Implementation of a Secure System Based on PUFs

Physical Unclonable Functions (PUFs) exploit manufacturing process and physical environmental variations to generate unique signatures. These signatures can be used for key generation or in challenge-response protocols.

In this work, a secure system should be implemented on FPGA, which uses a PUF to enable security features. For this purpose, an existing PUF-implementation with corresponding key derivation must be transferred to the target platform. Afterwards, a operating system must be taken into operation on the target platform and security mechanisms for the system must be established based on the PUF.

During the course of the thesis, the following should be covered (the tasks are scheduled for a Master thesis; for other kinds of theses subtasks will be selected):

- Get familiar with the target platform and requirements for the thesis
- Plan and conduct the implementation
- Test the implementation, e.g. w.r.t. performance

This work can be conducted in German or English. The results of this work will be used in the BMBF funded project ALESSIO. Please contact the thesis supervisor for further details. In case of a high quality of the work, results might be published.

Prerequisites

- Good VHDL skills
- Good MC programming skills
- Good knowledge about security mechanisms (e.g. through the lecture Embedded Systems and Security)

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