

FLIPPYRAM: A Large-Scale Study of Rowhammer Prevalence

Martin Heckel^{1,2}, Nima Sayadi², Jonas Juffinger¹,
Carina Fiedler¹, Daniel Gruss¹, and Florian Adamsky²

February 24, 2026

¹ Graz University of Technology

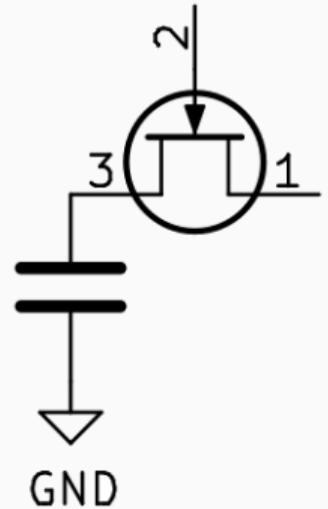
² Hof University of Applied Sciences



Background

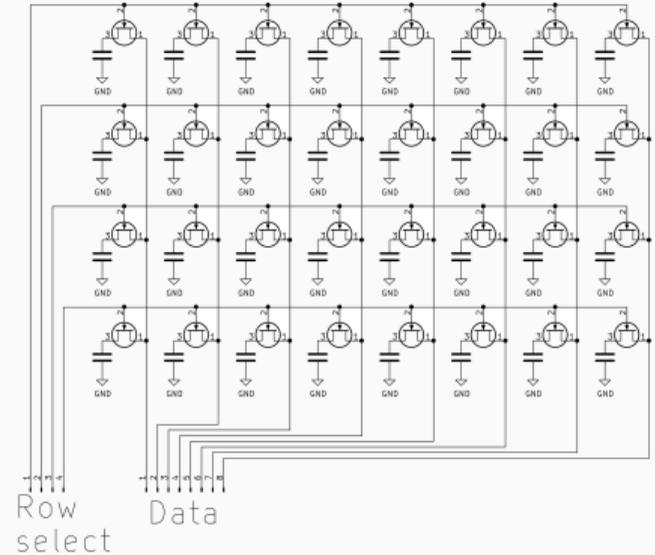
DRAM – Cells

- 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



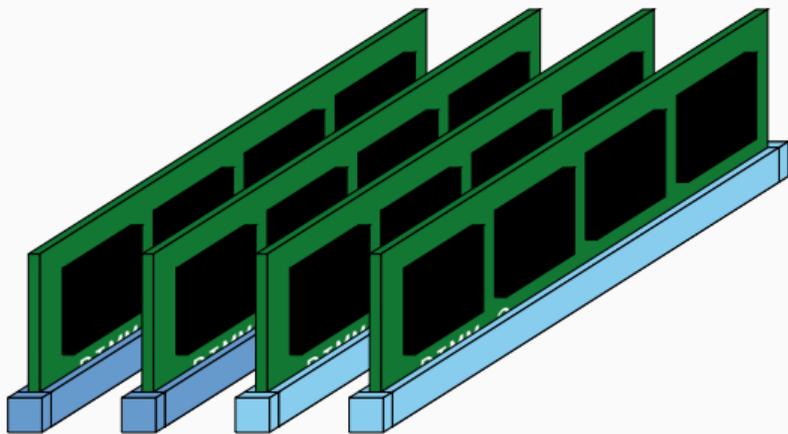
DRAM – Array

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

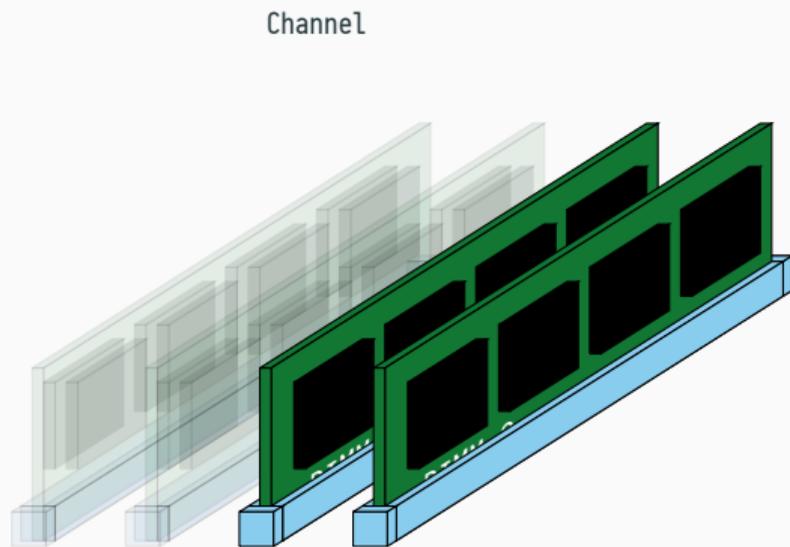


DRAM – Physical Architecture

System DRAM

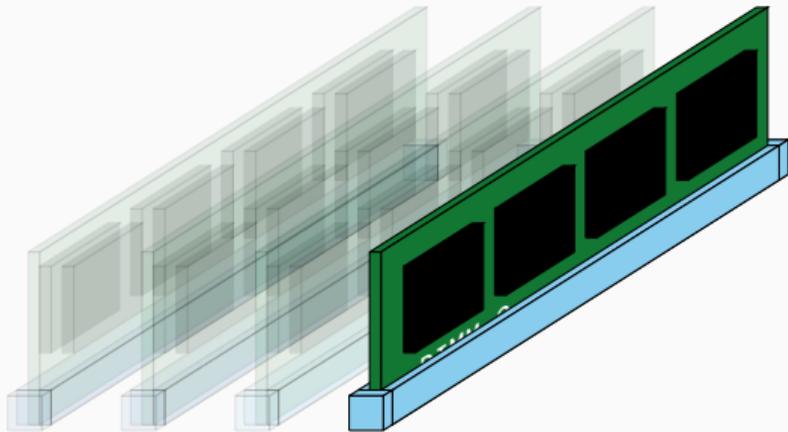


DRAM – Physical Architecture

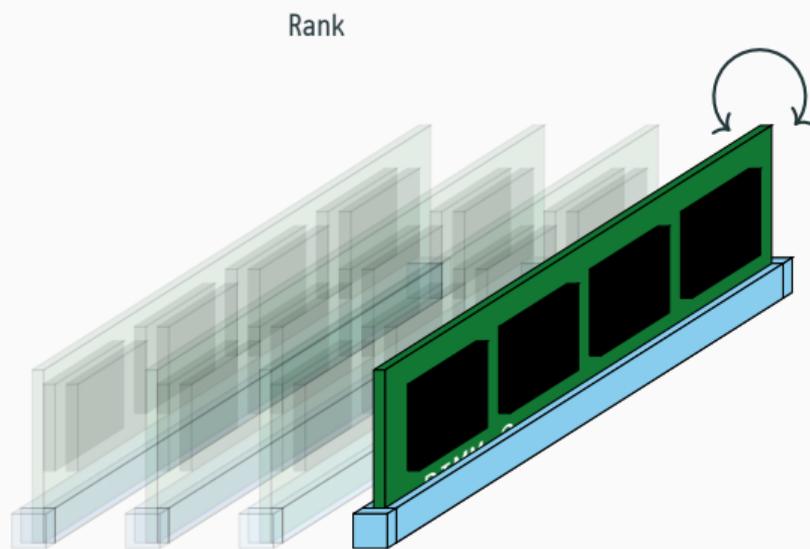


DRAM – Physical Architecture

DIMM

