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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>99.1%</td>
<td>98.9%</td>
<td>98.0%</td>
<td>99.2%</td>
</tr>
</tbody>
</table>

**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**

Vulnerable Temperature Range

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Vulnerable Temperature Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>50°C</td>
<td></td>
</tr>
<tr>
<td>90°C</td>
<td></td>
</tr>
</tbody>
</table>

**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**

Vulnerable Temperature Range

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Vulnerable Temperature Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>70°C</td>
<td></td>
</tr>
</tbody>
</table>

No bit flips

SAFARI
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:
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**

Minimum Activation Count to Observe a Bit Flip ($HC_{first}$)
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.
A small fraction of DRAM rows are significantly more vulnerable to RowHammer than the vast majority of the rows.

Minimum Activation Count to Observe a Bit Flip ($HC_{first}$)

[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. Heating up or cooling down the chip temperature can cause bit flips outside this range.

- No bit flips within the range of 50°C to 70°C.
- Bit flips occur at temperatures outside this range:
  - Heating up: 45°C to 55°C
  - Cooling down: 65°C to 75°C

[More Attack Improvements in the paper]
Defense Improvement: Leveraging the variation across DRAM rows

Breakdown of DRAM Rows

$10\%$ $\rightarrow H C_{first}$

$90\%$ $\rightarrow 2 \times H C_{first}$

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
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
DRAM Organization

DRAM Chip

Bank

Chip I/O

DRAM Bank

Subarray

DRAM Subarray

Bitline

DRAM Cell

Wordline

Row Buffer

DRAM Row

SAFARI
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

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

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

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

- **Two DRAM standards**
- **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 Yağlıkç*  
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.

<table>
<thead>
<tr>
<th>Type</th>
<th>Chip Manufacturer</th>
<th>Chip Identifier</th>
<th>Module Vendor</th>
<th>Module Identifier</th>
<th>Freq. (MT/s)</th>
<th>Date Code</th>
<th>Density</th>
<th>Die Rev.</th>
<th>Org.</th>
<th>#Modules</th>
<th>#Chips</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C: SK Hynix</td>
<td>D1024N9CQBGK</td>
<td>G.SKILL</td>
<td>F4-2400C17S-8GNT [35]</td>
<td>2400</td>
<td>2012</td>
<td>4Gb</td>
<td>B</td>
<td>x8</td>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>D: Nanya</td>
<td>D1028N9CQBGK</td>
<td>Kingston</td>
<td>K9V264M7S8-3 [75]</td>
<td>2400</td>
<td>2016</td>
<td>8Gb</td>
<td>C</td>
<td>x8</td>
<td>4</td>
<td>32</td>
</tr>
</tbody>
</table>

| DDR3 | A: Micron | MT4K512M8JA-167-F [22] | Crucial | CT5124BF16DJMLFP | 1600 | 1703 | 4Gb | P | x8 | 1 | 5 |
| | B: Samsung | K4B4G0846Q | Samsung | M471B5179Q1F0-YK0 [131] | 1600 | 3416 | 4Gb | Q | x8 | 1 | 8 |
| | C: SK Hynix | H5TC4G83FR-PBA | SK Hynix | HMT451S6BFR-A7 [139] | 1600 | 1535 | 4Gb | B | x8 | 1 | 8 |
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

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Lower Bound</th>
<th>Upper Bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mfr. A</td>
<td>99.1%</td>
<td></td>
</tr>
<tr>
<td>Mfr. B</td>
<td>98.9%</td>
<td></td>
</tr>
<tr>
<td>Mfr. C</td>
<td>98.0%</td>
<td></td>
</tr>
<tr>
<td>Mfr. D</td>
<td>99.2%</td>
<td></td>
</tr>
</tbody>
</table>

**Observation 1**

Most DRAM cells are vulnerable to RowHammer throughout a continuous temperature range
Different DRAM cells are vulnerable to RowHammer within specific temperature ranges.
OBSERVATION 2

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

**29.8%** of the cells experience bit flips at all tested temperatures.
A small fraction of all vulnerable DRAM cells are vulnerable to RowHammer only in a very narrow temperature range.

