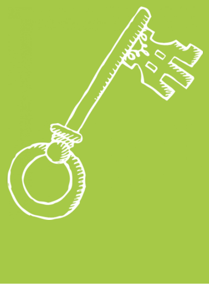
ISEC | Institute of Information Security



Finding Differential Characteristics for Block Ciphers with SAT Solvers

Advisor: **Marcel Nageler**

Motivation

Differential Cryptanalysis is one of the main analysis techniques to evaluate the security of block ciphers. We have developed *AutoDiVer*, a tool to analyze the assumptions made for differential cryptanalysis. The tool already includes implementations for many ciphers, and it should be possible to adapt it to search for differential characteristics instead.

In your thesis, you will

- Become familiar with SAT modeling and block cipher internals
- Adapt AutoDiVer to search for differential characteristics
- Experiment with different approaches to find *good* differential characteristics

Goals and Tasks

- Understand block cipher internals and how to model them in SAT.
- Contribute a model of the difference distribution table to AutoDiVer.
- Find interesting new differential characteristics.

Literature

- M. Nageler et al.
  AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

Recommended if you’re studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Interest in Cryptography and SAT modeling
- Knowledge of Python

Advisor Contact

marcel.nageler@tugraz.at