ASHMAN

A NOVEL MEMORY MANAGEMENT FOR RISC-V ENCLAVES

Haonan Li[1], Weijie Huang[1], Mingde Ren[1,2], Hongyi Lu[1], Zhenyu Ning[1], Heming Cui[2], Fengwei Zhang[1]
Southern University of Science and Technology[1]
The University of Hong Kong[2]

ENCLAVE / TEE (TRUSTED EXECUTION ENVIRONMENT)

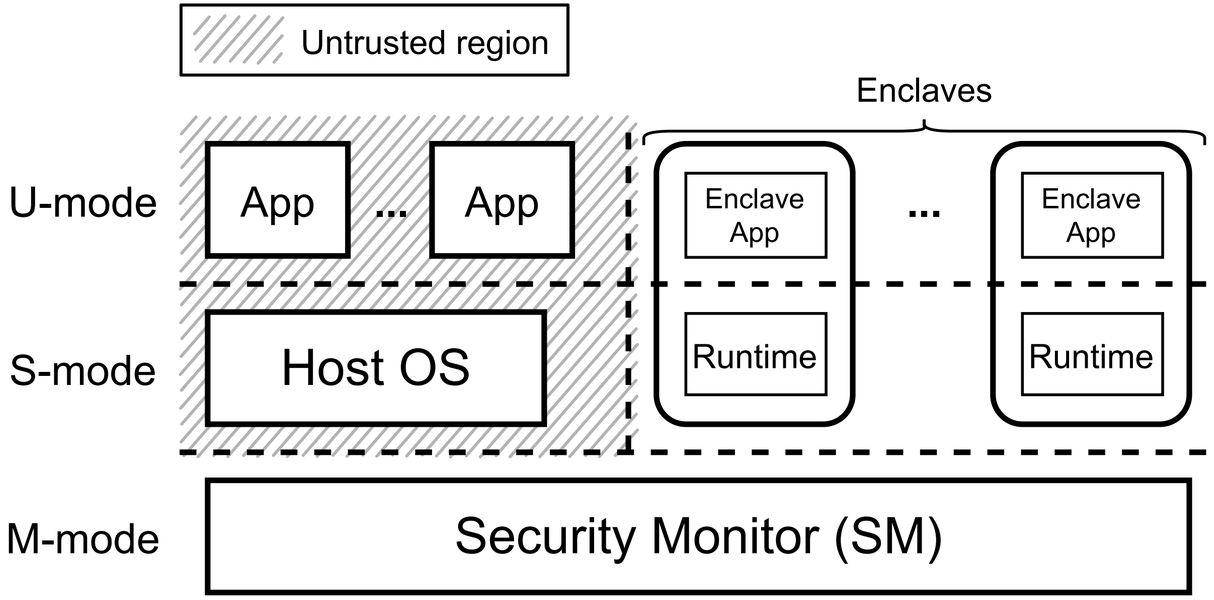


Figure 1: TEE Overview on RISC-V

Two limitations of enclave apps:

- # of concurrent apps
- memory request

PHYSICAL MEMORY PROTECTION

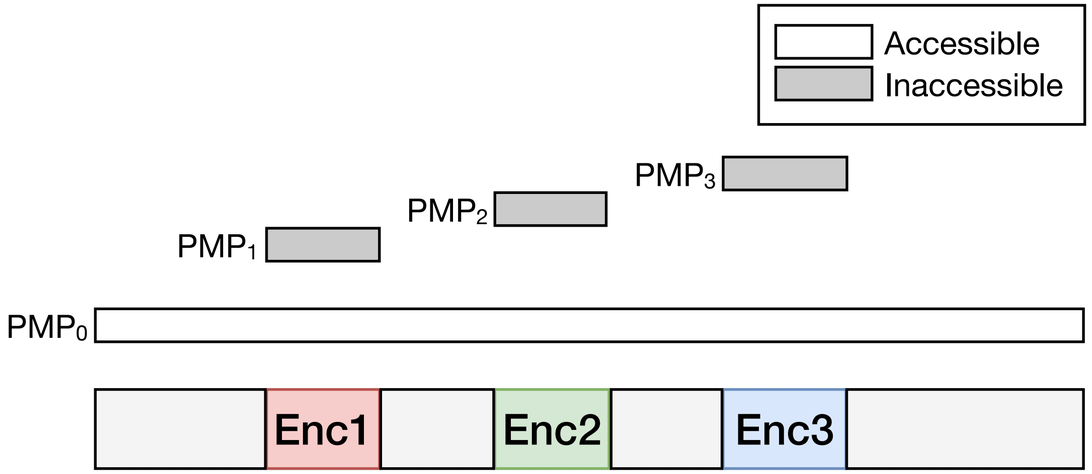


Figure 2: PMP Config for Host OS

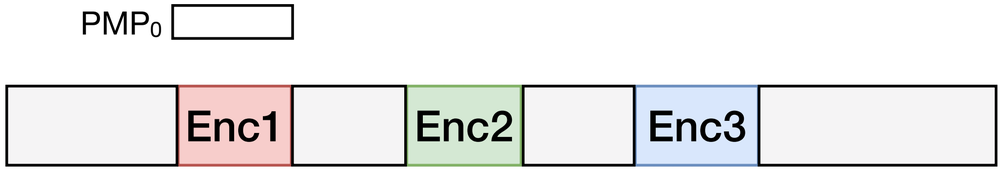


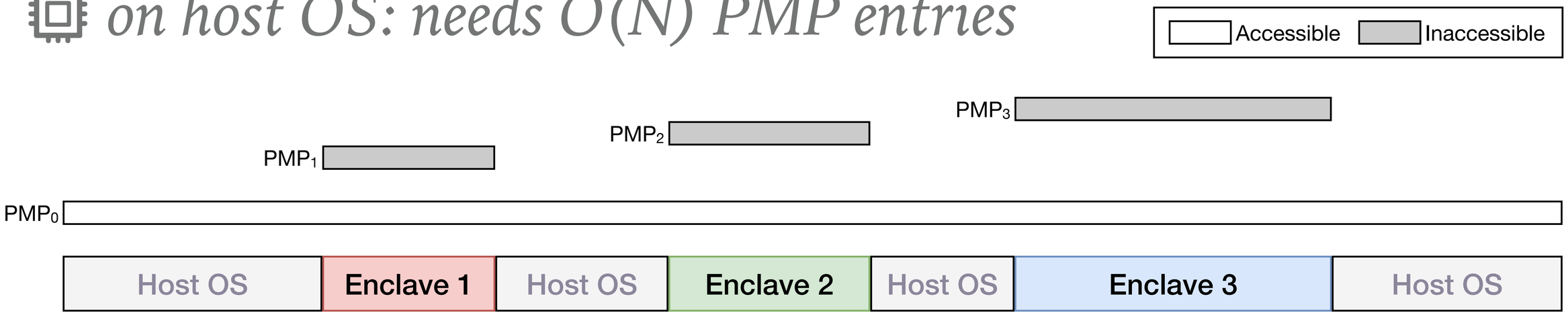
Figure 3: PMP Config for Enc1

Configure for contiguous memory

limited entries, at most 16

LIMITATION 1: MULTIPLE ENCLAVES USE MULTIPLE PMP ENTRIES

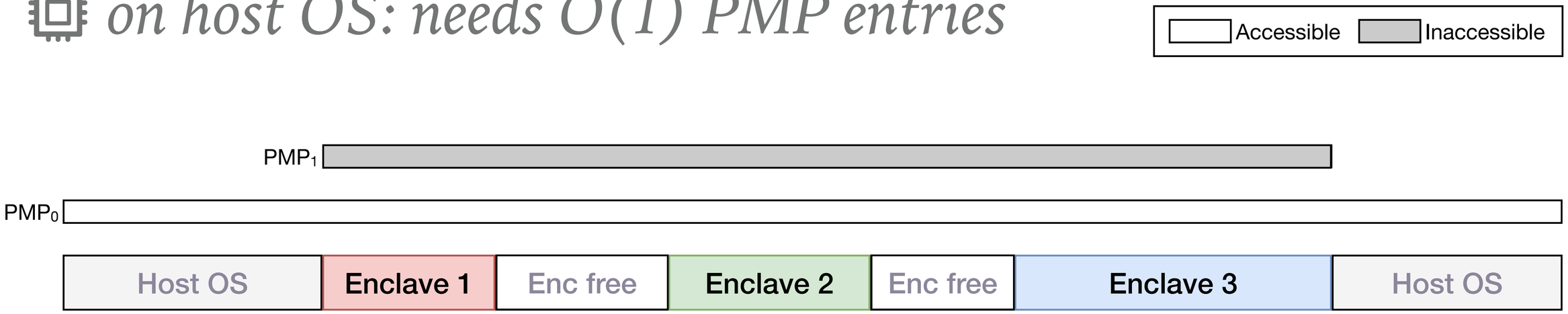
on host OS: needs O(N) PMP entries



① The number of concurrent enclaves is limited!

