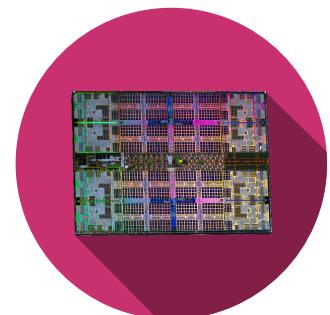




Computer Architecture History His

Information and Communication Systems program

Silvan Zahno silvan.zahno@hevs.ch

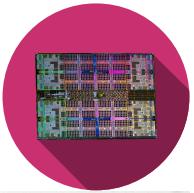
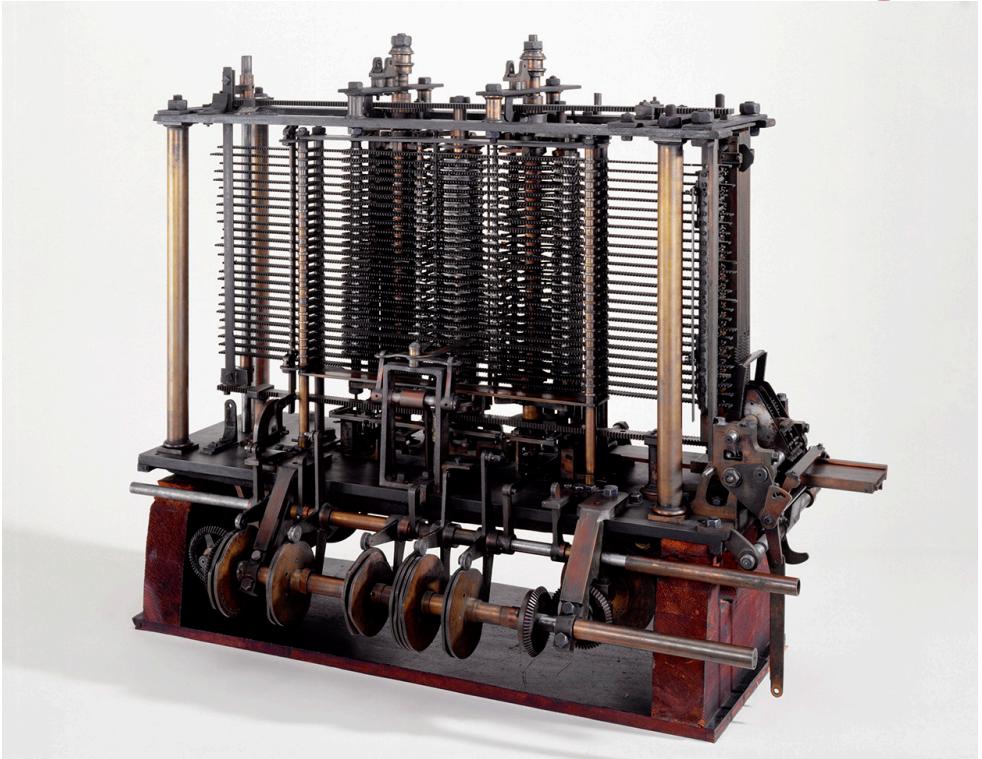


First Computer

Babbage Analytical Engine

- 1834-1871

- Arithmetical calculations
- Punch cards to input instructions
- Components
 - Mill for arithmetic calculations
 - Store acting as memory

