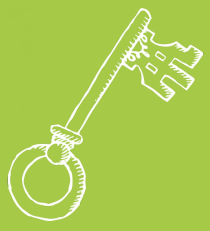

Showing the Resistance of QARMA against Integral Cryptanalysis

Advisor: **Simon Gerhalter**

Motivation

Integral cryptanalysis is one of the main ways to assess the security of a cipher. Historically, we used structural properties of ciphers to find integral attacks. Newer techniques, like monomial prediction, use a link between integral attacks and the algebraic degree of a cipher.

In order to provide strong arguments against integral attacks, Hebborn et al. [1] conceived the integral-resistance property. While they show this property for ciphers with sparse linear layers like SKINNY and PRESENT, their method is too computationally expensive against ciphers like AES. To bridge this gap, Zeng and Tian [2] introduce a dedicated tool able to show the integral-resistance property for 5-rounds of AES.

A next step is to use this new method to show the integral-resistance property for other ciphers.

Goals and Tasks

- Study integral cryptanalysis.
- Get familiar with a rust framework used to show integral-resistance for ciphers with complex linear layers.
- Implement QARMA in the framework and show the integral-resistance.
- Explore the possibility to apply the technique to other ciphers.

Literature

- P. Hebborn et al.
  Strong and Tight Security Guarantees Against Integral Distinguishers
  ASIACRYPT 2021
  https://eprint.iacr.org/2021/1502
- F. Zeng and T. Tian
  A New Method for Constructing Integral-Resistance Matrix for 5-Round AES
  IET Information Security 2025

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 algebra
- Interest in `rust`, `python`

Advisor Contact

simon.gerhalter@tugraz.at