SCIENCE
PASSION
TECHNOLOGY

Memory Band-Aid

A Principled Rowhammer Defense-in-Depth

Carina Fiedler, Jonas Juffinger, Sudheendra Raghav Neela, Martin Heckel, Hannes Weissteiner, Abdullah Giray Yağlıkçı, Florian Adamsky, and Daniel Gruss

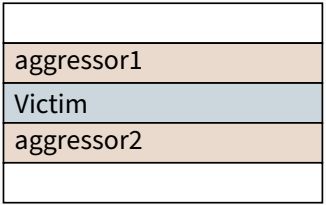
Graz University of Technology

NDSS 2026

› isec.tugraz.at

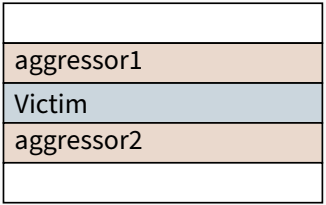
Rowhammer

- Hardware fault of the DRAM



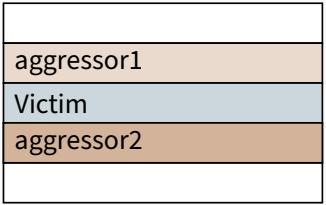
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



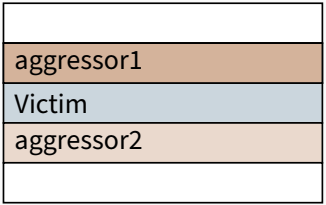
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



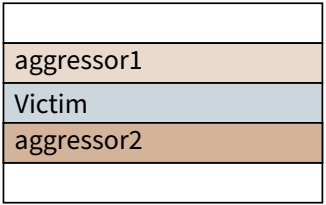
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



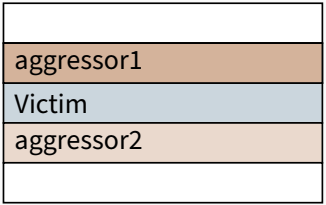
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



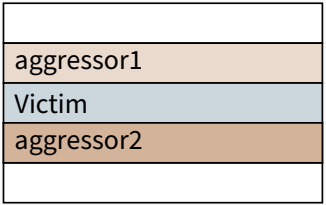
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



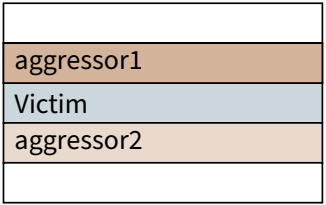
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



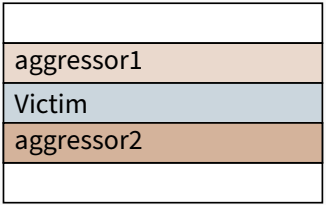
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



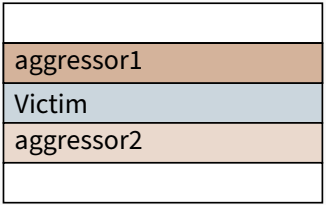
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



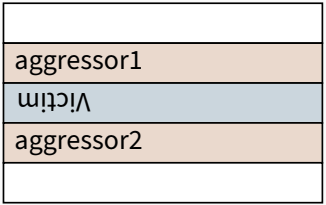
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



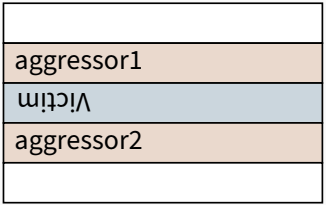
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows



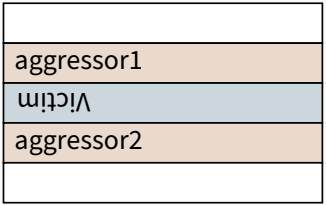
Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows
- Worse with every new DRAM generation



Rowhammer

- Hardware fault of the DRAM
- Frequent accesses flip bits in neighboring rows
- Worse with every new DRAM generation
- Enables attacks, many countermeasures proposed



Reaching DRAM

- Cache stores data on access

Reaching DRAM

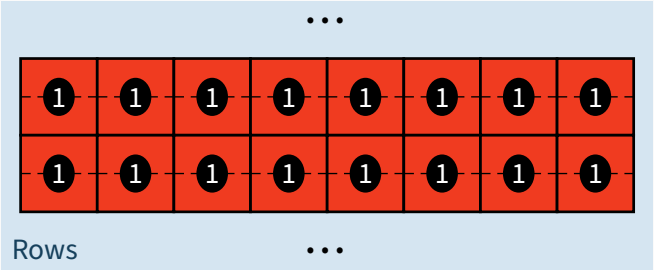
- Cache stores data on access
- `clflush` instruction removes data from cache

Reaching DRAM

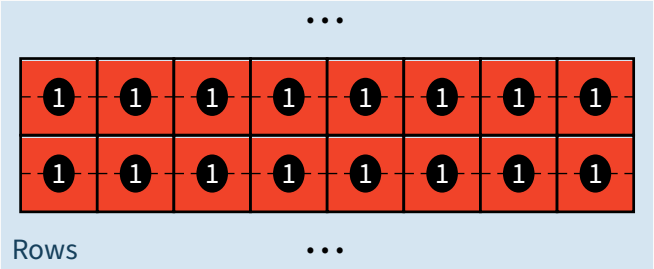
- Cache stores data on access
- `clflush` instruction removes data from cache
- Flush+Reload loop

```
for (i = 0; i < N; ++i) {
  *aggressor1;
  *aggressor2;
  flush(aggressor1);
  flush(aggressor2);
}
```

