ulm university universität ulm

Bachelor's Thesis:
Helper Data Methods for Error Correction in PUFs

M.Sc. Sven Müelich (sven.mueelich@uni-ulm.de)
Institute of Communications Engineering

Background

A Physical Unclonable Function (PUF) is a, typically digital, circuit that possesses an intrinsic randomness due to process variations during manufacturing and can therefore be used to generate random cryptographic keys. These keys can be reproduced on demand. However, the PUF output when reproducing a key varies, which can be interpreted as errors. Thus, error correction must be used in order to compensate this effect. Since for a given code, the PUF response is not a codeword with high probability, so-called helper data methods are required. There are several known ways of generating helper data in PUFs. The two most common methods are the code-offset and the syndrome construction cf. [Maes12, Section 6.2.1].

Idea

Instead of extracting helper data in order to reproduce a key, it was currently studied in [MB16] if a PUF response can be directly used as codeword. Therefore, an individual code has to be constructed for each PUF instance, such that its response is a codeword. In [MB16] we showed, that this approach is possible and explained how suitable codes can be constructed.

Task

In a theoretical part, the student should become familiar with different techniques for error correction in PUFs. Existing helper data methods, their advantages and disadvantages should be summarized from the literature. In a practical part, based on [MB16], suitable codes should be constructed. This requires the implementation in any programming language and performing simulations.

Prerequisites

- Good programming skills in any programming language are required.
- Basic knowledge about coding theory (Einführung in die Nachrichtentechnik)

Literature

[Maes12] Roel Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*, 2012

[MB16] Sven Müelich, Martin Bossert, *A New Error Correction Scheme for Physical Unclonable Functions*, 2016

Published: 12.10.2016

NACHRICHTENTECHNIK Universität Ulm

Ulm University
Albert-Einstein-Allee 43
89081 Ulm, Germany