Enabling Efficient and Scalable Read Disturbance Mitigation

via New Experimental Insights into Modern Memory Chips

agyaglikci.github.io

Abdullah Giray Yaglikci

agyaglikci@gmail.com

https://agyaglikci.github.io

7 March 2024

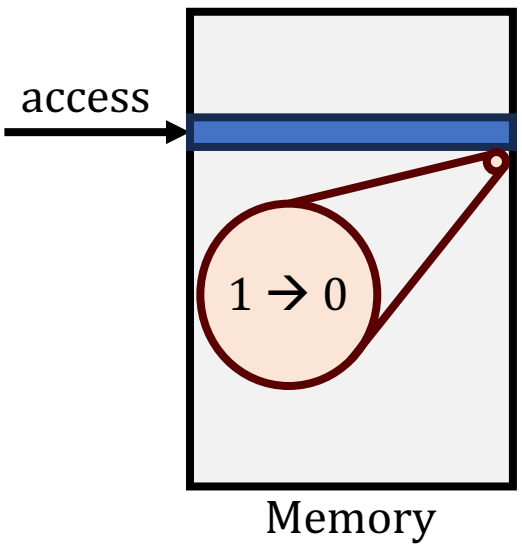
University of Glasgow

safari.ethz.ch

SAFARI

ETH zürich

Lack of Memory Isolation



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

Compromise Application **Correctness**

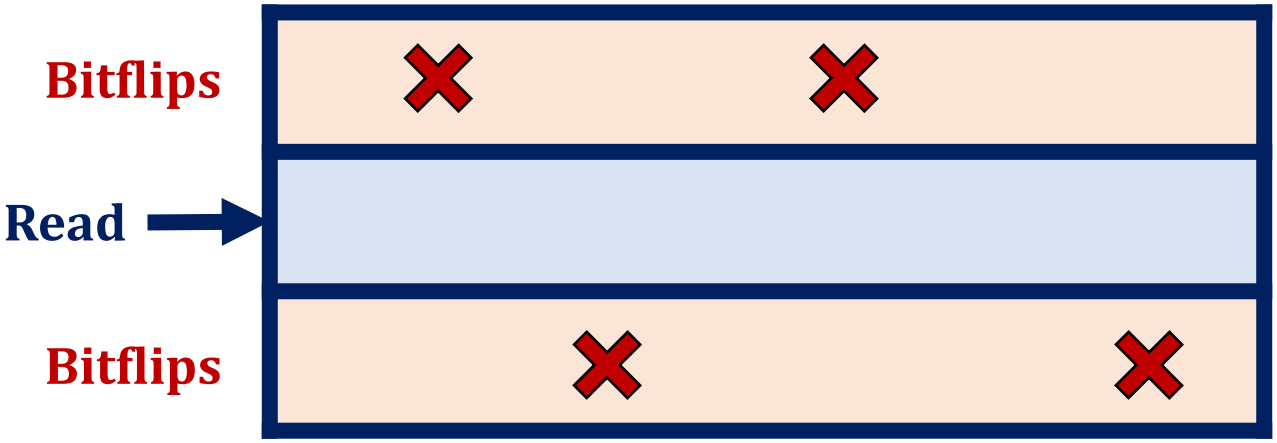
Leak Private Information

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 Read Disturbance

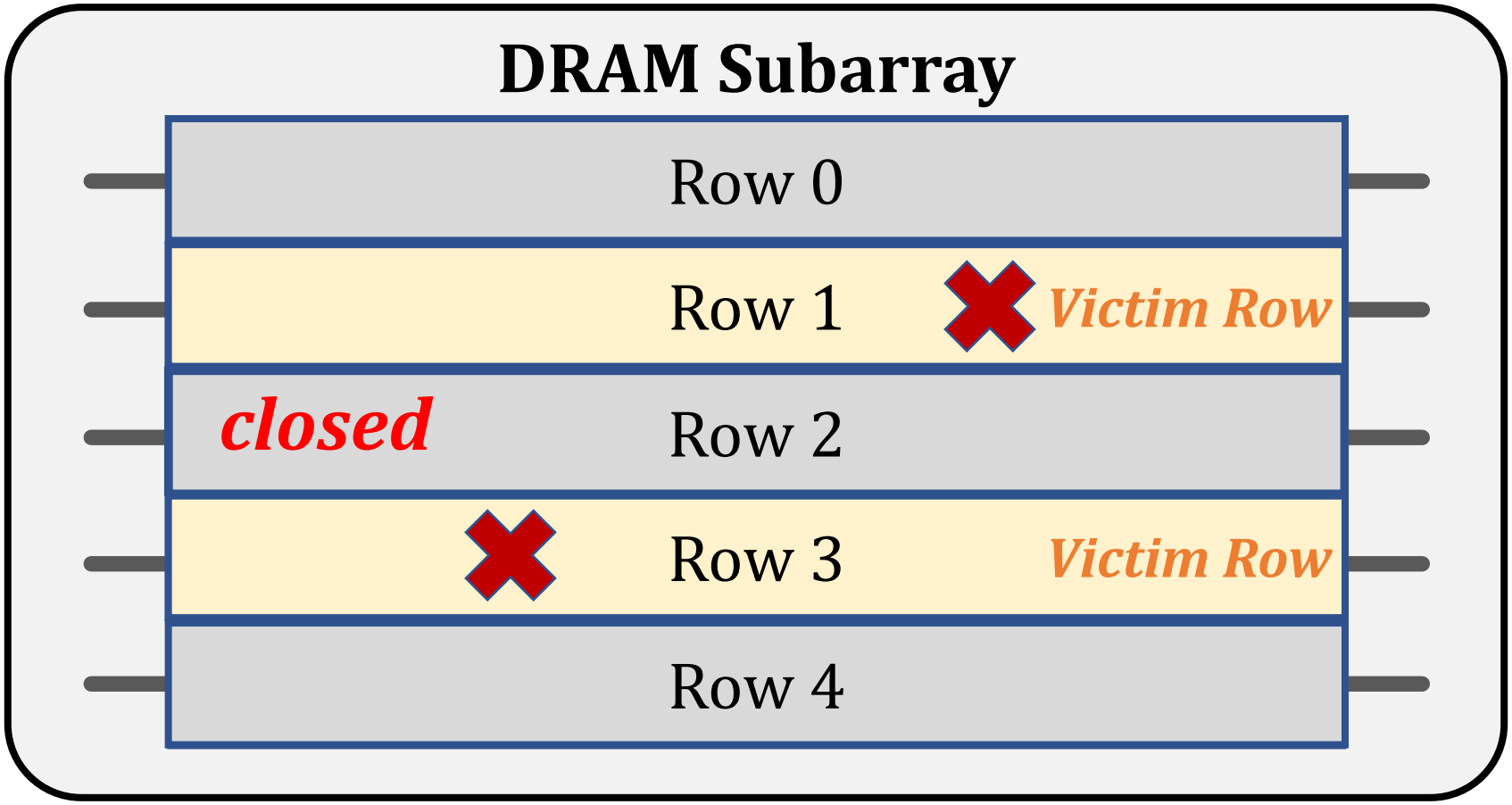


Reading from a memory location
disturbs data in **physically nearby** locations

DRAM Read Disturbance – Swimming Pool Analogy

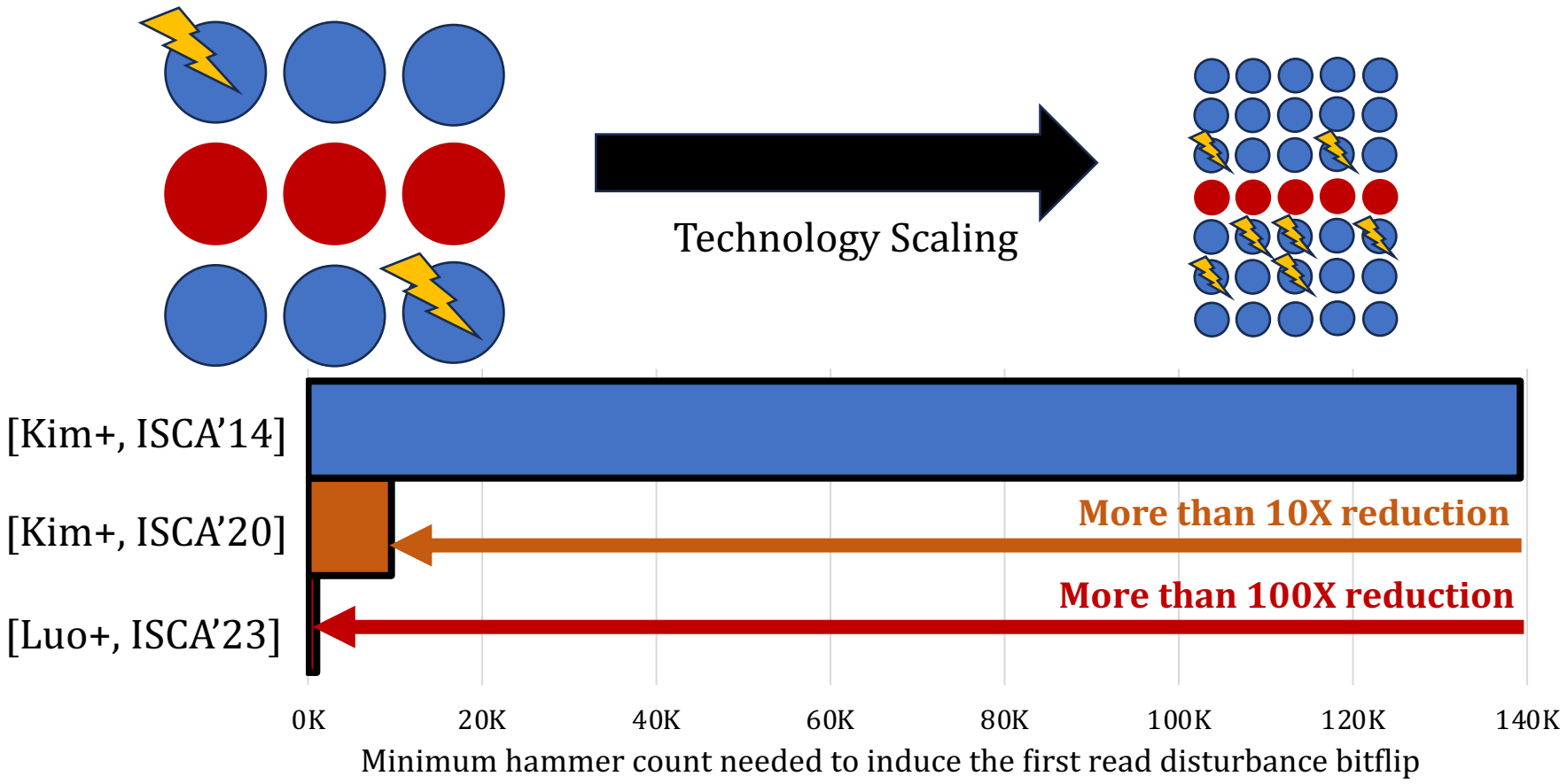
Swimming **in a lane** disturbs **nearby lanes**

The RowHammer Vulnerability [Kim+, ISCA'14]



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

Motivation



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

Thesis Statement

Developing

a deeper understanding of DRAM read disturbance

and

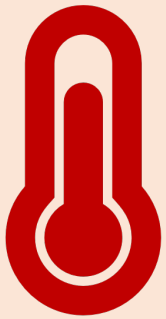
revisiting memory controller designs

enable scientists and engineers to build

reliable, secure, and safe DRAM-based systems

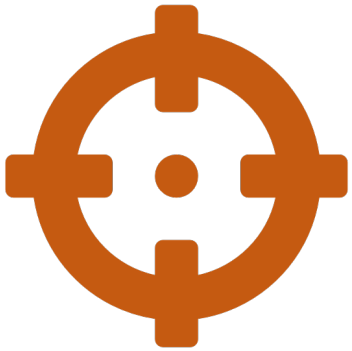
My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns



Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

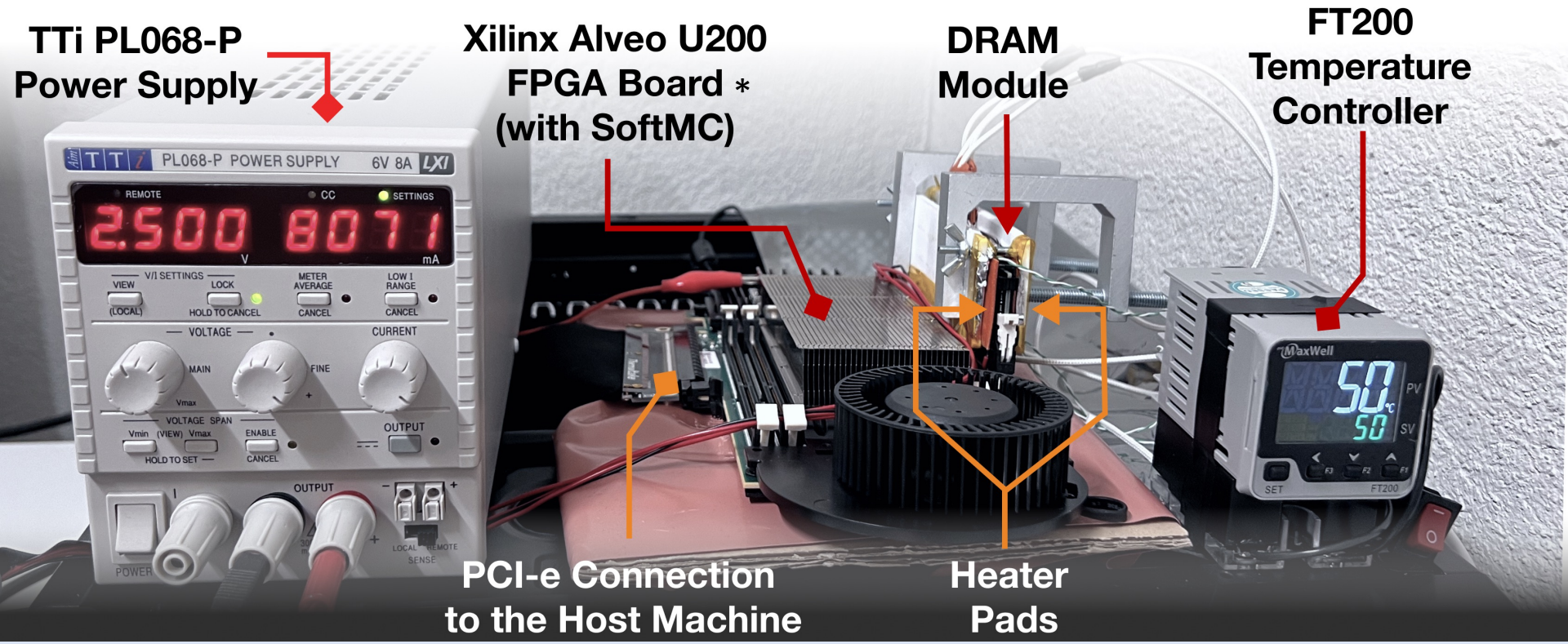
Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actio

DRAM Testing Infrastructure

DRAM Bender on a Xilinx Virtex UltraScale+ XCU200



Fine-grained control over **DRAM commands**, **timing parameters (±1.5ns)**, **temperature (±0.5°C)**, and **wordline voltage (±1mV)**

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

DRAM Chips Tested

Two DRAM standards

Mfr.	DDR4 DIMMs	DDR3 SODIMMs	# Chips	Density	Die	Org.
A (Micron)	9	1	144 (8)	8Gb (4Gb)	B (P)	x4 (x8)
B (Samsung)	4	1	32 (8)	4Gb (4Gb)	F (Q)	x8 (x8)
C (SK Hynix)	5	1	40 (8)	4Gb (4Gb)	B (B)	x8 (x8)
D (Nanya)	4	-	32 (-)	8Gb (-)	C (-)	x8 (-)

4 Major Manufacturers

272 DRAM Chips in total

DRAM Chips Tested

A Deeper Look into RowHammer's Sensitivities: Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses

Lois Orosa* ETH Zürich
A. Giray Yağlıkçı* ETH Zürich
Haocong Luo ETH Zürich
Ataberk Olgun ETH Zürich, TOBB ETÜ
Jisung Park ETH Zürich
Hasan Hassan ETH Zürich
Minesh Patel ETH Zürich
Jeremie S. Kim ETH Zürich
Onur Mutlu ETH Zürich

Table 4: Characteristics of the tested DDR4 and DDR3 DRAM modules.

Type	Chip Manufacturer	Chip Identifier	Module Vendor	Module Identifier	Freq. (MT/s)	Date Code	Density	Die Rev.	Org.	#Modules	#Chips
DDR4	A: Micron	MT40A2G4WE-083E:B	Micron	MTA18ASF2G72PZ-2G3B1QG [94]	2400	1911	8Gb	B	x4	6	96
						1843				2	32
						1844				1	16
	B: Samsung	K4A4G085WF-BCTD [132]	G.SKILL	F4-2400C17S-8GNT [35]	2400	2021 Jan ★	4Gb	F	x8	4	32
	C: SK Hynix	DWCW (Partial Marking) †	G.SKILL	F4-2400C17S-8GNT [35]	2400	2042	4Gb	B	x8	5	40
	D: Nanya	D1028AN9CPGRK ‡	Kingston	KVR24N17S8/8 [75]	2400	2046	8Gb	C	x8	4	32
DDR3	A: Micron	MT41K512M8DA-107:P [22]	Crucial	CT51264BF160BJ.M8FP	1600	1703	4Gb	P	x8	1	8
	B: Samsung	K4B4G0846Q	Samsung	M471B5173QH0-YK0 [131]	1600	1416	4Gb	Q	x8	1	8
	C: SK Hynix	H5TC4G83BFR-PBA	SK Hynix	HMT451S6BFR8A-PB [139]	1600	1535	4Gb	B	x8	1	8

SAFARI

DRAM Testing Methodology

To characterize our DRAM chips at **worst-case** conditions:

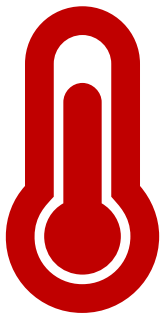
1. Prevent sources of interference during core test loop

- **No DRAM refresh**: to avoid refreshing victim row
- **No DRAM calibration events**: to minimize variation in test timing
- **No RowHammer mitigation mechanisms**: to observe circuit-level effects
- Test for **less than a refresh window (32ms)** to avoid retention failures
- **Repeat tests** for ten times

2. Worst-case access sequence

- We use **worst-case** access sequence based on prior works' observations
- For each row, **repeatedly access the two physically-adjacent rows as fast as possible**

