

## 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. However, the library does not take advantage of multi-core systems, which would increase the performance significantly. Therefore, it is the goal of this project extend the library such that it benefits from multi-core systems.

## Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Parallelizing aspects of the search algorithm
- ▶ Utilizing multi-core systems
- ▶ Performance analysis

## Literature

- ▶ [F. Mendel and T. Nad.](#)  
A distinguisher for the compression function of simd-512.  
In B. K. Roy and N. Sendrier, editors, *INDOCRYPT*, volume 5922 of *Lecture Notes in Computer Science*, pages 219–232. Springer, 2009.
- ▶ [The CodingTool Library.](#)  
[CodingTool webpage.](#)
- ▶ [The OpenMP API.](#)  
[OpenMP 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](mailto:tomislav.nad@iaik.tugraz.at)