Side-Channel Attacks on Optane Persistent Memory

Sihang Liu, Suraaj Kanniwadi, Martin Schwarzl, Andreas Kogler, Daniel Gruss, Samira Khan

Usenix Security Symposium 2023
Overview: Motivation
Overview: Motivation
Overview: Motivation
Overview: Contributions
Overview: Contributions
Overview: Contributions
Background

Optane, Persistent Memory, and Side Channels
Optane Persistent Memory
Optane Persistent Memory
Optane Persistent Memory
Optane Persistent Memory
Stable storage with Direct Access
Stable storage with Direct Access
Stable storage with Direct Access
Stable storage with Direct Access
Stable storage with Direct Access
In the system hierarchy
In the system hierarchy

- 100 ns
- 300 ns
- 100 μs
In the system hierarchy

- 100 ns
- 300 ns
- 100 μs
- 16 GB
- 256 GB
- 1 TB
A Side Channel Attack?
A Side Channel Attack?
A Side Channel Attack?
A Side Channel Attack?
Reverse-Engineering of Optane

A glimpse into the Optane DIMM
Optane: Prior Work
Optane: Prior Work
Optane: Prior Work

RMW Buffer
Optane: Prior Work
Optane: Prior Work
Optane: Prior Work

Optane

RMW Buffer

AIT Buffer

Optane Media

16 KB

256 B
Optane: Prior Work

- Optane Media
- AIT Buffer
- RMW Buffer

Optane

16 KB

16 MB

256 B

4 KB
Optane: Prior Work

Optane

- RMW Buffer
- AIT Buffer
- Optane Media

16 KB

256 B

16 MB

4 KB

Wear-levelling? Maybe?
Optane: We have more!

- Optane Media
- AIT Buffer
- RMW Buffer

Optane
Optane: We have more!

- Optane Media
- AIT Buffer
- RMW Buffer

Cache Details
- Associativity?
- Replacement Policy?
Optane: We have more!

- RMW Buffer
- AIT Buffer
- Optane Media

Cache Details
- Associativity?
- Replacement Policy?

Wear-levelling
- When? What? How?
Optane: We have more!

Cache Details
- Associativity?
- Replacement Policy?

Wear-levelling
- When? What? How?

Other surprising details!
On-DIMM caches

- Optane Media
  - AIT Buffer
    - RMW Buffer
  - 16 KB
    - 256 B
  - 16 MB
    - 4 KB
On-DIMM caches

- Optane Media
- AIT Buffer
- RMW Buffer

Fully associative (Pseudo) LRU Replacement

16 MB

4 KB
On-DIMM caches

- Optane Media
- AIT Buffer
- RMW Buffer

Fully associative (Pseudo) LRU Replacement

16-way set associative (Pseudo) LRU Replacement
Wear-levelling in Memories

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes to the rescue!
Wear-levelling in Memories

Repeated Writes

Memory Cells

Repeated Writes

Wear-levelling to the rescue!

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells

Wear-levelling to the rescue!

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells

Wear-levelling to the rescue!

Repeated Writes

Memory Cells
Wear-levelling in Memories

Repeated Writes

Memory Cells

Wear-levelling to the rescue!

Repeated Writes

Memory Cells
Wear-levelling in Optane: When/What?
Wear-levelling in Optane: When/What?

- Latency
  - 40 μs
  - ~1 μs

- Write #
Wear-levelling in Optane: When/What?

Typical Write Latency

Latency

Write #

40 μs

~1 μs

Typical Write Latency

Write #
Wear-levelling in Optane: When/What?

Typical Write Latency

Latency

40 μs

~1 μs

Write #
Wear-levelling in Optane: When/What?

Typical Write Latency

~1 μs

~11000 writes

Write #
Wear-levelling in Optane: When/What?

Typical Write Latency

~1 μs

~11000 writes

40x !!

40 μs

Write #
Wear-levelling in Optane: When/What?

Typical Write Latency

4K Data Migration

40x !!

~11000 writes

~1 μs

40 μs
<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Wear-levelling in Optane: How?