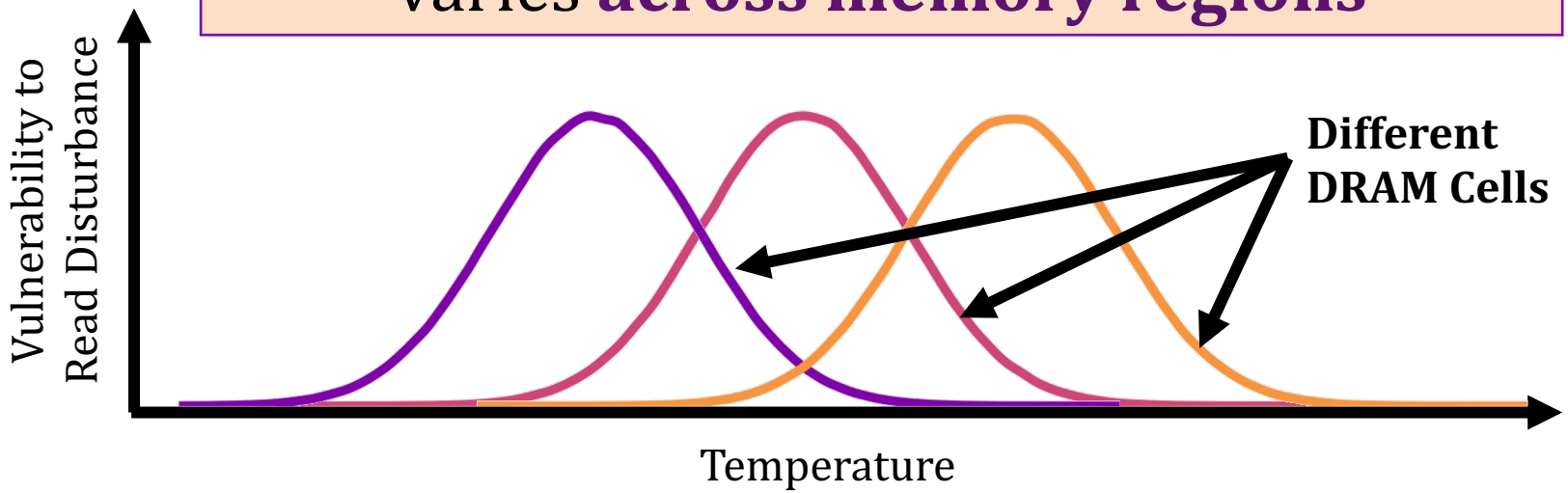
Key Findings: Temperature



Temperature

DRAM read disturbance is more effective **within a temperature range**

Vulnerable temperature range varies **across memory regions**

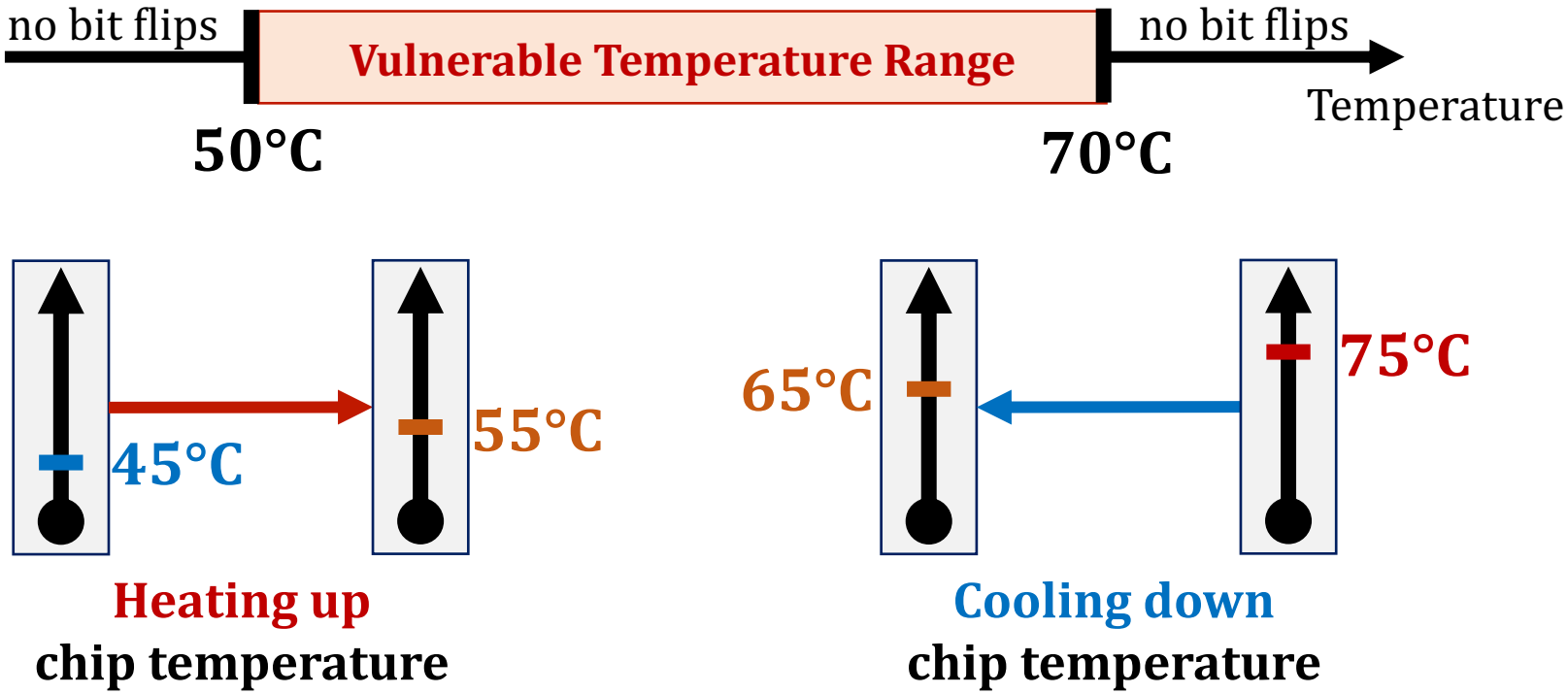


A DRAM cell should be tested at **each possible** operating temperature

Attack Improvement 1:
Making DRAM Cells More Vulnerable

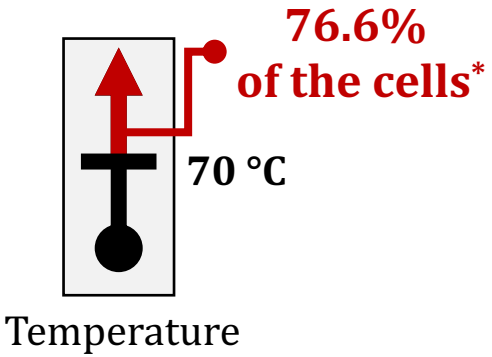
An attacker can **manipulate temperature** to make the cells that store sensitive data **more vulnerable**

DRAM cells are vulnerable in a **bounded temperature range**

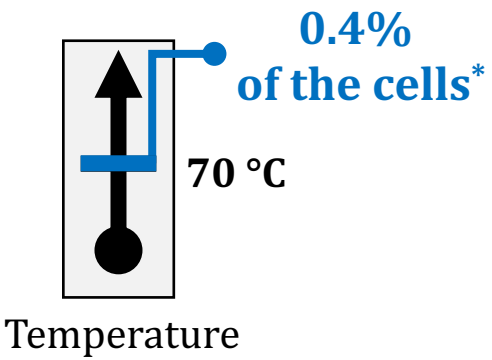


Attack Improvement 2:
Temperature-Dependent Trigger

1. Identify **abnormal increase** in temperature to attack a data center **during its peak hours**



2. **Precisely measure** the temperature **to trigger an attack** exactly at the desired temperature



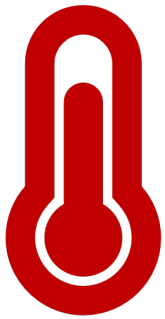
*Example fraction values from SK Hynix modules

Contributions to Understanding RowHammer

- Lois Orosa*, **Abdullah Giray Yağlıkçı***, Haocong Luo, Ataberk Olgun, Jisung Park, Hasan Hassan, Minesh Patel, Jeremie S. Kim, and Onur Mutlu,
  "A Deeper Look into RowHammer's Sensitivities: Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses"
  *Proceedings of the 54th International Symposium on Microarchitecture (**MICRO**)*, Virtual, October 2021.
  [Slides (pptx) (pdf)] [Talk Video (21 minutes)]
  [Short Talk Slides (pptx) (pdf)]
  [Lightning Talk Slides (pptx) (pdf)] [Lightning Talk Video (1.5 minutes)]
  [arXiv version]

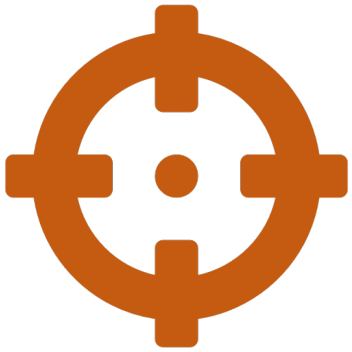
My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns



Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

Leveraging Heterogeneity

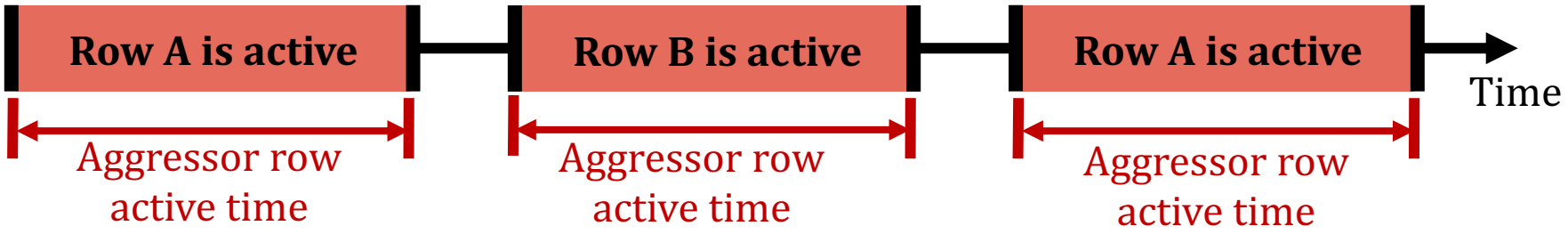
Throttling Unsafe Accesses

Parallelizing Preventive Actio

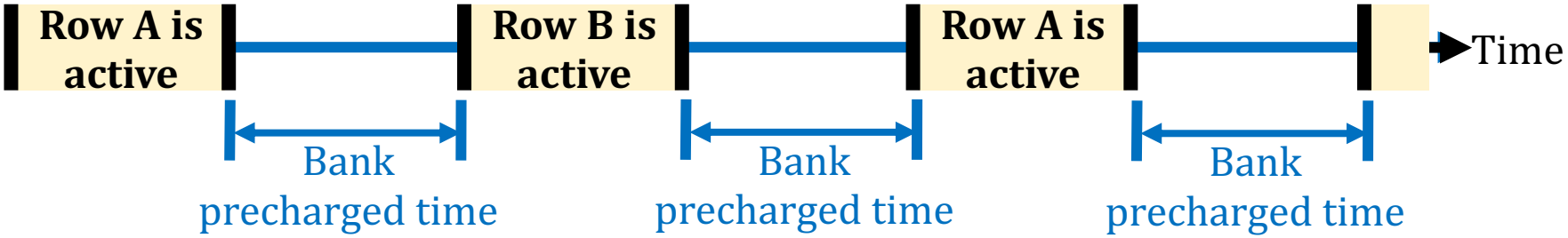
Memory Access Patterns in Aggressor Row Active Time Analysis

- Baseline access pattern:

- Increasing **aggressor row active time**:



- Increasing **bank precharged time**:



Key Findings: Memory Access Patterns

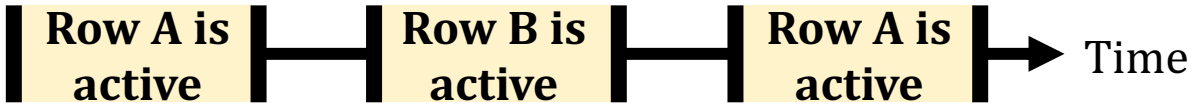
Memory Access Patterns

Read disturbance is **more effective** if the **read memory region** stays **active longer**

Fewer reads cause a **more significant** read disturbance when the read memory region stays **active longer**

Attack Improvement 3:
Bypassing Defenses with Aggressor Row Active Time

Activating aggressor rows **as frequently as possible**:



Keeping the aggressor rows **active for a longer time**:

Reduces the minimum activation count to induce a bit flip **by 36%**

Bypasses defenses that do not account for this reduction

Contributions to Understanding RowHammer

- Lois Orosa*, **Abdullah Giray Yağlıkçı***, Haocong Luo, Ataberk Olgun, Jisung Park, Hasan Hassan, Minesh Patel, Jeremie S. Kim, and Onur Mutlu,
  "A Deeper Look into RowHammer's Sensitivities: Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses"
  *Proceedings of the 54th International Symposium on Microarchitecture (**MICRO**)*, Virtual, October 2021.
  [Slides (pptx) (pdf)] [Talk Video (21 minutes)]
  [Short Talk Slides (pptx) (pdf)]
  [Lightning Talk Slides (pptx) (pdf)] [Lightning Talk Video (1.5 minutes)]
  [arXiv version]

RowPress [Luo+, ISCA 2023] (Follow up of our analysis)

- 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

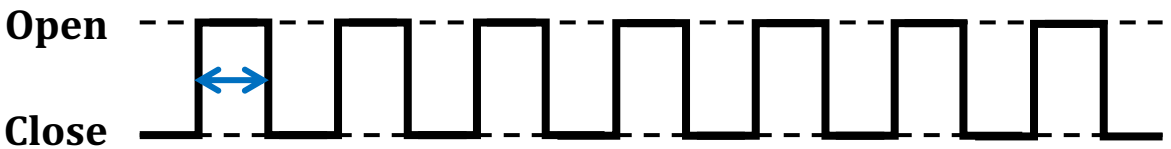
Haocong Luo Ataberk Olgun A. Giray Yağlıkçı Yahya Can Tuğrul Steve Rhyner
Meryem Banu Cavlak Joël Lindegger Mohammad Sadrosadati Onur Mutlu
ETH Zürich

RowPress vs. RowHammer

Instead of using a high activation count,

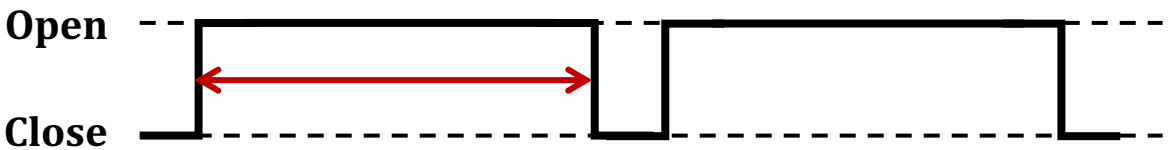
☞ increase the time that the aggressor row stays open

RowHammer Aggressor Row



36ns, 47K activations to induce bitflips

RowPress Aggressor Row



7.8µs, only 5K activations to induce bitflips

We observe bitflips even with **ONLY ONE activation** in extreme cases where the row stays open for 30ms

RowPress [Luo+, ISCA 2023]

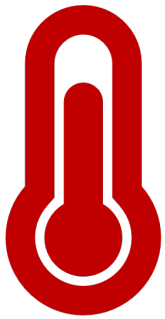
- Haocong Luo, Ataberk Olgun, Giray Yaglikci, Yahya Can Tugrul, Steve Rhyner, M. Banu Cavlak, Joel Lindegger, Mohammad Sadrosadati, and Onur Mutlu,
  "RowPress: Amplifying Read Disturbance in Modern DRAM Chips"
  Proceedings of the 50th International Symposium on Computer Architecture ***(ISCA)***, Orlando, 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

