# Efficient and Side-Channel Resistant Hardware Implementation of Ascon

Advisor(s): Hannes Groß

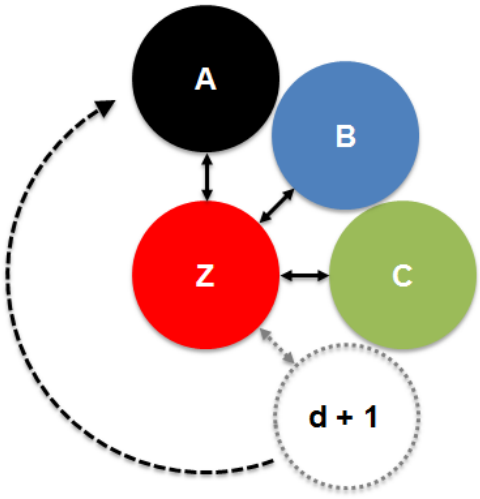
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

## Motivation

The efficient protection of cryptographic implementations against so-called side-channel analysis (SCA) attacks is a fundamental need of todays embedded devices. Without the protection against SCA attacks, cryptographic implementations can be broken by simply extracting the used key material from physical side-channels like the power consumption or the electromagnetic emanation.
In this project, the CAESAR competition participant ASCON shall be implemented to counteract SCA attacks. Since one of the most important metrics for protected hardware implementations is the amount of required randomness, new ways of saving the amount of randomness and its implications to the efficiency of the design will be investigated.

## Goals and Tasks

- Make yourself familiar with ASCON
- Understand techniques to prevent side-channel analysis attacks
- Implement ASCON according to the Domain-Oriented Masking scheme
- Compare the suitability of saving randomness versus the overall implementation costs




Domain-Oriented Masking

## Literature

- C. Dobraunig et al.
  Ascon – Submission to the CAESAR competition
  http://ascon.iaik.tugraz.at
- H. Gross, S. Mangard, and T. Korak
  Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order
  http://eprint.iacr.org/2016/486
- G. Barthe et al.
  Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model
  http://eprint.iacr.org/2016/912

## 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

## Prerequisites

- VHDL programming

## Advisor / Contact

hannes.gross@iaik.tugraz.at