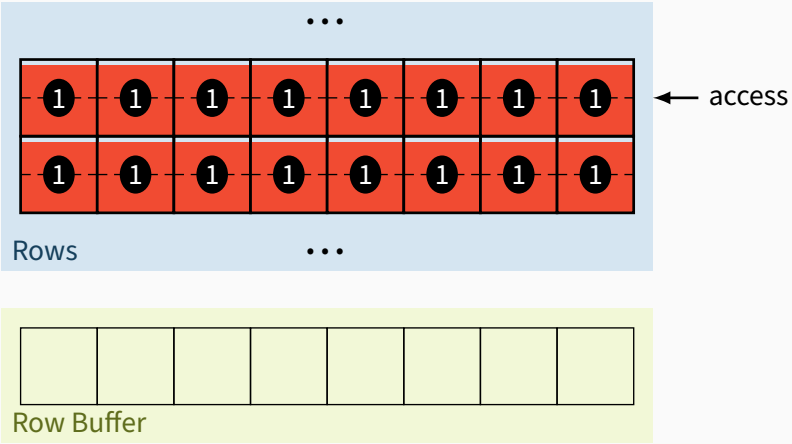
Cell Discharge



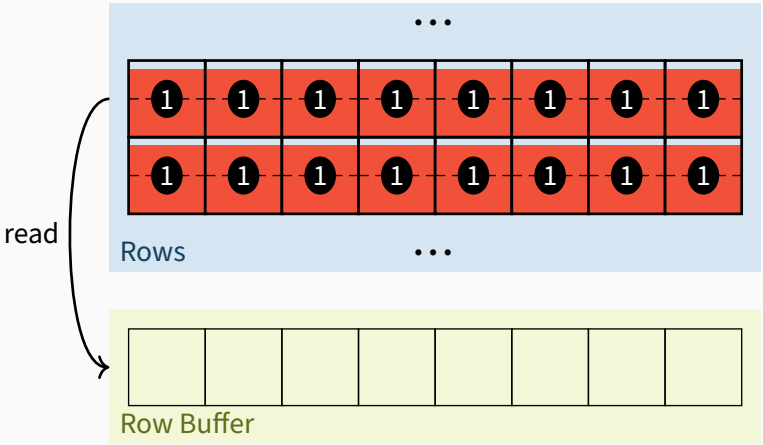
Cell Discharge



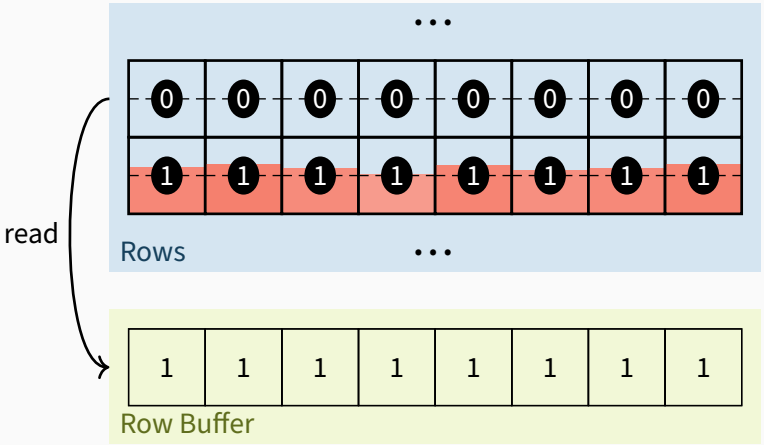
Cell Discharge



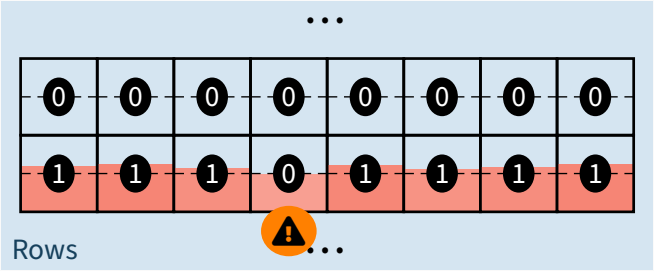
Cell Discharge



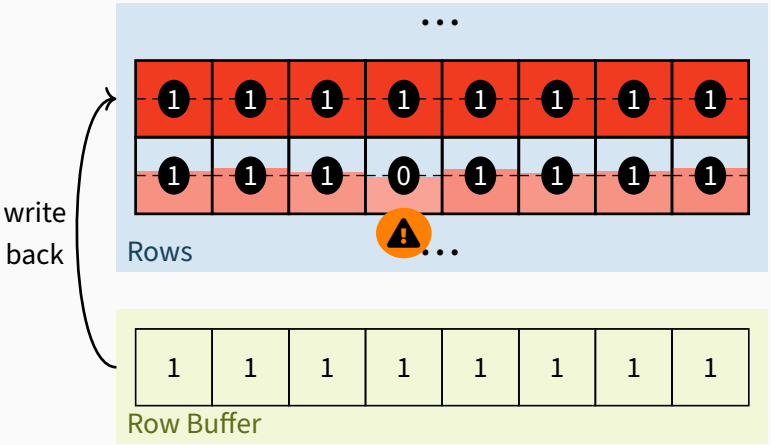
Cell Discharge



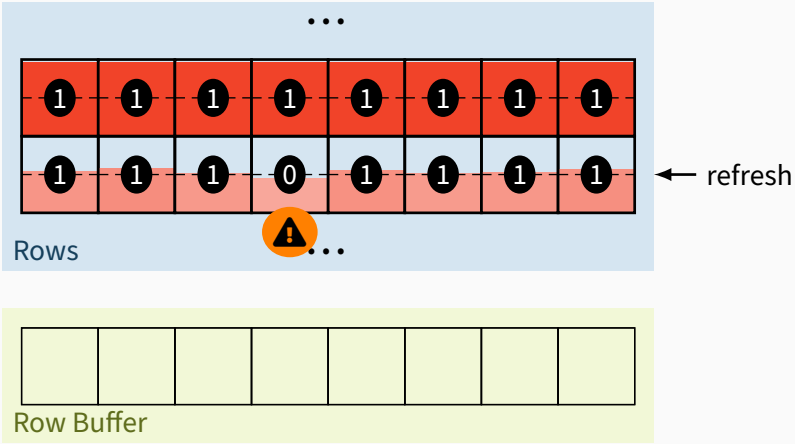
Cell Discharge



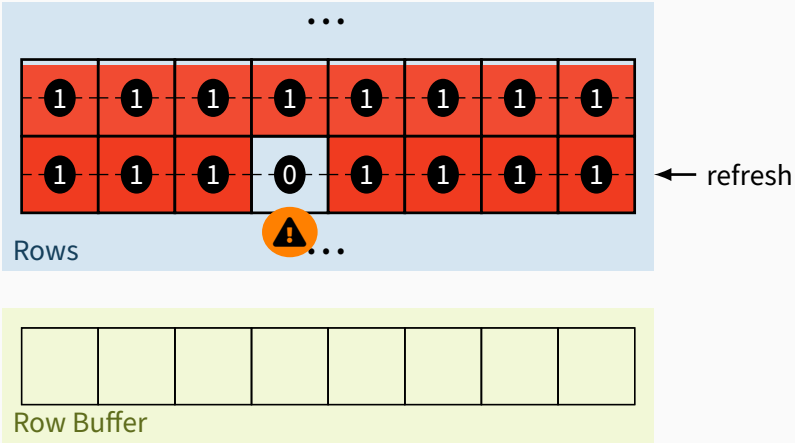
Cell Discharge



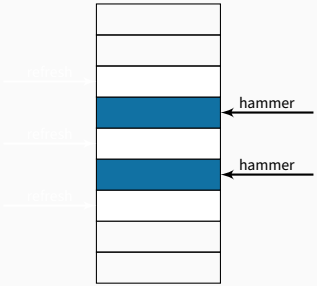
Cell Discharge



Cell Discharge

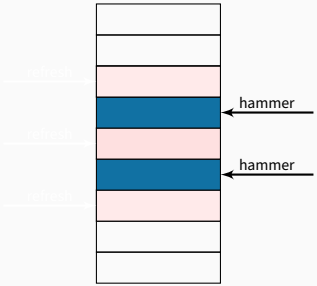


Target Row Refresh (TRR)



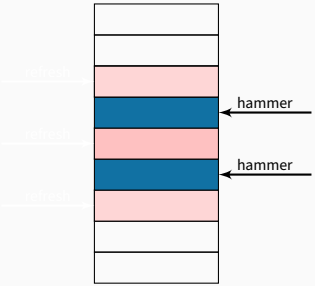
Target Row Refresh (TRR)

- Counter per row



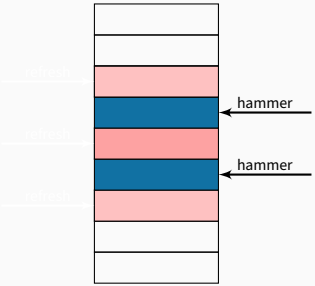
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



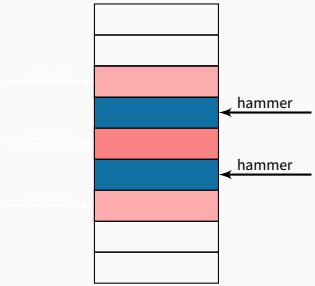
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



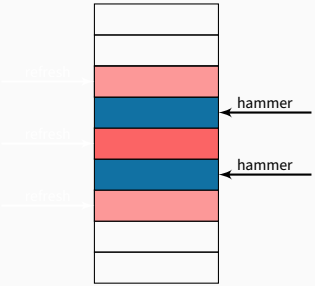
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



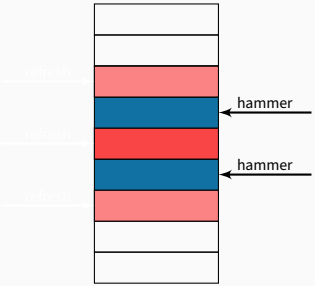
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



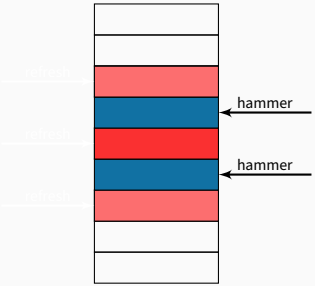
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



