# Attack Directories, Not Caches: Side Channel Attacks in a Non-Inclusive World

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

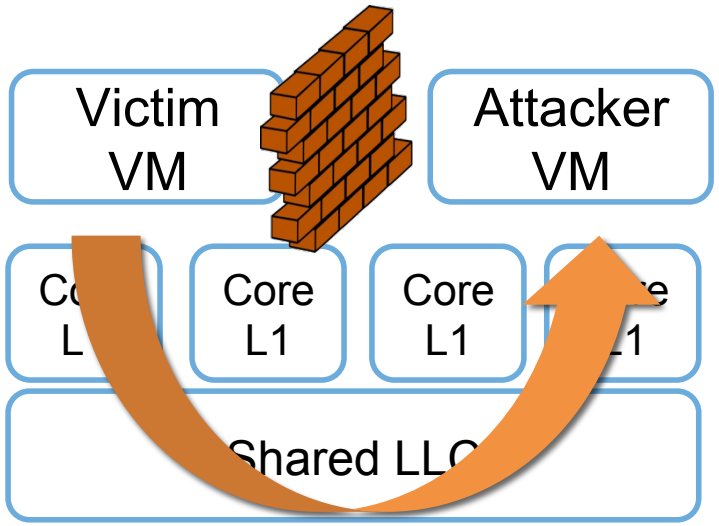
University of Illinois at Urbana-Champaign

S&P'19 May 21

ILLINOIS

# Cache Side Channel Attacks Are Popular And Effective

## VM Isolation




## Attack Platforms


## Target Applications

# Why another cache side channel attack?

# Cache Side Channel Attacks on Inclusive Caches

Flush+Reload

Flush+Flush

Flush+Flush

Prime+Probe

Prime+Abort

Evict+Reload

Invalidate+Transfer

Flush+Prefetch

…….

Conflict-based attacks.

