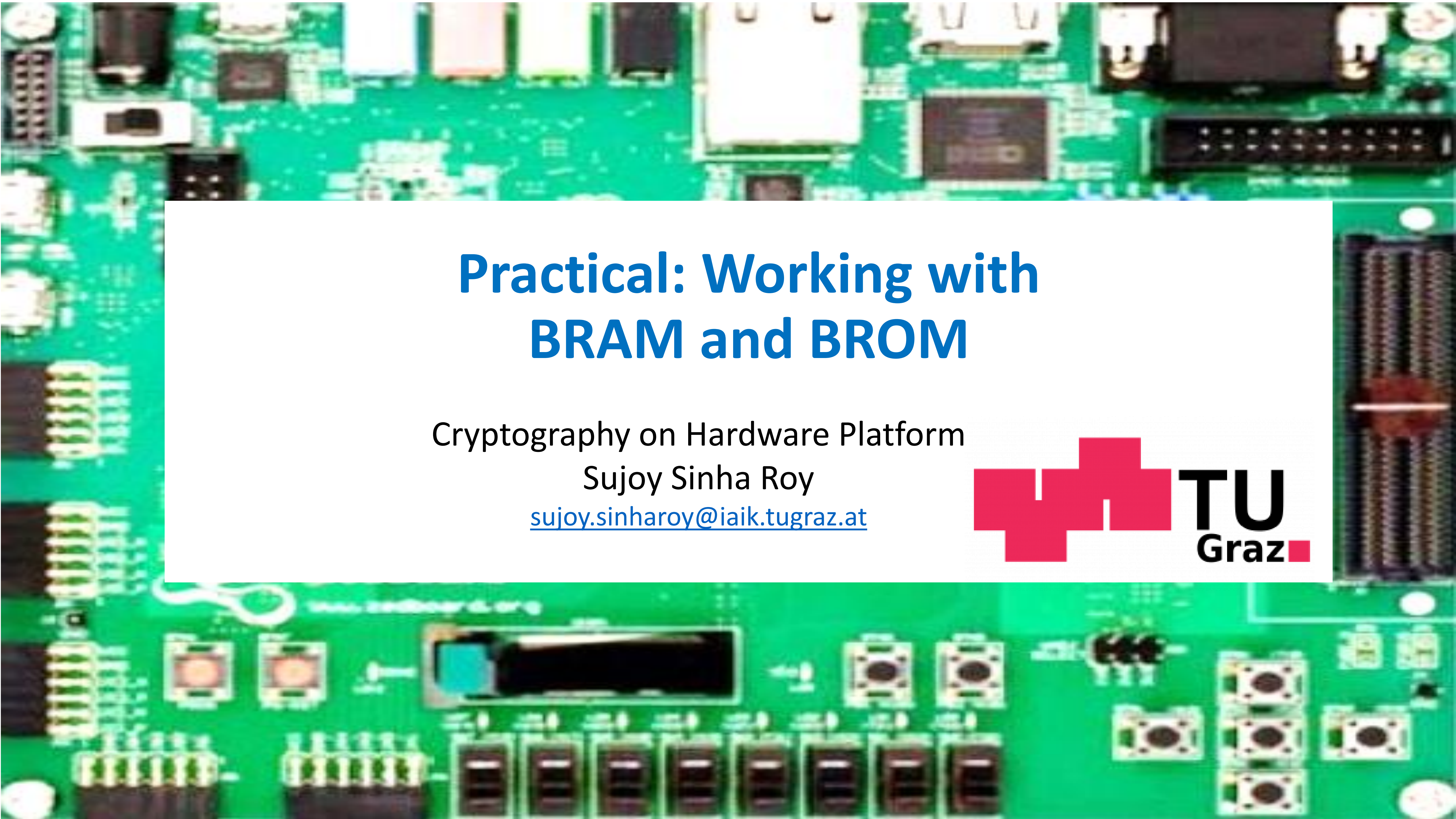


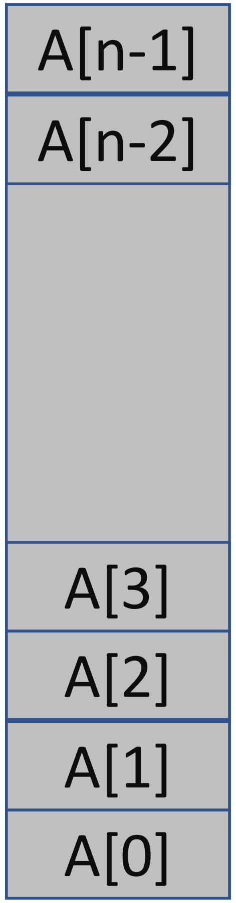
Practical: Working with BRAM and BROM

Cryptography on Hardware Platform

Sujoy Sinha Roy
sujoy.sinharoy@iaik.tugraz.at

Block Random Access Memory (BRAM)

