A Deeper Look into RowHammer's Sensitivities

Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses

Lois Orosa **Abdullah Giray Yağlıkçı**

Haocong Luo Ataberk Olgun Jisung Park

Hasan Hassan Minesh Patel Jeremie S. Kim Onur Mutlu

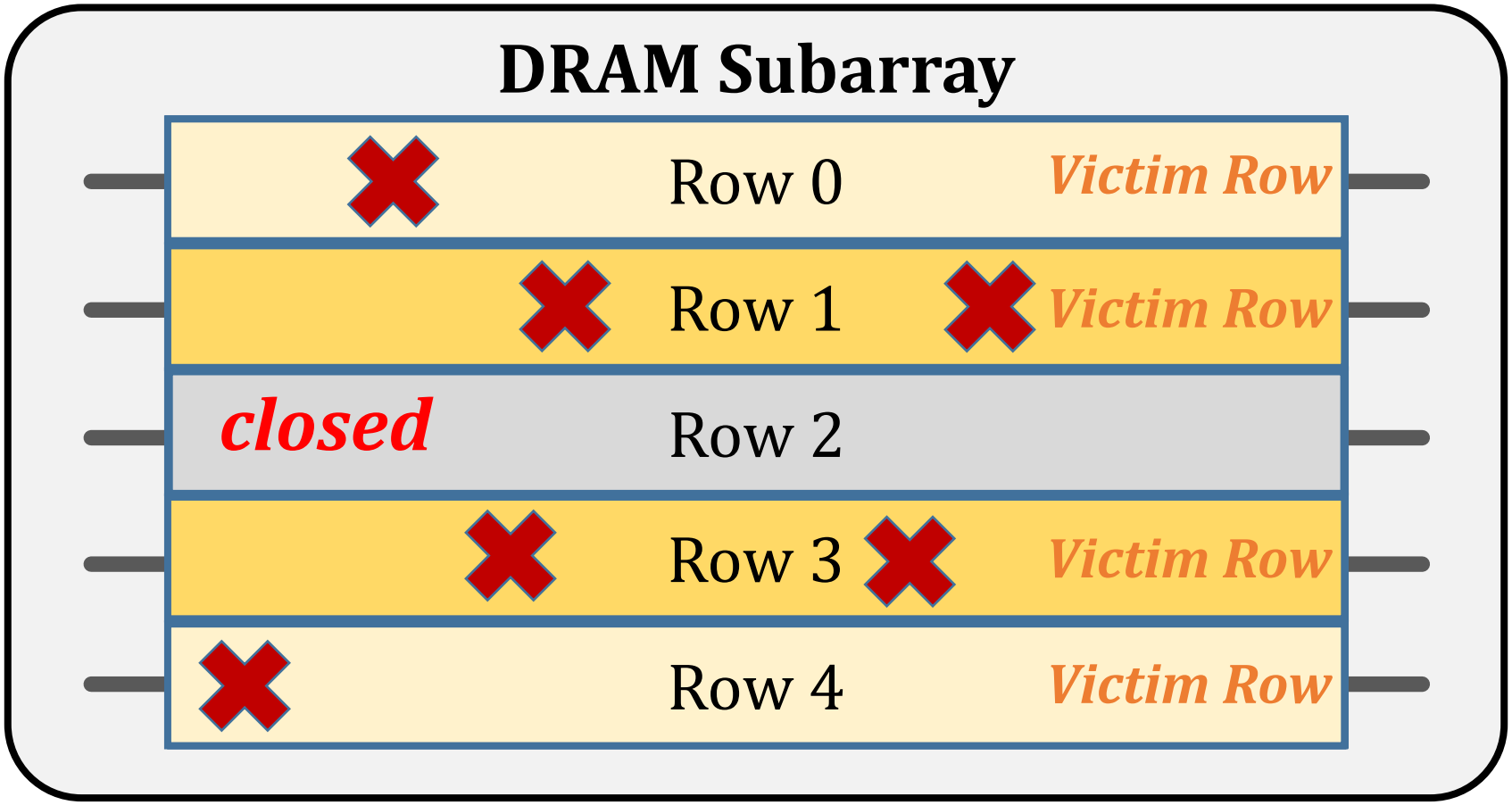
SAFARI

ETH zürich

TOBB ETÜ

University of Economics & Technology

The RowHammer Vulnerability



Repeatedly **opening** (activating) and **closing** (precharging) a DRAM row causes **RowHammer bit flips** in nearby cells

Executive Summary

- **Motivation**: Understanding RowHammer enables designing **effective and efficient solutions**, but **no rigorous study** demonstrates how vulnerability varies under different conditions

- **Goal**: Provide insights into **three fundamental properties** of RowHammer that can be leveraged to design **more effective and efficient attacks and defenses**
  1) DRAM chip **temperature**
  2) The time that an **aggressor row stays active**
  3) Victim DRAM cell's **physical location**

- **Experimental study**: **272 DRAM chips** from **four major manufacturers**

- **Key Results:** A RowHammer bit flip is **more likely to occur**
  1) in **a bounded range of temperature**
  2) if the aggressor row is **active for longer time**
  3) in **certain physical regions** of the DRAM module under attack

- **Conclusion:** Our novel observations can inspire and aid future work
  - Craft **more effective attacks**
  - Design **more effective and efficient defenses**

Key Takeaways from Temperature Analysis

Key Takeaway 1

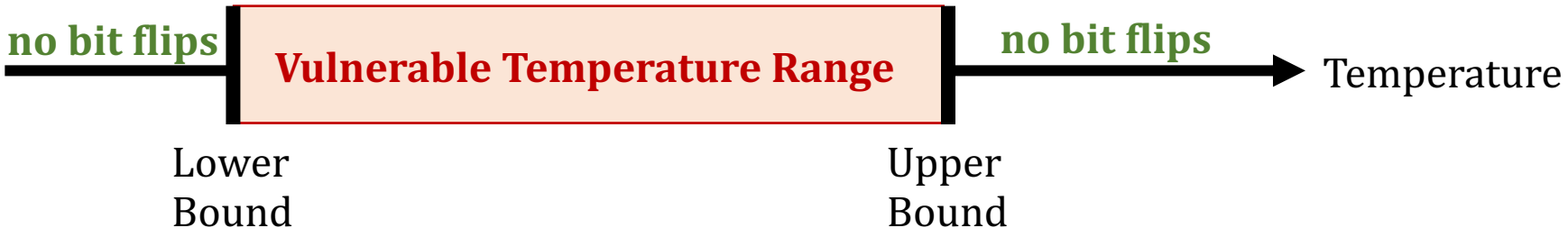
To ensure that a DRAM cell is **not vulnerable** to RowHammer, we **must characterize** the cell at **all operating temperatures**

Key Takeaway 2

RowHammer vulnerability **tends to worsen as DRAM temperature increases**

However, **individual DRAM rows** can exhibit behavior **different from the dominant trend**

Impact of Temperature on DRAM Cells



The fraction of vulnerable DRAM cells, experiencing bit flips **at all temperature levels** within their vulnerable temperature range

Mfr. A	Mfr. B	Mfr. C	Mfr. D
99.1%	98.9%	98.0%	99.2%

OBSERVATION 1

Most DRAM cells are vulnerable to RowHammer throughout **a continuous temperature range**

Impact of Temperature on DRAM Cells

OBSERVATION 2

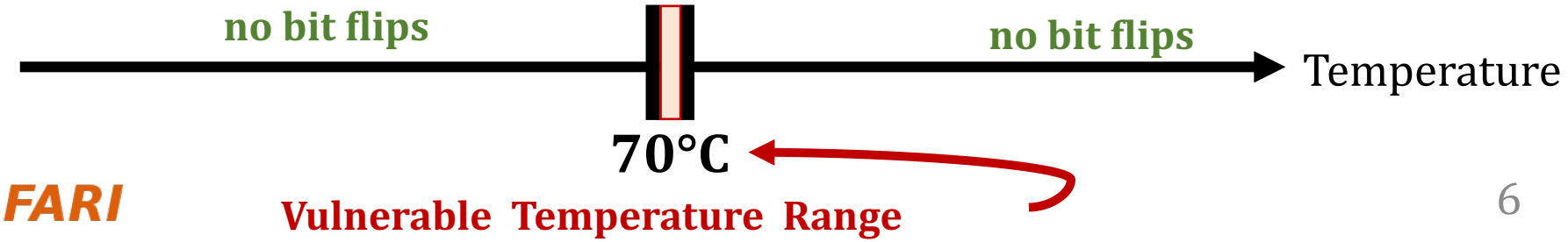
A **significant fraction** of vulnerable DRAM cells exhibit bit flips at **all tested temperatures**

29.8% of the cells **in Mfr. D** experience bit flips **at all tested temperatures**

OBSERVATION 3

A **small fraction** of all vulnerable DRAM cells are vulnerable to RowHammer **only in a very narrow temperature range**

0.2% of the cells in Mfr. D experience bit flips **only at 70°C**



Key Takeaways from Aggressor Row Active Time Analysis

Key Takeaway 3

As an aggressor row stays **active longer**,
victim DRAM cells become **more vulnerable** to RowHammer

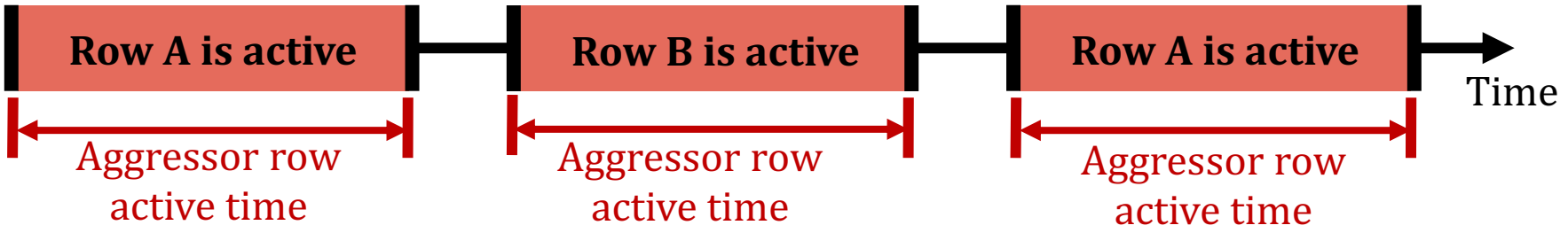
Key Takeaway 4

RowHammer vulnerability of victim cells **decreases**
when the bank is **precharged for a longer time**

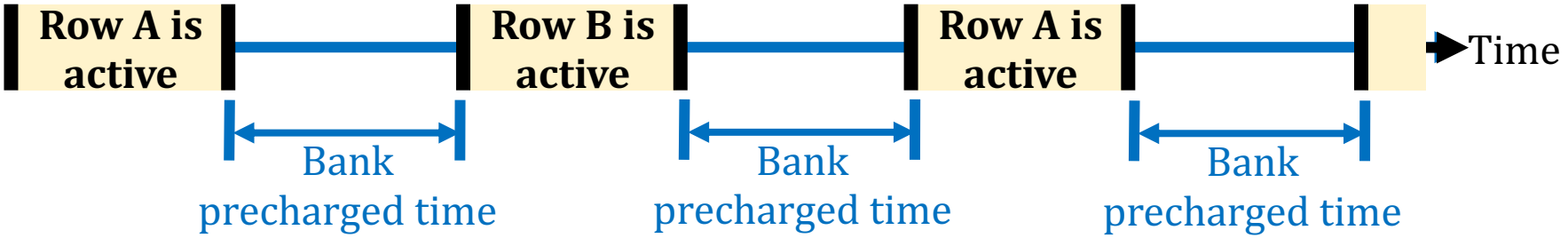
Memory Access Patterns in Aggressor Row Active Time Analysis

- Baseline access pattern:

- Increasing **aggressor row active time**:



- Increasing **bank precharged time**:



Increasing Aggressor Row Active Time

OBSERVATION 8

As the **aggressor row stays active longer**, **more DRAM cells** experience RowHammer bit flips and they experience RowHammer bit flips **at lower activation counts**

[More analysis and observations in the paper]

Key Takeaways from Spatial Variation Analysis

Key Takeaway 5

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

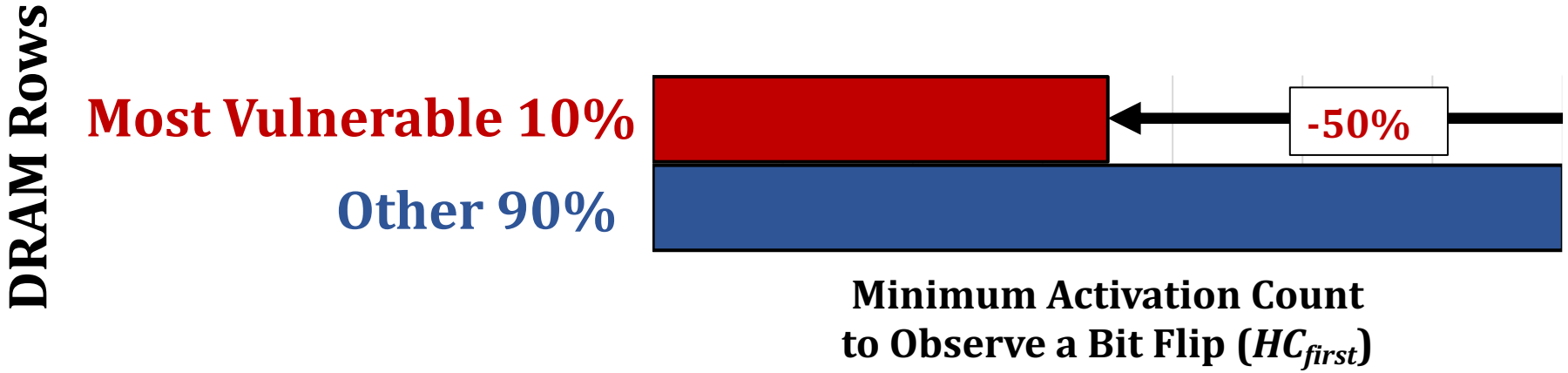
Key Takeaway 6

The distribution of **the minimum activation count to observe bit flips (HC_{first})** exhibits **a diverse set of values in a subarray** but **similar values across subarrays** in the same DRAM module

Spatial Variation across Rows

OBSERVATION 12

A small fraction of DRAM rows are **significantly more vulnerable** to RowHammer than **the vast majority** of the rows



[More analysis and observations in the paper]

Implications on Attacks and Defenses

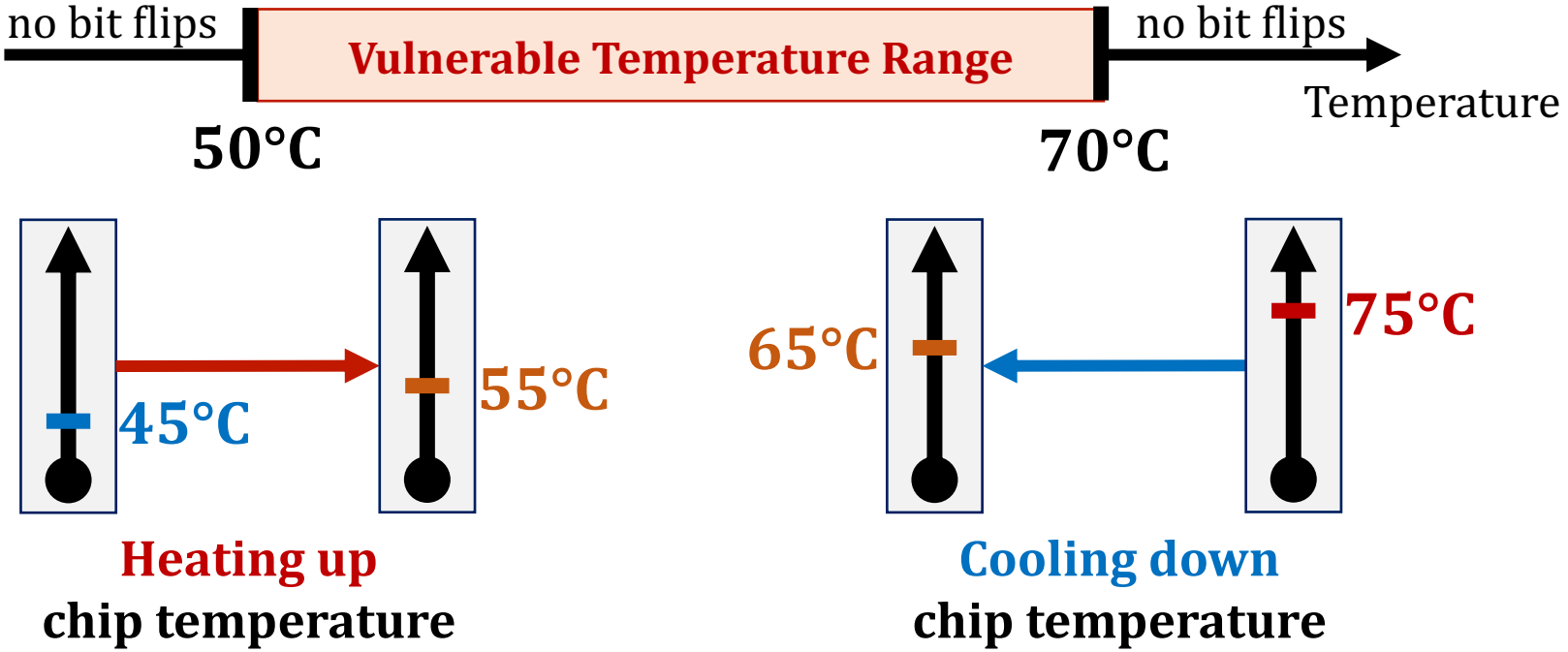
Our observations can be leveraged to craft
more effective RowHammer attacks

Our observations can be leveraged to design
more effective and efficient RowHammer defenses

Attack Improvement:
Making DRAM Cells More Vulnerable

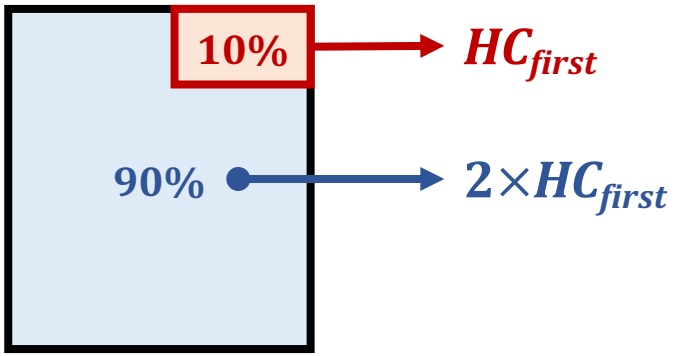
An attacker can **manipulate temperature** to make the cells that store sensitive data **more vulnerable**

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



[More Attack Improvements in the paper]

Defense Improvement:
Leveraging the variation across DRAM rows



Aggressiveness can be reduced:

33% area reduction
for BlockHammer [Yağlıkçı+, HPCA'21]

80% area reduction
for Graphene [Park+, MICRO'20]

[More Defense Improvements in the paper]

Also in the paper

- **More** temperature, aggressor row active time, and spatial variation **analysis**

