Epistemology of Rowhammer Attacks:

Threats to Rowhammer Research Validity

Martin Heckel[1,2], Hannes Weissteiner[1], Florian Adamsky[2], and Daniel Gruss[1]

September 22, 2025

[1] Graz University of Technology
[2] Hof University of Applied Sciences

TU Graz

Hochschule Hof
University of Applied Sciences

NeRAM

FWF
Der Wissenschaftsfonds.

DFG Deutsche Forschungsgemeinschaft

Outline

Background

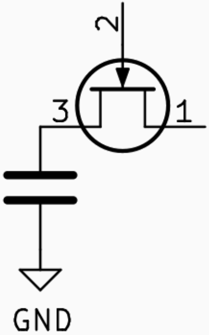
Methodology

Threats to Rowhammer Research Validity

Background

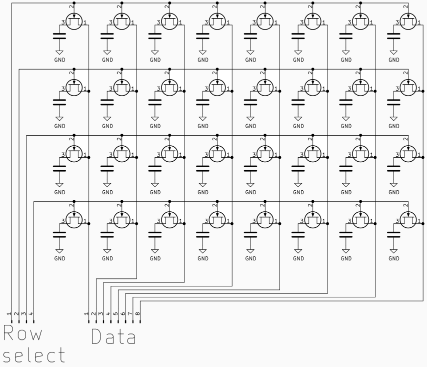
DRAM – Cells

- A single cell consists of:
  - Capacitor storing the data in form of electric charge
  - Transistor controlling the access to the capacitor
- Reading procedure: Enable the control pin and read the voltage at the access pin
- Writing procedure: Apply the level that should be written to the access pin and enable the control pin

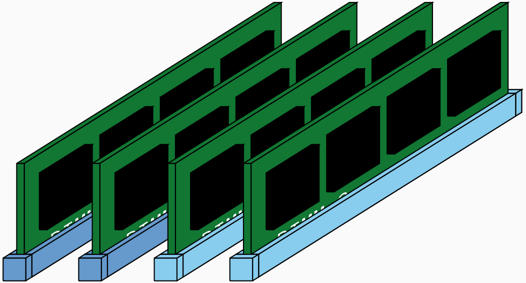


DRAM – Array

- Multiple cells are organized in an array
- Control pins of the cells connected in rows (only entire rows can be enabled)
- Access pins of the cells conneted in columns (entire rows are accessed at once)
- Capacitors loose chage over time, so it is required to refresh the cells periodically (64 ms by default)