BRAM is an addressable memory element (IP) with at most two ports.



A[n-1]

A[n-2]

A[3]

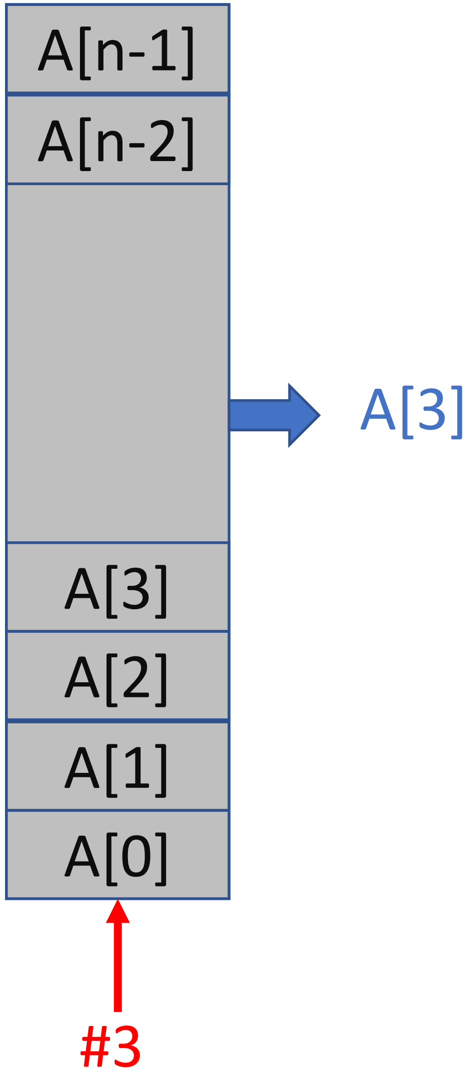
A[2]

A[1]

A[0]

Block Random Access Memory (BRAM)

BRAM is an addressable memory element (IP) with at most two ports.

