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

Presented at Micro 2021

Seminar in Computer Architecture

2022-06-02

Presented by Quirin Bitter

Executive Summary

Motivation

RowHammer is (still) a current and urgent problem. Modern DRAM chips are built denser and are therefore even more vulnerable.

Goal

Investigate the influence of the DRAM chip temperature, the aggressor row active time and DRAM cell location. Use the insights to design more efficient attacks and defenses.

Key Results

A RowHammer bit flip is more likely to occur

- in a bounded temperature range
- if the aggressor row stays active longer
- in certain locations of the DRAM module

Conclusion

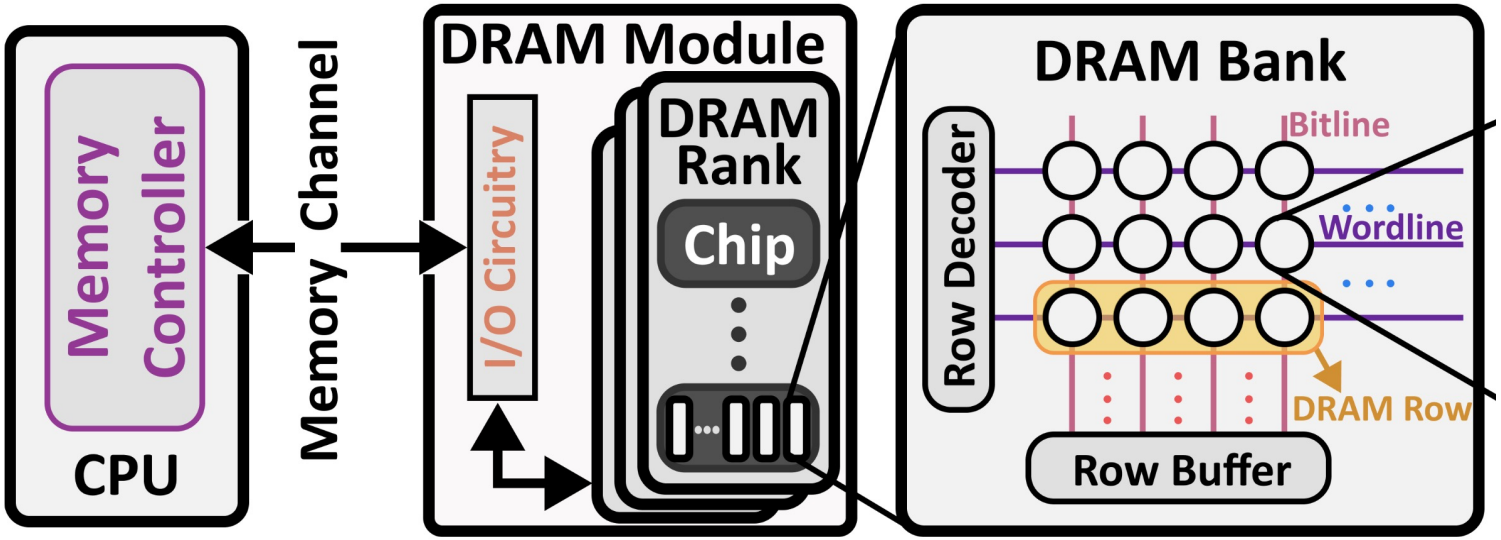
The novel observations aids future work in crafting more effective attacks and defenses.

Outline

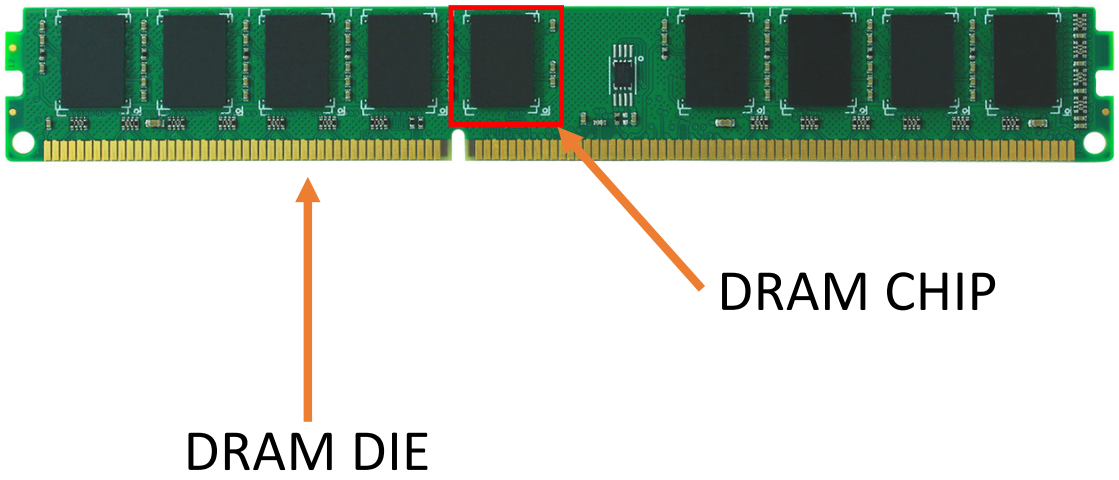
- Background
- Motivation
- Methodology
- Findings
- Improvements

