250P: Computer Systems Architecture

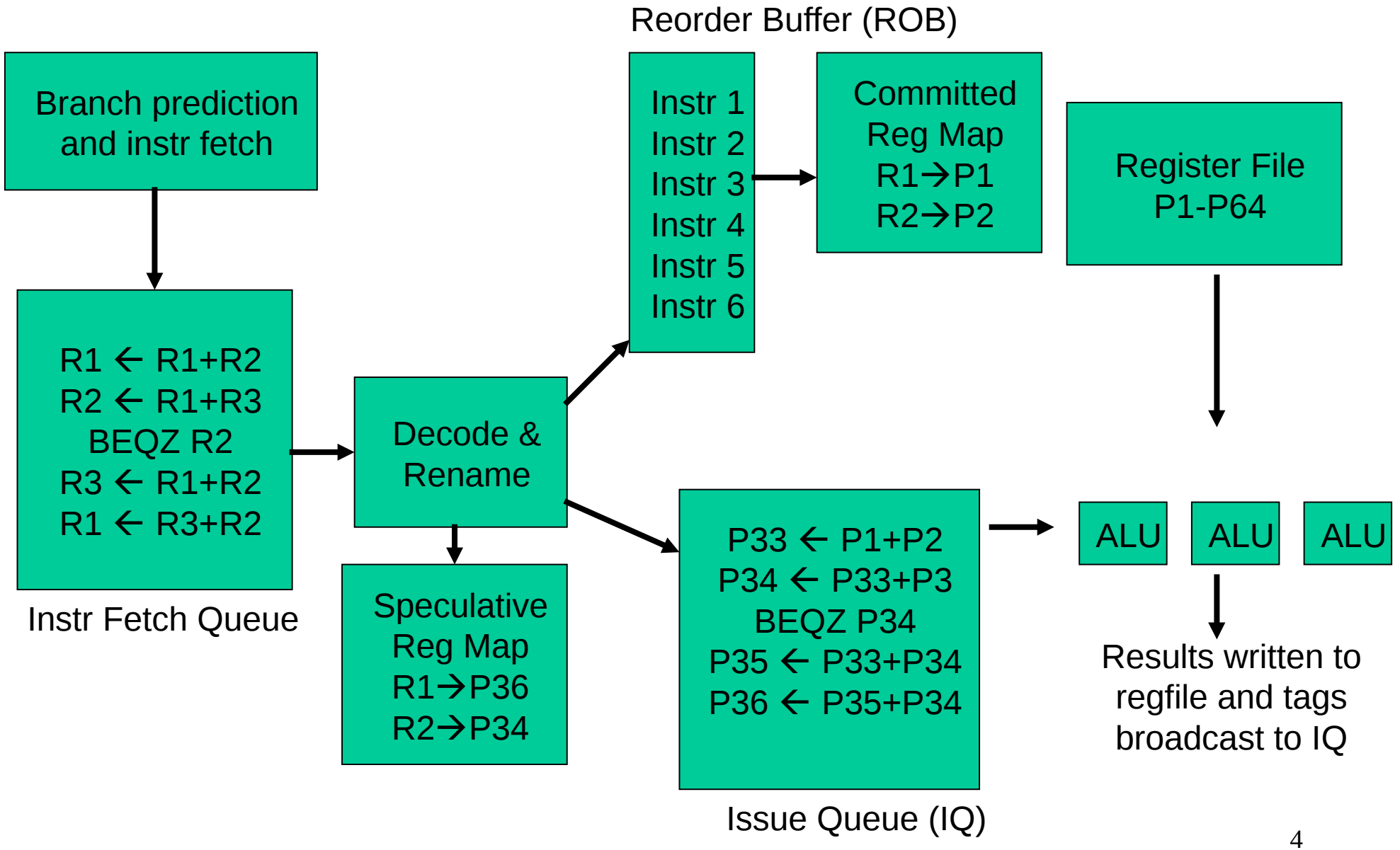
Lecture 15: Side channel attacks Meltdown and Spectre

