New Error Correction Schemes for Physical Unclonable Functions

Abstract
Physical Unclonable Functions (PUFs) are an alternative to conventional key storage for cryptographic keys ranging from consumer IoT devices to next-generation high-security applications. The secret inside the PUF is created by manufacturing variations. Syndrome coding and quantization enable error correction by storing individual external helper data for each device. In addition, error-correcting codes are used to improve the reliability of the key.

Currently, there are several open topics, covering different aspects of syndrome coding, quantization, error-correcting codes, as well as efficient implementations.

Requirements:
- Background in Communications Engineering
- MATLAB/Scilab/Octave Programming Skills
- Creativity and Independent Work Style
- Background in Channel Coding preferred
- C, Assembler or VHDL Programming Skills preferred
- Additional Knowledge in Cryptography, Information Theory or Statistics preferred

Date: 29.10.2018
Start: any time

Contact
Dr.-Ing. Matthias Hiller
Fraunhofer Institute AISEC
Physical Security Technologies Group
Parkring 4, 85748 Garching (near Munich)
E-Mail: matthias.hiller@aisec.fraunhofer.de
Phone: +49 89 322-9986-162