Structure of DRAM

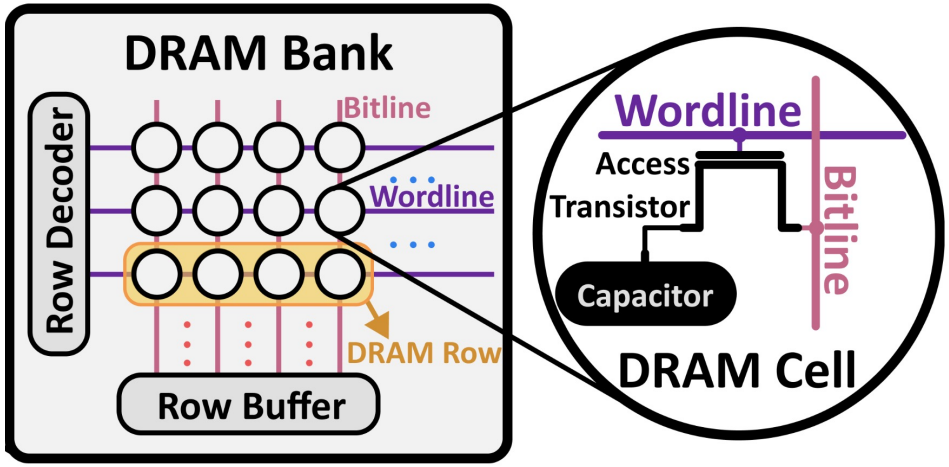
DRAM Module > DRAM Rank > DRAM Chip > DRAM Bank > DRAM Subarray



Structure of DRAM

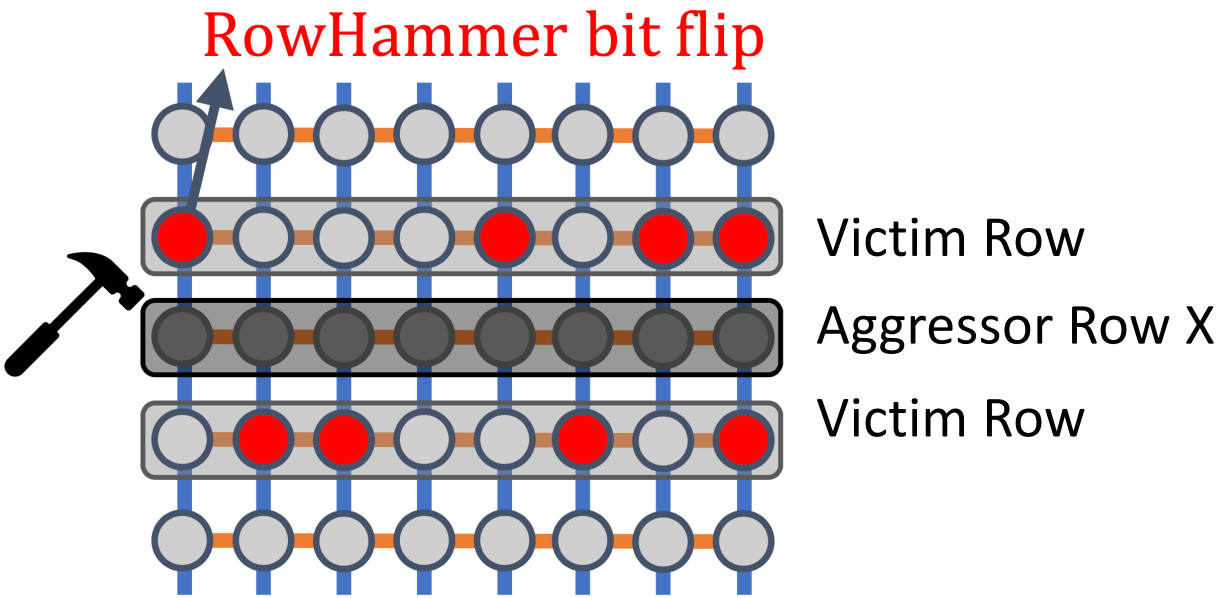


Structure of DRAM

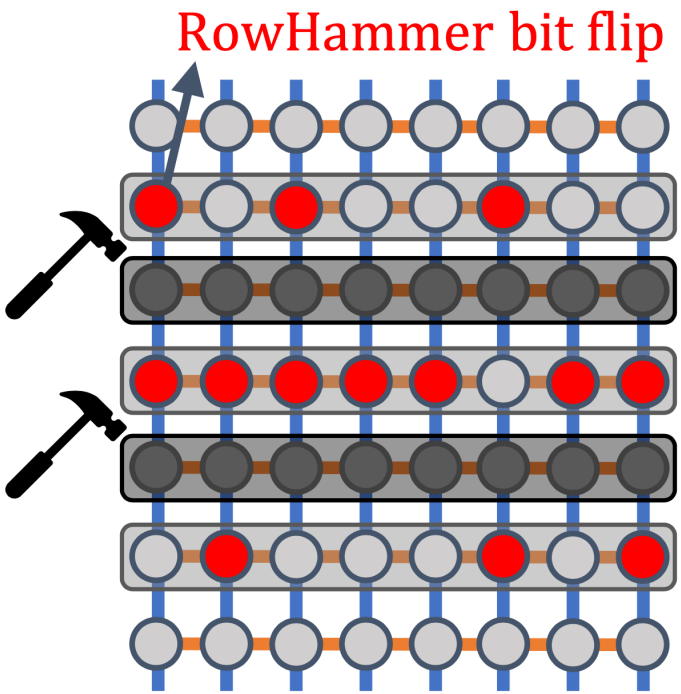


Note that the capacitor state must be restored after a row activation.