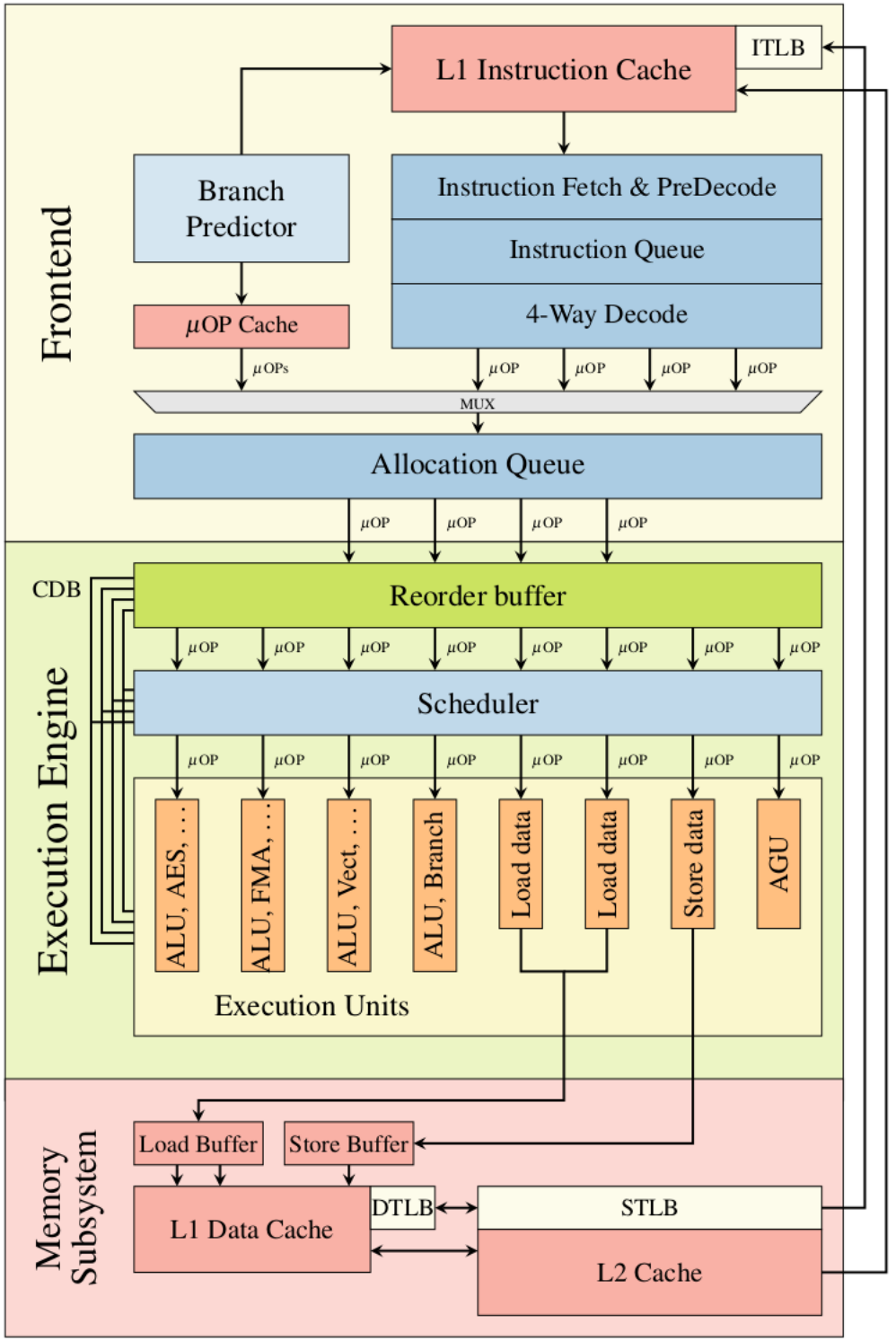
Anton Burtsev
March, 2019

Meltdown

Page tables and protection

The Alpha 21264 Out-of-Order Implementation



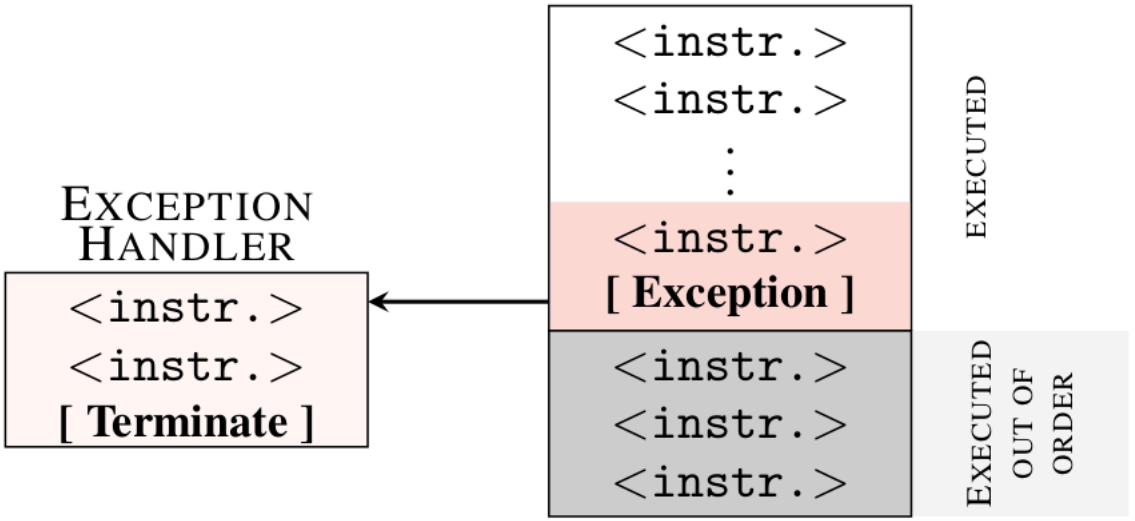


Skylake (simplified)

