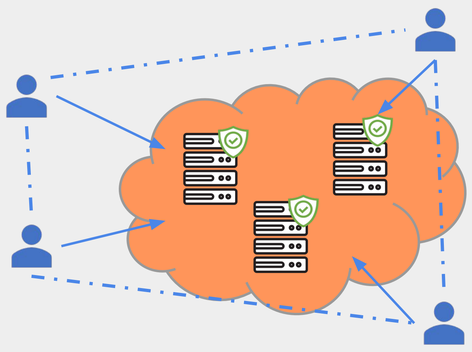
Toleo: Scaling Freshness to Tera-scale Memory using CXL and PIM

UNIVERSITY OF MICHIGAN

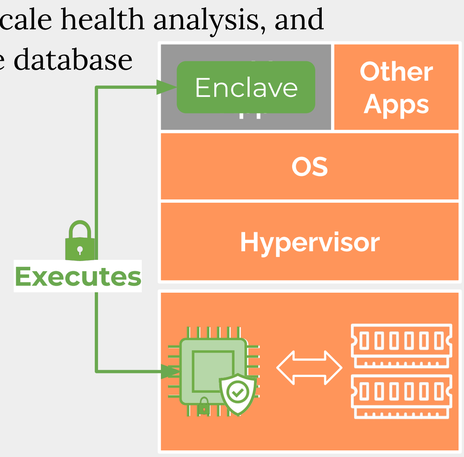
Juechu Dong, Jonah Rosenblum, Satish Narayanasamy

BACKGROUND

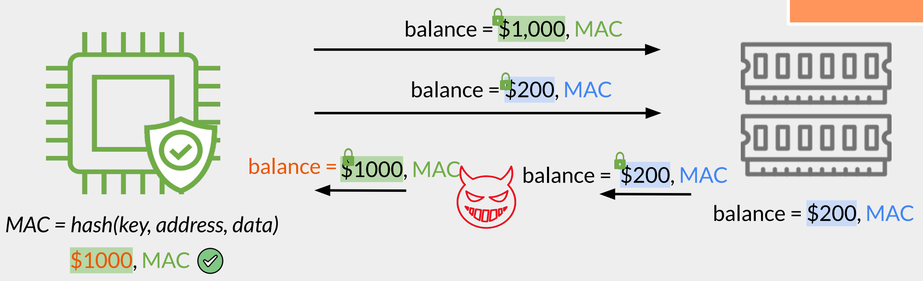
Trusted Execution Environment (TEE)
protects **confidentiality**, **integrity** & **freshness** of data and code "in use" on untrusted thirty party systems such as public cloud.



- use trusted processor as the root of trust.
- allows mutually untrusted parties to pool data
- vital for privacy-preserving AI service, population scale health analysis, and collaborative database

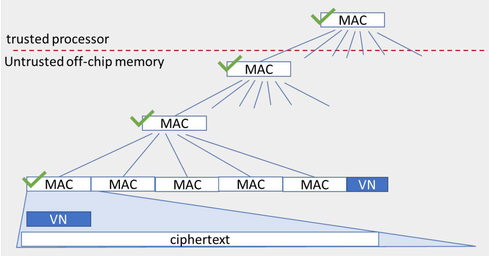


Replay attacks
-- Replay old memory transaction
-- Enables code injection attacks
-- Compromise enclave confidentiality



Freshness defends replay attacks: A memory read returns **last written value.**

Problem: Freshness is expensive
Intel® SGX[1] supports only 128MB of secure memory.
Uses **Merkle tree --** not scalable to large memory

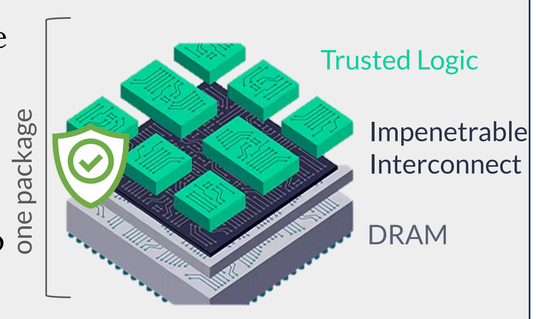


Version Number Merkle Tree

- A **non-repeating version number** for each memory block
- Version numbers **stored in memory** as leafs of a Merkle tree
- Root of Mekle tree securely stored on the trusted processor.
- Traverse the tree to verify freshness.

SMART MEMORY

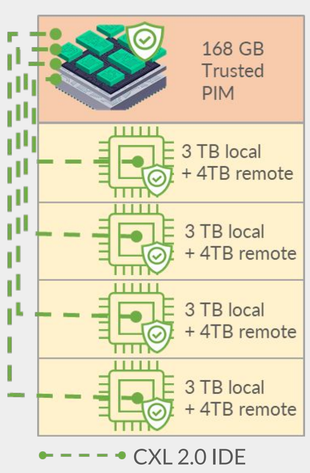
- Logic and memory tightly integrated in the same package
- Layers connected via Through Silicon Via (TSV) and/or µ-bumps: impenetrable without breaking the silicon packaging.
- Expensive: 5x - 10x $ per byte compared to DDR DRAM



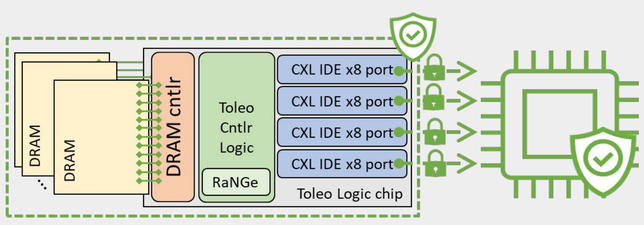
DESIGN

Toleo as the root of trust for freshness for **securely storing stealth versions.**

- Toleo: Trusted smart with crypto logic closely integrated with DRAM.
  - Establishes secure channel (CXL IDE) between the trusted processor and Toleo using crypto local onboard
  - Trusted version compression logic



Toleo Protected Rack



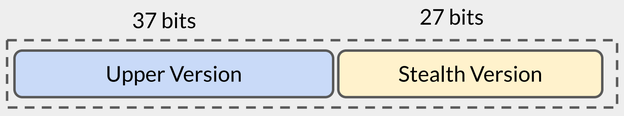
Toleo Design

- Expanding trust from CPU -> smart memory logic
- One device shared across multiple nodes on a rack
- Version Compression to save PIM space.

