

Ten Years of Rowhammer

A Retrospect (and Path to the Future)

Martin Heckel^{1,2} (@lunkw1ll)

Daniel Gruss¹ (@lavados)

Florian Adamsky² (@c1t)

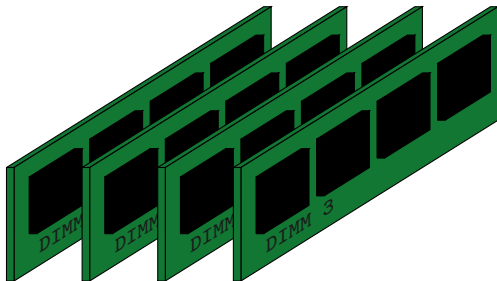
¹ Graz University of Technology

² Hof University of Applied Sciences

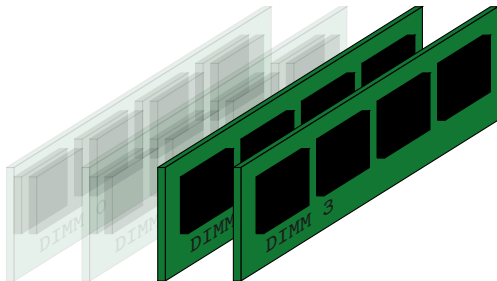


Origins and Root Cause

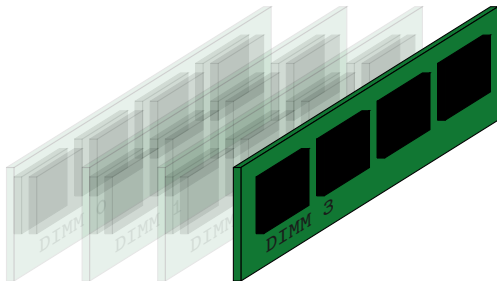
System DRAM

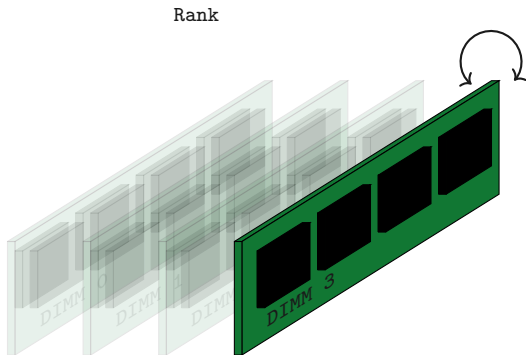


Channel

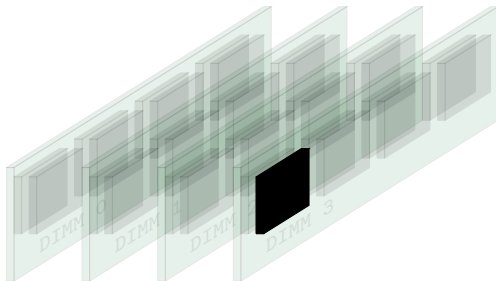


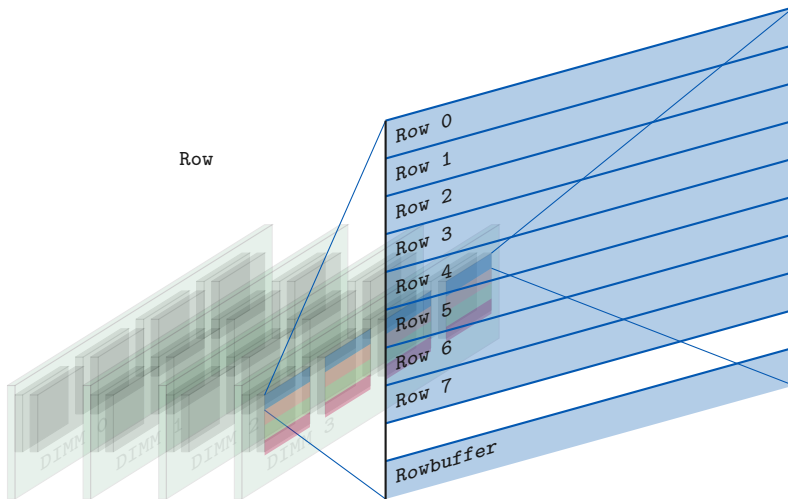
DIMM

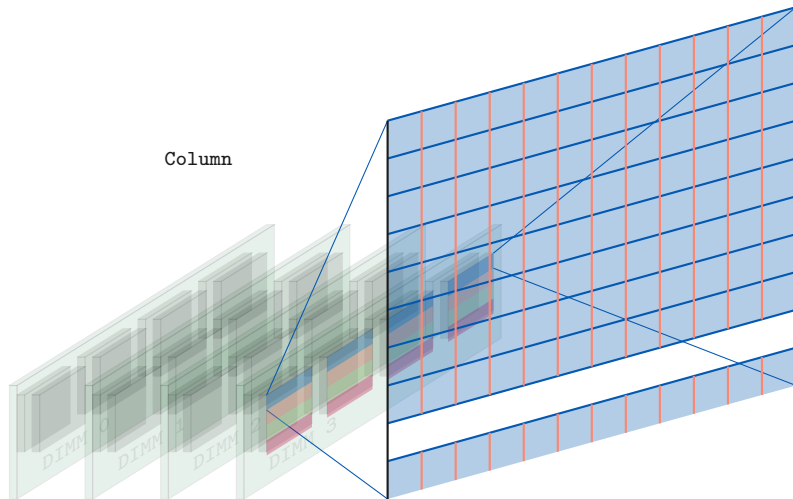


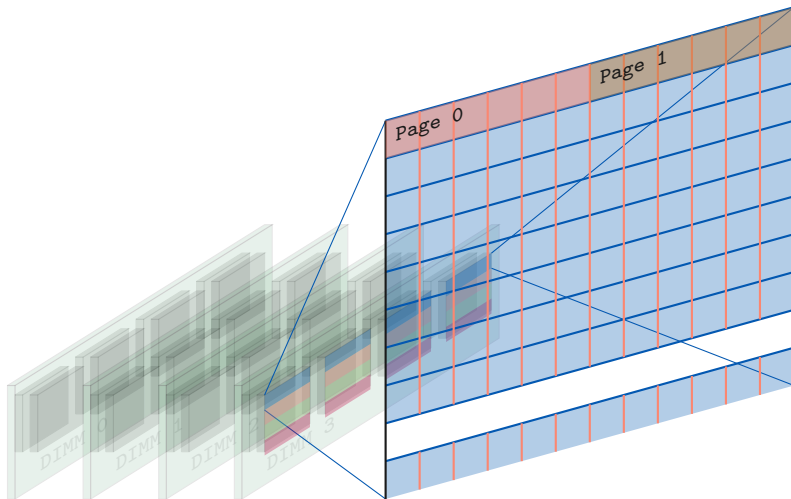


Chip

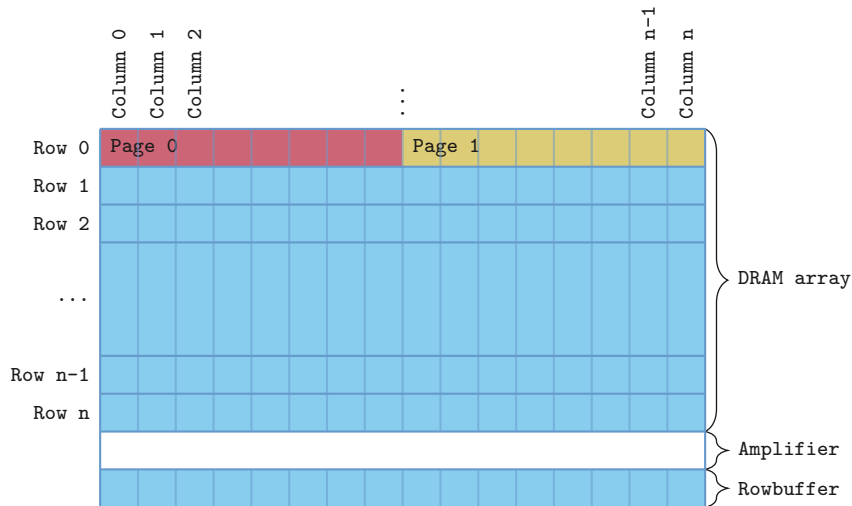


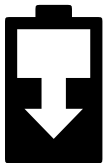


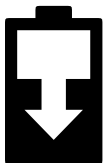


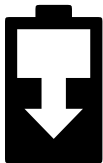


Structure within a DRAM bank

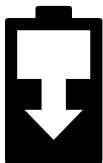




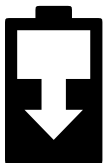




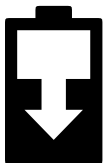
1. Capacitor loses its voltage over time