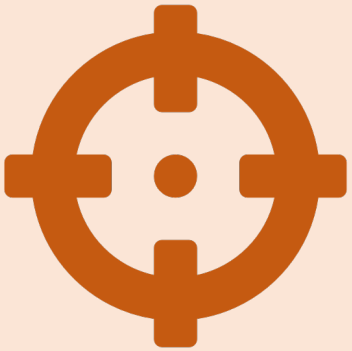
My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns



Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

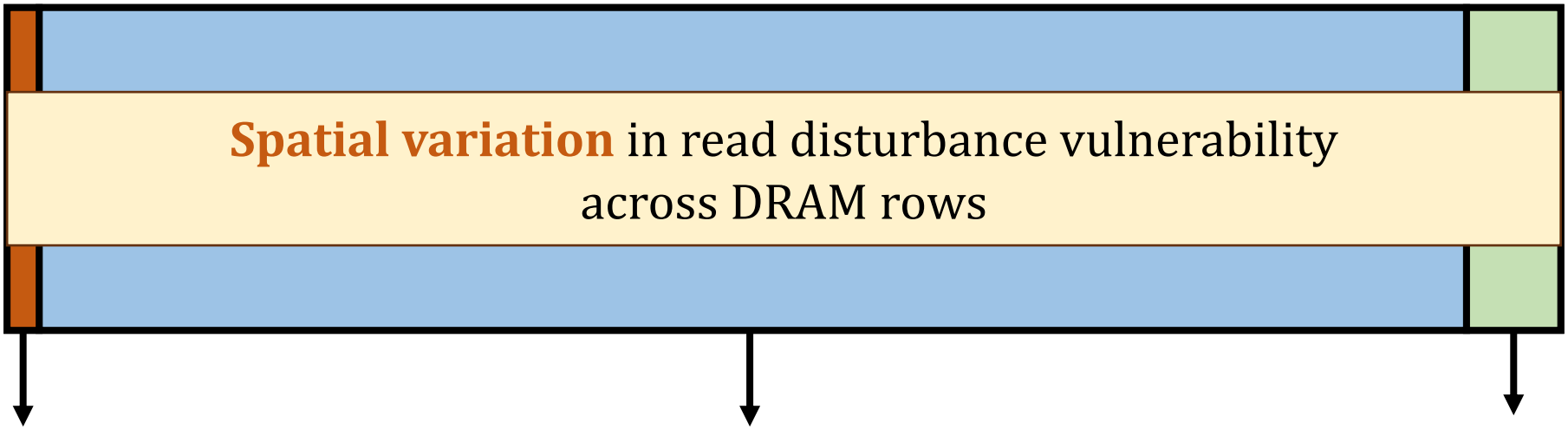
Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actio

Spatial Variation in Read Disturbance Vulnerability Across DRAM Rows

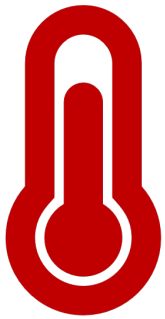
- To induce a **read disturbance bitflip,** one should access a row



- Read disturbance solutions are configured **for the worst row**
- **Not all rows** need the **same level** of protection
- Read disturbance solutions incur **large performance overheads** due to **overprotecting many rows**

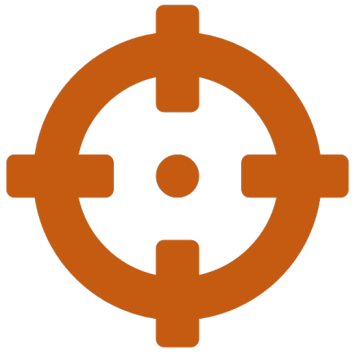
My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns



Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actio

Motivation

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

Existing solutions become **more aggressive**

Overprotecting many rows significantly increases their **performance overhead**

Motivation

Can we **leverage the variation** in read disturbance **vulnerability** across **DRAM rows**

to **reduce the performance overheads** of existing read disturbance solutions?

Problem

No prior work rigorously studies

spatial variation of DRAM read disturbance
across all DRAM rows

&

this variation's implications
on **future solutions**

Our Goal

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

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

Tested DRAM Chips

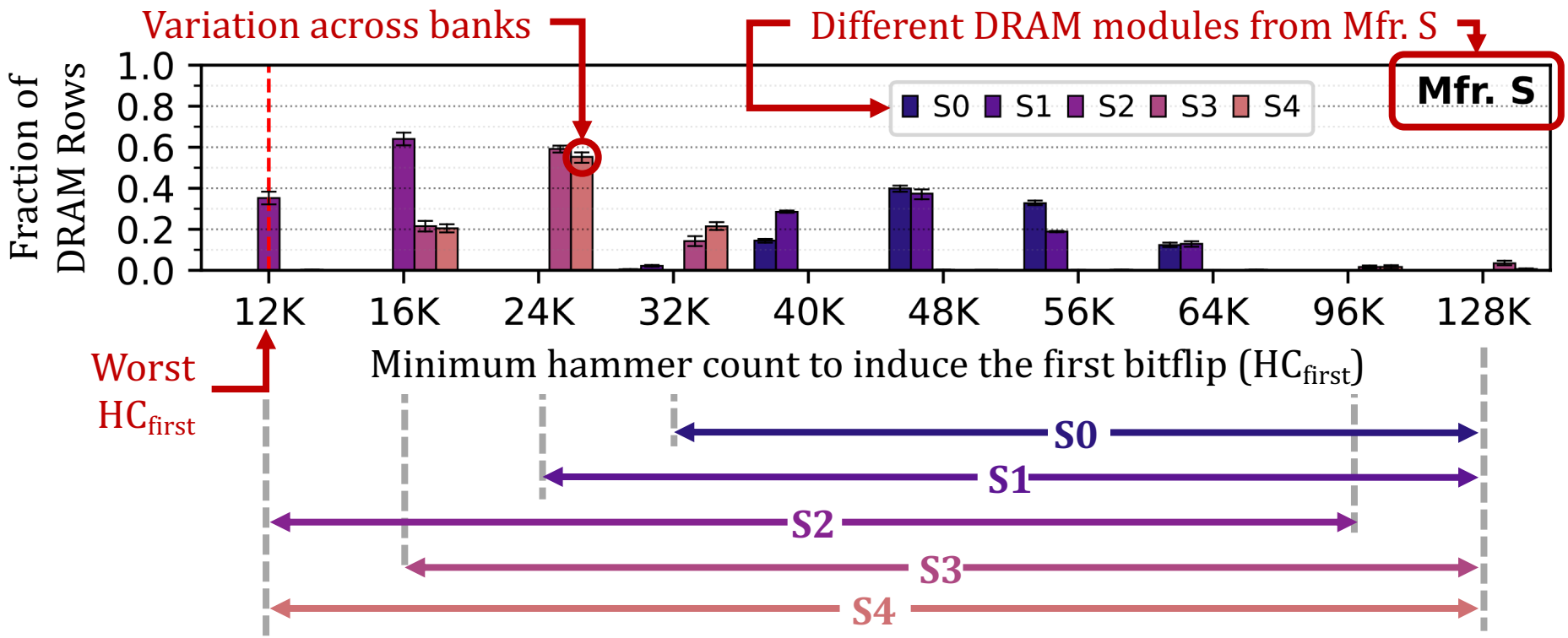
144 DRAM chips from SK Hynix, Micron, and Samsung

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 – B	x8	10-21
	S3	8	4Gb – F	x8	N/A
	S4	16	8Gb – C	x4	35-21

Key Takeaway from Real Chip Experiments

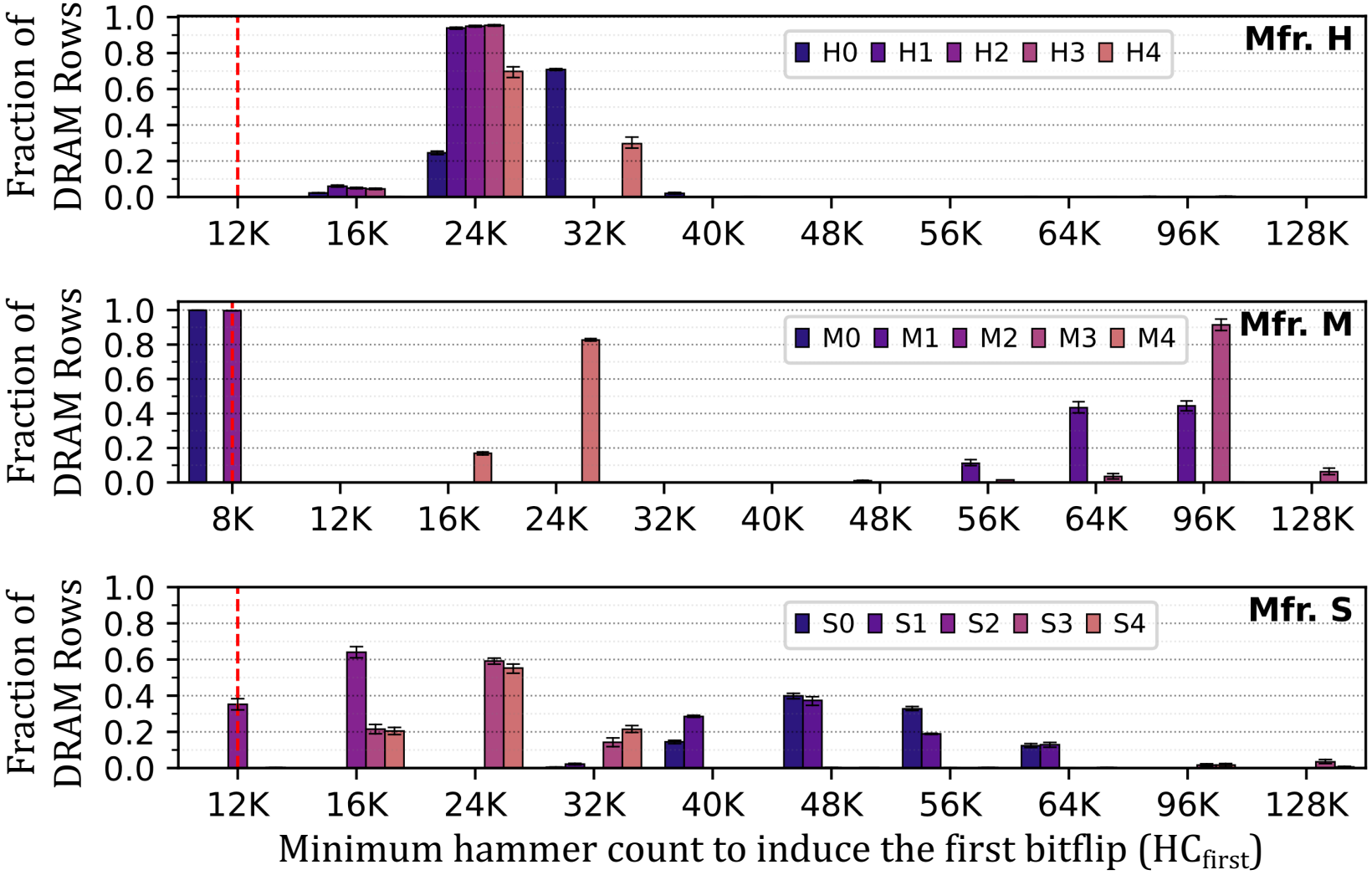
Read disturbance vulnerability varies
significantly and **irregularly**
across DRAM rows