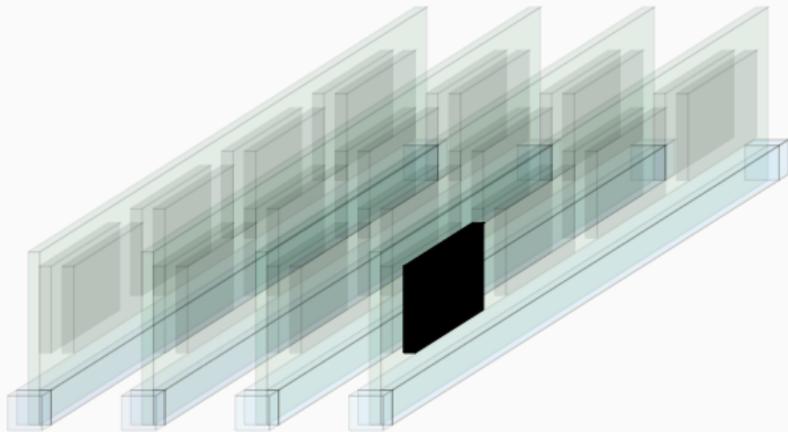


DRAM – Physical Architecture

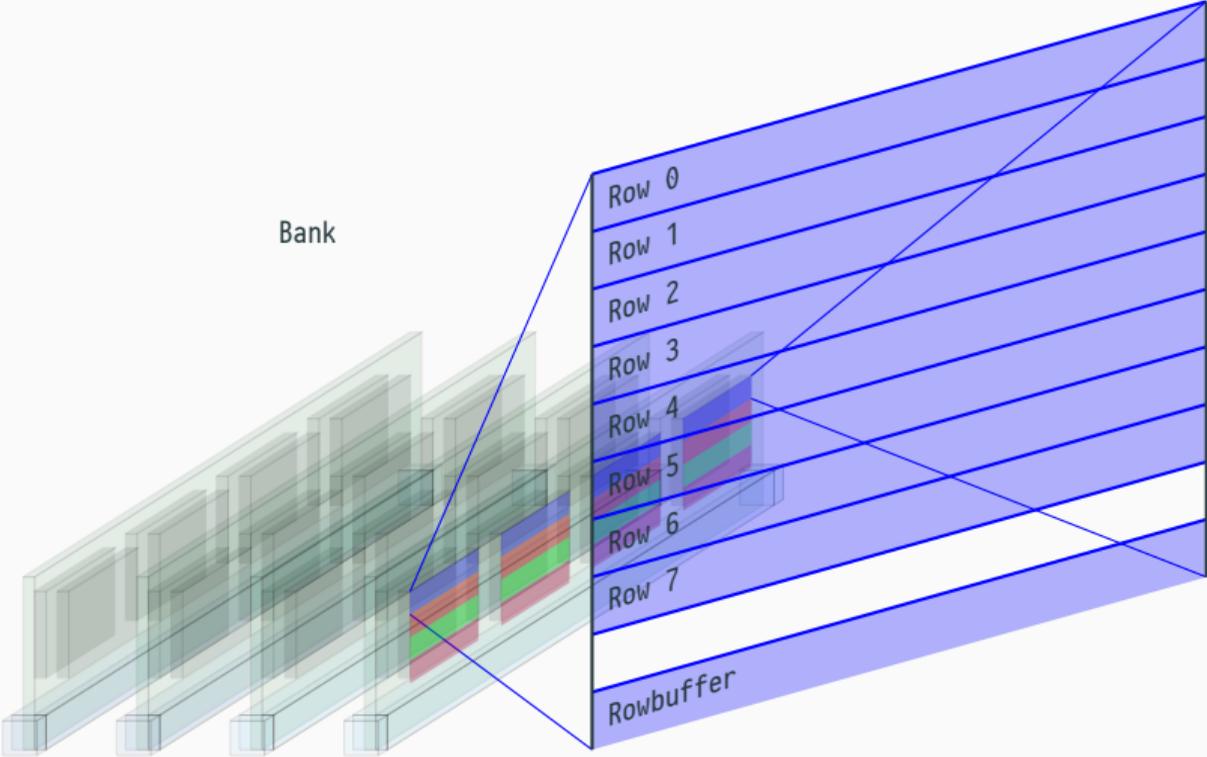


DRAM – Physical Architecture

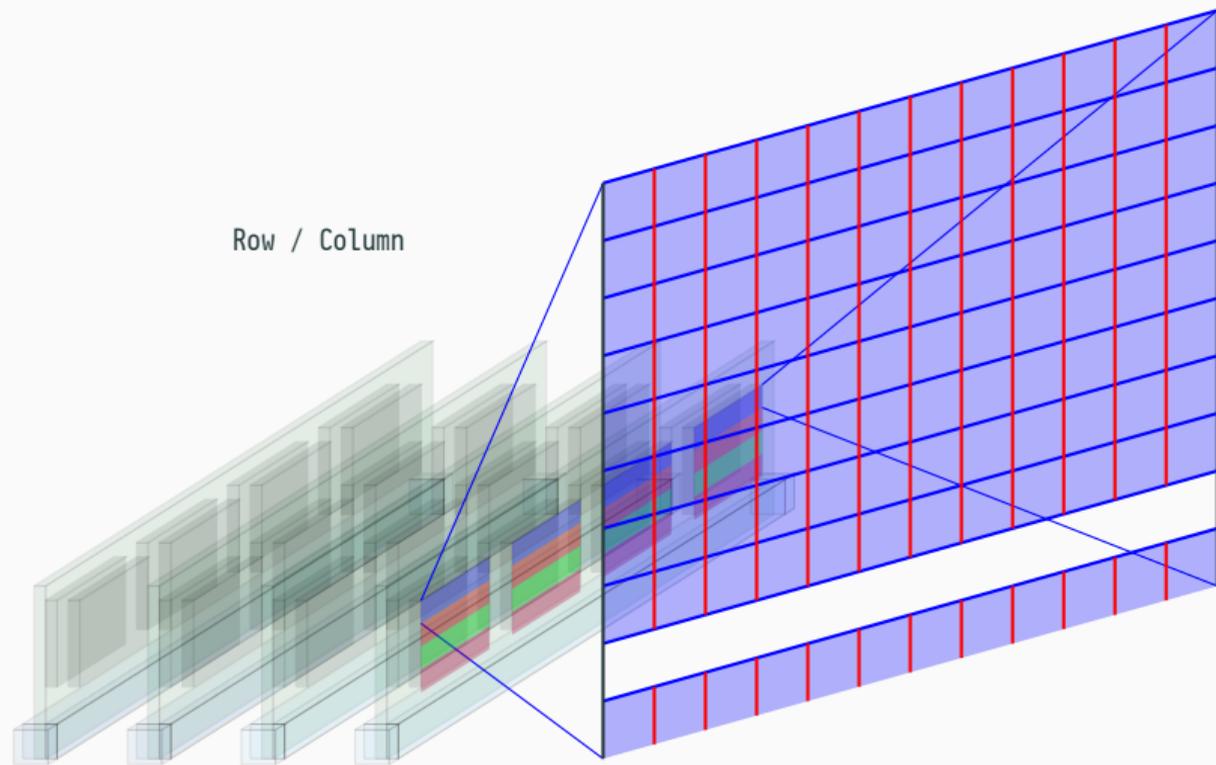
Chip



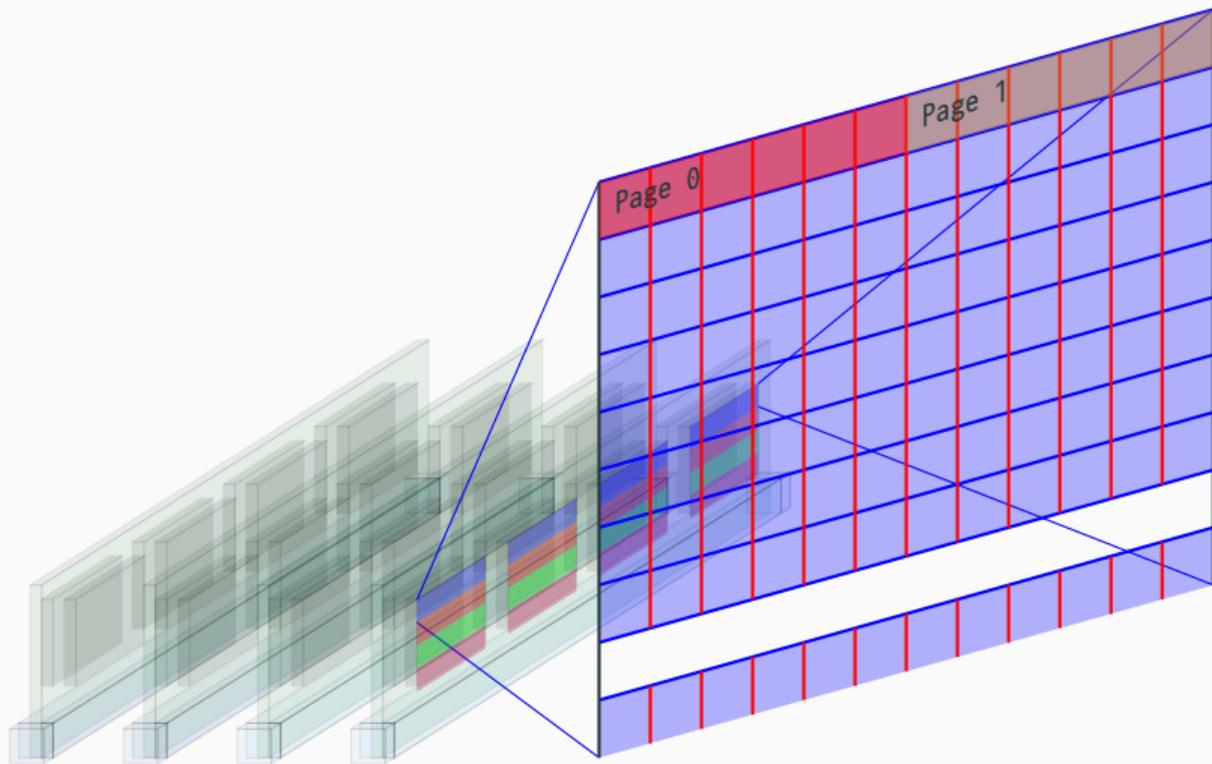
DRAM – Physical Architecture



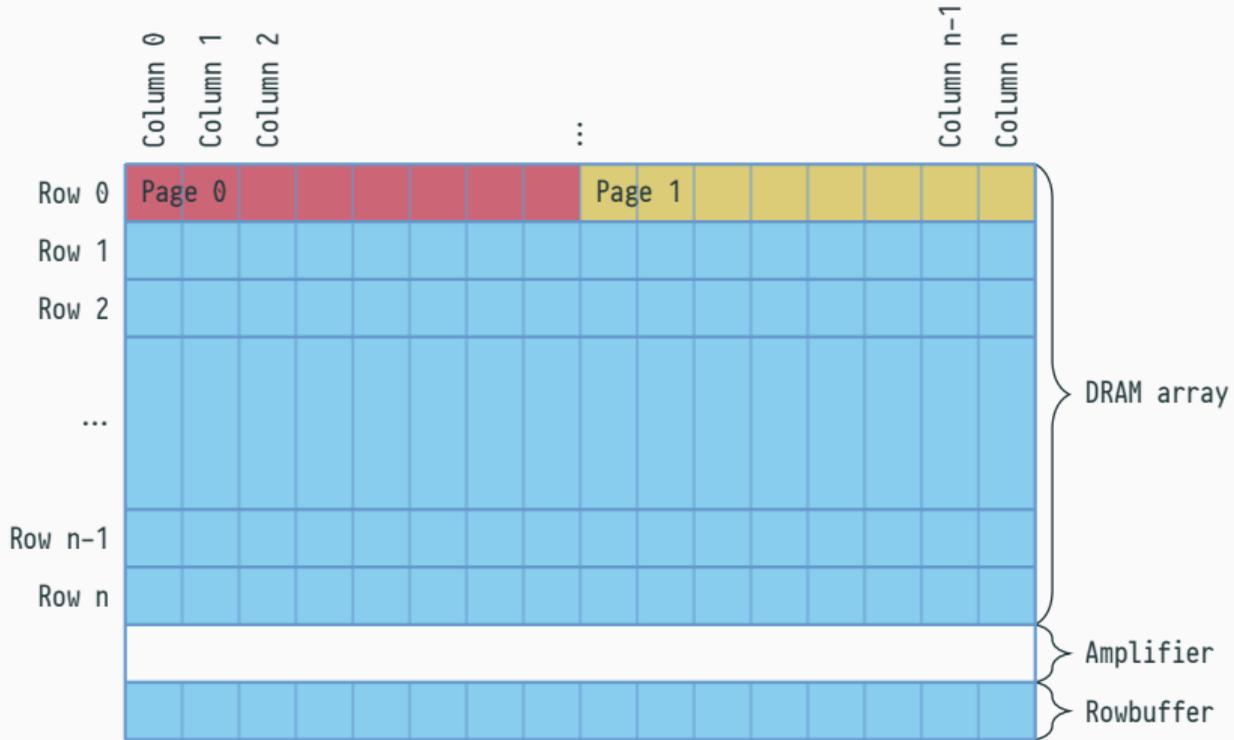
DRAM – Physical Architecture



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



Simple Example of Rowhammer

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
```


Simple Example of Rowhammer

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
```

Simple Example of Rowhammer

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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
```

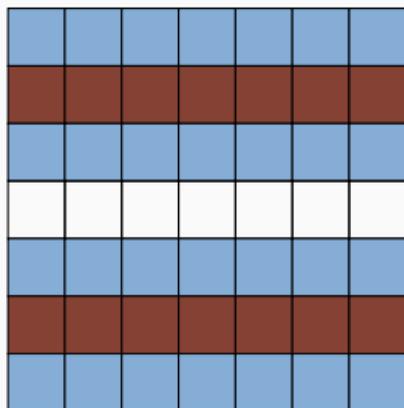
```
clflush (Row 0)
```

