Spatial Variation-Aware Read Disturbance Defenses:
Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Abdullah Giray Yağlıkçı

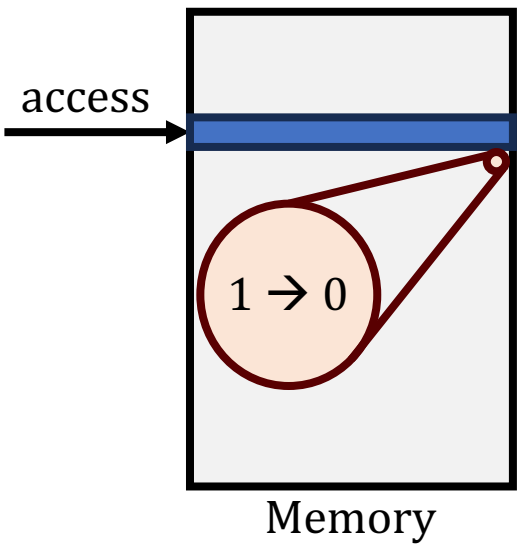
Yahya Can Tuğrul Geraldo F. Oliveira İsmail Emir Yüksel

Ataberk Olgun Haocong Luo Onur Mutlu

SAFARI

ETH zürich

Memory Isolation



Data **Loss** or **Corruption**

Compromise Application **Correctness**

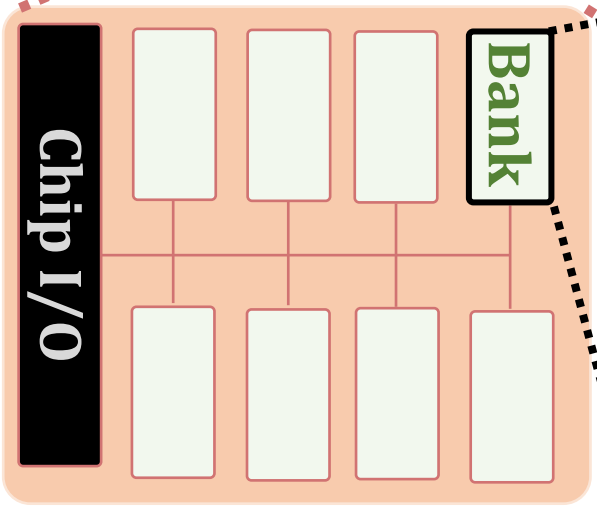
Leak Private Information

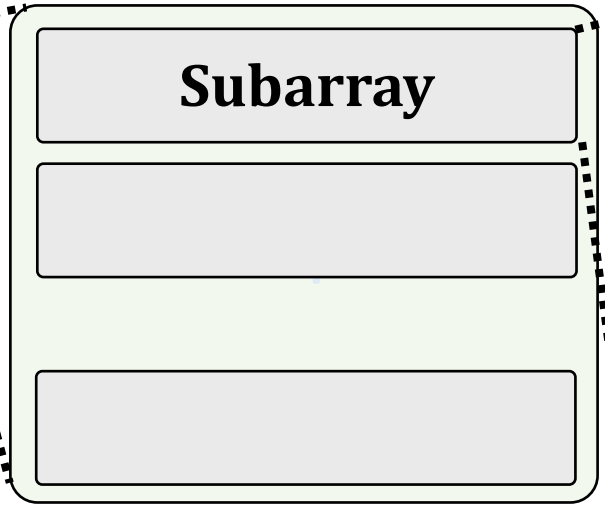
Take Over a Computer

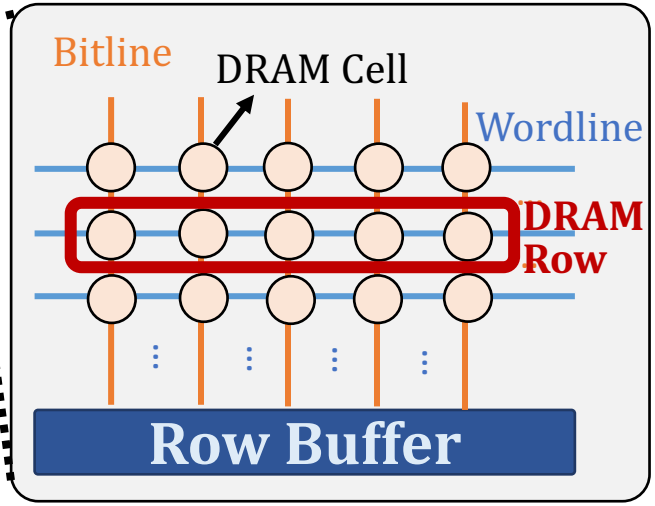
An access to one memory address
should not have **unintended side effects**
on data stored in **other addresses**

Memory isolation is **difficult in modern memory chips**

DRAM Organization

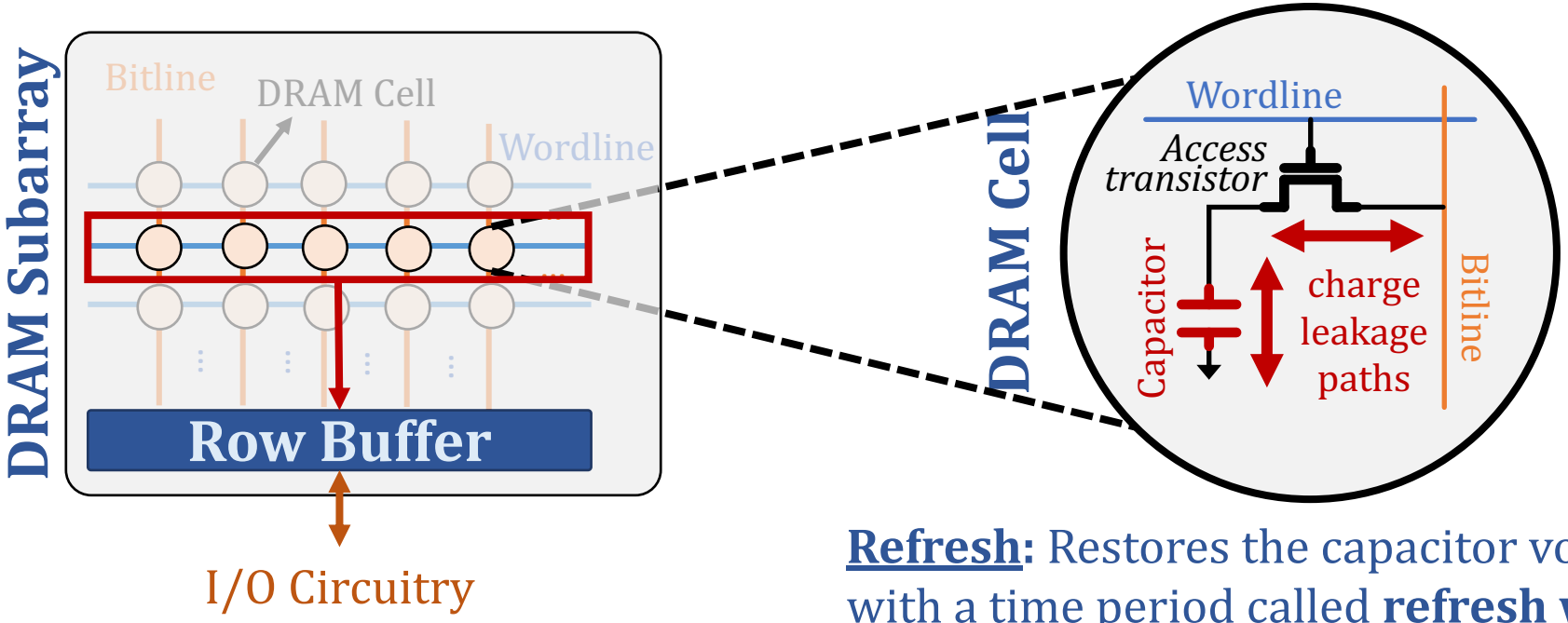






DRAM Chip **DRAM Bank** **DRAM Subarray**

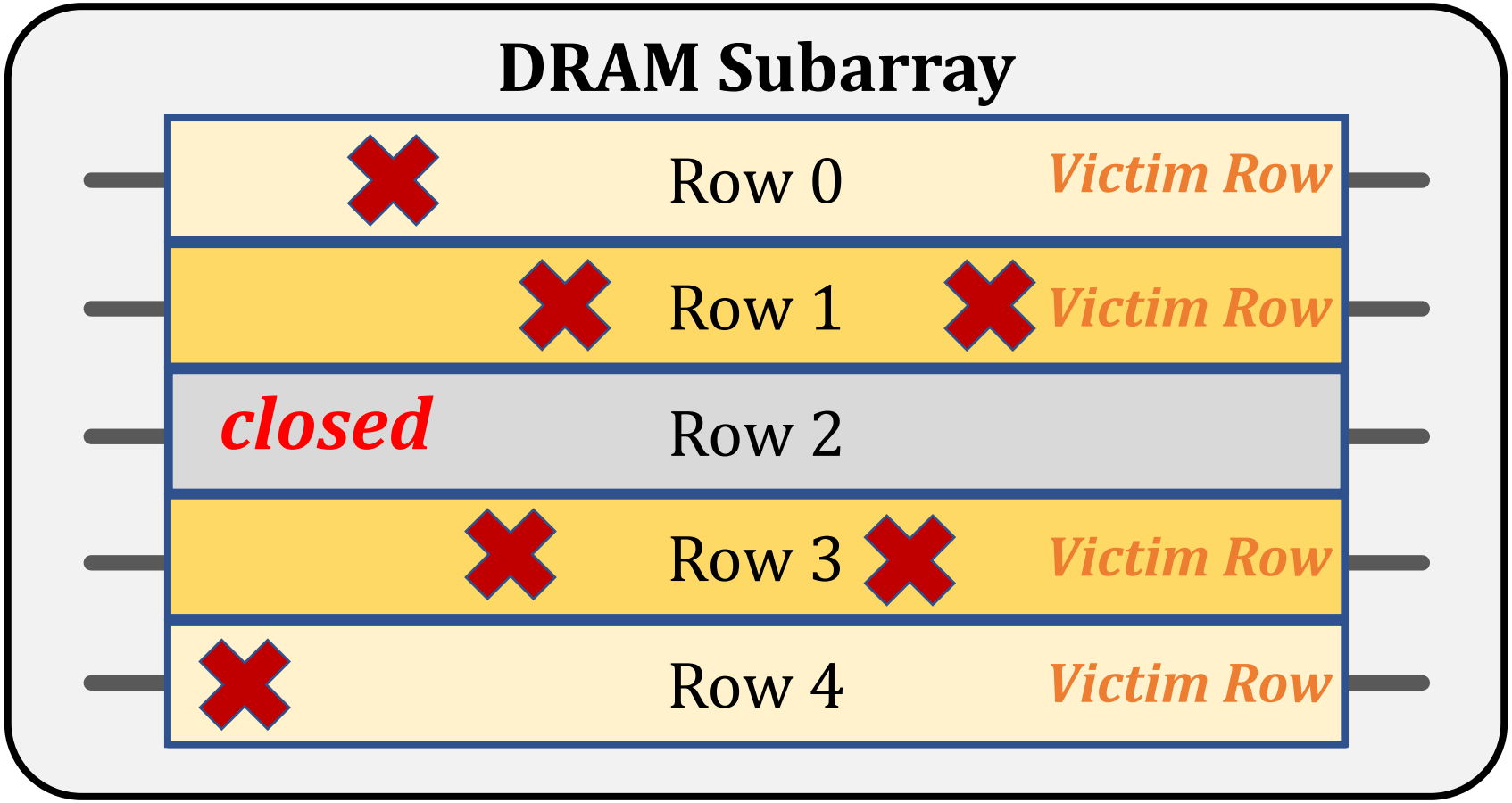
DRAM Operation



Refresh: Restores the capacitor voltage with a time period called **refresh window**

1. **Row Activation:** Fetch the row's content into the row buffer
2. **Column Access:** Read/Write a column in the row buffer
3. **Precharge:** Disconnect the row from the row buffer

The RowHammer Vulnerability



Repeatedly **opening** (activating) and **closing** (precharging) a DRAM row causes **RowHammer bitflips** in nearby cells and breaks **memory isolation**

Executive Summary

Motivation:
- **Read disturbance worsens** with technology node scaling
- Existing solutions have **significant overheads** (e.g., performance, energy, cost)

Problem: No rigorous prior work on
- **Spatial variation of DRAM read disturbance** across DRAM rows
- Variation's **implications on future solutions**

Goal:
- To understand the **spatial variation in read disturbance** across DRAM rows
- To leverage this understanding to **improve the existing solutions**

Experimental study:
- **144 DDR4 DRAM chips** from **three major vendors**
- Characterize **all rows in a bank** and a bank from **each bank group**
- **Takeaway: A large and irregular variation in read disturbance across DRAM rows**

Key Idea: Dynamically tune a solution's aggressiveness (e.g., perform more/less refresh) to the **victim row's vulnerability** to DRAM read disturbance

Svärd: Spatial Variation-Aware Read Disturbance Defenses
- Tunes **the solution's threshold** of performing a preventive action
- Implemented either in **the DRAM chip** or in **the memory controller**

Evaluation:
- **Reduces the solution's performance overhead**
- **Improves system performance** significantly (e.g., >2.5x for BlockHammer and RRS)

Outline

Motivation and Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

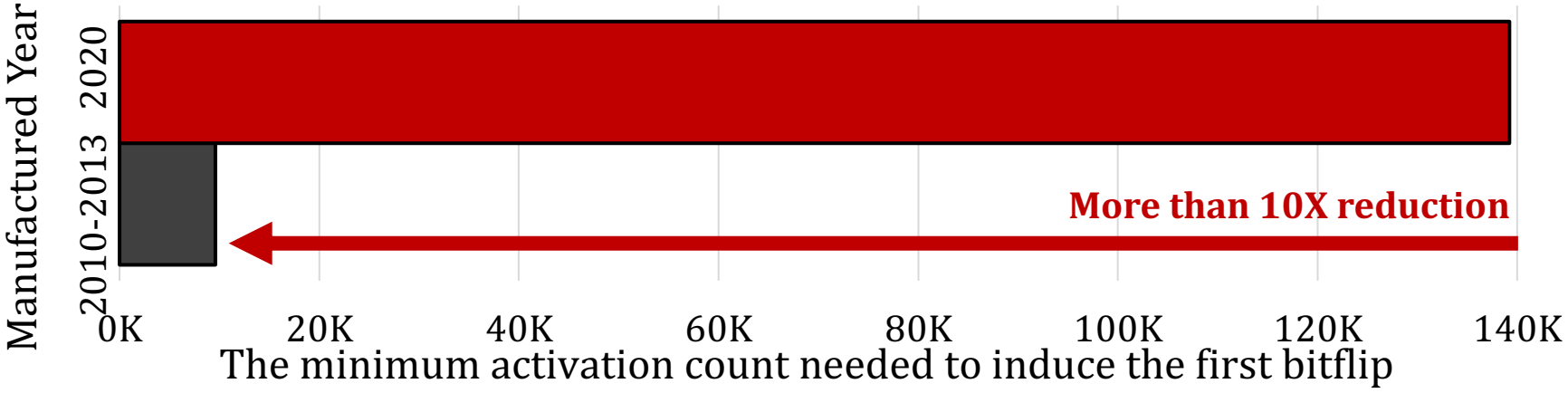
Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

Motivation

DRAM chips are **increasingly more vulnerable** to **read disturbance** with **technology scaling**



Motivation

DRAM read disturbance worsens
as DRAM **chip density increases**

Existing solutions become **more aggressive**

Aggressive preventive behavior makes them
prohibitively expensive

Problem

No prior work rigorously studies

spatial variation of DRAM read disturbance **across all DRAM rows**

&

implications on **future solutions**

Outline

Motivation and Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

Our Goal

To understand the **spatial variation in read disturbance** across DRAM rows

To leverage this understanding **to improve** the existing **read disturbance solutions**