DESIGN

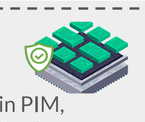
Version Compression #1: **Partial Stealth Version**

✗ strictly non-repeating versions
✔ randomized stealth version



Chance of replay attack due to shortened stealth version is <1.7e-19 in 8 years.

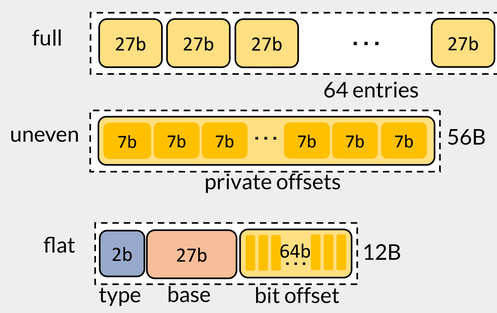

in main memory


in PIM, freshness guaranteed.

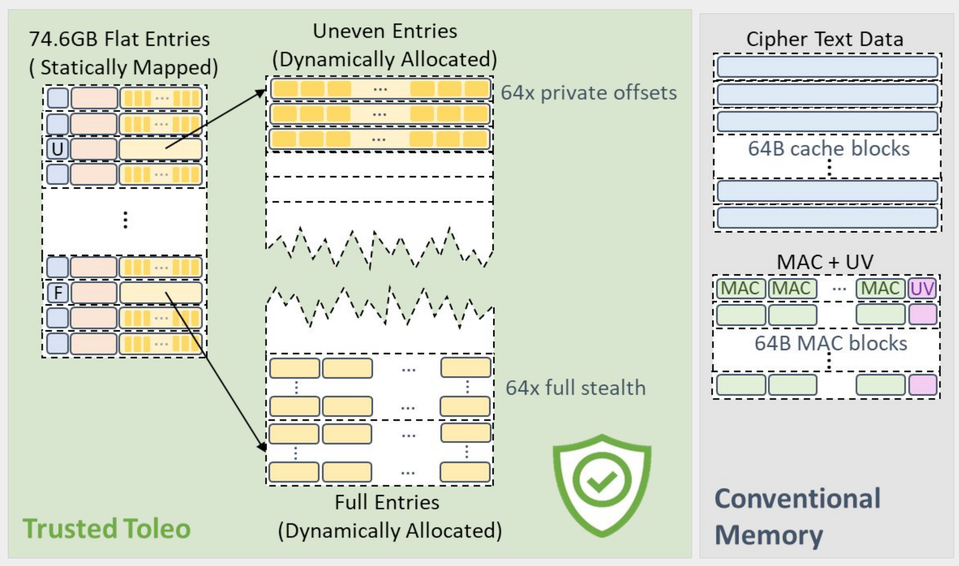
Version Compression #2: **Trip format**

Version locality:

Adjacent values are written similar amount of times due to Spatial locality



- 64 cache blocks from a page share a version base
- \+ 1 bit, 7 bit or 27 bit private offset
- On-demand upgrade

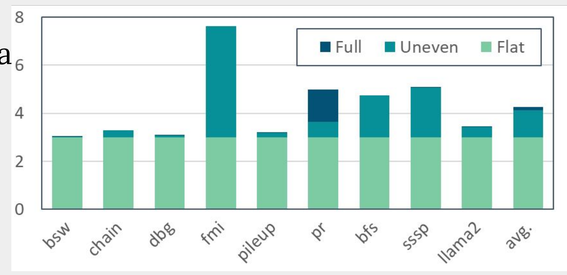


EVALUATION

2% overhead for providing freshness support via Toleo.
Comparable to an expensive all PIM[2] solution.

5.1GB Toleo usage per TB Protected Data

A single PIM device from UPMEM holds 168 GB
-> protects **28 TB** data across the rack



Peak Toleo Usage per TB Protected Data

SUMMARY

Problem:

Merkle-Tree for maintaining versions doesn't scale.

128 MB protected main memory from Intel's implementation.

Intel is dropping freshness to scale to large memory[3]

128MB → 28TB

Solution:

Trusted memory (trusted logic in PIM) to store versions

168 GB of trusted PIM can support nearly 28 TB of main memory

Negligible performance overhead

REFERENCES

[1] Shay Gueron. A memory encryption engine suitable for general purpose processors. Cryptology ePrint Archive, Paper 2016/204, 2016. https://eprint.iacr.org/2016/204.
[2] Shaizeen Aga and Satish Narayanasamy. Invisimem: Smart memory defenses for memory bus side channel. ACM SIGARCH Computer Architecture News, 45(2):94–106, 2017.
[3] Amy Santoni Simon Johnson, Raghunandan Makaram and Vinnie Scarlata. Supporting Intel SGX on Multi-Socket Platform. Technical report, Intel Corporation, 2022.

ASPLOS 2025