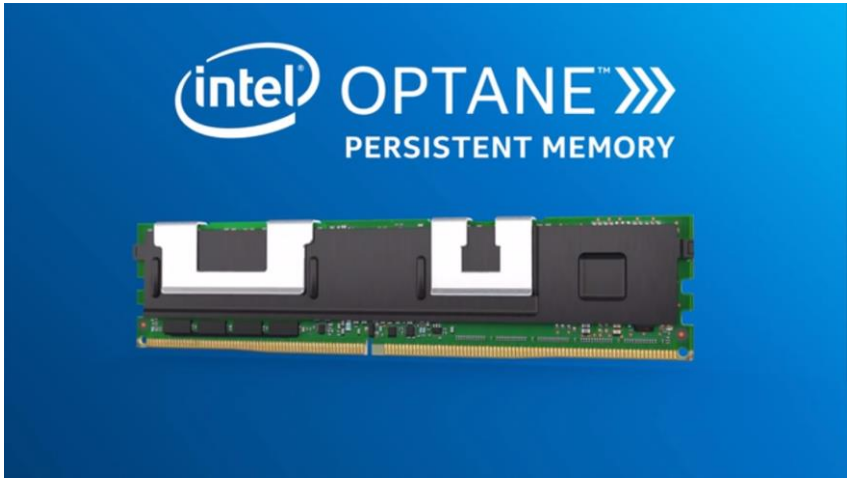
Side-Channel Attacks on Optane Persistent Memory

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

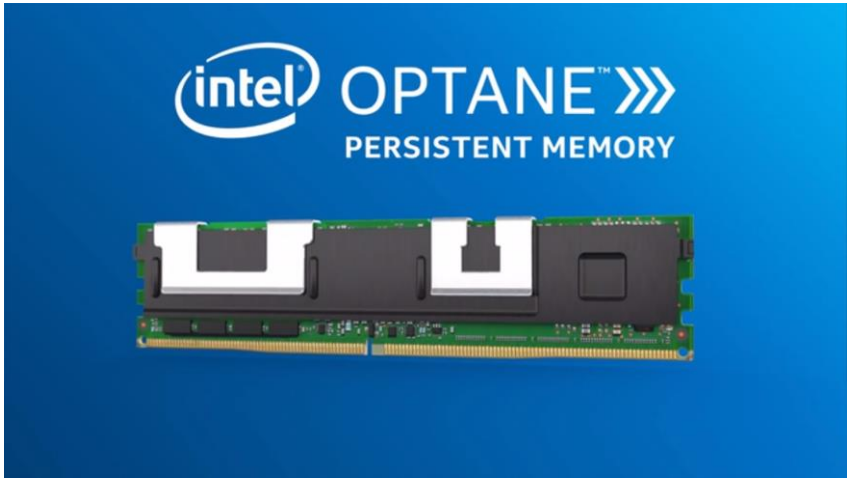
Usenix Security Symposium 2023

Overview: Motivation

Overview: Motivation

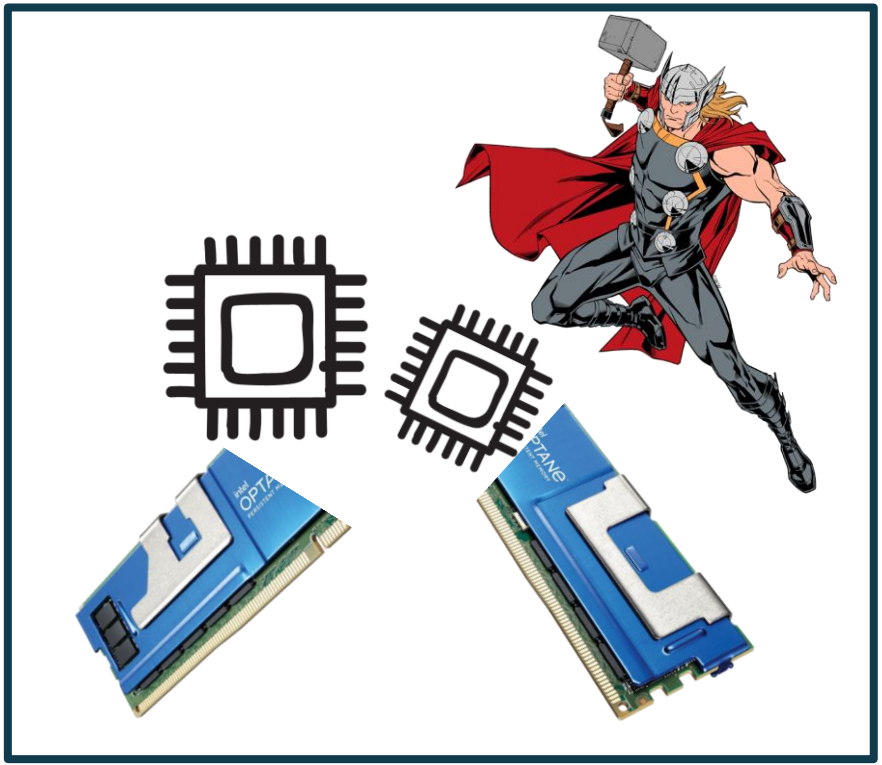


Overview: Motivation

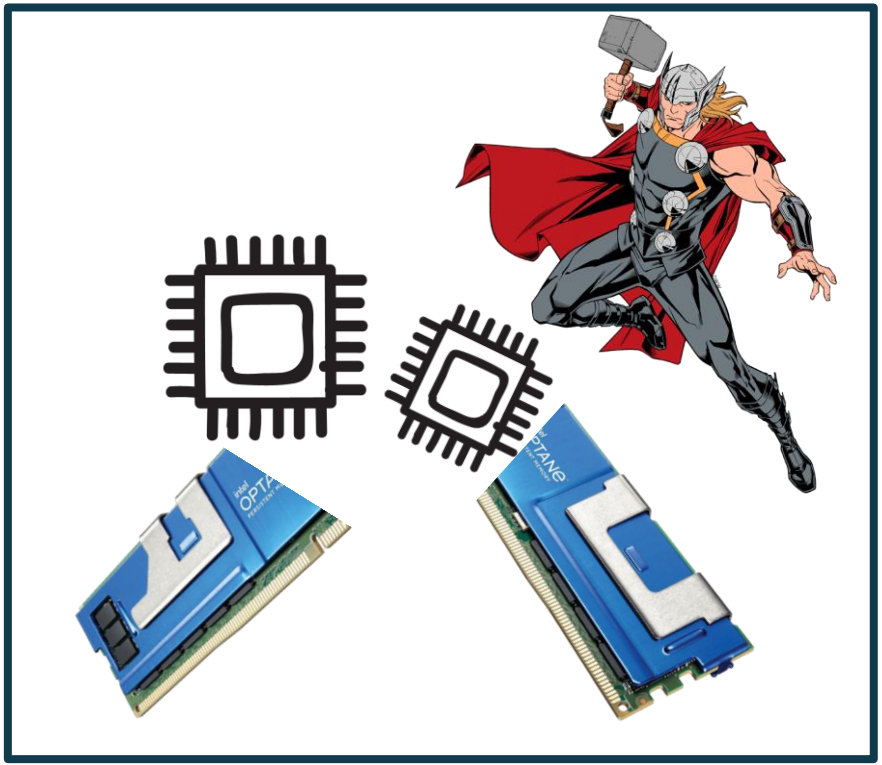


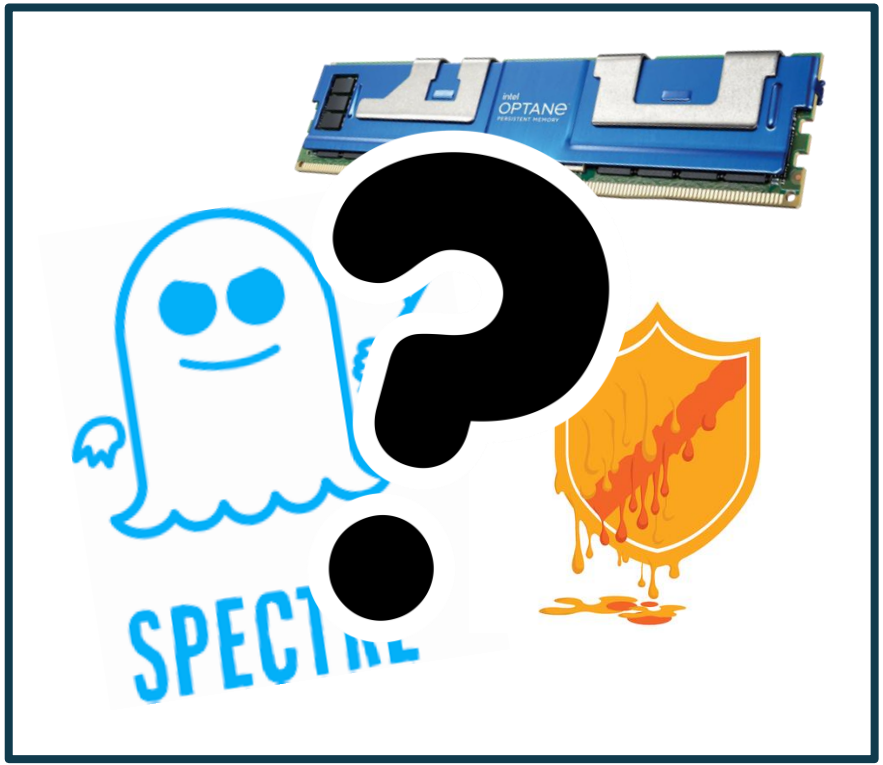
Overview: Contributions

Overview: Contributions



Overview: Contributions



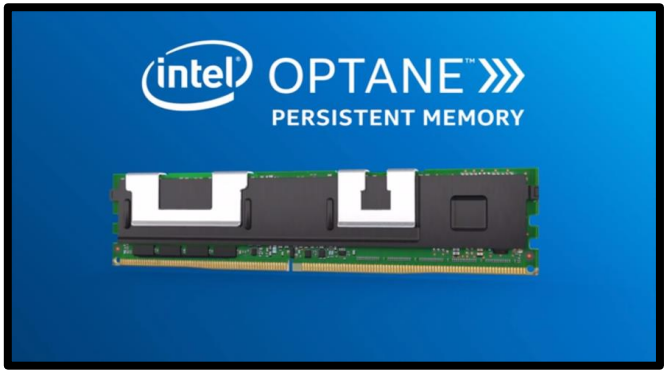


Background

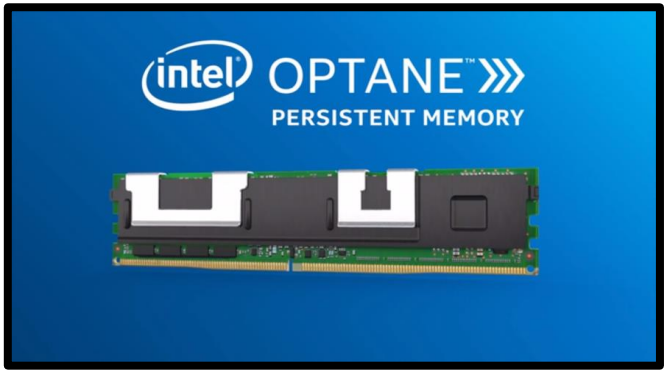
Optane, Persistent Memory, and Side Channels