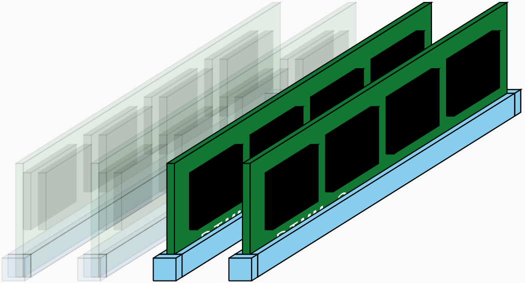
DRAM – physical architecture



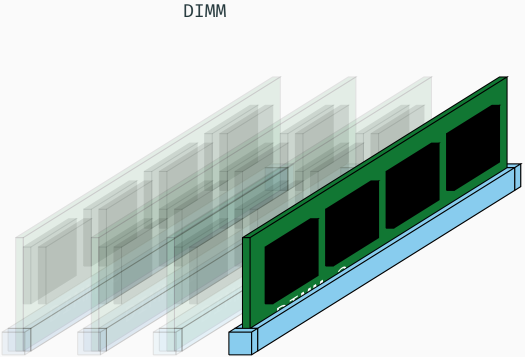
System DRAM

DRAM – physical architecture

Channel

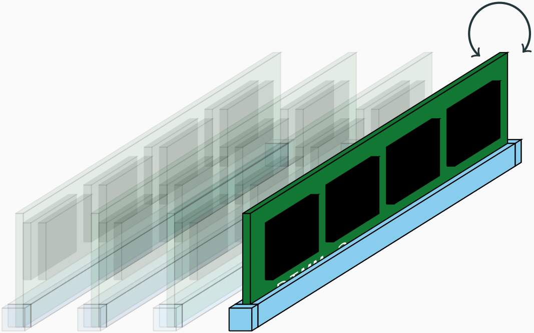


DRAM – physical architecture



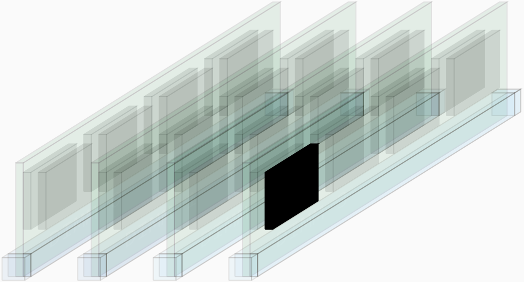
DRAM – physical architecture

Rank

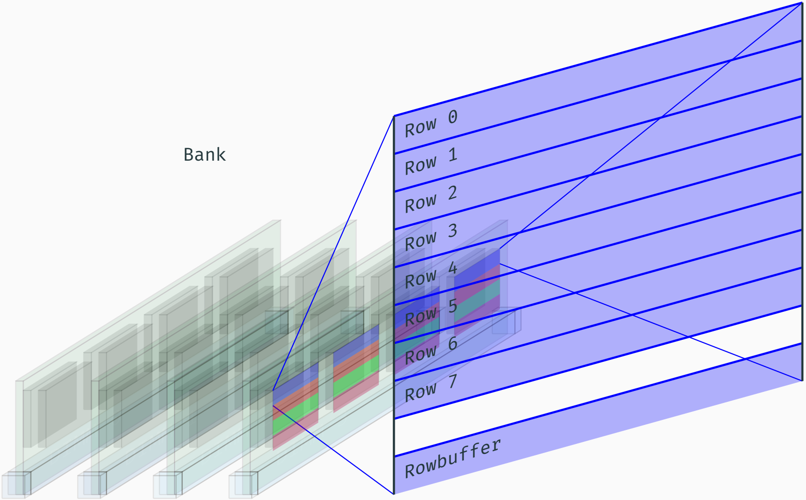


DRAM – physical architecture

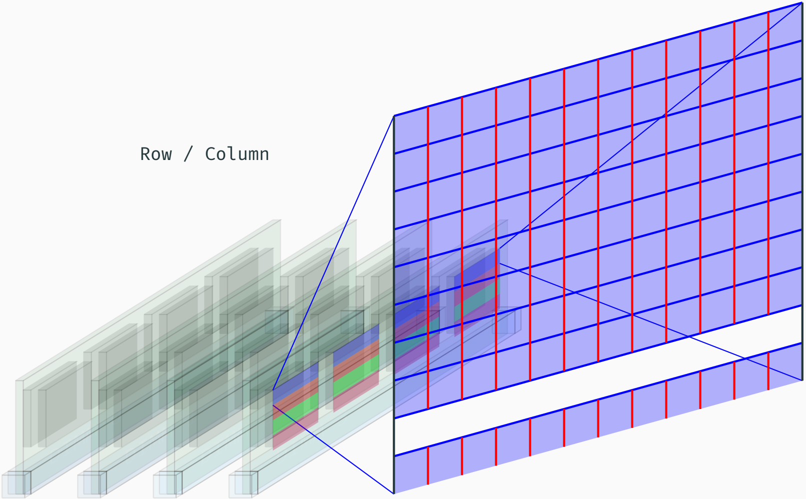
Chip



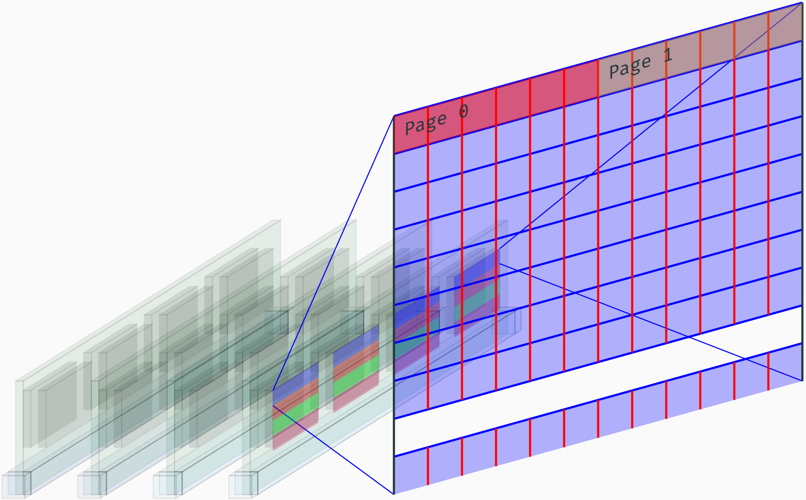
DRAM – physical architecture



