How Sharp is SHARP?

WOOT'19@USENIX-SECURITY

Dixit Kumar *(Indian Institute of Technology Kanpur),*
Chavhan Sujeet Yashavant *(Indian Institute of Technology Kanpur),*
Biswabandan Panda *(Indian Institute of Technology Kanpur), and*
Vishal Gupta *(Manipal University Jaipur and Indian Institute of Technology Kanpur)*

SHARP [Yan et al., ISCA ‘17]

SHARP [Yan et al., ISCA ‘17]

Secure hierarchy-aware cache replacement policy

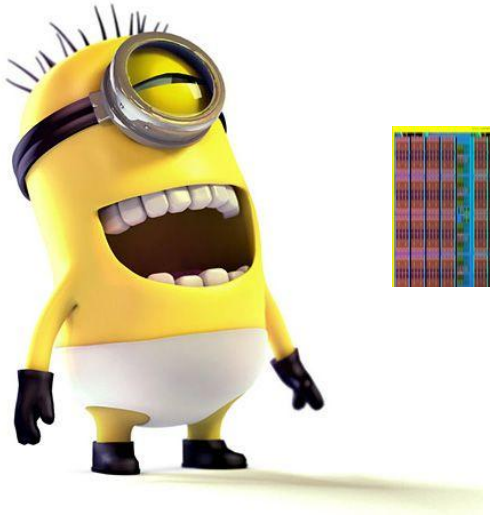
SHARP [Yan et al., ISCA ‘17]

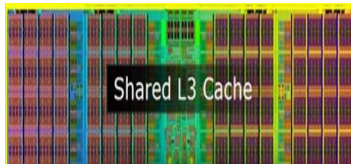
Secure hierarchy-aware cache replacement policy

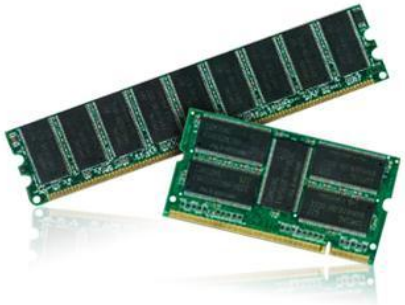
Mitigation for side-channel attacks

Side Channel Attacks

Attacker

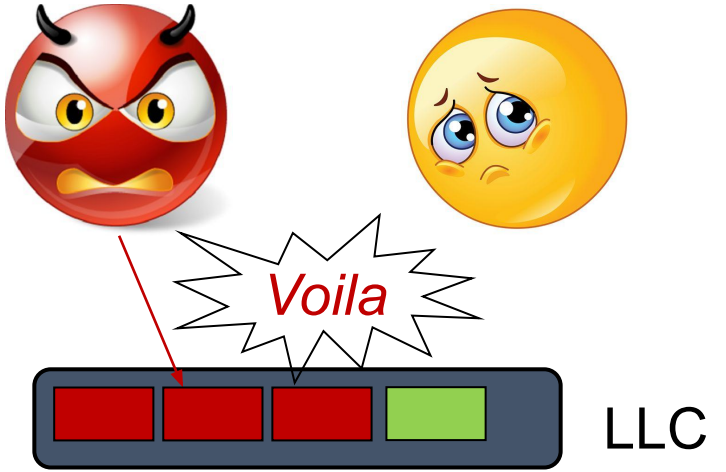




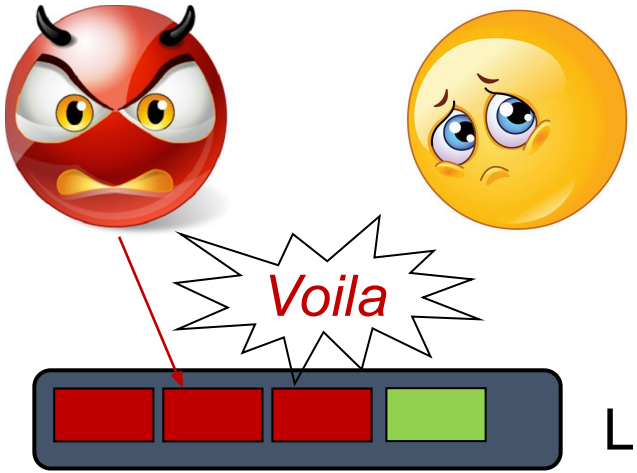


Victim

Eviction based Cache Attacks: (Prime+Probe)

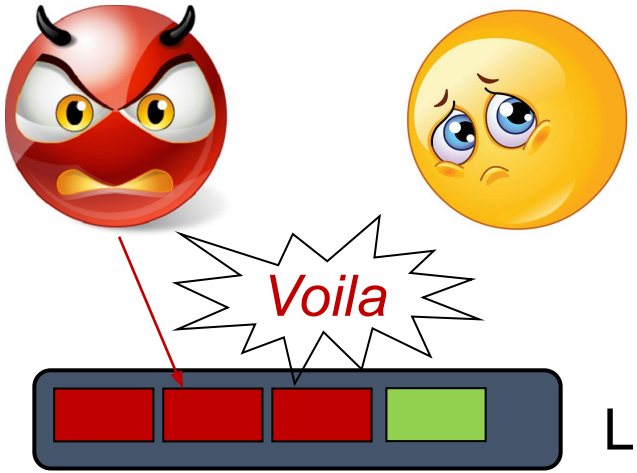


Eviction based Cache Attacks: (Prime+Probe)



Step 0: Attacker *fills* the entire shared cache (set)

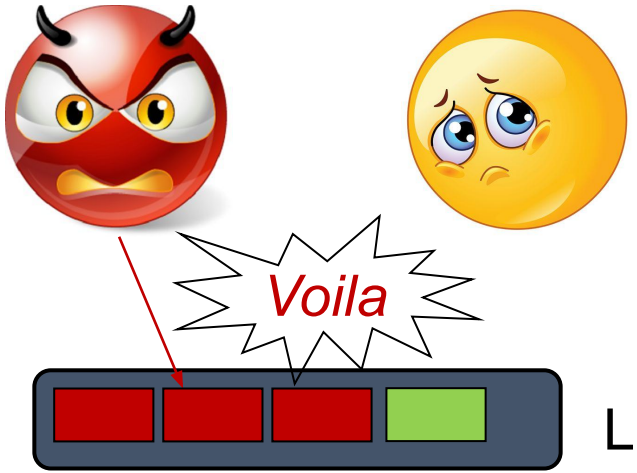
Eviction based Cache Attacks: (Prime+Probe)



Step 0: Attacker *fills* the entire shared cache (set)

Step 1: Victim *evicts* cache blocks while running

Eviction based Cache Attacks: (Prime+Probe)

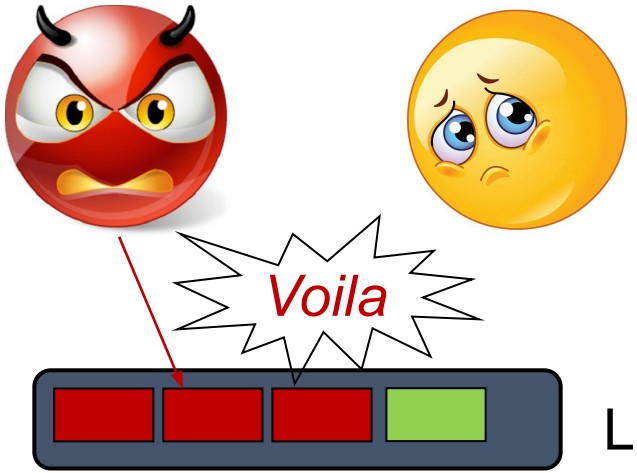


Step 0: Attacker *fills* the entire shared cache (set)

Step 1: Victim *evicts* cache blocks while running

Step 2: Attacker *probes* the cache set

Eviction based Cache Attacks: (Prime+Probe)



Step 0: Attacker *fills* the entire shared cache (set)

Step 1: Victim *evicts* cache blocks while running

Step 2: Attacker *probes* the cache set

If *misses* then victim has accessed the set

Various Mitigations

Various Mitigations

Cache Layout [HPCA ‘16]

Various Mitigations

Cache Layout [HPCA ‘16]

Fuzzing the timer [ISCA ‘12]

Various Mitigations

Cache Layout [HPCA ‘16]

Fuzzing the timer [ISCA ‘12]

Cache Addressing [MICRO ‘18]

Various Mitigations

Cache Layout [HPCA ‘16]

Fuzzing the timer [ISCA ‘12]

Cache Addressing [MICRO ‘18]

Cache replacement policy [ISCA ‘17]

SHARP [Yan et al., ISCA ‘17]

Secure hierarchy-aware cache replacement policy

Mitigation for side-channel attacks

SHARP [Yan et al., ISCA ‘17]

Secure hierarchy-aware cache replacement policy

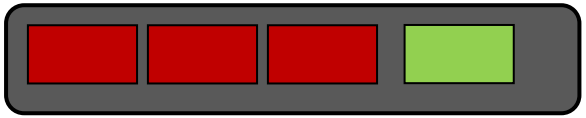
Mitigation for side-channel attacks

Prevents cross-core back invalidation

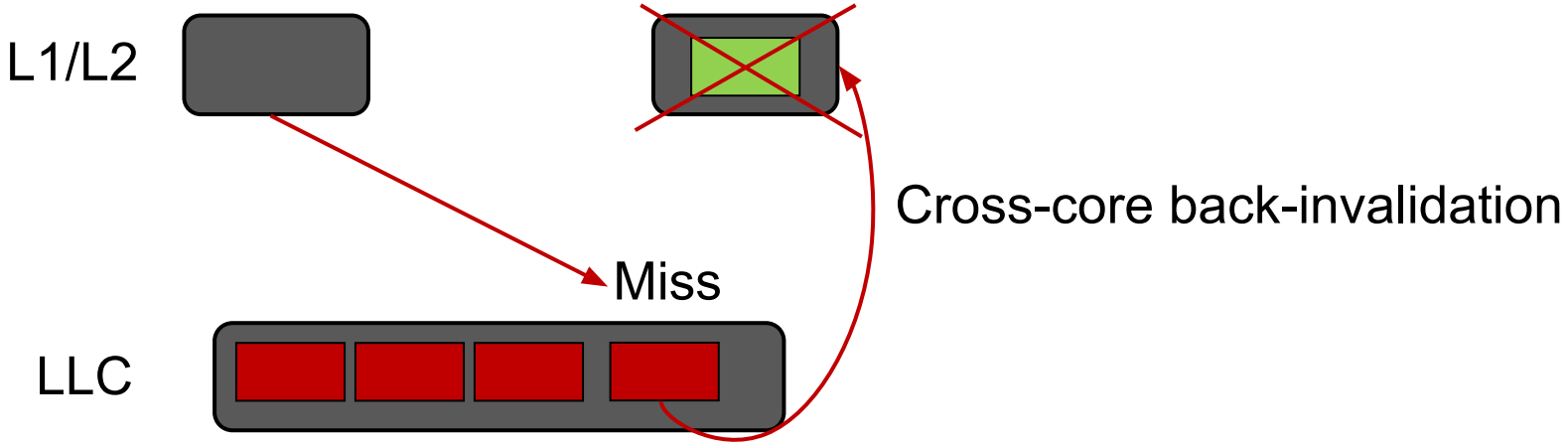
Cross-core Back-Invalidation - I

L1/L2

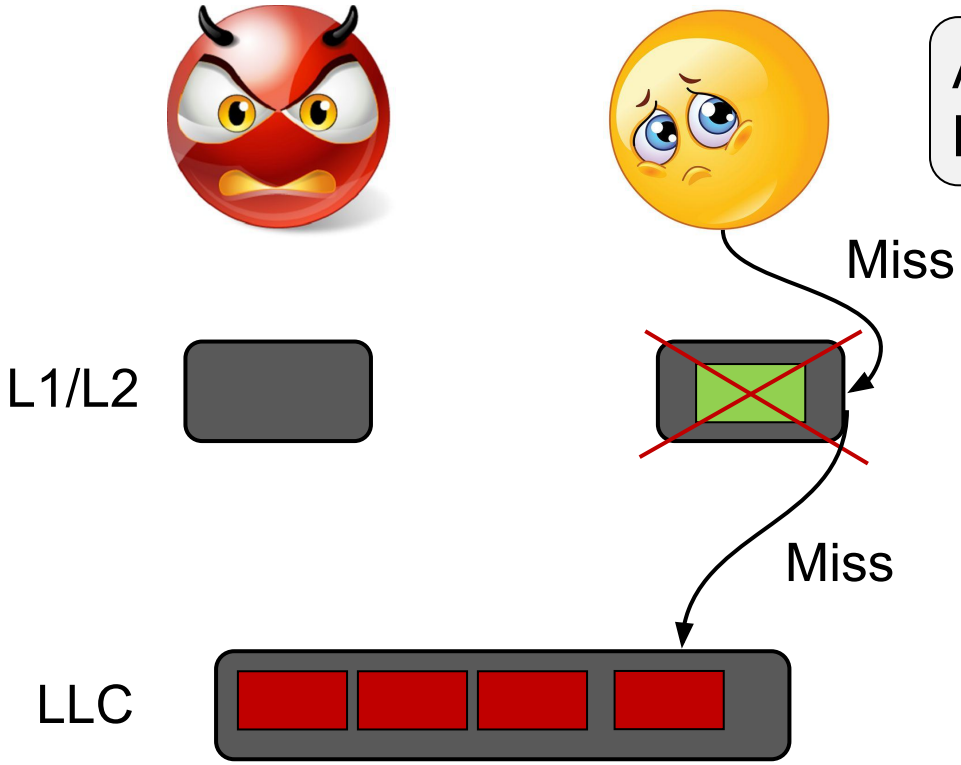
LLC



Cross-core Back-Invalidation - II



Cross-core Back-Invalidation - III



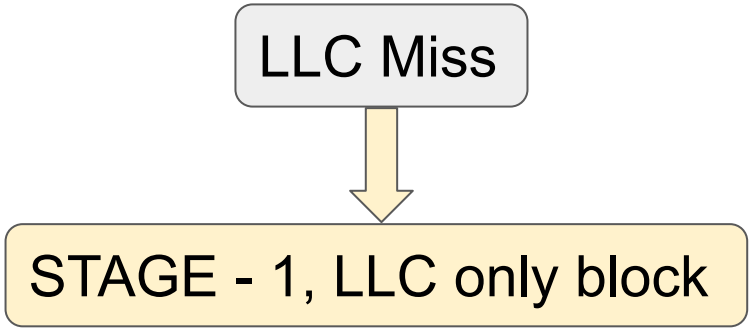
Attacker knows whether victim has accessed it or not

How SHARP Works?

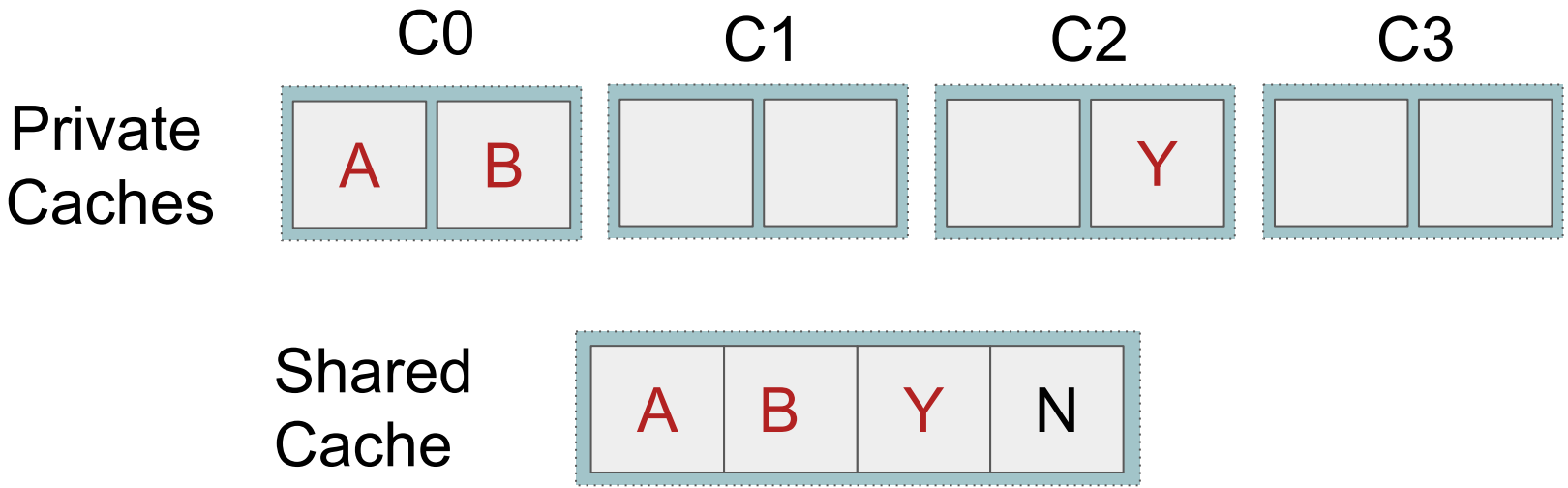
How SHARP Works?

LLC Miss

How SHARP Works?

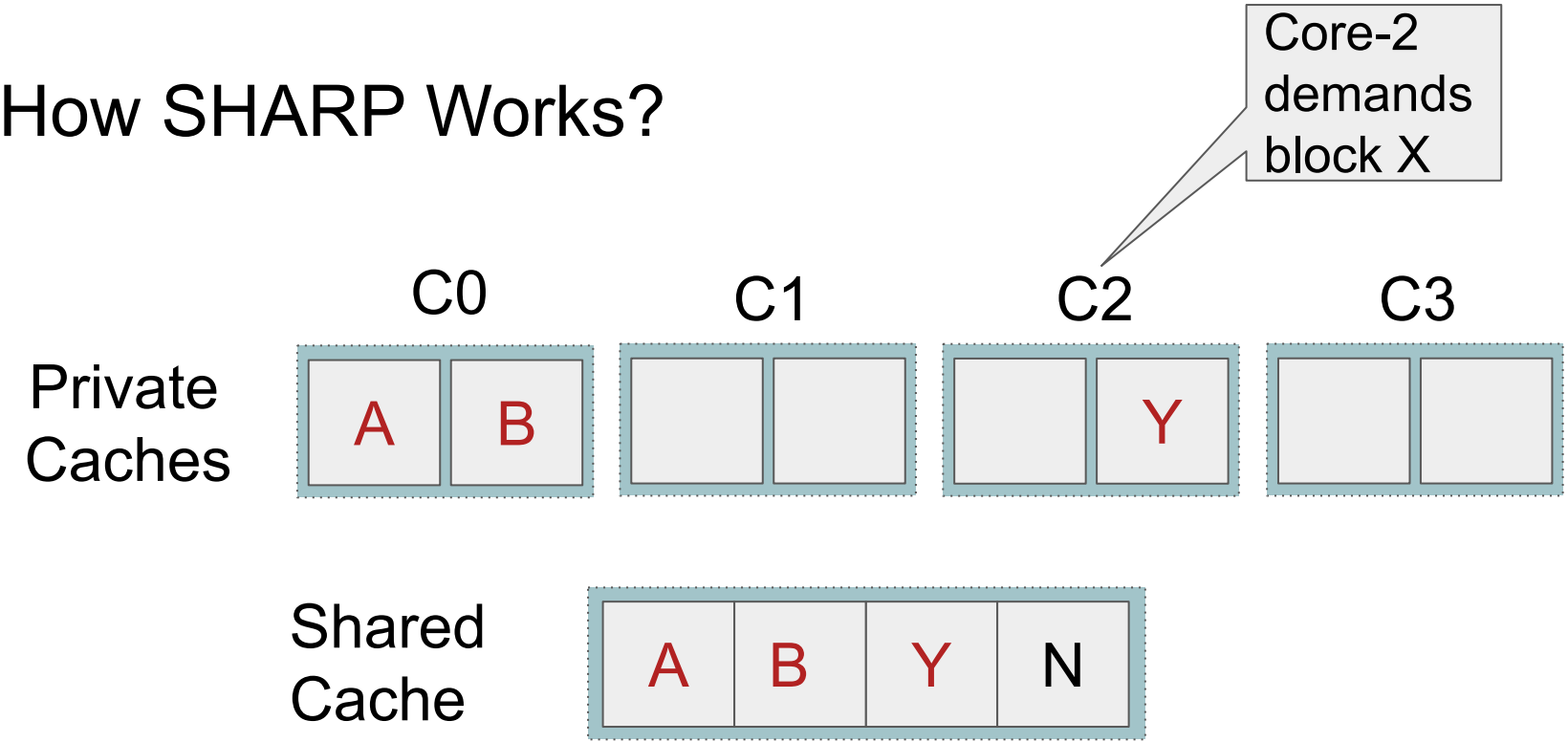


How SHARP Works?



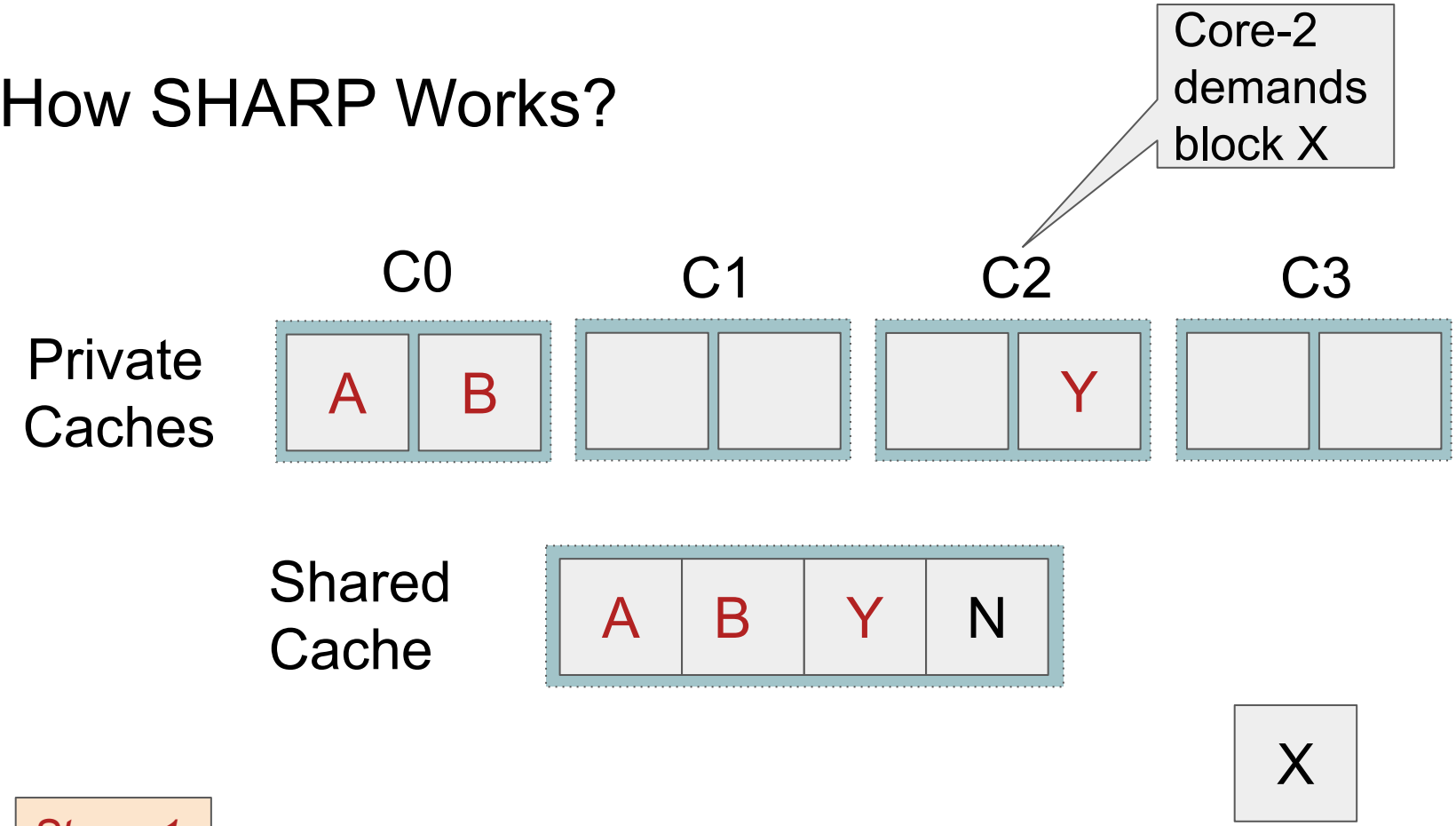
Stage-1

How SHARP Works?

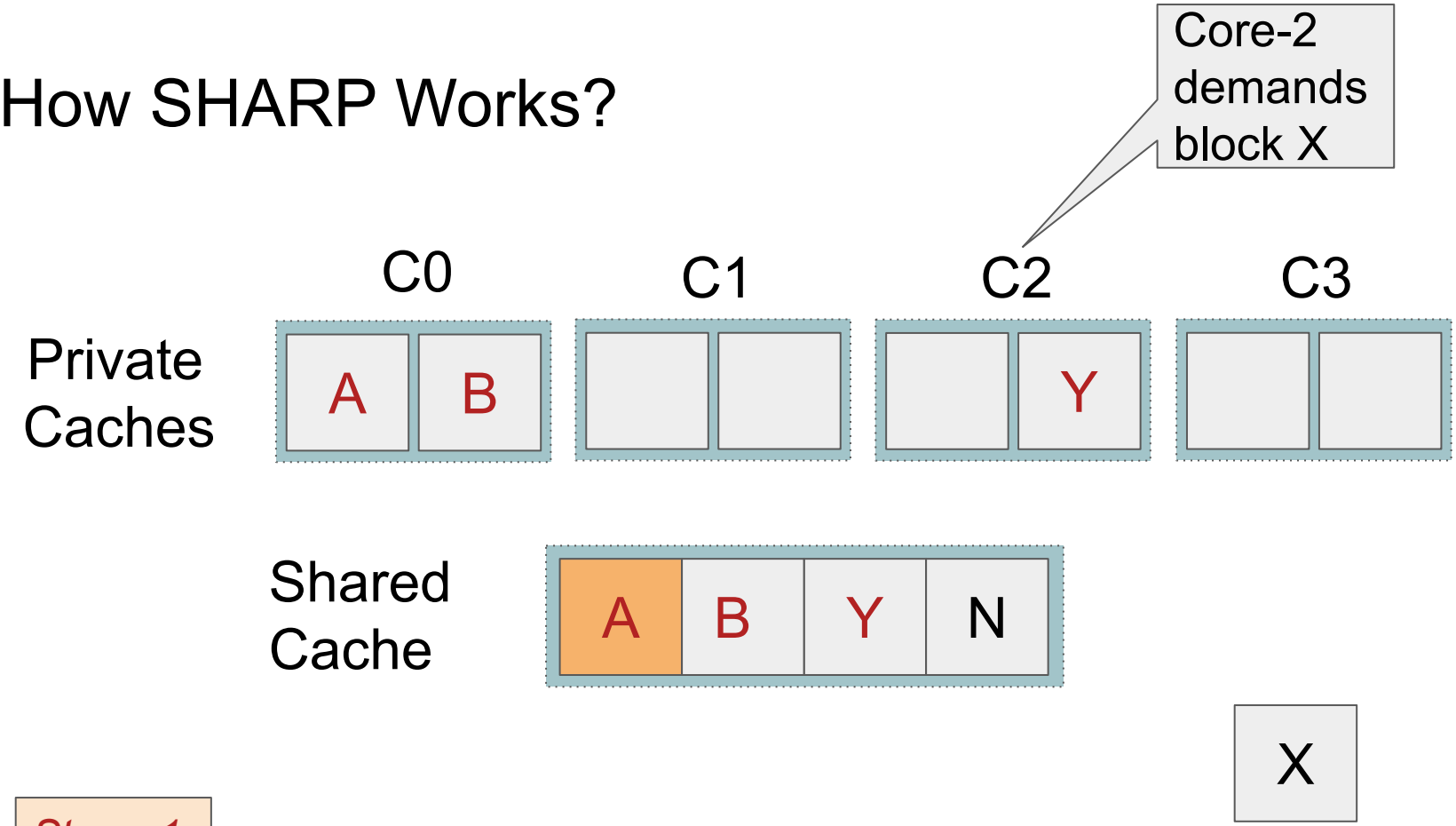


Stage-1

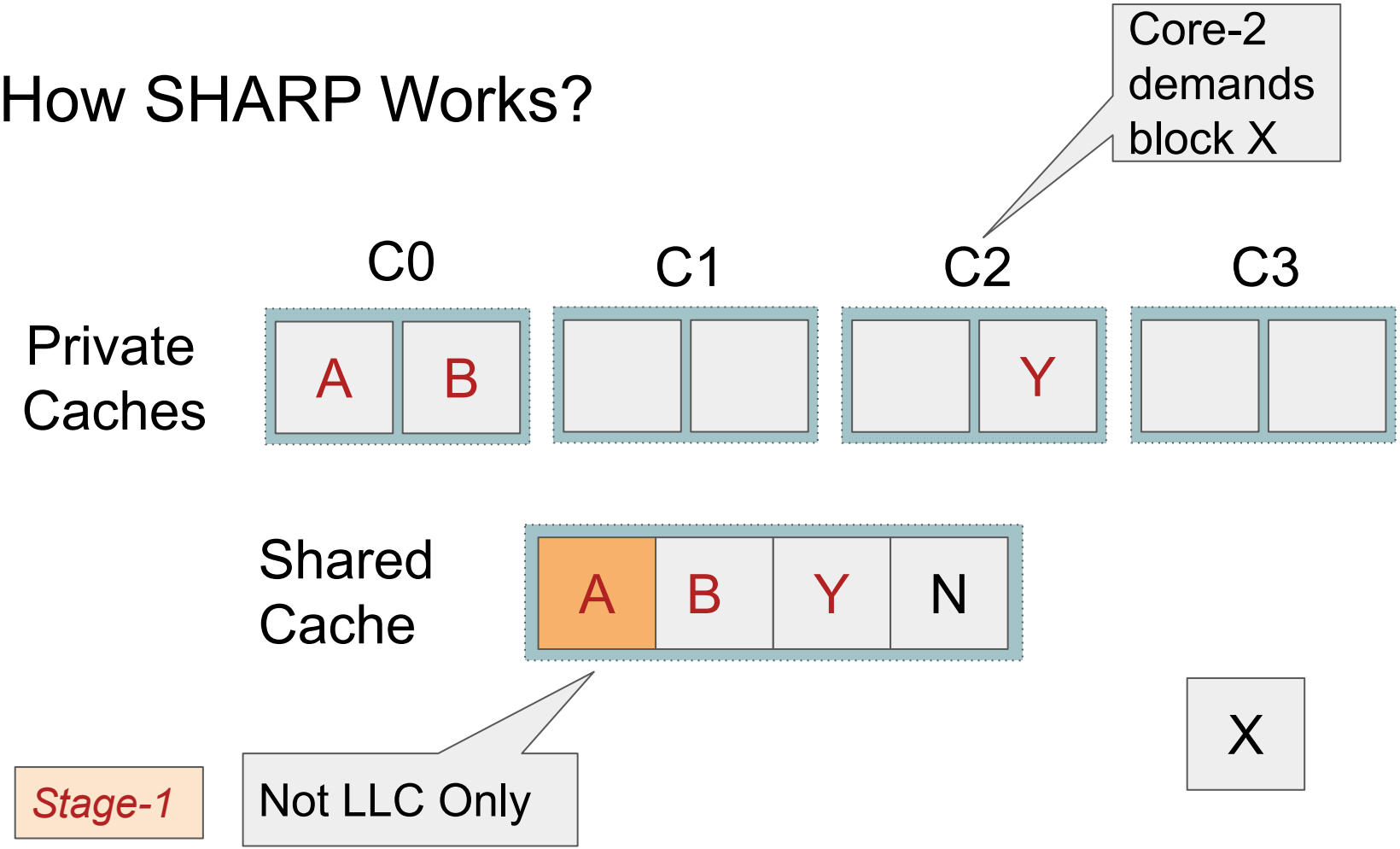
How SHARP Works?



