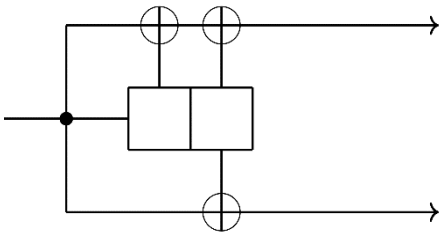
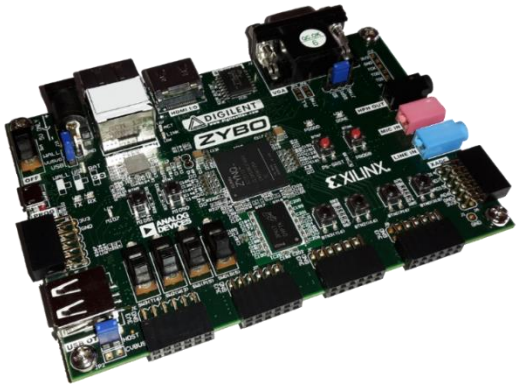
PUF Error Correction using Convolutional Codes on an FPGA

Bachelor -Thesis

Physical Unclonable Functions (PUFs) generate random and reproducible information from the inherent mismatches of circuit components. Their behavior depends on limited control at the time of fabrication, making their responses not only unpredictable but also physically unclonable. 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.

Convolutional codes became popular in applications like GSM, UMTS or LTE as they provide efficient maximum-likelihood and soft-decision decoding. Additionally the easy hardware implementation makes them very useful for PUFs.





The goal of this thesis will be the implementation of an error correction unit using convolutional codes on a Xilinx FPGA. The hardware has to be optimized for runtime and area efficiency. An existing test framework should be used to evaluate the functionality with real PUF responses.

What we expect: Knowledge of one programming language (best c) and basic circuit design. Basic knowledge about coding theory ("Einführung in die Nachrichtentechnik" or similar lectures.) Organized and well documented research and dedication to successful work.

Contact

M. Sc. Holger Mandry, Email: holger.mandry@uni-ulm.de
Institute of Microelectronics, www.uni-ulm.de/in/mikro/
M. Sc. Sven Müelich, Email: sven.mueelich@uni-ulm.de
Institute of Communications Engineering, www.uni-ulm.de/in/nt/

Published: 07.08.2019