RowHammer Internals



RowHammer Internals



Victim Row

Aggressor Row X

Victim Row

Aggressor Row Y

Victim Row

One Hammer

```
loop:
  ACT X
  PRE
  ACT Y
  PRE
```

Notation

BER (bit error rate):

The number of bitflips in a DRAM row. The higher the BER, the more severe the vulnerability.

HC_{first} (hammer count first):

The number of “hammers” until the first bit flip occur. The lower the Hc_{first}, the more severe the vulnerability.

Outline

- Background
- Motivation
- Methodology
- Findings
- Improvements

Motivation

Rigorous analysis of

- DRAM chip temperature
- aggressor row active time
- physical location of victim cell

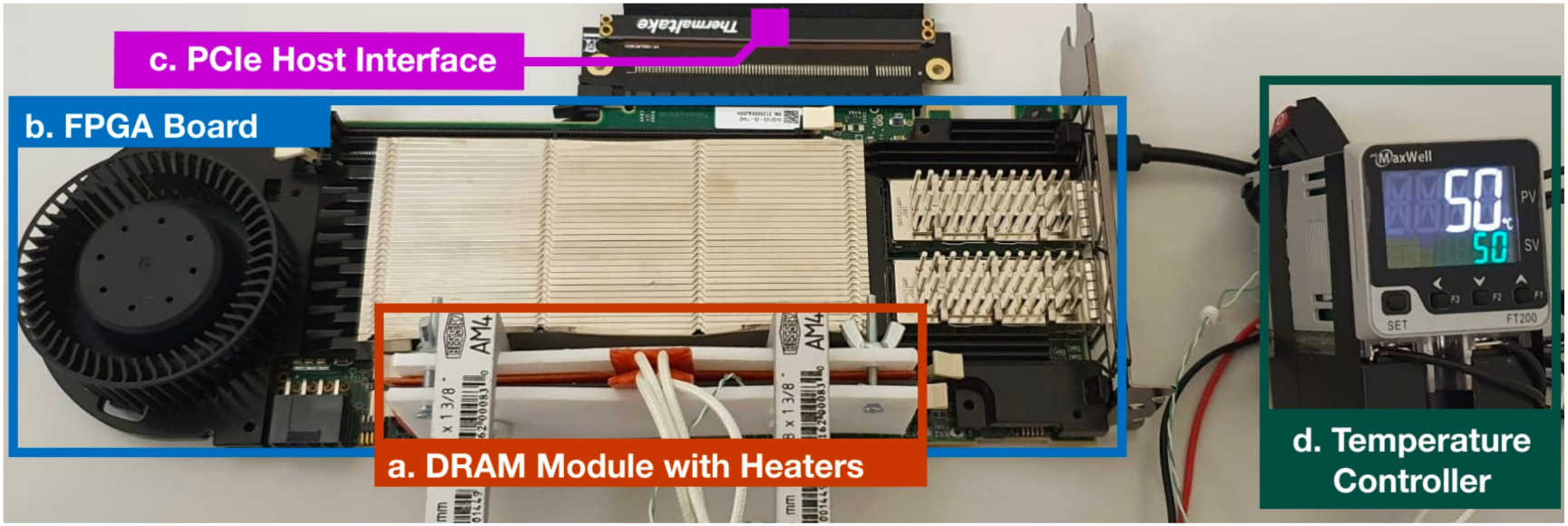
First rigorous analysis of these properties.

Preliminary work was not extensive enough.

Outline

- Background
- Motivation
- Methodology
- Findings
- Improvements

Methodology: SoftMC



SoftMC: A Flexible and Practical Open-Source Infrastructure for Enabling Experimental DRAM Studies – Hasan Hassan et al.

Methodology

- Disabled and avoided mitigation mechanisms to test a circuit rather than system level.

- Use RAM without ECC

- Use the most successful data patterns, identified from previous work

Row Address	Colstripe†	Checkered†	Rowstripe†	Random
$V^* \pm [0, 2, 4, 6, 8]$	0x55	0x55	0x00	random
$V^* \pm [1, 3, 5, 7]$	0x55	0xaa	0xff	random

*V is the physical address of the victim row

†We also test the complements of these patterns

Methodology

- Double-sided RowHammering at highest activation rate possible (limited by t_{RAS}, t_{RP})

- Logical to physical row mapping is identified first.
  Executed single sided RowHammering on a row.
  The row with the most bit flips are assumed to be adjacent.