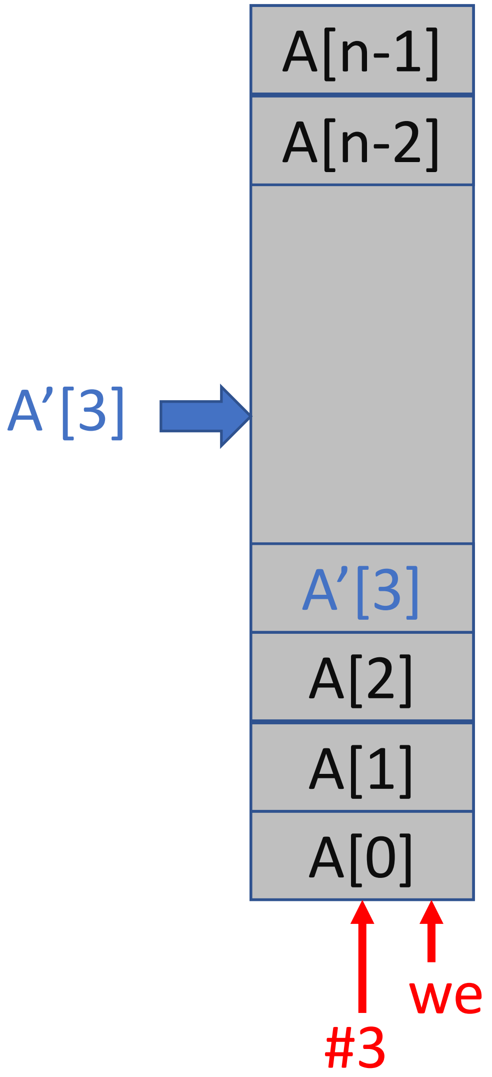


1. To read a cell, we provide the address of the cell to the address port of the BRAM IP.

2. The data from the cell is obtained at the read port

Block Random Access Memory (BRAM)

BRAM is an addressable memory element (IP) with at most two ports.



1. To write to a cell, we provide the address of the cell.

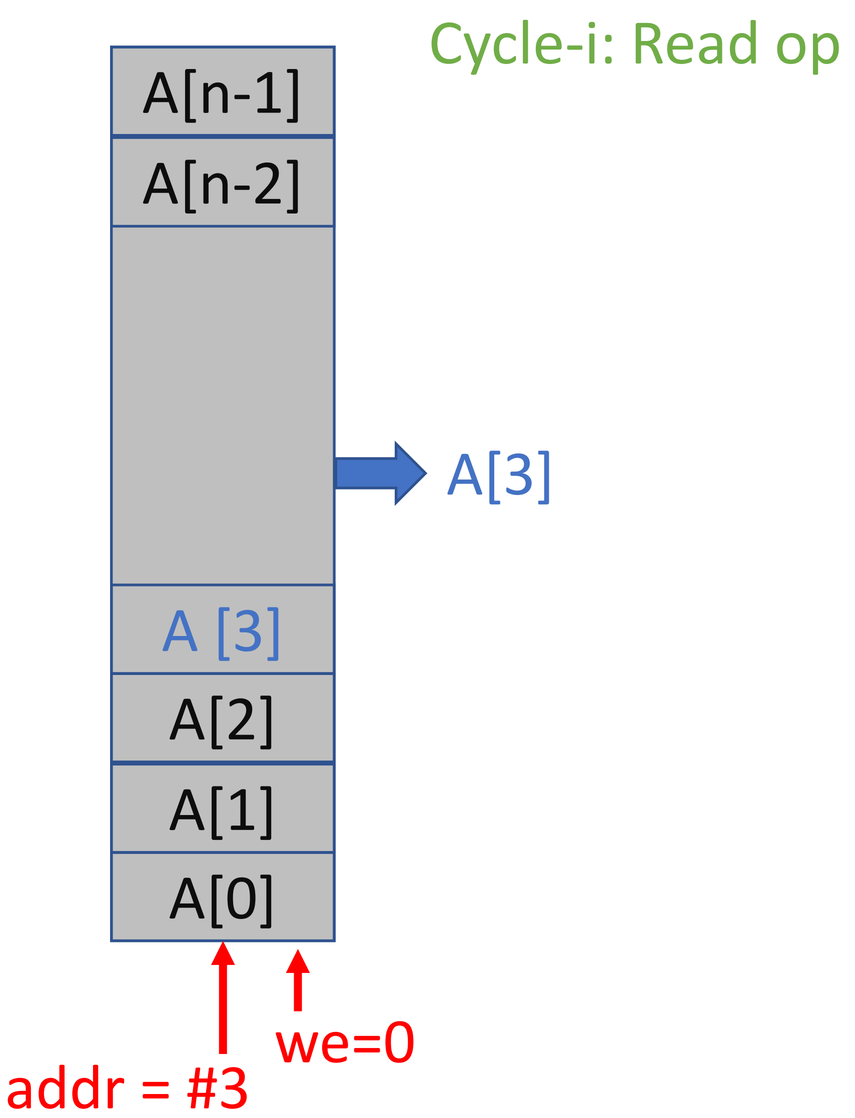
2. We also provide the write-enable signal.