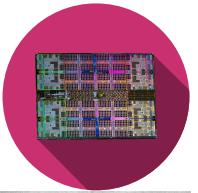
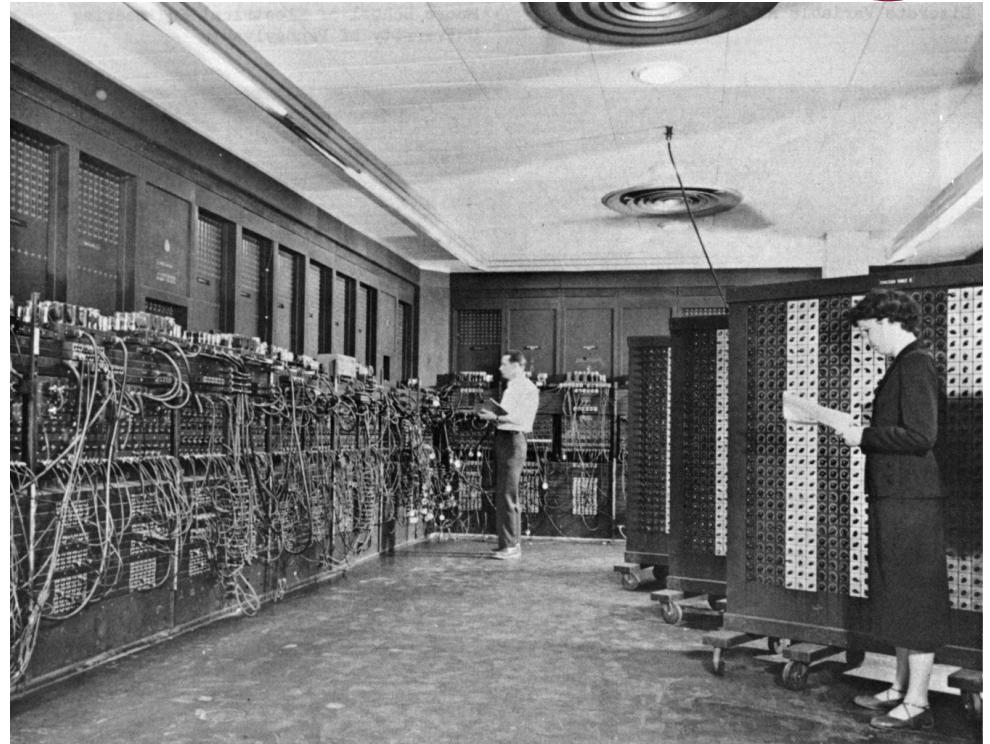


First Computer

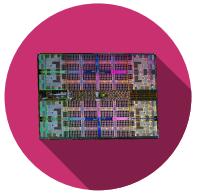
ENIAC

- 1945

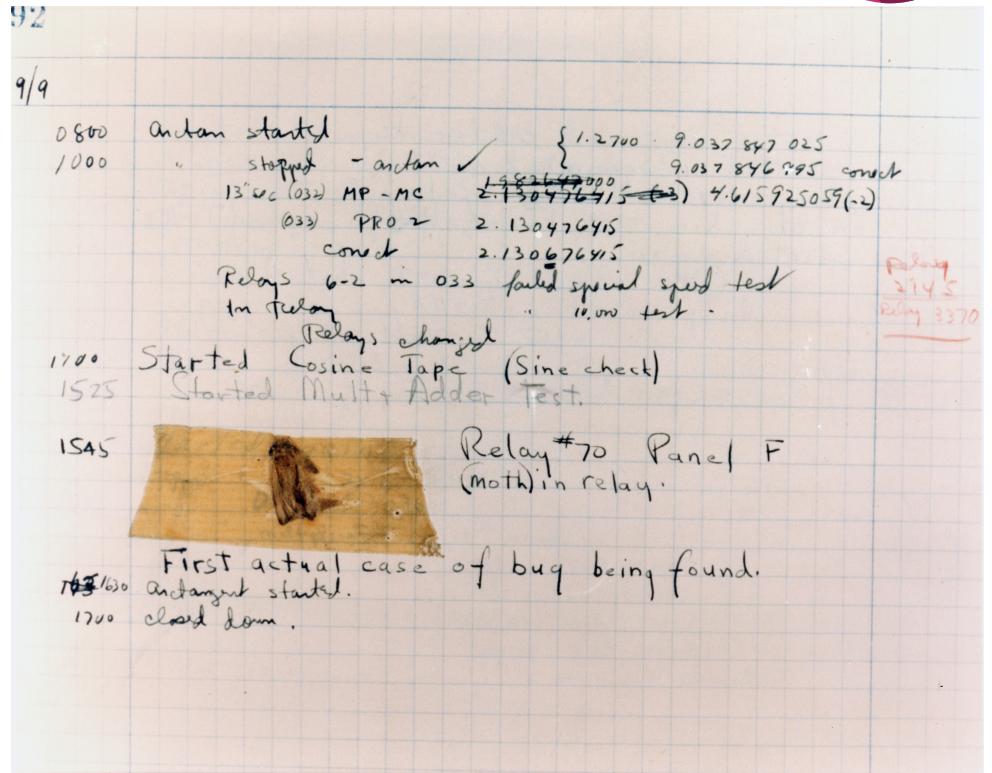
- Electronic Numerical Integrator and Computer
- For calculating ballistic tables
- 18'000 vacuum tubes
- 5'000 calculation/sec
- Programmed with cables and switches



