Exploration of Context Tree Weighting as a Compression Algorithms for Physical Unclonable Functions

Physical Unclonable Functions (PUFs) extract secrets from inherently available manufacturing variations in hardware. One criterion for the quality of PUFs is the entropy which can be extracted from it. However, entropy cannot be computed accurately in these cases. Thus, a bound for entropy is computed by compression.

The approach which is used for the approximation by compression in the context of PUFs is the Context Tree Weighting Method (CTW). During the course of the thesis the following should be covered (tasks are scheduled for a Master thesis; for other kinds of theses subtasks will be selected).

1. Research, what properties make CTW a good candidate for entropy evaluation of PUFs and compare to other approaches.

2. Improve a given implementation of CTW to improve accuracy and to improve the benefit gained from the analysis.

3. Analysis of the CTW implementation w.r.t. the realized improvements.

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
Advisors

Michael Pehl