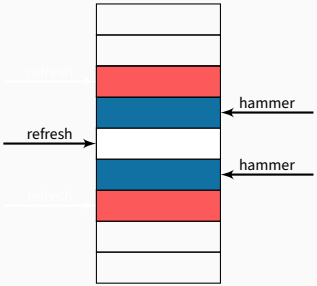
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows



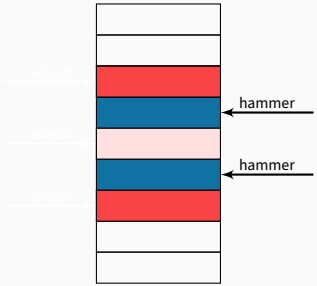
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows
- Refresh when counter reaches a threshold



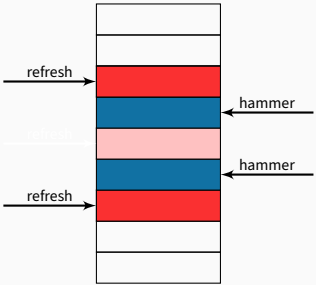
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows
- Refresh when counter reaches a threshold



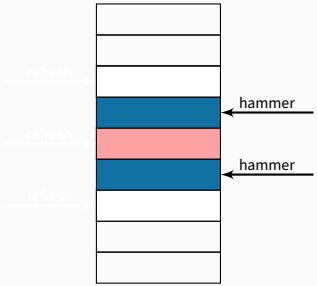
Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows
- Refresh when counter reaches a threshold



Target Row Refresh (TRR)

- Counter per row
- Increment neighbor rows
- Refresh when counter reaches a threshold

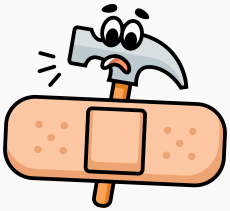


Limitations of Rowhammer Mitigations

- Not deployed in practice
- High overheads
- Can be bypassed

Limitations of Rowhammer Mitigations

- Not deployed in practice
- High overheads
- Can be bypassed
- $\rightarrow$ modern and future systems may still be vulnerable



Memory Band-Aid: A Principled Rowhammer Defense-in-Depth

Carina Fiedler, Jonas Juffinger, Sudheendra Raghav Neela, Martin Heckel,
Hannes Weissteiner, Abdullah Giray Yağlıkçı, Florian Adamsky, and Daniel Gruss.