Outline

Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

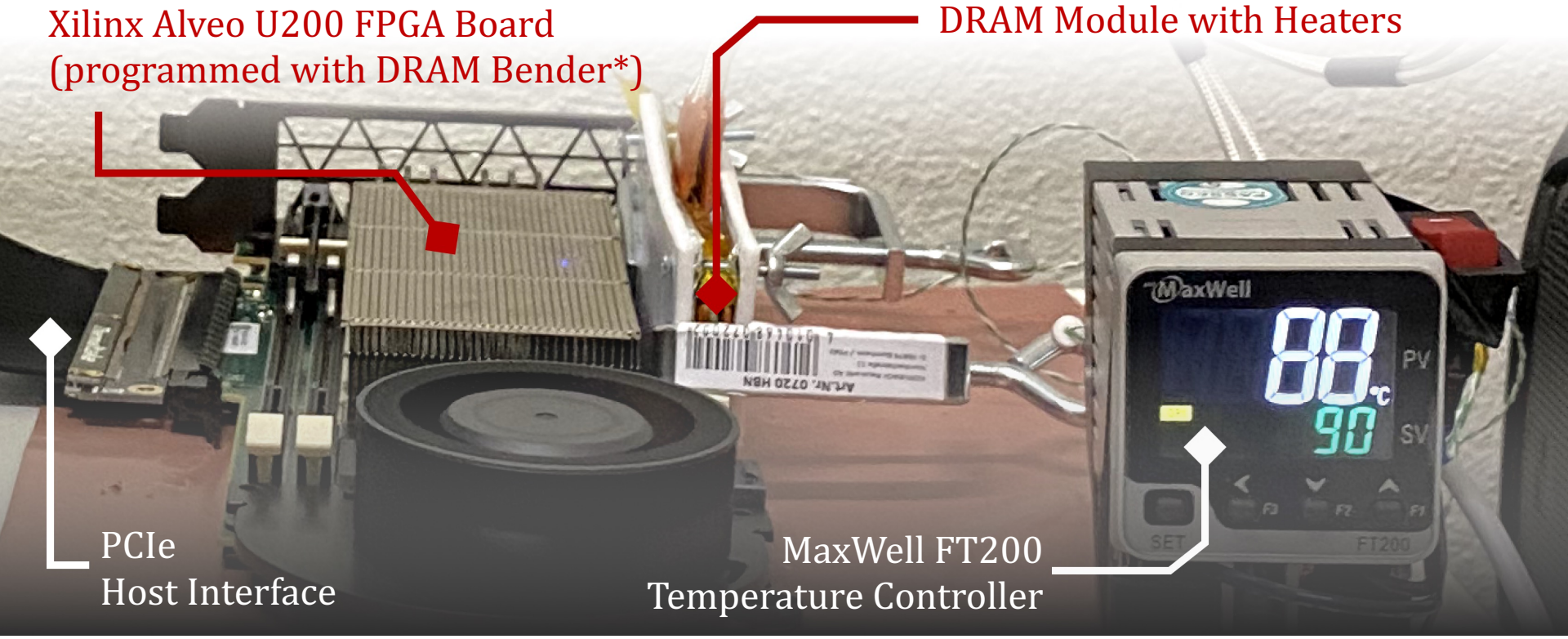
Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

DRAM Testing Infrastructure

DRAM Bender on a Xilinx Virtex UltraScale+ XCU200



Fine-grained control over **DRAM commands**,
timing parameters (±1.5ns), and **temperature (±0.5°C)**

*Olgun et al., "DRAM Bender: An Extensible and Versatile FPGA-Based Infrastructure to Easily Test State-of-the-Art DRAM Chips," TCAD, 2023. [GitHub: https://github.com/CMU-SAFARI/DRAM-Bender]

Tested DRAM Chips

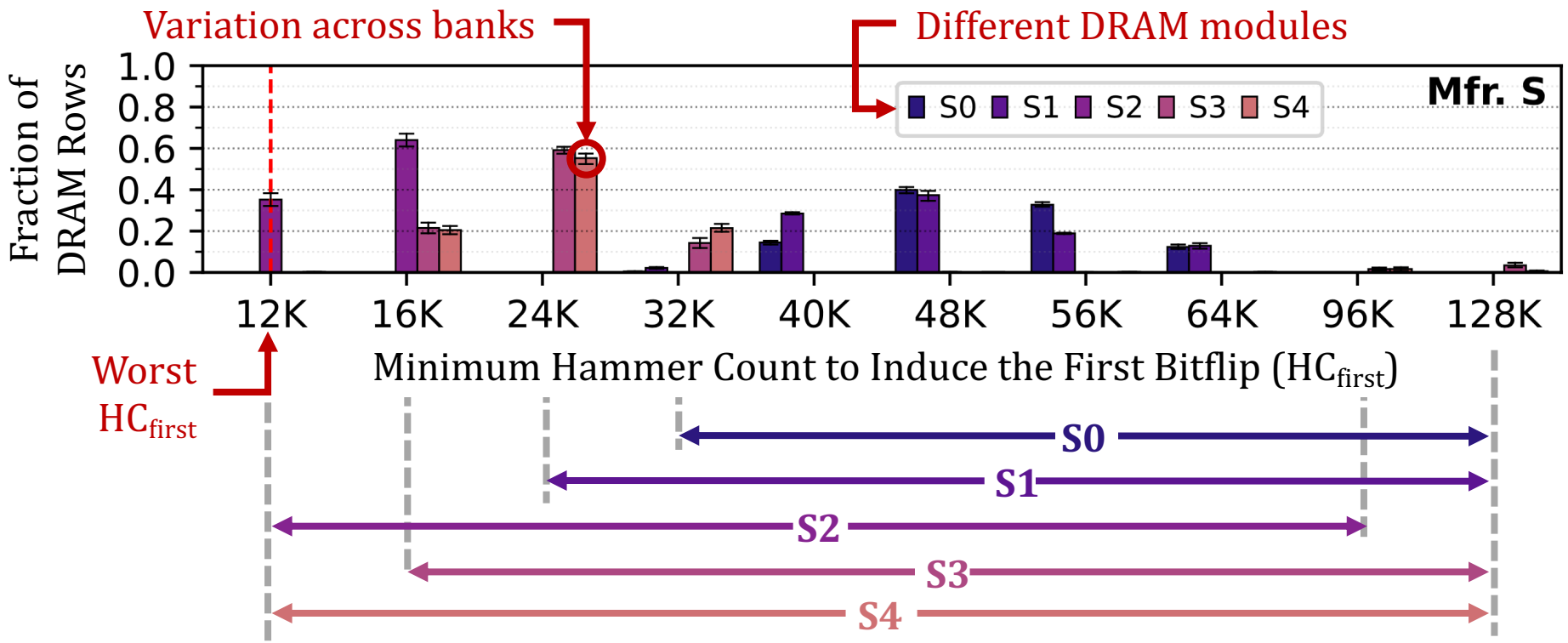
144 DRAM chips from SK Hynix, Micron, and Samsung

Mfr.	DIMM ID	# of Chips	Density Die Rev.	Chip Org.	Date (ww-yy)
Mfr. H (SK Hynix)	H0	8	16Gb – A	x8	51-20
	H1, H2, H3	3 × 8	16Gb – C	x8	48-20
	H4	8	8Gb – D	x8	48-20
Mfr. M (Micron)	M0	4	16Gb – E	x16	46-20
	M1, M3	2 × 16	8Gb – B	x4	N/A
	M2	16	16Gb – E	x4	14-20
	M4	4	16Gb – B	x16	26-21
Mfr. S (Samsung)	S0, S1	2 × 8	8Gb – B	x8	52-20
	S2	8	8Gb – D	x8	10-21
	S3	8	4Gb – F	x8	N/A
	S4	16	8Gb – C	x4	35-21

Key Takeaway from Real Chip Experiments

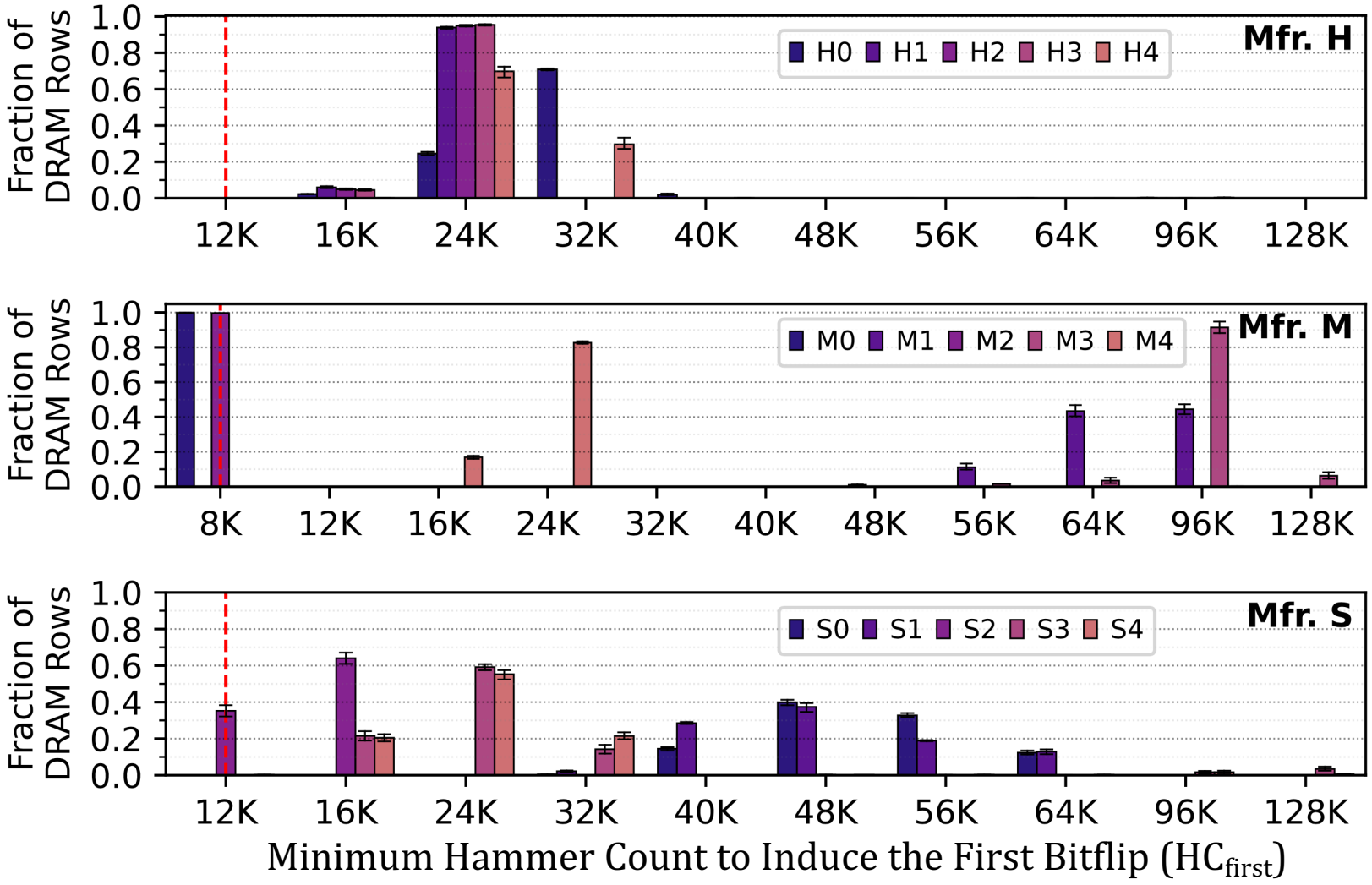
Read disturbance vulnerability varies
significantly and **irregularly**
across DRAM rows

Spatial Variation in the Minimum Hammer Count to Induce the First Bitflip across DRAM Rows

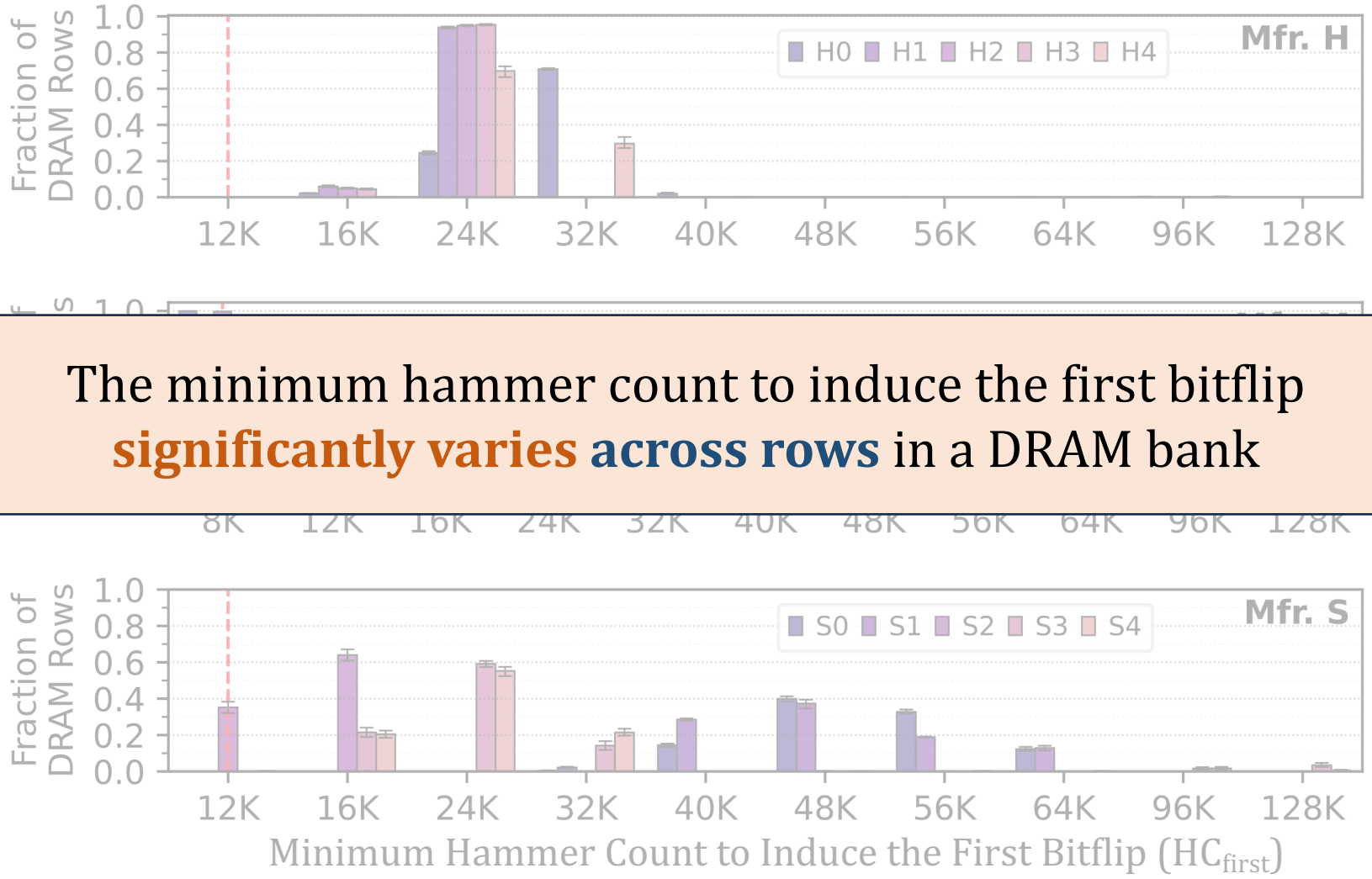


The minimum hammer count to induce the first bitflip **significantly varies across rows** in a DRAM bank

Spatial Variation in the Minimum Hammer Count to Induce the First Bitflip across DRAM Rows



Spatial Variation in the Minimum Hammer Count to Induce the First Bitflip across DRAM Rows



The minimum hammer count to induce the first bitflip **significantly varies** **across rows** in a DRAM bank

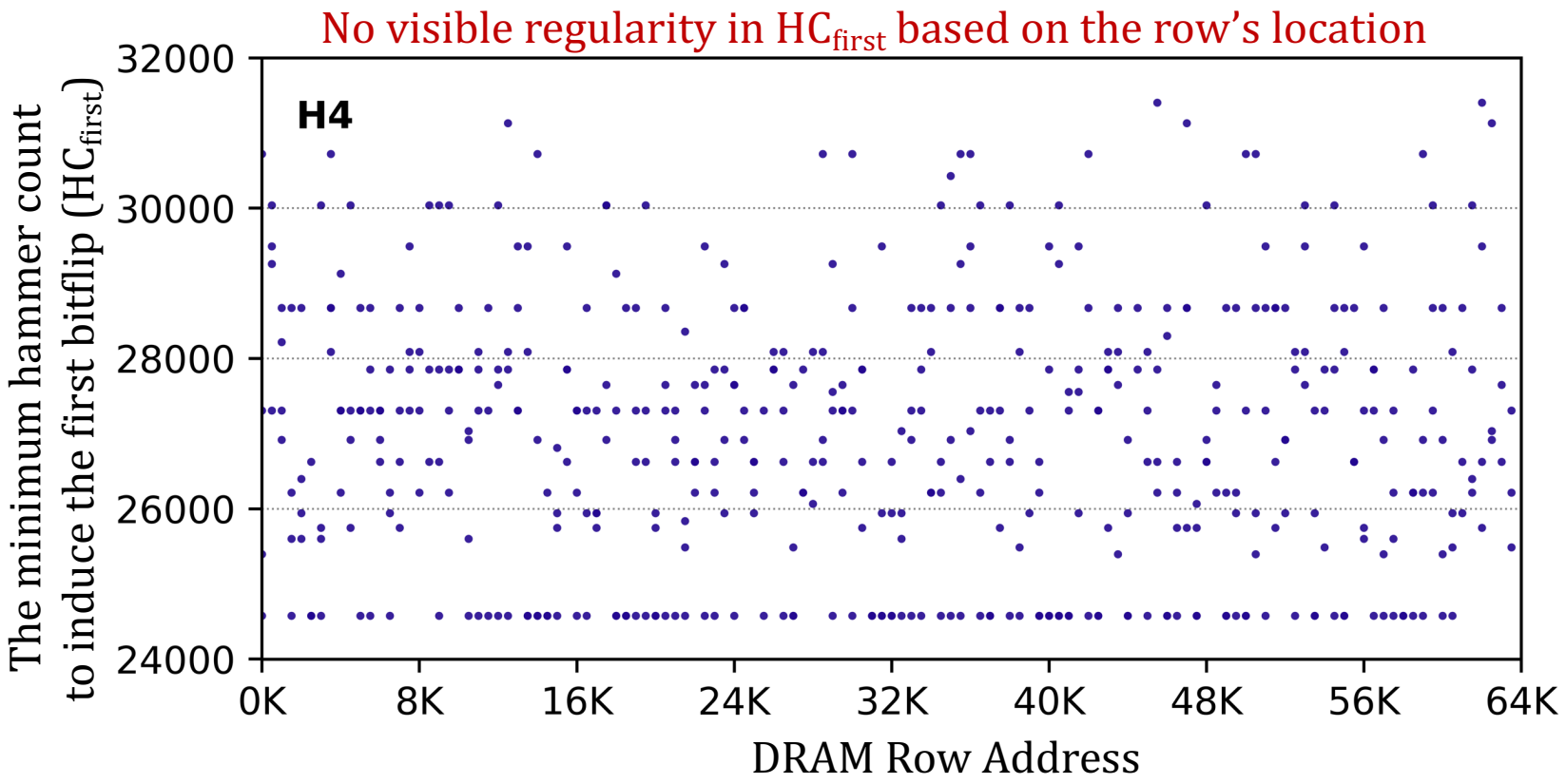
More Detailed Information in the Extended Version

Table 5: Characteristics of the tested DDR4 DRAM modules.

