SCAR: Selective Cache Address Remapping for Mitigating Cache Side-Channel Attacks

Pavitra Prakash Bhade
Indian Institute of Technology Goa, India
pavitra19231101@iitgoa.ac.in

Olivier Sentieys
University of Rennes, Inria, France
olivier.sentieys@inria.fr

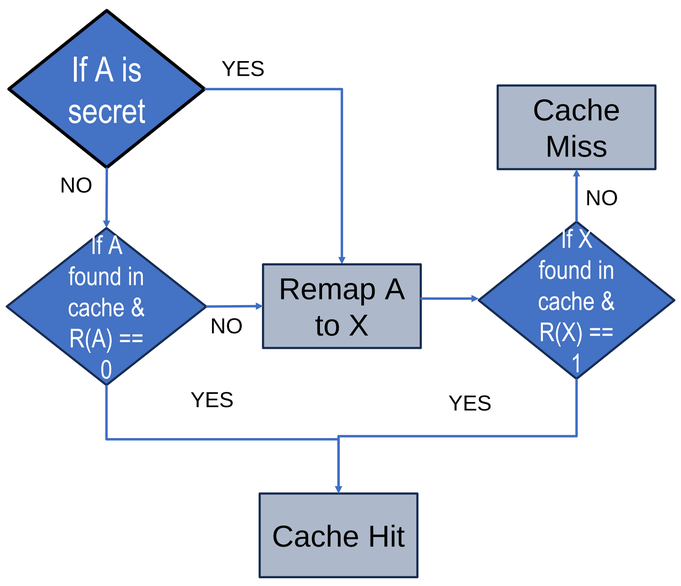
Sharad Sinha
Indian Institute of Technology Goa, India
sharad@iitgoa.ac.in

Introduction

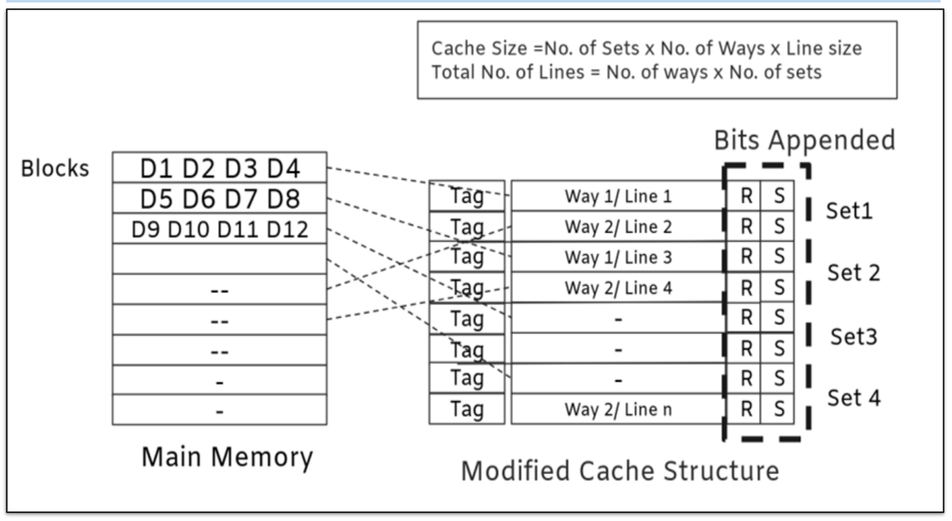
- Cache side-channel attacks (CSCA), exploiting cache conflicts, pose serious risks in shared cache environments.
- Current defenses rely on full encryption of cache mappings to prevent eviction-based attacks like Flush+Reload, Prime+Probe.
- Full mapping encryption introduces significant performance overhead and is vulnerable to predictive analysis due to uniform address coverage.
- SCAR is a selective mapping technique that encrypts only critical regions, reducing attack surfaces and performance impact.
- The approach requires minimal changes to cache micro-architecture and replacement policies, making it ideal for RISC-V systems.
- Implementation on a RISC-V core shows only negligible performance overhead with improved security.

