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

Forschungspraxis, Bachelor's Thesis

Quantitative Comparison of Different Side Channels

Despite any theoretical strength a cryptographics algorithm might offer, a real-world application can only be as good as the eventual implementation. For example, side channel leakage is a common problem: unless particular care is taken during the implementation, any computation running on real hardware leaks information about the processed secrets. Common examples include timing side channels, where the execution time depends on secret bits, or power side channels, where e.g. a CPU's power draw depends on the processed data.

This work is concerned with gathering measurement data from cryptographic algorithms running on embedded hardware before running attacks based on the collected traces. Ultimately, the aim is a quantitative comparison of different operating conditions and side channels, assessing the information content of the emanated signals and the resulting complexity of extracting the processed secrets using a side channel attack.

Prerequisites

- Necessary: Experience programming in Python
- Preferrable: Basic understanding of cryptographics algorithms
- Preferrable: Experience programming microcontrollers in C
- Optional: HDL hardware design experience

Contact

If you are interested in this work, please contact me via email with a short CV and grade report. We will then arrange a short meeting where we can discuss the details.

Jonas Ruchti, M.Sc.
Technical University of Munich, Chair of Security in Information Technology
Room N1014
E-Mail: j.ruchti@tum.de

Advisors

Lars Tebelmann, Jonas Ruchti