FlippyRAM: A Large-Scale Study of Rowhammer Prevalence

Martin Heckel[1,2], Nima Sayadi[2], Jonas Juffinger[1],
Carina Fiedler[1], Daniel Gruss[1], and Florian Adamsky[2]

February 24, 2026

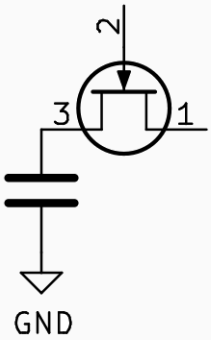
[1] Graz University of Technology
[2] Hof University of Applied Sciences

NeRAM
FWF Der Wissenschaftsfonds.
DFG Deutsche Forschungsgemeinschaft
Kofinanziert von der Europäischen Union

Background

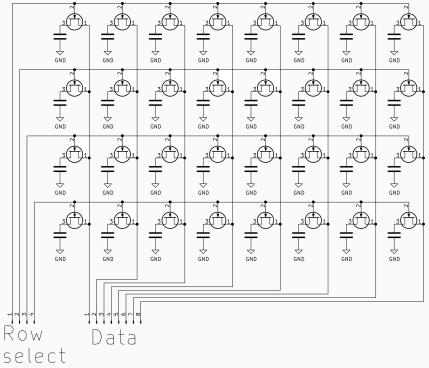
DRAM – Cells

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



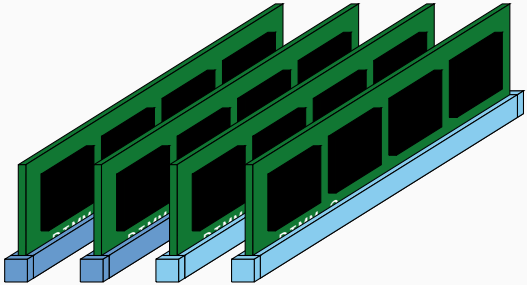
DRAM – Array

- 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
- Capacitors loose chage over time, so it is required to refresh the cells periodically (by default 64 ms for DDR3 and DDR4, 32 ms for DDR5)