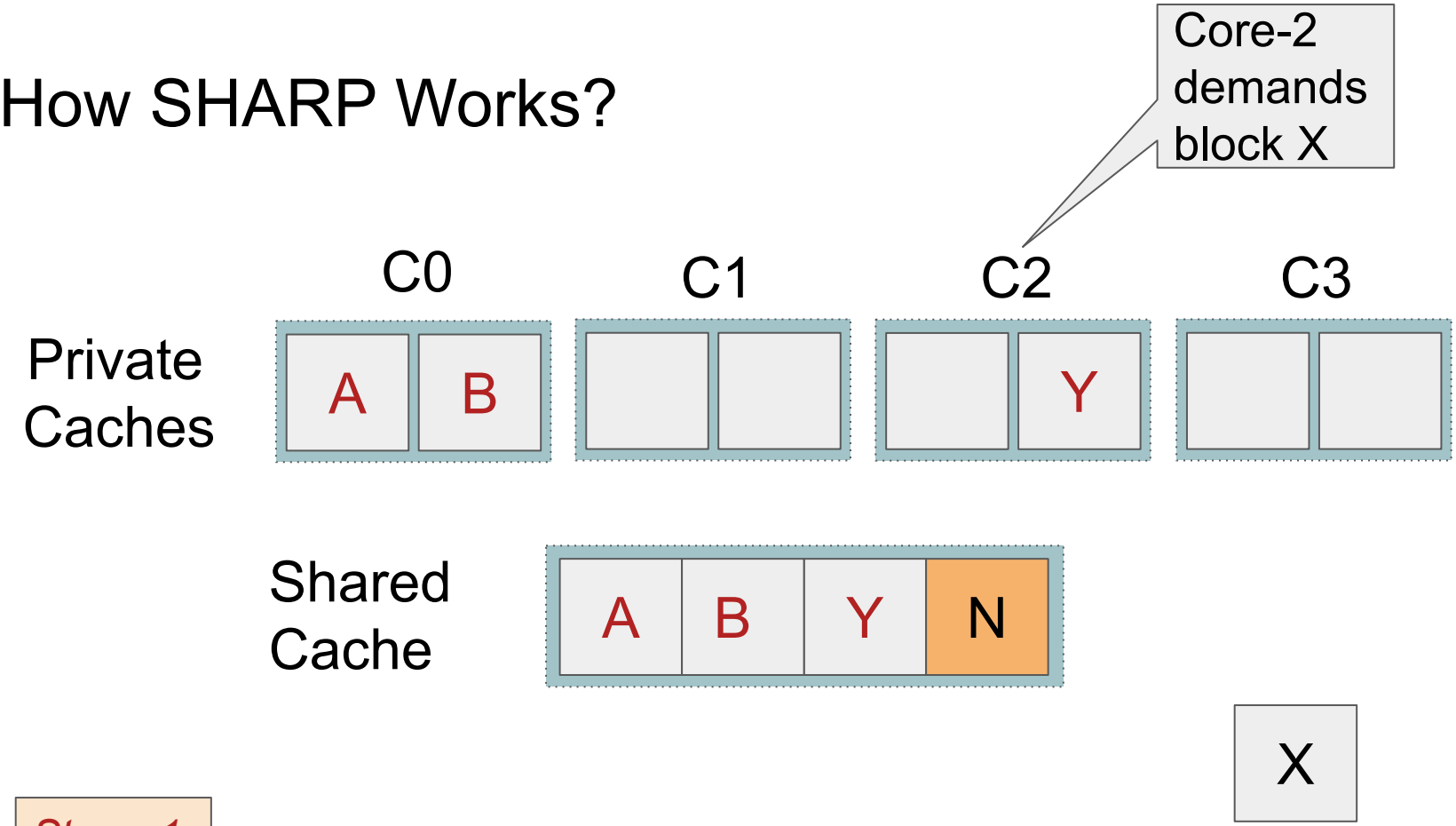
How SHARP Works?



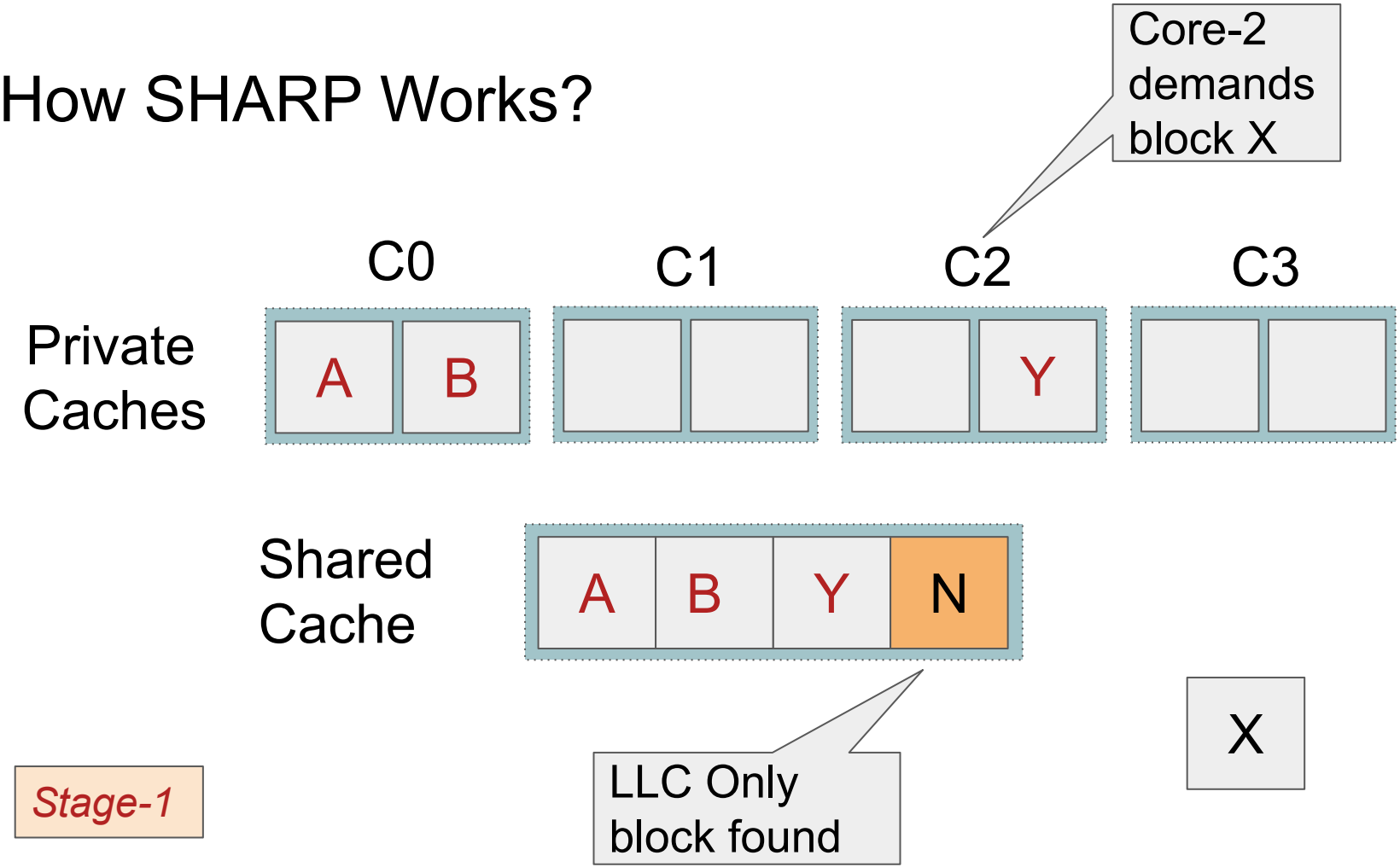
How SHARP Works?



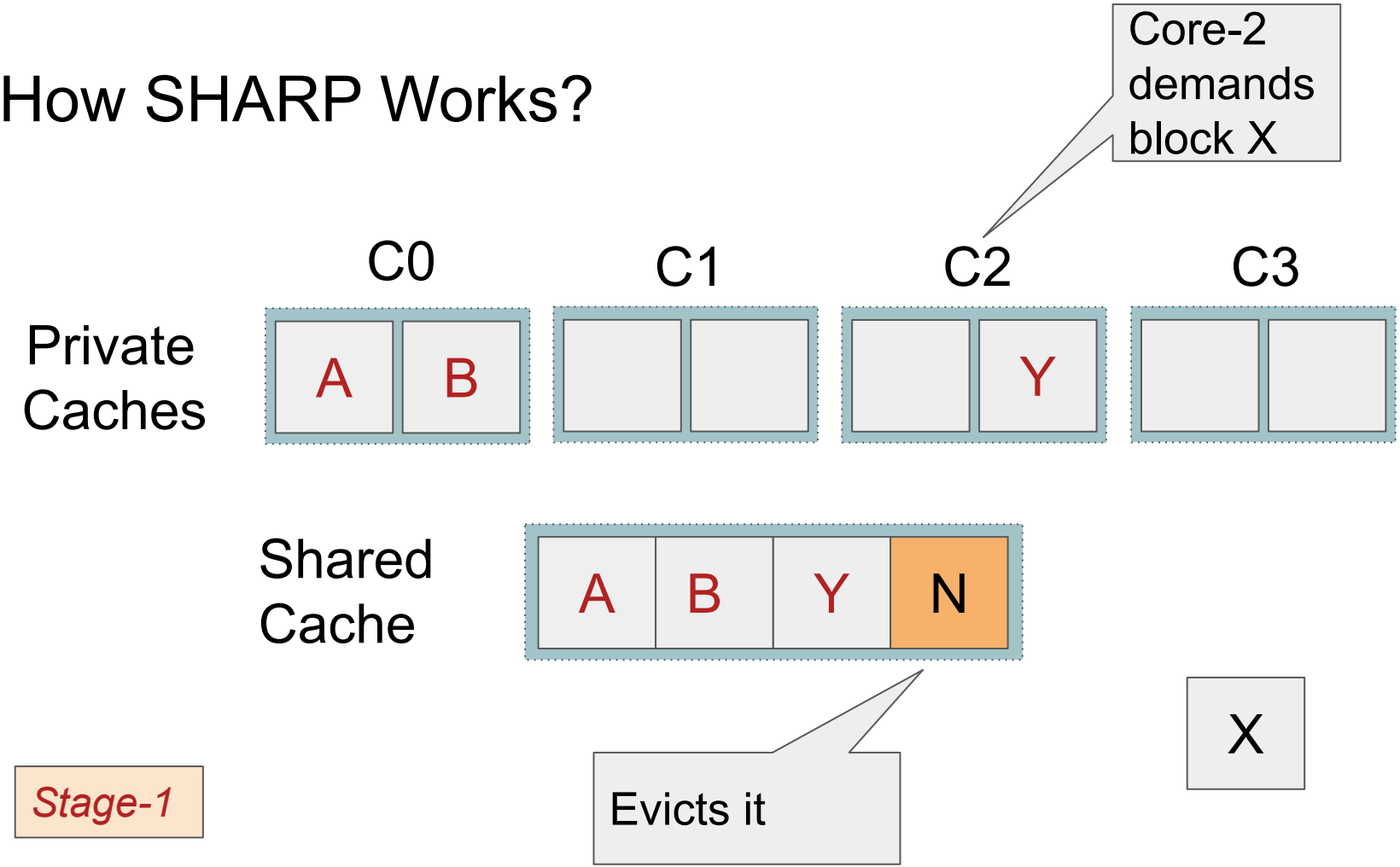
How SHARP Works?



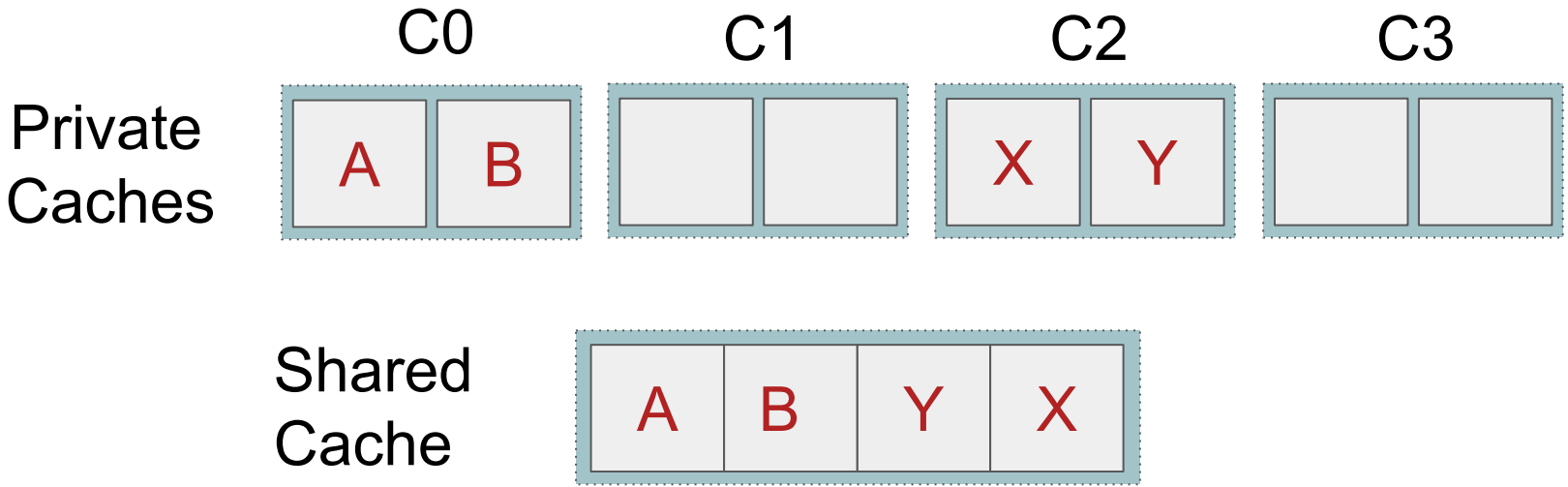
How SHARP Works?



How SHARP Works?

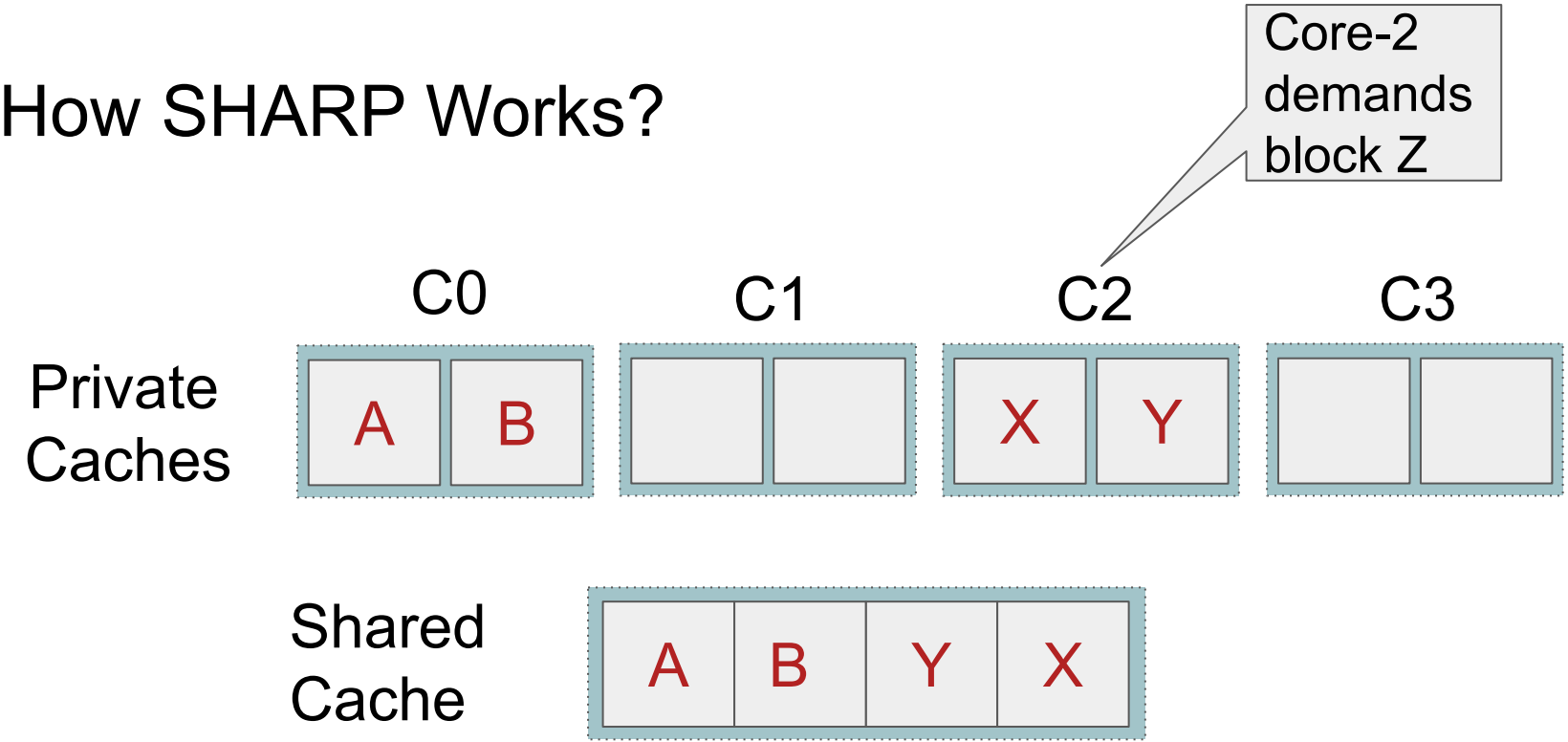


How SHARP Works?



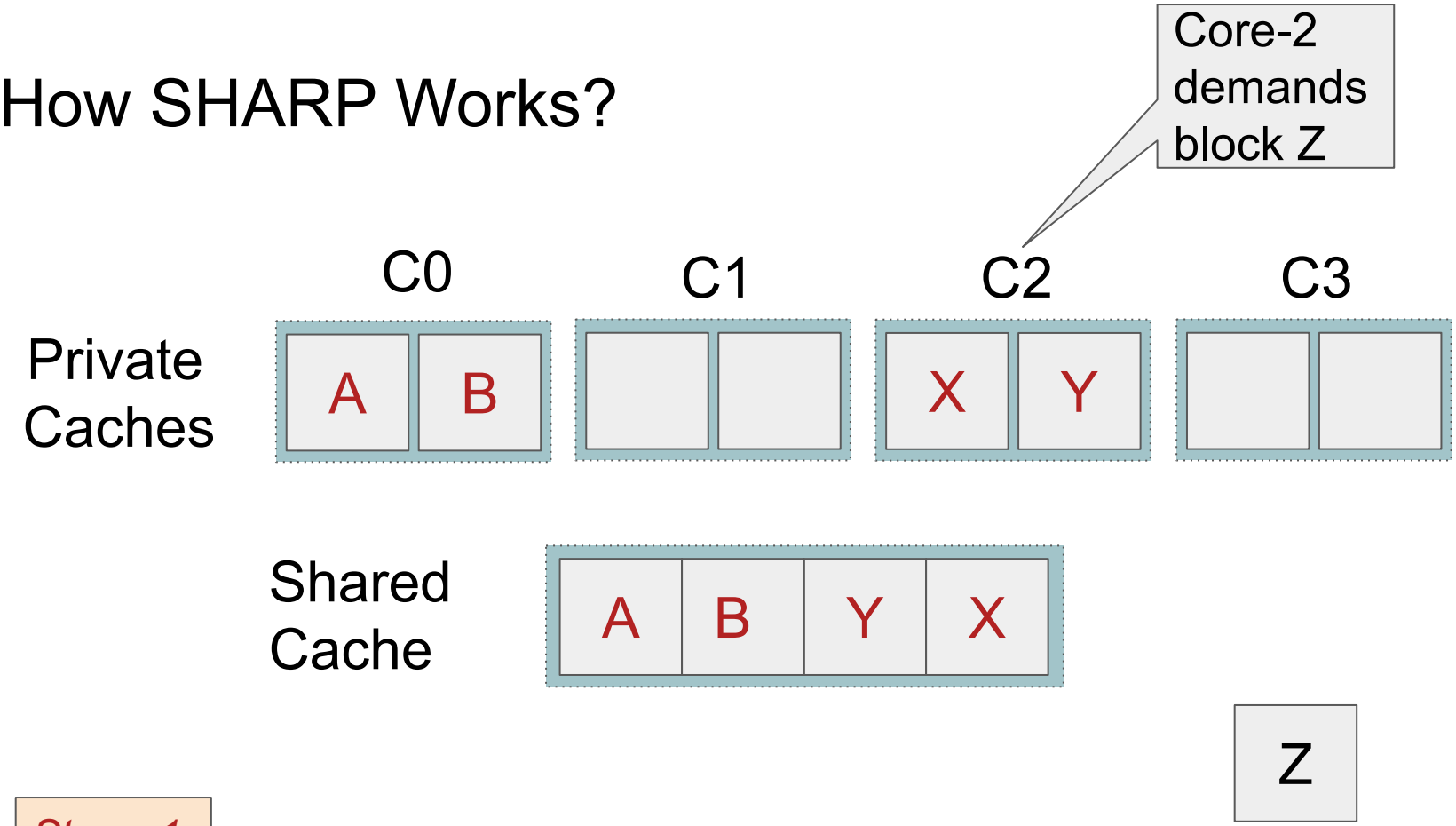
Stage-1

How SHARP Works?

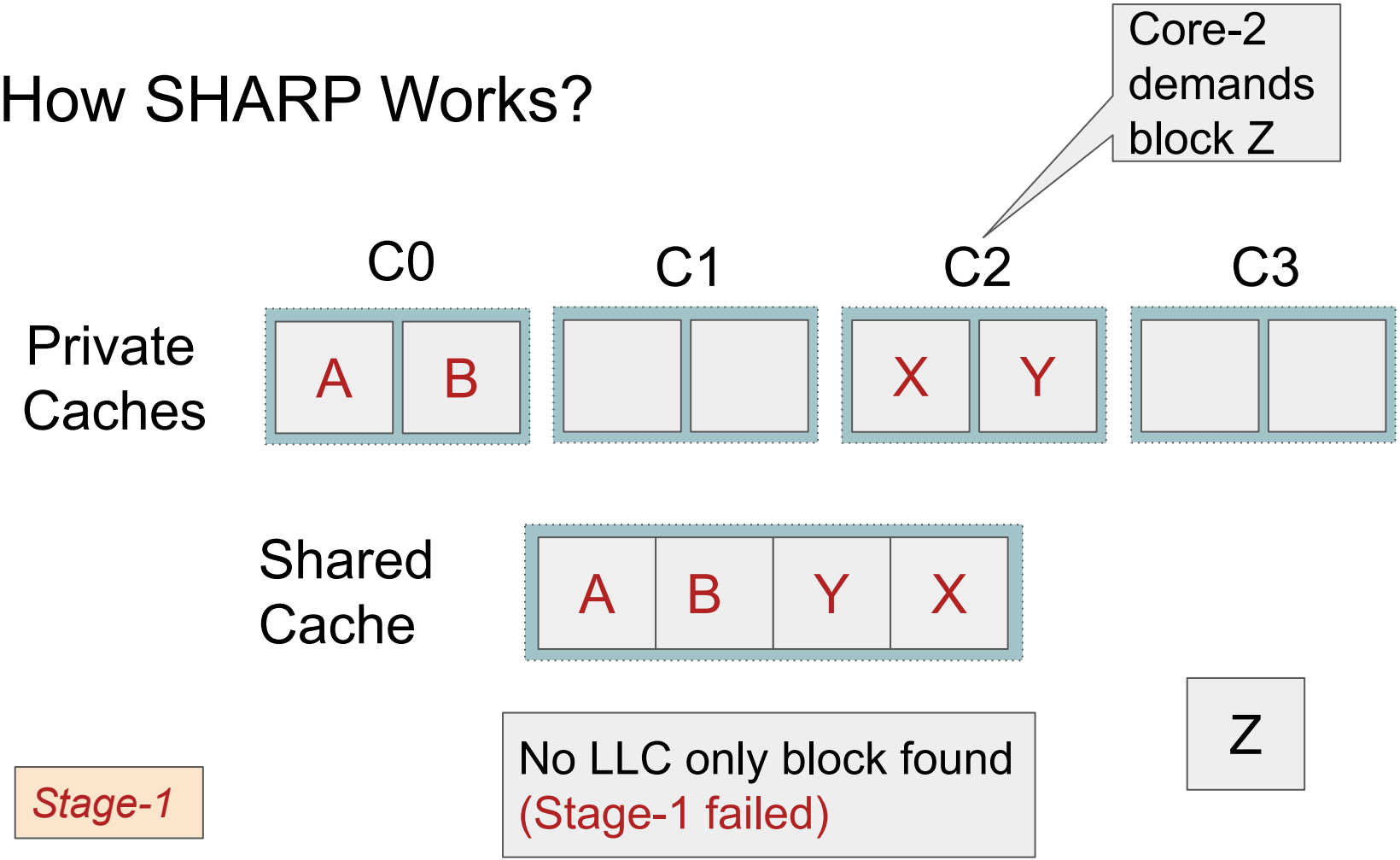


Stage-1

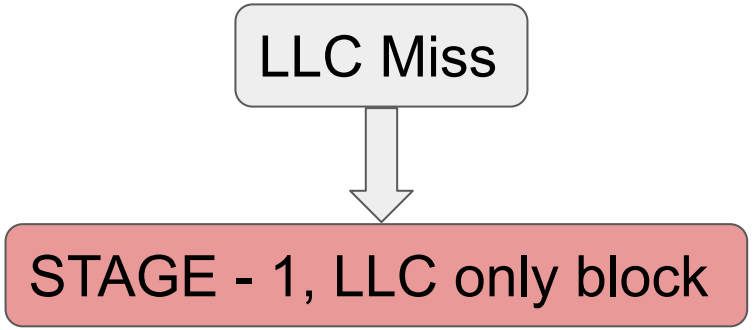
How SHARP Works?



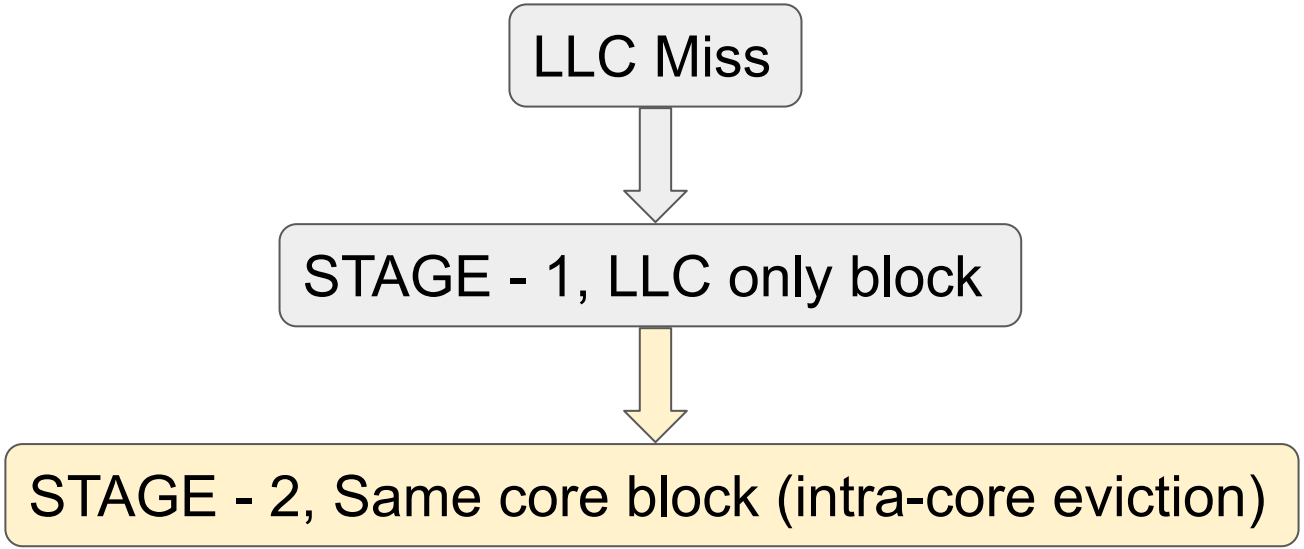
How SHARP Works?



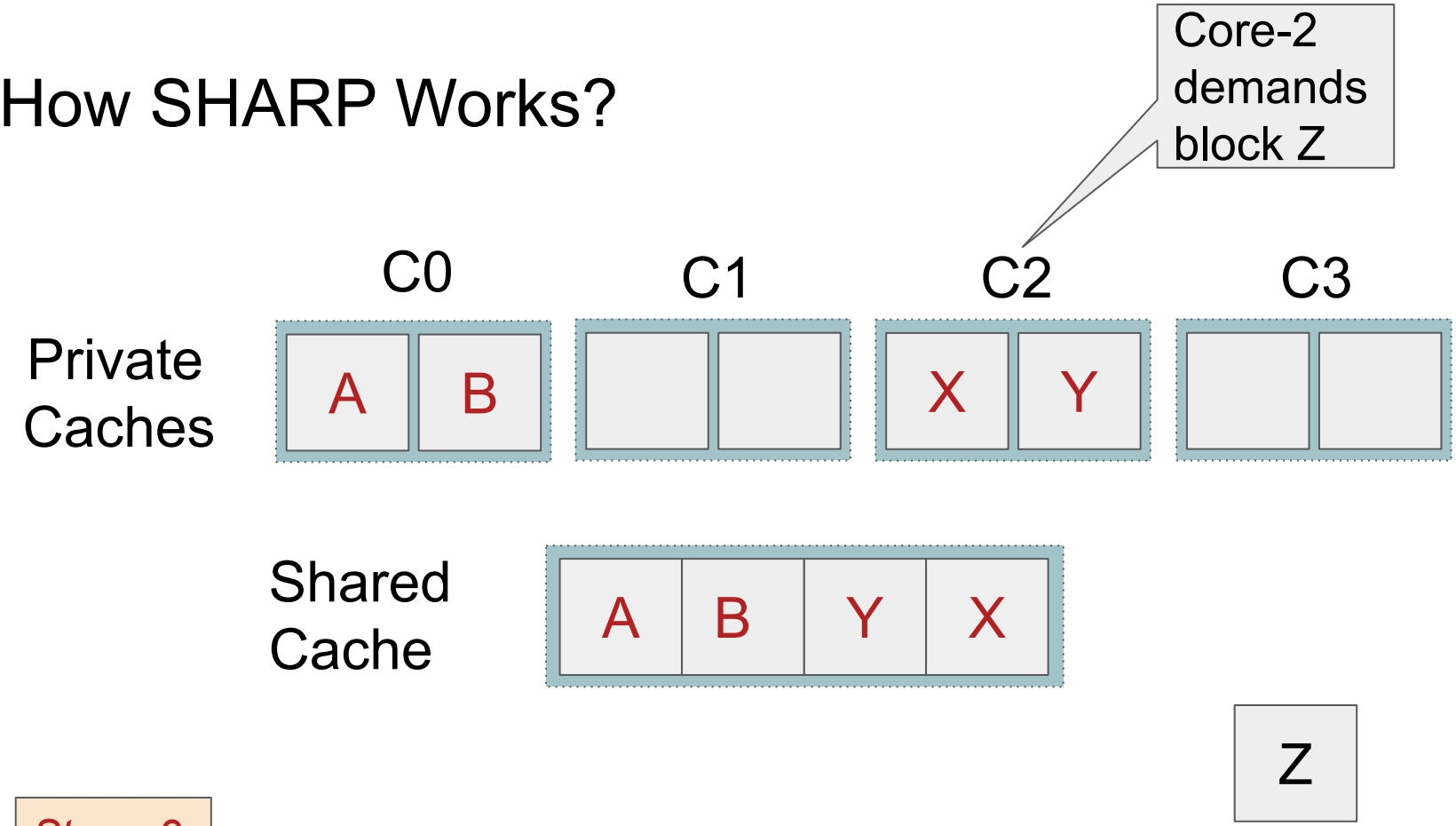
How SHARP Works?



