

Contents

1	Future work	1
1.1	Current expirement: FAT pointer based range addresses . . .	1
1.1.1	Objectives (Todo steal research questions from the paper)	1
1.1.2	Hardware	2
1.1.3	Evaluation (Steal evaluation from the paper)	2
1.1.4	limitation	2
1.2	Cheri RISCv to prevent using the TLB	2
1.2.1	Hardware modifications	2

1 Future work

This documents is decision making to highlight potential paths to take for this PhD. We will initially talk about the current expirement which is a FAT pointer based memory allocator and will then expand into 2 potential paths:

- Cheri RISCv to prevent using the TLB.
- Allocator evaluation based on stripping instruction calls for larger allocators like Jemalloc.

1.1 Current expirement: FAT pointer based range addresses

- TODO add diagram

The objective of this expirement was to ensure we can use the Cheri bounds as tracking mechanism of allocations instead of using multiple TLB entries. Using this approach we can use a single Huge page entry with bounds to ensure that the bounds (Which is the top and base address) can be extracted from the pointer using the Cheri compressed bounds mechanism. We implemented a simple allocator which uses this technique with a basic malloc and free.

1.1.1 Objectives (Todo steal research questions from the paper)

- Reduce the number of TLB walks (Reducing each transaltion to 2 CPU CYCLES with huge pages).
- Using a block based style allocations inside huge pages.

1.1.2 Hardware

- ARM morello (Huge page size 1GB used)

1.1.3 Evaluation (Steal evaluation from the paper)

1.1.4 limitation

- Using Huge page still requires a TLB entry which could be mitigated (Refer to the FPGA work).
- ARMv8 only supports using to virtual addresses so it's required to bypass the TLB for address translation.

1.2 Cheri RISC-V to prevent using the TLB

In the current ARM Morello setup, address translations rely on the TLB. The future approach on RISC-V Tooba involves storing the offset directly within the pointer. This is possible due to CHERI's capability model, which supports fine-grained memory protection and can encode bounds within pointers. Utilizing Bounds in CHERI for Block-Based Allocation: CHERI capabilities allow pointers to carry metadata about memory bounds, providing hardware-enforced memory safety. By encoding the offset and bounds within the pointer, the system can directly access memory without needing intermediate translations via the TLB. This enables the implementation of a block-based allocator that can efficiently manage memory allocations and deallocations within defined bounds. Bypassing the TLB in RISC-V Tooba.

1.2.1 Hardware modifications

The Bluespec design of the RISC-V processor will be modified to allow certain memory operations to bypass the TLB. This means that when a pointer with encoded offset and bounds is used, the system can directly compute the physical address from the capability information. This modification reduces the dependency on the TLB, decreasing latency. and improving performance, especially for frequent memory operations.