**BA:**

**Implementation of a built-in self test for PUFs**

Physical unclonable functions (PUFs) utilize inherent manufacturing variations to derive device dependent secrets for key storage or device authentication. The binary response of a certain PUF instance should be unpredictable even for the manufacturer, who is able to thoroughly analyze a large number of instances of the exact same design. At the same time, the PUF response should remain stable over the lifetime of the device and environmental conditions like supply voltage or temperature. To detect failures of the PUF primitive due to extreme environmental conditions or physical attacks, a built-in self test (BIST) based on the NIST test suite for TRNGs has been proposed [1].

In this Bachelor's Thesis, a BIST based on different tests, which were developed at the chair, shall be implemented in VHDL on a state-of-the-art FPGA platform.

**Prerequisites:**

- Solid VHDL skills
- Curiosity regarding PUFs

**Please apply to:**

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Dipl.-Ing. Florian Wilde
Arcisstraße 21
80333 München
or via email: florian.wilde@tum.de

Visit us at https://www.sec.ei.tum.de/

**References**