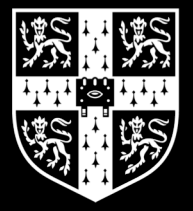
SafeBet: Validication of safe, aggressive speculation

Jonathan Woodruff, Simon W. Moore, Robert N. M. Watson

RISE Annual Conference, London

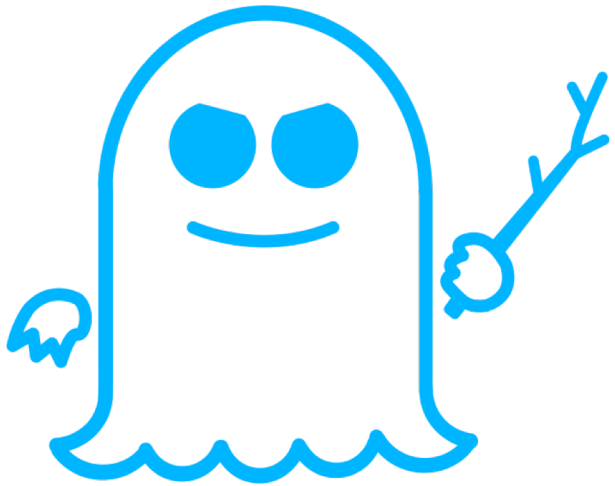
21th November 2019

Funded by GCHQ under the RISE initiative (ref: 4213054)



UNIVERSITY OF CAMBRIDGE
Computer Science and Technology

Motivation: new speculative execution attacks



SPECTRE

MELTDOWN

FORESHADOW

TLBLEED

All speculatively execute code that that leak secret information via a side-channel

Stages of SafeBet Project

- Instrument RISCY-OOO processor for TestRIG
- Develop sequence generators to demonstrate Spectre vulnerabilities
- Evaluate proposed mitigations, including CHERI capabilities

Ingredients of a Study on Spectre Vulnerability Discovery

1. Classification of Spectre vulnerabilities
2. Open-source Out-of-Order Processor Implementations
3. Flexible Validation Tools for Timing-Sensitive Reproduction

Classification of Spectre Attacks

- Suggests automated discovery of the presence of each class of vulnerability.
- Conversely, validation that each attack is not possible.