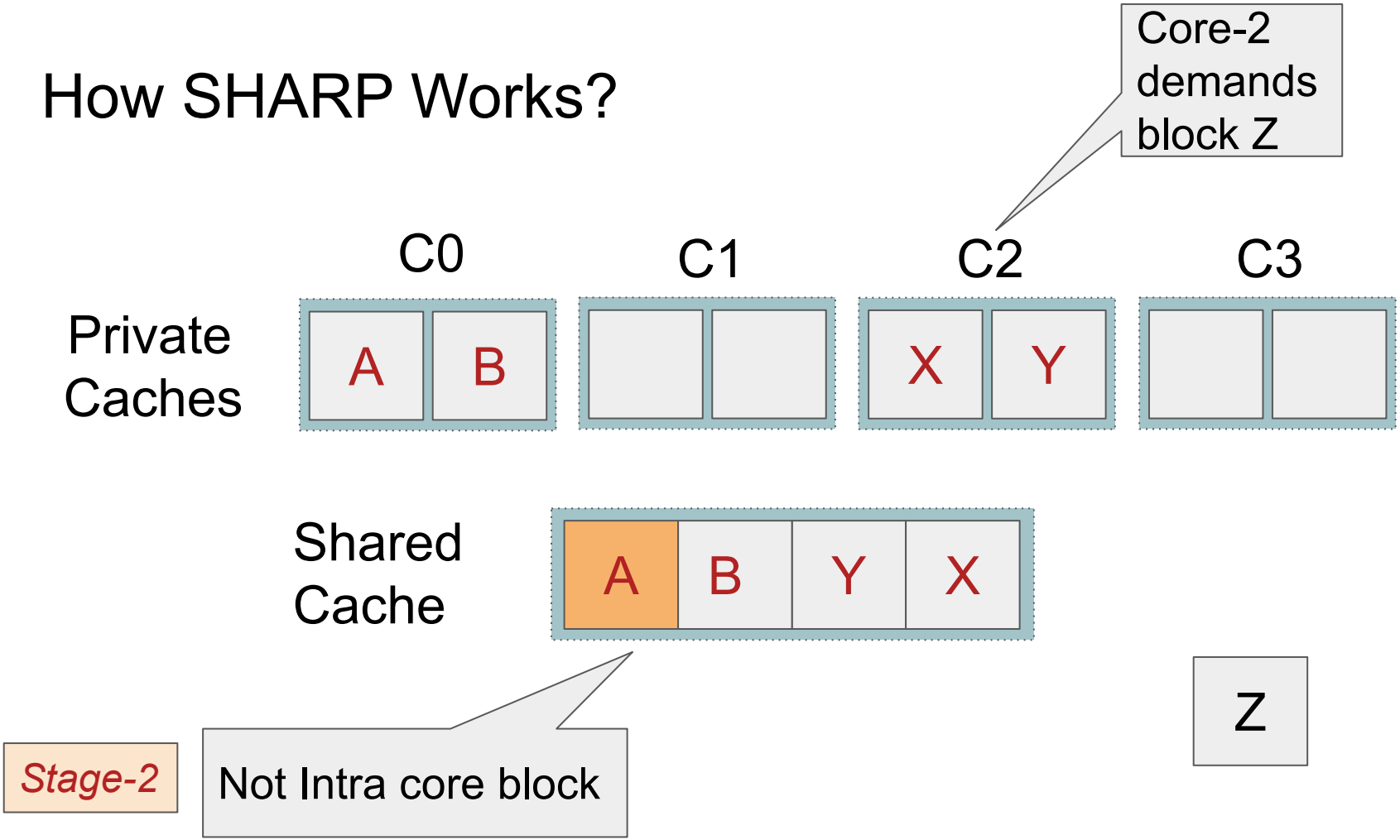
How SHARP Works?



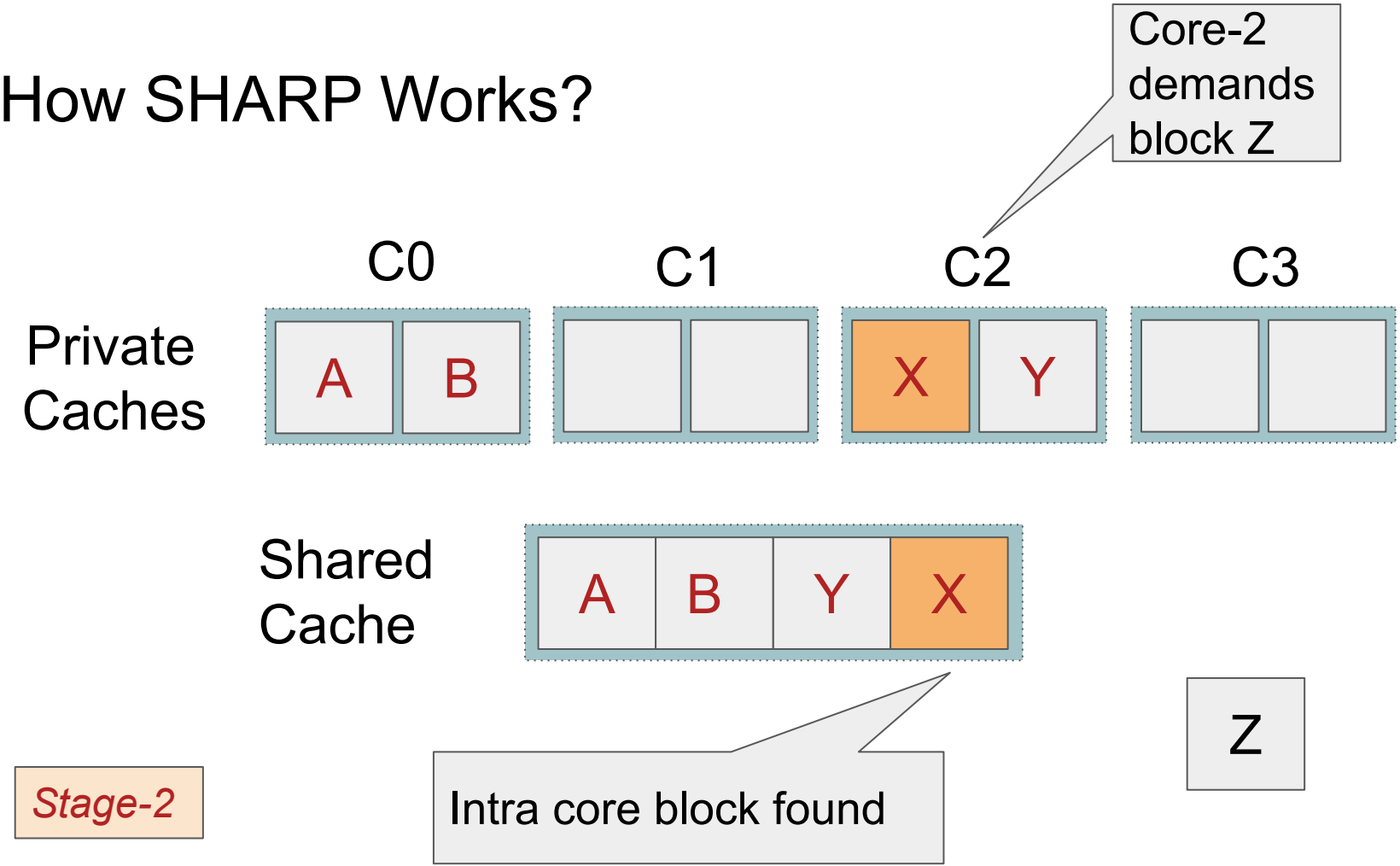
How SHARP Works?



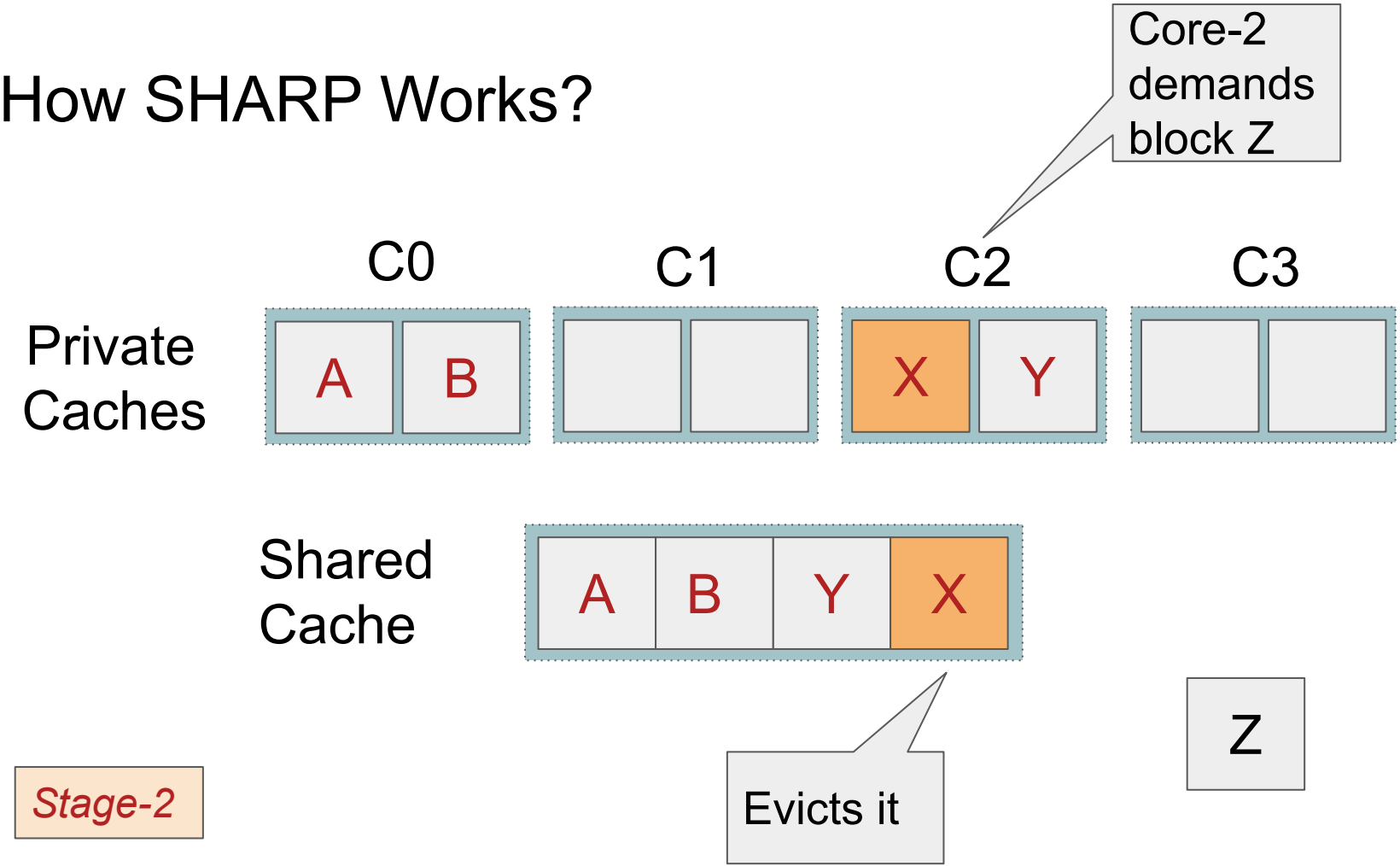
How SHARP Works?



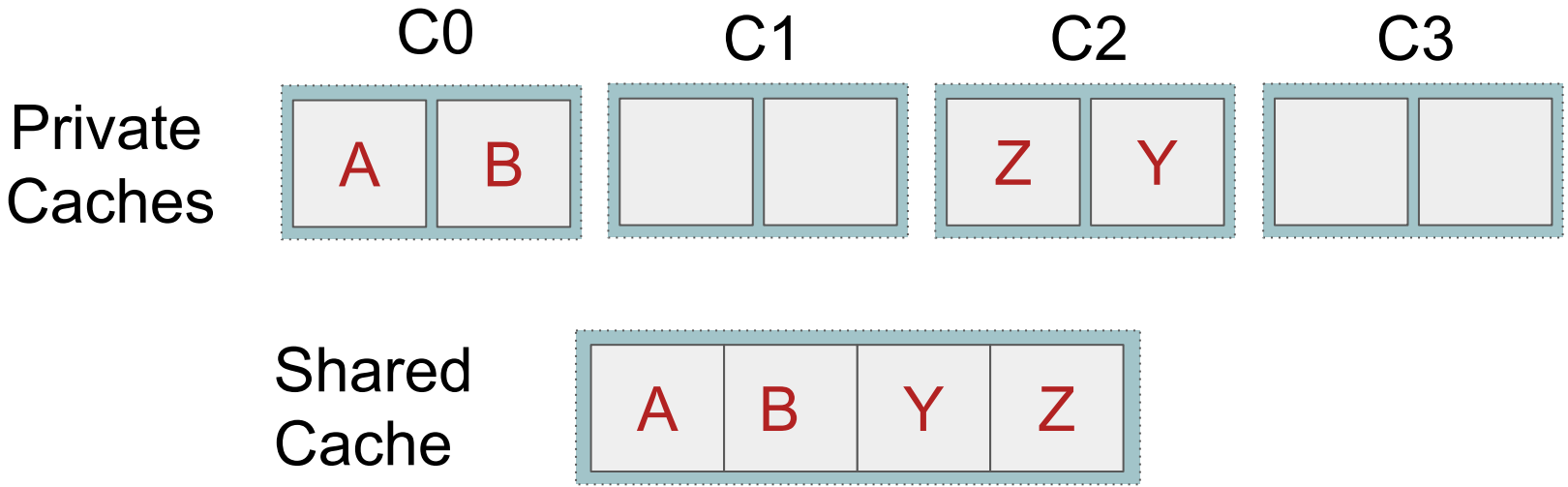
How SHARP Works?



How SHARP Works?

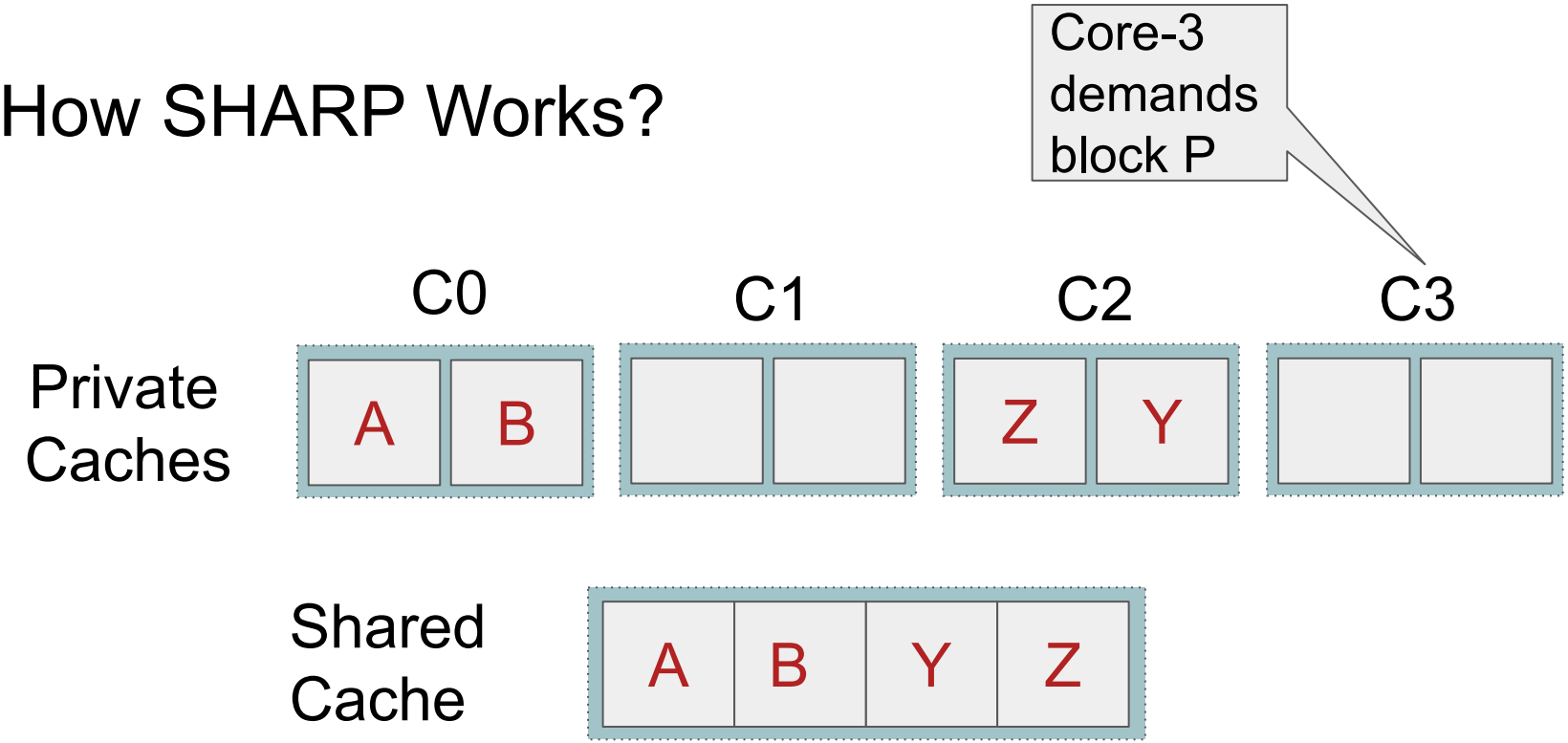


How SHARP Works?



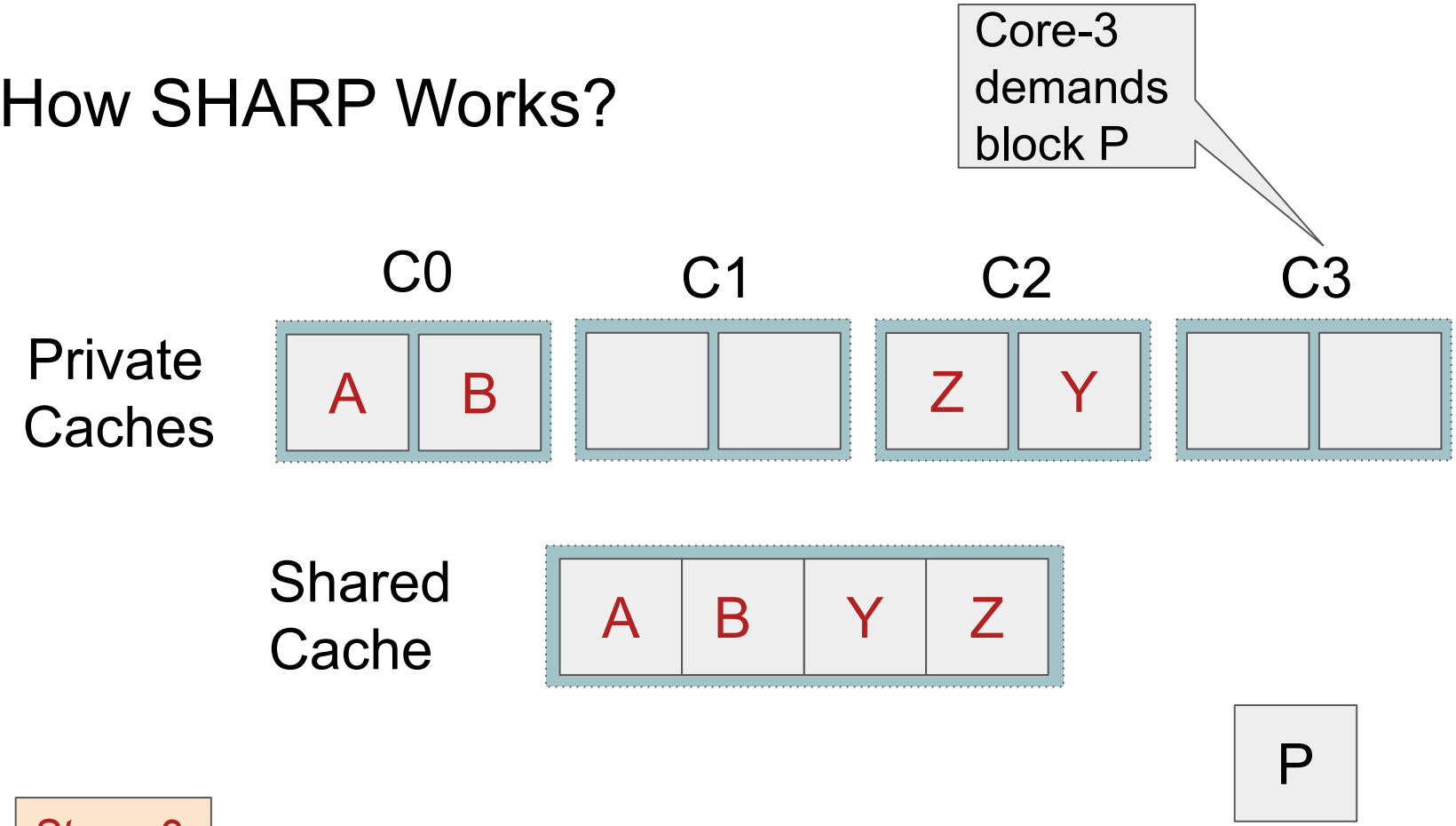
Stage-2

How SHARP Works?



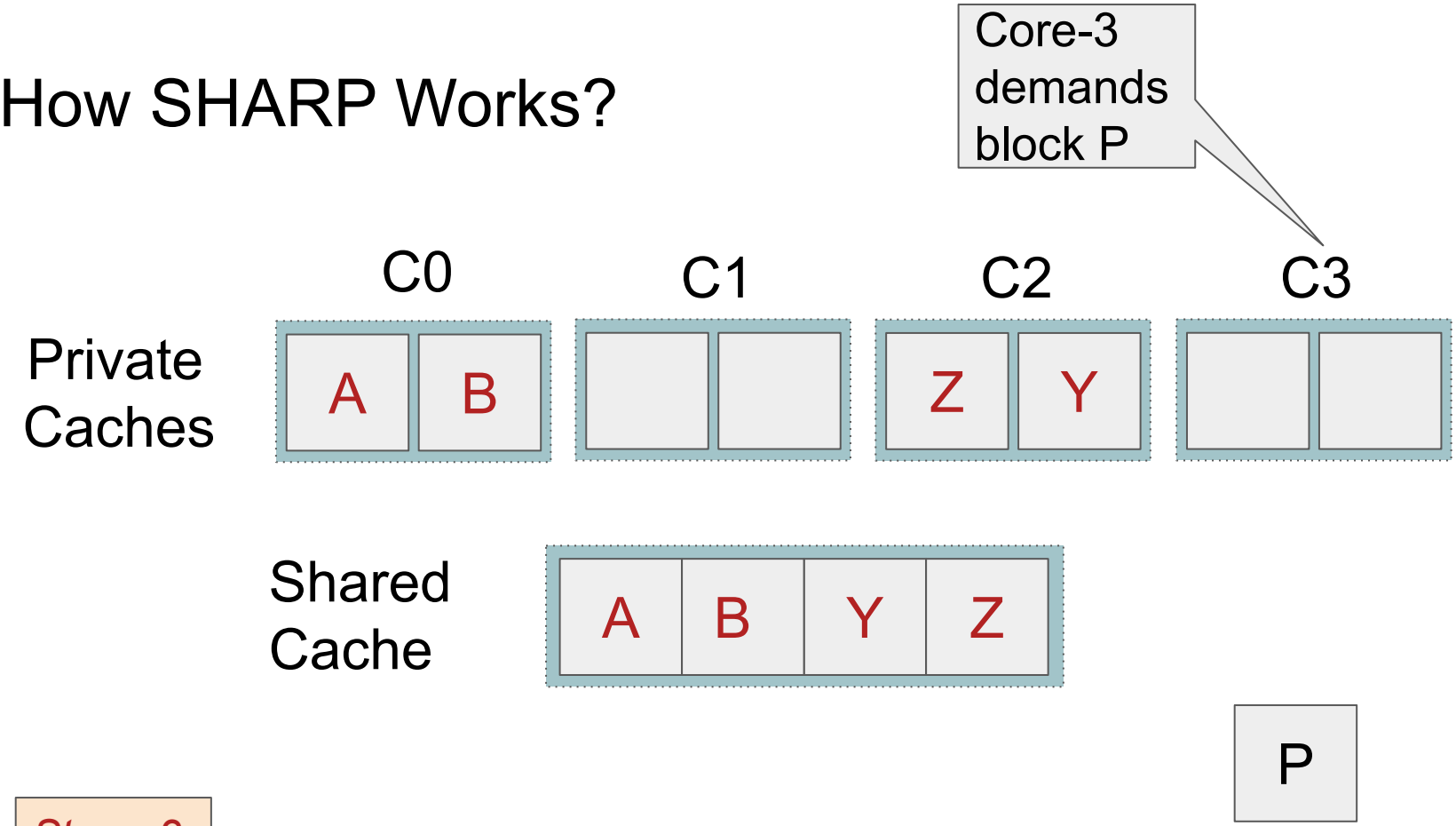
Stage-2

How SHARP Works?



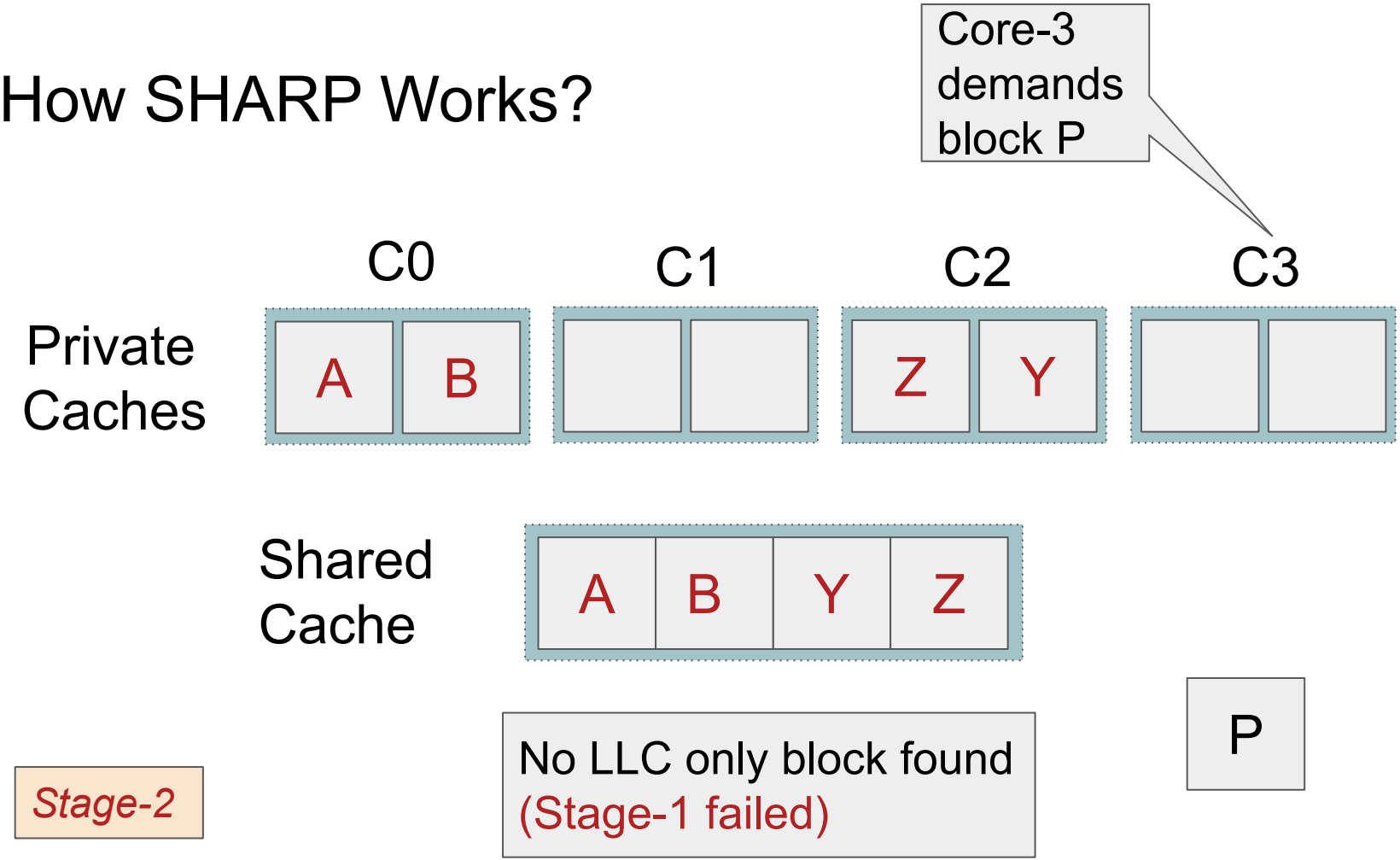
Stage-2

How SHARP Works?

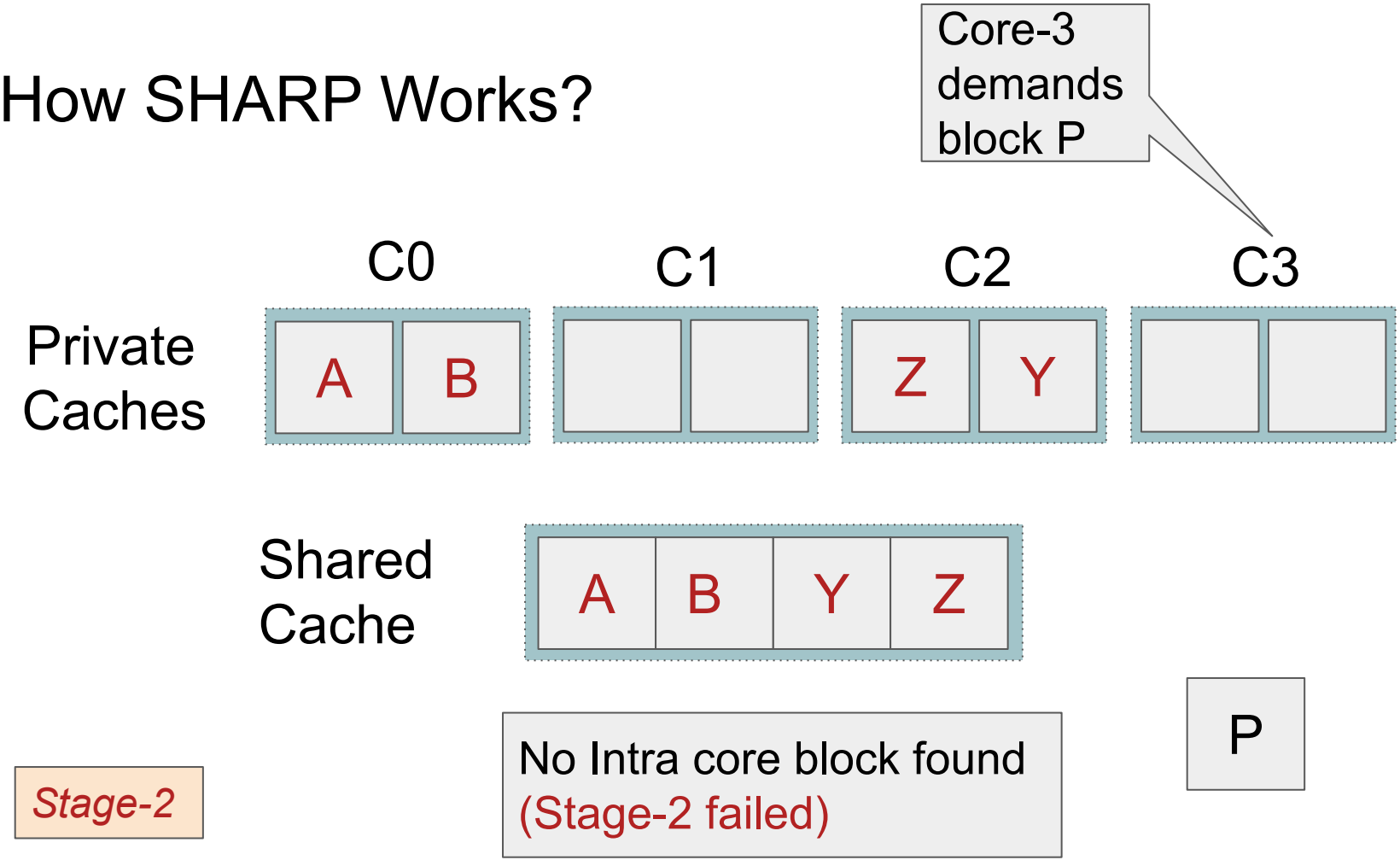


Stage-2

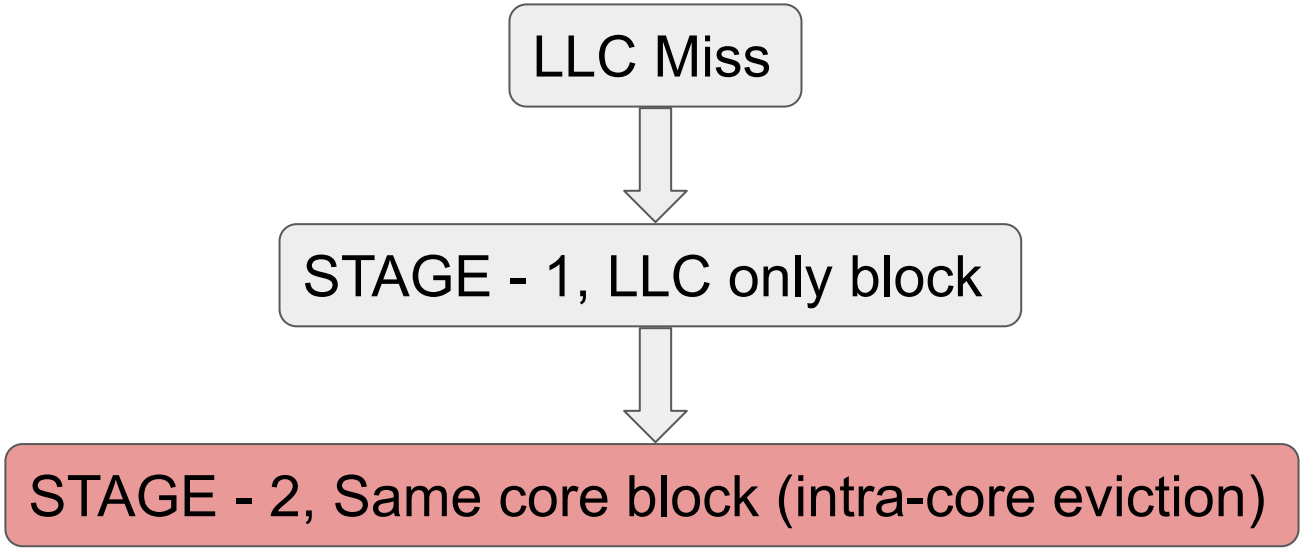
How SHARP Works?