NDSS 2026

Core Idea

- Modern systems have many banks

Core Idea

- Modern systems have many banks
- Addressing functions distribute accesses across banks

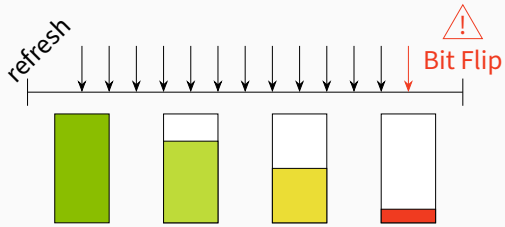
Core Idea

- Modern systems have many banks
- Addressing functions distribute accesses across banks
- Attacks circumventing TRR need many accesses **per bank**

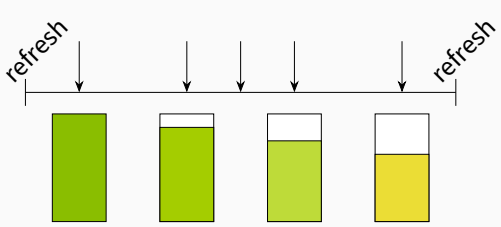
Core Idea

- Modern systems have many banks
- Addressing functions distribute accesses across banks
- Attacks circumventing TRR need many accesses **per bank**
- $\rightarrow$ limit bandwidth per bank

Per-Bank Bandwidth Limit



unrestricted

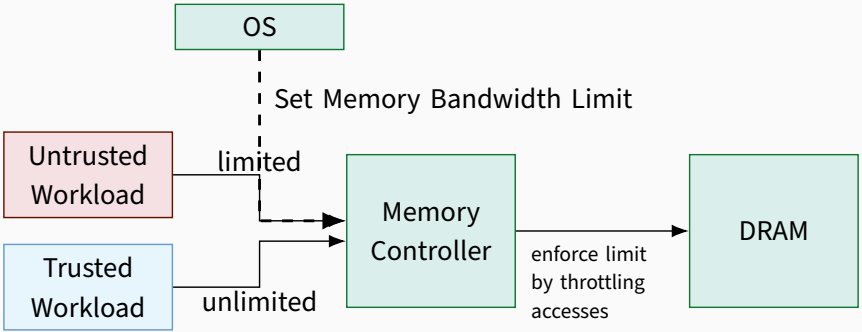


rate-limited

Mitigation Criteria

- Prevent bit flips
- Maintain performance
- Configurability

Memory Band-Aid



How does the Memory Controller know?

Quality-of-Service Features

- Monitor and restrict cache and memory utilization

Quality-of-Service Features

- Monitor and restrict cache and memory utilization
- e.g. limit memory bandwidth via

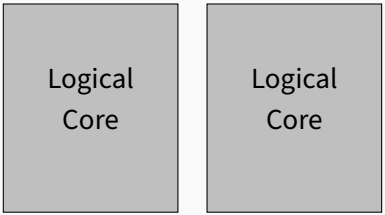
Quality-of-Service Features

- Monitor and restrict cache and memory utilization
- e.g. limit memory bandwidth via
- AMD: L3 External Bandwidth Enforcement (L3BE)
  - 128 $\mathrm{MiB/s}$ increments

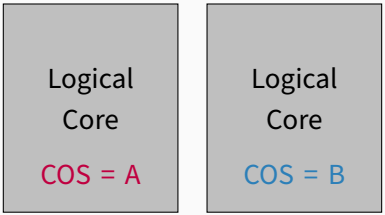
Quality-of-Service Features

- Monitor and restrict cache and memory utilization
- e.g. limit memory bandwidth via
- AMD: L3 External Bandwidth Enforcement (L3BE)
  - 128 $\mathrm{MiB/s}$ increments
- Intel: Memory Bandwidth Allocation (MBA)
  - 10 % of system bandwidth increments

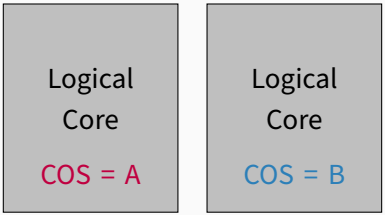
Class of Service (COS)



Class of Service (COS)

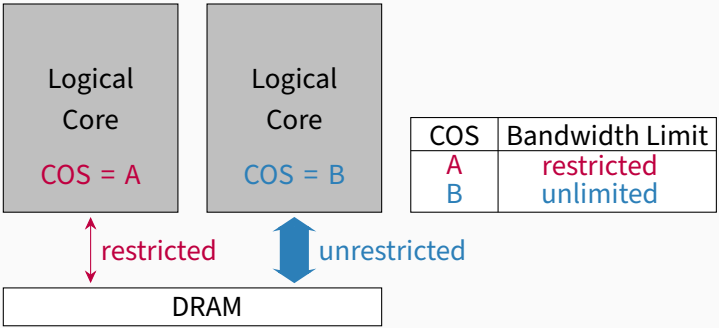


Class of Service (COS)

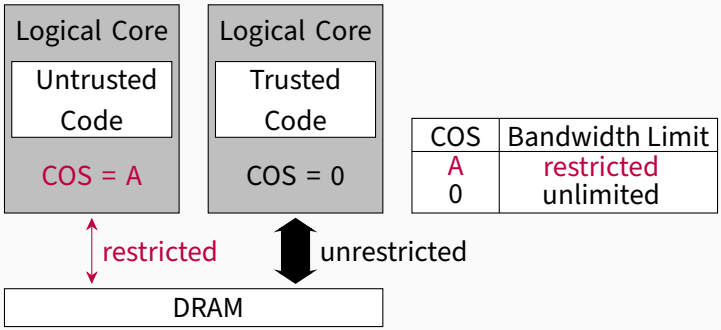


COS	Bandwidth Limit
A	restricted
B	unlimited

Class of Service (COS)