Proposed Algorithms and Cache Structure

Cache Search

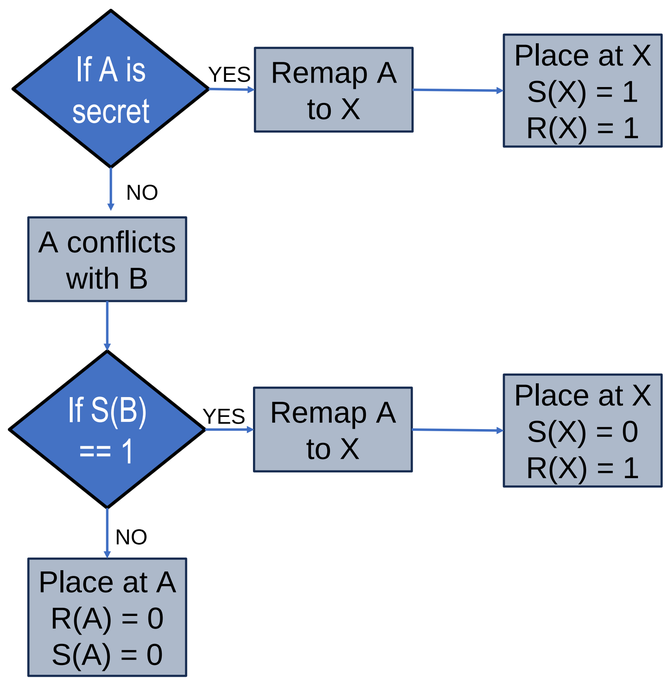


SCAR Cache Structure



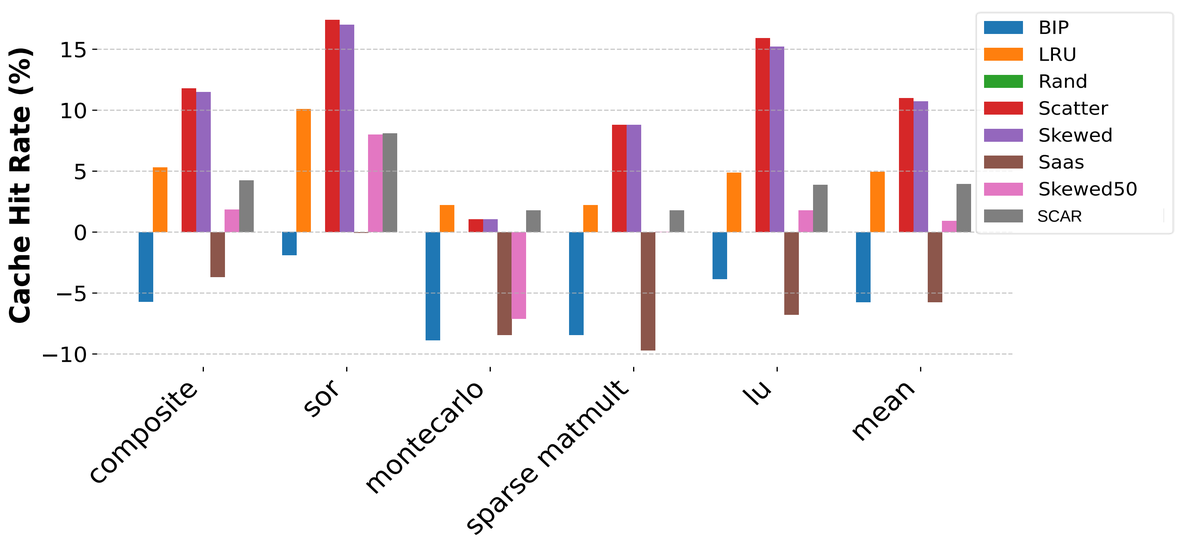
- Each cache line is appended with S (“SECRET”) and R (“REMAPPED”) bits
- SCAR is integrated with Comet RISC V processor - remap logic is described in HLS in the cache controller of the processor.
- This is transformed into the Register-Transfer Level (RTL) description using the Catapult HLS High-Level Synthesis (HLS) toolchain.
- This RTL description is further fed to Synopsys Design Compiler to transform it into a gate-level netlist using a 28nm FDSOI technology.

