Optical Fault Injection Attacks: Single-mode versus Multi-mode Laser

Dmytro Petryk[1] Zoya Dyka[1] Peter Langendörfer[1],[2]

[1]IHP – Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

33rd Crypto Day, 17 September 2021

crypto day matters 33 (2021)
Beiträge vom 33. Kryptotag, 17.09.2021, online.
doi:10.18420/cdm-2021-33-23

To reveal the secret data used in a cryptographic operation Fault Injection (FI) attacks can be performed for example optical FI attacks using a laser. Here we compare the optical FI attacks performed with two different lasers: a red (808 nm) multi-mode laser from Riscure [1] and a red (808 nm) single-mode laser from Alphanov [2]. Single-mode lasers have smaller laser beam spot sizes than the multimode lasers, i.e. they allow to inject faults more precisely, but their beam output power is lower compared to multi-mode ones. This imposes that using single-mode lasers the attacks can be performed with higher spatial accuracy than when using multi-mode ones. In this work we assess the influence of the different lasers on success of FIs. We attacked a chip implemented in an old IHP's 250 nm technology. The chip contains 4 types of gates: inverter, NAND, NOR and Flip-Flop gates. The details of the chip structure can be found in [3]. We chose this chip due to the fact that it is manufactured without any metal fillers, i.e. all transistors, connections, wires, etc. are clearly visible from top of the chip using microscope camera, i.e. a laser beam can reach the transistor level barrier-free from the front side of the chip. The both lasers were used in the modified Riscure Diode Laser Station (DLS) [4], i.e. the laser beams were focused by the same optical system. In [3] we have successfully injected faults into the same chips using standard Riscure DLS before its modification. The modification was done by Riscure with the goal to support the both lasers. In our experiments, we were able to inject repeatable faults into all 4 types of gates with a slight deviation of laser beam output power using 100× and 50× magnification objective. TABLE 1 shows the minimum laser beam power that we applied in our experiments to inject repeatable faults. In all experiments done the laser beam pulse duration was set to 100 ns, corresponding to Riscure Inspector Fault Injection software.

Using the multi-mode laser in the modified DLS we injected faults into different gates starting from 35 % and 25 % laser beam power with 100× and 50× magnification objective respectively. Compared to the results given in [3] to inject faults using modified DLS higher laser beam power is required. Using the

Table 1: Minimum laser beam power that ensures successful FIs into IHP Libval025 chips.

Laser	Multi-mode Riscure laser				Single-mode Alphanov laser	
DLS	standard		modified		modified	
Magnification objective	100×	50×	100×	50×	100×	50×
Minimum laser beam power applied for repeatable fault injections, %*	18	19	35	25	10	15

* Measurement unit of power in the Riscure Inspector FI software.

single-mode laser in the modified DLS we observed successfully injected faults starting from 10 % and 15 % laser beam power with 100× and 50× magnification objective respectively. According to our observations, faults can be injected successfully with significantly lower laser beam power using single-mode Alphanov laser (total peak power is 0.848 mW measured at 100 kHz/100 ns according to the laser certificate) than when using multi-mode Riscure laser (peak power is 14 W according to [1]). These results clearly show that the optical FI attacks can be successfully performed using also a low-power laser source: the size of the laser beam spot and the spatial distribution of the beam intensity are the decisive factors. The detailed information about the laser beam parameters is usually not provided by the laser manufacturer.

References

[1] Riscure (2011). *Diode Laser Station. Inspector Datasheet.* URL `https://www.riscure.com/security-tools/inspector-hardware/`.

[2] Alphanov (2020). *Pulse-on-Demand Modules.* URL `https://www.alphanov.com/en/products-services/pdm-laser-sources`.

[3] D. Petryk, Z. Dyka & P. Langendörfer (2020). Sensitivity of Standard Library Cells to Optical Fault Injection Attacks in IHP 250 nm Technology. *9th Mediterranean Conference on Embedded Computing (MECO)* 1–4.

[4] D. Petryk, Z. Dyka, R. Sorge, J. Schäffner & P. Langendörfer (accepted). Optical Fault Injection Attacks against Radiation-Hard Shift Registers. *24th Euromicro Conference on Digital System Design (DSD)* .