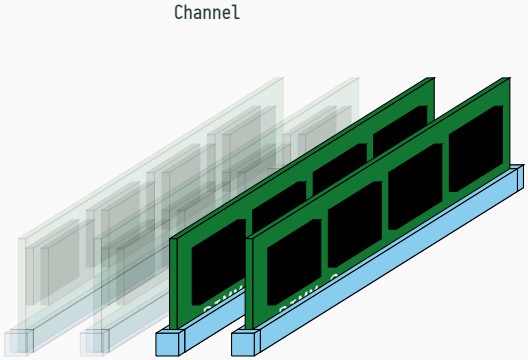


DRAM – Physical Architecture

System DRAM

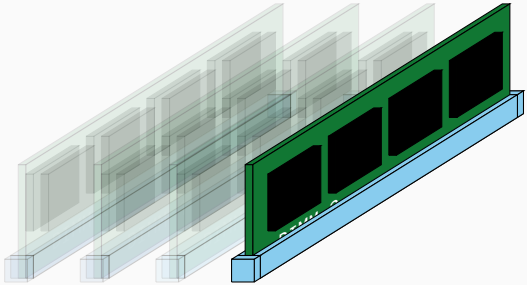


DRAM – Physical Architecture

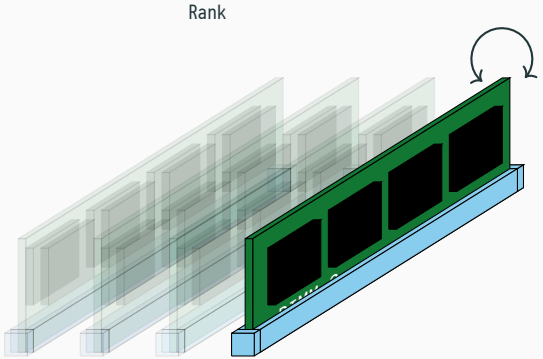


DRAM – Physical Architecture

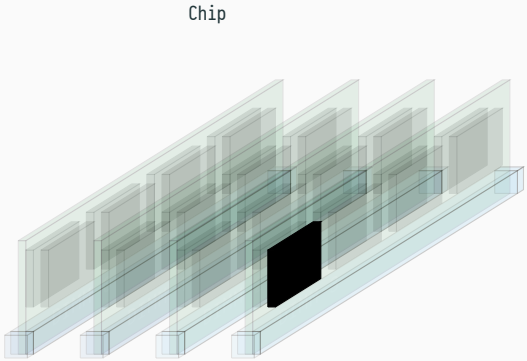
DIMM



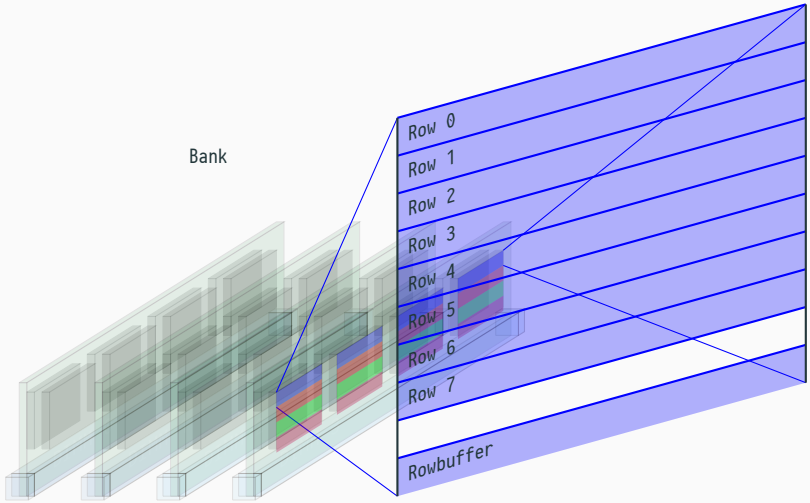
DRAM – Physical Architecture



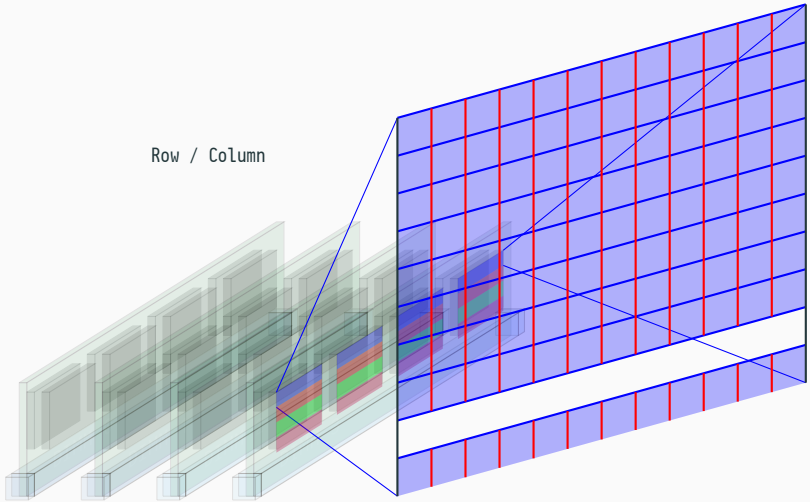
DRAM – Physical Architecture



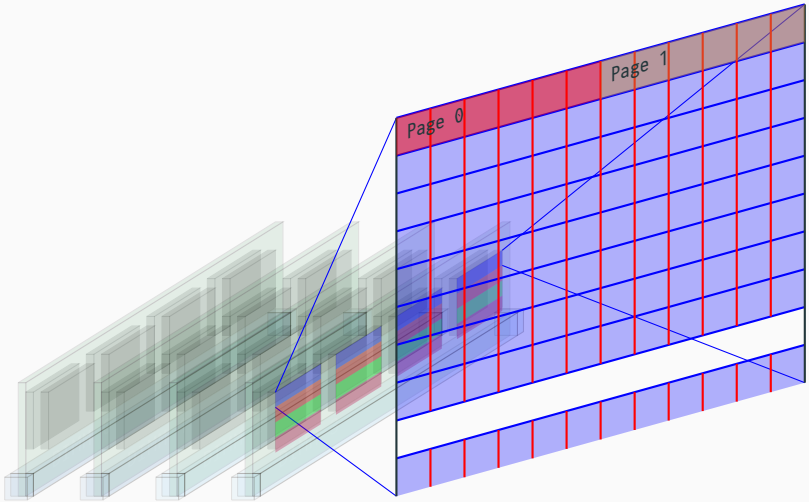
DRAM – Physical Architecture



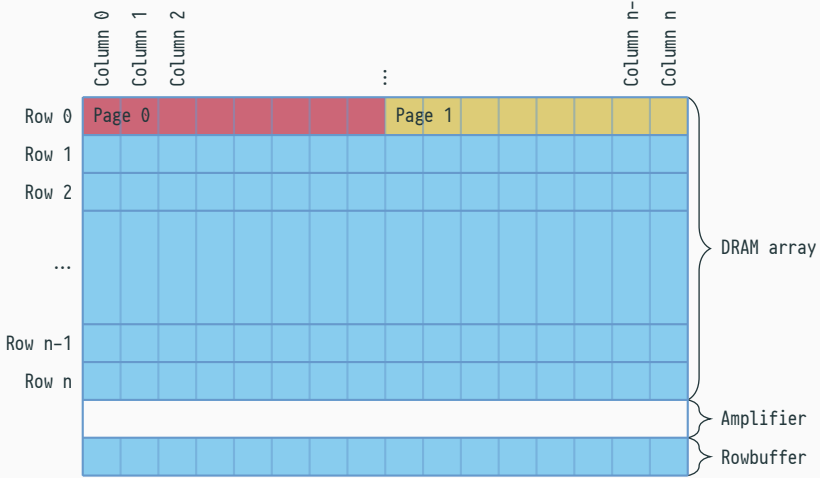
DRAM – Physical Architecture



DRAM – Physical Architecture

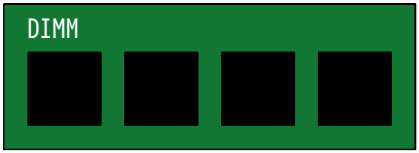


Structure within a DRAM bank

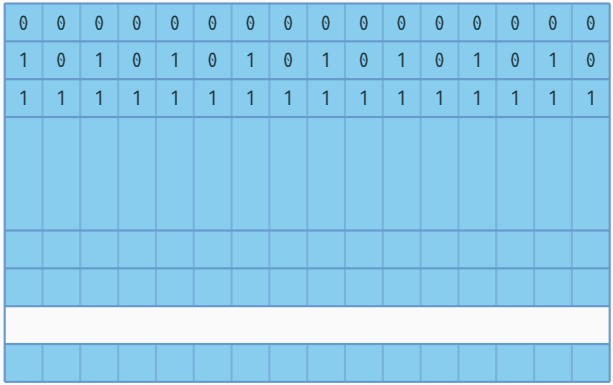


DRAM Addressing

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

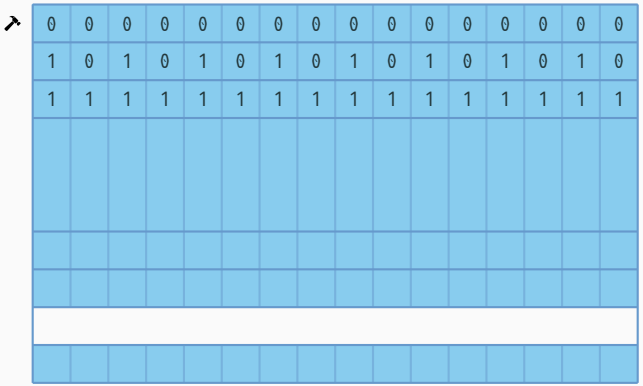


Simple Example of Rowhammer



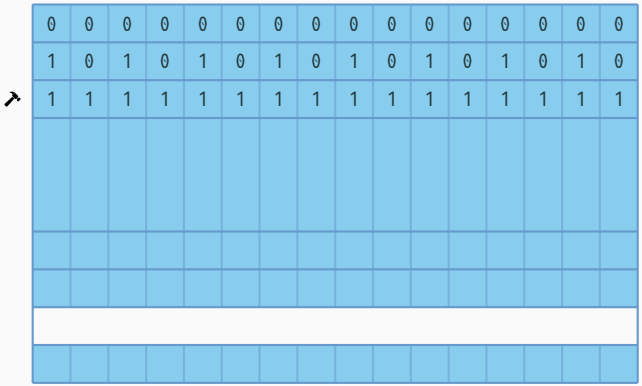

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer



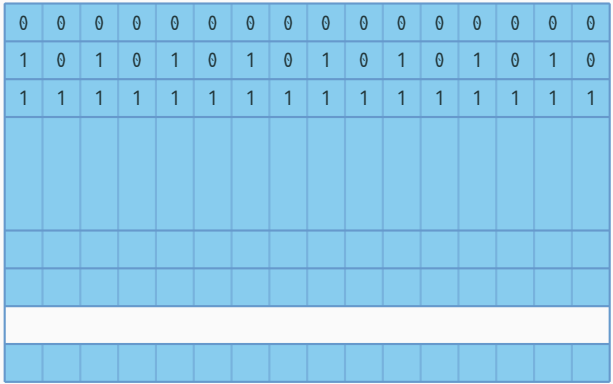

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer



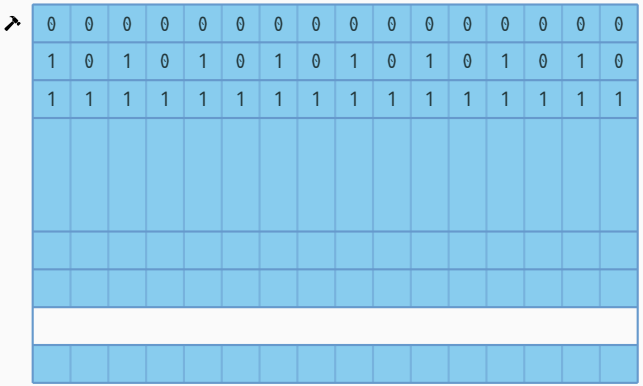

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer



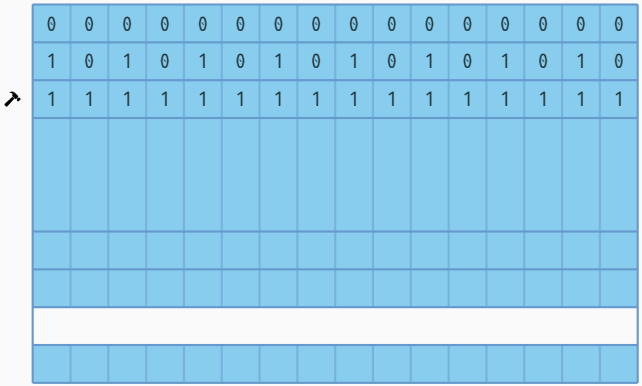

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer




```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer




```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

Simple Example of Rowhammer

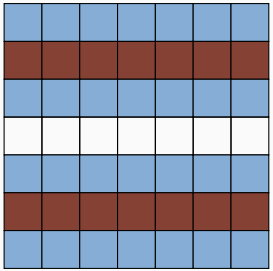
We can touch this!