- Temperature range: 50˚ - 90˚ Celsius with accuracy of ± 0.1˚

Outline

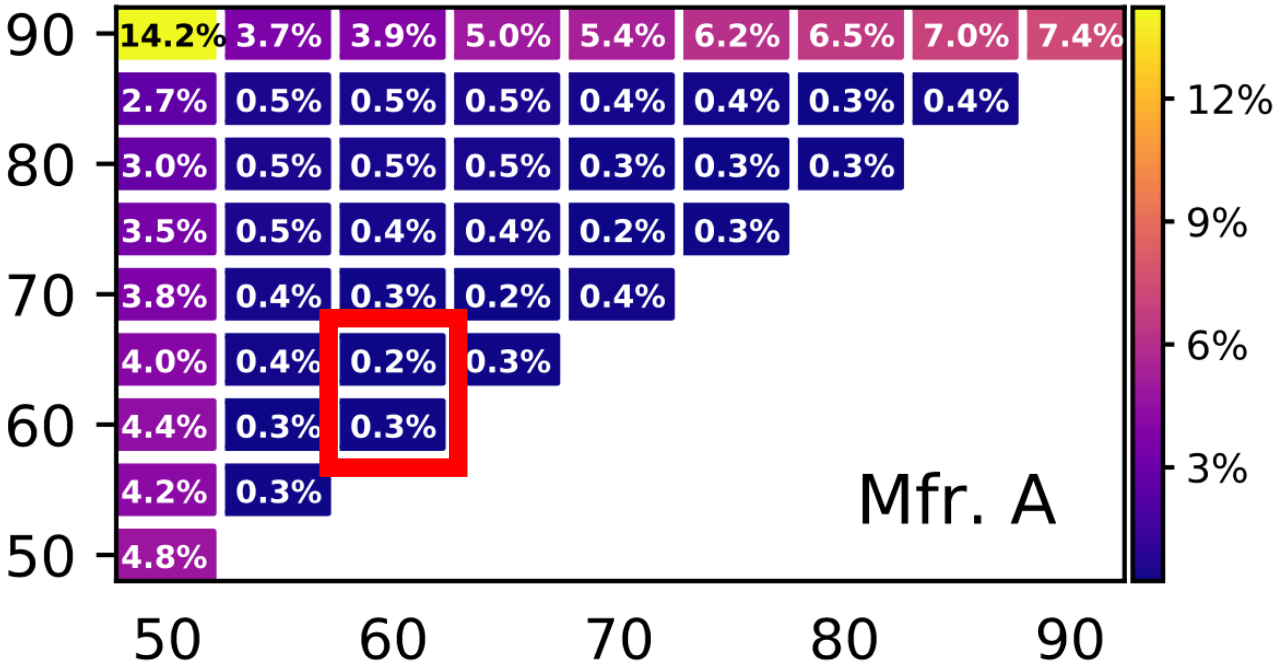
- Background
- Motivation
- Methodology
- Findings
- Improvements

Findings: Temperature Analysis

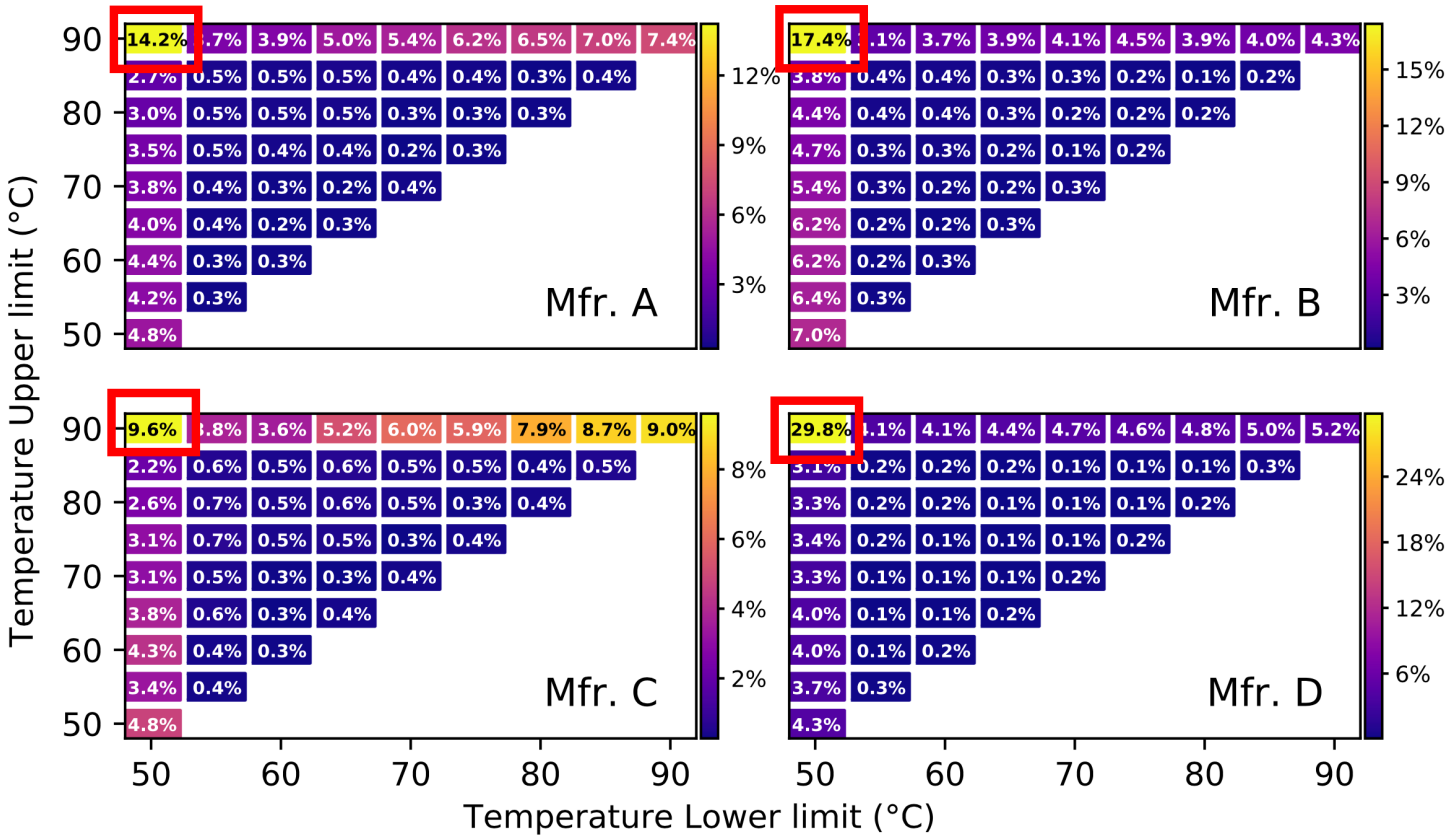
Analysis on Cells

- Cells are vulnerable at specific temperature range
- Most cells are vulnerable at all tested temperature ranges (50˚ - 90˚ Celsius with accuracy of ± 0.1˚)
- Small amount of cells are only vulnerable at a narrow temperature range