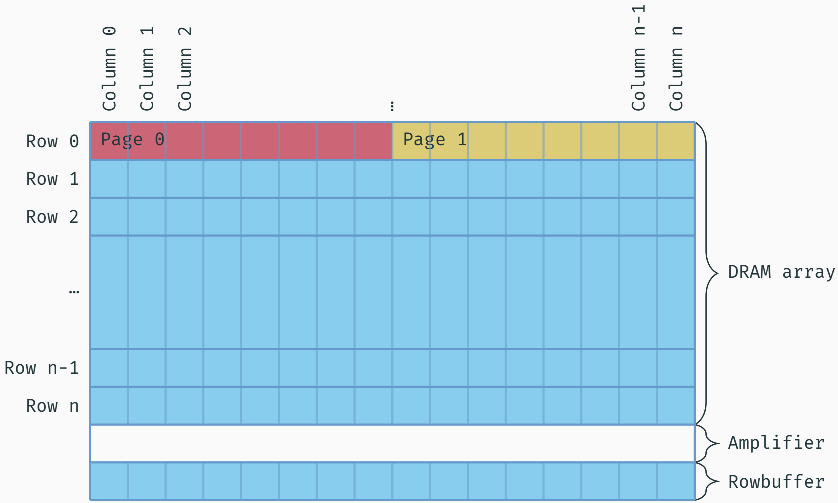
DRAM – physical architecture



DRAM – physical architecture

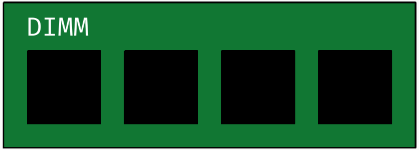


Structure within a DRAM bank



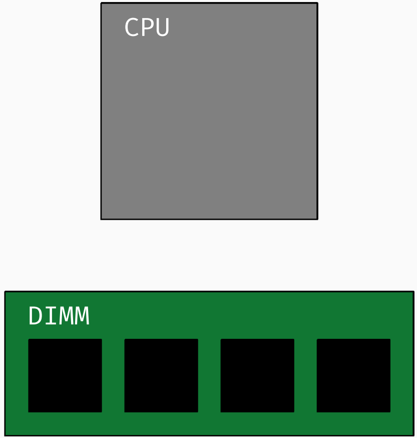
DRAM addressing

- Data is stored in physical memory:
    - Channel
    - DIMM
    - Rank
    - Bank
    - Row
    - Column
- The Memory Controller translates physical addresses to memory locations



Rowhammer

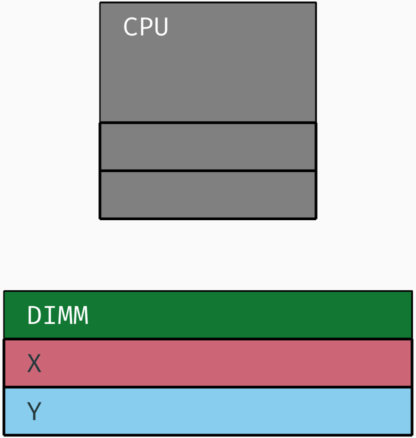
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

