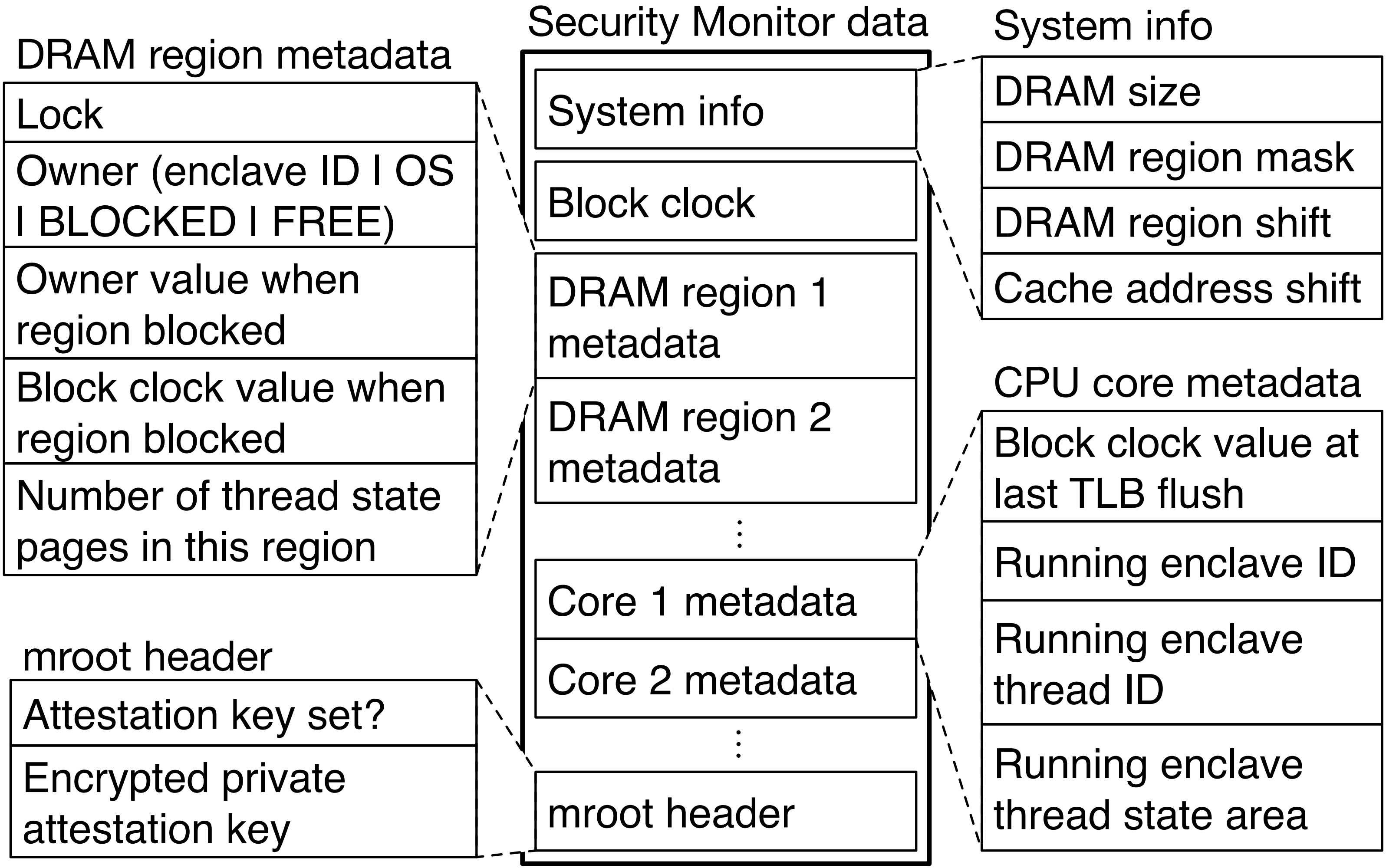
Security Monitor data
System info
Block clock
DRAM region 1 metadata
DRAM region 2 metadata
⋮
Core 1 metadata
Core 2 metadata
⋮
mroot header
DRAM region metadata
Lock
Owner (enclave ID | OS | BLOCKED | FREE)
Owner value when region blocked
Block clock value when region blocked
Number of thread state pages in this region
mroot header
Attestation key set?
Encrypted private attestation key
System info
DRAM size
DRAM region mask
DRAM region shift
Cache address shift
CPU core metadata
Block clock value at last TLB flush
Running enclave ID
Running enclave thread ID
Running enclave thread state area