Findings: Temperature Analysis



Findings: Temperature Analysis



Findings: Temperature Analysis

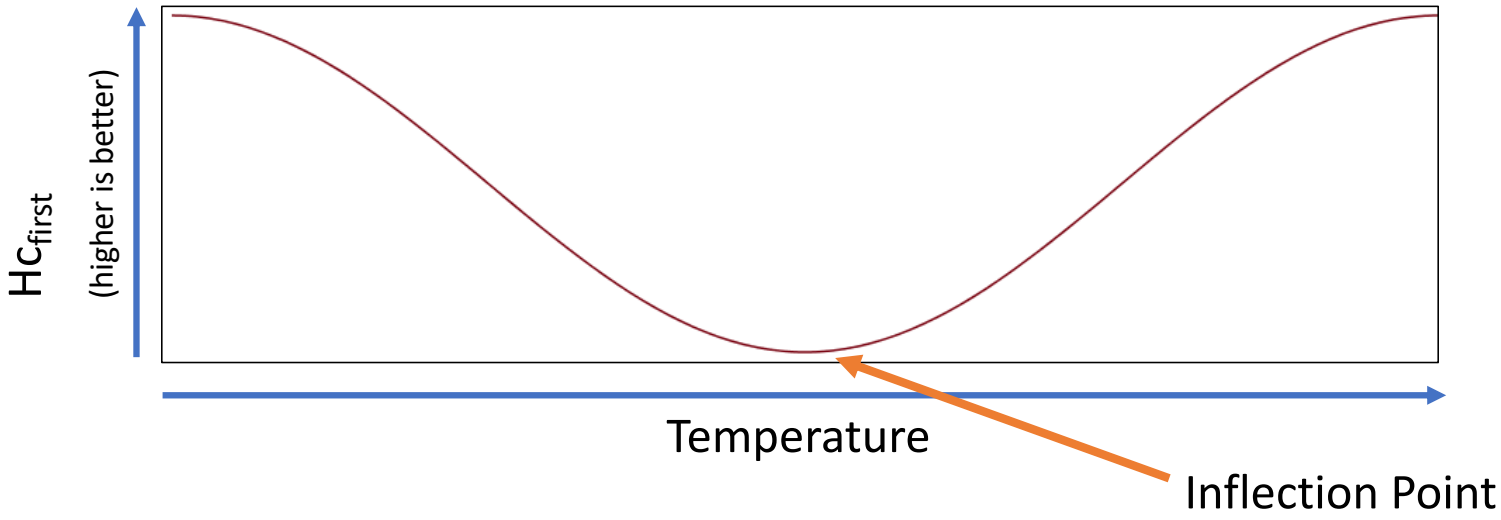
Analysis on Rows

- BER increases/decrease with an increasing temperature (depending on the DRAM manufacturer)
- HC_{first} generally decreases with the temperature increase
- HC_{first} changes tend to be larger at larger temperature changes

For argumentation about RowHammer security one must consider all operating temperatures.