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

```
hammertime:
  mov (Row 0), %eax
  mov (Row 2), %ebx
  clflush (Row 0)
  clflush (Row 2)
  jmp hammertime
```

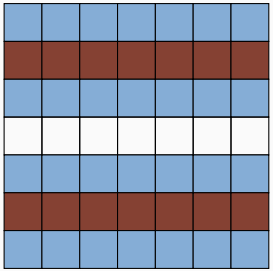
Various Hammering Patterns

Single-Sided

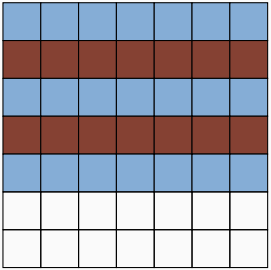


Various Hammering Patterns

Single-Sided

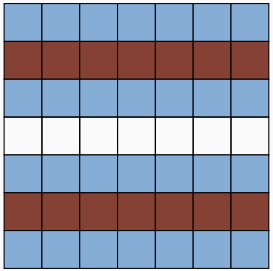


Double-Sided

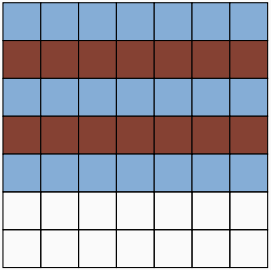


Various Hammering Patterns

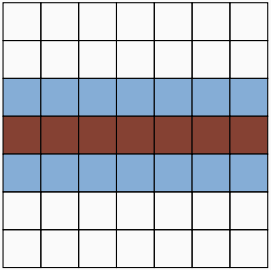
Single-Sided



Double-Sided

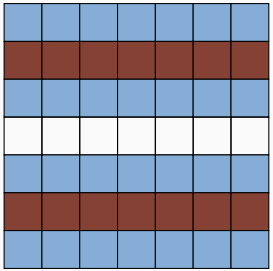


One-Location

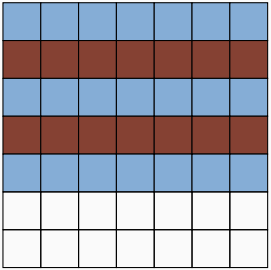


Various Hammering Patterns

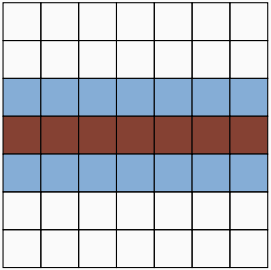
Single-Sided



Double-Sided



One-Location



… and several more (e.g., many-sided hammering)

FlippyRAM– Large-Scale Rowhammer Study

Overview

Overview

User Agreements
Privacy Policy
Risk Agreement

Overview

User Agreements
Privacy Policy
Risk Agreement

System Information
Retrieval

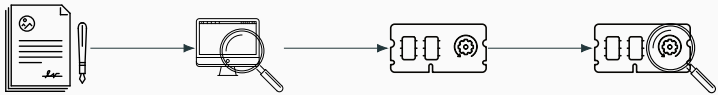
Overview

User Agreements
Privacy Policy
Risk Agreement

System Information
Retrieval

Reverse Engineering
of the Address-
ing Functions

Overview



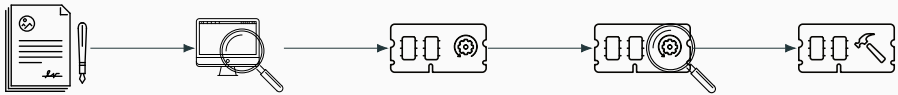
User Agreements
Privacy Policy
Risk Agreement

System Information Retrieval

Reverse Engineering of the Address-ing Functions

Verification & Injection of the Addressing Functions in the Rowhammer PoCs

Overview



User Agreements
Privacy Policy
Risk Agreement

System Information Retrieval

Reverse Engineering of the Addressing Functions

Verification & Injection of the Addressing Functions in the Rowhammer PoCs

Running different Rowhammer Tools

Overview

User Agreements
Privacy Policy
Risk Agreement

System Information Retrieval

Reverse Engineering of the Addressing Functions

Verification & Injection of the Addressing Functions in the Rowhammer PoCs

Running different Rowhammer Tools

Optional uploading the data to our server

How could Users participate?

How could Users participate?

- Get a free bootable USB stick from us

How could Users participa

How could Users participate?

How could Users participate?

- Get a free bootable USB stick from us
- Download bootable ISO from `https://FlippyR.am`

How could Users participate?

- Get a free bootable USB stick from us
- Download bootable ISO from `https://FlippyR.am`
- Verify the hash either way!

Hash mismatches and other hickups

- Flashing thousands of USB sticks over Christmas

Hash mismatches and other hickups

- Flashing thousands of USB sticks over Christmas
- Actually a small bug in the framework:

Hash mismatches and other hickups

- Flashing thousands of USB sticks over Christmas
- Actually a small bug in the framework:
  - Plan: write a nice summary for users

Hash mismatches and other hickups

- Flashing thousands of USB sticks over Christmas
- Actually a small bug in the framework:
  - Plan: write a nice summary for users
  - Testing first stick (took $\approx$ 8 hours) while flashing more $\rightarrow \approx 700$ drives done

Hash mismatches and other hickups

- Flashing thousands of USB
- Actually a small bug in the
  - Plan: write a nice summa
  - Testing first stick (took ≈ s done

Hash mismatches and other hickups

- Flashing thousands of USB sticks over Christmas
- Actually a small bug in the framework:
  - Plan: write a nice summary for users
  - Testing first stick (took $\approx$ 8 hours) while flashing more $\rightarrow \approx 700$ drives done
  - Bug: summary is missing $\rightarrow$ Bugfix $\rightarrow$ different hash!

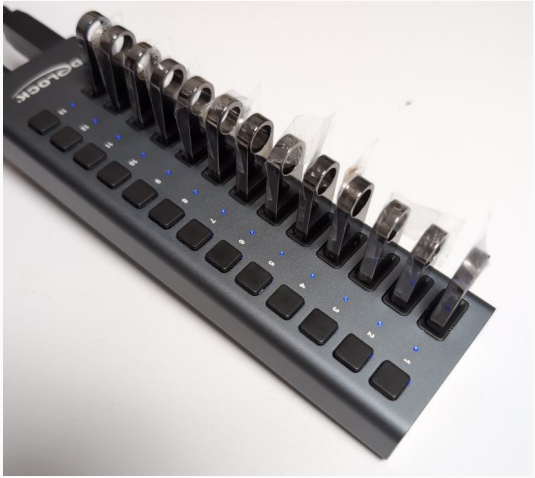
Flashing left Scratches ...

Flashing left Scratches ...

Flashing left Scratches ...

