Optical Fault Injections: Most Often Used Setups

Dmytro Petryk Zoya Dyka Peter Langendoerfer

IHP
Frankfurt (Oder), Germany

Optical Fault Injection (FI) attacks are significant threats for semiconductor devices. It aims to induce an error into the device to disrupt its normal functioning. This can lead to access to confidential data, such as passwords, logins, etc. that are stored in the device memory. FI attacks using laser sources are semi-invasive attacks that require physical access to the internal structure of the attacked device. The main advantages of optical FI attacks are accurate timing and precise spatial location. Success of optical FIs depends on a lot of parameters, such as wavelength, spot size, timing, pulse width and intensity of light. Our work presents an overview of optical FI attacks concentrating on the comparison of laser systems setup, especially on the most often used equipment. The data given Table 1 are based on our investigation of about 40 papers. Most optical FI attacks are carried out with near infrared (NIR) (∼1064 nm) and red (∼808 nm) laser sources. Wavelengths of green light (∼532 nm) are used more seldom e.g. with the Gemalto laser fault injection platform [2]. NIR range wavelengths are used for attacks through the backside (substrate) and visible light for frontside attacks. Most used setups for optical FI consists of a multimode laser source that leads to increased spot size in comparison to the single mode lasers. For example typical spot sizes of Riscure laser systems are $6\times1.4\ \mu m^2$ for 808 nm and 1064 nm wavelengths with 50× magnification lens [4]. Single mode laser, for example, Alphanov laser system with 1064 nm wavelength can be focused to a spot of $1.77\ \mu m^2$ with 50× magnification lens [1].

Table 1: Most often used laser systems for optical FI attacks

Manufacturer	Multimode	Wavelength	Spot size	Pulse duration	Power	Number of references
Riscure	yes	808/1064 nm	6×1.4 µm²	20-100000 ns	14/20 W	11 of 36
Alphanov	no	1064 nm	1.77 µm²	2-CW[2] ns	4.6 W	2 of 36
Gemalto[1]	yes	532 nm	220 µm²	6 ns	no information	2 of 36

[1] The parameters of the laser system are given in [3].
[2] Continuous wave.

The recent manufacturing technologies of semiconductor devices reduce the success rate of FI attacks due to the increased number of metal layers blocking the line-of-sight and due to the fact that the dimension of the laser spot affects a larger number of transistors. Also the use of BGA packages reduces the success of optical FI attacks significantly due to the more complex attack preparation process. Nevertheless the mostly reported in the literature attacks – 29 from 36 publications – used an infrared laser for the backside FI.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-11

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 722325.

References

[1] Alphanov (2018). *Pulse On Demand Modules*. URL http://www.alphanov.com/.

[2] Gemalto (2006). URL https://www.gemalto.com/companyinfo.

[3] Y. Monnet, M. Renaudin, R. Leveugle, N. Feyt, P. Moitre & F. M'Buwa Nzenguet (2006). Practical Evaluation of Fault Countermeasures on an Asynchronous DES Crypto Processor. *IOLTS* 125–130. ISSN 1942-9401. URL https://dx.doi.org/10.1109/IOLTS.2006.50.

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