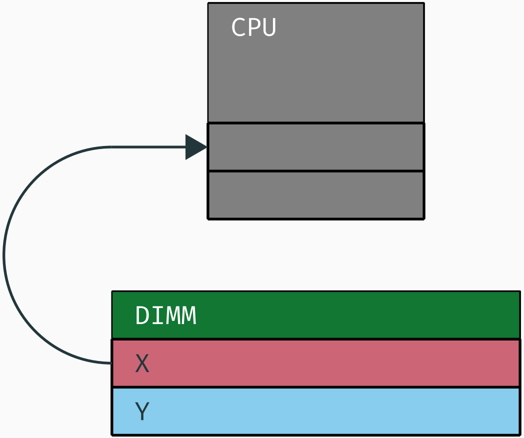
```
hammer:
    mov eax, X
    mov ebx, Y
    clflush X
    clflush Y
    jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

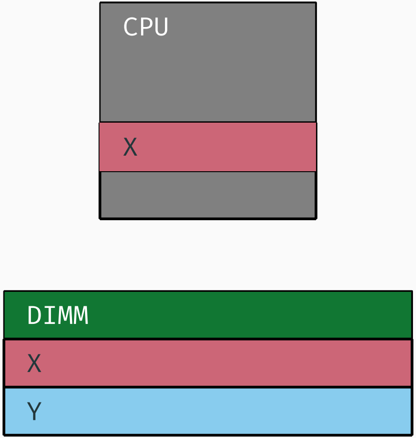
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

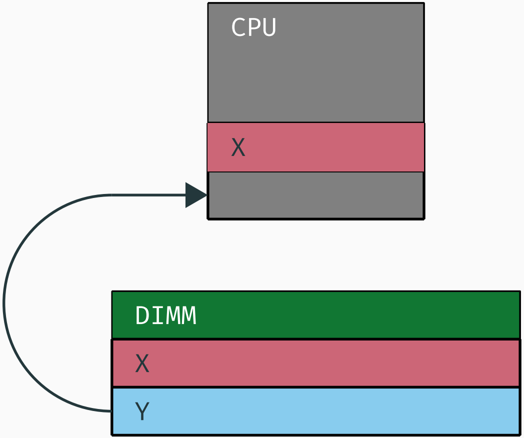
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```

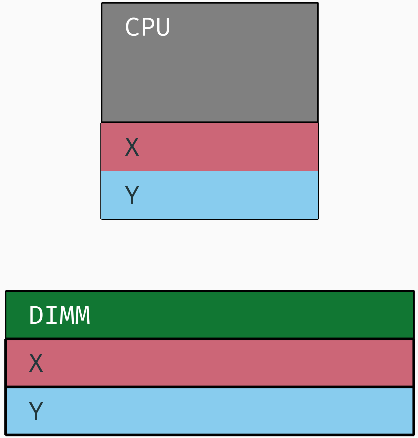


Source code from Kim et al. [1]

Rowhammer

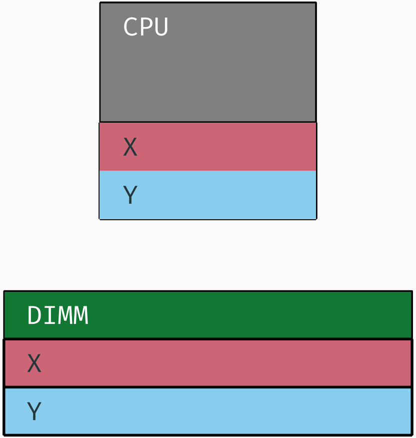
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```

Source code from Kim et al. [1]



Rowhammer

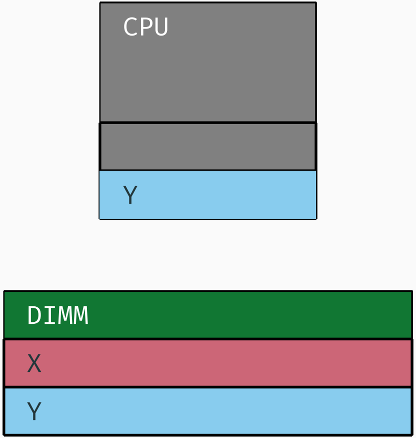
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```

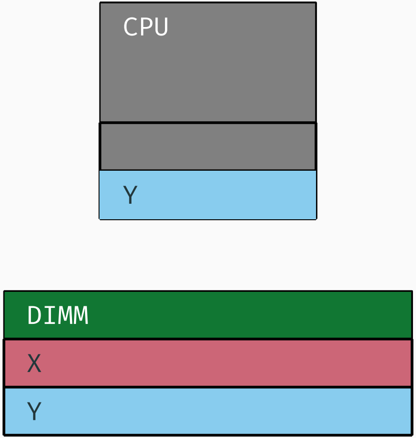


Source code from Kim et al. [1]

Rowhammer

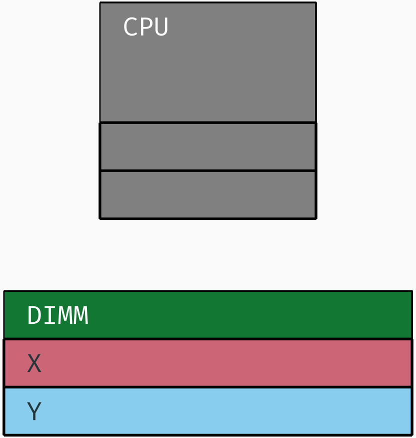
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```

Source code from Kim et al. [1]



Rowhammer

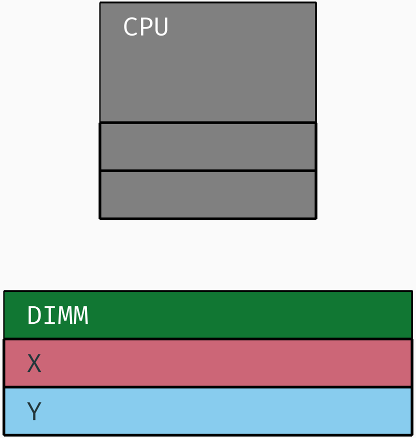
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

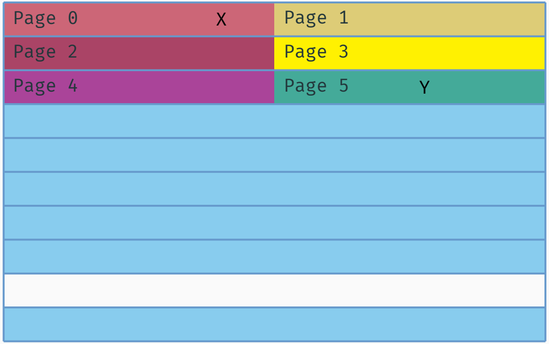
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

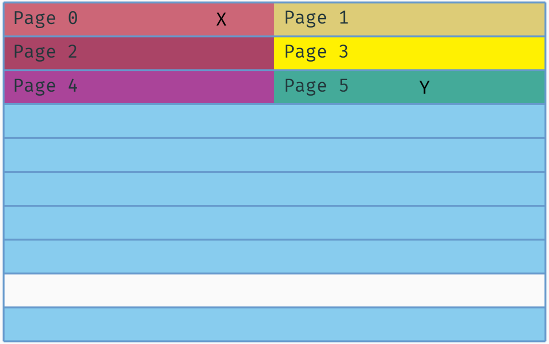
```
hammer:
    mov eax, X
    mov ebx, Y
    clflush X
    clflush Y
    jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