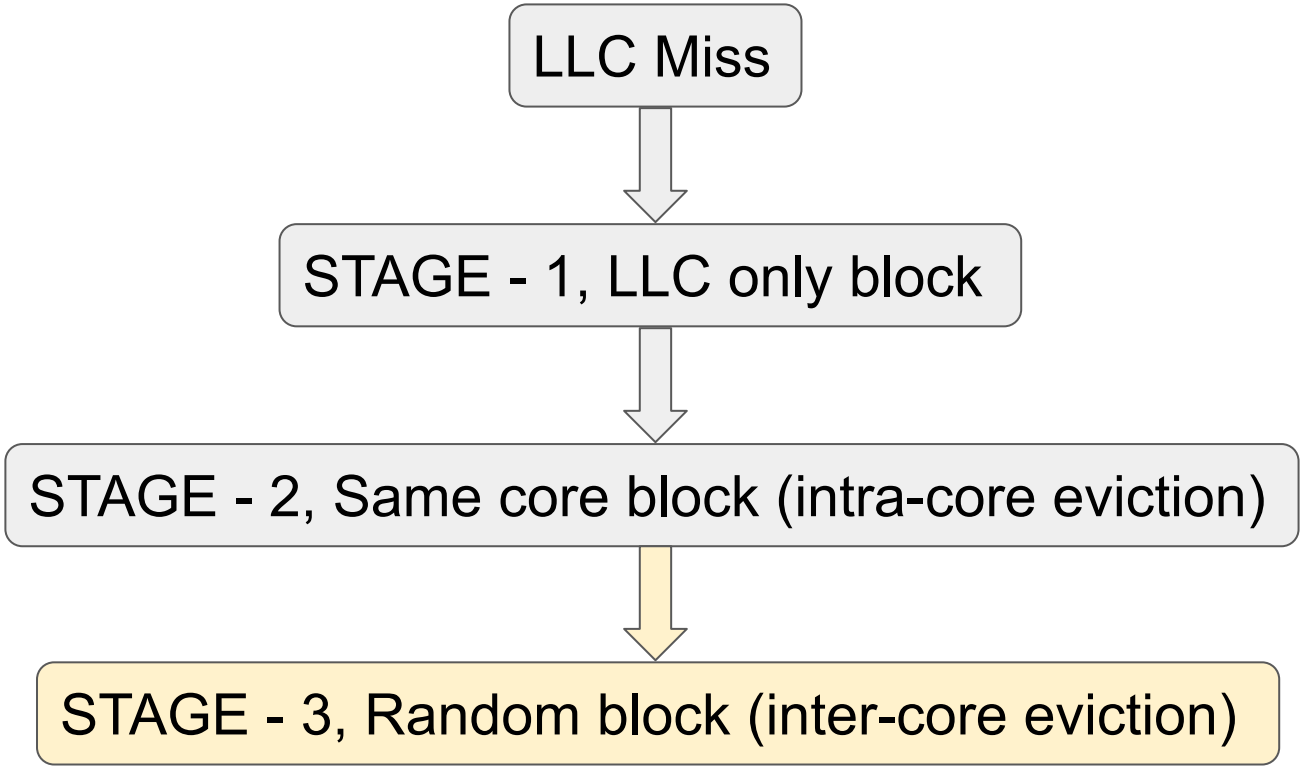
How SHARP Works?



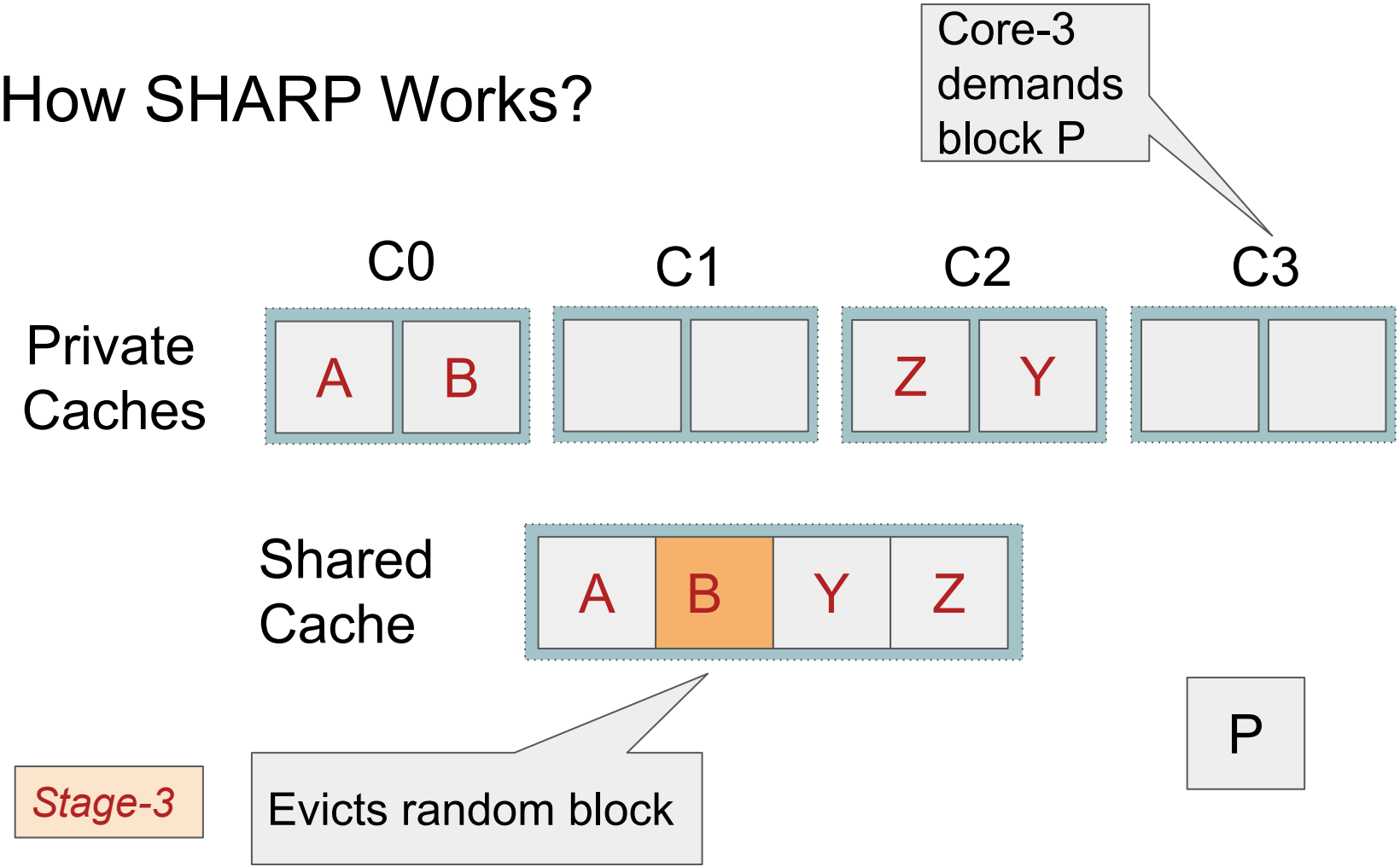
How SHARP Works?



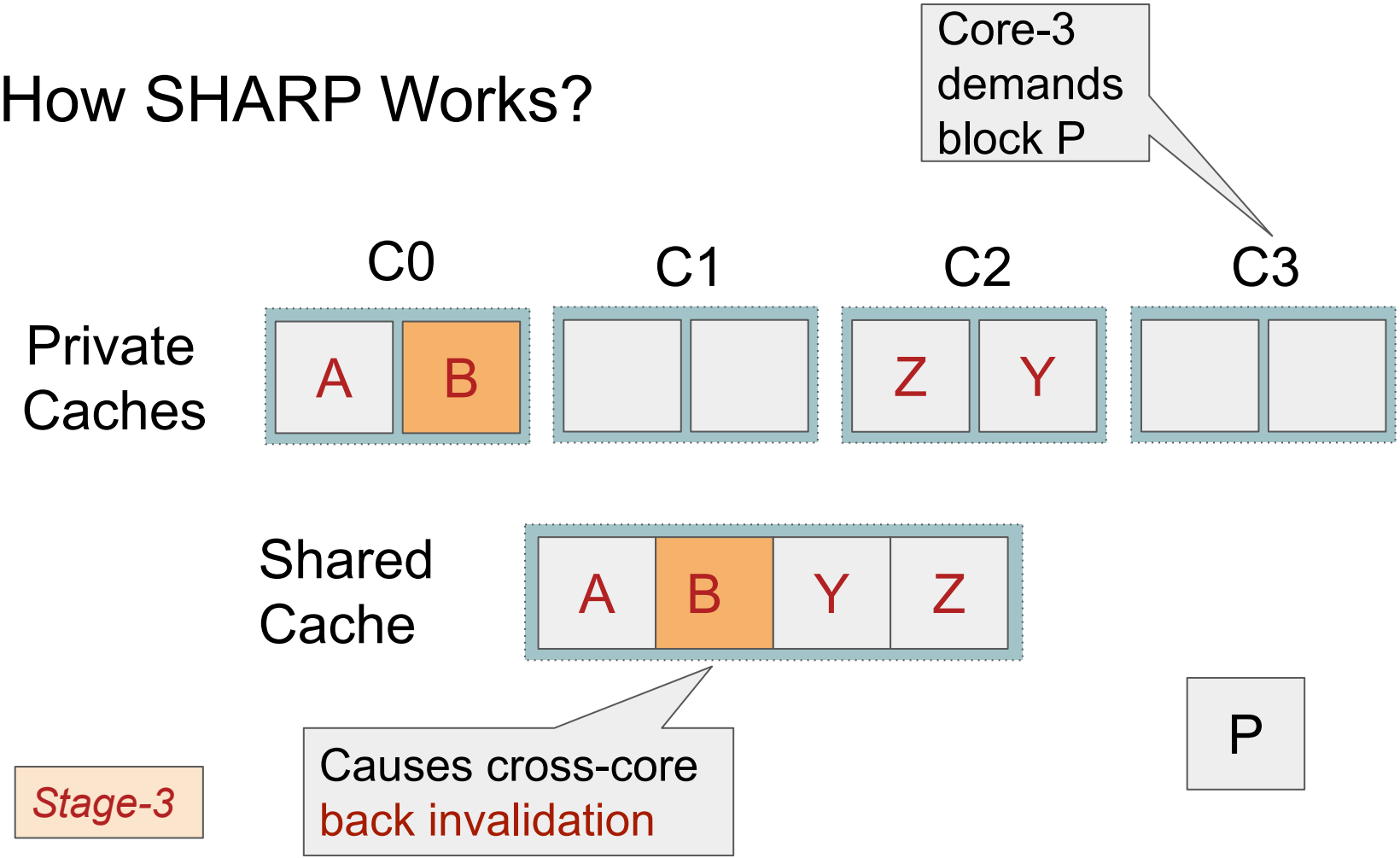
How SHARP Works?



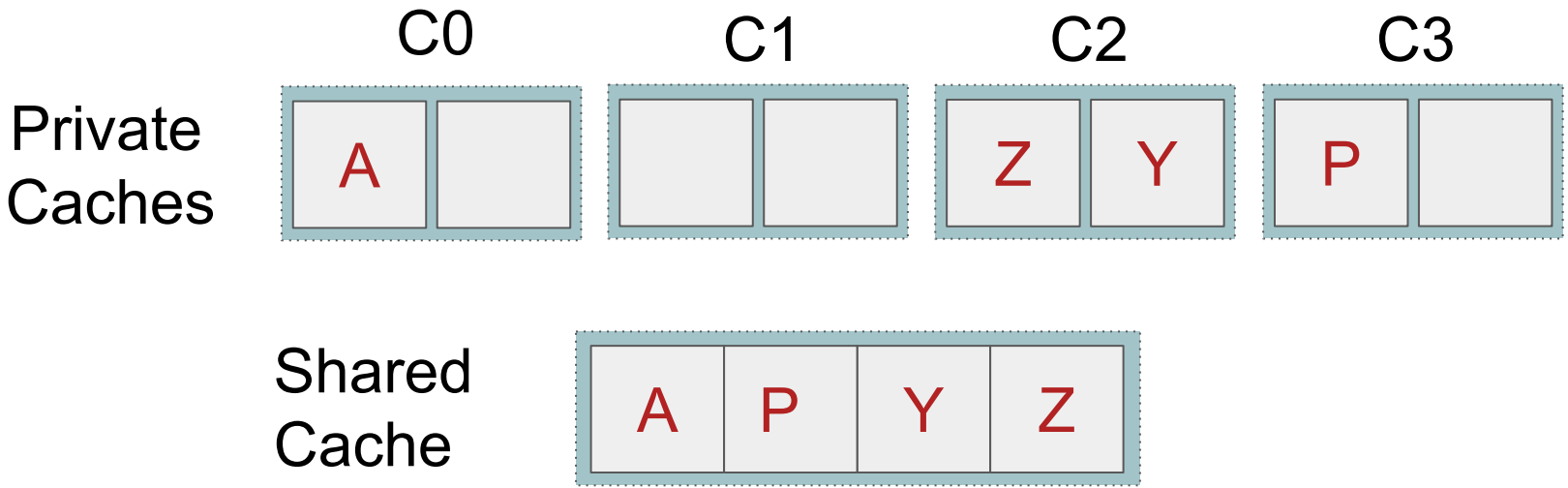
How SHARP Works?



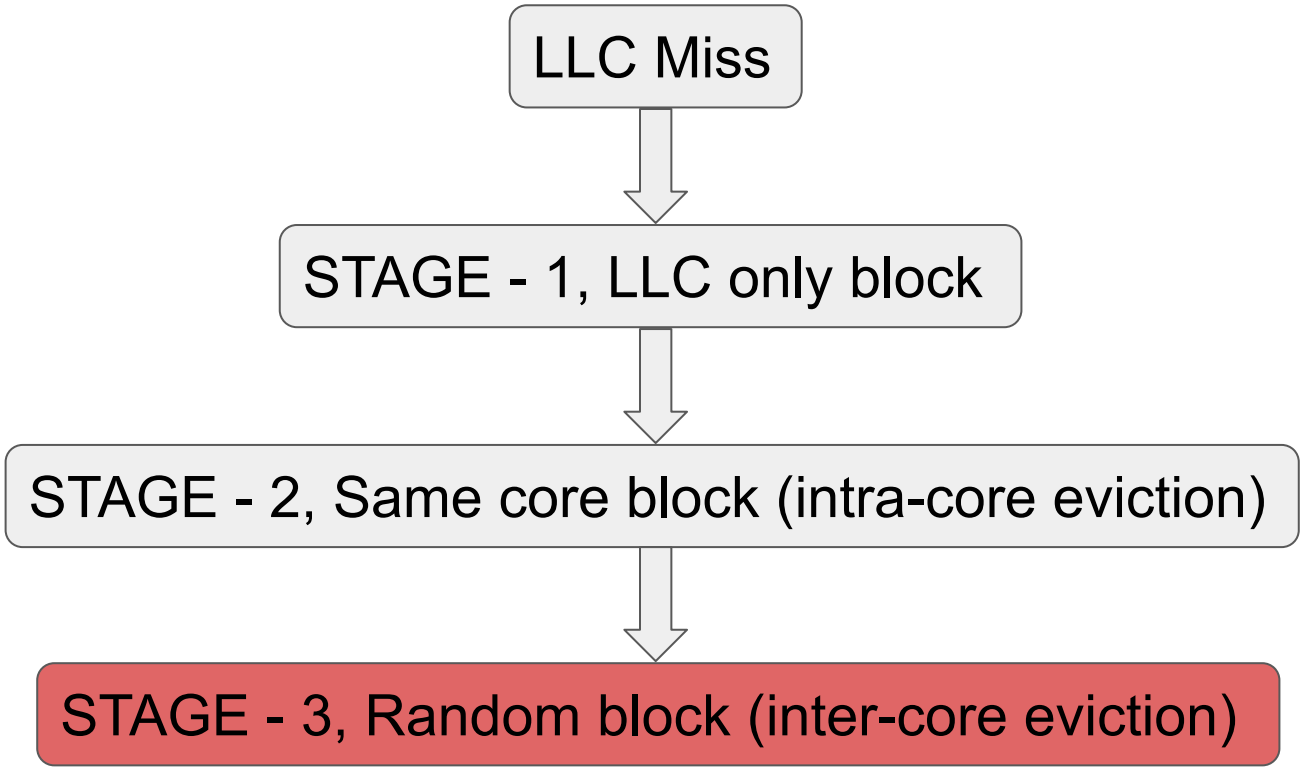
How SHARP Works?



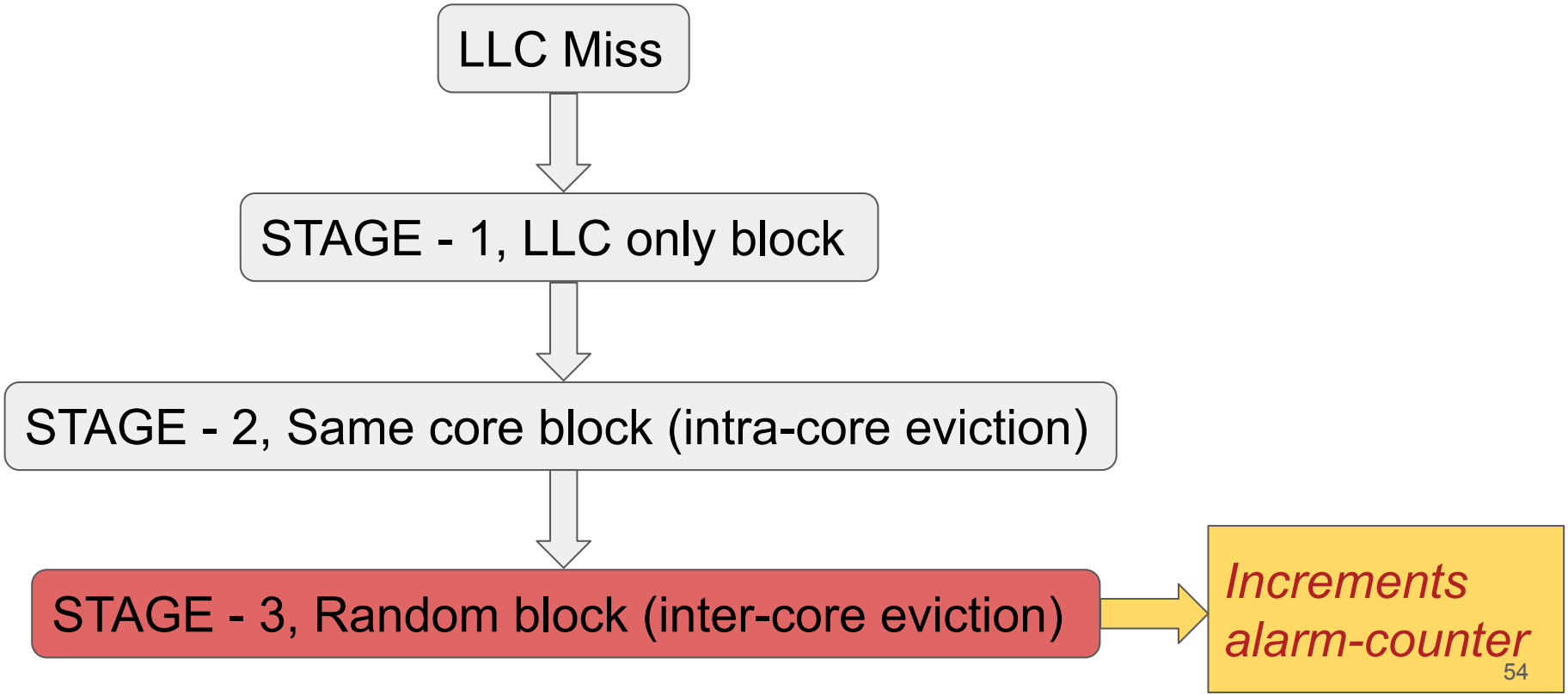
How SHARP Works?



How SHARP Works?



How SHARP Works?



SHARP Alarm Counter

Counter per core

SHARP Alarm Counter

Counter per core

Increments on inter-core eviction

SHARP Alarm Counter

Counter per core

Increments on inter-core eviction

For 1 billion cycles, the threshold value is 2000

SHARP Alarm Counter

Counter per core

Increments on inter-core eviction

For 1 billion cycles, the threshold value is 2000

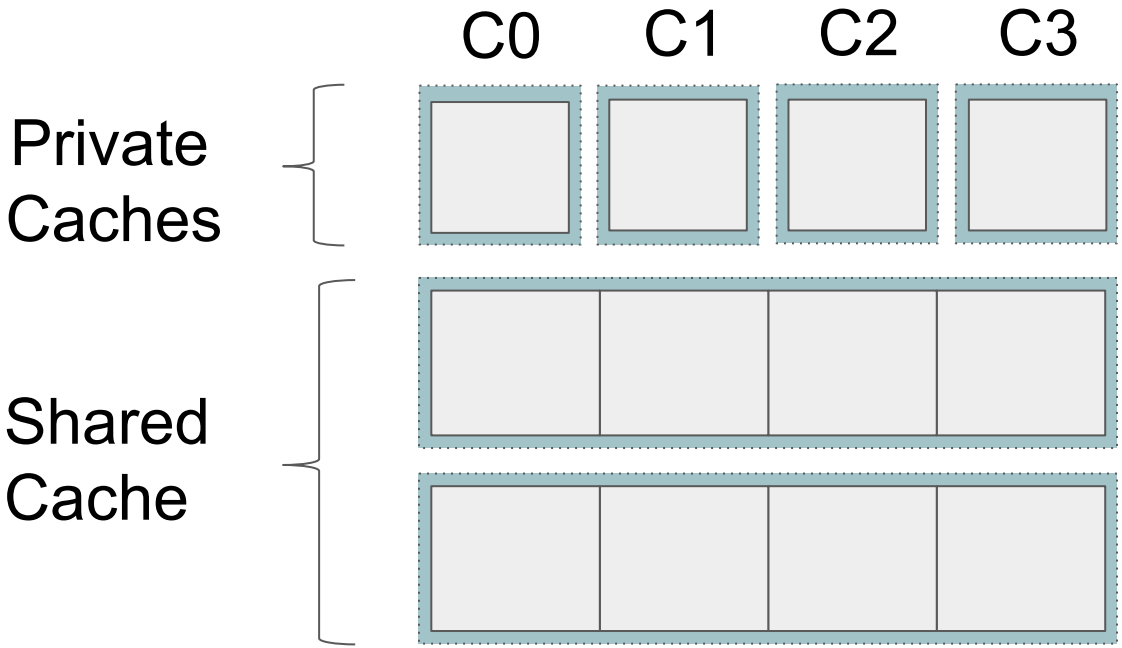
On exceeding threshold, SHARP triggers OS interrupt

Questions That We Ask?

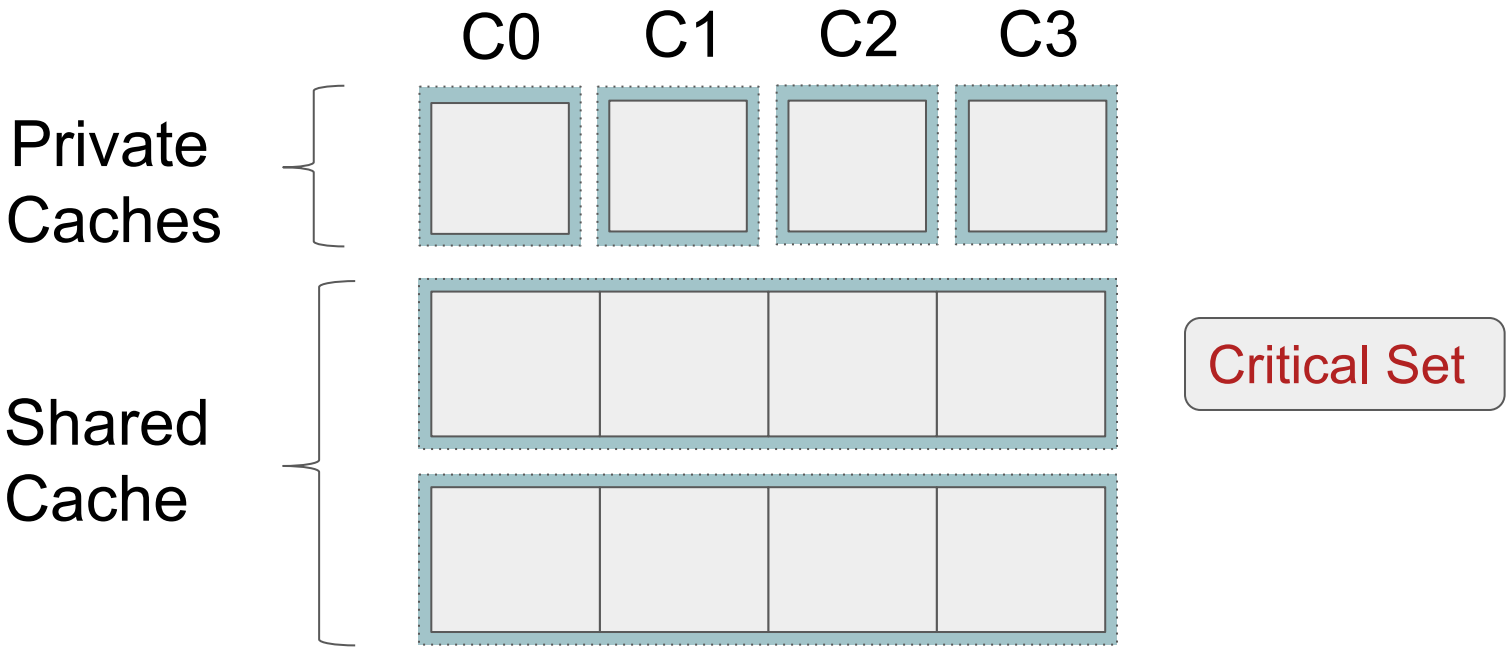
Questions That We Ask?

Does SHARP mitigate all attacks?