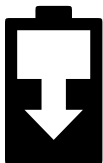
1. Capacitor loses its voltage over time
 - Cells must be refreshed regularly (refresh rate)



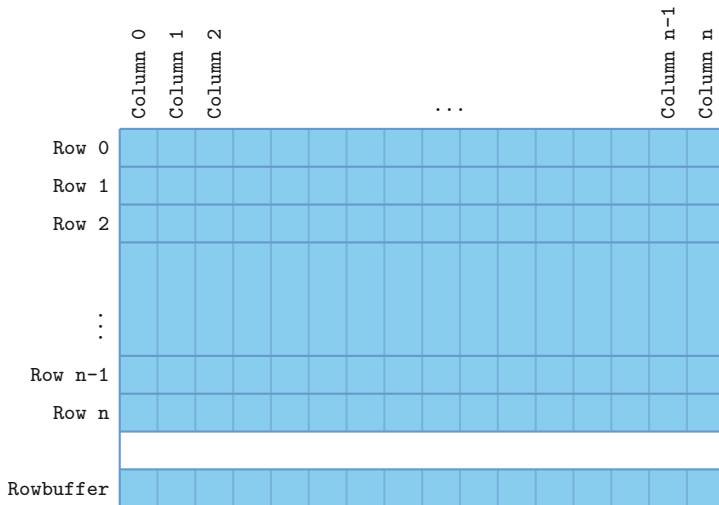
1. Capacitor loses its voltage over time
 - Cells must be refreshed regularly (refresh rate)
 - Cells are normally refreshed every 64 ms



1. Capacitor loses its voltage over time
 - Cells must be refreshed regularly (refresh rate)
 - Cells are normally refreshed every 64 ms
2. When reading a row, we destroy the data in this row



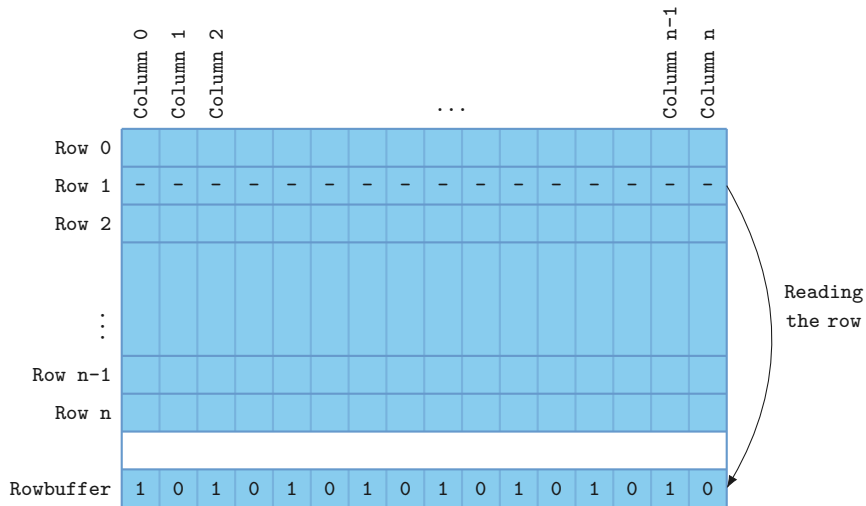
1. Capacitor loses its voltage over time
 - Cells must be refreshed regularly (refresh rate)
 - Cells are normally refreshed every 64 ms
2. When reading a row, we destroy the data in this row
 - Intermediate memory in the row buffer

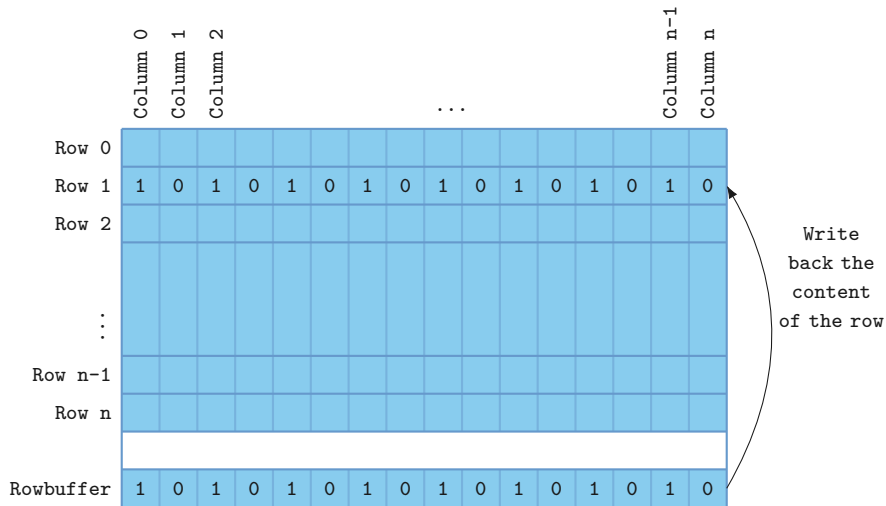


Row Buffer

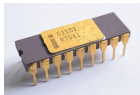
	Column 0	Column 1	Column 2	...										Column n-1	Column n
Row 0															
Row 1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Row 2															
⋮															
Row n-1															
Row n															
Rowbuffer															

Row Buffer



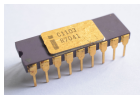






Intel 1103 (DRAM IC)
were pattern-sensitive

1971

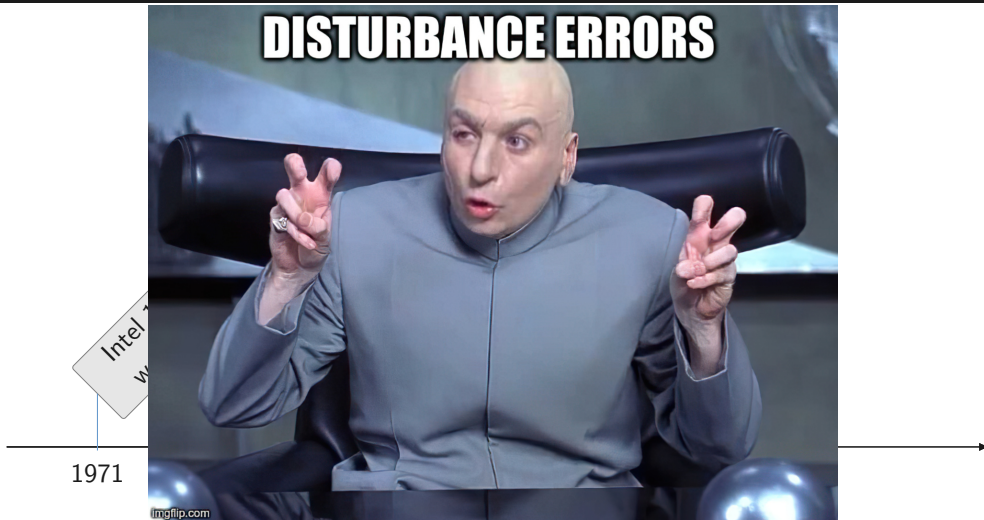


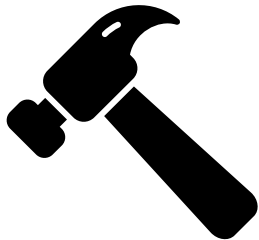
Intel 1103 (DRAM IC)
were pattern-sensitive

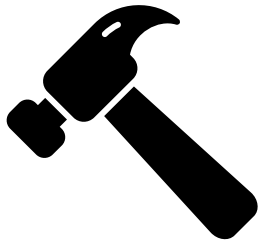
Several Patents about the
Row Hammer Event