Module Label	Module Vendor	Module Identifier / Chip Identifier	Freq (MT/s)	Mfr. Date ww-yy	Chip Den.	Die Rev.	Chip Org.	Num. of Rows per Bank	HC_{first} Min.	HC_{first} Avg.	HC_{first} Max.
H0	SK Hynix	HMAA4GU6AJR8N-XN [287] H5ANAG8NAJR-XN [288]	3200	51-20	16Gb	A	×8	128K	16K	46.2K	96K
H1		HMAA4GU7CJR8N-XN [289] H5ANAG8NCJR-XN [231]	3200	51-20	16Gb	C	×8	128K	12K	54.0K	128K
H2		HMAA4GU7CJR8N-XN [289] H5ANAG8NCJR-XN [231]	3200	36-21	16Gb	C	×8	128K	12K	55.4K	128K
H3		HMAA4GU7CJR8N-XN [289] H5ANAG8NCJR-XN [231]	3200	36-21	16Gb	C	×8	128K	12K	57.8K	128K
H4		KSM32RD8/16HDR [290] H5AN8G8NDJR-XNC [232]	3200	48-20	8Gb	D	×8	64K	16K	38.1K	96K
M0	Micron	MTA4ATF1G64HZ-3G2E1 [233] MT40A1G16KD-062E [234]	3200	46-20	16Gb	E	×16	128K	8K	24.5K	40K
M1		MTA18ASF2G72PZ-2G3B1QK [235] MT40A2G4WE-083E:B [291]	2400	N/A	8Gb	B	×4	128K	40K	64.5K	96K
M2		MTA36ASF8G72PZ-2G9E1TI [236] MT40A4G4JC-062E:E [292]	2933	14-20	16Gb	E	×4	128K	8K	28.6K	48K
M3		MTA18ASF2G72PZ-2G3B1QK [235] MT40A2G4WE-083E:B [291]	2400	36-21	8Gb	B	×4	128K	56K	90.0K	128K
M4		MTA4ATF1G64HZ-3G2B2 [237] MT40A1G16RC-062E:B [293]	3200	26-21	16Gb	B	×16	128K	12K	42.2K	96K
S0	Samsung	M393A1K43BB1-CTD [294] K4A8G085WB-BCTD [230]	2666	52-20	8Gb	B	×8	64K	32K	57.0K	128K
S1		M393A1K43BB1-CTD [294] K4A8G085WB-BCTD [230]	2666	52-20	8Gb	B	×8	64K	24K	59.8K	128K
S2		M393A1K43BB1-CTD [294] K4A8G085WB-BCTD [230]	2666	10-21	8Gb	B	×8	64K	12K	42.7K	96K
S3		F4-2400C17S-8GNT [295] K4A4G085WF-BCTD [296]	2400	04-21	4Gb	F	×8	32K	16K	59.2K	128K
S4		M393A2K40CB2-CTD [229] K4A8G045WC-BCTD [297]	2666	35-21	8Gb	C	×4	128K	12K	55.4K	128K

https://arxiv.org/pdf/2402.18652.pdf

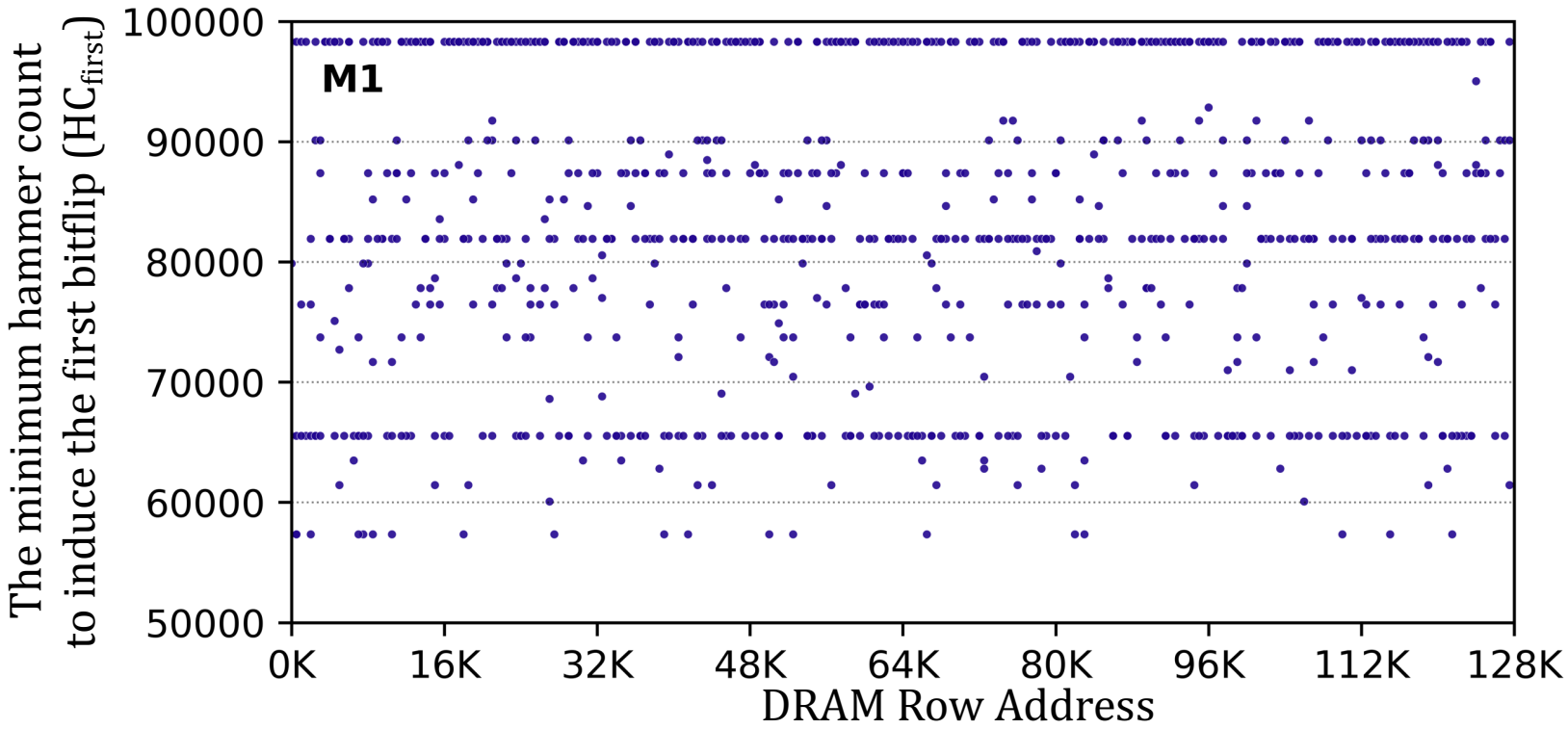
Regularity in Spatial Variation of DRAM Read Disturbance across DRAM Rows



The minimum hammer count to induce the first bitflip **irregularly varies** with respect to row's location in DRAM bank

Regularity in Spatial Variation of DRAM Read Disturbance across DRAM Rows

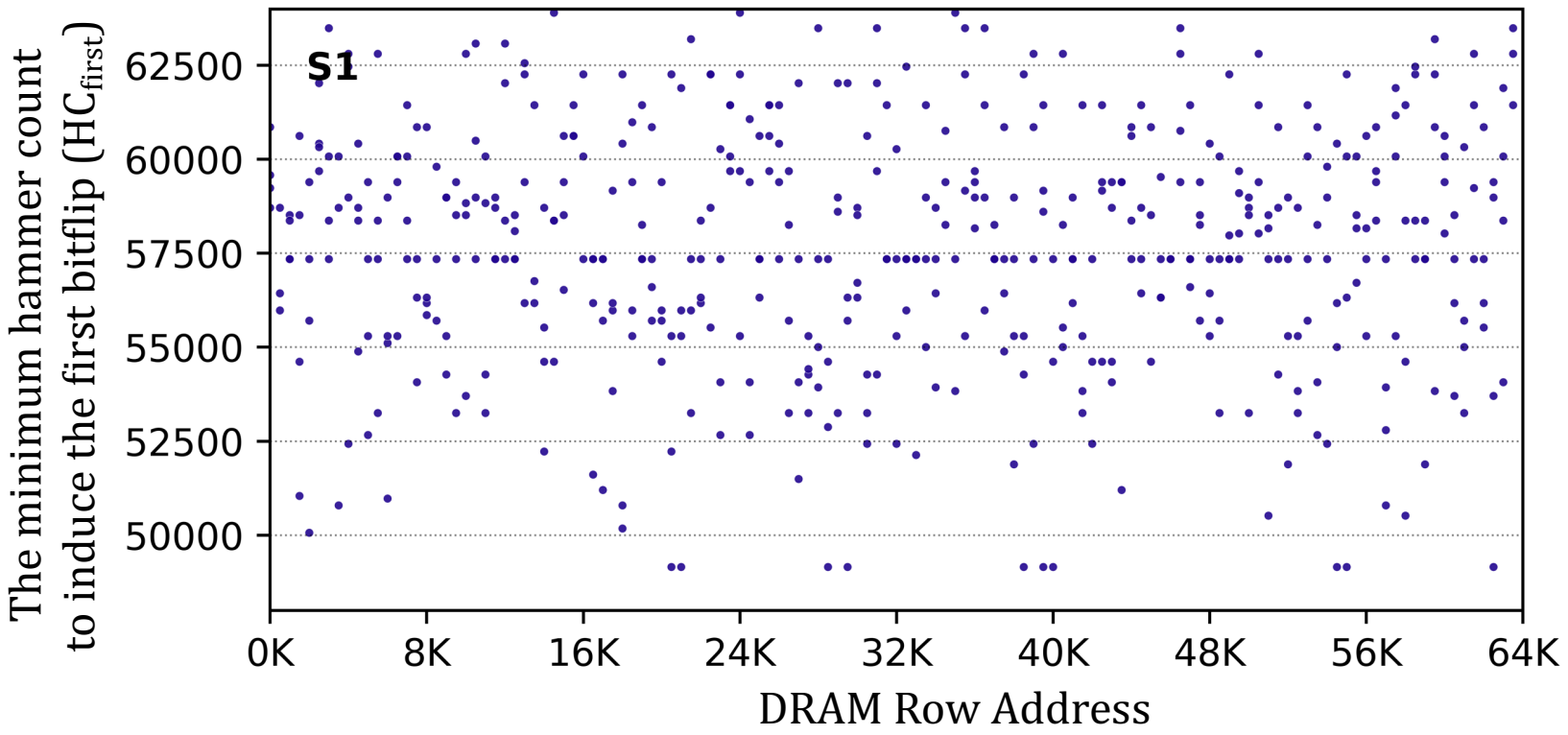
No visible regularity in HC_{first} based on the row's location



The minimum hammer count to induce the first bitflip **irregularly varies** with respect to row's location in DRAM bank

Regularity in Spatial Variation of DRAM Read Disturbance across DRAM Rows

No visible regularity in HC_{first} based on the row's location



The minimum hammer count to induce the first bitflip **irregularly varies** with respect to row's location in DRAM bank

Outline

Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

Predictability of Spatial Variation

Predictability of

- a DRAM row's read disturbance vulnerability
- based on the row's spatial features
  - bank address bits
  - subarray address bits
  - row address bits
  - row's distance to local row buffer

Methodology

- Cluster DRAM rows into 15 bins based on each row's minimum hammer count to induce the first bitflip (HC_{first})
- Predict whether a row is in a cluster or not based on each spatial feature
- Measure the F1 score for each spatial feature

Key Result: Only a few spatial features have F1 scores > 0.7 only for Mfr. S

No good prediction observed between a row's
spatial features & **read disturbance vulnerability**

Key Takeaway from Real Chip Experiments

Read disturbance vulnerability varies
significantly and **irregularly**
across DRAM rows

More in the Paper

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Abdullah Giray Yağlıkçı Geraldo F. Oliveira Yahya Can Tuğrul
İsmail Emir Yüksel Ataberk Olgun Haocong Luo Onur Mutlu
ETH Zürich

Read disturbance in modern DRAM chips is a widespread phenomenon and is reliably used for breaking memory isolation, a fundamental building block for building robust systems. RowHammer and RowPress are two examples of read disturbance in DRAM where repeatedly accessing (hammering) or keeping active (pressing) a memory location induces bitflips in other memory locations. Unfortunately, shrinking technology node size exacerbates read disturbance in DRAM chips over generations. As a result, existing defense mechanisms suffer from significant performance and energy overheads, limited effectiveness, or prohibitively high hardware complexity.

In this paper, we tackle these shortcomings by leveraging the spatial variation in read disturbance across different memory locations in real DRAM chips. To do so, we 1) present the

Many prior works demonstrate attacks on a wide range of systems that exploit read disturbance to escalate privilege, leak private data, and manipulate critical application outputs [1, 3–53, 71–84]. To make matters worse, various experimental studies [1, 1, 25, 33, 36, 37, 61, 70] find that newer DRAM chip generations are more susceptible to read disturbance. For example, chips manufactured in 2018-2020 can experience RowHammer bitflips at an order of magnitude fewer row activations compared to the chips manufactured in 2012-2013 [61]. As read disturbance in DRAM chips worsens, ensuring robust (i.e., reliable, secure, and safe) operation becomes more expensive in terms of performance overhead, energy consumption, and hardware complexity [61, 85, 86]. Therefore, it is critical to understand the read disturbance vulnerabilities

https://arxiv.org/pdf/2402.18652.pdf

Outline

Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

Svärd: Spatial Variation-Aware Read Disturbance Defenses

- **Key Experimental Takeaway:** Read disturbance vulnerability **varies significantly** and **irregularly** across DRAM rows
- **Key Idea:** Leverage the variation in read disturbance vulnerability across DRAM rows
- **Svärd:** Spatial Variation-Aware DRAM Read Disturbance Defenses **Dynamically tunes the aggressiveness** of existing solutions to **the victim row's read disturbance vulnerability**
- Svärd performs **fewer preventive actions (e.g., refresh)** for rows that are **less vulnerable to read disturbance**

Svärd significantly **reduces the performance overhead** of existing solutions

Svärd is Swedish for sword, a weapon with a long blade for cutting or thrusting [Merriam-Webster]

