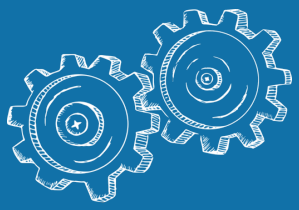


Coco for Masked Hardware Designs

Advisor: **Barbara Gigerl**

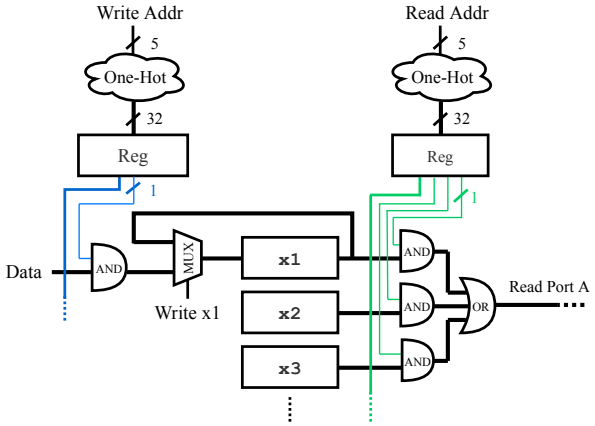
Motivation

Power analysis attacks allow attackers to recover sensitive data from cryptographic implementations by observing a device's power consumption. Masking is one of the most powerful countermeasures against such attacks. The basic idea of masking is to split secrets into multiple, random shares such that the observation of one share does not reveal the secret. In the case of masked hardware implementations this means that at no point in the implementation, secret shares are combined.

Tools like Rebecca [1], and more recently Coco [2], help to formally verify the correctness of such implementations. While the focus of Rebecca lies completely on hardware implementations, Coco operates more on the boundary between hardware and software. We want to investigate to which extend Coco can be used with pure hardware implementations.

Goals and Tasks

- Get familiar with power analysis attacks, masking, Rebecca and Coco
- Make the necessary adaptions to Coco such that verifying pure hardware circuits is possible
- Compare Coco and Rebecca



Literature

- R. Bloem et al.
  Formal Verification of Masked Hardware Implementations in the Presence of Glitches
  EUROCRYPT 2018
- B. Gigerl et al.
  Coco: Co-Design and Co-Verification of Masked Software Implementations on CPUs
  Cryptology ePrint Archive, Report 2020/1294 2020
  https://eprint.iacr.org/2020/1294

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

Prerequisites

- Interest in the topic area
- Programming (Verilog, Python)

Advisor / Contact

barbara.gigerl@iaik.tugraz.at