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>4K</td>
<td></td>
</tr>
<tr>
<td>4K</td>
<td></td>
</tr>
<tr>
<td>4K</td>
<td></td>
</tr>
</tbody>
</table>
Wear-levelling in Optane: How?

Expectations

Reality

4K

256 B

4K

256 B

4K

256 B

4K

256 B
### An Optane Curveball: clflush

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An Optane Curveball: \textit{clflush}

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{cl == cache line}</td>
<td></td>
</tr>
</tbody>
</table>
An Optane Curveball: \textit{clflush}

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>cl == cache line</td>
<td></td>
</tr>
<tr>
<td>== CPU cache line</td>
<td></td>
</tr>
</tbody>
</table>

### Expectations
- cl == cache line
- == CPU cache line

### Reality
- None

16
## An Optane Curveball: `clflush`

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl == cache line</code></td>
<td></td>
</tr>
<tr>
<td><code>== CPU cache line</code></td>
<td></td>
</tr>
<tr>
<td>&quot;<code>clflush</code> flushes only CPU caches&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Expectations
- cl == cache line
- == CPU cache line
- “*clflush flushes only CPU caches*”

### Reality
- *clflush reaches Optane!*
An Optane Curveball: *clflush*

<table>
<thead>
<tr>
<th>Expectations</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>cl == cache line</td>
<td><em>clflush</em> reaches Optane!</td>
</tr>
<tr>
<td>== CPU cache line</td>
<td>Flashes RMW Buffer!</td>
</tr>
<tr>
<td>“<em>clflush</em> flushes only CPU caches”</td>
<td></td>
</tr>
</tbody>
</table>
An Optane Curveball: *clflush*

### Expectations

- $cl == \text{cache line}$
- $\Rightarrow CPU \text{ cache line}$

- "*clflush* flushes only CPU caches"

### Reality

- *clflush* reaches Optane!
- Flushes RMW Buffer!

![Graph showing read latency and frequency]

- No *clflush* (150 ns)
- *clflush* (350 ns)
An Optane Curveball: R/W Contention
An Optane Curveball: R/W Contention

Isolated Reader
(400 ns)
An Optane Curveball: R/W Contention

Frequency

Read Latency

Isolated Reader
(400 ns)

With Concurrent Writer
(1200 ns)
The Attacks

Exploring the security implications of our new attack primitives
A Bird’s Eye view
A Bird’s Eye view

Optane
A Bird’s Eye view

- Attack Primitives
- RW Contention
- Internal Buffers
- Optane
A Bird’s Eye view

- Optane
  - RW Contention
  - Internal Buffers
  - Wear Levelling
- Attack Primitives
A Bird’s Eye view

- Attack Primitives
- RW Contention
- Internal Buffers
- Wear Levelling

Our Attacks
A Bird’s Eye view

Optane

- RW Contention
- Internal Buffers
- Wear Levelling

Attack Primitives

Our Attacks

Local Covert Channel
A Bird’s Eye view

- Attack Primitives
  - RW Contention
  - Internal Buffers
  - Wear Levelling

- Our Attacks
  - Local Covert Channel
  - Local Side Channel
A Bird’s Eye view

- Attack Primitives
  - RW Contention
  - Internal Buffers
  - Wear Levelling

- Our Attacks
  - Local Covert Channel
  - Local Side Channel
  - Remote Covert Channel
A Bird’s Eye view

Opotane

- RW Contention
- Internal Buffers
- Wear Levelling

Attack Primitives
- Local Covert Channel
- Local Side Channel
- Remote Covert Channel
- The Noteboard Attack

Our Attacks
Attack: Noteboard Covert Channel

Encoding secret messages on Optane’s wear-levelling metadata
The Idea
The Idea

<table>
<thead>
<tr>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
# The Idea

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

![Image of top secret folder and calculator with binary code]

![Image of three children writing with pencils]
## The Idea

<table>
<thead>
<tr>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
</tr>
</tbody>
</table>