0.2% of the cells experience bit flips only at 70°C.
Impact of Temperature on DRAM Rows

More cells experience bit flips as temperature increases
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 ($HC_{\text{first}}$) when **temperature changes**:

<table>
<thead>
<tr>
<th>OBSERVATION 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM rows can show either <strong>higher</strong> or <strong>lower</strong> $HC_{\text{first}}$ when <strong>temperature</strong> increases</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBSERVATION 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$HC_{\text{first}}$ tends to generally <strong>decrease</strong> as <strong>temperature change</strong> ($\Delta T$) increases</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBSERVATION 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>The $HC_{\text{first}}$ change ($\Delta HC_{\text{first}}$) tends to be <strong>larger</strong> as <strong>temperature change</strong> ($\Delta T$) increases</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Author</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lois Orosa</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>A. Giray Yaşlıkçı*</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Haocong Luo</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Ataberk Olgun</td>
<td>ETH Zürich, TOBB ETÜ</td>
</tr>
<tr>
<td>Jisung Park</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Hasan Hassan</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Minesh Patel</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Jeremie S. Kim</td>
<td>ETH Zürich</td>
</tr>
<tr>
<td>Onur Mutlu</td>
<td>ETH Zürich</td>
</tr>
</tbody>
</table>

### 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

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

**OBSERVATION 8**
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 Yaşılıkçı* 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
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.
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

High RowHammer vulnerability across all chips → design-induced variation

Larger Variation across DRAM Chips

High variation in vulnerability across chips → manufacturing-process-induced variation

SAFARI
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.
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**

---

**Vulnerable Temperature Range**

- **50°C**
- **55°C**
- **65°C**
- **70°C**

- **45°C**
- **55°C**
- **65°C**
- **75°C**

**Heating up chip temperature**

**Cooling down chip temperature**

---

*SAFARI*
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:

- Row A is active
- Row B is active
- Row A is active

Keeping the aggressor rows active for a longer time:

- Row A is active
- Row B is active

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

- A DRAM cell experiences **bit flips** within a **bounded temperature range**
- A row can be **disabled** within the row’s **vulnerable temperature range**

\[ \text{Breakdown of DRAM Rows} \]

- 10% \[ HC_{first} \]
- 90% \[ 2 \times HC_{first} \]

**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

**Vulnerable Temperature Range**

- A DRAM cell experiences **bit flips** within a **bounded temperature range**
- A row can be **disabled** within the row’s **vulnerable temperature range**

\[ \text{Breakdown of DRAM Rows} \]

- Disable RowA
- Disable RowB
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.
• 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*  A. Giray Yağlıkçı*  Haocong Luo  Ataberk Olgun  Jisung Park
ETH Zürich  ETH Zürich  ETH Zürich  ETH Zürich, TOBB ETÜ  ETH Zürich
Hasan Hassan  Minesh Patel  Jeremie S. Kim  Onur Mutlu
ETH Zürich  ETH Zürich  ETH Zürich  ETH Zürich

• Cooling DRAM chips can reduce overall bit error rate.
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 $HC_{first}$

Percentage Change in Minimum Activation Count to Observe a Bit Flip ($HC_{first}$)

Temperature change
- From 50°C to 55°C
- From 50°C to 90°C

Rows Ordered by $HC_{First}$ change

Less Vulnerable

More Vulnerable
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 $HC_{\text{first}}$

**OBSERVATION 6**

$HC_{\text{first}}$ tends to generally **decrease** as **temperature change** ($\Delta T$) increases.
Distribution of the Change in $HC_{first}$

OBSERVATION 7

The $HC_{first}$ change ($\Delta HC_{first}$) tends to be larger as temperature change ($\Delta T$) 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. The 3D TCAD model [Yang+, EDL'19] is used to analyze these effects.

![Graph showing temperature vs. N_{RH}(10^3) for different traps.](image)

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

$H_{C_{first}}$ decreases as temperature increases, until a temperature inflection point where $H_{C_{first}}$ 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 ($t_{\text{AggOn}}$)

**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 $HC_{\text{first}}$ change across rows when the **aggressor row stays active longer**

**OBSERVATION 9**

RowHammer vulnerability **consistently worsens** as $t_{\text{AggOn}}$ 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 ($t_{\text{AggOff}}$)

<table>
<thead>
<tr>
<th>ACT (RowA)</th>
<th>$t_{\text{RAS}}$</th>
<th>PRE</th>
<th>$t_{\text{AggOff}}$</th>
<th>ACT (RowB)</th>
<th>$t_{\text{RAS}}$</th>
<th>PRE</th>
</tr>
</thead>
</table>

### Bit Error Rate

- **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 $t_{\text{AggOff}}$ increases** across all tested DRAM rows**

---

*Coefficient of Variation (CV) = \( \frac{\text{Standard Deviation}}{\text{Average}} \)

** 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

Minimum Activation Count to Observe a Bit Flip ($HC_{first}$)

$HC_{first}$ worst-to-best ratio in this range: $P100/P90$

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
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 $HC_{\text{first}}$ (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.