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

Jeremie S. Kim Minesh Patel A. Giray Yağlıkçı Hasan Hassan Roknoddin Azizi Lois Orosa Onur Mutlu

UC RIVERSIDE

CONTENT

UC RIVERSIDE

01 INTRODUCTION

RowHammer is a circuit-level DRAM vulnerability where repeatedly accessing data in a DRAM row can cause bit flips in nearby rows.

Since it stems from physical circuit-level so that interference effects can be worsen with continued DRAM density scaling as DRAM manufacturers primarily depend on density scaling to increase DRAM capacity.

Many RowHammer mitigation mechanisms from both industry and academia can help while existing mechanisms either are not scalable or suffer from large performance overheads in future devices given the observed trends of RowHammer vulnerability.

Recently a hypothesis has been identified as a precise circuit-level charge leakage mechanism that may be responsible for RowHammer. This leakage mechanism affects nearby circuit components, which implies that as manufacturers continue to employ aggressive technology scaling for generational storage density improvements, circuit components that are more tightly packed will likely increase a chip's vulnerability to RowHammer.

01 INTRODUCTION

To mitigate the impact of the RowHammer problem, numerous works proposed. These include mechanisms to make RowHammer conditions impossible or very difficult to attain and mechanisms that explicitly detect RowHammer conditions and intervene. However, all of these solutions merely treat the symptoms of a RowHammer attack without solving the core circuit vulnerability.

Our goal in this work is to experimentally demonstrate how vulnerable modern DRAM chips are to RowHammer at the circuit-level and to study how this vulnerability will scale going forward with rigorous experiments from 300 modern DRAM modules from across all three major DRAM manufacturers.

- disable all accessible RowHammer mitigation mechanisms.

01 INTRODUCTION

- We provide the first rigorous RowHammer failure characterization study of a broad range of real modern DRAM chips across different SDRAM types, technology node generations, and manufacturers. We experimentally study 1580 DRAM chips from 300 DRAM modules and present our RowHammer characterization results for both aggregate RowHammer failure rates and the behavior of individual cells while sweeping the hammer count (HC) and stored data pattern.
- Via our rigorous characterization studies, we definitively demonstrate that the RowHammer vulnerability significantly worsens in newer DRAM chips
- We demonstrate, based on our rigorous evaluation of five state-of-the-art RowHammer mitigation mechanisms, that even though existing RowHammer mitigation mechanisms are reasonably effective at mitigating RowHammer in today's DRAM chips, they will cause significant overhead in future DRAM chips with even lower HCfirst values.
- We evaluate an ideal refresh-based mitigation mechanism that selectively refreshes a row only just before it is about to experience a RowHammer bit flip, and find that in chips with high vulnerability to RowHammer, there is still a significant opportunity for developing a refresh-based RowHammer mitigation mechanism with low-performance overhead that scales to low HCfirst values. We conclude that it is critical to research more effective solutions to RowHammer, and we provide promising directions for future research.

02 MOTIVATION

Despite the considerable research effort expended towards understanding and mitigating RowHammer, scientific literature still lacks rigorous experimental data on how the RowHammer vulnerability is changing with the advancement of DRAM designs and process technologies.

Difficulties to address with existing data:

- How vulnerable to RowHammer are future DRAM chips expected to be at the circuit level?
- What types of RowHammer solutions would cope best with increased circuit-level vulnerability due to continued technology node scaling?

Evaluate and understand how the RowHammer vulnerability of real DRAM chips at the circuit level changes across different chip types, manufacturers, and process technology node generations. Doing so enables us to predict how the RowHammer vulnerability in DRAM chips will scale as the industry continues to increase storage density and reduce technology node size for future chip designs.

3.1 Testing Infrastructure

(1) the SoftMC framework capable of testing DDR3 and DDR4 DRAM modules in a temperature-controlled chamber and (2) an in-house temperature-controlled testing chamber capable of testing LPDDR4 DRAM chips.

