

103ns



MELTDOWN: STASHAWAY - SLEDGEHAMMER

3

2











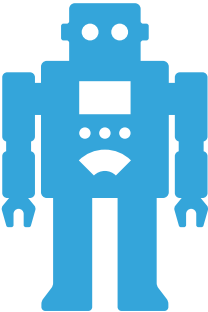












CRUCORE

VALUE

Read

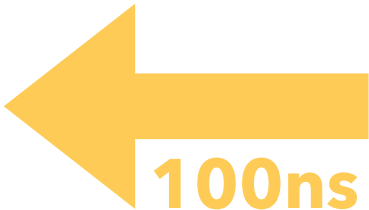
Cache



Read



RAM



VALUE (IN CACHE)

Gamechane

RAM

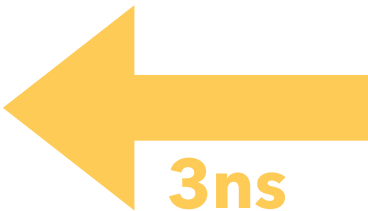
- ▶ Reading one byte stalls the CPU for hundreds of μ OPs
- ▶ CPU caches considerably speed this up
- ▶ E.g. reading cached takes 3ns, reading uncached 103ns



Not in cache



In cache



3ns

Then we ask up *“what is the value at address X?”* This is called *“address X is cache”*

“READ” INSTRUCTION

For a CPU the “READ value from memory at 4711” instruction looks like this (μOPs):

1. Check that program may read from address 1
2. Store the value at address in register¹ 2

If 1 fails the program is aborted.

This can be handled by the program.

¹ Register: The CPU's scratchpad

MELTDOWN: STASHING AWAY – SIDECCHANNEL



- ▶ Reading one byte stalls the CPU for hundreds of μ OPs
- ▶ CPU caches considerably speed this up
- ▶ E.g. reading cached takes 3ns, reading uncached 103ns

The cache speeds up "what is the value at address X?". This is called "(address) X is cached"