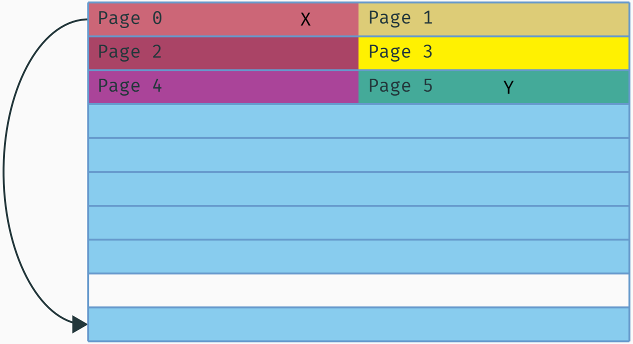
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

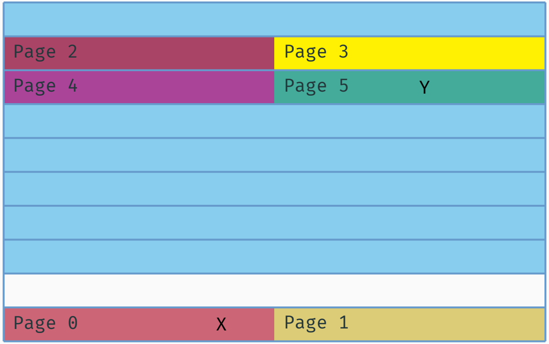
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

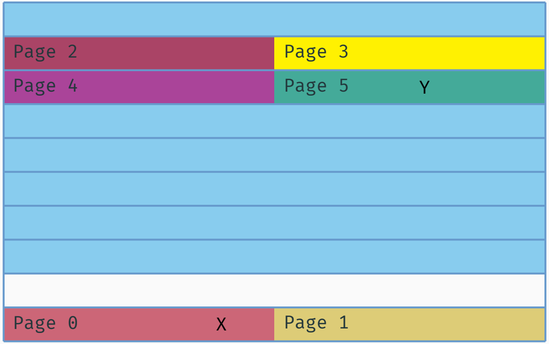
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

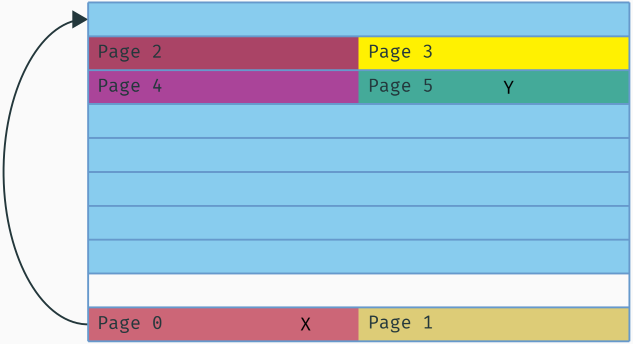
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

