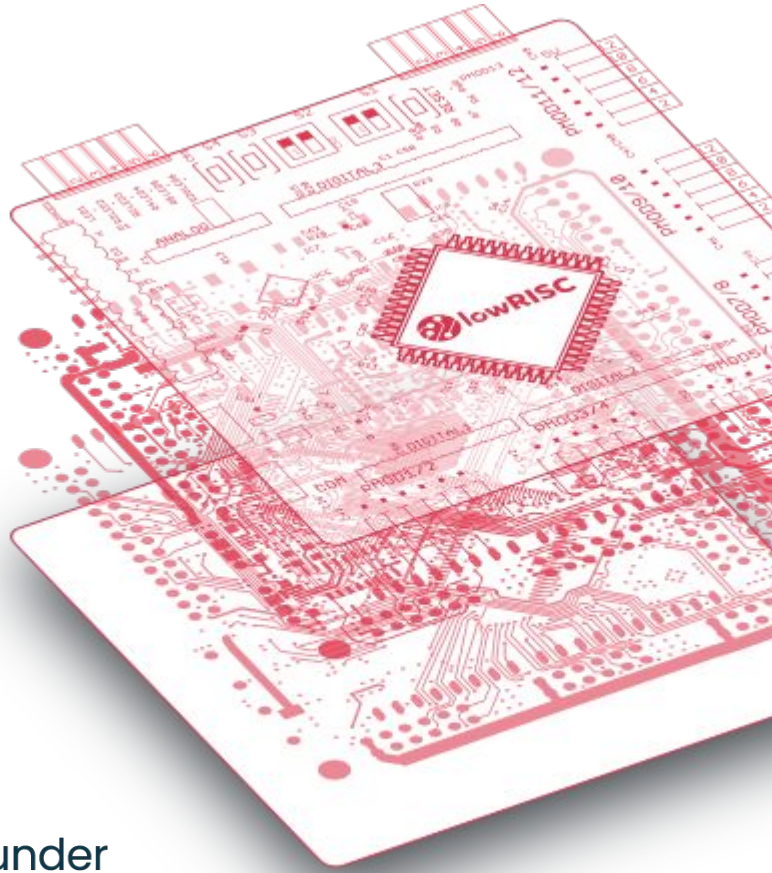
CHERI Prototyping and Open Source

Cybersecurity by design - from research to industry conference

Greg Chadwick, Digital Design Lead, lowRISC
gac@lowrisc.org

lowRISC

CHERI Alliance Founder



Open Source and Open Silicon

- Open source software is widely deployed and a foundational part of modern computing, but what about open silicon?

- Unlike open software we don't see much open silicon 'in the wild'
  - Though lowRISC is helping change that with OpenTitan

- CHERI development has benefited from open silicon
  - Open Silicon prototype CPUs have enabled research and development
  - Microsoft's CHERIoT Ibex core is moving towards production

- What challenges stand in the way of open silicon?

