**Background**

**Fault Injection Attacks** allow to break mathematically secure cryptographic schemes by disturbing the execution of the actual implementation, e.g., on a microcontroller or a smartcard. In the past, semi-invasive techniques based on the exposure of an IC to *laser light* have proven to be particularly successful.

**What can you do?**

Our group is currently building an advanced lab setup for performing laser fault injection attacks. As the existing fault injection environment is based on a FPGA board, the aim is to extend this platform to include laser-based attacks. The new setup features two independent laser diodes to overcome certain countermeasures, e.g., redundant computation in two independent parts of the IC.

The first focus of the thesis is thus on implementing the logic required to control the position and the timing of the laser beams, capture images using a built-in camera, and provide a user interface on the controlling PC. Next, practical attacks on real-world devices can be realised. Optionally, advanced topics such as a combination of fault injection and side-channel analysis may be included.

The topic is well suited both for students of ITS and ET/IT. To practically implement the algorithms, it is required that you are familiar with VHDL and at least one suitable PC programming language, e.g., C or C++. However, this is not a strict requirement, as most concepts base on simple ideas that are quickly understood. It is possible to realize only a part of the whole project as a Studien- or Bachelorarbeit.

**Contact**

If this sounds interesting to you, please contact Falk Schellenberg ([falk.schellenberg@rub.de](mailto:falk.schellenberg@rub.de)).