Side Channels

Understanding Hardware Vulnerabilities

Siddhesh Poyarekar

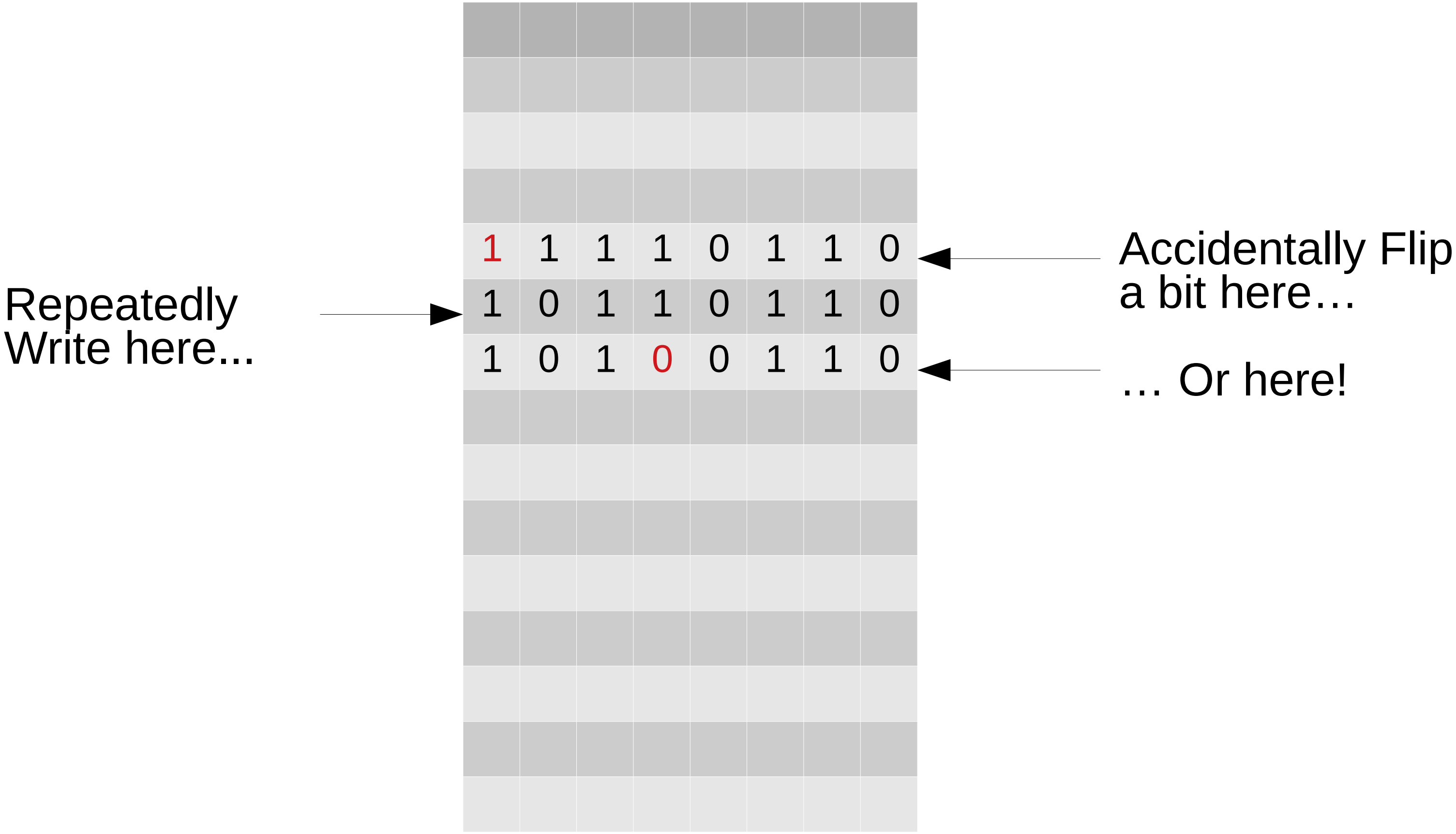
Not a Talk!

- Open discussion about hardware vulnerabilities
  - IANAE
  - I introduce, WE discuss
- Rowhammer
- Speculative Execution for fun and profit
- Side Channels
- ...