Open Silicon - Challenges

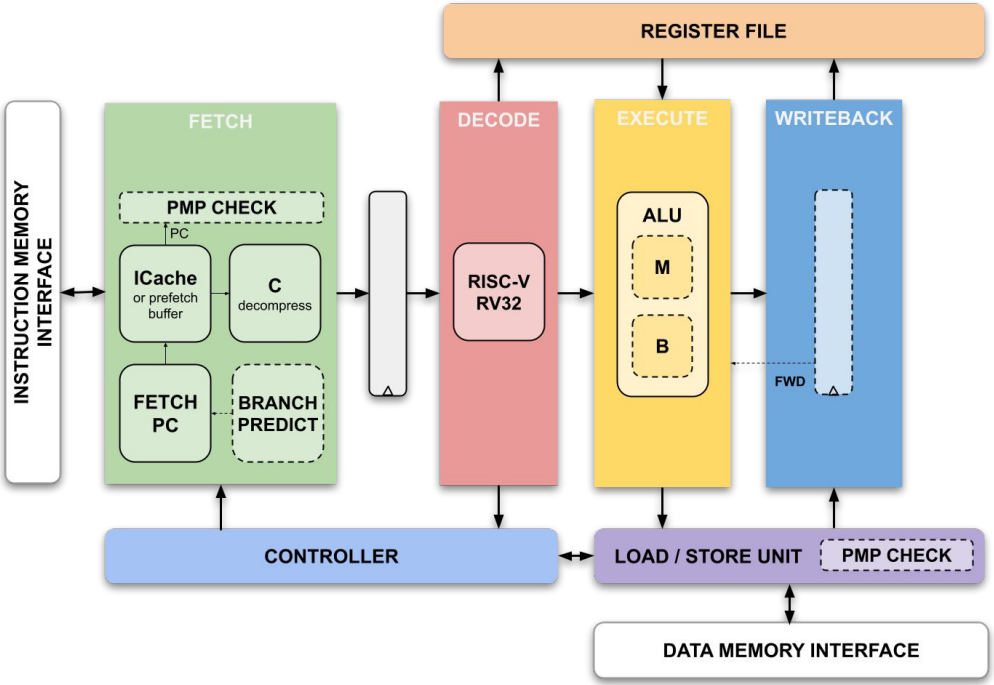
- Design Verification (DV) is vital, verification needs to be complete with full coverage
  - No-one will commit to using your design if they don't have high confidence it will work
- Standards are very high for commercial tape-outs
- Chip tape-outs are expensive and have long lead times
- Tooling is expensive and proprietary

Answers from the software world?

- Open-source software and libraries are produced in a collaborative and decentralised manner
- Can we learn from this and apply to areas beyond software?

	Software (typical project)	**Silicon design (typical project)**
Available skilled engineers	Many	Few
Tooling	Largely free	Mostly proprietary & expensive
Design turnaround	Months	Years
Bug fixes after deployment	Straightforward	Often impossible
End product	Virtual	Physical (mask costs, distribution etc.)
100% open IP for end product	Often possible	Currently impossible
Design flow	Iterative	Waterfall

RISC-V at the Core: Ibex®



https://github.com/lowRISC/ibex

Highly configurable **open source** RV32IMCB core with security features that include:

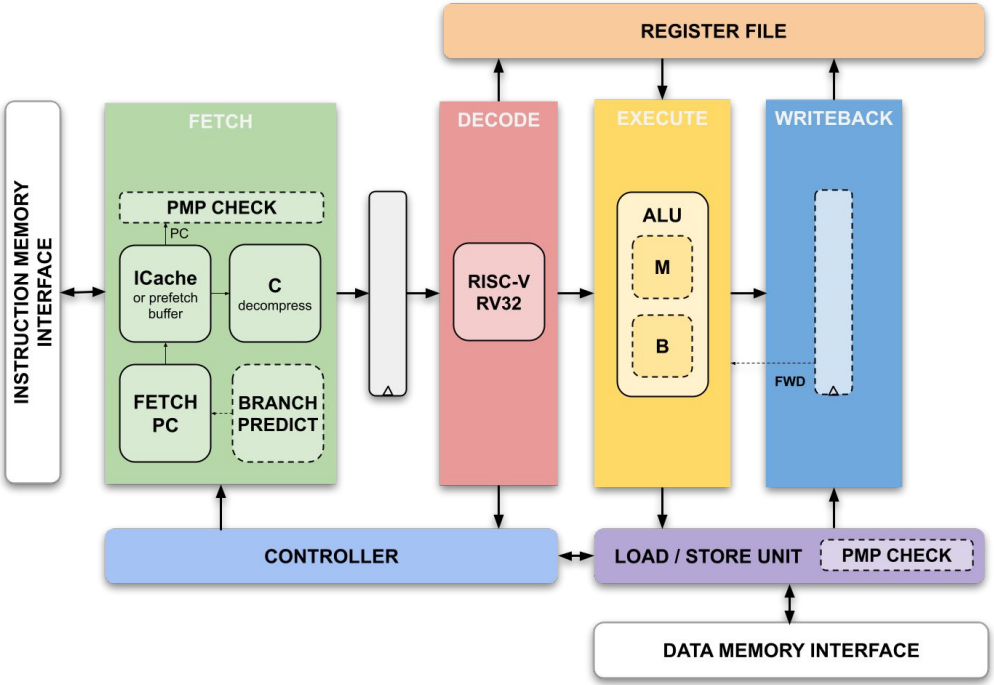
- ➔ Instruction cache memory scrambling
- ➔ Dual-core lockstep
- ➔ Data independent timing
- ➔ Dummy instruction insertion
- ➔ Bus and register file integrity
- ➔ Hardened PC