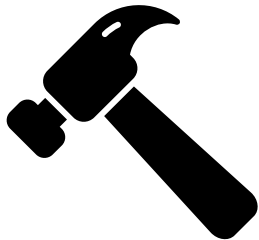
1971

2012

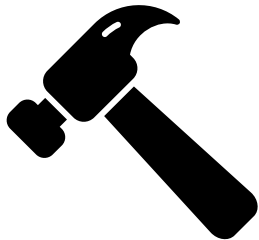




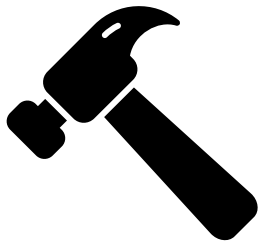




- Memory rows are disturbed by frequent accesses



- Memory rows are disturbed by frequent accesses
- Results in bit flips in adjacent rows



- Memory rows are disturbed by frequent accesses
- Results in bit flips in adjacent rows
- Exploited through clever hammering techniques

Simple Example of Rowhammer

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

hammertime:

```
mov (Row 0), %eax
```

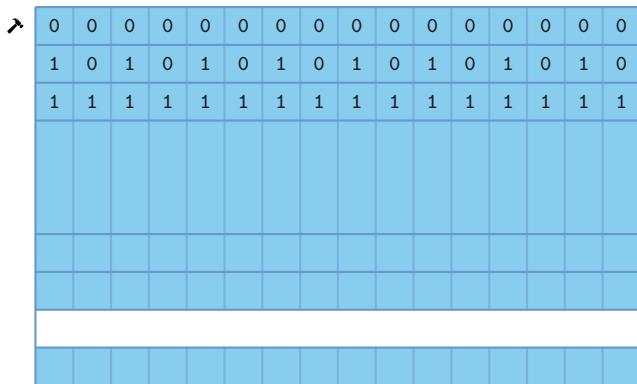
```
mov (Row 2), %ebx
```

```
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	0
1	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
```

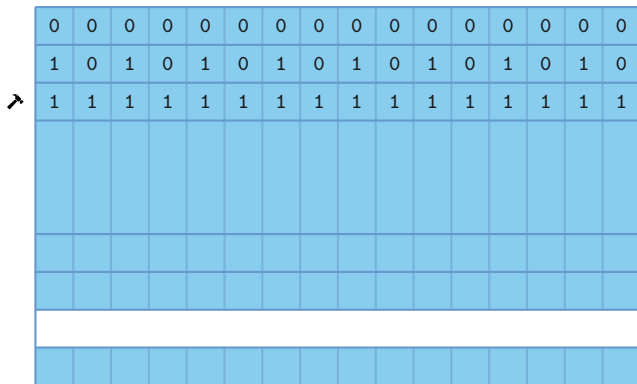
```
mov (Row 2), %ebx
```

```
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	0
1	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	0
1	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
```

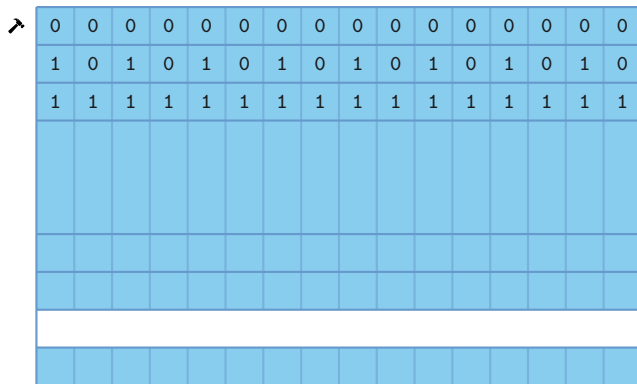
```
mov (Row 2), %ebx
```

```
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	0
1	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
```

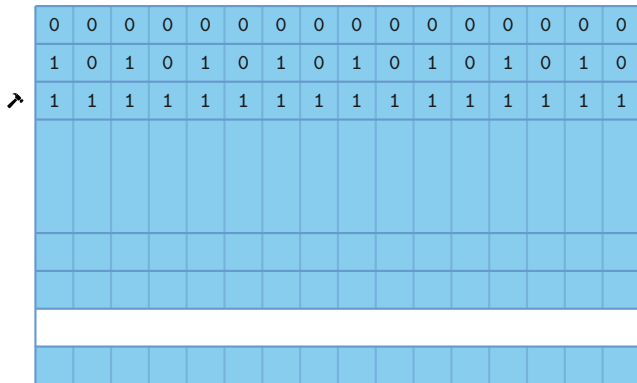
```
mov (Row 2), %ebx
```

```
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	0
1	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

We can touch this!



0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
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	

hammertime:

```
mov (Row 0), %eax
```

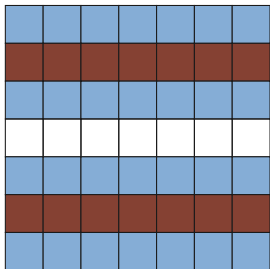
```
mov (Row 2), %ebx
```

```
clflush (Row 0)
```

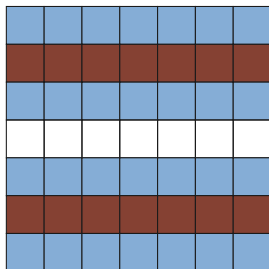
```
clflush (Row 2)
```