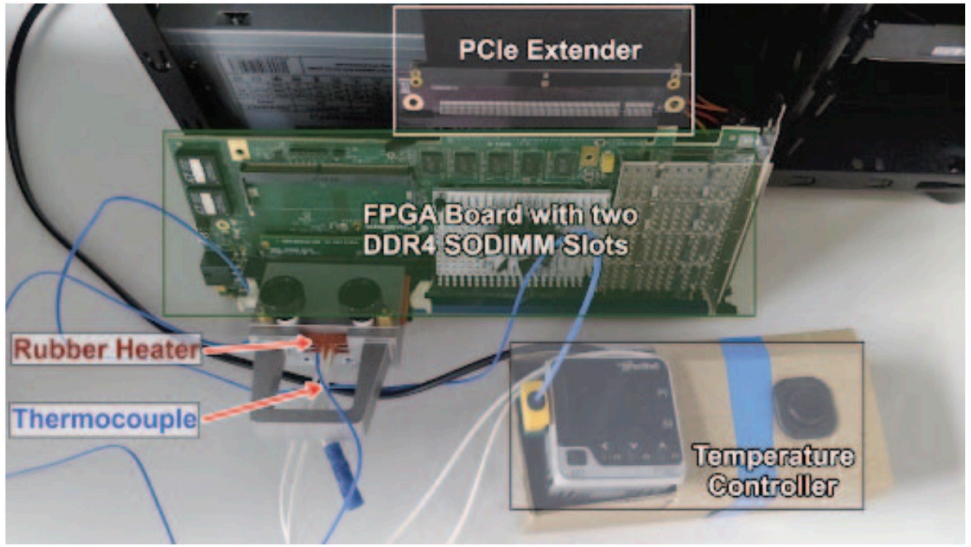

Table 1: Summary of DRAM chips tested.

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)**

UC RIVERSIDE

3.2 RowHammer Characterization

- run without interference (e.g., without DRAM refresh or RowHammer mitigation mechanisms)
- systematically test each DRAM row's vulnerability to RowHammer by issuing the **worst-case sequence** of DRAM accesses for that particular row.
  - First, a repeatedly accessed row (i.e., aggressor row) has the greatest impact on its immediate physically-adjacent rows
  - Second, a double-sided hammer targeting physical victim row N causes the highest number of RowHammer bit flips in row N compared to any other access pattern.
  - Third, increasing the rate of DRAM activations (i.e., issuing the same number of activations within shorter time periods) results in an increasing number of RowHammer bit flips

3.2 RowHammer Characterization

- **RowHammer Vulnerability**
  - We first examine which of the chips that we test are susceptible to RowHammer. Across all of our chips, we sweep the hammer count (HC) between 2K and 150K and observe whether we can induce any RowHammer bit flips at all in each chip. We find that we can induce RowHammer bit flips in all chips except many DDR3 chips.

Table 2: Fraction of DDR3 DRAM chips vulnerable to RowHammer when $HC < 150k$.

DRAM type-node	RowHammerable chips *Mfr. A*	*Mfr. B*	*Mfr. C*
DDR3-old	24/88	0/88	0/28
DDR3-new	8/72	44/52	96/104

Newer DRAM chips appear to be more vulnerable to RowHammer based on the increasing fraction of RowHammerable chips from DDR3-old to DDR3-new DRAM chips of manufacturers B and C.

UC RIVERSIDE

3.2 RowHammer Characterization

- **Data Pattern Dependence**

  Data pattern (DP). We test several commonly-used DRAM data patterns where every byte is written with the same data: Solid0 (SO0: 0x00), Solid1 (SO1: 0xFF), Colstripe0 (CO0: 0x55), Colstripe1 (CO1: 0xAA) [54,83,99]. In addition, we test data patterns where each byte in every other row, including the row being hammered, is written with the same data, Checkered0 (CH0: 0x55) or Rowstripe0 (RS0: 0x00), and all other rows are written with the inverse data, Checkered1 (CH1: 0xAA) or Rowstripe1 (RS1: 0xFF), respectively.