Findings: Temperature Analysis

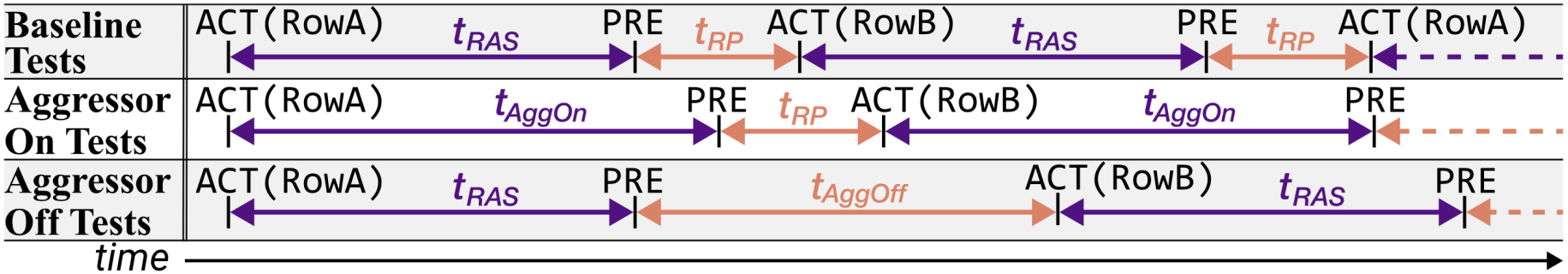
Circuit-Level Justification



[Trap-Assisted DRAM Row Hammer Effect]
Thomas Yang and Xi-Wei Lin

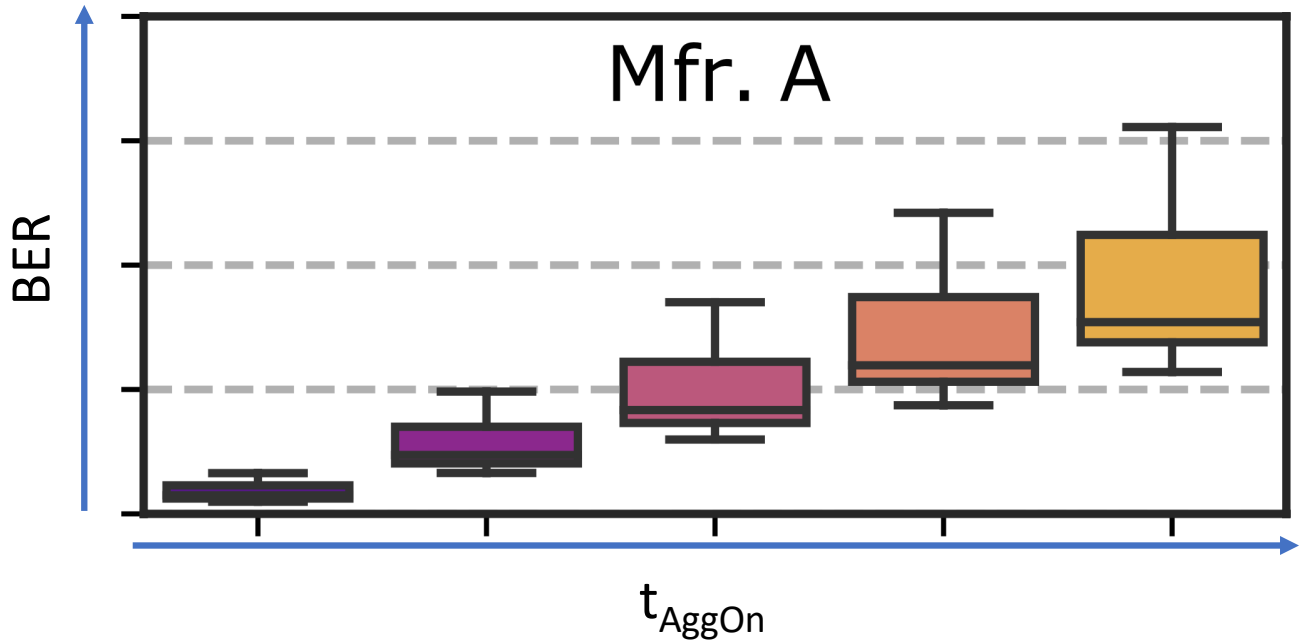
Findings: Aggressor Row Active Time

$\mathbf{t_{RAS}}$ = "minimum time after activation before pre-charge command"
$\mathbf{t_{RP}}$ = "minimum time after pre-charge command before the next activation command"



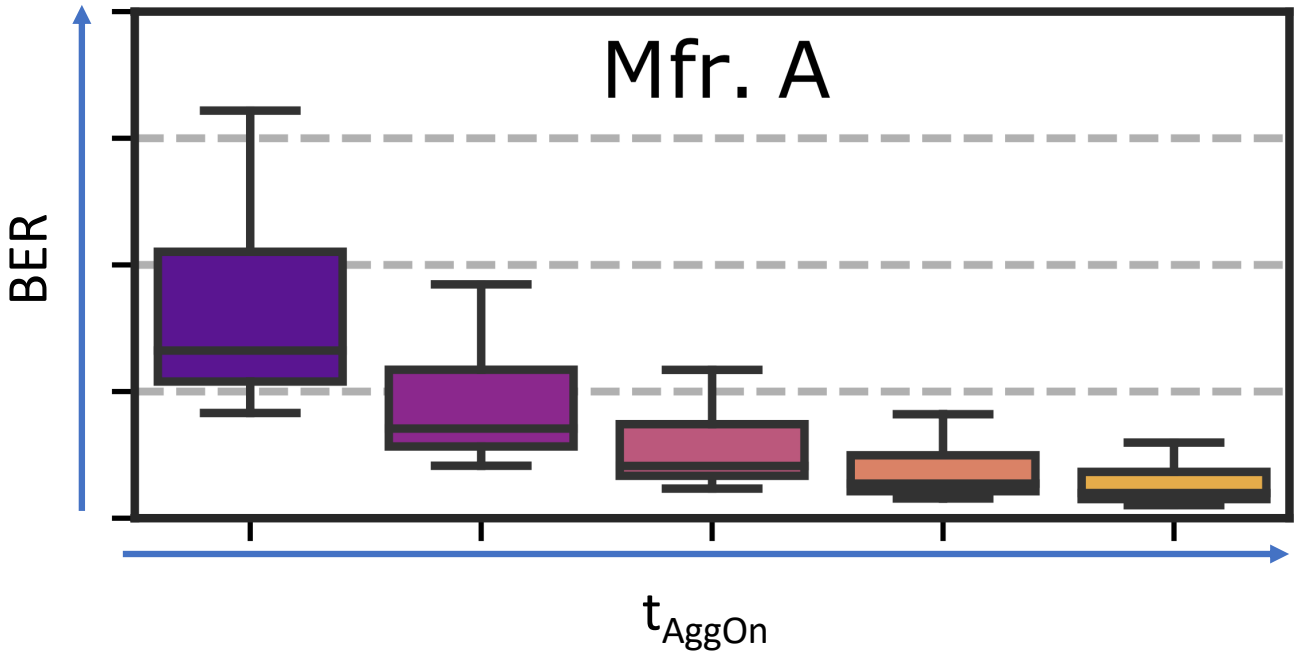
Findings: Aggressor Row Active Time

Impact OnTime: Increasing t_{AggOn} leads to bit flips for more cells at lower hammer counts. Facilitates Row Hammer.



