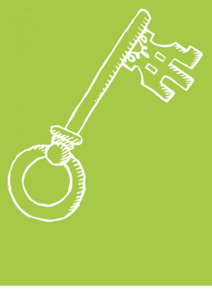
IAIK | Institute of Applied Information Processing and Communications



Analyzing Block Ciphers for Key Dependencies

Advisor: **Marcel Nageler**

Motivation

Differential Cryptanalysis is one of the main analysis techniques to evaluate the security of block ciphers. However, certain assumptions, that are often assumed, do not always hold in practice. One of them is the *Hypothesis of Stochastic Equivalence*, that states that the attack works approximately the same for all keys.

We developed *AutoDiVer*, a tool to automatically find for which keys a differential characteristic is (im)possible. It is based on modeling the valid pairs one searches for in an attack using SAT solvers.

In your thesis, you will

- Become familiar with SAT modeling and block cipher internals
- Model a block cipher in SAT and add it to AutoDiVer.
- Analyze differential characteristics using the tool.

Goals and Tasks

- Understand block cipher internals and how to model them in SAT.
- Contribute a new block cipher to AutoDiVer.
- Find new results for when the analyzed characteristics are possible.

Literature

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

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 ☑ MATH

Prerequisites

- Interest in Cryptography and SAT modeling
- Basic knowledge of Python

Advisor Contact

marcel.nageler@iaik.tugraz.at