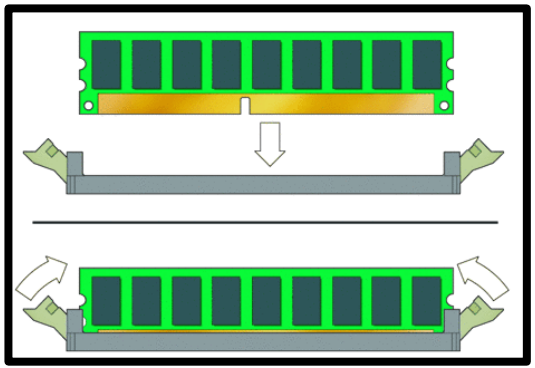
Optane Persistent Memory

Optane Persistent Memory

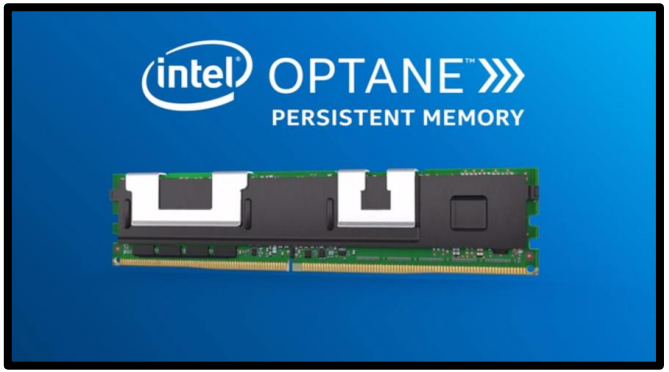


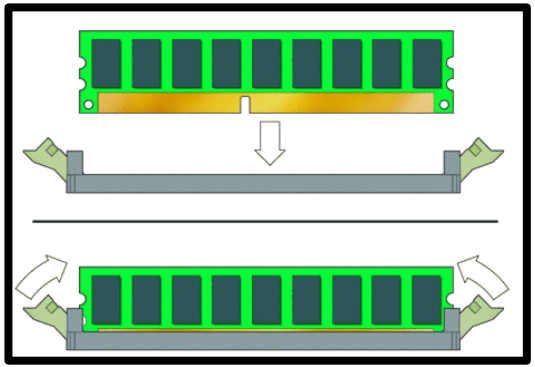
Optane Persistent Memory



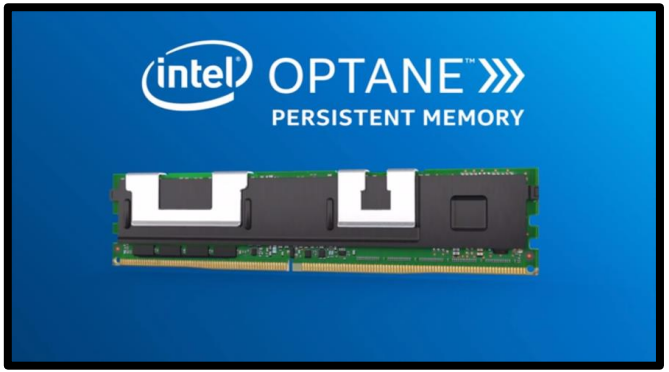


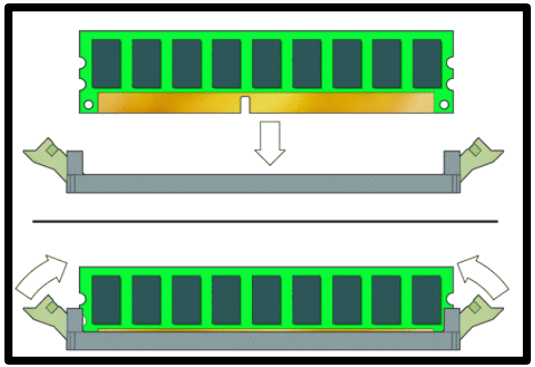
Optane Persistent Memory

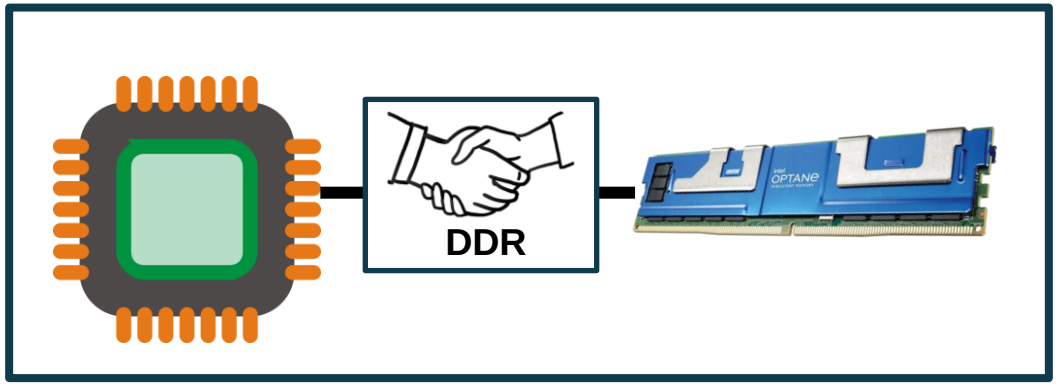




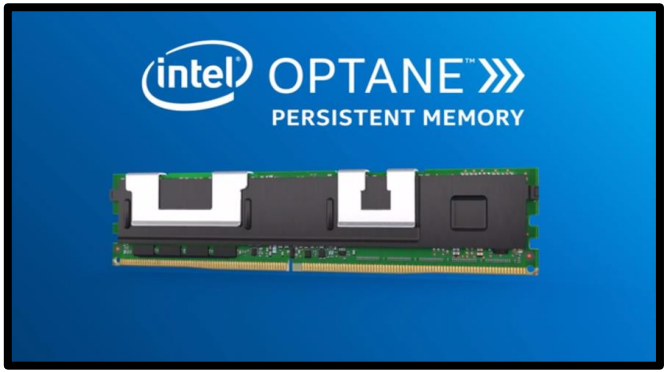
Optane Persistent Memory

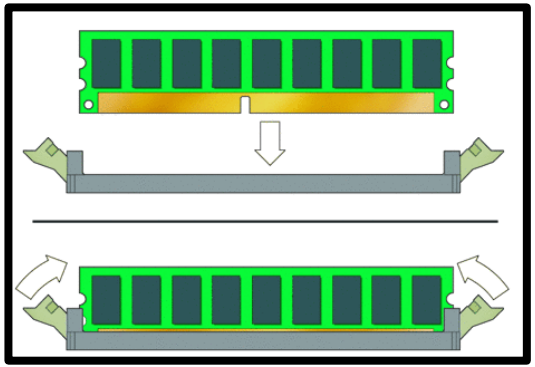


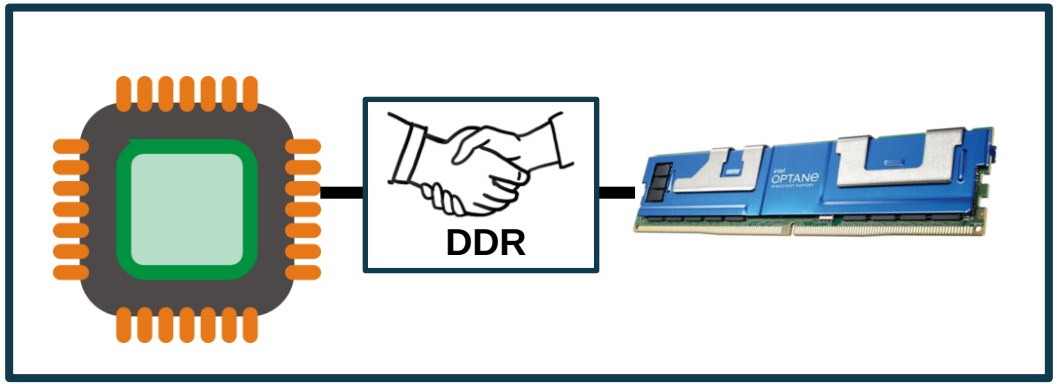


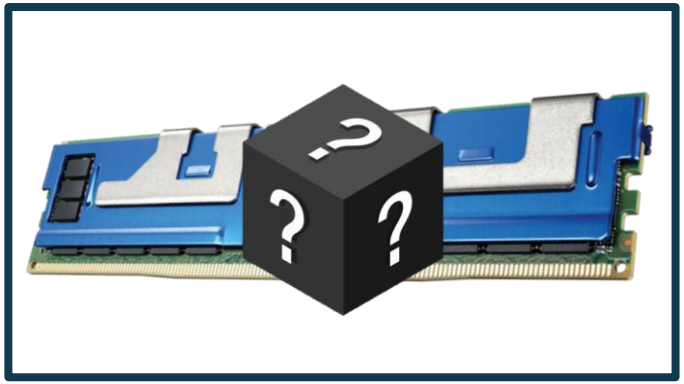


Optane Persistent Memory



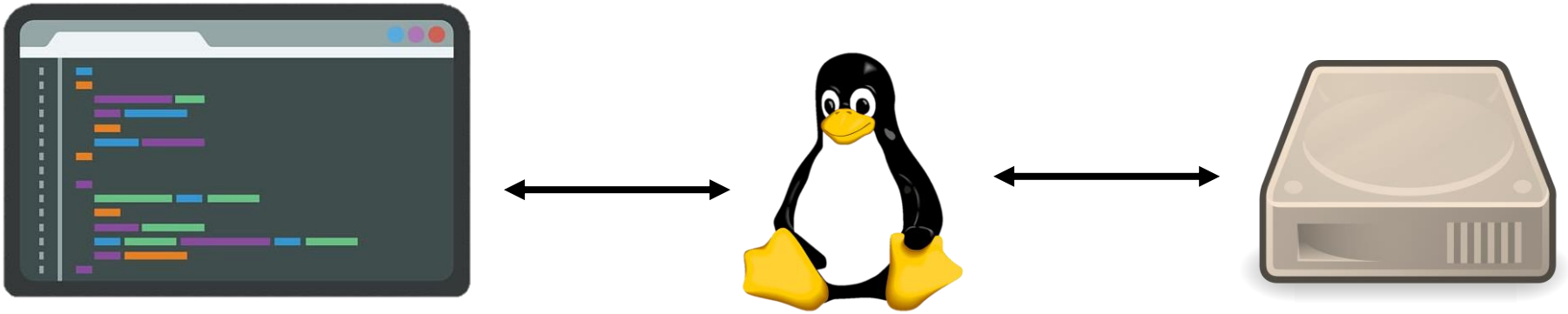




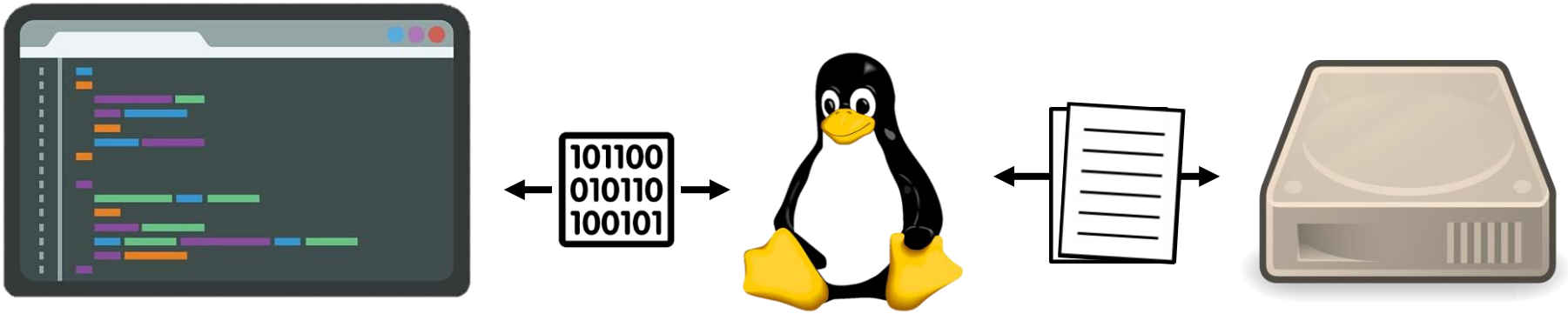


Stable storage with Direct Access

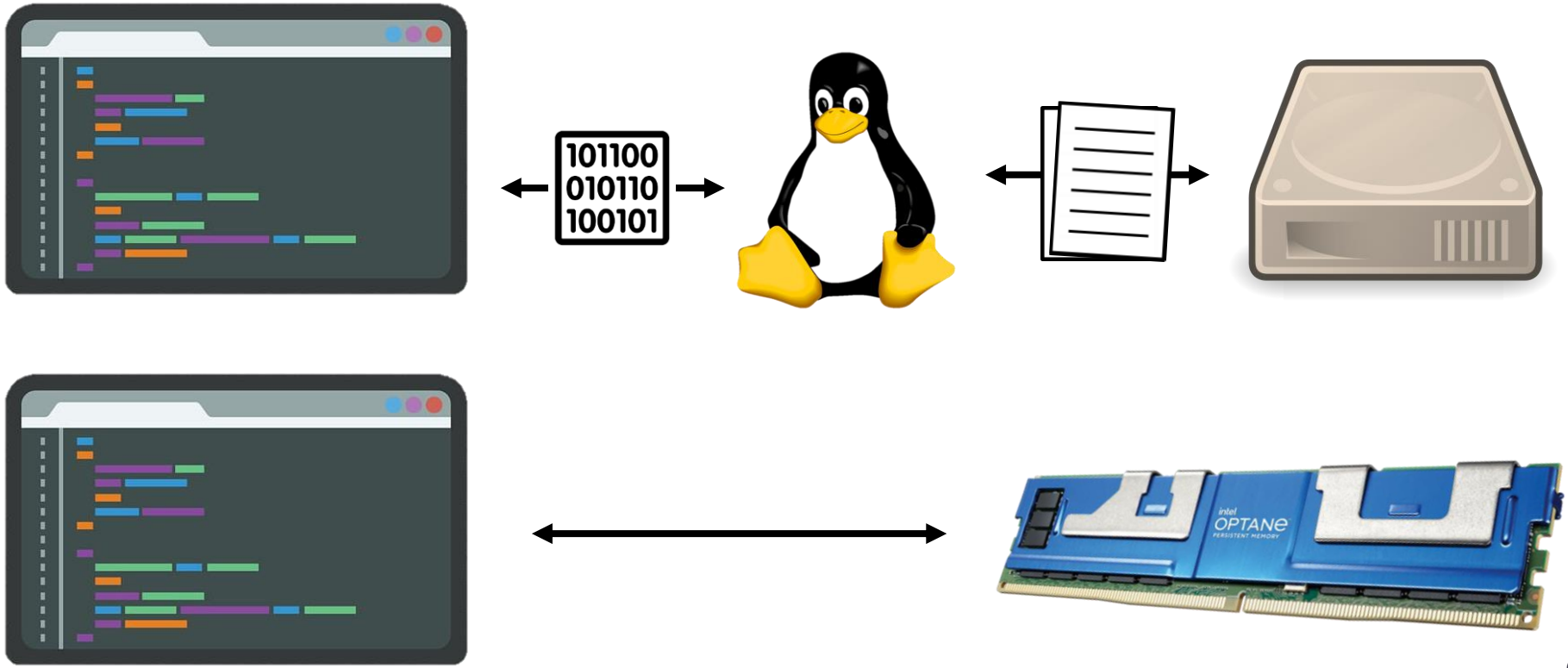
Stable storage with Direct Access



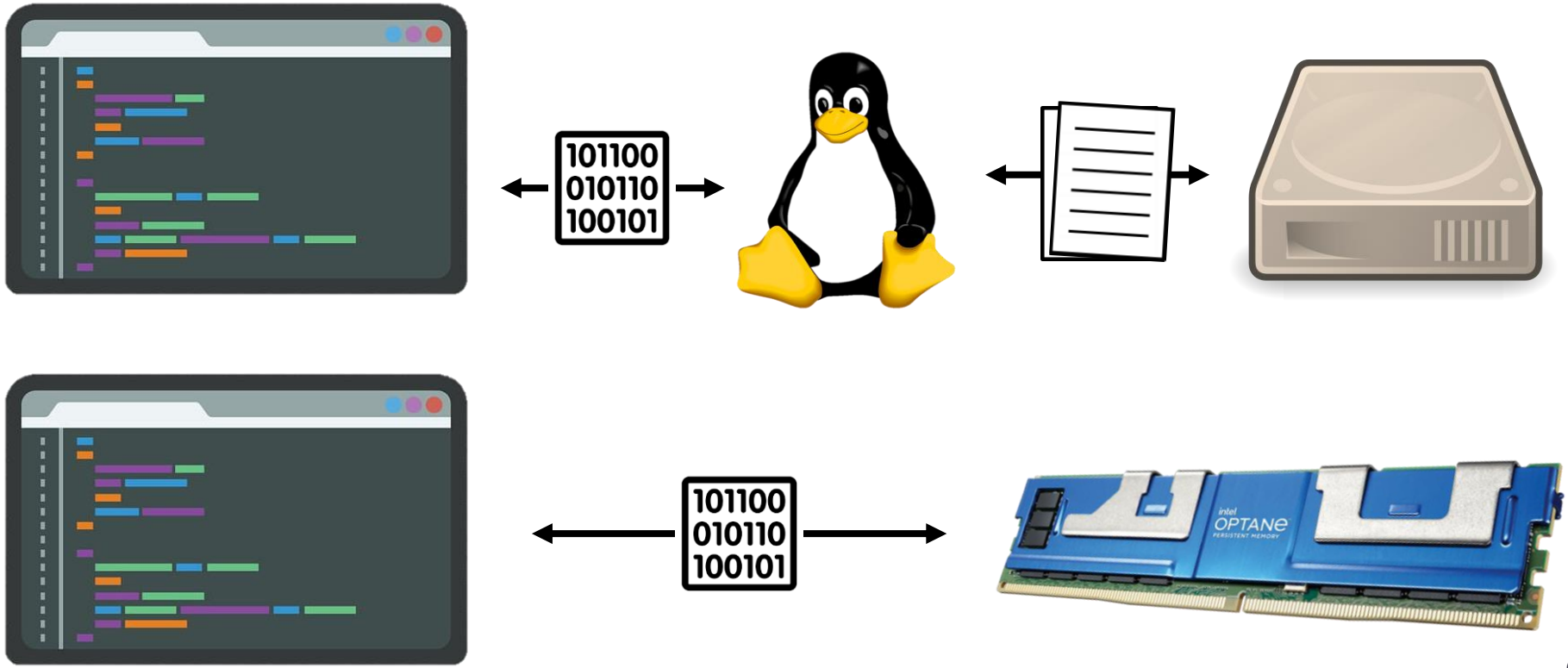
Stable storage with Direct Access



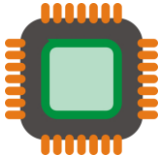
Stable storage with Direct Access

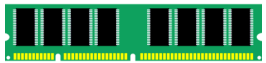


Stable storage with Direct Access

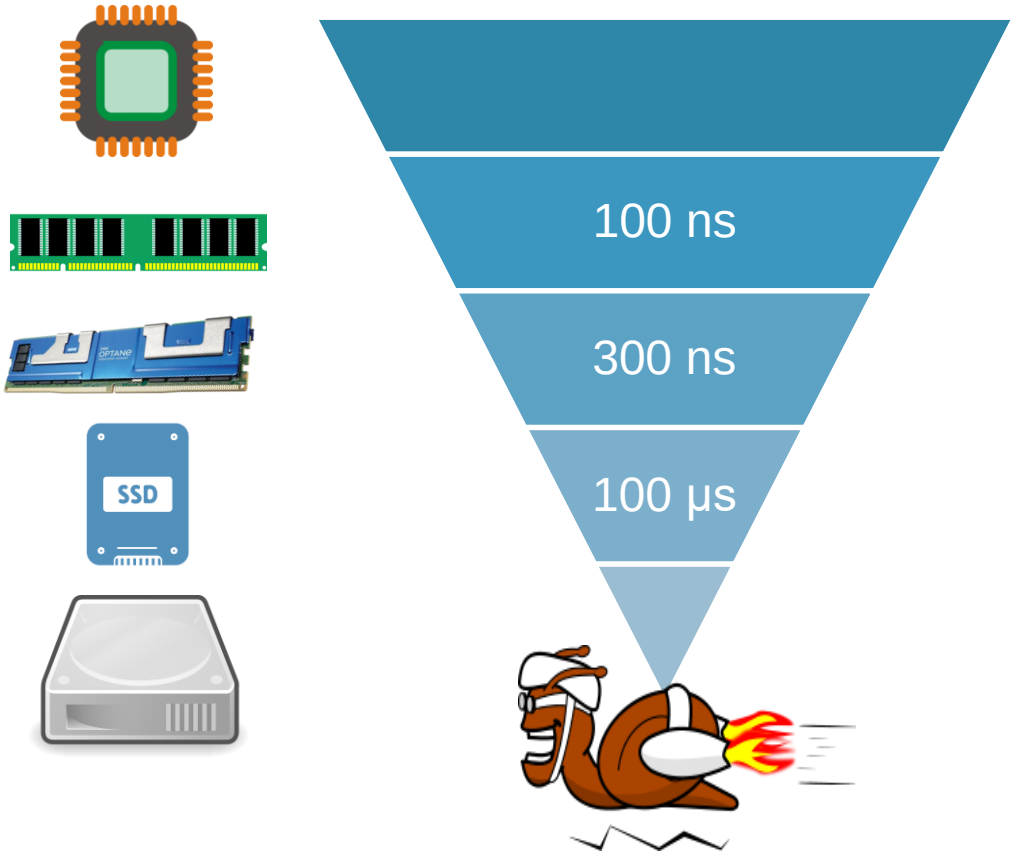


In the system heirarchy

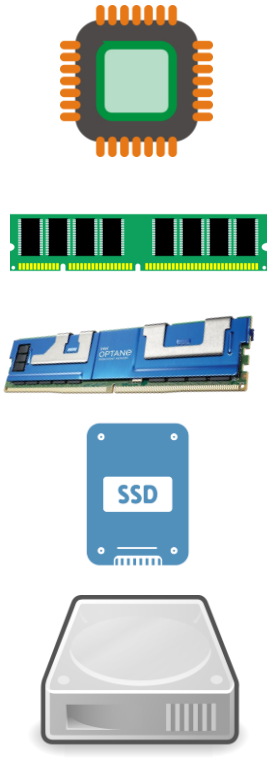


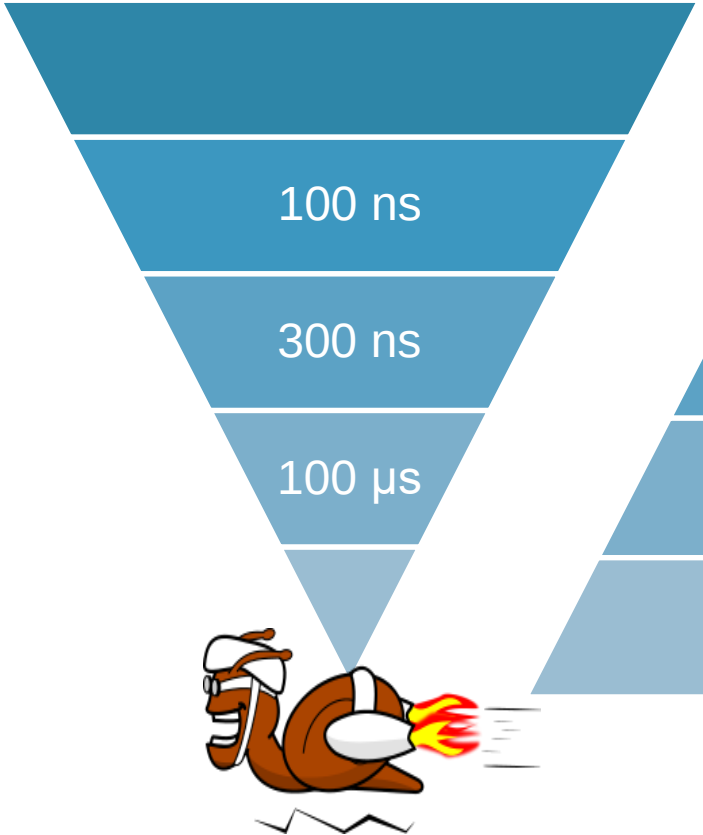


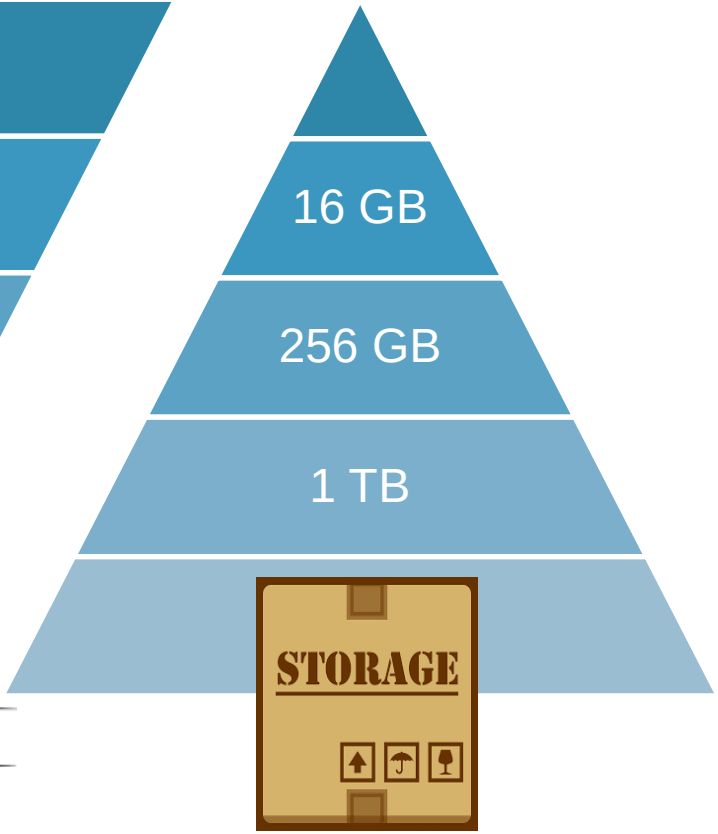
In the system heirarchy



In the system heirarchy

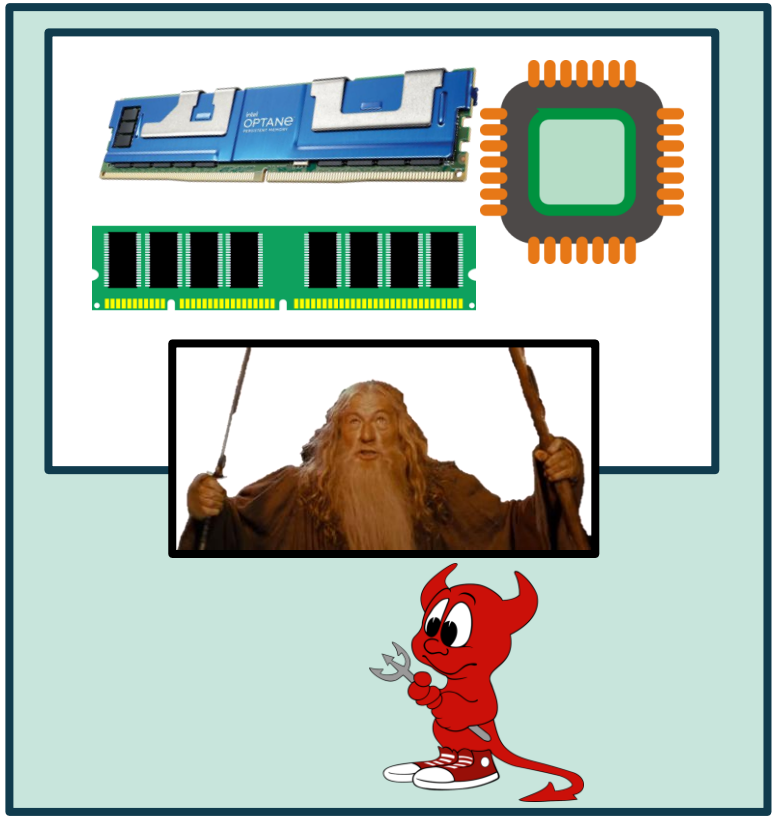




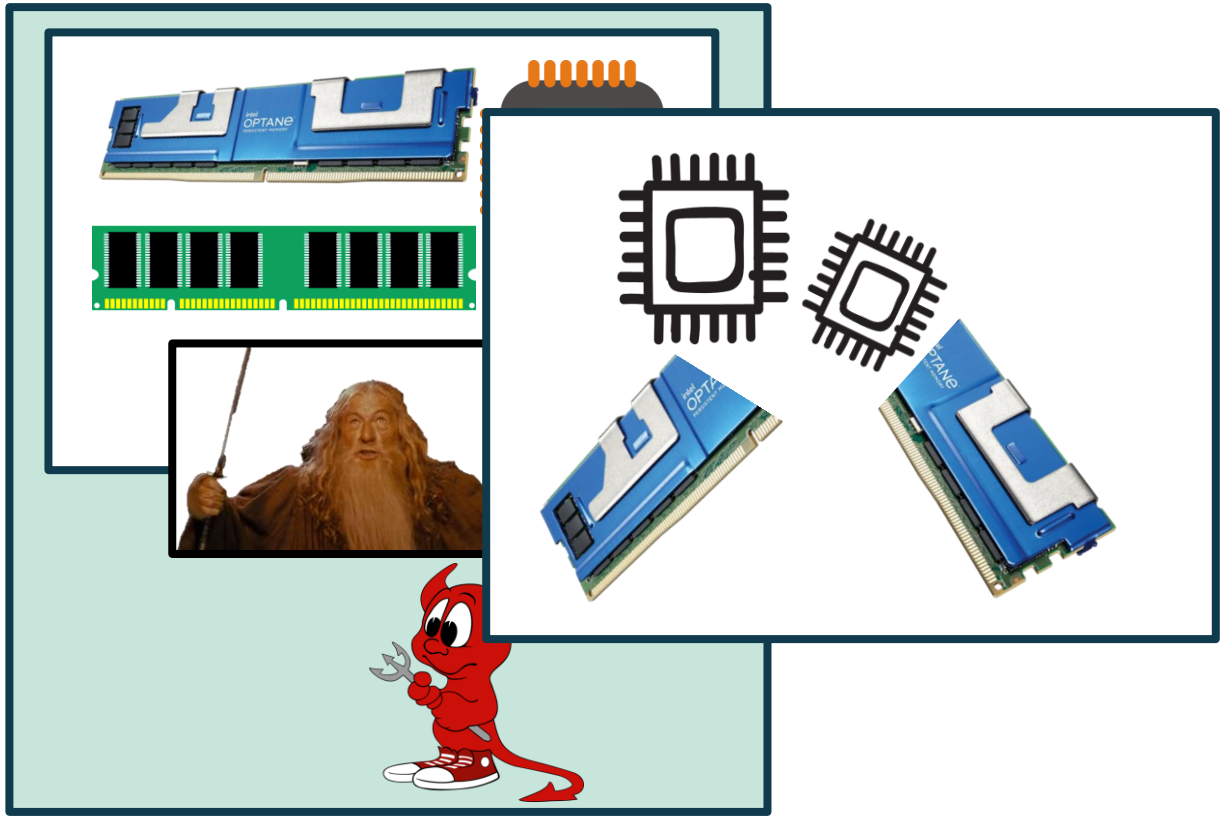


A Side Channel Attack?

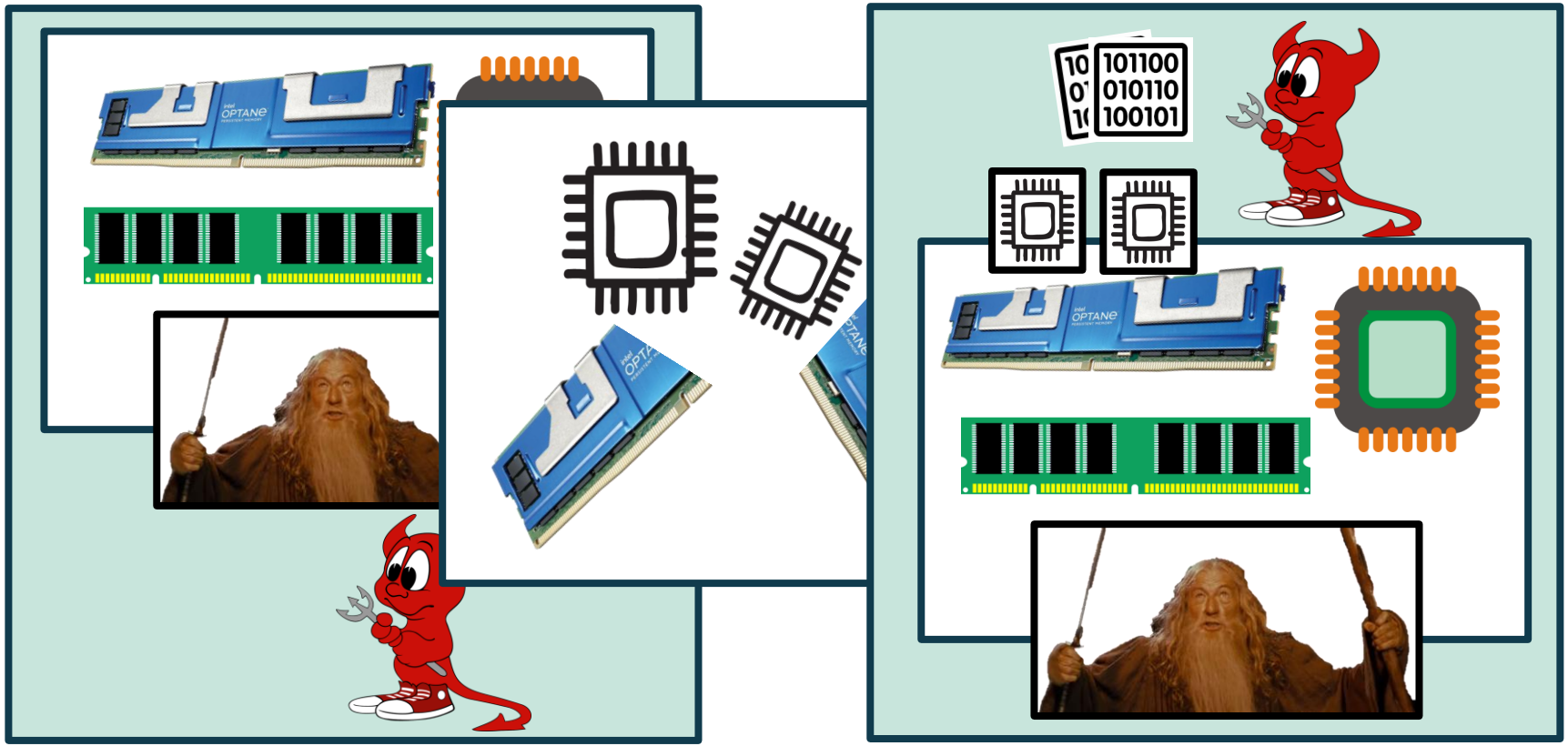
A Side Channel Attack?



A Side Channel Attack?



A Side Channel Attack?