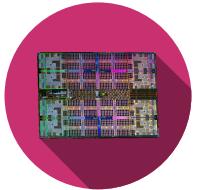
First Bug



- Grace Hopper 1947
- Harvard Mark II
- Moth was found in relay #70

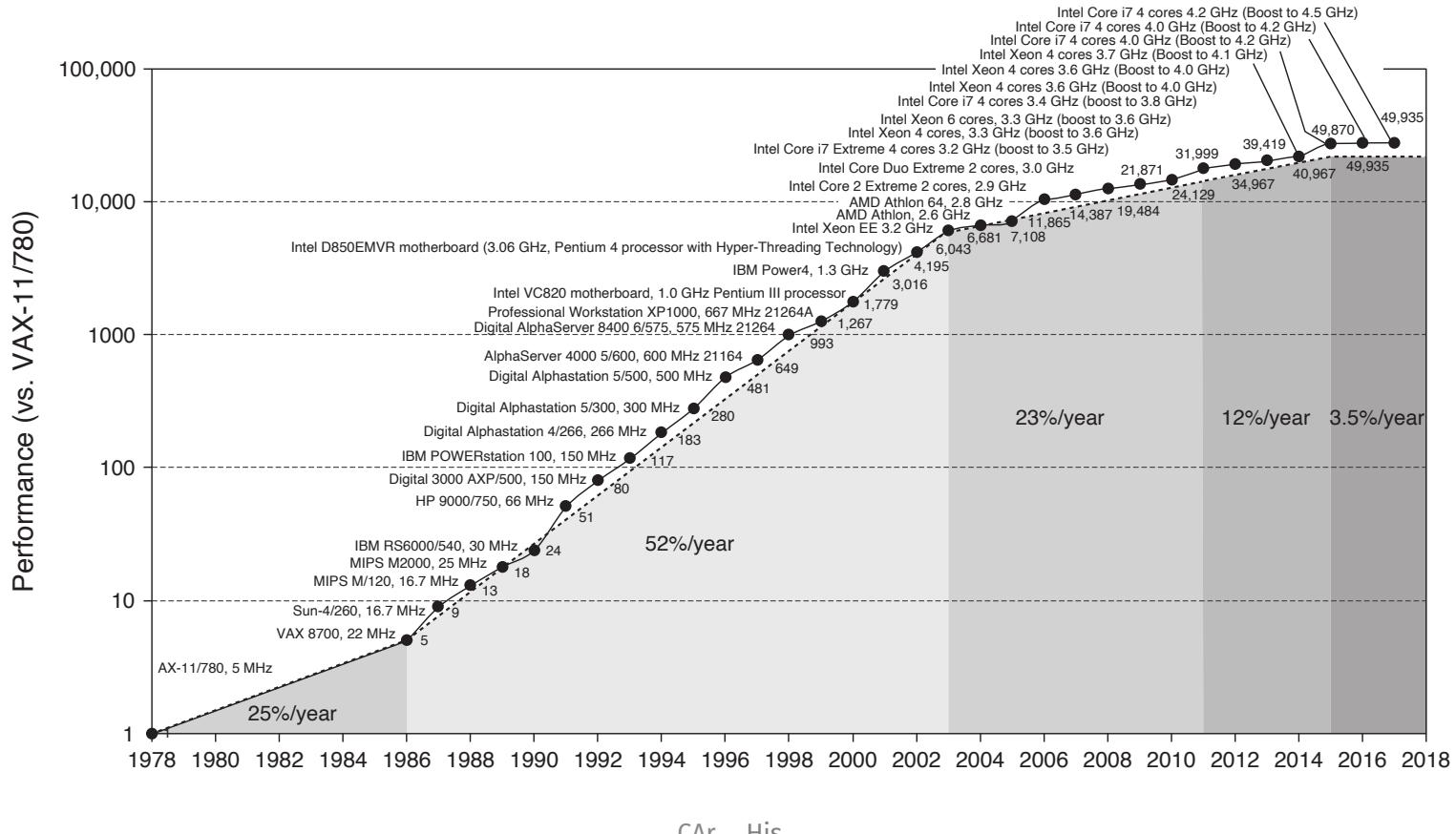
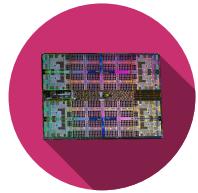