```
clflush (Row 2)
```

```
jmp hammertime
```

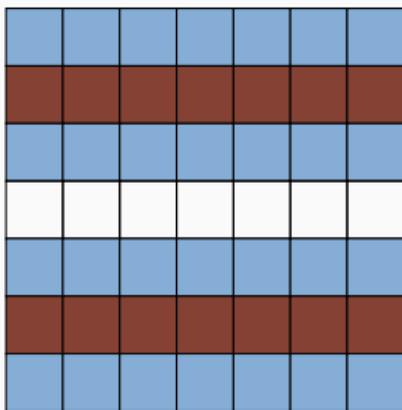

Various Hammering Patterns

Single-Sided

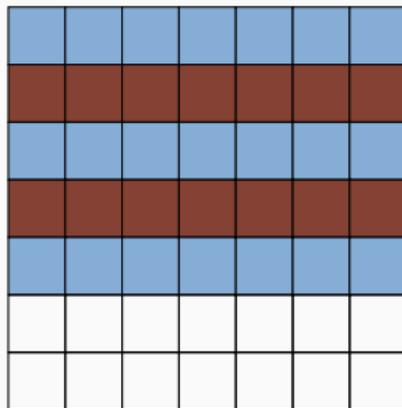


Various Hammering Patterns

Single-Sided

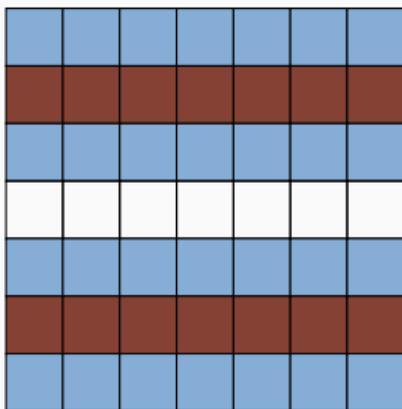


Double-Sided

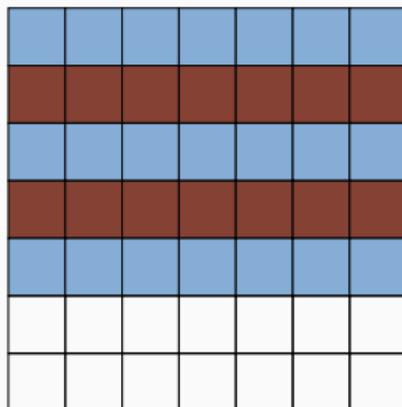


Various Hammering Patterns

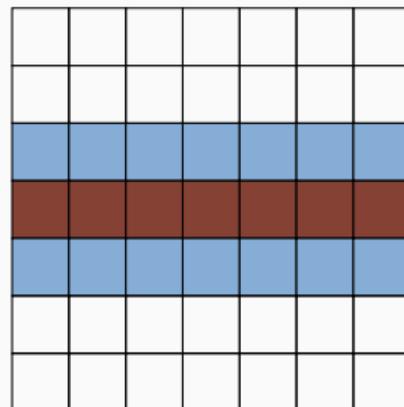
Single-Sided



Double-Sided

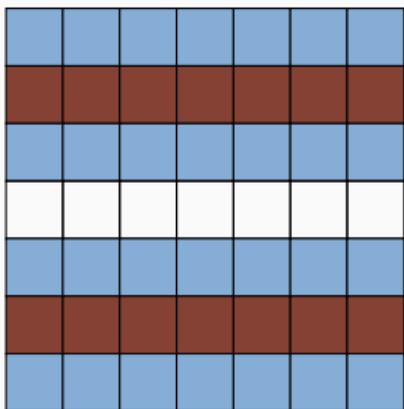


One-Location

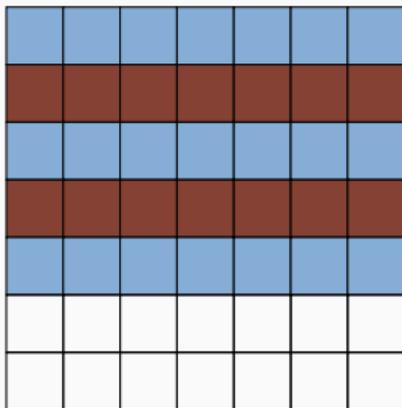


Various Hammering Patterns

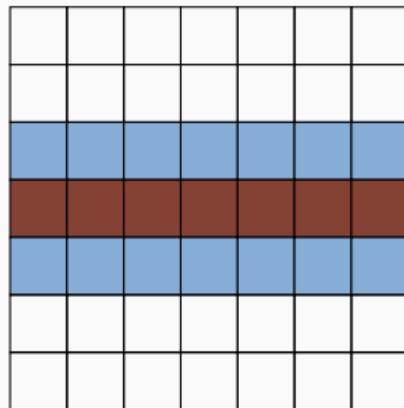
Single-Sided



Double-Sided



One-Location



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

FLIPPYRAM– Large-Scale Rowhammer Study

Overview



User Agreements
Privacy Policy
Risk Agreement

Overview



User Agreements System Information
Privacy Policy Retrieval
Risk Agreement

Overview



User Agreements
Privacy Policy