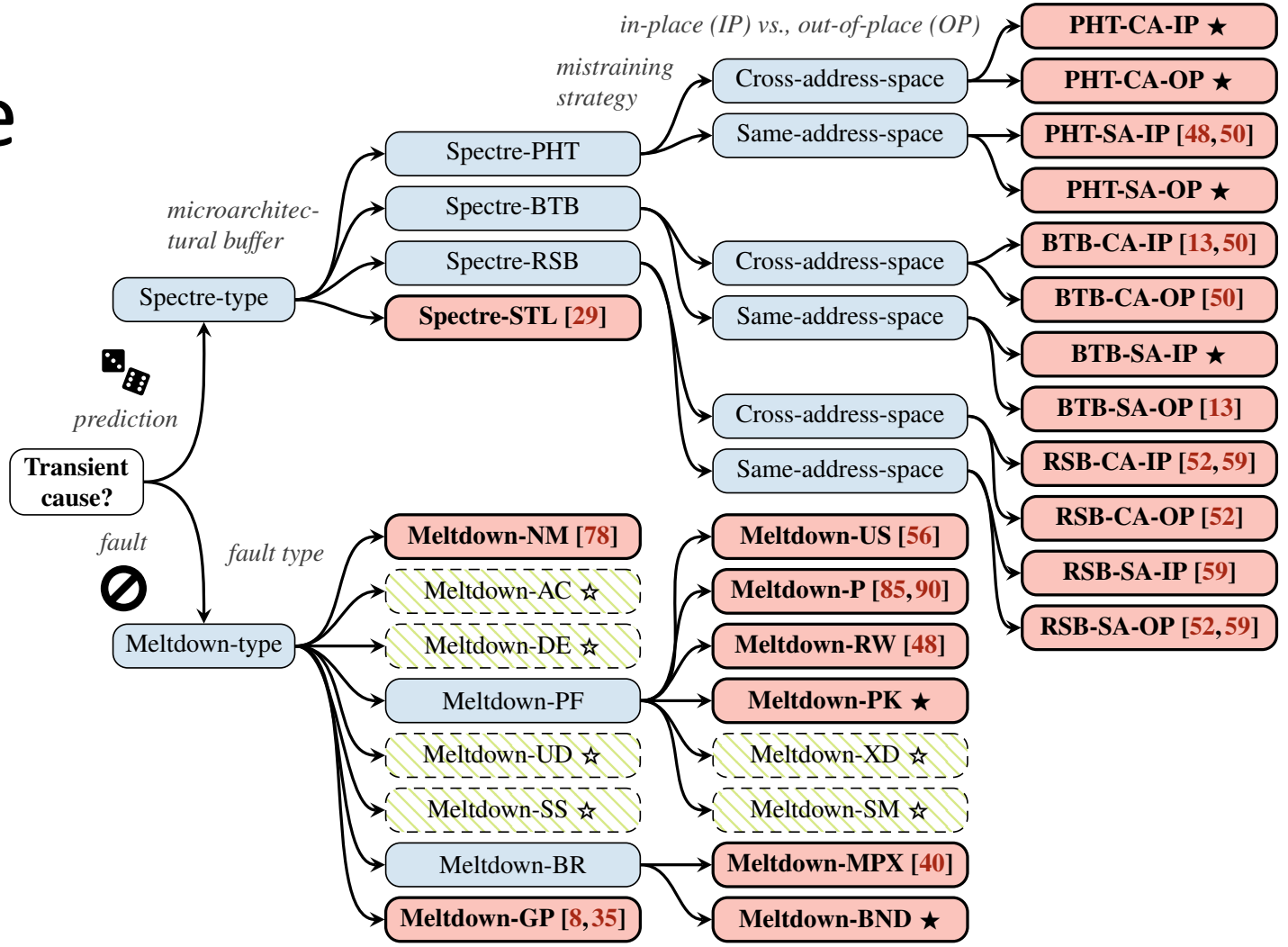


Figure 1: Transient execution attack classification tree with demonstrated attacks (red, bold), negative results (green, dashed), some first explored in this work (★ / ☆).

A Systematic Evaluation of Transient Execution Attacks and Defenses, Claudio Canella, et al.

Open-source Superscalar Out-of-Order CPUs

RISCY-OOO (MIT, language: Bluespec)

