SuperMem: Enabling Application-transparent Secure Persistent Memory with Low Overheads

Pengfei Zuo[1,2], Yu Hua[1], Yuan Xie[2]

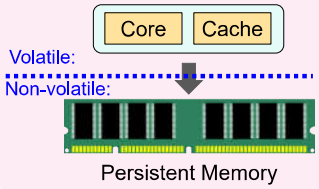
[1] Huazhong University of Science and Technology, China

[2] University of California at Santa Barbara, USA

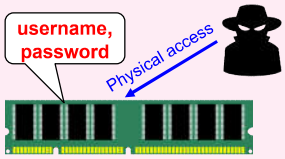
Background

Persistent memory as main memory
- PCM, ReRAM, STT-RAM, 3D-Xpoint
- High scalability, high density, and low standby power

Persistence issue
- Crash inconsistency

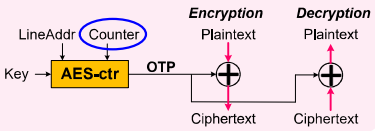


Security issue
- Physical-access attacks

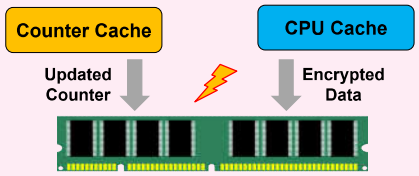


Consistency guarantee
- Cache line flush (*clflush*)
- Memory fence (*mfence*)
- Logging
- Copy-on-write

Memory encryption
- Counter mode encryption

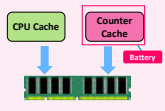


The gap between persistence and security
- *Clflush* and *mfence* cannot operate the counter cache
- Data and counter cannot reach NVM in the same time



Existing solutions (write-back counter cache)

Large Battery Backup
[Awad et al. ASPLOS'16]



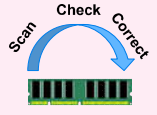
Expensive

Software-level Modification
[Liu et al., HPCA'18]

New programming primitives
- counter_cache_writeback()
- CounterAtomic

Portability limitation

Error Correction
[Ye et al., MICRO'18]



Long recovery time

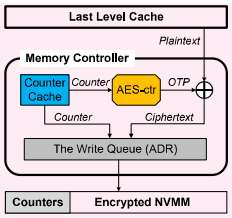
The SuperMem Design

SuperMem: an application-transparent secure persistent memory by leveraging a write-through counter cache.

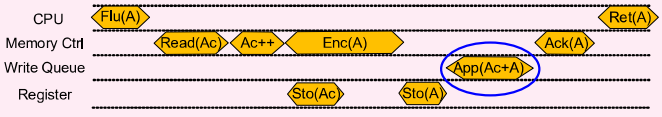
A write-through counter cache
- No large battery backup
- No software-level modifications
- No need to correct counters

Counter write coalescing
- Reduce the number of writes

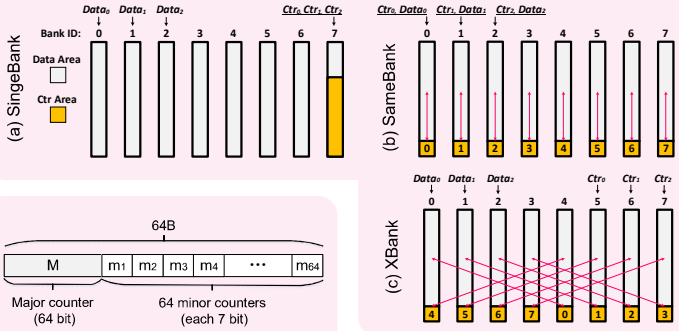
Cross-bank counter storage
- Speed up memory writes



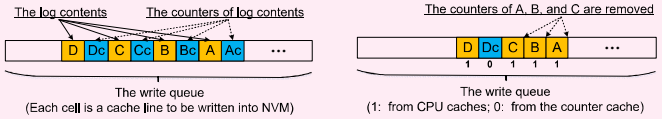
Write-through counter cache
- Ensure that data and its counter reach the write queue in the same time



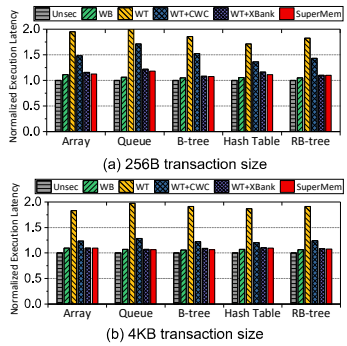
Cross-bank counter storage (XBank)
- Ensure that data and its counter reach the write queue in the same time



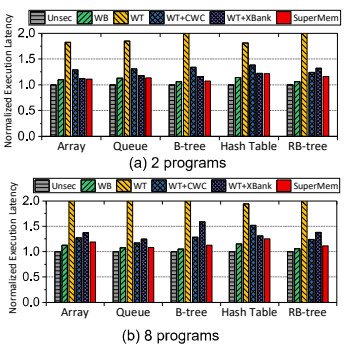
Locality-aware counter write coalescing (CWC)
- Leverage spatial locality of counter storage and data writes
- Coalesce counter cache lines in write queue



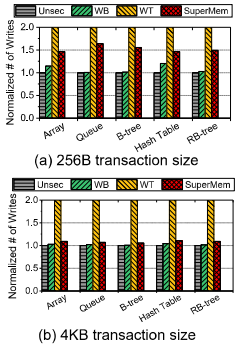
Evaluation



Singe-core performance



Multi-core performance



NVM writes

Comparisons
UnSec: An un-encrypted NVM
WB: A ideal write-back scheme
WT: A write-through scheme
WT+CWC: A write-through scheme with CWC
WT+Xbank: A write-through scheme with XBank
SuperMem

NVMW 2021