Svärd: Spatial Variation-Aware Read Disturbance Defenses Integration Showcase

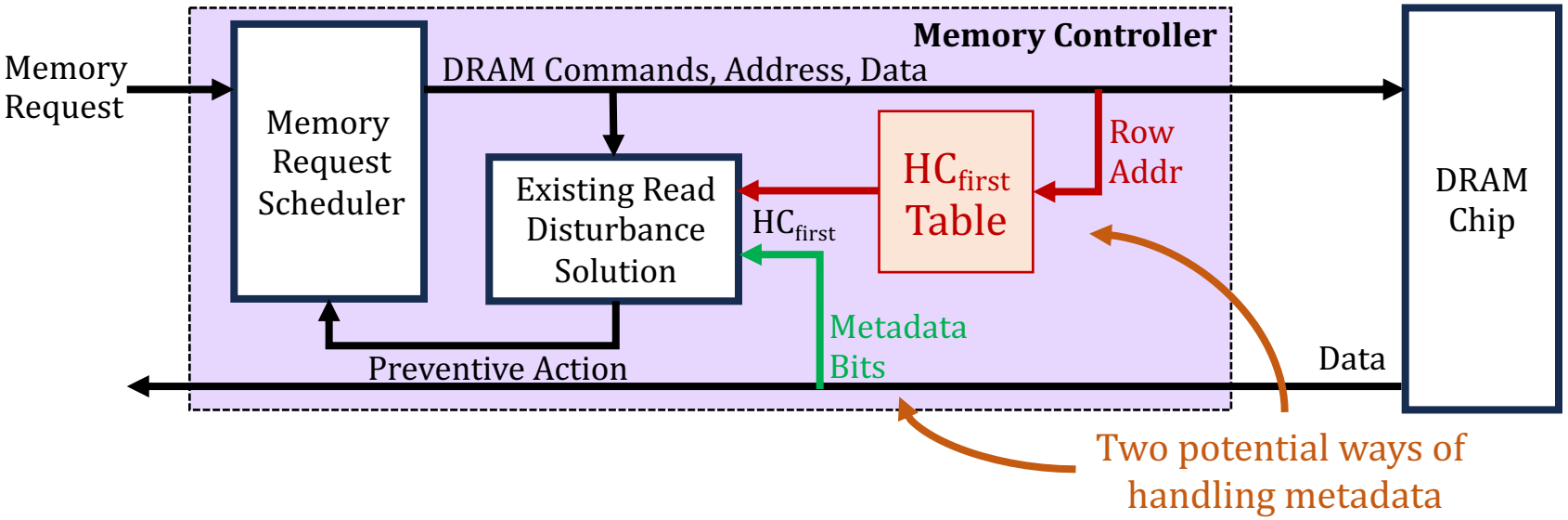
- Integrate Svärd with five solutions
- PARA [Kim+, ISCA'14]
  - Generates **a random number**
  - Compares the random number with **a threshold**
  - **Refreshes the victim row** if the random number exceeds **the threshold**
- BlockHammer [Yaglikci+, HPCA'21]
  - Counts **the number of activations** per DRAM row
  - Compares the activation count **with a threshold**
  - **Throttles accesses** to the aggressor row if the activation count reaches **the threshold**
- Hydra [Qureshi+, ISCA'22]
  - Counts **the number of activations** per DRAM row
  - Compares the activation count **with a threshold**
  - **Refreshes the victim row** when the activation count reaches **the threshold**
- AQUA [Saxena+, MICRO'22] and RRS [Saileshwar+, ASPLOS'22]
  - Counts **the number of activations** per DRAM row
  - Compares the activation count **with a threshold**
  - **Relocates the aggressor row** when the activation count reaches **the threshold**

Svärd tunes **the threshold** based on the **victim row's vulnerability**

Svärd is Swedish for sword, a weapon with a long blade for cutting or thrusting [Merriam-Webster]

Svärd: Spatial Variation-Aware Read Disturbance Defenses
Implementation Showcase 1

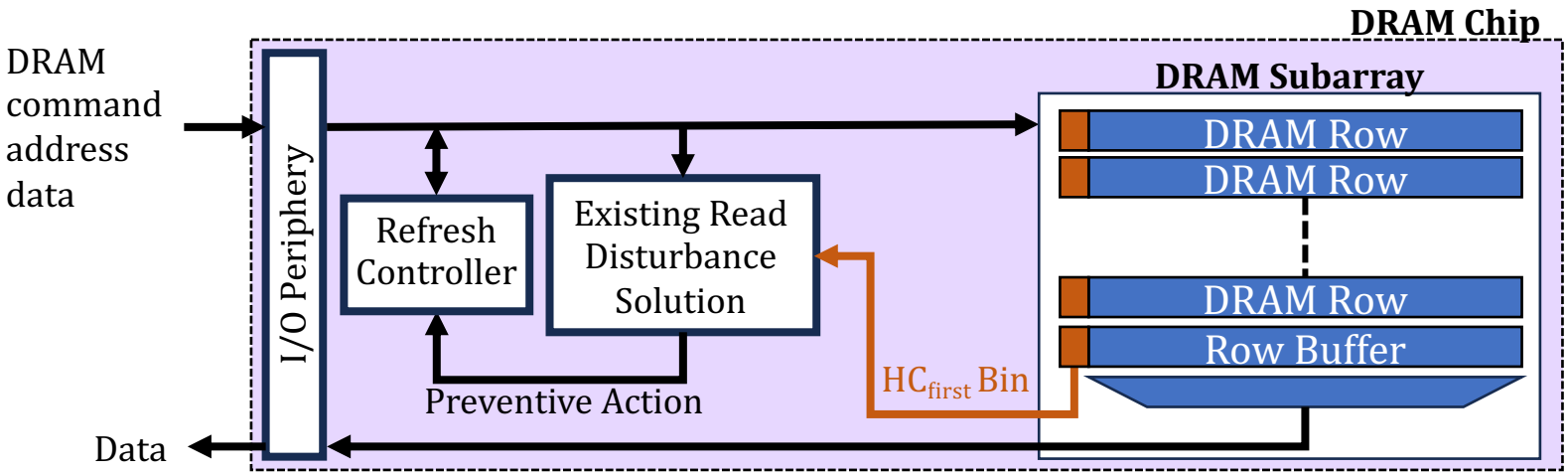
- Classifies DRAM rows into **several vulnerability-level bins**
  - Maintains **a few (e.g., four) bits** per DRAM row
- Implemented in either the memory controller or the DRAM chip
- The memory controller-based implementation:



Svärd is Swedish for sword, a weapon with a long blade for cutting or thrusting [Merriam-Webster]

Svärd: Spatial Variation-Aware Read Disturbance Defenses
Implementation Showcase 2

- Classifies DRAM rows into **several vulnerability-level bins**
  - Maintains **a few (e.g., four) bits** per DRAM row
- Implemented in either the memory controller or the DRAM chip
- The DRAM chip-based implementation:
  - Additional few (e.g., four) bits per DRAM row (e.g., 8Kb)



Svärd is Swedish for sword, a weapon with a long blade for cutting or thrusting [Merriam-Webster]

Outline

Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

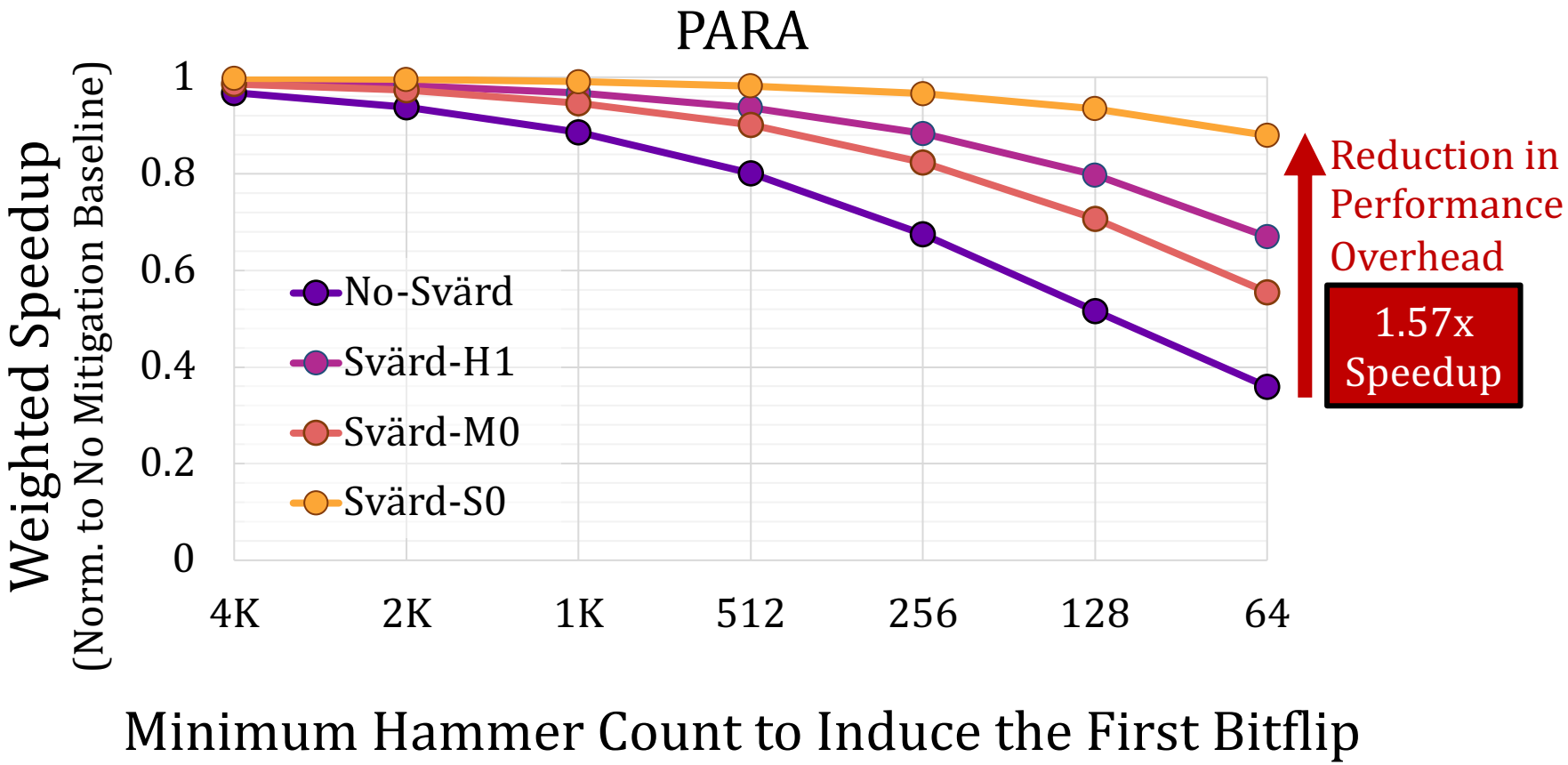
Performance Evaluation

- Cycle-level simulations using **Ramulator 2.0** [Luo+, CAL 2023]
- **System Configuration**:

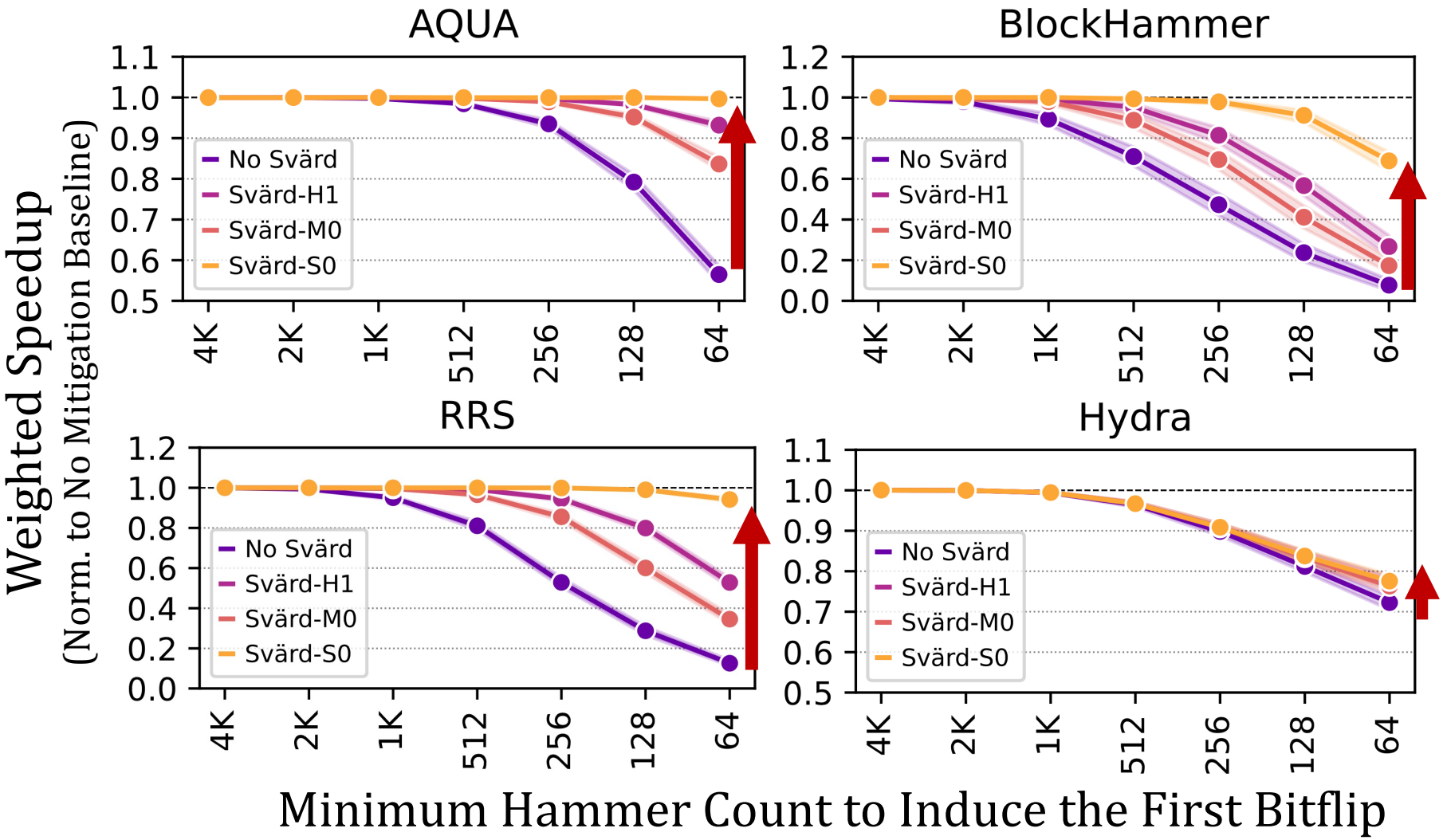
Processor	3.2 GHz, 8 core, 4-wide issue, 128-entry instr. window
Last-Level Cache	64-byte cache line, 8-way set-associative, 8 MB
Memory Scheduler	FR-FCFS
Address Mapping	Minimalistic Open Pages
Main Memory	DDR4, 4 bank group, 4 banks per bank group (16 banks per rank)

- **Workloads**: **120** different **8-core** multiprogrammed workloads from **SPEC CPU2006, SPEC CPU2017, TPC, MediaBench,** and **YCSB** benchmark suites
- Paired with **AQUA, BlockHammer, PARA, Hydra,** and **RRS**
- **HC_{first}**: {4K, 2K, 1K, 512, 256, 128, 64} hammers
  The **minimum hammer count** needed to induce **the first bitflip**

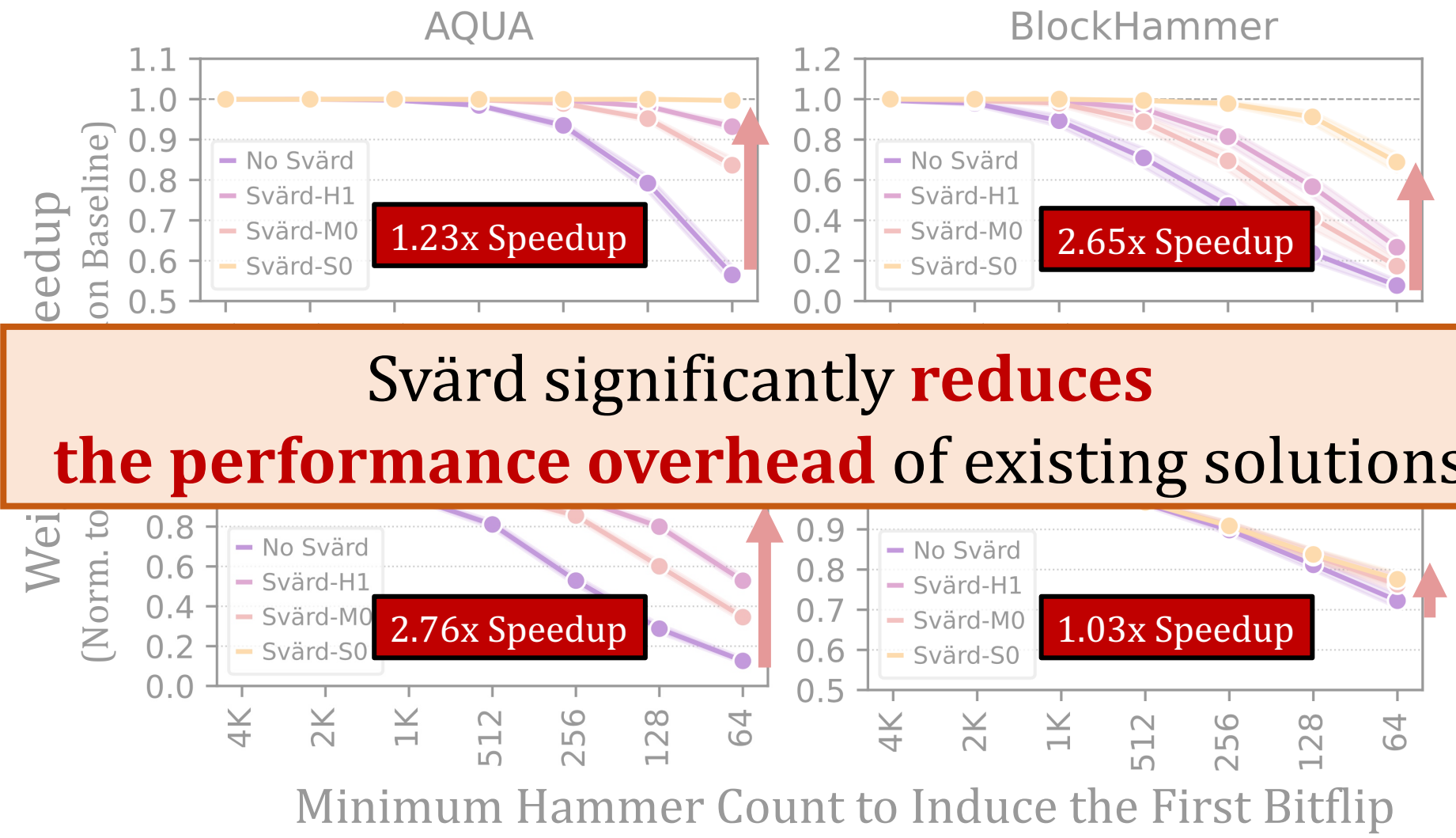
Implications on Future Solutions



Implications on Future Solutions



Implications on Future Solutions



Svärd significantly **reduces**
the performance overhead of existing solutions

More in the Paper

- Spatial variation in read disturbance **bit error rate** across rows
- Spatial variation of **RowPress [Luo+ ISCA23]** across DRAM rows
- **Algorithms and details** of our experiments
- Reverse-engineering of **subarray boundaries**
- Hardware in Complexity Analysis
  - Chip area cost
    - MC-based: 0.027% of a processor die per DRAM bank
    - DRAM-based: 0.006% increase the DRAM array (4 bits per row per chip)
  - No additional latency overhead
- A preliminary analysis of **the effect of aging** on DRAM read disturbance vulnerability

