Hide and Seek

Side-Channel based exfiltration of cryptographic secrets is an long-standing and ever occuring problem when implementing cryptographic algorithms under the assumption of real hardware.

Established formally-proved countermeasures against side channels do not provide definite protection. In the real world, a multitude of hardening measures are necessary to provide in depth-protection.

In this thesis, you will try and compare different methods of in-depth protection.

Prerequisites

The following list of prerequisites is neither complete nor binding, but shall give you an idea, what the topic is about.

- Sufficient knowledge in a High-Level Programming language such as python for measurement automisation etc.
- Basic to intermediate knowledge of a hardware description language such as vhdl or verilog for designing the hardening measures
- In the optimum case experience with FPGAs to try the measures in the real world.
- Knowledge in design/architecture of cryptographic algorithms to know when and how to do the hardening.

Contact

If you are interested in this topic, don’t hesitate to ask for an appointment via

alex.hepp@tum.de

Please include a grade report and a CV, so I can evaluate different focus areas to fit your experience.

Advisors

Alexander Hepp