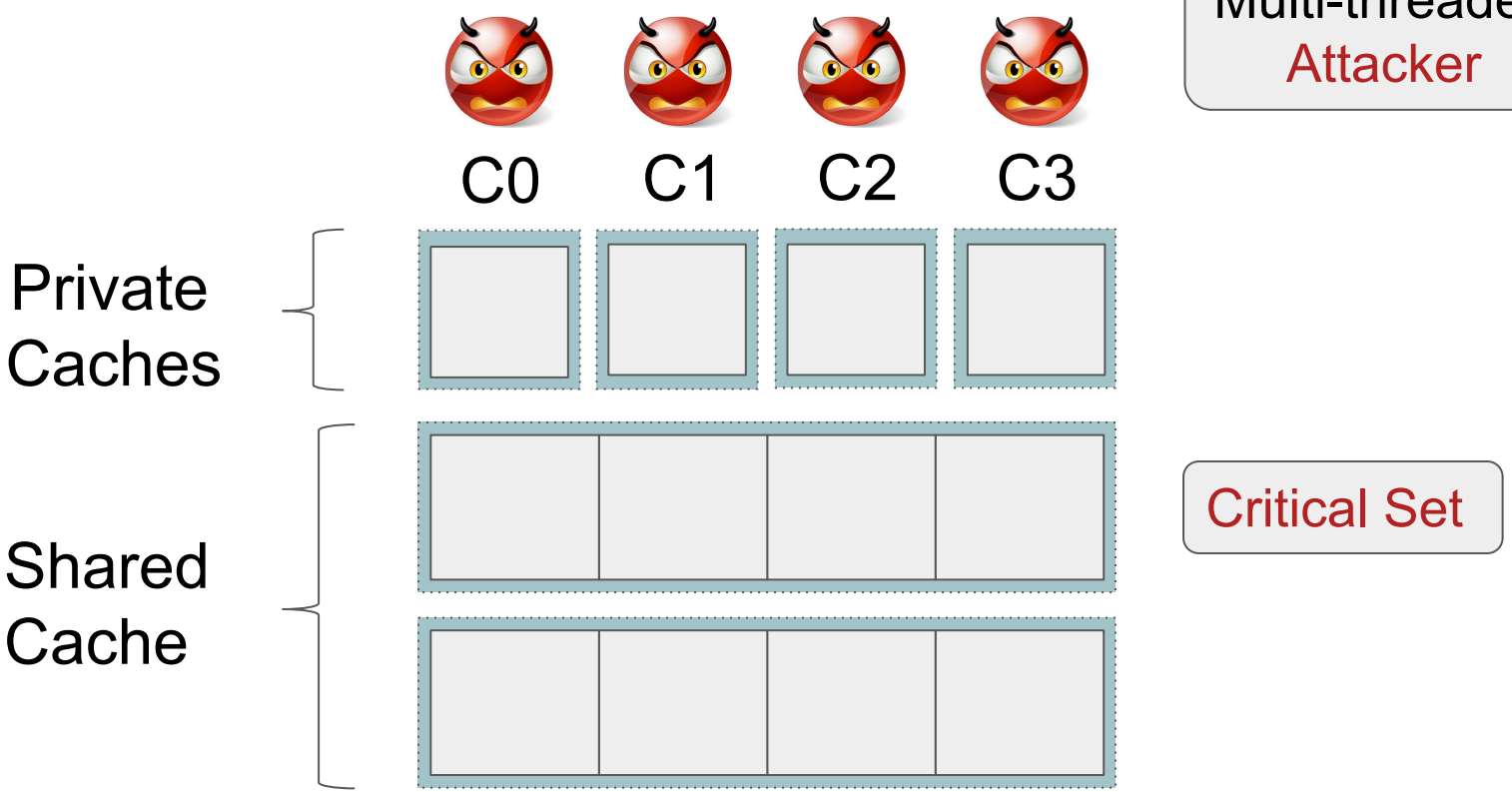
Prime+Reprime+Probe



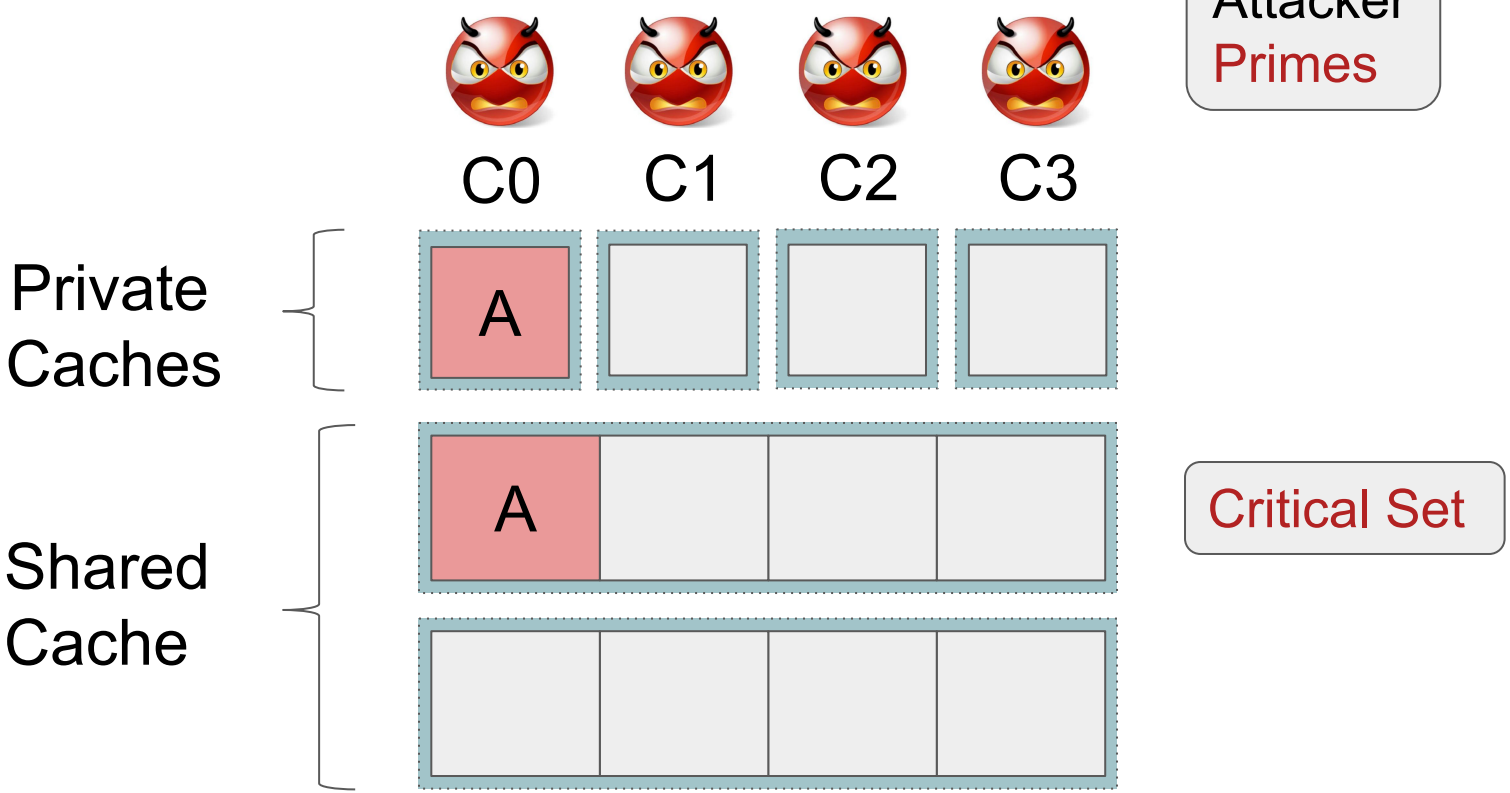
Prime+Reprime+Probe



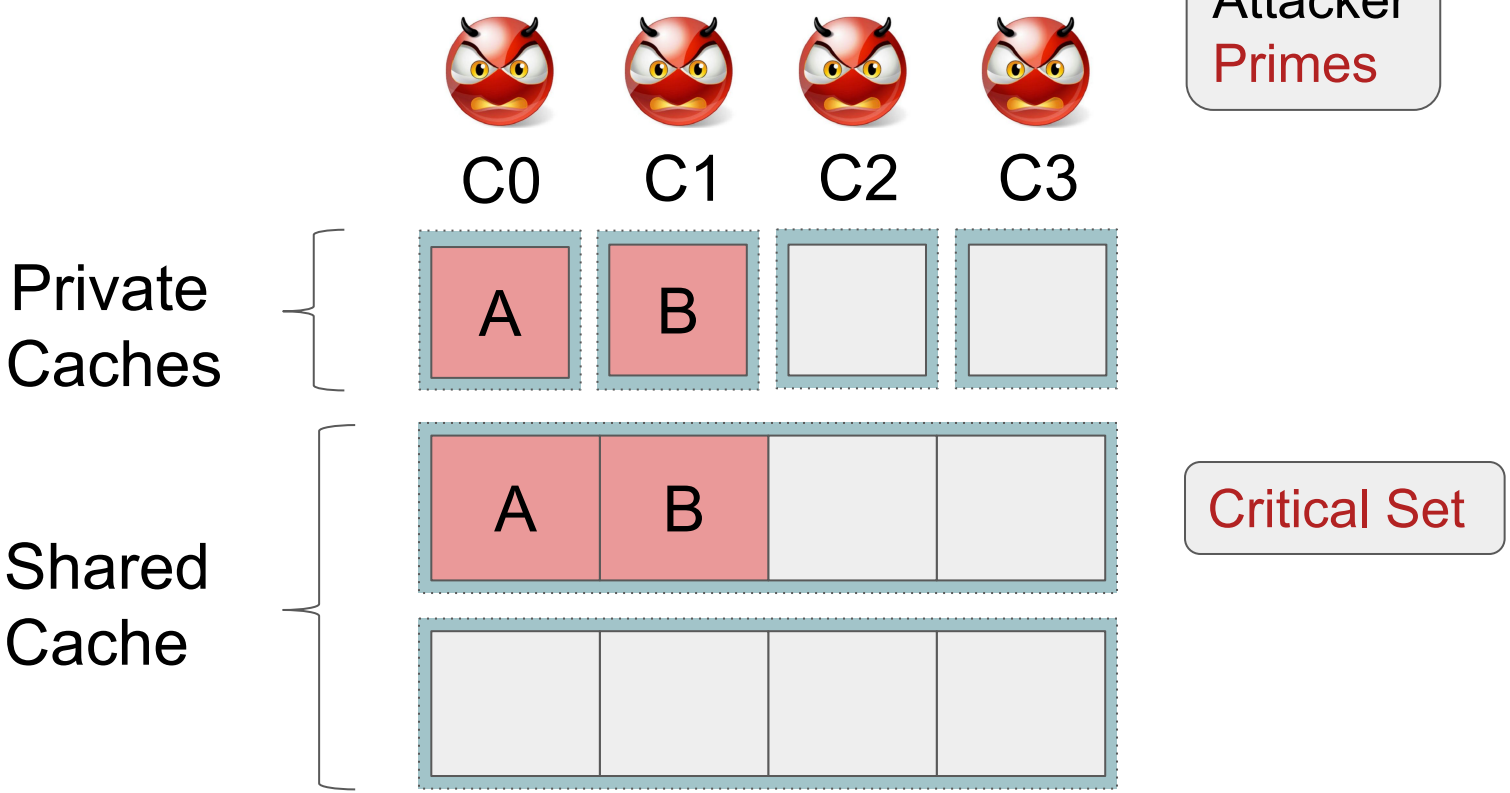
Prime+Reprime+Probe



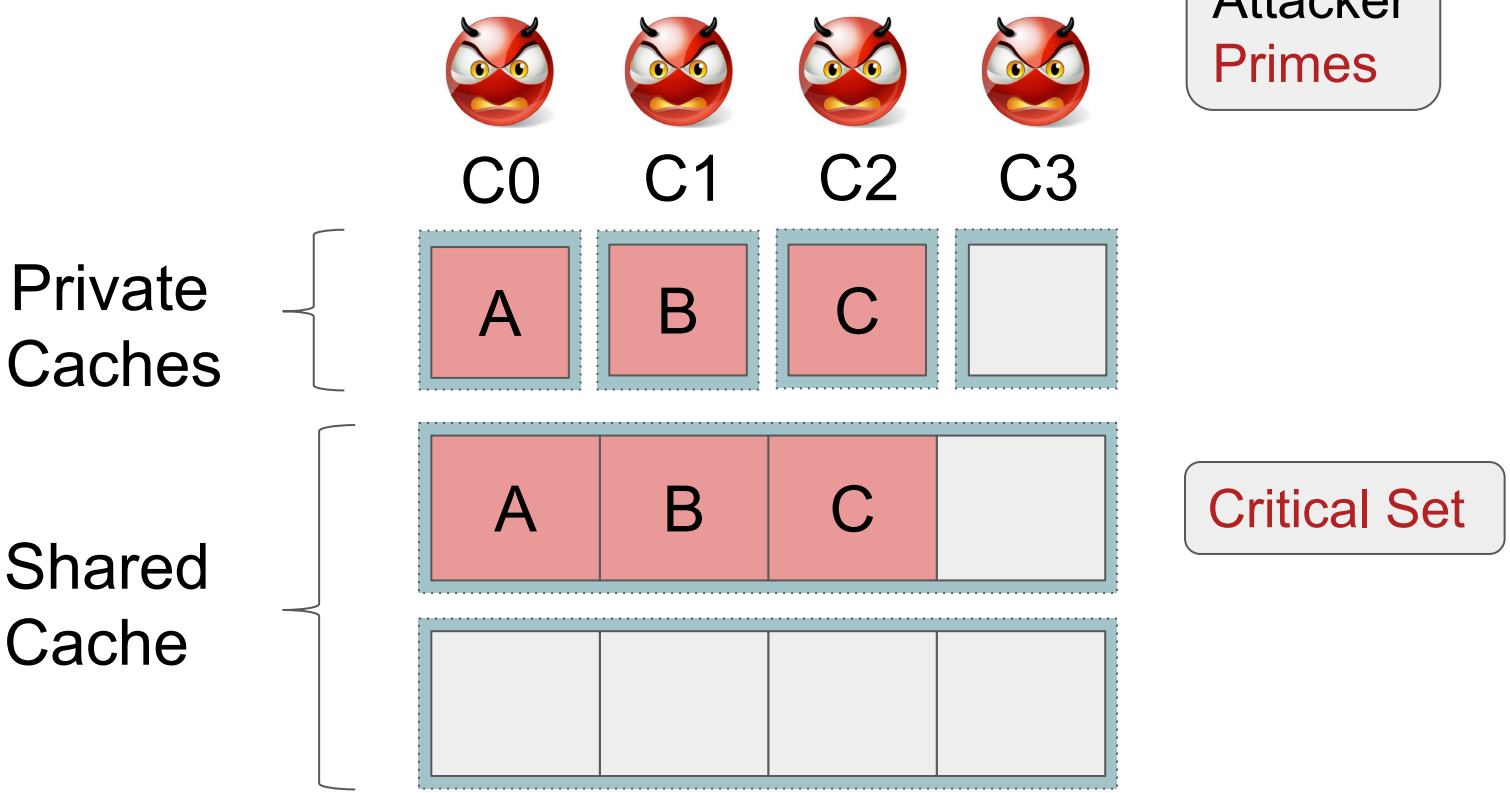
Prime+Reprime+Probe



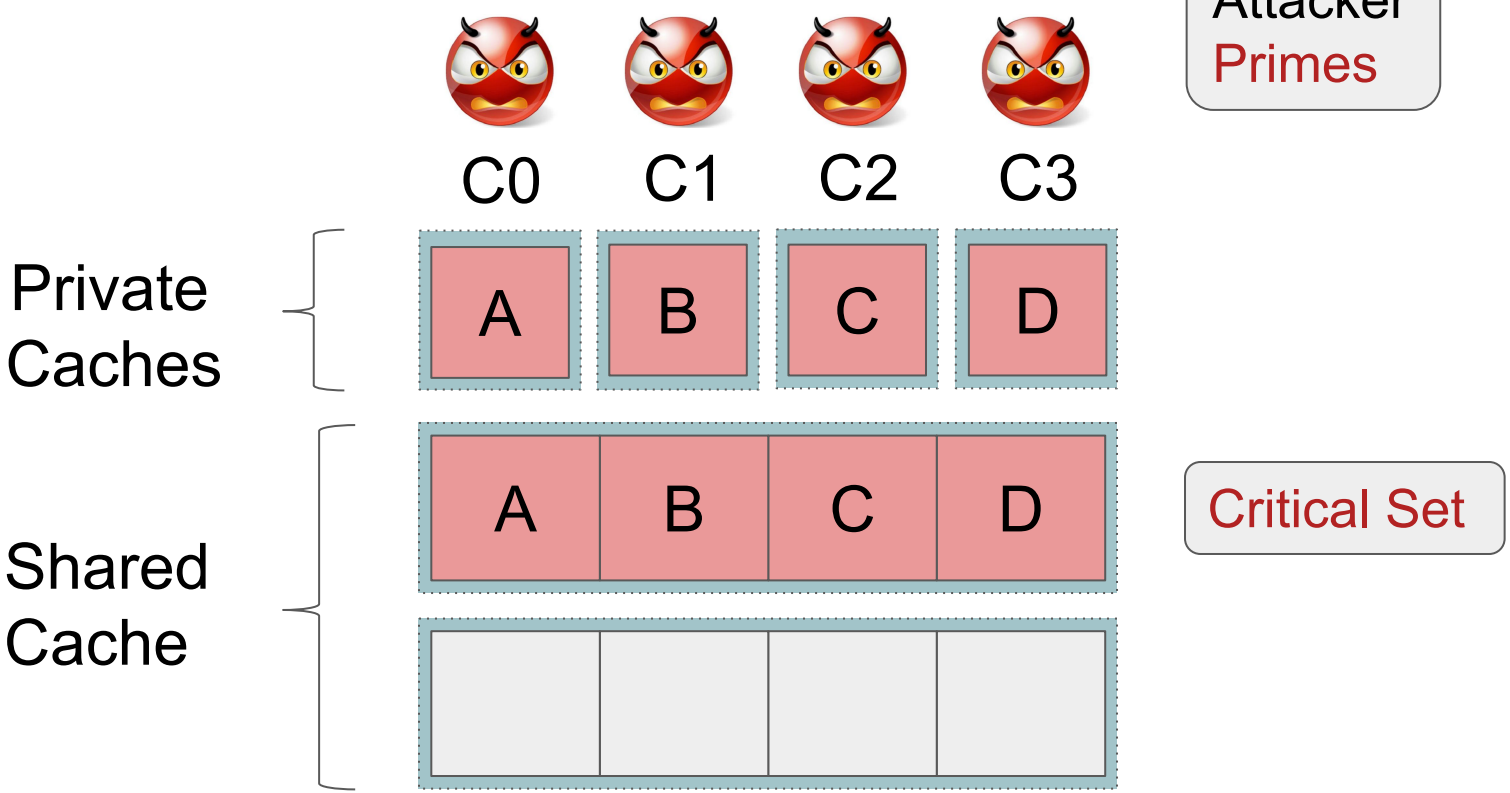
Prime+Reprime+Probe



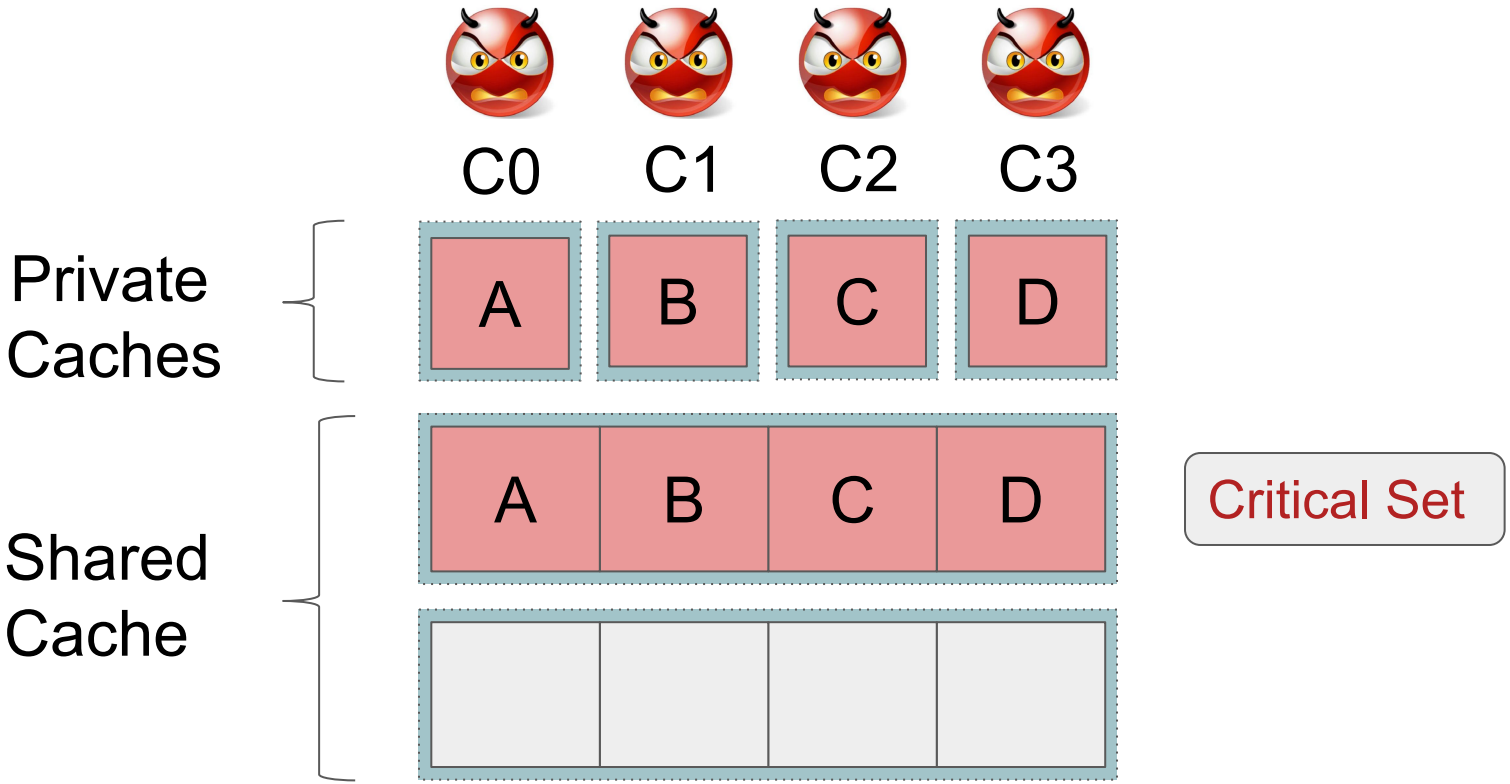
Prime+Reprime+Probe



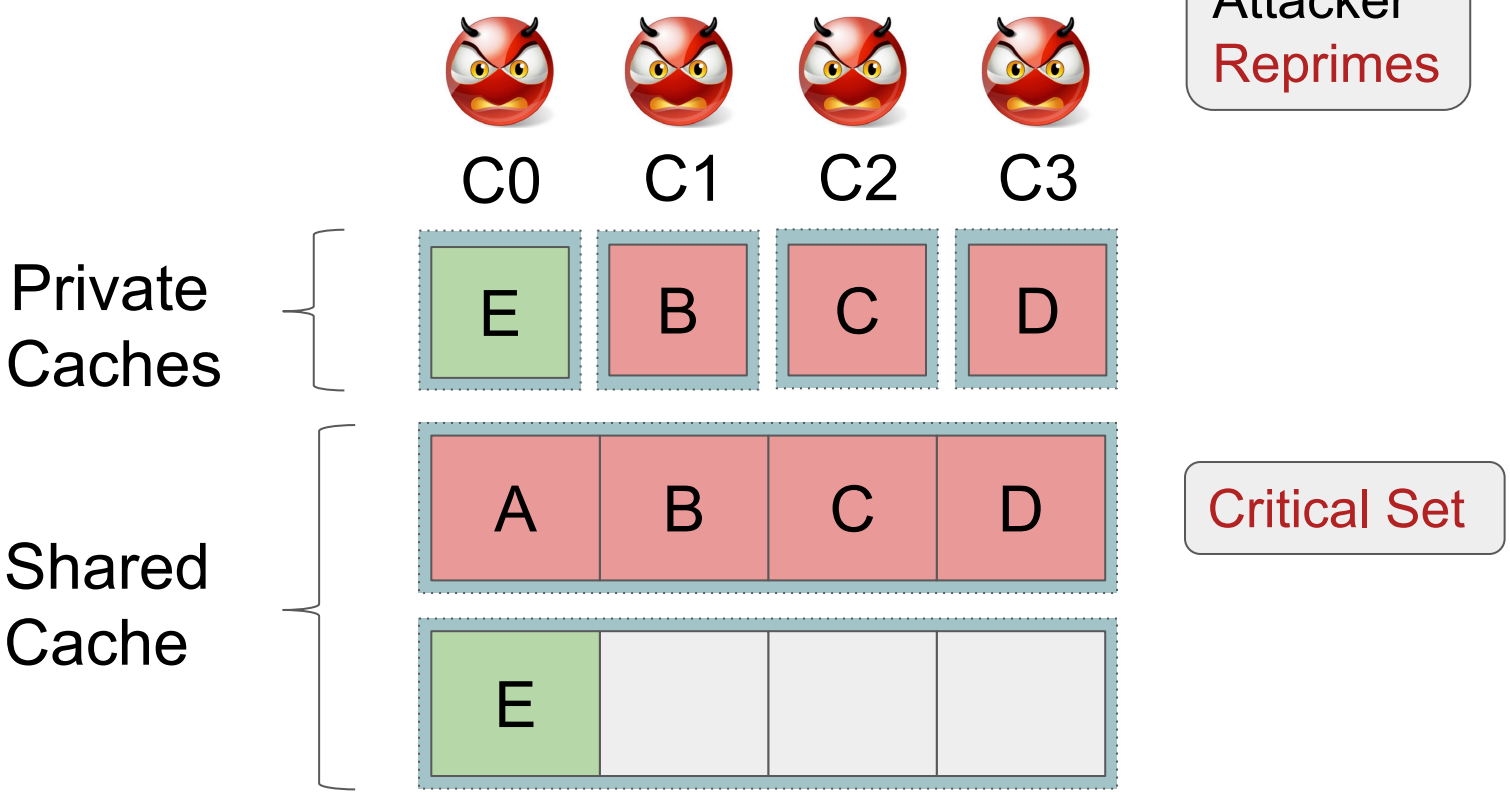
Prime+Reprime+Probe



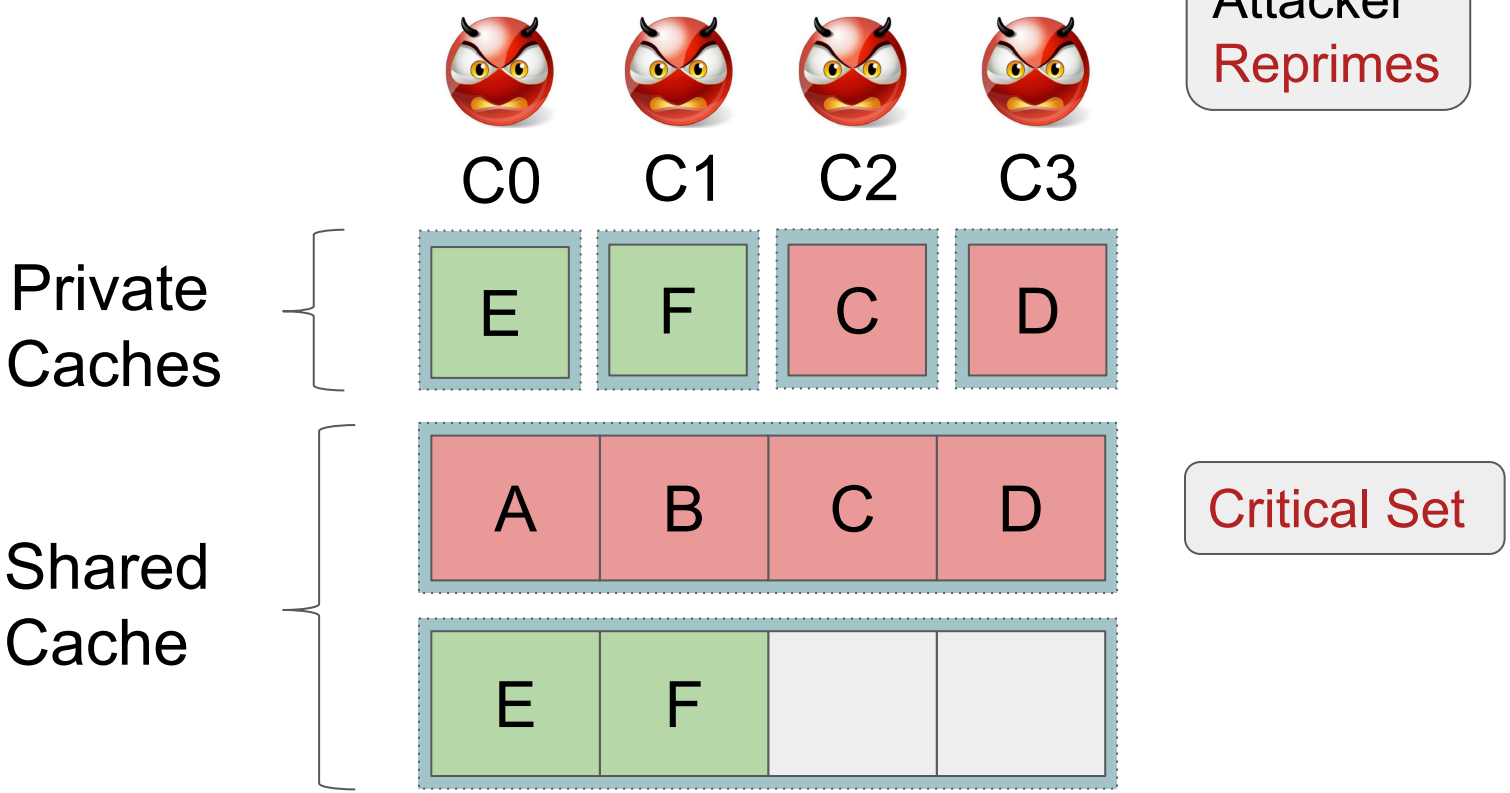
Prime+Reprime+Probe



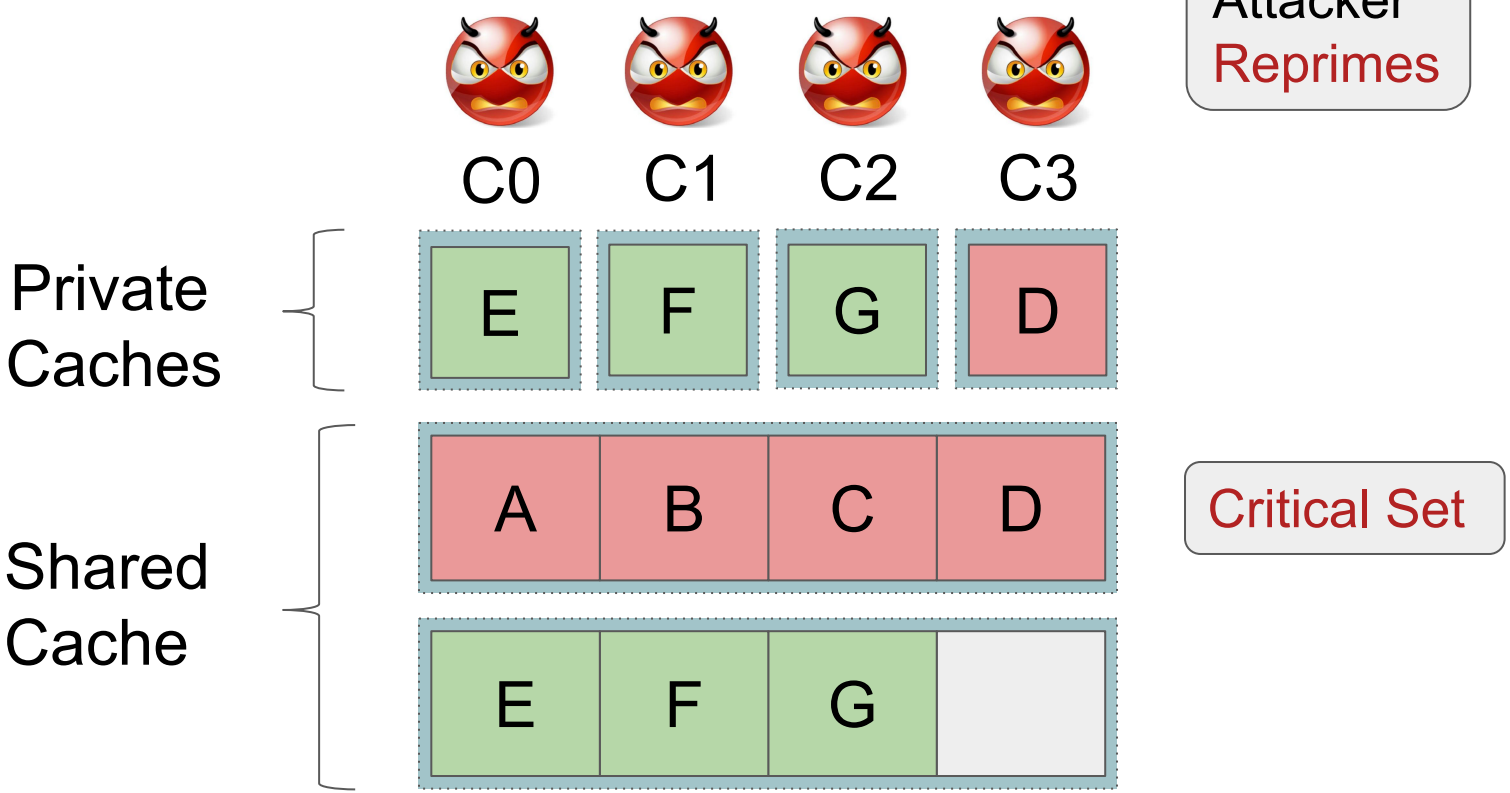
Prime+Reprime+Probe



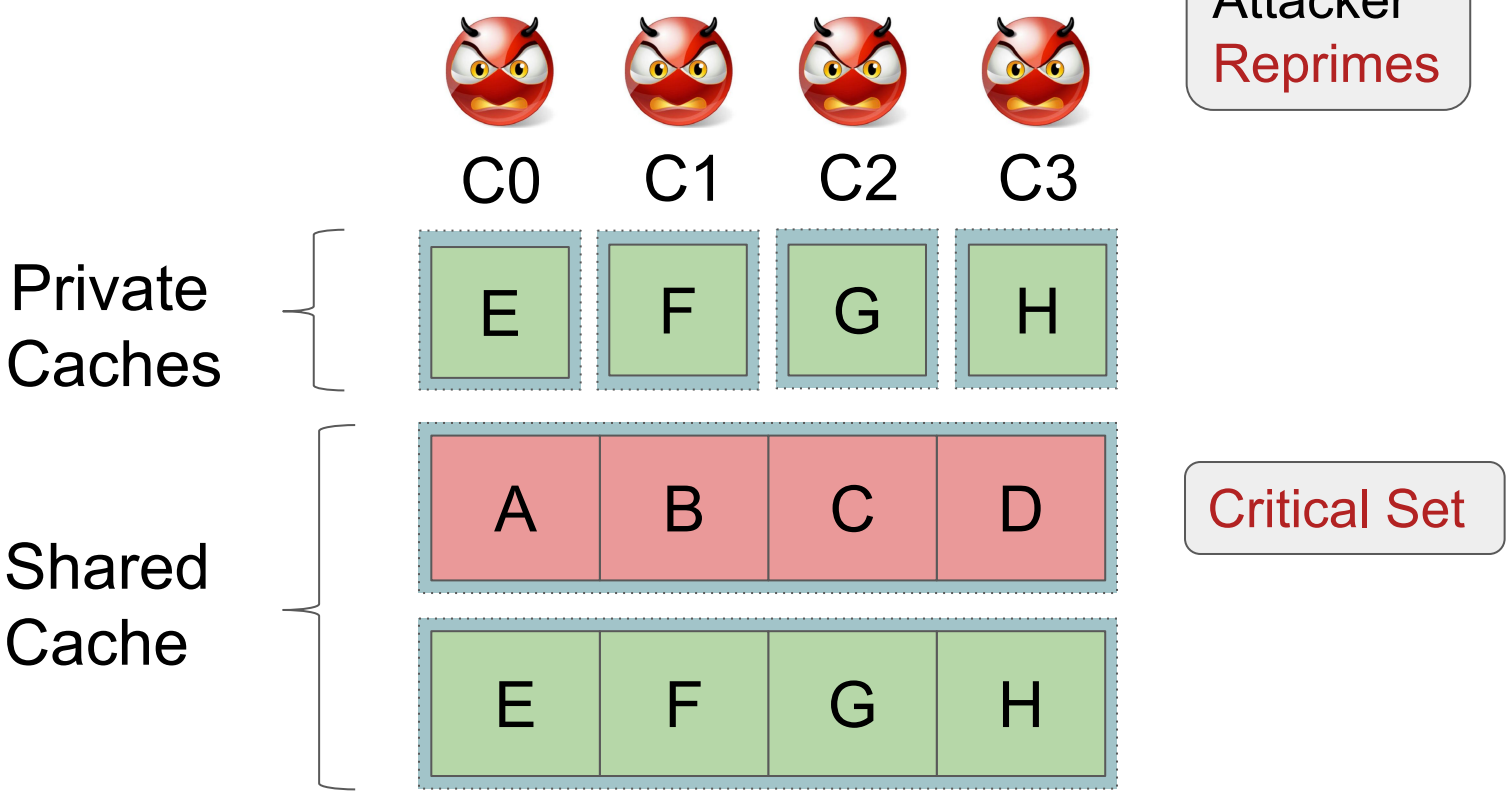
Prime+Reprime+Probe



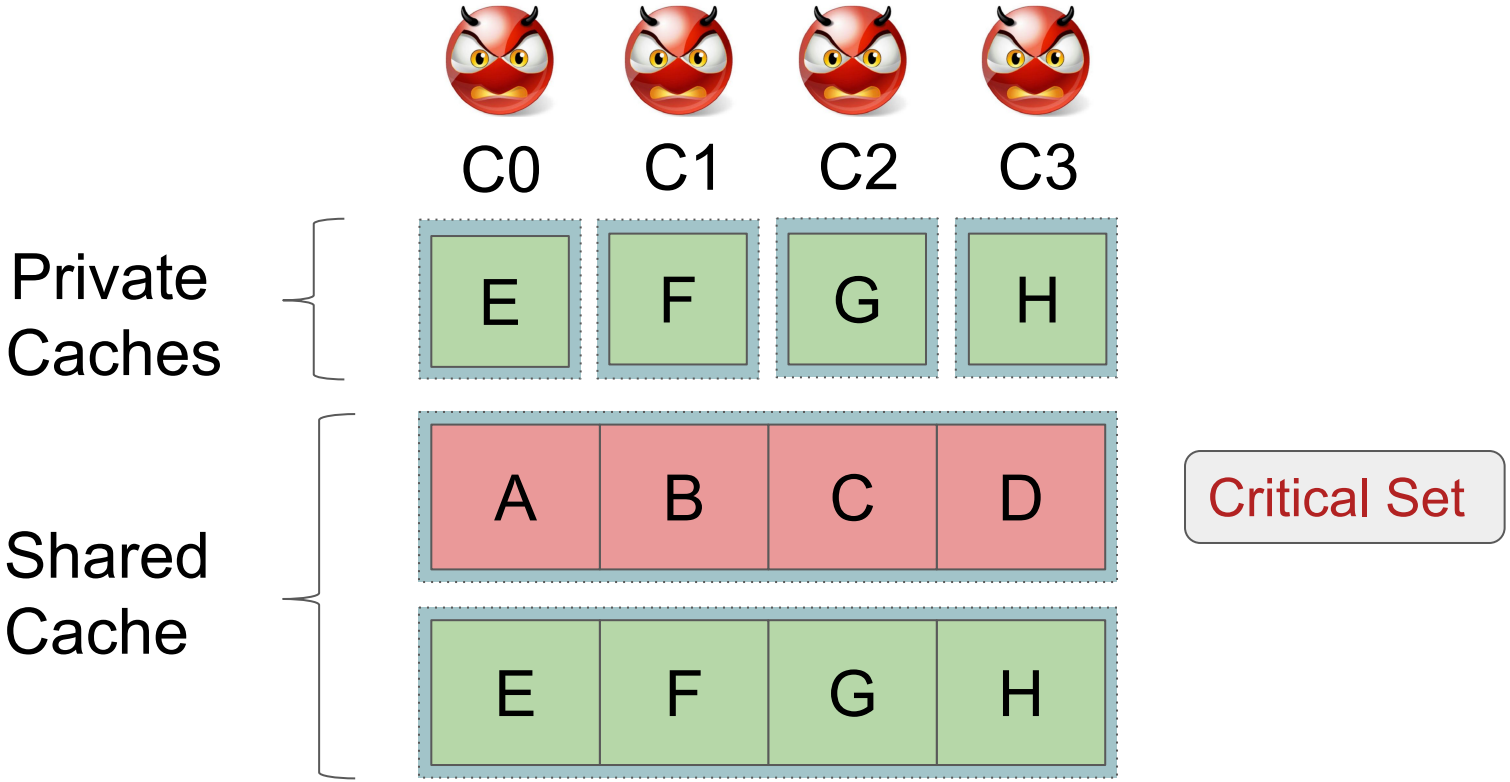