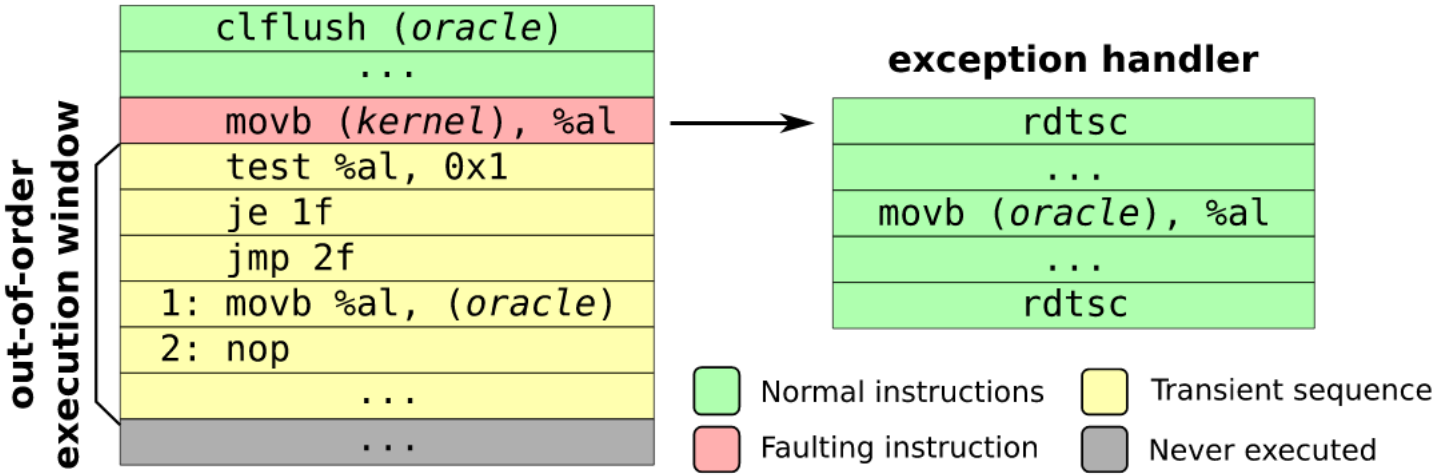
Exceptions and speculation

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

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



Exceptions and speculation



Cache access time

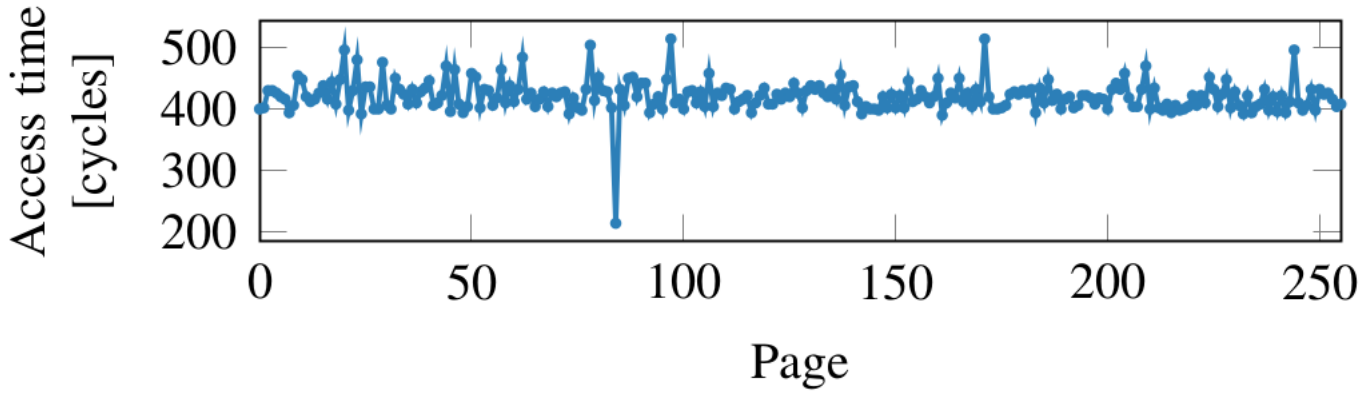


Figure 4: Even if a memory location is only accessed during out-of-order execution, it remains cached. Iterating over the 256 pages of `probe_array` shows one cache hit, exactly on the page that was accessed during the out-of-order execution.

