# Cross-Core Prime+Probe Attacks on Non-inclusive Caches

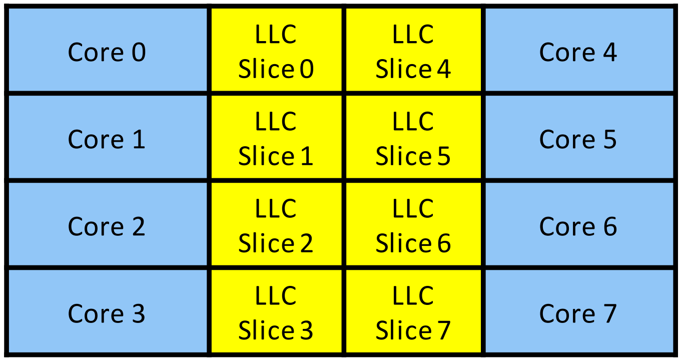
**Mengjia Yan**, Read Sprabery, Bhargava Gopireddy,
Christopher Fletcher, Roy Campbell, Josep Torrellas

University of Illinois at Urbana-Champaign

# Modern Cache Hierarchies

- Modern systems are moving to non-inclusive cache hierarchies
  - Latest Intel server processor uses non-inclusive caches

| | **Skylake-S<br>(Sep 2015)** | **Skylake-X/Skylake-SP<br>(Jun 2017)** |
|---|---|---|
| L2 | 256KB/core<br>16-way, inclusive | 1MB/core<br>16-way, inclusive |
| LLC | 2MB/core<br>16-way, **inclusive** | 1.375MB/core<br>11-way, **non-inclusive** |



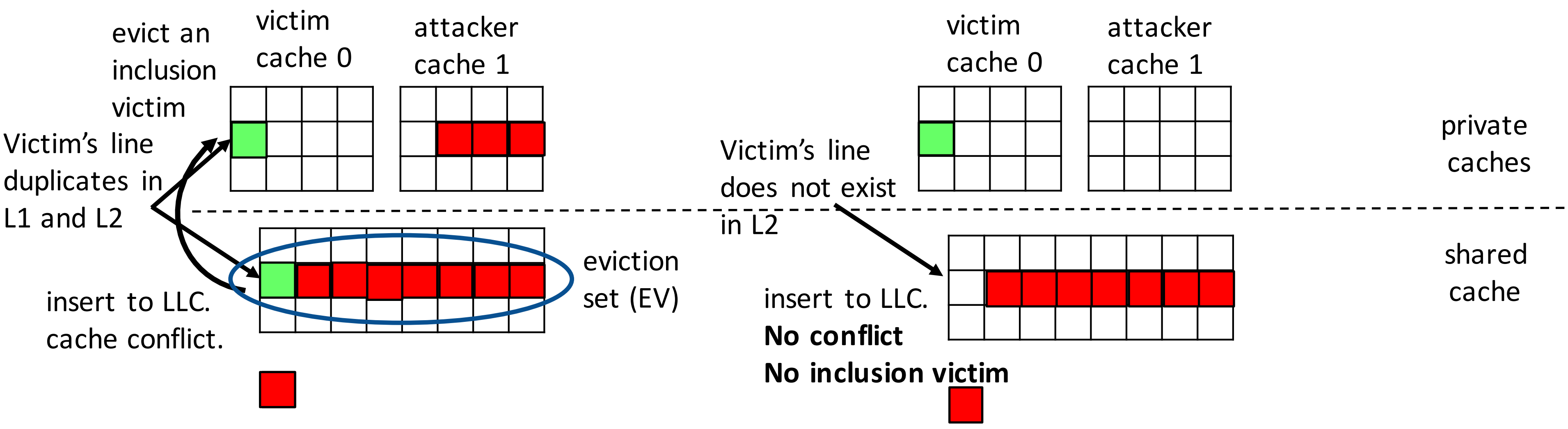
| | | | |
|---|---|---|---|
| Core 0 | LLC<br>Slice 0 | LLC<br>Slice 4 | Core 4 |
| Core 1 | LLC<br>Slice 1 | LLC<br>Slice 5 | Core 5 |
| Core 2 | LLC<br>Slice 2 | LLC<br>Slice 6 | Core 6 |
| Core 3 | LLC<br>Slice 3 | LLC<br>Slice 7 | Core 7 |

- Existing conflict-based attacks do not work on sliced non-inclusive caches

# Challenges of Prime+Probe Attacks

- Lack of Visibility into the Victim's Private Cache

🟩 target address 🟥 eviction addresses



evict an inclusion victim

victim cache 0

attacker cache 1

Victim's line duplicates in L1 and L2

insert to LLC. cache conflict.

eviction set (EV)

victim cache 0

attacker cache 1

Victim's line does not exist in L2

insert to LLC.

