Calibration Done Right: Noiseless Flush+Flush Attacks

Guillaume DIDIER

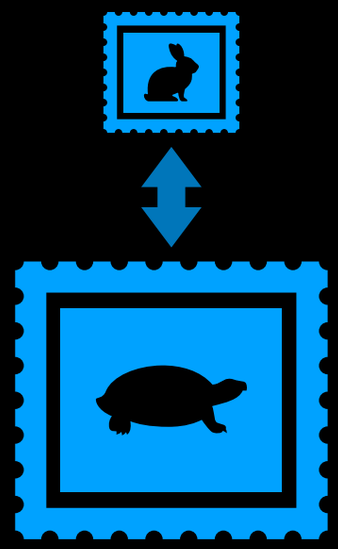
To appear in DIMVA 21', work by myself and Clémentine MAURICE

What is Flush+Flush ?

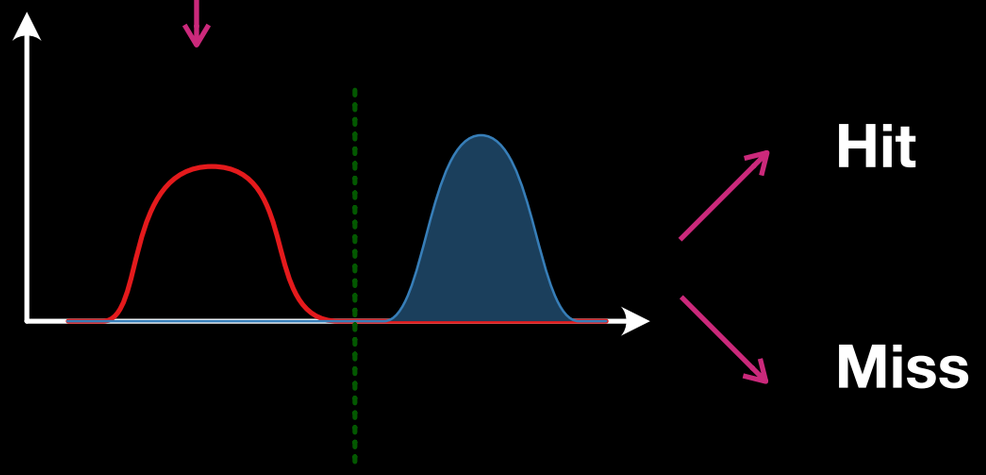
