250P: Computer Systems Architecture

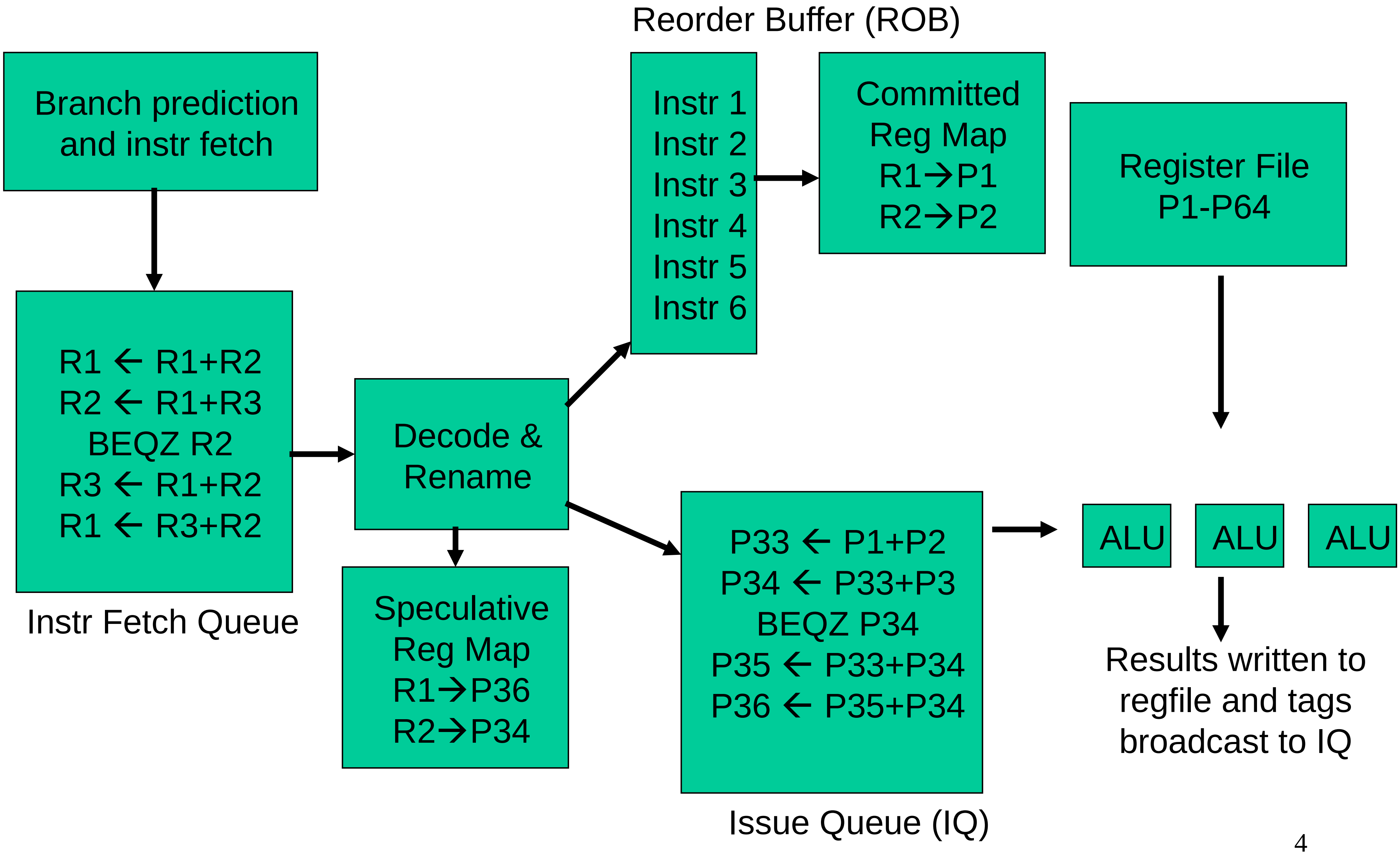
Lecture 13: Side channel attacks Meltdown and Spectre

Anton Burtsev
December, 2019

Meltdown

Page tables and protection

The Alpha 21264 Out-of-Order Implementation



Branch prediction and instr fetch

R1 ← R1+R2
R2 ← R1+R3
BEQZ R2
R3 ← R1+R2
R1 ← R3+R2

Instr Fetch Queue

Decode & Rename

Speculative Reg Map
R1→P36
R2→P34

Reorder Buffer (ROB)

Instr 1
Instr 2
Instr 3
Instr 4
Instr 5
Instr 6

Committed Reg Map
R1→P1
R2→P2

Register File
P1-P64

P33 ← P1+P2
P34 ← P33+P3
BEQZ P34
P35 ← P33+P34
P36 ← P35+P34

Issue Queue (IQ)

