ETH zürich

SAFARI

Understanding the Security Benefits and Overheads of Emerging Industry Solutions to DRAM Read Disturbance

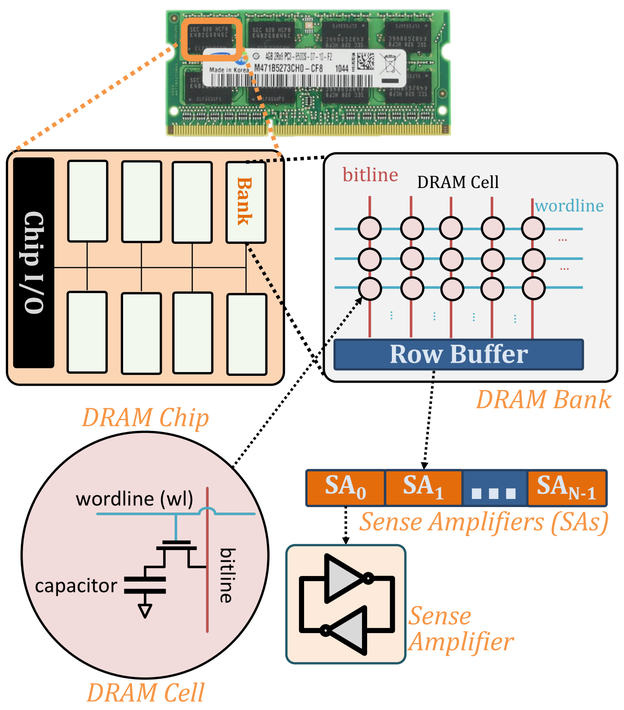
Contact Info

Oğuzhan Canpolat A. Giray Yağlıkçı Geraldo Oliveira Ataberk Olgun
Oğuz Ergin Onur Mutlu

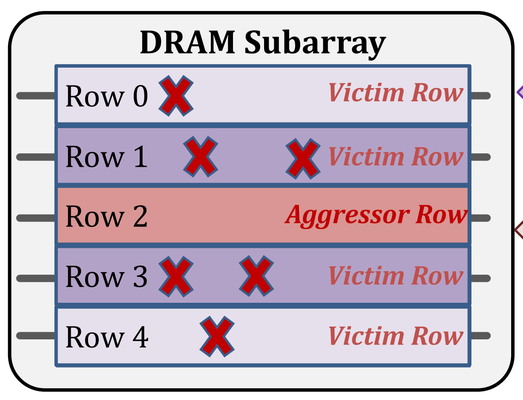
Full Paper

1. DRAM Background

DRAM Organization



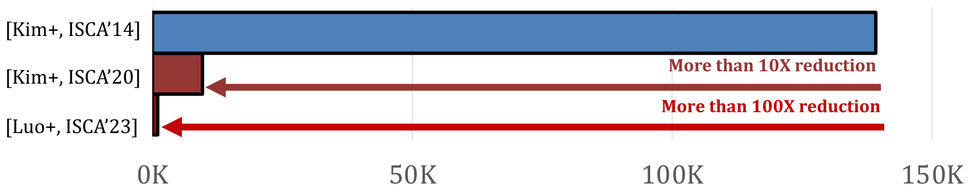
DRAM Read Disturbance



RowHammer [Kim+ ISCA'14]

RowPress [Luo+ ISCA'23]

Repeatedly **opening** and **closing** **OR** **keeping open** a DRAM row causes **bitflips** in nearby cells

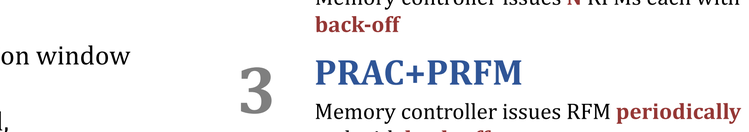


Minimum hammer count needed to induce the first read disturbance bitflip

2. Cutting Edge Industry Solutions

Preventive Refresh in DDR5 Specifications

Preventive refresh is a **blocking** operation



Memory controller sends an **RFM command** to allow time for preventive refreshes

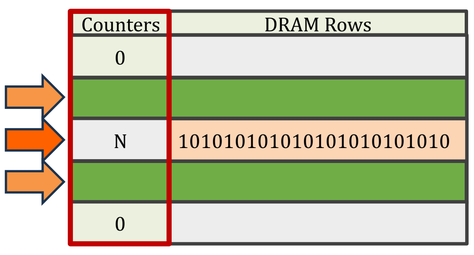
Periodic Refresh Management (PRFM)

Memory controller **periodically** issues RFM commands

Per Row Activation Counting (PRAC)

DRAM chip **tracks** row activations for each row and **requests** RFMs by sending **back-off** signals