SOLUTION 1: MULTIPLE ENCLAVES USE SAME PMP ENTRY

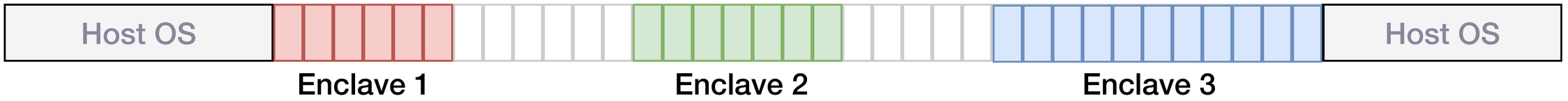
on host OS: needs O(1) PMP entries



- Single PMP to cover the entire enclave memory
- “Sandwiches” can be only used for enclave

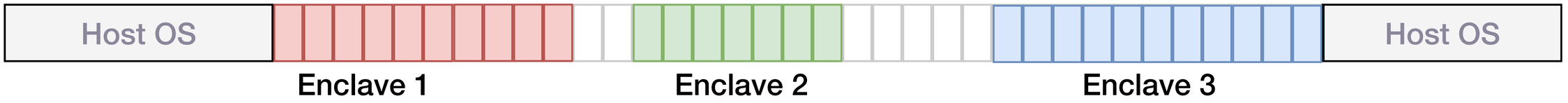
LIMITATION 2: ENCLAVE REQUESTS MEMORY

Case Study: Enclave 1 needs 



LIMITATION 2: ENCLAVE REQUESTS MEMORY

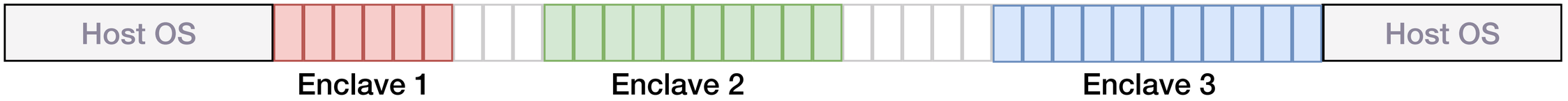
Case Study: Enclave 1 needs



- Case 1: requests succeed

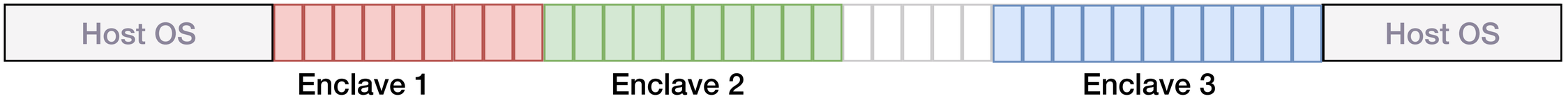
LIMITATION 2: WHEN ENCLAVE REQUESTS MORE MEMORY

Case Study: Enclave 1 needs 



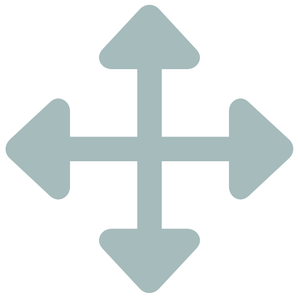
LIMITATION 2: WHEN ENCLAVE REQUESTS MORE MEMORY

Case Study: Enclave 1 needs 



- Case 2: requests fail (can only allocate 3 areas)
- Limitation: memory requests depends on others' usage

②*The memory request is limited!*

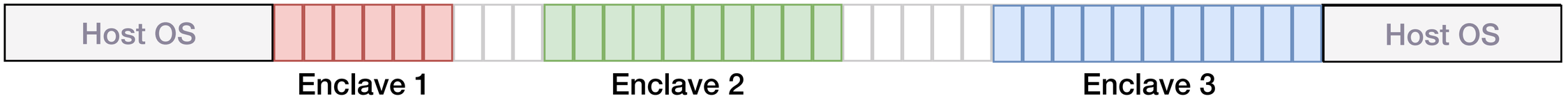


MEMORY MIGRATION

Move memory to another space

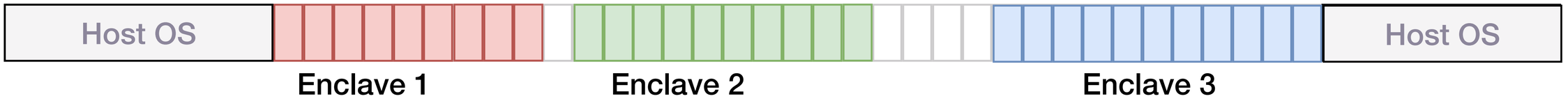
SOLUTION 2: MEMORY REQUEST WITH MIGRATION

