Compression Algorithms for 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 both cases it is important to have high entropy in the PUF-response. However, since response bits of a PUF might be correlated, computation of entropy is not trivial. Therefore, compression algorithms are used to approximate the entropy in a PUF-response.

The goal of the project is to compare different compression algorithms and to apply them to different real-world data sets measured from PUFs.

The thesis will include the following steps (the tasks are scheduled for a Master thesis; for other kinds of theses subtasks will be selected):

- Get familiar with currently available compression algorithms.
- Implementation of selected compression algorithms and adaptation to special requirements in the PUF-context (C++)
- Definition of a test setup and test of the implemented algorithms.
- Evaluation of different real-world PUFs using the implemented algorithms.

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.

References:

- Ignatenko, T.; Schrijen, G.-J.; Skoric, B.; Tuyls, P.; Willems, F.;"Estimating the Secrecy Rate of Physical Uncloneable Functions with the Context-Tree Weighting Method"; ISIT 2006

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

Florian Wilde, Michael Pehl