Tool Exploration for PUF-Analysis

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 both cases it is important to have unpredictable PUF-responses.

In this work, a tool for statistical analysis should be explored w.r.t. its applicability of PUFs.

During the course of the thesis, the following should be done:

- Get familiar with PUFs and their requirements as well as with the tool which should be applied to PUFs.
- Define a test set for the tool using known unpredictable and predictable real world PUF-responses and virtual data.
- Apply the tool to evaluate the usability and the limits.
- Justify found limitations mathematically.

This work can be conducted in German or English. Please contact the thesis supervisor for further details. In case of a high quality of the work, results might be published.

Prerequisites

- Good mathematical skills (especially in stochastics)
- Good programming skills in C/C++

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