Revisiting RowHammer: An Experimental Analysis of Modern DRAM Devices and Mitigation Techniques

Jeremie Kim[1,2], Minesh Patel[1], A. Giray Yağlıkçı[1],
Hasan Hassan[1], Roknoddin Azizi[1], Lois Orosa[1], and Onur Mutlu[1,2]

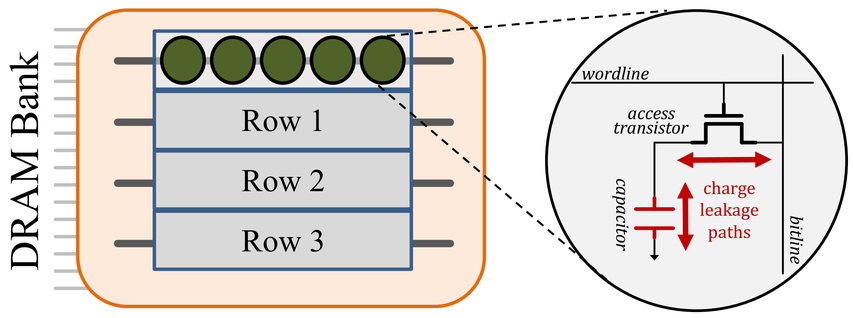
[1] ETH zürich [2] Carnegie Mellon

SAFARI

Full Paper
https://people.inf.ethz.ch/omutlu/pub/Revisiting-RowHammer_isca20.pdf

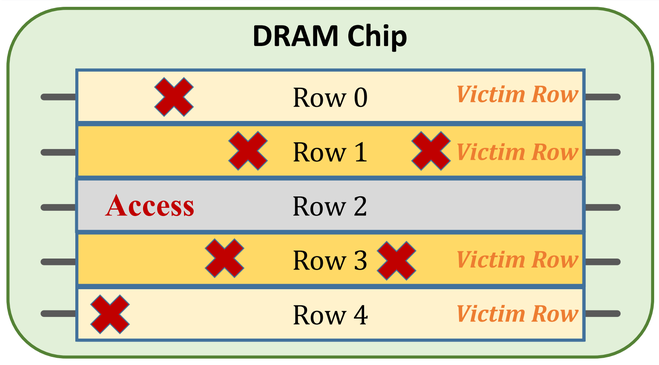
Full Talk Video
https://www.youtube.com/watch?v=Lqxc4_ToMUw

1: DRAM Background

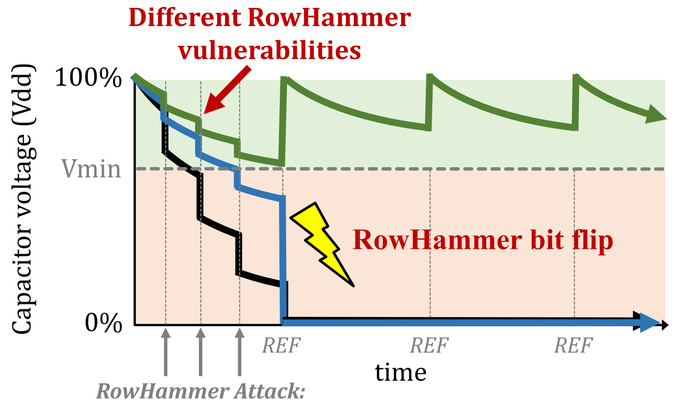


Stored data is **corrupted** if too much charge leaks (i.e., the capacitor voltage degrades too much)
DRAM cells are refreshed periodically to maintain data correctness

2: The RowHammer Phenomenon



Repeatedly **opening (ACT)** and **closing (PRE)** a DRAM row causes failures in nearby rows



If a nearby row is activated enough times within a refresh window, the charge leakage rate can be accelerated to the point of **failure.** Some cells require more hammers to fail.

3: Motivation

- Denser DRAM chips are **more vulnerable** to RowHammer
- **No comprehensive experimental study** demonstrating **how vulnerability scales** across DRAM types and tech node sizes
- **Unclear whether current mitigation mechanisms will remain viable** for future DRAM chips that are likely to be more vulnerable to RowHammer

4: Our Goal

1. **Experimentally demonstrate** how vulnerable modern DRAM chips are to RowHammer and **predict how this vulnerability will scale** going forward
2. Examine the viability of current mitigation mechanisms on **more vulnerable chips**