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

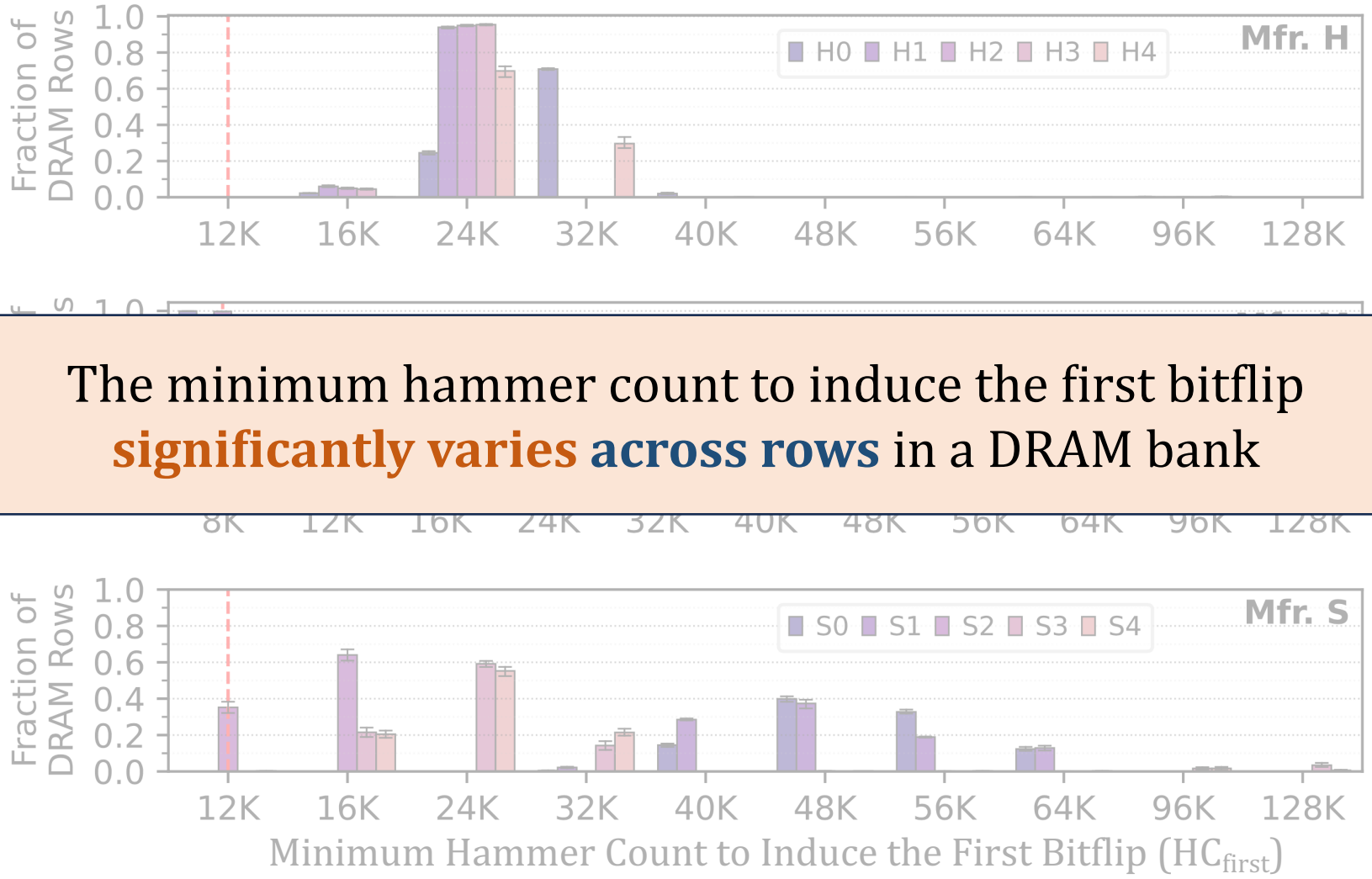


The minimum hammer count to induce the first bitflip **significantly varies across rows** in a DRAM bank

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

Svärd: Spatial Variation-Aware Read Disturbance Defenses

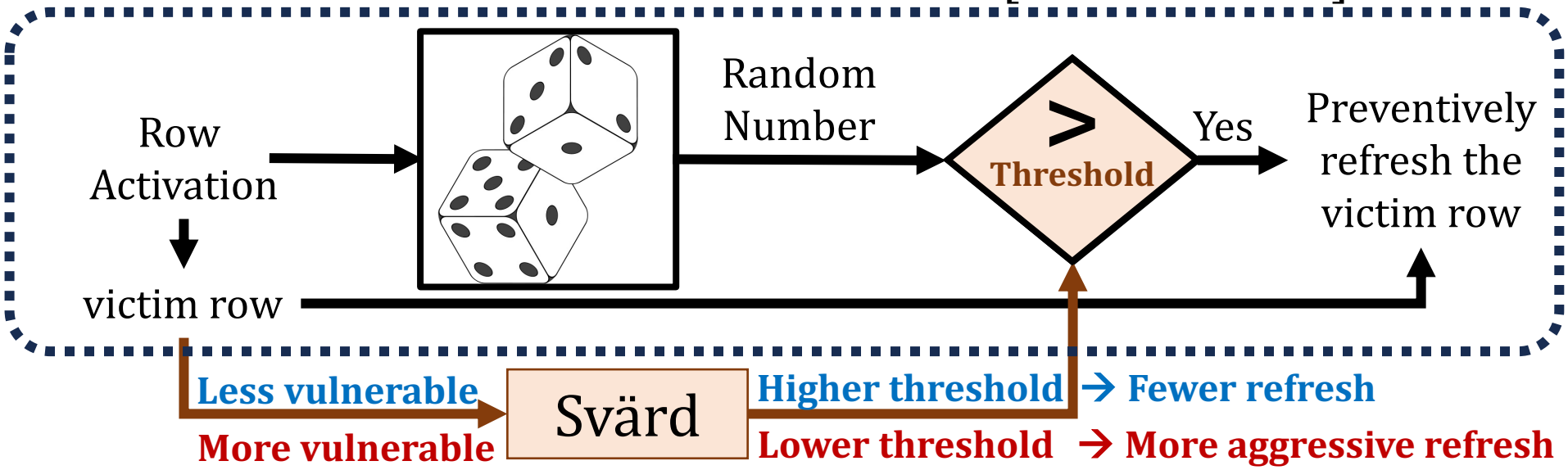
- **Key Experimental Takeaway:** Read disturbance vulnerability **varies significantly** and **irregularly** across DRAM rows
- **Key Idea:** Leverage the variation in read disturbance vulnerability across DRAM rows
- **Svärd:** Spatial Variation-Aware DRAM Read Disturbance Defenses **Dynamically tunes 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: Integration with Existing Read Disturbance Solutions

PARA: Probabilistic Row Activation [Kim+, ISCA'14]



Svärd dynamically tunes **PARA's threshold** to the **victim row's vulnerability**

Svärd works with **many read disturbance solutions**, including:

BlockHammer [Yaglikci+, HPCA'21]

Hydra [Qureshi+, ISCA'22]

RRS [Saileshwar+, ASPLOS'22]

AQUA [Saxena+, MICRO'22]

Svärd: Metadata Management

- Classifies DRAM rows into **several vulnerability bins**
  Maintains **a few (e.g., four) bits** per DRAM row
- Implemented **where the read disturbance solution is**
- Memory controller-based implementation:
  Metadata can be maintained in
  - SRAM table in the memory controller
  - Data integrity bits in the DRAM chip
  - …
- In-DRAM implementation:
  Metadata can be maintained in
  - DRAM rows
  - Separate DRAM array
  - …

Performance Evaluation

- Cycle-level simulations using **Ramulator 2.0** [Luo+, CAL 2023]
  https://github.com/CMU-SAFARI/ramulator2

- **System Configuration**:

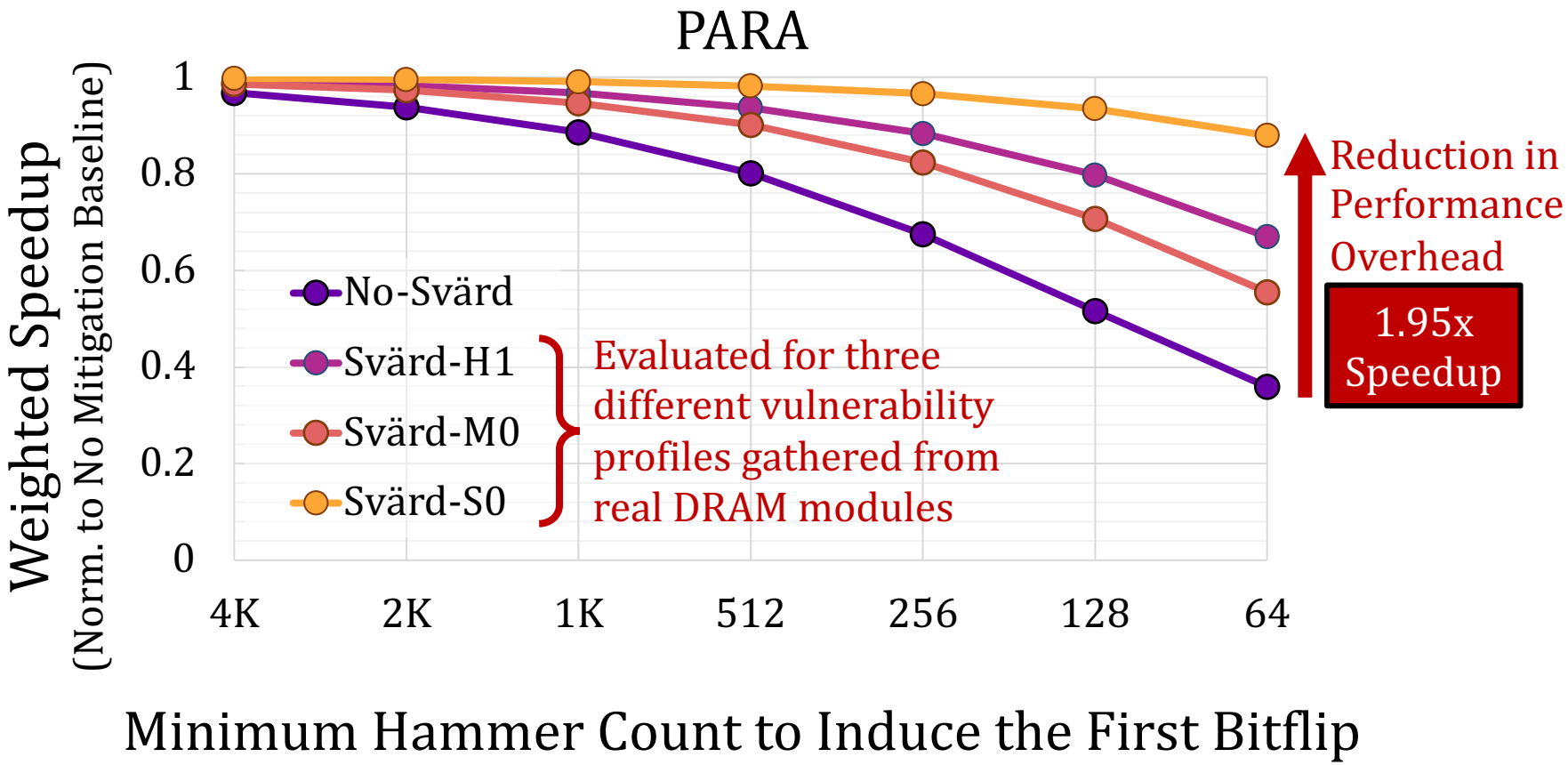
Processor	3.2 GHz, 8 core, 4-wide issue, 128-entry instr. window
Last-Level Cache	64-byte cache line, 8-way set-associative, 8 MB
Memory Scheduler	FR-FCFS
Address Mapping	Minimalistic Open Pages
Main Memory	DDR4, 4 bank group, 4 banks per bank group (16 banks per rank)