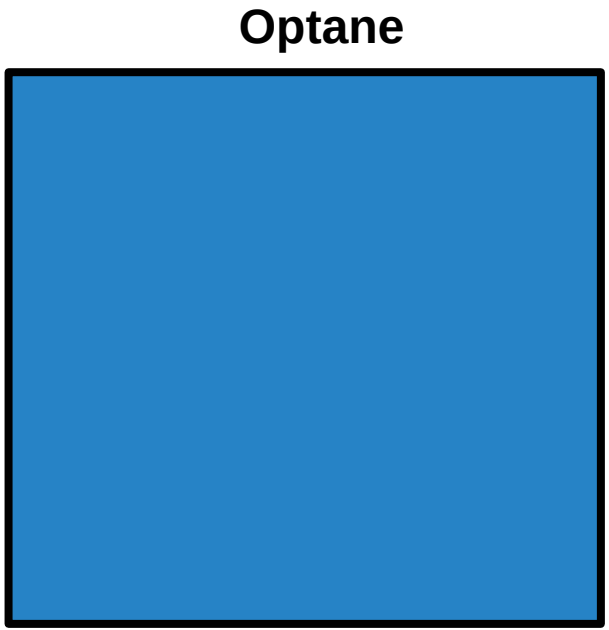


Reverse-Engineering of Optane

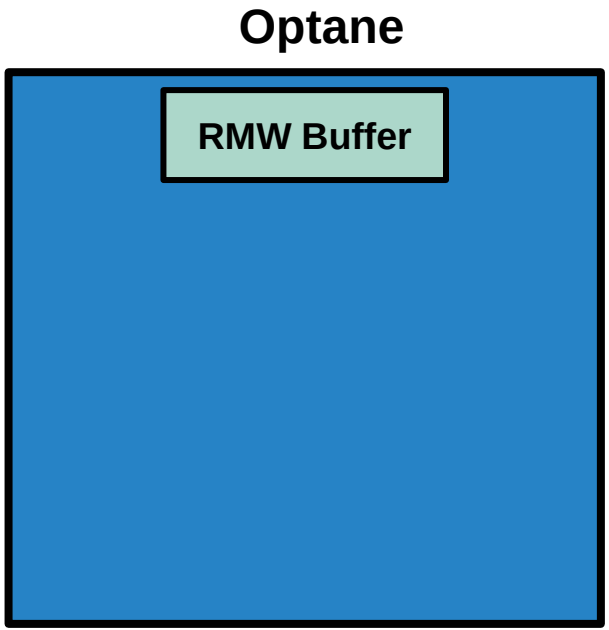
A glimpse into the Optane DIMM

Optane: Prior Work

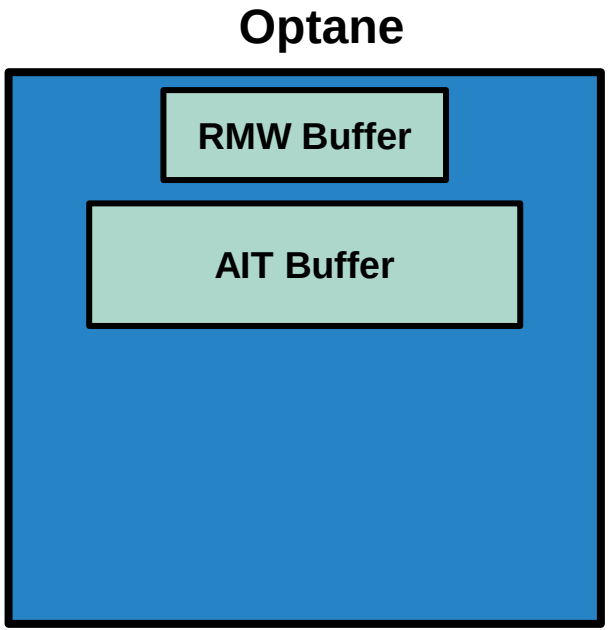
Optane: Prior Work



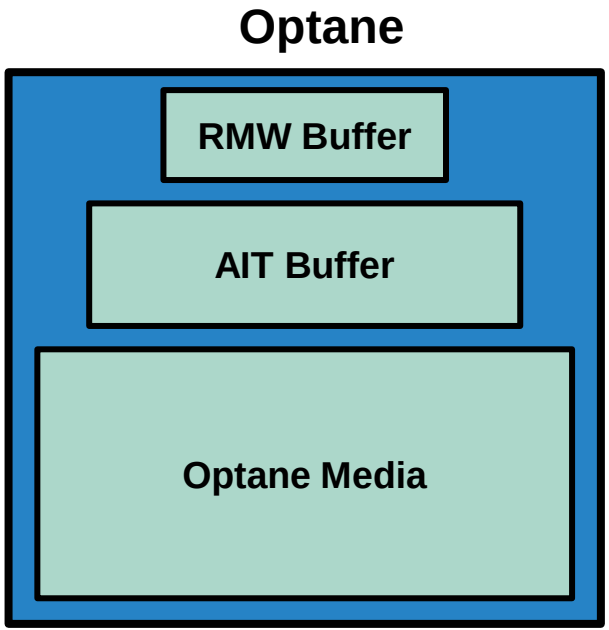
Optane: Prior Work



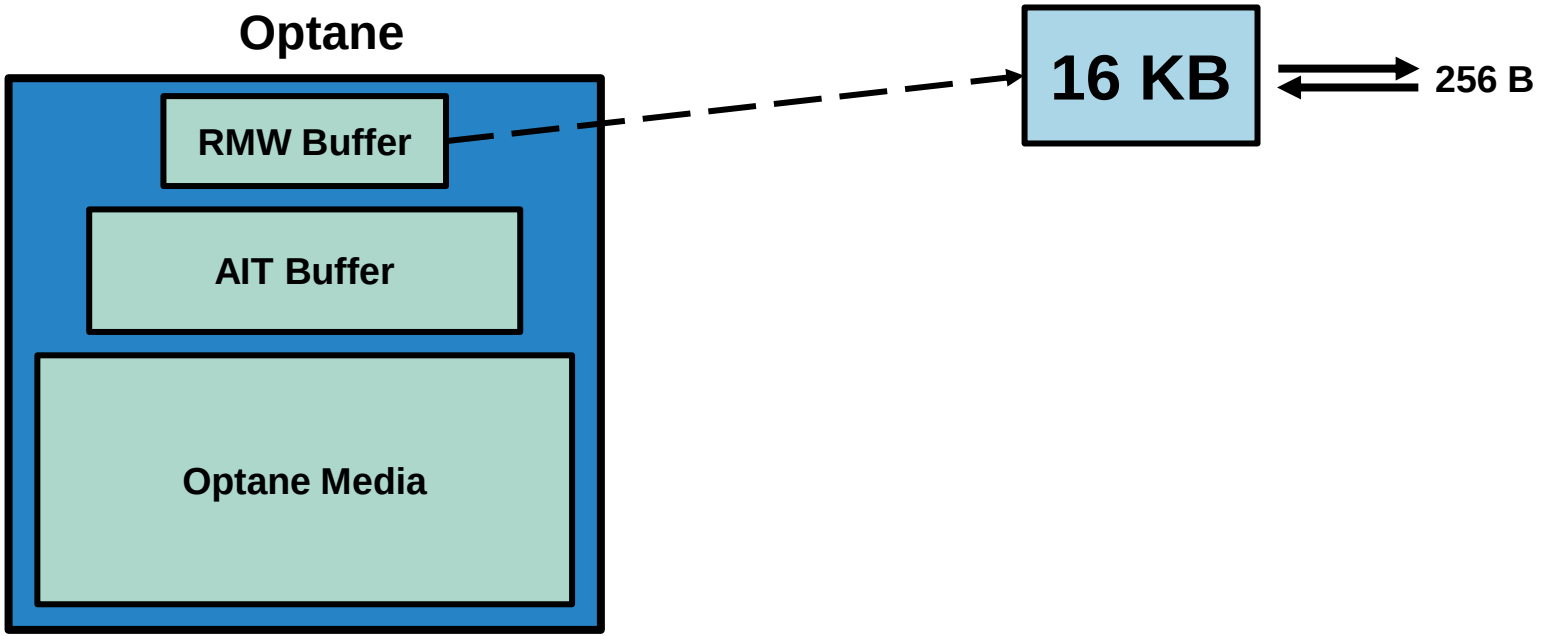
Optane: Prior Work



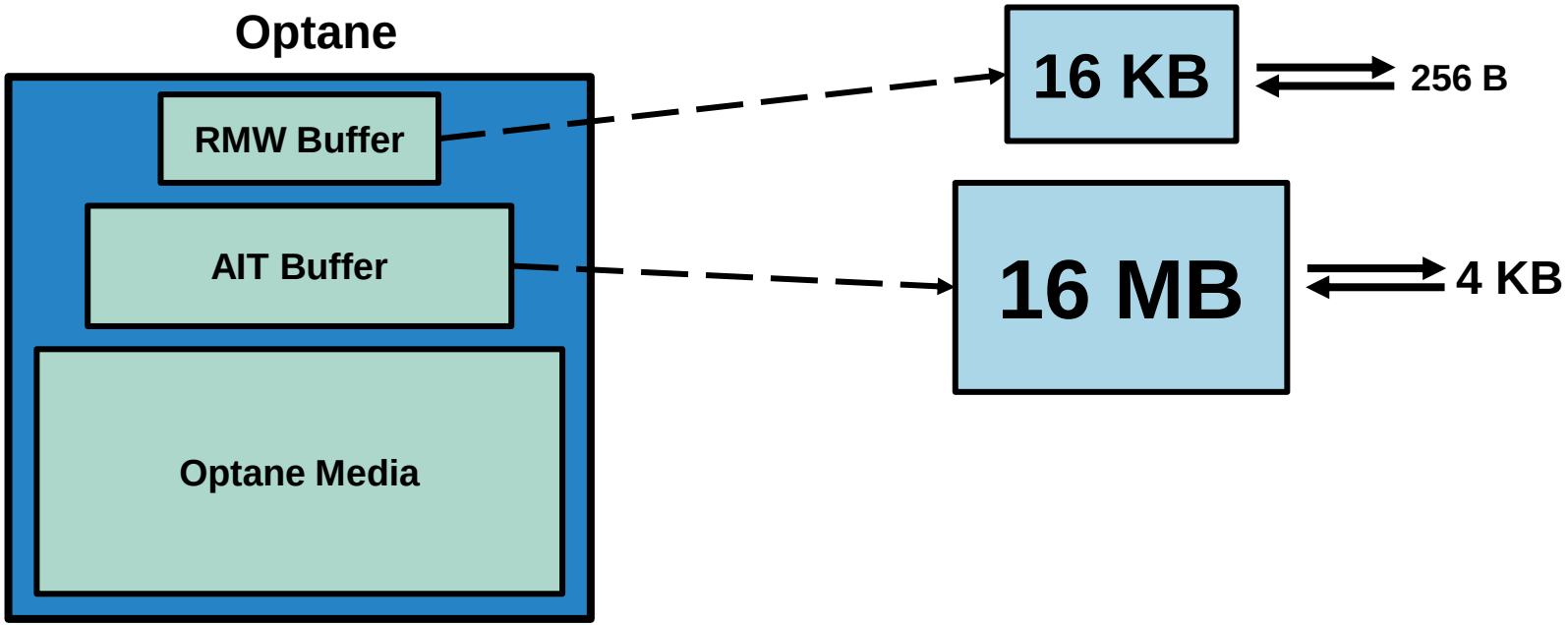
Optane: Prior Work



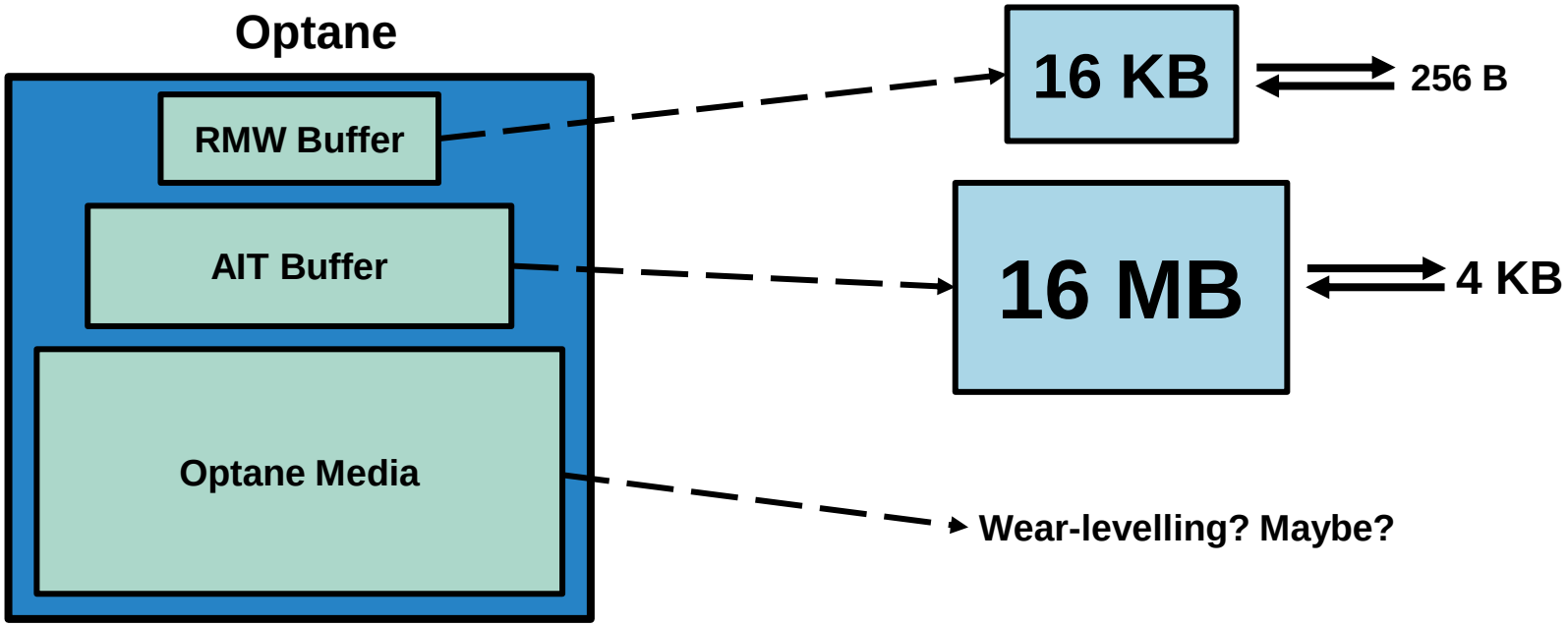
Optane: Prior Work



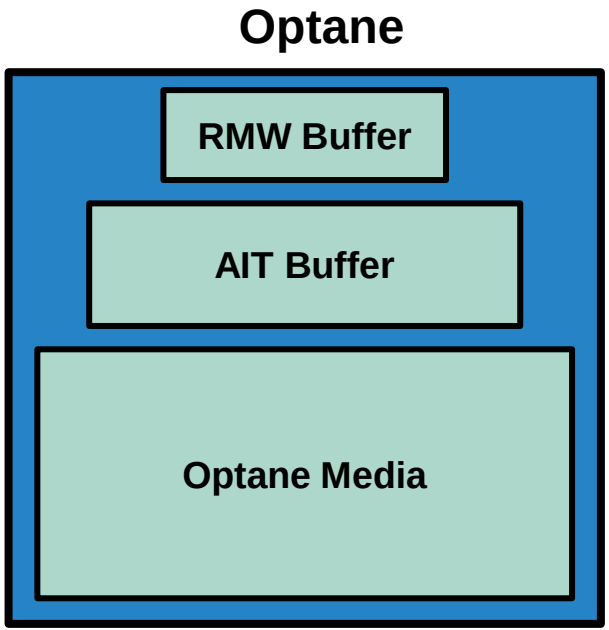
Optane: Prior Work



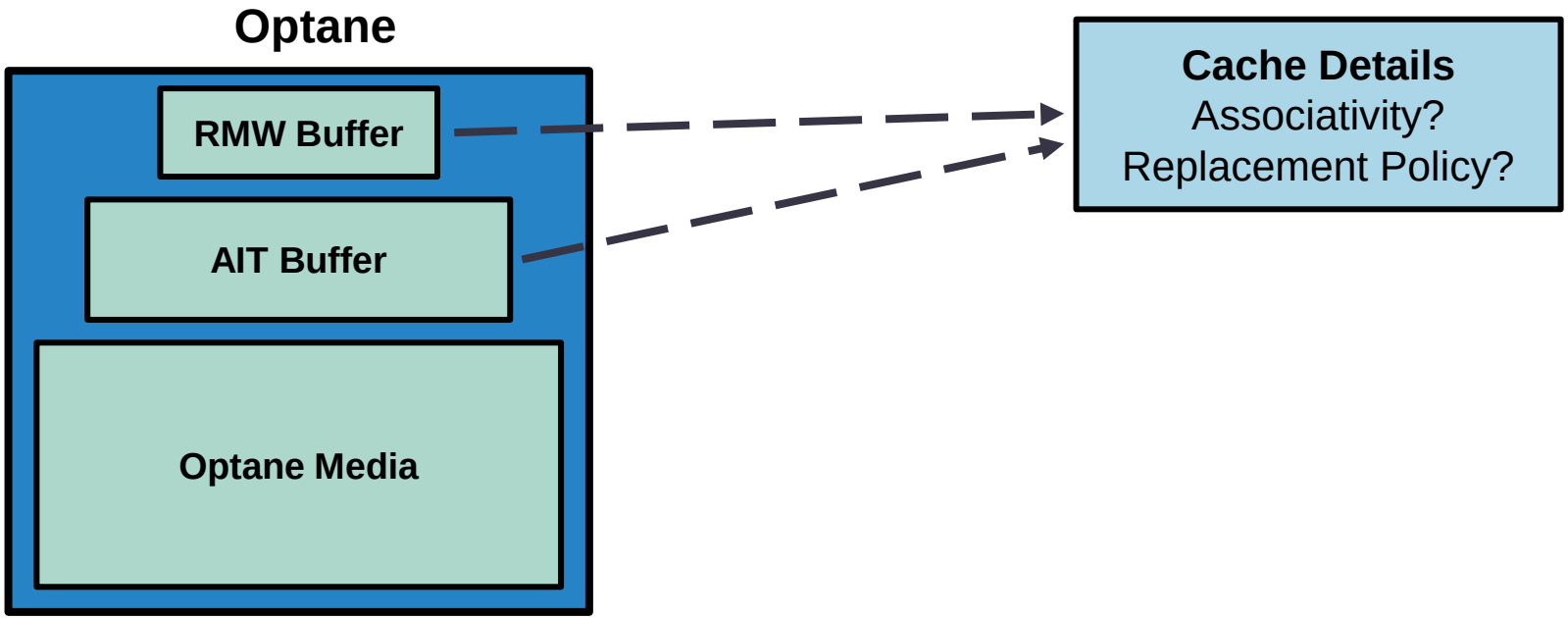
Optane: Prior Work



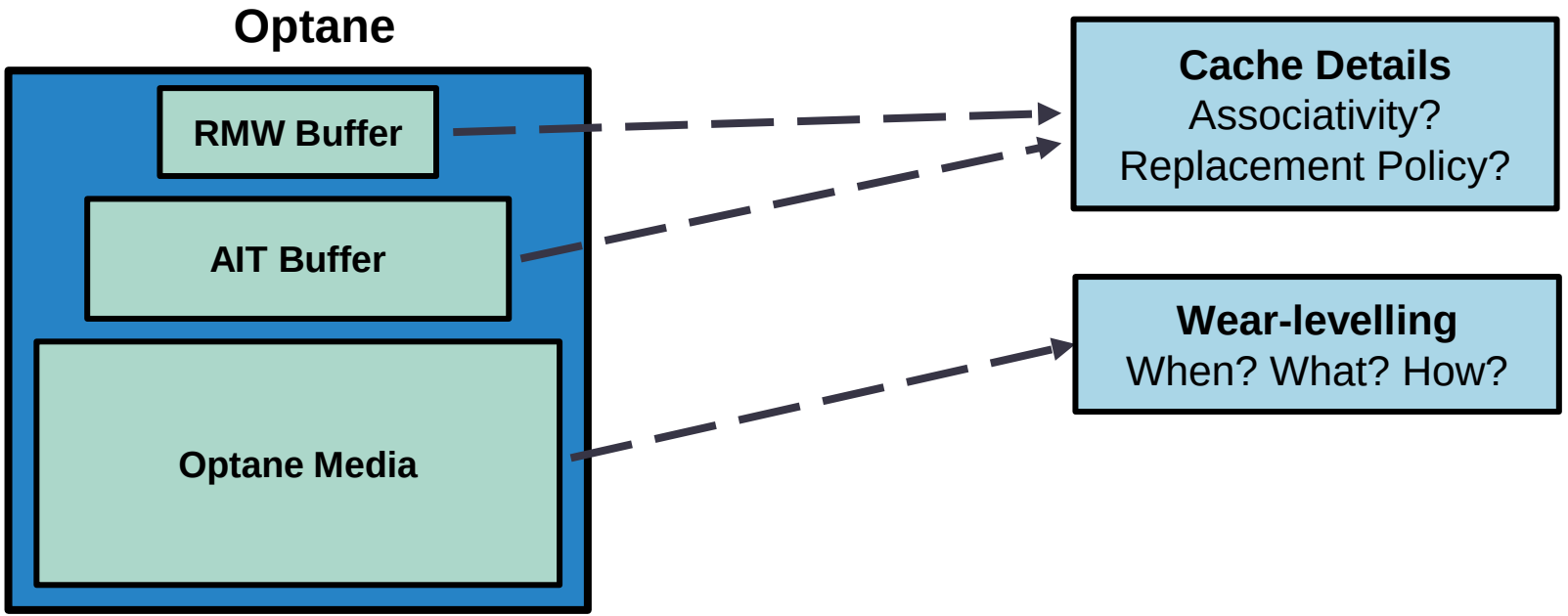
Optane: We have more!



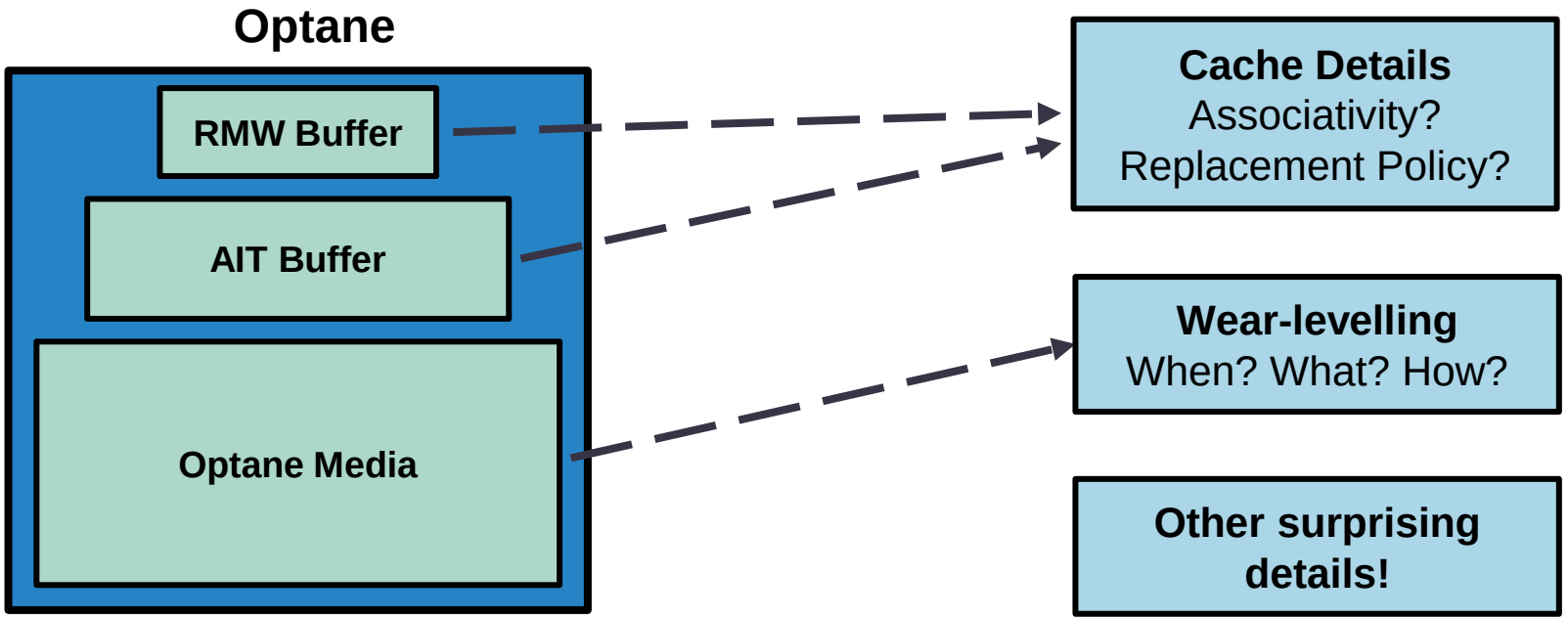
Optane: We have more!



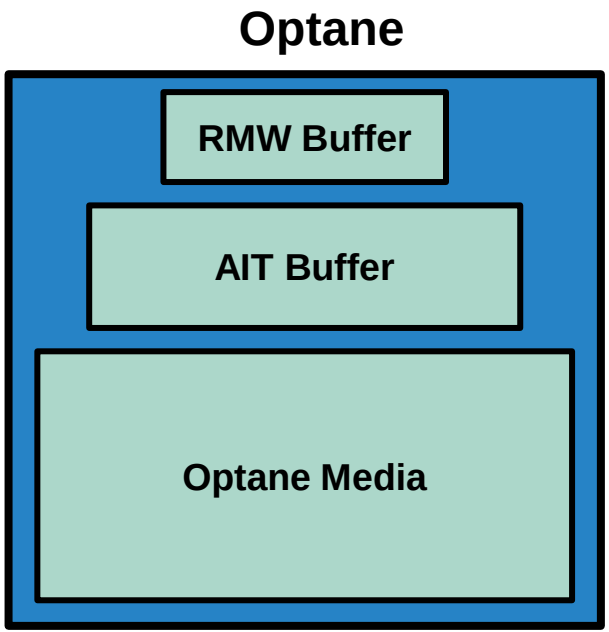
Optane: We have more!



Optane: We have more!



