

No Goals Left: Verifying Symmetric Cryptanalysis in Lean

Advisor: **Nedžma Mušović**

Motivation

Cryptanalytic attacks on block ciphers rely on structural properties that propagate through the rounds of a cipher. Establishing these properties requires careful, step-by-step reasoning.

Interactive theorem provers such as *Lean* allow such reasoning to be formalized and checked by a computer. A cipher is modeled as an executable definition, and a cryptanalytic property becomes a theorem whose proof is verified in every detail.

In this thesis, you will build on an existing framework for verified cryptanalysis in Lean. The framework already proves a classical attack for one well-known block cipher. Your task is to take it to a new, standardized cipher with a slightly different structure: model the cipher in Lean, prove that the attack applies, and find out which parts of the existing proofs carry over and where we need adjustements.

Goals and Tasks

- Get familiar with Lean, symmetric cryptanalysis, and the existing framework
- Formalize a new cipher or attack in Lean by extending the framework
- Investigate the capabilities and limits of Lean for cryptanalysis

Literature

- L. de Moura and S. Ullrich
  The Lean 4 Theorem Prover and Programming Language
  CADE 2021
  doi:10.1007/978-3-030-79876-5_37

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

Prerequisites

- Interest in formal methods and cryptography
- Programming experience
- No prior experience with Lean required

Advisor Contact

nedzma.musovic@tugraz.at