More complicated flashing Process required

More complicated flashing Process required



More complicated flashing Process required

More complicated flashing Process required

Results

Overview

User Agreements
Privacy Policy
Risk Agreement

System Information Retrieval

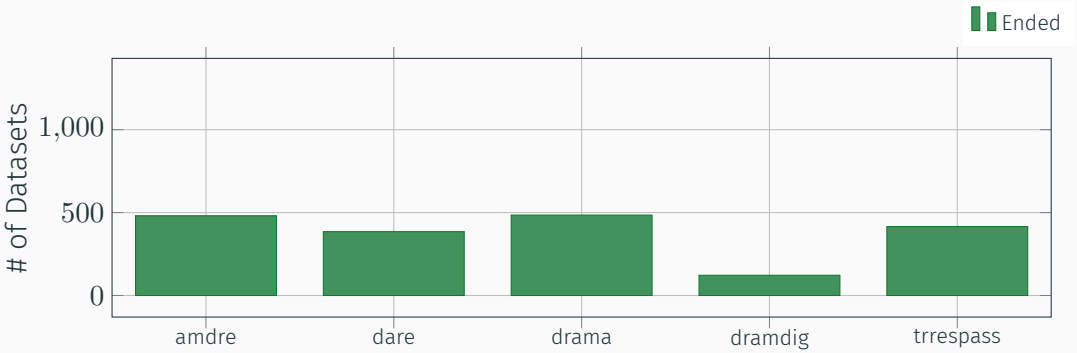
Reverse Engineering of the Addressing Functions

Verification & Injection of the Addressing Functions in the Rowhammer PoCs

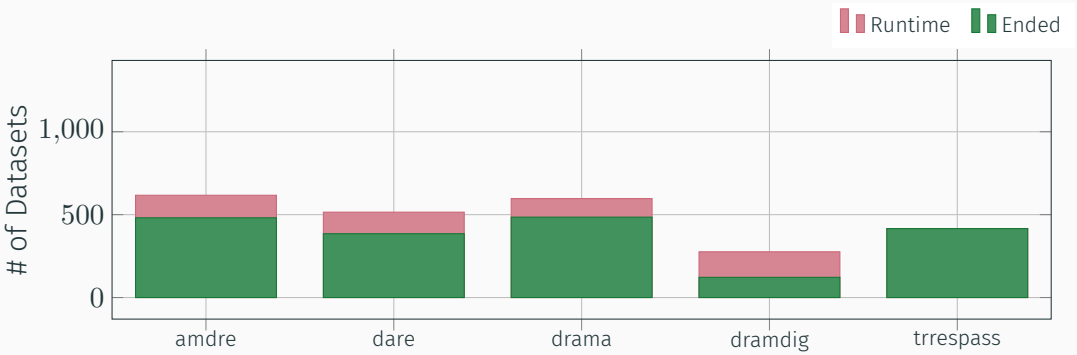
Running different Rowhammer Tools

Optional uploading the data to our server

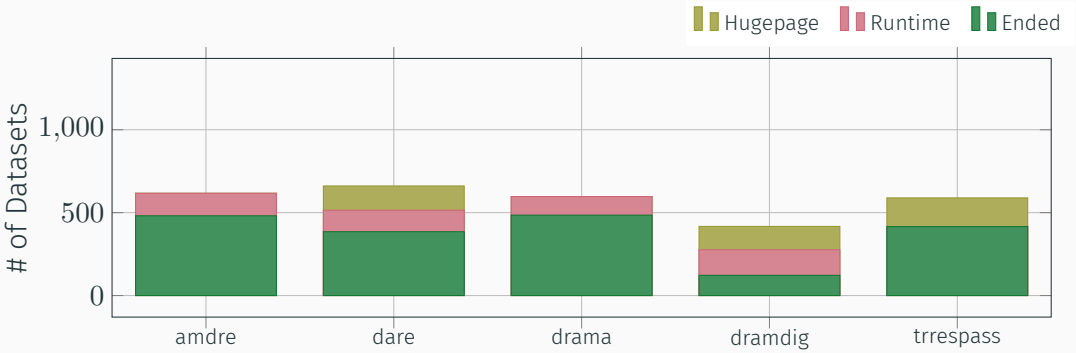
Reverse Engineering of the Addressing Functions



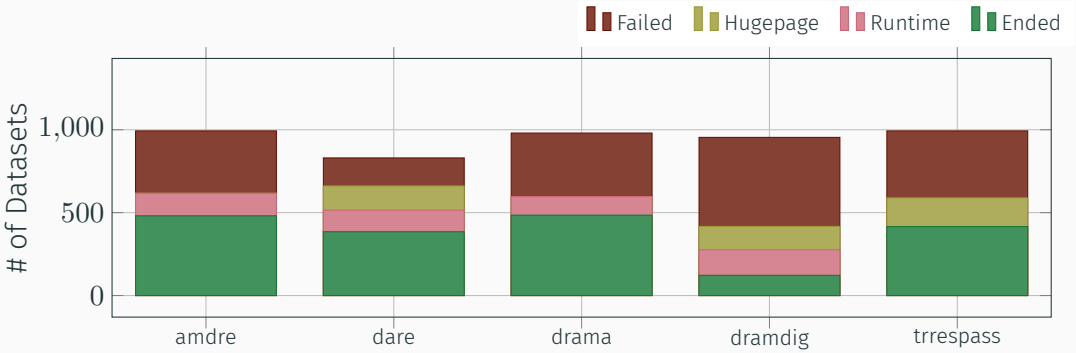
Reverse Engineering of the Addressing Functions



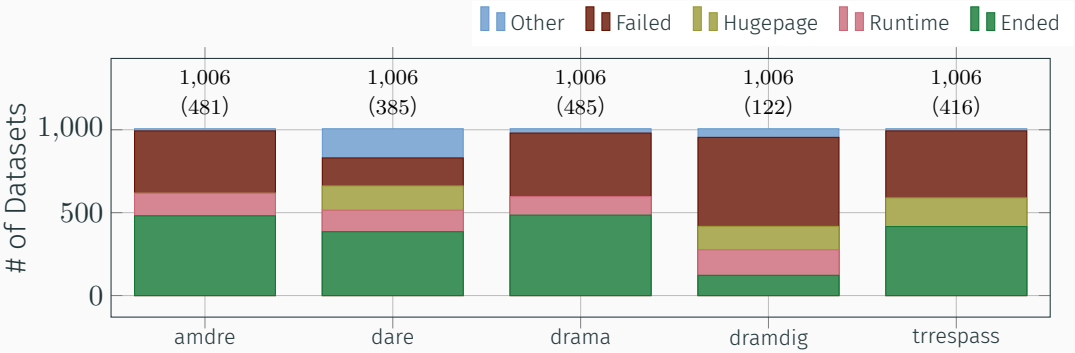
Reverse Engineering of the Addressing Functions



