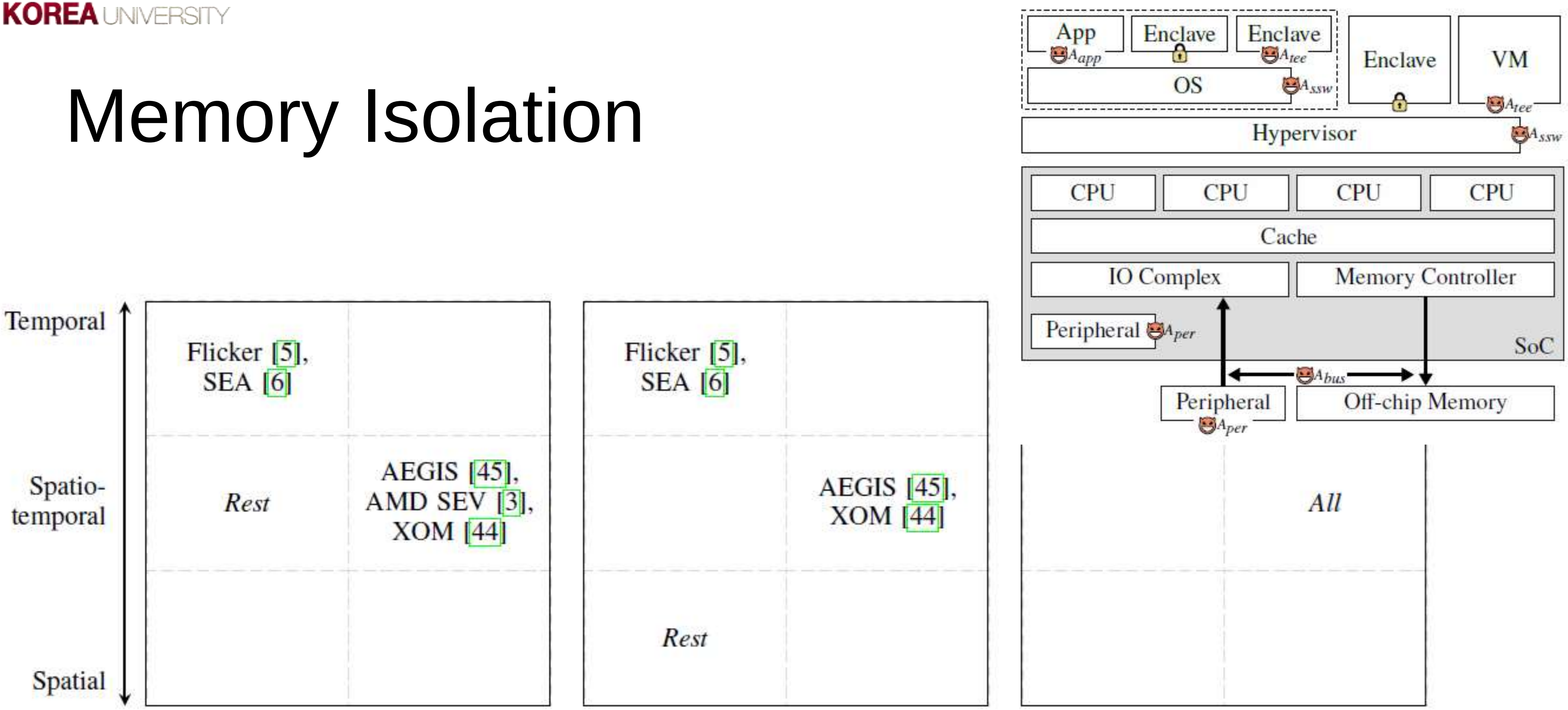
Memory Isolation

- Memory isolation is particularly challenging as it must protect:
  - Off-chip memory
  - On-chip microarchitectural structures (caches)
  - Translation structures (page tables)
  - Translation look-aside buffers (TLBs)
- Unlike CPU isolation where all TEEs use the same approach, memory isolation strategies are diverse.
  - Many TEEs use different strategies based on the type of attacker being considered.

