Cryptanalysis of CAESAR Candidates

Advisor(s): Florian Mendel, Maria Eichlseder, Christoph Dobraunig

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Authenticated encryption algorithms are an essential ingredient for secure communication: they provide both confidentiality and authenticity for messages transmitted over an insecure channel. The cryptographic community is currently engaging in an open competition to design new, modern authenticated ciphers: the CAESAR competition. Over 50 designs were submitted, leaving the community with the overwhelming task of analyzing the ciphers for their security against different attacks.

We have developed several automatic tools for the cryptanalysis of hash functions. Adapt this toolbox for application to the new authenticated ciphers, and find out which methods work best for which ciphers.

Goals and Tasks

- Understand linear and/or differential cryptanalysis
- Select and understand authenticated ciphers
- Get used to the existing automatic tools
- Adapt and optimize them to attack the ciphers

Literature

- Authenticated Encryption Zoo
  CAESAR candidates
  https://aezoo.compute.dtu.dk

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW ☒ TM

Prerequisites

- C/C++ programming

Advisor / Contact

florian.mendel@iaik.tugraz.at