Hardware Implementation of an Error-Correction Code for PUFs

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.

The aim of this work is the implementation of an error correction code decoder in hardware. This implementation should be adapted to the use in a PUF key storage system and should be flexible enough for the use in multiple scenarios. The decoder can either be an adaptation of an existing open-source decoder or a new implementation.

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: Experience using either VHDL or Verilog.
- Favourably: Basic knowledge of error-correction codes.
- Optionally: Background knowledge of physical unclonable functions.

Contact

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