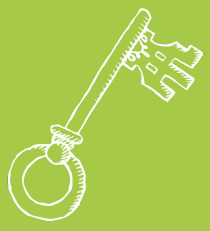


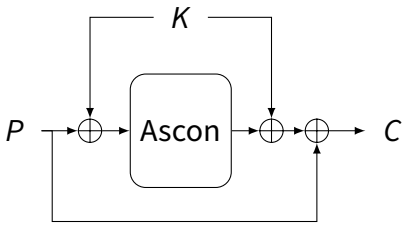
Analyzing a pseudorandom function based on Ascon

Advisor: **Simon Gerhalter**

Motivation

The Ascon family of lightweight cryptographic algorithms recently became a NIST standard [1]. Ascon can be used in various modes of operations, like authenticated encryption, hashing, and as an extendable output function. Most of these modes of operation are well studied.

For this thesis, the goal is to analyze Ascon when used as a pseudorandom function (PRF). A way to realized this is in the form of a Davies-Meyer construction:



Goals and Tasks

- Study various cryptanalysis techniques.
- Establish whether techniques used for analyzing Zip-Ciphers [2] can be reused.
- Use tool assistance to find attacks on Ascon PRF.

Literature

- C. Dobraunig et al.
  Ascon v1.2
  Submission to Round 1 of the NIST Lightweight Cryptography project 2019
  https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ascon-spec.pdf
- A. Flórez-Gutiérrez et al.
  General practical cryptanalysis of the sum of round-reduced block ciphers and ZIP-AES
  International Conference on the Theory and Application of Cryptology and Information Security

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