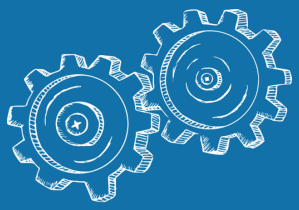

# Implementing Upcoming RISC-V Security Extensions on the BOOM Core

Advisor: **Paul Gollob**

## Motivation

RISC-V is an open instruction set architecture whose specification is developed openly by RISC-V International. Many new security extensions are currently in development, e.g., for confidential computing (*Supervisor Domains*, *CoVE*) or memory isolation. Before ratification, such drafts need hardware prototypes that show whether the specification is complete and what it costs in a real processor.

The *Berkeley Out-of-Order Machine* (BOOM) is an open-source, high-performance **out-of-order** RISC-V core written in Chisel. Adding security checks to such a core is challenging, as speculation, caches, and TLBs interact with them in complex ways.

In this topic, you will implement a draft RISC-V security extension on BOOM and evaluate it in simulation or on FPGA. Your results are shared openly and directly **contribute to the ongoing specification development**. The topic can be done as a master project, a master's thesis, or a **project followed by a thesis**.

## Goals and Tasks

- Get familiar with the BOOM microarchitecture, Chisel, and the Chipyard framework.
- Study a selected draft RISC-V security extension and its open questions.
- Implement the extension in BOOM with software support for testing.
- Evaluate the security, performance, and area overhead of your implementation.
- Report findings and possible specification issues back to the RISC-V task groups.

## Literature


- J. Zhao et al.
  SonicBOOM: The 3rd Generation Berkeley Out-of-Order Machine
  CARRV 2020
  https://carrv.github.io/2020/papers/CARRV2020_paper_15_Zhao.pdf
- RISC-V International
  RISC-V Supervisor Domains Access Protection (Draft)
  https://github.com/riscv/riscv-smmtt


## Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

## Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

## Prerequisites

- Computer architecture, HDL (Verilog, Chisel)
- Interest in open hardware security

## Advisor Contact

paul.gollob@tugraz.at