Restore Buffer Overflow Attacks:
Breaking Undo-Based Defense Schemes

Jongmin Lee, Gunjae Koo

Korea University

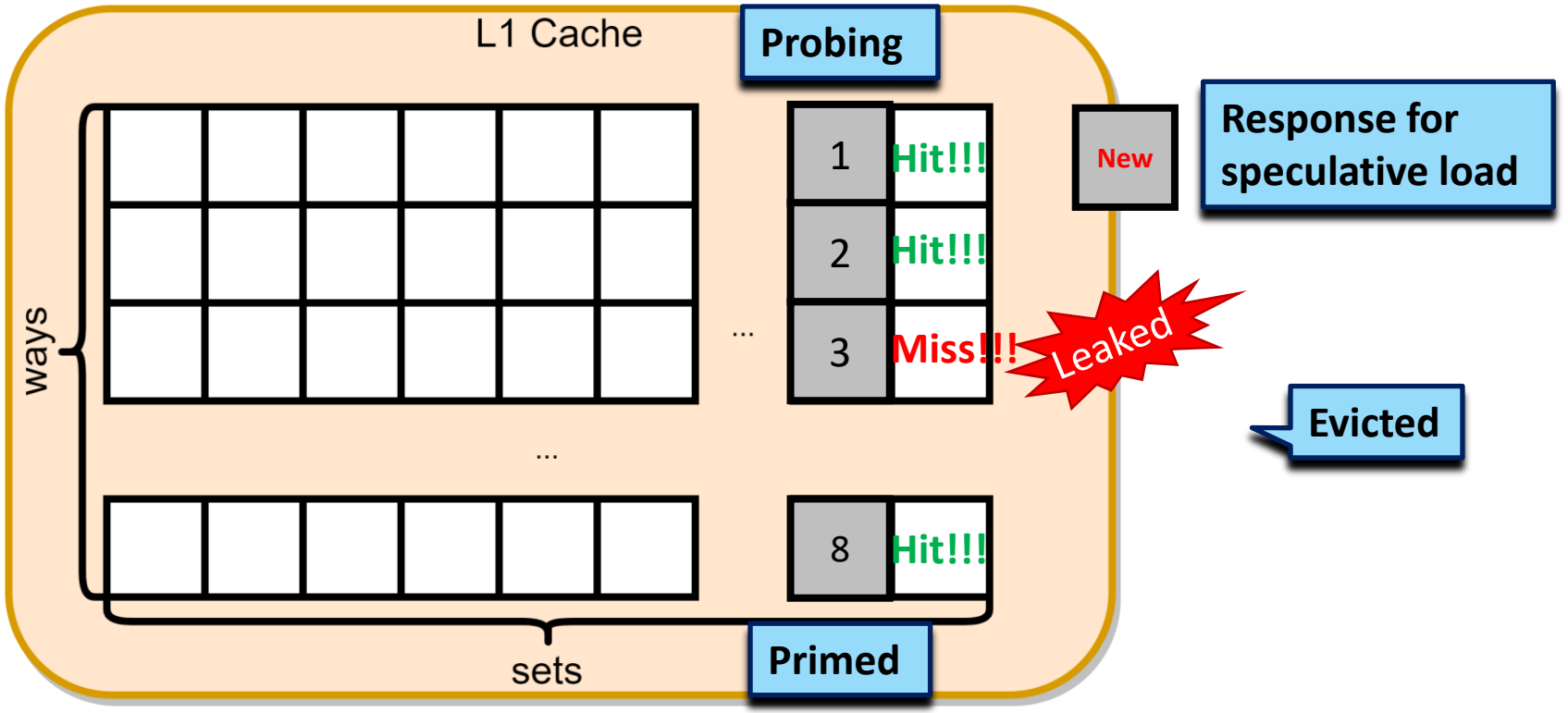
KOREA UNIVERSITY

Outline

- ***Backgrounds***
- ***Idea***
- ***Evaluation***
- ***Conclusion***

