Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Interdisciplinary Project, Bachelor's Thesis, Master's Thesis, Forschungspraxis

Side - channel analysis of error - correcting codes for PUFs

Physical Unclonable Functions (PUFs) exploit manufacturing process variations to generate unique signatures. PUF and error-correcting codes can be joined together to reliably generate cryptographically strong keys. However, the implementation of error-correcting codes is prone to physical attacks like side-channel attacks. Side-channel attacks exploit the information leaked during the computation of secret intermediate states to recover the secret key. Therefore, the implementation of error-correcting codes must also involve the implementation of proper countermeasures against side-channel attacks.

The goal of this thesis is to evaluate the side-channel resistance of a secure implementation of error-correcting codes for PUFs on FPGA. The thesis consists of the following steps:

- Get familiar with currently available implementations of error-correcting codes for PUFs
- Adapt and improve current implementations (VHDL)
- Develop a measurement setup for side-channel analysis (Matlab/Python)
- Perform side-channel analysis using the state-of-the-art EMF measurement equipment in our lab (Oscilloscope knowledge + Matlab/Python required)

Prerequisites

The ideal candidate should have:

- Previous experience in field of digital design (VHDL/Vivado/Xilinx FPGA)
- Basic knowledge on using lab equipment (e.g Oscilloscope,...)
- Basic knowledge in statistics
- Good programming skills in Matlab/Python
- Attendance at the lecture “Secure Implementation of Cryptographic Algorithms” is advantageous

Contact

Dr.-Ing. Michael Pehl
Chair for Security in Information Technology
Head: Prof. Dr.-Ing. Georg Sigl
Technical University of Munich
Arcisstr. 21, 80333 Munich (Germany)

Email: m.pehl@tum.de

Advisors

Michael Pehl, Lars Tebelmann