Cache Replacement

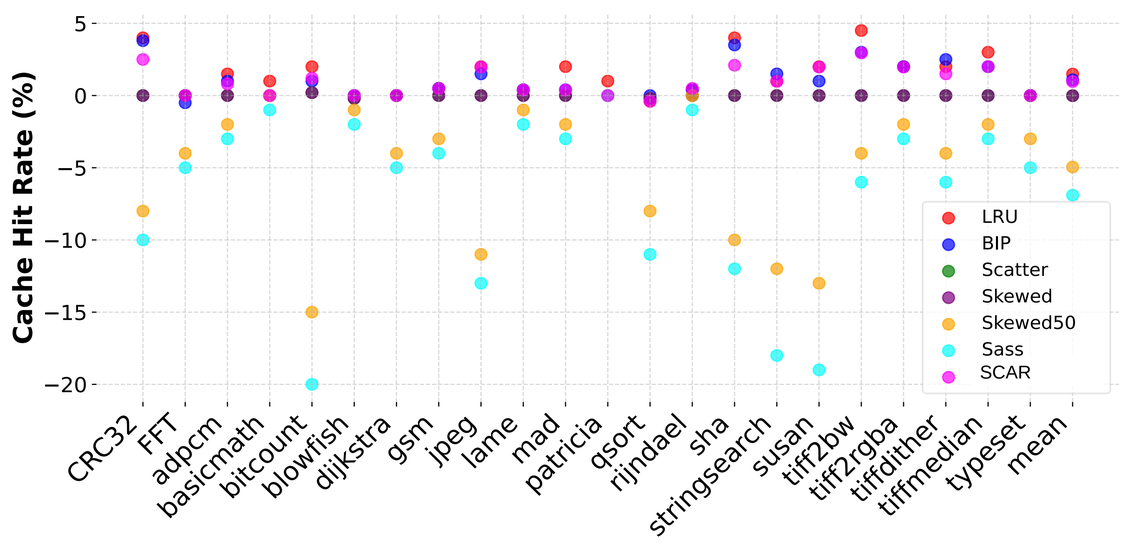


Results

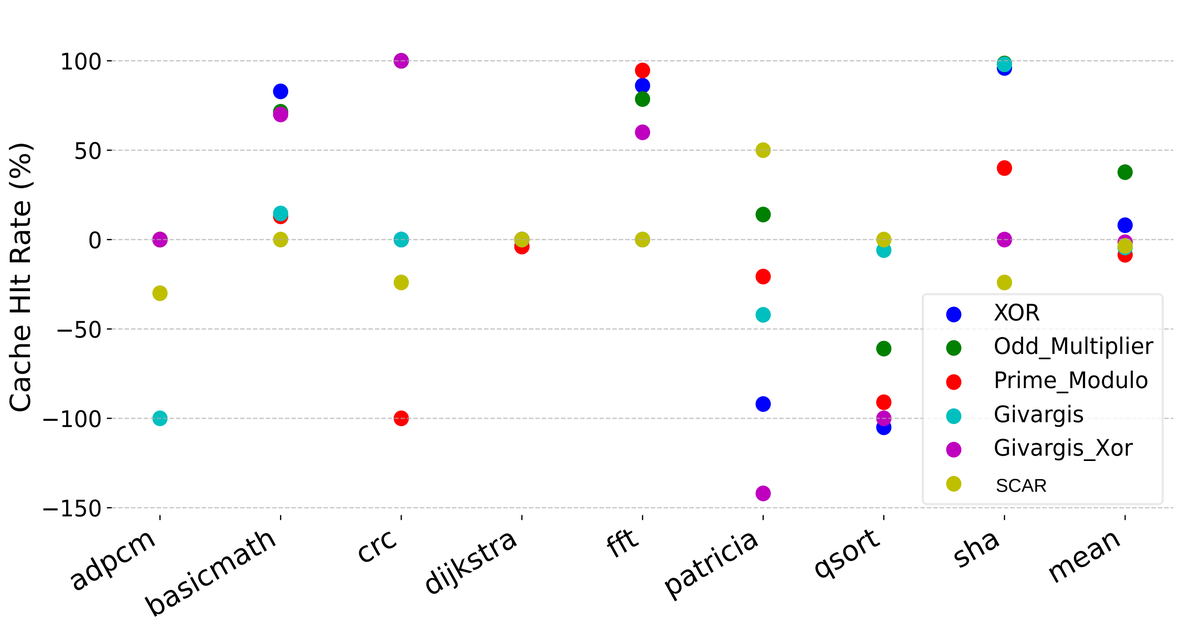
Cache hit comparison on 32KB cache with SOTA for Scimark2 (baseline Rand)



Cache hit comparison on 32KB cache with SOTA for MiBench (baseline Rand)



Cache hit rate comparison on different cache indexing schemes for 32KB cache with MiBench



Conclusion

- Targeting RISC-V cores, we propose a minimal enhancement in the cache microarchitecture and replacement policy to mitigate conflict-based CSCA.
- We introduce SCAR, selective remapping through modified cache structure and search/replacement policies, targeting only conflict-prone secret instructions.
- This approach limits cache hit reduction to less than 2% (5–6% in prior techniques) and improves performance by 1.18 fewer cycles per instruction, with less than 2% area and power overhead.
- Two additional bits per cache line are used as metadata for mapping and replacement with a small area overhead (0.3%) in a 64B cache line.

RISC-V SUMMIT EUROPE 2025 (Paris, France)