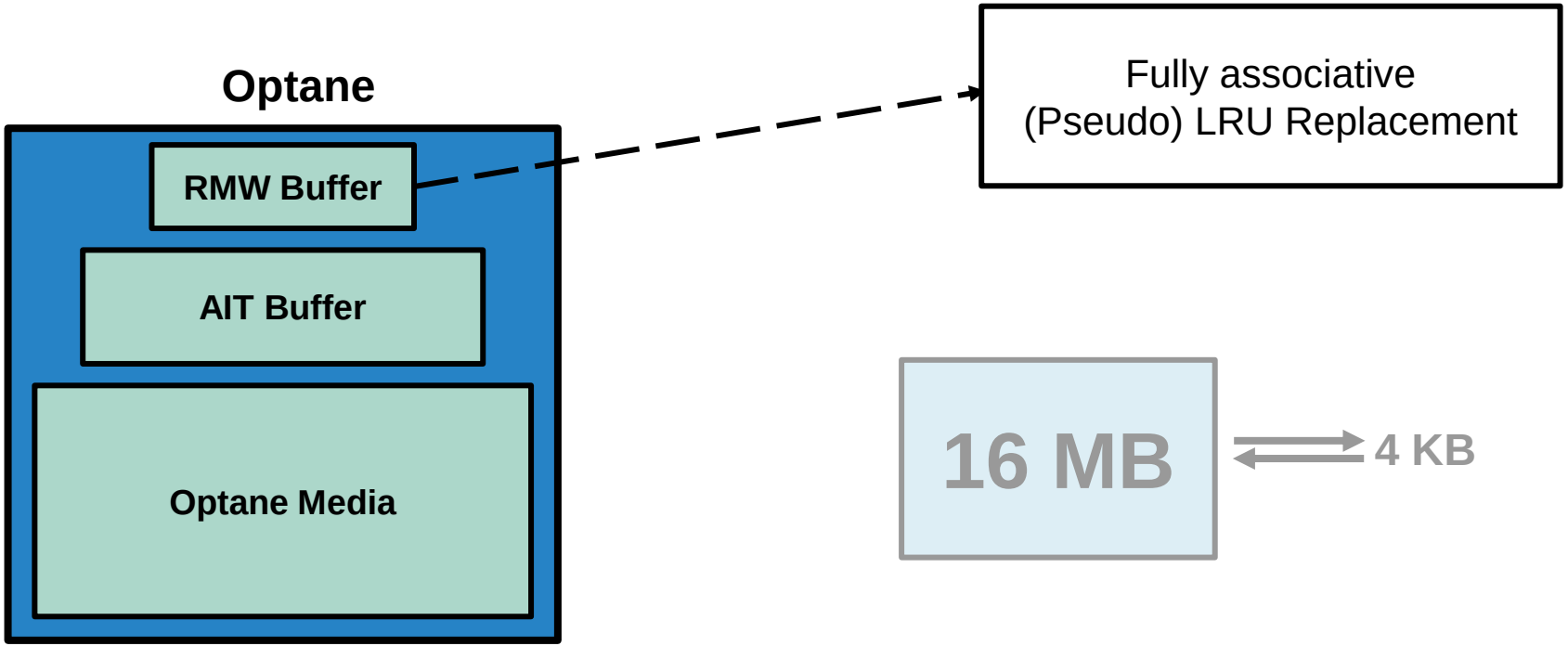
On-DIMM caches



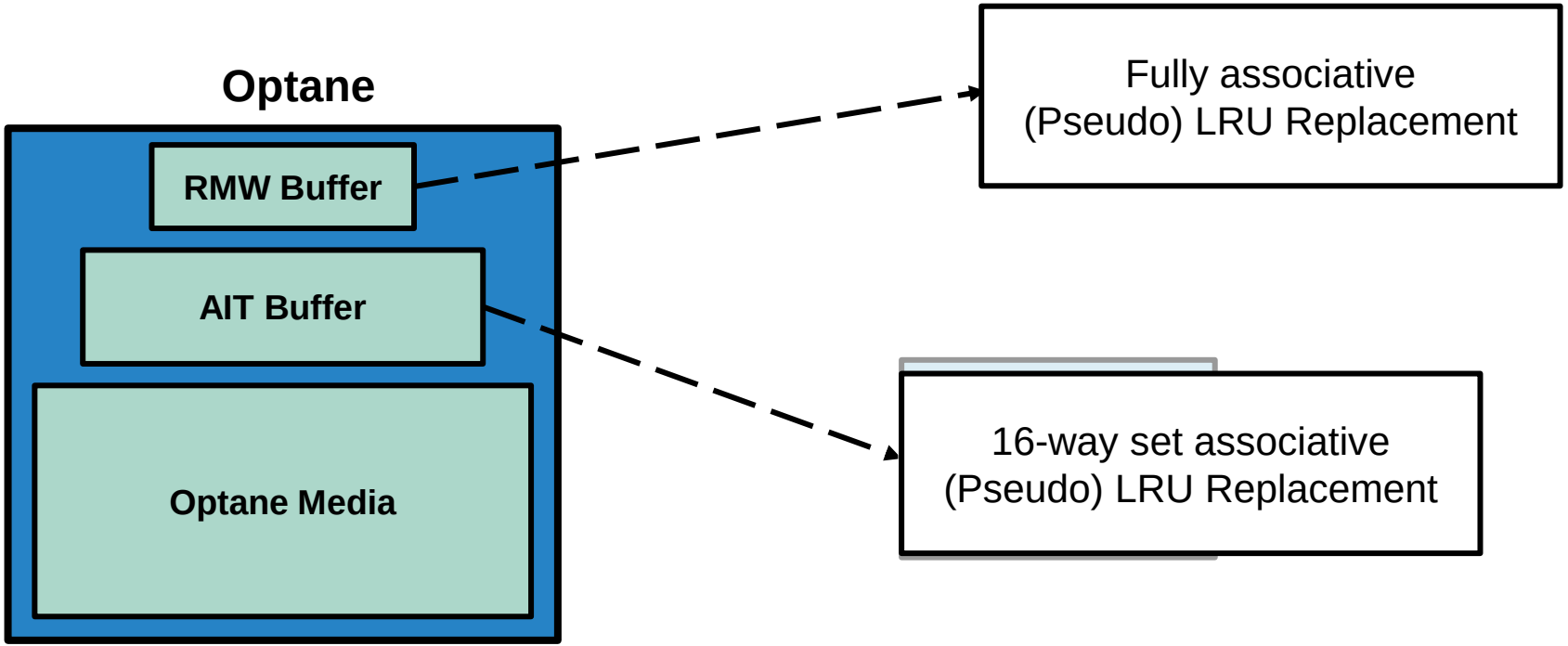
16 KB ⇄ 256 B

16 MB ⇄ 4 KB

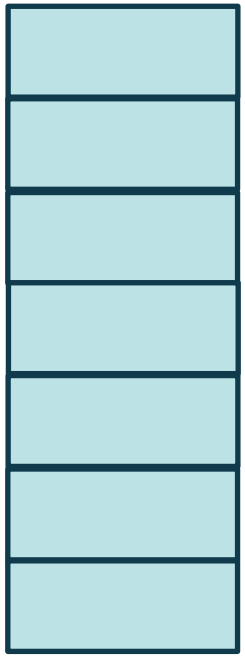
On-DIMM caches



On-DIMM caches

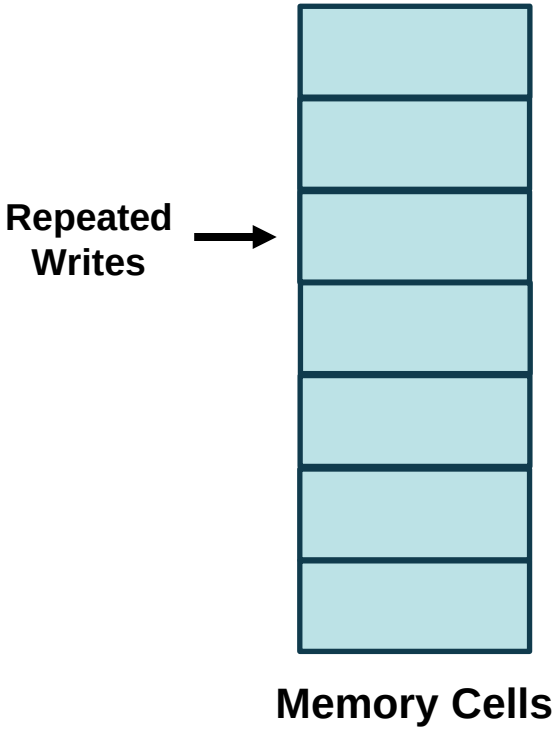


Wear-levelling in Memories

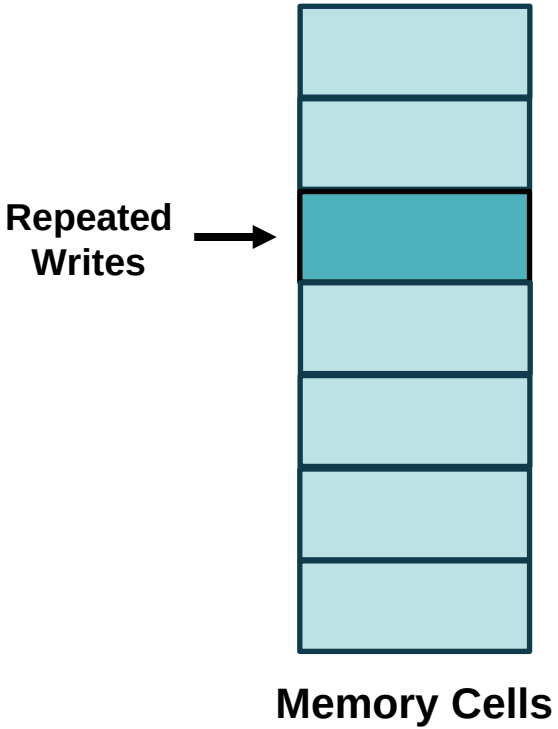


Memory Cells

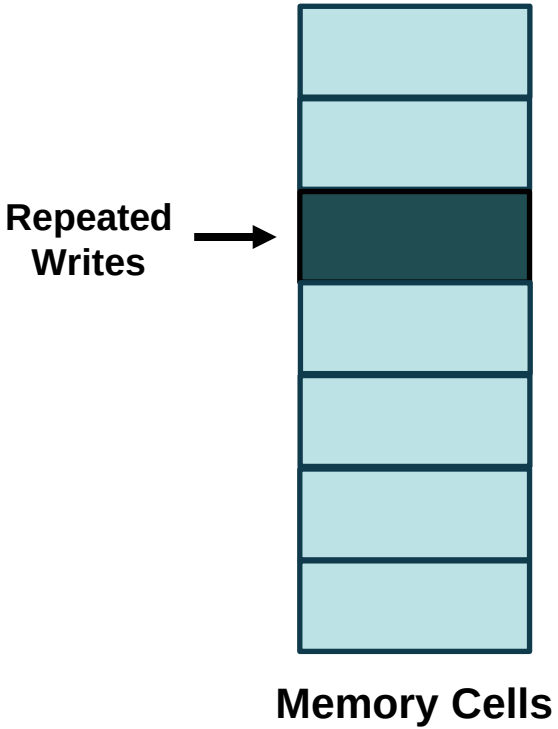
Wear-levelling in Memories



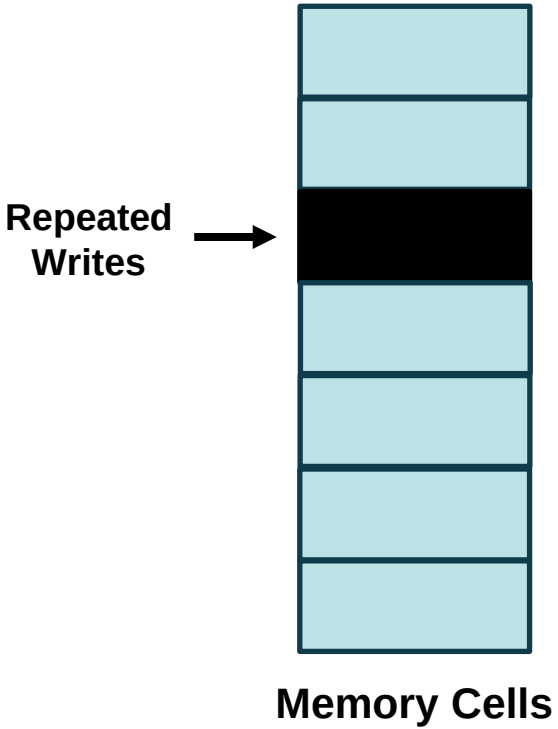
Wear-levelling in Memories



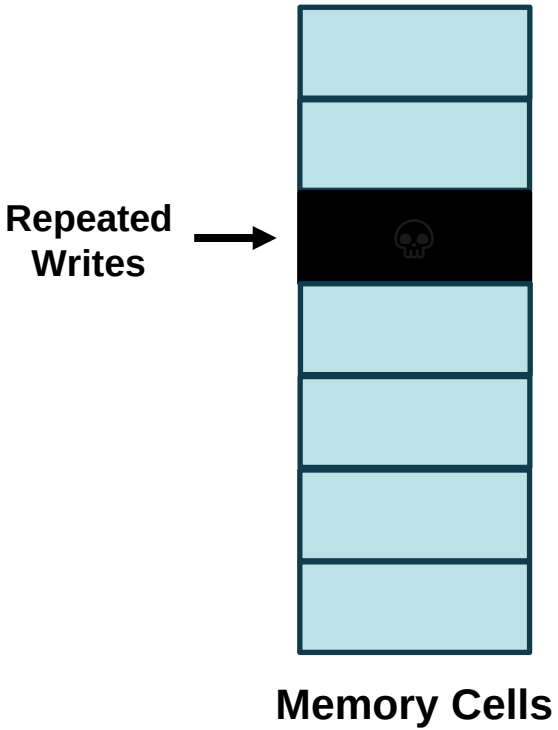
Wear-levelling in Memories



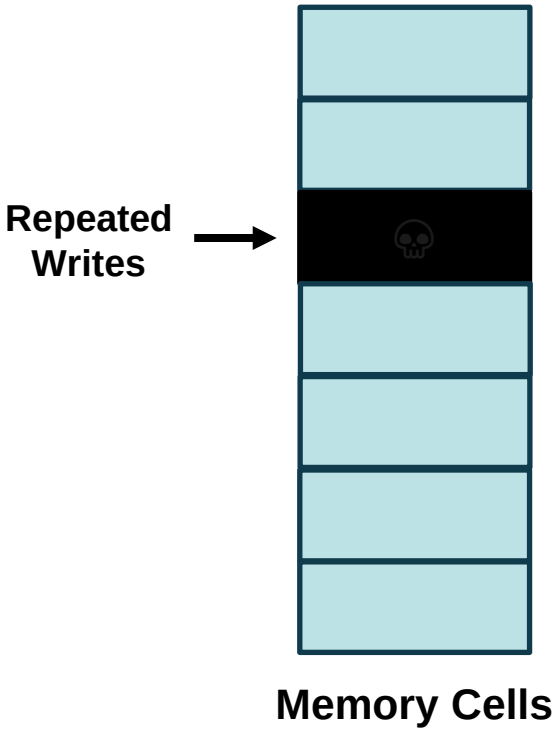
Wear-levelling in Memories



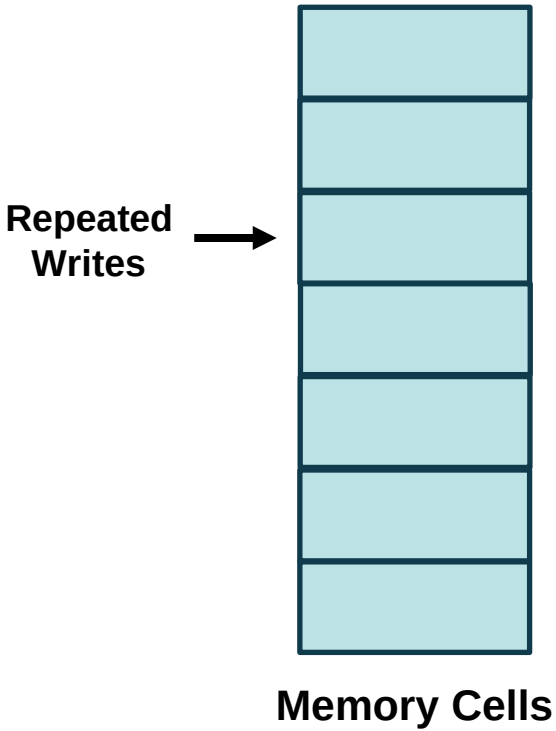
Wear-levelling in Memories



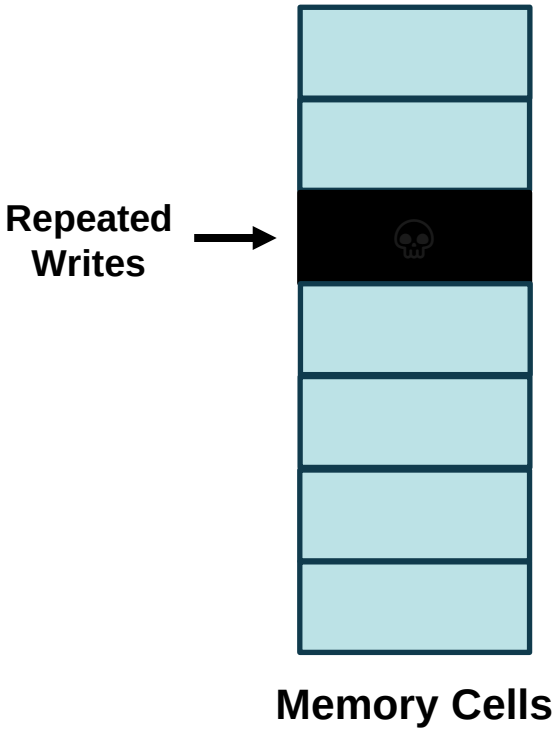
Wear-levelling in Memories



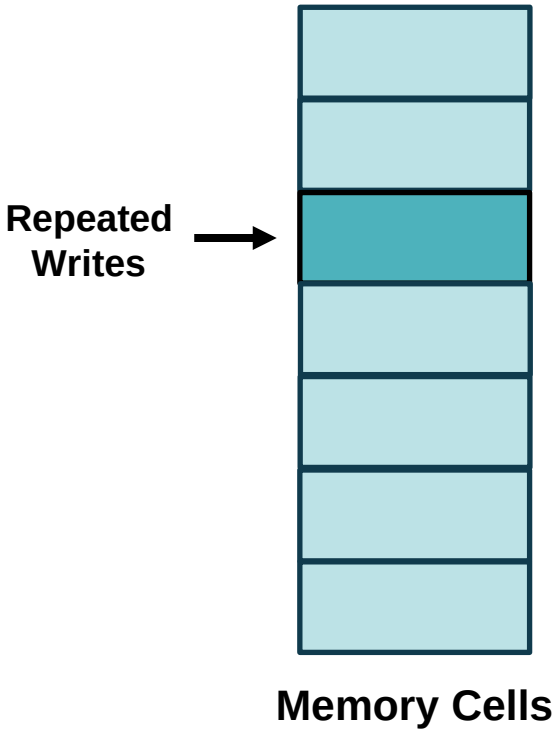
Wear-levelling to the rescue!



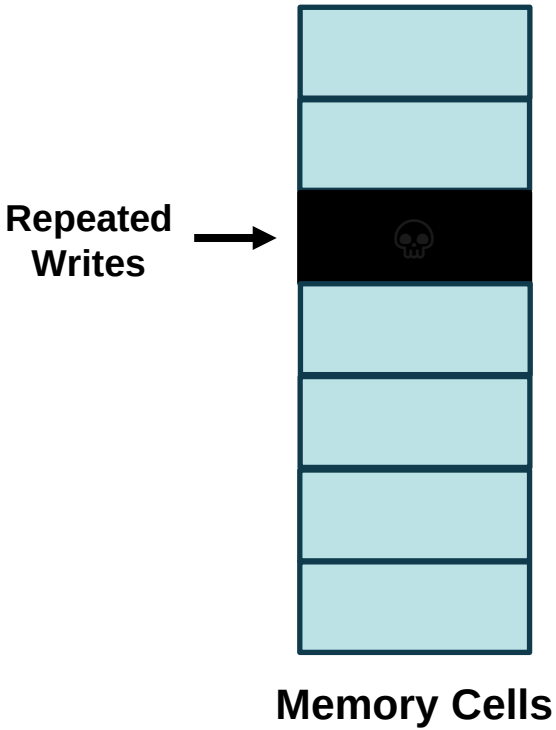
Wear-levelling in Memories



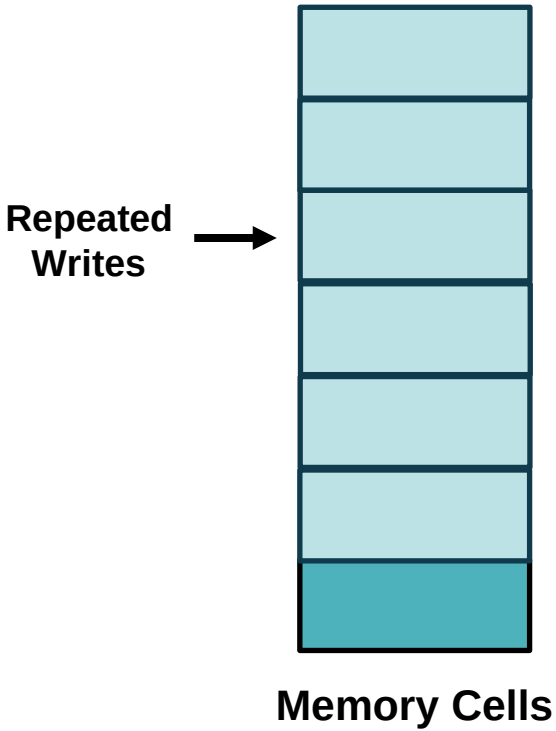
Wear-levelling to the rescue!



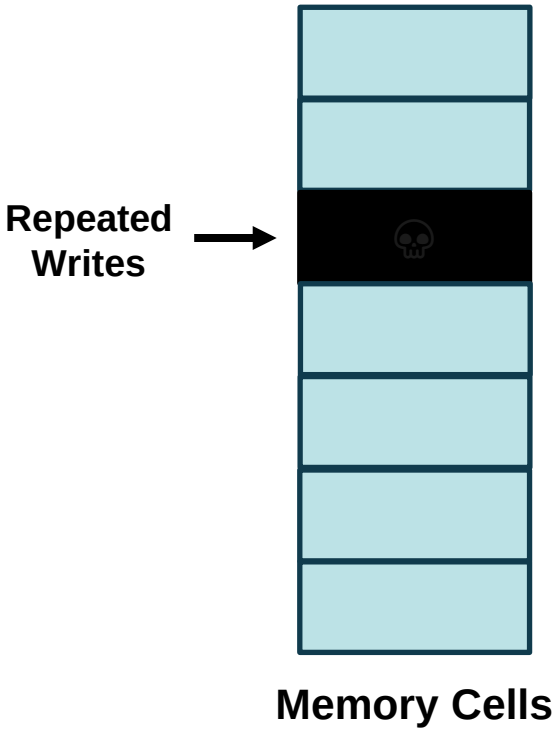
Wear-levelling in Memories



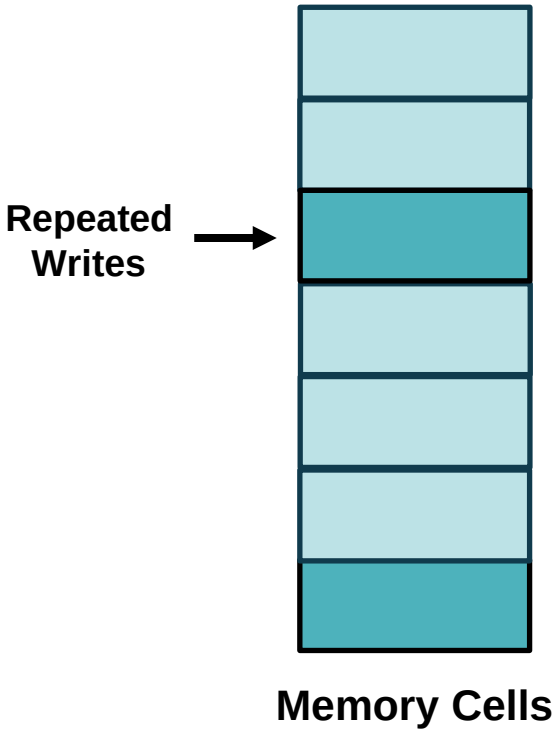
Wear-levelling to the rescue!



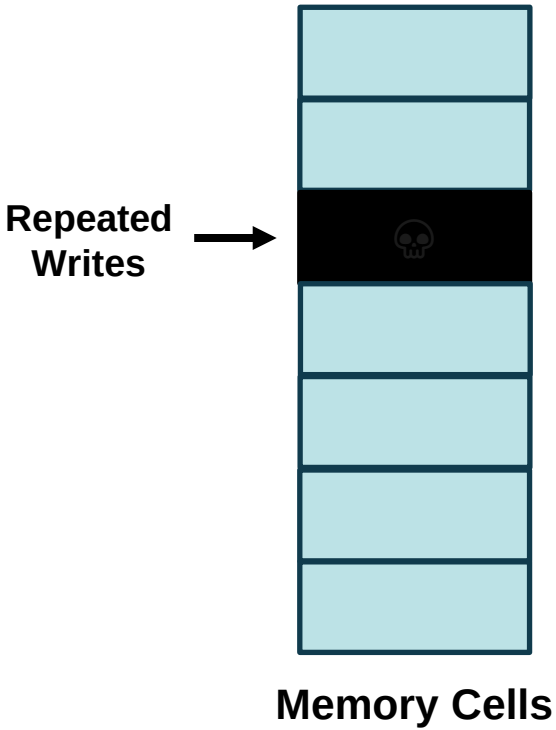
Wear-levelling in Memories



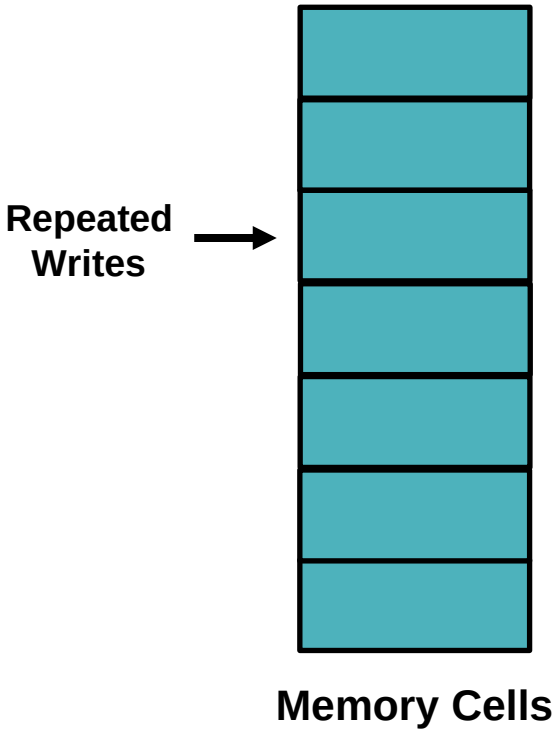
Wear-levelling to the rescue!



Wear-levelling in Memories

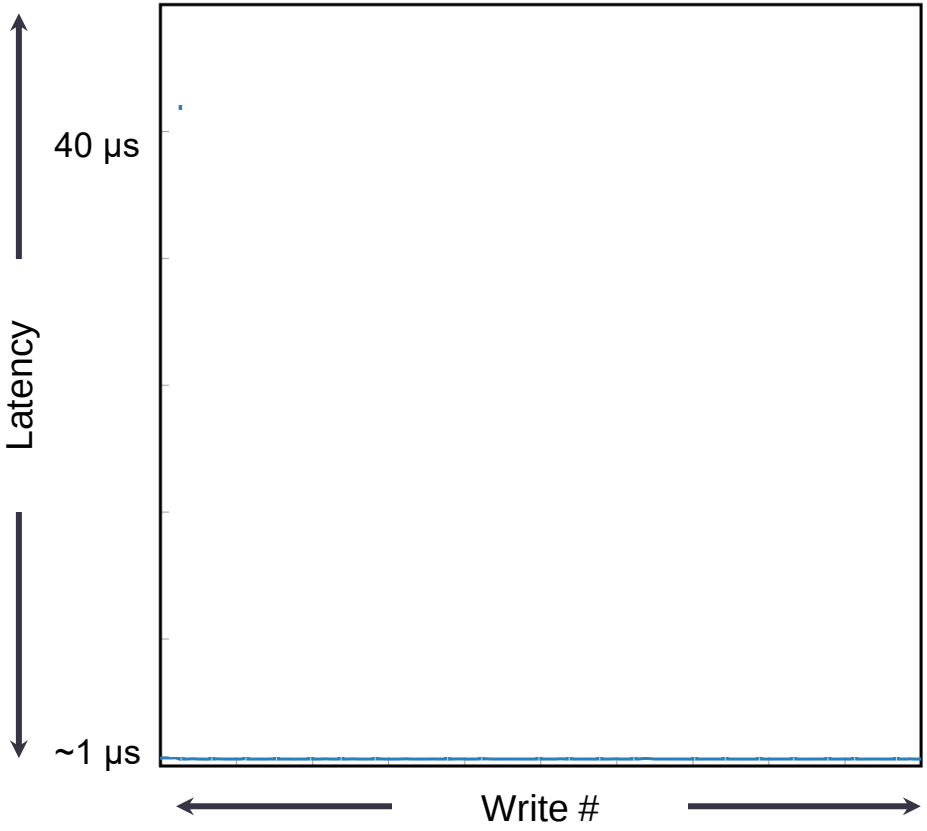


Wear-levelling to the rescue!