/

Access memory
Change cache content

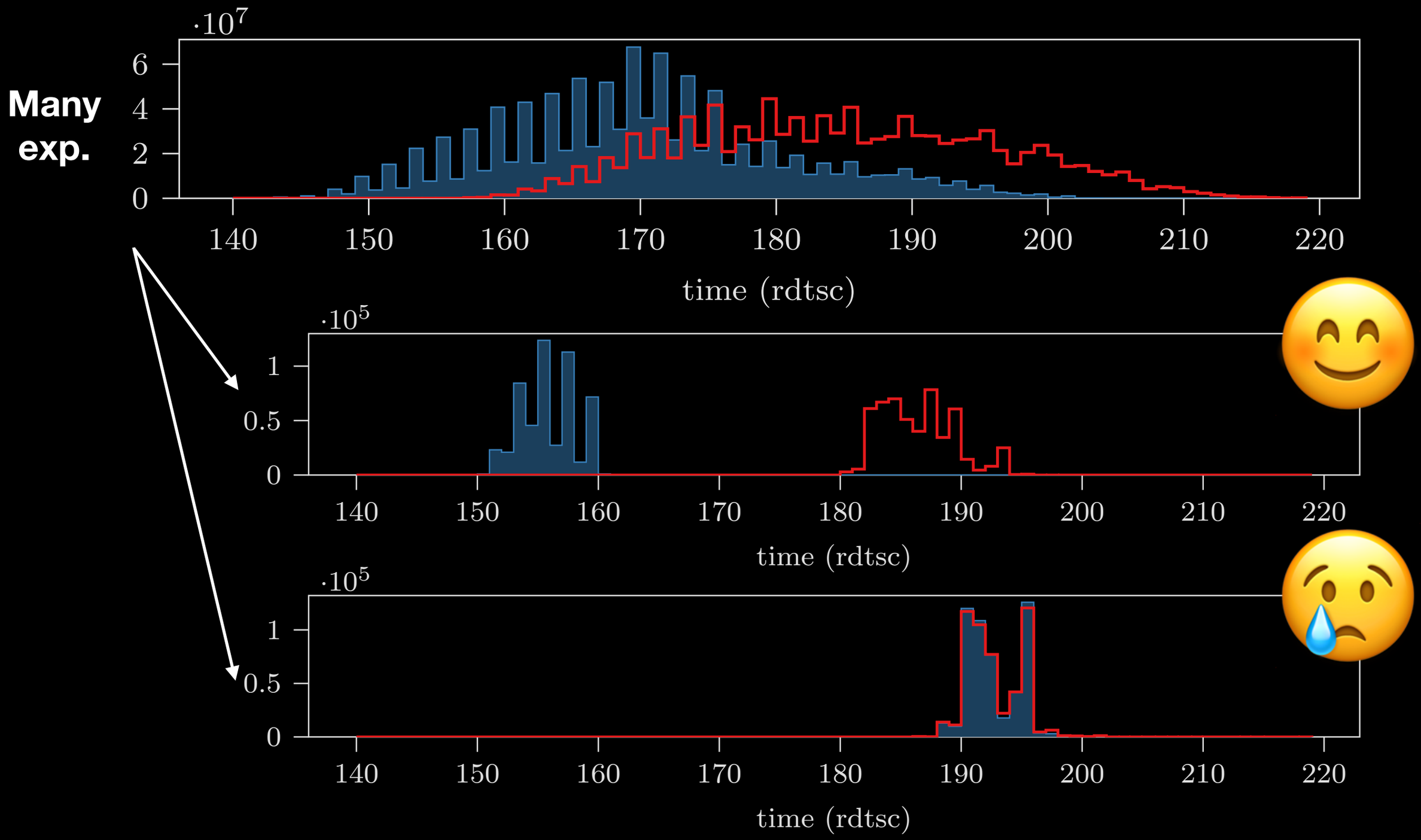
Timed `clflush`



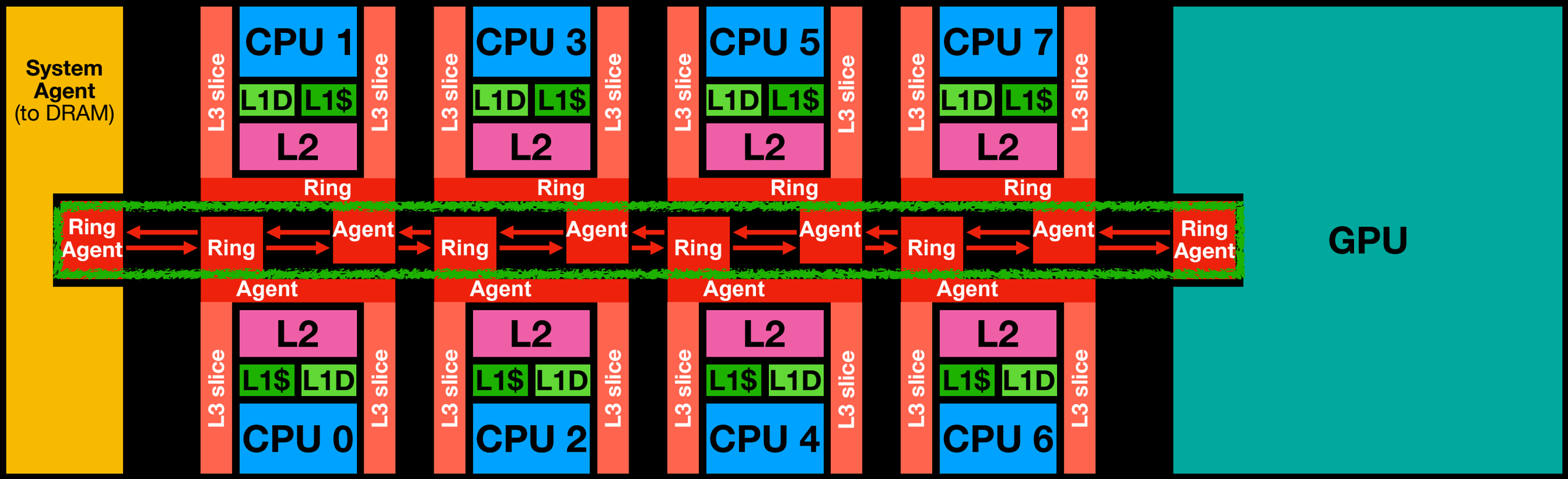
Read-only
shared memory



The problem

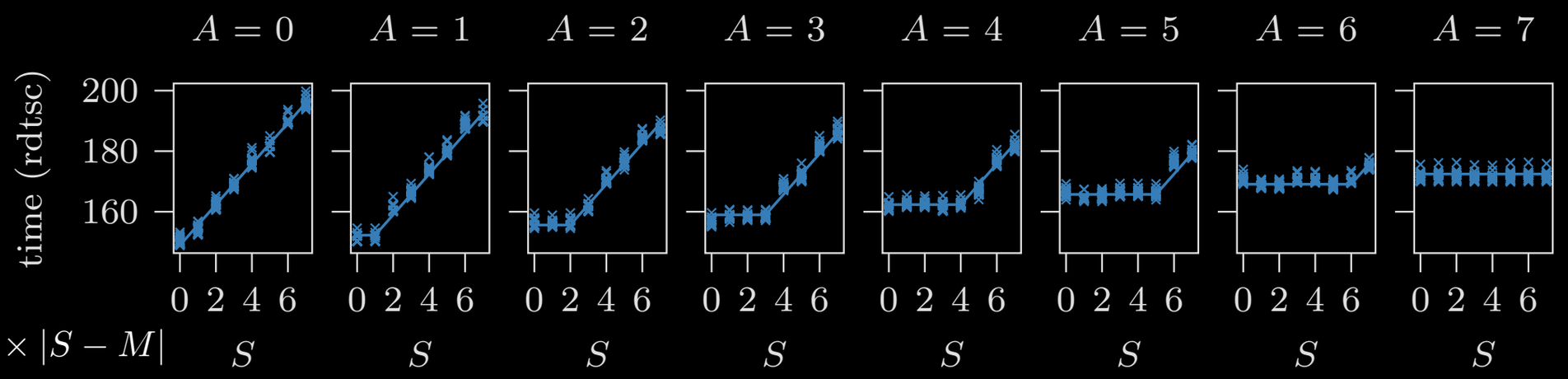

Many exp.
$\cdot 10^7$
6
4
2
0
140
150
160
170
180
190
200
210
220
time (rdtsc)
$\cdot 10^5$
1
0.5
0
140
150
160
170
180
190
200
210
220
time (rdtsc)
$\cdot 10^5$
1
0.5
0
140
150
160
170
180
190
200
210
220
time (rdtsc)