Findings: Aggressor Row Active Time

Impact OffTime: Increasing t_{AggOff} leads to bit flips for less cells at higher hammer counts. Impedes RowHammer.



Findings: Aggressor Row Active Time

Circuit-Level Justification

Reasons for RowHammer bit flips:

- Electron injection into victim cell
- Wordline-to-Wordline cross talk noise

Hypothesis:

Increased electron injection causes the observed behavior.

Findings: Spatial Variation

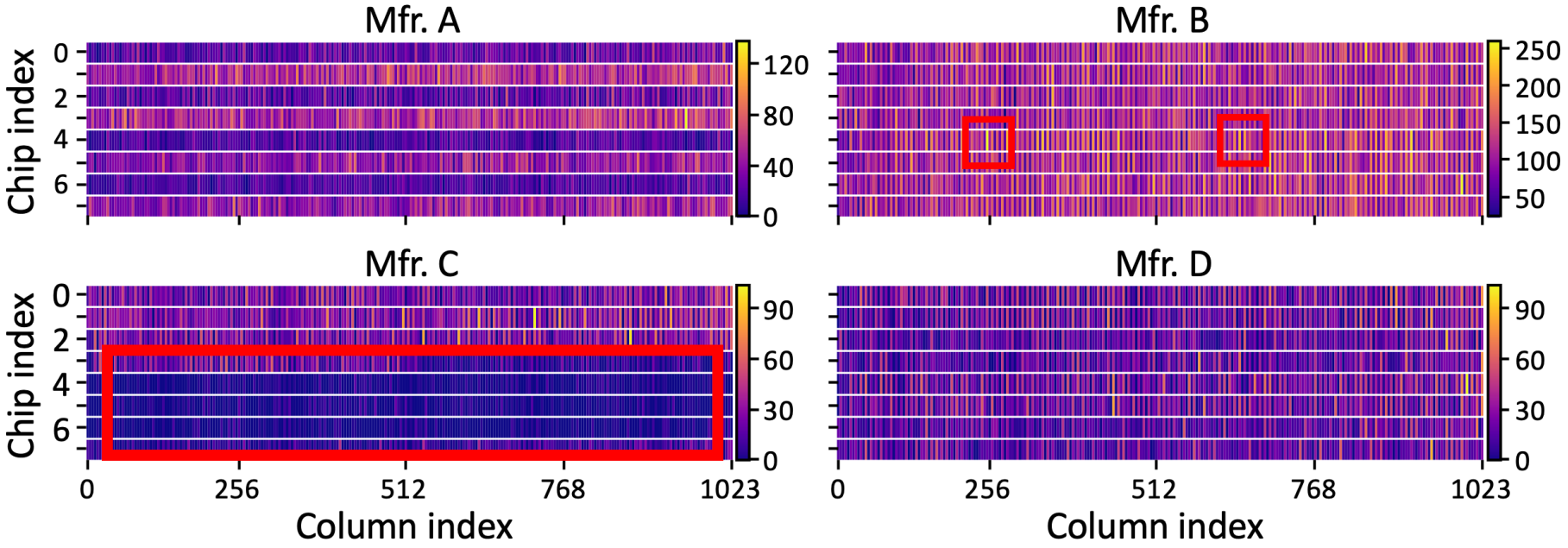
Variation across Rows:
Small number of rows shows lower HC_{first}

Variation across Columns:

Some columns are significantly more vulnerable.

Design/Variation of/in the manufacturing process influence the column vulnerability.

Findings: Spatial Variation



Findings: Spatial Variation

Circuit-Level Justification

Manufacturing process variation causes differences in the cell size and the wordline/bitline impedance values,

and

design-induced variation causes cell access latency based on cell location.

$\Longrightarrow$ observed difference in vulnerability based on location.

Outline

- Background
- Motivation
- Methodology
- Findings
- Improvements

Improvements

Improvements on Attacking with RowHammer

- RowHammer attack may be more successful if attacker can control the target temperature
- RowHammer can be used as temperature dependent trigger
- Increase aggressor row active time to reduce HC_{first}

Improvements

Improvements on Defense against RowHammer

- Trigger mitigation mechanisms for higher HC_{first}
- Monitor temperature and disable rows which are vulnerable at the current temperature
- Keep overall temperature low

Improvements

Improvements on Defense against RowHammer

- Monitor (aggressor) row active time
- Optimize ECC for non-uniform bit errors and chipkill to disable most vulnerable DRAM chips

Executive Summary - Conclusion

Motivation

RowHammer is (still) a current and urgent problem. Modern DRAM chips are built denser and are therefore even more vulnerable.

Goal

Investigate the influence of the DRAM chip temperature, the aggressor row active time and DRAM cell location. Use the insights to design more efficient attacks and defenses.

Key Results

A RowHammer bit flip is more likely to occur

- in a bounded temperature range
- if the aggressor row stays active longer
- in certain locations of the DRAM module

Conclusion

The novel observations aids future work in crafting more effective attacks and defenses.

Further References

- First Paper Covering RowHammer
  Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors – Kim et al.