Memory Isolation



(a) Enclave memory isolation against A_{app}, A_{tee}, and A_{ssw}.

(b) TCB memory isolation against A_{app}, A_{tee}, and A_{ssw}.

(c) Memory isolation strategy against A_{bus}.

Memory Protection Mechanisms

Memory Protection Unit (MPU)

- Checks physical address and access type against access control information
- Supports limited number of memory regions
- Suitable for coarse-grained protection
- Used in many academic TEEs

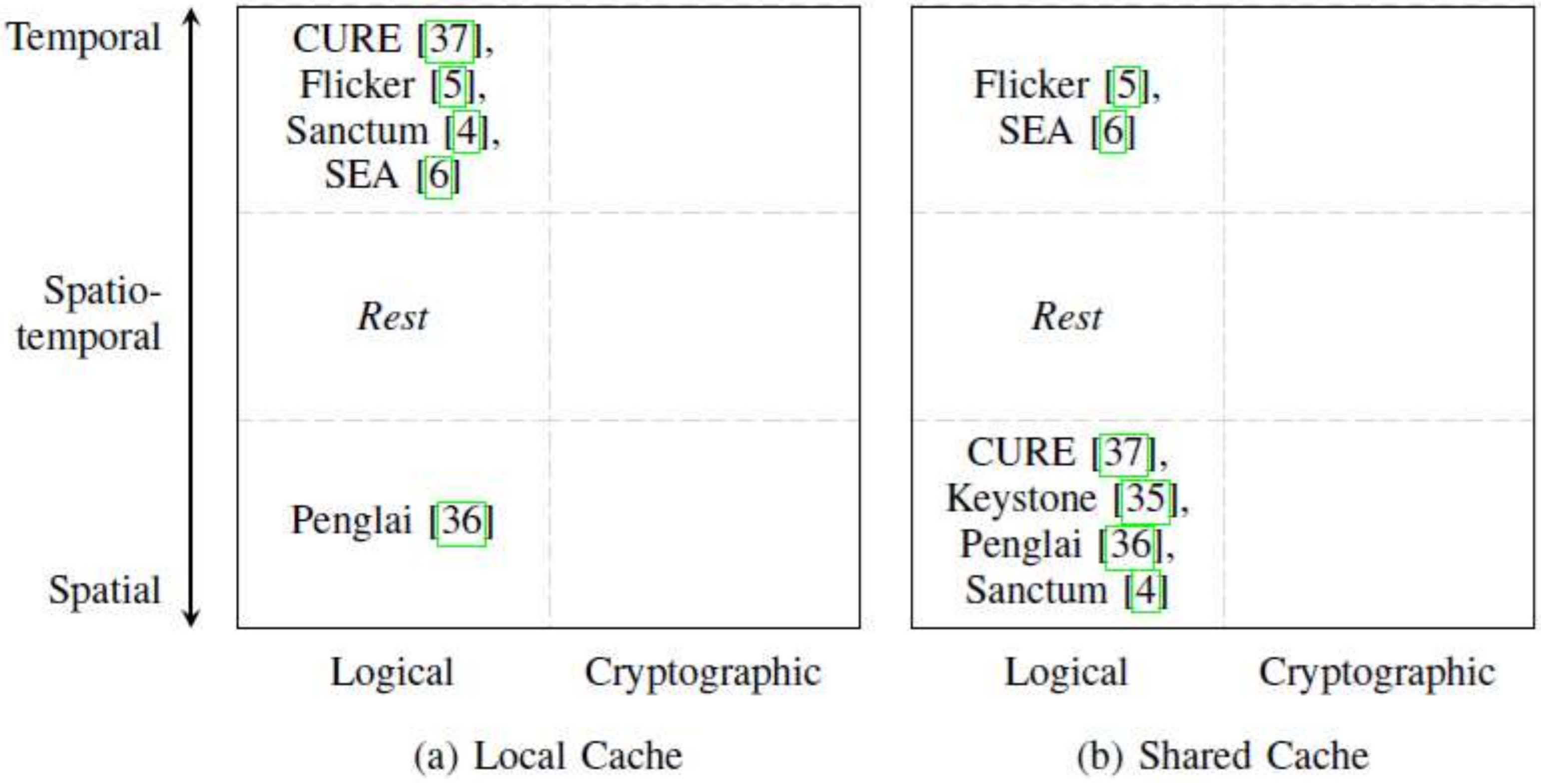
Memory Management Unit (MMU)