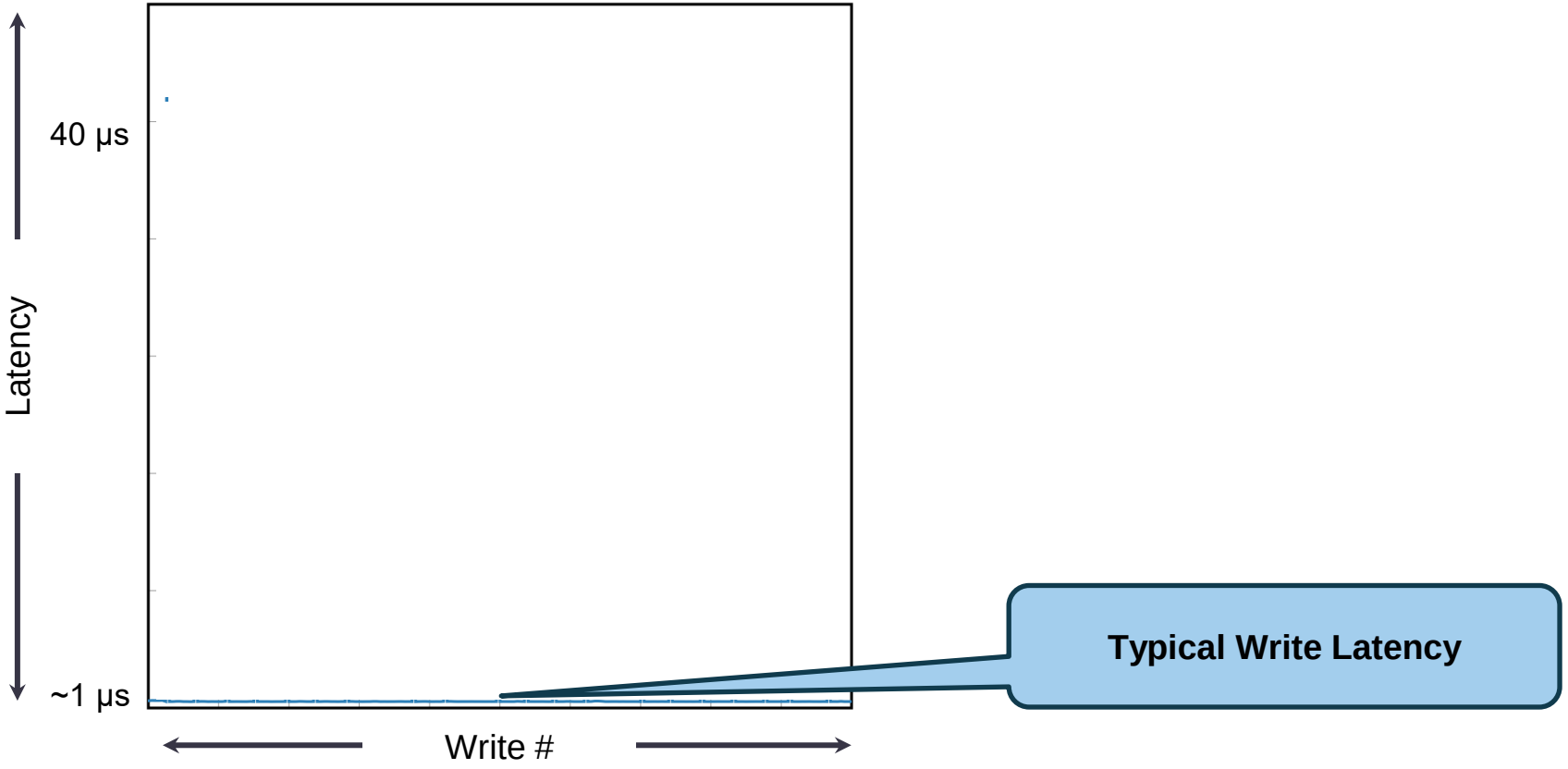


Wear-levelling in Optane: When/What?

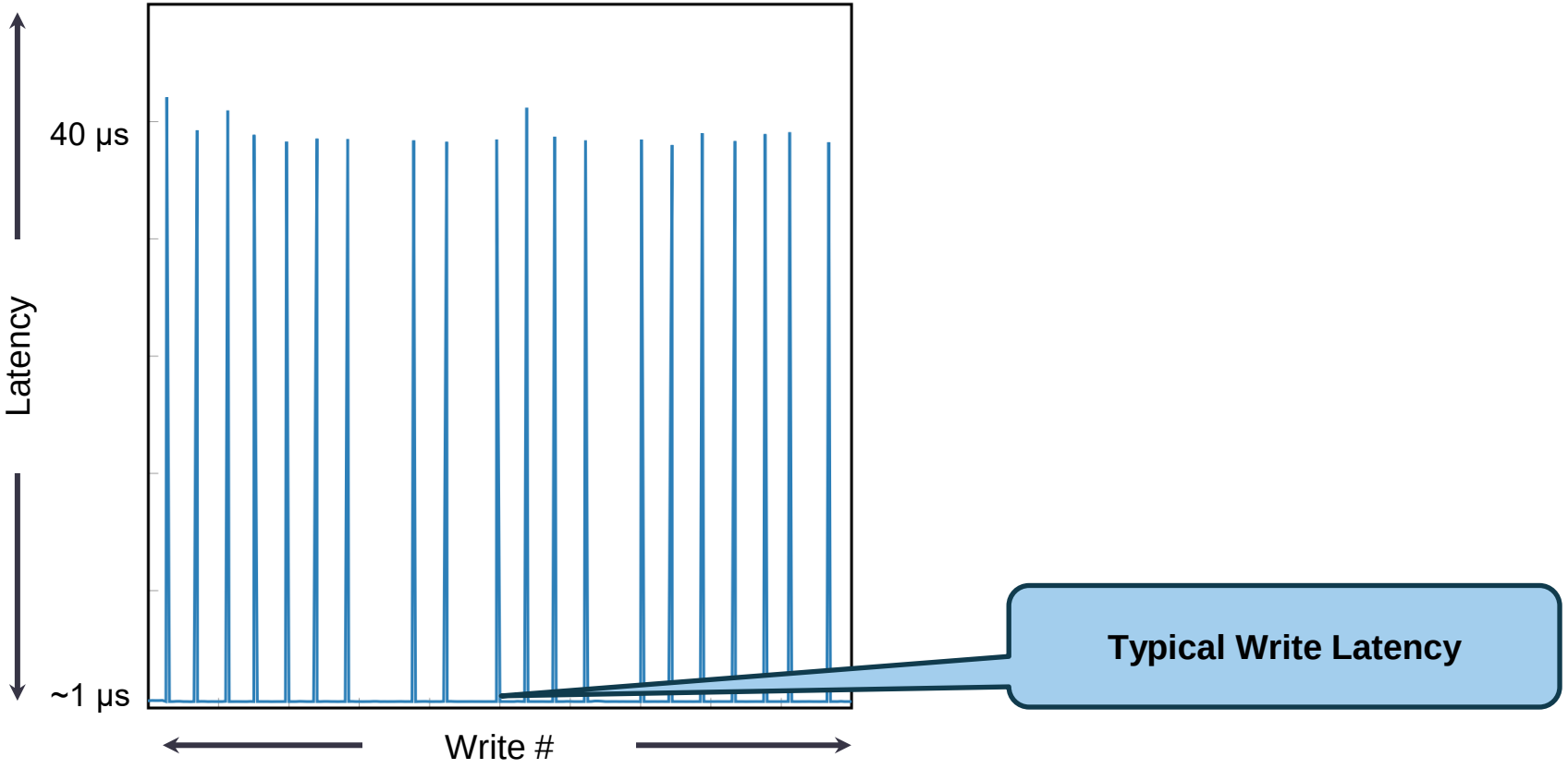
Wear-levelling in Optane: When/What?



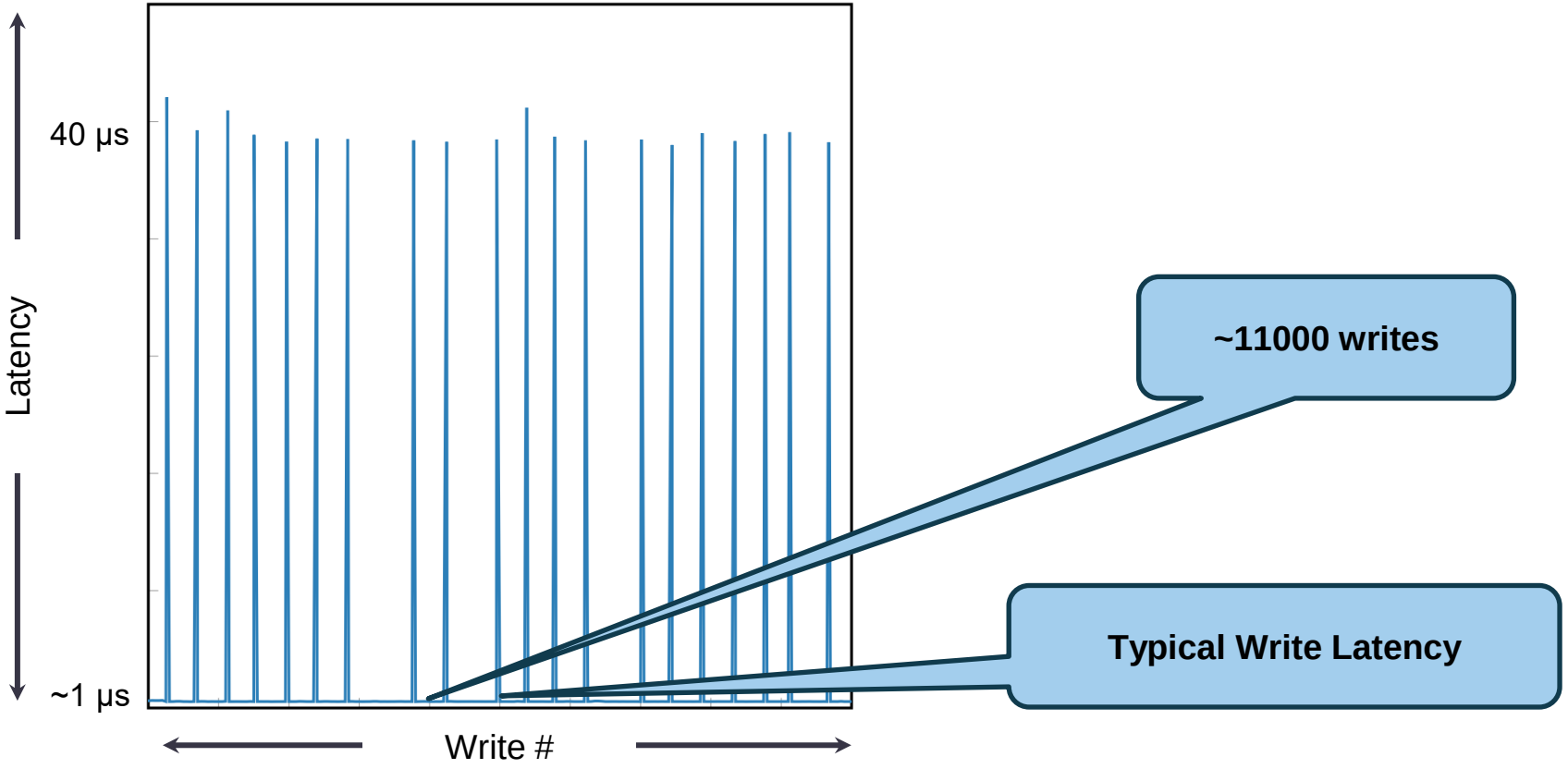
Wear-levelling in Optane: When/What?



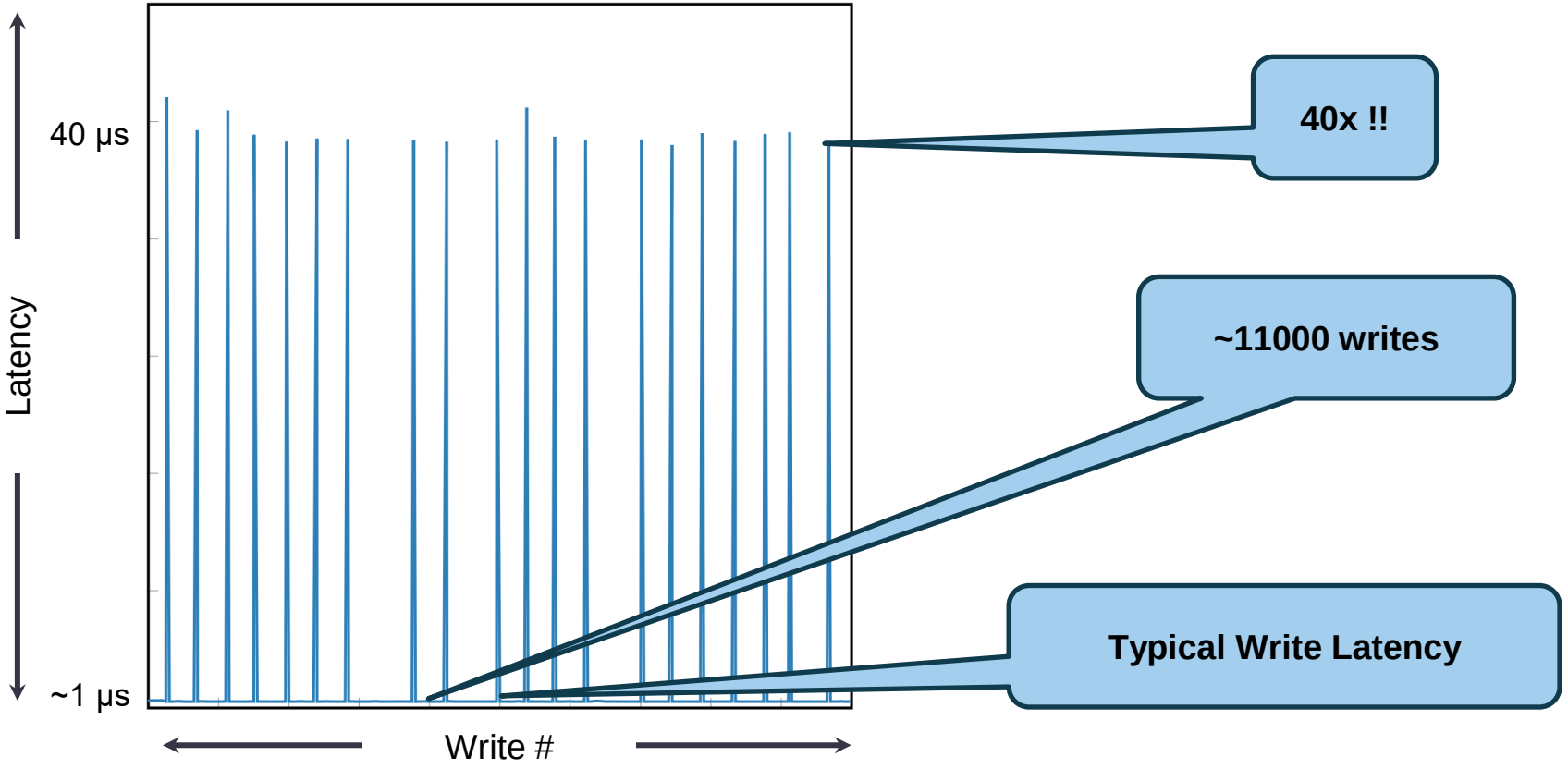
Wear-levelling in Optane: When/What?



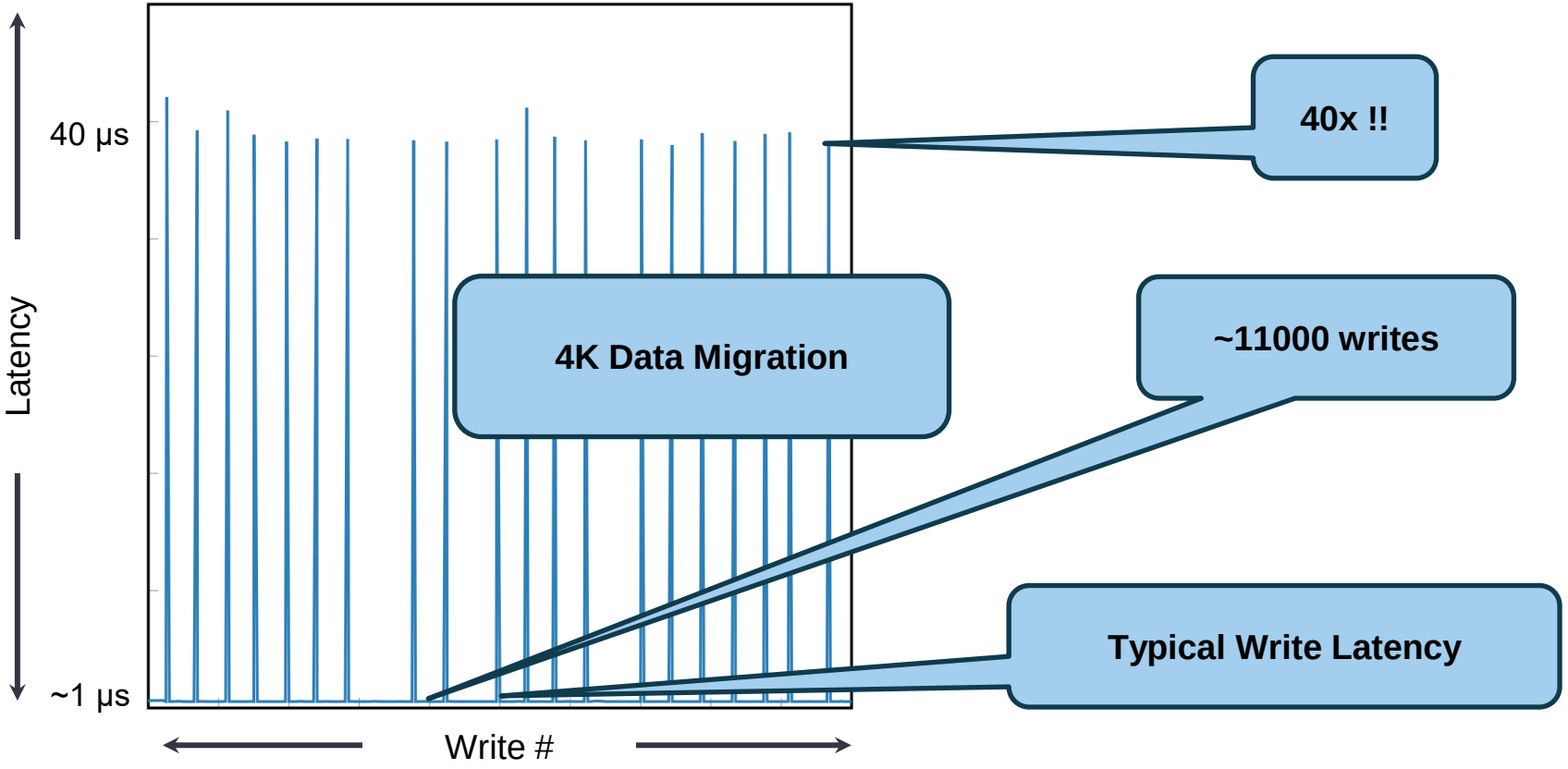
Wear-levelling in Optane: When/What?



Wear-levelling in Optane: When/What?



Wear-levelling in Optane: When/What?

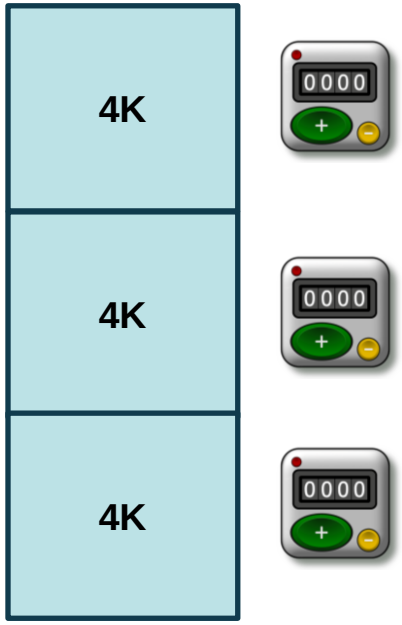


Wear-levelling in Optane: How?

Expectations	Reality

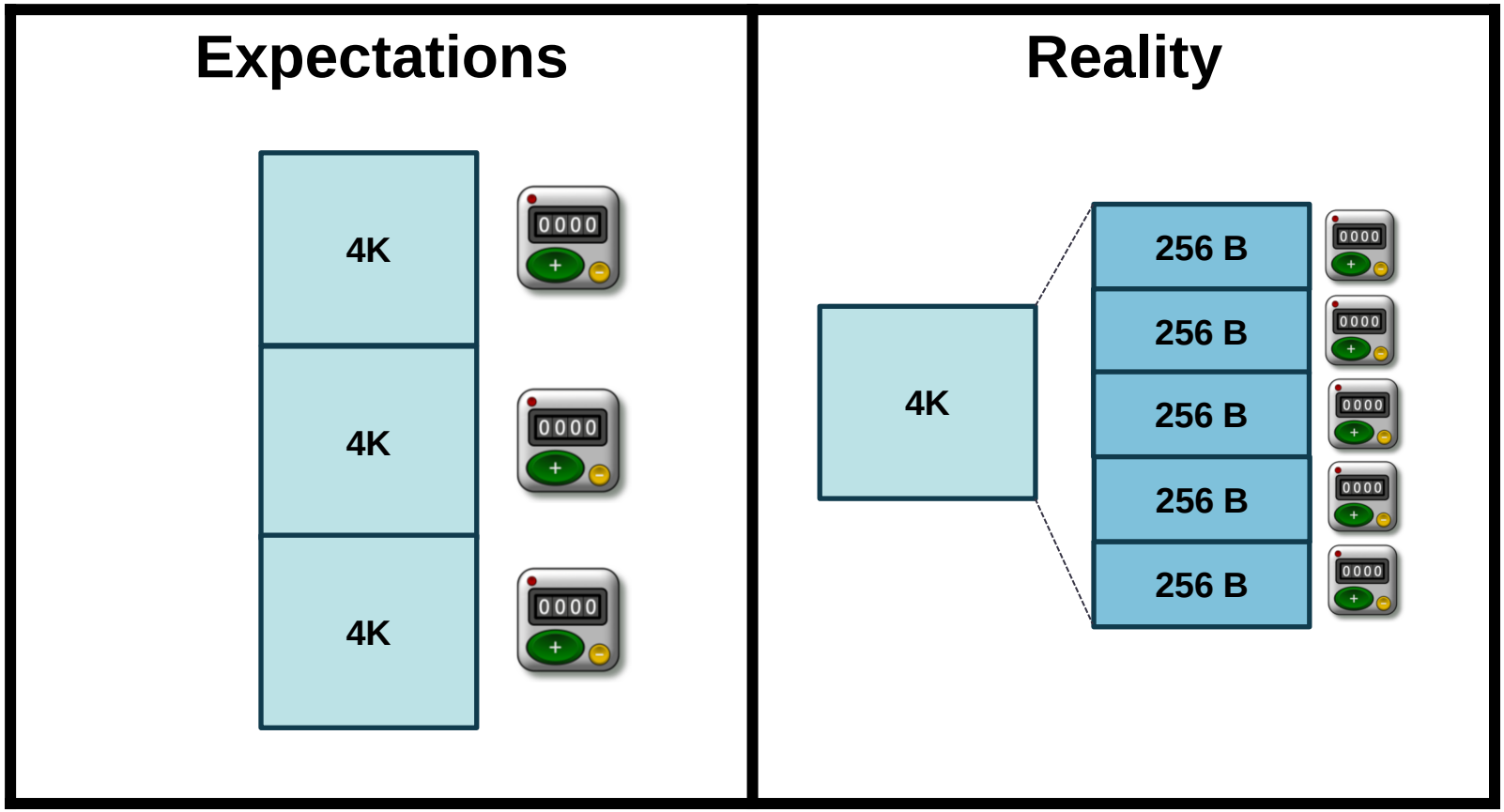
Wear-levelling in Optane: How?

Expectations



Reality

Wear-levelling in Optane: How?



An Optane Curveball: *clflush*

Expectations	Reality

An Optane Curveball: *clflush*

Expectations	Reality
cl == cache line	

An Optane Curveball: *clflush*

Expectations	Reality
cl == cache line == CPU cache line	

An Optane Curveball: *clflush*

Expectations	Reality
cl == cache line == CPU cache line **"*clflush* flushes only CPU caches"**	

An Optane Curveball: *clflush*

Expectations	Reality
cl == cache line	*clflush* reaches Optane!
== CPU cache line	
"*clflush* flushes only CPU caches"	

An Optane Curveball: *clflush*

Expectations	Reality
cl == cache line	*clflush* reaches Optane!
== CPU cache line	Flushes RMW Buffer!
"*clflush* flushes only CPU caches"	

An Optane Curveball: *clflush*

Expectations

cl == cache line

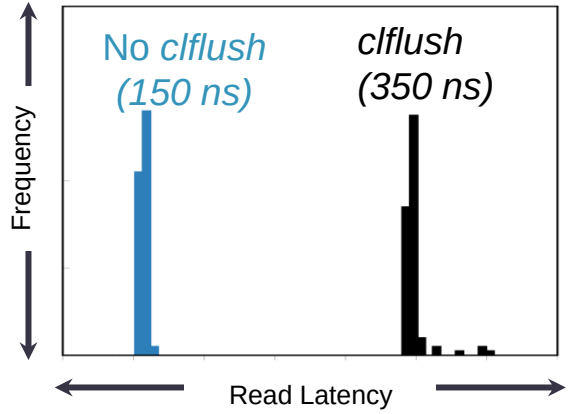
== CPU cache line

“*clflush* flushes only CPU caches”

Reality

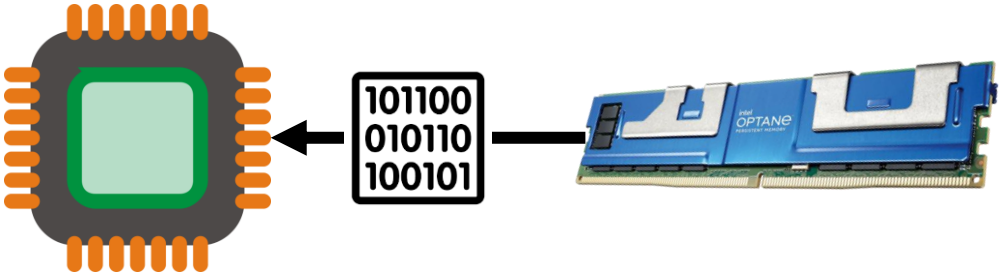
clflush reaches Optane!