- **16** total **new observations** and 6 key takeaways

- **3** total **attack improvements**

- **6** total **defense improvements**

A Deeper Look into RowHammer's Sensitivities

Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses

Lois Orosa **Abdullah Giray Yağlıkçı**

Haocong Luo Ataberk Olgun Jisung Park

Hasan Hassan Minesh Patel Jeremie S. Kim Onur Mutlu

SAFARI

ETH zürich

TOBB ETÜ
University of Economics & Technology

A Deeper Look into RowHammer's Sensitivities

Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses

20-min Talk

Lois Orosa **Abdullah Giray Yağlıkçı**

Haocong Luo Ataberk Olgun Jisung Park

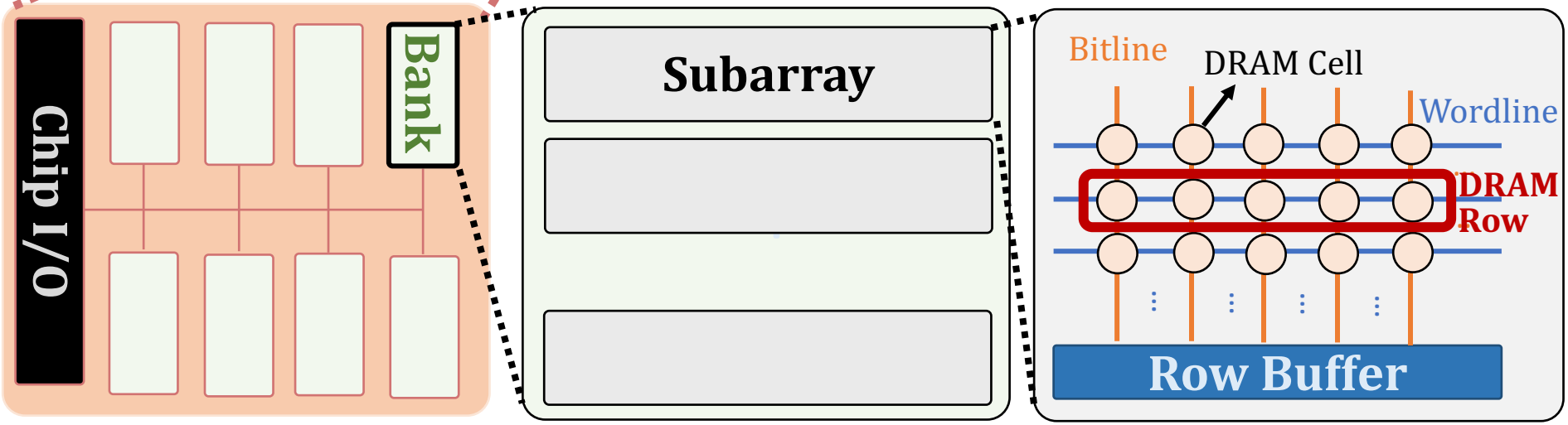
Hasan Hassan Minesh Patel Jeremie S. Kim Onur Mutlu

SAFARI

ETH zürich

TOBB ETÜ
University of Economics & Technology

DRAM Organization

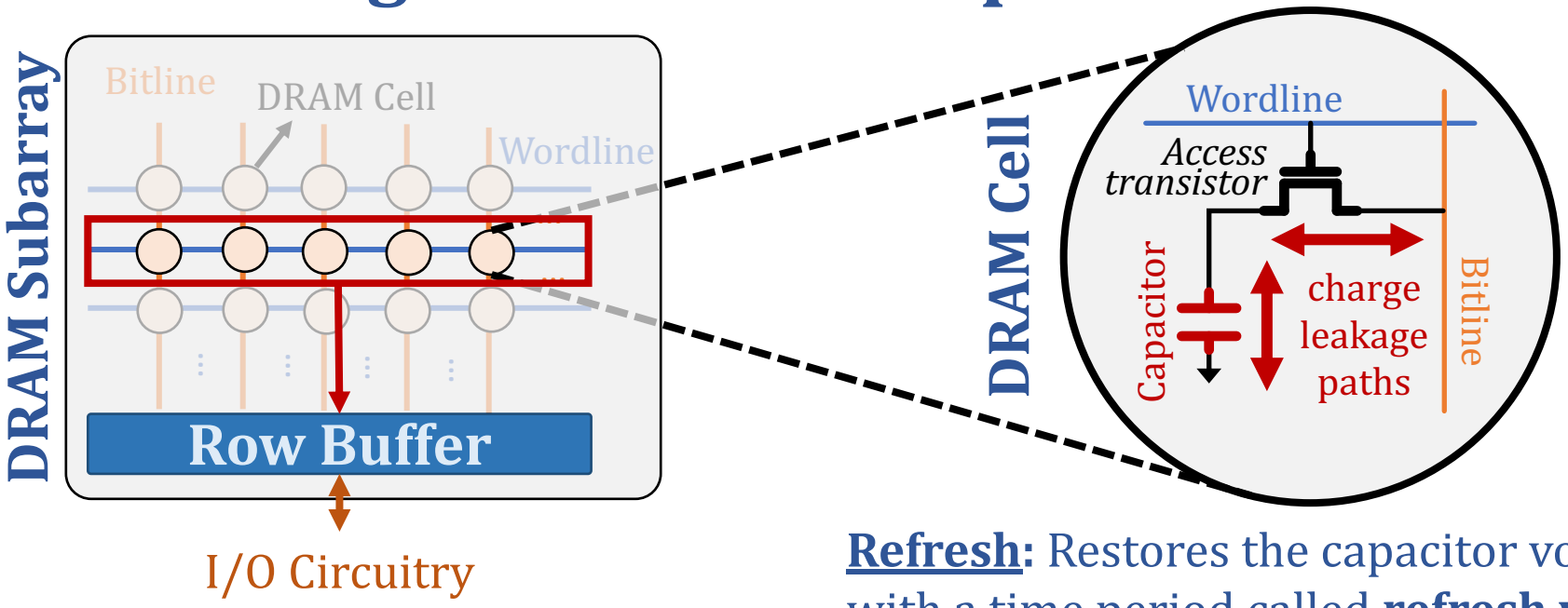


DRAM Chip

DRAM Bank

DRAM Subarray

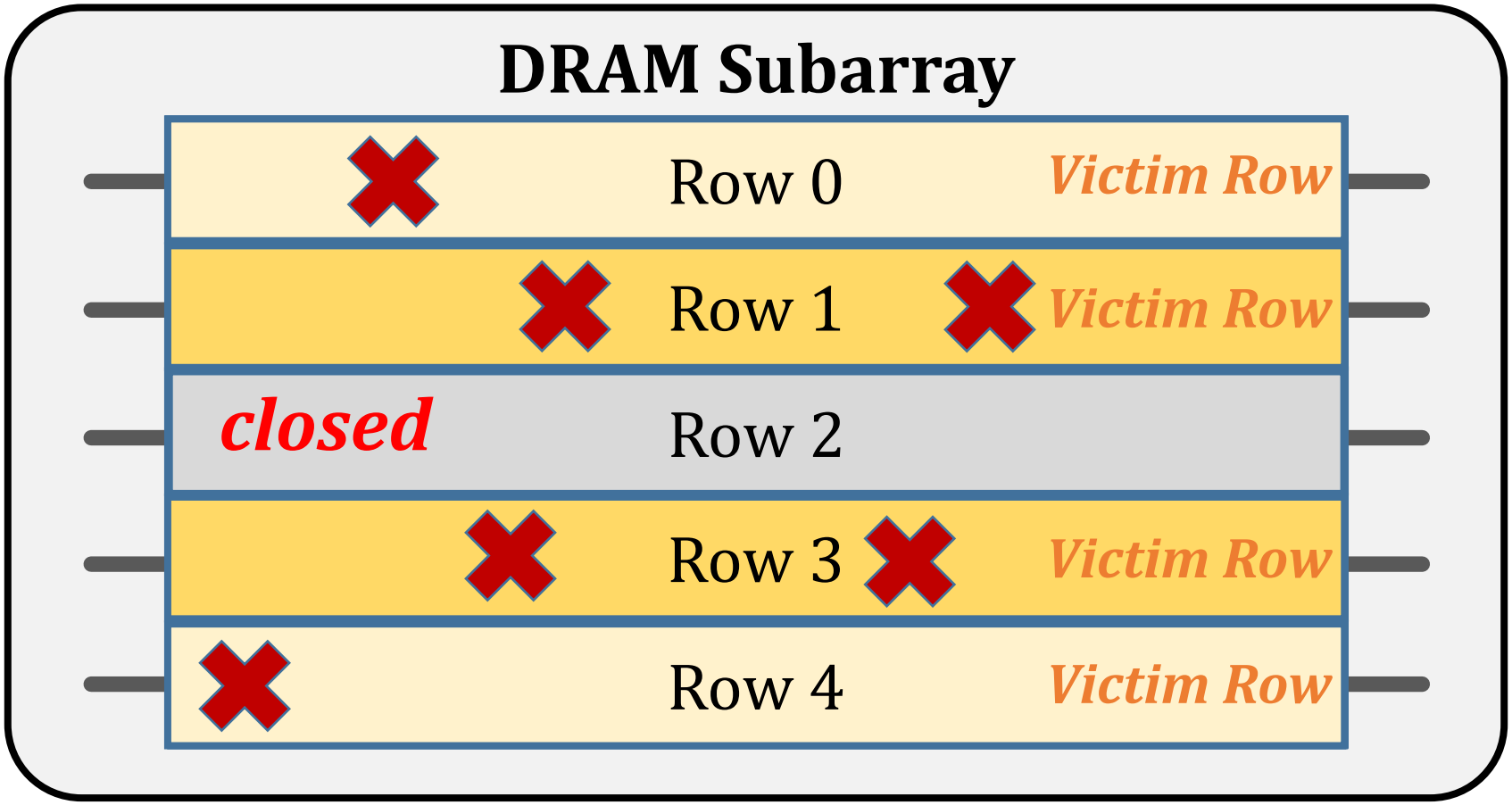
DRAM Organization and Operation



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 bit flips** in nearby cells

Executive Summary

- **Motivation**:
  - Denser DRAM chips are **more vulnerable** to RowHammer
  - Understanding RowHammer enables designing **effective and efficient solutions**, but **no rigorous study** demonstrates how vulnerability varies under different conditions
- **Goal**: Provide insights into **three fundamental properties** of RowHammer that can be leveraged to design **more effective and efficient attacks and defenses**
  1) DRAM chip **temperature**
  2) The time that an **aggressor row stays active**
  3) Victim DRAM cell's **physical location**
- **Experimental study**: **272 DRAM chips** from **four major manufacturers**
- **Key Results:** We provide **6 takeaways** from **16 novel observations**
  A RowHammer bit flip is **more likely to occur**
  1) in **a bounded range of temperature**
  2) if the aggressor row is **active for longer time**
  3) in **certain physical regions** of the DRAM module under attack
- **Conclusion:** Our novel observations can inspire and aid future work
  - Craft **more effective attacks**
  - Design **more effective and efficient defenses**

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

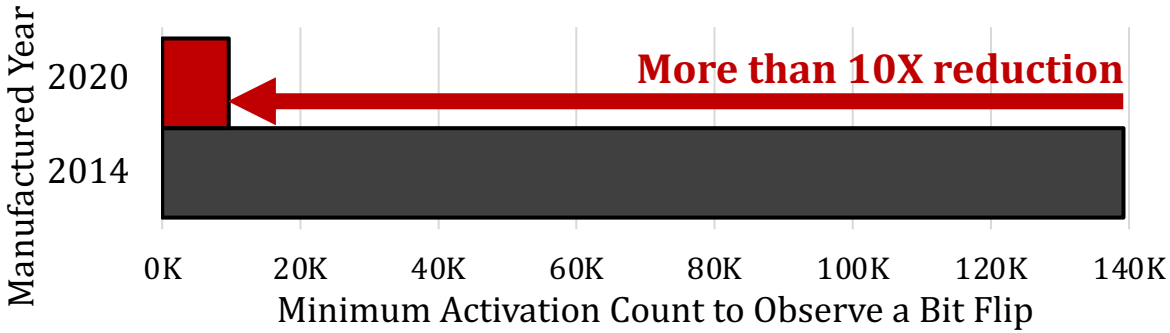
Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Motivation

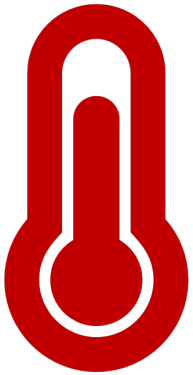


- Defenses are becoming **prohibitively expensive**
- A **deeper understanding** is needed
- **No rigorous experimental study** on fundamental properties of RowHammer to find **effective and efficient** solutions

It is **critical** to gain insights into RowHammer and its **fundamental properties**

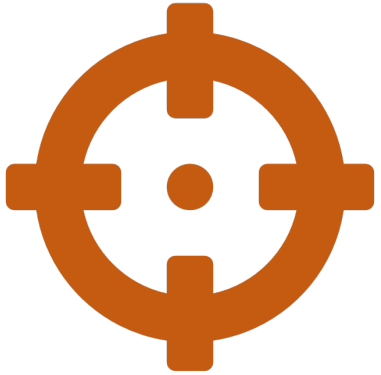
Our Goal

Provide insights into **three fundamental properties**



Temperature

Aggressor Row
Active Time



Victim DRAM Cell's
Physical Location

To find **effective and efficient** attacks and defenses

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

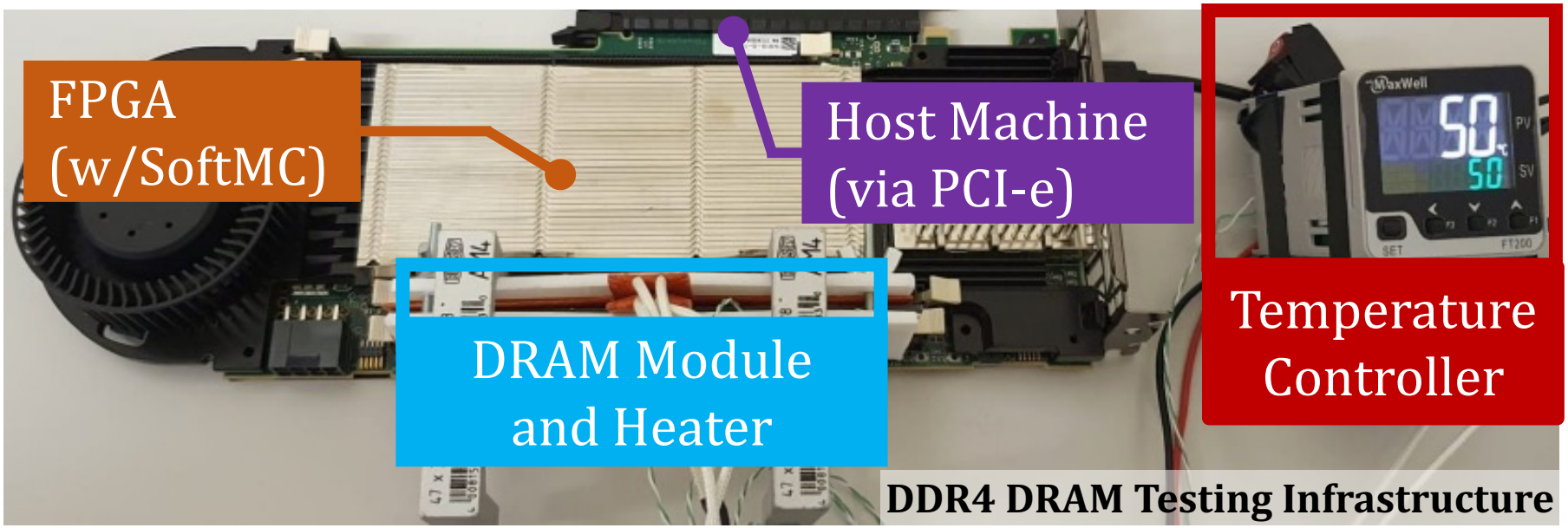
Implications on Attacks and Defenses

Conclusions

DRAM Testing Infrastructures

Two separate testing infrastructures

1. **DDR3:** FPGA-based SoftMC (Xilinx ML605)
2. **DDR4:** FPGA-based SoftMC (Xilinx Virtex UltraScale+ XCU200)



DDR4 DRAM Testing Infrastructure

Fine-grained control over **DRAM commands**, **timing parameters** and **temperature (±0.1°C)**

DRAM Testing Methodology

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

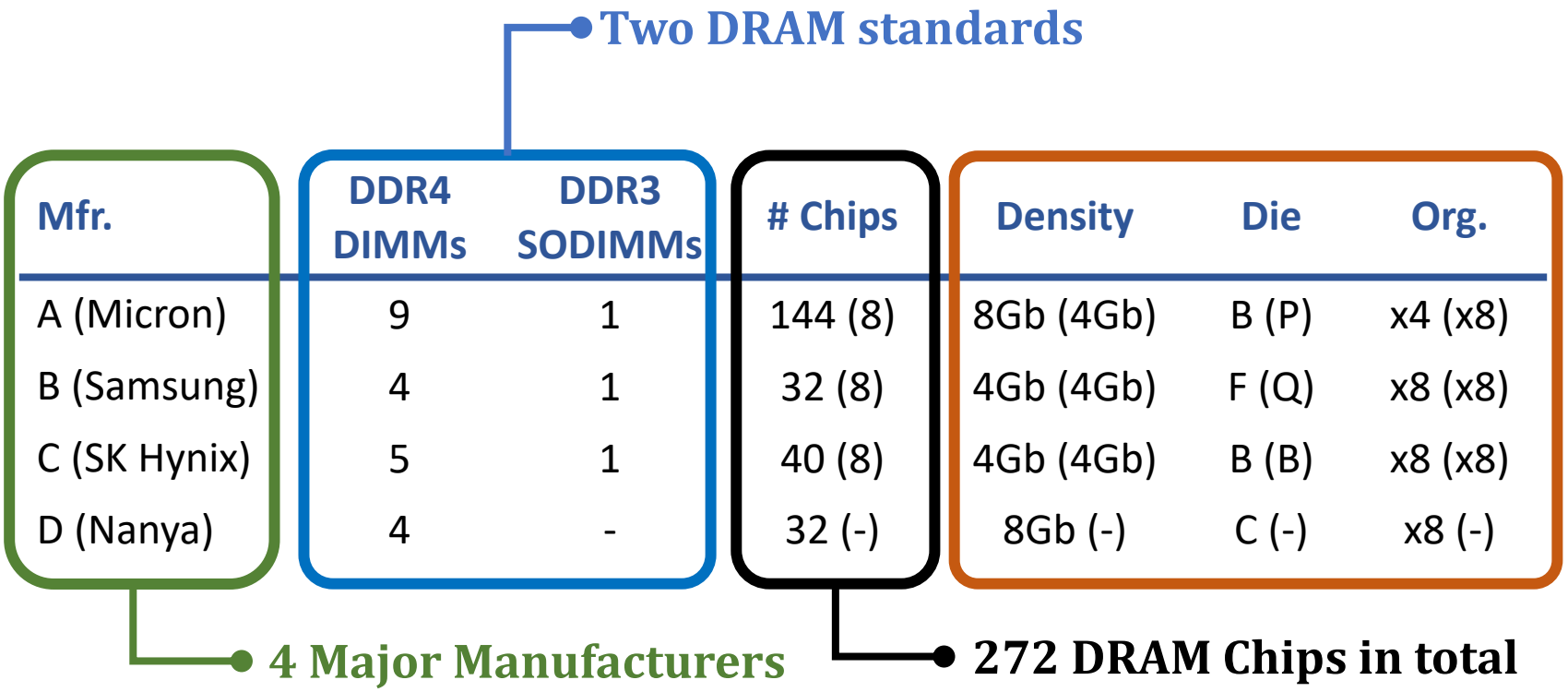
1. Prevent sources of interference during core test loop

- **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

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**

DRAM Chips Tested



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 (-)

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

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Key Takeaways from Temperature Analysis