```
jmp hammertime
```

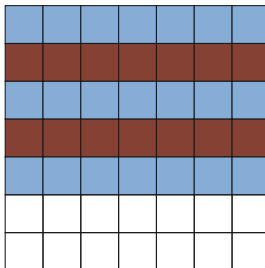
Single-Sided



Single-Sided



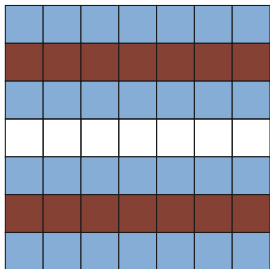
Double-Sided



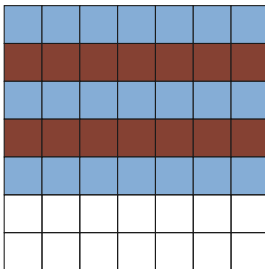
Various Hammering Patterns



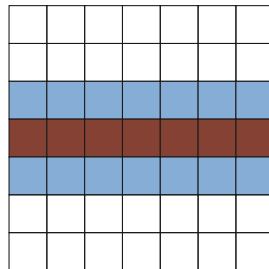
Single-Sided



Double-Sided



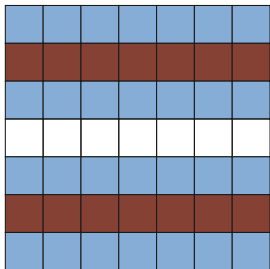
One-Location



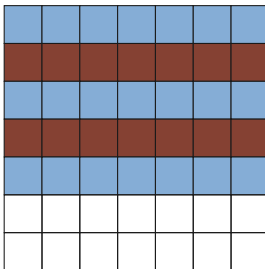
Various Hammering Patterns



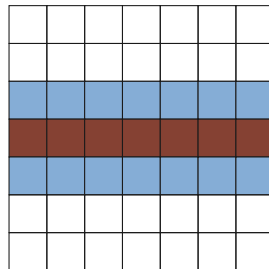
Single-Sided



Double-Sided



One-Location

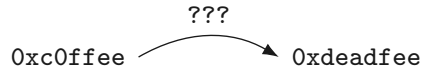


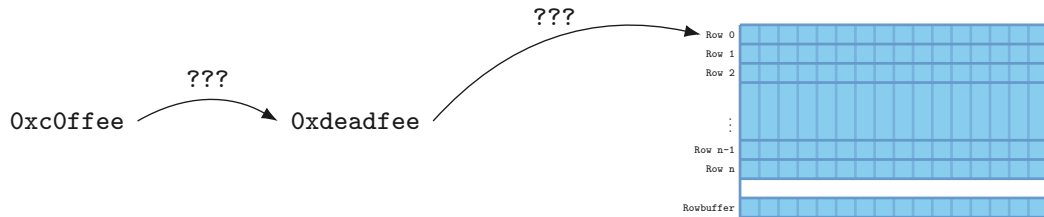
... and several more (e.g., many-sided hammering)





0xc0ffee



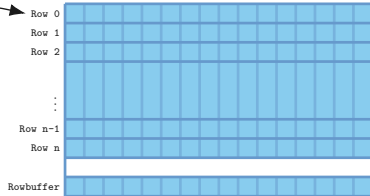


1



0xdeadfee

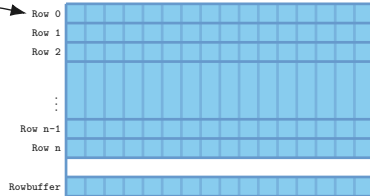
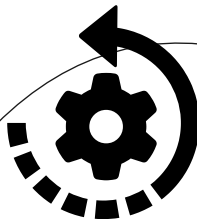
???





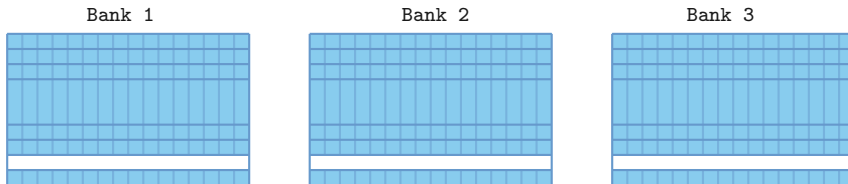
0xc0ffee

0xdeadfee

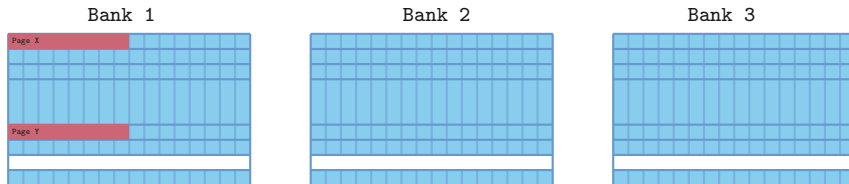


Reverse Engineering
to the Rescue!

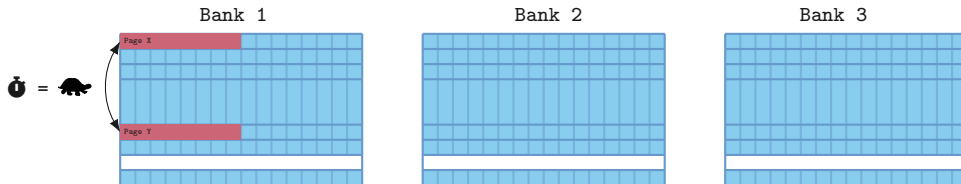
Reverse Engineering DRAM Addressing Functions