Which computer architectures do you know?



Sequential Processor Performance

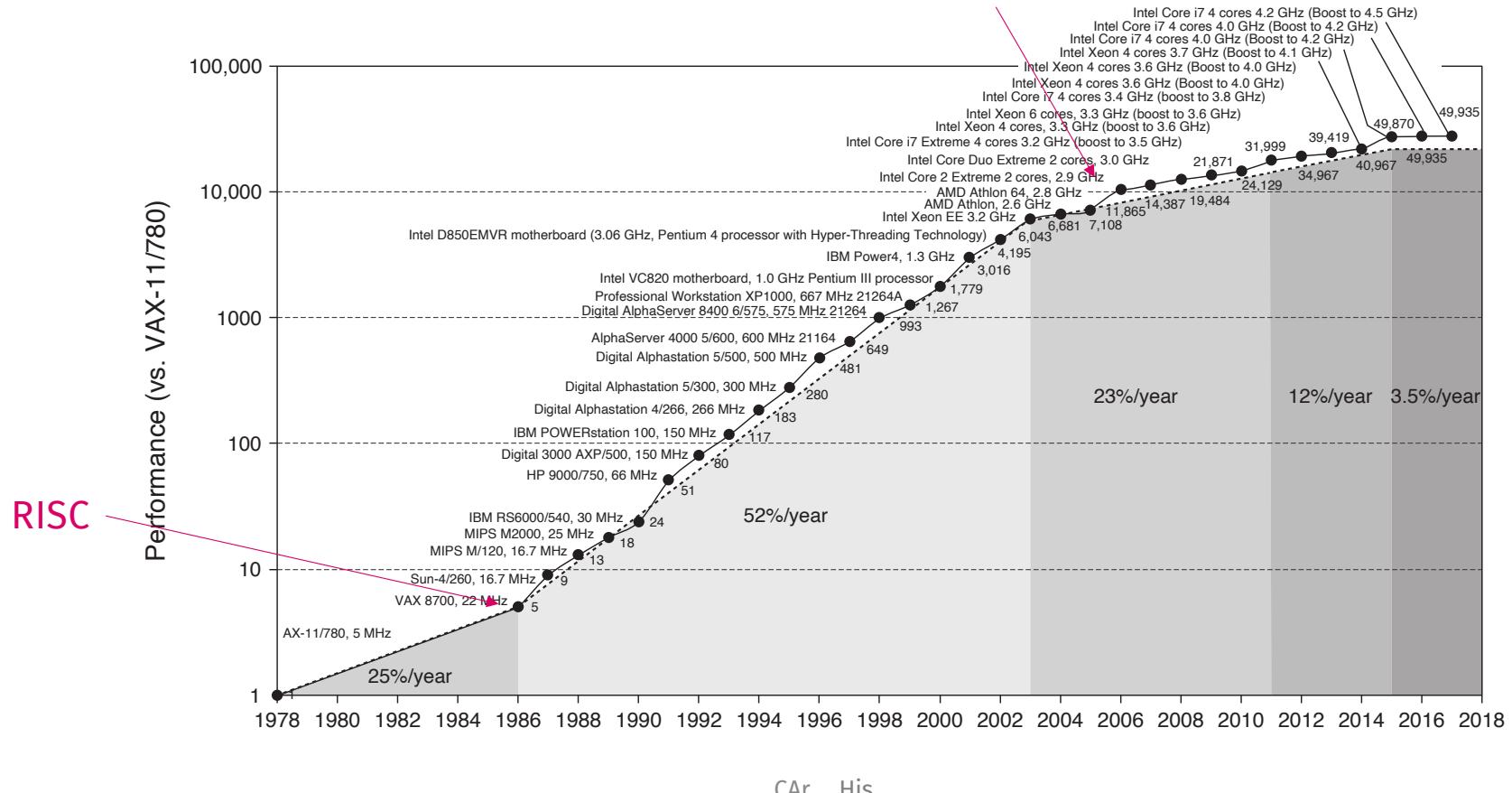
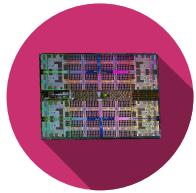
Logplot - Performance vs. Years