Key Takeaway 1

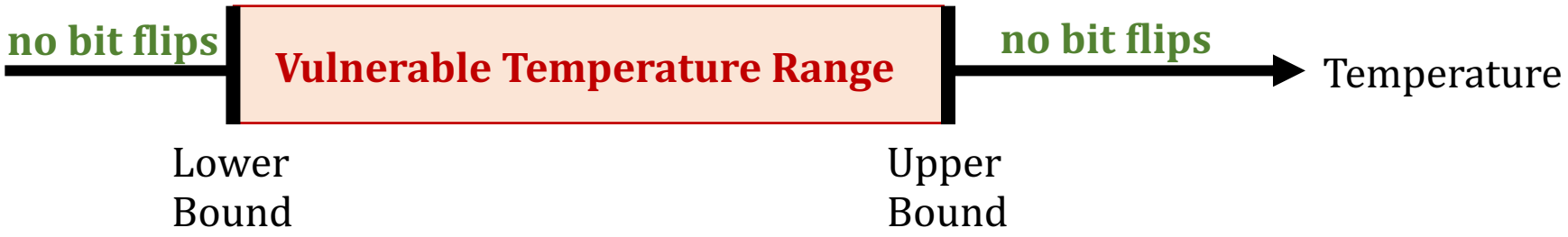
To ensure that a DRAM cell is **not vulnerable** to RowHammer, we **must characterize** the cell at **all operating temperatures**

Key Takeaway 2

RowHammer vulnerability **tends to worsen as DRAM temperature increases**

However, **individual DRAM rows** can exhibit behavior **different from the dominant trend**

Impact of Temperature on DRAM Cells



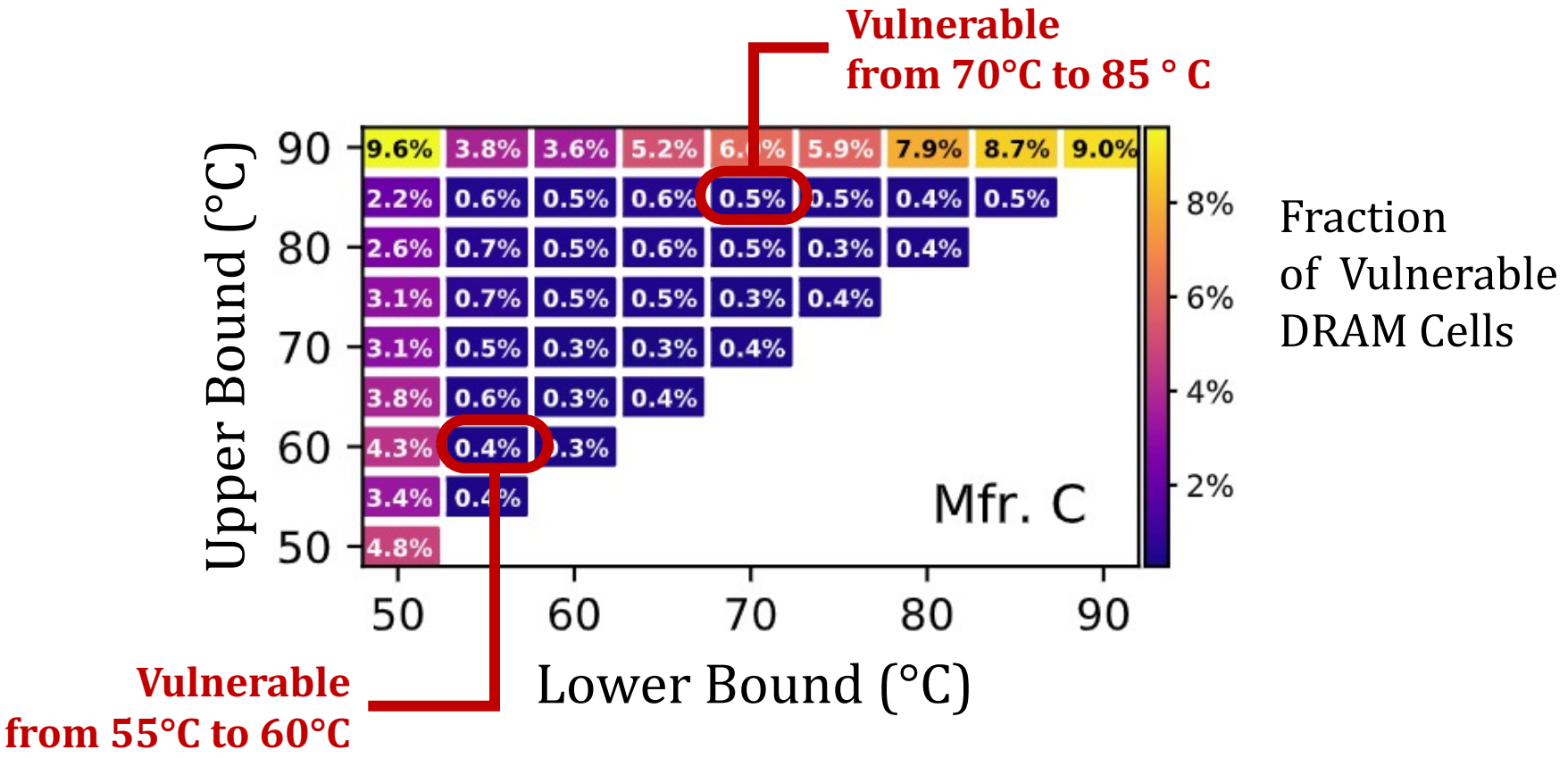
The fraction of vulnerable DRAM cells, experiencing bit flips **at all temperature levels** within their vulnerable temperature range

Mfr. A	Mfr. B	Mfr. C	Mfr. D
99.1%	98.9%	98.0%	99.2%

OBSERVATION 1

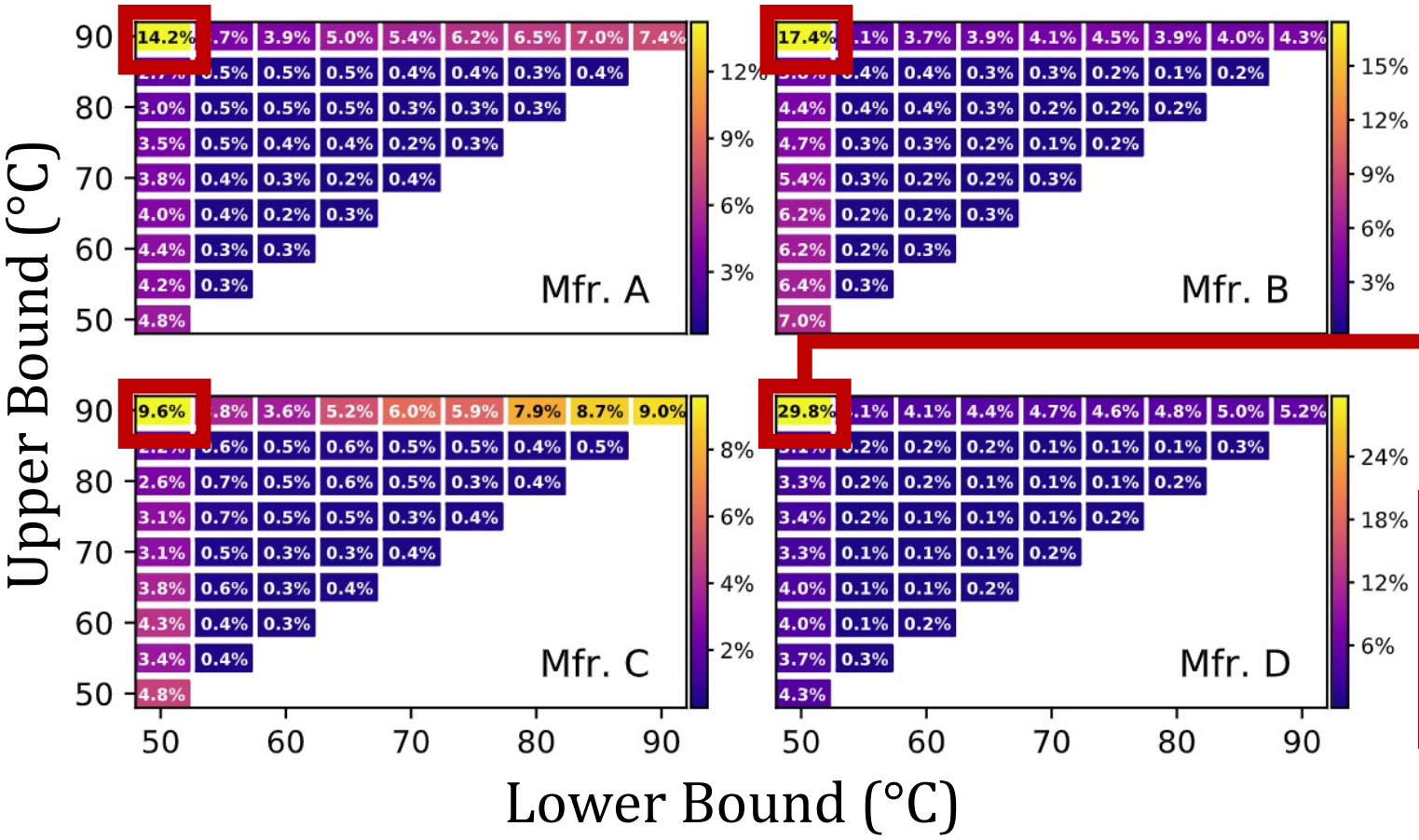
Most DRAM cells are vulnerable to RowHammer throughout **a continuous temperature range**

Impact of Temperature on DRAM Cells



Different DRAM cells are vulnerable to RowHammer
within specific temperature ranges

Impact of Temperature on DRAM Cells

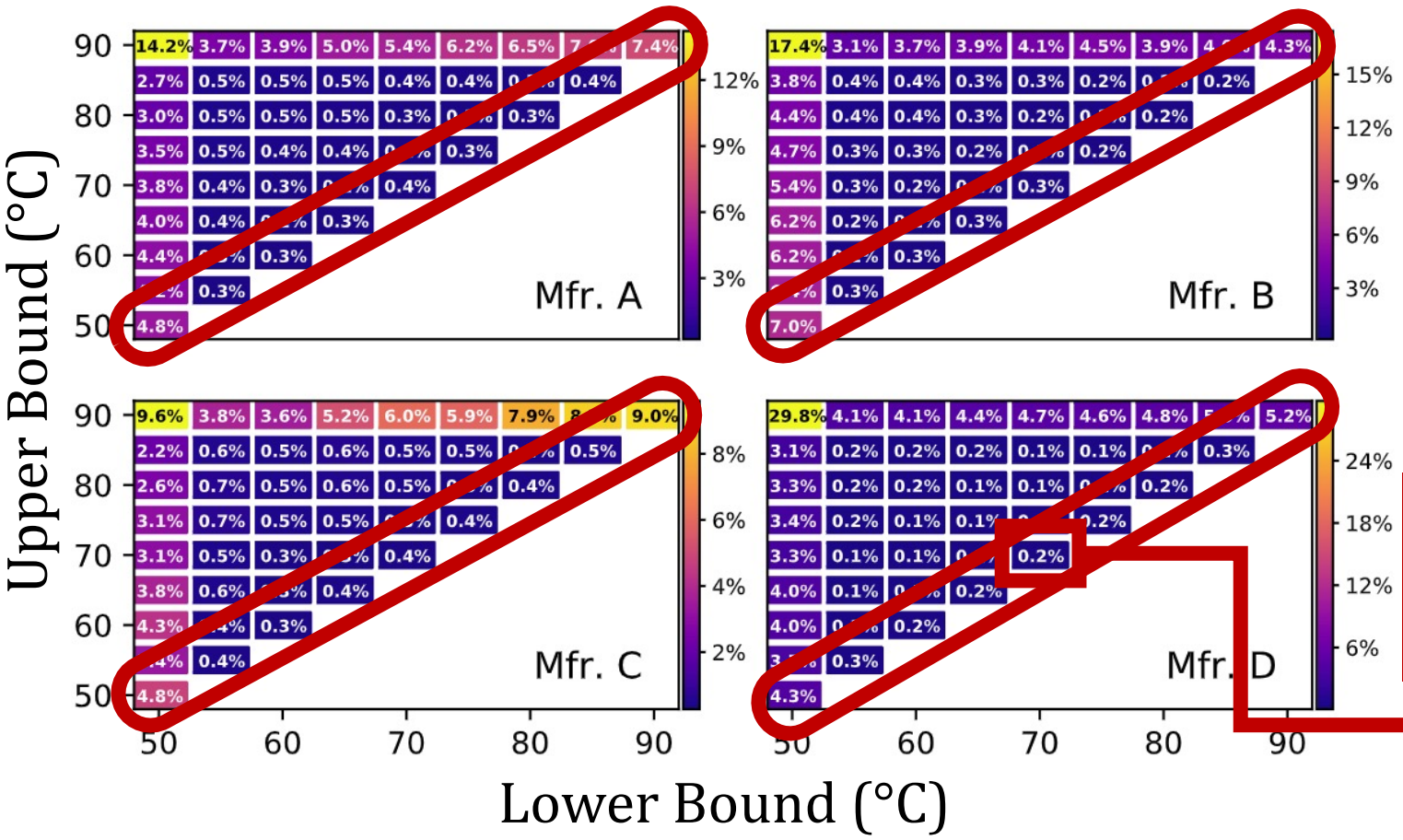


29.8% of the cells experience bit flips **at all tested temperatures**

OBSERVATION 2

A **significant fraction** of vulnerable DRAM cells exhibit bit flips at **all tested temperatures**

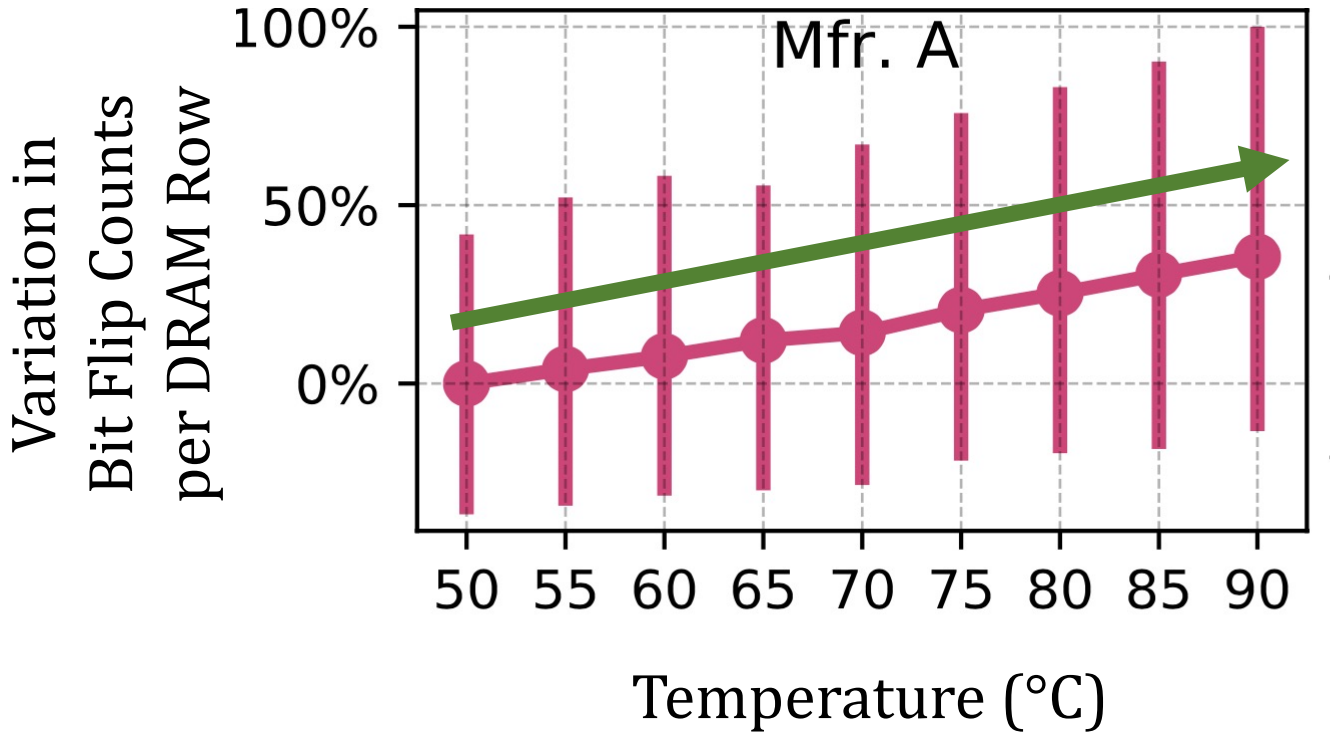
Impact of Temperature on DRAM Cells



OBSERVATION 3

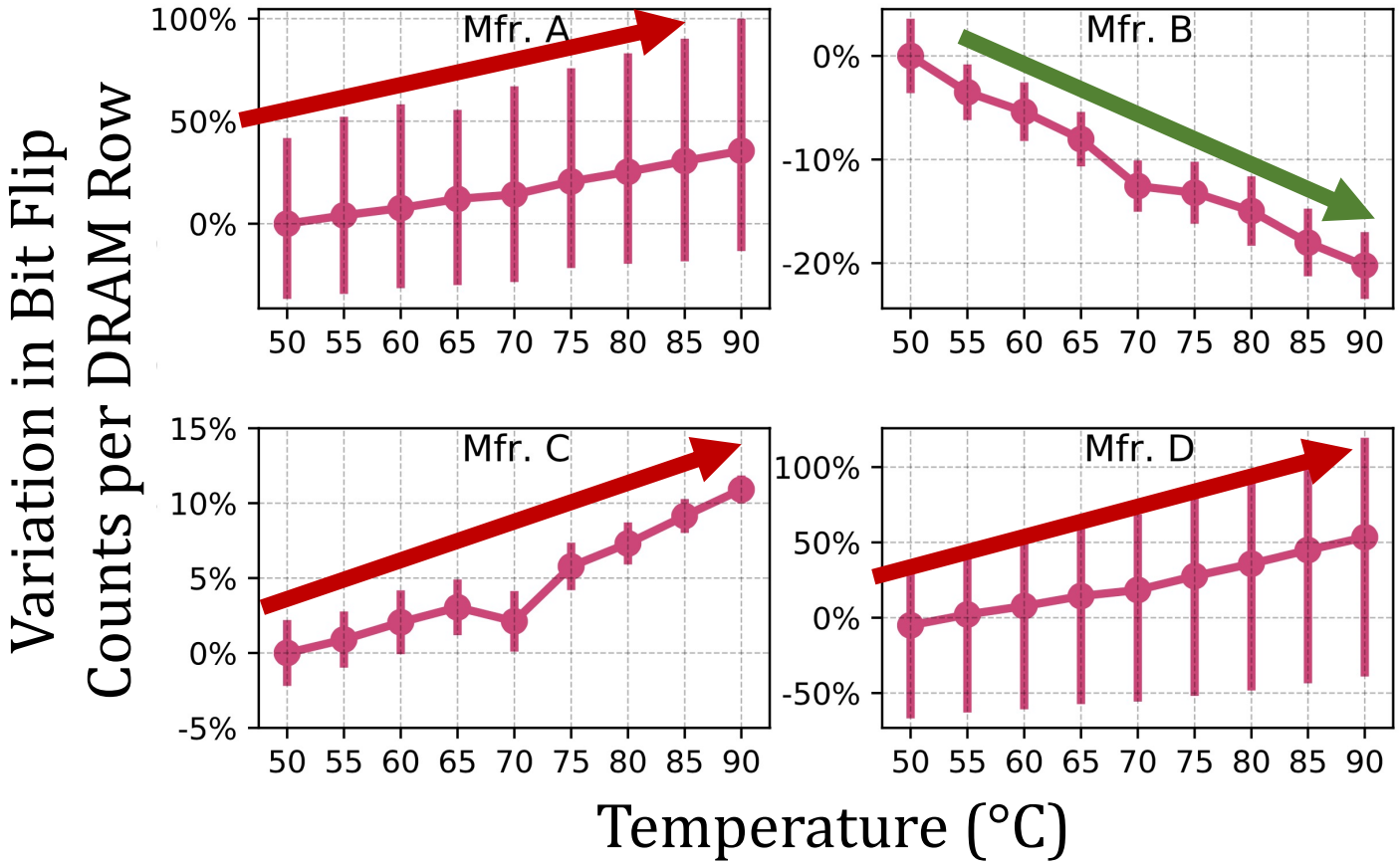
A **small fraction** of all vulnerable DRAM cells are vulnerable to RowHammer **only in a very narrow temperature range**

