MILP Solvers in Cryptography

Advisor(s): Maria Eichlseder and Daniel Kales

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Differential cryptanalysis is one of the most prominent attack methods on block ciphers. However, finding a suitable differential characteristic for a block cipher is not trivial. One method to find such characteristics is to model a reduced (also called truncated) version of the cipher, find a good solution for this truncated model and try to extend it to a full solution. Mixed-Integer Linear Programming (MILP) Solvers are a tool well suited to evaluate these truncated models and to find optimal solutions. However, basic truncated models are often not precise enough representations of the full cipher, which leads to solutions for the truncated model having no valid assignments for the full cipher. Recent research has tried to extend basic truncated MILP models with additional restrictions to improve the results when extending the truncated solutions.

Your task in this thesis is to first investigate different existing MILP solvers and evaluate them with regards to their usability, configurability and performance. Afterwards you will develop and implement a general method to model truncated differential characteristics of block ciphers.

Goals and Tasks

- Get familiar with the required background: MILP solvers, tweakable ciphers, differential cryptanalysis
- Study existing attacks and methods
- Perform an evaluation of existing MILP solvers
- Develop and implement methods to model truncated differential characteristics

Literature

- C. Cid et al.
  A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers
  IACR Trans. Symmetric Cryptol. 2017

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in cryptanalysis
- Programming (C/C++, Python)

Advisor / Contact

daniel.kales@iaik.tugraz.at