Lehrstuhl für Sicherheit in der Informationstechnik
Fakultät für Elektrotechnik und Informationstechnik
Technische Universität München

**FP/BA/MA:**

# Improving an Optical Fault Injection Setup

## Description:

Fault attacks pose a serious threat to the implementation of cryptographic algorithms, as they can be performed using even low cost equipment [1]. Usually localized semi invasive optical fault attacks are considered out of reach for attackers with a limited budget. But as shown by [2] it is indeed possible to carry out this kind of attacks. Your objective would be to improve the existing open-fi[1] setup in terms of spatial and temporal resolution.

# 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*, 94(2):370–382, feb 2006.

[2] Oscar M. Guillen, Michael Gruber, and Fabrizio De Santis. Low-cost setup for localized semi-invasive optical fault injection attacks. In *Constructive Side-Channel Analysis and Secure Design*, pages 207–222. Springer International Publishing, 2017.

## Please apply to:

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
M.Sc. Michael Gruber
Theresienstraße 90
80333 München
or via email: m.gruber@tum.de

Visit us at https://www.sec.ei.tum.de/

[1] `https://github.com/open-fi/fault-injector/`

*January 27, 2019*