Reverse Engineering of the Addressing Functions

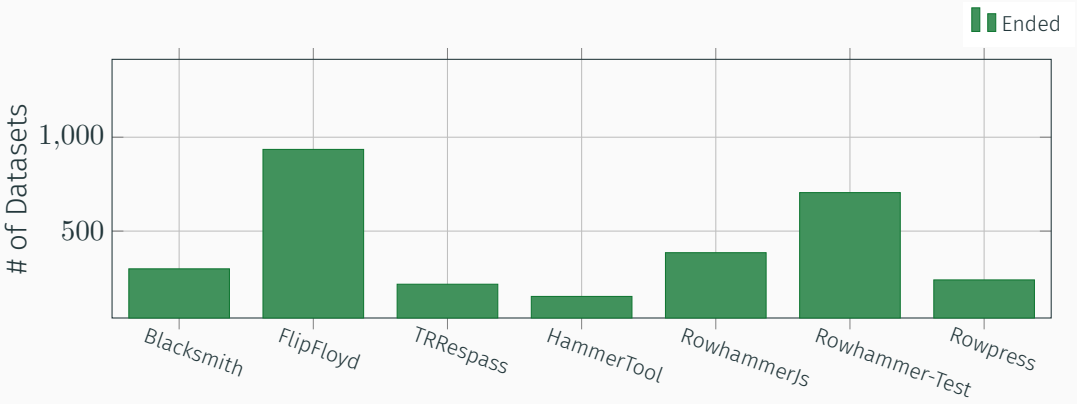


Reverse Engineering of the Addressing Functions

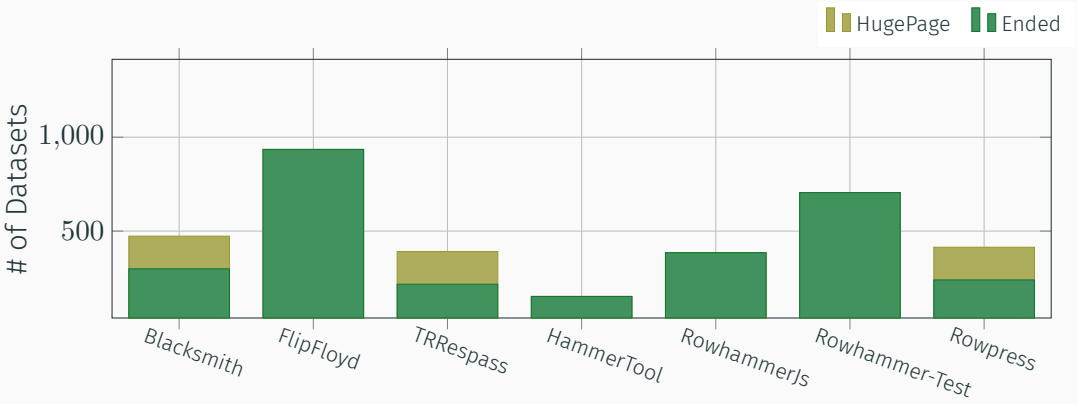


👁 (#1): Majority of cases: reverse-engineering tools fail, crash, or exceed time limits!

