static power consumption of a chip by illuminating selected cells with a red laser. Nevertheless, the influence on the success of the attack was insignificant. The correctness of the best key candidates deviates in a range of ±2 %. We assume that laser illumination did not influence the attack's success rate significantly due to the low laser output power (laser limitations) and to the small area illuminated compared to the area of the whole design. We illuminated only from 0.01 to 0.11 % of area of the accelerator.

In future work, we plan to experiment with other laser sources that offer larger spots with higher output power with the goal to improve SCA attack. We expect that increasing the laser beam output power will cause bigger changes of the static power consumption. We expect a significant influence of the laser illumination on the static power consumption of the attacked chip. Attacks exploiting the Static Consumption under Laser Illumination (SCuLI attacks) are novel, and not investigated yet. Feasibility and potential of SCuLI attacks have to be evaluated. If they are feasible appropriate countermeasures have to be investigated. We also plan to perform SCuLI attacks against chips manufactured in a scaled technology.

V. Conclusion

Our results highlight the importance of cross-validation with different measurement tools, as security test results and by that the final risk assessment can vary significantly. The measurement equipment even that from a world-renowned security-test company, can indicate a high resistance to attacks but the same analysis of the traces measured using equipment from another manufacturer can indicate a high vulnerability of the design under assessment. Our measurements demonstrate that laser illumination influences the power consumption of the illuminated chip. The potential of such attacks has to be investigated since they can be especially dangerous against chips manufactured in scaled technologies.

References

[1] S. P. Skorobogatov et al., "Optical Fault Induction Attacks", Cryptographic Hardware and Embedded Systems, Feb 2002, pp. 2-12.

[2] J. Di-Battista et al., "When Failure Analysis Meets Side-Channel Attacks", In: Mangard, S., Standaert, FX. (eds) Cryptographic Hardware and Embedded Systems, CHES 2010. Lecture Notes in Computer Science, vol 6225, Springer, Berlin, Heidelberg, pp. 188-202.

[3] S. Skorobogatov, "Optically Enhanced Position-Locked Power Analysis", In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 61–75. Springer, Heidelberg, pp. 61–75.

[4] J. Sakamoto et al., "Laser irradiation on EEPROM sense amplifiers enhances side-channel leakage of read bits", 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Taiwan, Dec. 2016, pp. 1-6.

[5] I. Kabin, "Horizontal address-bit SCA attacks against ECC and appropriate countermeasures", Doctoral thesis, BTU Cottbus – Senftenberg, 2023. DOI: 10.26127/BTUOpen-6397

[6] Riscure. Diode Laser Station Datasheet, 2011. URL: https://getquote.riscure.com/en/inspector-fault-injection.html

[7] Alphanov PDM laser sources. URL: https://www.alphanov.com

[8] Riscure. Current Probe. URL: https://getquote.riscure.com/en/quote/2101059/current-probe.htm

[9] Teledyne LeCroy. Differential probe ZD1500. URL: https://www.teledynelecroy.com/probes/differential-probes-1500-mhz/zd1500

[10] D. Petryk, "Investigation of sensitivity of different logic and memory cells to Laser Fault Injections", Doctoral thesis, BTU Cottbus – Senftenberg, 2024. DOI: 10.26127/BTUOpen-6664

[11] Riscure. About Riscure. URL: https://www.riscure.com/about-riscure

[12] D. Petryk et al., "On the Influence of the Laser Illumination on the Logic Cells Current Consumption", 2023 30th IEEE International Conference on Electronics, Circuits and Systems, Istanbul, Turkiye, 2023, pp. 1-6.

[1] A world-renowned company that performs security testing and certification for many companies [11] and provides equipment for SCA and FI attacks.

[2] A world-leading provider of test and measurement solutions.

[3] It shows how many bits of the 232 bits key are correctly revealed. E.g. 70 % correctness of the key candidate means that ~162 bits were successfully revealed and ~70 bits have yet to be revealed.