Technical Report

UCAM-CL-TR-982
ISSN 1476-2986

Number 982

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Arm Morello Programme: Architectural security goals and known limitations

Robert N. M. Watson, Graeme Barnes, Jessica Clarke, Richard Grisenthwaite, Peter Sewell, Simon W. Moore, Jonathan Woodruff

July 2023

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

https://www.cl.cam.ac.uk/

This work was supported by the Innovate UK project Digital Security by Design (DSbD) Technology Platform Prototype, 105694.

We gratefully acknowledge UK Research and Innovation (UKRI), who sponsored the creation of Morello, and also the significant investment by DARPA in supporting the creation of CHERI and its earlier prototypes.

We also acknowledge Arm Limited and Google, Inc.

Technical reports published by the University of Cambridge Computer Laboratory are freely available via the Internet:

https://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

Abstract

Arm's Morello prototype incorporates a first-generation CHERI-enabled Armv8-A CPU prototype. We have developed Morello to enable CHERI-based research by a growing community of researchers seeking access to potentially transformative architectural security improvement. This includes supporting experimentation, evaluation, and demonstration across microarchitecture and software. Morello is an exciting opportunity to work with – and improve – CHERI, and we seek your help and collaboration in preparing CHERI for mainstream use.

The purpose of this document is to lay out the specific architectural security objectives of the Arm Morello prototype, as well as areas that fell out of scope for the project. We invite not only your feedback, but also your collaboration, in helping us to create a future class of CHERI-extended processors that dramatically enhance software security.

Contents

1 Introduction

Arm's Morello prototype incorporates a first-generation CHERI-enabled Armv8-A CPU prototype [3, 4]. We have developed Morello to enable CHERI-based research by a growing community of researchers seeking access to potentially transformative architectural security improvement. This includes supporting experimentation, evaluation, and demonstration across microarchitecture and software. Morello is an exciting opportunity to work with – and improve – CHERI, and we seek your help and collaboration in preparing CHERI for mainstream use.

The purpose of this document is to lay out the specific architectural security objectives of the Arm Morello prototype, as well as areas that fell out of scope for the project. We invite not only your feedback, but also your collaboration, in helping us to create a future class of CHERI-extended processors that dramatically enhance software security.

2 Architectural security aims and experimental validation

A key area of overall investigation and desired feedback enabled by Morello is the potential impact of CHERI on practical software security – in particular its ability to support vulnerability mitigation through fine-grained memory protection and scalable software compartmentalization. The architectural aim is therefore to faithfully implement the CHERI protection model in a high-performance Arm processor implementation.

Morello was developed by extending an existing, mature microarchitecture, the Neoverse N1 [2], which utilises the Armv8.2-A Instruction-Set Architecture (ISA).

Selecting this existing processor baseline enabled rapid engineering that focused primarily on the CHERI extensions rather than baseline architecture, and also allowed the project to complete within a one-year microarchitecture development cycle set by the sponsor, UKRI. However, this approach means that the known limitations of the baseline architecture and microarchitecture constrain certain forms of experiments and evaluation.

The intention of the Morello architecture was a clean and tight integration of CHERI protection into the Armv8.2-A ISA [1], synchronised to CHERI ISAv8 [5]. There are, however, some notable variations from CHERI ISAv8 required by differences in underlying architectures as well as microarchitectural constraints, including:

- The capability bounds compression scheme differs modestly.
- Richer capability-aware instruction encodings are enabled by switching to the capability mode via branches to addresses with the least significant bit set; a similar design choice has now been adopted in CHERI-RISC-V using a capability flag.
- Arm's exception handling support includes multiple banked registers, including the stack pointer, requiring different CHERI integration.
- The specific sets of capability permissions, capability-related exception codes, and other details differ.

- There are additional variations on domain-transition instructions, to support evaluating further options, including executive/restricted modes and indirect unsealing branch instructions.

There are also some areas in which the richer Arm instruction set required CHERI composition choices not explored in the CHERI ISA baseline, including:

- Virtualization extensions
- Vector instructions

In these areas, the primary focus was on not violating design goals of the CHERI extensions to other aspects of the architecture – e.g., enforcing capability protections, retaining capability provenance validation, and monotonicity.

3 Constraints of the Armv8.2-A baseline ISA

The Neoverse N1 supports Armv8.2-A, but a number of further security features have been added to later architectures, including:

- Pointer Authentication Codes (PAC),
- Branch Target Identification (BTI),
- Memory Tagging Extension (MTE), and
- Realm Management Extension (RME) features.