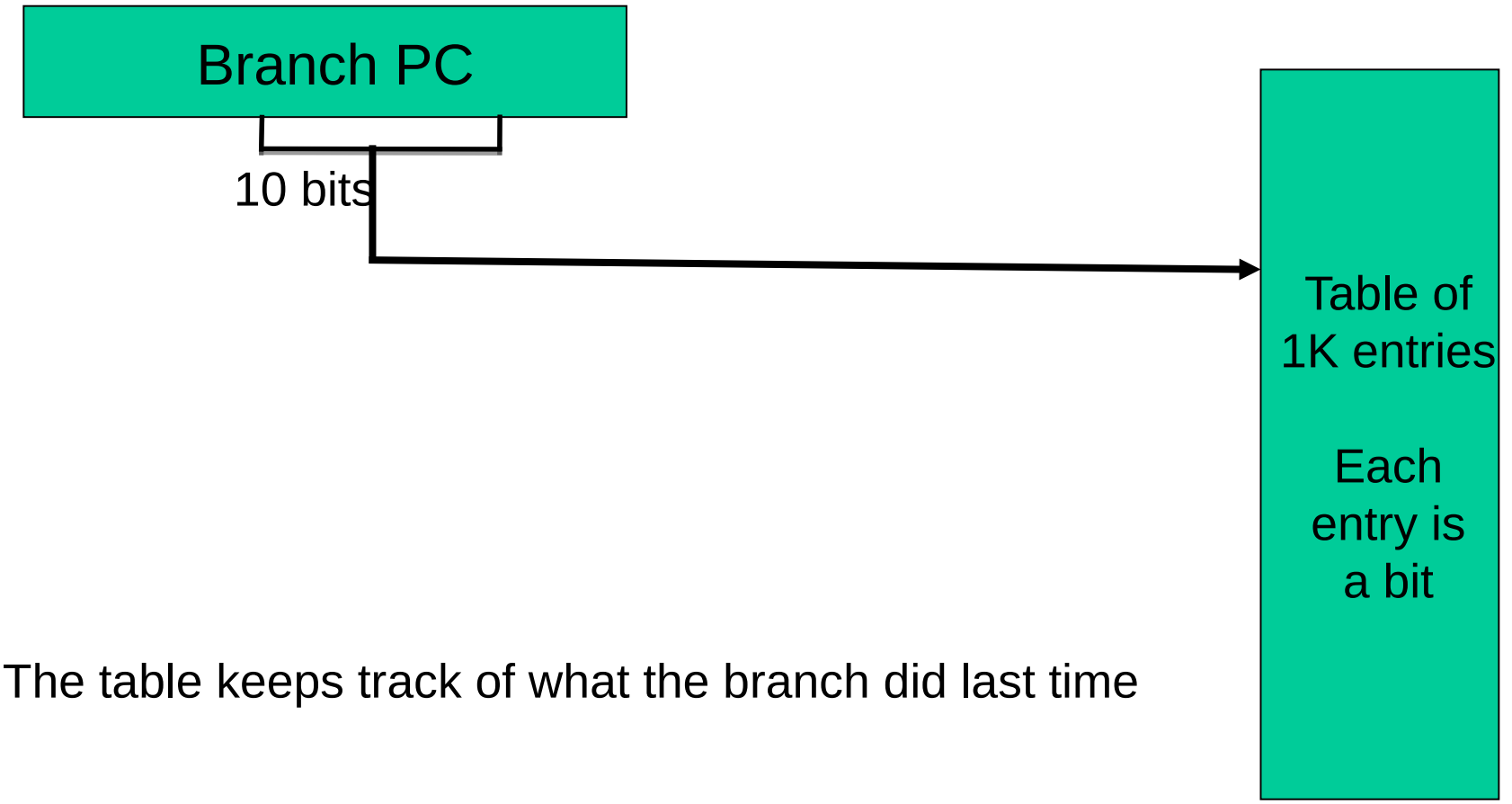
Spectre

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
           …
        }
