Forschungspraxis/Master’s Thesis:

The next Level of BCH Codes & PUFs

Possible in German or English

Abstract:
PUFs exploit characteristics of hardware similar to a fingerprint to derive secret keys. Error correcting codes are required to deal with any bit errors induced by noisy PUFs. While BCH Codes are state-of-the-art for this task, the current approach can be pushed further by enhancing the decoder: more powerful coding techniques can correct more errors at the cost of a higher complexity.

The goal is a software implementation of such a BCH decoder in the context of PUFs. Therefore, the following tasks are likely:

- Getting familiar with PUFs and BCH codes
- Conducting research of suitable algorithms
- Implementing the new approach to test its feasibility

Knowledge in the following topics is helpful:

- Good programming Skills Matlab/Python
- Basic knowledge about error correcting codes

Contact:
M.Sc. Christoph Frisch
Technical University of Munich
Chair for Security in Information Technology
Head: Prof. Dr.-Ing. Georg Sigl
Arcisstr. 21, 80333 Munich (Germany)
Email: chris.frisch@tum.de