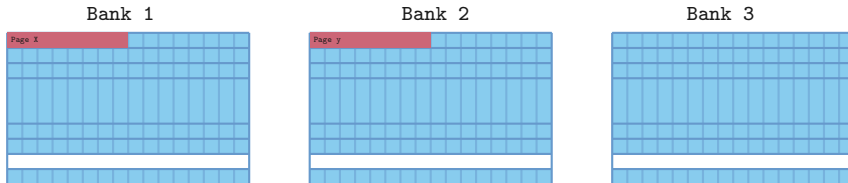
Reverse Engineering DRAM Addressing Functions



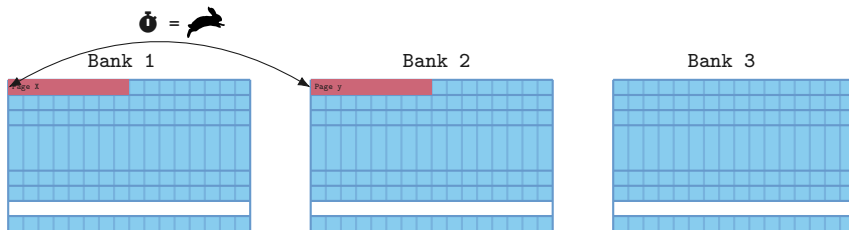
Reverse Engineering DRAM Addressing Functions

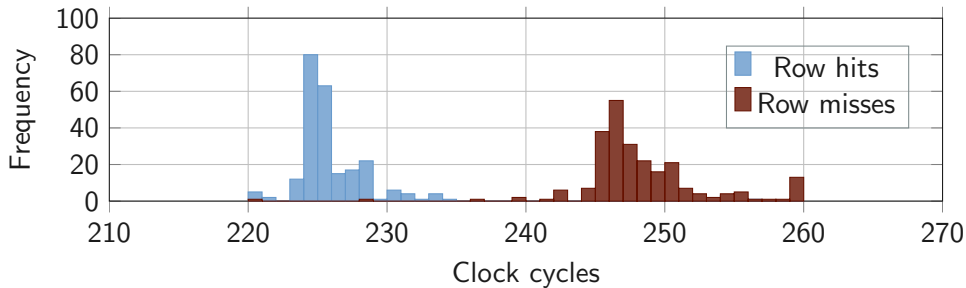


Reverse Engineering DRAM Addressing Functions



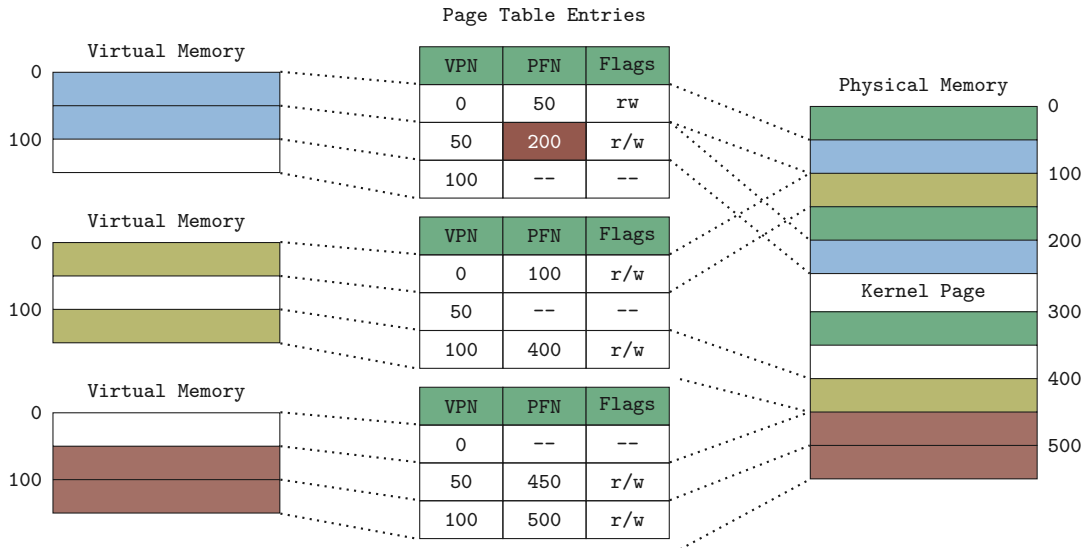
Reverse Engineering DRAM Addressing Functions



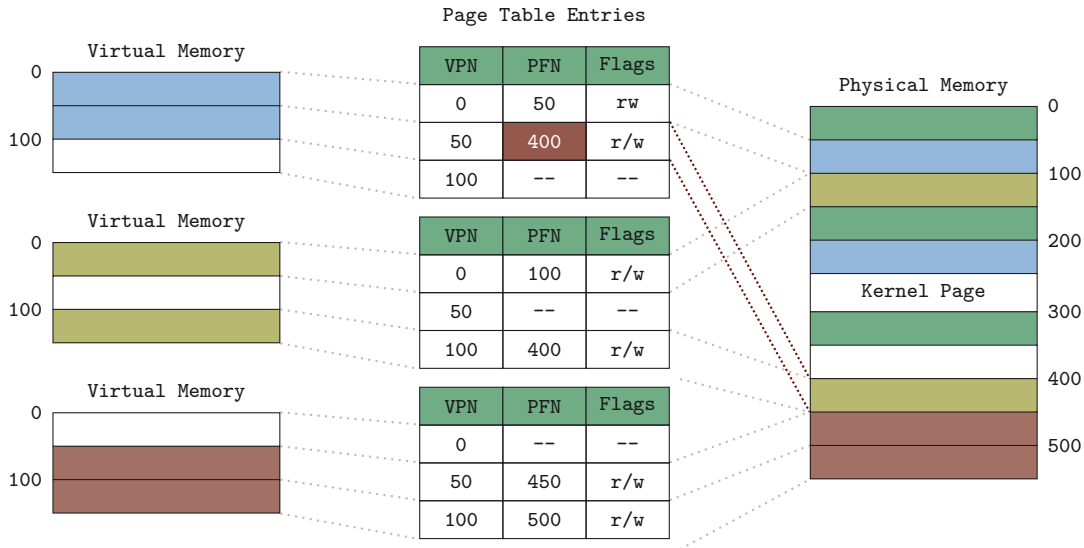


But how can we exploit it?

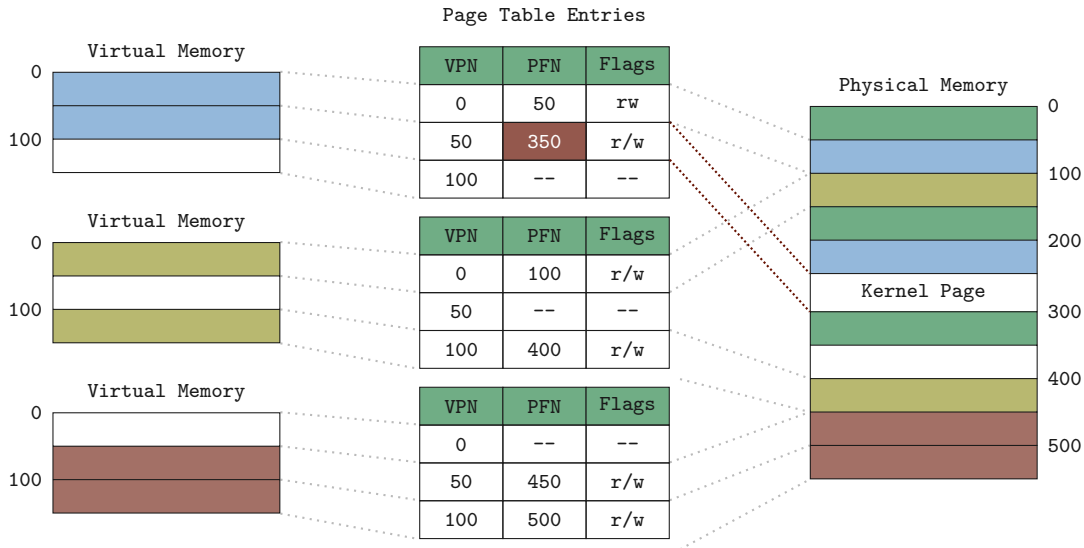
Reminder: Page Table Entries (simplified)



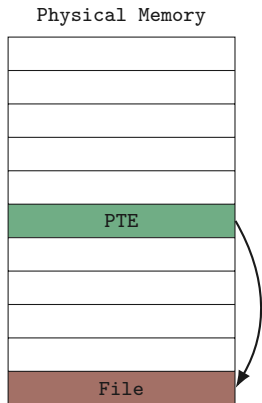
Reminder: Page Table Entries (simplified)



Reminder: Page Table Entries (simplified)

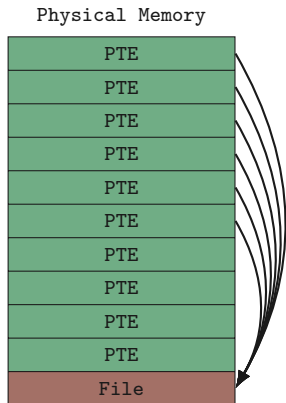


Increasing our chances with PTE Spraying

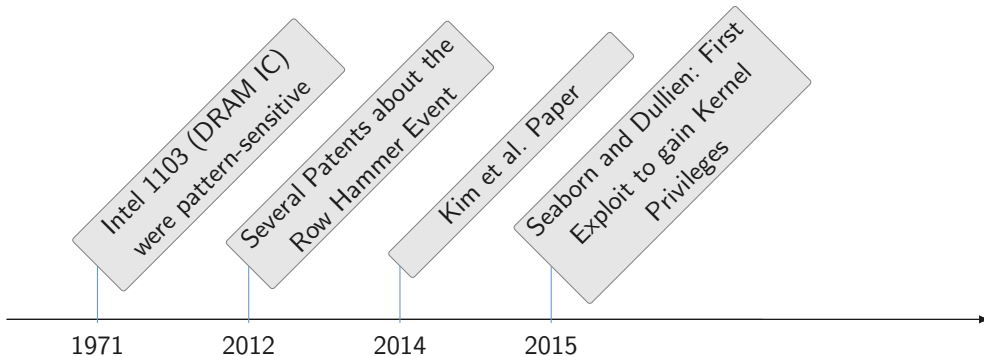
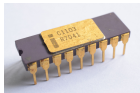


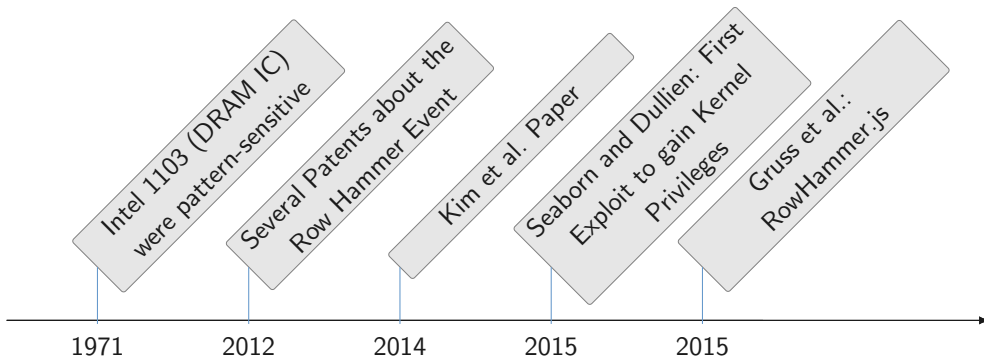
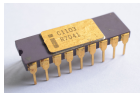
```
for (int i = 0; i < N; i++)  
    mmap(NULL, FSIZE, PROT_READ | PROT_WRITE,  
        MAP_SHARED, fd, 0);
```

Increasing our chances with PTE Spraying