- **Workloads**: **120** different **8-core** multiprogrammed workloads from **SPEC CPU2006, SPEC CPU2017, TPC, MediaBench,** and **YCSB** benchmark suites

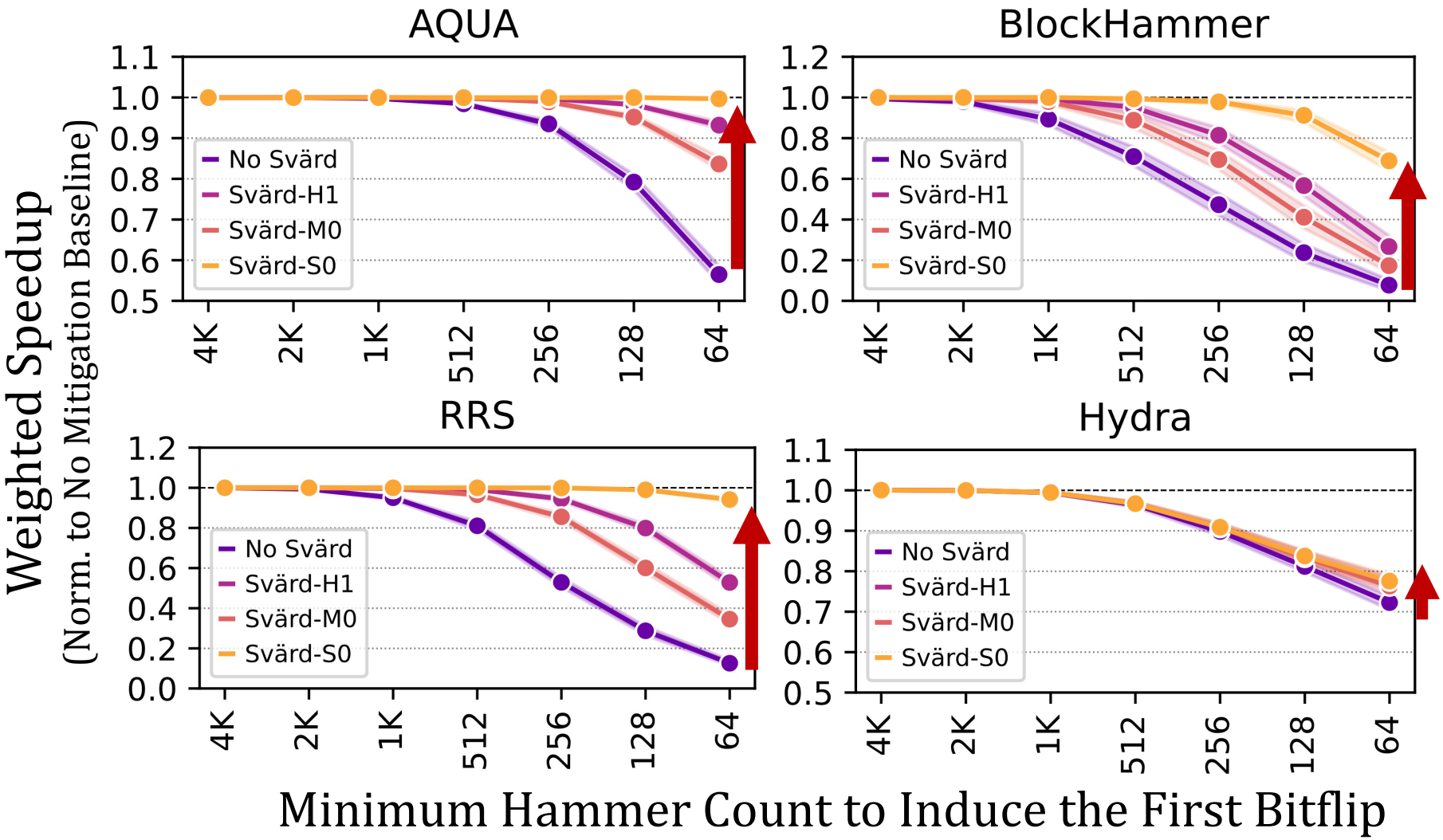
- Integrated with **AQUA, BlockHammer, PARA, Hydra,** and **RRS**

- **HC_{first}**: {4K, 2K, 1K, 512, 256, 128, 64} hammers
  Minimum **hammer count** needed to induce **the first bitflip**

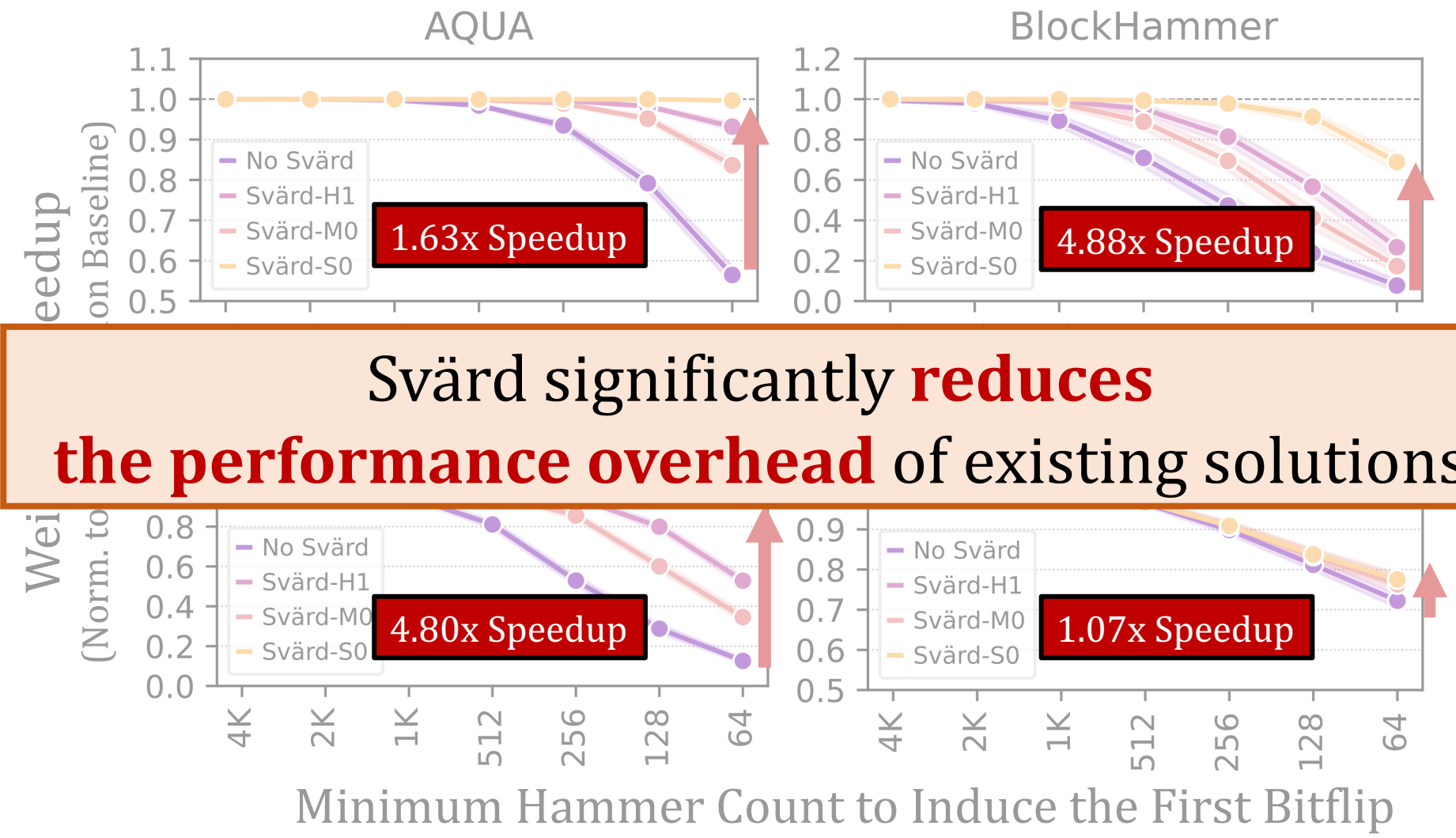
Implications on Future Solutions



Implications on Future Solutions



Implications on Future Solutions



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

Spatial Variation-Aware Read Disturbance Defenses

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

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

- **Svärd: Spatial Variation-Aware Read Disturbance Defenses**
  - **Dynamically tunes** a solution's aggressiveness (e.g., perform more/less refresh) to the **victim row's vulnerability** to DRAM read disturbance
  - Implemented either in **the memory controller** or in **the DRAM chip**

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

Svärd may present itself to any worthy read disturbance solution

Enabling Efficient and Scalable Solutions

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.

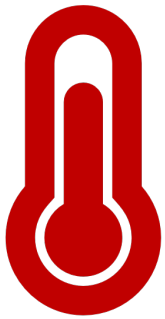
In this paper, we tackle these shortcomings by leveraging the spatial variation in read disturbance across different memory locations in real DRAM chips. To do so, we 1) present the

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

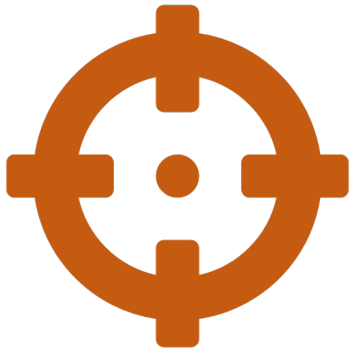
My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns



Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

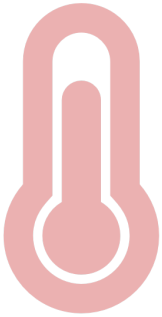
Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actions

My Dissertation Works

- A deeper look into DRAM read disturbance



Temperature

Memory access patterns

Victim cell's physical location

Voltage

- Solutions to DRAM read disturbance

Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actions

Current and Future Challenges


Reliability


Performance


Fairness


Energy Efficiency

While the memory systems

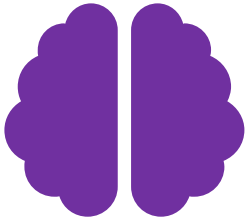
1. **scale-up and are shared** across many users (e.g., disaggregated memory systems)