More in the Paper

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Abdullah Giray Yağlıkçı Geraldo F. Oliveira Yahya Can Tuğrul
İsmail Emir Yüksel Ataberk Olgun Haocong Luo Onur Mutlu
ETH Zürich

Read disturbance in modern DRAM chips is a widespread phenomenon and is reliably used for breaking memory isolation, a fundamental building block for building robust systems. RowHammer and RowPress are two examples of read disturbance in DRAM where repeatedly accessing (hammering) or keeping active (pressing) a memory location induces bitflips in other memory locations. Unfortunately, shrinking technology node size exacerbates read disturbance in DRAM chips over generations. As a result, existing defense mechanisms suffer from significant performance and energy overheads, limited effectiveness, or prohibitively high hardware complexity.

In this paper, we tackle these shortcomings by leveraging the spatial variation in read disturbance across different memory locations in real DRAM chips. To do so, we 1) present the

Many prior works demonstrate attacks on a wide range of systems that exploit read disturbance to escalate privilege, leak private data, and manipulate critical application outputs [1, 3–53, 71–84]. To make matters worse, various experimental studies [1, 1, 25, 33, 36, 37, 61, 70] find that newer DRAM chip generations are more susceptible to read disturbance. For example, chips manufactured in 2018-2020 can experience RowHammer bitflips at an order of magnitude fewer row activations compared to the chips manufactured in 2012-2013 [61]. As read disturbance in DRAM chips worsens, ensuring robust (i.e., reliable, secure, and safe) operation becomes more expensive in terms of performance overhead, energy consumption, and hardware complexity [61, 85, 86]. Therefore, it is critical to understand the read disturbance vulnerabilities

https://arxiv.org/pdf/2402.18652.pdf

Outline

Problem

Our Goal

Experimental Characterization of Real DRAM Chips

Spatial Variation Analysis

Svärd: Spatial Variation-Aware Read Disturbance Defenses

Performance Evaluation

Conclusion

Conclusion

- **The first rigorous experimental study** on the spatial variation of DRAM read disturbance across DRAM rows
  - **144 DDR4 DRAM chips** from **three major vendors**
  - Characterize **all rows in a bank** and a bank from **each bank group**

Read disturbance vulnerability varies **significantly** and **irregularly** across DRAM rows

Key Idea: Dynamically tune a solution's aggressiveness (e.g., perform more/less refresh) to the **victim row's vulnerability** to DRAM read disturbance

Svärd: Spatial Variation-Aware Read Disturbance Defenses

- Tunes **the solution's threshold** of performing a preventive action
- Implemented either in **the DRAM chip** or in **the memory controller**

Svärd significantly **reduces** **the performance overhead** of existing solutions

Spatial Variation-Aware Read Disturbance Defenses:
Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Full Paper

Abdullah Giray Yağlıkçı

Yahya Can Tuğrul Geraldo F. Oliveira İsmail Emir Yüksel

Ataberk Olgun Haocong Luo Onur Mutlu

SAFARI

ETH zürich

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Backup Slides

Abdullah Giray Yağlıkçı

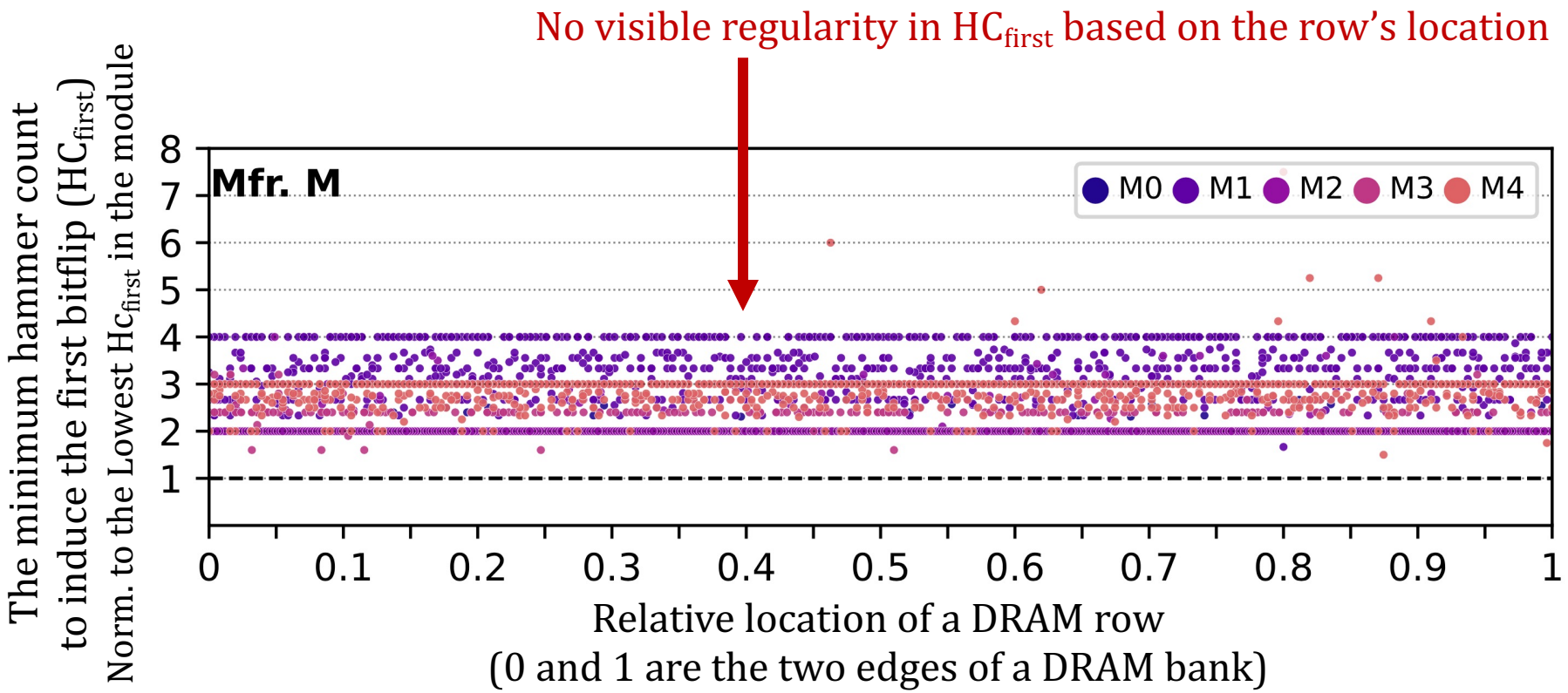
Yahya Can Tuğrul Geraldo F. Oliveira İsmail Emir Yüksel

Ataberk Olgun Haocong Luo Onur Mutlu

SAFARI

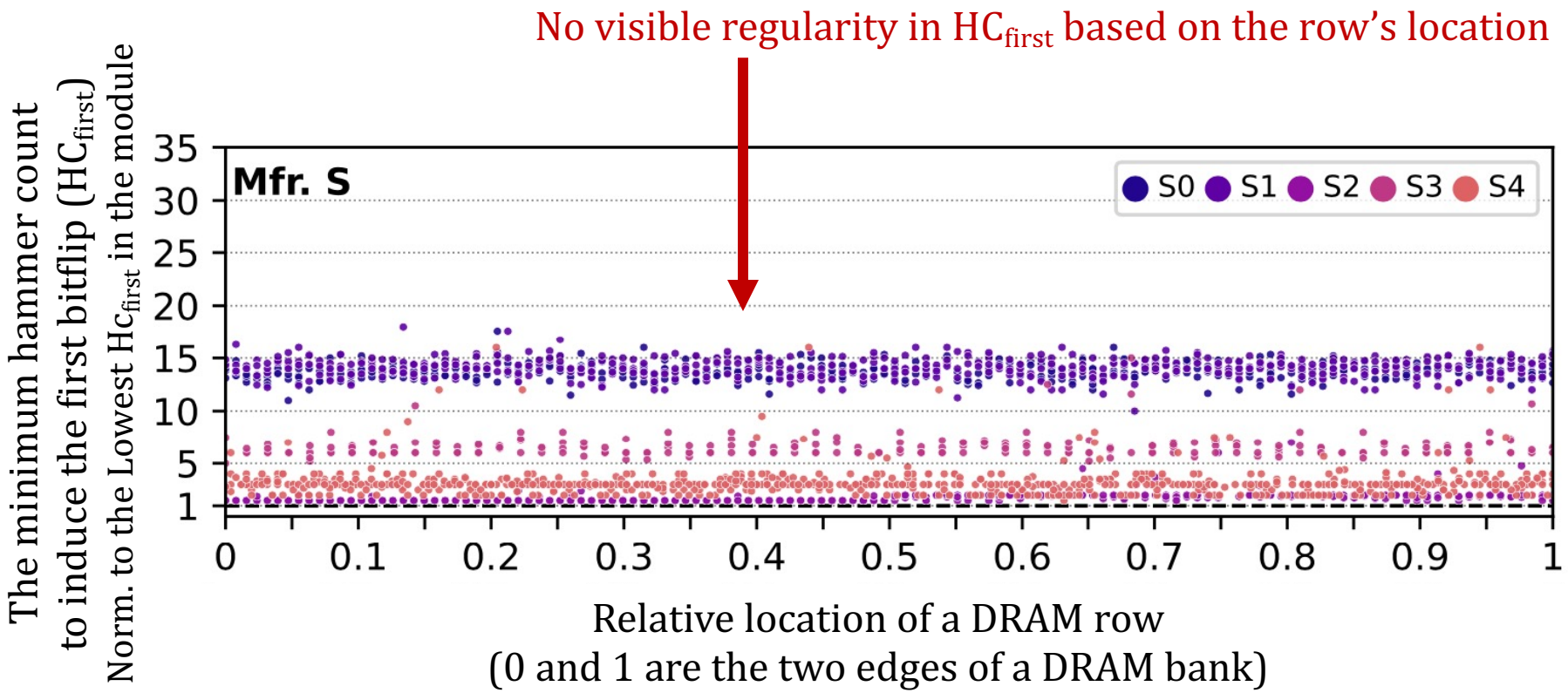
ETH zürich

The Minimum Hammer Count to Induce the First Bitflip across DRAM Rows



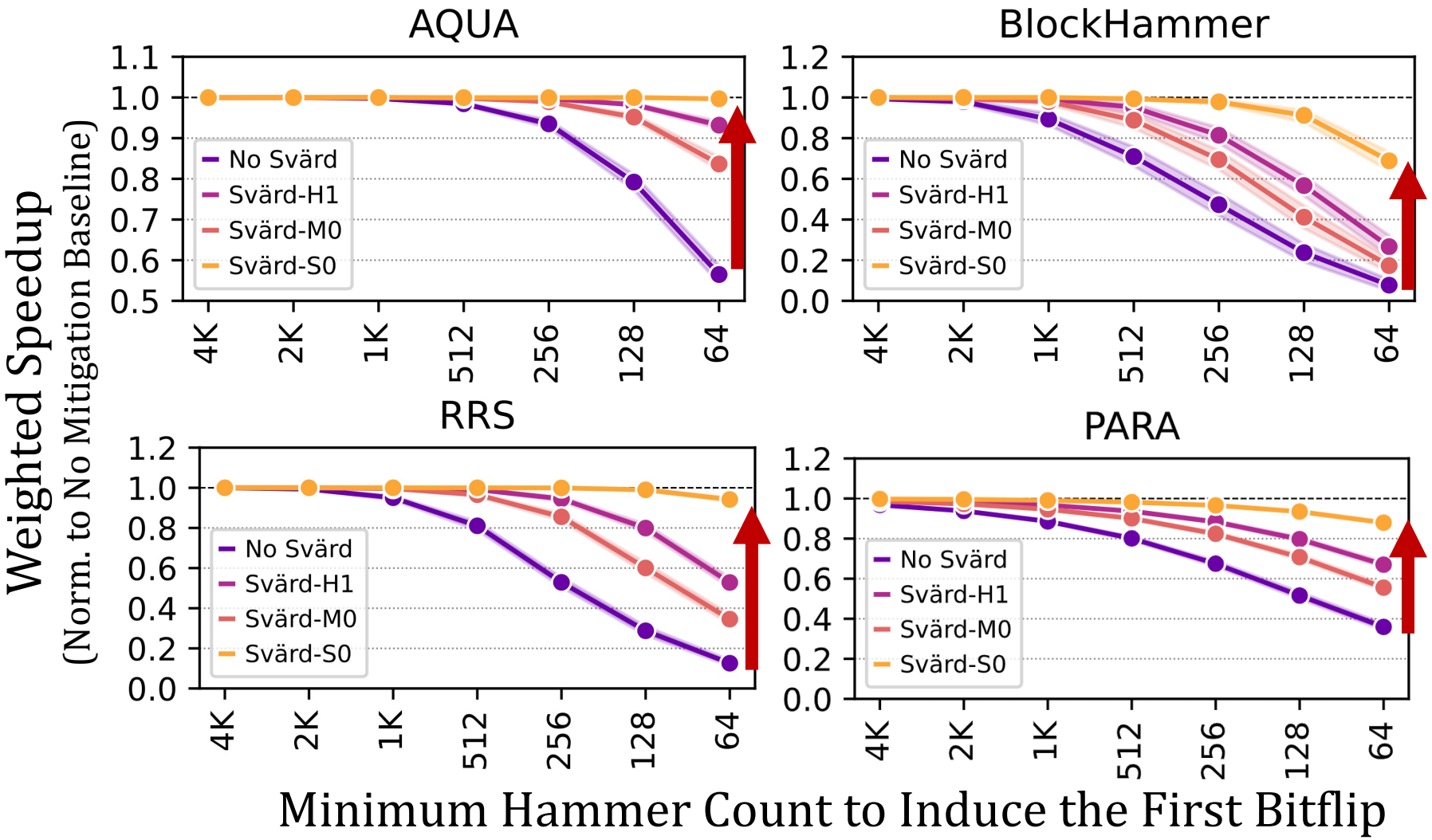
The minimum hammer count to induce the first bitflip **irregularly varies** with respect to row's location in DRAM bank