3. Per Row Activation Counting (PRAC) [JEDEC, JESD79-5C, April 2024]

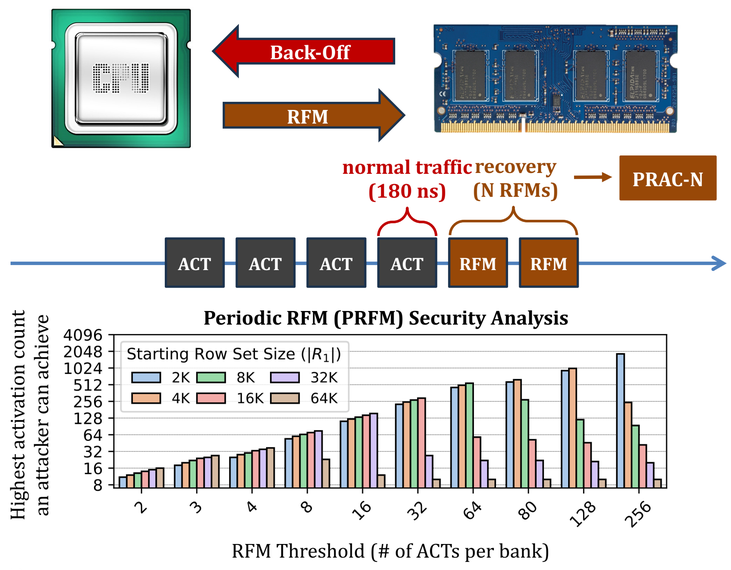


PRAC allows accurate tracking of aggressor row activations ✓

Row counter updates are **not completely** parallelized with DRAM access ✗

t_{RP}	: +21ns	(+140%)
t_{RAS}	: -16ns	(-50%)
t_{RTP}	: -2.5ns	(-33%)
t_{WR}	: -20ns	(-66%)
t_{RC}	: +5ns	(+10%)

Timing parameter changes for DDR5-3200AN speed bin [JEDEC JESD79-5C, April 2024]



4. Performance Evaluation

Cycle-level simulations using
Ramulator 2.0 [Luo+, CAL 2023]
DRAMPower [Chandrasekar+, DATE 2013]

System Configuration:

Processor
4 cores, 4.2GHz clock frequency,
4-wide issue, 128-entry instruction window
DRAM
DDR5, 1 channel, 2 rank/channel,
8 bank groups x 4 banks x 64K rows
Memory Ctrl.
64-entry read and write requests queues,
FR-FCFS scheduling with a column cap of 4
Last-Level Cache 8 MiB (4-core)

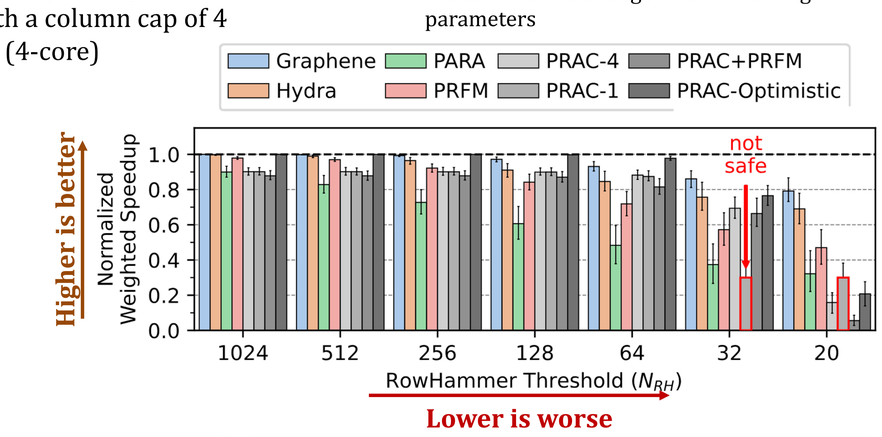
Workloads:
60 mixes from
SPEC CPU2006,
SPEC CPU2017,
TPC, MediaBench,
and YCSB

1 **PRF**
Memory controller **periodically** issues RFM

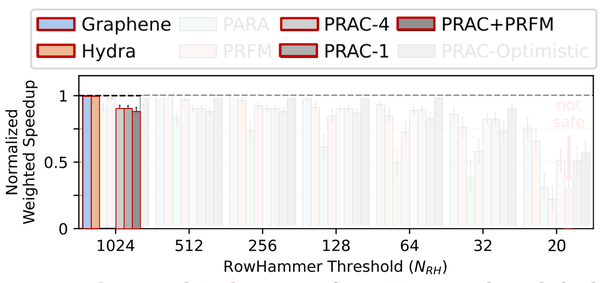
2 **PRAC**
Memory controller issues **N** RFMs each with **back-off**

3 **PRAC+PRFM**
Memory controller issues RFM **periodically** and with **back-offs**