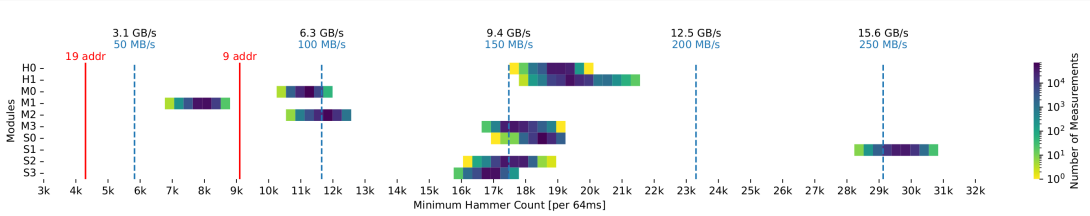
Proof-of-Concept Implementation



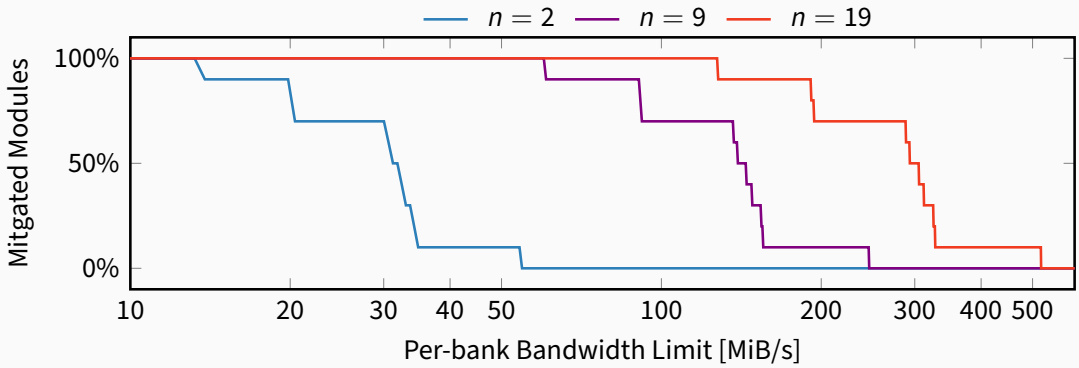
- OS sets COS on context switch: restricted = untrusted vs unrestricted = trusted
- Sandboxes or userspace vs kernelspace

What are suitable limits?

Minimum Hammer Counts



Mitigated Modules



Evaluation

Test Systems

Abbreviation	Processor	OS	DRAM Vendor	DRAM Speed	Configuration	Ranks	Total Banks	ECC	MBA/L3BE
A1	AMD Ryzen 7700X	Ubuntu 22.04	Kingston	DDR5	$2 \times$ 16GB	1	64	✗	✓
A2	AMD Epyc 8024P	Ubuntu 22.04		4800	$3 \times$ 16GB	1	96	✓	✓
I1	Intel Xeon 4514Y	Ubuntu 24.04		MT/s	$8 \times$ 16GB	1	256	✓	✓
I2	Intel Xeon 4410T	Ubuntu 22.04		62.7 $\mathrm{GiB/s}$	$4 \times$ 16GB	1	128	✓	✓

Limitations on Current Hardware

- No per-bank limits

Limitations on Current Hardware

- No per-bank limits
- No support on Intel consumer devices

Limitations on Current Hardware

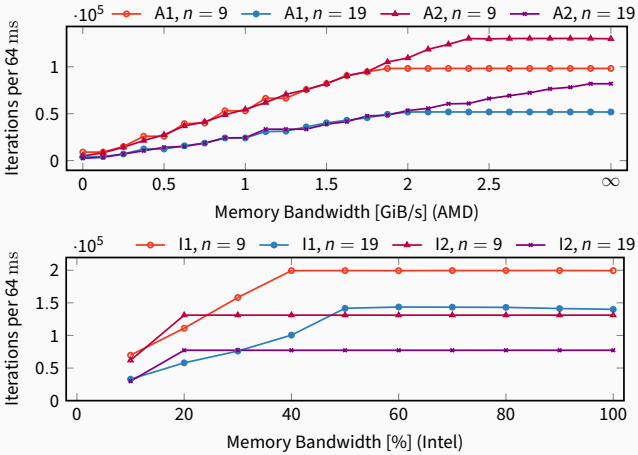
- No per-bank limits
- No support on Intel consumer devices
- Limit granularity and precision

Limitations on Current Hardware

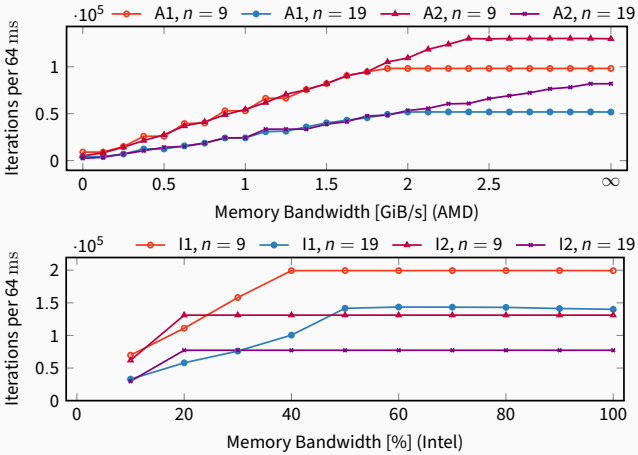
- No per-bank limits
- No support on Intel consumer devices
- Limit granularity and precision
- Per-core limits

Are available limits secure?