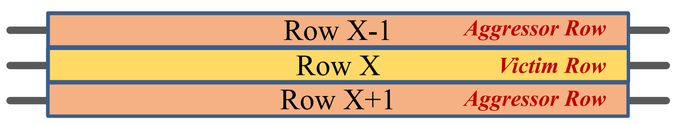
5: Experimental Methodology

1580 total chips tested from **300** modules

DRAM type-node	Number of Chips (Modules) Tested *Mfr. A*	*Mfr. B*	*Mfr. C*	*Total*
DDR3-old	56 (10)	88 (11)	28 (7)	**172 (28)**
DDR3-new	80 (10)	52 (9)	104 (13)	**236 (32)**
DDR4-old	112 (16)	24 (3)	128 (18)	**264 (37)**
DDR4-new	264 (43)	16 (2)	108 (28)	**388 (73)**
LPDDR4-1x	12 (3)	180 (45)	N/A	**192 (48)**
LPDDR4-1y	184 (46)	N/A	144 (36)	**328 (82)**

Experimental Testing Infrastructures
1. **DDR3:** SoftMC [Hassan+, HPCA'17] (Xilinx ML605)
2. **DDR4:** SoftMC [Hassan+, HPCA'17] (Xilinx Virtex UltraScale 95)
3. **LPDDR4:** In-house testing hardware

1. **Prevent sources of interference during core test loop**
We disable:
DRAM refresh: to avoid refreshing victim row
DRAM calibration events: to minimize variation in test timing
RowHammer mitigation mechanisms: to observe circuit-level effects
Test for **less than 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 directly physically-adjacent rows as fast as possible**

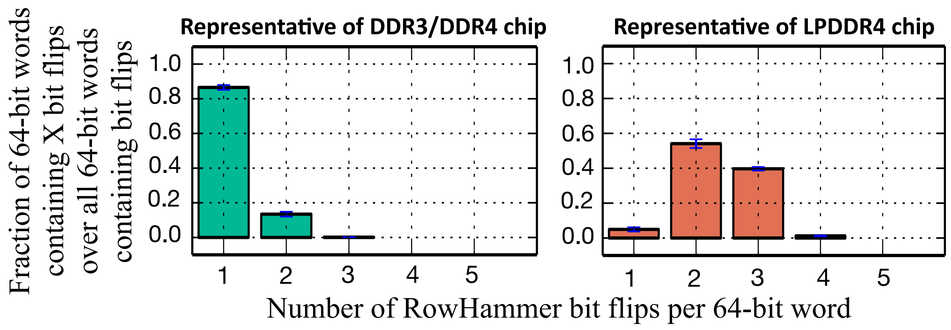


6: Characterization Results

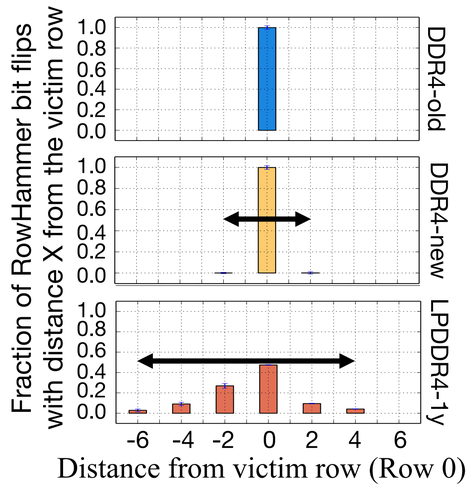
a) RowHammer Vulnerability
- **Newer DRAM chips are more vulnerable to RowHammer**

b) Data Pattern Dependence
- Worst-case data pattern is **same for chips** of same mfg. and type-node config.

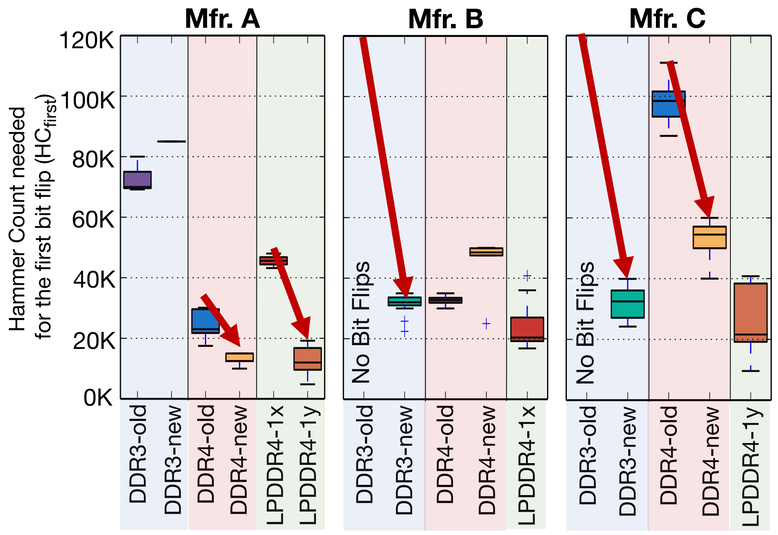
c) Hammer Count Effects
- **RowHammer bit flip rates increase with technology node generation**