Prime+Reprime+Probe



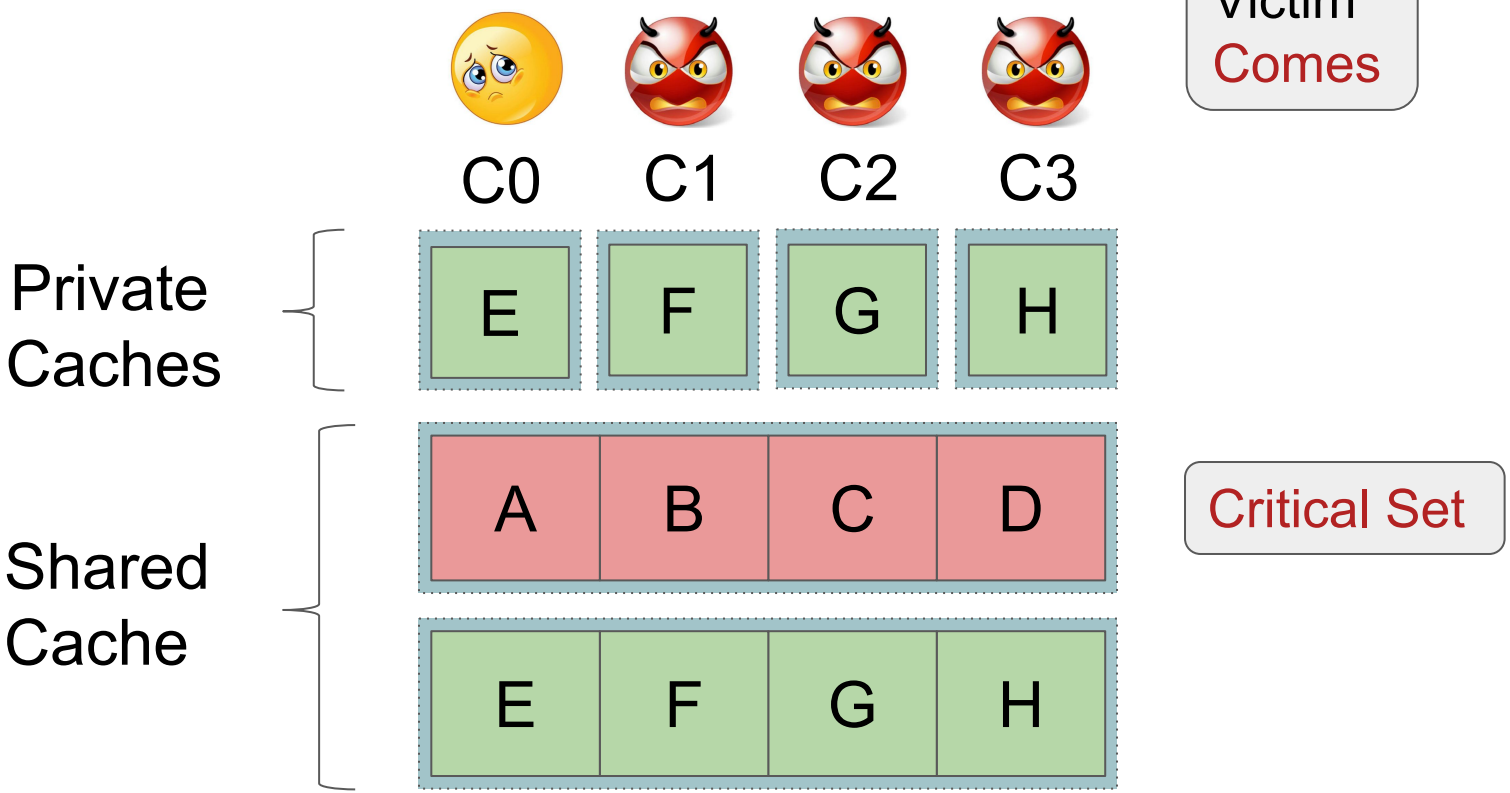
Prime+Reprime+Probe



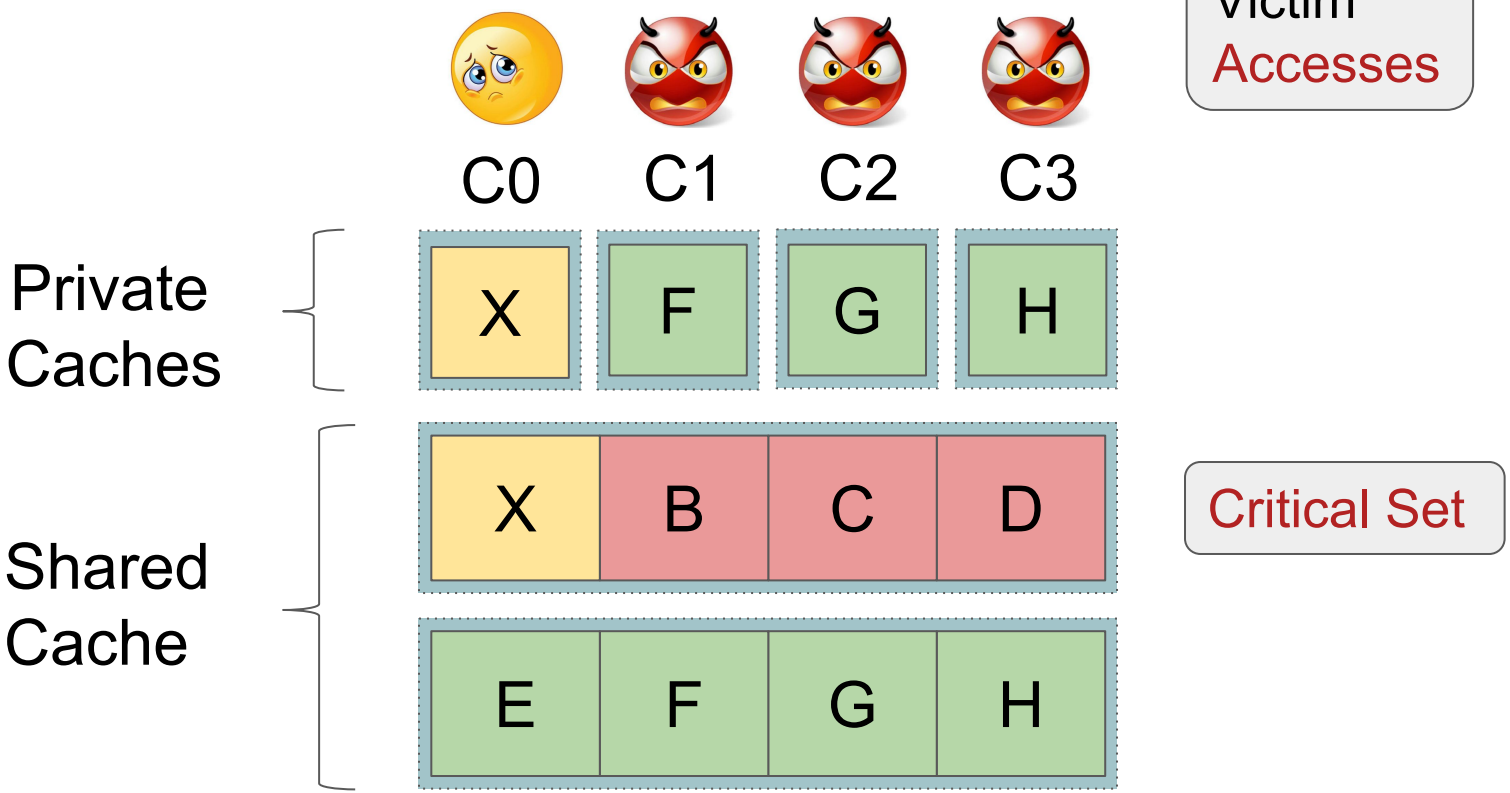
Prime+Reprime+Probe



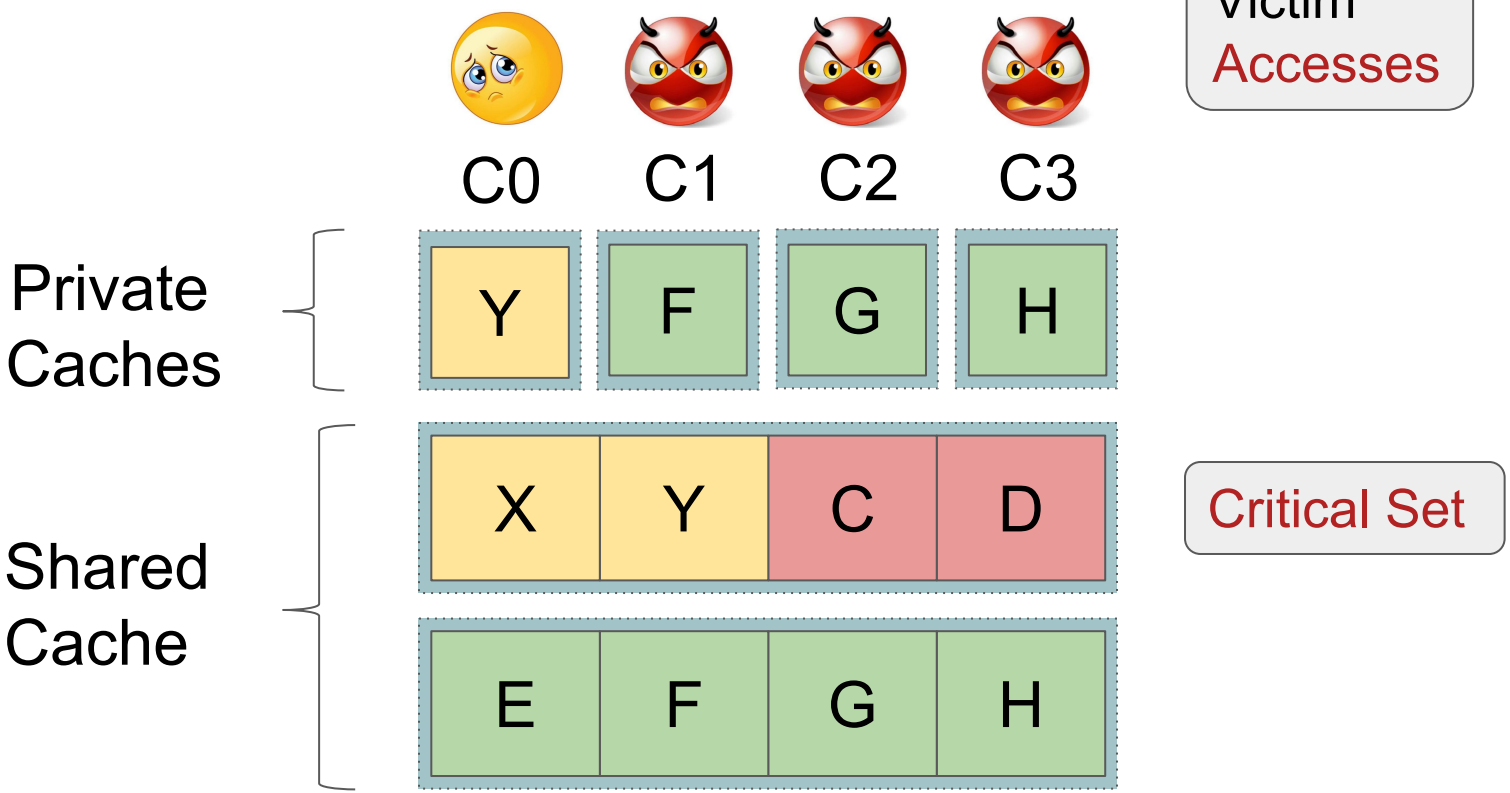
Prime+Reprime+Probe



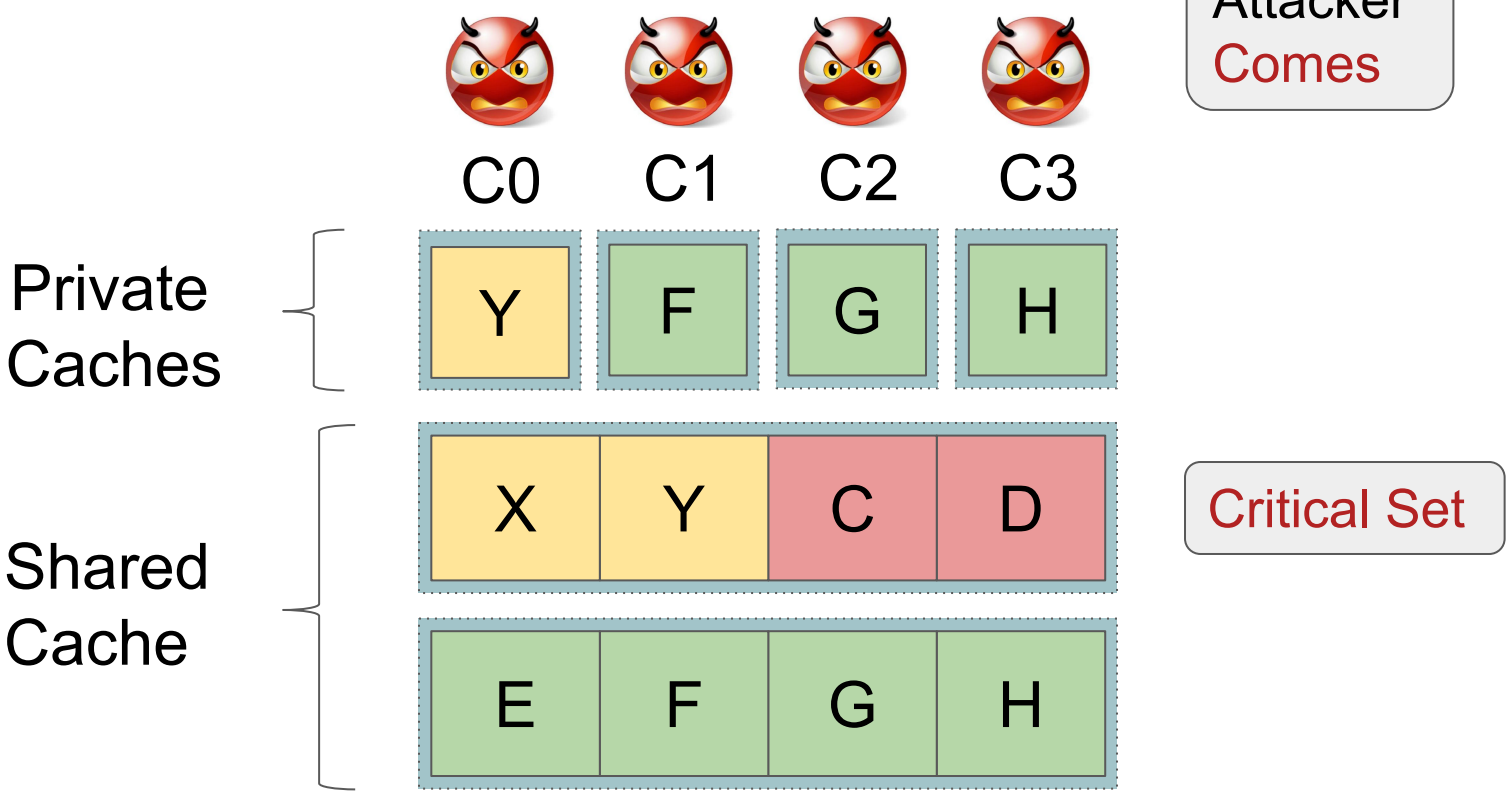
Prime+Reprime+Probe



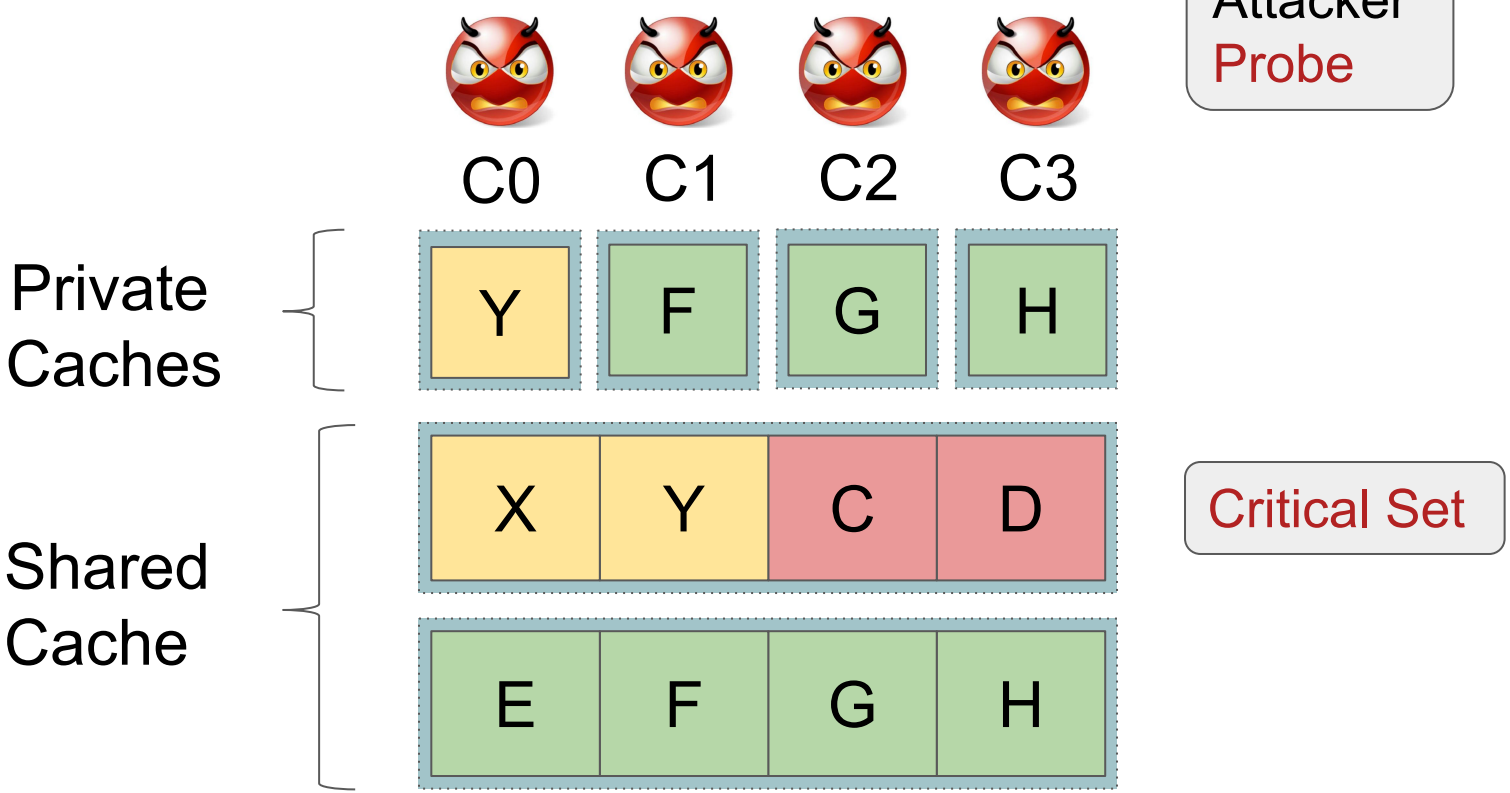
Prime+Reprime+Probe



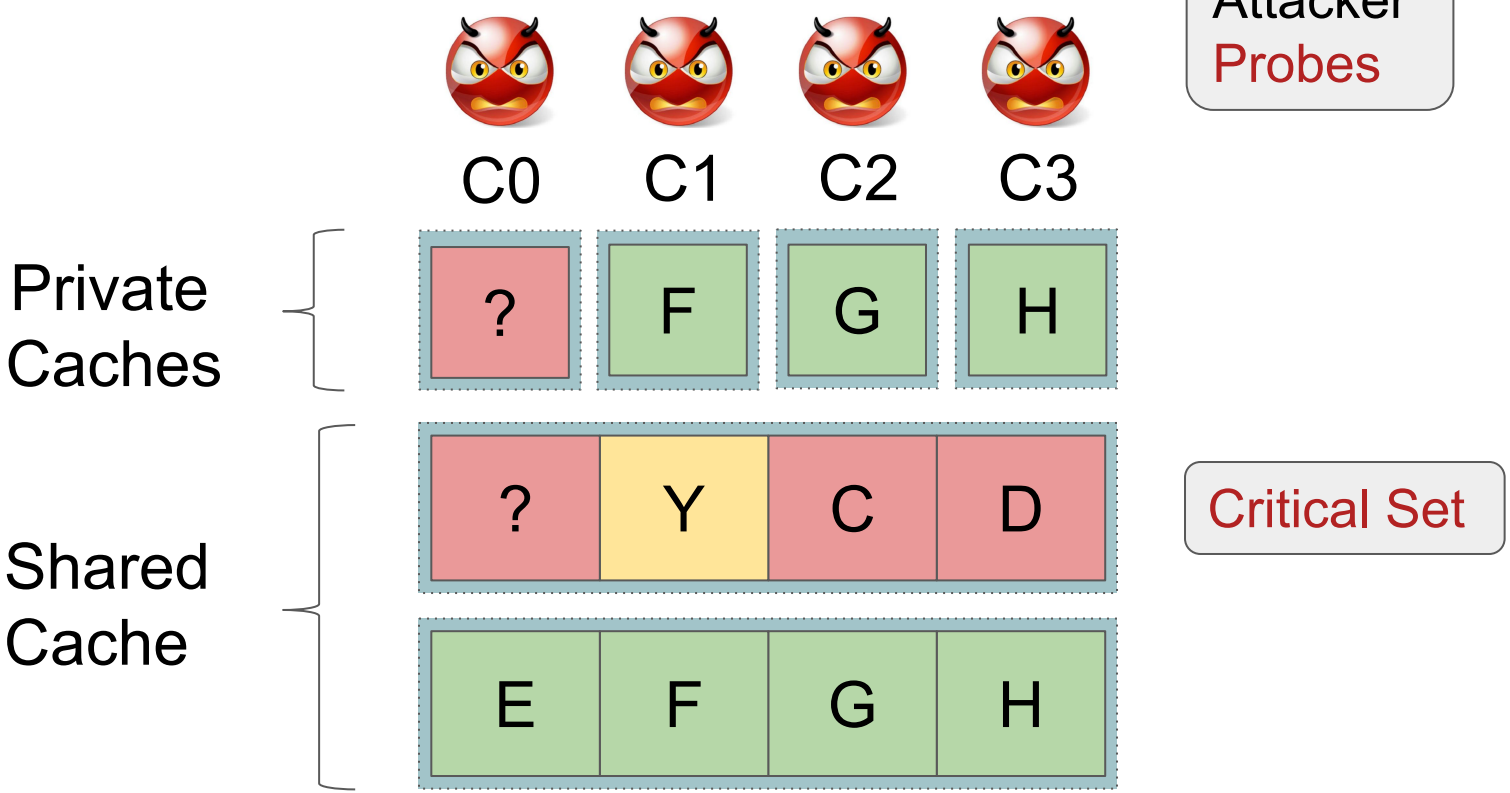
Prime+Reprime+Probe



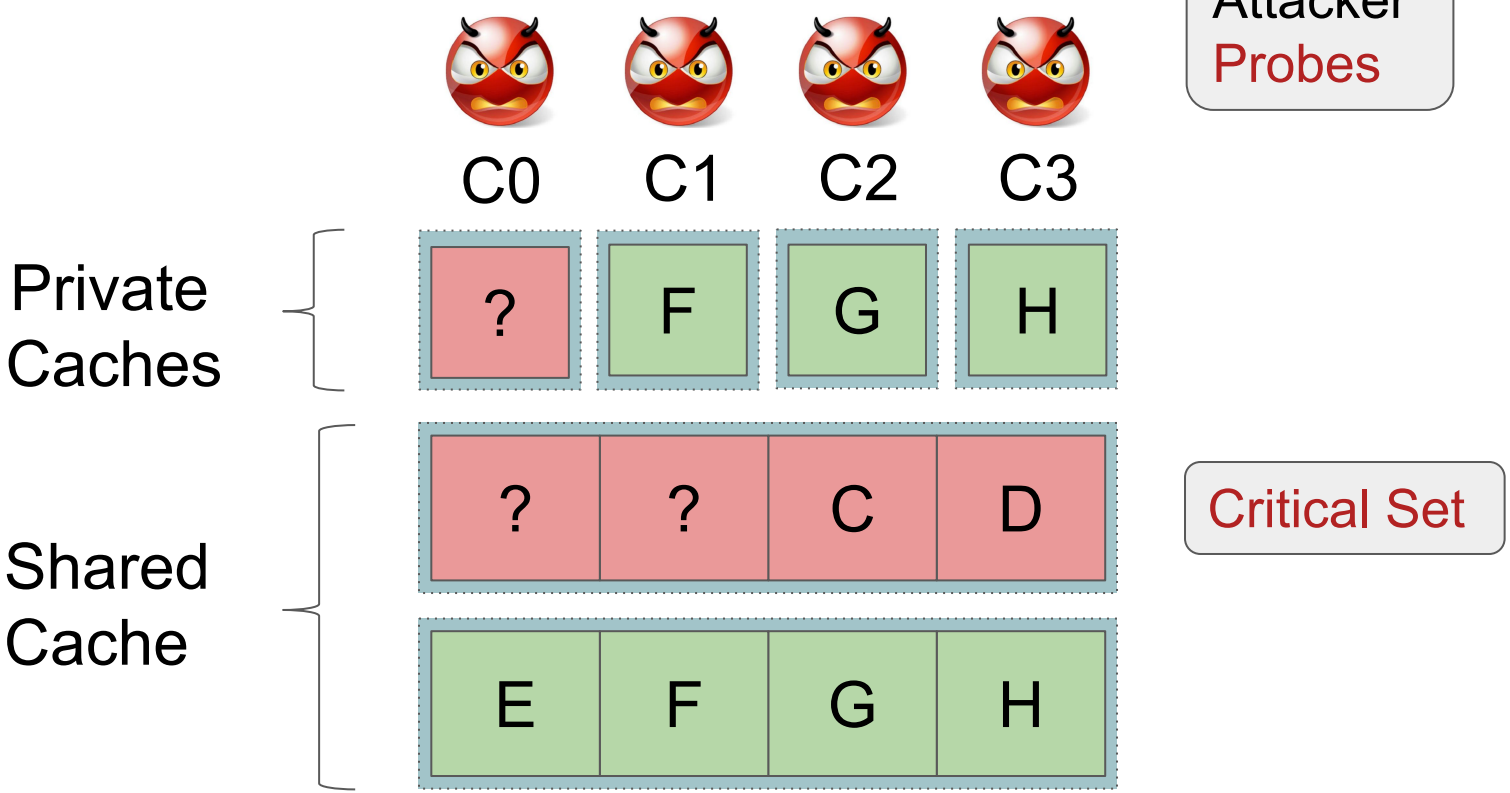
Prime+Reprime+Probe



Prime+Reprime+Probe



Prime+Reprime+Probe



Questions That We Ask?

Does SHARP mitigate all attacks?

No ☹

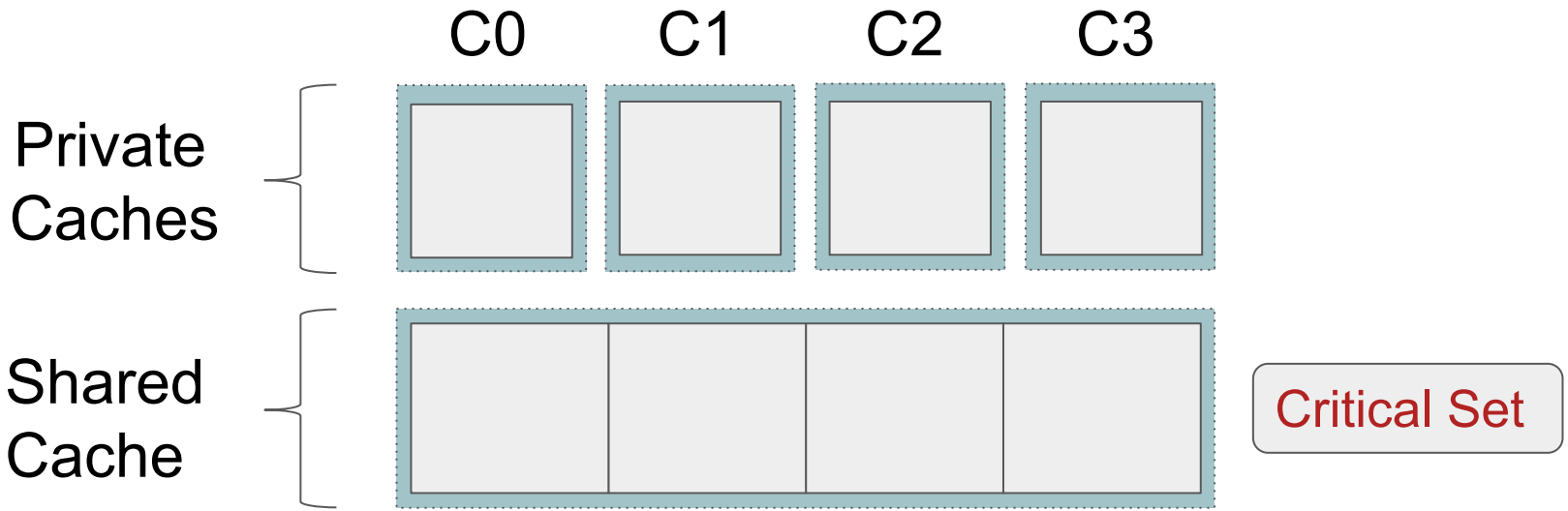
Questions That We Ask?

Does SHARP mitigate all attacks?