Risk Agreement

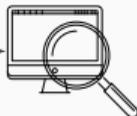
System Information
Retrieval

Reverse Engineering
of the Address-
ing Functions

Overview



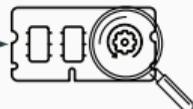
User Agreements
Privacy Policy
Risk Agreement



System Information
Retrieval

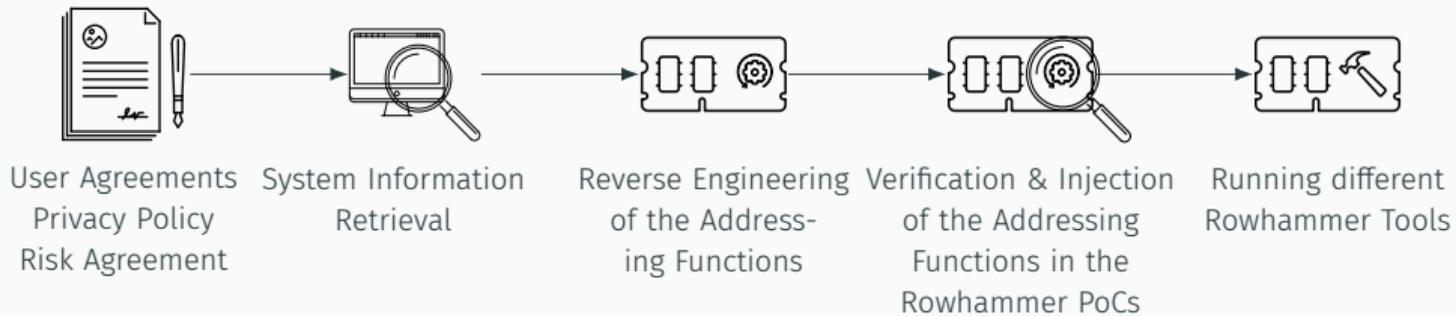


Reverse Engineering
of the Address-
ing Functions

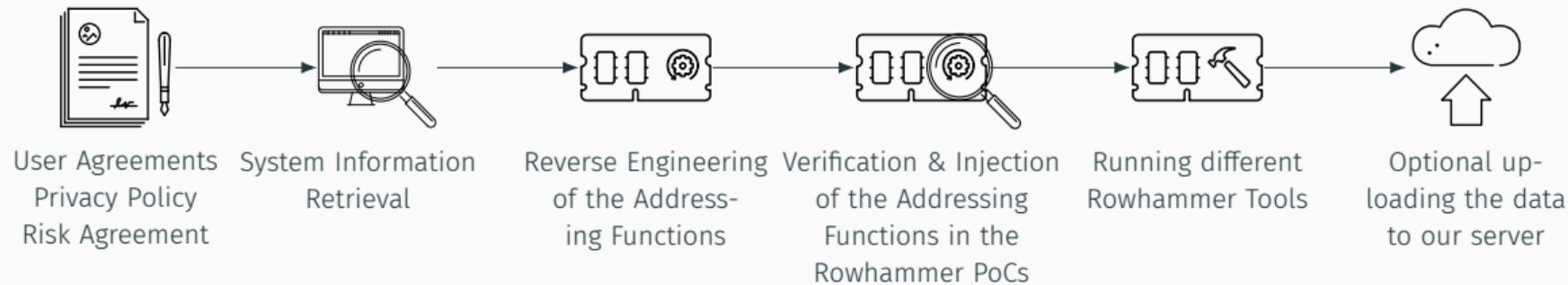


Verification & Injection
of the Addressing
Functions in the
Rowhammer PoCs

Overview



Overview



How could Users participate?



How could Users participate?



- Get a free bootable USB stick from us

How could Users participa



**YOU WANT TO HAND OUT
USB STICKS AT A HACKER CONFERENCE?**

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!

- 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 ≈ 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 summary