Flush+Reload Iteration Limits

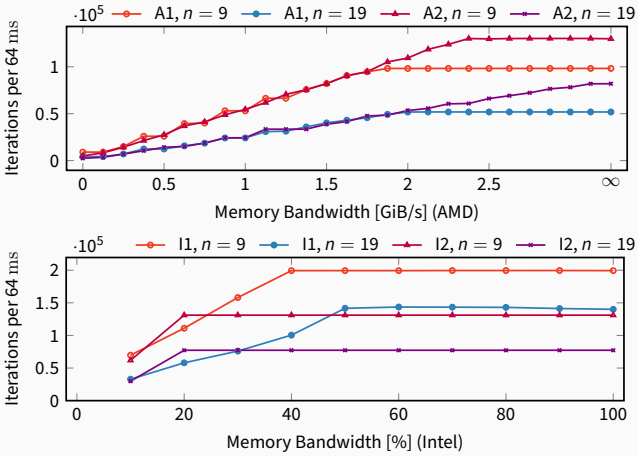


Flush+Reload Iteration Limits



- ☑ AMD: prevent many-sided attacks

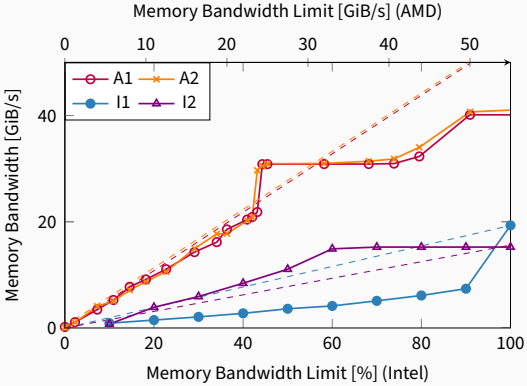
Flush+Reload Iteration Limits



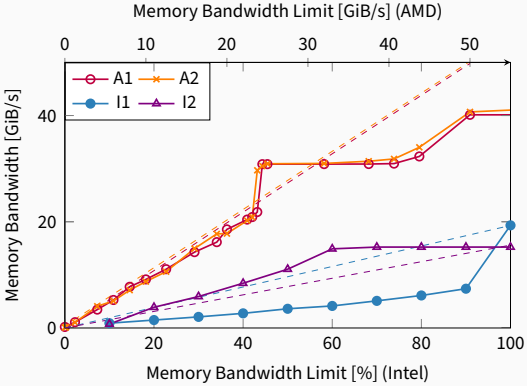
- ☑ AMD: prevent many-sided attacks
- ✗ Intel: insufficient limits

What is the performance impact?

Memory Sweep

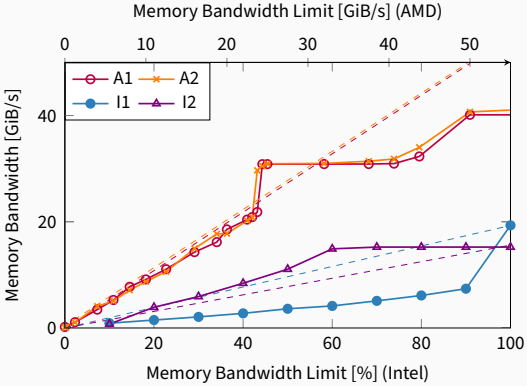


Memory Sweep



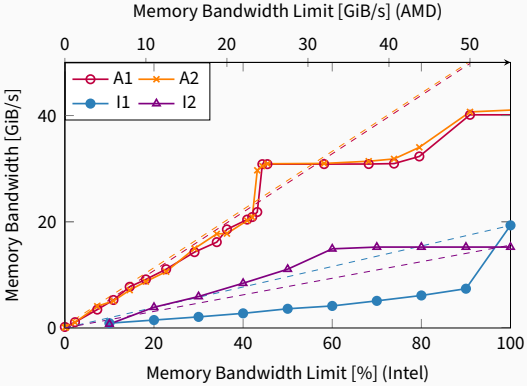
☑ Necessary slow-down

Memory Sweep



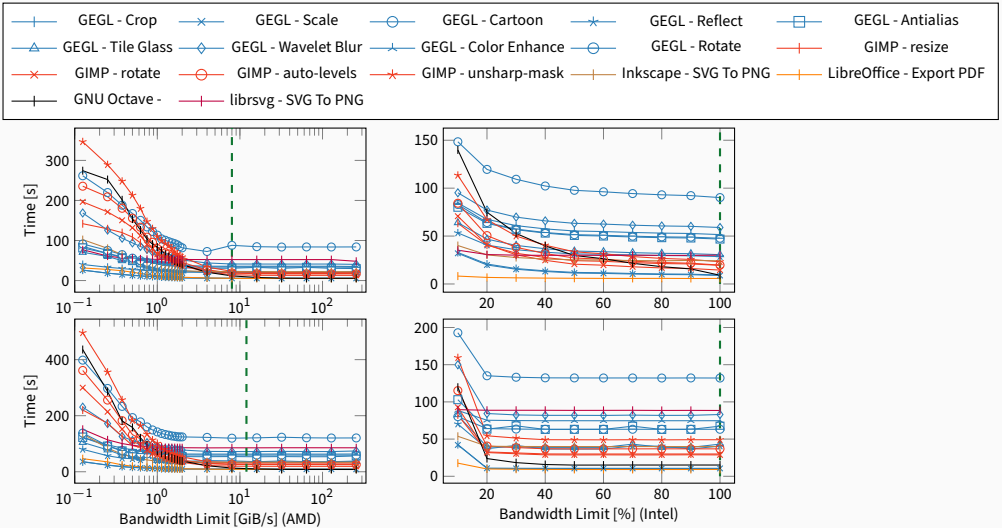
- ☑ Necessary slow-down
- ✗ Lack of adherence to limit