No ☹️

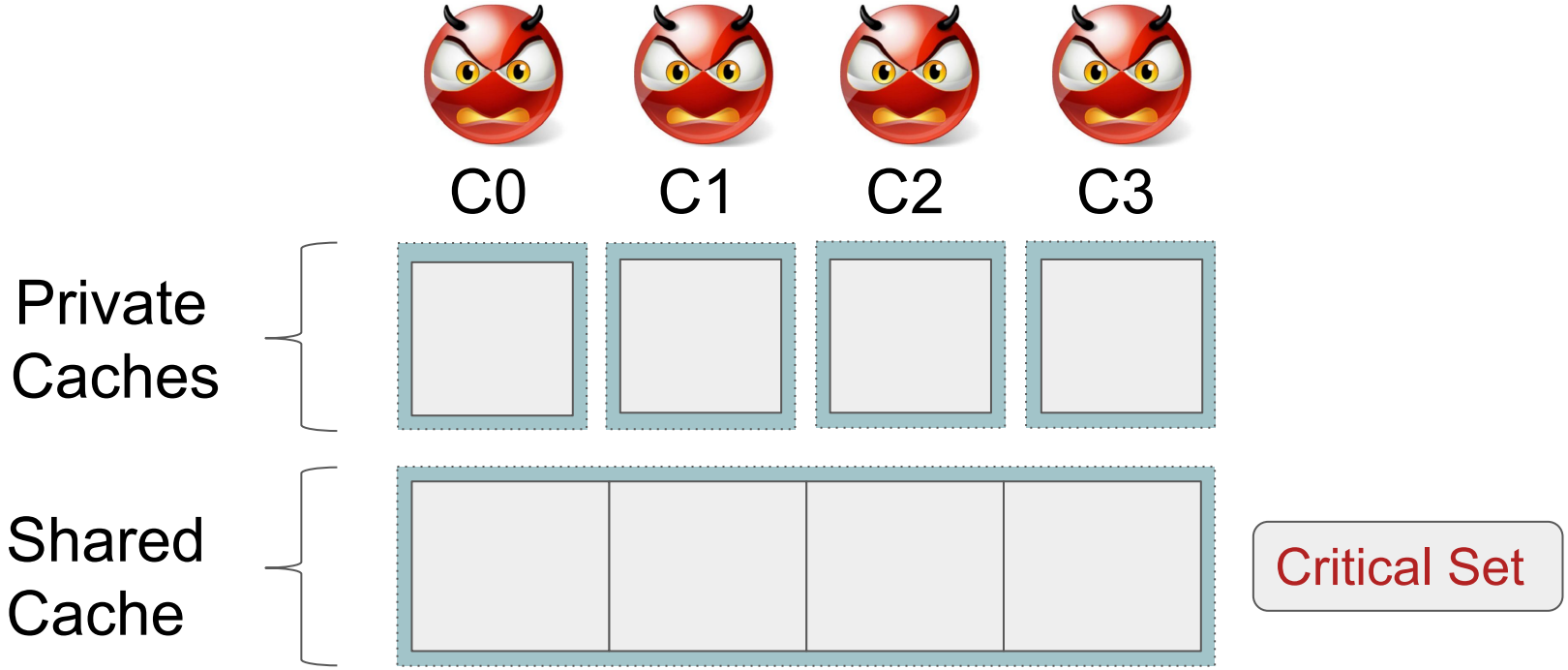
Does SHARP facilitate few more attacks?

Denial of Service Attack

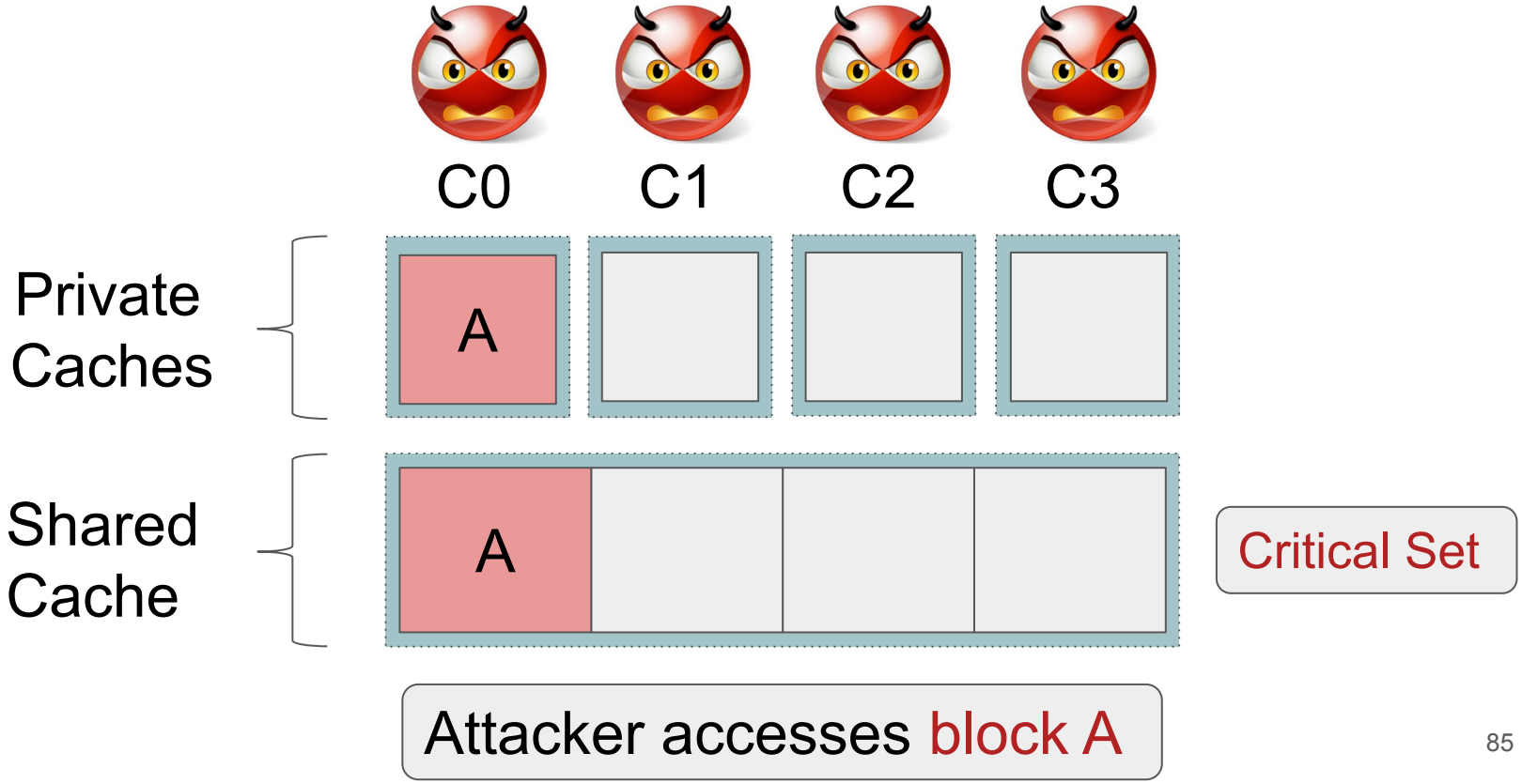


Denial of Service Attack

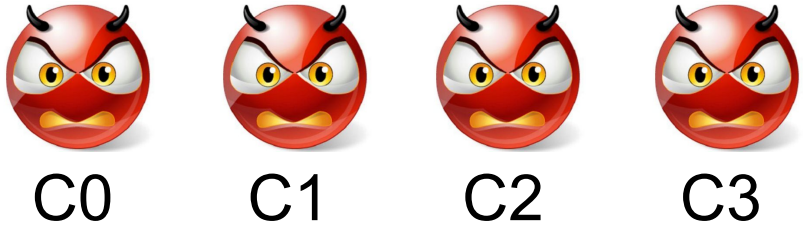
Multi-threaded Attacker



Denial of Service Attack

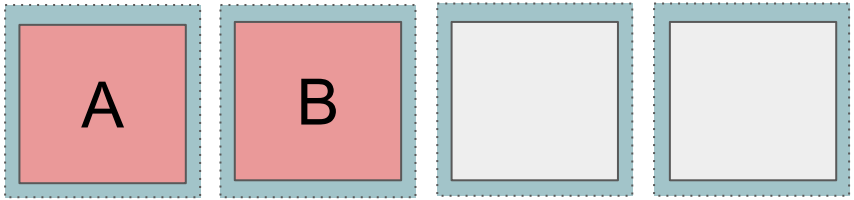


Denial of Service Attack

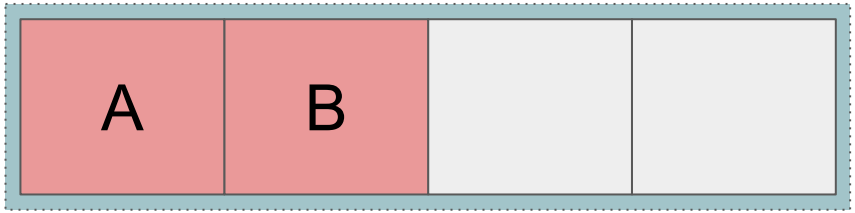


C0 C1 C2 C3

Private Caches



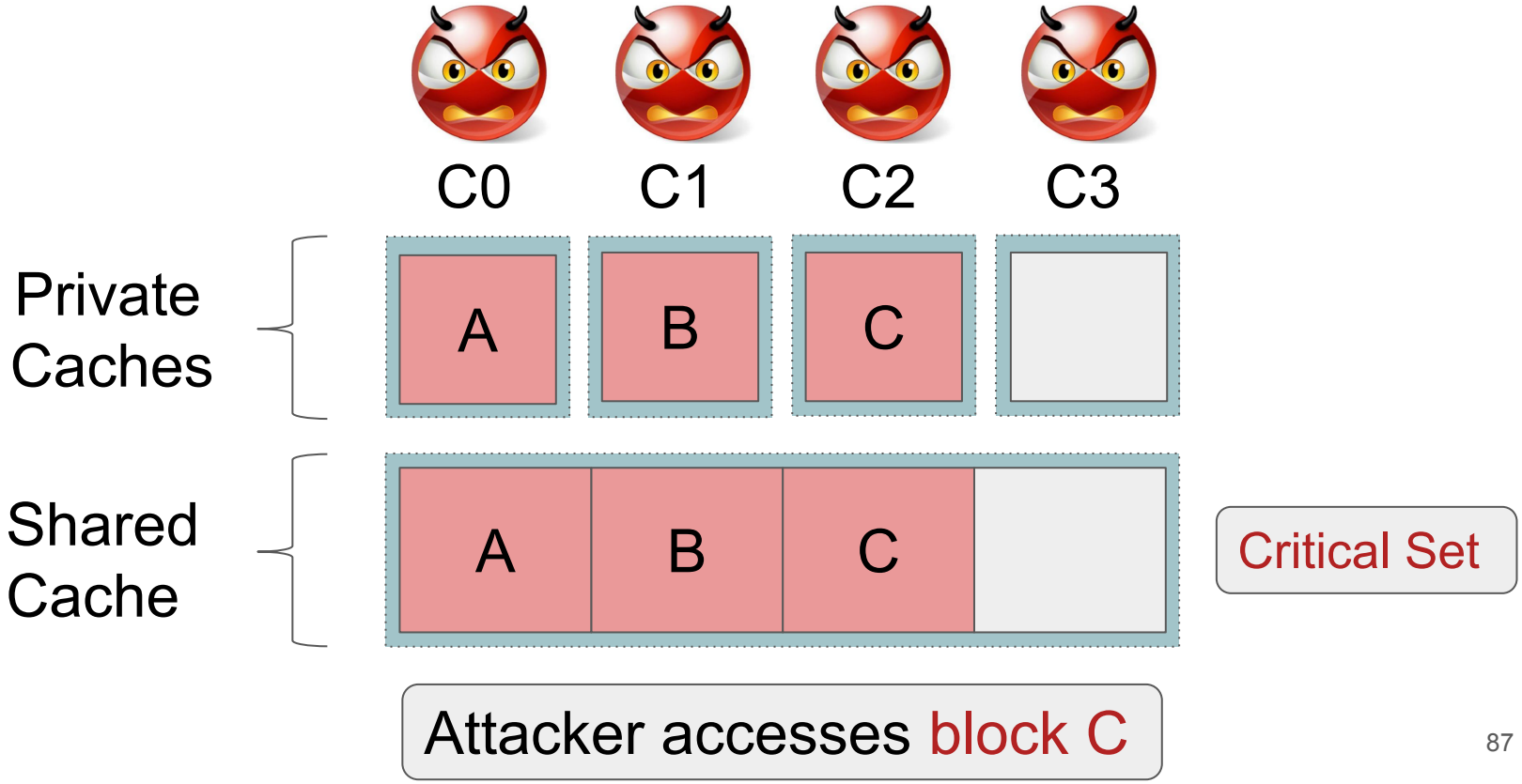
Shared Cache



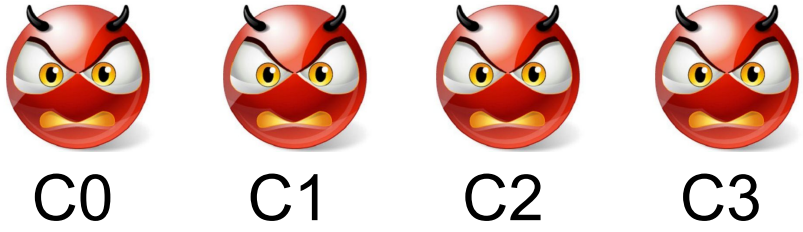
Critical Set

Attacker accesses block B

Denial of Service Attack



Denial of Service Attack



C0 C1 C2 C3

Private Caches

A B C D

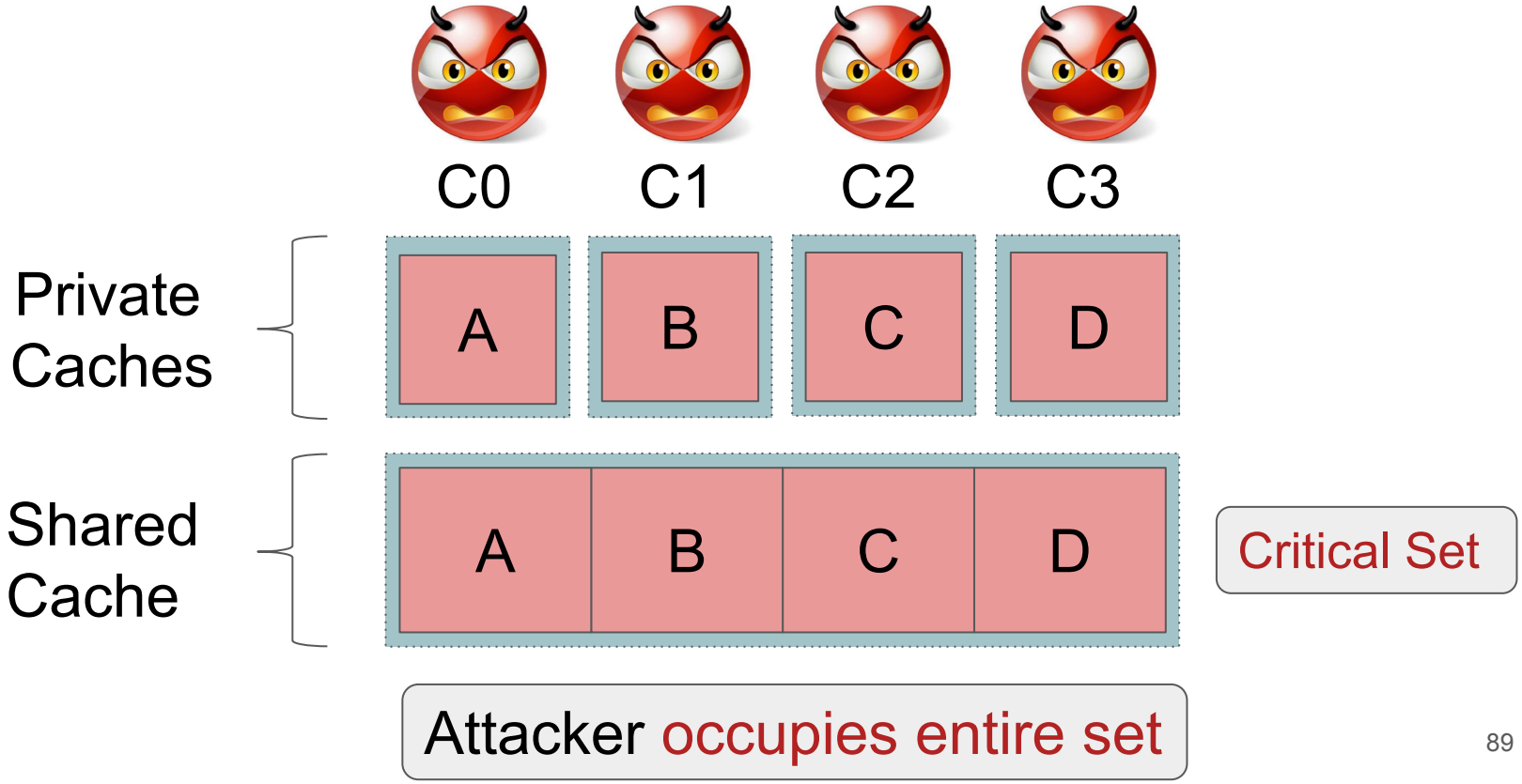
Shared Cache

A B C D

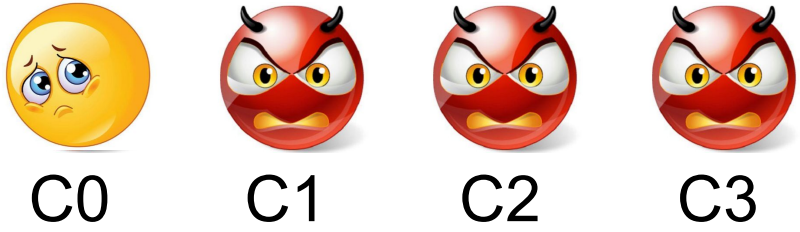
Critical Set

Attacker accesses block D

Denial of Service Attack



Denial of Service Attack



C0 C1 C2 C3

Private Caches

A B C D

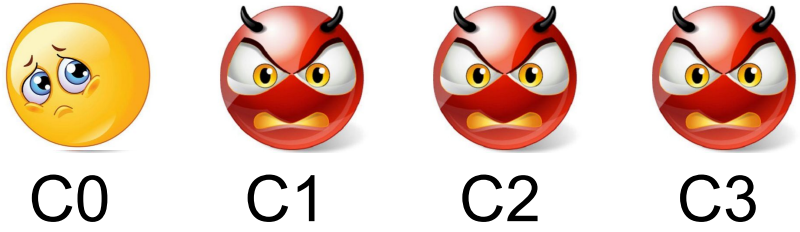
Shared Cache

A B C D

Critical Set

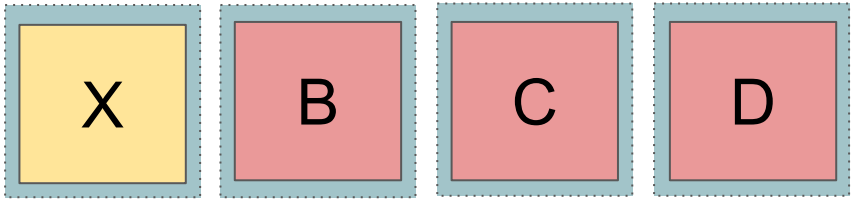
Victim comes

Denial of Service Attack

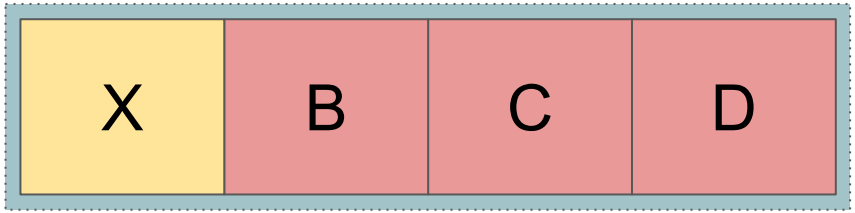


C0 C1 C2 C3

Private Caches



Shared Cache



Critical Set

Victim accesses block X

Denial of Service Attack

C0 C1 C2 C3

Private Caches

Y B C D

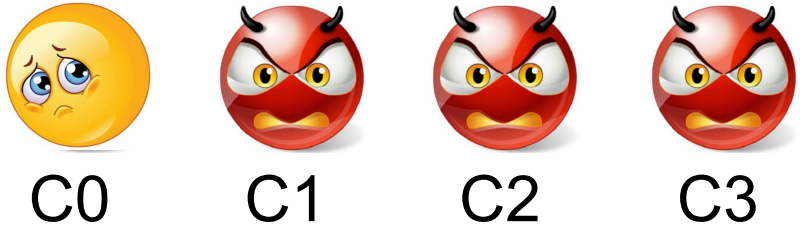
Shared Cache

Y B C D

Critical Set

Victim accesses block Y

Denial of Service Attack



C0 C1 C2 C3

Private Caches

Z B C D

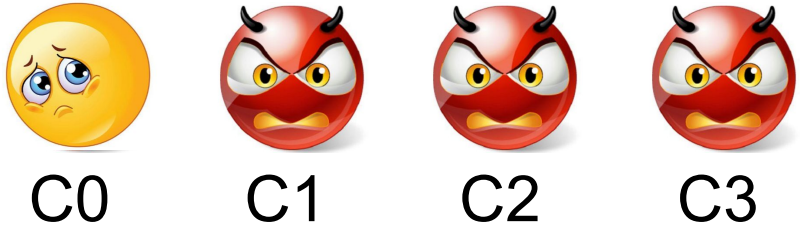
Shared Cache

Z B C D

Critical Set

Victim accesses block Z

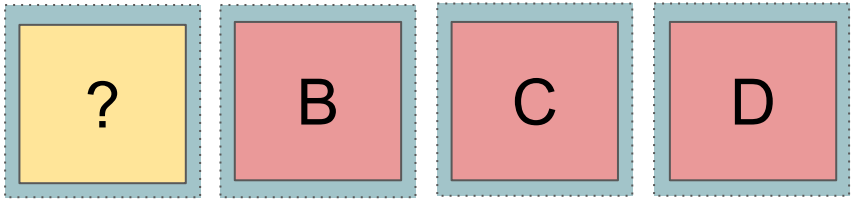
Denial of Service Attack

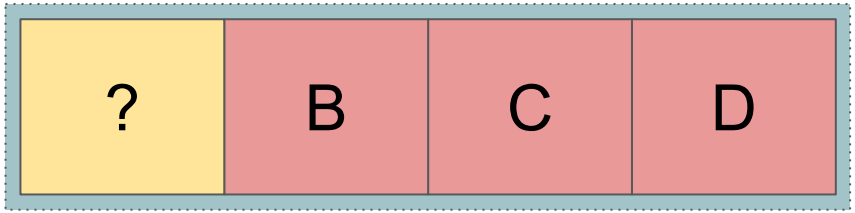


C0 C1 C2 C3

Private Caches

Shared Cache





Critical Set

Victim strives for other ways

Questions That We Ask?

Does SHARP mitigate all attacks?

No ☹

Does SHARP facilitate few more attacks?

Yes ☹

Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications?

Simulation

Simulation

ChampSim, a trace driven simulator

Simulation

ChampSim, a trace driven simulator

Simulated SHARP on a 16-core system with three levels of caches and huge pages

Simulation

ChampSim, a trace driven simulator

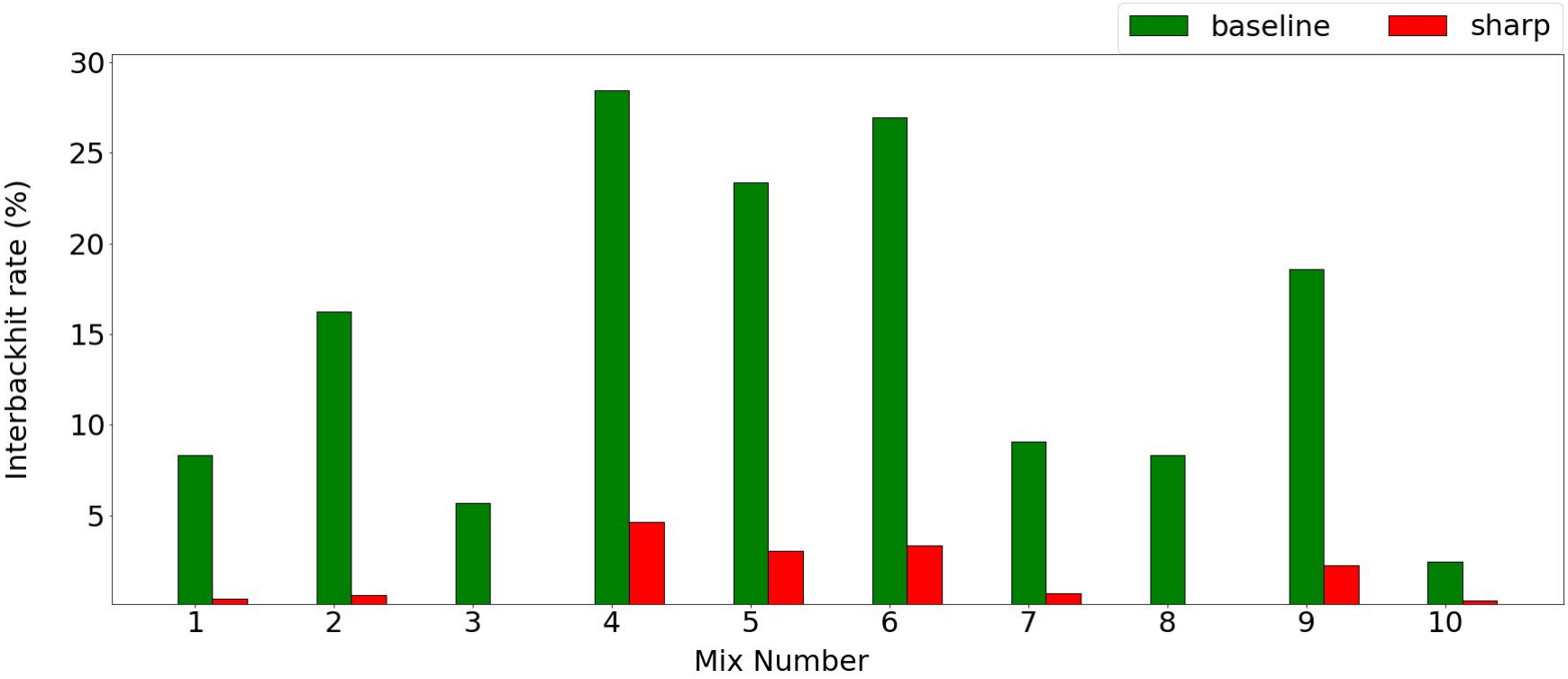
Simulated SHARP on a 16-core system with three levels of caches and huge pages

Used different combinations of LLC thrashing and LLC fitting applications
Example, 16:0 denotes 16 thrashing and zero fitting

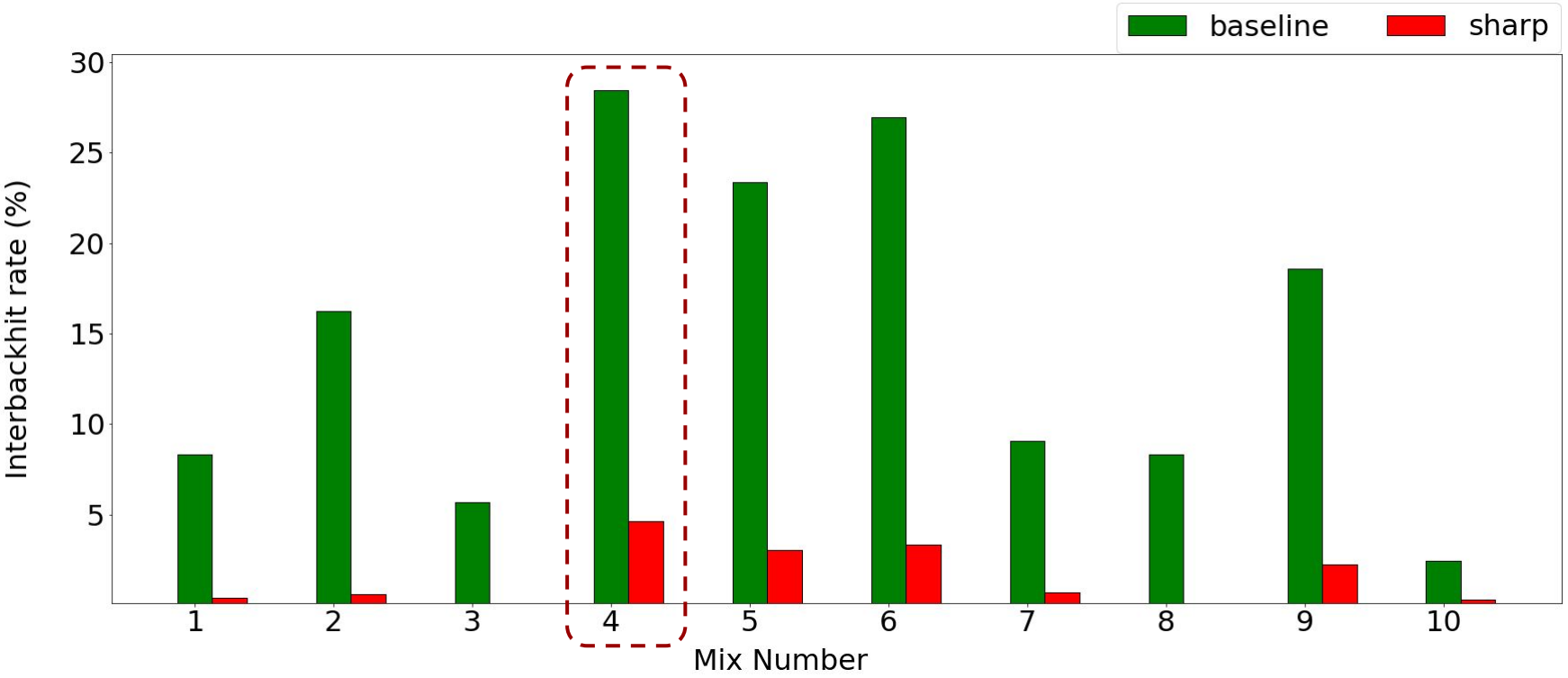
LLC Thrashing Benchmarks [SPEC CPU 2017]

Mix No	Thrashing Benchmarks
1	605.mcf-484B
2	605.mcf-665B
3	605.mcf-994B
4	607.cactubssn-2421B
5	620.omnetpp-141B
6	620.omnetpp-874B
7	621.wrf-6673B
8	623.xalancbmk-10B
9	649.fotonik-10881B
10	654.roms-523B

