

→ Key enabler: Requests for same address are merged in MSHR

→ Stage 1: Flush → Spy flushes blocks

→ Stage 2: Wait → generally the phase is long. But here it is not.

Bit 1: ⇒ Trojan will request some block A.

→ The request reaches MSHR

→ Spy will request same block A

→ Padding
between $T_{hit} + \phi$ & $T_{hit} + (T_{mm} - (T_c + T_q))$

→ Both request would merge in MSHR

↓
Avg hit

↓
Main mem fetch

↓
wire comm

↓
Request Queue wait

Bit 0: ⇒ Trojan does nothing

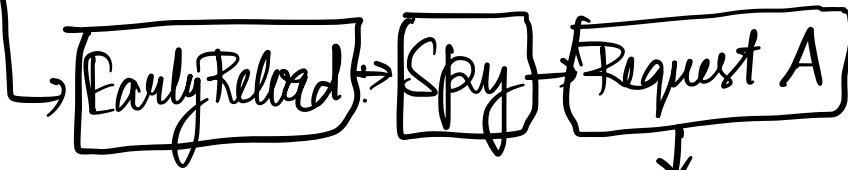
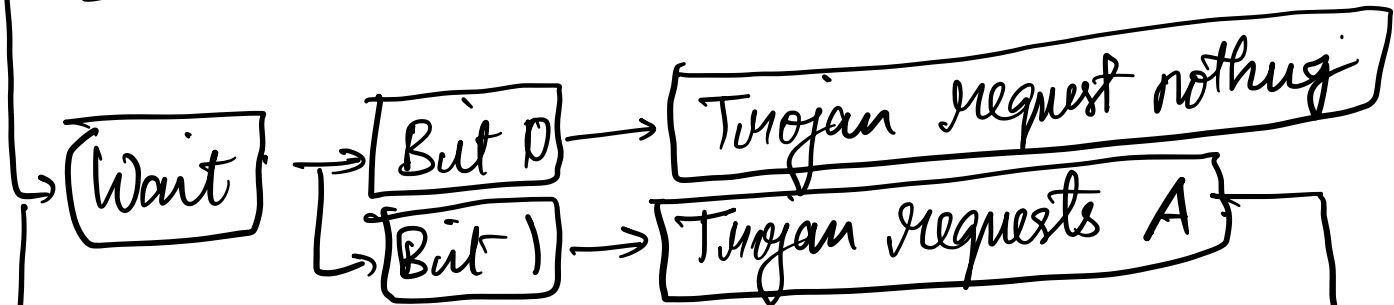
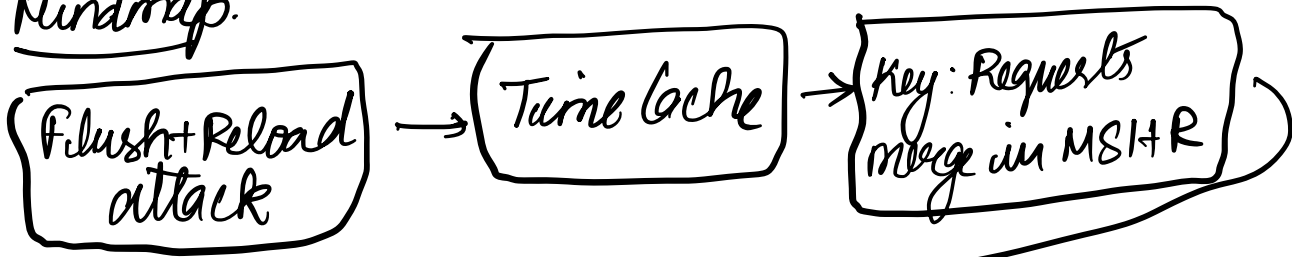
Spy request for block A between

$T_{hit} + \phi$ & $T_{hit} + (T_{mm} - (T_c + T_q))$

If spy gets the block faster ⇒ Bit - 1

slower \Rightarrow Bit - 0

Mindmap:



Between
 $T_{hit} + \phi$ & $T_{hit} + T_{mm} - (T_c + T_q)$