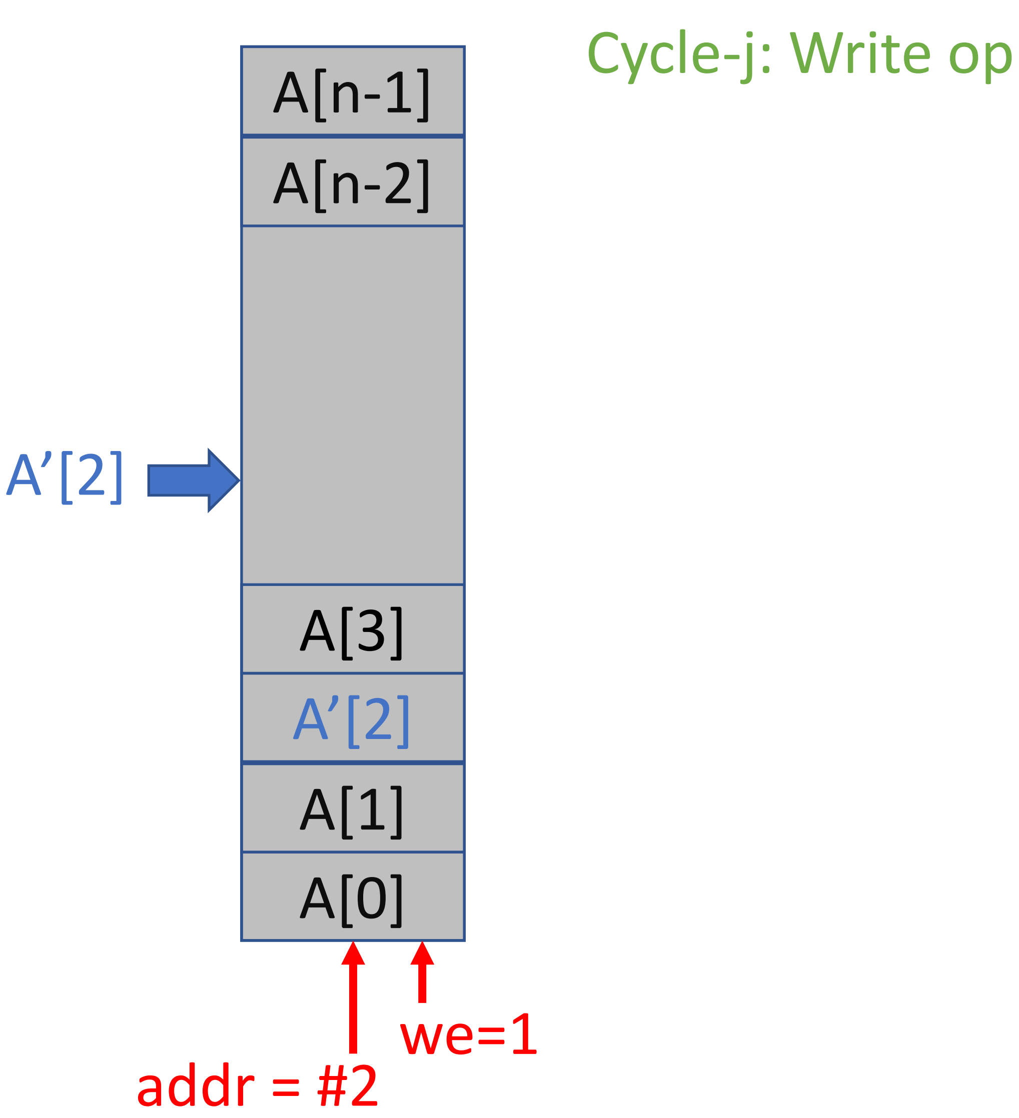
3. We provide the data value.

