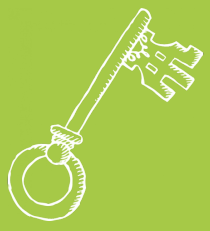

Finding Low-Data Integral Distinguisher

Advisor: **Simon Gerhalter**

Motivation

Integral cryptanalysis is one of the most powerful tools for evaluating the security of symmetric ciphers. With techniques such as monomial prediction, it is possible to automatically find the longest integral distinguishers for a given cipher. However, these distinguishers typically require a large amount of data, often close to the full codebook. In practice, modes of operation or restrictions set by the cipher designers may limit the data available to an attacker to far below the block size. Finding the best distinguisher under such a data limit is a much harder problem, as the search space of possible input sets quickly becomes infeasible to explore exhaustively.

The goal of this thesis is to use machine learning to find good integral distinguishers for a given data limit. One possible approach is to sample the effectiveness of random input sets and train a model to identify promising distinguishers. Alternatively, an iterative approach could be used, in which the input set of the distinguisher is improved step by step.

Goals and Tasks

- Become familiar with integral cryptanalysis and monomial prediction.
- Identify suitable ciphers, in particular those with strict data limits.
- Investigate and design suitable machine learning approaches for the search.
- Implement the approach and use it to find new integral distinguishers with minimal data complexity.
- Evaluate the results and compare them with existing distinguishers.

Literature

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Interest in symmetric cryptanalysis
- Interest in machine learning
- Programming (Python, MILP, SAT)

Advisor Contact

simon.gerhalter@tugraz.at