Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Assistant (Student)

PUF Error Correction Code Hardware Implementation Optimisation

Physical unclonable functions (PUFs) are gaining traction as a method for the storage of secrets: The security issues of nonvolatile memory for key storage are avoided entirely by using device hardware fingerprints to reconstruct the secrets at run time, keeping them in memory only while they are needed.

Being based on subtle manufacturing tolerances, PUFs are naturally affected by ageing and environmental effects and are thus unreliable on their own. Consequently, using a PUF necessitates employing an error-correction code to compensate these effects and sustain a high availability in spite of noisy PUF measurements.

Different coding schemes have been proposed and analysed for PUFs. Some insight into their properties can already be gained from software simulations, but a more complete security evaluation can only be based on a concrete hardware implementation.

A VHDL decoder implementation, which is adaptable to different parameters via a Python script, already exists, but suffers from high hardware overhead, which hinders FPGA experiments and comparability to other codes.

The aim of this work is the evaluation of more advanced optimisation techniques for this decoder design, with the goal of shrinking it significantly.

This work can either be conducted in German or in English.

I am happy to provide more details and answer your questions upon request.

Prerequisites

- Necessary: Advanced experience using either VHDL or Verilog.
- Favourably: Basic knowledge of error-correction codes and their implementation.
- Optionally: Background knowledge of physical unclonable functions.

Contact

If you are interested in this work, please contact me via email with a short CV and grade report. We will then arrange a short meeting where we can discuss the details.

Jonas Ruchti, M.Sc.
Technical University of Munich, Chair of Security in Information Technology
Room N1014
E-Mail: j.ruchti@tum.de

Advisors

Jonas Ruchti