Sequential Processor Performance

Logplot - Performance vs. Years

Multi-Processor

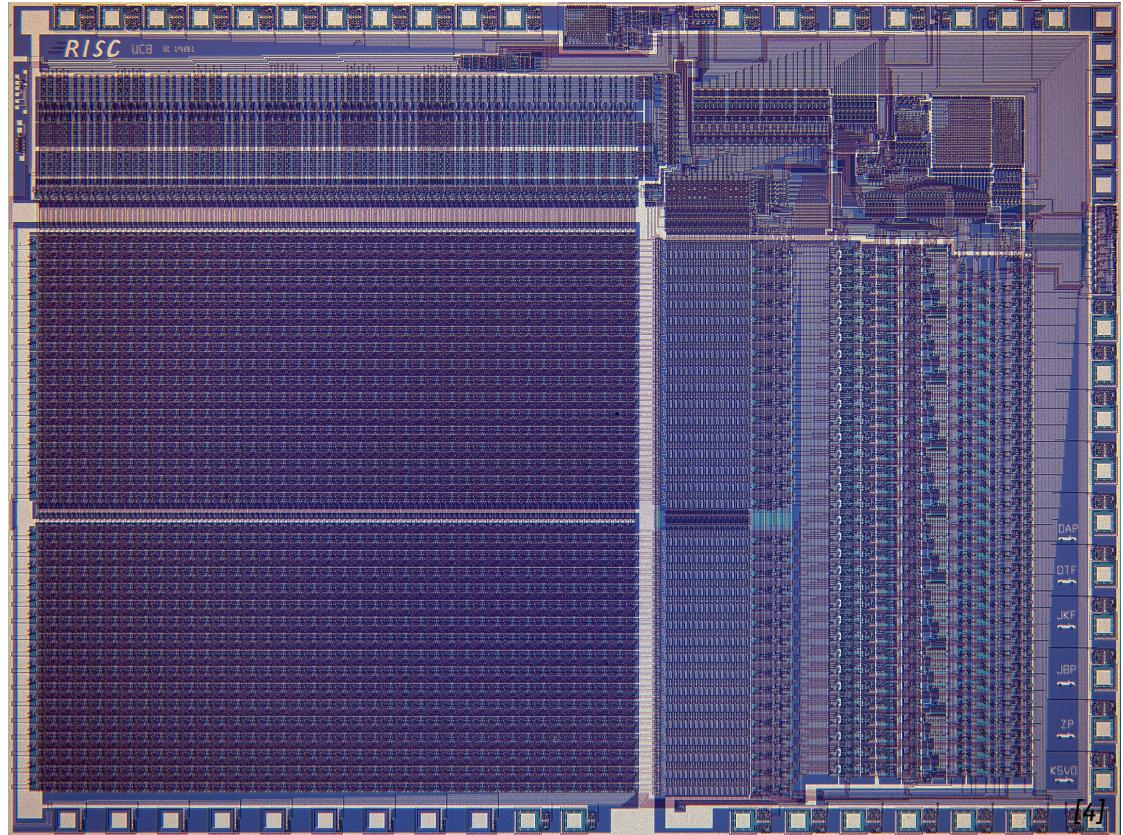
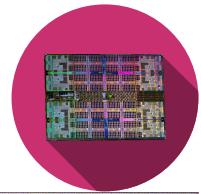