d) Hammer Count Effects
- The distribution of RowHammer bit flip density per word **changes in LPDDR4 chips** from other DRAM types likely due to **on-die ECC**
- At a bit flip rate of 10^{-6}, a 64-bit word can contain up to **4 bit flips**. Even at this very low bit flip rate, a **very strong ECC** is required to prevent failures



e) Spatial Effects
- The number of RowHammer bit flips that occur in a given row decreases as the distance from the **victim row (row 0)** increases
- Chips of newer DRAM technology nodes can exhibit RowHammer bit flips 1) in **more rows** and 2) **farther away** from the victim row



f) First RowHammer Failure per Chip
- In a DRAM type, **HC_{first} reduces significantly** from old to new chips, i.e., **DDR3:** 69.2k to 22.4k, **DDR4:** 17.5k to 10k, **LPDDR4:** 16.8k to 4.8k
- In LPDDR4-1y chips from manufacturer A, there are chips whose weakest cells fail after only **4800 hammers**

7: Evaluation of Mitigation Mechanisms

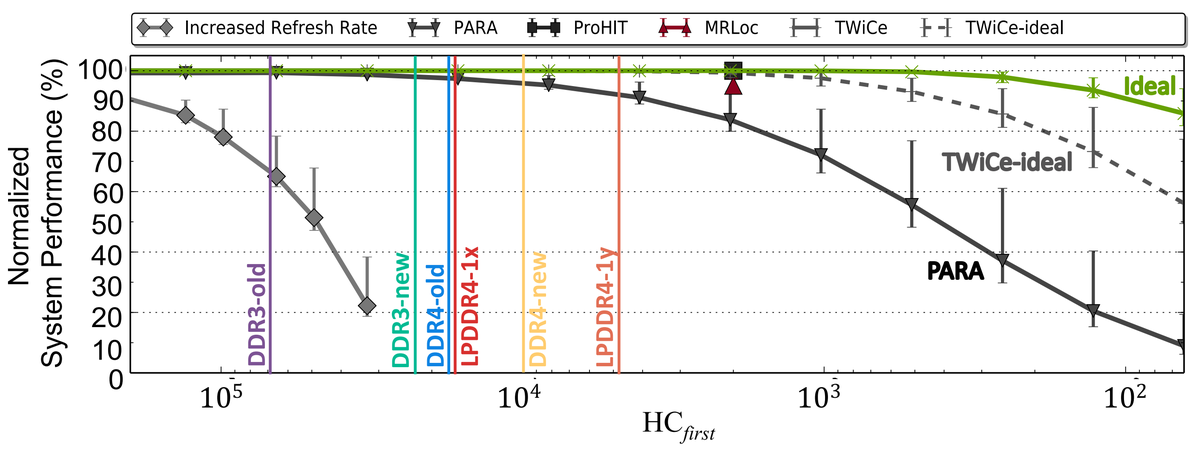
Increased Refresh Rate: Substantial overhead for high HC_{first} values. **Prohibitively high refresh rates** required for **HC_{first} < 32k.**

PARA: **Scales to low HC_{first} values**, but significantly high performance overheads **(e.g., 80% performance loss when HC_{first} = 128).**

ProHIT **MRLoc:** Models for scaling ProHIT and MRLoc for **HC_{first} < 2k** are not provided and how to do so is not intuitive.

TWiCe: **Does not support HC_{first} < 32k**, but we evaluate an ideal version ignoring two critical issues. Ideal performs better than PARA.

Ideal: ideal refresh-based mechanism provides reasonably high normalized system performance across all tested HC_{first} values.



Key Takeaways

1. **PARA, ProHIT, and MRLoc** mitigate RowHammer bit flips in **worst chips** with reasonable performance (92%, 100%, 100%)

2. **Only PARA scales to low HC_{first}** but has **low normalized system performance**

3. **Ideal** mechanism is **significantly better** than existing mechanisms for **HC_{first} < 1024**

4. **Significant opportunity** for developing a scalable and low overhead solution

8: Future Work and Conclusion

Future Research Directions

1. **DRAM-system cooperation**
- A DRAM-based or system-level mechanism alone ignores potential benefits of a holistic solution

2. **Profile-guided**
- Accurately profiling RowHammer-susceptible cells in DRAM provides a powerful substrate for building targeted RowHammer solutions e.g.:
  - **Increasing refresh rate:** increase refresh rate for rows with RowHammer-susceptible cell
  - **Access counters:** only count accesses to rows containing RowHammer-susceptible cells
- A **fast and accurate** profiling mechanism is a key research challenge for developing low-overhead and scalable RowHammer solutions

Conclusion: It is critical to research more effective solutions to RowHammer for future DRAM chips that will likely be even more vulnerable to RowHammer