Case Study: Enclave 1 needs 



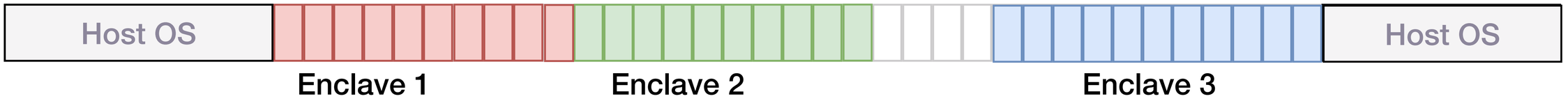
SOLUTION 2: MEMORY REQUEST WITH MIGRATION

Case Study: Enclave 1 needs 



SOLUTION 2: MEMORY REQUEST WITH MIGRATION

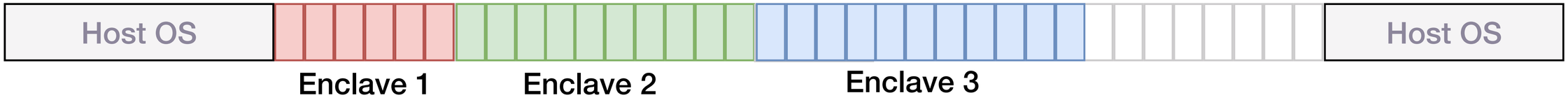
Case Study: Enclave 1 needs



SOLUTION 2: MEMORY MIGRATION (CONT.)

Case Study: Enclave 1 needs 

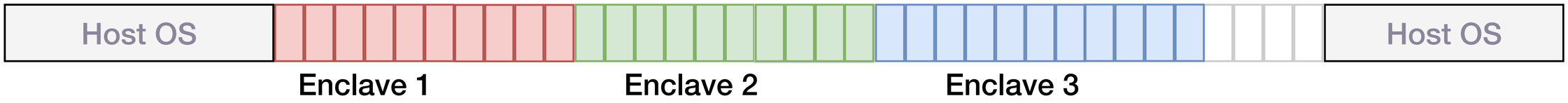
*Worst case: N enclaves, request M; O(N*M) migration*

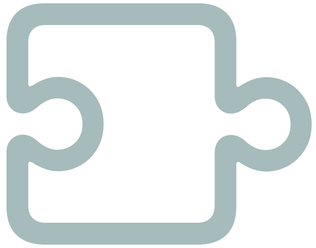


SOLUTION 2: MEMORY MIGRATION (CONT.)

Case Study: Enclave 1 needs

*Worst case: N enclaves, request M; O(N*M) migration*



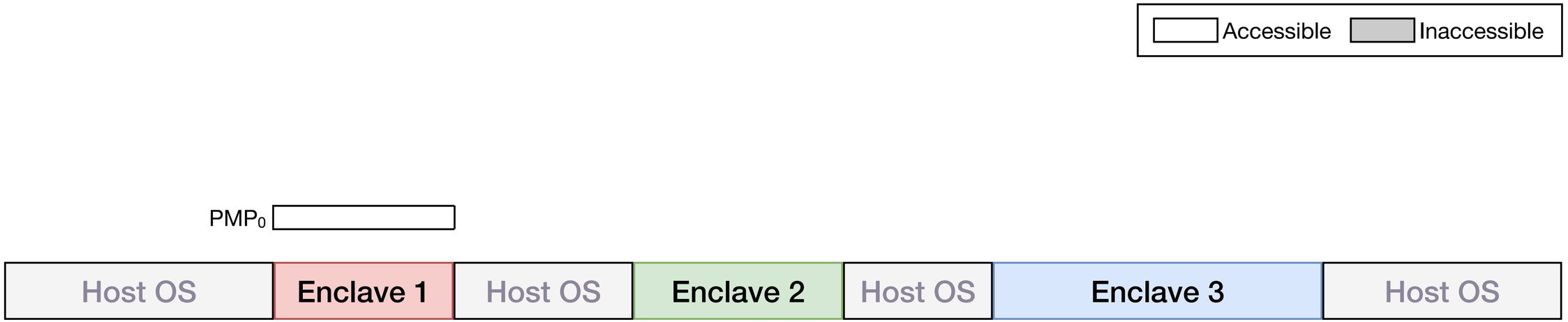


FRAGMENTATION

Allow enclave to have multiple fragments

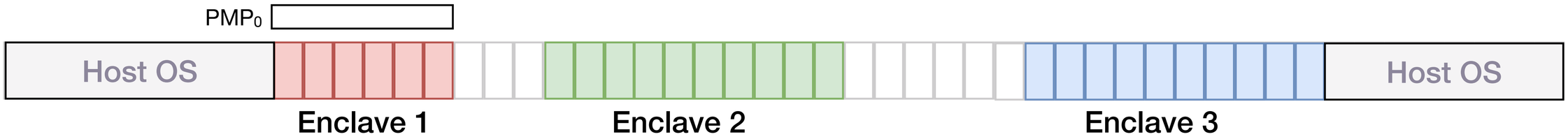
RECALL: HOW TO RESTRICT ENCLAVES?