Interconnect topology



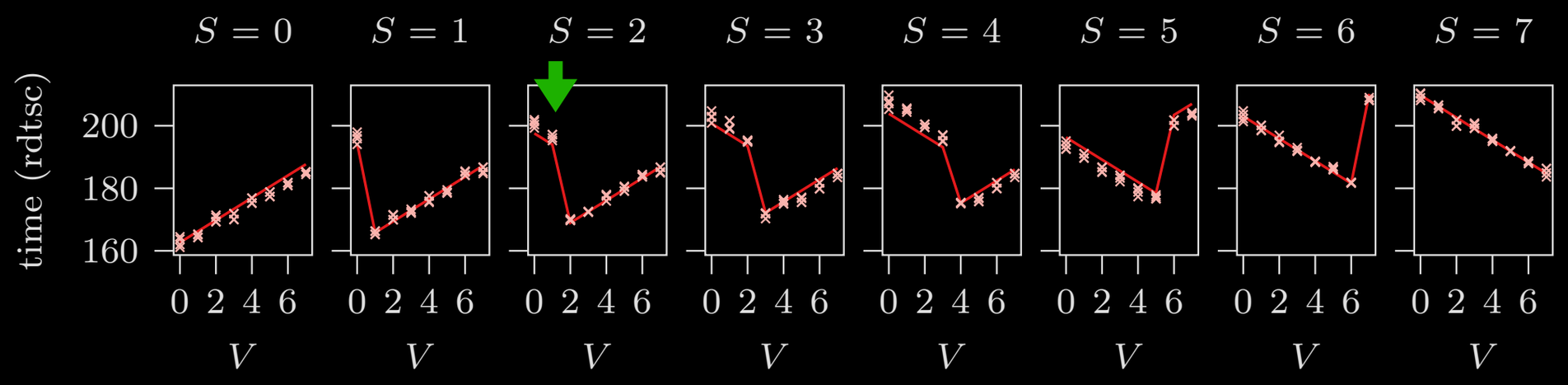
clflush timing

I state



$$t_I(A,S) = C + h \times |A - S| + h \times |S - M|$$

E state

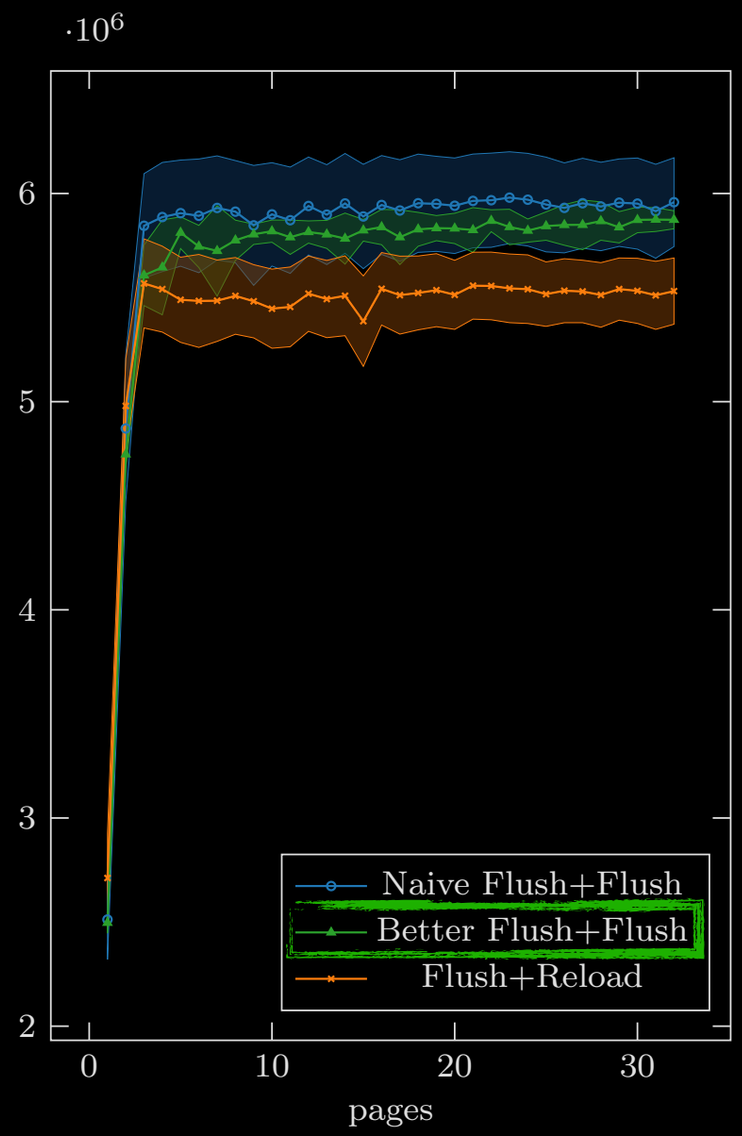


$$t_E(A,V,S) = \begin{cases} C' + h \times |A - S| + h \times |R - (V - M)| & \text{if } S \leqslant \frac{N}{2} \text{ and } V < S \\ C' + h \times |A - S| + h \times |S - V| & \text{if } S \leqslant \frac{N}{2} \text{ and } V \geqslant S \\ C' + h \times |A - S| + h \times |S - V| & \text{if } S > \frac{N}{2} \text{ and } V \leqslant S \\ C' + h \times |A - S| + h \times |M - V| & \text{if } S > \frac{N}{2} \text{ and } V > S, \end{cases}$$