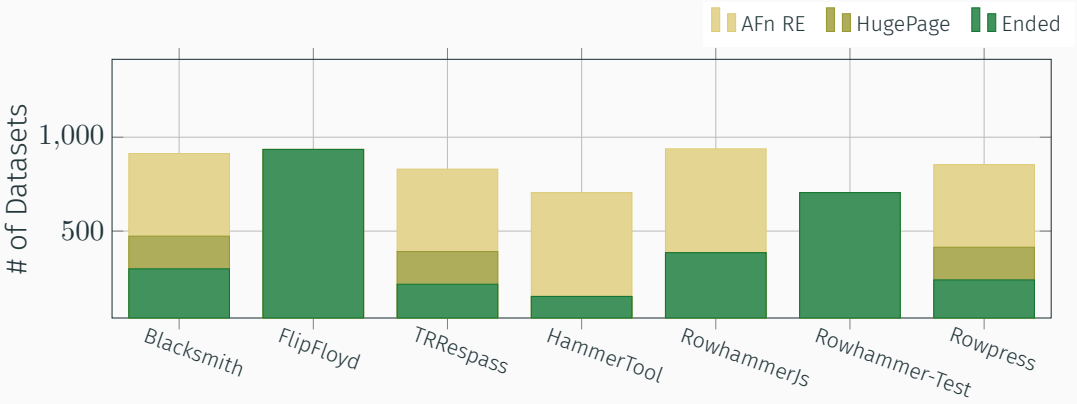
Running different Rowhammer Tools



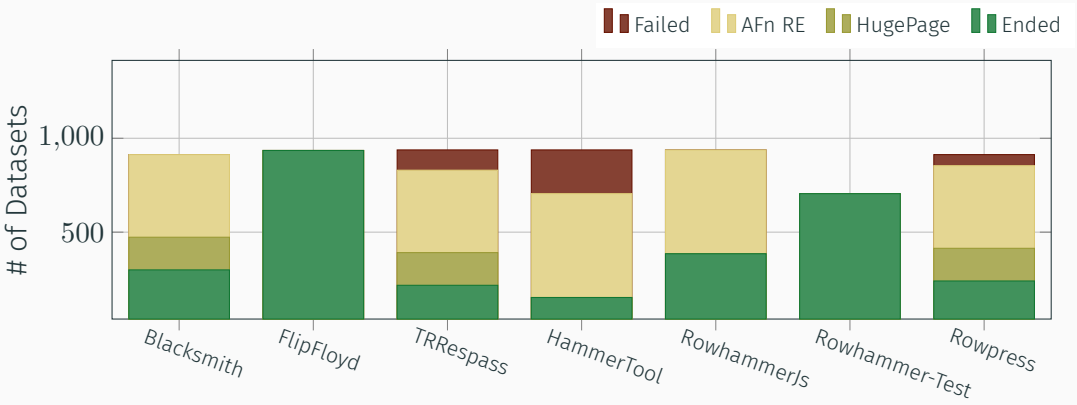
Running different Rowhammer Tools



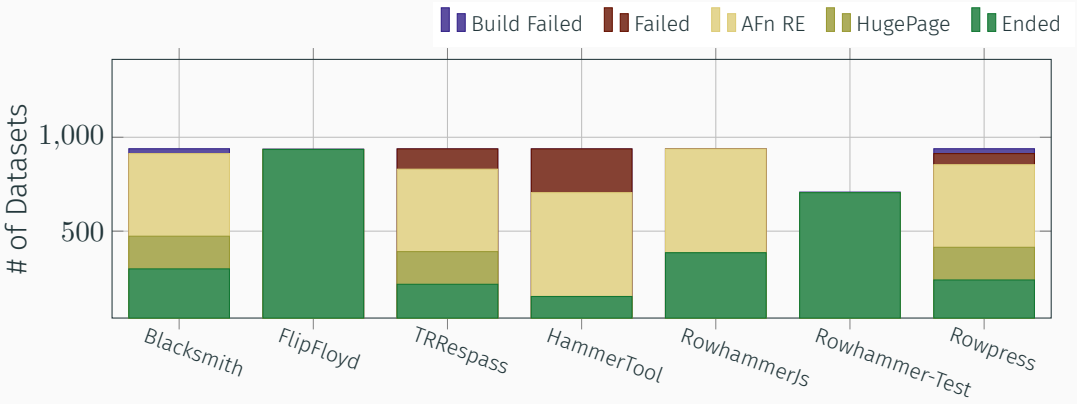
Running different Rowhammer Tools



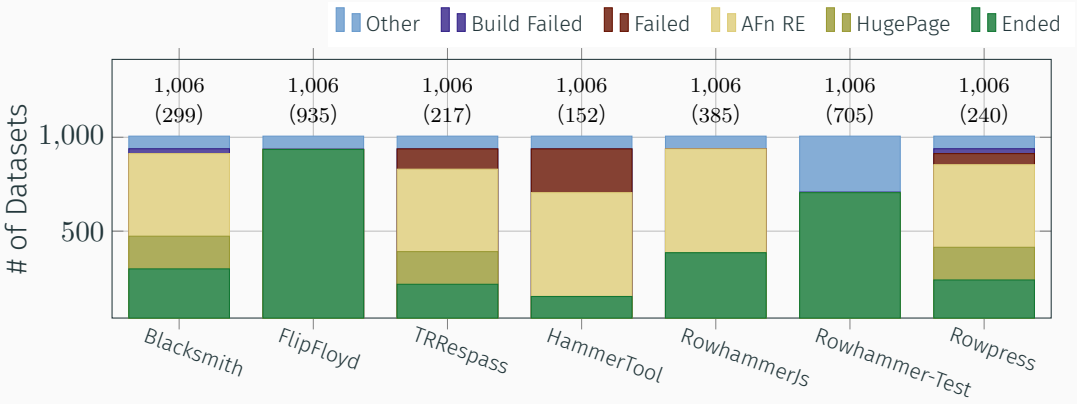
Running different Rowhammer Tools



Running different Rowhammer Tools

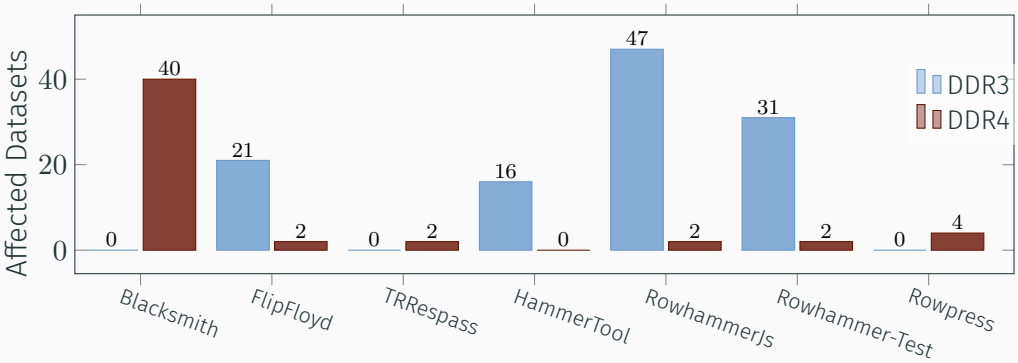


Running different Rowhammer Tools



👁 (#2): Many Rowhammer tools failed because of missing DRAM functions or 1 GiB hugepages.

Affected by Tool

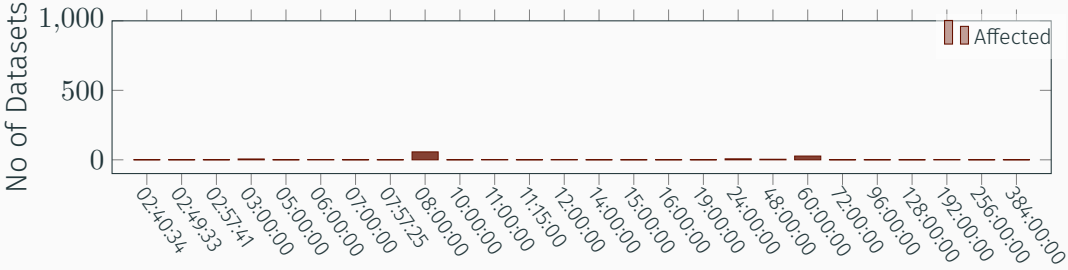


👁 (#3): 126 ($12.5\,\%$) out of 1006 datasets are vulnerable to fully-automated Rowhammer attacks!

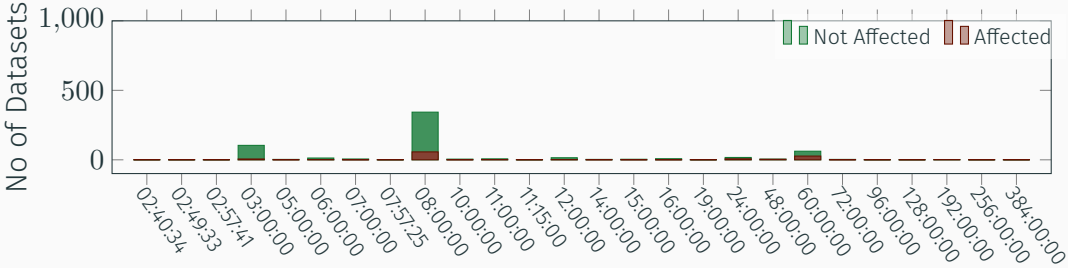
👁 (#4): DDR3 $\rightarrow$ simple fast patterns (RowhammerJS); DDR4 with TRR $\rightarrow$ pattern fuzzing for non-uniform patterns (Blacksmith)

👁 (#5): The minimum time to the first bit flip was between $0\,\mathrm{min}$ and $115\,\mathrm{min}$ on average, which is a practical time frame for real-world attacks.

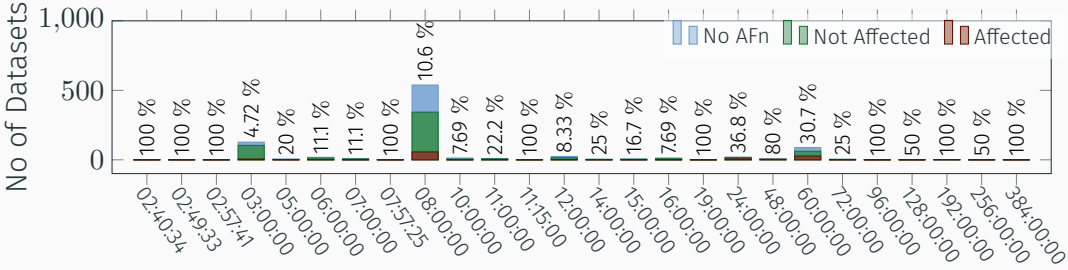
Affected systems by Runtime



Affected systems by Runtime

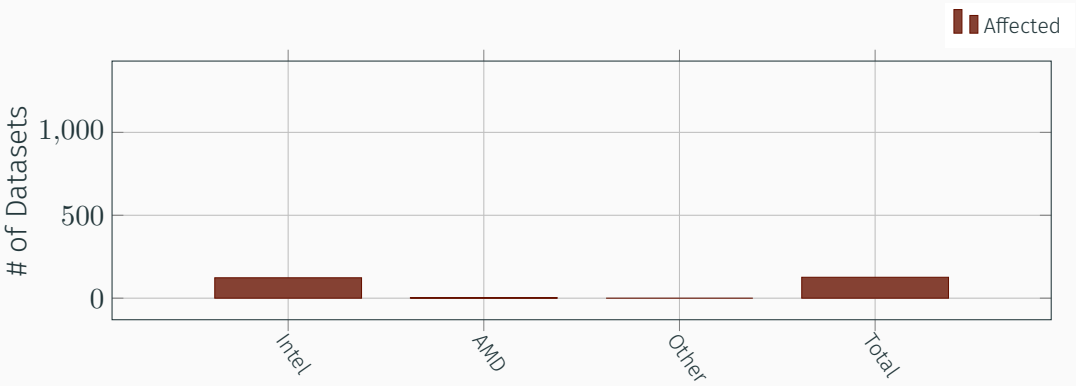


Affected systems by Runtime

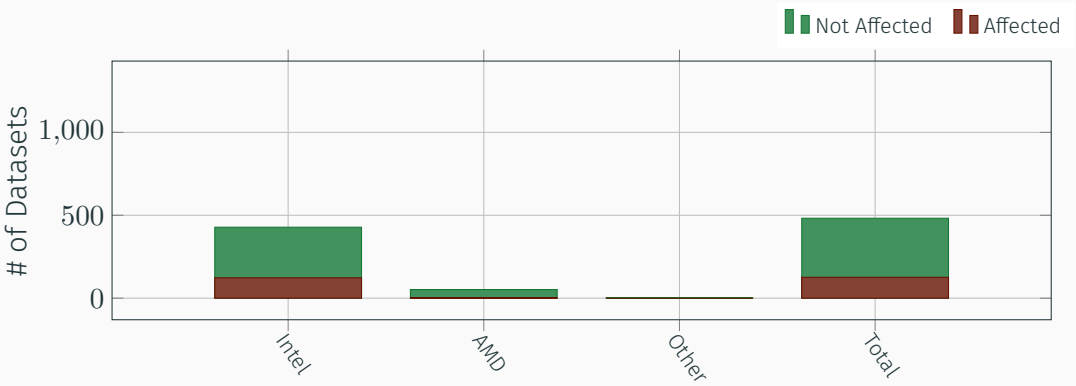


👁 (#6): On barely susceptible systems it can take very long to find flips (up to $617\,\mathrm{min}$ in our datasets), so longer testing times lead to more accurate detection.