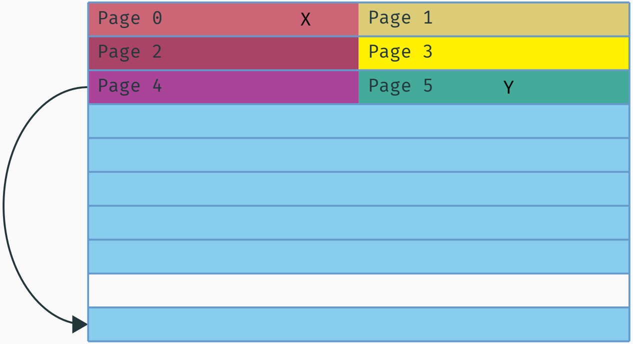
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

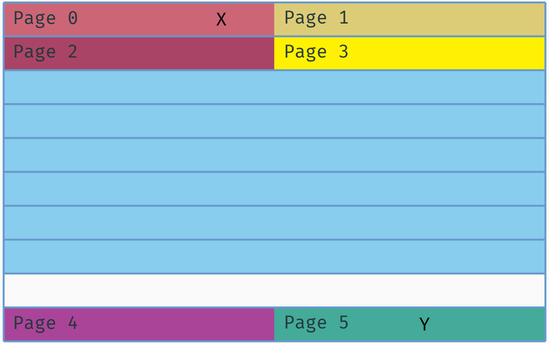
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

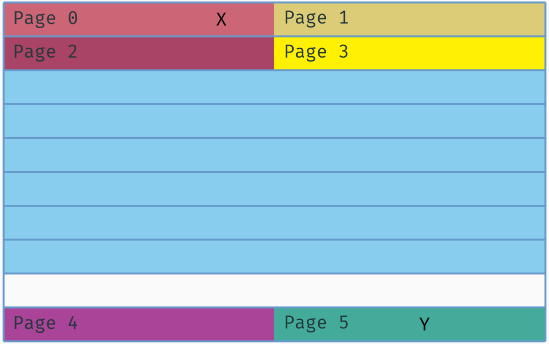
```
hammer:
  mov eax, X
  mov ebx, Y
  clflush X
  clflush Y
  jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

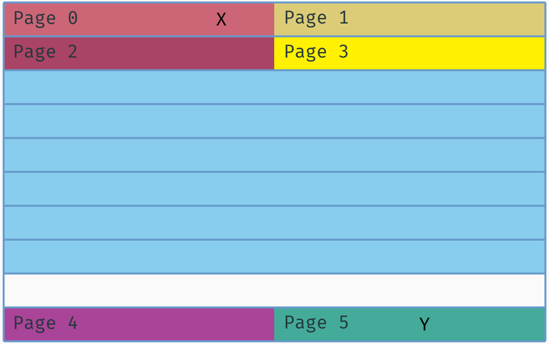
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer

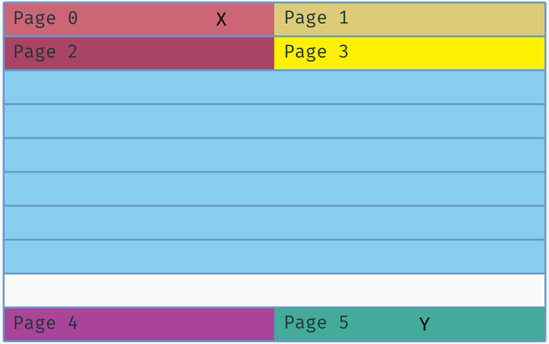
```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

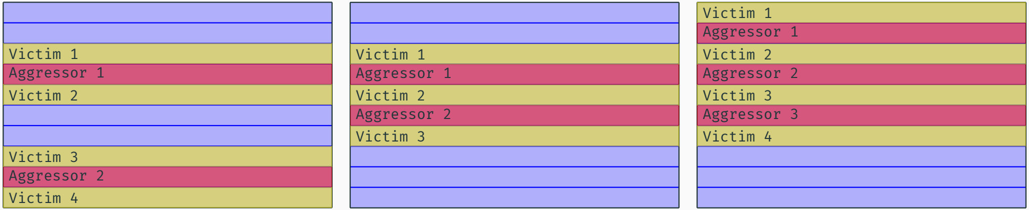
Rowhammer

```
hammer:
 mov eax, X
 mov ebx, Y
 clflush X
 clflush Y
 jmp hammer
```



Source code from Kim et al. [1]

