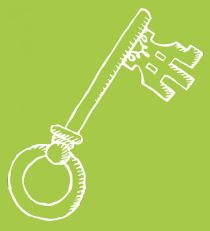

Imporved Key Recovery via Walsh Spectrum Puncturing

Advisor: **Simon Gerhalter**

Motivation

Walsh spectrum puncturing is a recent technique (EUROCRYPT 2024) for making key recovery in linear attacks cheaper. The exact key-recovery function is replaced by an approximation obtained by deleting chosen coefficients from its Walsh spectrum. This trades a controlled increase in data for fewer guessed key bits. The technique has already improved the best known attacks on several well-studied ciphers, but so far it has been applied to only a handful of designs. Many structurally similar ciphers have not yet been analysed with it.

Goals and Tasks

- Study linear cryptanalysis, the Walsh spectrum puncturing framework and its existing applications.
- Select a cipher that has not yet been attacked with this technique, and analyse its key-recovery rounds to decide which Walsh coefficients can be removed cheaply.
- Implement the cipher and the punctured key-recovery attack, and verify correlations and success rates experimentally on reduced-round versions.
- Compare the resulting attack with the best known attacks on the cipher.
- Optionally, extend the technique to differential-linear attacks, where it has so far been applied only to stream ciphers.

Literature

- A. Flórez-Gutiérrez and Y. Todo
  Improving Linear Key Recovery Attacks Using Walsh Spectrum Puncturing
  EUROCRYPT 2024
  doi:10.1007/978-3-031-58716-0_7

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Interest in symmetric cryptanalysis
- Interest in linear algebra
- Programming (Python, CP, MILP)

Advisor Contact

simon.gerhalter@tugraz.at