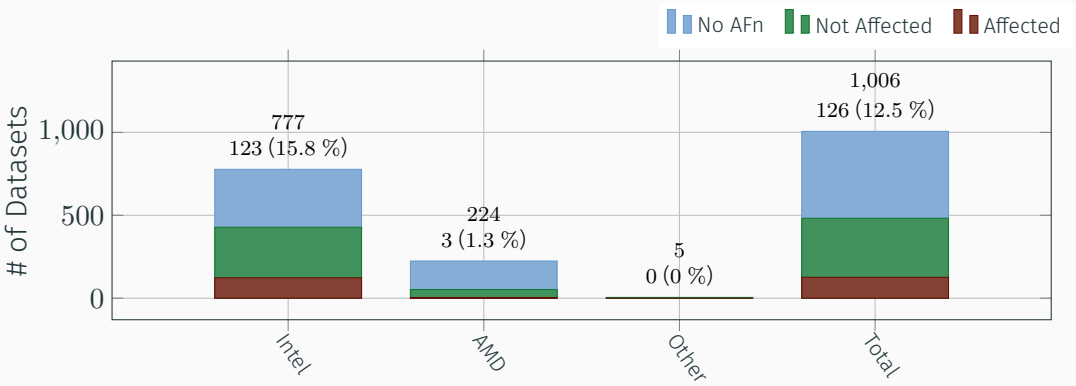
Affected systems by CPU Vendor



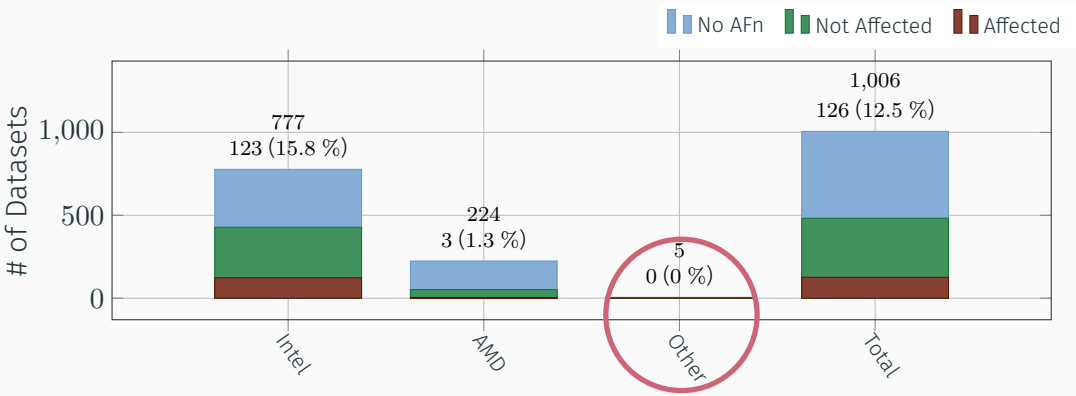
Affected systems by CPU Vendor



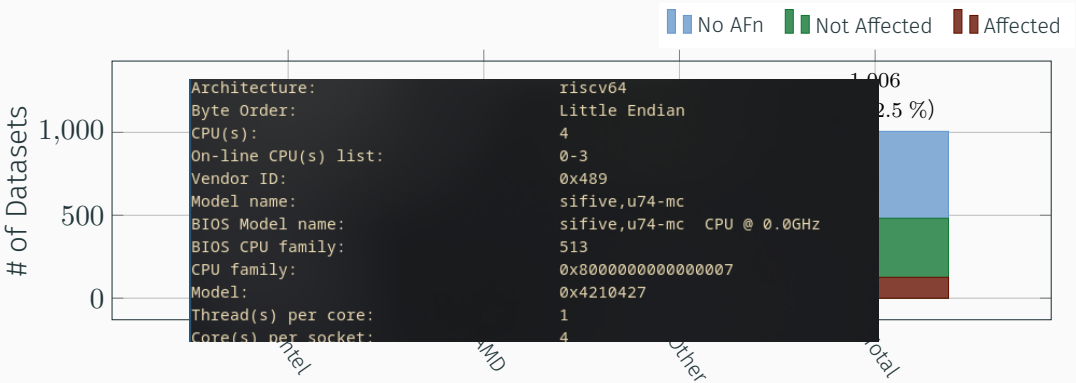
Affected systems by CPU Vendor



Affected systems by CPU Vendor

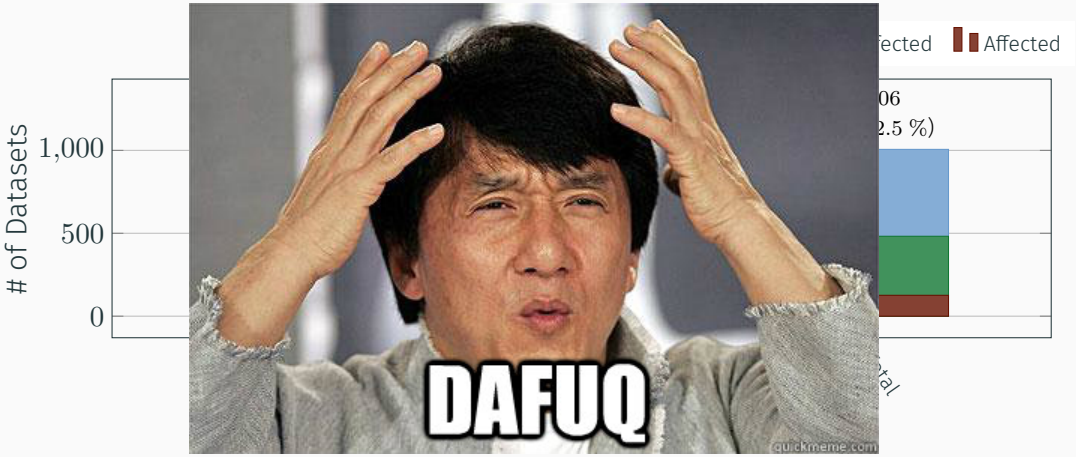


Affected systems by CPU Vendor



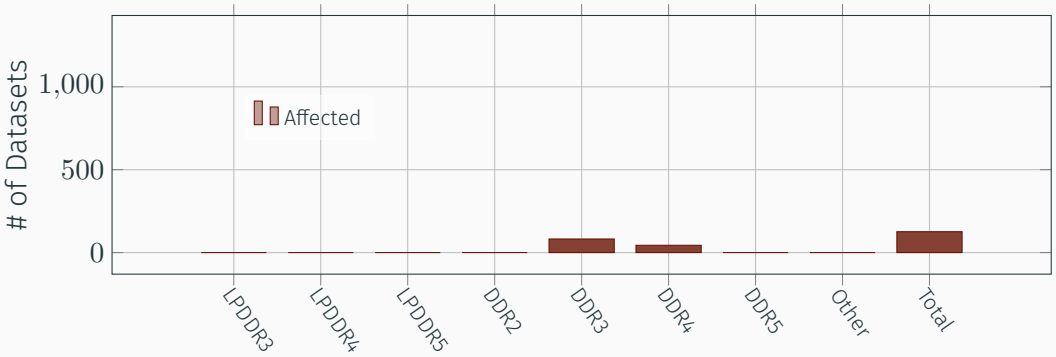

```
Architecture:                    riscv64
Byte Order:                      Little Endian
CPU(s):                          4
On-line CPU(s) list:             0-3
Vendor ID:                       0x489
Model name:                      sifive,u74-mc
BIOS Model name:                 sifive,u74-mc  CPU @ 0.0GHz
BIOS CPU family:                 513
CPU family:                      0x8000000000000007
Model:                           0x4210427
Thread(s) per core:              1
Core(s) per socket:              4
```