4. In the next cycle, the data value gets written into the memory cell.

BRAM configurations: Single Port

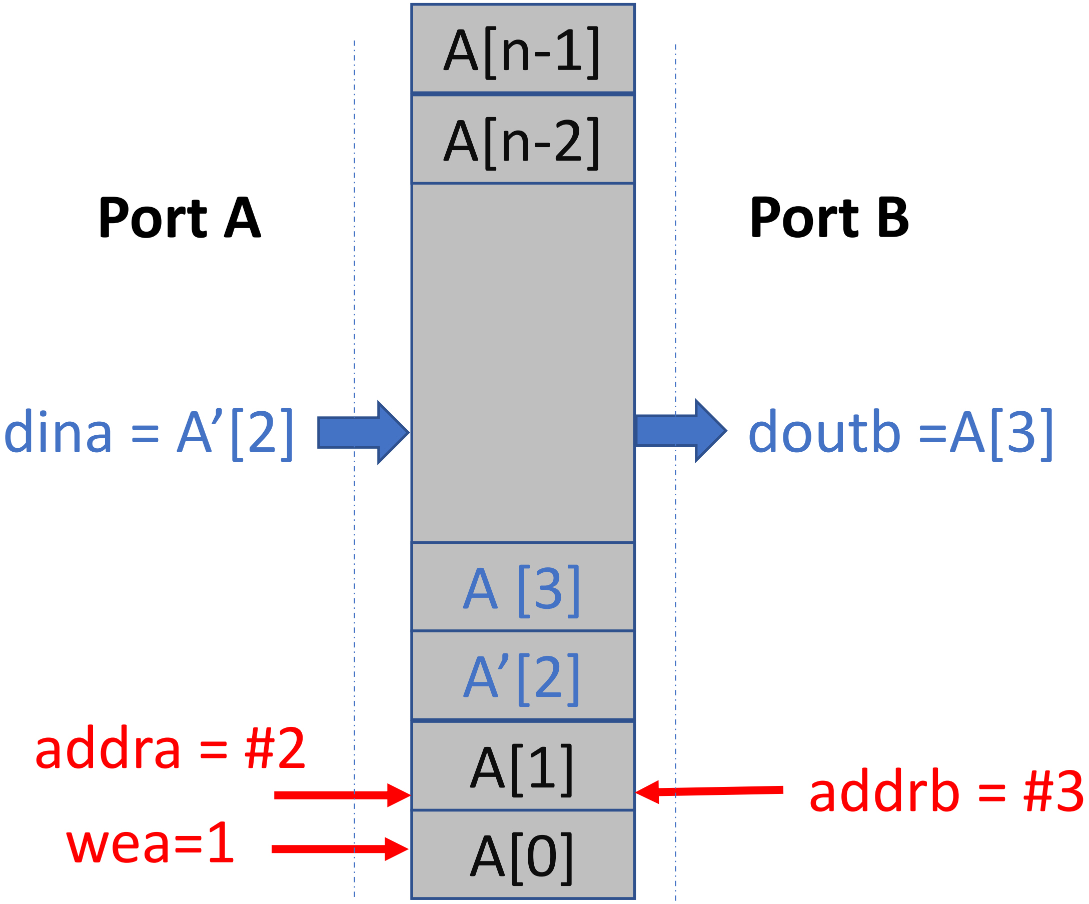
Single port BRAM has only one port. At any cycle, you can do either read or write.