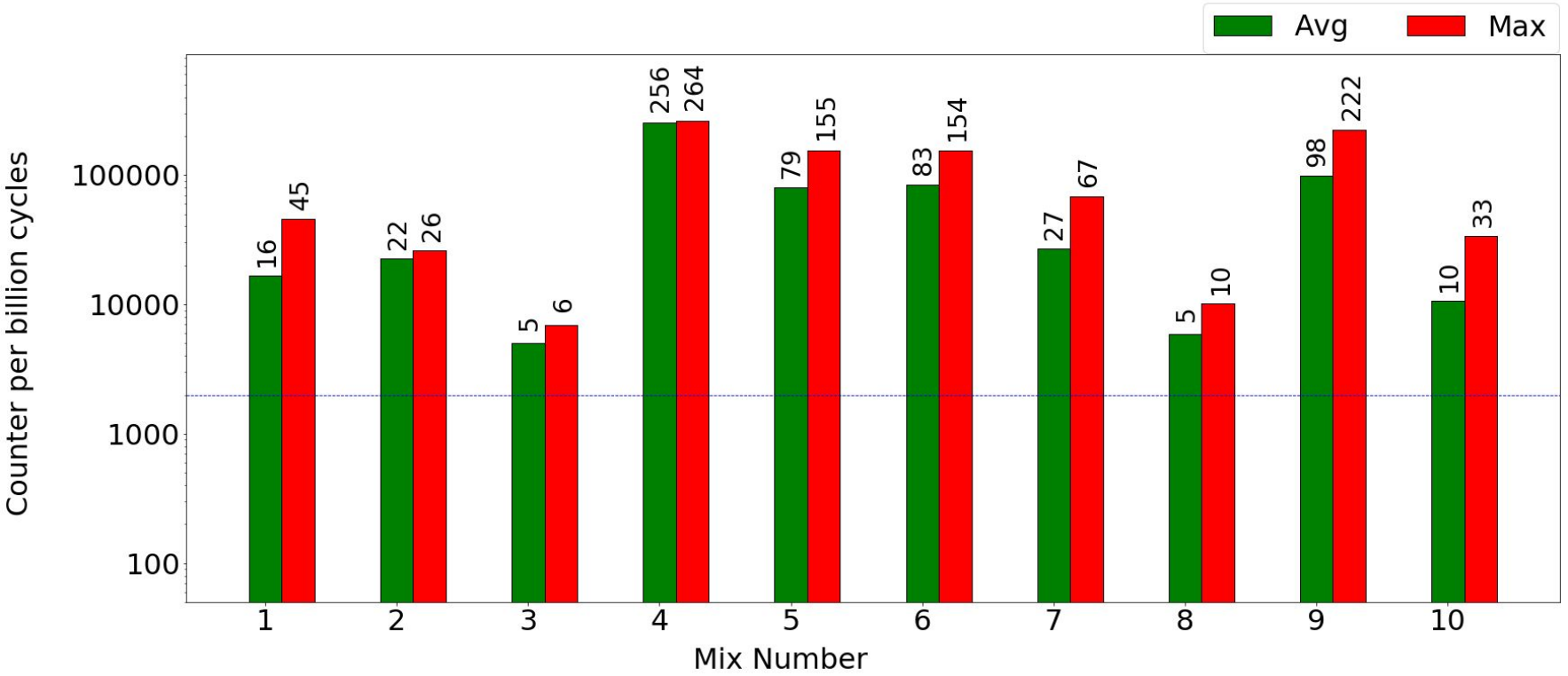
Interbackhit Rate



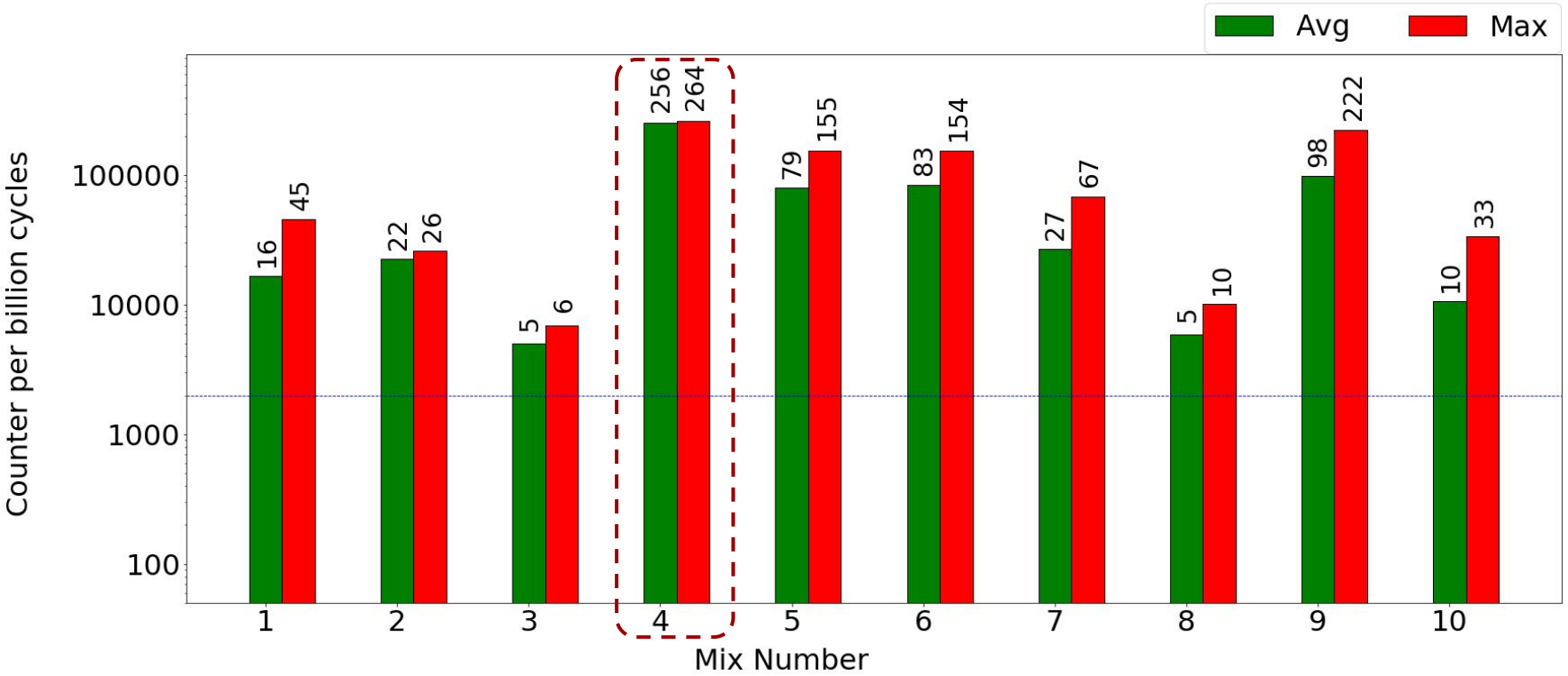
Interbackhit Rate



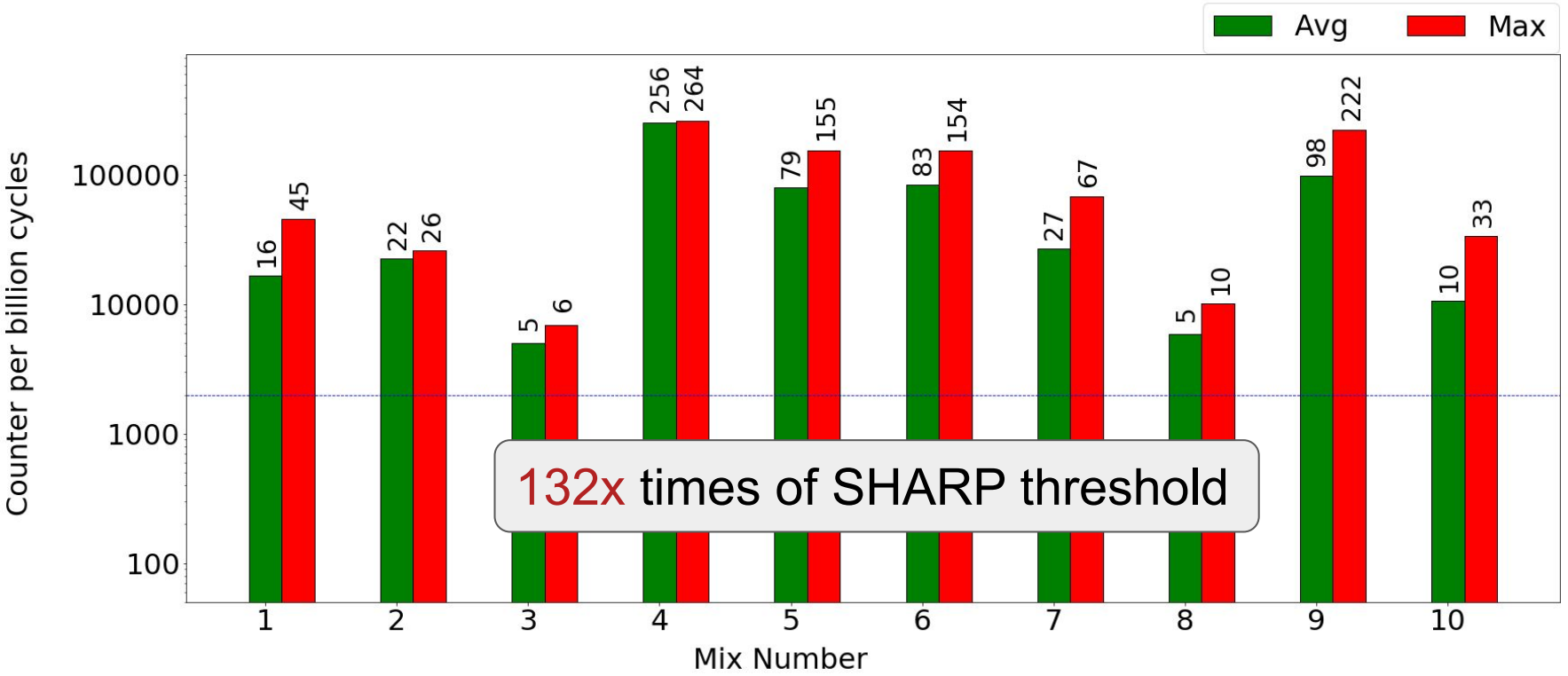
Interbackhit Counter



Interbackhit Counter



Interbackhit Counter



Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications? — *Yes* ☹

Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications? — *Yes* ☹

What does OS do when it receives an interrupt?

Speculating Possible OS Mitigations

Speculating Possible OS Mitigations

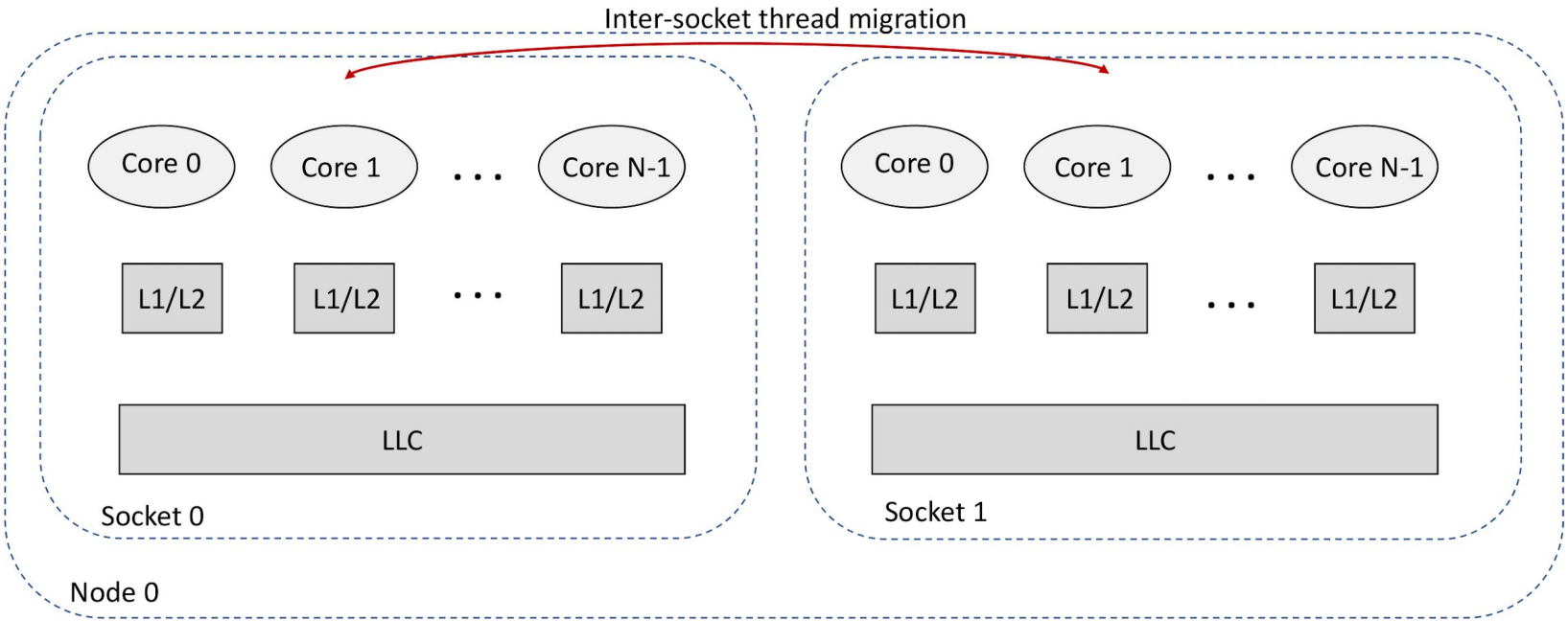
To deschedule

Speculating Possible OS Mitigations

To deschedule

To migrate to another socket

Migration to Another Socket



Speculating Possible OS Mitigations

To deschedule

To migrate to another socket

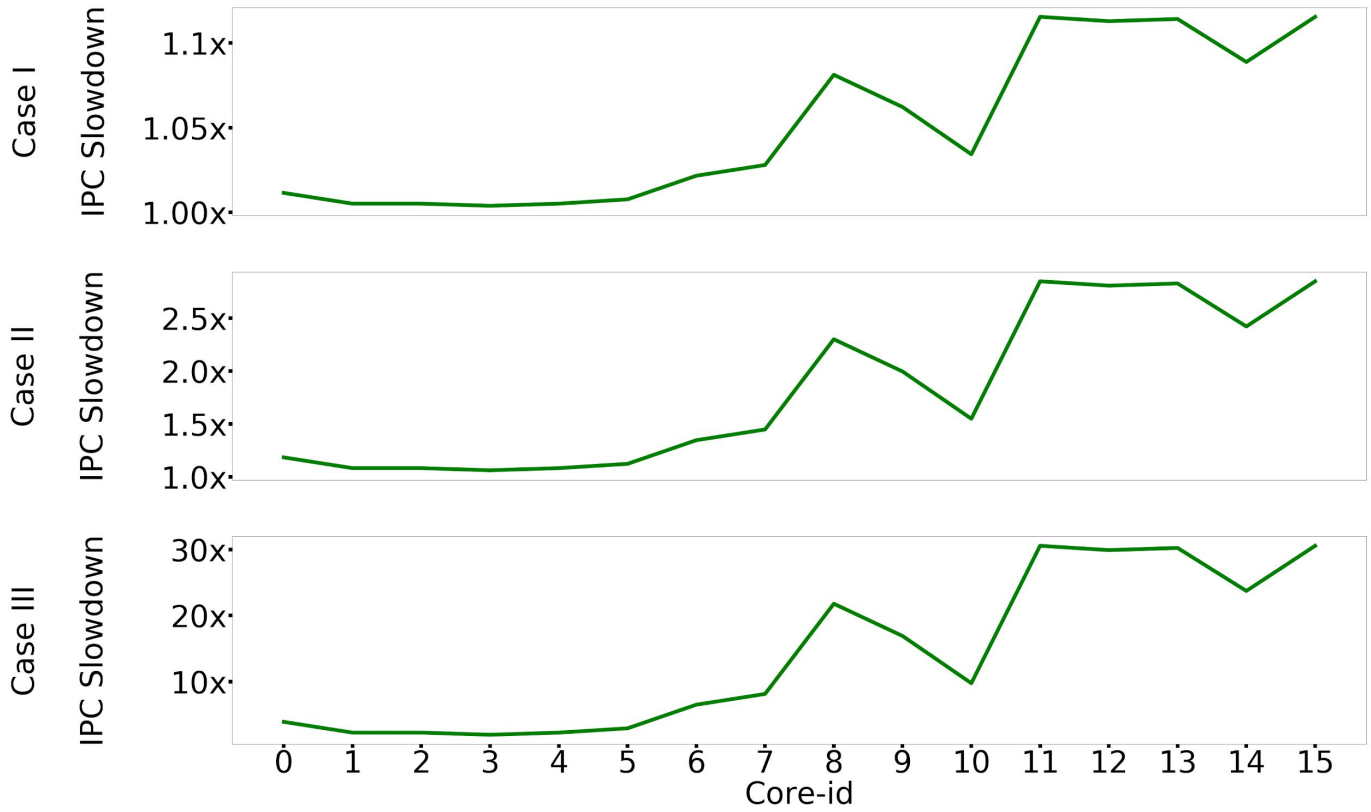
Speculating Possible OS Mitigations

To deschedule

To migrate to another socket

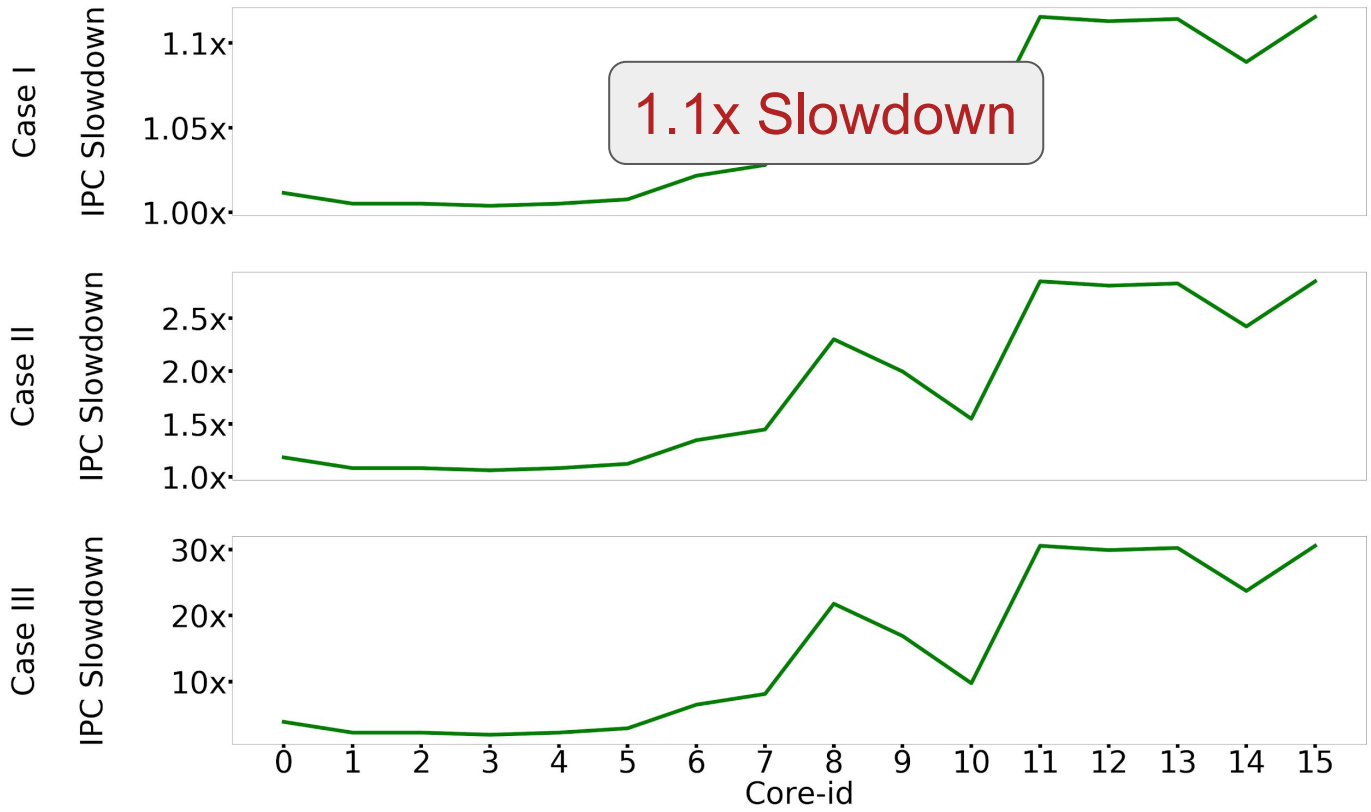
Causes performance overhead

Delay Cost : IPC Slowdown



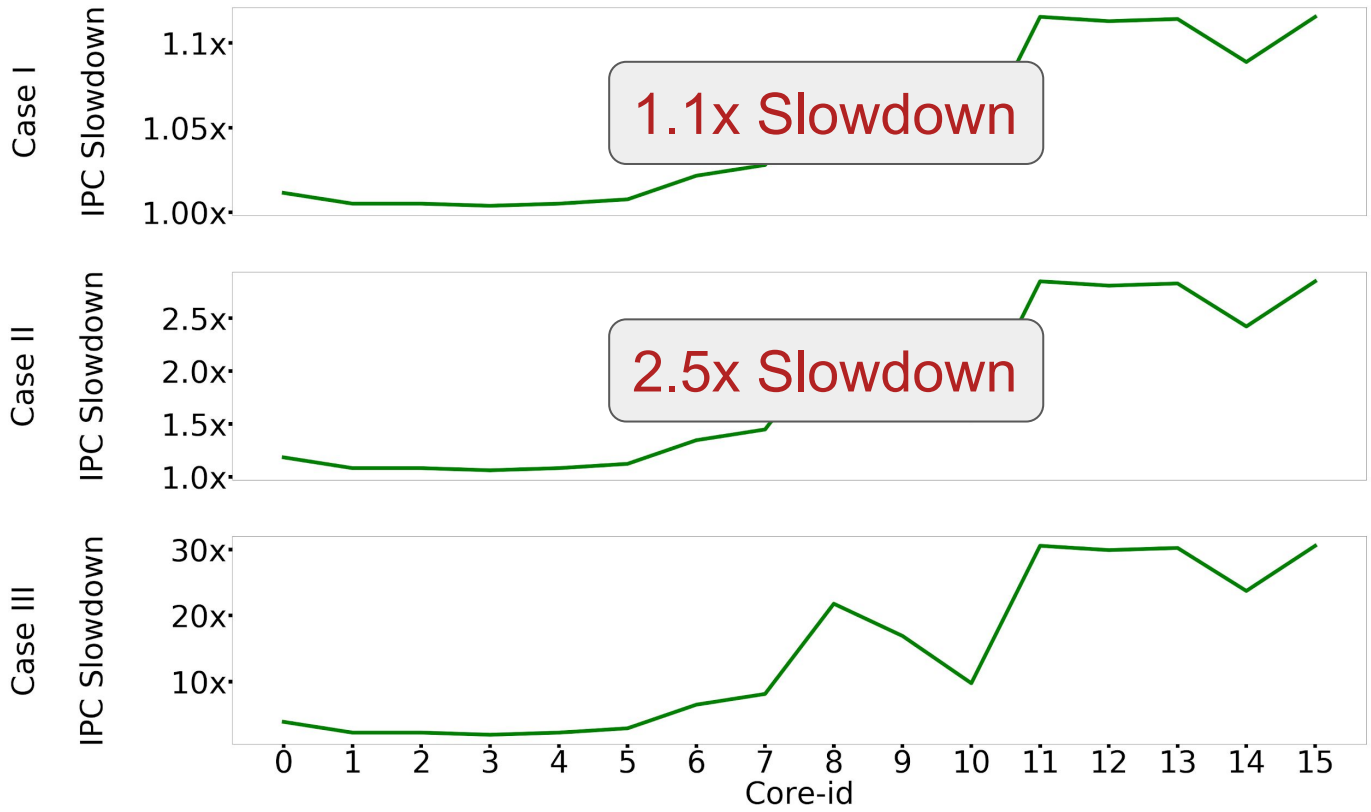
Case	Mitigation Delay
I	1 Million cycle
II	16 Million cycle
III	256 Million cycle

Delay Cost : IPC Slowdown



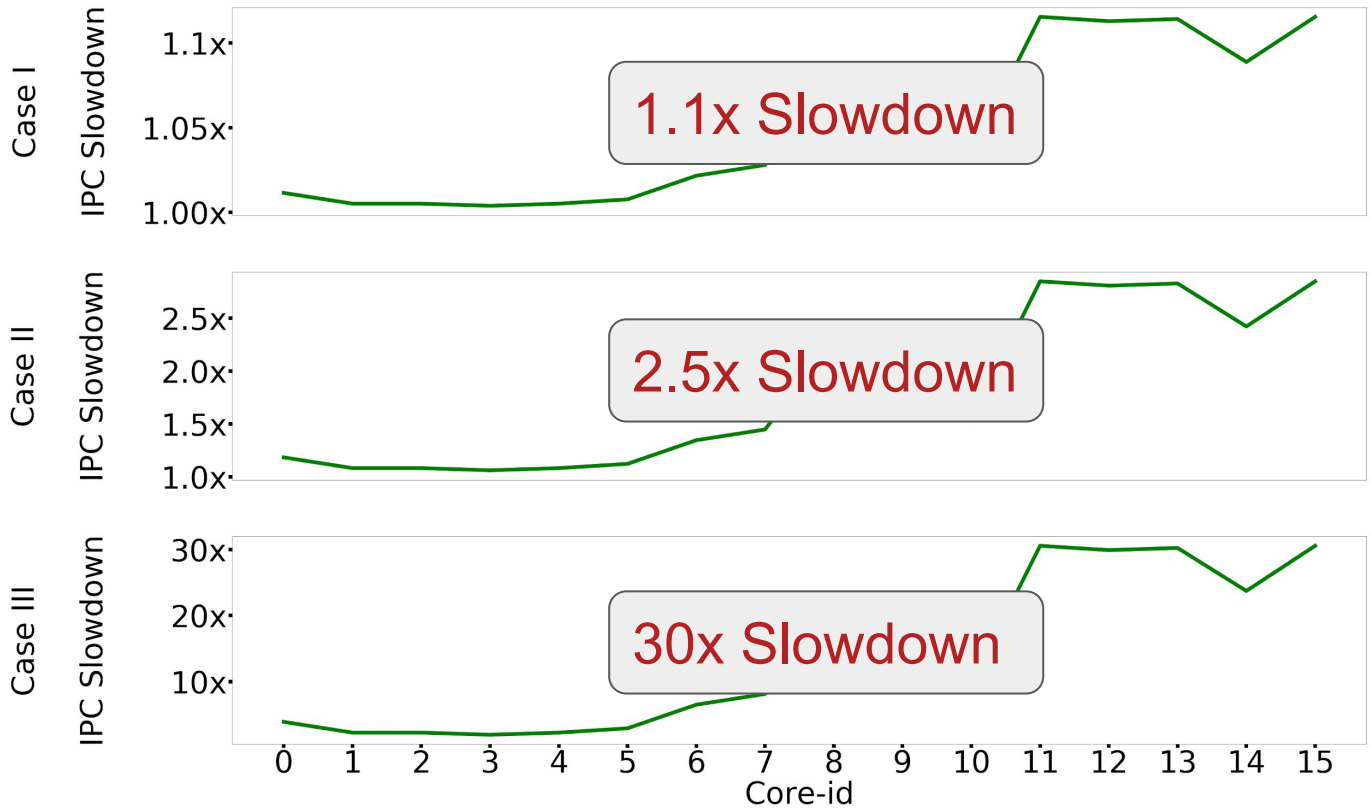
Case	Mitigation Delay
I	1 Million cycle
II	16 Million cycle
III	256 Million cycle

Delay Cost : IPC Slowdown



Case	Mitigation Delay
I	1 Million cycle
II	16 Million cycle
III	256 Million cycle

Delay Cost : IPC Slowdown



Case	Mitigation Delay
I	1 Million cycle
II	16 Million cycle
III	256 Million cycle

Speculating Possible OS Mitigations

To deschedule

To migrate to an another socket

Speculating Possible OS Mitigations

To deschedule

causes slowdown ☹

To migrate to an another socket

causes significant slowdown ☹

Speculating Possible OS Mitigations

To deschedule

causes slowdown ☹

To migrate to an another socket

causes significant slowdown ☹

To kill

Speculating Possible OS Mitigations

To deschedule

causes slowdown ☹

To migrate to an another socket

causes significant slowdown ☹

To kill

16-0 Mix, 100% apps got killed ☹

Speculating Possible OS Mitigations

To deschedule

causes slowdown ☹

To migrate to an another socket

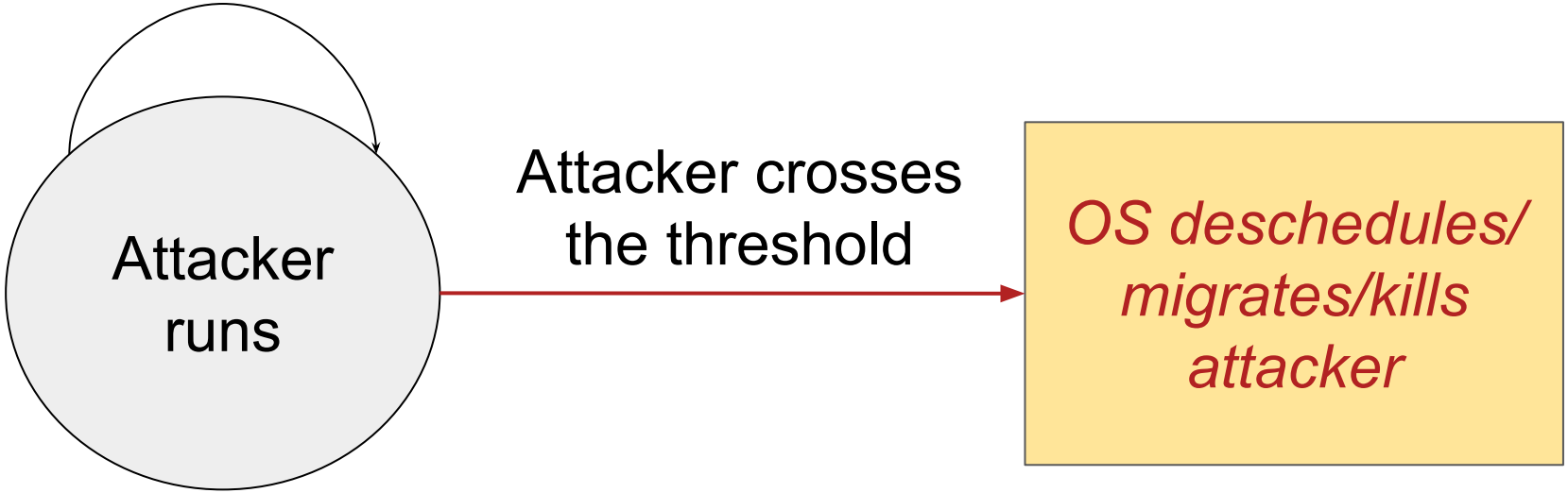
causes significant slowdown ☹

To kill

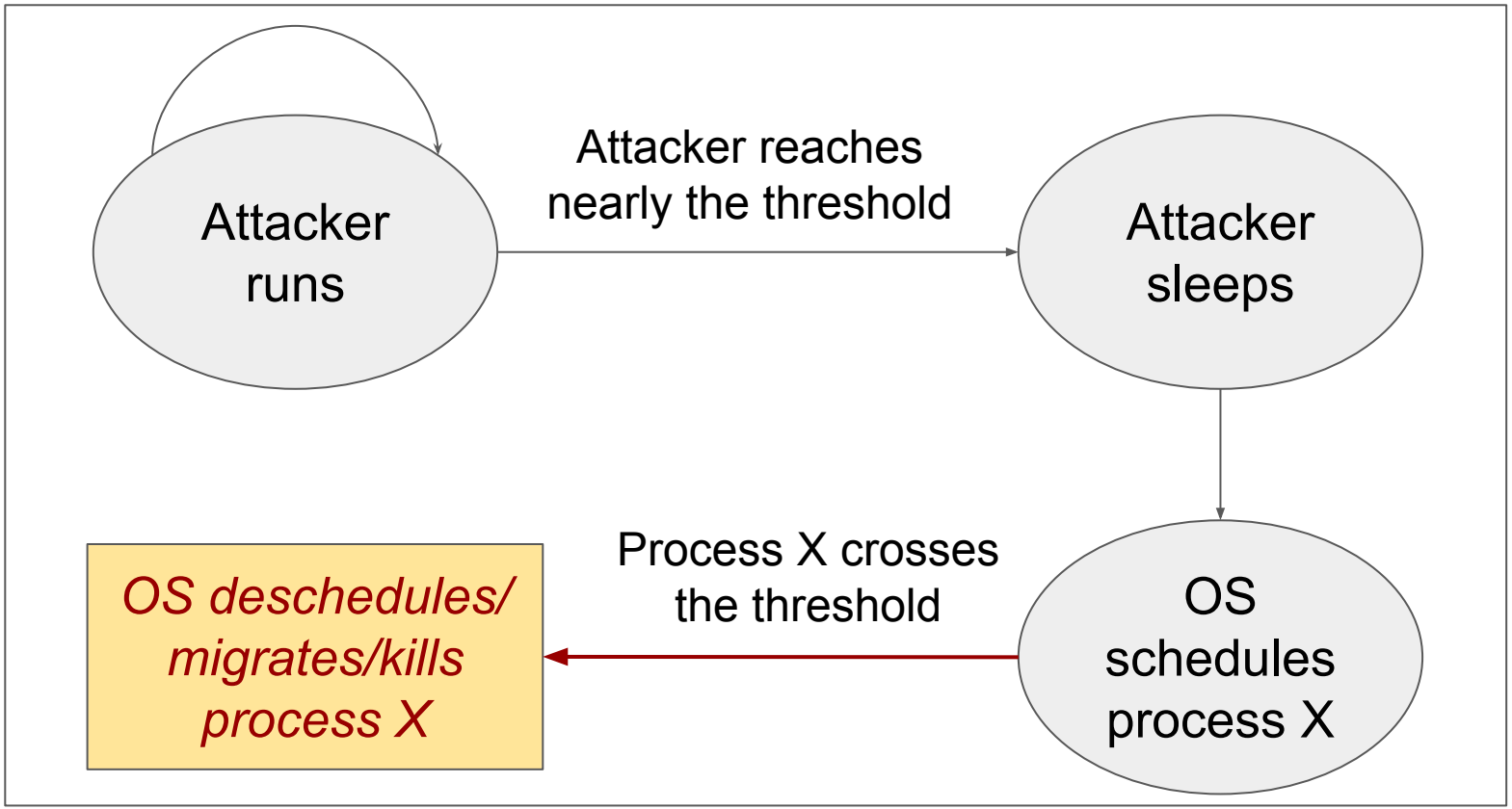
16-0 Mix, 100% apps got killed ☹

Does mitigation strategy facilitates any new attack?

Threshold Aware Attack - I



Threshold Aware Attack - II



Speculating Possible OS Mitigations

To deschedule

causes slowdown ☹

To migrate to another socket

causes significant slowdown ☹

To kill

16-0 Mix, 100% apps got killed ☹

Does mitigation strategy facilitates any new attack?

Yes ☹

Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications? — *Yes* ☹

What does OS do when it receives an interrupt?

Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications? — *Yes* ☹

What does OS do when it receives an interrupt?

Is SHARP secure in terms of information leakage?

Questions That We Ask?

Does SHARP mitigate all attacks? — *No* ☹

Does SHARP facilitate few more attacks? — *Yes* ☹

Does threshold affect benign applications? — *Yes* ☹

What does OS do when it receives an interrupt?

Is SHARP secure in terms of information leakage? — *Not really* ☹

Conclusion

SHARP is not that sharp

Facilitates new attacks

Don’t mitigates all attacks

Role of OS is not defined

Performance overhead to benign applications

Thank You!

Semiconductor Research Corporation