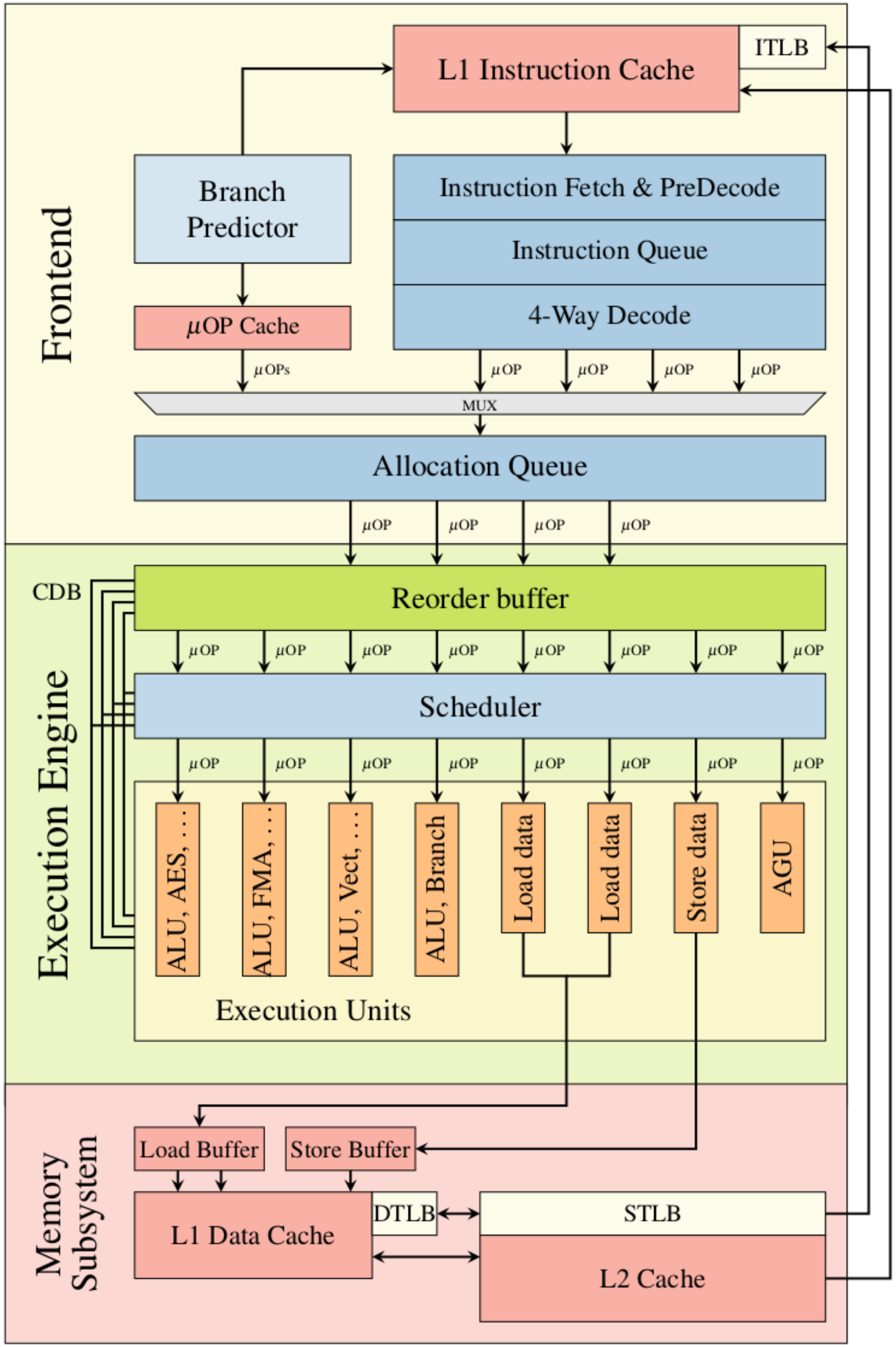
ALU

ALU

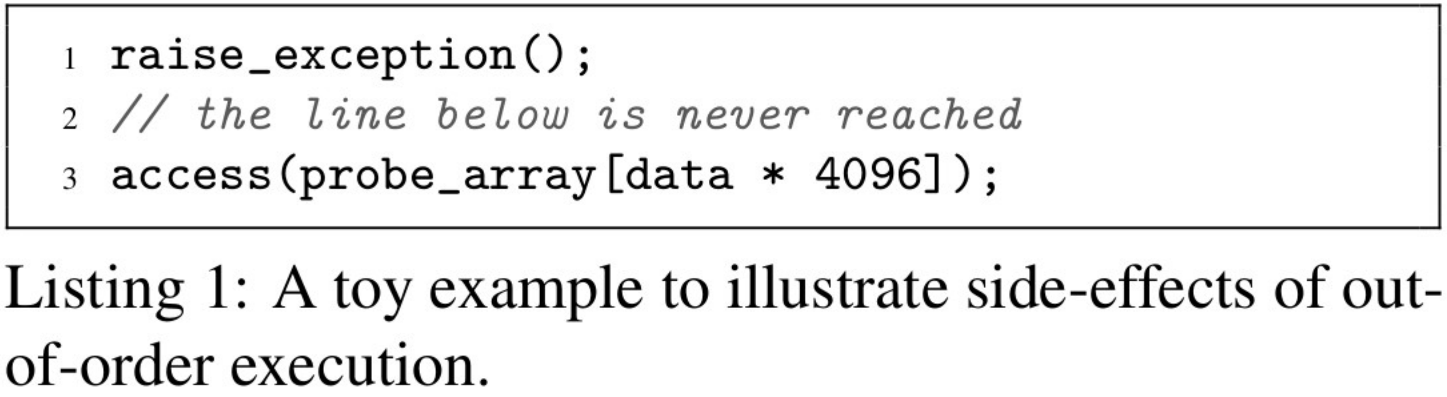
ALU

Results written to regfile and tags broadcast to IQ

Skylake (simplified)