The Minimum Hammer Count to Induce the First Bitflip across DRAM Rows

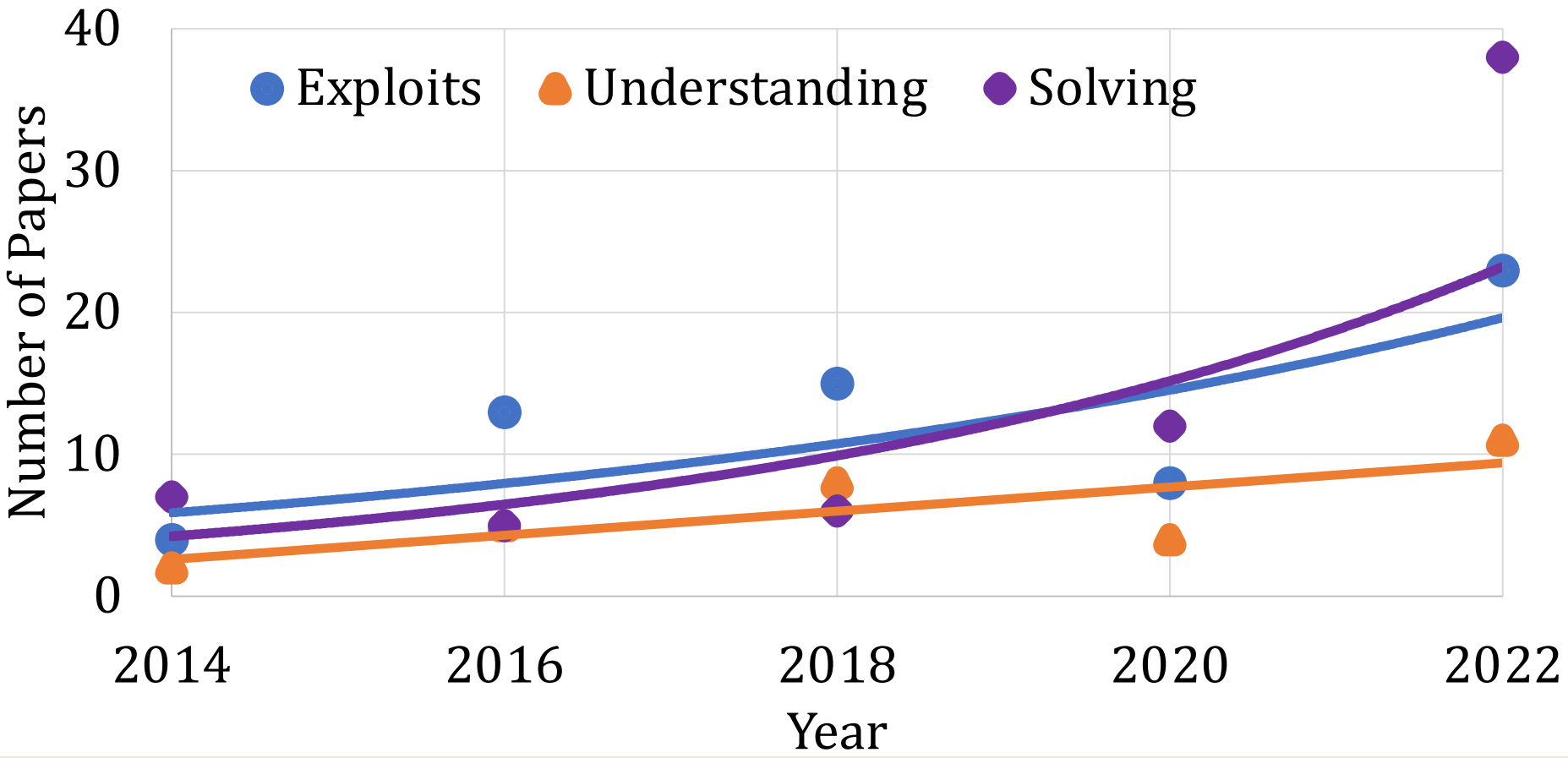


The minimum hammer count to induce the first bitflip **irregularly varies** with respect to row's location in DRAM bank

Implications on Future Solutions



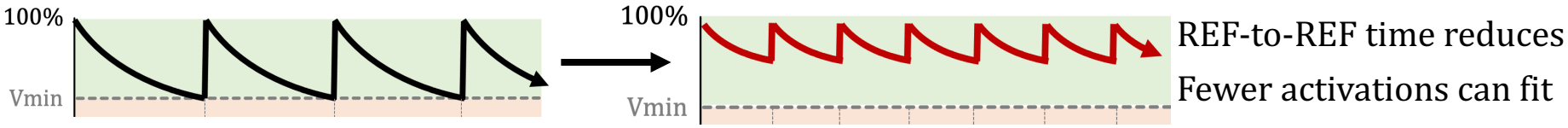
Read Disturbance in DRAM



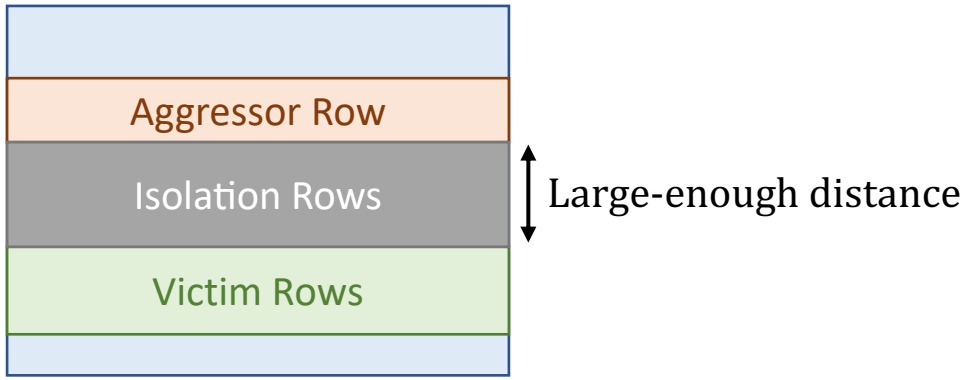
Increasing focus on **exploiting**, **understanding**, and **solving** DRAM read disturbance

RowHammer Mitigation Approaches

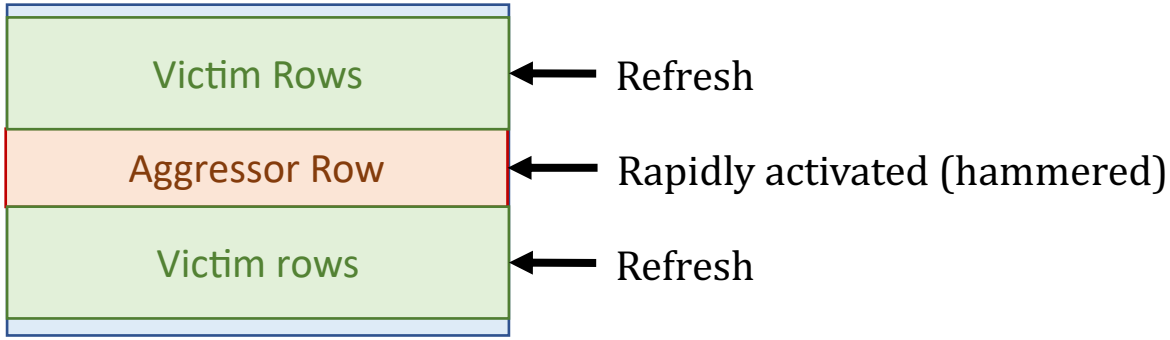
- Increased refresh rate



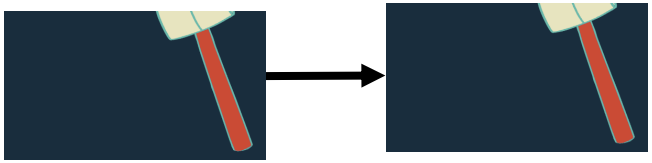
- Physical isolation



- Reactive refresh



- Proactive throttling



More in the Paper

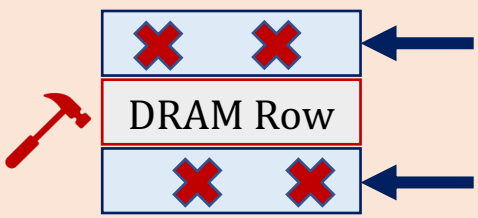
- Security Proof
  - Mathematically represent **all possible** access patterns
  - We show that **no row can be activated high-enough times** to induce bit-flips when BlockHammer is configured correctly
- Addressing **Many-Sided Attacks**
- Evaluation of **14 mechanisms** representing **four mitigation approaches**
  - Comprehensive Protection
  - Compatibility with Commodity DRAM Chips
  - Scalability with RowHammer Vulnerability
  - Deterministic Protection

Approach	Mechanism	Comprehensive Protection	Compatible w/ Commodity DRAM Chips	Scaling with RowHammer Vulnerability	Deterministic Protection
Increased Refresh Rate [2, 73]		✓	✓	✗	✓
Physical Isolation	CATT [14]	✗	✗	✗	✓
	GuardION [148]	✗	✗	✗	✓
	ZebRAM [78]	✗	✗	✗	✓
Reactive Refresh	ANVIL [5]	✗	✗	✗	✓
	PARA [73]	✓	✗	✗	✗
	PRoHIT [137]	✓	✗	✗	✗
	MRLoc [161]	✓	✗	✗	✗
	CBT [132]	✓	✗	✗	✓
	TWiCe [84]	✓	✗	✗	✓
	Graphene [113]	✓	✗	✓	✓
Proactive Throttling	Naive Throtl. [102]	✓	✓	✗	✓
	Throtl. Supp. [40]	✓	✗	✗	✓
	BlockHammer	✓	✓	✓	✓

Two Main Types of DRAM Refresh

1 **Periodic Refresh:** Periodically **restores** the charge DRAM cells leak **over time**

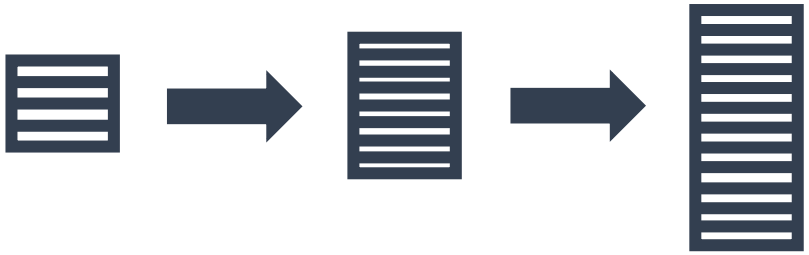
2 **RowHammer:** **Repeatedly accessing** a DRAM row can cause **bit flips** in other **physically nearby rows**



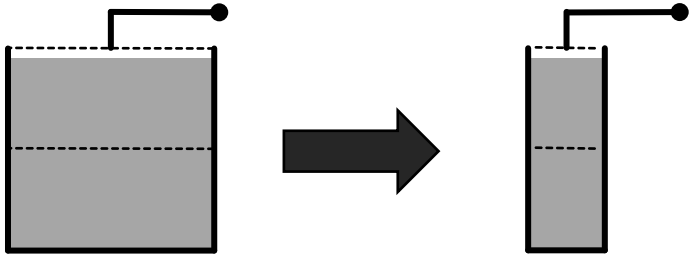
Preventive Refresh: Mitigates RowHammer by **refreshing physically nearby rows** of a repeatedly accessed row

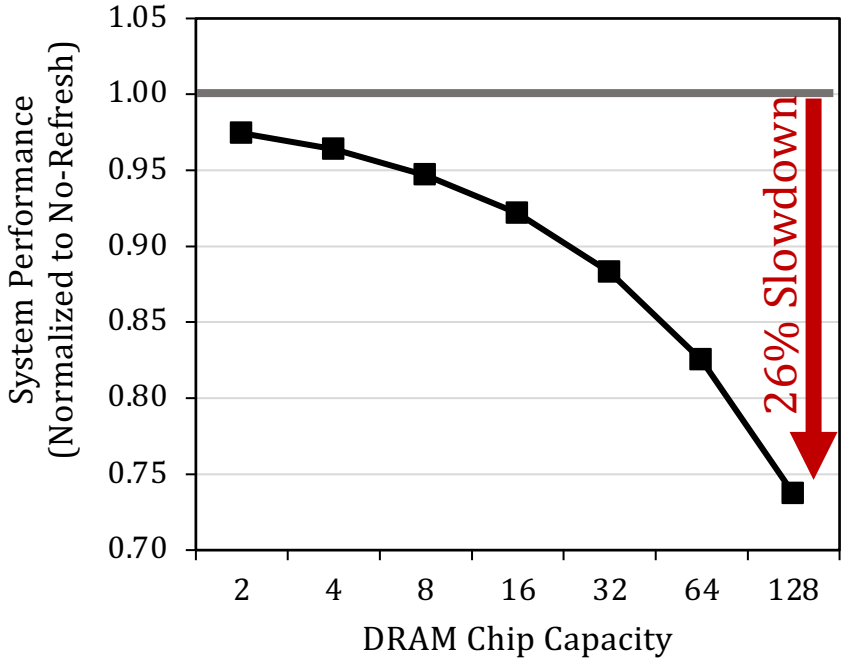
Periodic Refresh with Increasing DRAM Chip Density

A **larger capacity** chip has **more rows to be refreshed**



A **smaller** cell stores **less charge**





More periodic refresh operations incur **larger performance overhead** as DRAM **chip density increases**

Leveraging Heterogeneity

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Abdullah Giray Yağlıkçı Geraldo F. Oliveira Yahya Can Tuğrul
İsmail Emir Yüksel Ataberk Olgun Haocong Luo Onur Mutlu
ETH Zürich

Read disturbance in modern DRAM chips is a widespread phenomenon and is reliably used for breaking memory isolation, a fundamental building block for building robust systems. RowHammer and RowPress are two examples of read disturbance in DRAM where repeatedly accessing (hammering) or keeping active (pressing) a memory location induces bitflips in other memory locations. Unfortunately, shrinking technology node size exacerbates read disturbance in DRAM chips over generations. As a result, existing defense mechanisms suffer from significant performance and energy overheads, limited effectiveness, or prohibitively high hardware complexity.

In this paper, we tackle these shortcomings by leveraging the spatial variation in read disturbance across different memory locations in real DRAM chips. To do so, we 1) present the

Many prior works demonstrate attacks on a wide range of systems that exploit read disturbance to escalate privilege, leak private data, and manipulate critical application outputs [1, 3–53, 71–84]. To make matters worse, various experimental studies [1, 1, 25, 33, 36, 37, 61, 70] find that newer DRAM chip generations are more susceptible to read disturbance. For example, chips manufactured in 2018-2020 can experience RowHammer bitflips at an order of magnitude fewer row activations compared to the chips manufactured in 2012-2013 [61]. As read disturbance in DRAM chips worsens, ensuring robust (i.e., reliable, secure, and safe) operation becomes more expensive in terms of performance overhead, energy consumption, and hardware complexity [61, 85, 86]. Therefore, it is critical to understand the read disturbance vulnerabilities

Abdullah Giray Yağlıkçı, Yahya Can Tuğrul, Geraldo F. Oliveira, Ismail Emir Yuksel, Ataberk Olgun, Haocong Luo, and Onur Mutlu, **"Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions,"** to appear in HPCA, 2024.

Solutions to DRAM Read Disturbance

Throttling Unsafe Accesses

=

Parallelizing Preventive Actions

≠

Leveraging Heterogeneity

Our Goal

To understand the **spatial variation in read disturbance** across DRAM rows

To leverage this understanding **to improve** the existing **read disturbance solutions**

Detailed Information on Tested DRAM Chips

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Abdullah Giray Yağlıkçı Geraldo F. Oliveira Yahya Can Tuğrul
İsmail Emir Yüksel Ataberk Olgun Haocong Luo Onur Mutlu
ETH Zürich

Read disturbance in modern DRAM chips is a widespread phenomenon and is reliably used for breaking memory isolation, a fundamental building block for building robust systems. RowHammer and RowPress are two examples of read disturbance in DRAM where repeatedly accessing (hammering) or keeping active (pressing) a memory location induces bitflips in other memory locations. Unfortunately, shrinking technology node size exacerbates read disturbance in DRAM chips over generations. As a result, existing defense mechanisms suffer from significant performance and energy overheads, limited effectiveness, or prohibitively high hardware complexity.