Transient Execution Attacks

Prime+Probe Spectre Attack Example

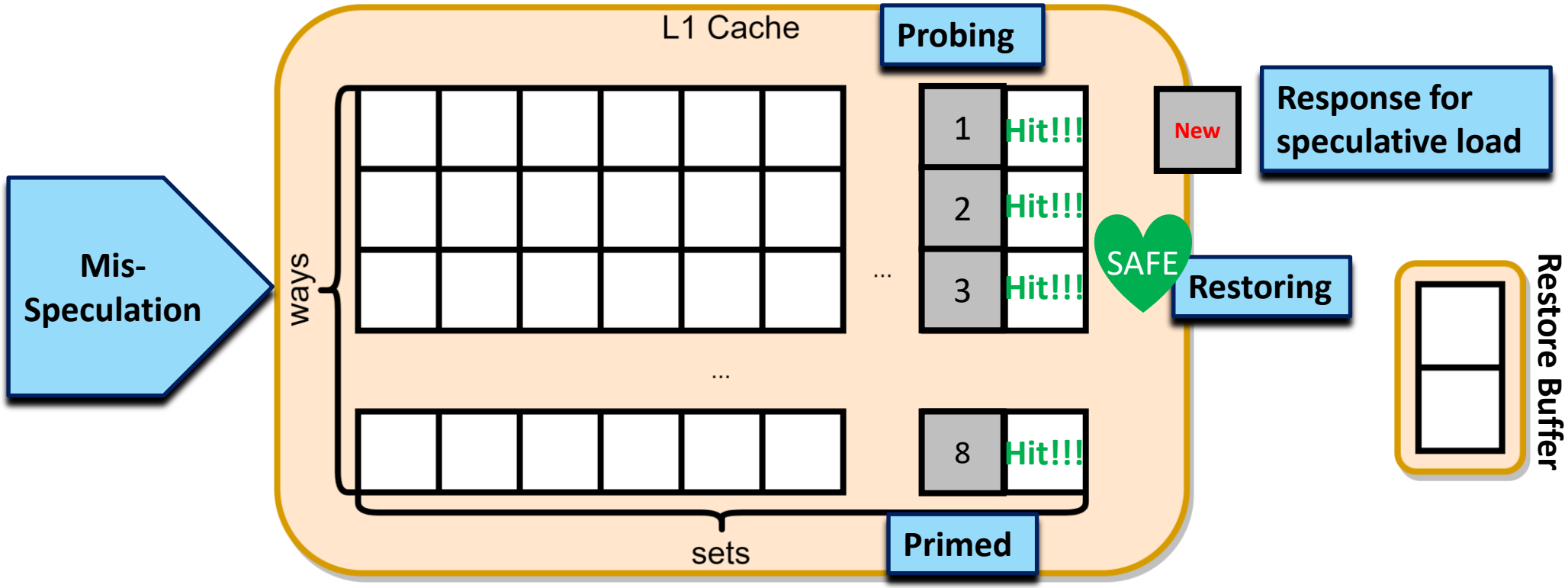


Hardware-Based Mitigations against Spectre

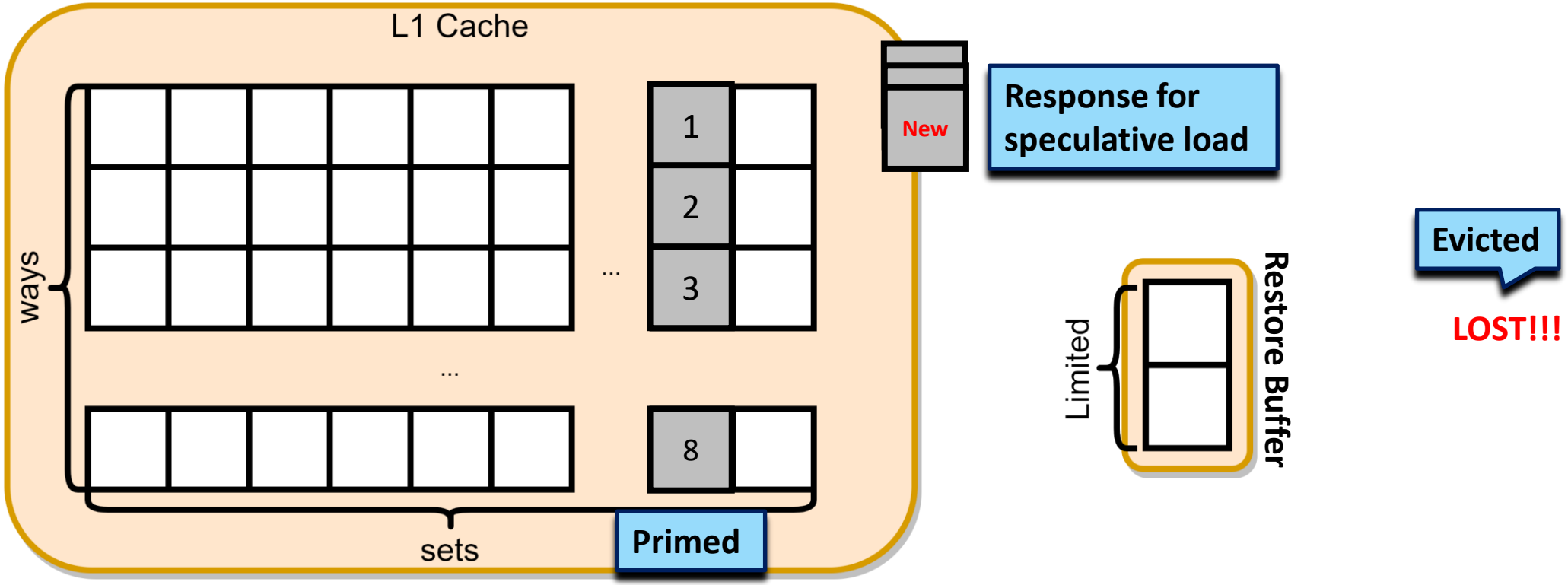
- Delaying
  - InvisiSpec
  - SafeSpec
  - SelectiveDelay