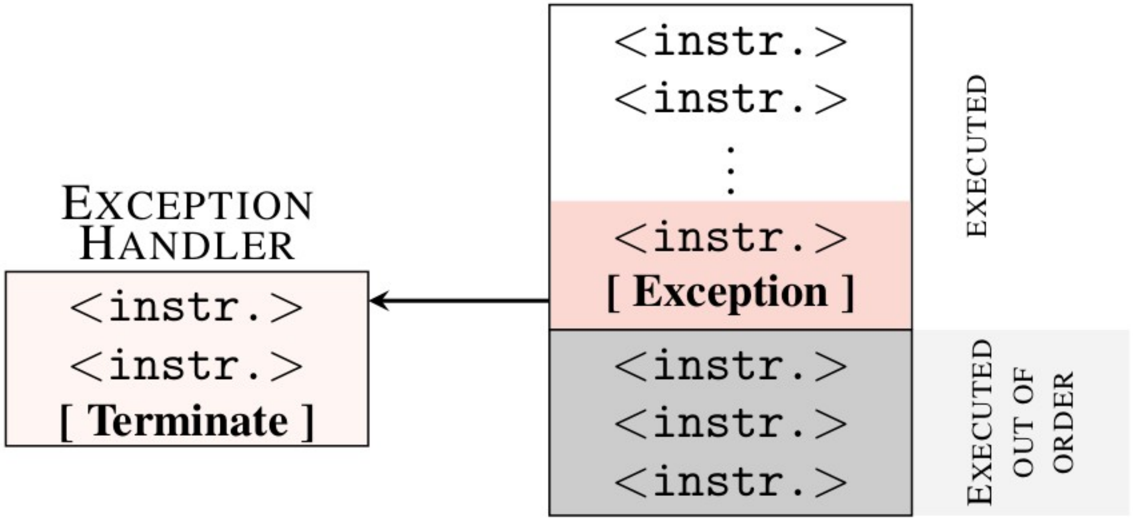


Exceptions and speculation

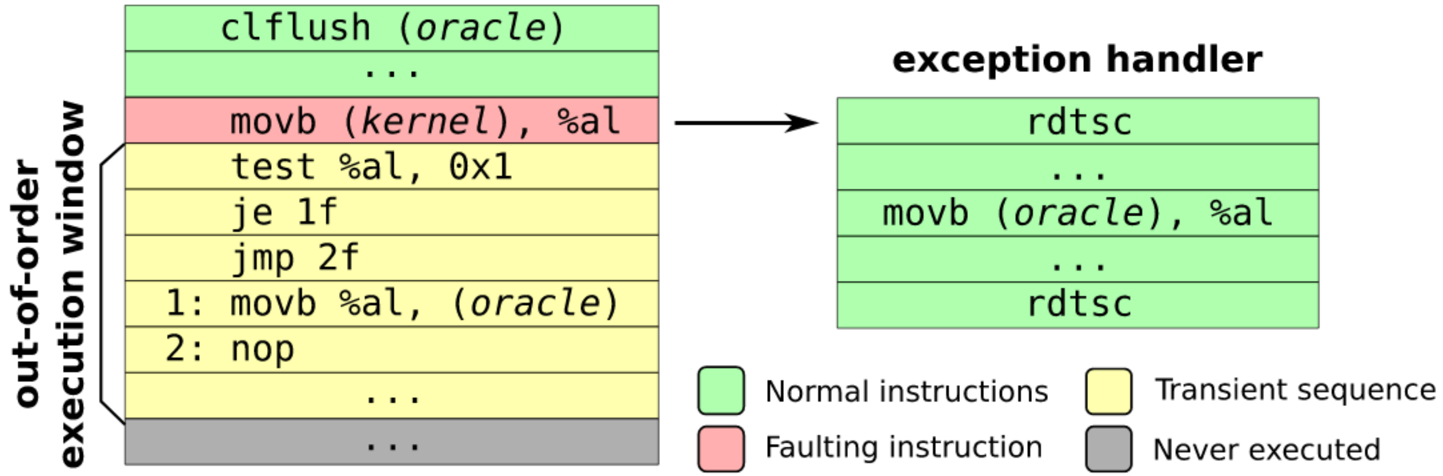


```
raise_exception();
// the line below is never reached
access(probe_array[data * 4096]);
```

Listing 1: A toy example to illustrate side-effects of out-of-order execution.



Exceptions and speculation



```
    clflush (oracle)
    ...
    movb (kernel), %al
    test %al, 0x1
    je 1f
    jmp 2f