Impact of Temperature on DRAM Rows



More cells experience bit flips as **temperature increases**

Impact of Temperature on DRAM Rows



OBSERVATION 4

A DRAM row's bit error rate can either **increase** **or** **decrease** **with temperature** depending on the DRAM manufacturer

Also in the Paper

The **minimum activation count** at which a victim row experiences a bit flip (**HC_{first}**) when **temperature changes:**

OBSERVATION 5

DRAM rows can show **either higher or lower HC_{first}** when **temperature increases**

OBSERVATION 6

HC_{first} tends to generally **decrease** as **temperature change (ΔT) increases**

OBSERVATION 7

The **HC_{first} change (ΔHC_{first})** tends to be **larger** as **temperature change (ΔT) increases**

Also in the Paper

The **minimum activation count** at which a victim row experiences a bit flip (HC_{first}) when **temperature changes:**

KEY OBSERVATION 5

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

KEY OBSERVATION 7

The HC_{first} **change** (ΔHC_{first}) tends to be **larger** as **temperature change** (ΔT) **increases**

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Key Takeaways from Aggressor Row Active Time Analysis

Key Takeaway 3

As an aggressor row stays **active longer**,
victim DRAM cells become **more vulnerable** to RowHammer

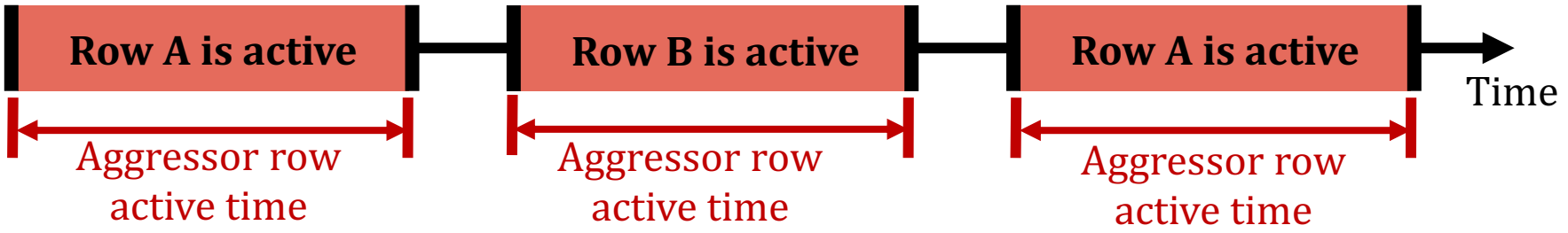
Key Takeaway 4

RowHammer vulnerability of victim cells **decreases**
when the bank is **precharged for a longer time**

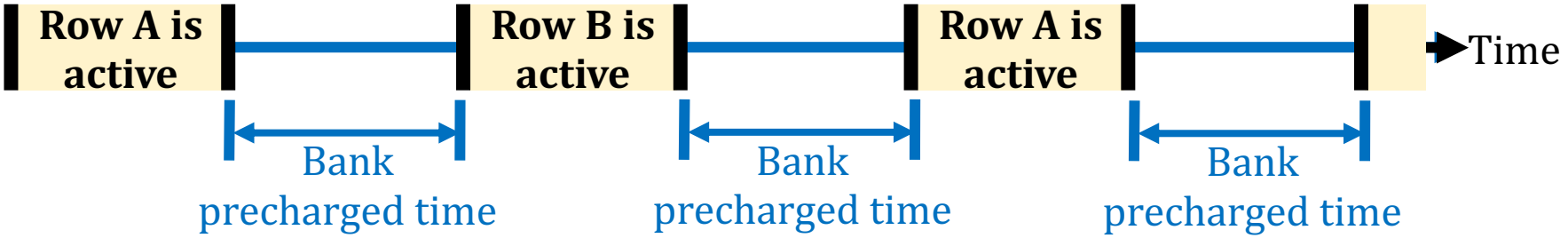
Memory Access Patterns in Aggressor Row Active Time Analysis

- Baseline access pattern:

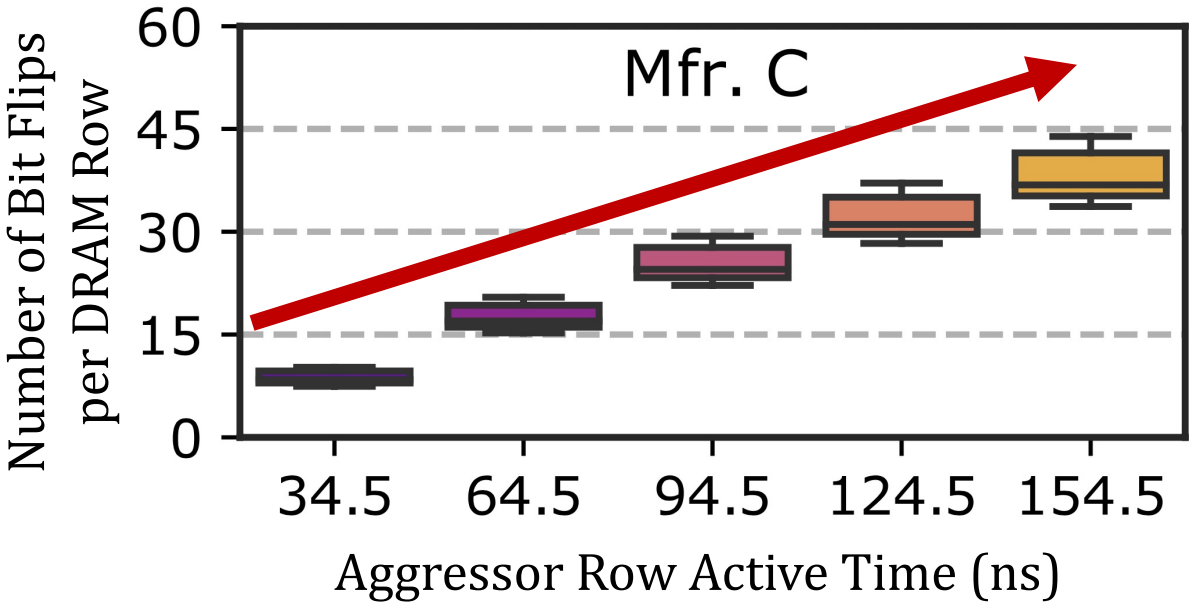
- Increasing **aggressor row active time**:



- Increasing **bank precharged time**:

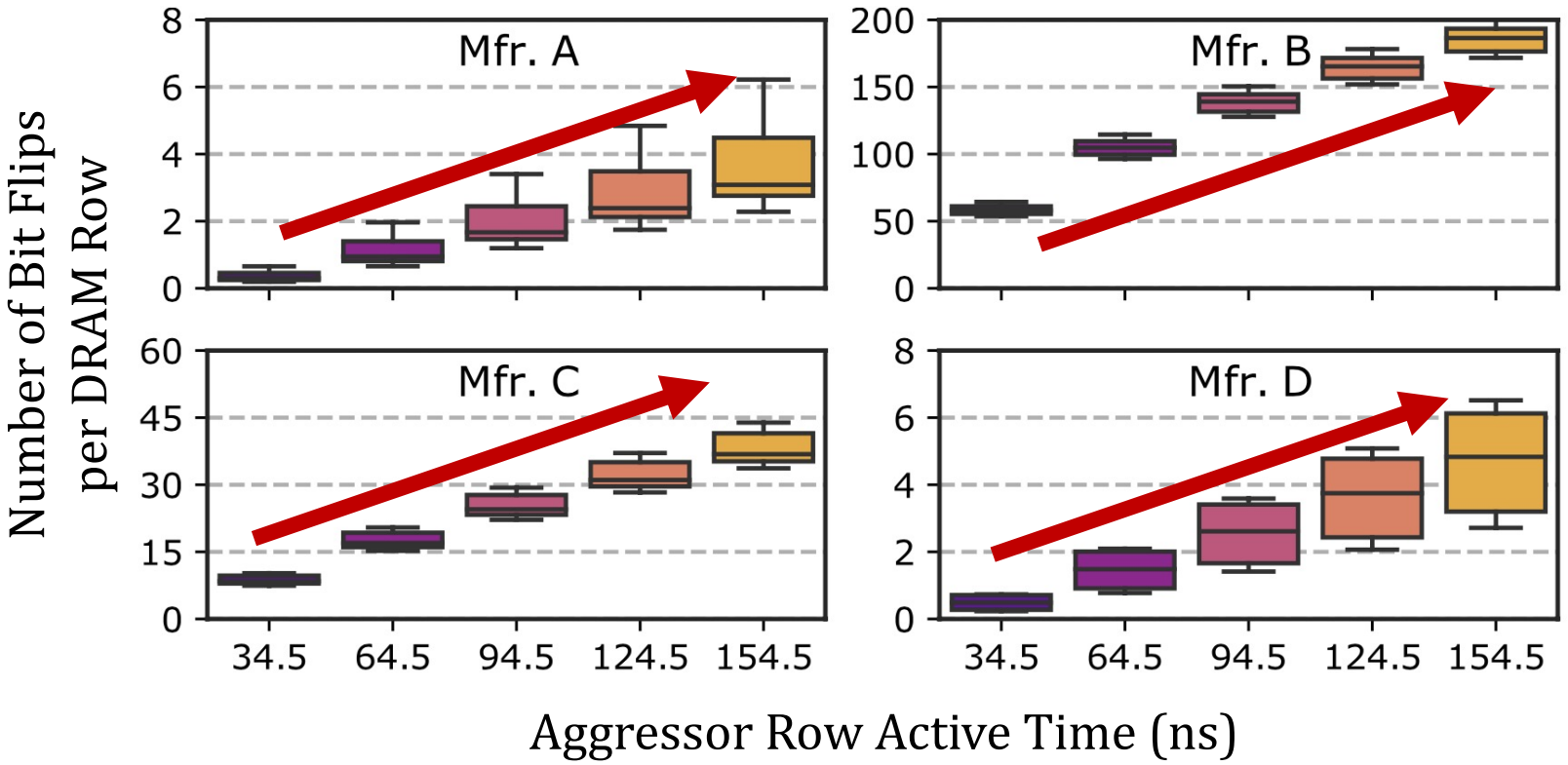


Increasing Aggressor Row Active Time



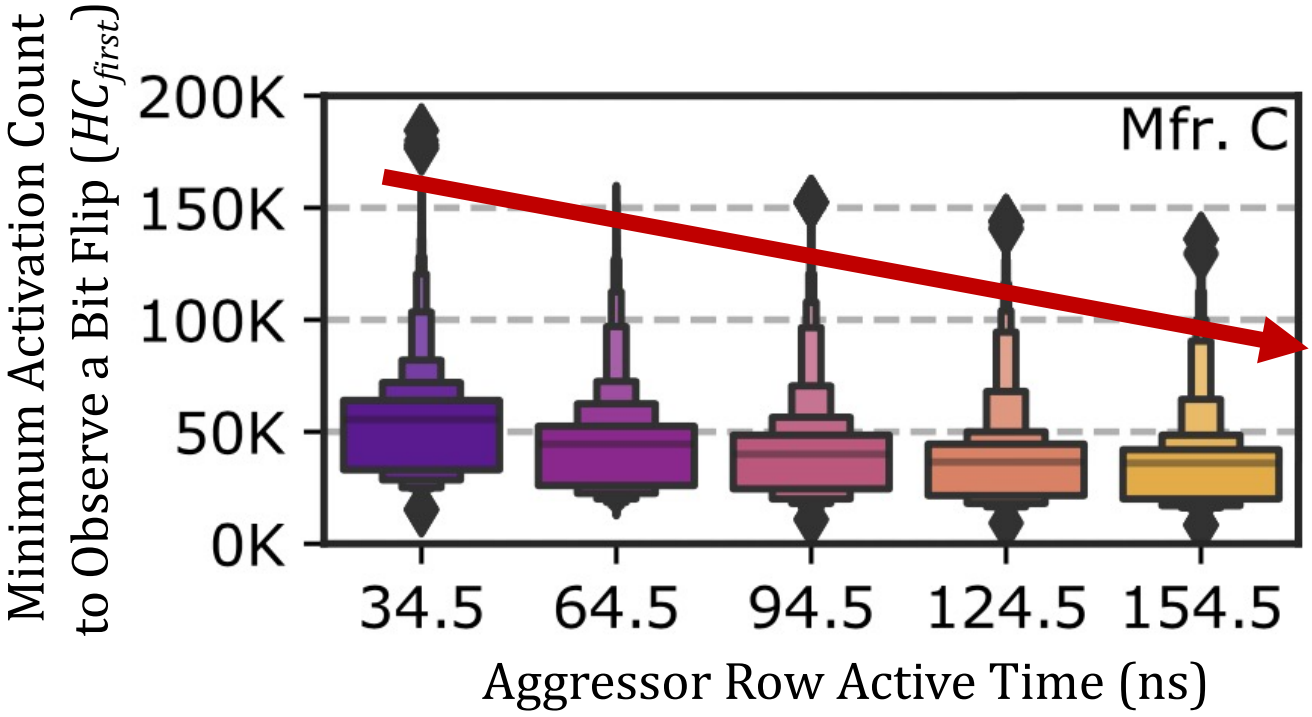
As the **aggressor row stays active longer**, **more DRAM cells** experience RowHammer bit flips

Increasing Aggressor Row Active Time



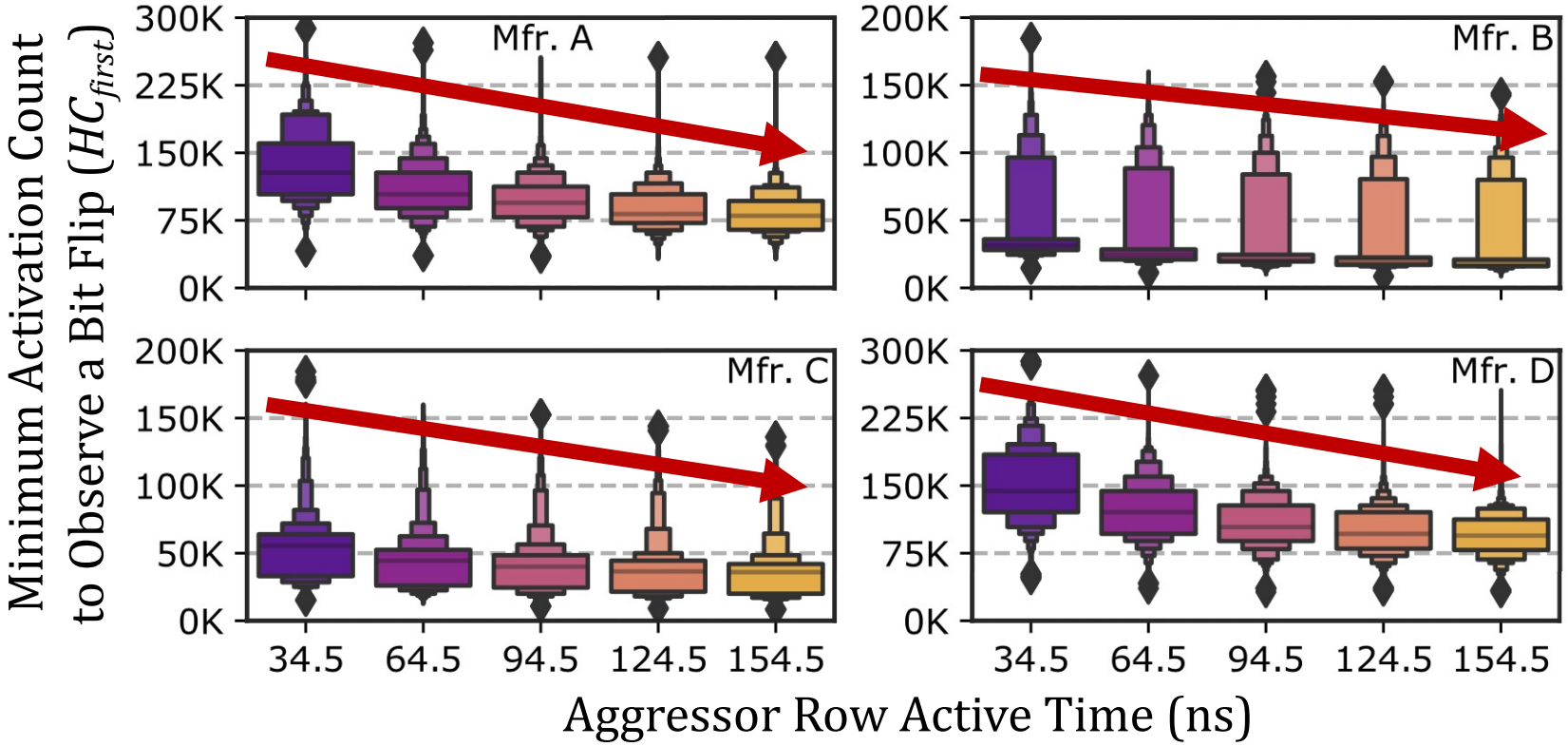
As the **aggressor row stays active longer**, **more DRAM cells** experience RowHammer bit flips

Increasing Aggressor Row Active Time



Fewer activations are required to cause RowHammer bit flips when aggressor rows stay active **for longer time**

Increasing Aggressor Row Active Time



OBSERVATION 8

As the **aggressor row stays active longer**, **more DRAM cells** experience RowHammer bit flips and they experience RowHammer bit flips **at lower activation counts**

Also in the Paper

The **variation** in aggressor row active time's effects across DRAM rows and the effect of increasing **bank precharged time**

OBSERVATION 9

As the **aggressor row stays active longer**, the RowHammer vulnerability **consistently worsens** across tested DRAM rows

OBSERVATION 10

As the **bank stays precharged longer**, **fewer DRAM cells** experience RowHammer bit flips and they experience RowHammer bit flips **at higher activation counts**

OBSERVATION 11

As the **bank stays precharged longer**, the RowHammer vulnerability **consistently reduces** across tested DRAM rows

Also in the Paper

The **variation in these behaviors across DRAM rows** and the effect of increasing **bank precharged time**

KEY OBSERVATION 9

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

KEY OBSERVATION 11

As the **bank stays precharged longer**, the RowHammer vulnerability **consistently reduces** across tested DRAM rows

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Key Takeaways from Spatial Variation Analysis

