FETCHBENCH: SYSTEMATIC IDENTIFICATION AND CHARACTERIZATION OF PROPRIETARY PREFETCHERS

Till Schlüter, *Amit Choudhari, Lorenz Hetterich, Leon Trampert, Hamed Nemati, Ahmad Ibrahim, Michael Schwarz, Christian Rossow, Nils Ole Tippenhauer*

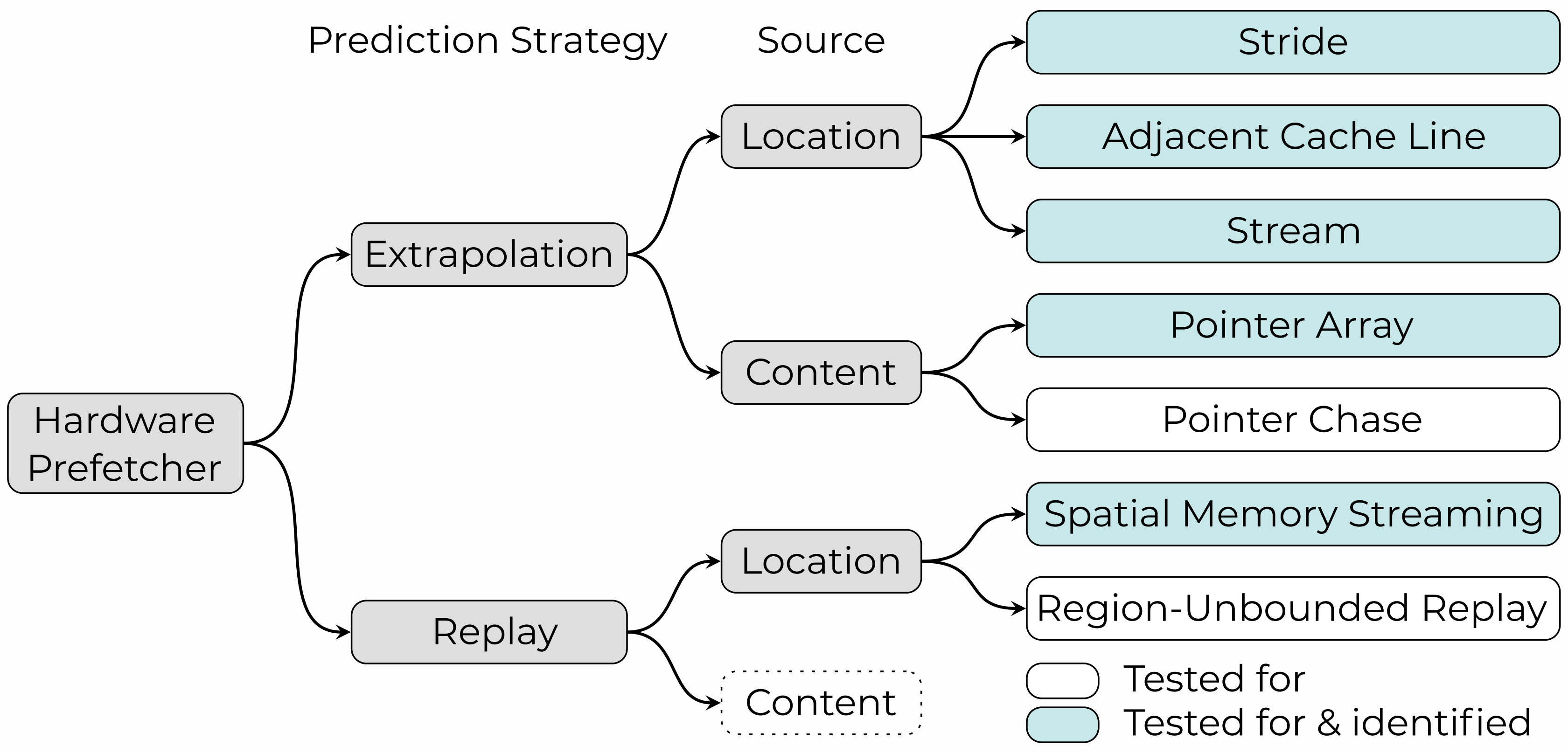
UNKNOWN PREFETCHERS → UNCLEAR SECURITY LEVEL

CPUs implement proprietary prefetchers. Prior work identified **side-channel vulnerabilities** in individual prefetchers, but no systematic analysis has been conducted.