Memory Sweep

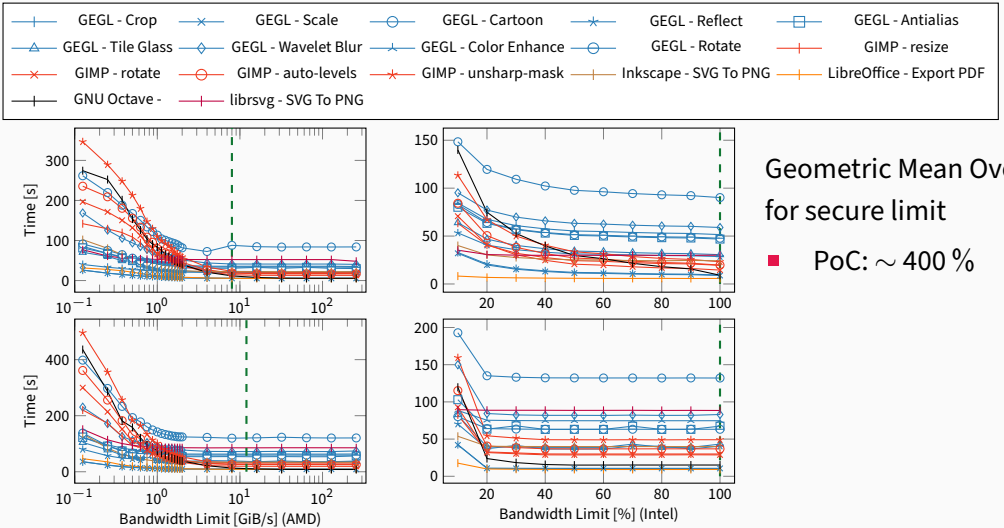


- ☑ Necessary slow-down
- ✗ Lack of adherence to limit
- ⚠ Wasted performance

Phoronix Productivity Testsuite



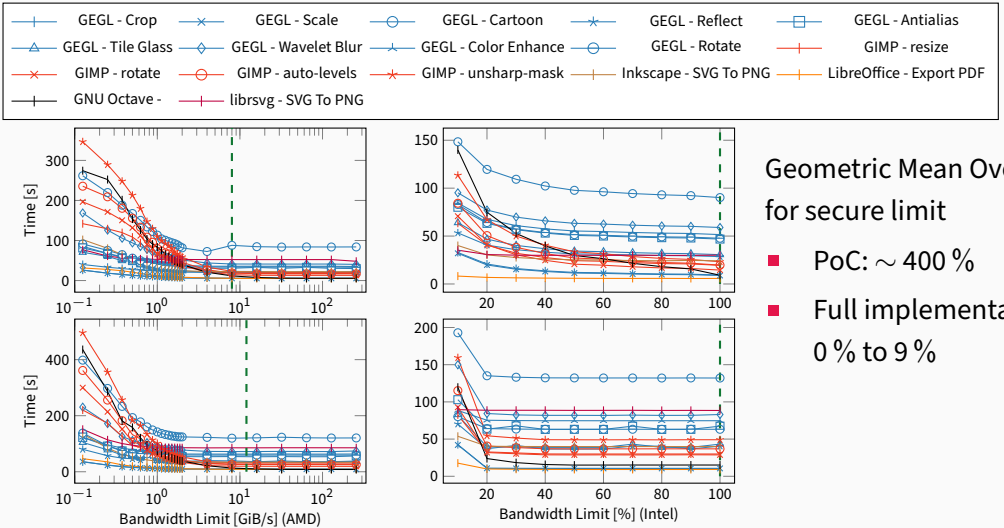
Phoronix Productivity Testsuite



Geometric Mean Overhead for secure limit

- PoC: $\sim 400\,\%$

Phoronix Productivity Testsuite

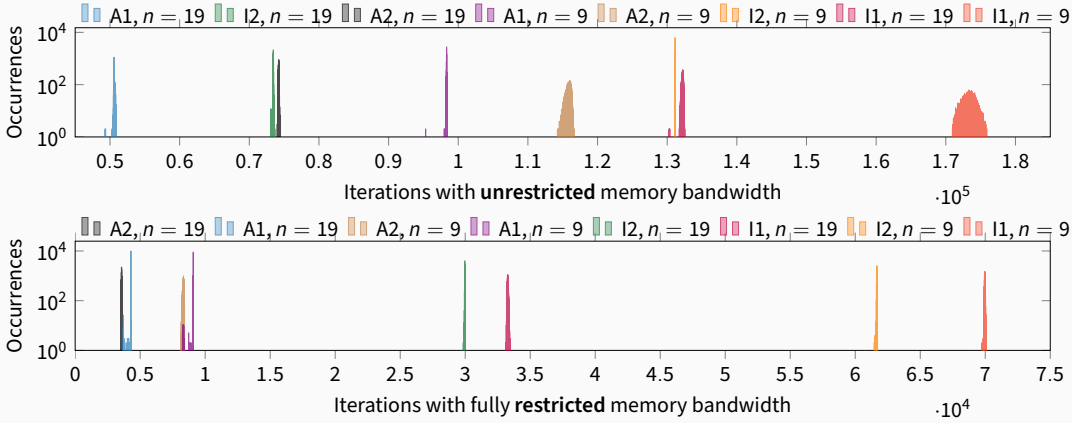


Geometric Mean Overhead for secure limit

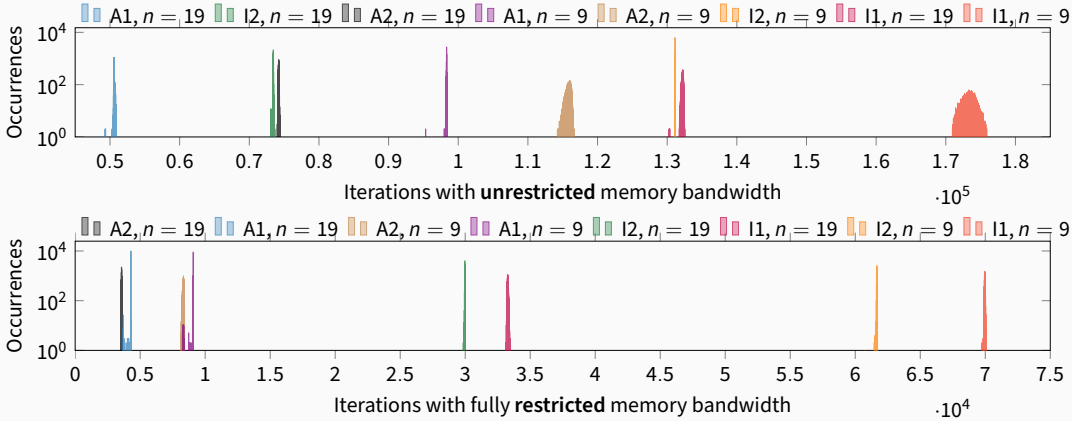
- PoC: $\sim 400\,\%$
- Full implementation: $0\,\%$ to $9\,\%$

How tightly are the limits adhered to?

