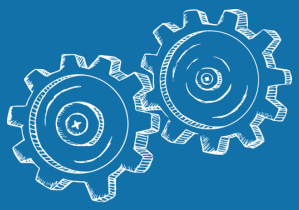

Optimized Implementations of Symmetric Cryptography

Advisor: **Christoph Dobraunig**

Motivation

Symmetric cryptographic algorithms play a central role in the security of our connected world. Two algorithms that received a lot of attention in the scientific research community are Ascon, the first choice for lightweight applications in CAESAR, and Isap v2.0, designed provide increased resistance against side-channel and fault attacks. Both algorithms have been co-designed by members of the IAIK.

It is essential to provide software implementation for a wide-range of target architectures to facilitate the widespread adoption of both algorithms. If you are interested in optimizing implementations, either for size or speed, this is the right project for you.

Goals and Tasks

- Get familiar with the target platform and algorithms
- Identify potential bottlenecks of existing reference implementations for the target platform
- Optimize existing reference implementations for the target platform
- Benchmark the code and make it public

Literature

- C. Dobraunig et al.
  Ascon v1.2
  CAESAR, https://competitions.cr.yp.to/caesar-submissions.html 2016
- C. Dobraunig et al.
  Isap v2.0
  IACR Trans. Symmetric Cryptol. 2020
  https://doi.org/10.13154/tosc.v2020.iS1.390-416

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Knowledge of C
- Interest in computer architectures

Advisor / Contact

christoph.dobraunig@iaik.tugraz.at