Key Takeaway 5

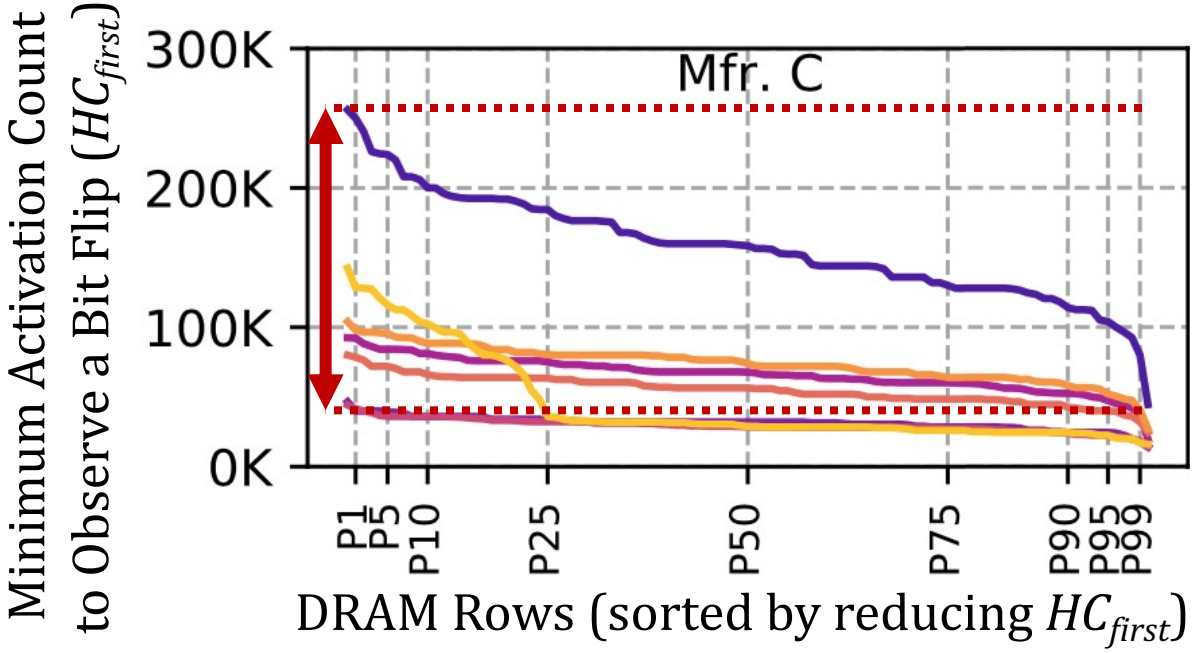
RowHammer vulnerability **significantly varies** across DRAM rows and columns due to **design-induced** and **manufacturing-process-induced** variation

Key Takeaway 6

The distribution of **the minimum activation count to observe bit flips (HC_{first})** exhibits **a diverse set of values in a subarray** but **similar values across subarrays** in the same DRAM module

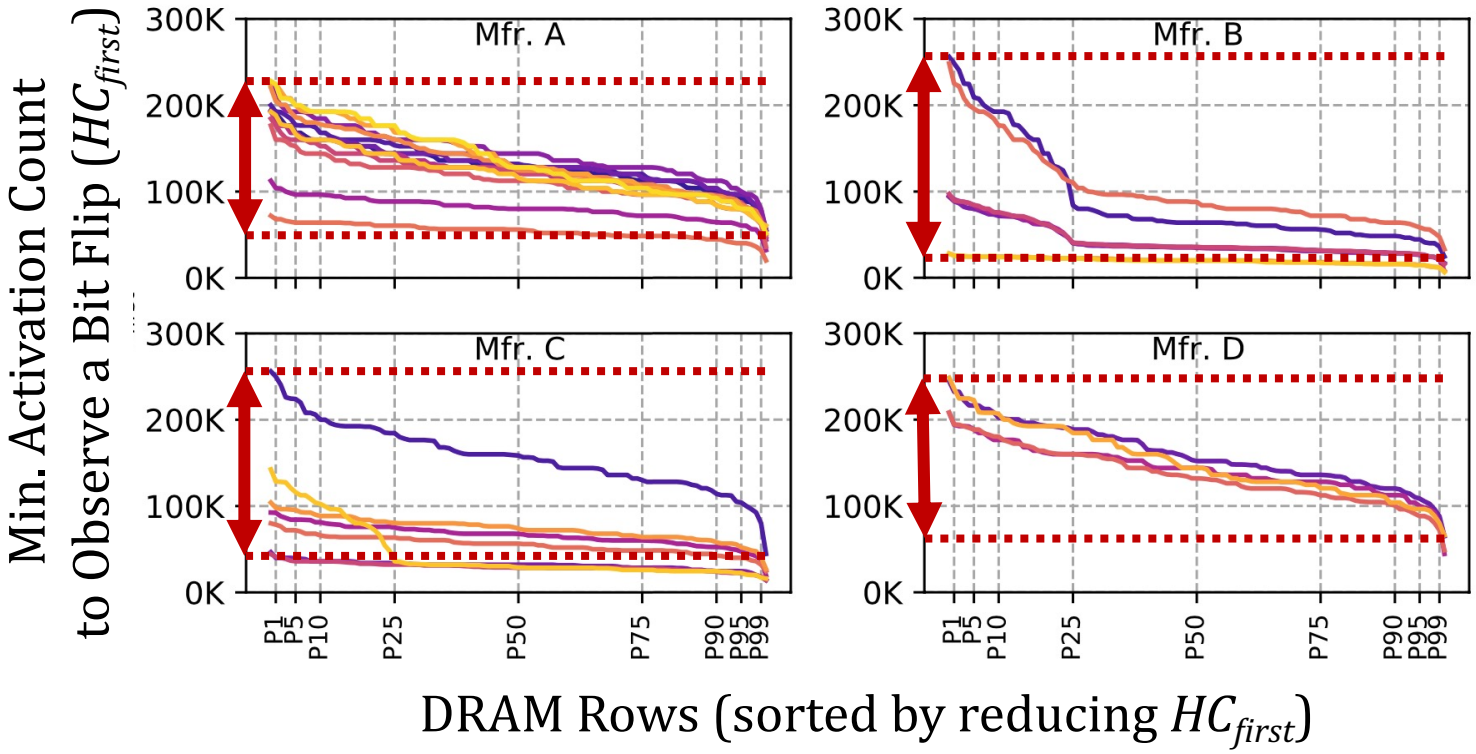
Spatial Variation across Rows

The **minimum activation count** to observe bit flips **(HC_{first})** across **DRAM rows:**



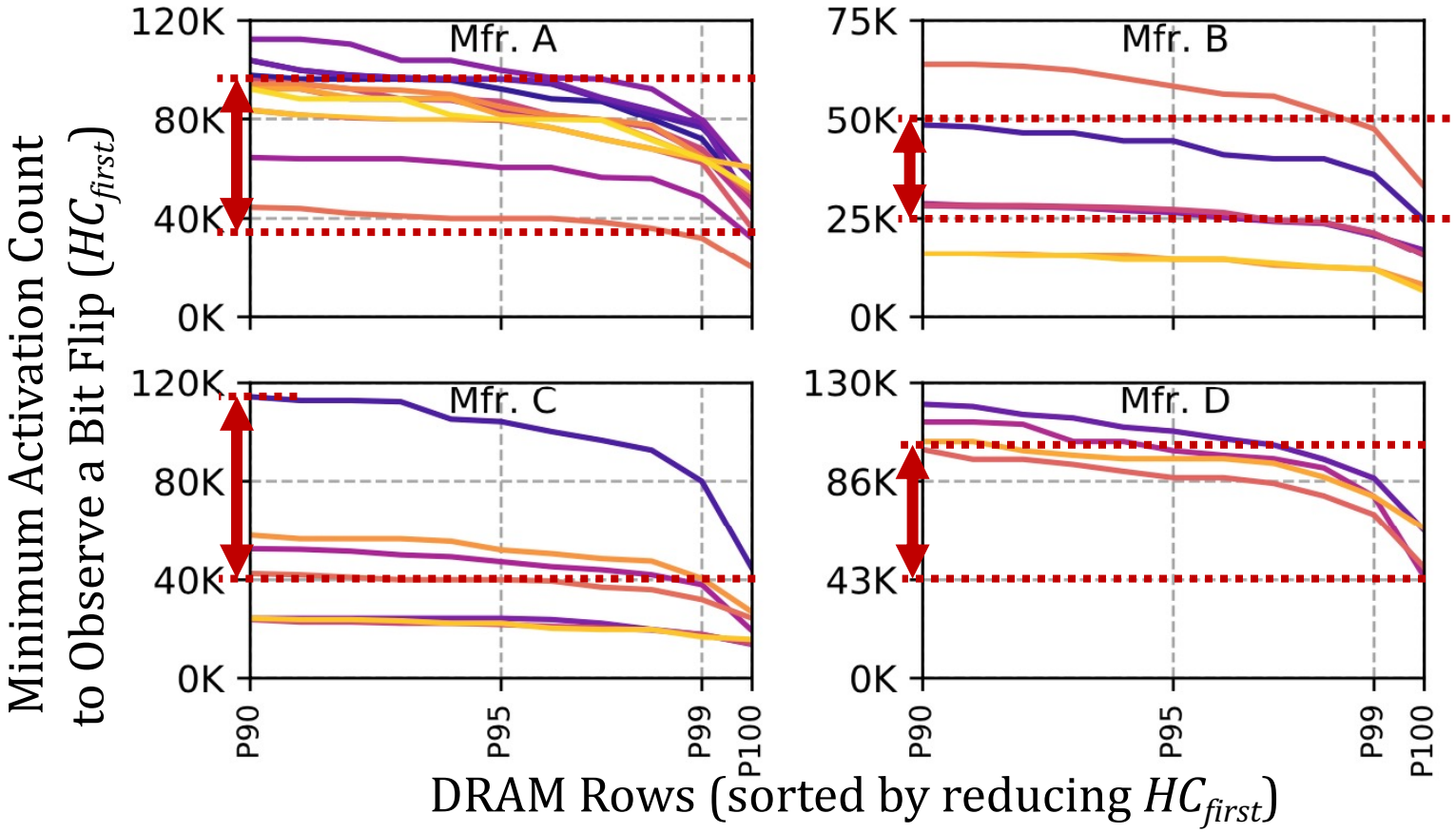
The RowHammer vulnerability **significantly varies** across DRAM rows

Spatial Variation across Rows



The RowHammer vulnerability **significantly varies** across DRAM rows

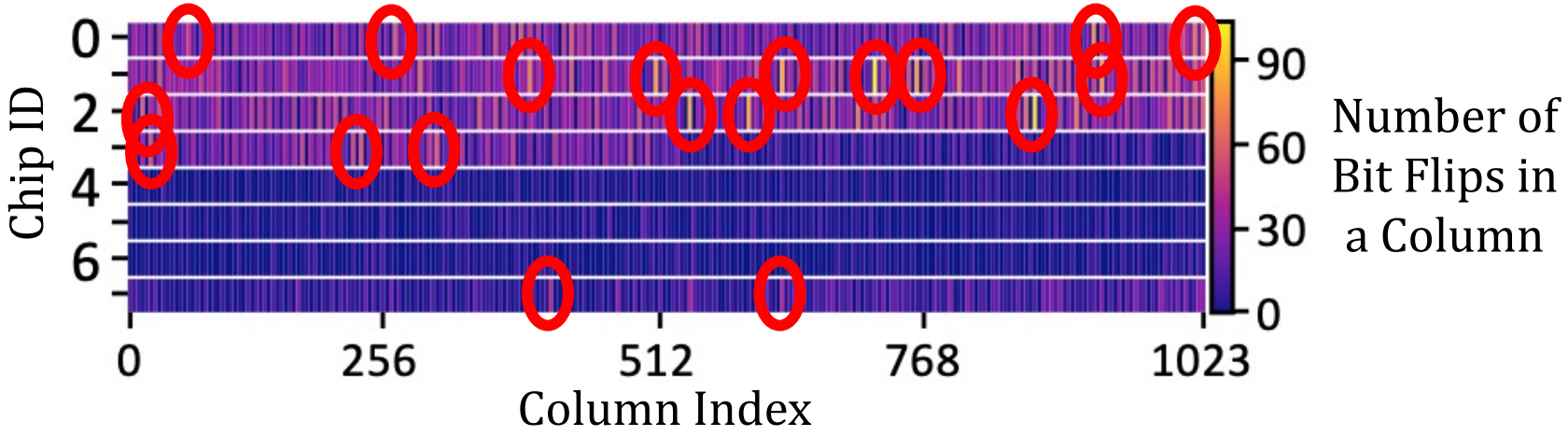
Spatial Variation across Rows



OBSERVATION 12

A small fraction of DRAM rows are **significantly more vulnerable** to RowHammer than **the vast majority** of the rows

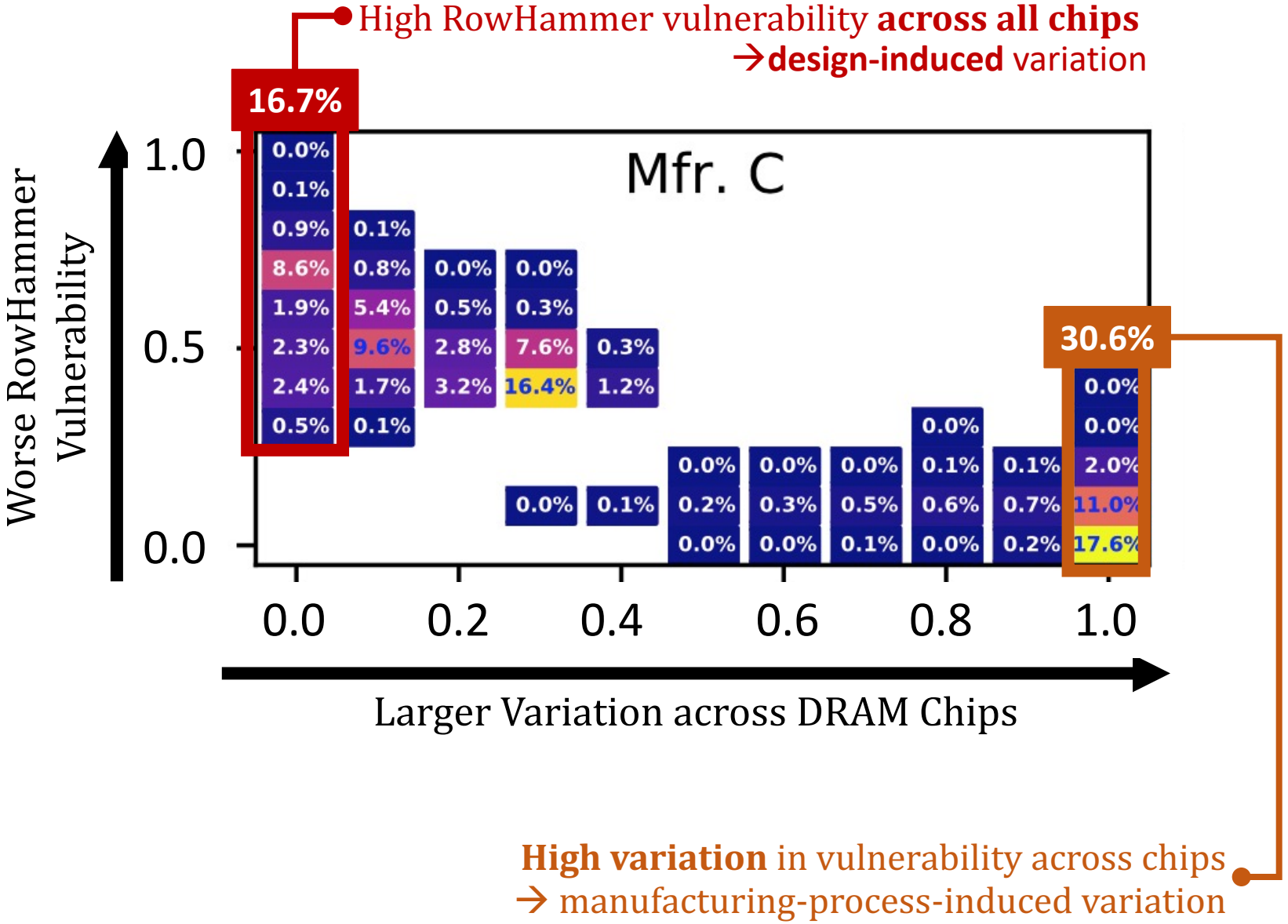
Spatial Variation across Columns



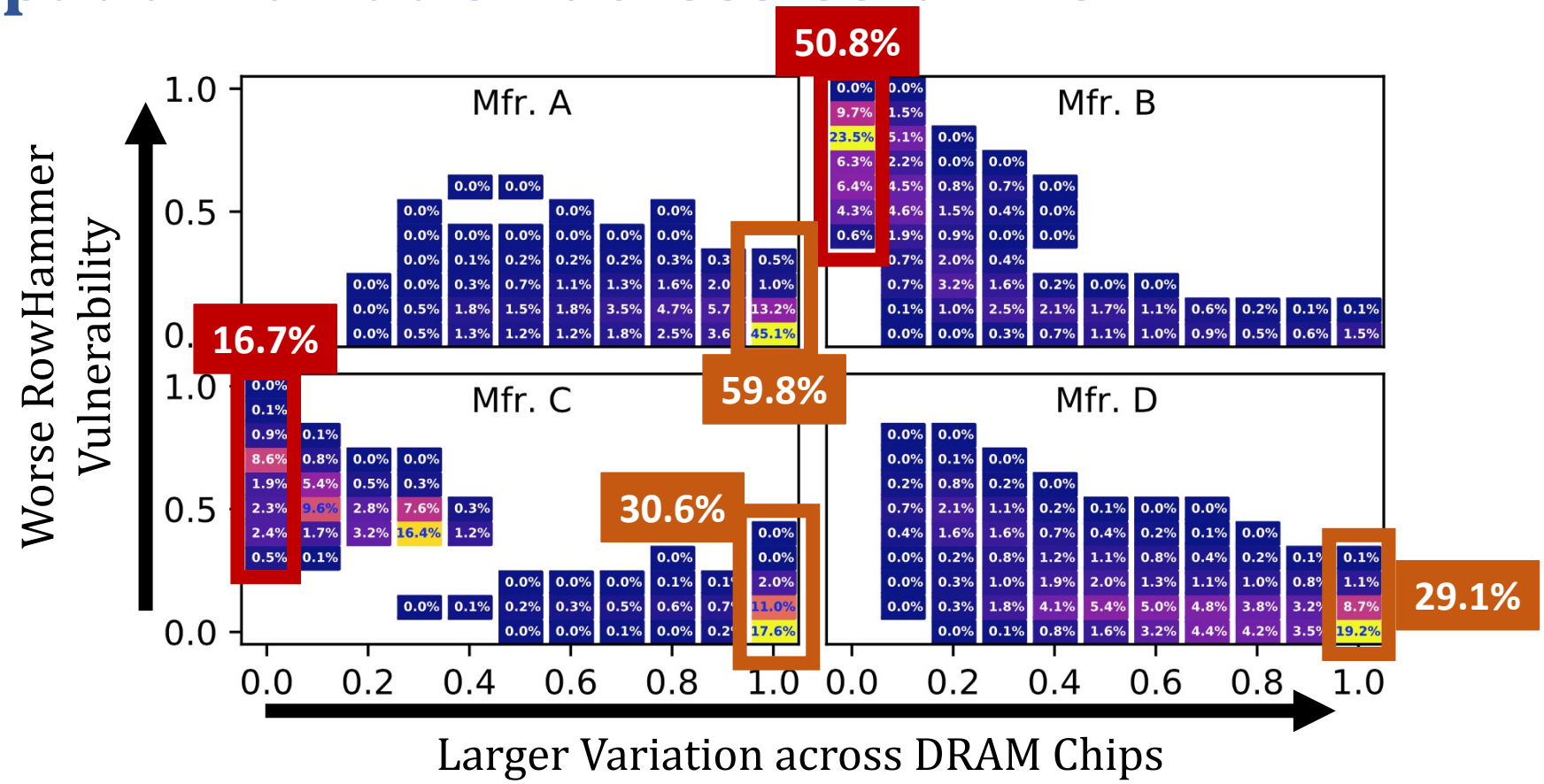
OBSERVATION 13

Certain columns are **significantly more vulnerable** to RowHammer than other columns

Spatial Variation across Columns



Spatial Variation across Columns



OBSERVATION 14

Both **manufacturing process** and **design** affect a **DRAM column's RowHammer vulnerability**

