X730: Codasip's X730 CHERI -RISC-V Application Core

Tariq Kurd[1]
[1] Codasip, UK

Abstract

The X730 core adds CHERI-RISC-V to a dual-issue 4-ALU in-order RVA22 compliant core, already running CHERI-Linux, which is available from the CHERI-Alliance open-source repository. It is the first commercially available CHERI-RISC-V application core, and is certainly the first of many. CHERI is a game-changing security extension for deterministic memory safety and memory compartmentalization. Once ratified, this standard will see huge adoption across the industry, greatly accelerating the ecosystem development, with multiple vendors planning silicon for 2025. CHERI aims to address the root cause of the problems that are caused by a lack of memory safety in common implementations of languages such as C/C++, which are responsible for around 70% of security vulnerabilities in modern systems.

Introduction

The Codasip X730 cores take a traditional dual-issue 4-ALU, with early/late scheduling, micro-architecture and adds CHERI functionality to it seamlessly.

The X730 supports two executions modes: 100% RVA22 compatibility, running any RVA22 binary in a secure compartment, and also running re-compiled CHERI code offering fine-grained memory protection.

The X730 supports all the optional extensions listed in the CHERI specification, such as Zcherilevels, fir the best possible RVA22 compliant user experience.

The poster will talk about performance results of running CHERI vs legacy RISC-V code on the same CPU, and the impact on core area from adding in the CHERI hardware. It will also include some details of what was required to include CHERI into the pipeline.