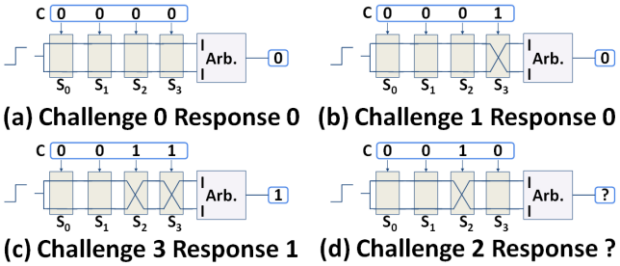
Chair for Embedded Systems

Prof. Dr. J. Henkel

Bachelor/Master Thesis

Characterization of Physical Unclonable Functions (PUFs)



(a) Challenge 0 Response 0 (b) Challenge 1 Response 0

(c) Challenge 3 Response 1 (d) Challenge 2 Response ?

With the rise of the IoT, resource-constrained and power-constrained devices attract more attention. The need for lightweight solutions as alternatives to resource-intensive applications became more urgent. Moreover, as the number of connected devices grew, authenticating them became more challenging. Traditionally, this would be performed by using hash functions and secure memory to store a key, which both come at a high cost.

PUFs emerged as a suitable lightweight alternative to hash functions to authenticate the devices. Using the inherent minute differences between ICs, they can generate IC-specific responses for input challenges coming from a so-called verifier. The PUF design is not a secret, however, without having physical access to the IC that implements it, its behavior cannot be predicted. Numerous works investigated the usage of PUFs for different applications, such as RFID tags and electronic transaction protocols.

At CES we already implemented some PUF designs on FPGAs. The aim is to use them as accelerators loaded dynamically at runtime. In order to reliably use them, characterization of the PUFs needs to be performed. Initial characterization is already done but it needs to be extended to different environmental and runtime scenarios. Such as increased temperature or increased noise from other designs on the same FPGA.

Tasks of the student

Tasks will vary according to the thesis topic and scope (master or bachelor). Tasks of the student might include but are not limited to:

- Developing new PUF designs by partially reusing existing accelerator designs
- Measuring and collecting Challenge Response Pairs from different runtime scenarios
- Designing a framework for automated collection and test of the PUFs
- Extending our designs to other FPGA types and boards

Skills beneficial for the thesis

- Programming Skills (C, C++, Python)
- Knowledge of VHDL

Skills acquired with the Thesis

- Work in a research environment
- Hands-on experience in Hardware and Software development
- In depth knowledge of Hardware Security

Contact

- Hassan Nassar, M.Sc., hassan.nassar@kit.edu http://ces.itec.kit.edu/~nassar
- Dr.-Ing. Lars Bauer, lars.bauer@kit.edu http://ces.itec.kit.edu/~bauer