The Hammering RAM

- A classical hardware bug
- Design error in RAM DIMMs
- Charge leak into adjacent rows

The Hammering RAM



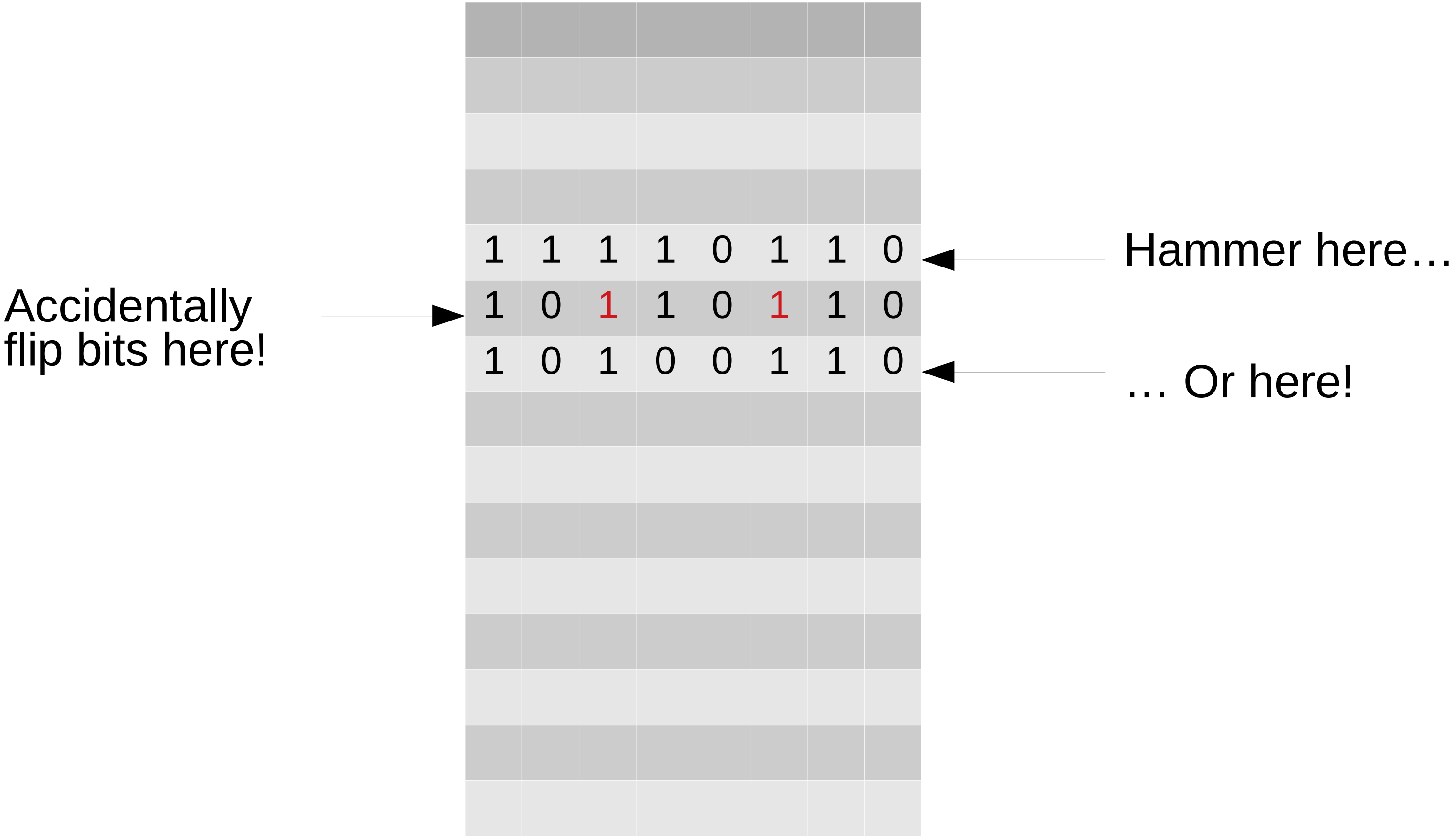
Repeatedly
Write here...

1	1	1	1	0	1	1	0
1	0	1	1	0	1	1	0
1	0	1	0	0	1	1	0

Accidentally Flip
a bit here…

… Or here!

Hammering Both Ends



Hammer here…

Accidentally flip bits here!

… Or here!

1	1	1	1	0	1	1	0
1	0	1	1	0	1	1	0
1	0	1	0	0	1	1	0

Rowhammer

- Has shown to be used for writing to arbitrary memory
  - Spray memory with the desired result
  - Repeatedly read and flush address(es) adjacent to target PTE
  - PTE modified

Speculative Execution

- Powerful performance tool in CPU Design
- Execute beyond branches
  - Commit only if branch is taken
  - Final result is always consistent
- What could go wrong?!

We are still finding out

- Speculation across privilege boundaries
  - Meltdown
- Branch predictor Speculation
  - Spectre variant 2
- Speculation during context switches
  - Reading FP regs before regs are restored
- Speculation across stores
  - Why would you even do that
    - It’s OK Alpha, you can do whatever you want. I was asking the nicer architectures

Side Channels

- Analyzing the computer’s droppings
  - Observe the surroundings if you cannot directly observe the subject
  - The computer ‘drops’ way more information than the average tiger!
- Cache effects of speculative execution
- Heat, Power, Radiation signatures
- Timing Signatures