Only demonstrated on **inclusive cache hierarchies.**

# New Intel Processors Use Non-inclusive Caches


Skylake-X/SP
*(released in 2017)*

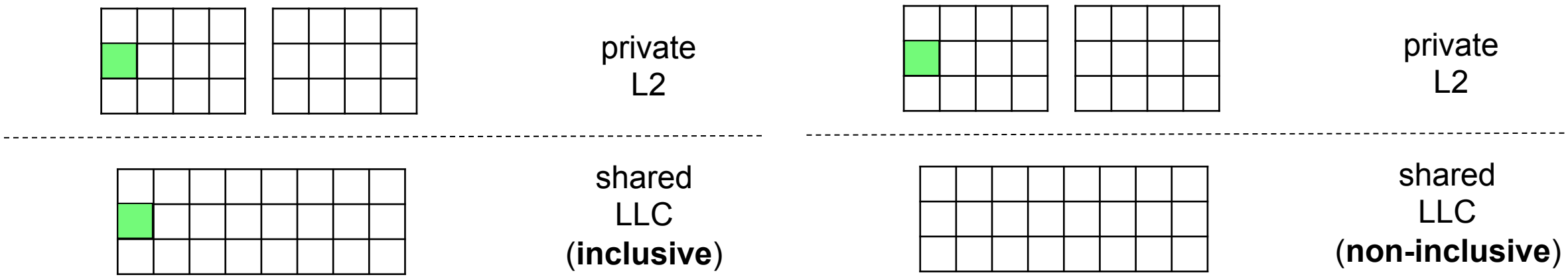
TECHNOLOGY BLOG

**New Intel CPU Cache Architecture Boosts Protection Against Side-Channel Attacks**

We challenge this assumption and prove that it is wrong