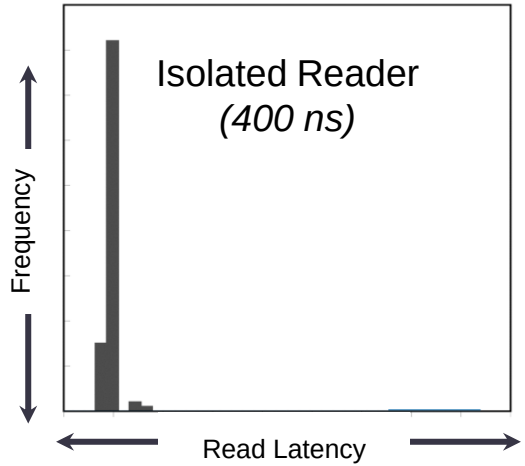
Flushes RMW Buffer!



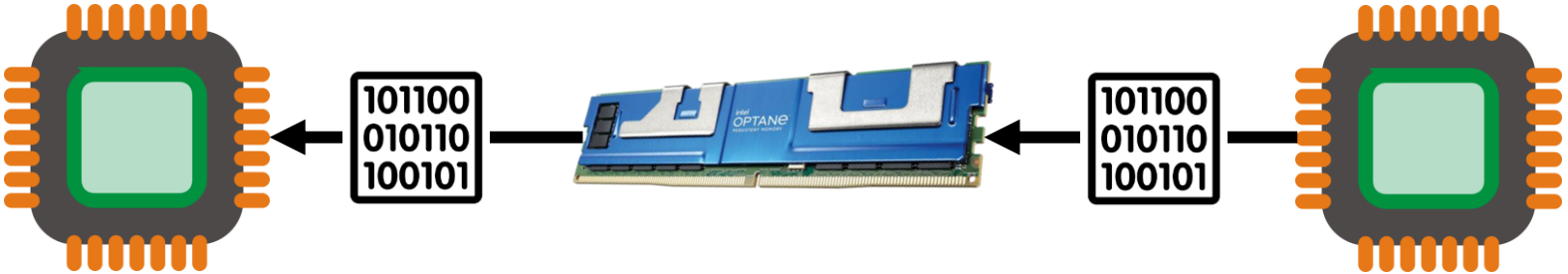
An Optane Curveball: R/W Contention

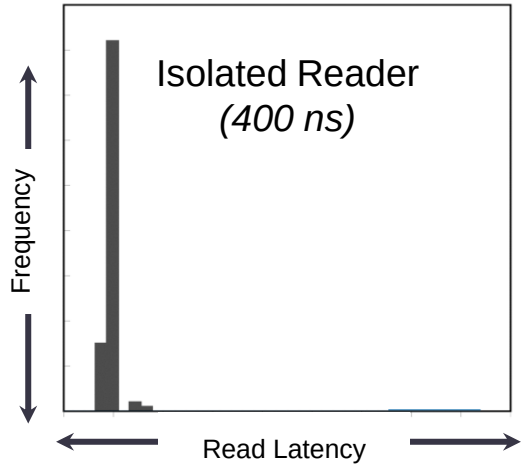
An Optane Curveball: R/W Contention

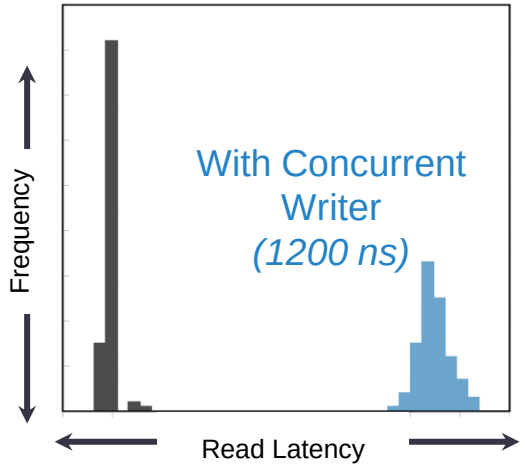




An Optane Curveball: R/W Contention







The Attacks

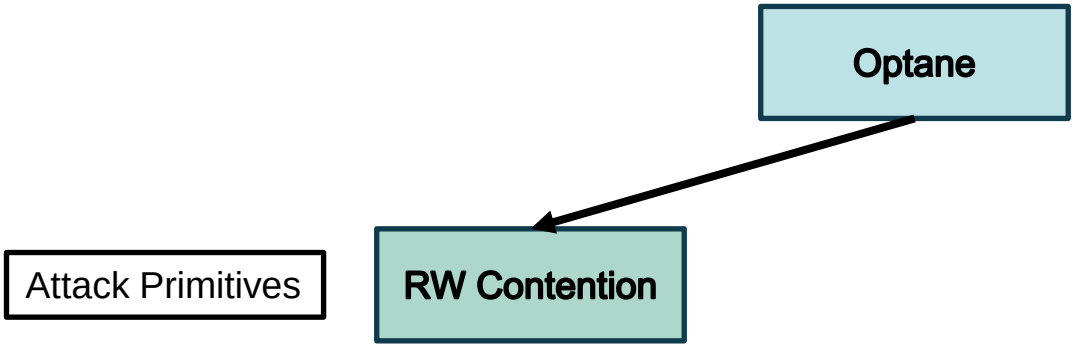
Exploring the security implications of our new attack primitives