As a result, we were not able to explore the composition with CHERI with these post-8.2 features using this processor baseline. A future production architecture would compose these features, and we specifically seek to understand requirements and use cases for those compositions.

4 Limitations of the experimental software stack

The software toolchain also remains early and experimental, although these are being actively pursued by the Arm, Cambridge, and Linaro engineering teams and we expect updates to address these issues as the programme proceeds:

- Application Binary Interfaces (ABIs) to support memory protection and software compartmentalisation remain in development, and contain known limitations such as with respect to protections for thread-local storage.

- Techniques to implement fine-grained memory safety and scalability software compartmentalization in software, including the operating system, compiler, runtime, and applications, remain an active area of research. This is especially true with respect to compiler optimization, temporal memory safety, and software compartmentalization.
- More generally, there are complex tradeoffs between protection and performance across variations in ABIs, code generation, and linkage for CHERI, and these are only now becoming understood as the Morello platform allows experimentation with larger and richer software stacks. These will all change substantially in coming years as understanding improves.

It is expected that limitations will be found with these experimental prototypes, and feedback is sought on both usage models and specific software implementations. It is reasonable to expect that this experimental software will contain vulnerabilities.

5 Limitations on the hardware threat model

There are also other aspects of the Morello programme scope that evaluators should be aware of, and relate to the scope of the starting microarchitecture and its relationship to the research programme goals. The baseline Neoverse N1 was not designed to resist the following threats, and the derived Morello microarchitecture is therefore neither intended to nor expected to resist them:

- Speculative execution and side-channel attacks.
- Rowhammer and related DRAM glitching techniques.
- Analogue attacks such as power glitching and RF leakage.

Other research in academia and industry continues to explore and attempt to address these concerns, but they do not lie within the scope of the CHERI research, which focuses on software-level vulnerabilities. Despite CHERI not seeking to address these problems, we are extremely interested in the composition of these attack techniques and CHERI – for example, the potential interactions between side-channel attacks, memory protection, and compartmentalisation. More generally, the aim of CHERI is to address only problems well addressed in computer architecture and microarchitecture – and cannot be a panacea for all security problems.

6 Acknowledgements

We gratefully acknowledge the helpful feedback from our colleagues, including John Baldwin, David Chisnall, Brooks Davis, Nathaniel Filardo, Paul Gotch, Peter G. Neumann, Alexander Richardson, and Konrad Witaszczyk. This work was supported by the Innovate UK project Digital Security by Design (DSbD) Technology Platform Prototype, 105694. We gratefully acknowledge UK Research and Innovation (UKRI), who sponsored the creation of Morello,

and also the significant investment by DARPA in supporting the creation of CHERI and its earlier prototypes. We also acknowledge Arm Limited and Google, Inc.

References

[1] *Arm Architecture Reference Manual Supplement: Morello for A-profile Architecture*. Arm Limited. 2020.

[2] *Arm Neoverse N1 Core: Technical Reference Manual, Revision r4p1*. Arm Limited. 2020.

[3] Richard Grisenthwaite, Graeme Barnes, Robert N. M. Watson, Simon W. Moore, Peter Sewell and Jonathan Woodruff. 'The Arm Morello Evaluation Platform—Validating CHERI-Based Security in a High-Performance System'. In: *IEEE Micro* 43.3 (2023), pp. 50–57. DOI: 10.1109/MM.2023.3264676.

[4] Robert N. M. Watson, Simon W. Moore, Peter Sewell and Peter G. Neumann. *An Introduction to CHERI*. Tech. rep. UCAM-CL-TR-941. University of Cambridge, Computer Laboratory, Sept. 2019. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-941.pdf.

[5] Robert N. M. Watson, Peter G. Neumann, Jonathan Woodruff, Michael Roe, Hesham Almatary, Jonathan Anderson, John Baldwin, David Chisnall, Jessica Clarke, Brooks Davis, Nathaniel Wesley Filardo, Alexandre Joannou, Ben Laurie, A. Theodore Markettos, Simon W. Moore, Steven J. Murdoch, Kyndylan Nienhuis, Robert Norton, Alexander Richardson, Peter Rugg, Peter Sewell, Stacey Son and Hongyan Xia. *Capability Hardware Enhanced RISC Instructions: CHERI Instruction-Set Architecture (Version 8)*. Tech. rep. UCAM-CL-TR-951. 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom, phone +44 1223 763500: University of Cambridge, Computer Laboratory, Sept. 2020. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-951.pdf.