



The CHERI Capability Architecture

Advisor: **Moritz Waser**

Motivation




Capability Hardware Enhanced RISC Instructions (CHERI) [1] extends existing instruction set architectures (ISAs) with the integration of capability-based addressing. CHERI integrates dedicated capability registers and capability instructions designed for performing access and permission checks in hardware. CHERI's *capabilities* use a fat pointer approach (i.e. 128-bit capabilities on 64-bit architectures). In addition to the regular 64-bit address, these capabilities contain compressed bounds, permission bits, and an object type identifier.

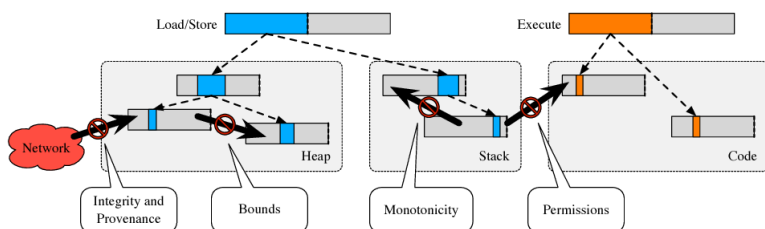
In addition to the regular CHERI specification, there is also the CHERIoT platform, which targets embedded applications with smaller, 64-bit capabilities on a 32-bit architecture.

This Project

This project aims to utilize CHERI to build novel secure systems, as well as extend CHERI with new features that address shortcomings in the current design. Both pure-software projects and HW/SW-codesigns are possible.

Goals and Tasks

-  Familiarize yourself with the CHERI ISA
-  Set up the toolchain and run some experiments
-  Develop novel extensions in software and hardware



CHERI guarantees pointer provenance and integrity, alongside permission monotonicity and bounds enforcement.

Literature

- > [R. N. M. Watson et al.](#)
Capability Hardware Enhanced RISC Instructions: CHERI Instruction-Set Architecture (Version 9)
Tech. rep.
2023
<https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-987.pdf>

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 low-level system security
- > Interest in hardware extensions
- > Programming (C/C++, Python)
- > HDL (SystemVerilog)

Advisor Contact

moritz.waser@iaik.tugraz.at