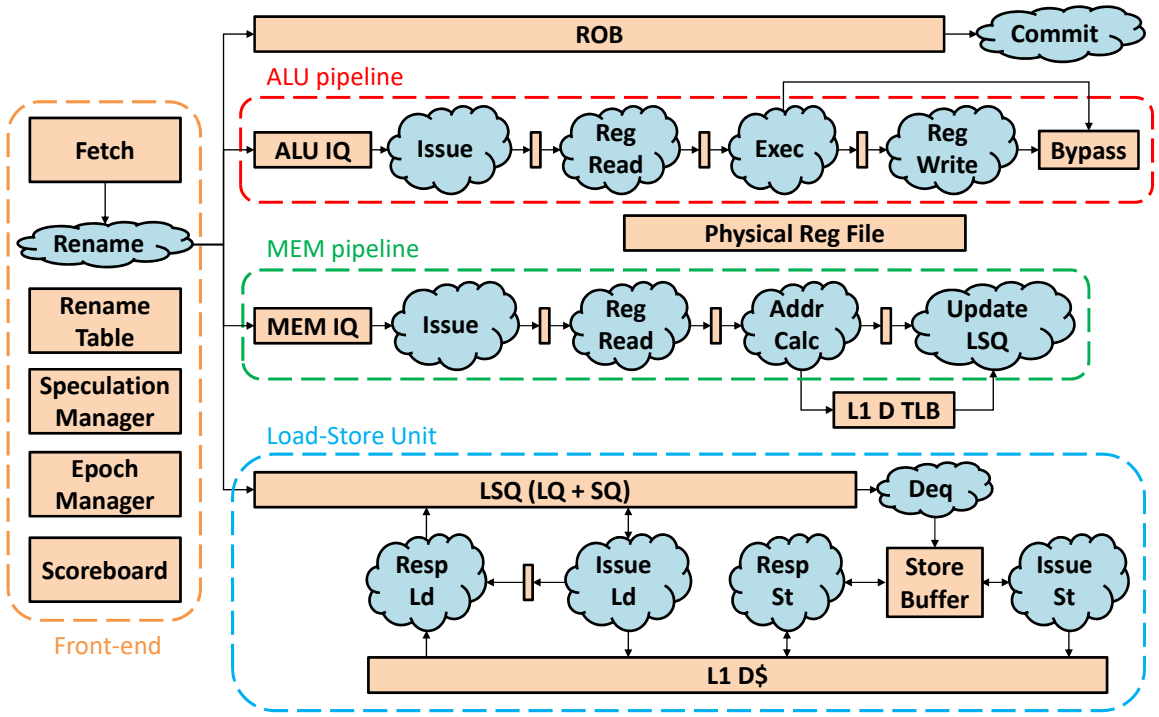


Fig. 9. Structure of the OOO core

Composable Building Blocks to Open up Processor Design, Sizhou Zhang, et al.

BOOM (Berkeley, language: Chisel)