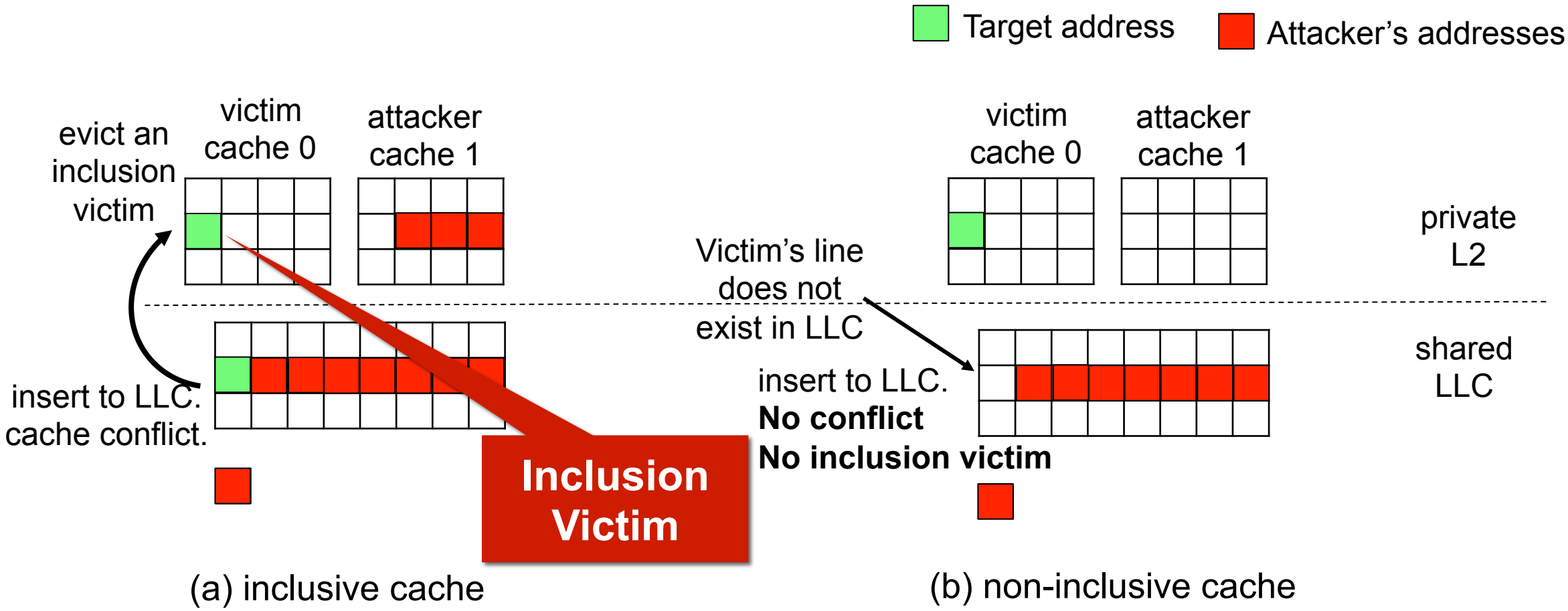
# Inclusive Caches v.s. Non-inclusive Caches

- Inclusive: Private L2 lines are also present in LLC
- Non-inclusive: Private L2 lines *may or may not be* present in LLC



# Challenges of Conflict-based Attacks

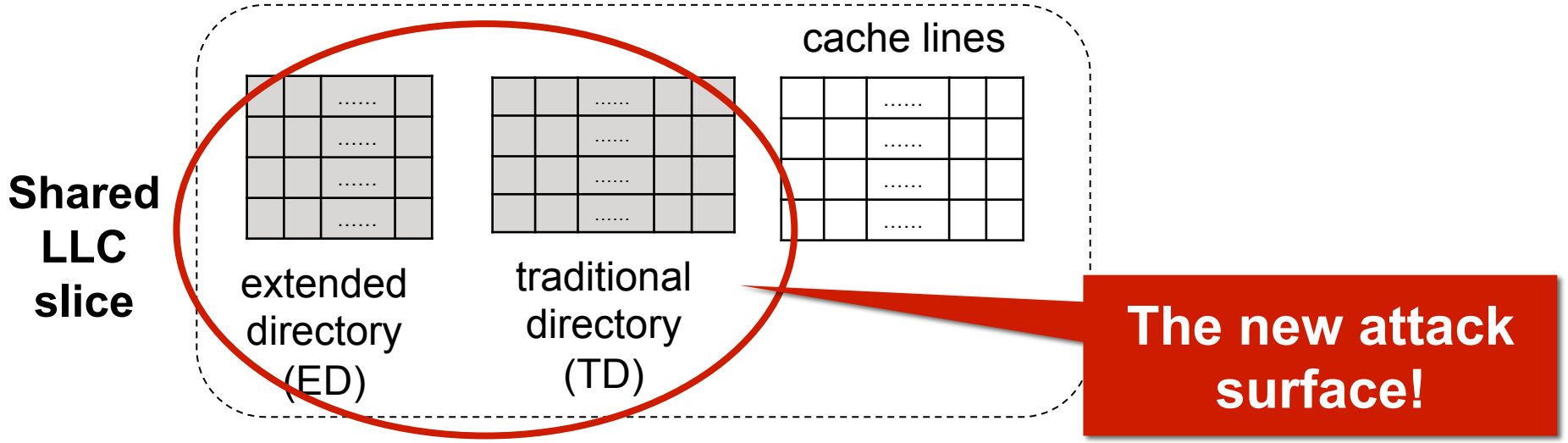
- Lack of Visibility into the Victim's Private Cache