**No conflict**

**No inclusion victim**

private caches

shared cache

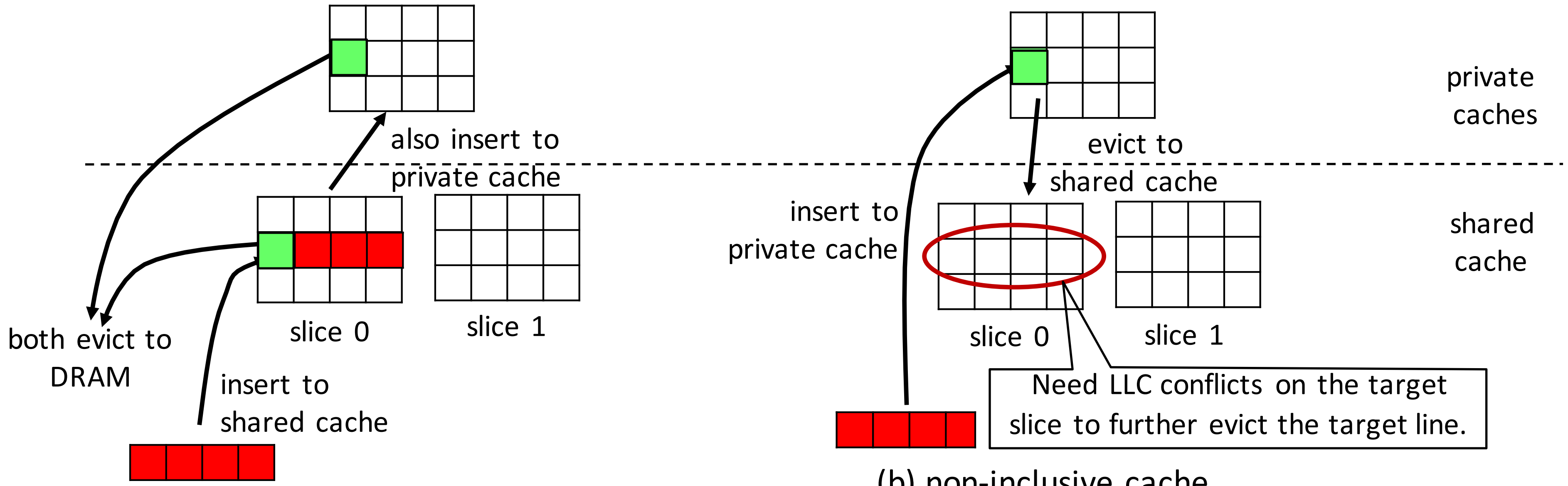
(a) inclusive cache

(b) non-inclusive cache

# Challenges of Prime+Probe Attacks

- Eviction Set Construction is Hard

🟩 target address 🟥 eviction address



private caches

shared cache

also insert to private cache

both evict to DRAM

insert to shared cache

slice 0

slice 1

(a) inclusive cache

evict to shared cache

insert to private cache

slice 0

slice 1

Need LLC conflicts on the target slice to further evict the target line.

(b) non-inclusive cache

Eviction is only determined by the LLC replacement policy.

Eviction is affected by the replacement policies in multiple caches, and address slice distributions.