on enclave: only one PMP entry needed



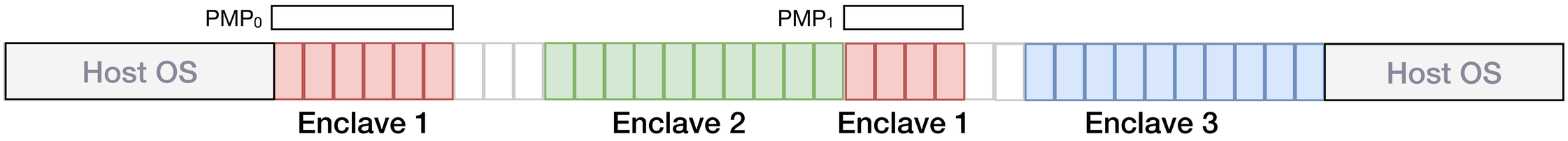
SOLUTION 2.1: MEMORY REQUEST WITH MULTIPLE PMP ENTRIES

Case Study: Enclave 1 needs 



SOLUTION 2.1: MEMORY REQUEST WITH MULTIPLE PMP ENTRIES

Case Study: Enclave 1 needs



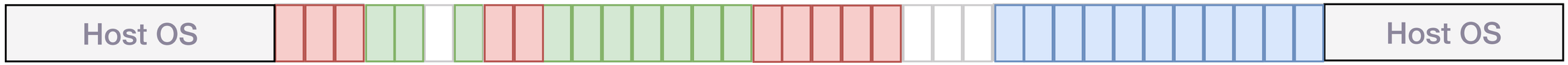
- Hint 1: allow fragmentations, make full use of PMP entries

SOLUTION 2.2: MEMORY REQUEST WITH SMALLEST FRAGMENT MIGRATION

Case Study: Enclave 1 needs 

SOLUTION 2.2: MEMORY REQUEST WITH SMALLEST FRAGMENT MIGRATION

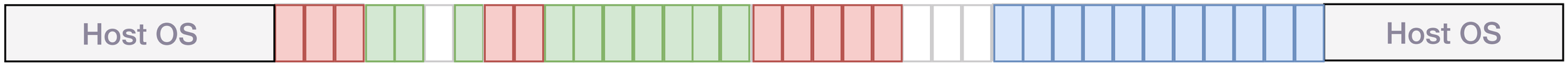
Case Study: Enclave 1 needs



- Hint 2: When PMP entries run out, migrate the smallest fragment

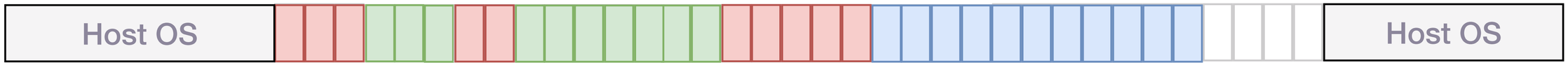
SOLUTION 2.3: MEMORY REQUEST WITH MEMORY COMPACTION