Computer Architectures

RISC 1

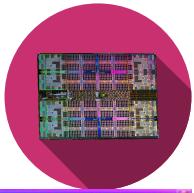
- Basic Pipelined Processor

~50'000 Transistors



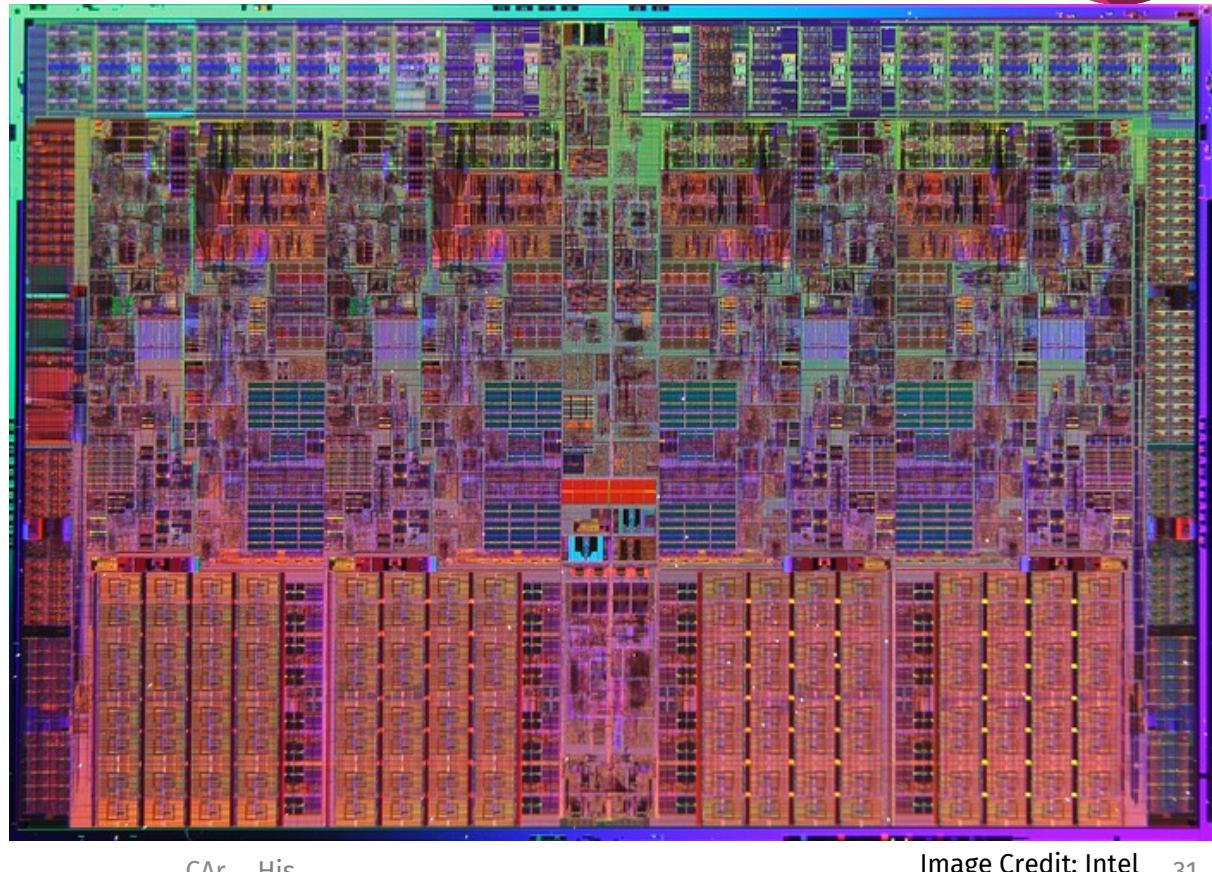
Computer Architectures

Original i7 Nehalem



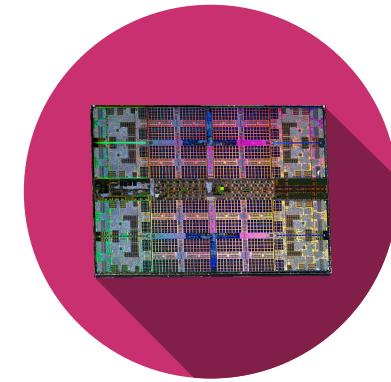
- Instruction Level Parallelism
 - Superscalar
 - Very Long Instruction Word (VLIW)
- Long Pipelines
- Advanced Memory and Caches
- Data Level Parallelism
 - Vector
 - GPU
- Thread Level Parallelism
 - Multithreading
 - Multiprocessor
 - Multicore
 - Manycore

~700'000'000 Transistors



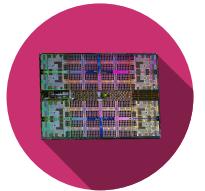
Car His

Image Credit: Intel 31



Processor Bugs / Vulnerabilities

Vulnerabilities in modern computers



Meltdown

Reading Kernel Memory from User Space

```
# rcx = kernel address, rbx = probe array
xor rax, rax          # Clear rax (set to 0) to avoid residual values
retry:
mov al, byte [rcx]    # Load a single byte from the kernel address in rcx
shl rax, 0xc           # Multiply the byte value by 4096 (0x1000)
                      # to create an index for the probe array