# Contributions

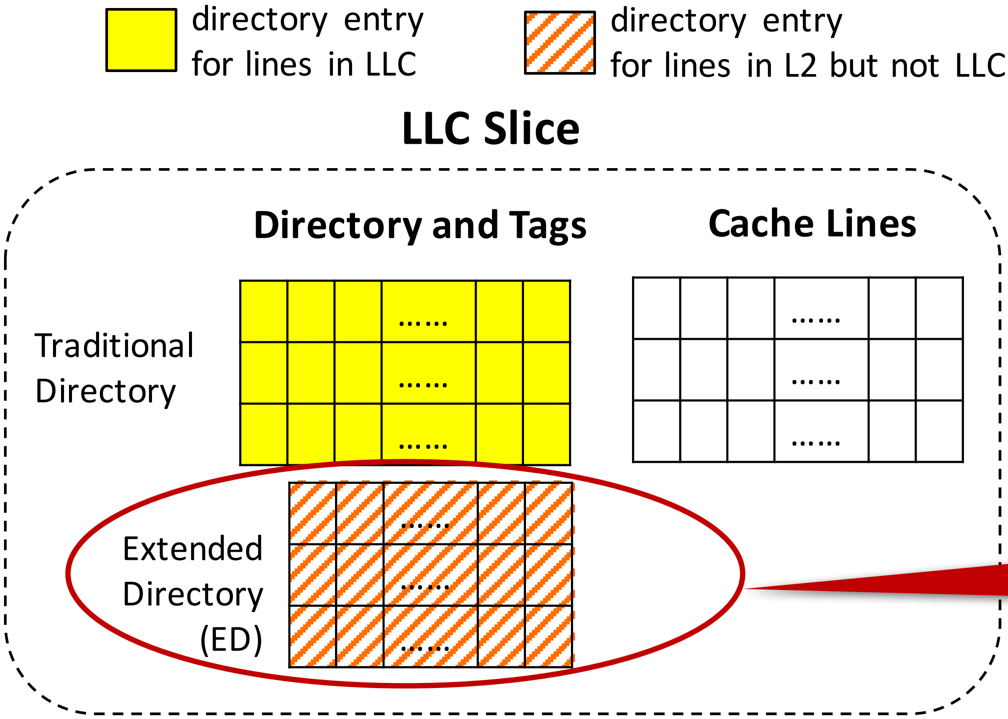
1) We develop an algorithm to create Eviction Set on sliced non-inclusive caches.
2) We reverse engineer the directory structure in Intel Skylake-X processors.

Previous attacks on inclusive caches are an example of directory attack.

3) We identify that directory as a **unified** structure to bootstrap conflict-based cache attacks for different cache hierarchies.
4) Based on our insights into the directory, we design the first Prime+Probe attack on sliced non-inclusive LLCs.

# The Inclusive Directory Structure

- Insight: Directory must be inclusive to maintain tracking information for all the cache lines resident in the cache hierarchies.



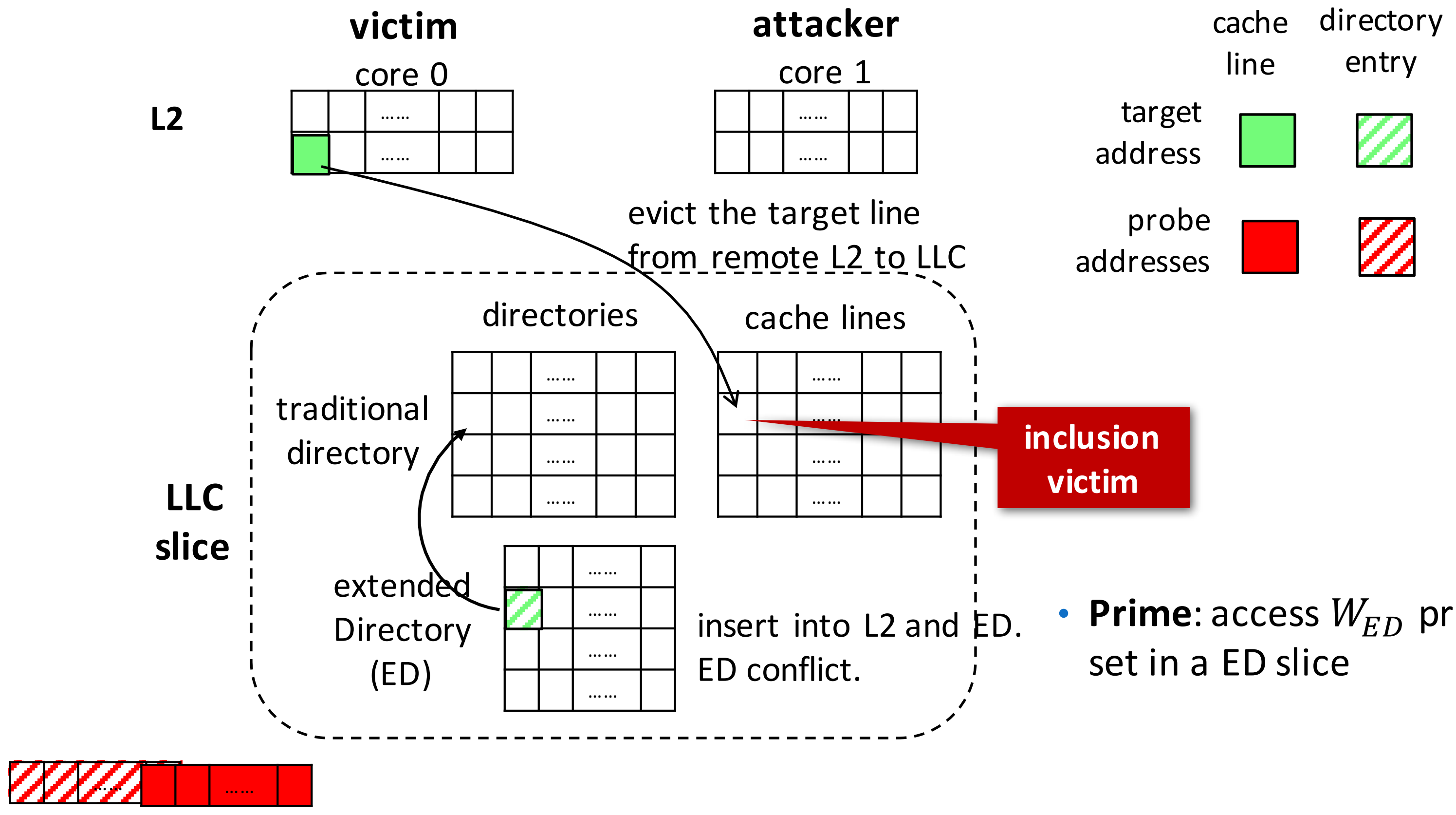
Attack opportunity analysis:

$$W_{ED} = 12 < W_{L2} = 16$$

- Due to the associativity difference, we can create ED conflicts.
- Can ED conflicts lead to inclusion victims?

**The new attack surface!**

# Creating Inclusion Victims via ED Conflicts



**victim**

core 0

**attacker**

core 1

**L2**

evict the target line from remote L2 to LLC

**LLC slice**

directories

cache lines

traditional directory

extended Directory (ED)

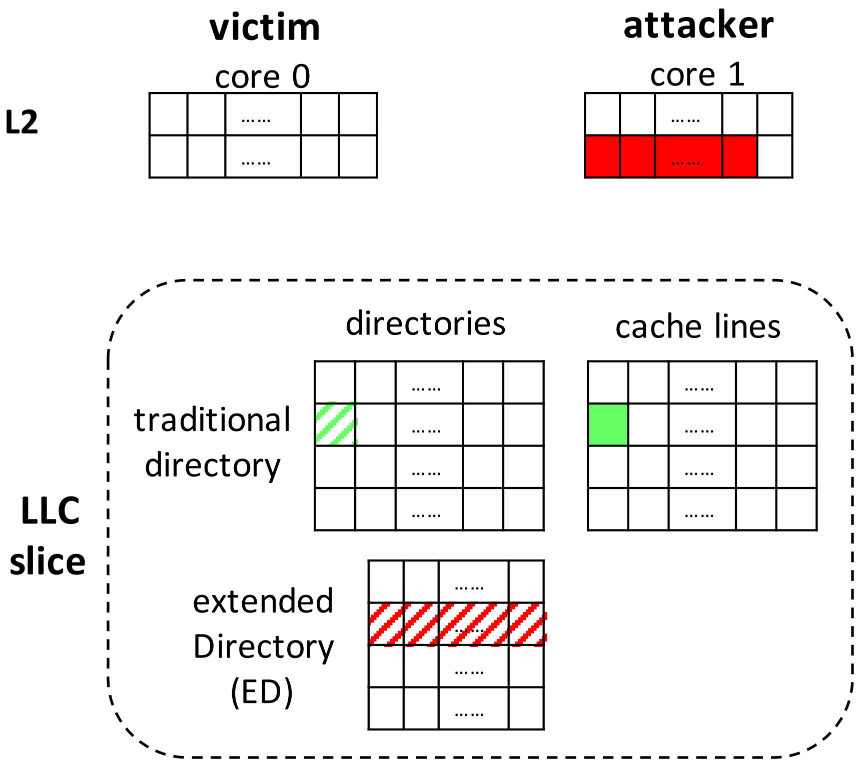
insert into L2 and ED. ED conflict.