Case Study: Enclave 1 needs 



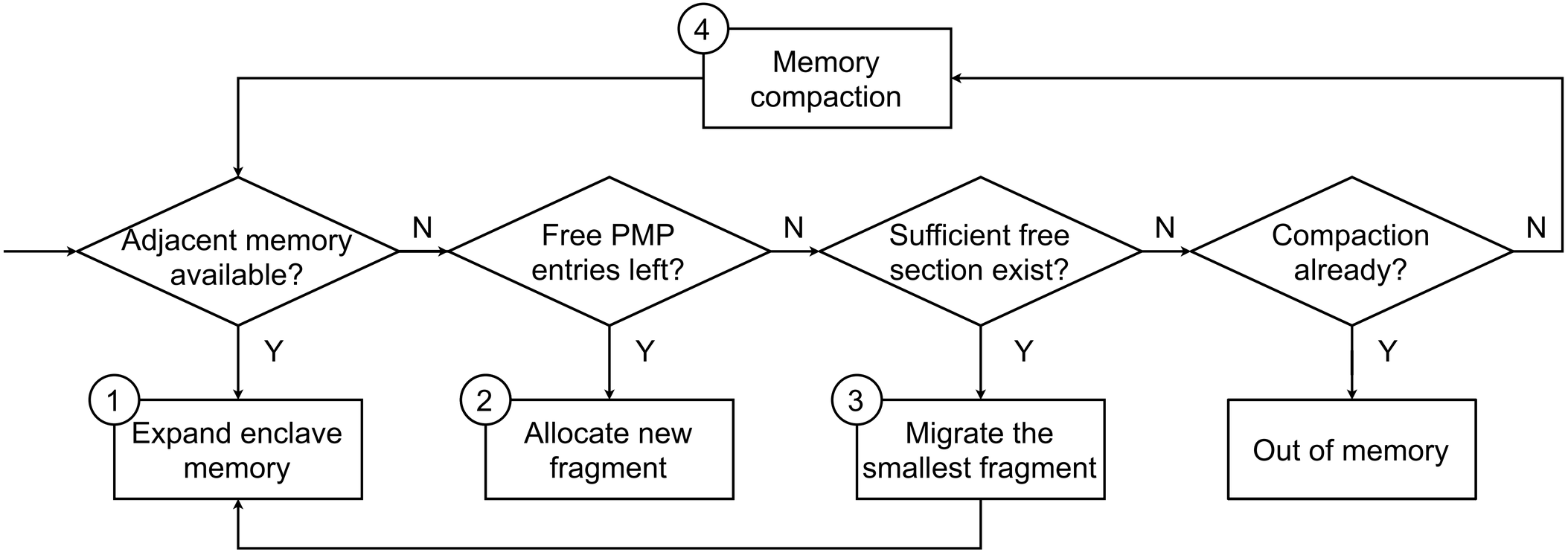
SOLUTION 2.3: MEMORY REQUEST WITH MEMORY COMPACTION

Case Study: Enclave 1 needs 



- Hint 3: memory compaction, make the largest free space
- But… memory compaction won't mitigate fragmentation
- Ultimate solution: compaction with merging fragmentations (future work)