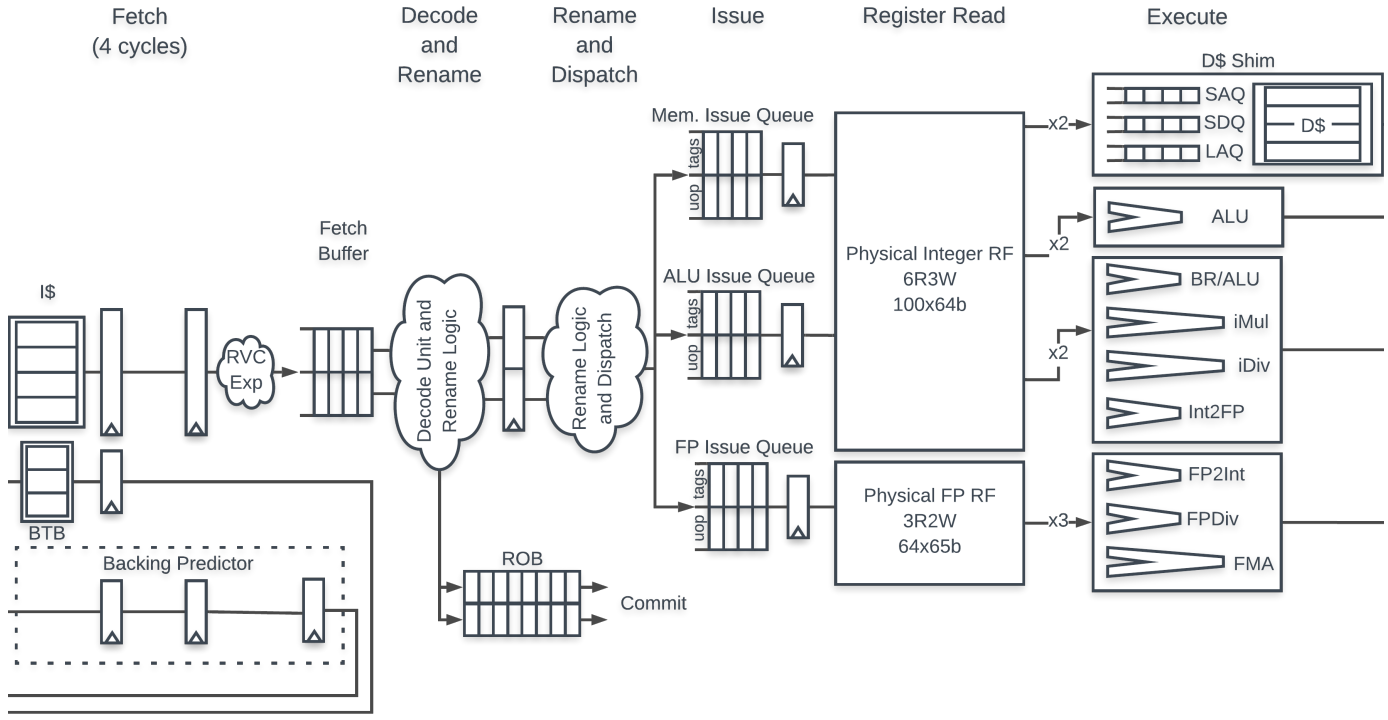


Figure 1: Overview of BOOM Pipeline

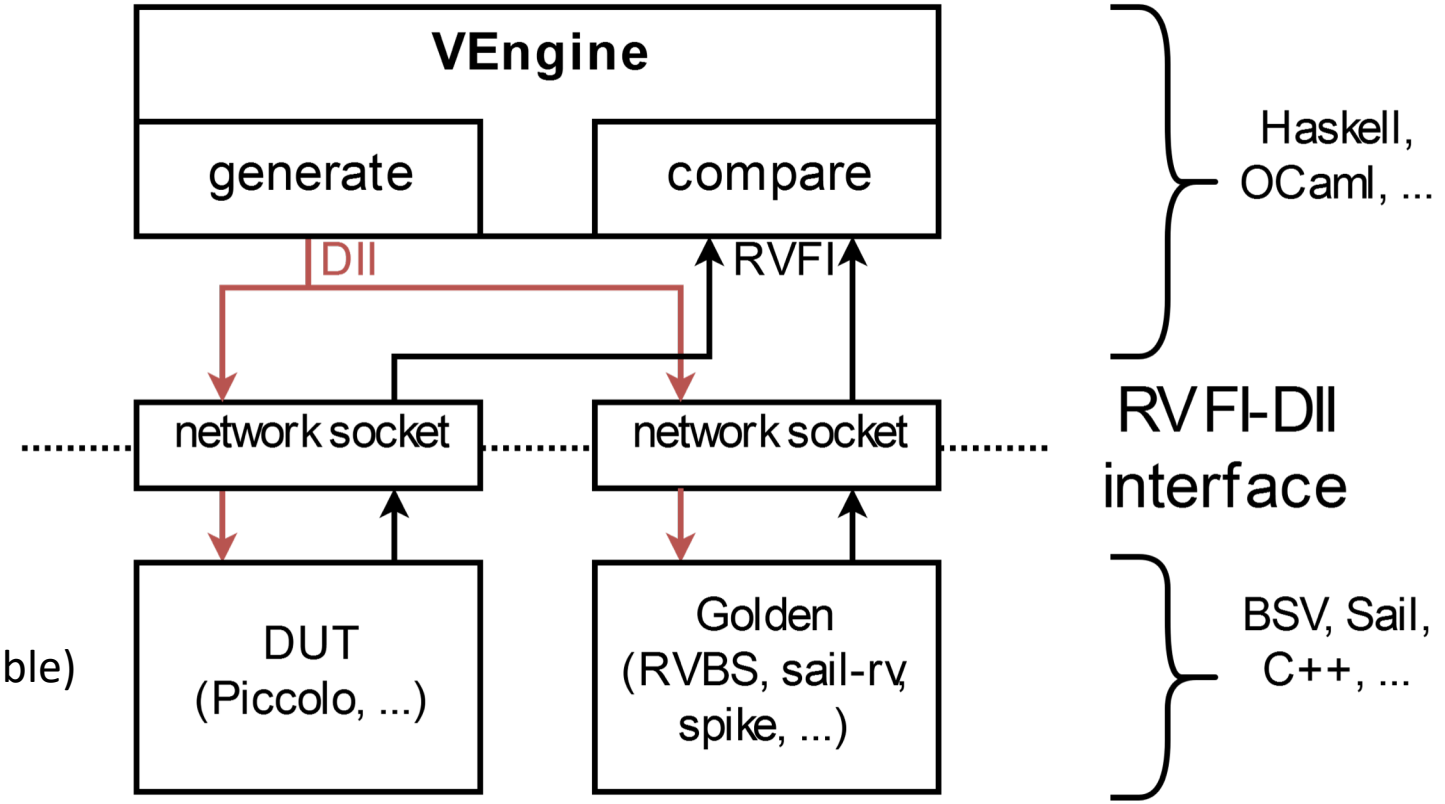
Replicating and Mitigating Spectre Attacks on a Open Source RISC-V Microarchitecture, Abraham Gonzalez, et al.