2. **scale-down** in manufacturing technology node size

3. support **processing near/using memory**

Future Research for Better Memory Systems

Deeper Understanding of
Physics and Vulnerabilities



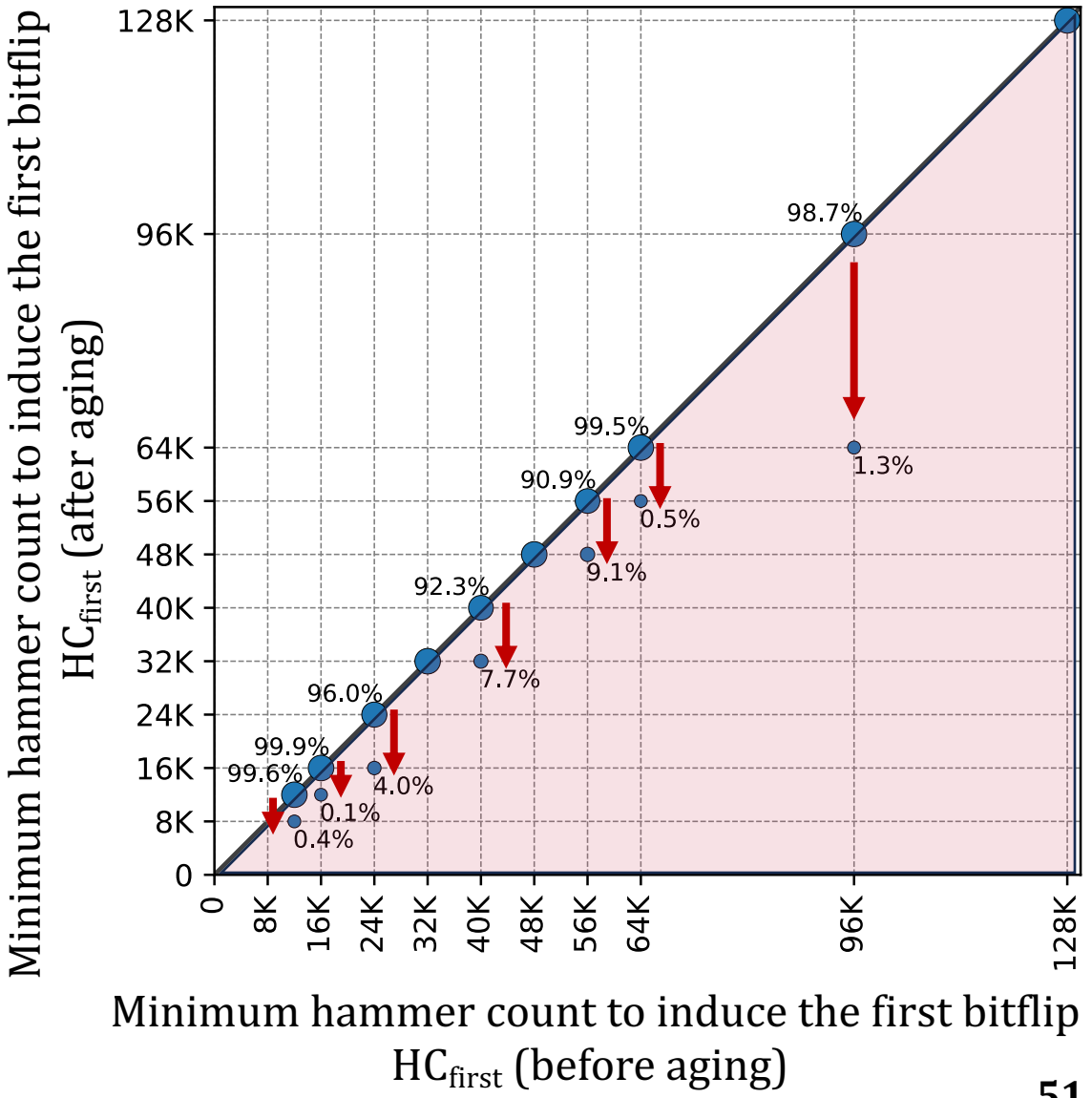
Flexible and Intelligent Memory
Chips, Interfaces, Controllers

Cross-Layer
Communication

Deeper Understanding of Physics and Vulnerabilities

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

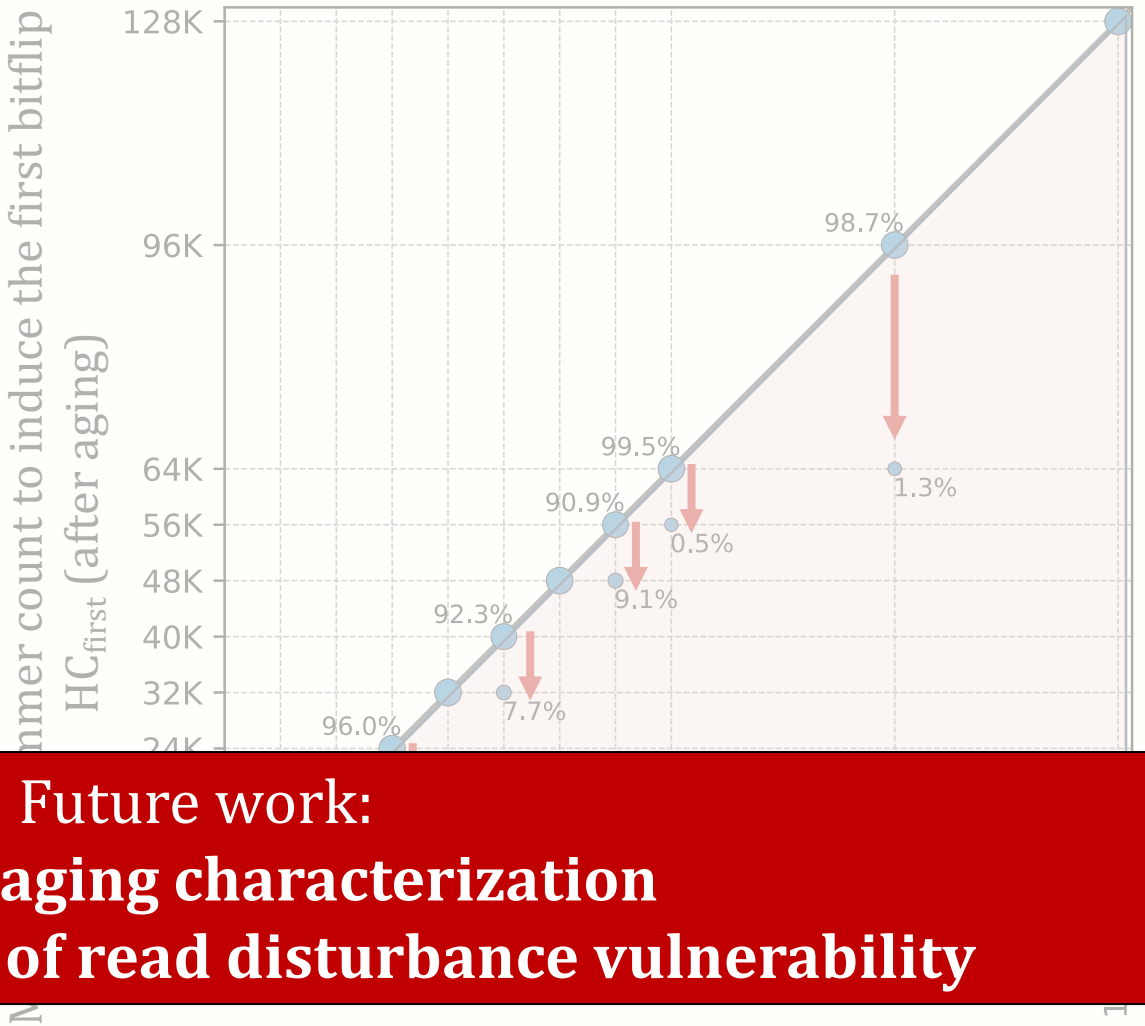
Aging can lead to read disturbance bitflips at **smaller** hammer counts



Deeper Understanding of Physics and Vulnerabilities

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

Aging can lead to read disturbance bitflips at **smaller** hammer counts



Future work:
rigorous aging characterization
and **online profiling of read disturbance vulnerability**

Deeper Understanding of Physics and Vulnerabilities

- The effect of **aging**

- **Interactions** across different error mechanisms
  - RowHammer
  - RowPress
  - Data retention time errors
  - Variable retention time
  - ...

Deeper Understanding of Physics and Vulnerabilities

- The effect of **aging**
- **Interactions** across different error mechanisms
- What is **the worst-case**?
  - Temperature
  - Data pattern
  - Memory access pattern
  - Spatial variation
  - Voltage

What is **the worst-case** considering all **these sensitivities**?

What is **the minimum hammer count** to induce a read disturbance bitflip?

Deeper Understanding of Physics and Vulnerabilities

- The effect of **aging**
- **Interactions** across different error mechanisms
- What is **the worst-case**?

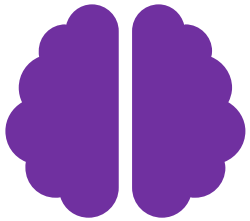
How reliable are our DRAM chips?

How reliable will our DRAM chips be tomorrow?

We **do not** know! This is an **open research problem**

Future Research for Better Memory Systems

Deeper Understanding of
Physics and Vulnerabilities



Flexible and Intelligent Memory
Chips, Interfaces, Controllers

Cross-Layer
Communication

Flexible and Intelligent Chips, Interfaces, Controllers

- **In-field patching** is necessary

DRAM read disturbance solution is here

Configuration

DRAM chip is here

Reconfiguration is needed

+ add more hardware counters
+ increase metadata cache capacity

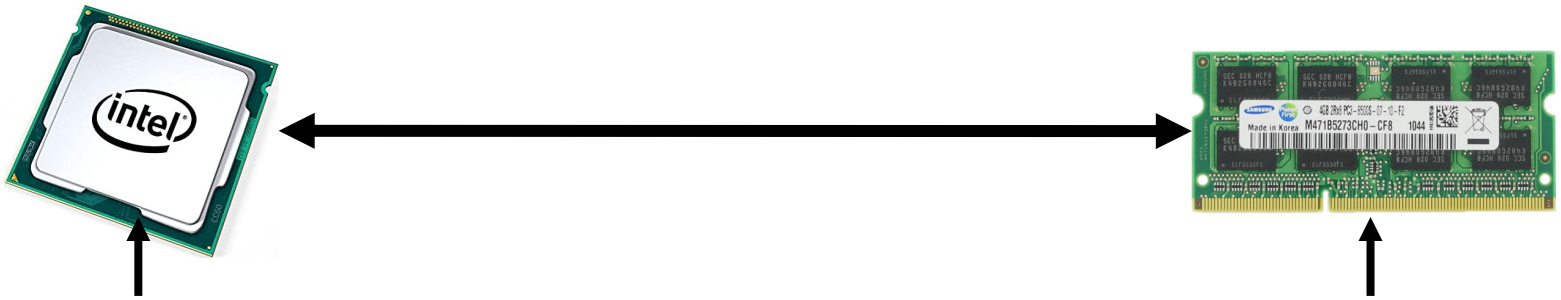
DRAM module can be replaced

Aging might change the chip's characteristics

Deployed solutions should be patchable in field

Flexible and Intelligent Chips, Interfaces, Controllers

- **In-field patching** is necessary
- Interfaces should be **more flexible**



Memory controller decides what should be done when

DRAM chip has read disturbance solution inside (tracking+prevention)

- The memory controller should provide the DRAM chip with **necessary time window** to perform **preventive actions (e.g., refreshing rows)**
- The memory controller **does not have** the tracking information
- Communicating is **not straightforward** due to strict communication protocol

A more flexible interface is necessary

Flexible and Intelligent Chips, Interfaces, Controllers

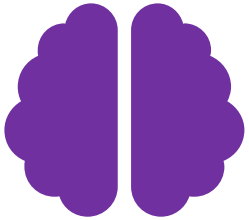
- **In-field patching** is necessary
- Interfaces should be **more flexible**
- Memory controllers should be **more intelligent** in detecting **malicious activity**

- DRAM chips become **more and more vulnerable** to RowHammer **and RowPress**
- **Key Insight:**
  - **A thousand activations** are enough **to induce bitflips**
  - Benign applications **perform as many activations**
- **Problem:** DRAM read disturbance solutions are getting **prohibitively expensive**
- **Research Question:** How to identify malicious threads/processes/users?
- More **intelligent detection** mechanisms are needed → AI can play an important role
- The **memory controller** observes all memory accesses → has the ground truth data

More intelligent memory controllers can help

Future Research for Better Memory Systems

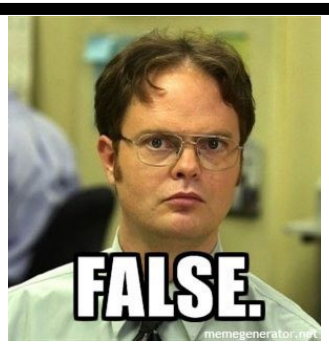
Deeper Understanding of
Physics and Vulnerabilities