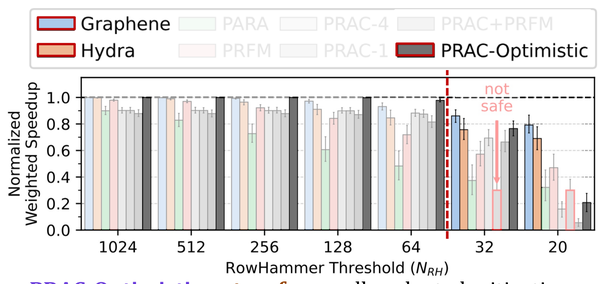
4 **PRAC-Optimistic**
PRAC-4 with **no** change in DRAM timing parameters



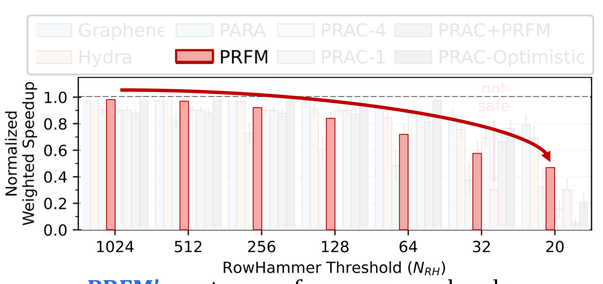
5. Key Observations



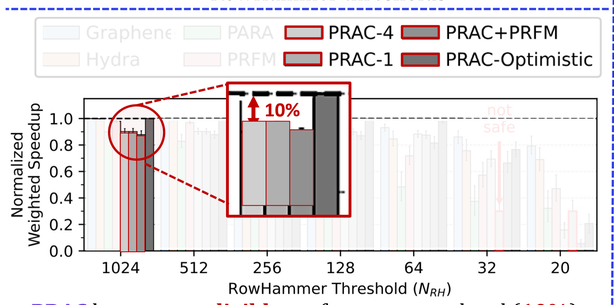
Graphene and **Hydra** outperform **PRAC** at relatively high RowHammer thresholds



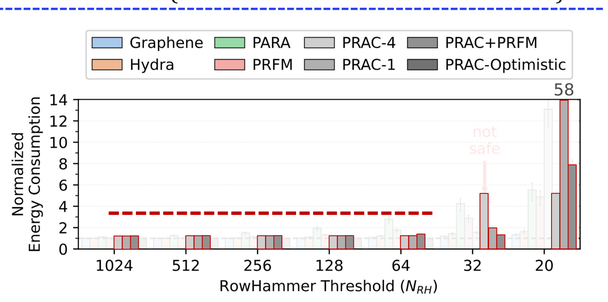
PRAC-Optimistic outperforms all evaluated mitigation mechanisms (RowHammer threshold of 64 and more)



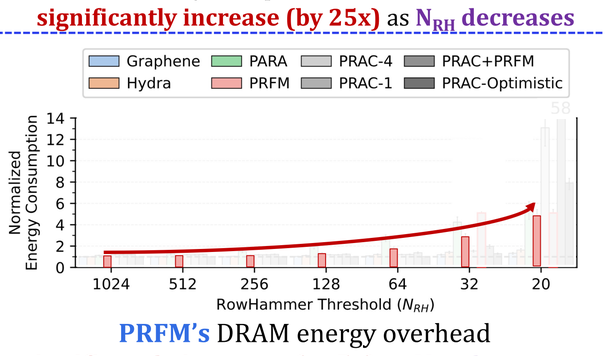
PRFM's system performance overheads **significantly increase (by 25x)** as N_{RH} **decreases**



PRAC has **non-negligible** performance overhead (**10%**) due to **increased** access latency



PRAC incurs significant performance and energy overheads if the RowHammer threhold is smaller than 64



PRFM's DRAM energy overhead **significantly increase (to 5x)** as N_{RH} **decreases**

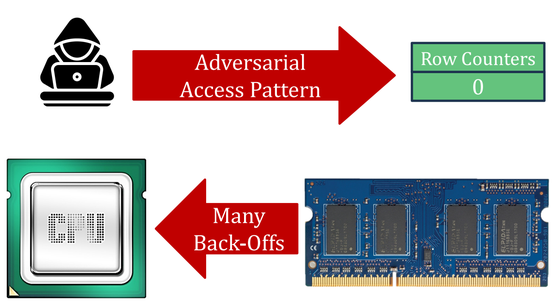
6. Open-Source

Simulator is available online

https://github.com/CMU-SAFARI/ramulator2

7. A New Attack Vector

Access pattern to trigger **most** back-offs with **fewest** activations possible by targeting a single row



Mathematical worst-case analysis at the RowHammer threshold of 20: Hogs up to **79% of DRAM throughput**

Cycle-level simulation results: Degrades system performance by up to **98%** (94% on average)

8. Conclusion and Future Work

- The first **rigorous security** and **performance** analyses of PRAC
- **RowHammer-safe for thresholds > 20**
- **Non-negligible overheads** for modern chips
- **Poorly scales** with worsening RowHammer vulnerability
- **Memory performance attacks** can exploit PRAC

Future work:
More research is needed to improve PRAC by tackling
- **increased DRAM access latencies**
- **increasing performance loss** as RowHammer worsens
- memory performance attacks exploiting PRAC