jz retry              # If rax == 0, retry (optional mitigation attempt)
mov rbx, qword [rbx + rax]
                      # Access the probe array at an index based on the secret byte.
                      # This causes a **cache access** that leaks the byte through timing.
```

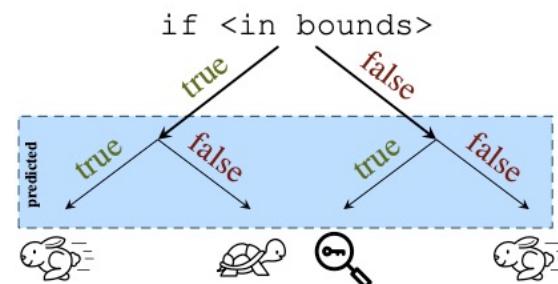


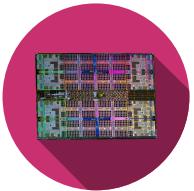
C4

Spectre

Microarchitectural attack which exploits out-of-order execution

Instructions are not executed in the correct order





References

[1]

“Analytical Engine,” *Wikipedia*. Jul. 03, 2022. Accessed: Jul. 13, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Analytical_Engine&oldid=1096269852

[2]

“Bug (engineering),” *Wikipedia*. Jun. 16, 2022. Accessed: Jul. 13, 2022. [Online]. Available: [https://en.wikipedia.org/w/index.php?title=Bug_\(engineering\)&oldid=1093361677](https://en.wikipedia.org/w/index.php?title=Bug_(engineering)&oldid=1093361677)

[3]

“ENIAC,” *Wikipedia*. Jul. 10, 2022. Accessed: Jul. 13, 2022. [Online]. Available: <https://en.wikipedia.org/w/index.php?title=ENIAC&oldid=1097477750>

[4]

