CHERI Processor Models

Simon W. Moore

Robert N. M. Watson, Peter G. Neumann, Jonathan Woodruff, Jonathan Anderson, Hadrien Barral, Ruslan Bukin, David Chisnall, Nirav Dave, Brooks Davis, Lawrence Esswood, Khilan Gudka, Alexandre Joannou, Chris Kitching, Ben Laurie, A. Theo Markettos, Alan Mujumdar, Steven J. Murdoch, Robert Norton, Philip Paeps, Alex Richardson, Michael Roe, Colin Rothwell, Hassen Saidi, Stacey Son, Munraj Vadera, Hongyan Xia, and Bjoern Zeeb

University of Cambridge, SRI International

CHERI Microkernel Workshop – 23 April 2016

SRI International

UNIVERSITY OF CAMBRIDGE

Introduction

- CHERI modelled as extensions to 64-bit MIPS ISA

- Different CHERI processor models:

  - Bluespec SystemVerilog (FPGA hardware & cycle accurate simulation; microarchitectural features)

  - Qemu (fast simulator)

  - L3 (formal ISA model)

- Counterpart:

  - ISA test suite

- All processor models are complete and will boot FreeBSD, run applications, etc.

ISA Test Suite

- Code (assembler/C) + known output

- Embodies/encodes our understanding of the correct behavior of the 64-bit MIPS ISA and CHERI extensions

- Used to develop and regression test the models

- N.B. can also test the models against each other

L3 formal model

- L3 – language developed in Cambridge for ISA modeling

  - simple encoding of ISA, so more likely to be correct

  - still challenges in encoding MIPS manual!

- Can export model to HOL4 for formal verification (not currently doing this)

- Can export an ML model for simulation

  - gold model for test-suite results, co-simulation

  - a bit slow but complete and can boot FreeBSD

Qemu

- Fast ISA simulator

- Extended base MIPS model with CHERI support

- Provides a fast model for software development and trace collection

  - relatively easy to use

  - fast I/O

  - doesn't require you to own FPGA hardware

SRI International

UNIVERSITY OF CAMBRIDGE

Bluespec SystemVerilog Hardware

- Bluespec SystemVerilog (BSV) – higher-level hardware description language originally from MIT

- Rich type system and much automatic control-logic synthesis

  - faster design and more likely to be correct

- Implementations:

  - Verilog➜FPGA to give ~100MHz design

  - C-model: reasonably fast cycle-accurate simulator

- CHERI and CHERI2 models includes caches, interrupts/PIC, stream trace/debug, multicore

- but slower I/O due to limitations of FPGA board IP

Hardware Instances

CHERI Tablet

CHERI Cloud Servers