}
```

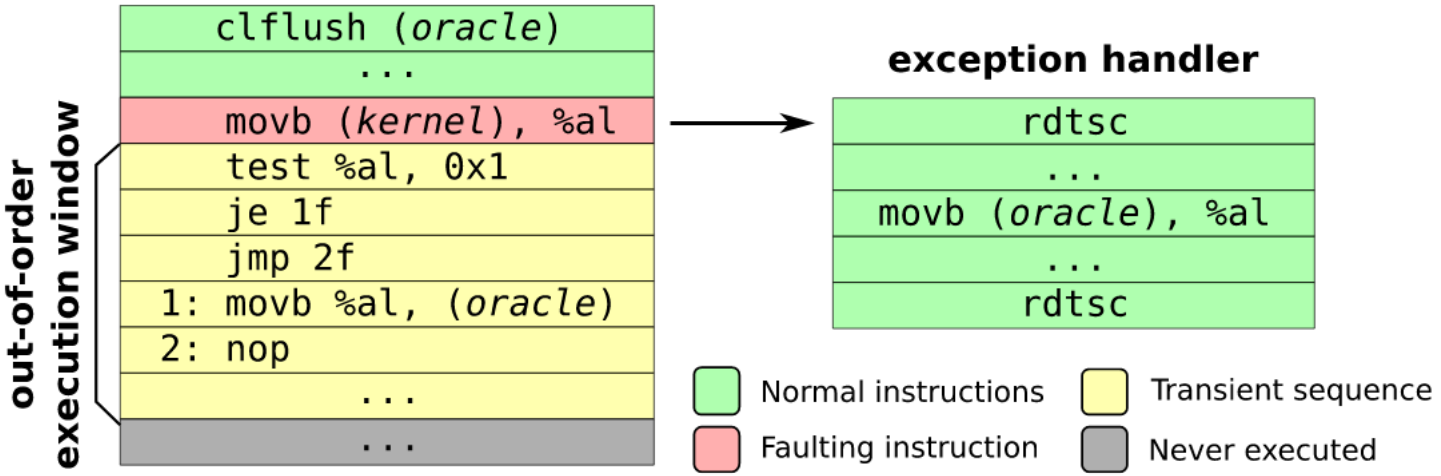
Bimodal 1-Bit Predictor



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