- Conclusion & Perspective
  The RowHammer Problem and Other Issues We May Face as Memory Becomes Denser – Onur Mutlu

- Physical Background
  On DRAM Rowhammer and the Physics of Insecurity – Walker et al.

Questions

Strengths

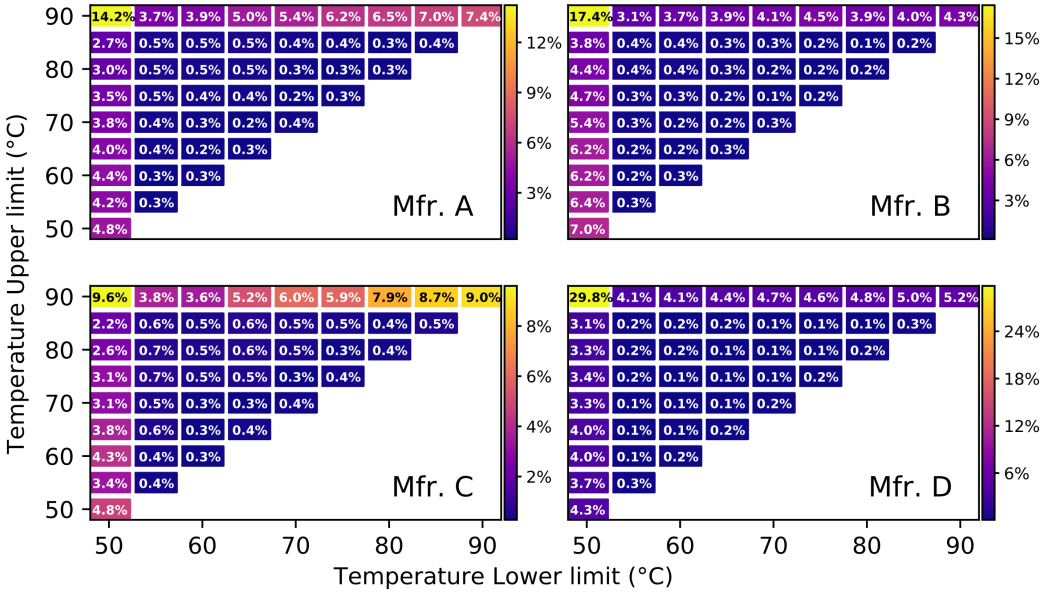
- Rigorous in many ways
  - Result are described in great detail
  - Environment is well documented – reader could reproduce results
  - Tested 272 real DRAM chips
- Proposing further attacks and defenses
- Indirectly describes how RowHammer could be used for temperature measurement

Weaknesses

- Spatial Variation analysis conducted at fix temperature point (75˚ C)
- Further work could have considered influence of mitigation mechanisms

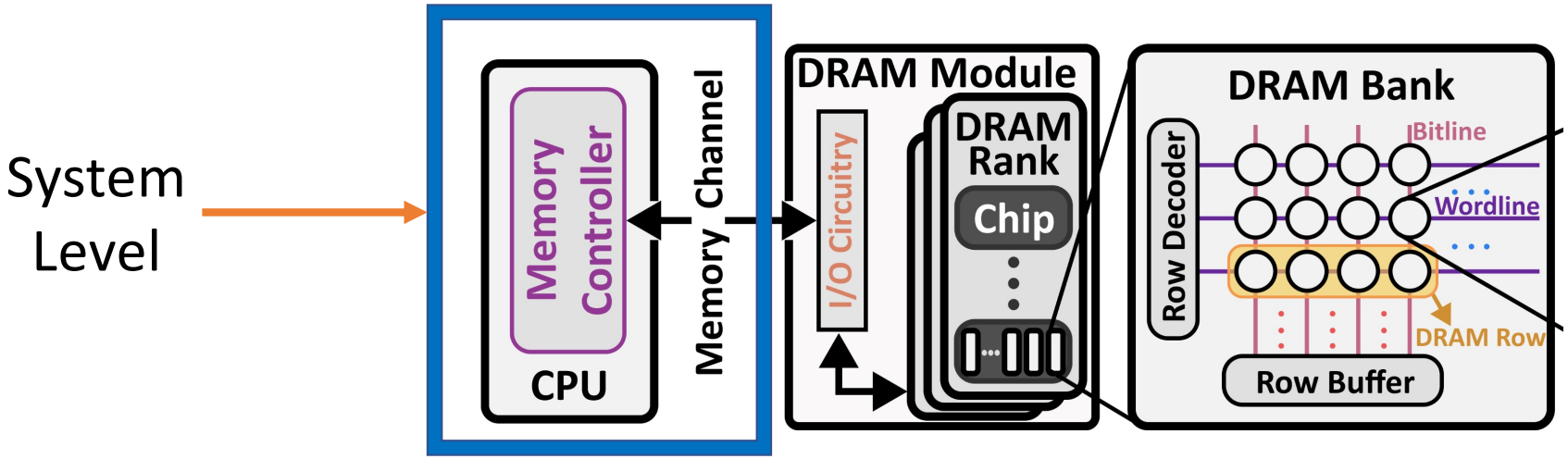
Discussion

As RowHammer can be used to measure temperatures, could you imagine attacks that are temperature triggered?



Discussion

The paper investigates RowHammer on circuit level. Would you also consider the System Level (for defense mechanisms)?



Discussion

Should one accept a higher RowHammer vulnerability for better DRAM performance?