Includes full production quality DV, also open source

CHERIoT Ibex - A brief history

- ETH Zürich creates a small open silicon RISC-V CPU called zero-riscy
- It is contributed to lowRISC and renamed Ibex®, intended for use in OpenTitan®
- Working with OpenTitan® partners lowRISC expands it, adding many features and builds production grade DV
- Microsoft begins a project to scale the key ideas from CHERI down to embedded cores
- CHERIoT is born and Ibex is chosen as the base for the first implementation
- lowRISC begins the Sunburst project to provide evaluation platforms for CHERIoT
- SCI announces Iceni, the first commercial CHERIoT implementation based on CHERIoT Ibex

RISC-V at the Core: Ibex®



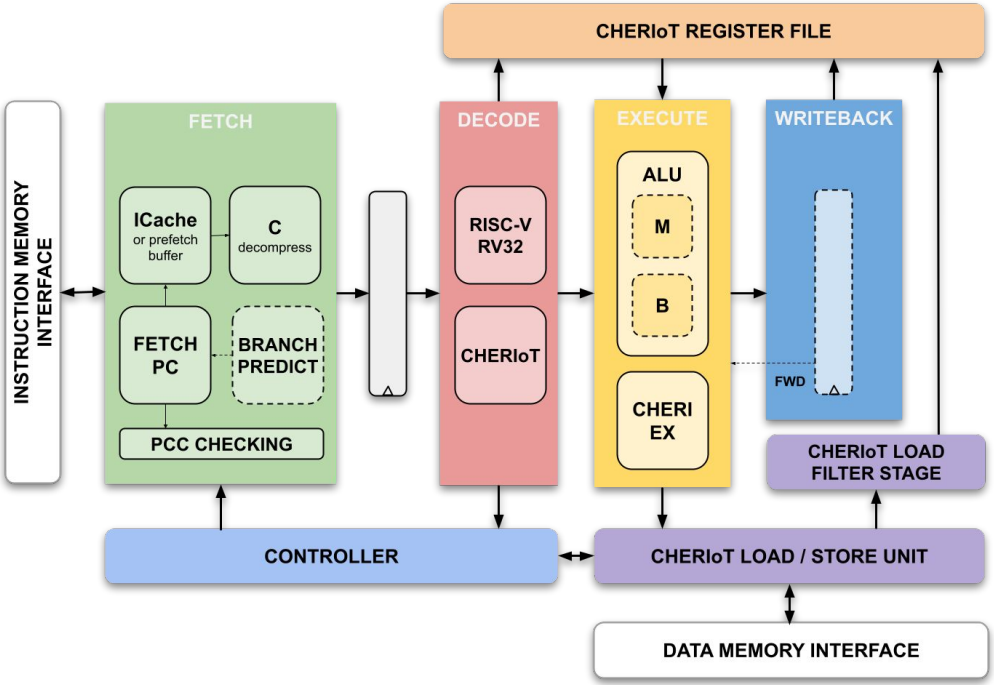
https://github.com/lowRISC/ibex

Highly configurable **open source** RV32IMCB core with security features that include:

- ➔ Instruction cache memory scrambling
- ➔ Dual-core lockstep
- ➔ Data independent timing
- ➔ Dummy instruction insertion
- ➔ Bus and register file integrity
- ➔ Hardened PC