# The Inclusive Directory Structure in Skylake-X

- Directory (snoop filter): tracks presence information for cache lines
- TD holds directory entries for lines in LLC slice
- ED holds directory entries for lines in L2 but not LLC
- Directory is **inclusive**

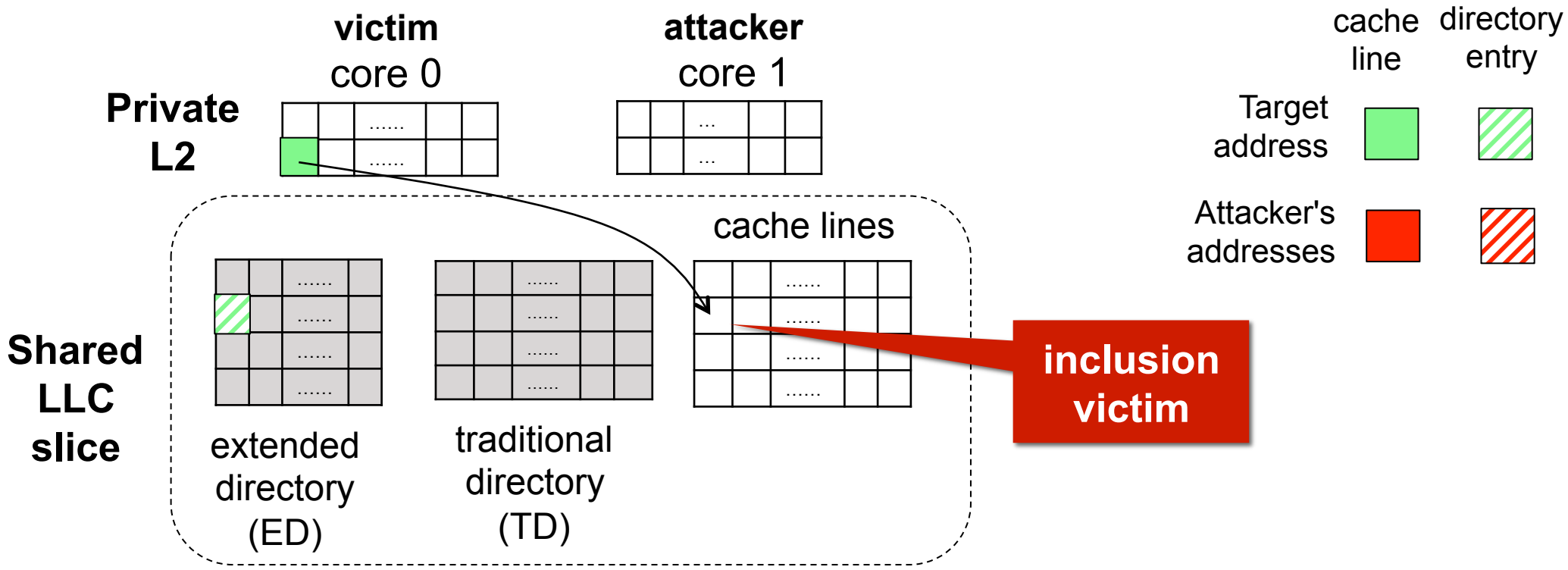
1000 0000



# Prime+Probe Attacks on Skylake-X

**Prime**

- The attacker causes conflicts in ED
  → evict victim's line from L2 to LLC

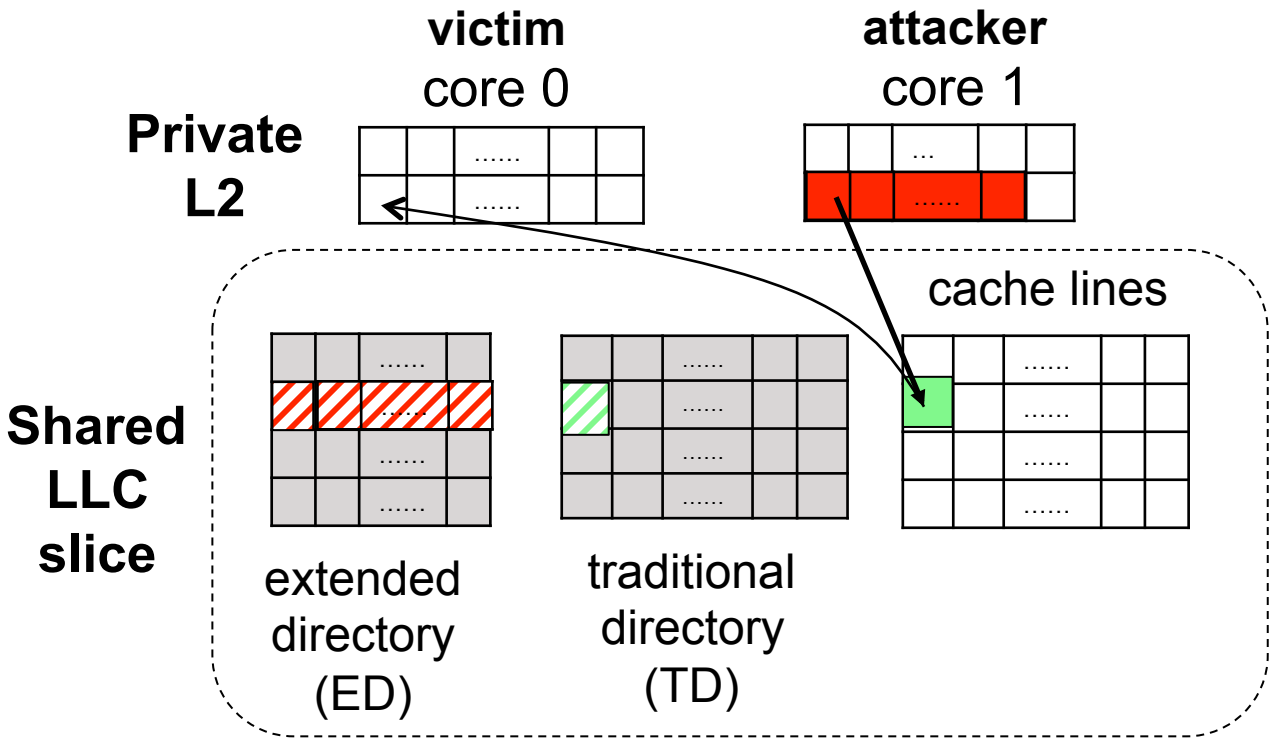


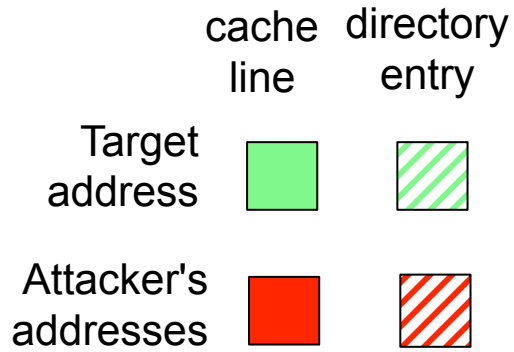
# Prime+Probe Attacks on Skylake-X

**Probe**

- The victim re-accesses the line

  → Directory entry reloaded and attacker can observe



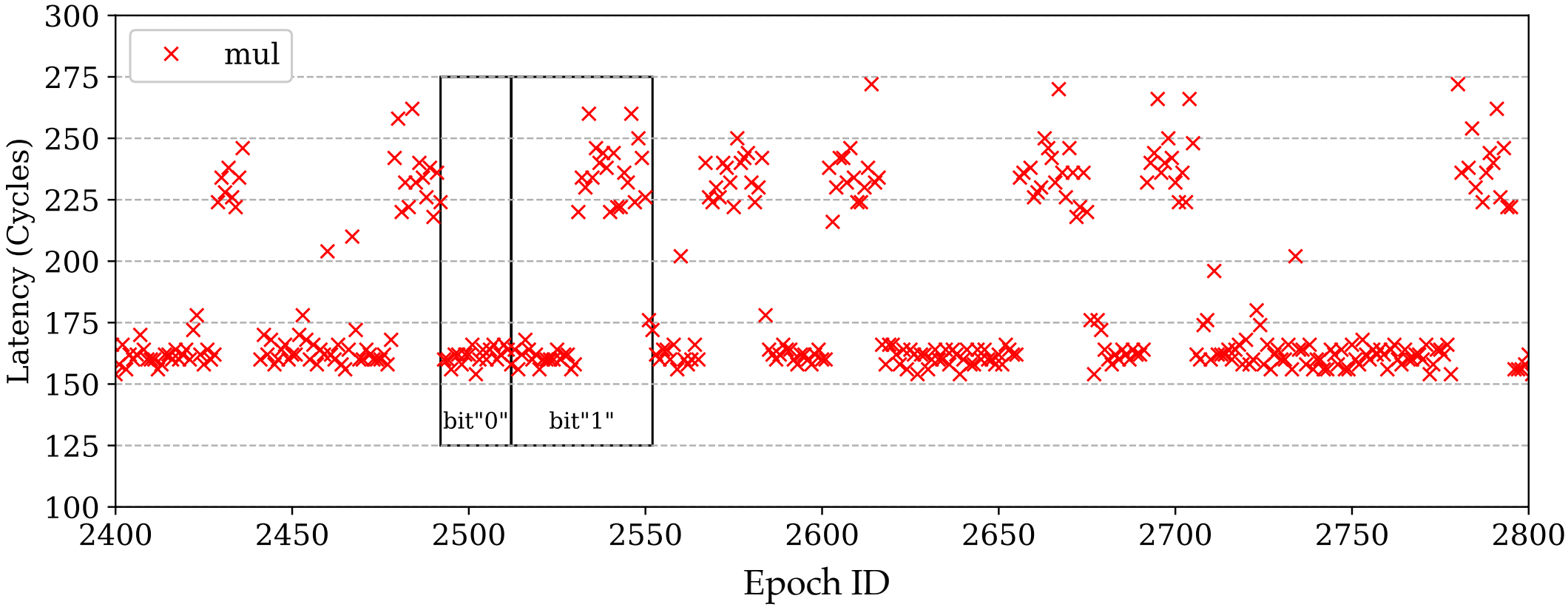



# Evaluation on RSA Encryption Algorithm

- Square-and-Multiply Exponentiation (GnuPG 1.4.13)

```
for i = n-1 to 0 do
        r = sqr(r) mod n
        if e_i == 1 then
                r = mul(r, b) mod n
        end
end
```

# Evaluation Trace




*Access latencies measured in the probe operation in Prime+Probe.*
*A sequence of "01010111011001" can be deduced as part of the exponent.*

# More in the Paper

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

# Countermeasures

- Increase directory associativity → unrealistic
- Way-partition of the directory → not feasible

**SecDir: A Secure Directory to Defeat Directory Side Channel Attacks *[ISCA'19]***

Mengjia Yan, Jen-Yang Wen, Christopher W. Fletcher, and Josep Torrellas

University of Illinois at Urbana-Champaign

# Main Contributions


Reverse engineer
the directory structure

First two cache attacks
on non-inclusive caches

Evaluate on RSA

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

# Thank You!