- Restoring (Undo-Style)
  - CleanupSpec
    - Restores data from **L2 cache**
  - ReViCe
    - Restores data from additional **victim cache**

Undo-Style Defense against Prime+Probe

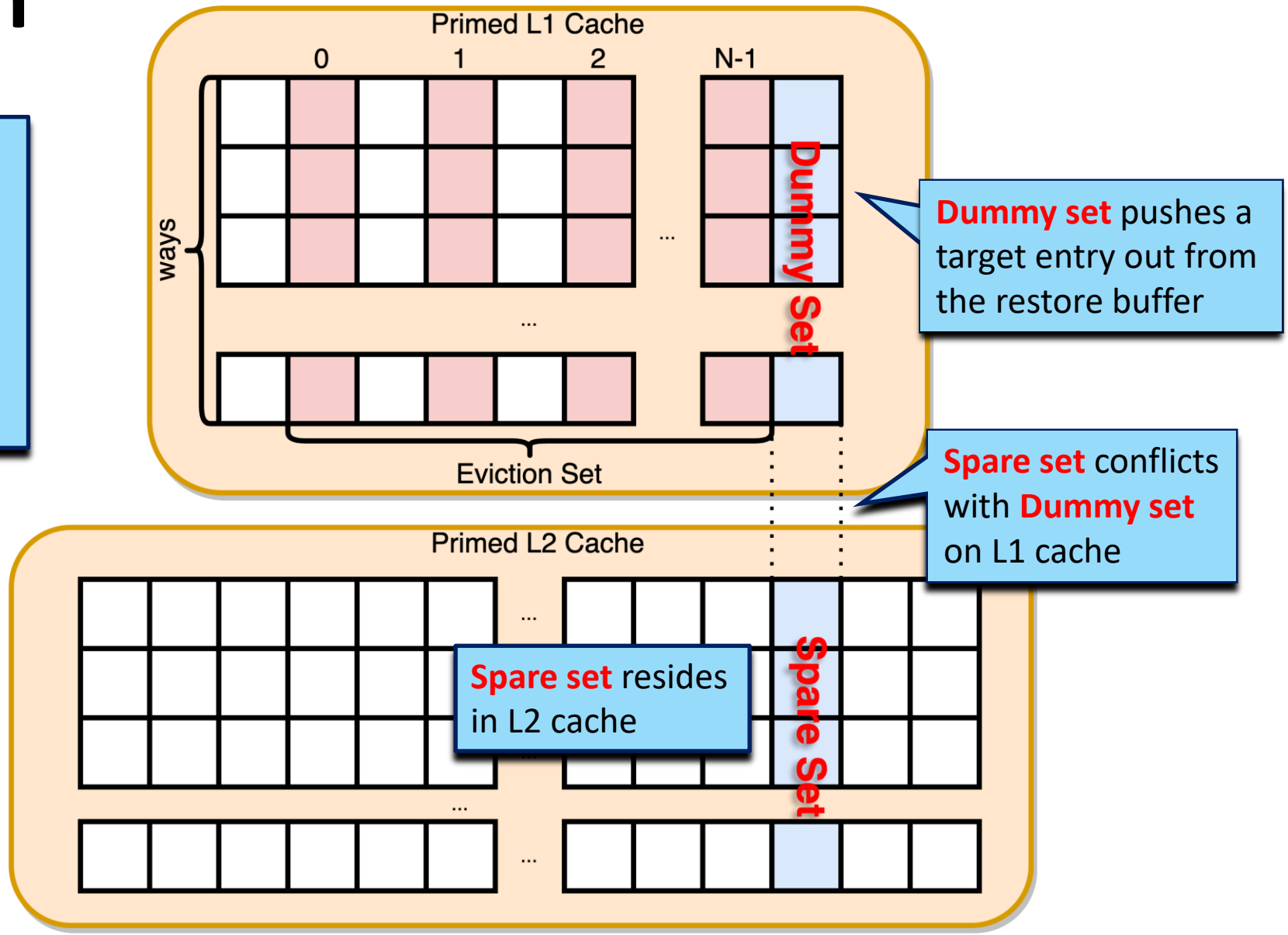