 - 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 ≈ 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 ...



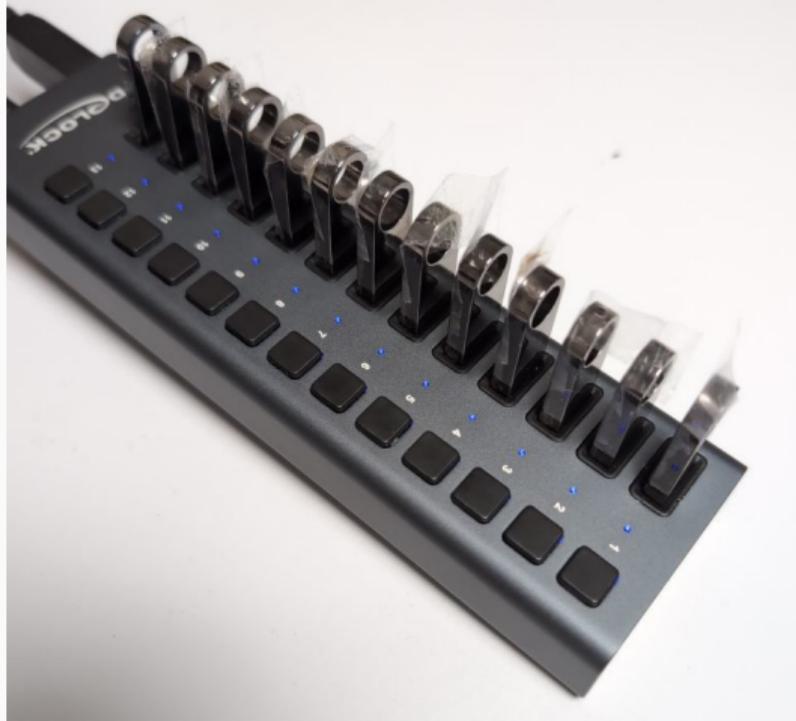
Flashing left Scratches ...



More complicated flashing Process required



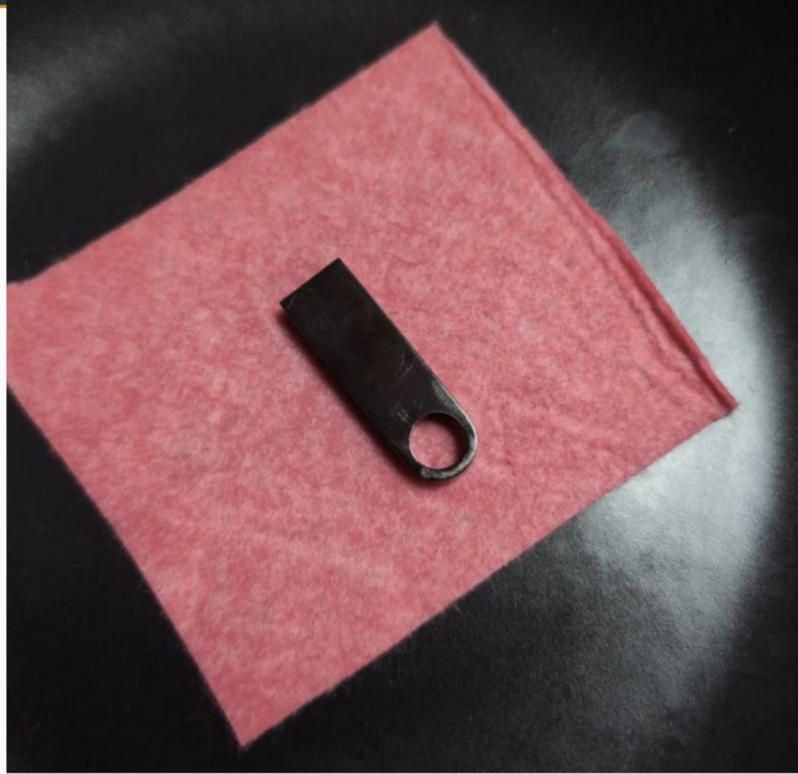
More complicated flashing Process required



More complicated flashing Process required

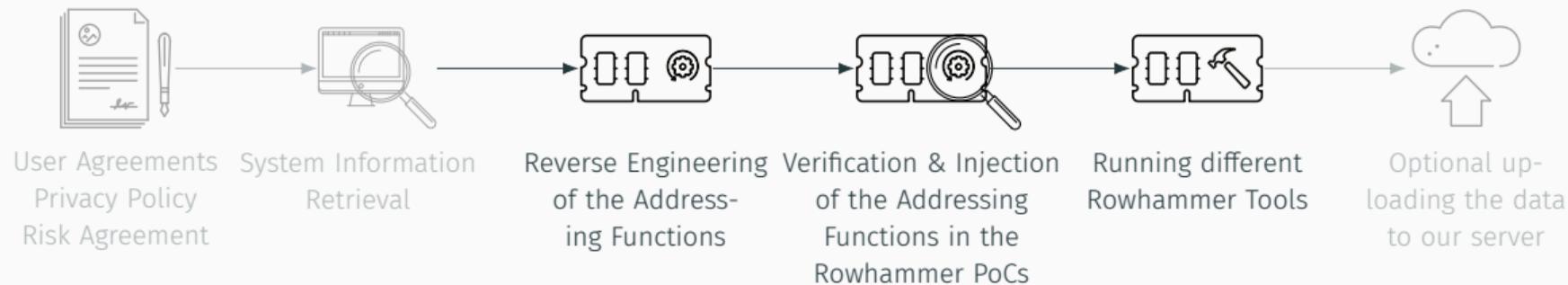


More complicated flashing Process required

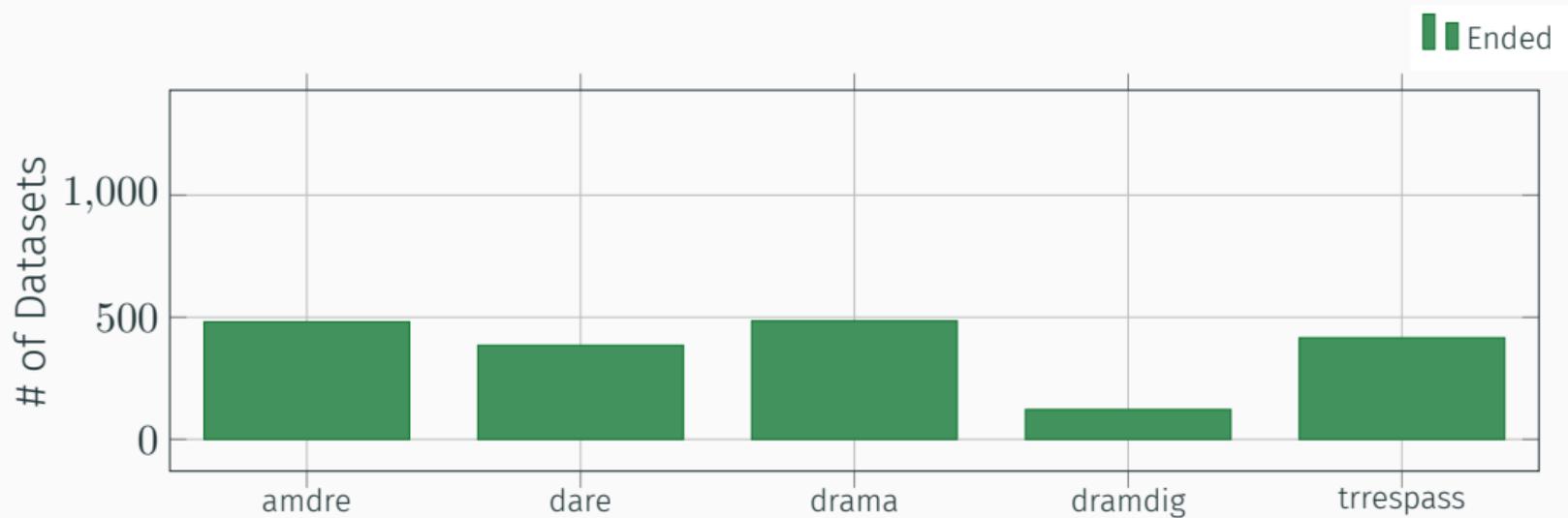


Results

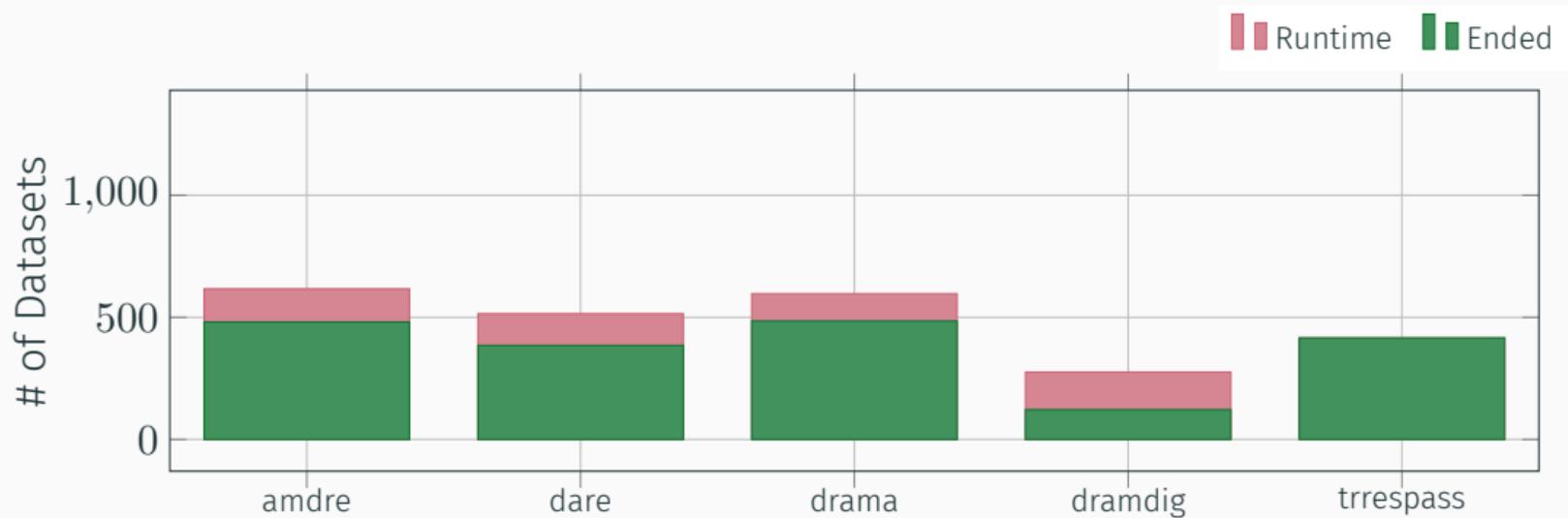
Overview



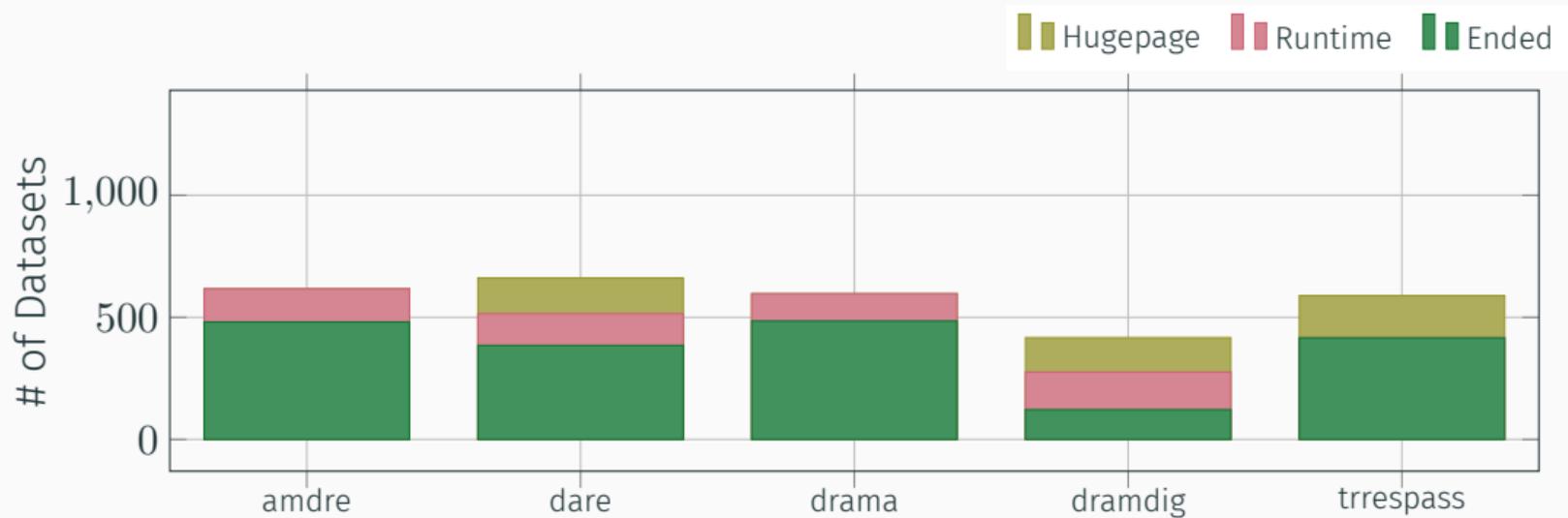
Reverse Engineering of the Addressing Functions



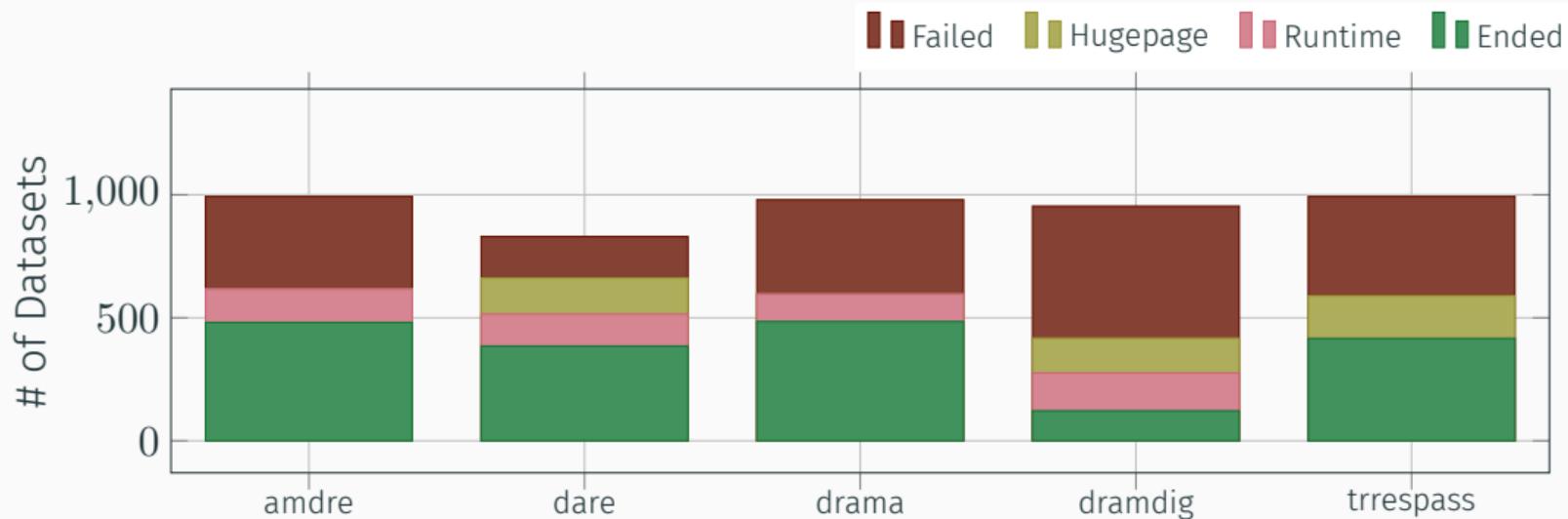
Reverse Engineering of the Addressing Functions



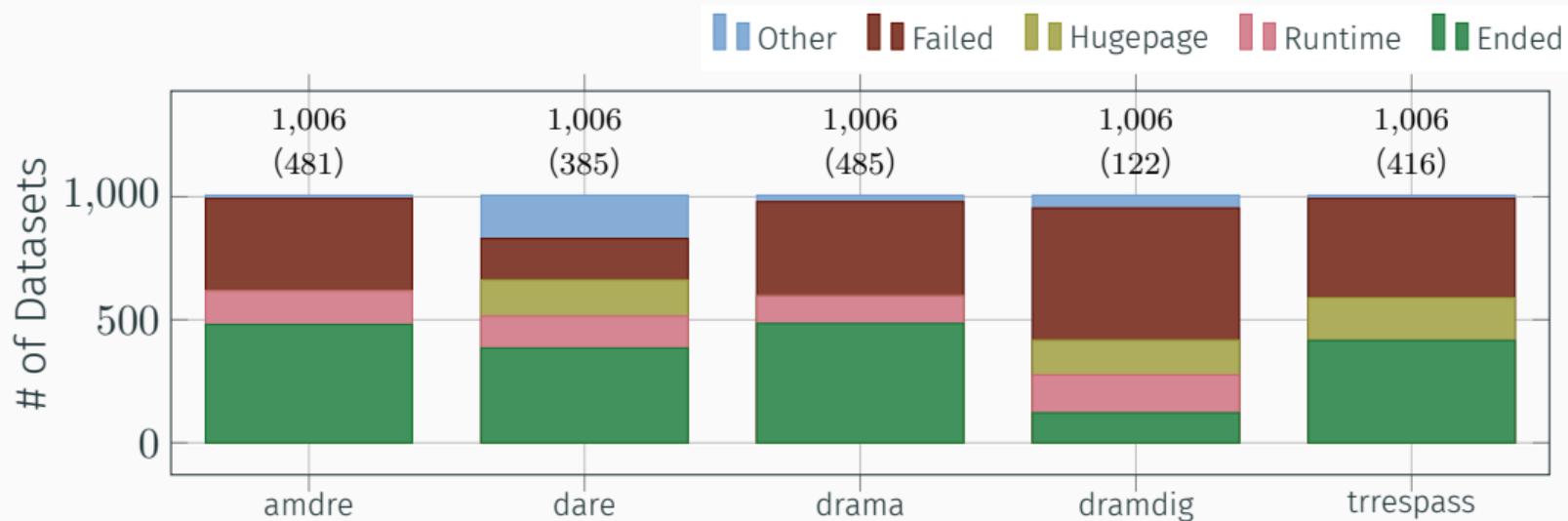
Reverse Engineering of the Addressing Functions



Reverse Engineering of the Addressing Functions

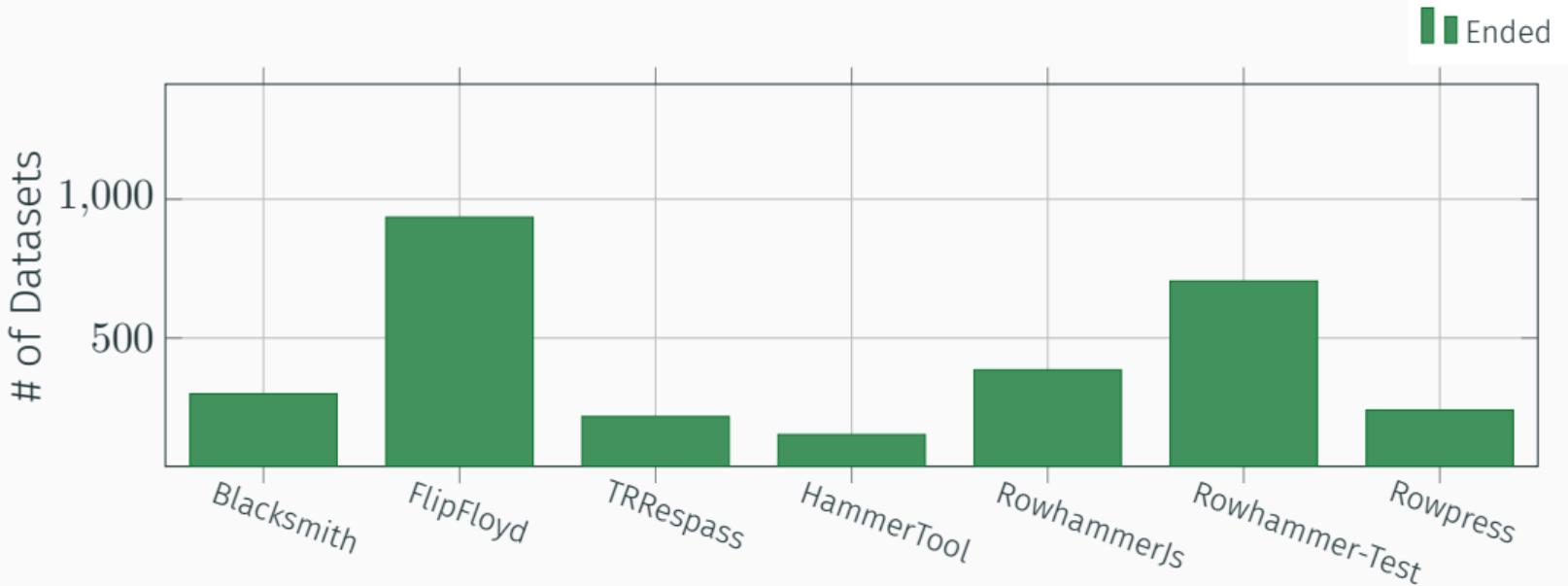