BRAM configurations: Simple dual Port

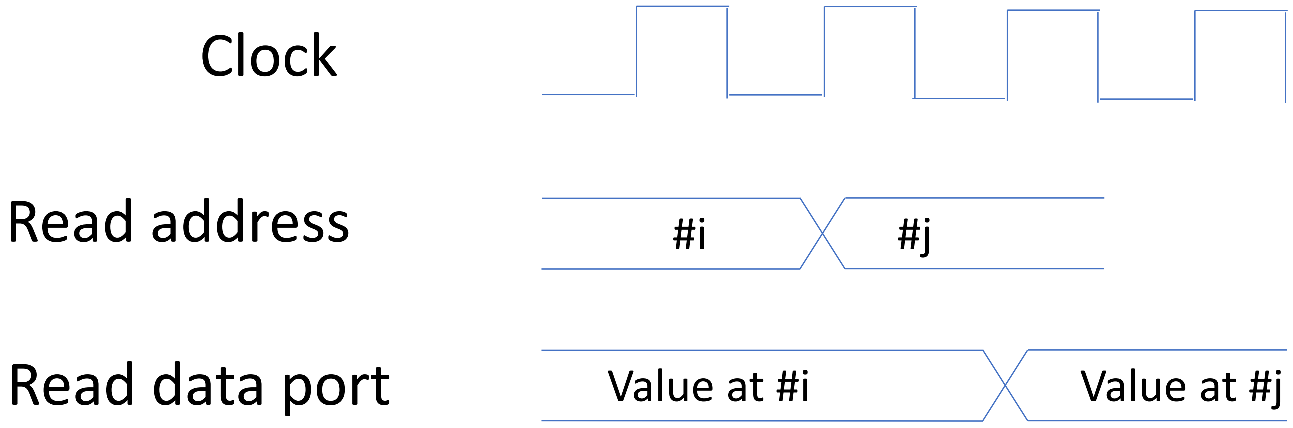
There are 2 ports. Port-A is used for only Write. Port-B used for only Read.



Cycle-i:
Read address 3 and
Write address 2 in parallel.

At most 1 read and 1 write per cycle.

BRAM READ has a latency of 1 cycle.



Clock

Read address

#i

#j

Read data port

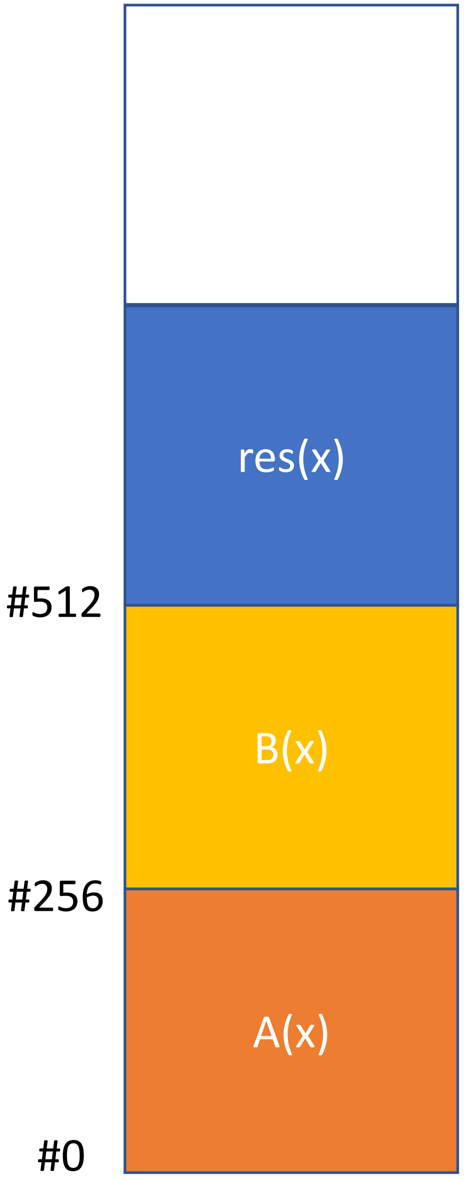
Value at #i

Value at #j

Working with Simple dual Port BRAM

Watch demo video.

Hands on: Coefficient-wise polynomial multiplication



Simple dual port BRAM64x1024

Question: Two polynomials A(x) and B(x) of 256 coefficients are stored in the BRAM.