- Converts virtual addresses to physical addresses using page tables
- Stores permissions alongside mappings
- Offers fine-grained protection
- Used in many commercial TEEs

The access control information used by MPUs and MMUs must itself be protected against unauthorized access, typically through spatial partitioning.

Cache Isolation

Against software adversaries (A_{app}, A_{tee}, and A_{ssw}).

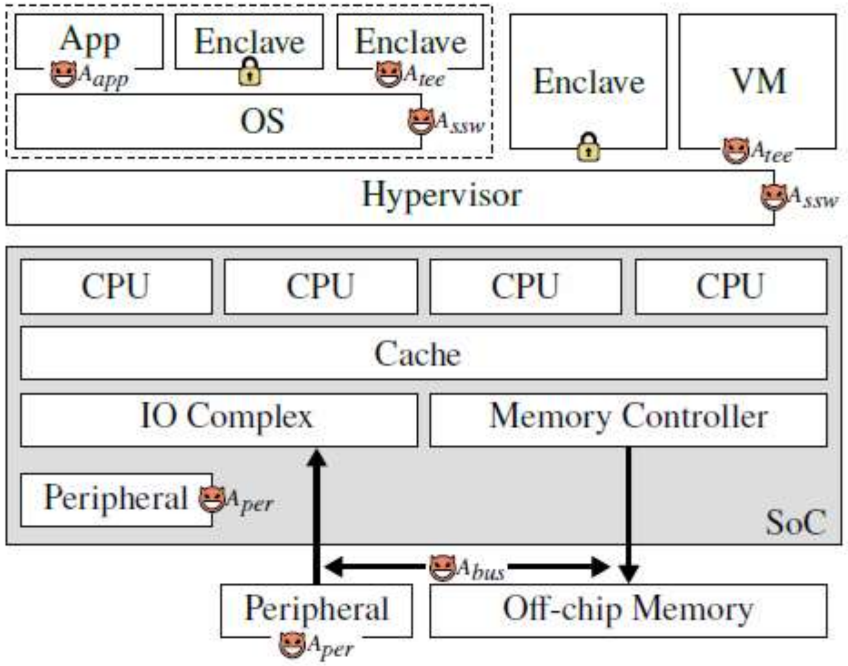


(a) Local Cache

	Logical	Cryptographic
Temporal	CURE [37], Flicker [5], Sanctum [4], SEA [6]	
Spatio-temporal	*Rest*	
Spatial	Penglai [36]	

(b) Shared Cache

	Logical	Cryptographic
Temporal	Flicker [5], SEA [6]	
Spatio-temporal	*Rest*	
Spatial	CURE [37], Keystone [35], Penglai [36], Sanctum [4]	



Translation Look-aside Buffers (TLBs)

TLBs hold recent virtual-to-physical address translations and must be protected to prevent leakage:

Spatial Partitioning

Dedicated TLBs per logical processor provide inherent spatial partitioning

Temporal Partitioning

TLBs are flushed on context switches to prevent reuse of stale translations

Optimization

Modern processors support partial TLB flushes using context identifiers

Cryptographic isolation is not used for TLBs due to performance overheads.