

Cryptanalysis of Symmetric Primitives

Advisor: **Maria Eichlseder**

Motivation




Cryptanalytic attacks define the security of cryptographic algorithms, and understanding them is crucial to understand cryptographic design.

In our research on secure symmetric cryptography, we typically work on:

- > Different symmetric primitives: **block ciphers**, permutations, tweakable block ciphers, ...
- > Different security notions: mathematical **cryptanalytic security**, implementation security and resilience
- > Different goals: **finding attacks** or proving security properties
- > Different analysis techniques: **differential, linear, integral, algebraic, ...**
- > Different approaches: **pen-and-paper**, theory, computer-aided cryptanalysis with **MILP/SAT solvers** or dedicated **automated tools**, ...

Even if no specific cryptanalysis topic is currently listed on the IAIK topics list, we usually have some currently open questions suitable for master's theses or projects – just ask us to see if one of them matches your interests.

Typical Goals and Tasks

-  Get familiar with the basics and existing methods
-  Develop improved methods
-  Perform some experiments and evaluate them



Literature

- > *depends on topic*

Courses & Deliverables

- Master Project**
 - Project code
 - Report
 - Presentation
- OR –
- Master's Thesis + DiplomandInnenseminar (CS)**
 - Initial presentation
 - Project code
 - Thesis (60+ pages)
 - Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > *Cryptography*
- > (Optional) *Cryptanalysis*
- > Programming (typically Python)

Advisor Contact

maria.eichlseder@iaik.tugraz.at