  Hammer count (HC). We count each pair of activations to the two neighboring rows as one hammer

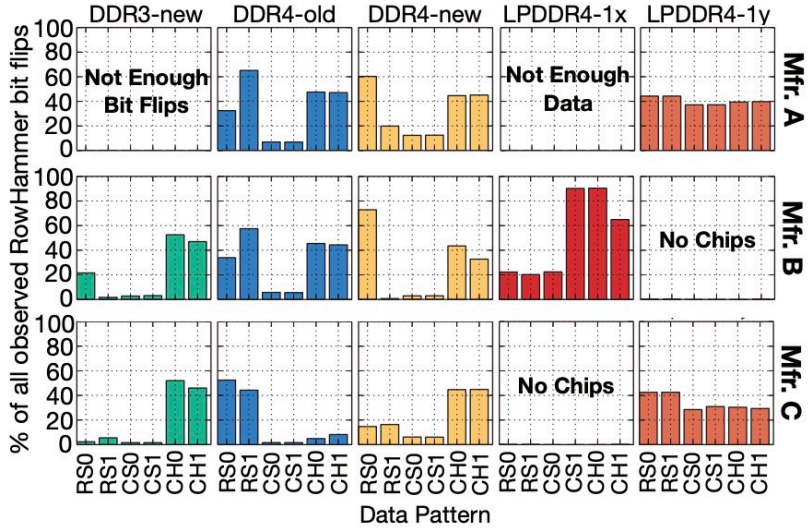

Figure 4: RowHammer bit flip coverage of different data patterns (described in Section 4.3) for a single representative DRAM chip of each type-node configuration.

3.2 RowHammer Characterization

- **Hammer Count (HC) Effects**

Figure 5 plots the effects of increasing the number of hammers on the RowHammer bit flip rate for our tested DRAM chips of various DRAM type-node configurations across the three major DRAM manufacturers. For all chips, we hammer each row, sweeping HC between 10,000 and 150,000. For each HC value, we plot the average rate of observed RowHammer bit flips across all chips of a DRAM type-node configuration.

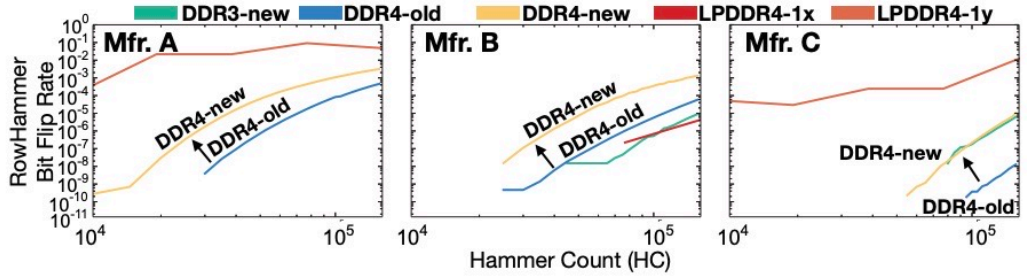

Figure 5: Hammer count (*HC*) vs. RowHammer bit flip rate across DRAM type-node configurations.

The log of the number of RowHammer bit flips has a linear relationship with the log of HC.

Newer DDR4 DRAM technology nodes show a clear trend of increasing RowHammer bit flip rates: the same HC value causes an increased average RowHammer bit flip rate from DDR4-old to DDR4 new DRAM chips of all DRAM manufacturers.

UC RIVERSIDE

3.2 RowHammer Characterization

- **First RowHammer Bit Flips**

Newer chips from a given DRAM manufacturer appear to be more vulnerable to RowHammer bit flips. This is demonstrated by the clear reduction in HCfirst values from old to new DRAM generations.