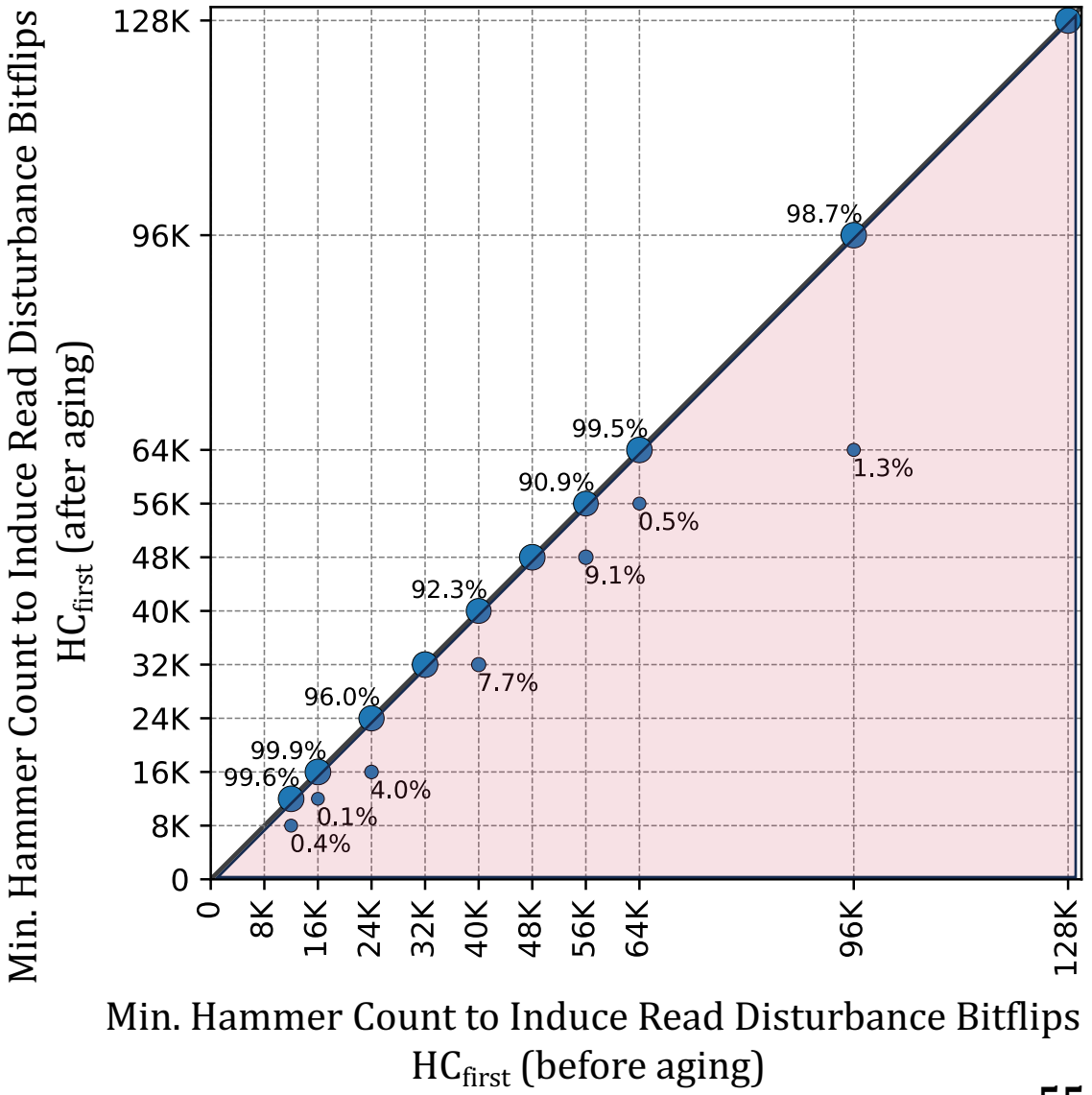
In this paper, we tackle these shortcomings by leveraging the spatial variation in read disturbance across different memory locations in real DRAM chips. To do so, we 1) present the

Many prior works demonstrate attacks on a wide range of systems that exploit read disturbance to escalate privilege, leak private data, and manipulate critical application outputs [1, 3–53, 71–84]. To make matters worse, various experimental studies [1, 1, 25, 33, 36, 37, 61, 70] find that newer DRAM chip generations are more susceptible to read disturbance. For example, chips manufactured in 2018-2020 can experience RowHammer bitflips at an order of magnitude fewer row activations compared to the chips manufactured in 2012-2013 [61]. As read disturbance in DRAM chips worsens, ensuring robust (i.e., reliable, secure, and safe) operation becomes more expensive in terms of performance overhead, energy consumption, and hardware complexity [61, 85, 86]. Therefore, it is critical to understand the read disturbance vulnerabilities

Abdullah Giray Yağlıkçı, Yahya Can Tuğrul, Geraldo F. Oliveira, Ismail Emir Yuksel, Ataberk Olgun, Haocong Luo, and Onur Mutlu, **"Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions,"** to appear in HPCA, 2024.

Future Research

- The effect of **aging**
- Preliminary data on aging via 68-day of hammering



Aging can lead to read disturbance bitflips at **fewer** hammers

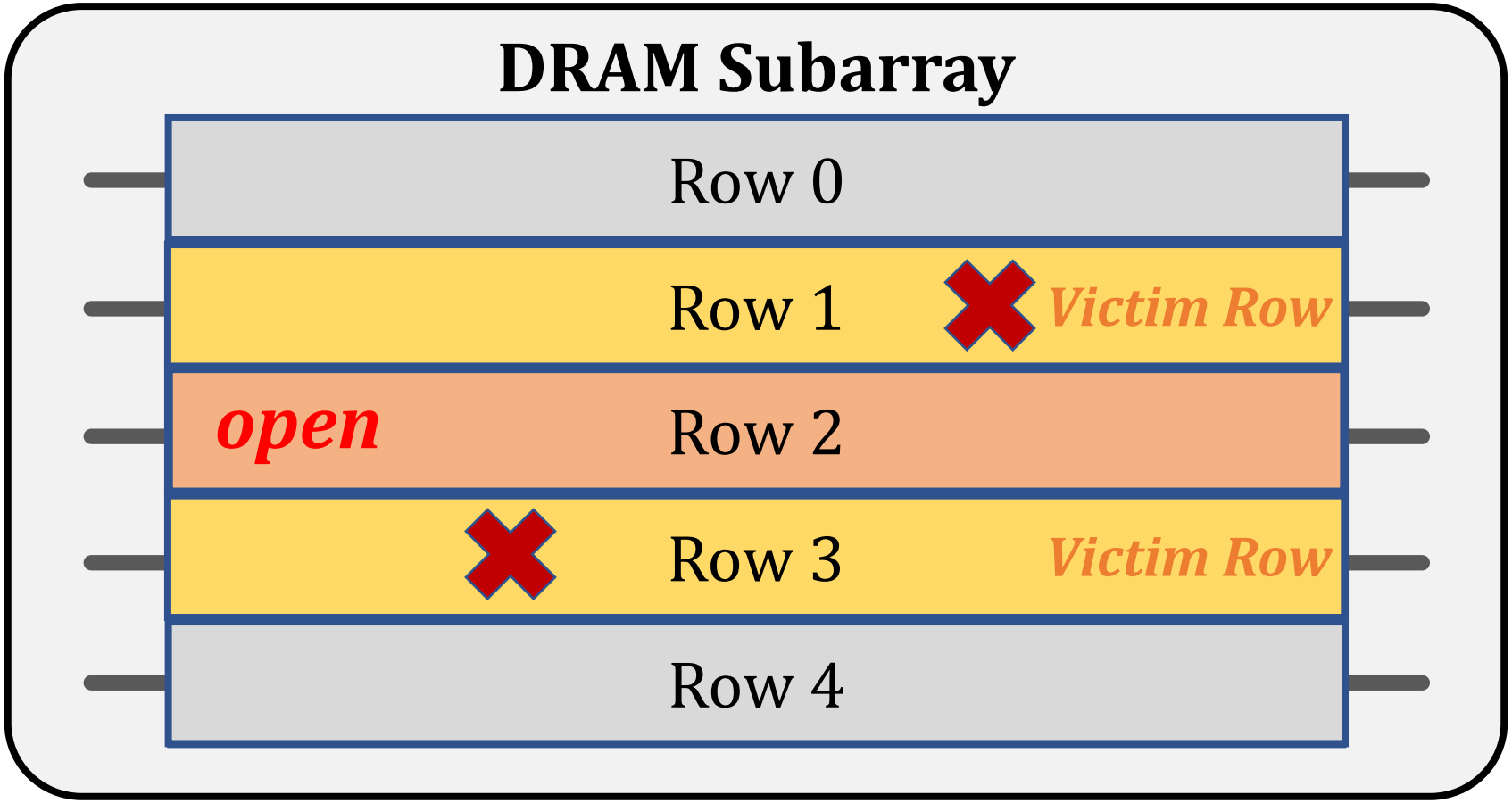
RowPress [ISCA 2023]

- Haocong Luo, Ataberk Olgun, Giray Yaglikci, Yahya Can Tugrul, Steve Rhyner, M. Banu Cavlak, Joel Lindegger, Mohammad Sadrosadati, and Onur Mutlu,
  "RowPress: Amplifying Read Disturbance in Modern DRAM Chips"
  Proceedings of the 50th International Symposium on Computer Architecture (***ISCA***), Orlando, FL, USA, June 2023.
  [Slides (pptx) (pdf)]
  [Lightning Talk Slides (pptx) (pdf)]
  [Lightning Talk Video (3 minutes)]
  [RowPress Source Code and Datasets (Officially Artifact Evaluated with All Badges)]
  Officially artifact evaluated as available, reusable and reproducible.
  Best artifact award at ISCA 2023.

RowPress: Amplifying Read-Disturbance in Modern DRAM Chips

Haocong Luo Ataberk Olgun A. Giray Yağlıkçı Yahya Can Tuğrul Steve Rhyner
Meryem Banu Cavlak Joël Lindegger Mohammad Sadrosadati Onur Mutlu
ETH Zürich

RowPress A New DRAM Read Disturbance Phenomenon



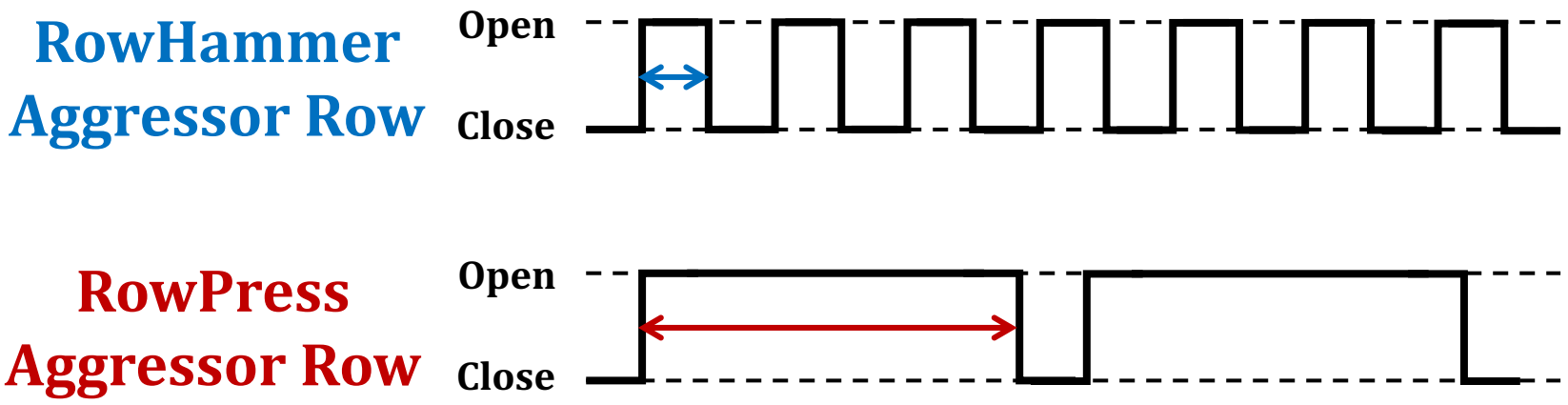
Keeping a DRAM row **open** (activated)

causes **RowPress bitflips** in nearby cells

Two Prime Examples of DRAM Read Disturbance: RowHammer and RowPress

Instead of using a high activation count,

☞ increase the time that the aggressor row stays open



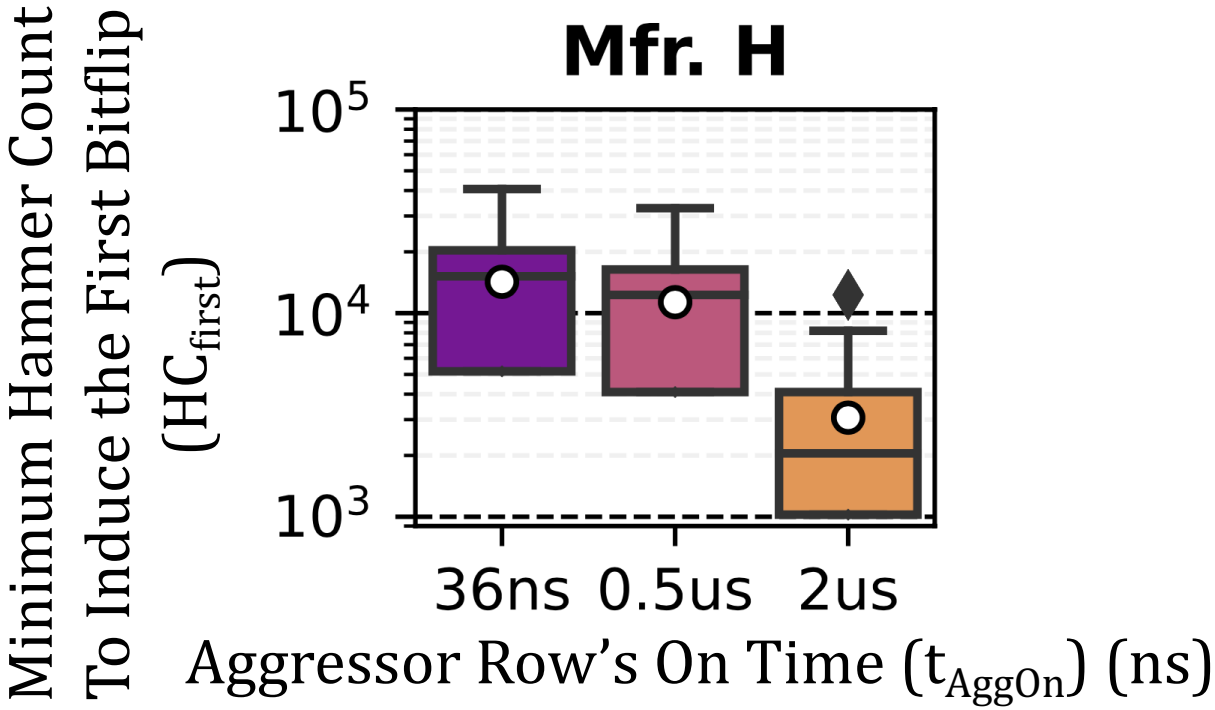
RowPress [ISCA 2023]

- Haocong Luo, Ataberk Olgun, Giray Yaglikci, Yahya Can Tugrul, Steve Rhyner, M. Banu Cavlak, Joel Lindegger, Mohammad Sadrosadati, and Onur Mutlu,
  "RowPress: Amplifying Read Disturbance in Modern DRAM Chips"
  Proceedings of the 50th International Symposium on Computer Architecture (***ISCA***), Orlando, FL, USA, June 2023.
  [Slides (pptx) (pdf)]
  [Lightning Talk Slides (pptx) (pdf)]
  [Lightning Talk Video (3 minutes)]
  [RowPress Source Code and Datasets (Officially Artifact Evaluated with All Badges)]
  Officially artifact evaluated as available, reusable and reproducible.
  Best artifact award at ISCA 2023.