1:  movb %al, (oracle)
2:  nop
    ...
    ...
```

exception handler

```
rdtsc
...
movb (oracle), %al
...
rdtsc
```

Cache access time

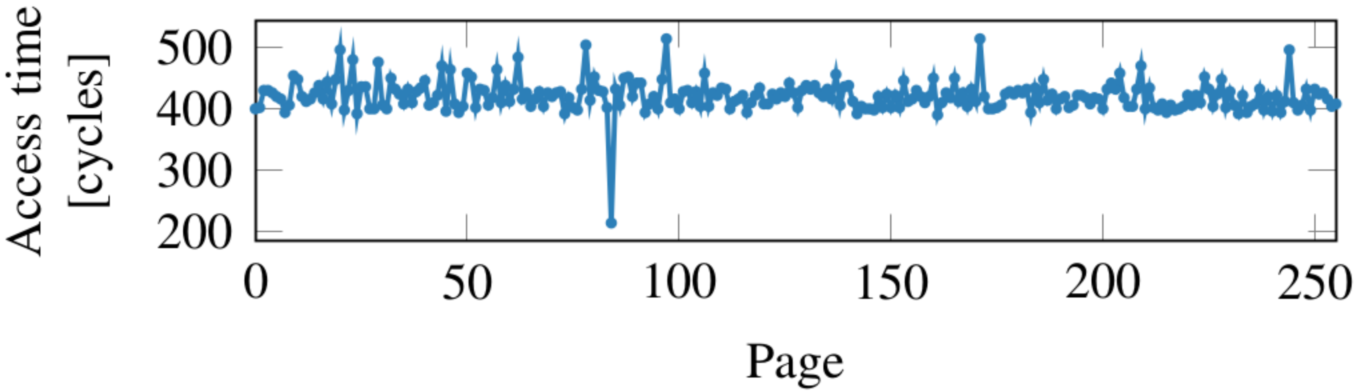


Figure 4: Even if a memory location is only accessed during out-of-order execution, it remains cached. Iterating over the 256 pages of `probe_array` shows one cache hit, exactly on the page that was accessed during the out-of-order execution.