Rowhammer



Victim 1
Aggressor 1
Victim 2
Victim 3
Aggressor 2
Victim 4

(a) Single Side

Victim 1
Aggressor 1
Victim 2
Aggressor 2
Victim 3

(b) Double Side

Victim 1
Aggressor 1
Victim 2
Aggressor 2
Victim 3
Aggressor 3
Victim 4

(c) Three Side

Figure 1: Examples of rowhammer patterns

Rowhammer: Academia vs Real-World Exploitation

- Academia:
  - The vast majority of systems is susceptible to Rowhammer
  - Exploitation of affected systems works in many cases
  - Exploitation works on multiple different platforms (x86, ARM, etc.)
  - Increasing number of papers related to Rowhammer
- However, no known case of Rowhammer being used in real-world attacks to the best of our knowledge

Methodology

Methodology

- Google Scholar search for the word *Rowhammer*: 2509 publications
- Publications with ≥ 5 mentions of the word *Rowhammer*: 463 publications
- Peer-reviewed papers that perform Rowhammer attacks: 55 publications
- Papers at A or A* conferences: 22 publications
- Added other relevant papers: 32 publications with 48 experimental evaluations

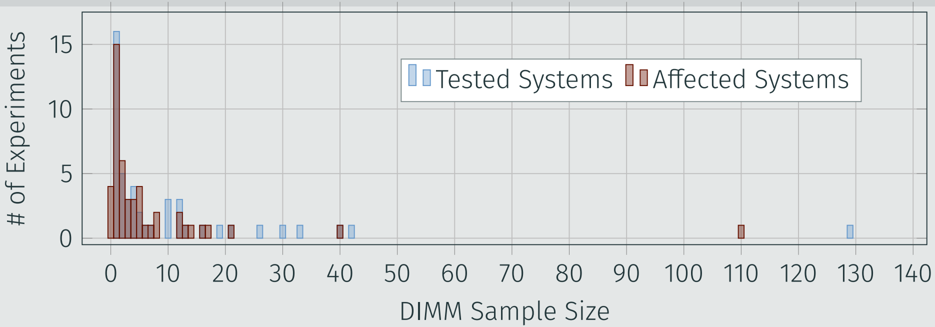
Threats to Rowhammer Research Validity

$\mathcal{T}$1 Sample Sizes Too Small

- Multiple potential causes for bit flips:
  - Bad memory cells
  - Temperature fluctuations
  - Cosmic rays
  - Voltage fluctuations
  - Manufacturing variations
  - Electrical properties of the motherboard

$\mathcal{T}$1 Sample Sizes Too Small

Sample Size of experimental Evaluations



$\mathcal{T}1$ Sample Sizes Too Small

$\mathcal{R}$1: DIMMs used in empirical research must be tested for other problems, e.g., using Memtest86 (except for integrated Rowhammer tests), to ensure that no other (non-Rowhammer) problems are present.

$\mathcal{R}$2: Increase the sample size to $\geq$ 30 DIMMs total, spread across 3 major vendors, each with at least 2 different capacities.

$\mathcal{R}$3: Do more reproduction studies of published work to gain more insights regarding the prevalence. More venues should accept reproduction studies.

$\mathcal{T}2$ Dependence on Elevated Attacker Privileges

- Seaborn [2] demonstrated two exploits based on Rowhammer in 2015
- Following, virtual-to-physical address mapping was made privileged
- Newer attacks use other concepts like uncached memory, Transparent Hugepages (THPs), or 1GB Hugepages
- Many prequisites of exploits have been mitigated as a reaction to the publication of these techniques
- Elevated attacker privileges make the attack more difficult to reproduce and may decrese trust in empirical results

$\mathcal{T}2$ Dependence on Elevated Attacker Privileges

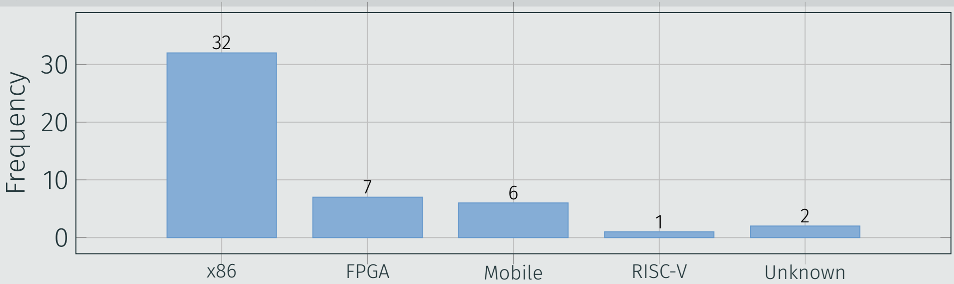
$\mathcal{R}4$: Attacks should only be classified as such when assessed under realistic attack scenarios, and there should be a more apparent distinction between actual attacks and potential (theoretical) attacks.