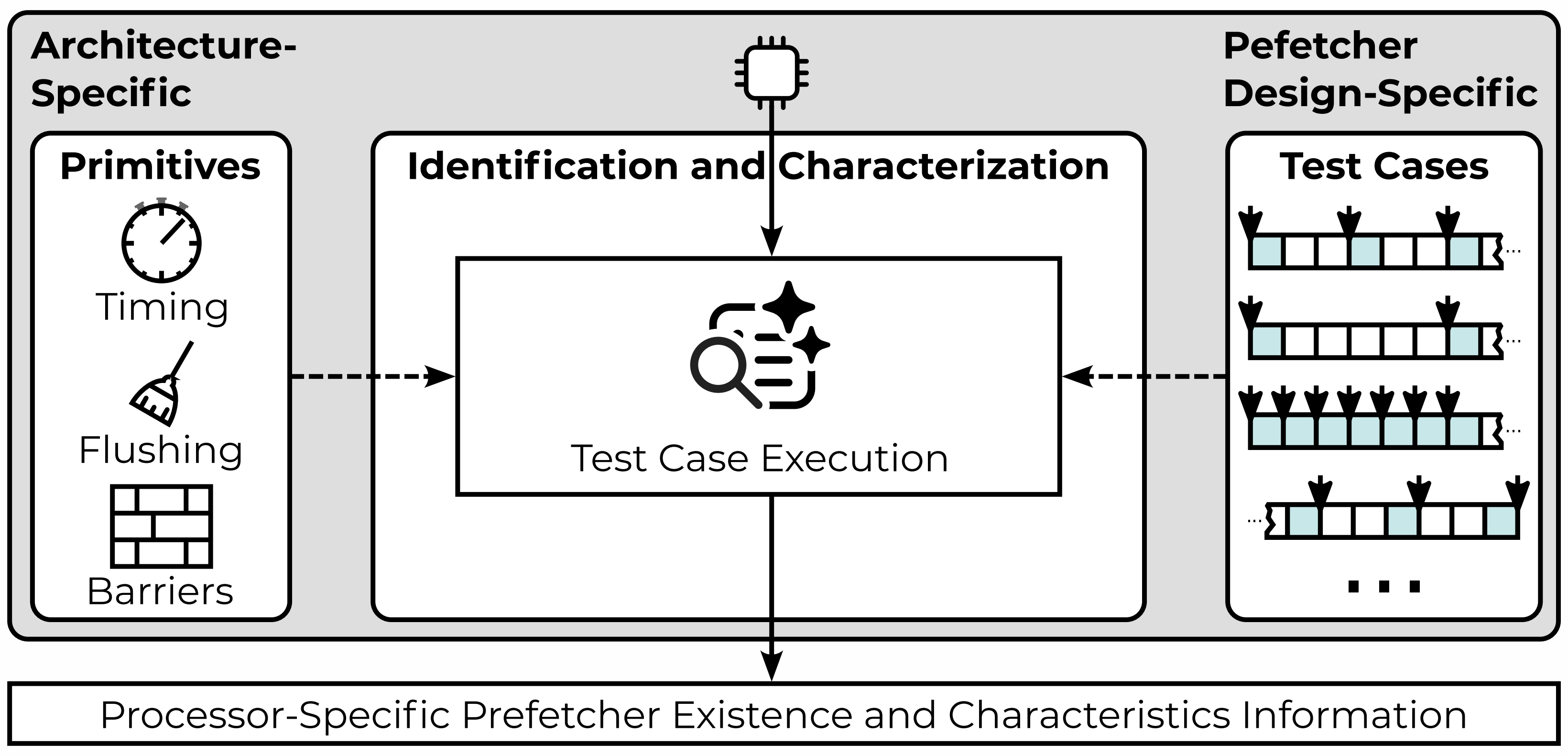
We study prefetcher security systematically:

- **RQ1** How to identify and characterize prefetchers?
- **RQ2** What prefetchers are regularly implemented?
- **RQ3** What are the security implications?