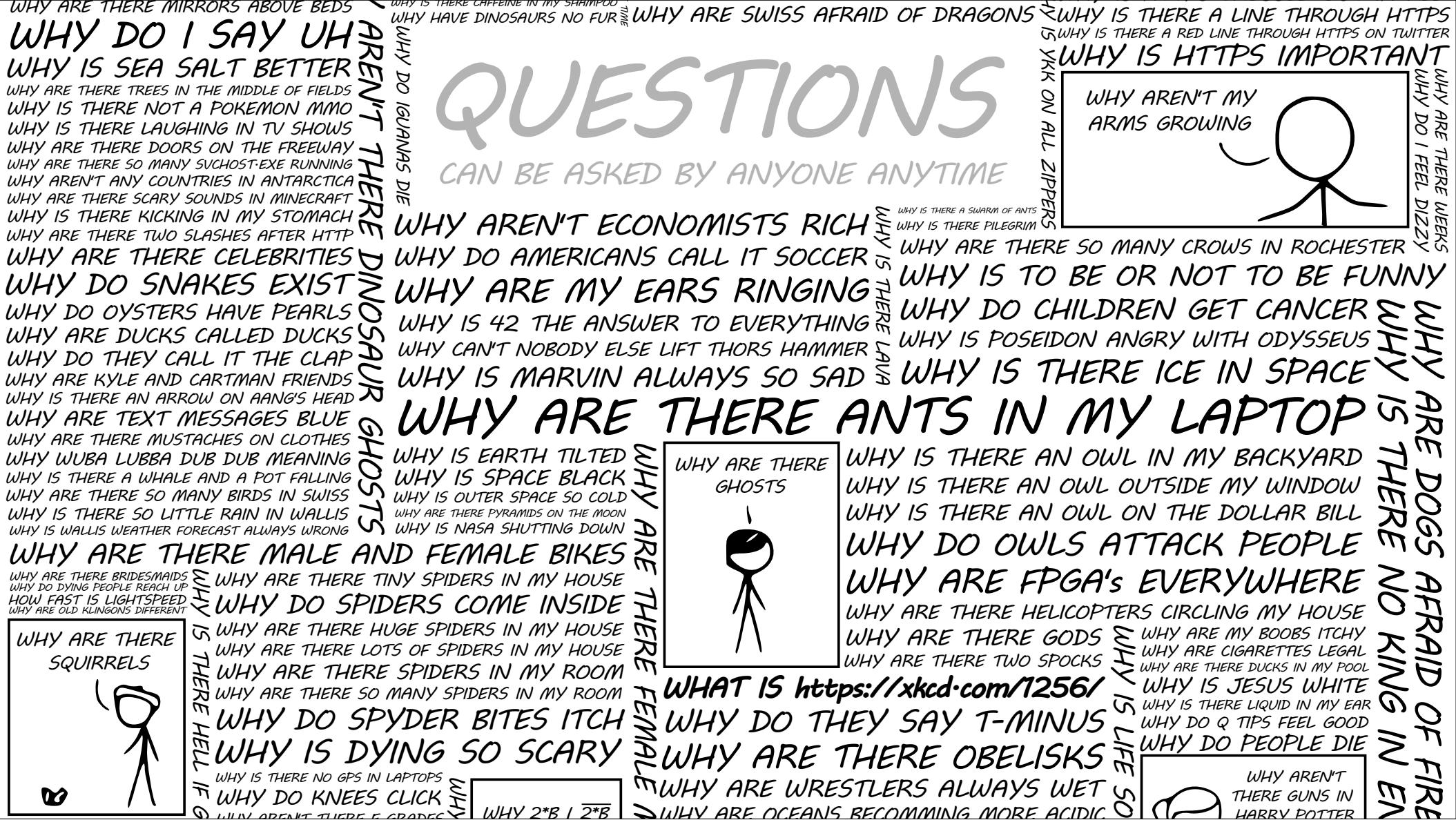
J. L. Hennessy and D. A. Patterson, *Computer Architecture: A Quantitative Approach*, 6th Edition. Elsevier, 2019.

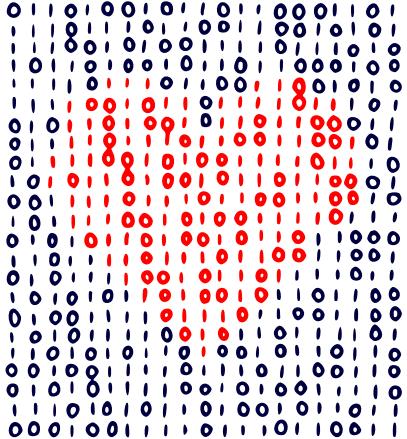
[5]

D. Wentzlaff, “Computer Architecture ELE 475 / COS 475.” Princeton University, 2019.

[6]

“Meltdown and Spectre.” Accessed: Mar. 11, 2025. [Online]. Available: <https://spectreattack.com/>





Hes·so // VALAIS
WALLIS



Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

Silvan Zahno silvan.zahno@hevs.ch