Affected systems by CPU Vendor

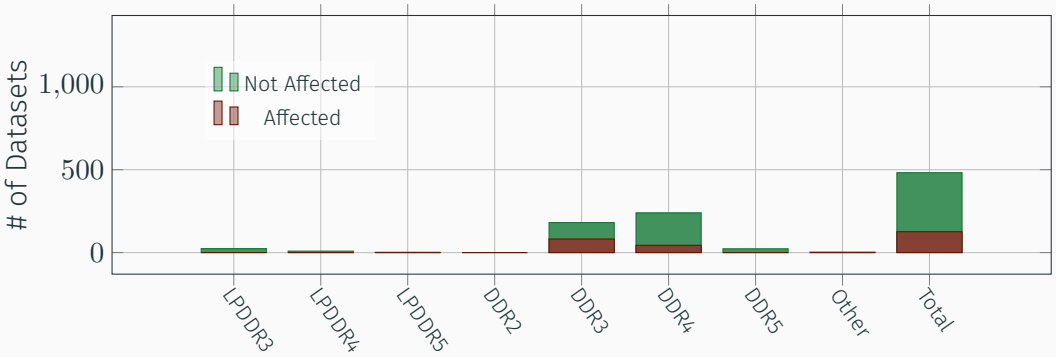


👁 (#7): Mainly tools for Intel, fewer AMD tools, especially when we started the study $\rightarrow$ we expect AMD to be equally affected.

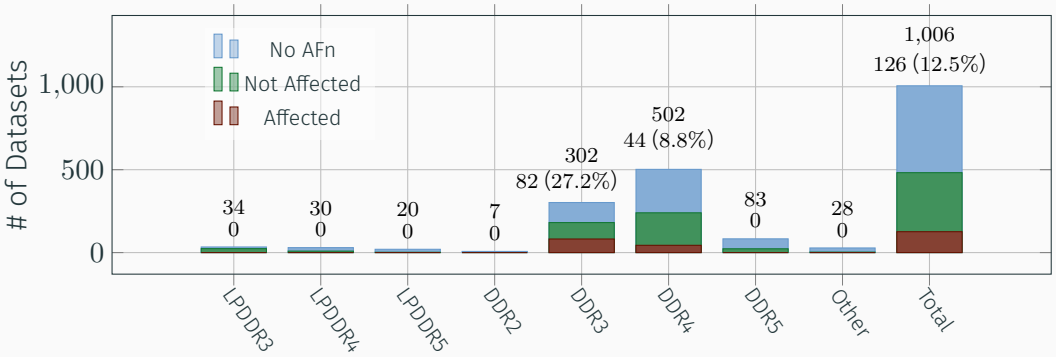
Affected DIMMs by DRAM Generation



Affected DIMMs by DRAM Generation

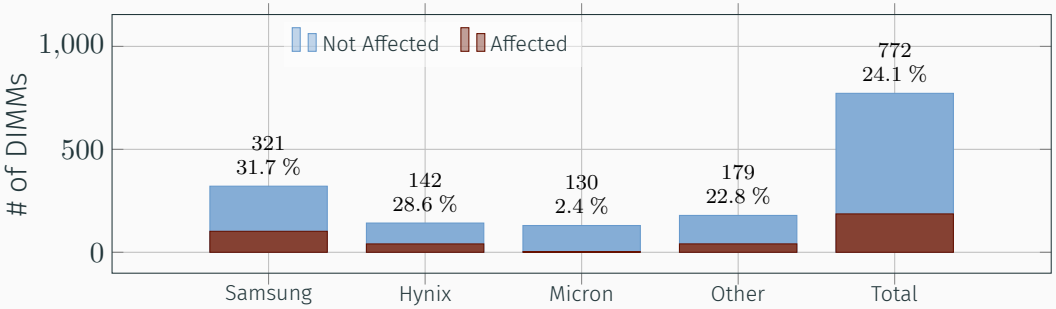


Affected DIMMs by DRAM Generation



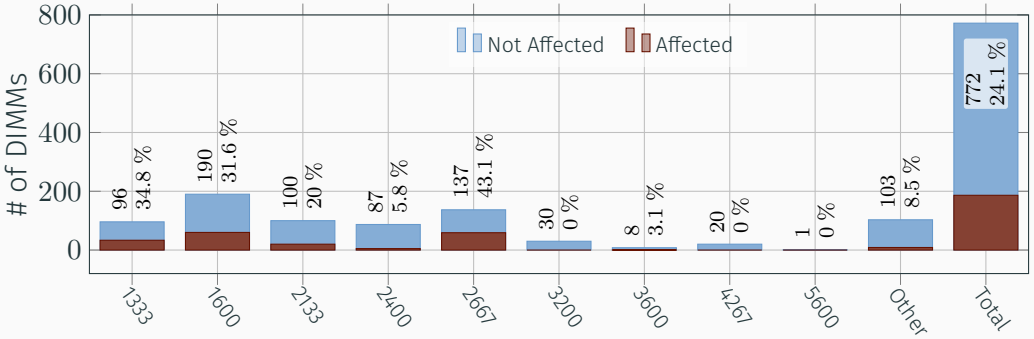
👁 (#8): Most affected systems are DDR3, followed by DDR4. No DDR5 systems were affected (lack of tools at the time we did our study).

Affected DIMMs by DRAM Vendor



👁 (#9): DRAM from Samsung, Hynix, and third-party resellers similarly affected by Rowhammer but only $2.4\,\%$ of Micron DIMMs?

Affected DIMMs by Transfer Rate



👁 (#10): Faster DIMMs $\rightarrow$ fewer bit flips?

Call for Action

- Improve experimental evaluations in Rowhammer research paper
  - Use FlippyRAM to evaluate your tools (e.g., computer rooms of your institution)
- Reduce effort to reproduce results and run large-scale Rowhammer studies
  - Add your tools and send pull requests so other people can use them

Conclusion

- A lower bound of $12.5\,\%$ of datasets are affected by fully-automated Rowhammer attacks
- Better tools are required for DRAM addressing function reverse-engineering
- Rowhammer Tools for systems with AMD and DDR5 should be added
- Rowhammer is a threat relevant for real-world systems

FlippyRAM: A Large-Scale Study of Rowhammer Prevalence

Martin Heckel[1,2], Nima Sayadi[2], Jonas Juffinger[1],
Carina Fiedler[1], Daniel Gruss[1], and Florian Adamsky[2]

February 24, 2026

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

NeRAM
FWF Der Wissenschaftsfonds.
DFG Deutsche Forschungsgemeinschaft
Kofinanziert von der Europäischen Union