Reverse Engineering of the Addressing Functions

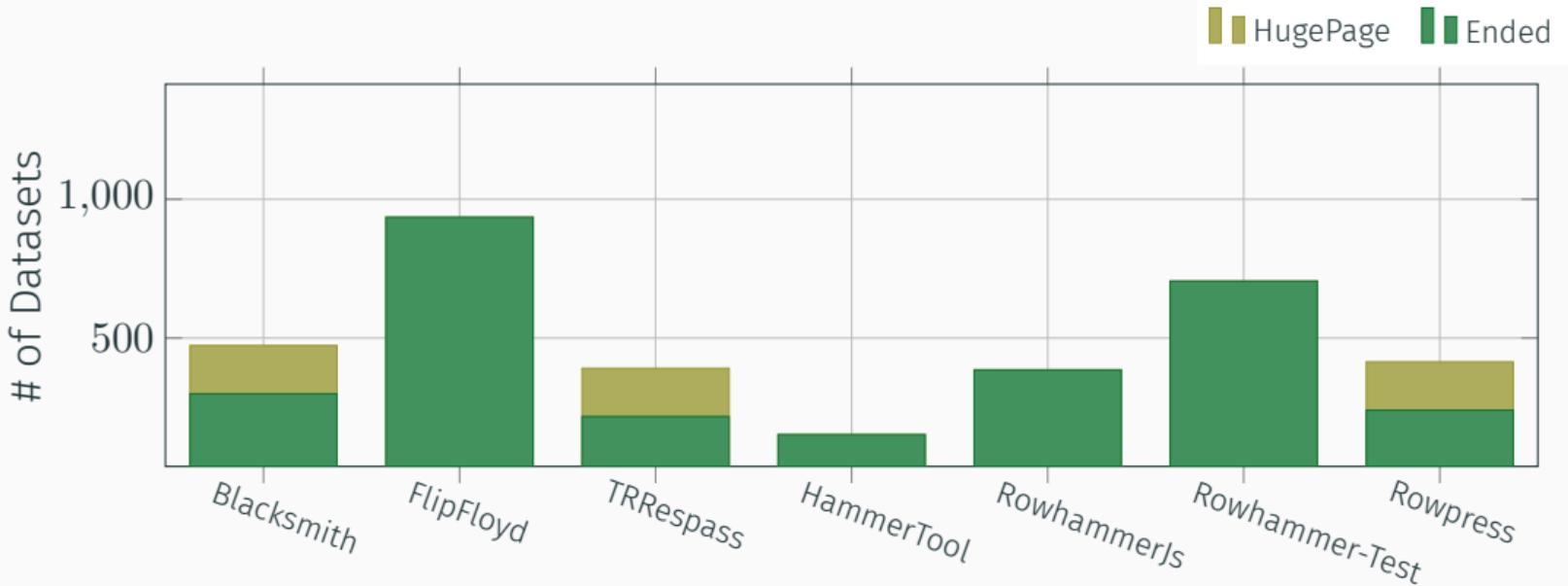


👁️ (#1): Majority of cases: reverse-engineering tools fail, crash, or exceed time limits!

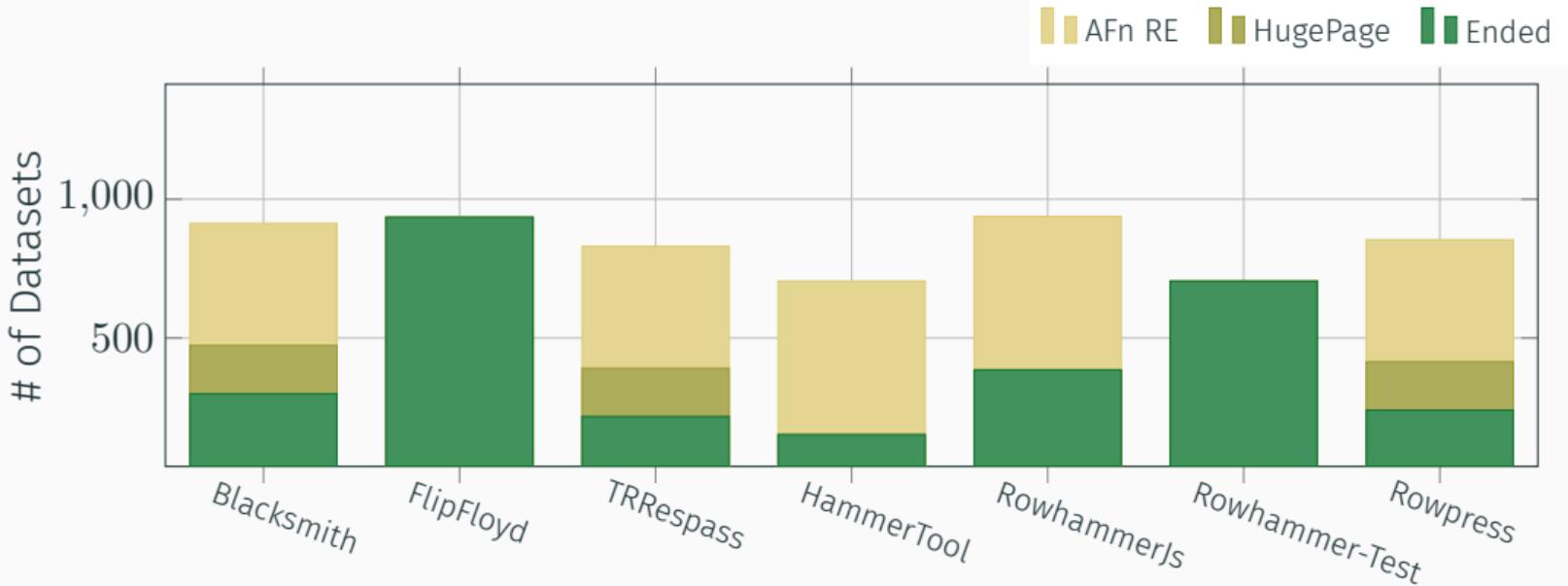
Running different Rowhammer Tools



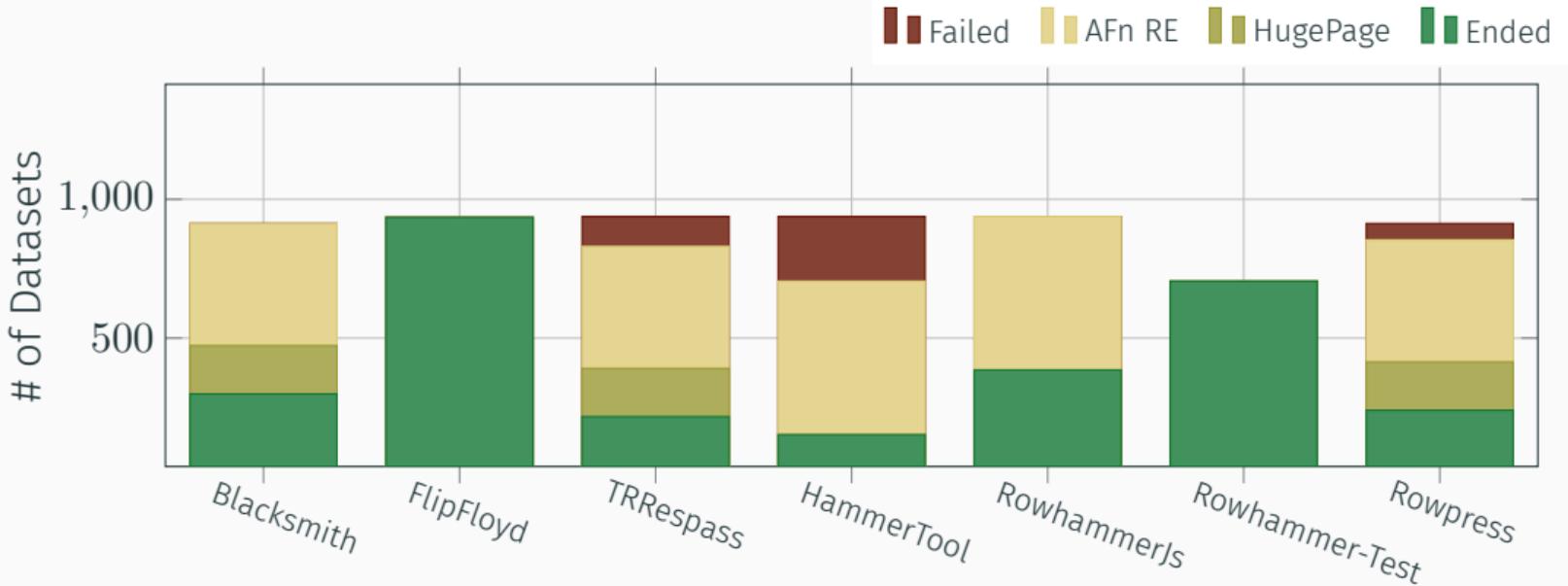
Running different Rowhammer Tools



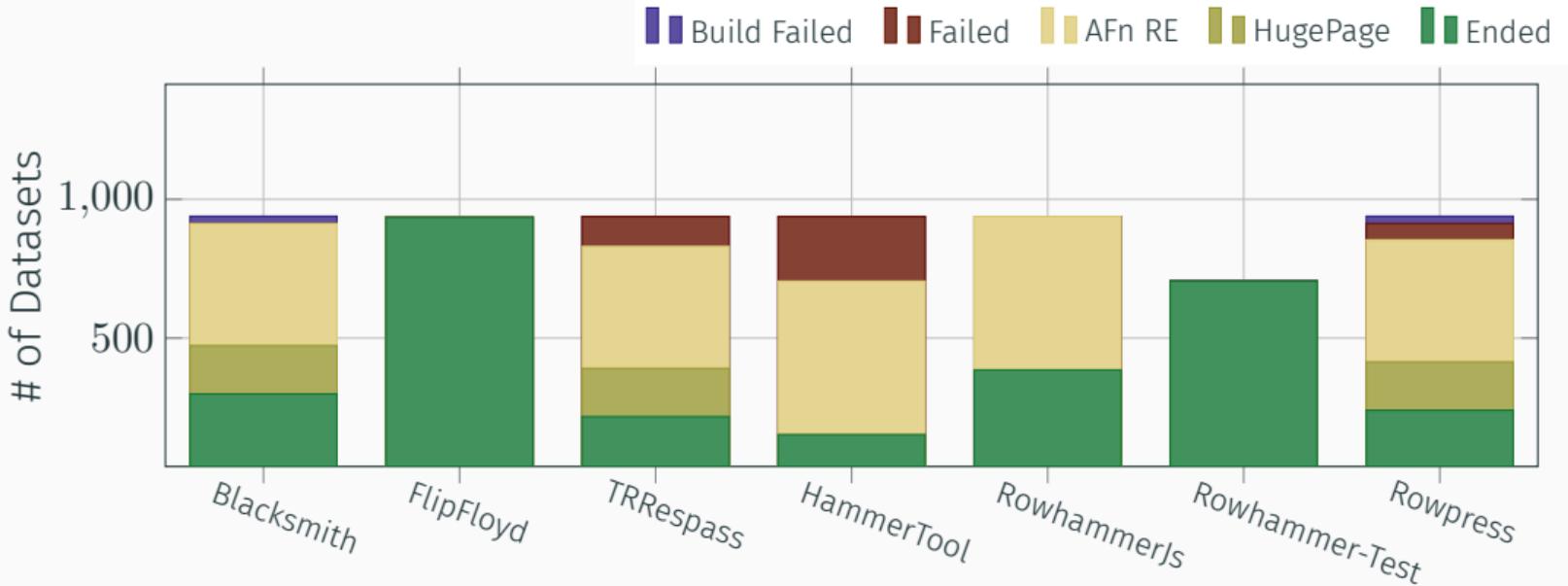
Running different Rowhammer Tools



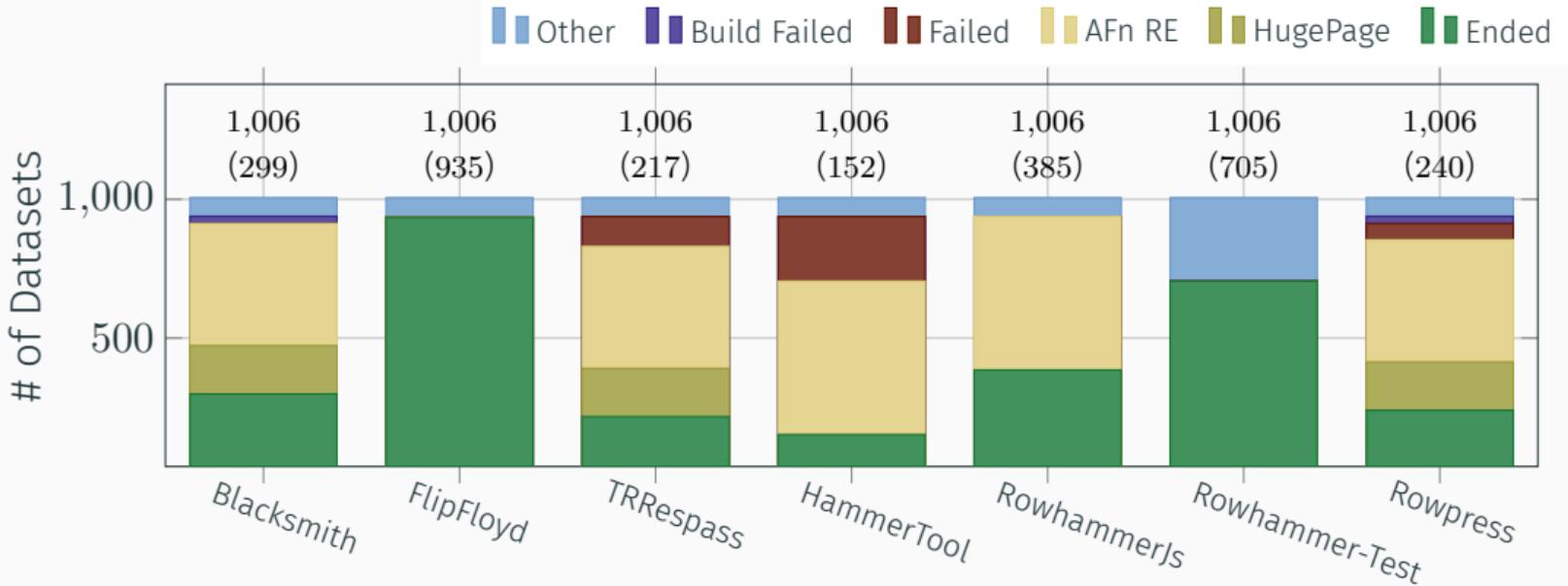
Running different Rowhammer Tools



Running different Rowhammer Tools

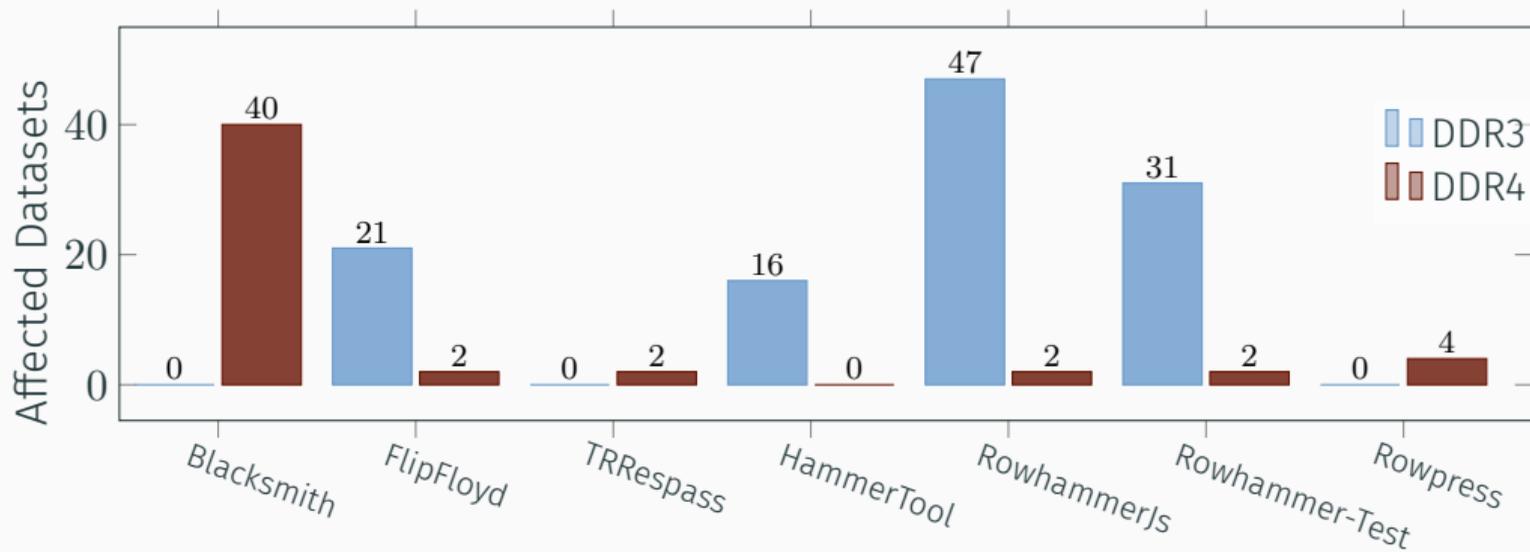


Running different Rowhammer Tools



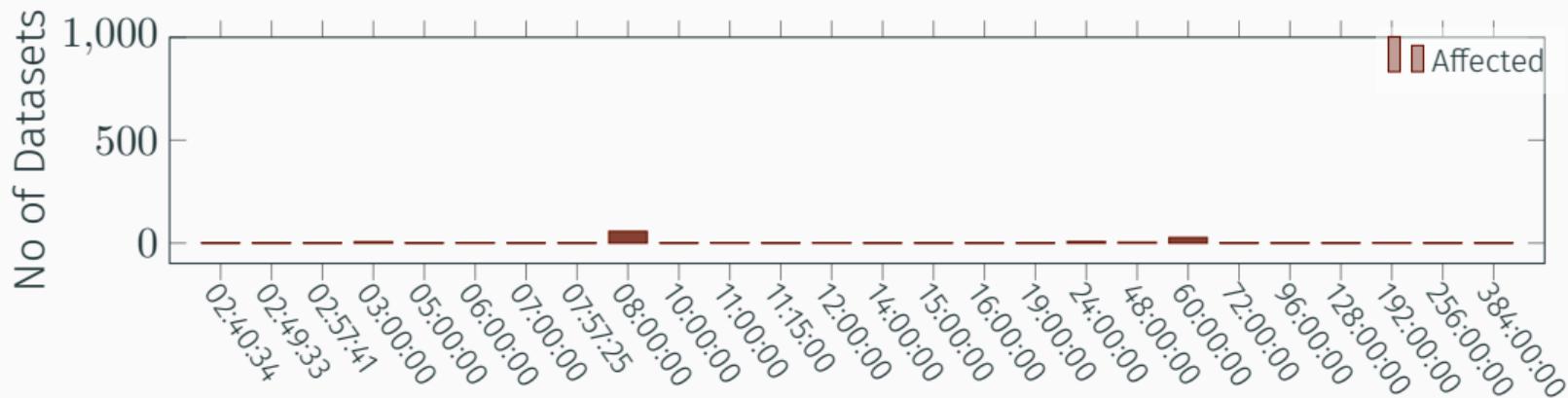
👁 (#2): Many Rowhammer tools failed because of missing DRAM functions or 1 GiB hugepages.

Affected by Tool

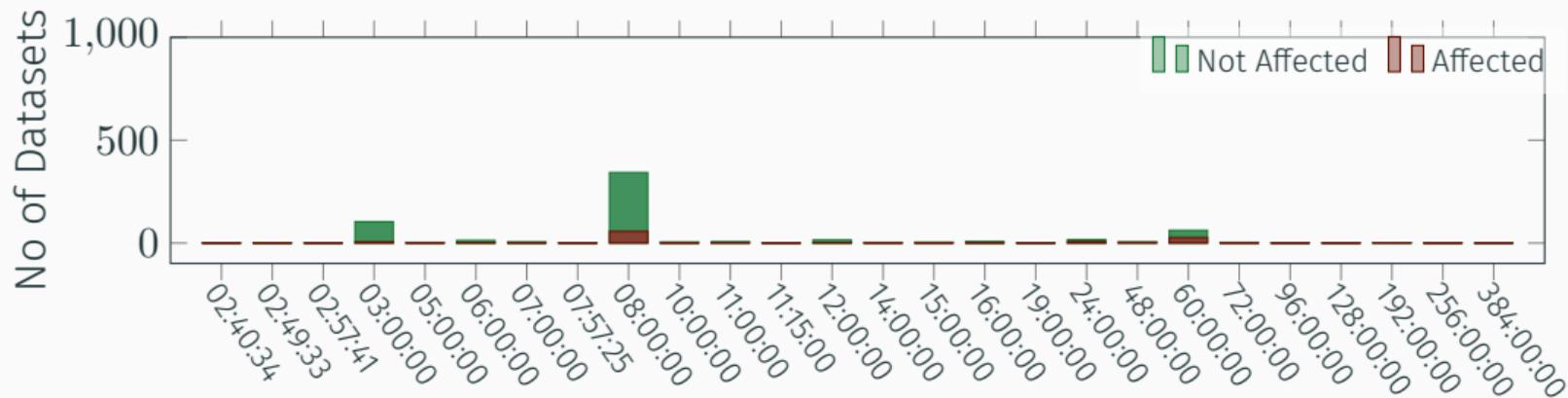


- 👁️ (#3): 126 (12.5 %) out of 1006 datasets are vulnerable to fully-automated Rowhammer attacks!