$\mathcal{T}3$ Uncertain Practical Applicability

- Some experiments are performed on:
  - Specialized hardware
  - Commodity hardware with extreme parameters
  - Rowhammer simulators
- While essential for understanding the Rowhammer effect, these results cannot be directly applied to real-world attacks
- $\mathcal{R}4$ applies again

$\mathcal{T}$3 Uncertain Practical Applicability

Frequencies of different experimental Setups



$\mathcal{T}$4 Comparability across Publications

- The position and number of bit flips depends on environmental parameters and the system and DIMMs that are evaluated
- In some publications, the experimental setup is not described sufficiently
- Even DIMMs that are the same model are affected differently by Rowhammer
- Hard to compare novel and existing attacks

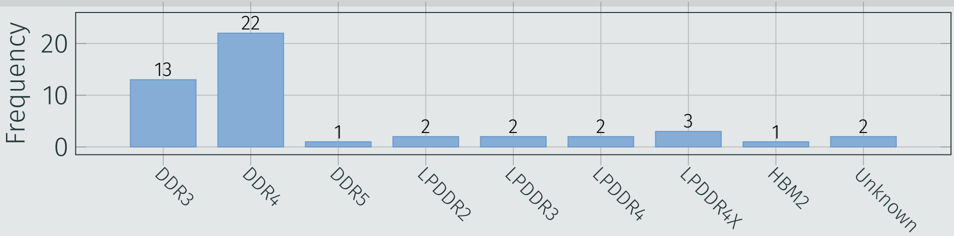
$\mathcal{T}$5 Unspecified Age and Wear of Hardware

- Aging affects the reliability of DRAM
- Bit flips induced by Rowhammer can “burn in”
- The implementation of on-DIMM mitigations like TRR strongly depends on the vendor and model of the DIMM
- In many publications, these information are not submitted, which increases the difficulty of reproducing results

$\mathcal{T}$5 Unspecified Age and Wear of Hardware

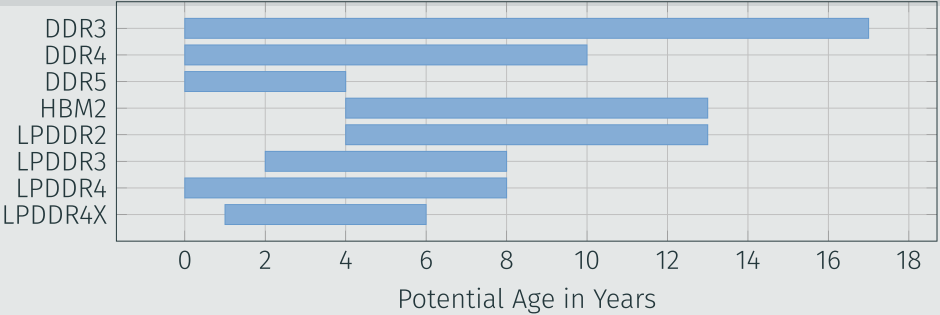
- Aging affects the reliability of DRAM

Different DRAM types



$\mathcal{T}$5 Unspecified Age and Wear of Hardware

Potential DRAM age



$\mathcal{T}$5 Unspecified Age and Wear of Hardware

$\mathcal{R}$5: Authors should publish the manufacturing date of the DIMMs used in experimental evaluation.

$\mathcal{R}$6: Authors should submit information about the DIMMs' wear in experimental evaluation.

$\mathcal{T}$6 Suboptimal Metrics for Comparison

- There are different metrics for the suscepbitility of systems:
    - Absolute number of bit flips in a given time or memory area
    - Minimal number of aggressor activations until the first bit flip
    - Percentage of times a bit flipped at a tested location
    - Time until the first (exploitable) bit flip is observed
- Different metrics are hard to compare
- Some metrics strongly depend on definitions, e.g., of *exploitable*

$\mathcal{T}$6 Suboptimal Metrics for Comparison

$\mathcal{R}$7: Authors should use multiple metrics for bit flips to allow for better comparisons to other works.

Conclusion

- There is a significant discrepance between Rowhammer Results in academia and real-world exploitation
- We analyzed 32 publications with 48 experimental evaluations
- We identified 6 threats to Rowhammer Research Validity
- We identified 7 recommendations future research should follow

Epistemology of Rowhammer Attacks:

Threats to Rowhammer Research Validity

Martin Heckel

September 22, 2025

[1] Graz University of Technology
[2] Hof University of Applied Sciences