A Bird’s Eye view

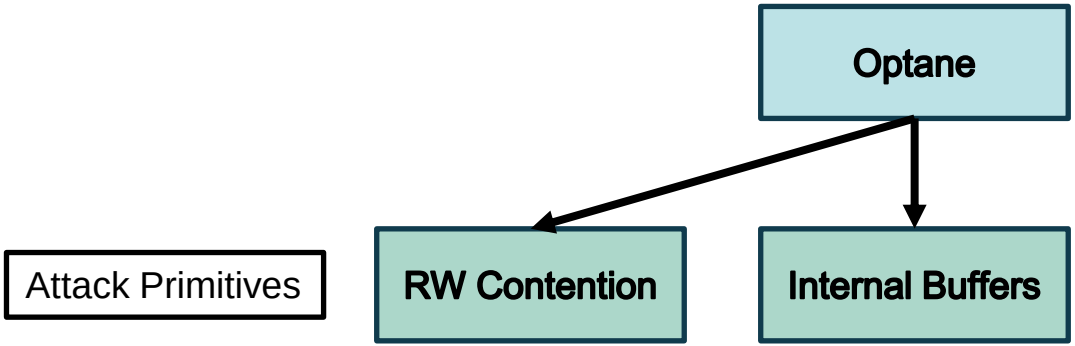
A Bird’s Eye view

A Bird’s Eye view

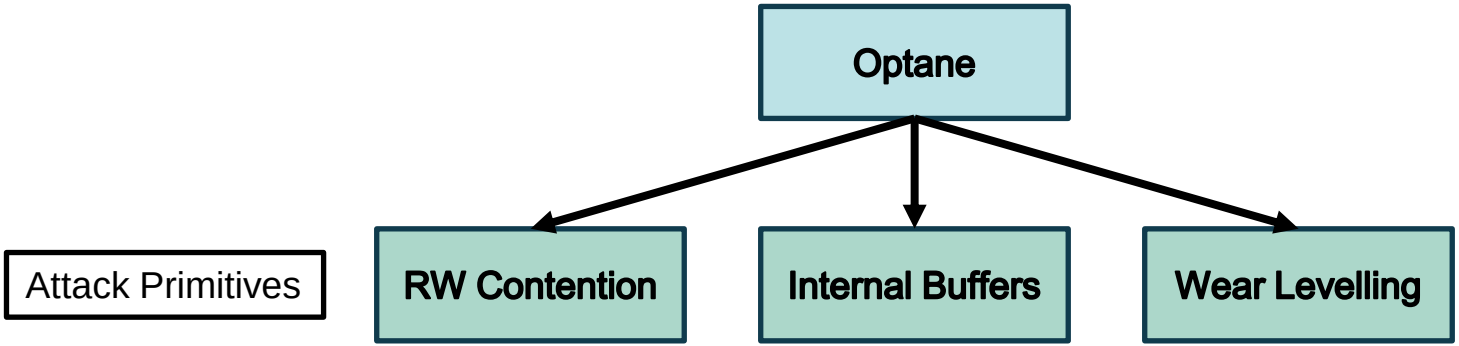
A Bird’s Eye view



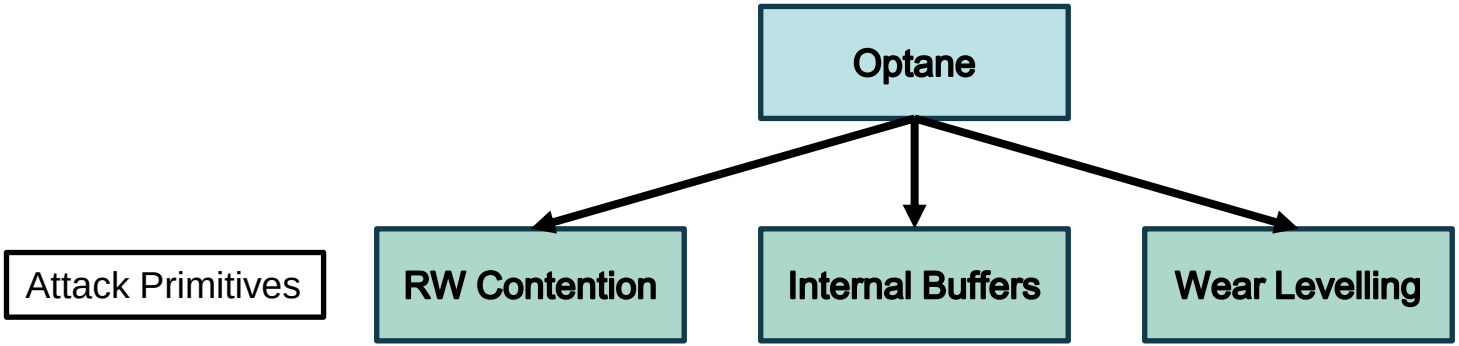
A Bird’s Eye view



A Bird’s Eye view

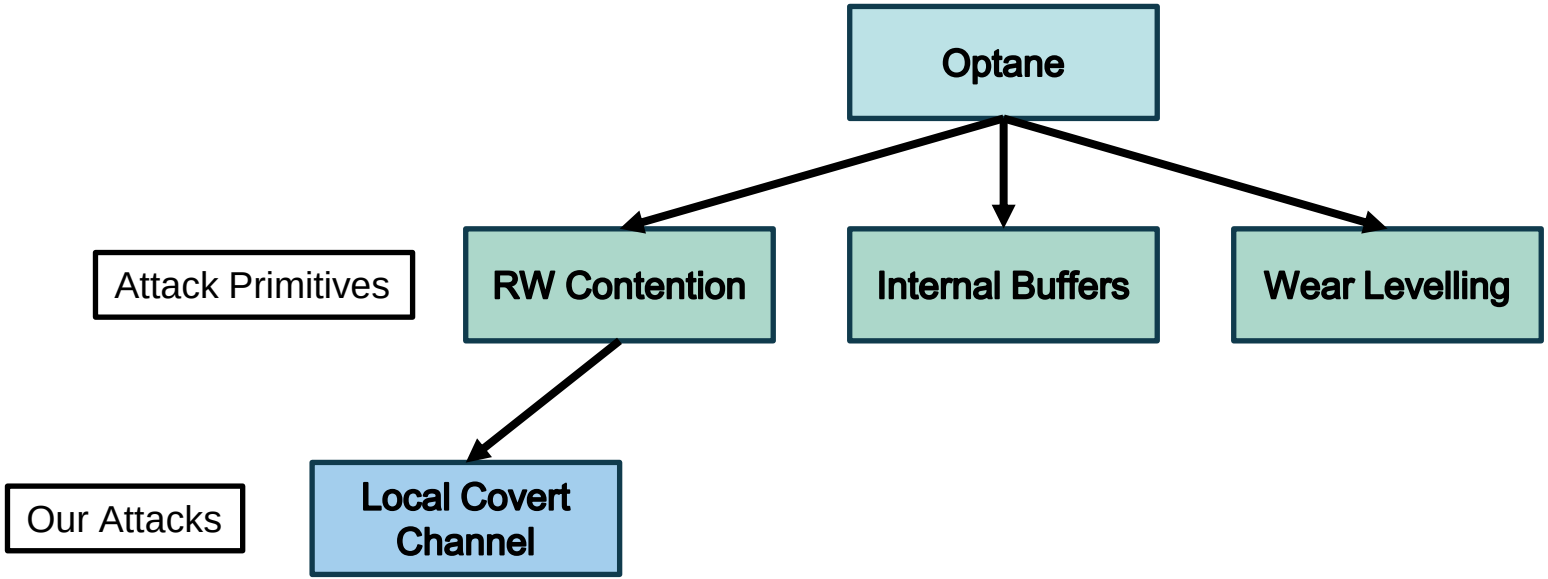


A Bird’s Eye view

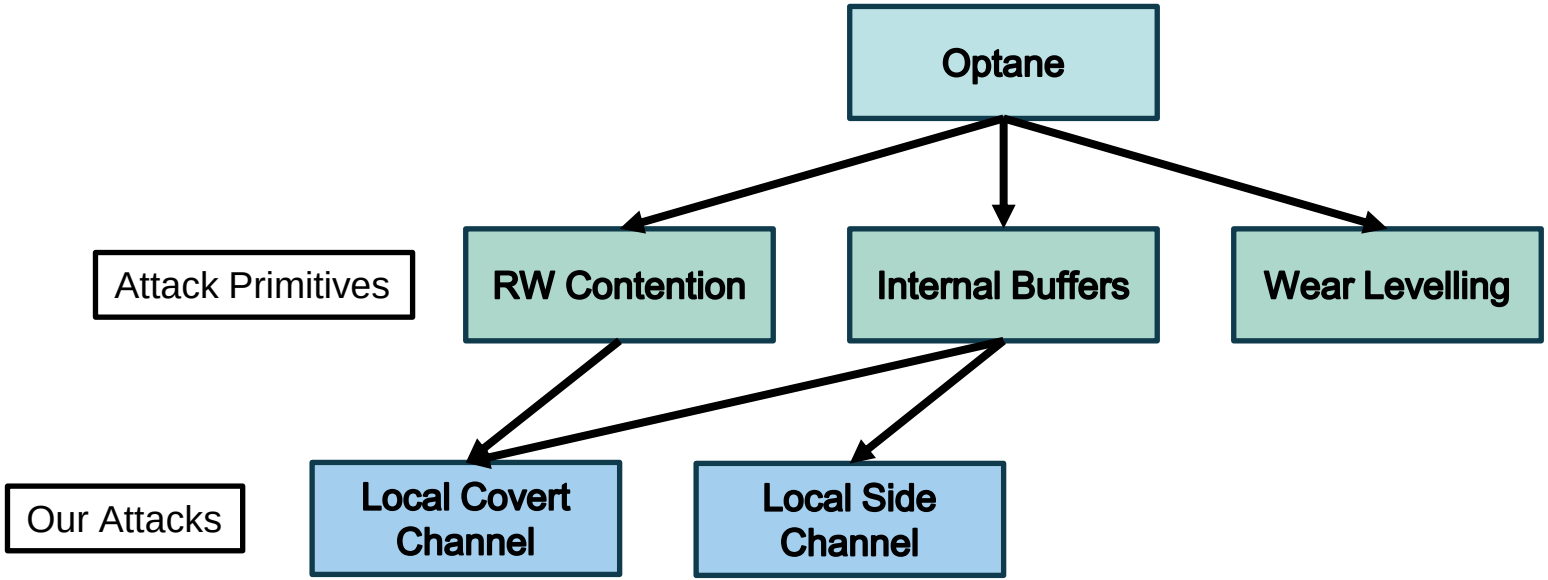


Our Attacks

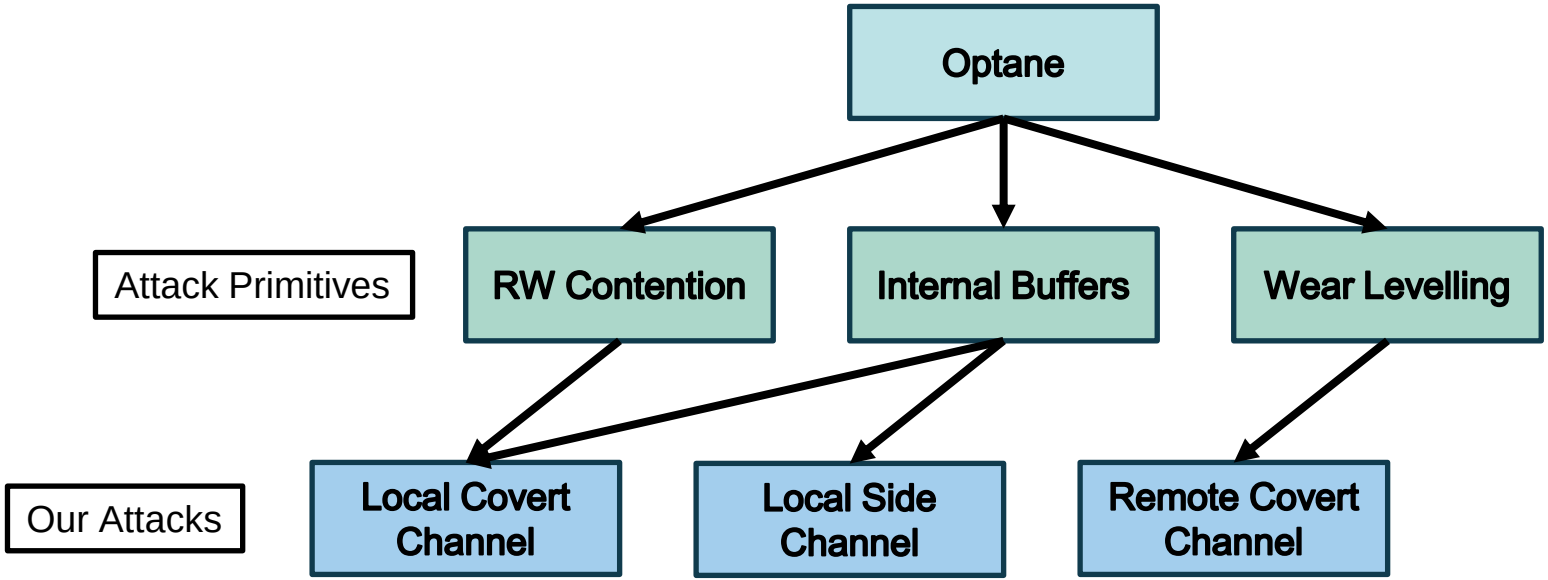
A Bird’s Eye view



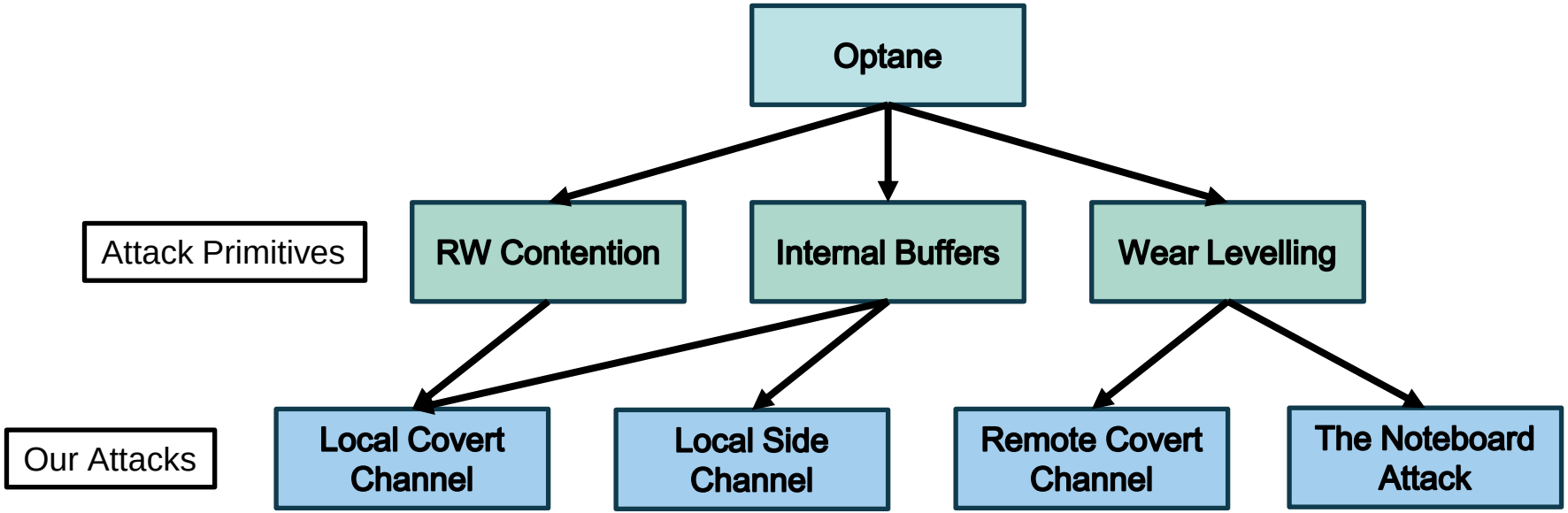
A Bird’s Eye view



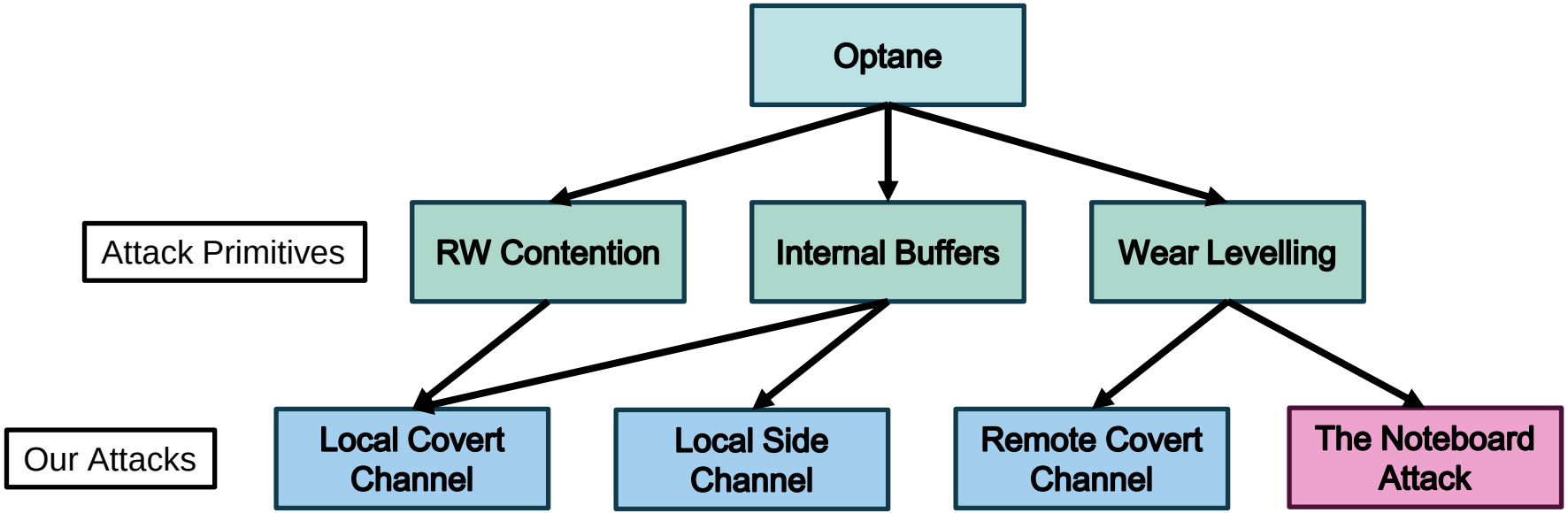
A Bird's Eye view



A Bird’s Eye view



A Bird's Eye view



Attack: Noteboard Covert Channel

Encoding secret messages on Optane’s wear-levelling metadata

The Idea

The Idea

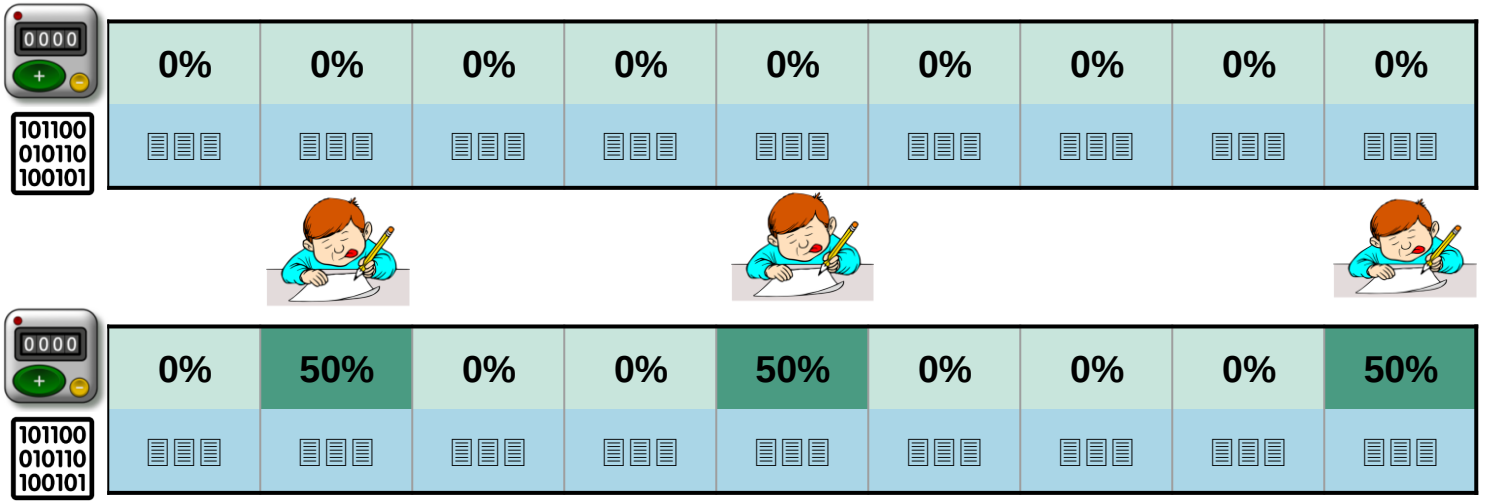
0%	0%	0%	0%	0%	0%	0%	0%	0%

The Idea

0%	0%	0%	0%	0%	0%	0%	0%	0%

The Idea


TOP
SECRET

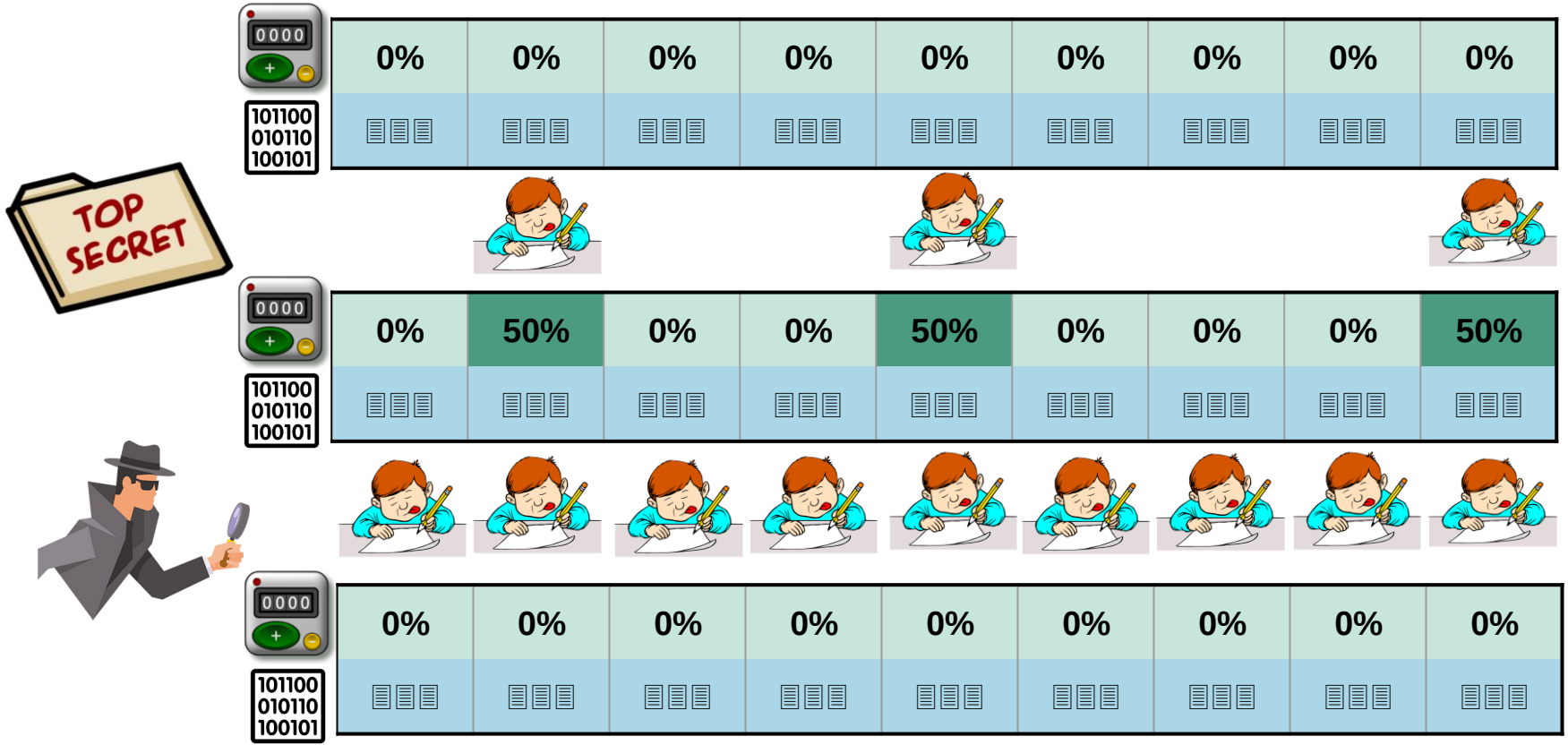

0000
101100
010110
100101
0%
0%
0%
0%
0%
0%
0%
0%
0%
0000
101100
010110
100101
0%
50%
0%
0%
50%
0%
0%
0%
50%

The Idea

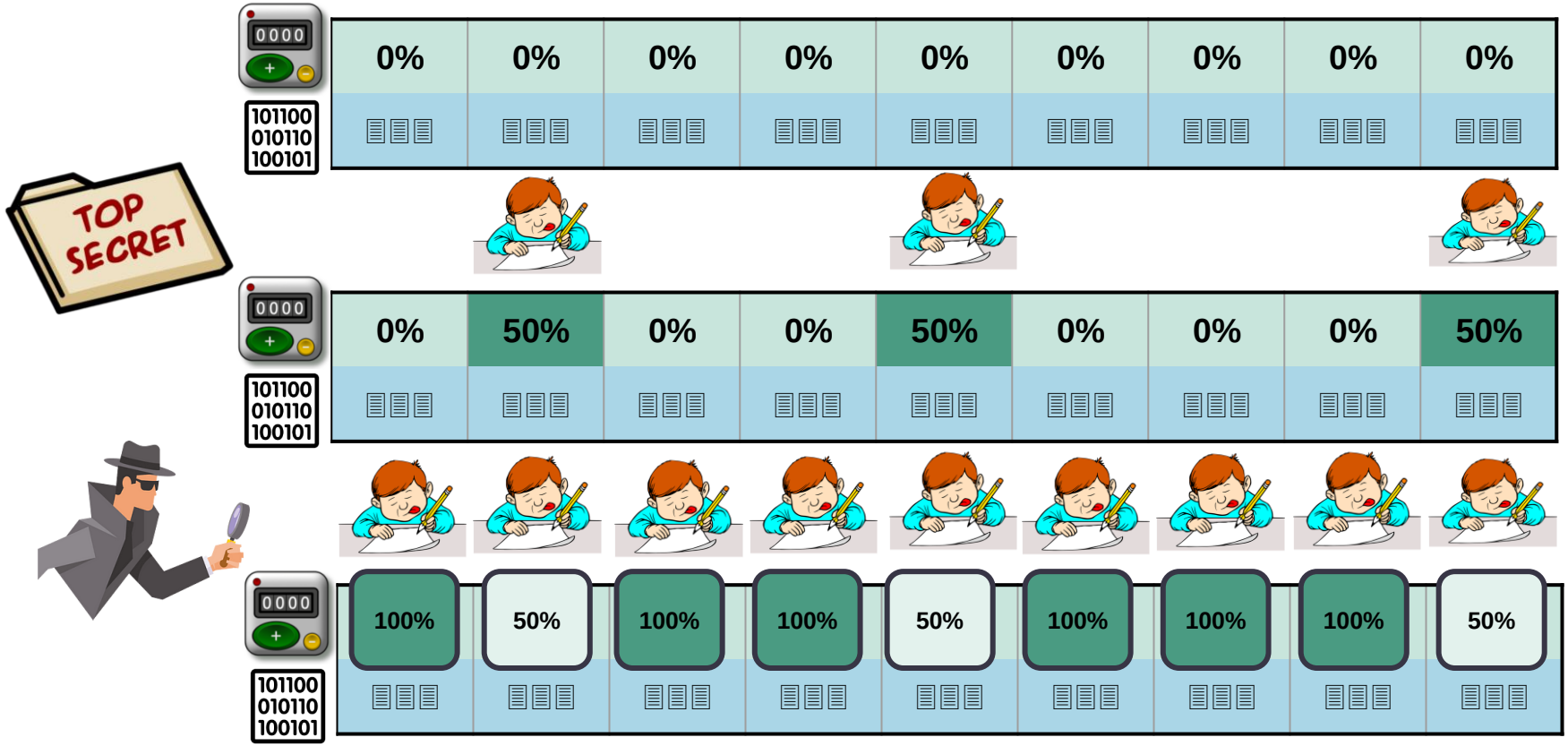
0%	0%	0%	0%	0%	0%	0%	0%	0%

0%	50%	0%	0%	50%	0%	0%	0%	50%

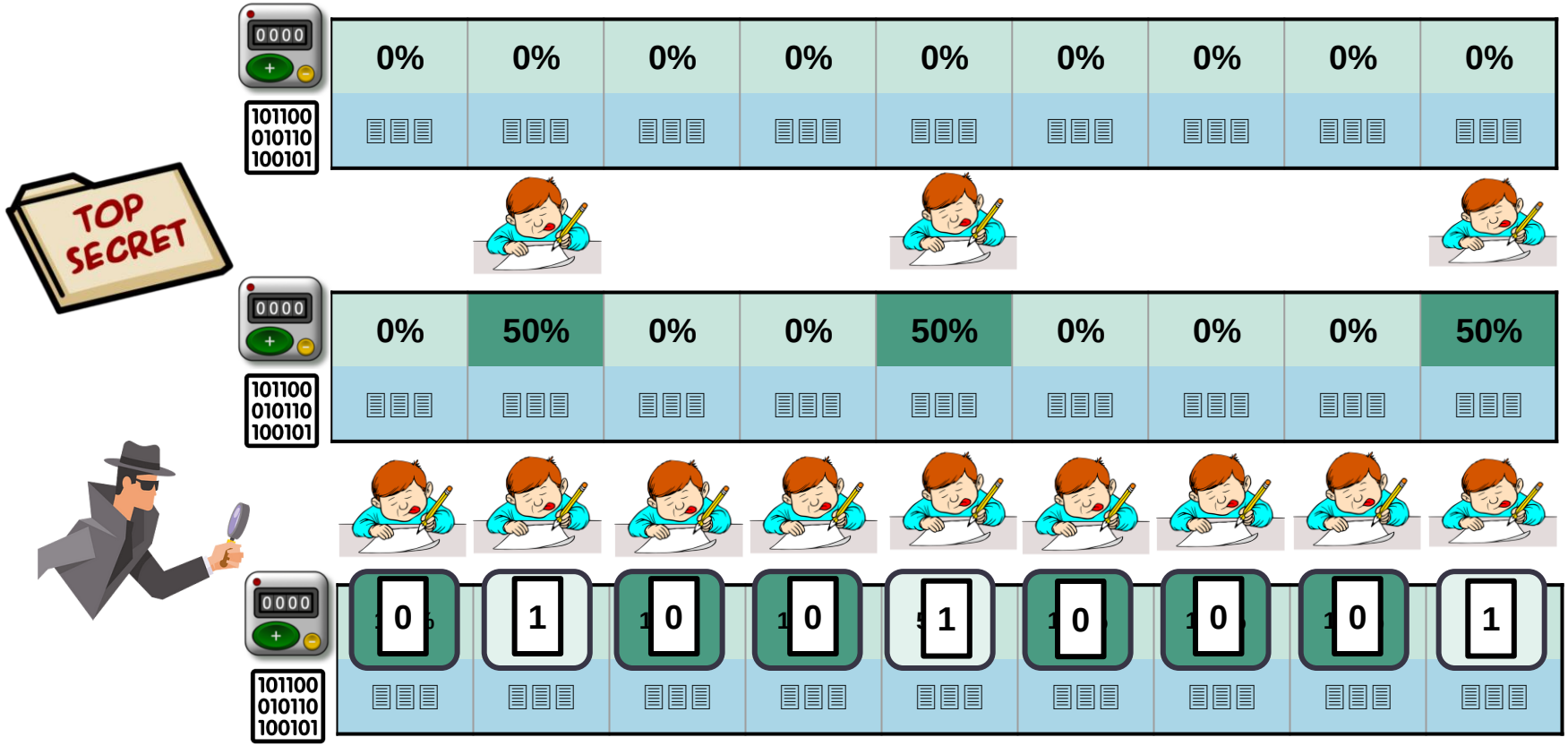
The Idea


0000
101100
010110
100101
0% 0% 0% 0% 0% 0% 0% 0% 0%
TOP SECRET
0000
101100
010110
100101
0% 50% 0% 0% 50% 0% 0% 0% 50%
0000
101100
010110
100101
0% 0% 0% 0% 0% 0% 0% 0% 0%

The Idea

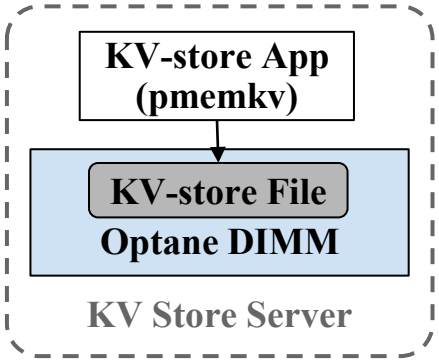

TOP SECRET
0000
101100
010110
100101
0% 0% 0% 0% 0% 0% 0% 0% 0%
0000
101100
010110
100101
0% 50% 0% 0% 50% 0% 0% 0% 50%
0000
101100
010110
100101
100% 50% 100% 100% 50% 100% 100% 100% 50%