Limit Consistency: Flush+Reload Iterations per 64 ms

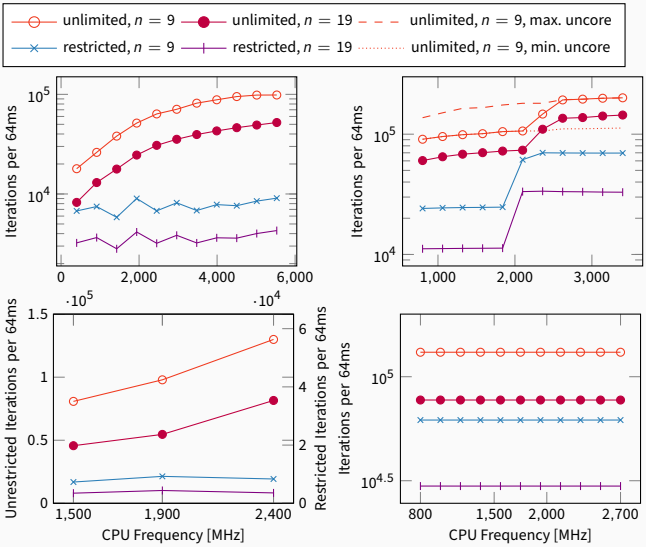


Limit Consistency: Flush+Reload Iterations per 64 ms

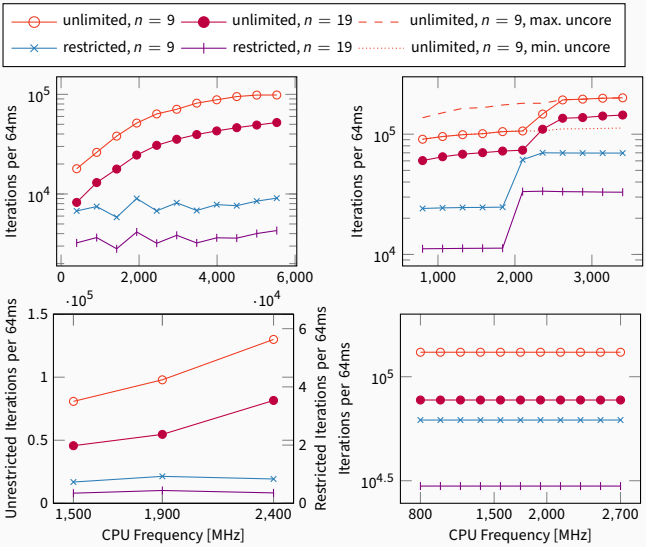


☑ Secure, but some performance loss

Frequency Impact

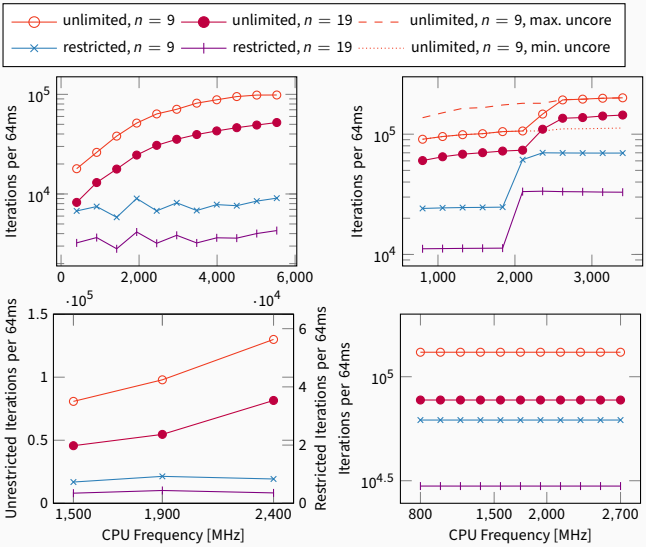


Frequency Impact



- CPU frequency can influence limit
- e.g. indirectly via uncore frequency

Frequency Impact



- ⚠ CPU frequency can influence limit
- ⚠ e.g. indirectly via uncore frequency
- ☑ Measurements already taken with maximum frequency

Memory Band-Aid Summary

- ☑ Effective defense against many-sided attacks
- ☑ Acceptable performance overhead
- ⚠ Current hardware support limited

Acknowledgments

This research was made possible by generous funding from:

Supported in part by the European Research Council (ERC project FSSec 101076409), the Austrian Science Fund (FWF SFB project SPyCoDe 10.55776/F85 and FWF project NeRAM 10.55776/I6054), the Deutsche Forschungsgemeinschaft (grant no. 503876675), and the European Union (grant no. ROF-SG20-3066-3-2-2). Additional funding was provided by generous gifts from Red Hat, Google, and Intel. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.

SCIENCE
PASSION
TECHNOLOGY

Memory Band-Aid

A Principled Rowhammer Defense-in-Depth

Carina Fiedler, Jonas Juffinger, Sudheendra Raghav Neela, Martin Heckel, Hannes Weissteiner, Abdullah Giray Yağlıkçı, Florian Adamsky, and Daniel Gruss

Graz University of Technology

NDSS 2026

› isec.tugraz.at