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

T_{hit} → Avg hit
T_{mm} → Main mem fetch
T_c → core commun
T_q → Request Queue wait

→ Both request would merge in MSHR

Bit 0 :⇒ Trojan does nothing
Spy request for block A between
$T_{hit} + \phi \leq T_{hit} + (T_{mm} - (T_c + T_q))$

If spy gets the block faster ⇒ Bit - 1

Slower ⇒ Bit - 0

Nundroap: