The CHERI-RISC-V open-source ecosystem

Peter Rugg, Jonathan Woodruff, Alexandre Joannou, Franz A. Fuchs, and Simon W. Moore
Department of Computer Science and Technology, University of Cambridge
peter.rugg@cl.cam.ac.uk
Project URL: cheri-cpu.org

UNIVERSITY OF CAMBRIDGE
Computer Science & Technology

CHERI-RISC-V Current Supported Stack

Operating System: CheriBSD

Orchestrating memory safety

CheriBSD is a port of FreeBSD that supports 128-bit CHERI pointers. CheriBSD fully supports CHERI-RISC-V (version 9). CheriBSD supports purecap user processes, providing capabilities for pointers in all kernel APIs.	CheriBSD: either **hybrid** or **purecap**. • **Hybrid** CheriBSD uses 64-bit pointers for kernel objects; pointers from purecap userspace processes are handled as capabilities in the kernel. • **Purecap** CheriBSD uses capabilities for all pointers in both the kernel and purecap processes.

Shared code base with Arm's CHERI Morello

Compiler: CHERI Clang/LLVM

Preserving intent in the executable

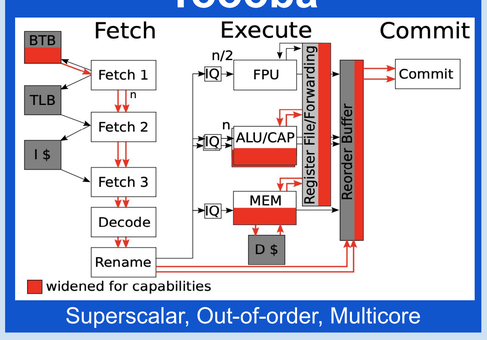
CHERI Clang/LLVM support compilation of C and C++ to both **hybrid** and **purecap** CHERI-RISC-V. CHERI Clang can compile **thousands of user-space applications** and the **CheriBSD kernel**.	CHERI Clang/LLVM supports code generation for both CHERI-RISC-V with 64-bit and 128-bit pointers (rv32xcheri, and rv64xcheri). CHERI compressed instruction support is included.

Shared code base with Arm's CHERI Morello

Implementations

CHERI-RISC-Vs for every occasion

Toooba



Superscalar, Out-of-order, Multicore

QEMU

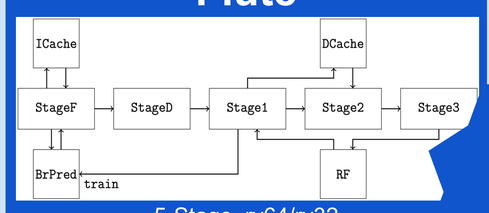
```
$ ./cheribuild.py --include-dependencies run-riscv64-purecap
[...]
Copyright (c) 1992-2020 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
FreeBSD is a registered trademark of The FreeBSD Foundation.
FreeBSD 13.0-CURRENT #0 ea692111dcc-c1(master)-dirty: Thu Dec  3 13:22:10 UTC 2020
    jrtc4@zeno.sec.cl.cam.ac.uk:/home/jrtc4/cheri/build/cheribsd-riscv64-purecap-bu
clang version 11.0.0 (https://github.com/CTSRD-CHERI/llvm-project.git ca275db7edb8f
CHERI hybrid kernel.
[...]
FreeBSD/riscv (cheribsd-riscv64-purecap) (ttyu0)

login:
```

High-speed ISA-level Emulation

Others…

- Piccolo 3-stage, 32-bit
- Ibex microcontroller
- SIMTight GPGPU
- Spike ISA simulator
- Proteus 5-stage SpinalHDL