Spectre

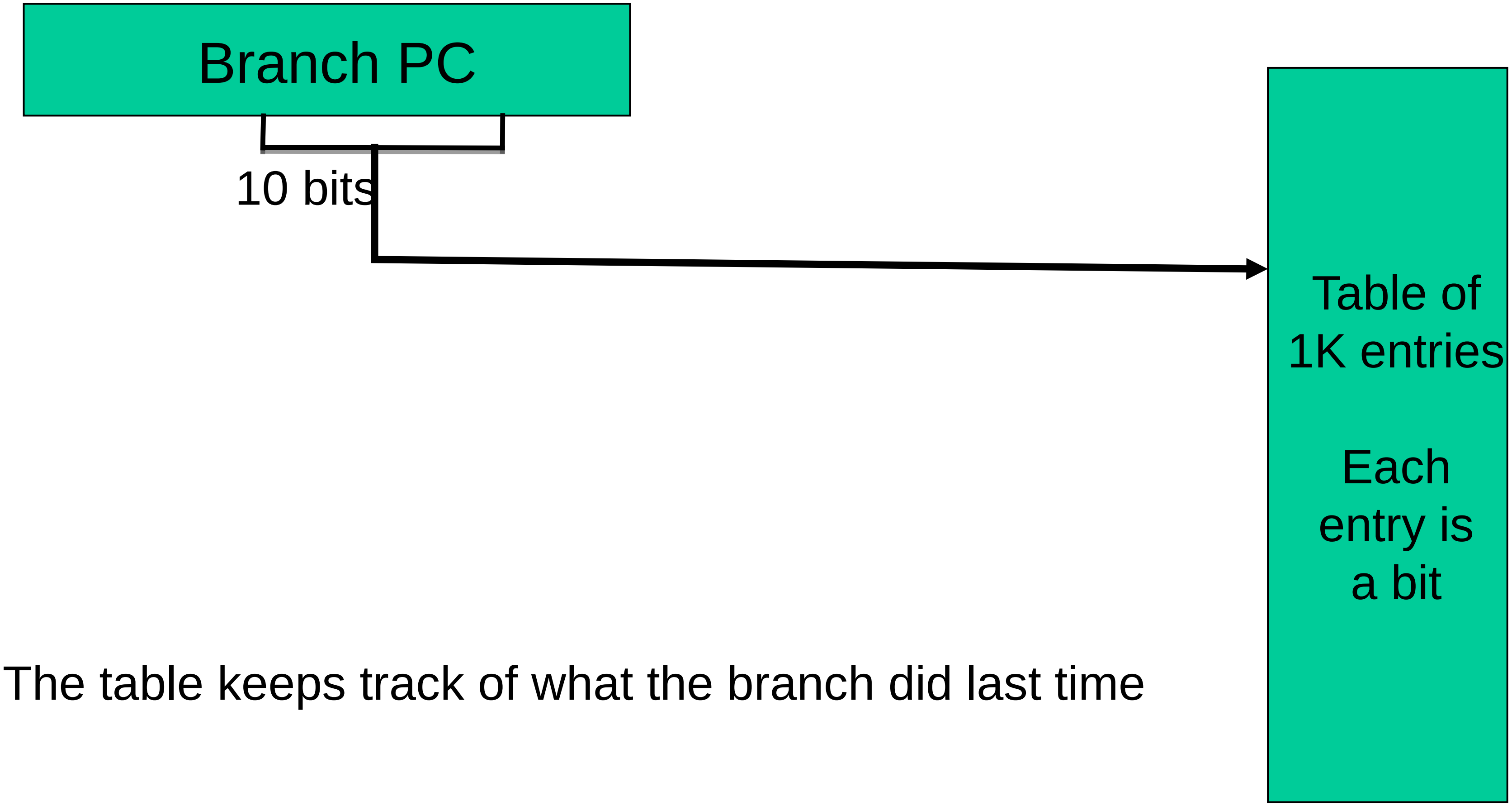
1-Bit Bimodal Prediction

- For each branch, keep track of what happened last time and use that outcome as the prediction

- What are prediction accuracies for branches 1 and 2 below:

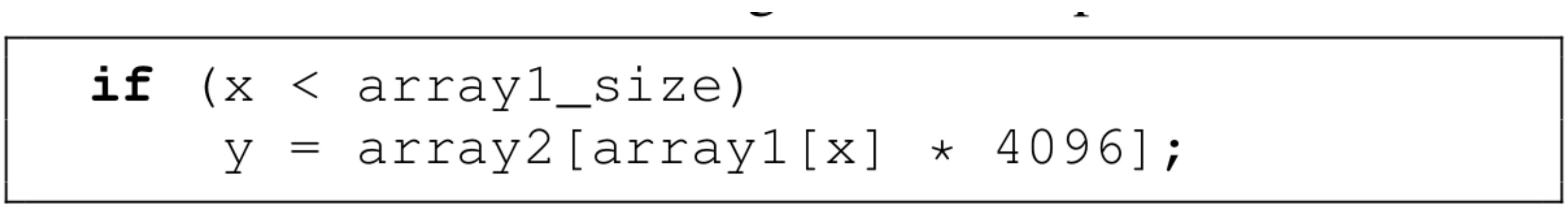
```
while (1) {
      for (i=0;i<10;i++) {                  branch-1
          …
      }
      for (j=0;j<20;j++) {                  branch-2
         …
      }
}
```

Bimodal 1-Bit Predictor



The table keeps track of what the branch did last time

Gadget



```
if (x < array1_size)
    y = array2[array1[x] * 4096];
```

Thank you!

Exceptions and speculation