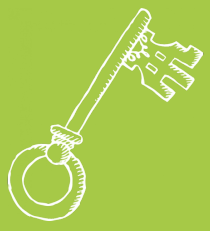

Analysis of Fork Ciphers and Zip Ciphers

Advisor: **Maria Eichlseder**

Motivation

Cryptanalytic attacks define the security of cryptographic algorithms, and understanding them is crucial to understand cryptographic design.

Recently, several new symmetric primitive designs have been proposed with the goal of developing more efficient pseudorandom functions. Examples include fork ciphers (like ForkSkinny) and zip ciphers. Unlike block ciphers, these primitives are not bijective, which impacts the applicability of classical cryptanalysis techniques. More research is necessary to develop a better understanding of the generic and concrete security properties of these primitives.

In this project, you will analyze fork and zip ciphers with selected cryptanalysis techniques in order to develop a better estimate of their concrete security margin.

Goals and Tasks

- Get familiar with the ideas behind fork ciphers and zip ciphers
- Investigate how different distinguishers (differential, linear, integral, …) can be applied to attack these new primitives
- Develop suitable key recovery strategies
- Apply the techniques to selected designs
- Improve the support for automated cryptanalysis of these primitives with a suitable framework

Literature

- E. Andreeva et al.
  Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages
  ASIACRYPT 2019
- A. Bariant, N. David, and G. Leurent
  Cryptanalysis of Forkciphers
  IACR Trans. Symmetric Cryptol. 2020
- A. Flórez-Gutiérrez et al.
  General Practical Cryptanalysis of the Sum of Round-Reduced Block Ciphers and ZIP-AES
  ASIACRYPT 2024

Courses & Deliverables

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

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- *Cryptography*
- *Cryptanalysis*
- Programming (typically Python)

Advisor Contact

maria.eichlseder@tugraz.at