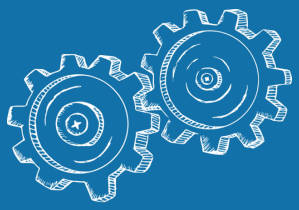


Verification of Masked Software Implementations on an Extended Ibex Design

Advisor: **Barbara Gigerl**

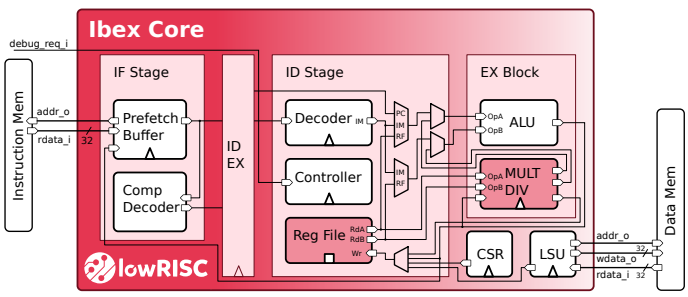
Motivation

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.

Coco [1] is a tool to formally verify that masked software implementations are executed leakage-free on microprocessors like the RISC-V Ibex core. Since the design of the Ibex core is open source, it is continuously being developed and new features are added steadily. Recently, a third pipeline stage for writing back computation results and an instruction cache were added to the Ibex core. We want to investigate which new vulnerabilities are created by adding these two features.

Goals and Tasks

- Get familiar with power analysis attacks, masking and Coco
- Write some test programs which target the usage of the write-back stage and instruction cache
- Verify the test programs with the updated Ibex design and see which vulnerabilities exist



The RISC-V Ibex core

Literature

- 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, C)

Advisor / Contact

barbara.gigerl@iaik.tugraz.at