OUR PREFETCHER TAXONOMY



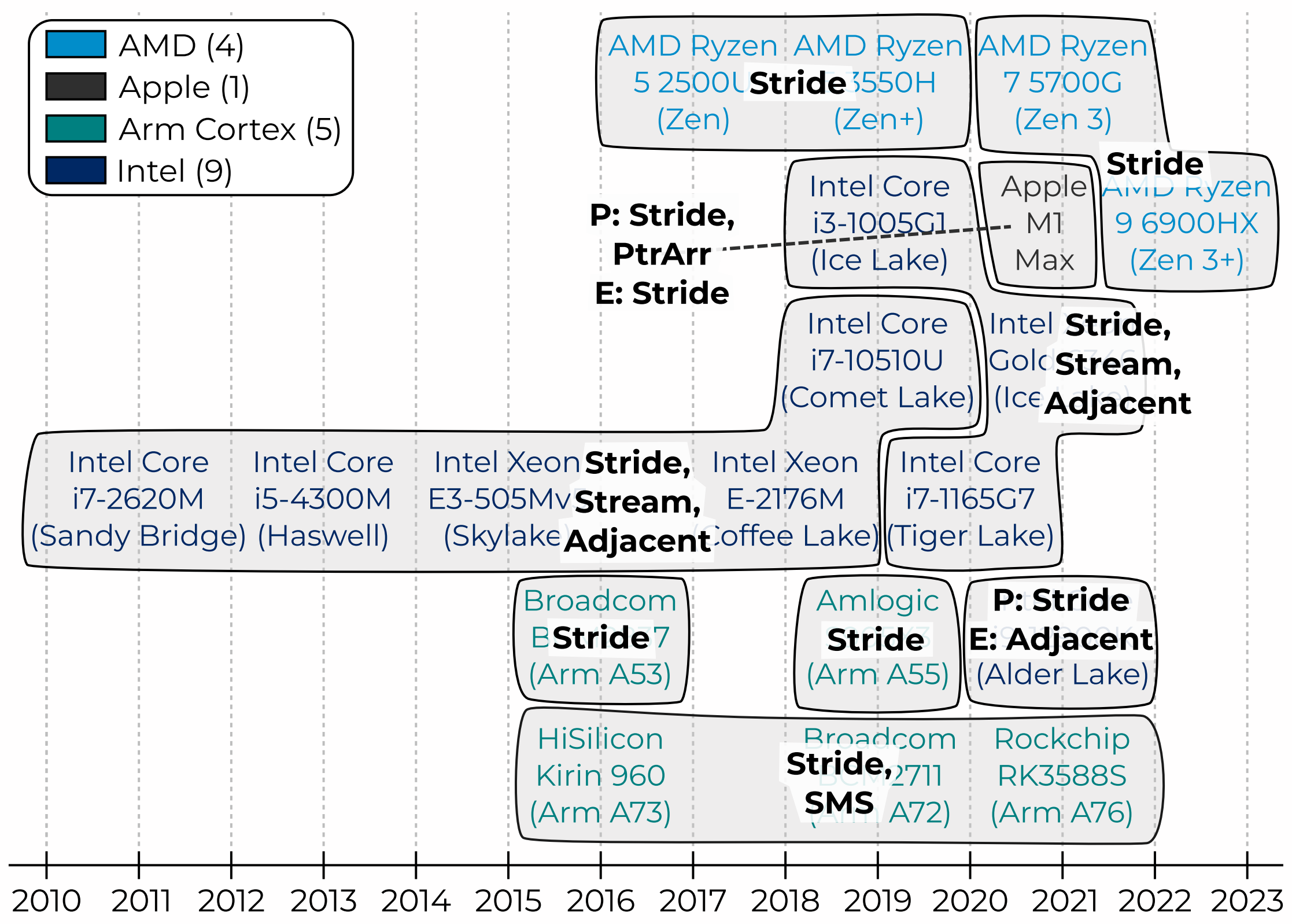
FETCHBENCH FRAMEWORK



Architecture-Specific
Pefetcher Design-Specific
Primitives
Timing
Flushing
Barriers
Identification and Characterization
Test Case Execution
Test Cases
...
Processor-Specific Prefetcher Existence and Characteristics Information

IDENTIFICATION AND CHARACTERIZATION RESULTS

- Characterized **19 CPUs** from 7 vendors
- 1-3 prefetchers per CPU
- **New:** SMS prefetcher
- The newer, the more complex