```
for (int i = 0; i < N; i++)  
    mmap(NULL, FSIZE, PROT_READ | PROT_WRITE,  
        MAP_SHARED, fd, 0);
```





{JS}

{JS}

{JS}

- double-sided hammer

{JS}

- double-sided hammer
- via JavaScript

{JS}

- double-sided hammer
- via JavaScript
- without `clflush`





ROOT privileges for web apps!

heise online > IT > Fake Screenshots die jeder selbst einfach anfertigen kann

Drei Milliarden Rechner durch Rowhammer-Angriffe kompromittiert

Hacker haben mittels Rowhammer-Angriffen aus JavaScript offenbar 3 Milliarden Rechner gehackt. Sowohl die USA als auch die EU haben den Notstand ausgerufen.



Artikel verschenken **NEU**



1.430.211



Martin Heckel (@lunkw1ll), Daniel Gruss (@lavados), Florian Adamsky (@c1t)

heise online > IT > Fake Screenshots die jeder selbst einfach anfertigen kann

Drei Milliarden Rechner durch Rowhammer-Angriffe kompromittiert

Hacker haben mittels Rowhammer-Angriffen aus JavaScript offenbar 3 Milliarden Rechner gehackt. Sowohl die USA als auch die EU haben den Notstand ausgerufen.



Artikel verschenken **NEU**



1.430.211

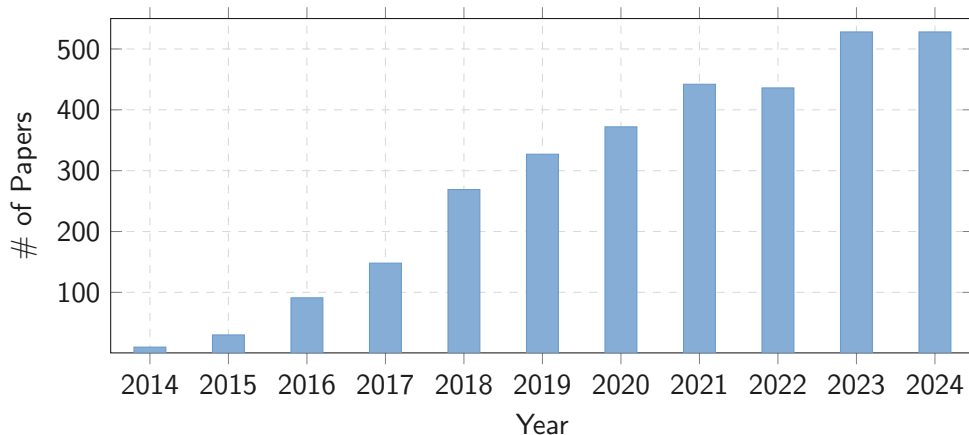


ROWHAMMER ATTACKS IN THE REAL WORLD?

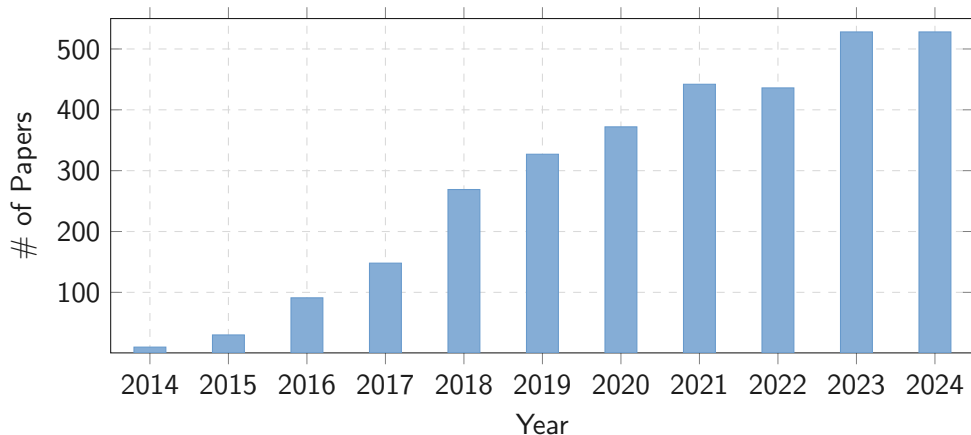


STILL NOTHING?

Scientific Papers about Rowhammer per Year



Scientific Papers about Rowhammer per Year

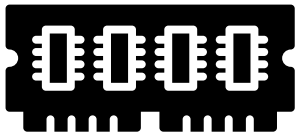


Too many works to discuss...

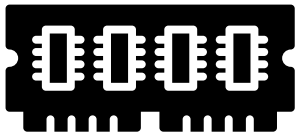
Why does Rowhammer even matter?



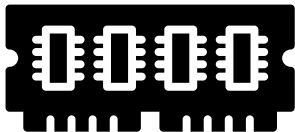
Why does Rowhammer even matter?



Why does Rowhammer even matter?

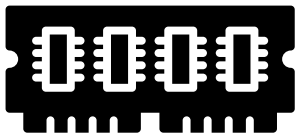


Why does Rowhammer even matter?

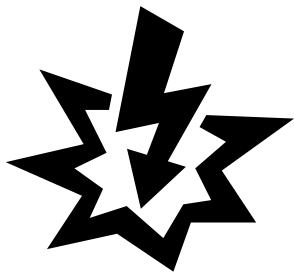


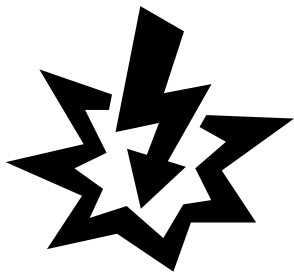
- Reliability

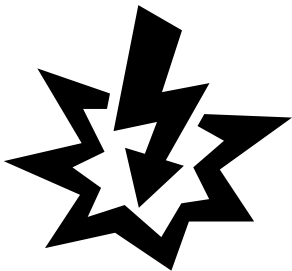
Why does Rowhammer even matter?



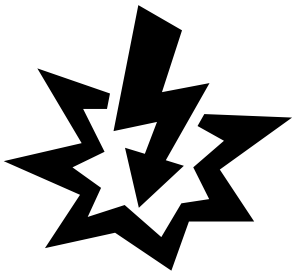
- Reliability
- Exploits



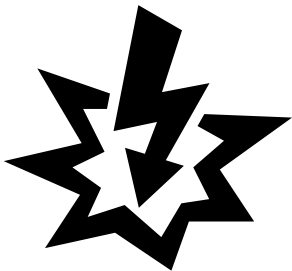




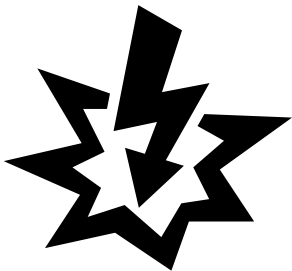
- Rowhammer enables privilege escalation attacks



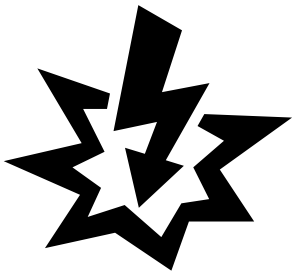
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers



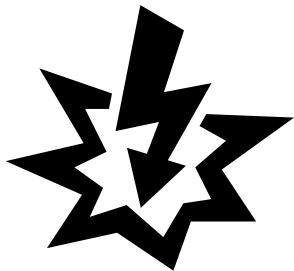
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:



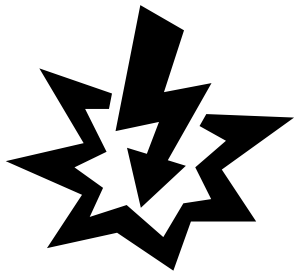
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:



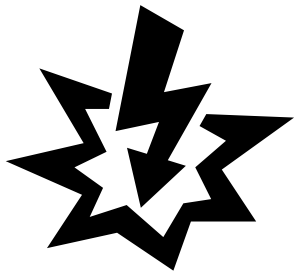
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)



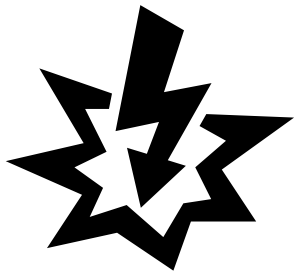
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)
 - Differences between environments



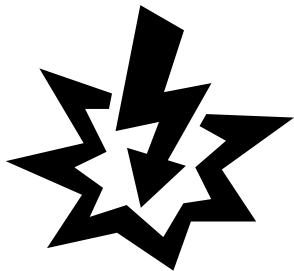
- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)
 - Differences between environments
 - **Right amount of bit flips in the right locations!**



- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)
 - Differences between environments
 - **Right amount of bit flips in the right locations!**
 - Flips reproducible (!?) → great for attacks



- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)
 - Differences between environments
 - **Right amount of bit flips in the right locations!**
 - Flips reproducible (!?) → great for attacks



- Rowhammer enables privilege escalation attacks
- Bypassing memory isolation barriers
- Challenges:
 - High-Resolution Timers (for the side channel / reverse-engineering)
 - Differences between environments
 - **Right amount of bit flips in the right locations!**
 - Flips reproducible (!?) → great for attacks (and PUFs...)

A Cat and Mouse Game









- Usually systems have a refresh rate of 64 ms



- Usually systems have a refresh rate of 64 ms



- Usually systems have a refresh rate of 64 ms
 - Can be increased by 2–4 times



- Usually systems have a refresh rate of 64 ms
 - Can be increased by 2–4 times
- More power is used

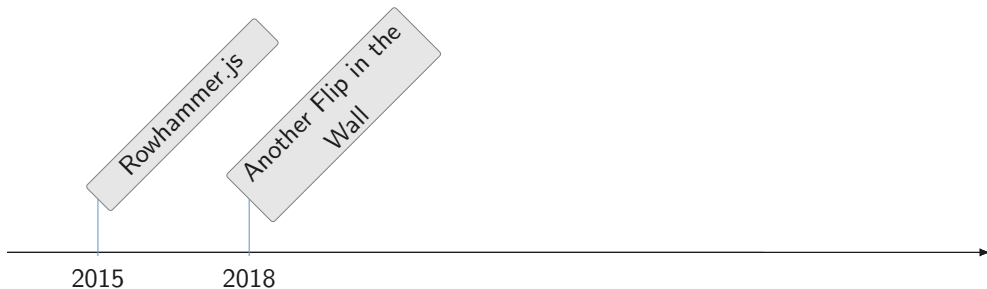


- Usually systems have a refresh rate of 64 ms
 - Can be increased by 2–4 times
- More power is used
- Will delay the requested data → less performance



- Usually systems have a refresh rate of 64 ms
 - Can be increased by 2–4 times
- More power is used
- Will delay the requested data → less performance
- Will not prevent Rowhammer

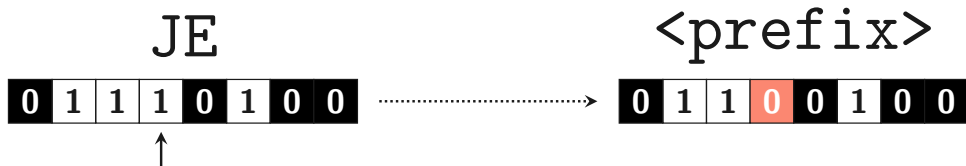
Cat and Mouse Game













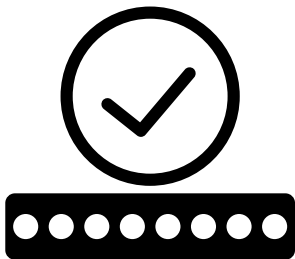


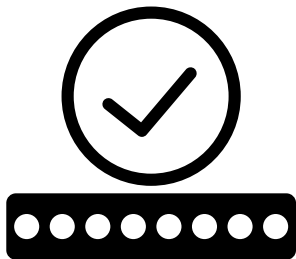




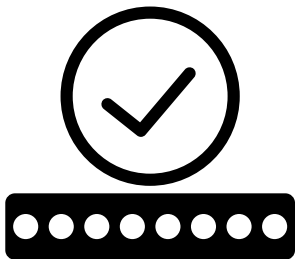


Not just opcodes → 29 exploitable bit flips in sudo

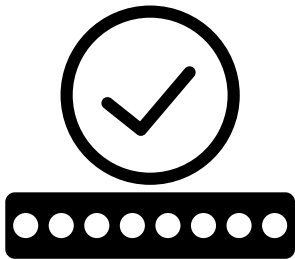




- ECC stores extra parity bits next to the data

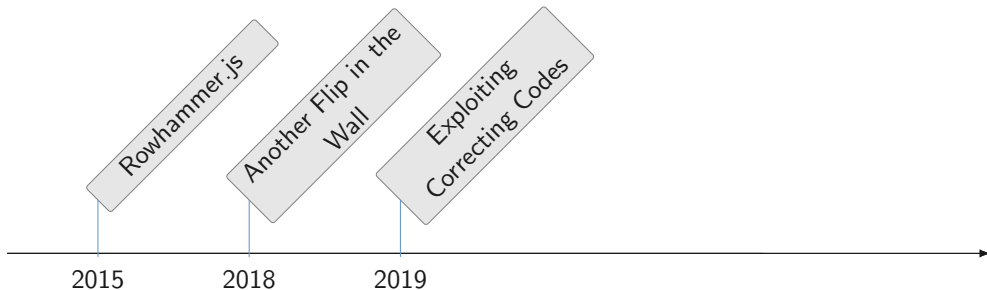


- ECC stores extra parity bits next to the data
- but it can be bypassed



- ECC stores extra parity bits next to the data
- but it can be bypassed
- reverse-engineering + multiple bit flips in the right locations → ECC bypassed

Cat and Mouse Game



Target Row Refresh (TRR)



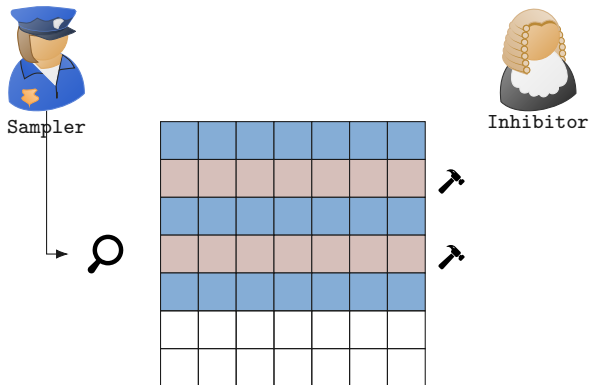
Sampler



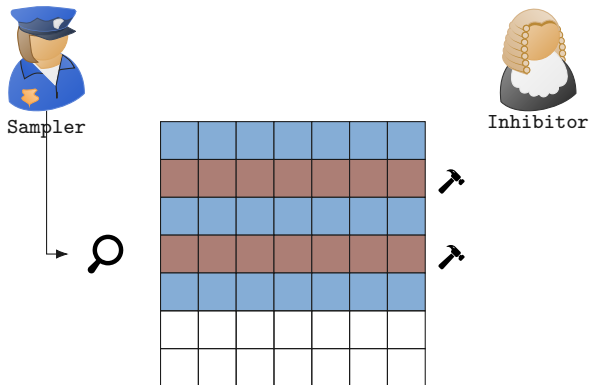
Inhibitor

Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Brown	Brown	Brown	Brown	Brown	Brown	Brown	Brown
Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Brown	Brown	Brown	Brown	Brown	Brown	Brown	Brown
Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
White	White	White	White	White	White	White	White
White	White	White	White	White	White	White	White

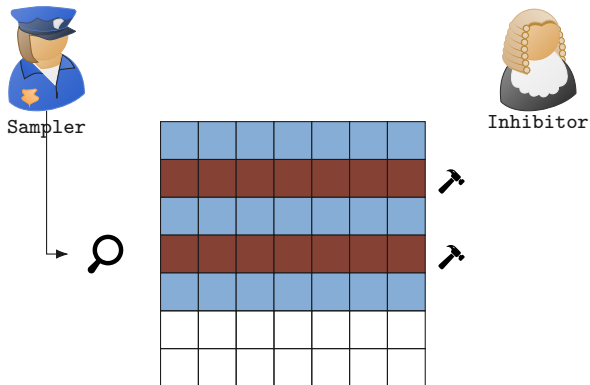
Target Row Refresh (TRR)



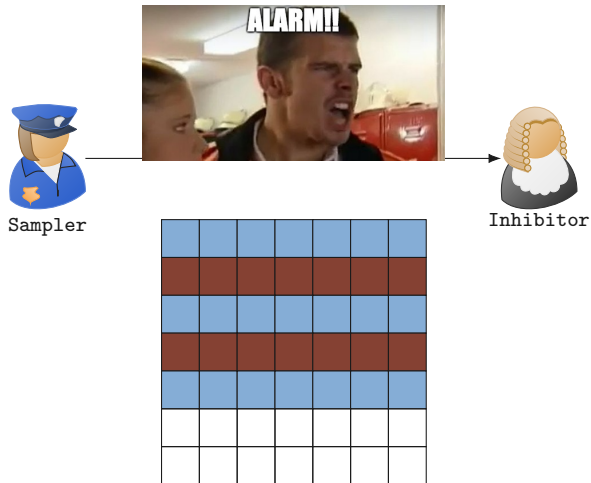
Target Row Refresh (TRR)



Target Row Refresh (TRR)



Target Row Refresh (TRR)