TestRIG: Reproducing Timing-sensitive Behaviour

Three interchangeable parts:

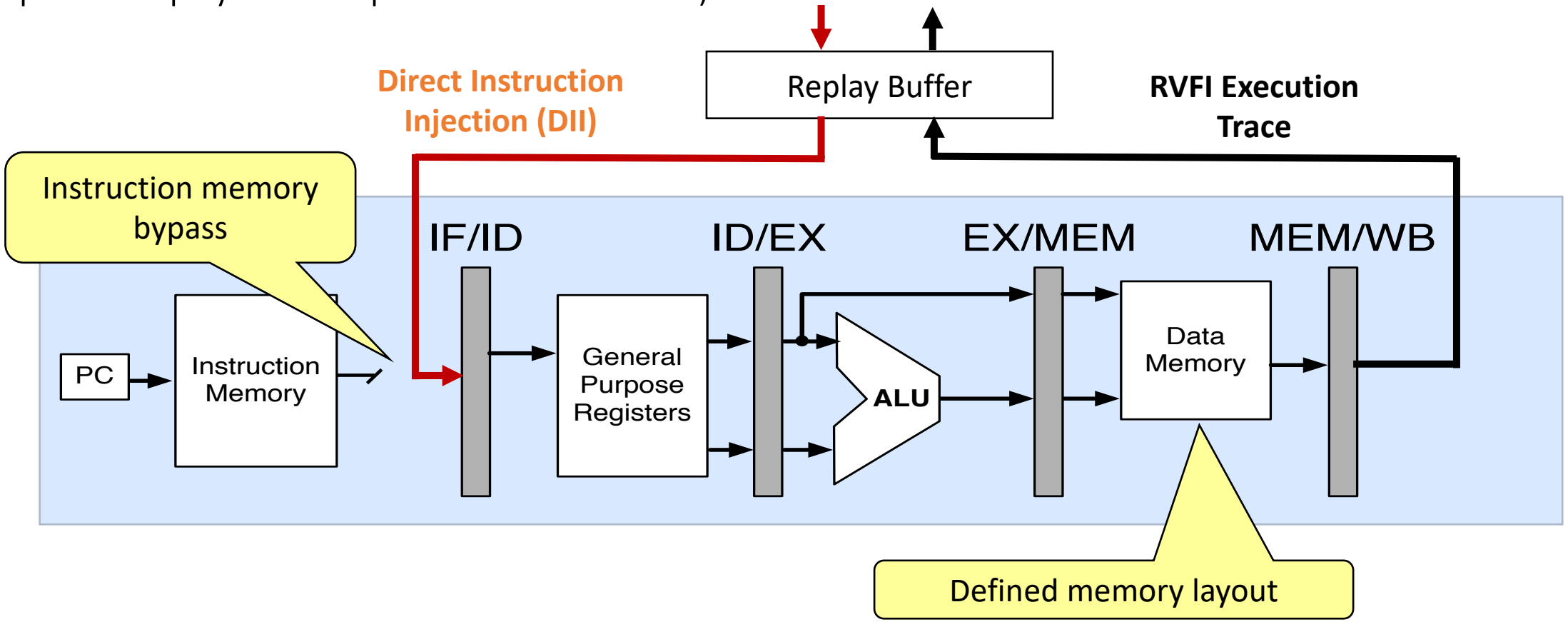
- Verification Engine, “VEngine”
  Generates interesting sequences
- Model
  Executable specification, or known-good implementation
- Implementation

(Models and implementations are interchangeable)



TestRIG: Reproducing Timing-sensitive Behaviour

Implementation instrumentation
(the price to pay for simplified verification)



Side Study - Spectre vs. CHERI

CHERI Opportunities: CHERI atomically ties bounds to pointers.

- Speculation limited to addresses within the object.
- Much better than to the entire address space!

Threats to CHERI:

- CHERI enables more fine-grained compartmentalization.
- User-space compartments that share a page table can now be targeted by Spectre.

Does CHERI give other handles for micro-architectural prevention of unsafe speculation?

Conclusion

Fully Open-source to facilitate community uptake and validation

All hardware and validation infrastructure is being developed open-source.

Much progress since 1 October 2019 start:

Currently adding TestRIG instrumentation of the RISCY-OO core
and familiarizing ourselves with a complex hardware design.

Jonathan.Woodruff@cl.cam.ac.uk