Includes full production quality DV, also open source

Evolving Ibex®: Memory Safety with CHERIoT



https://github.com/microsoft/CherIoT-ibex

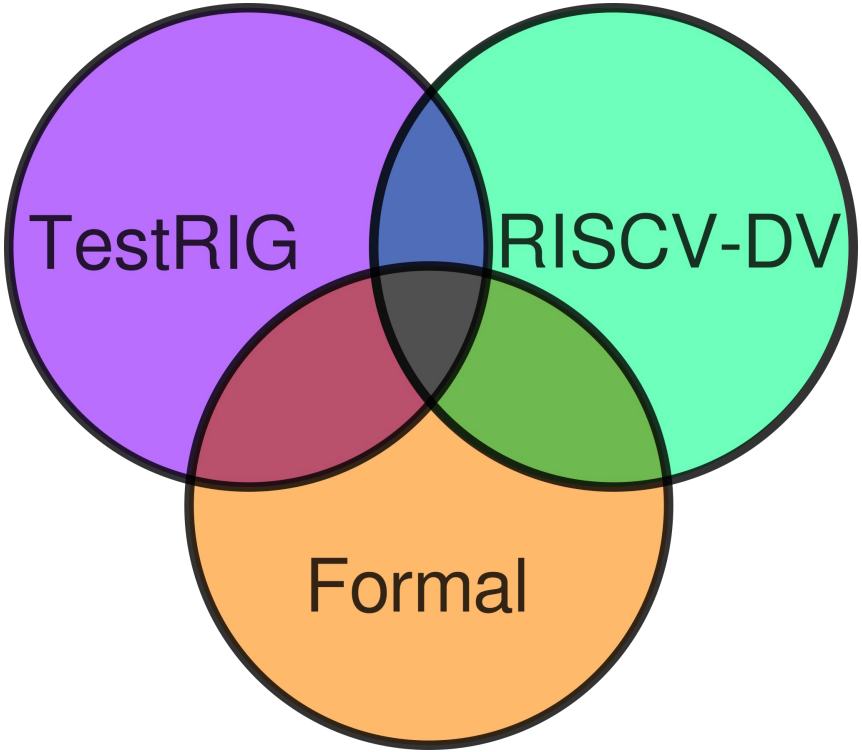
Microsoft lowRISC

"This is truly important foundational work, as it will help make CHERIoT-Ibex the world's first production grade, open-source CHERI-enabled microcontroller core. We're looking forward to seeing it broadly leveraged in commercial designs, bringing much-needed hardware security — in an efficient manner — to a broad swathe of critical applications."

Tony Chen
Partner Security Architect, Microsoft

CHERIoT Ibex DV

- Starting from a solid foundation with the base Ibex core already verified
- Extend RISCV-DV to generate CHERIoT code and add Sail to Ibex co-simulation
- Use TestRIG from Cambridge Computer Lab to better stimulate complex CHERI specific behaviour
- End to end formal to prove equivalence against Sail specification - Developed by group from Oxford University
- Each method has strengths and weaknesses
- Thanks to open source we can leverage all three, quickly putting research work in to practice



CHERIoT Ibex end to end formal

- Group at Oxford, led by Professor Tom Melham, have developed an end to end formal flow for CHERIoT Ibex
- Proves **un-bounded equivalence** against CHERIoT Sail model
- Tom's student, Louis-Emile Ploix, who has done significant work on the flow interned at lowRISC to expand it, including formally verifying the vanilla RISC-V Ibex core
- To be released soon under an Apache 2.0 license along with a paper
- Work could not have happened without open silicon as they needed a core to verify
  - Example of virtuous cycle as Oxford's work benefits the open silicon design

The key role of Open Silicon

- The production grade Ibex® gave Microsoft a solid base to build from
  - Concentrate on building CHERIoT, not sidetracked by basic core development
- Microsoft's decisions to release their extension work under the same Apache 2.0 license allowed usage and development of CHERIoT Ibex by everyone
- Sonata has allowed evaluation and use of CHERIoT in advance of production silicon
  - New DSbD cohort are all building on Sonata®
- OpenTitan IP is being re-used; Rivos integrating it into their SoC, Caliptra leveraging it for their RoT
- SCI can rapidly build production silicon by leveraging Sonata and CHERIoT Ibex along with peripheral IP from OpenTitan®

Moving beyond CHERI prototypes

- Open silicon has played a vital role in enabling CHERI research and development and the creation of FPGA based evaluation platforms
- Open silicon can continue to play a vital role in production CHERI silicon
- High-quality, fully verified, open silicon design provides a solid foundation for commercial designs
- More available silicon provides a healthy ecosystem others have confidence in building on
- History has shown that second sourcing is vital, don't want a fledgling ecosystem brought down by a single commercial failure
- Plenty of room for commercial innovation and differentiation on top of an open silicon base