Also in the Paper

The **minimum activation count** at which a victim row experiences a bit flip (**HC_{first}**) across rows in a subarray and across subarrays in a DRAM module**:**

OBSERVATION 15

The most vulnerable DRAM row in a subarray
is **significantly more vulnerable**
than the other rows **in the subarray**

OBSERVATION 16

HC_{first} distributions of subarrays **within a DRAM module**
are **significantly more similar** to each other
than those of subarrays **from different modules**

Also in the Paper

The **minimum activation count** at which a victim row experiences a bit flip (HC_{first}) across rows in a subarray and across subarrays in a module:

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

HC_{first} distributions of subarrays **within a DRAM module** are **significantly more similar** to each other than those of subarrays **from different modules**

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Implications on Attacks and Defenses

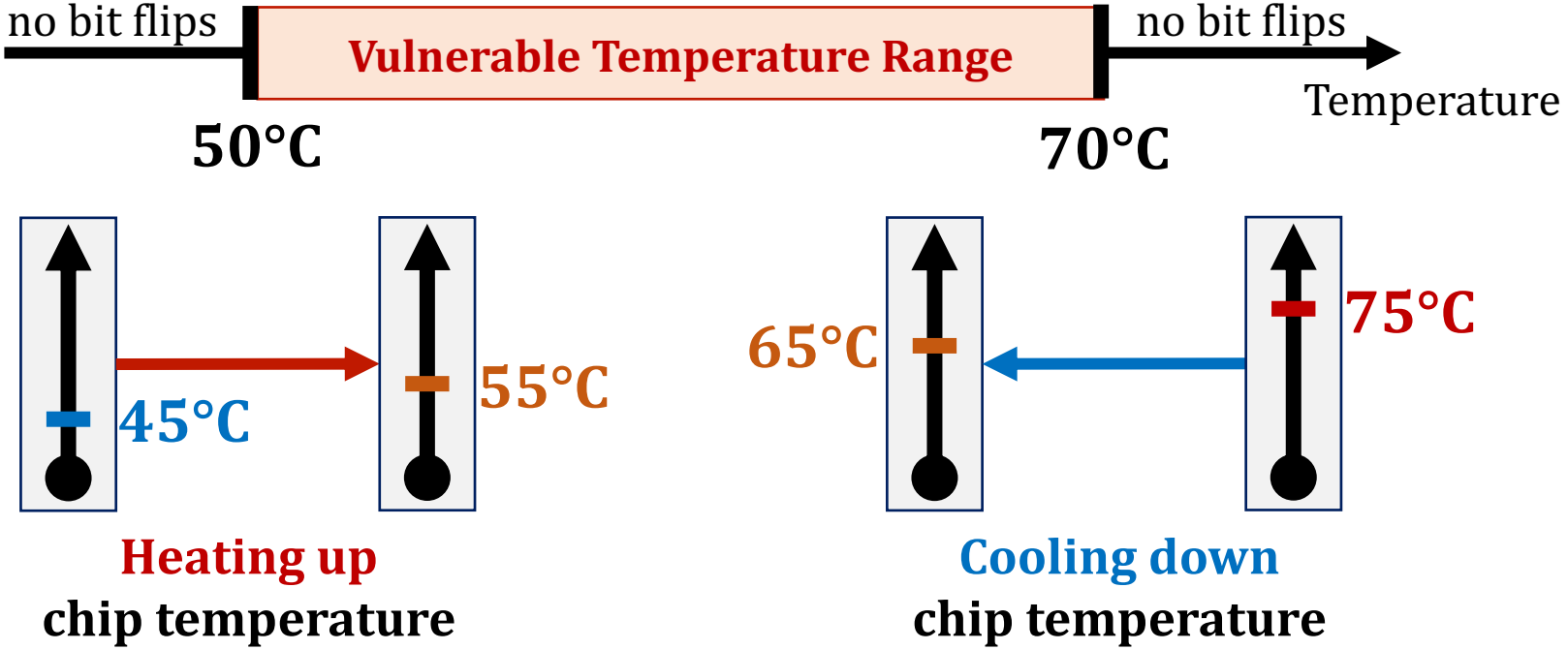
Our observations can be leveraged to craft
more effective RowHammer attacks

Our observations can be leveraged to design
more effective and efficient RowHammer defenses

Attack Improvement 1:
Making DRAM Cells More Vulnerable

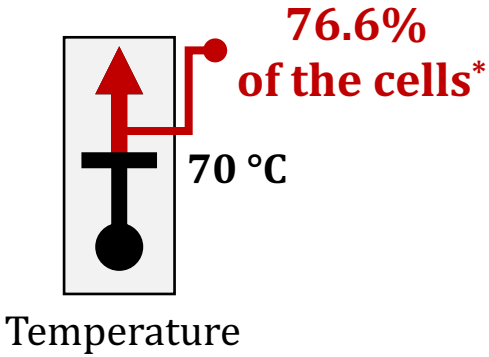
An attacker can **manipulate temperature** to make the cells that store sensitive data **more vulnerable**

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

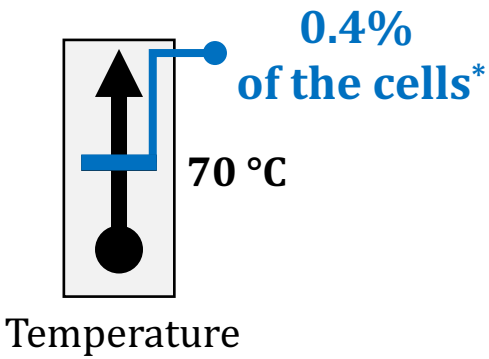


Attack Improvement 2:
Temperature-Dependent Trigger

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



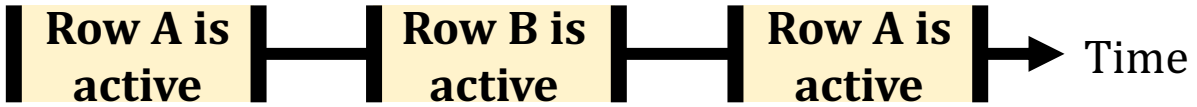
2. **Precisely measure** the temperature **to trigger an attack** exactly at the desired temperature



*Example fraction values from Mfr. C

Attack Improvement 3:
Bypassing Defenses with Aggressor Row Active Time

Activating aggressor rows as frequently as possible:



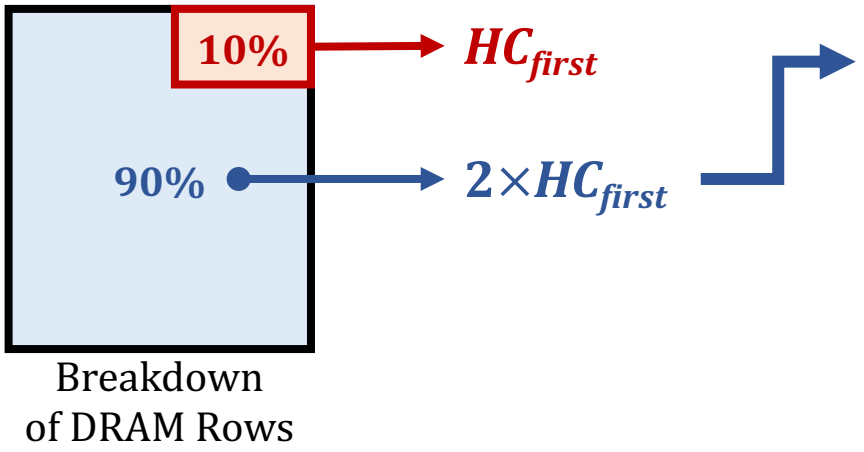
Keeping the aggressor rows active for a longer time:

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

Bypasses defenses that do not account for this reduction

Defense Improvements

- **Example 1: Leveraging the variation across DRAM rows**



Aggressiveness can be reduced:

33% area reduction
for BlockHammer [Yağlıkçı+, HPCA'21]

80% area reduction
for Graphene [Park+, MICRO'20]

- **Example 2: Leveraging the variation with temperature**
  - A DRAM cell experiences **bit flips** within **a bounded temperature range**

  - A row can be **disabled** within the row's **vulnerable temperature range**

More Defense Implications in the Paper

- Leveraging **the similarity across subarrays** in a DRAM module can **reduce the module's profiling time** for RowHammer errors

- Monitoring and limiting the **aggressor row active time** from the memory controller can **reduce the RowHammer vulnerability** and **make defenses more efficient**

- **ECC schemes** can target the **non-uniform bit error distribution** caused by **design-induced variation** across DRAM columns

- **Cooling** DRAM chips can **reduce overall bit error rate**

More Defense Implications in the Paper

- Leveraging the similarity across subarrays in a DRAM module to speed up profiling the module for RowHammer errors

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

- Cooling DRAM chips can reduce overall bit error rate

Outline

Motivation and Goal

Experimental Methodology

Temperature Analysis

Aggressor Row Active Time Analysis

Spatial Variation Analysis

Implications on Attacks and Defenses

Conclusions

Conclusion

- **Motivation**:
  - Denser DRAM chips are **more vulnerable** to RowHammer
  - Understanding RowHammer enables designing **effective and efficient solutions**, but **no rigorous study** demonstrates how vulnerability varies under different conditions
- **Goal**: Provide insights into **three fundamental properties** of RowHammer that can be leveraged to design **more effective and efficient attacks and defenses**
  1) DRAM chip **temperature**
  2) The time that an **aggressor row stays active**
  3) Victim DRAM cell's **physical location**
- **Experimental study**: **272 DRAM chips** from **four major manufacturers**
- **Key Results:** We provide **6 takeaways** from **16 novel observations**
  A RowHammer bit flip is **more likely to occur**
  1) in **a bounded range of temperature**
  2) if the aggressor row is **active for longer time**
  3) in **certain physical regions** of the DRAM module under attack
- **Conclusion:** Our novel observations can inspire and aid future work
  - Craft **more effective attacks**
  - Design **more effective and efficient defenses**

A Deeper Look into RowHammer's Sensitivities

Experimental Analysis of Real DRAM Chips and Implications on Future Attacks and Defenses

BACKUP SLIDES

Lois Orosa **Abdullah Giray Yağlıkçı**

Haocong Luo Ataberk Olgun Jisung Park

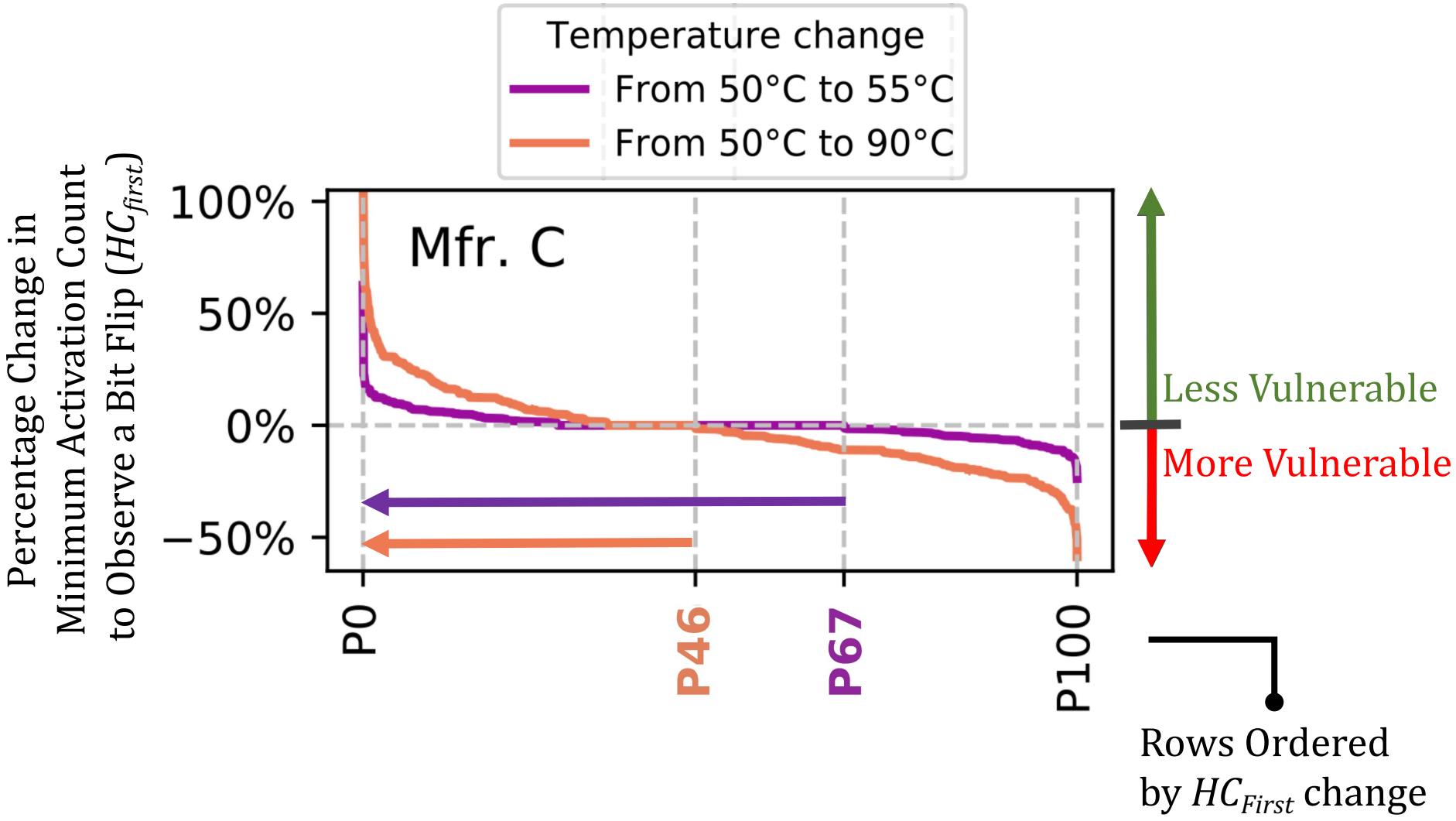
Hasan Hassan Minesh Patel Jeremie S. Kim Onur Mutlu

SAFARI

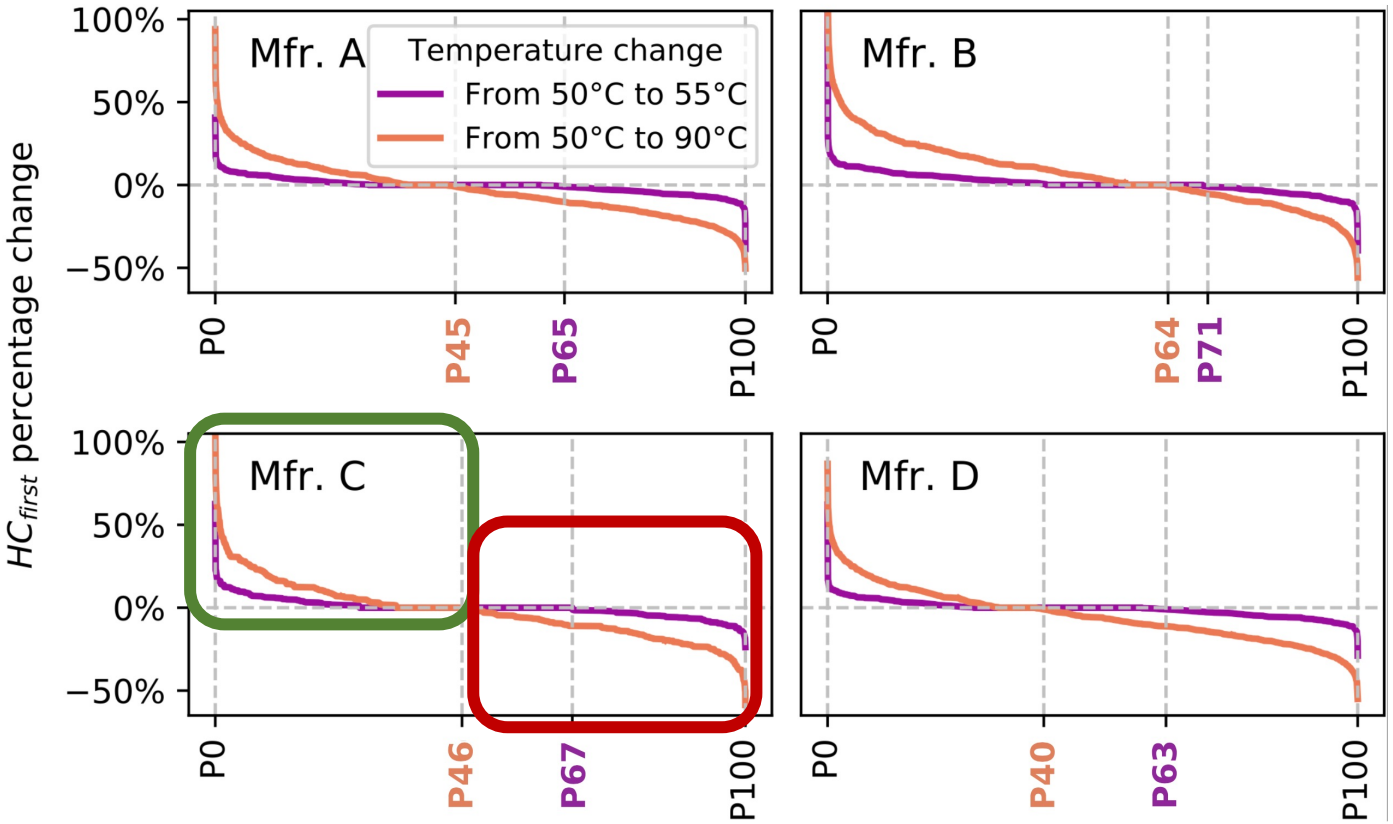
ETH zürich

TOBB ETÜ
University of Economics & Technology

Distribution of the Change in HC_{first}



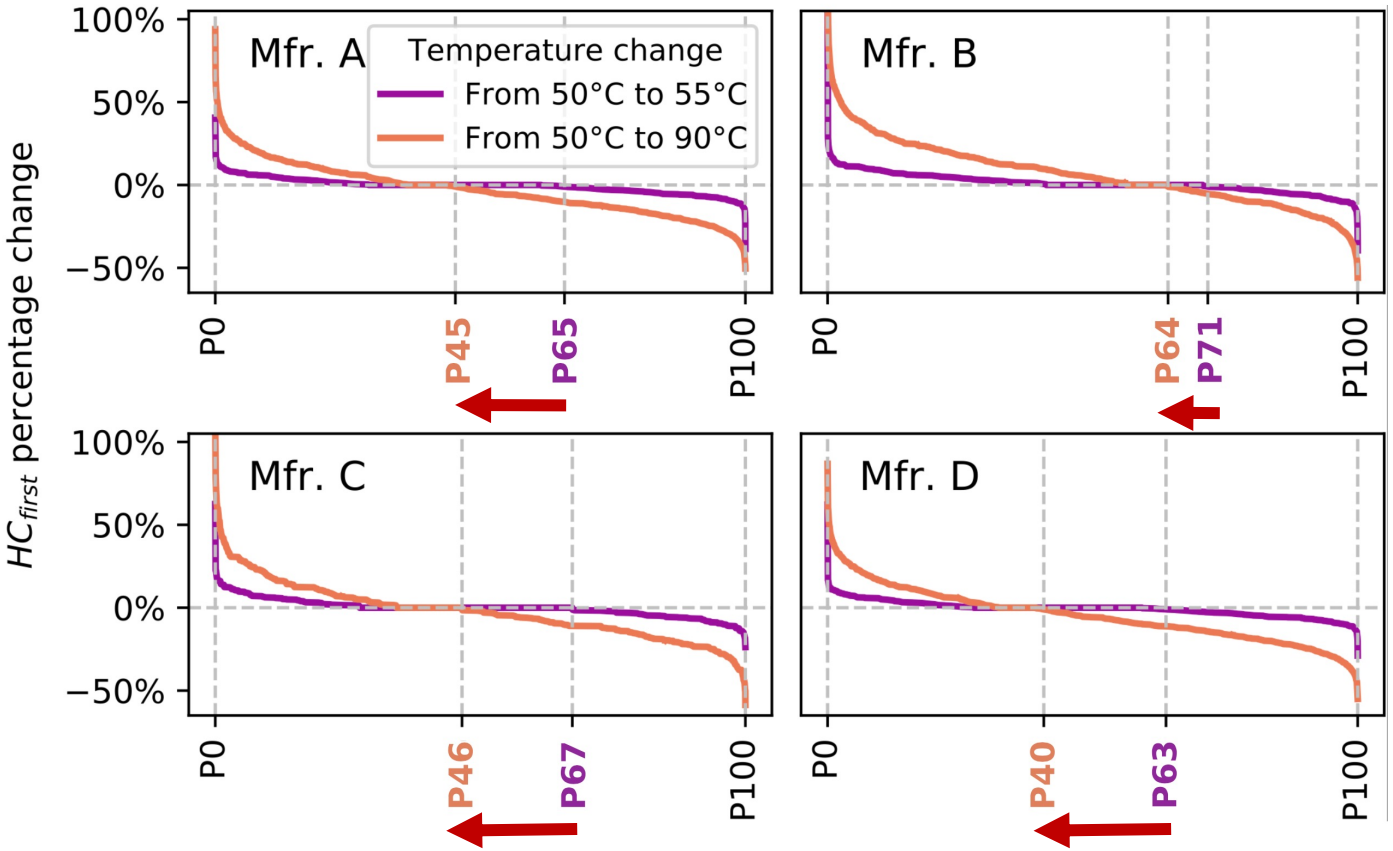
Distribution of the Change in HC_{first}