Overflowing the Restore Buffer

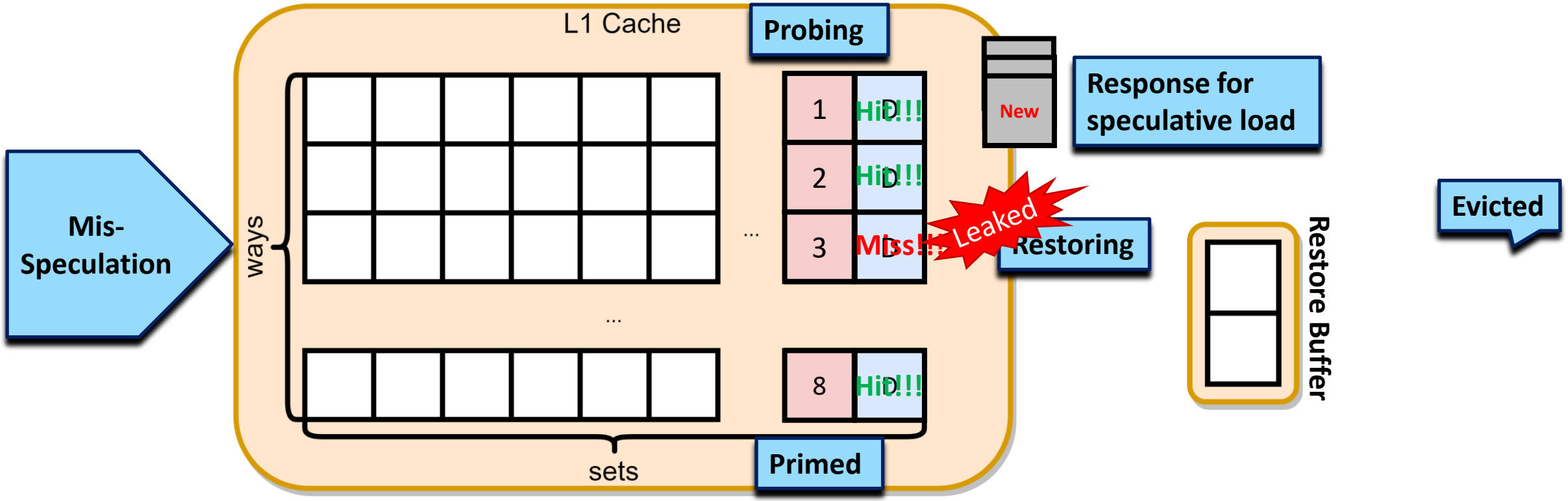


Attack Design

- Consecutive evictions must happen immediately **after** accessing the secret value
- Consecutive evictions must happen **before** the speculation is resolved