RECALL: THE WHOLE PROCEDURE OF MEMORY REQUEST



EVALUATION

Memory utilization & performance

MEMORY UTILIZATION

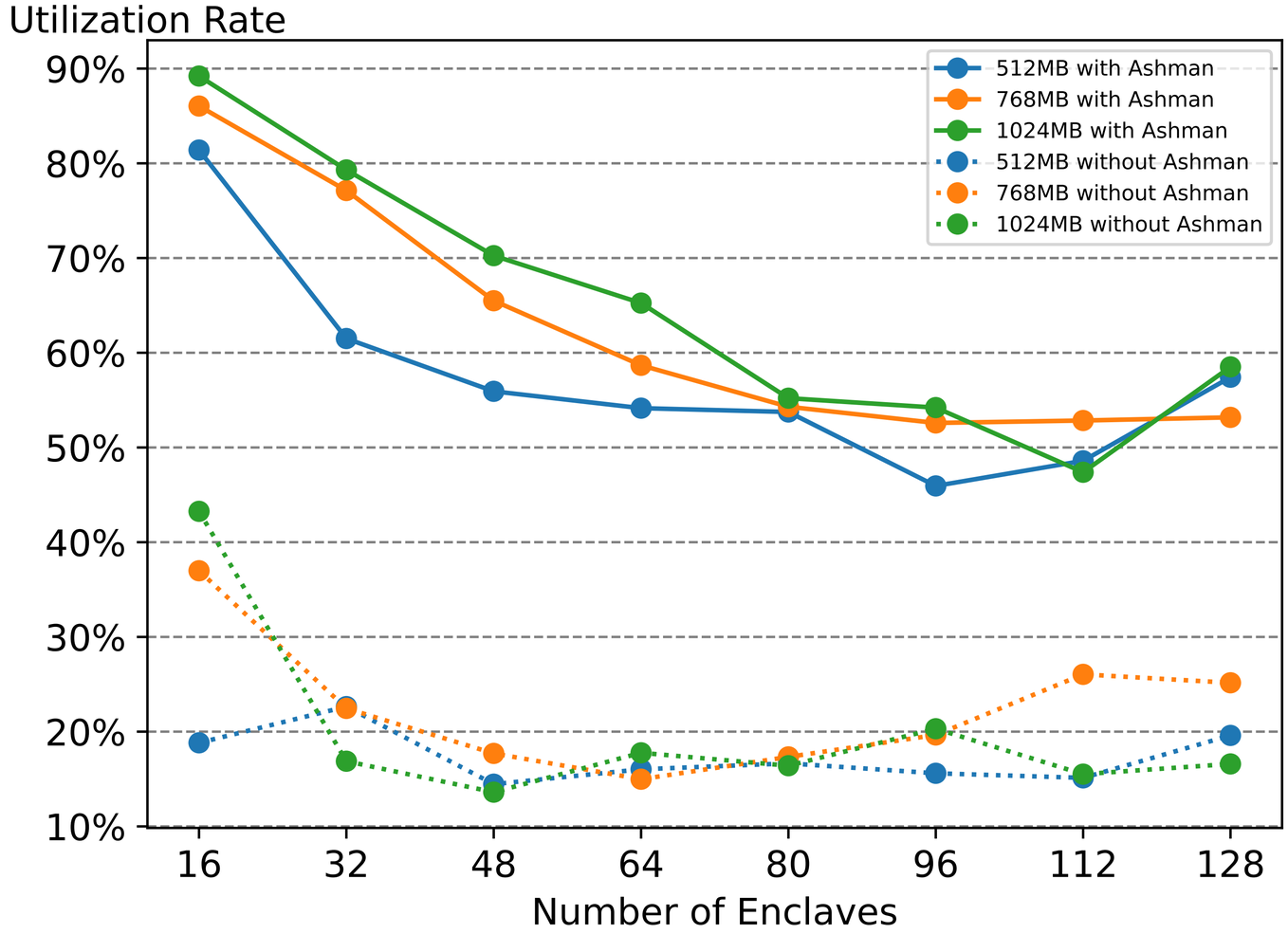


Figure 4: Memory Utilization Rate

- M_{used}/M_{pool}
- Improve by 149%~516%

PERFORMANCE OF MEMORY ALLOCATION

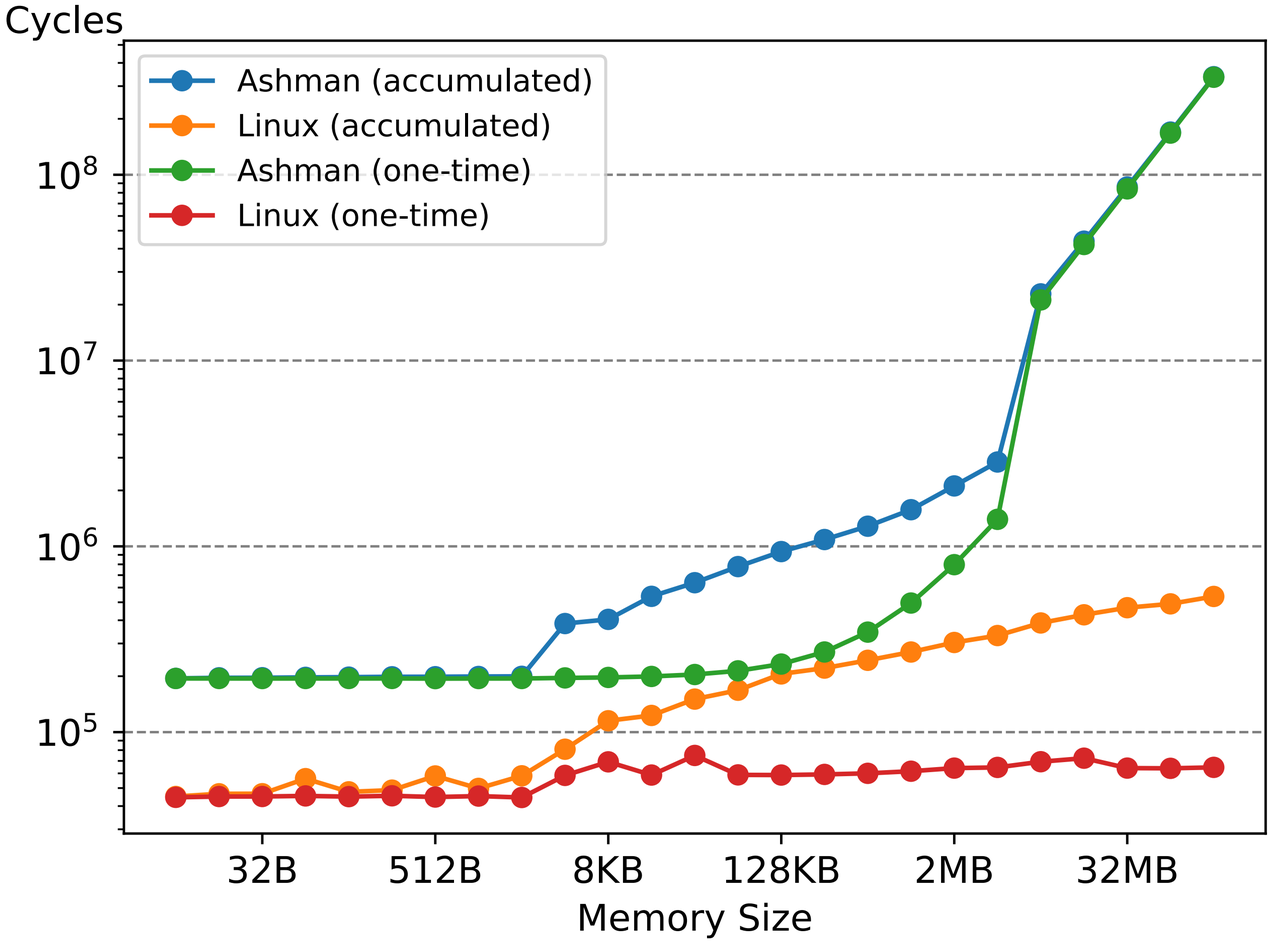


Figure 5: Performance of Memory Allocation

- Compare to Linux
- Turning point: 8M

PERFORMANCE OF MIGRATION & COMPACTION

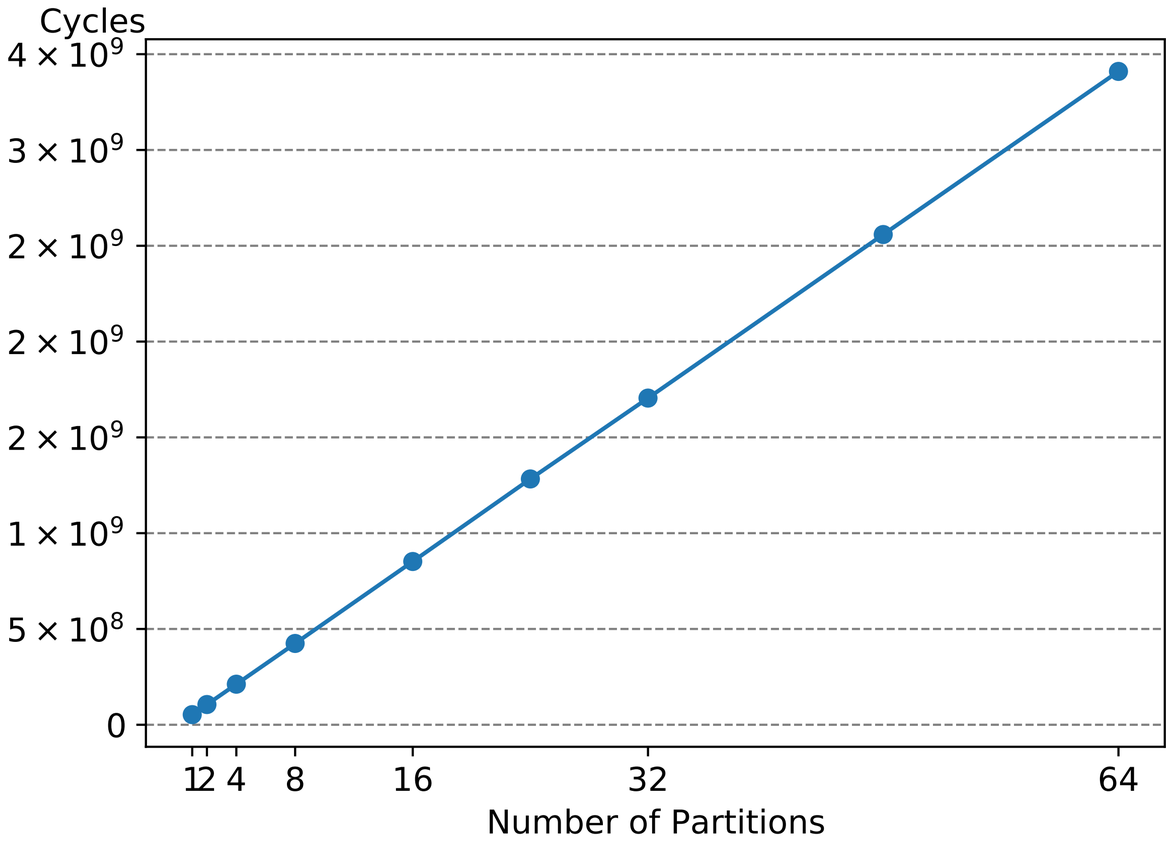


Figure 6: Performance of Memory Migration

- Migration time proportional to the size
- Memory partition: 8M
- Average compaction overhead:
  ~10 seconds for 768MB memory pool

CONCLUSION

- Memory management in enclaves is a problem

- Ashman tickles this problem
  - The enclave application can use memory as native applications
  - Only relies on RISC-V standard hardware
  - Overhead is low

- Open source: https://github.com/Compass-All/Ashman

QUESTIONS?

FOR PMP

- PMP entries up to 16
- But most boards only have 8
- For each fragments address $[2^x, 2^x + 2^y)$, then single entry, otherwise 2 entires
- SM**(1)**, accessible range for OS**(1)**, Only remain **6** entries to support **3** enclaves/ fragments!