RowPress: Amplifying Read-Disturbance in Modern DRAM Chips

Haocong Luo Ataberk Olgun A. Giray Yağlıkçı Yahya Can Tuğrul Steve Rhyner
Meryem Banu Cavlak Joël Lindegger Mohammad Sadrosadati Onur Mutlu
ETH Zürich

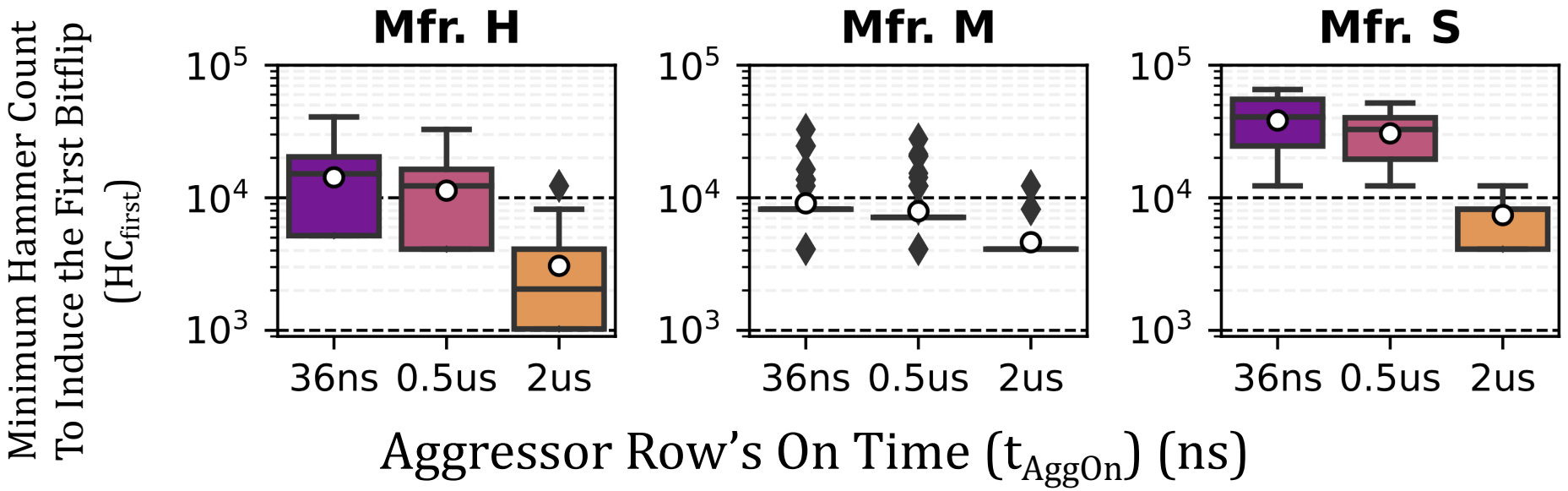
Effect of RowPress on Spatial Variation of Read Disturbance Vulnerability across Rows



RowPress reduces the mean of the distribution with increased t_{AggOn}

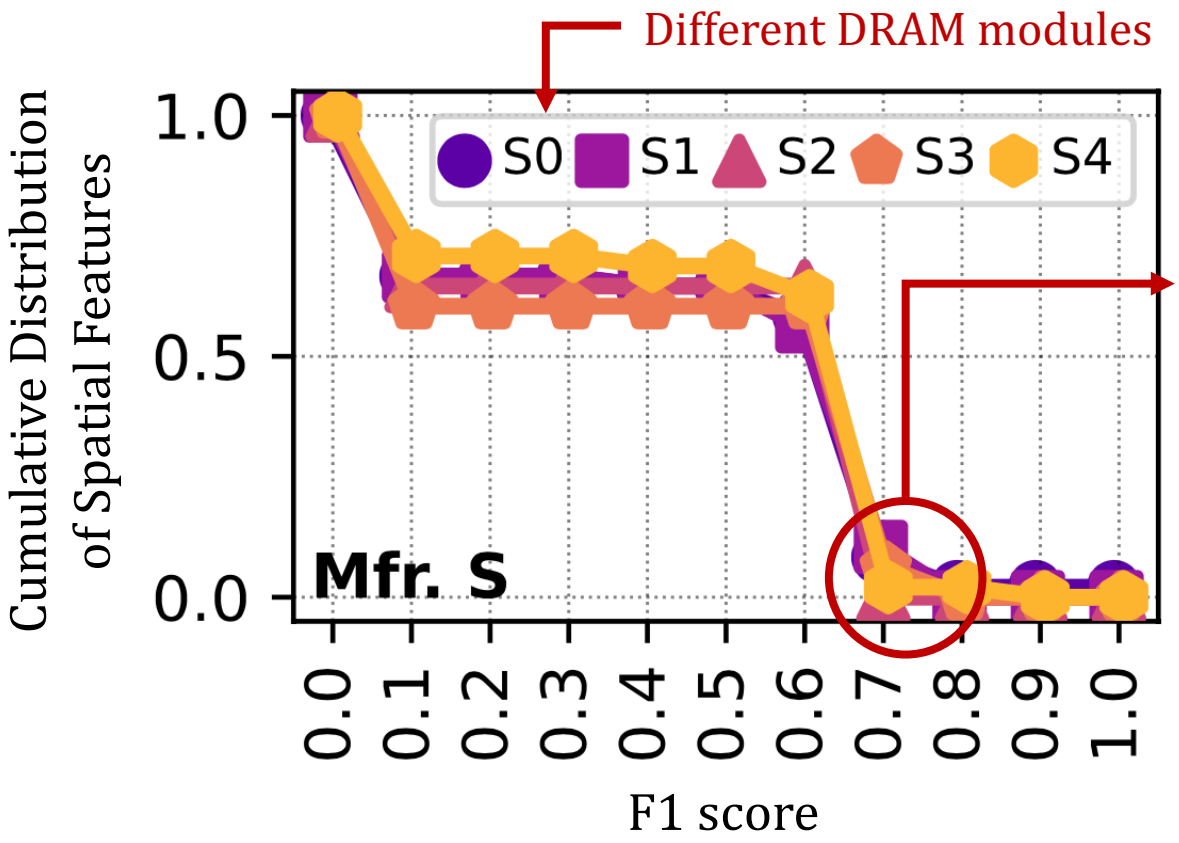
There is still significant variation in the HC_{first} across rows

Effect of RowPress on the HCfirst Distribution



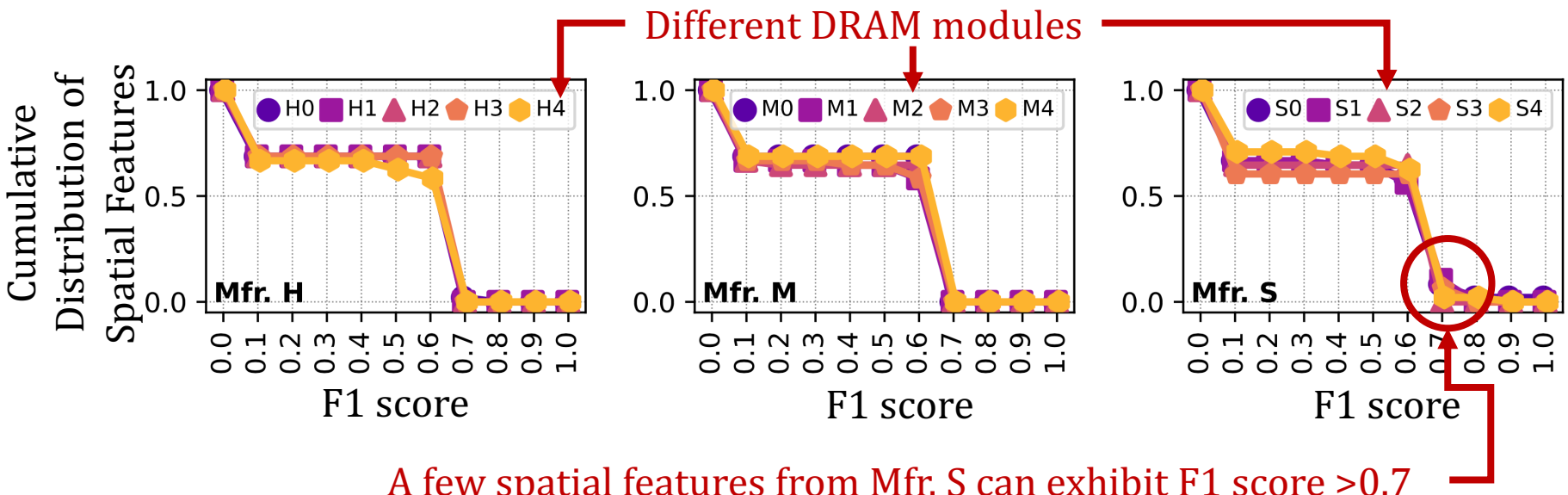
Bitflips occur at **lower hammer counts** with RowPress
and these hammer counts still **significantly vary** across DRAM rows

Cumulative Distribution of Spatial Features based on F1 Score



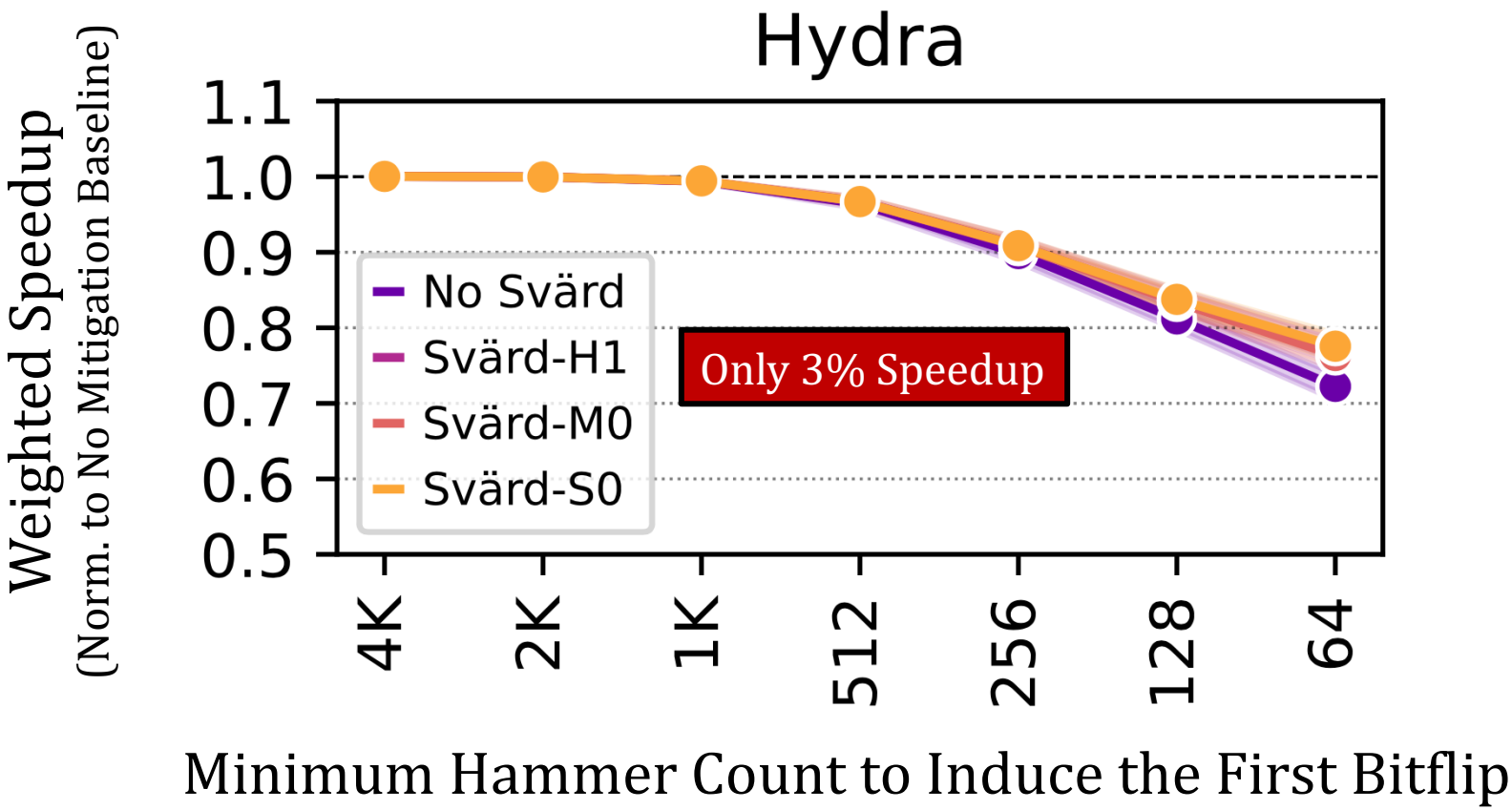
No good prediction observed between a row's **spatial features** & read disturbance **vulnerability**

Cumulative Distribution of Spatial Features based on F1 Score



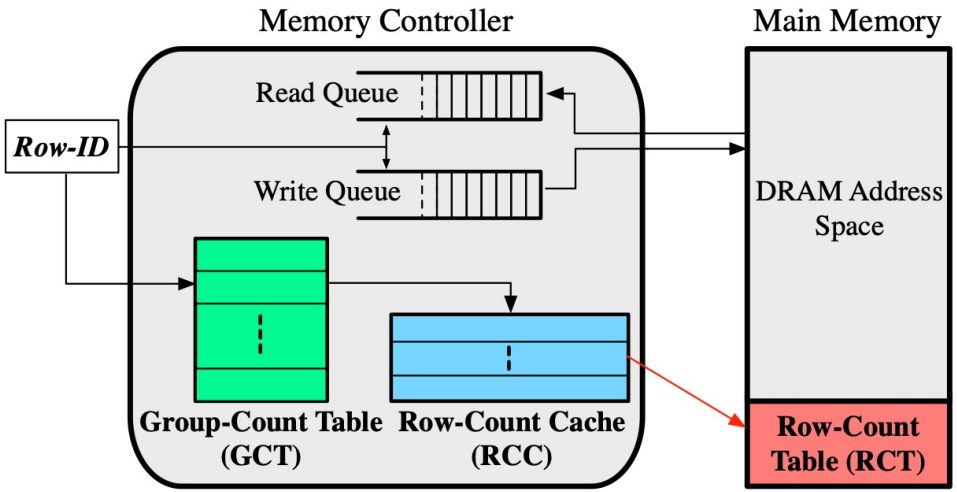
No good prediction observed between a row's **spatial features** & read disturbance **vulnerability**

An Outlier Solution: Hydra



Hydra Mitigation Mechanism

- Hydra maintains **a row activation counter for each DRAM row**
- **Stores** these activation counters **in the DRAM array**
- **Caches** the counters of hot rows **in the memory controller**
- At low HC_{first} configurations, **many rows are hot**
- **Fetching / evicting counters** dominate the performance overhead
- Svärd needs **further customizations** for Hydra



Qureshi, et al. **"Hydra: Enabling Low-Overhead Mitigation of Row-Hammer at Ultra-Low Thresholds via Hybrid Tracking," in ISCA, 2022.**

Conclusion

Experimental study: **136 DDR4 DRAM chips** from **3 major vendors**

- A **large variation** in the necessary activation count to induce the first bitflip
- No strong correlation between a row's **spatial features** and **its vulnerability** to read disturbance

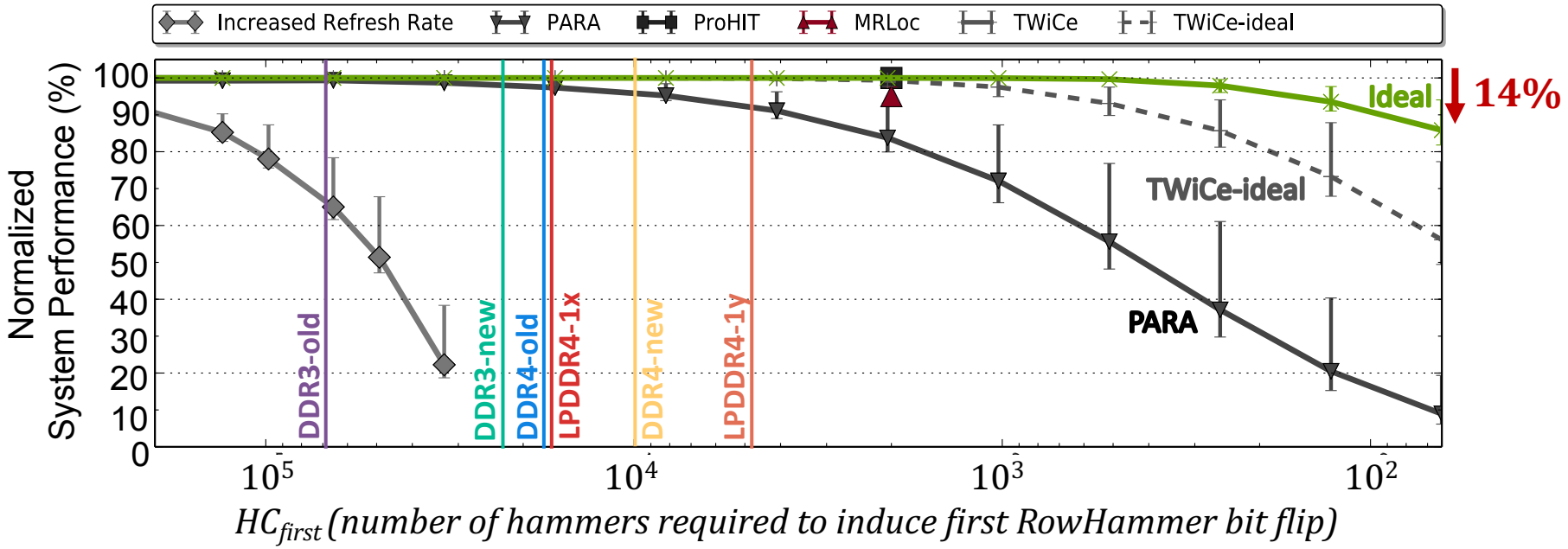
SVÄRD: Dynamically adapts the aggressiveness of mitigations

- Implemented in either **the DRAM chip** or **the memory controller**
- Reduces the performance overheads by **2.4x, 2.7%, 1.6x, and 3.0x** for **BlockHammer, Hydra, PARA,** and **RRS**

Future Work:

- A **deeper understanding** is needed to account for **irregularities** in **row and column addresses** across chips
- **Finding correlations** is essential **to reduce the hardware cost**
- Reducing also **the hardware cost of defenses**

RowHammer Mitigation across Generations



J. S. Kim, M. Patel, A. G. Yaglikci, H. Hassan, R. Azizi, L. Orosa, and O. Mutlu, "Revisiting RowHammer: An Experimental Analysis of Modern Devices and Mitigation Techniques," in *ISCA*, 2020.

Spatial Variation-Aware Read Disturbance Defenses: Experimental Analysis of Real DRAM Chips and Implications on Future Solutions

Backup Slides

Abdullah Giray Yağlıkçı

Yahya Can Tuğrul Geraldo F. Oliveira İsmail Emir Yüksel

Ataberk Olgun Haocong Luo Onur Mutlu

SAFARI

ETH zürich