The Idea



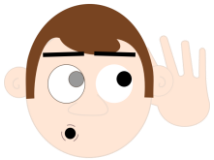
A Realization

A Realization

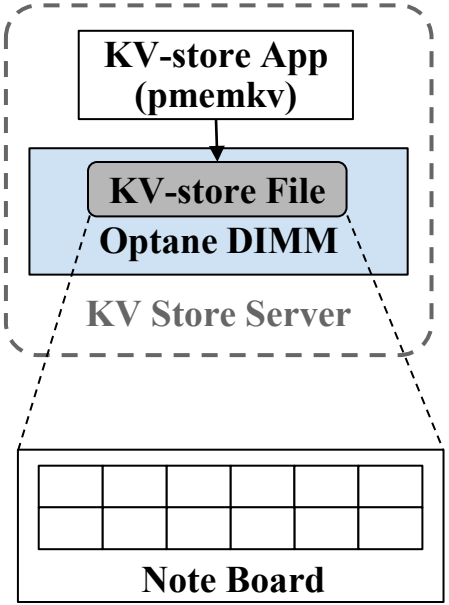


A Realization

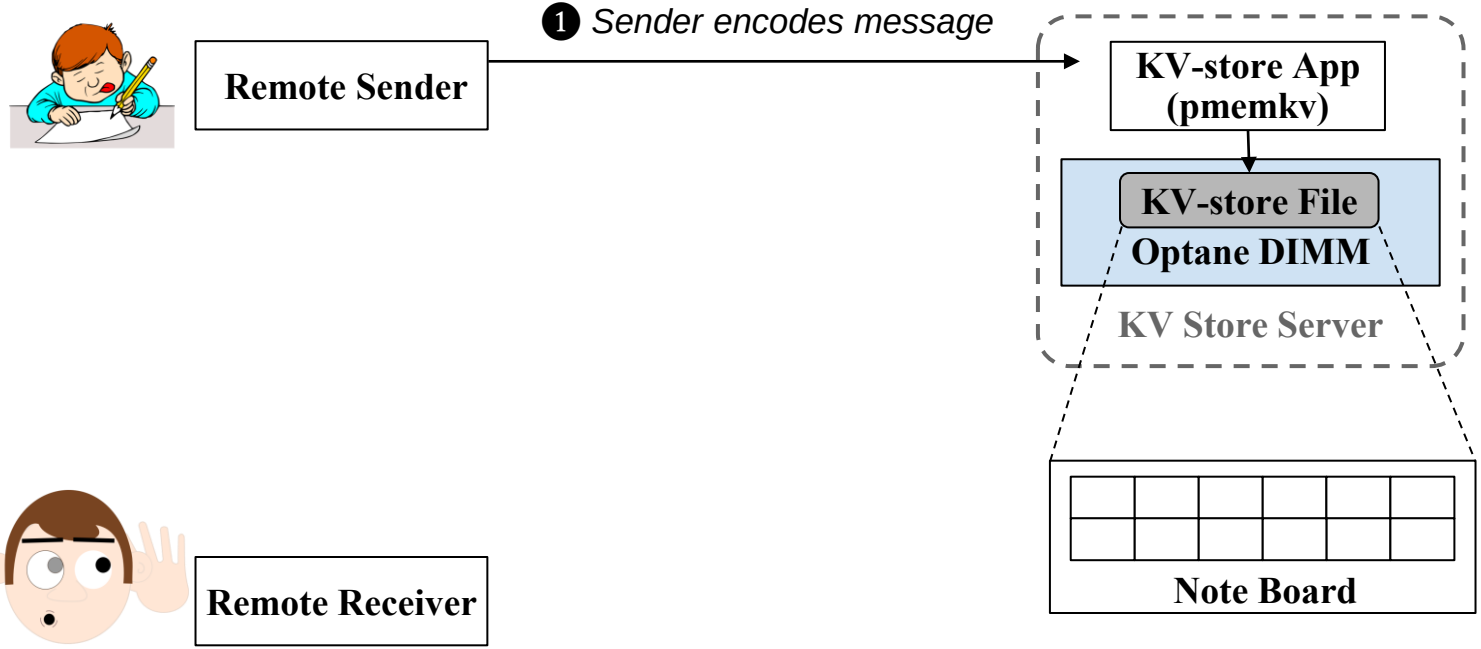
Remote Sender



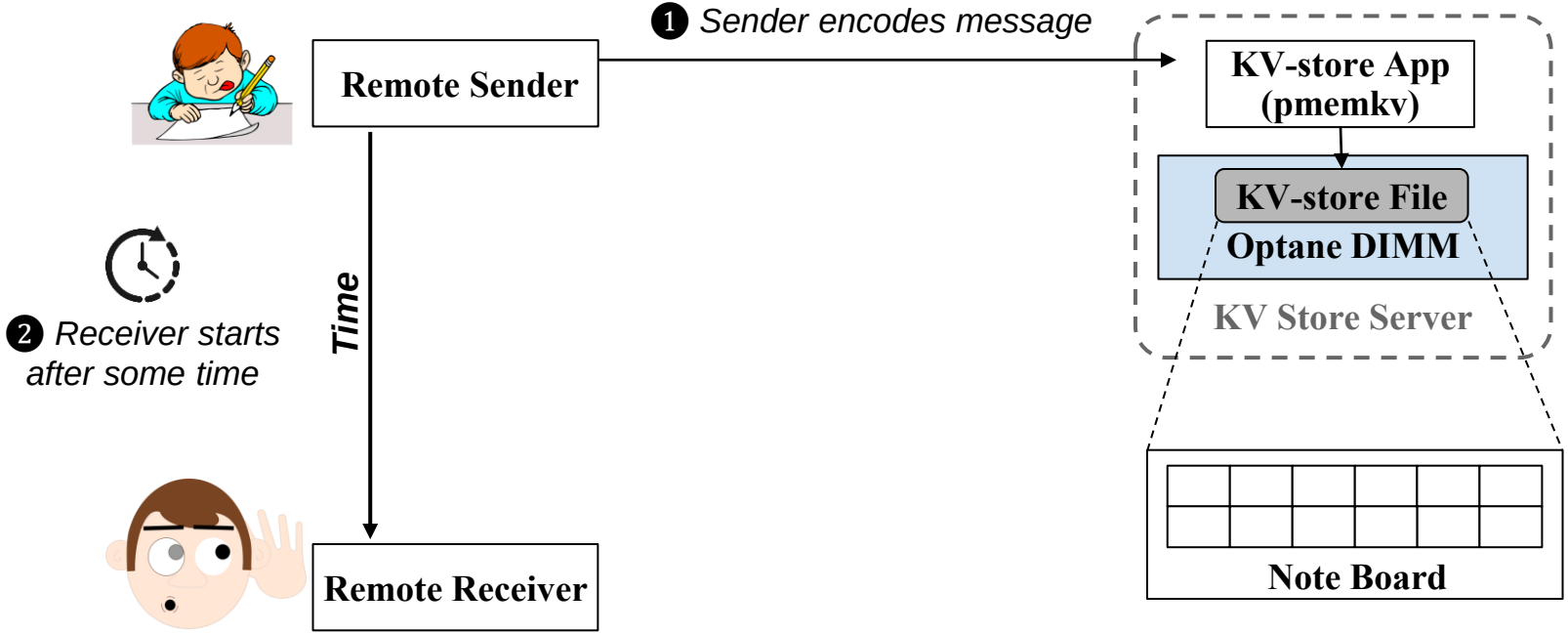
Remote Receiver



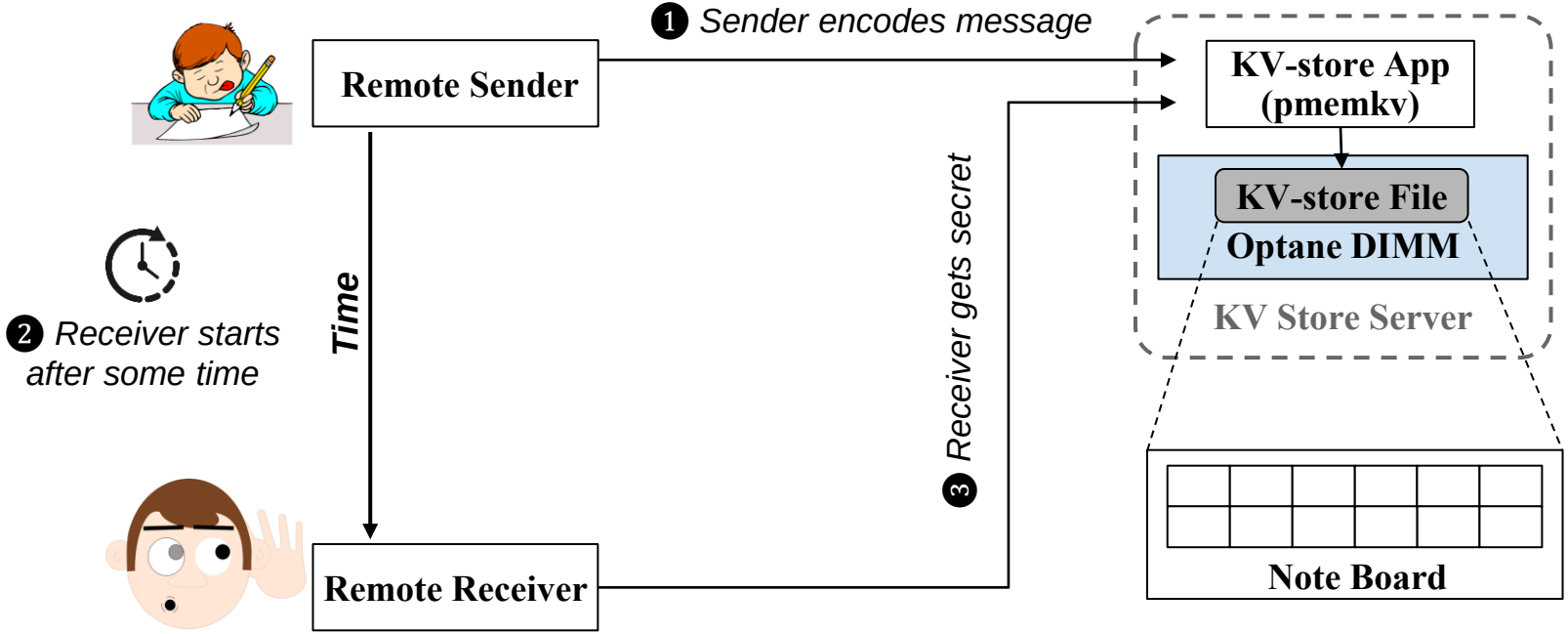
A Realization



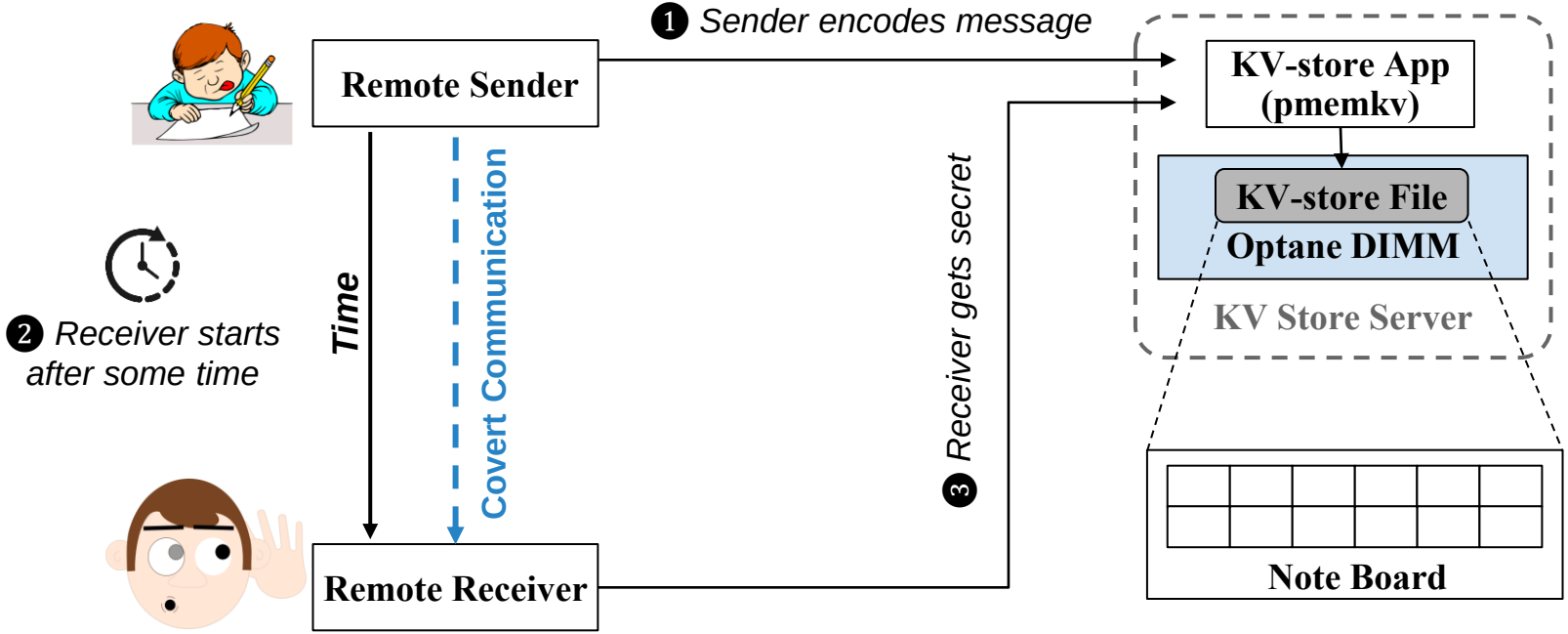
A Realization



A Realization



A Realization



A Realization

Result

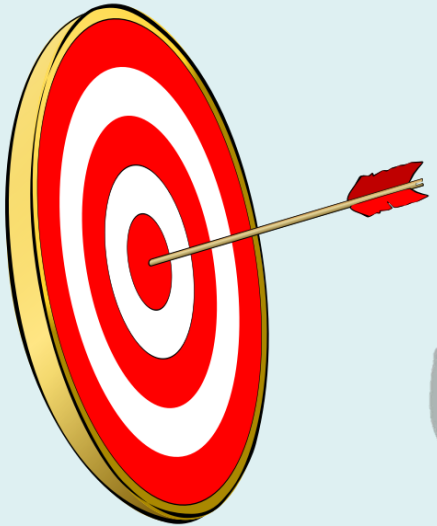
A Realization

Result

A Realization

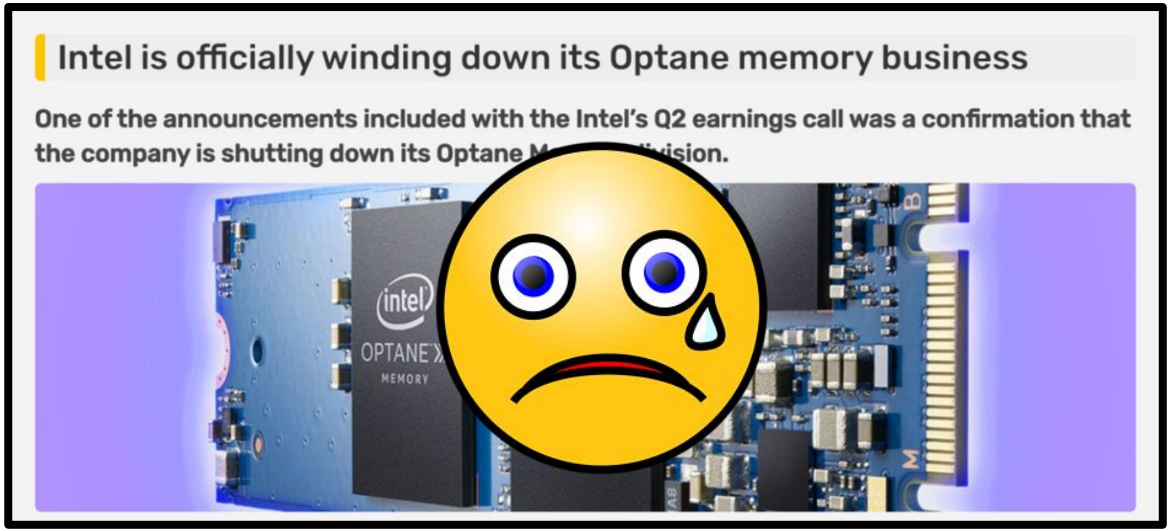
A Realization

Result

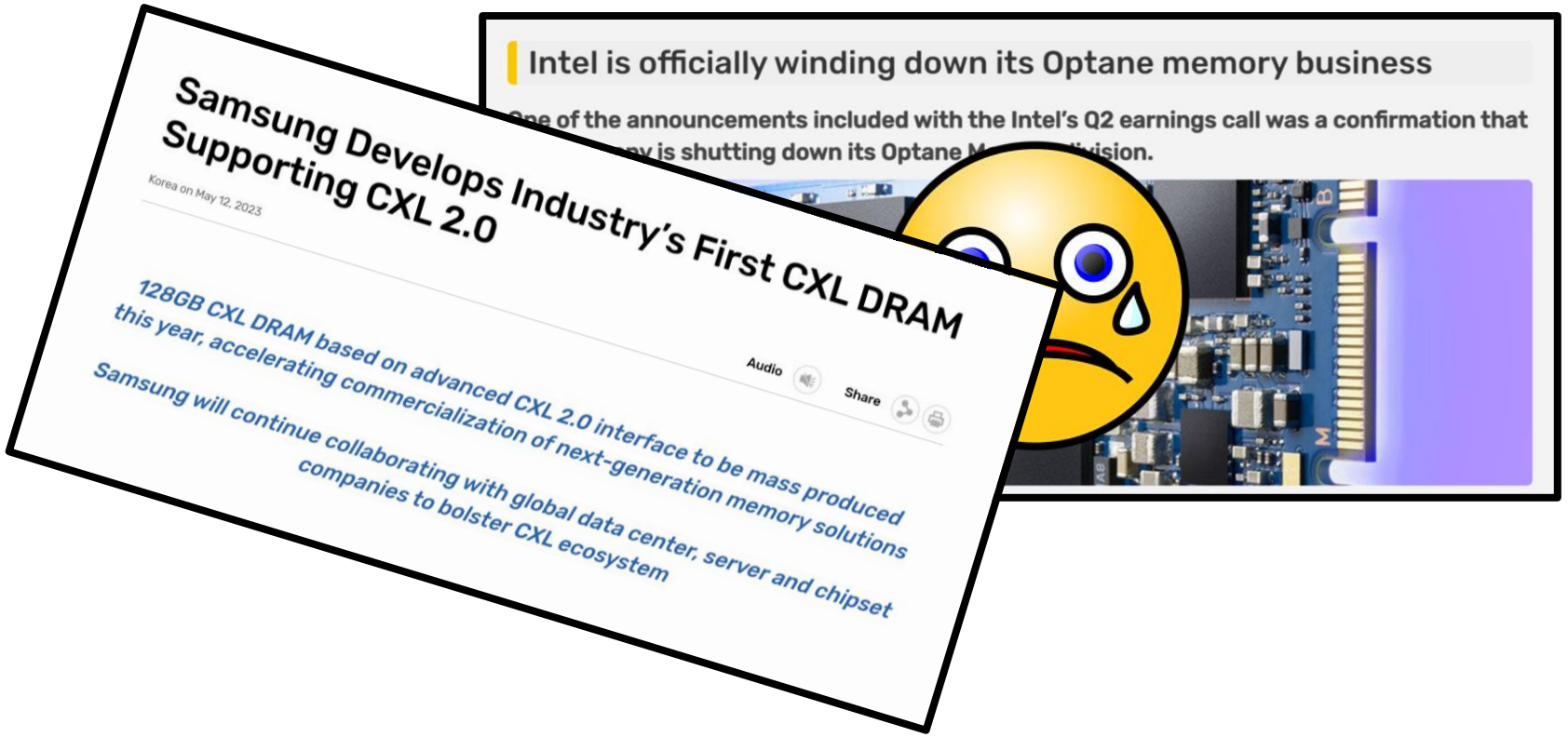


Looking at the Future

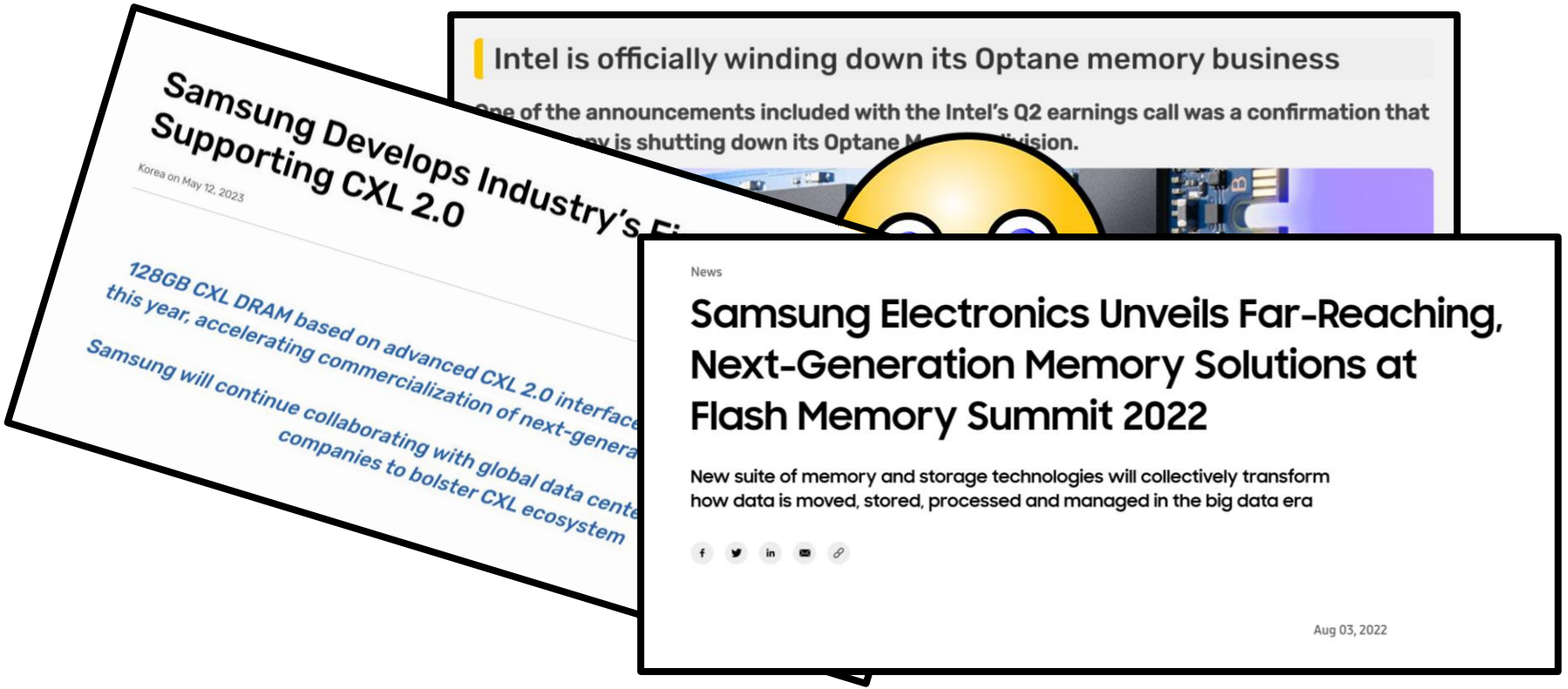
Looking at the Future



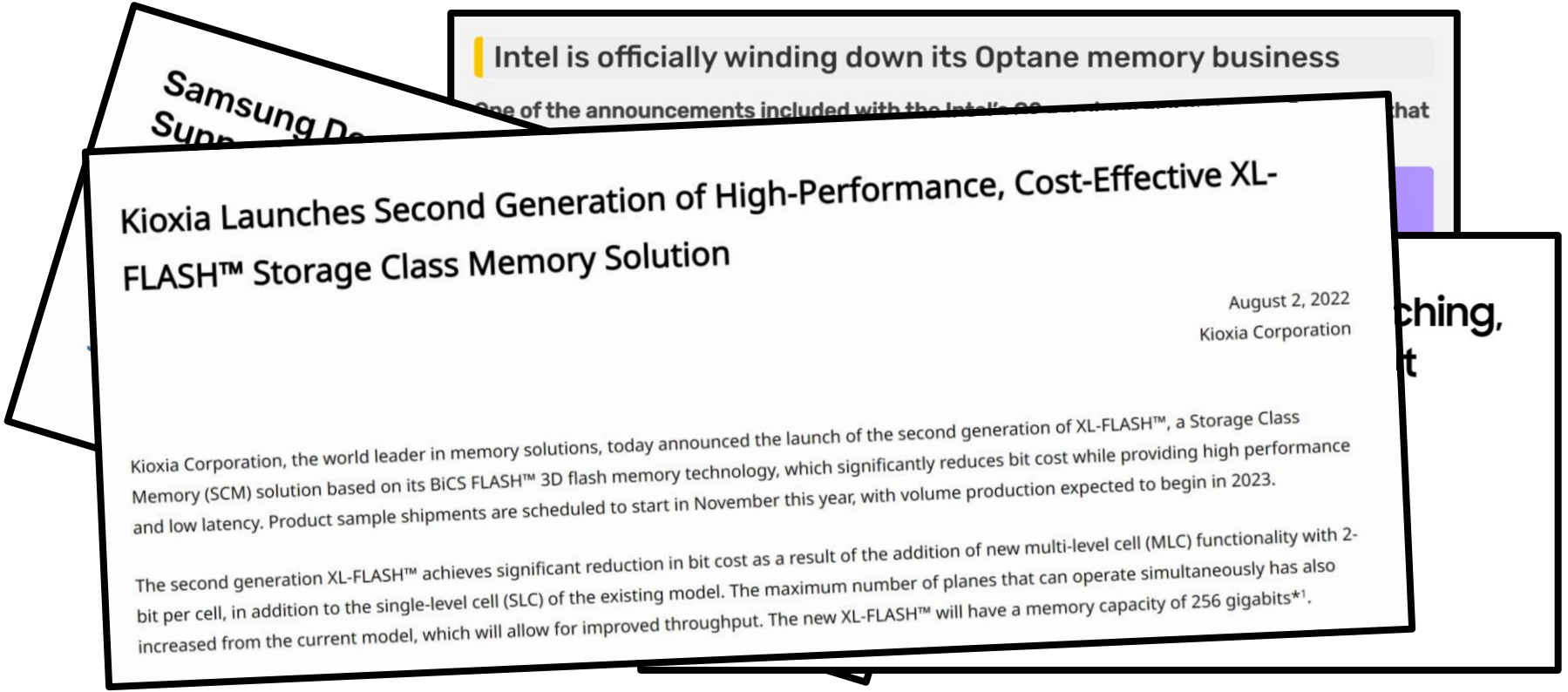
Looking at the Future



Looking at the Future

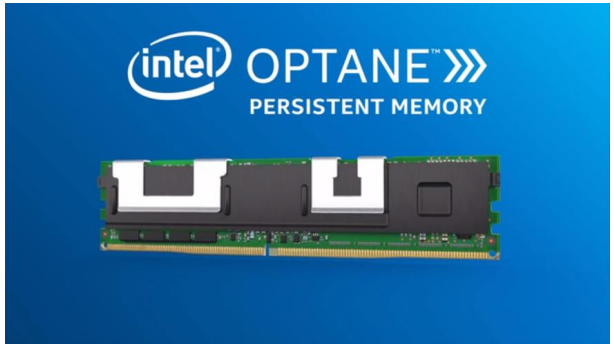


Looking at the Future

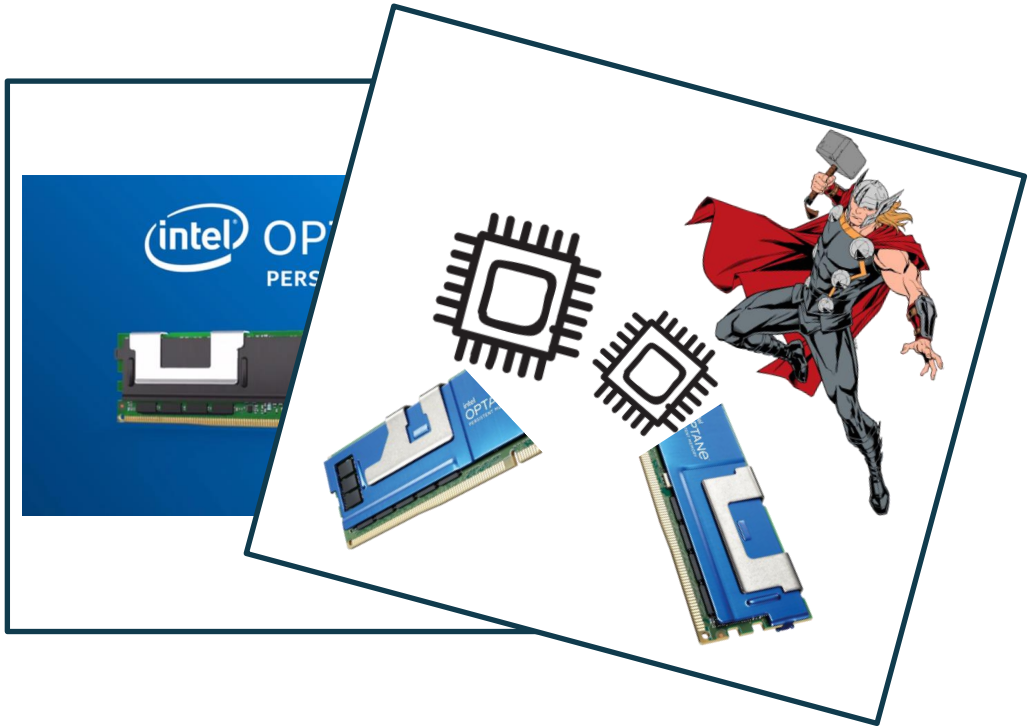


Summary

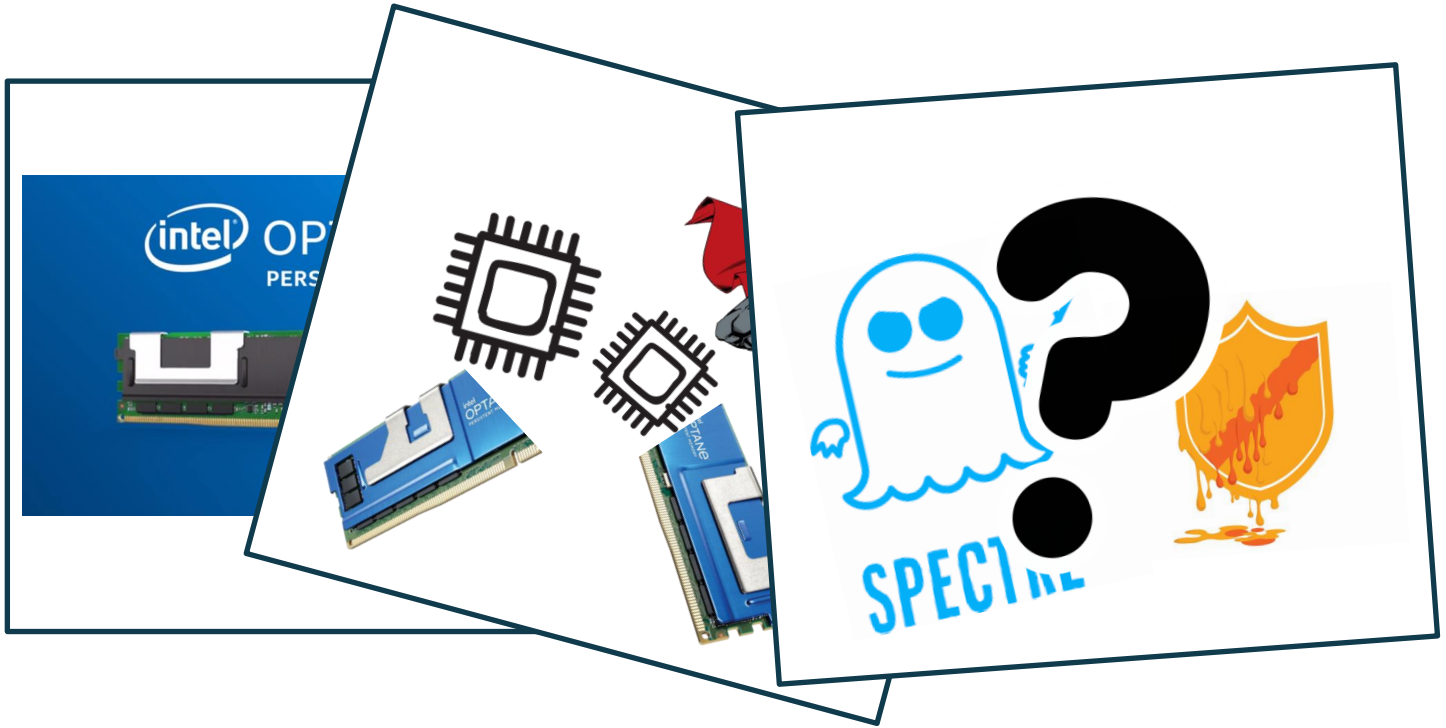
Summary



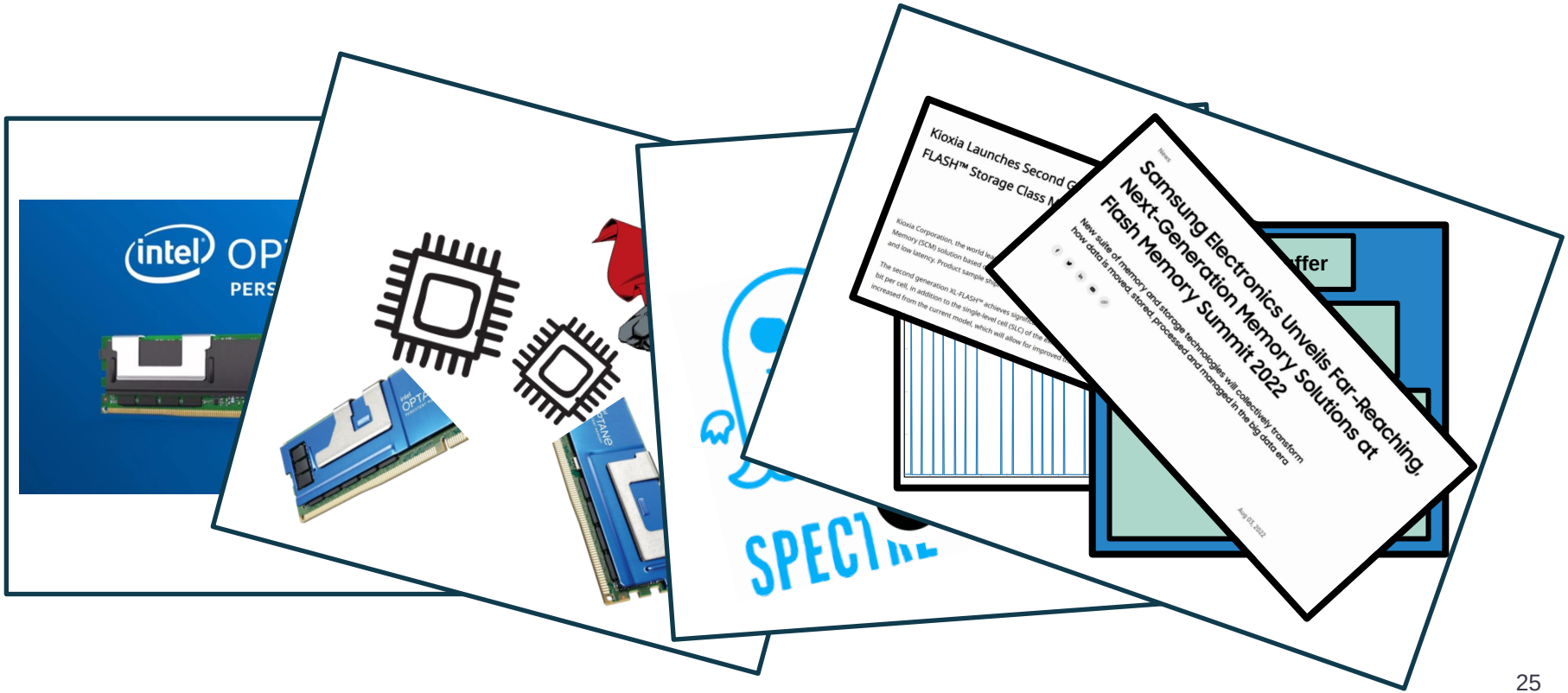
Summary



Summary



Summary


intel
Kioxia Launches Second G
FLASH™ Storage Class M
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
Aug 03, 2022
SPECTRE

Side-Channel Attacks on Optane Persistent Memory

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

Usenix Security Symposium 2023