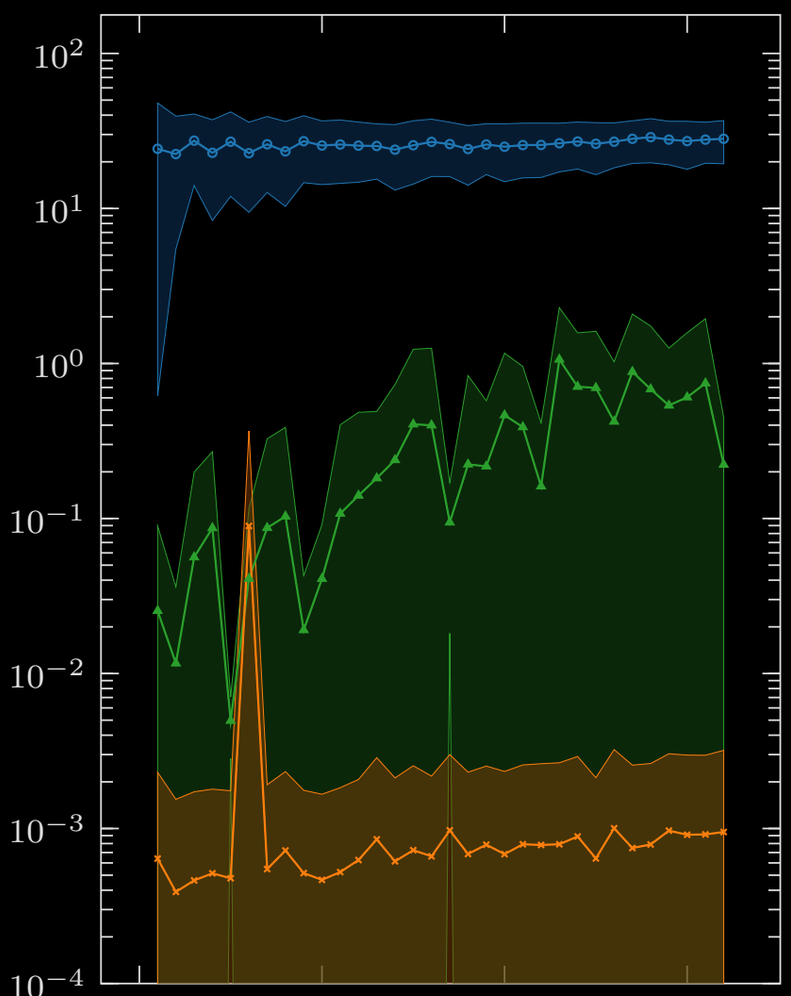
A = 0
other A give similar graphs

Improved F+F Covert Channel Result

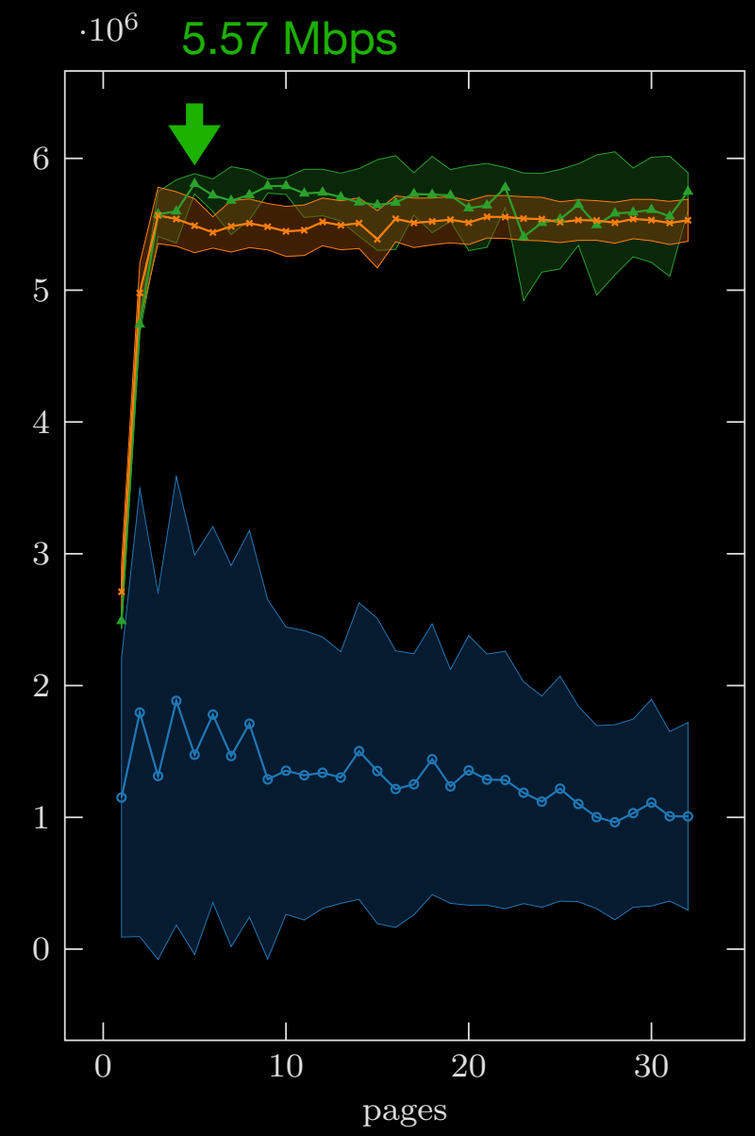
Raw bit rate (Mbps)



Error rate rate (%)



True capacity (Mbps)



Key take-aways

- Results
  - 3x improvement over Naive Flush+Flush
  - Better Flush+Flush beats Flush+Reload by 3-4 %
  - 8-core true capacity : 5.57 Mbit/s
  - Also improve AES T-table attack using Flush+Flush
- Think about **Cache Coherence**
- Think about **Slices** and **Topology**

Thank you

Questions ?