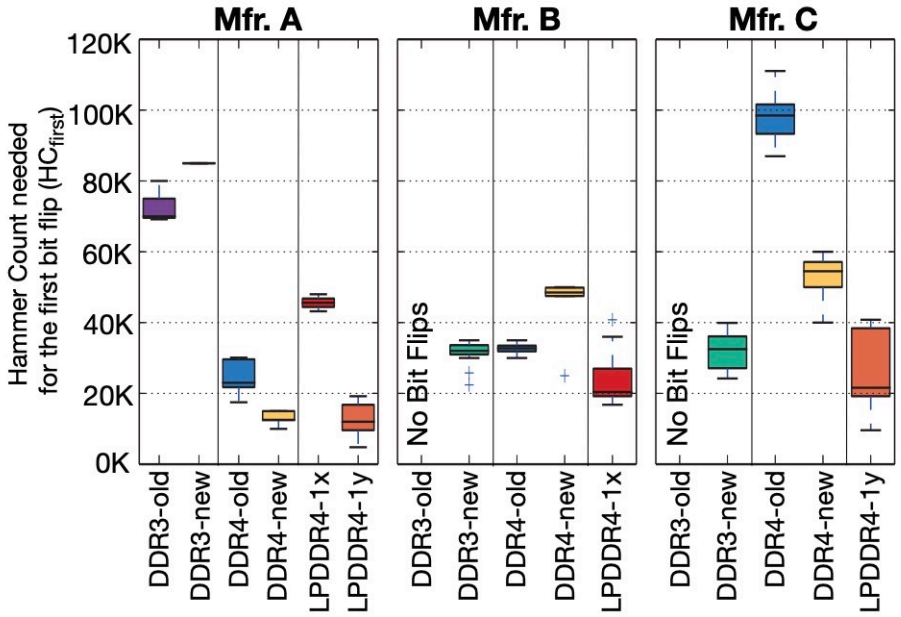

Figure 8: Number of hammers required to cause the first RowHammer bit flip (HC_{first}) per chip across DRAM type-node configurations.

UC RIVERSIDE

04 Implications for Future Systems

Our characterization results have major implications for continued DRAM technology scaling since DRAM's increased vulnerability to RowHammer means that systems employing future DRAM devices will likely need to handle significantly elevated failure rates. While prior works propose a wide variety of RowHammer failure mitigation techniques, these mechanisms will need to manage increasing failure rates going forward and will likely suffer from high overhead.

OUR SOLUTION: **Ideal Refresh-based Mitigation Mechanism**
We implement an ideal refresh-based mitigation mechanism that tracks all activations to every row in DRAM and issues a refresh command to a row only right before it can potentially experience a RowHammer bit flip (i.e., when a physically adjacent row has been activated).

.

04 Implications for Future Systems

Evaluation of Mitigation Mechanisms:

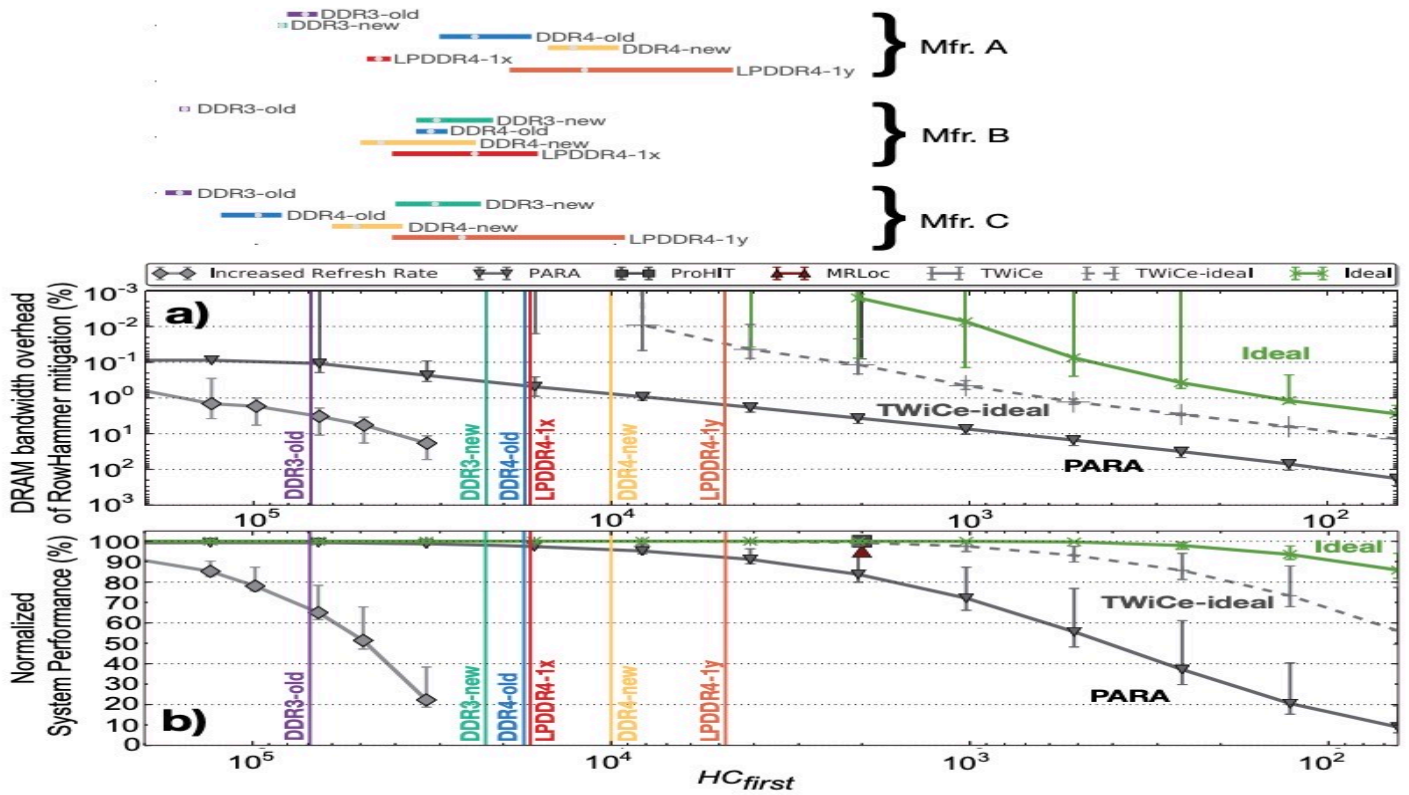

Figure 10: Effect of RowHammer mitigation mechanisms on a) DRAM bandwidth overhead (note the inverted log-scale y-axis) and b) system performance, as DRAM chips become more vulnerable to RowHammer (from left to right).

UC RIVERSIDE

04 Implications for Future Systems

Evaluation of Mitigation Mechanisms:

- First, DRAM bandwidth overhead is highly correlated with normalized system performance, as DRAM bandwidth consumption is the main source of system interference caused by RowHammer mitigation mechanisms. We note that several points are not visible in since we are plotting an inverted log graph and these points are very close to zero.
- Second, in the latest DRAM chips, only limited viable options for mitigating RowHammer bit flips with reasonable average normalized system performance.
- Third, only PARA's design scales to low HCfirst values that we may see in future DRAM chips, but has very low average normalized system performance. While TWiCe-ideal has higher normalized system performance over PARA, there are significant practical limitations in enabling TWiCe-ideal for such low HCfirst values.
- Fourth, ProHIT and MRLoc both exhibit high normalized system performance at their single data point, but these works do not provide models for scaling their mechanisms to lower HCfirst values and how to do so is not intuitive.
- Fifth, the ideal refresh-based mitigation mechanism is significantly and increasingly better than any existing mechanism as HCfirst reduces below 1024. This indicates that there is still significant opportunity for developing a refresh-based RowHammer mitigation mechanism with low performance overhead that scales to low HCfirst values.

04 Implications for Future Systems

Conclusion of Mitigation Mechanisms:

We conclude that while existing mitigation mechanisms may exhibit reasonably small performance overheads for mitigating RowHammer bit flips in modern DRAM chips, their overheads do not scale well in future DRAM chips that will likely exhibit higher vulnerability to RowHammer. Thus, we need new mechanisms and approaches to RowHammer mitigation that will scale to DRAM chips that are highly vulnerable to RowHammer bit flips.

05 CONCLUSION

We provide the first rigorous experimental RowHammer failure characterization study that demonstrates how the RowHammer vulnerability of modern DDR3, DDR4, and LPDDR4 DRAM chips scales across DRAM generations and technology nodes. Using experimental data from 1580 real DRAM chips produced by the three major DRAM manufacturers, we show that modern DRAM chips that use smaller process technology node sizes are significantly more vulnerable to RowHammer than older chips. Using simulation, we show that existing RowHammer mitigation mechanisms 1) suffer from prohibitively large performance overheads at projected future hammer counts and 2) are still far from an ideal selective-refresh based RowHammer mitigation mechanism. Based on our study, we motivate the need for a scalable and low-overhead solution to RowHammer and provide two promising research directions to this end.

UC RIVERSIDE

Thanks for Listening