Compute there coefficient-wise multiplication and store the result starting from address #512 in the BRAM.

```
For(i=0; i<256; i++)
        res[i] = A[i]*B[i] % q
```

If I have 24 hours and I have to design an architecture ….

My steps for digital design:

1. Spend 4 hours on understanding the algorithm very well.

2. Spend 4 hours thinking various design approaches, their merits/demerits, ease of implementation, ...

3. Spend 4 hours on drawing block architecture diagram

4. Spend remaining 12 hours on coding, testing, and debugging …

Diagram for Coefficient-wise polynomial multiplication

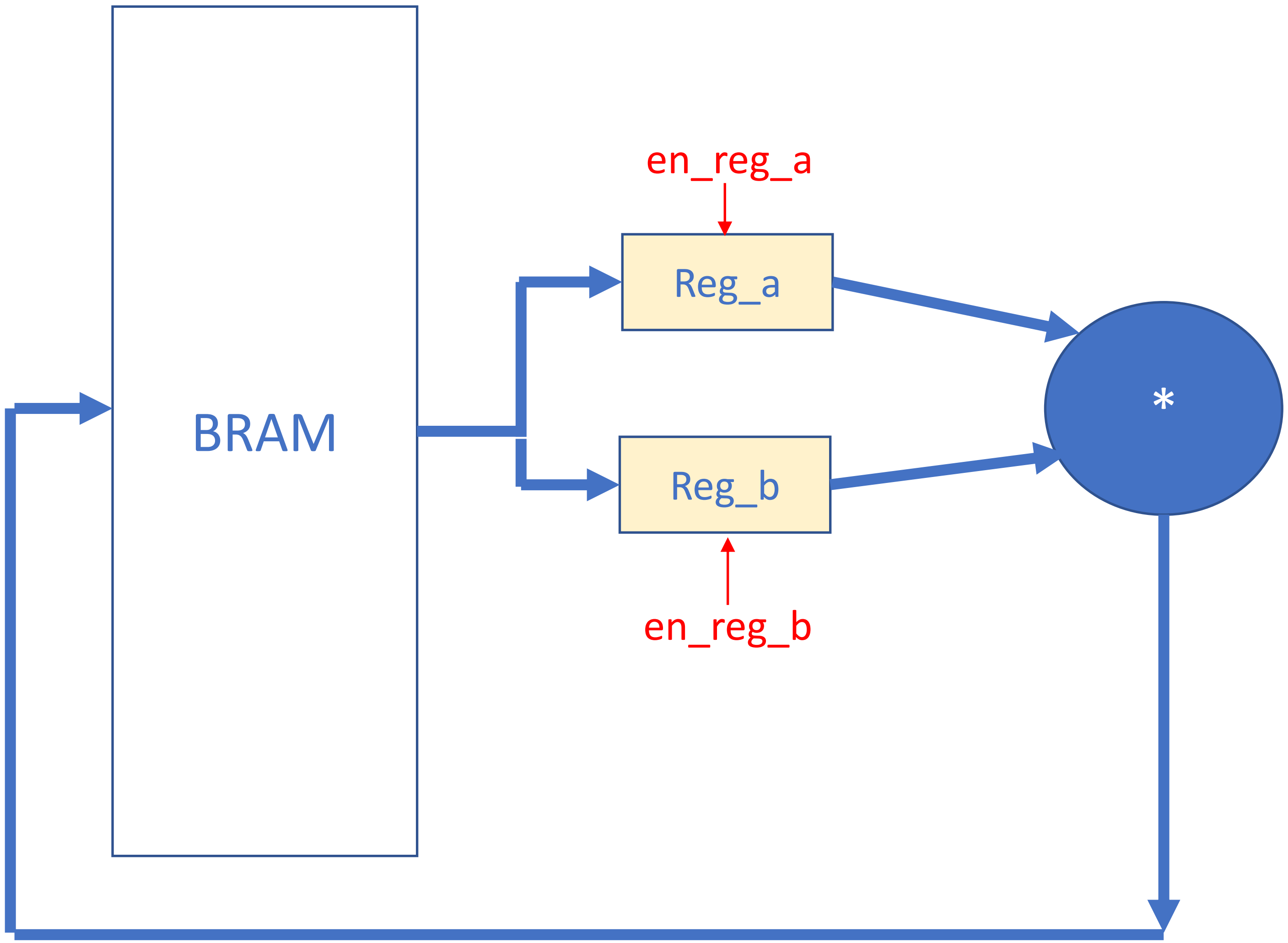
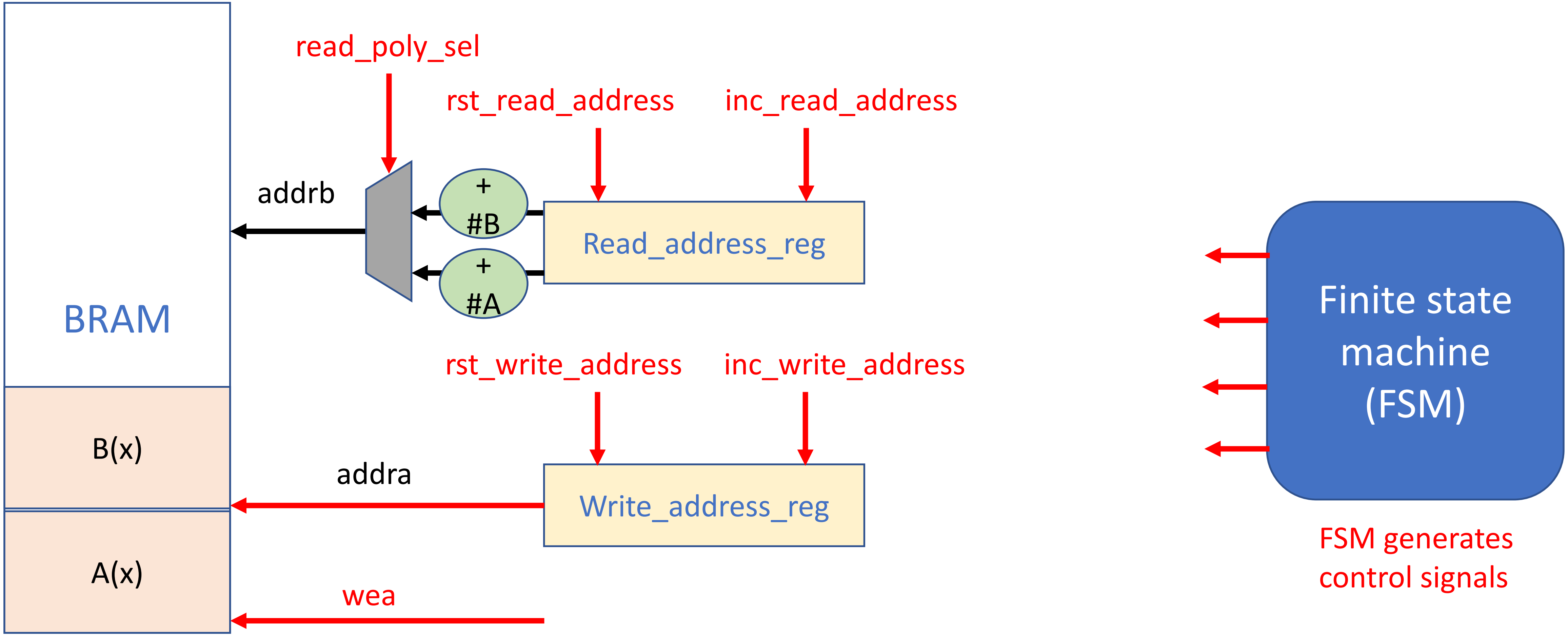


Diagram for Coefficient-wise polynomial multiplication

Generating control signals for the BRAM



FSM generates control signals