Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Master's Thesis

Side-Channel Attack on PUF Primitives Using Localized EM

Cryptographic key storage is an important requirement in embedded devices. Physical Unclonable Functions(PUFs) provide a cost-efficient alternative to secure key storage. They exploit manifacturing variations to derive device-specific secrets for key storage and device authentication.

Side-channel analysis (SCA) of PUFs exploits the fact, that certain characteristics of the PUF structures and their surrounding evaluation circuitry can be observed by an attacker, e.g., by high-resolution localized EM measurements [1-3].

Depending on your background and type of work, possible tasks of this project include

- Get familiar with PUF primitives and their implementation
- Implement a PUF design (VHDL)
- Develop/Extend a measurement set-up for localized EM side-channel analysis (Python)
- Perform SCA on PUF primitives using the IC scanner positioning system in our lab

This work can be conducted in English or German. In case of high quality of the work, results might be published.

References

[1] Merli et al.: Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures. 6th Workshop on Embedded Systems Security (WESS'2011), ACM, 2011
[2] Merli et al.: Localized electromagnetic analysis of RO PUFs. IEEE International Sympo-sium on Hardware-Oriented Security and Trust (HOST), 2013, 19-24
[3] Tebelmann et al.: Side-Channel Analysis of the TERO PUF. Constructive Side-Channel Analysis and Secure Design (COSADE), Springer International Publishing, 2019, 43-60

Prerequisites

- Basic knowledge of lab equipment (e.g. oscilloscope, voltage suppply, ...)
- Good programming skills in Python
- Basic experience in the field of digital design (ideally VHDL/Vivado/Xilinx FPGAs)

Contact

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Lars Tebelmann
Theresientr. 90, N1010
E-Mail: lars.tebelmann@tum.de

Advisors

Lars Tebelmann