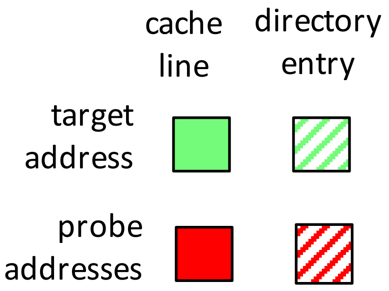
**inclusion victim**

|  | cache line | directory entry |
|---|---|---|
| target address | 🟩 | ▨ |
| probe addresses | 🟥 | ▨ |

- **Prime**: access $W_{ED}$ probe lines to occupy the target set in a ED slice

# Prime+Probe Attacks Targeting the Directory

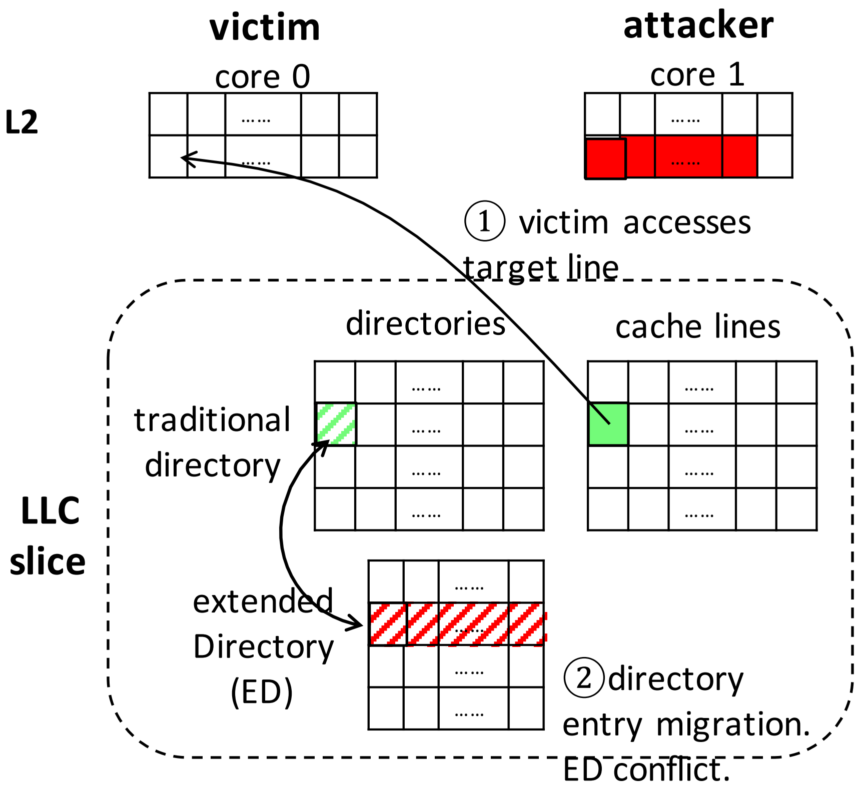




- **Prime**: access $W_{ED}$ probe lines to occupy the target set in a ED slice
- **Wait**: wait for the victim to perform an access
- **Probe**: re-access the $W_{ED}$ probe lines and measure access latency

victim does not perform access
→ Probe latency is short

# Prime+Probe Attacks Targeting the Directory



| | cache line | directory entry |
|---|---|---|
| target address | 🟩 | ▨ |
| probe addresses | 🟥 | ▨ |

- **Prime**: access $W_{ED}$ probe lines to occupy the target set in a ED slice
- **Wait**: wait for the victim to perform an access
- **Probe**: re-access the $W_{ED}$ probe lines and measure access latency

Victim performs access → Probe latency is higher

# Conclusion

- Directory = The unified structure for conflict-based cache attacks

- “Attack Directories, Not Caches: Side-Channel Attacks in a Non-Inclusive World” recently accepted in IEEE Symposium on Security and Privacy (SP’19).

## *More in the Paper*

- Eviction set construction algorithm.
- Steps of reverse engineering the directory structure.
- Root cause analysis of the the vulnerability
- A multi-threaded high-bandwidth Evict+Reload attack.
- Attack results on AMD machines.