OBSERVATION 5

DRAM rows can show **either higher or lower** HC_{first} when **temperature increases**

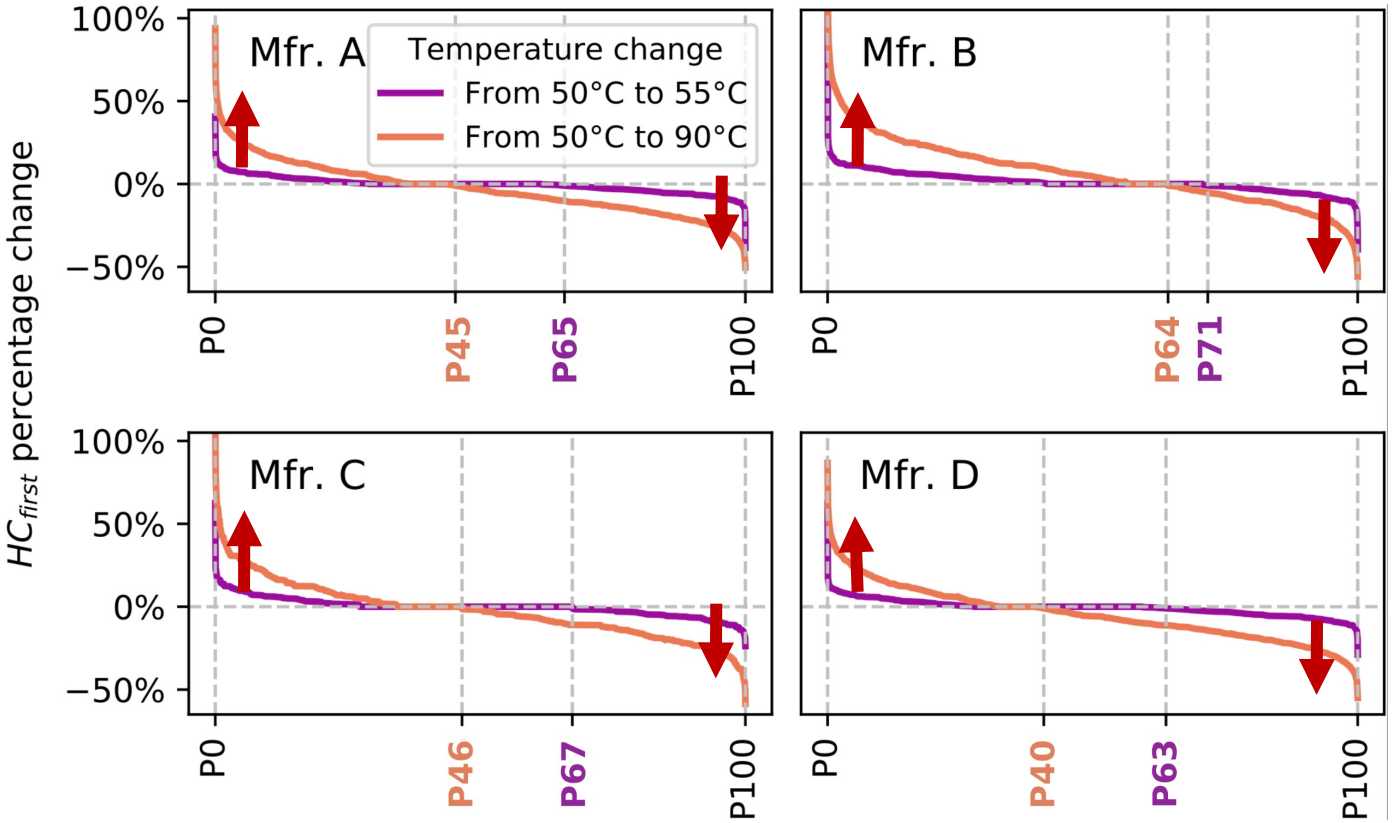
Distribution of the Change in HC_{first}



OBSERVATION 6

***HC*$_{first}$** tends to generally **decrease**
as **temperature change (Δ*T*) increases**

Distribution of the Change in HC_{first}



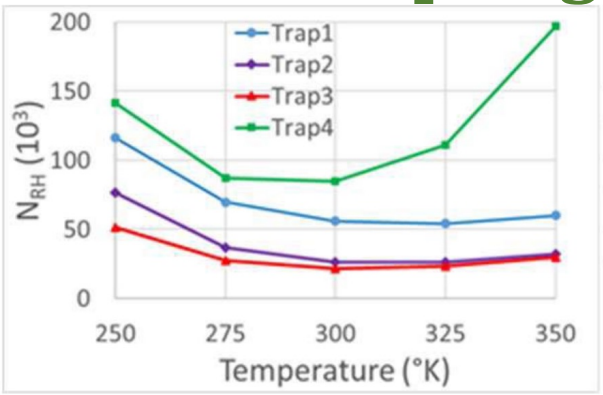
OBSERVATION 7

The ***HC*$_{first}$ change (Δ*HC*$_{first}$)** tends to be **larger** as **temperature change (Δ*T*) increases**

Circuit-Level Justification
Temperature Analysis

We hypothesize that our observations are caused by the **non-monotonic behavior of charge trapping** characteristics of DRAM cells

3D TCAD model [Yang+, EDL'19]



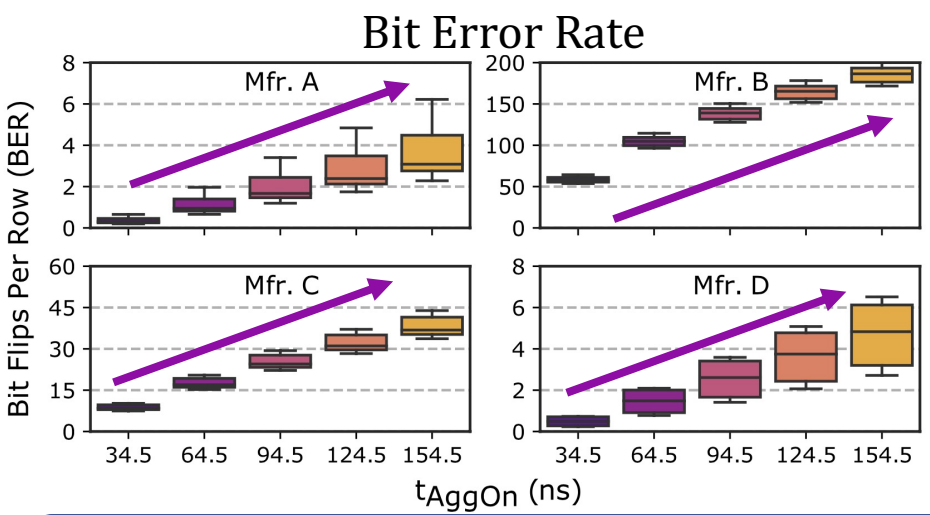
	Row	Column	Energy
Trap1	1	4	0.50eV
Trap2	2	3	0.45eV
Trap3	3	3	0.45eV
Trap4	4	3	0.45eV

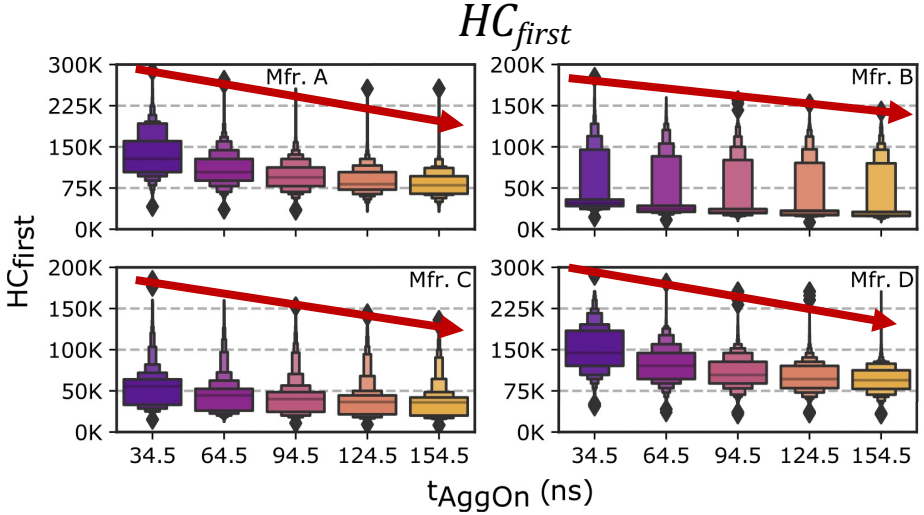
Fig. 6. Hammering threshold N_{RH} vs. temperature from 250 to 350°K for different traps. Location in row and column refers to matrix in Fig. 2b.

***HC_{first}* decreases as temperature increases**, until a temperature inflection point where ***HC_{first}* starts to increase as temperature increases**

A **cell is more vulnerable** to RowHammer at **temperatures close to its temperature inflection point**

Increasing Aggressor Row Active Time (t_{AggOn})





OBSERVATION 8

As the **aggressor row stays active longer**, **more DRAM cells** experience RowHammer bit flips and they experience RowHammer bit flips **at lower hammer counts**

We analyze how the ***coefficient of variation**** values for ***BER*** and ***HC_{first}*** change across rows when the **aggressor row stays active longer**

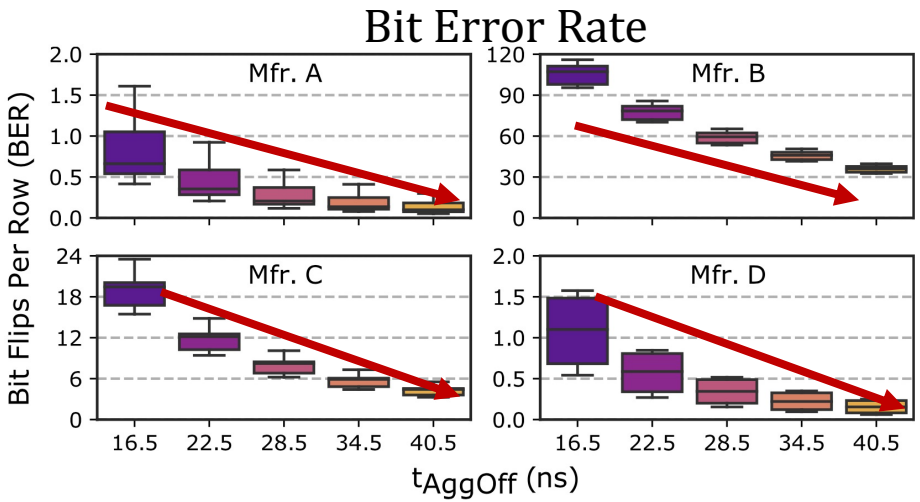
OBSERVATION 9

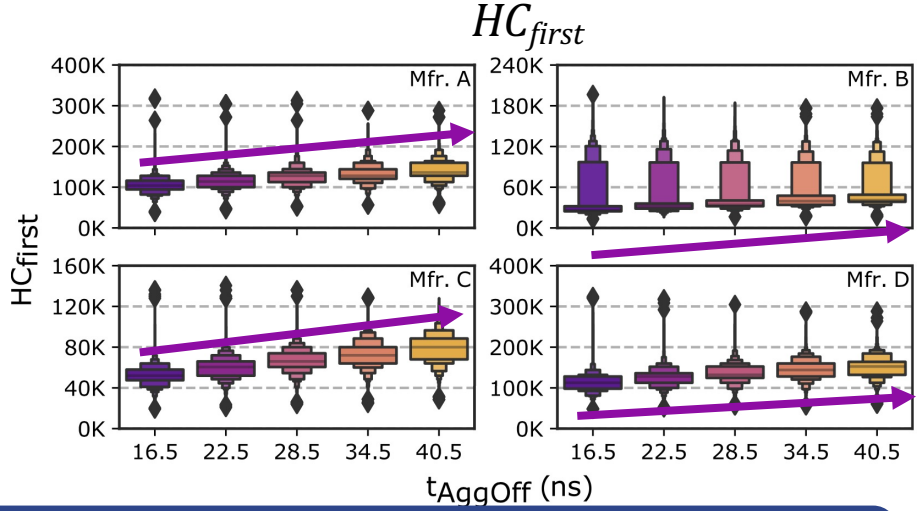
RowHammer vulnerability **consistently worsens as t_{AggOn} increases** across all tested DRAM rows**

*$Coefficient\ of\ Variation\ (CV) = Standard\ Deviation / Average$

** Please refer to the full paper for coefficient of variation-based (CV) analysis

Increasing Bank Precharged Time (t_{AggOff})





OBSERVATION 10

As the **bank stays precharged longer, fewer DRAM cells** experience RowHammer bit flips and they experience RowHammer bit flips **at higher hammer counts**

We repeat the ***coefficient of variation**** analysis for ***BER*** and ***HC_{first}*** change across rows when the **bank stays precharged longer**

OBSERVATION 11

RowHammer vulnerability **consistently reduces as t_{AggOff} increases** across all tested DRAM rows**

*$Coefficient\ of\ Variation\ (CV) = {Standard\ Deviation}/{Average}$

** Please refer to the full paper for coefficient of variation-based (CV) analysis

Circuit-Level Justification
Aggressor Row Active Time Analysis

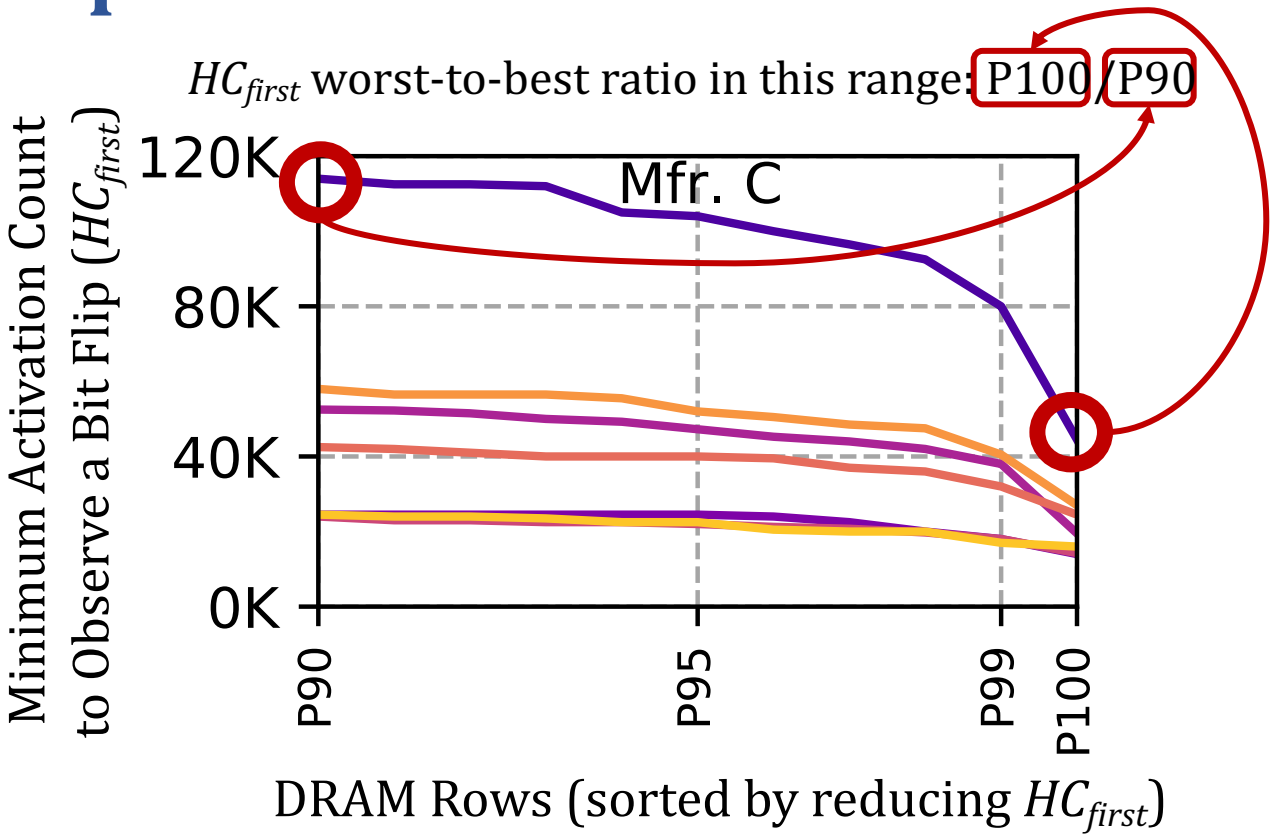
Two possible circuit level justifications for RowHammer bit flips:

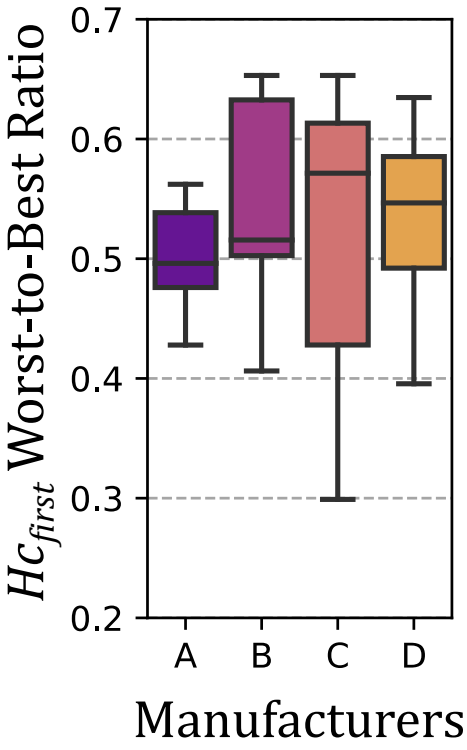
1. Electron injection in the victim cell **[Walker+, TED'21][Yang+, TDMR'16]**
2. Wordline-to-wordline cross-talk noise between aggressor and victim rows that occurs when the aggressor row is being activated **[Ryu+, IEDM'17][Walker+, TED'21]**

We hypothesize that **increasing the aggressor row's active time** (t_{AggOn}) **has a larger impact on exacerbating electron injection to the victim cell**, compared to the reduction in cross-talk noise due to lower activation frequency. Thus, RowHammer vulnerability worsens when t_{AggOn} increases

Increasing a bank's precharged time (t_{AggOff}) decreases RowHammer vulnerability because **longer t_{AggOff} reduces the effect of cross-talk noise without affecting electron injection** (since t_{AggOn} is unchanged).

