

Motivation

In cryptanalysis the technique of analyzing linearized cryptographic primitives using methods from the theory of linear codes become a powerful tool. An open-source implementation of such techniques is available under the name *The CodingTool Library*. The functionality and efficient implementation of the library makes it a powerful tool in cryptanalysis. The core part of the library is a probabilistic algorithm to search for codewords with low Hamming weight. Recently, a group of scientist proposed a new algorithm for this task. According to their claims it performs significantly better than existing algorithms. In this project we will implement this algorithm, include it in the existing framework and analyze its performance.

Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Understanding and implementation of the new algorithm
- ▶ Including it in the existing framework
- ▶ Performance analysis

Literature

- ▶ D. J. Bernstein, T. Lange, and C. Peters. Ball-collision decoding. *Cryptology ePrint Archive, Report 2010/585*, 2010. <http://eprint.iacr.org/>.
- ▶ The CodingTool Library. [CodingTool webpage](#).

Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

Project Schedule

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

Bachelor Project

Studies: INF SW TEL TM

Prerequisites

- ▶ C/C++ programming

Advisor / Contact

tomislav.nad@iaik.tugraz.at