- 👁️ (#4): DDR3 → simple fast patterns (RowhammerJS);
DDR4 with TRR → pattern fuzzing for non-uniform patterns (Blacksmith)
- 👁️ (#5): The minimum time to the first bit flip was between 0 min and 115 min on average, which is a practical time frame for real-world attacks.

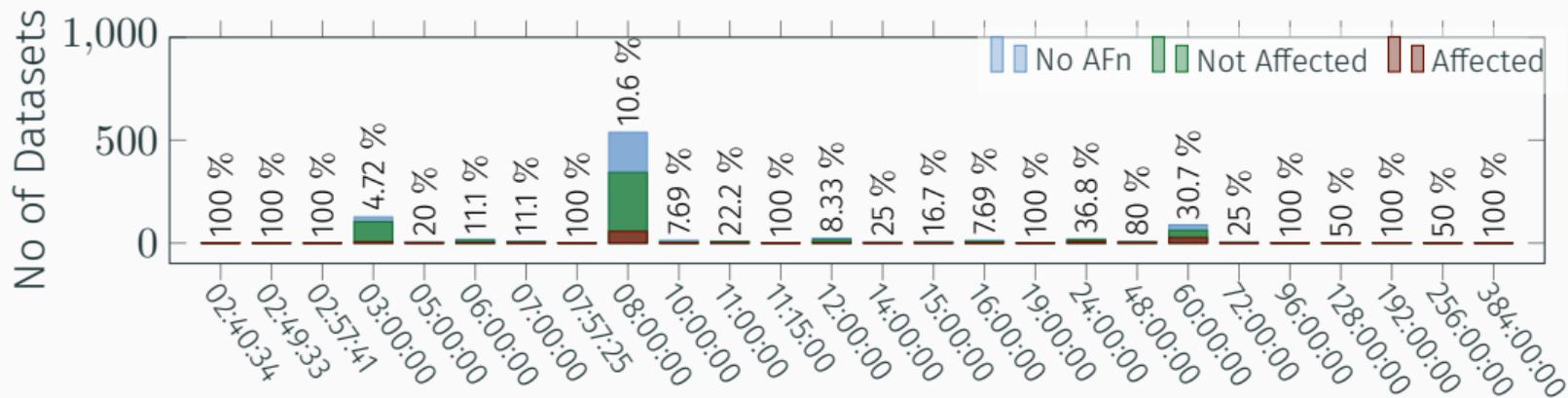
Affected systems by Runtime



Affected systems by Runtime

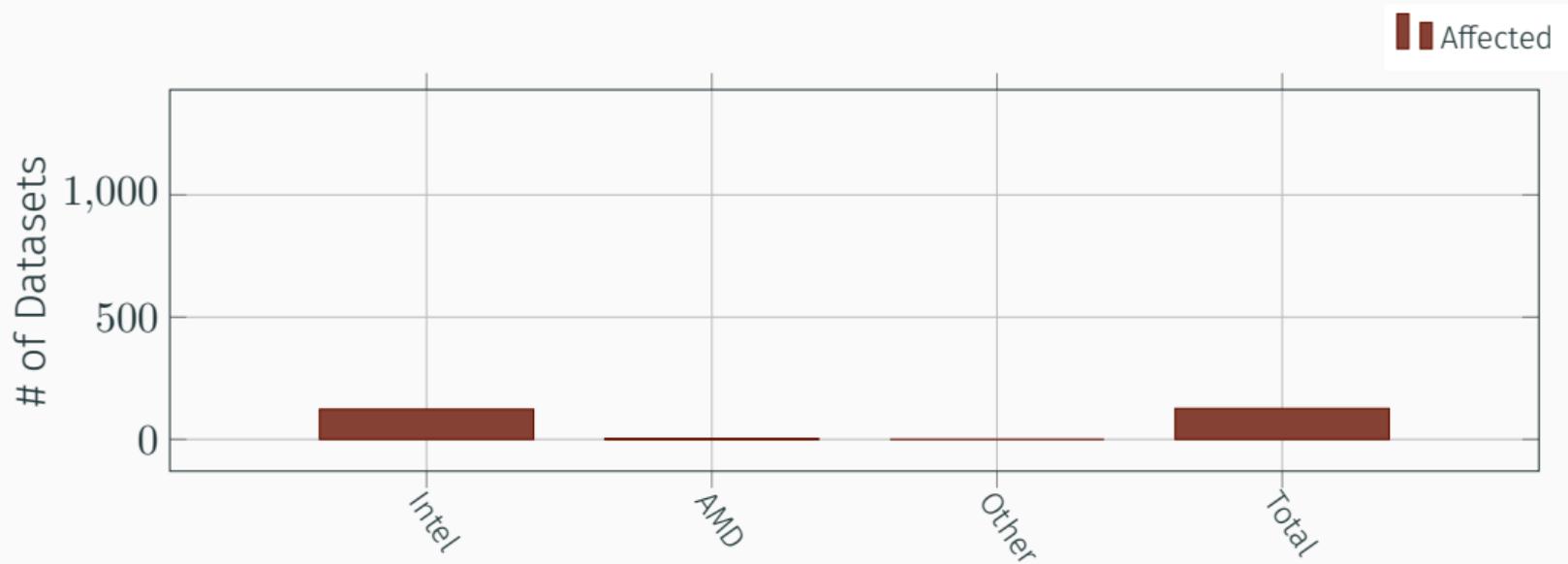


Affected systems by Runtime

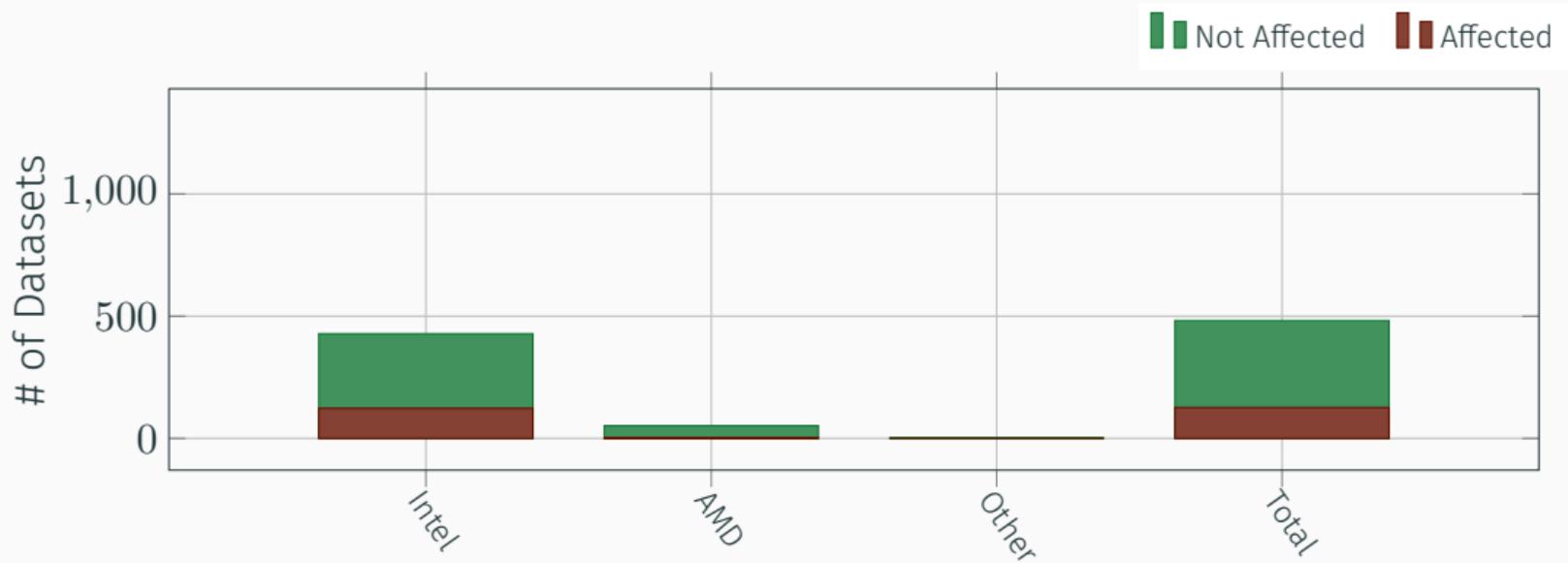


👁️ (#6): On barely susceptible systems it can take very long to find flips (up to 617 min in our datasets), so longer testing times lead to more accurate detection.

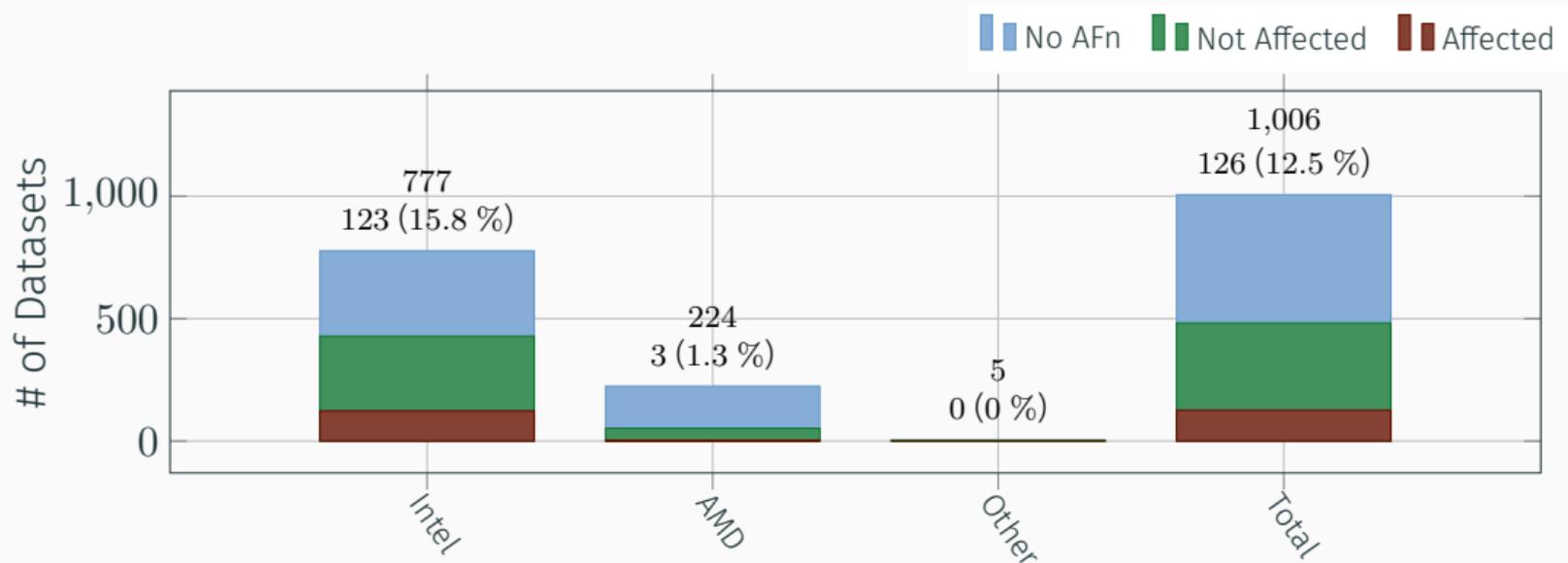
Affected systems by CPU Vendor



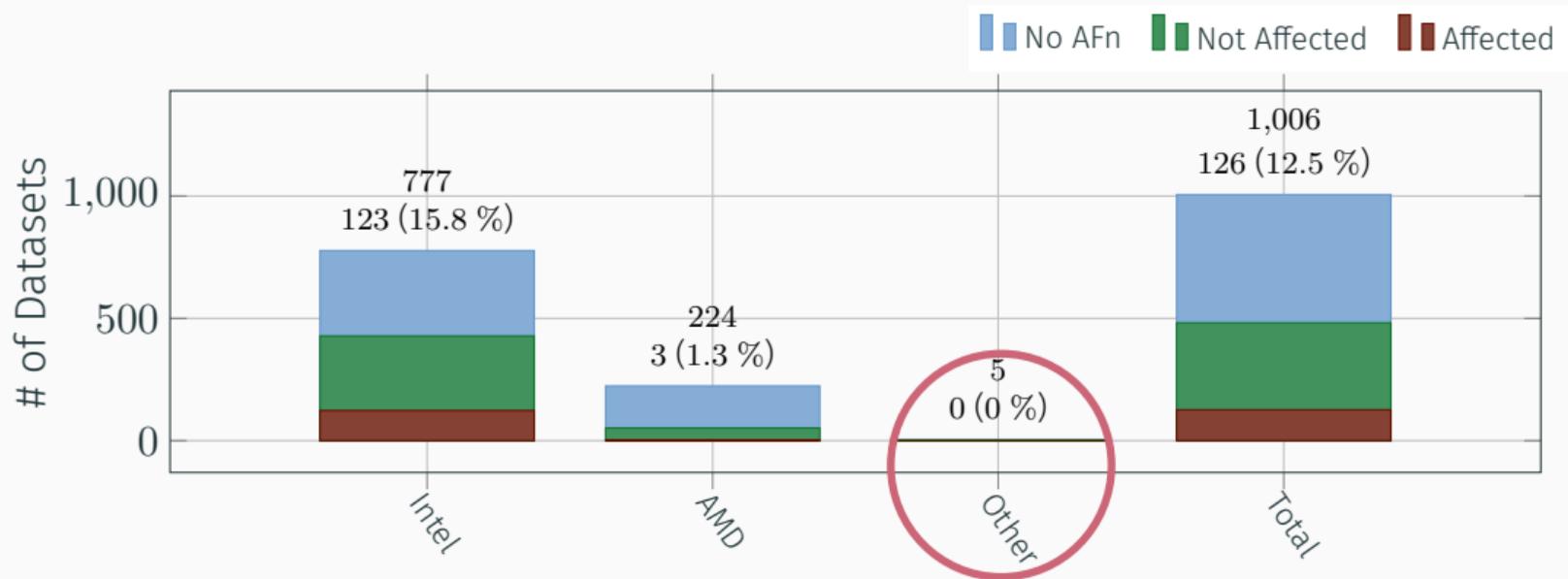
Affected systems by CPU Vendor



Affected systems by CPU Vendor



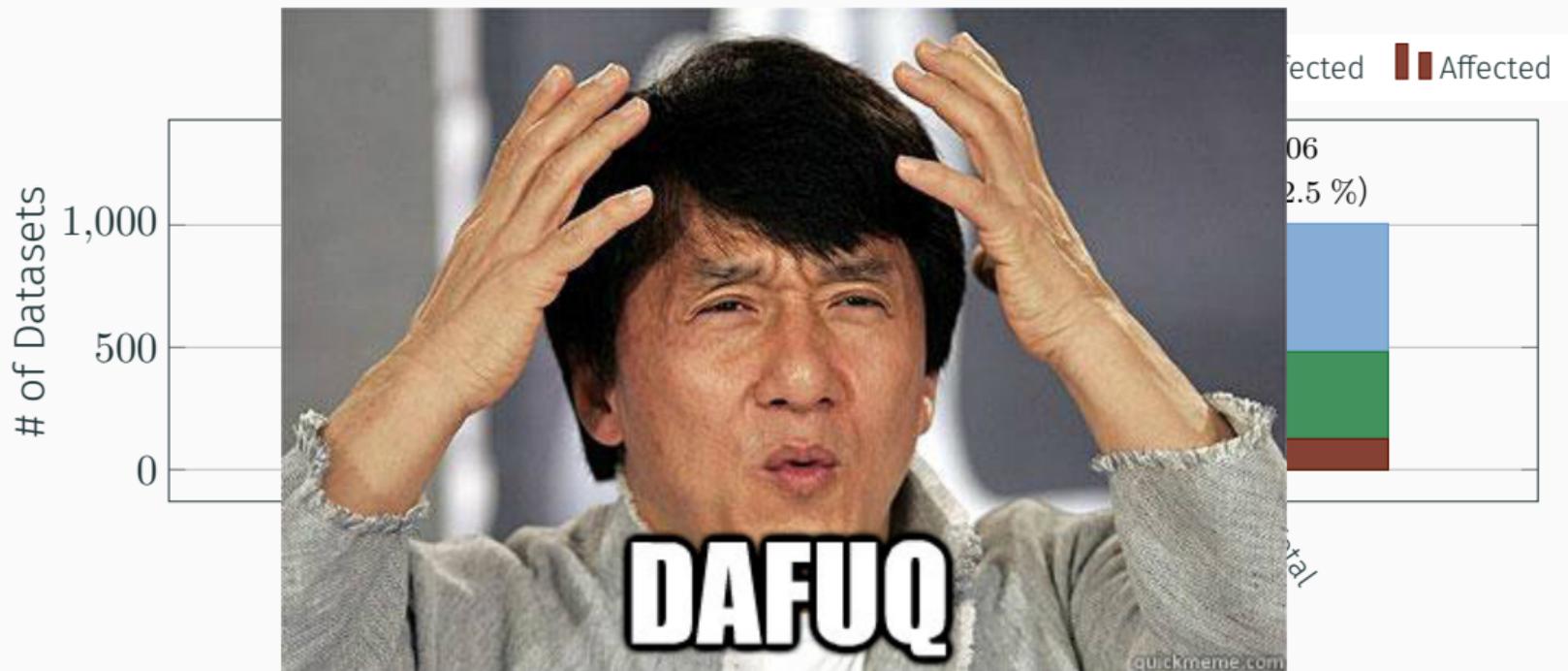
Affected systems by CPU Vendor



Affected systems by CPU Vendor

