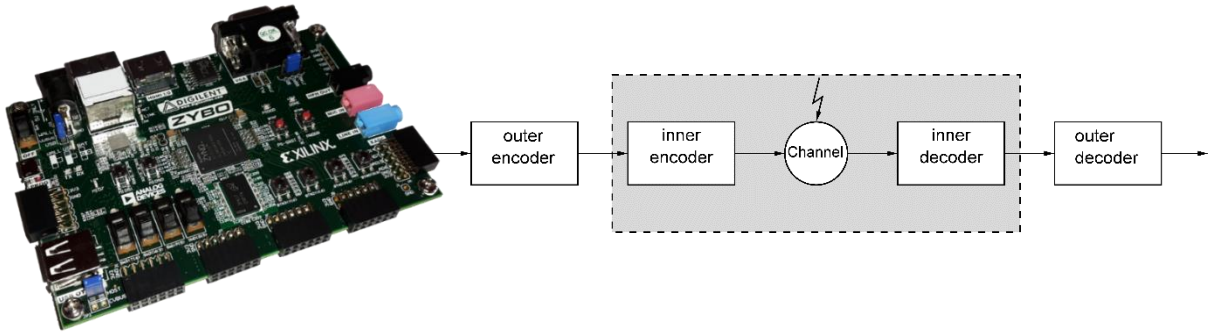
ulm university universität ulm

PUF Error Correction using Reed-Solomon Codes in a Concatenated Code Construction on an FPGA

Master -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.

Reed-Solomon codes are one of the most often used algebraic block codes. Data transmission in space missions, data storage on CDs/DVDs and QR codes belong to their various applications. Often, Reed-Solomon codes are also used in concatenated schemes, for example for error correction in the DVB and DSL standards. In general, long codes have better error correction capabilities than short codes, while short codes can be decoded more efficiently. The key benefit of code concatenation is to combine these features by using several short codes to construct one long code.



The goal of this thesis will be the implementation of concatenated codes using Reed-Solomon codes as their components on a Xilinx FPGA. The hardware has to be optimized for runtime and area efficiency. With an existing test framework the functionality with real PUF responses has to be evaluated and compared to existing implementations of other error correction techniques.

What we expect: Knowledge of one programming language (best c) and basic circuit design. Basic knowledge about channel coding ("Channel Coding" 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: 09.08.2019