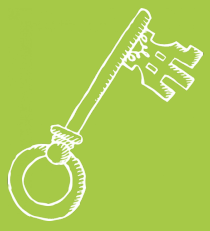


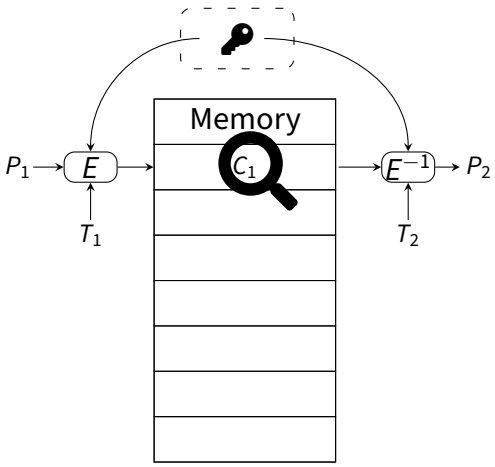
Differential-Linear Cryptanalysis of Low-Latency Cipher Beanie

Advisor: **Simon Gerhalter**

Motivation

Recently, a new low-latency cipher for memory encryption called Beanie has been proposed. This cipher uses a unique attack setting. The authors already conduct a wide range of cryptanalysis. An exception is differential-linear cryptanalysis [1].

In this thesis, you apply differential-linear cryptanalysis on Beanie.



Goals and Tasks

- Understand the unique attack setting used in Beanie.
- Study differential-linear cryptanalysis.
- Use tool assistance to find differential-linear attacks.

Literature

- S. K. Langford and M. E. Hellman
  Differential-linear cryptanalysis
  Annual International Cryptology Conference

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
- Interest in learning to use SAT/MILP solver

Advisor Contact

simon.gerhalter@tugraz.at