Optimising the Loop PUF

Physical Unclonable Functions (PUFs) are methods to measure hard-to-control manufacturing variabilities of electronic devices at runtime. These measurements can be used as device-unique fingerprints, or as a basis for authentication protocols or the storage of secret keys.

The Loop PUF is an established PUF design, which uses intrinsic delays in silicon logic to derive PUF responses by measuring frequencies of purpose-built on-device oscillators. The Loop PUF is easily integrated into FPGAs and more forgiving in its design than other PUFs—though these conservative design choices might leave room for optimisation. The focus of this work is to explore these areas while making sure the resulting PUF still meets its performance specifications.

The aim of this work is to

- gradually modify an existing Loop PUF FPGA design written in VHDL,
- carry out measurements using an existing Python measurement framework,
- evaluate the optimised PUFs performance, and
- summarise the findings in the context of a general Loop PUF.

Prerequisites

**Necessary:** Basic experience with VHDL, FPGAs
**Necessary:** Experience coding in Python

This work can either be conducted in German or in English. I am happy to provide more details and answer your questions upon request.

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