KU LEUVEN

Security through Transparency and Openness in Computer Design

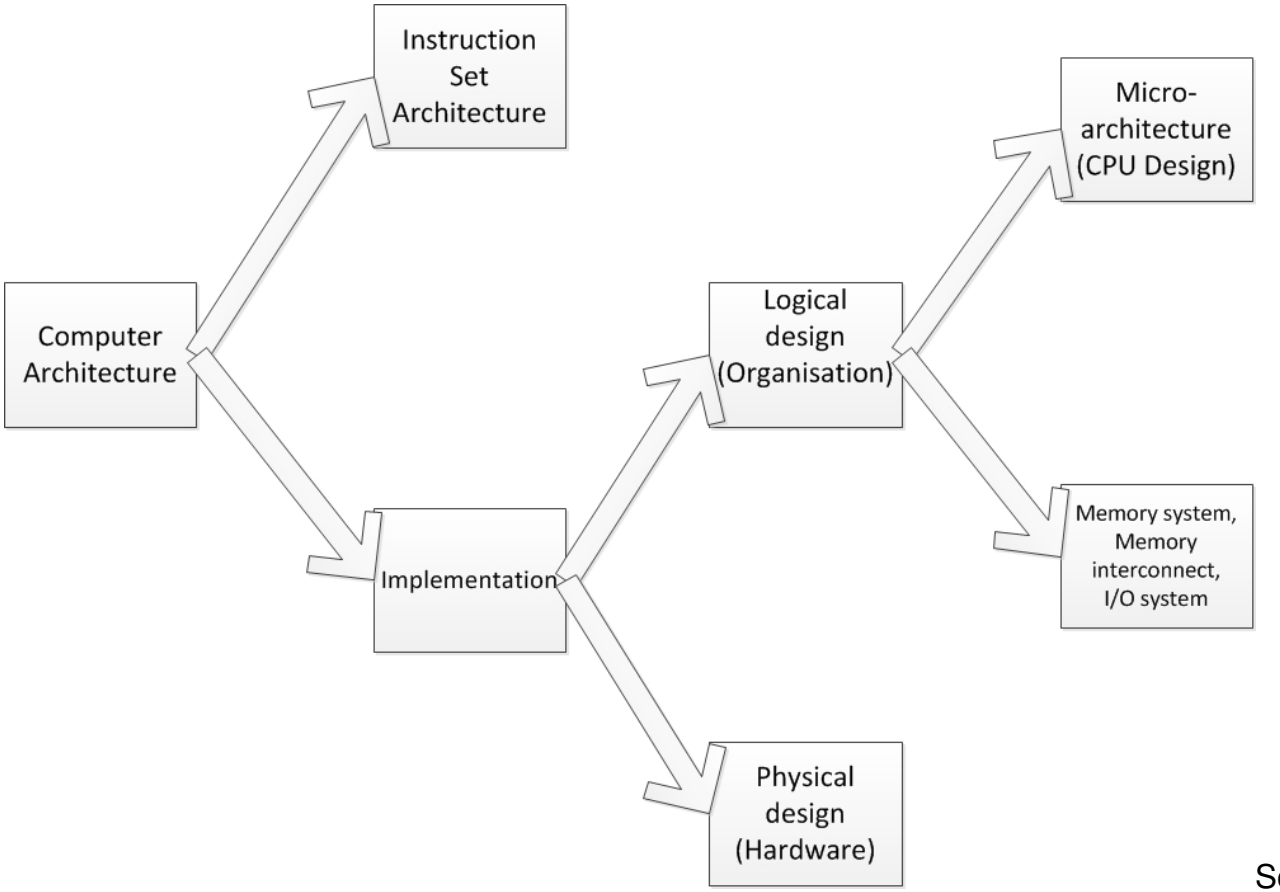
The Case for Free Instruction Set Architectures

Ivo Emanuilov, LL.M, Ph.D Cand.

Faculty of Law
Interdisciplinary Centre for IT & IP Law

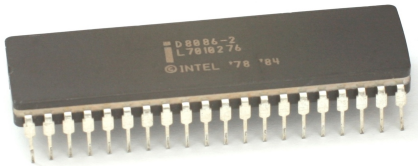
November 5, 2020

ISA in computer design



Source: *Wikimedia Commons*

Dominant ISAs



arm

CPU Engagement Models With ARM

Cortex License

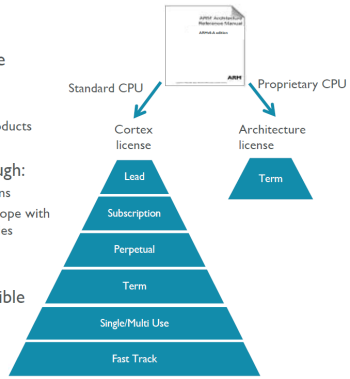
Partner licenses complete microarchitecture design

- Wide choices available
- Many different A, R & M products

CPU differentiation through:

- Flexible configuration options
- Wide implementation envelope with different process technologies

Range of licensing & engagement models possible



ANANDTECH
© ARM 2016

Architecture License

Partner designs complete CPU microarchitecture from scratch

- Clean room – no reference to Cortex designs

Freedom to develop any design

- Must conform to the rules & programmers model of a given architecture variant
- Must pass ARM architecture validation to preserve software compatibility