Spatial Variation across Rows



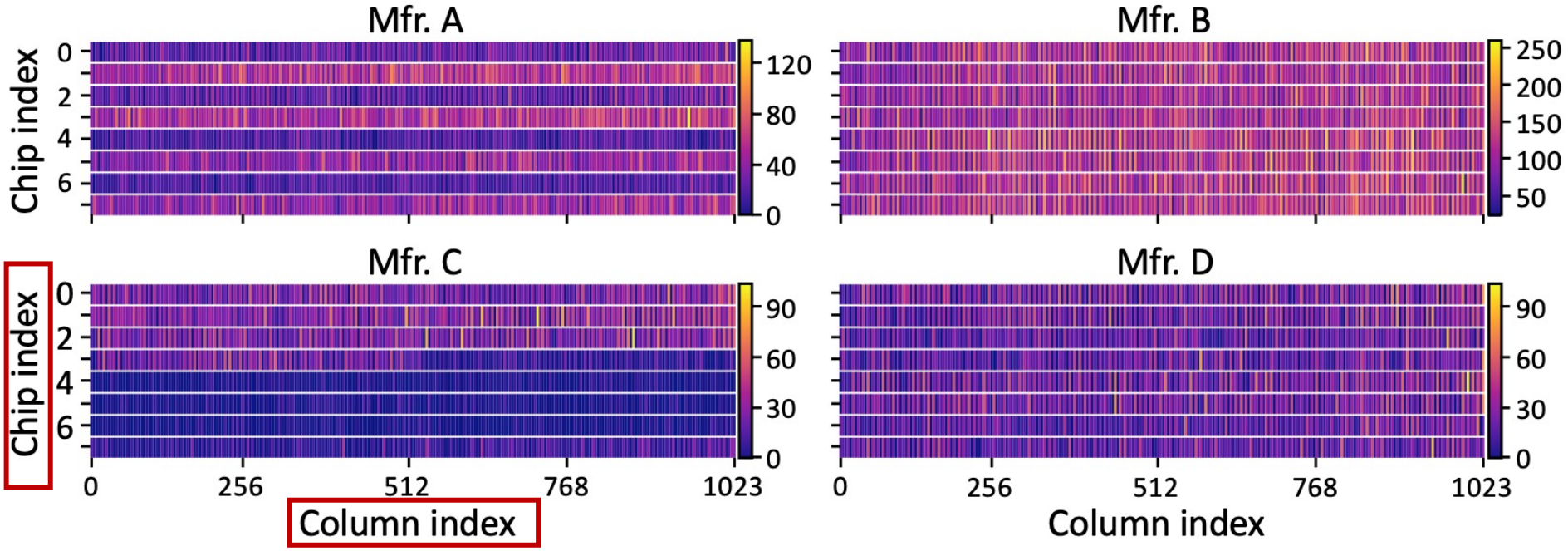


OBSERVATION 12

A small fraction of DRAM rows
are **significantly more vulnerable** to RowHammer
than **the vast majority** of the rows

Spatial Variation across Columns

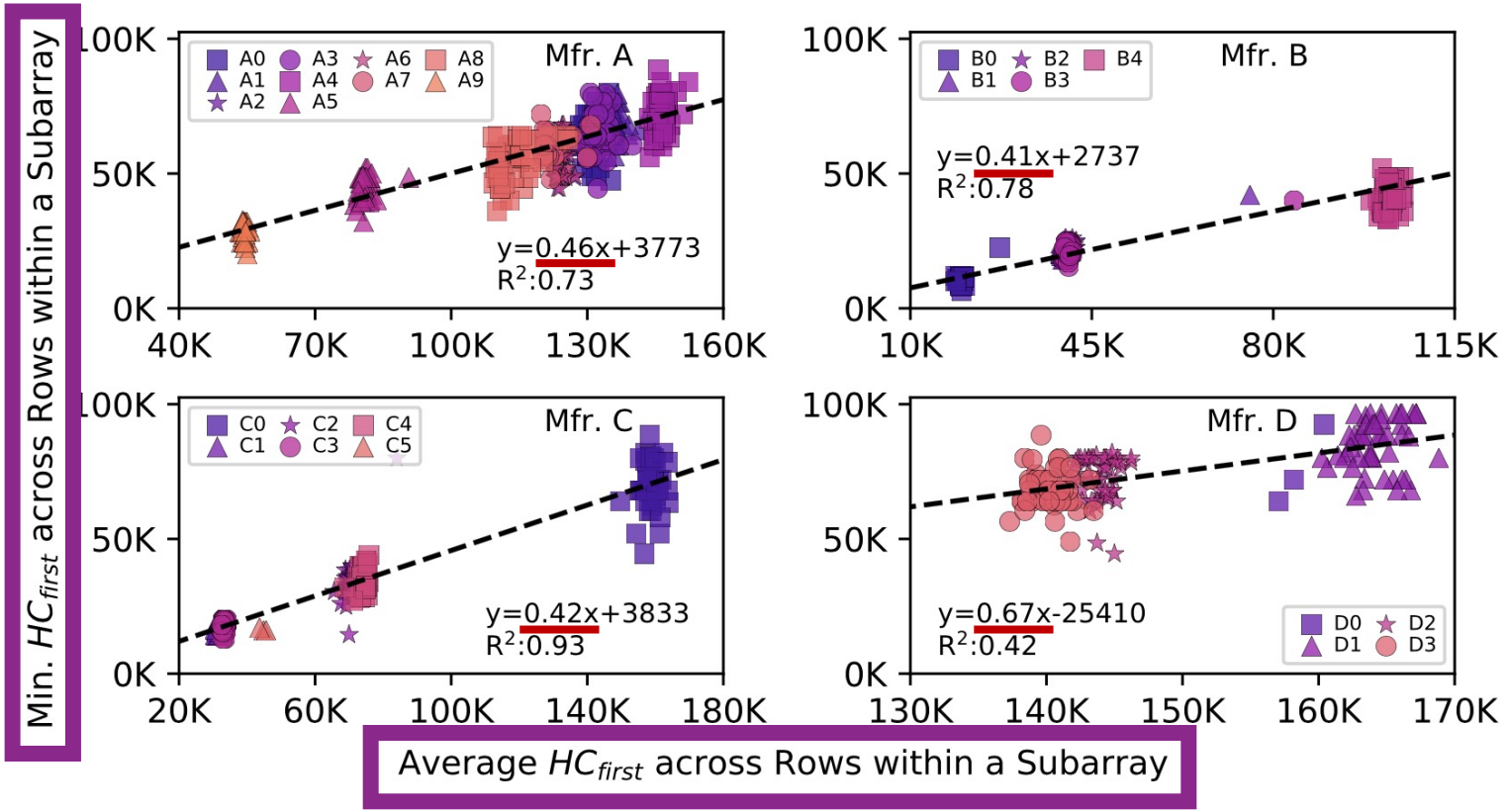
We analyze BER variation across DRAM columns



OBSERVATION 13

Certain columns are **significantly more vulnerable** to RowHammer than other columns

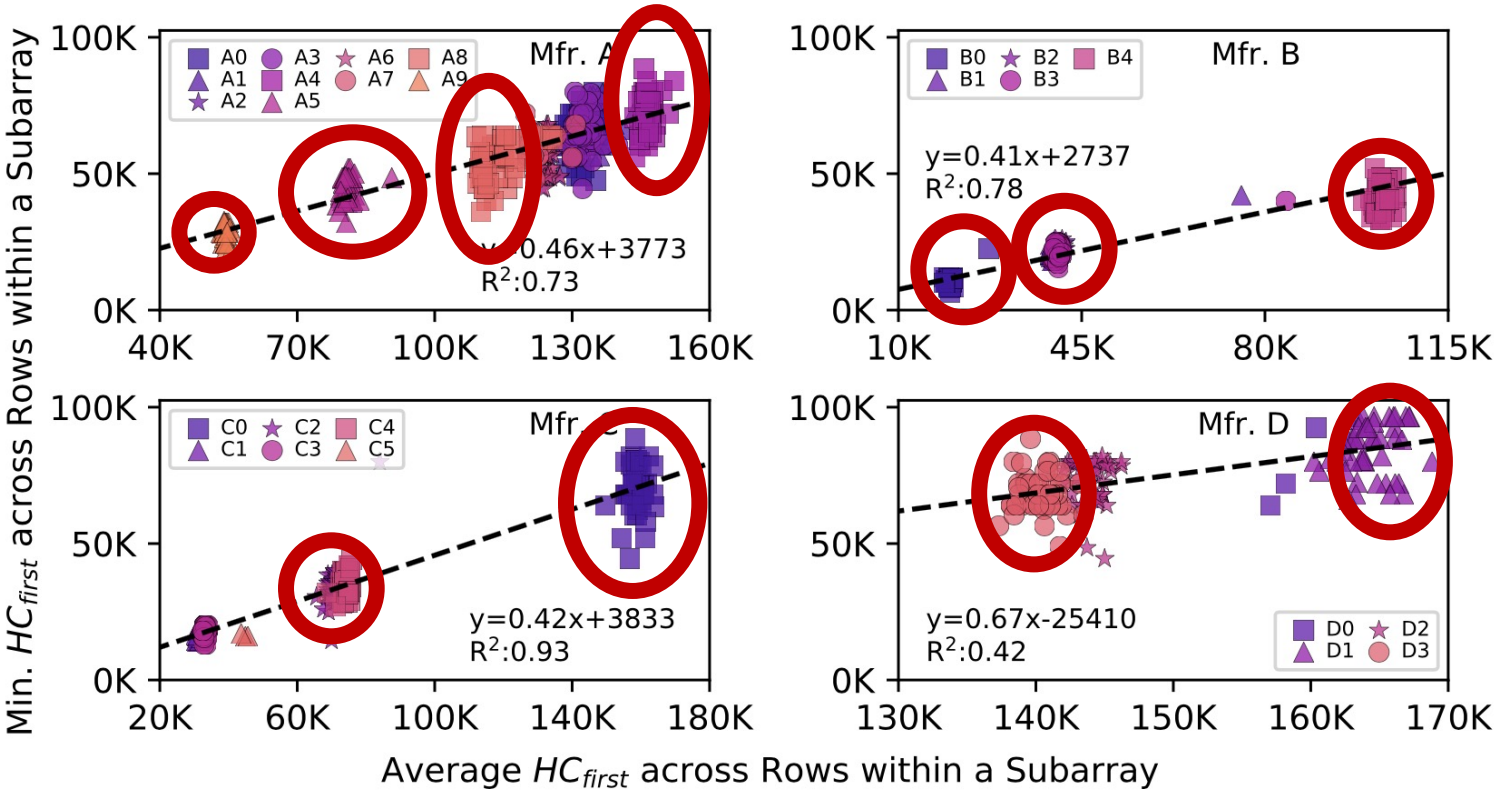
Spatial Variation across Subarrays



OBSERVATION 15

The most vulnerable DRAM row in a subarray
is **significantly more vulnerable**
than the other rows **in the subarray**

Spatial Variation across Subarrays



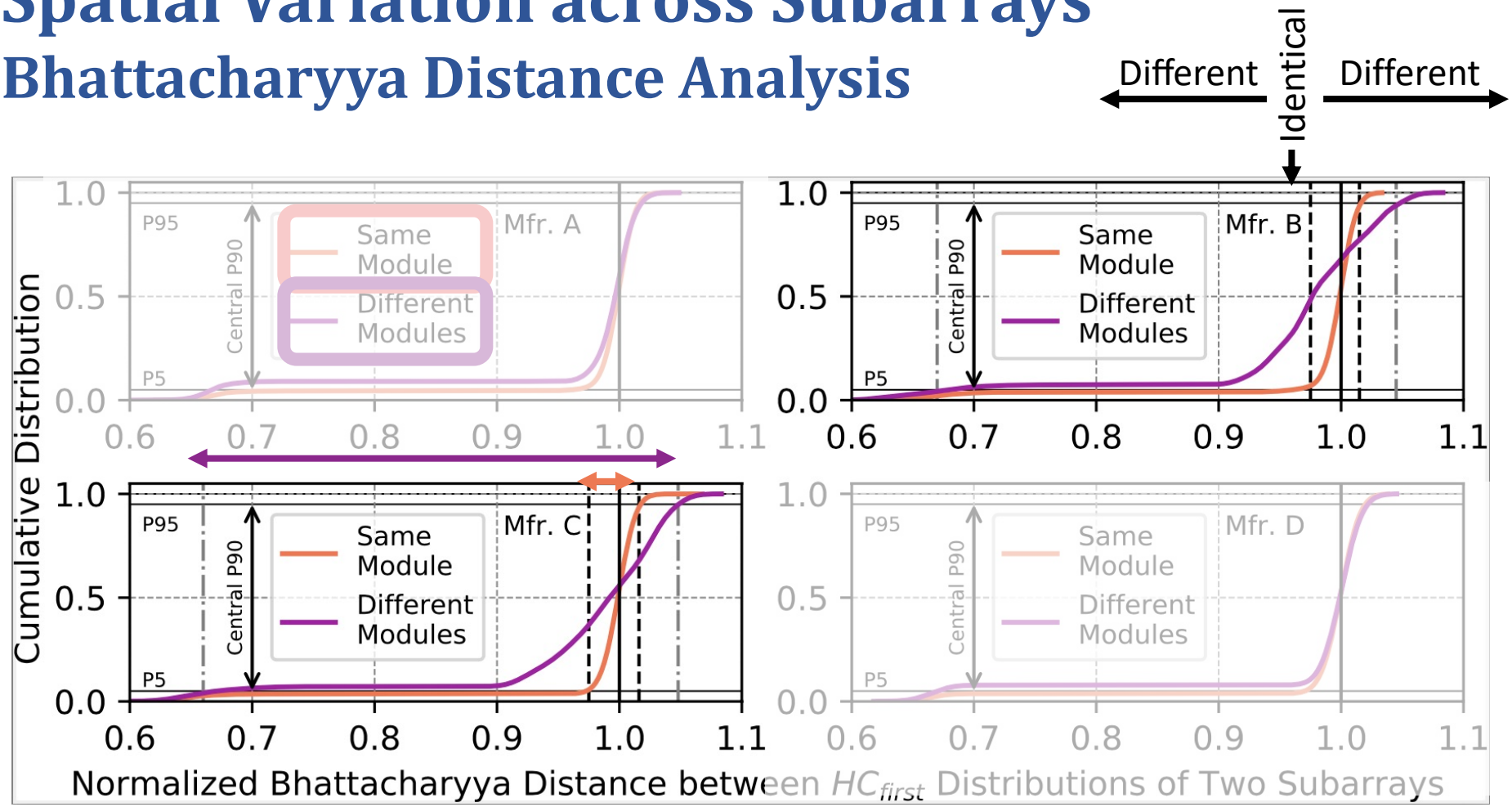
OBSERVATION 16

HC_{first} distributions of subarrays **within a DRAM module** are **significantly more similar** to each other than those of subarrays **from different modules**

* We analyze the similarity between Hcfirst distributions of different subarrays based on Bhattacharyya distance in the paper

Spatial Variation across Subarrays

Bhattacharyya Distance Analysis



HC_{first} distributions of subarrays **within a DRAM module** exhibit **significantly more similarity** to each other than HC_{first} distributions of subarrays **from different modules**

Circuit-Level Justification
Spatial Variation Analysis

Variation across rows, columns, and chips:

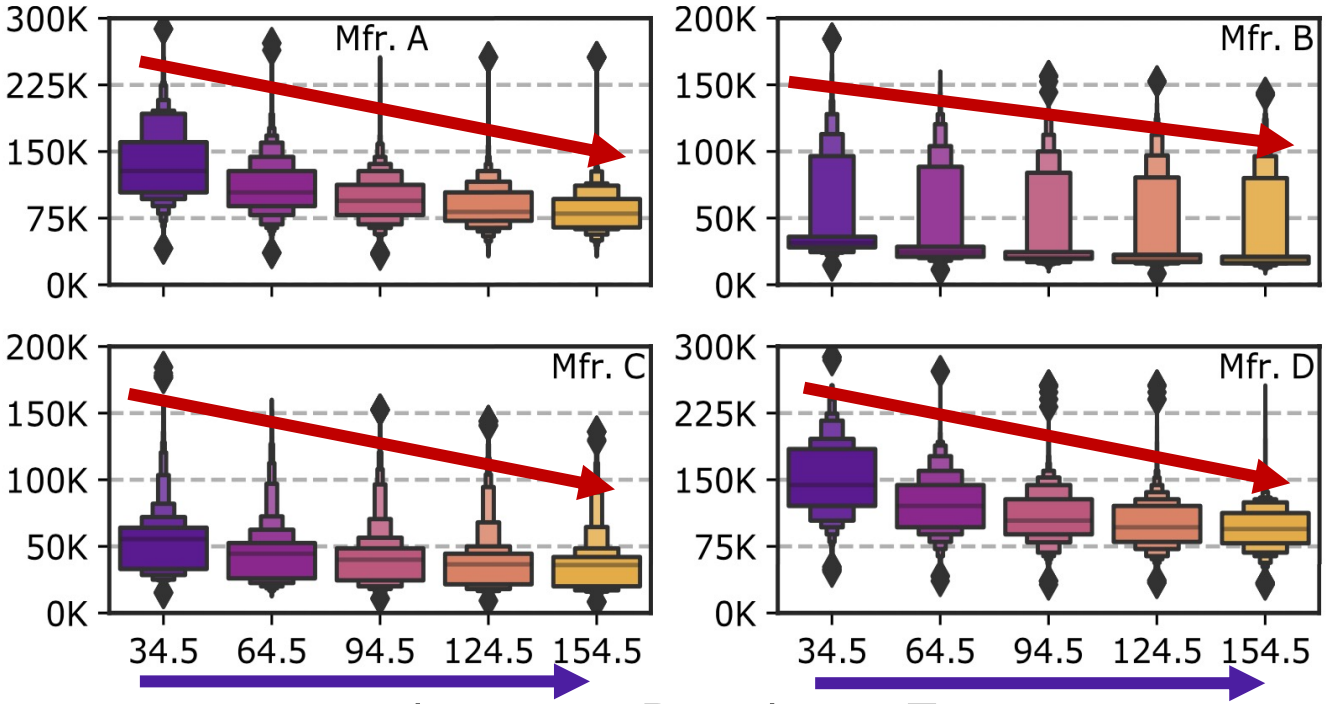
Manufacturing process variation causes **differences in cell size and bitline/wordline impedance values**, which introduces variation in cell reliability characteristics within and across DRAM chips

Design-induced variation causes cell access **latency characteristics to vary deterministically based on a cell's physical location** in the memory chip (e.g., its proximity to I/O circuitry)

Similarity across subarrays:

Cell's **access latency** is dominated by its **physical distance from the peripheral structures** (e.g., local senseamplifiers and wordline drivers) **within the subarray**, causing **corresponding cells in different subarrays to exhibit similar access latency** characteristics

Example Attack Improvements



- The attacker can **reduce HC_{first} (by 36%)** by **performing (10-15) additional READ** commands targeting the aggressor row **to bypass RowHammer defenses** that do not account for this reduction

These observations can be leveraged
to craft **more effective RowHammer attacks**