Flute

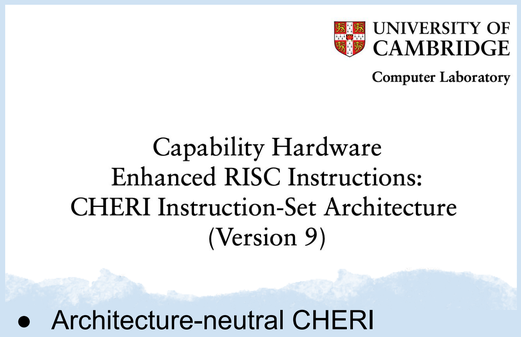


5-Stage, rv64/rv32

VCU118 and DE10 FPGA support

Architecture

Specification for clarity & verification



- Architecture-neutral CHERI specification, with application to CHERI-RISC-V
- Justification of design decisions
- Paths not taken
- Experimental/hypothetical extensions

Sail CHERI-RISC-V

- Formal executable model
- Excerpts used in ISA version 9
- Used in tandem verification with hardware and simulators via TestRIG
- Supports rv32/rv64

Ratification CHERI SIG and TG

https://github.com/riscv/riscv-cheri

Google LowRISC University of Cambridge RISC-V International Codasip +more!

Participants in CHERI Special Interest Group represent many organisations.

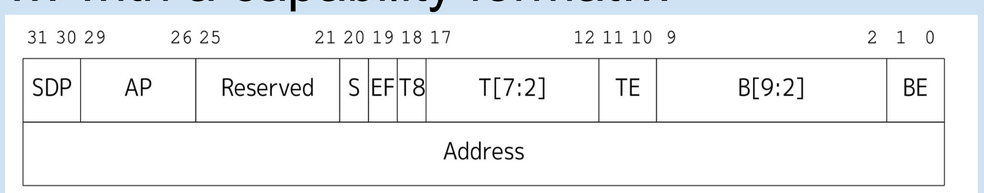
Progress

Herding caps

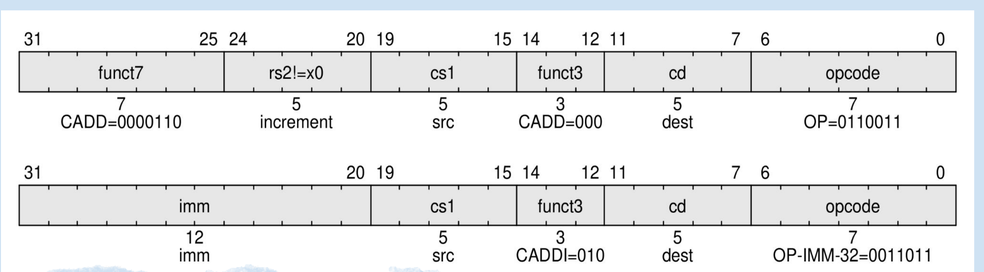
An AsciiDoc spec…

RISC-V Specification for CHERI Extensions

… with a capability format…

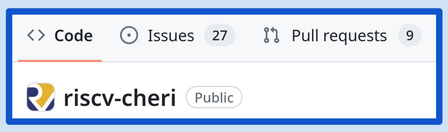


… and instruction definitions!

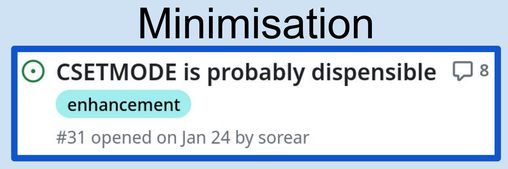


Prominent Issues

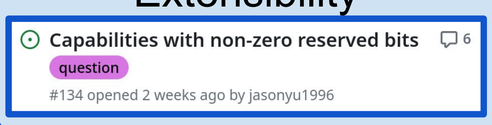
Active community input



Minimisation



Extensibility



Corner cases

CHERIoT

Collaborating and converging

Microsoft Research's instantiation of CHERI for embedded microcontrollers. Bespoke software stack allows use of more experimental features. Custom "CHERIoT RTOS" Emphasis on compartmentalisation and minimising trust.	Standardisation goals: • Lift limitations (small address size) • Integrate with specification for rv64 • Generalise to further use-cases • Support all the features (as another extension)?

SRI International

Parts of this work were supported by DARPA (HR0011-18-C-0016 "ECATS") and Innovate UK ISCF DSbD (105694).

CHERI