Long term strategic investment

ARM

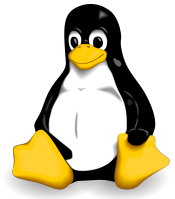
SPECTRE

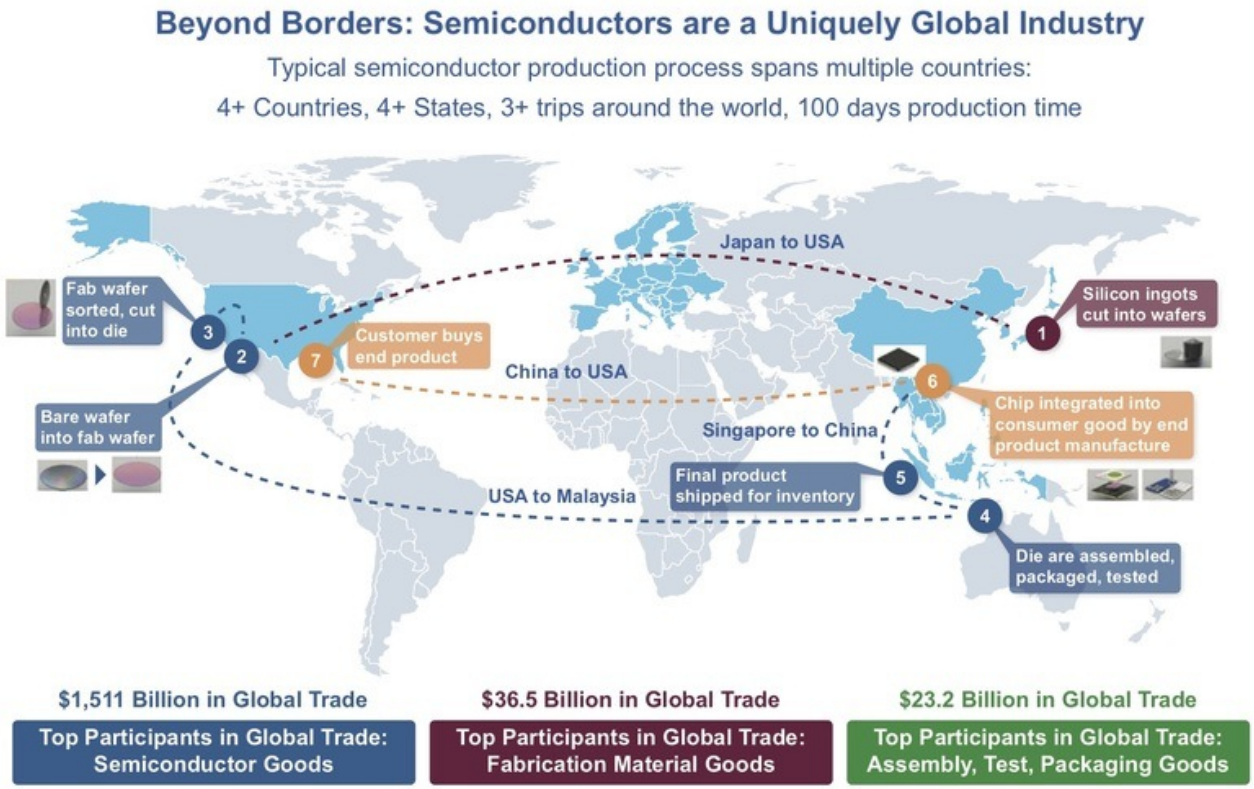
MELTDOWN

ISA's Role for Security

- What is 'correct implementation' of an ISA?
- Need of verification through open security review processes and 'security by design'
- Four issues with proprietary ISAs
  - Patents and licencing as barriers to (security) innovation
  - Independent software ecosystems and available expertise in open hardware communities
  - Dependency on a single company's vision and strategic goals
  - Transparency and shared core designs

The Case for Open ISAs: RISC-V





Security Promises of Open ISAs

Benefits	**Risks**
Modular design and extensibility	Ecosystem fragmentation
Transparency	Still chance of vulnerabilities
Long-term security evolution	Lack of interest by the community
Community review	Commercial and governmental support and scalability
Royalty-free use	Legacy compatibility, upfront transition costs

Table: Security Benefits and Risks of Open ISAs

Legal Perils of Open ISAs

Manageability, Collaboration & Competition

- Open ISAs can bring more competition in the market
- Modularity can create a market for customised solutions (eg, security-focused FPGAs)
- Democratisation of computer design
- Standardisation challenges
- Attacks from incumbent players
- Geopolitical concerns

RETAIL NOVEMBER 25, 2019 / 1:36 PM / UPDATED A YEAR AGO

U.S.-based chip-tech group moving to Switzerland over trade curb fears

Legal Perils of Open ISAs (cont'd)

Intellectual Property Rights and Licencing

- Uncertainty about copyleft licencing applied to open source hardware
- Lack of open source or low-cost toolchains
- Legal status of code incorporated by the toolchain into the output
- Legal status of the bitstream - is it a computer program and, if so, who is running it?

Legal Perils of Open ISAs (cont'd)

Liability

- Lawsuits in the aftermath of *Spectre* and *Meltdown*
- Case of *Intel Corp. CPU Marketing, Sales Practices and Product Liability Litigation, in the U.S. District Court for the District of Oregon*
- Liability for incorrect implementation?
- Liability for attacks combining software and hardware vulnerabilities?

Conclusion

- Transparency - key sociotechnical requirement for trust in computing
- Need to focus on transparency of the low-level building blocks of computing
- Address the technical, organisations and legal challenges all at once
- Account for the systemic challenges in the integrated circuit supply chain
- Towards an interdisciplinary approach to transparency regulation for cybersecurity

Q&A

Thank you for your attention!