Flexible and Intelligent Memory
Chips, Interfaces, Controllers

Cross-Layer
Communication

Cross-Layer Communication

		Detection	Mitigation
Software	• Memory allocations • Memory access patterns • Control flow patterns • Time / power measurements		++
uArch	• Memory request scheduling • Speculative execution • Prefetching, branch prediction • Power management	+	+
Device	• Bitflips occur • Memory isolation is broken	++	~

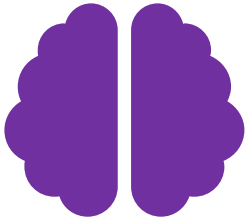
Cross-Layer Communication

		Detection	Mitigation
Software	• Memory allocations • Memory access patterns • Control flow patterns • Time / power measurements		++
Device	• Bitflips occur • Memory isolation is broken	++	~

Cross-layer communication is crucial going forward

Future Research for Better Memory Systems

Deeper Understanding of
Physics and Vulnerabilities



Flexible and Intelligent Memory
Chips, Interfaces, Controllers

Cross-Layer
Communication

Enabling Efficient and Scalable Read Disturbance Mitigation

via New Experimental Insights into Modern Memory Chips

agyaglikci.github.io

Abdullah Giray Yaglikci

agyaglikci@gmail.com

https://agyaglikci.github.io

7 March 2024

University of Glasgow

safari.ethz.ch

SAFARI

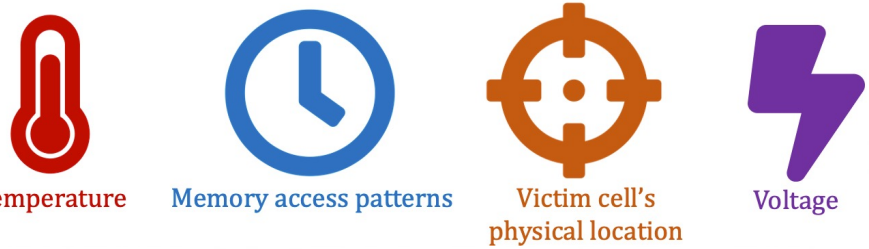
ETH zürich

A Deeper Look into DRAM Read Disturbance

SAFARI Live Seminars in Computer Architecture

A Deeper Look into RowHammer's Characteristics in Real Modern DRAM Chips

- A deeper look into RowHammer's characteristics



SPEAKER
Abdullah Giray Yağlıkçı
SAFARI Research Group, ETH Zurich

ETH zürich SAFARI SAFARI Research Group

JAN 17, 2024 5:00PM CET

https://www.youtube.com/live/CRtm1es4n3o?si=8N5zB6e_RUc5Ejl8

Solutions to DRAM Read Disturbance

SAFARI Live Seminars in Computer Architecture

Efficiently and Scalably Mitigating RowHammer in Modern and Future DRAM-Based Memory Systems

Leveraging Heterogeneity

Throttling Unsafe Accesses

Parallelizing Preventive Actions

SPEAKER

Abdullah Giray Yağlıkçı

SAFARI Research Group, ETH Zurich

ETH zürich SAFARI SAFARI Research Group

JAN 22, 2024 5:00PM CET

SAFARI https://www.youtube.com/live/YQwRYWpCsk0?si=jXPueMHb5wgs69-q

Enabling Efficient and Scalable Read Disturbance Mitigation via New Experimental Insights into Modern Memory Chips

Backup Slides

Abdullah Giray Yaglikci

agyaglikci@gmail.com

https://agyaglikci.github.io

7 March 2024

University of Glasgow

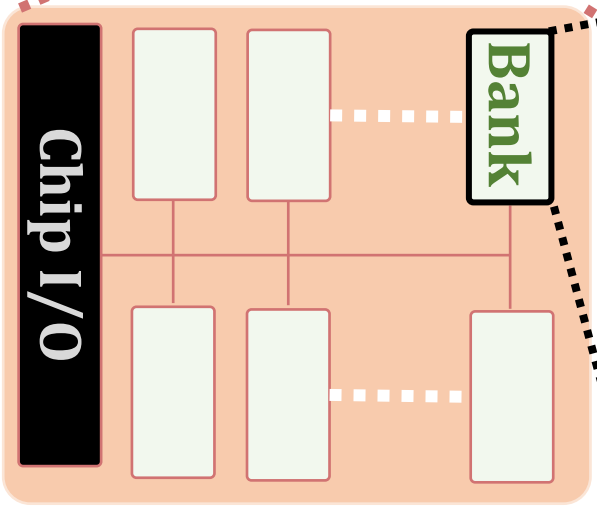
agyaglikci.github.io

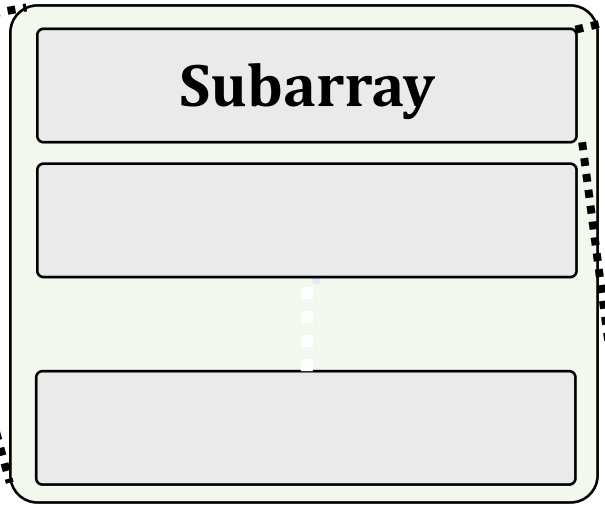
safari.ethz.ch

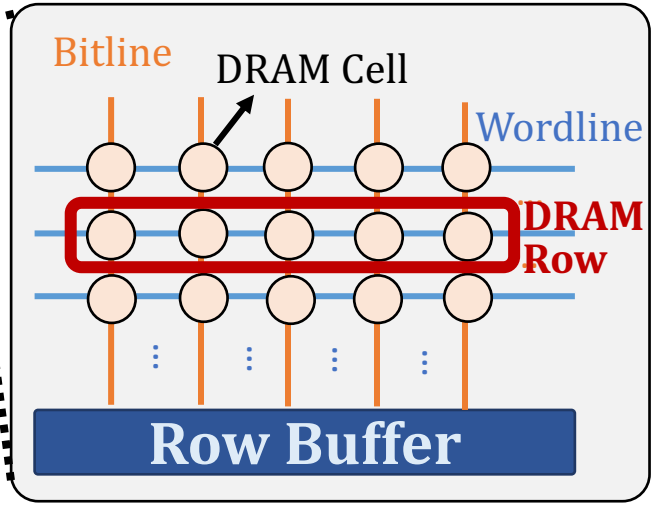
SAFARI

ETH zürich

DRAM Organization

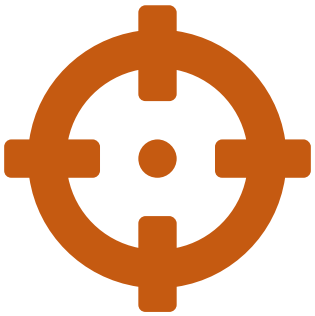






DRAM Chip **DRAM Bank** **DRAM Subarray**

Key Takeaways from Spatial Variation Analysis



In-Chip Variations

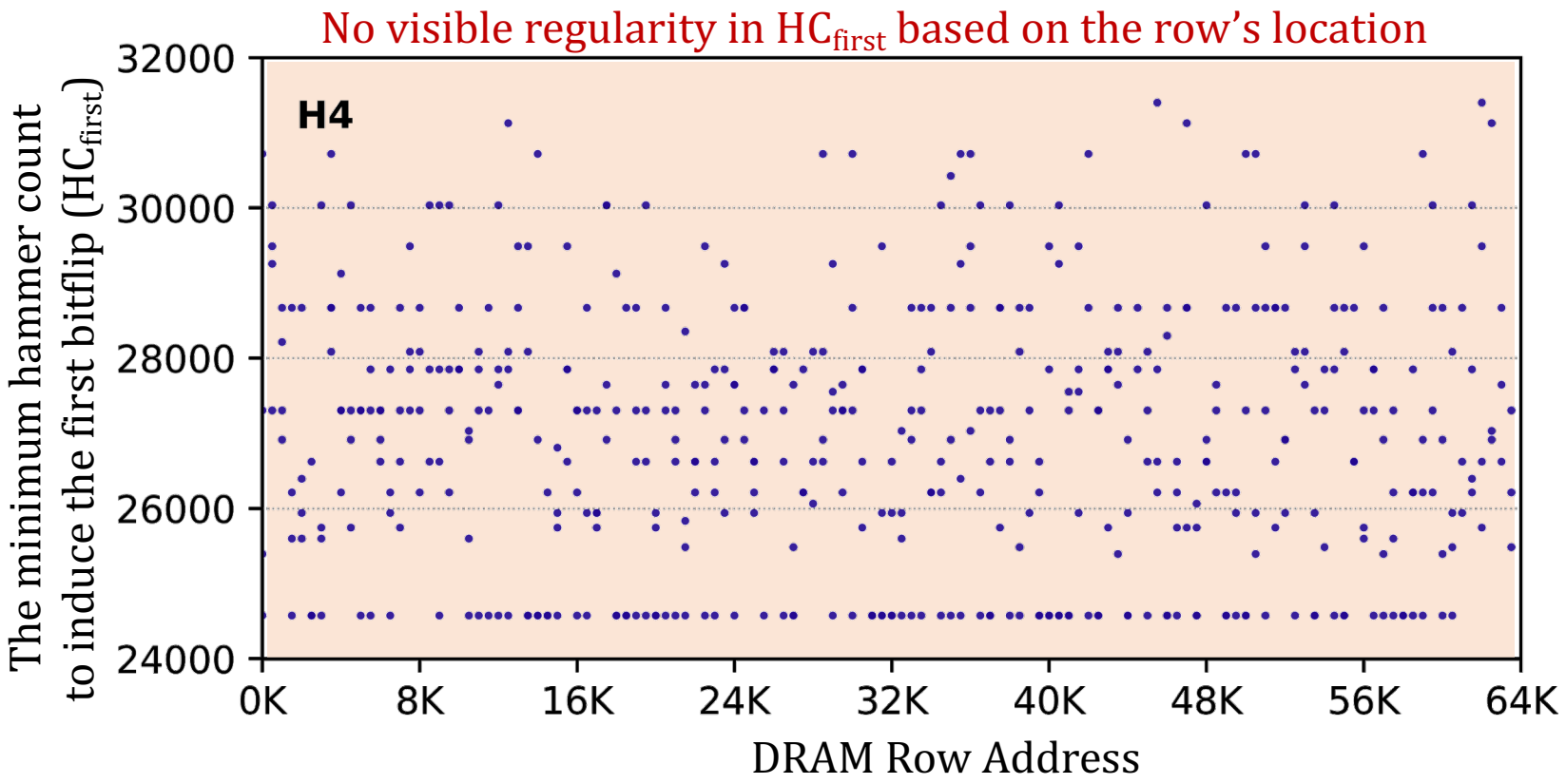
Key Takeaway 1

RowHammer vulnerability **significantly varies** across DRAM rows and columns due to **design** and **manufacturing-process**

Key Takeaway 2

Minimum hammer count to induce the first bitflip (HC_{first}) significantly varies **across rows in a subarray** but **not as much across subarrays**

Regularity in Spatial Variation of 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