### Top Secret

<table>
<thead>
<tr>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
</tr>
</tbody>
</table>

### Top Secret

<table>
<thead>
<tr>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
<td>🕖</td>
</tr>
</tbody>
</table>
## The Idea

### Table 1

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Table 2

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>50%</td>
<td>0%</td>
<td>0%</td>
<td>50%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>50%</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Diagram

- A top secret file
- A calculator
- A spy with a magnifying glass
- Students writing
# The Idea

<table>
<thead>
<tr>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
</table>
The Idea
The Idea

<table>
<thead>
<tr>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
<th>0%</th>
<th>0%</th>
<th>0%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A Realization
A Realization

KV-store App (pmemkv)

KV-store File
Optane DIMM

KV Store Server
A Realization

Remote Sender

Remote Receiver

KV-store App (pmemkv)

KV-store File
Optane DIMM

KV Store Server

Note Board
A Realization

1. Sender encodes message

Remote Sender

KV-store App (pmemkv)

KV-store File
Optane DIMM

KV Store Server

Remote Receiver

Note Board
A Realization

1. Sender encodes message

Remote Sender

KV-store App (pmemkv)

KV-store File
Optane DIMM

KV Store Server

Note Board

2. Receiver starts after some time

Time

Remote Receiver
A Realization

Remote Sender ➔ KV-store App (pmemkv) ➔ KV-store File Optane DIMM ➔ KV Store Server ➔ Note Board

1. Sender encodes message
2. Receiver starts after some time
3. Receiver gets secret

Time
Covert Communication

1. Sender encodes message
2. Receiver starts after some time
3. Receiver gets secret
A Realization

Result
A Realization

Result
A Realization

Result
A Realization

Result
Looking at the Future

Intel is officially winding down its Optane memory business

One of the announcements included with the Intel’s Q2 earnings call was a confirmation that the company is shutting down its Optane Memory division.
Looking at the Future

Samsung Develops Industry’s First CXL DRAM

Supporting CXL 2.0

128GB CXL DRAM based on advanced CXL 2.0 interface to be mass produced this year, accelerating commercialization of next-generation memory solutions

Samsung will continue collaborating with global data center, server and chipset companies to bolster CXL ecosystem

Intel is officially winding down its Optane memory business

One of the announcements included with the Intel’s Q2 earnings call was a confirmation that the company is shutting down its Optane Memory division.
Looking at the Future

Samsung Develops Industry’s First 128GB CXL DRAM, Supporting CXL 2.0

Samsung will continue collaborating with global data center companies to bolster CXL ecosystem.

Intel is Officially Winding Down its Optane Memory Business

One of the announcements included with the Intel’s Q2 earnings call was a confirmation that they are shuttering their Optane Memory division.

Samsung Electronics Unveils Far-Reaching, Next-Generation Memory Solutions at Flash Memory Summit 2022

New suite of memory and storage technologies will collectively transform how data is moved, stored, processed and managed in the big data era.
Kioxia Launches Second Generation of High-Performance, Cost-Effective XL-FLASH™ Storage Class Memory Solution

Kioxia Corporation, the world leader in memory solutions, today announced the launch of the second generation of XL-FLASH™, a Storage Class Memory (SCM) solution based on its BICS FLASH™ 3D flash memory technology, which significantly reduces bit cost while providing high performance and low latency. Product sample shipments are scheduled to start in November this year, with volume production expected to begin in 2023.

The second generation XL-FLASH™ achieves significant reduction in bit cost as a result of the addition of new multi-level cell (MLC) functionality with 2-bit per cell, in addition to the single-level cell (SLC) of the existing model. The maximum number of planes that can operate simultaneously has also increased from the current model, which will allow for improved throughput. The new XL-FLASH™ will have a memory capacity of 256 gigabits.4
Summary
Summary
Summary
Summary
Side-Channel Attacks on Optane Persistent Memory

Sihang Liu, Suraaj Kanniwadi, Martin Schwarzl, Andreas Kogler, Daniel Gruss, Samira Khan

Usenix Security Symposium 2023