Meltdown basically works like this:

1. READ secret from forbidden address
    1. Check that program may read from address
    2. Store the read value in register
2. Stash away secret
    1. *Magic*
3. *Retrieve secret (later)*

MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MELTDOWN: READING FORBIDDEN DATA

34


1


2


1


1

2


1

μOPs:

MELTDOWN: READING FORBIDDEN DATA

μOPs ordered by *instruction*	μOPs ordered by *execution*
1 Check access	2 Read into register
2 Read into register	1 *Magic*
1 *Magic*	1 Check access

The re-ordering on the right happens, when the “forbidden data” is already cached (because cache access is so fast).

MELTDOWN: READING FORBIDDEN DATA

Meltdown basically works like this:

- READ secret from forbidden address
  1. Check that program may read from address
  2. Store the read value in register
- Stash away secret
  1. *Magic*
- *Retrieve secret (later)*

µOPs: 1 2 1