Restore Buffer Overflow Attack

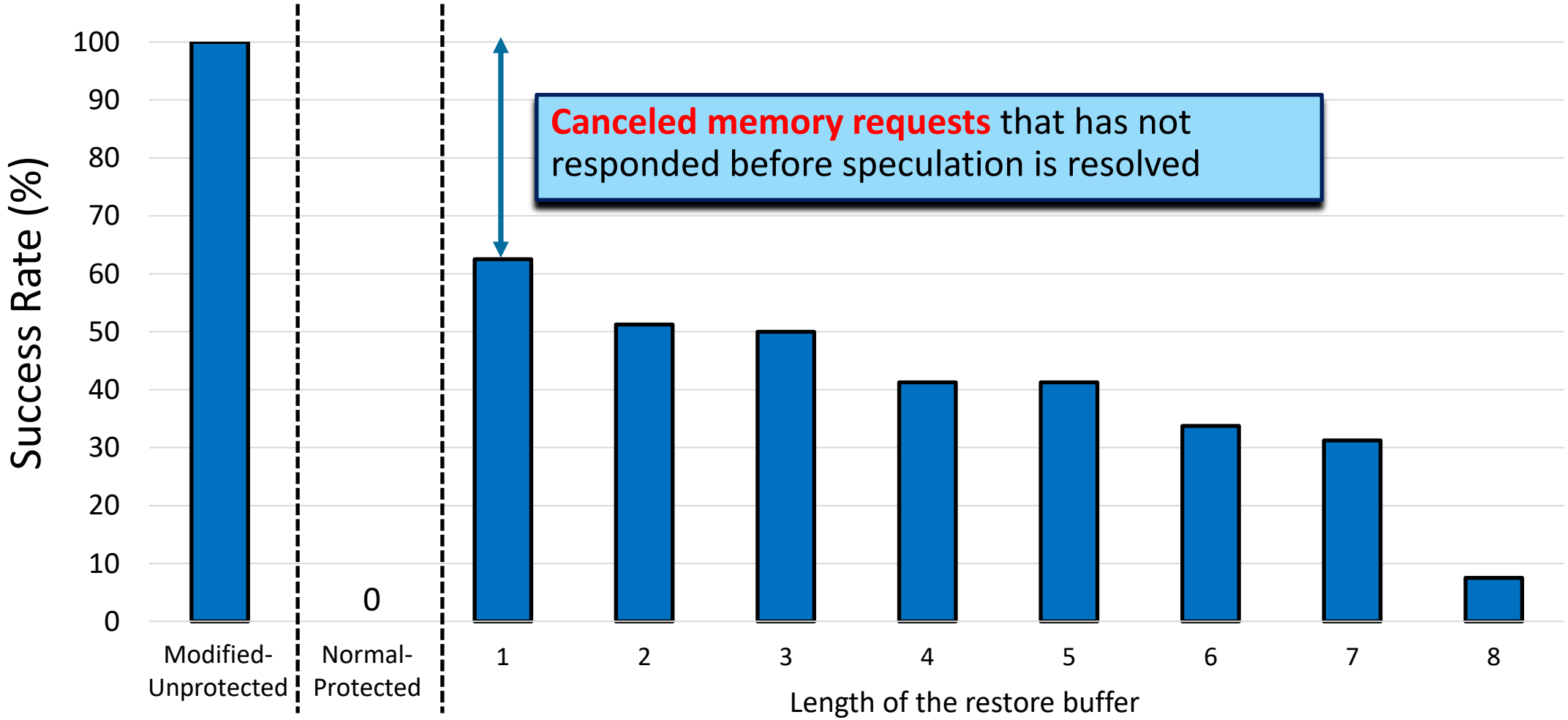


Evaluation

- Gem5 with SE mode
- Protected by undo-style defense with a restore buffer nearby L1 cache

Parameter	Configuration
Core	x86 ISA, out-of-order, no SMT, 64 IQ entries, 192 ROB entries, 32 LQ entries, 32 SQ entries
Branch Predictor	L-TAGE
L1-I cache	32 KB, 64B line, 8-way
L1-D cache	32 KB, 64B line, 8-way, 8 MSHR entries
L2 cache	256 KB, 64B line, 8-way
Data prefetcher	Disabled

Attack Results



Conclusion

- ***Limited restore buffer resources***
  - Undo-style defense relies on the limited restore buffer space
  - New side-channel: overflowing the restore buffer
- ***Characteristics of the attack***
  - Processor is more secure with larger restore buffer
  - Part of in-flight memory requests can be cancelled by the undo-style defense before speculation is resolved

Thank you

Restore Buffer Overflow Attacks: Breaking Undo-Based Defense Schemes

Jongmin Lee, Gunjae Koo

✉ **flackekd@korea.ac.kr**