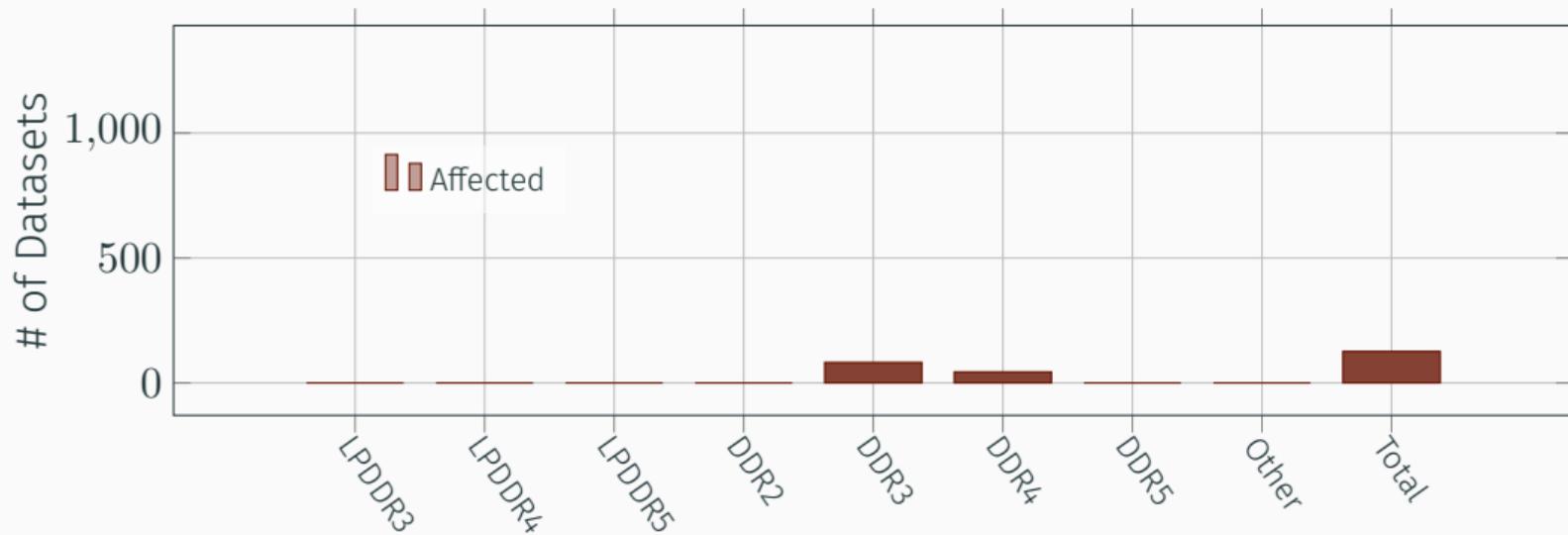


Affected systems by CPU Vendor

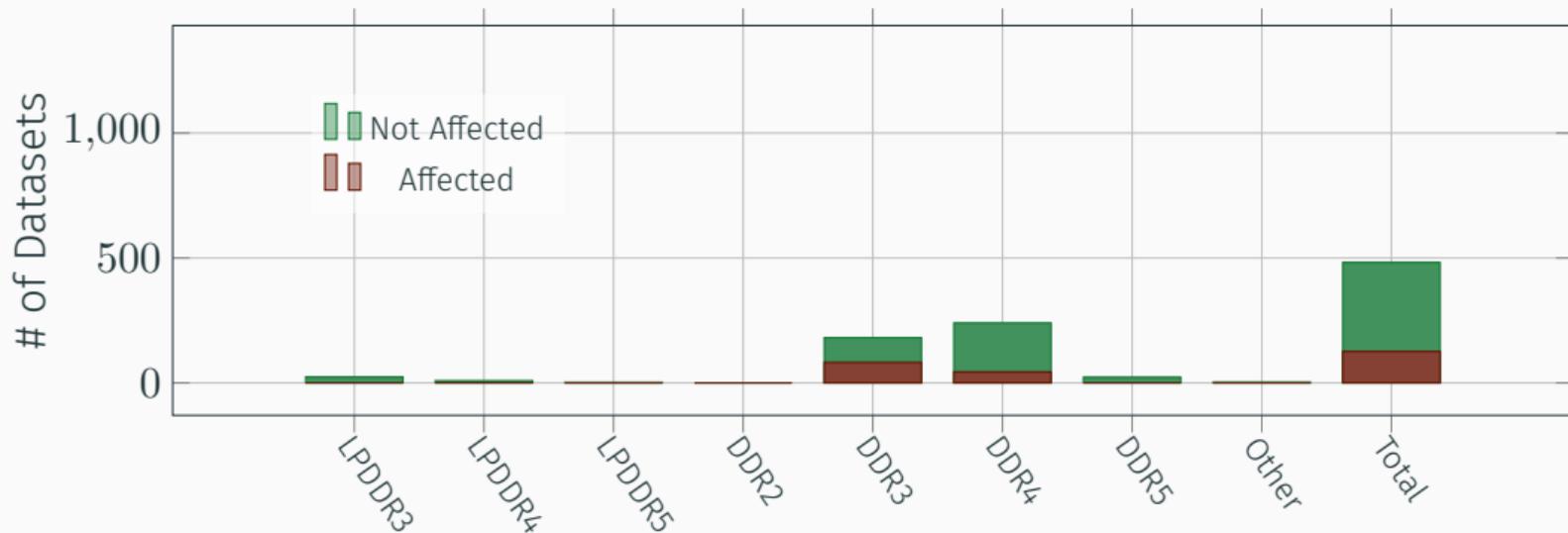


👁️ (#7): Mainly tools for Intel, fewer AMD tools, especially when we started the study → we expect AMD to be equally affected.

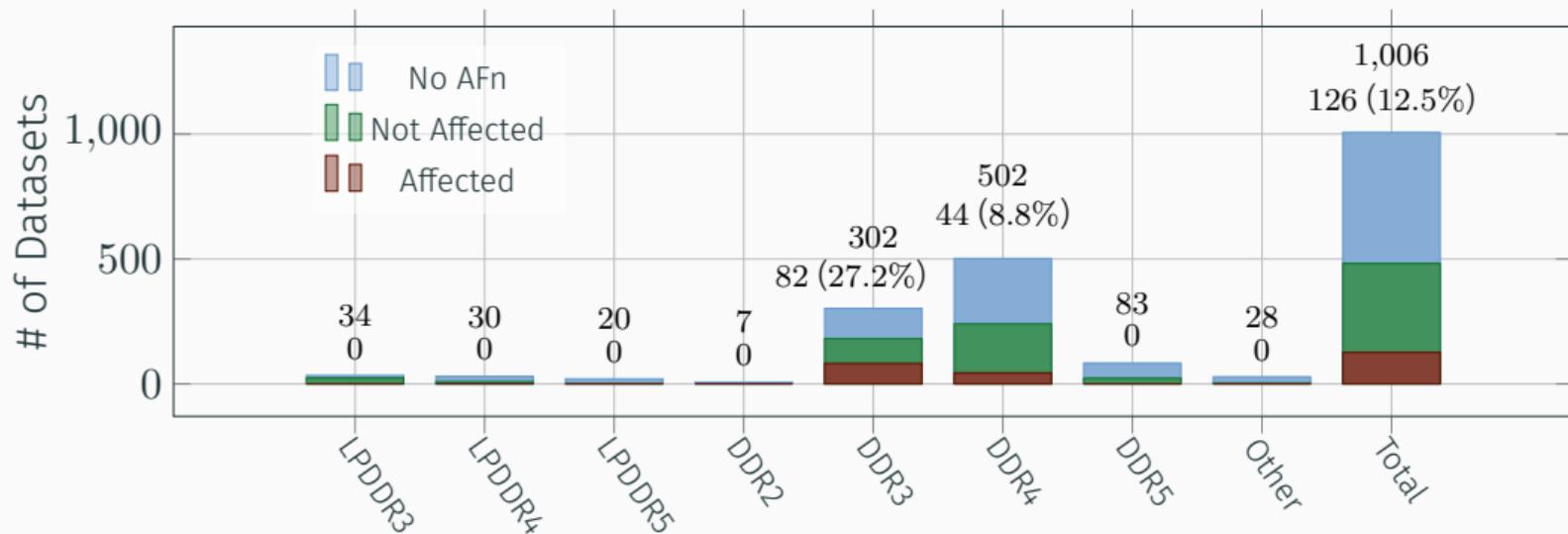
Affected DIMMs by DRAM Generation



Affected DIMMs by DRAM Generation

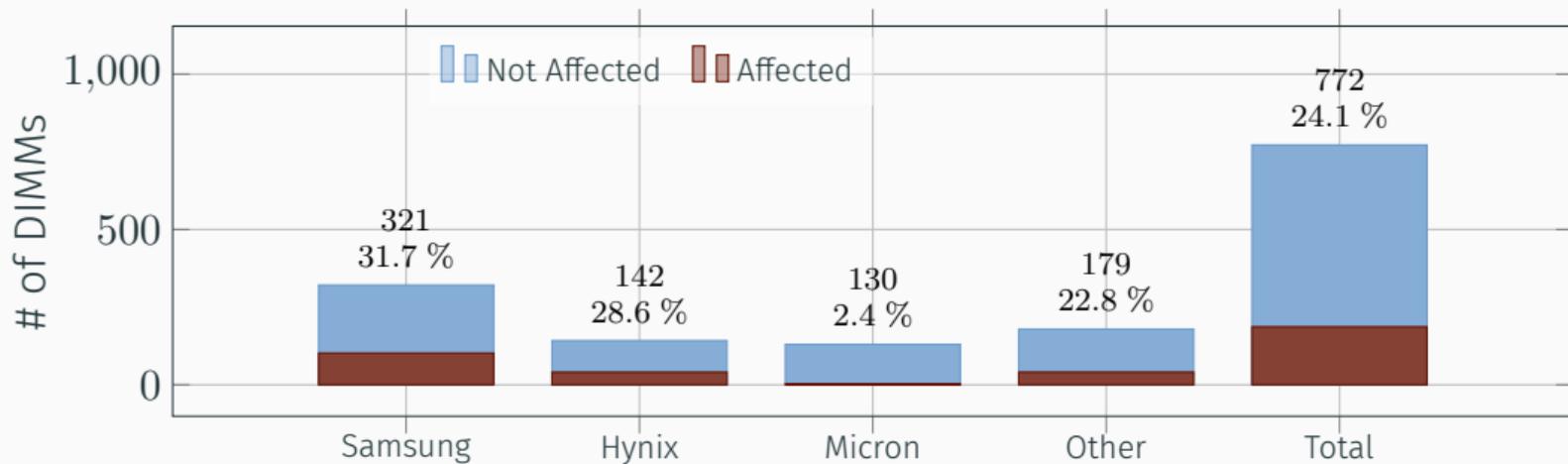


Affected DIMMs by DRAM Generation



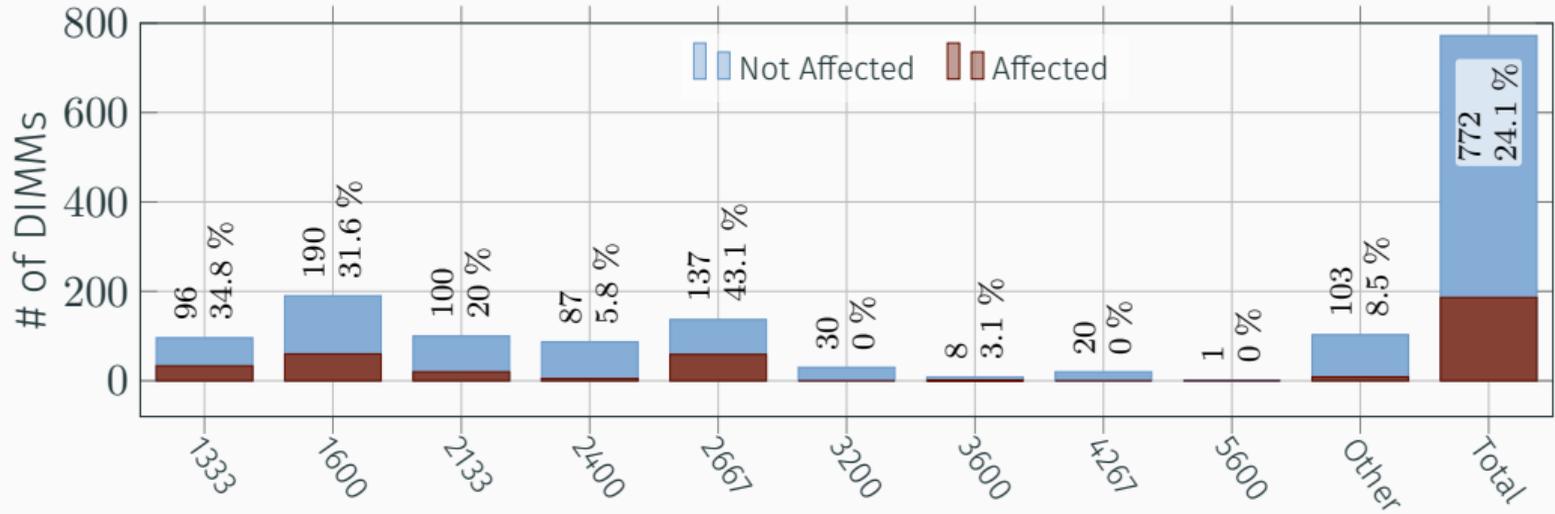
👁️ (#8): Most affected systems are DDR3, followed by DDR4. No DDR5 systems were affected (lack of tools at the time we did our study).

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 → 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 Sayadi², Jonas Juffinger¹,
Carina Fiedler¹, Daniel Gruss¹, and Florian Adamsky²

February 24, 2026

¹ Graz University of Technology

² Hof University of Applied Sciences