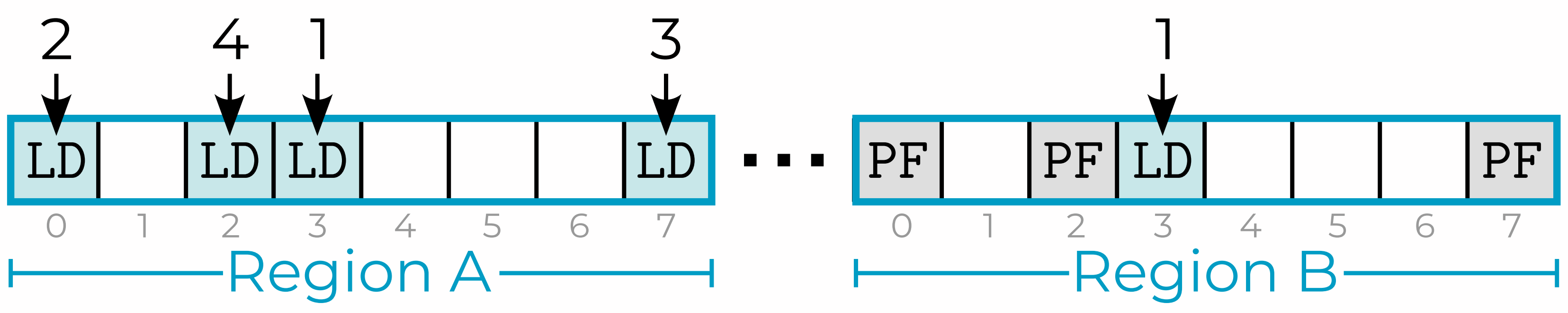


FIRST OBSERVED SMS PREFETCHER IN THE WILD

We are the first to identify a Spatial Memory Streaming (SMS) prefetcher in real-world CPUs, including the widely used Arm Cortex-A72.

The SMS prefetcher is **replay-** and **location-based**. It learns memory access patterns within a **spatial region**. The pattern is replayed once a load instruction at a specific address loads from a different region.

```
u8 *addrs[] = { &regA[3], &regA[0], &regA[7], &regA[2],
                &regB[3] };
for (u8 *addr : addrs)
    load(addr);
```

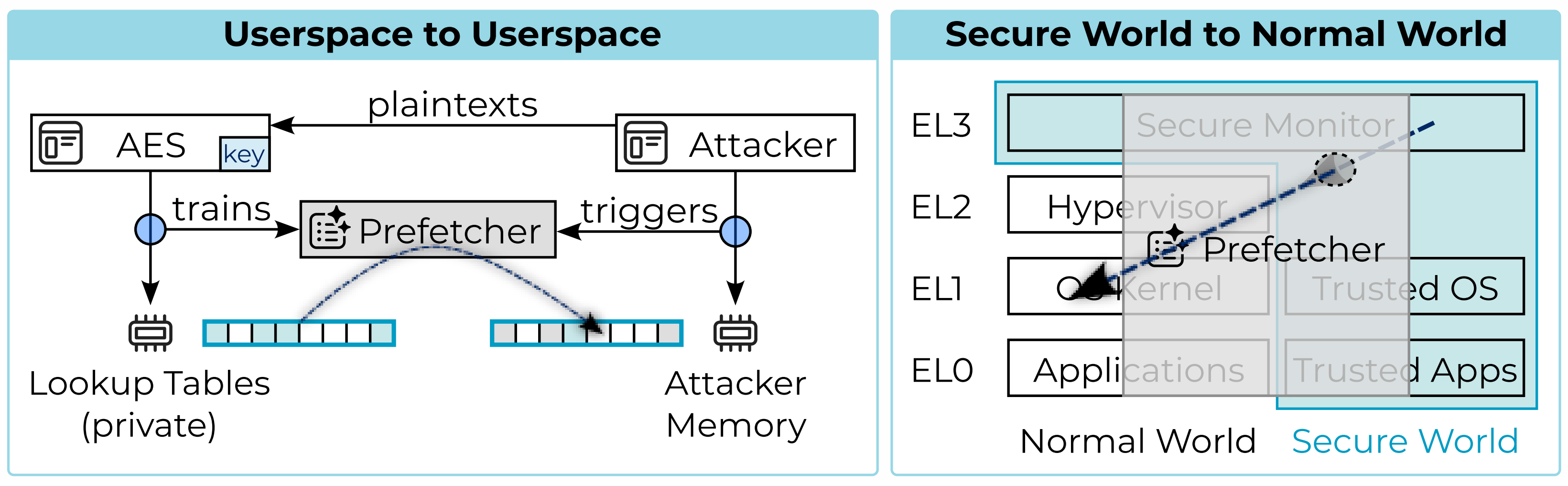


VULNERABILITY DISCOVERY AND DISCLOSURE

We find that the SMS prefetcher is **unaware of security boundaries**. It breaks platform security guarantees:

- Leaks information (such as keys) between processes
- Leaks data from Secure World (TEE) to Normal World

We disclosed our findings to Arm. Arm acknowledged and published an advisory.



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

This poster is based on the following publication:
Till Schlüter, Amit Choudhari, Lorenz Hetterich, Leon Trampert, Hamed Nemati, Ahmad Ibrahim, Michael Schwarz, Christian Rossow, Nils Ole Tippenhauer,
"FetchBench: Systematic Identification and Characterization of Proprietary Prefetchers"
Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'23)