Research Internship/Master’s Thesis:
Extension of Spatial Correlation Analysis for PUFs

Physical unclonable functions (PUFs) utilize inherent manufacturing variations to derive device dependent secrets for key storage or device authentication. To obtain high entropy secrets, it is essential that the individual bits of the PUF response are free from correlation and bias. However, not all manufacturing variations are local effects. Some cause gradual parameter changes over the die, which affect multiple bits of the PUF response together. Spatial correlation analysis (SPACA) has been shown to detect such effects for single-challenge PUFs like SRAM or Ring-Oscillator PUFs [1].

In this work the applicability of SPACA on multi-challenge PUFs like Arbiter or Bistable-Ring PUFs should be investigated. Experiments with real-world datasets should accomplish a theoretical discussion of the selected approach and its assumptions and restrictions. If the work is performed as Master’s Thesis, an implementation of the approach in Matlab, R, or Julia rounds the work off.

Prerequisites:

- Basic understanding of statistics
- 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