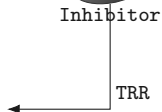
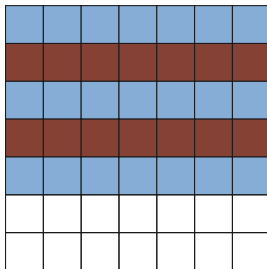
Target Row Refresh (TRR)



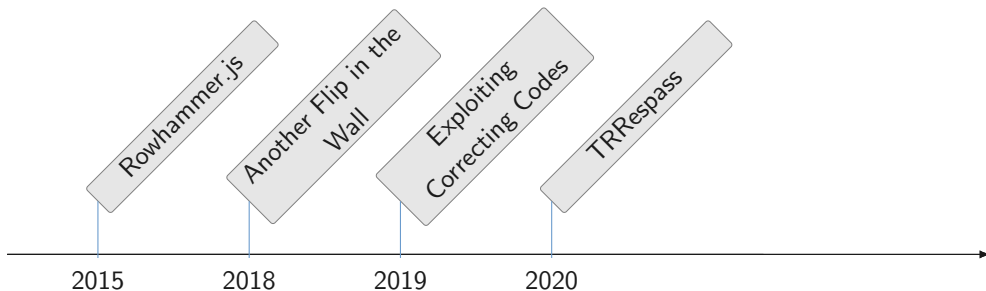
Sampler



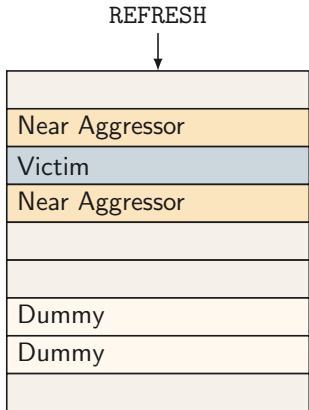
Inhibitor



Cat and Mouse Game



Near Aggressor
Victim
Near Aggressor
Dummy
Dummy



Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

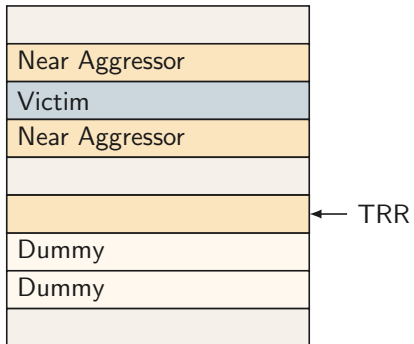
Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

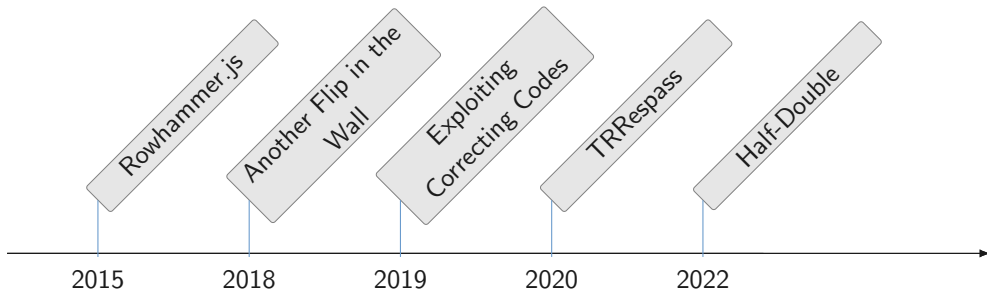


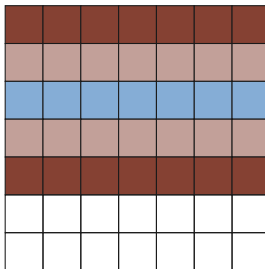
Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

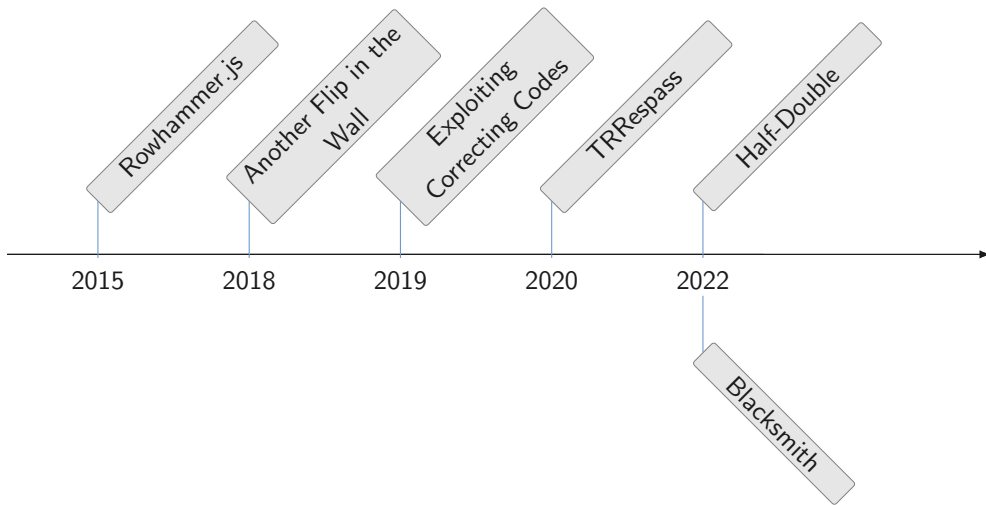
Near Aggressor
Victim
Near Aggressor
Dummy
Dummy

Cat and Mouse Game





Cat and Mouse Game











- Non-uniform Rowhammer Fuzzer



- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:



- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed



- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed

Phase: First hammer after start of a pattern



- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

Frequency: How often the aggressor row is accessed

Phase: First hammer after start of a pattern

Amplitude: How many consecutive hammers



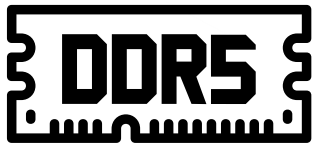
- Non-uniform Rowhammer Fuzzer
- Randomizes three characteristics:

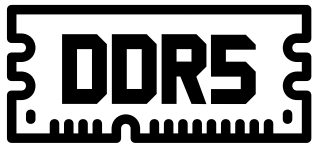
Frequency: How often the aggressor row is accessed

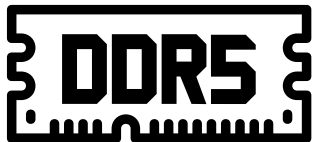
Phase: First hammer after start of a pattern

Amplitude: How many consecutive hammers

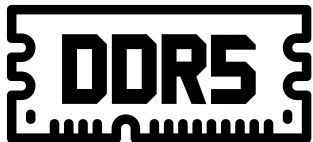
- Found bit flips in all 41 DIMMs tested





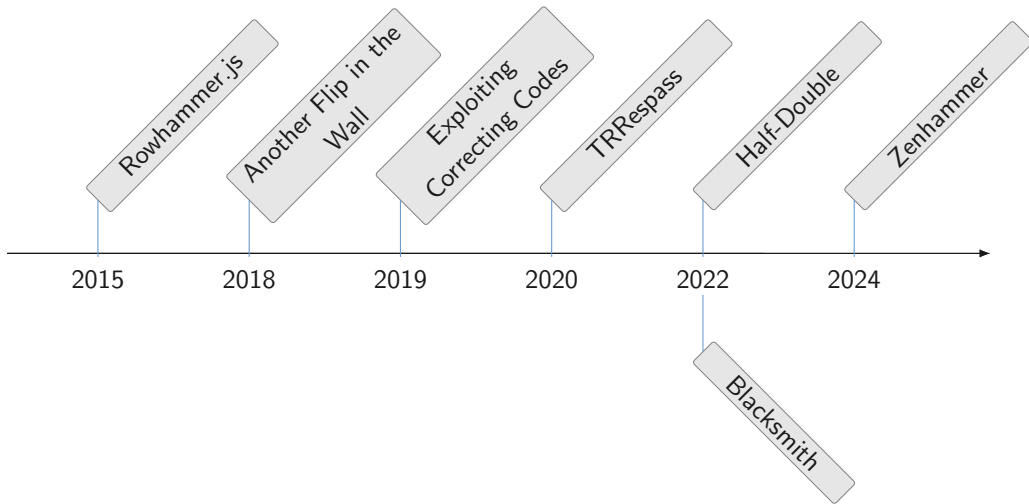


- Each row has its own activation counter



- Each row has its own activation counter
- Guarantee that every victim row is refreshed in a specific time frame

Cat and Mouse Game





- First Rowhammer bit flips on AMD



- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment



- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment
- First bit flips on DDR5



- First Rowhammer bit flips on AMD
- Different DRAM mapping, better refresh alignment
- First bit flips on DDR5 on 1 DIMM

Comprehensive Review of Rowhammer Papers

Comprehensive Review of Rowhammer Papers

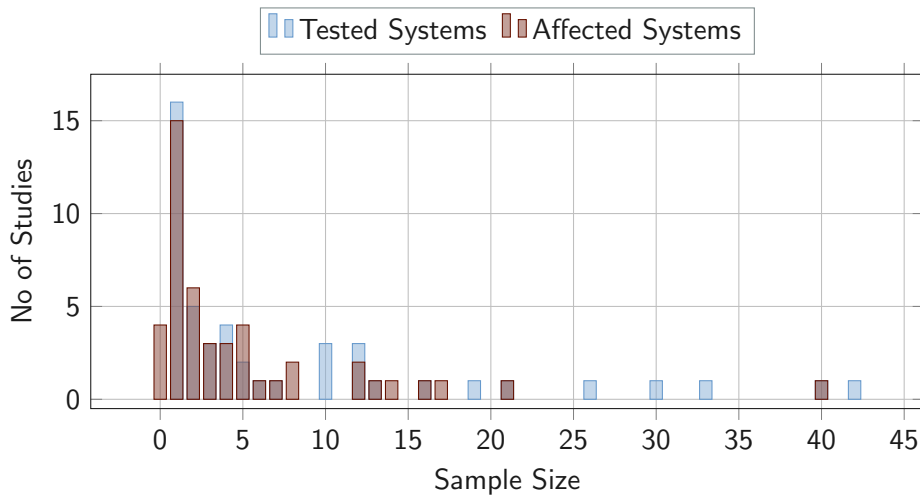
Paper	Pattern	Memory Type	Environment	Test Setup	Focus	Sample size	Flips observed on	Year
? A New Approach for Rowhammer Attacks	?	?	Unspecified	Unspecified	Exploitation	?	?	2018
Dedup Est Machine: Memory Deduplication as an Advanced Exploitation Vector	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
Dranner: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR2	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2016
Dranner: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR3	Unspecified	26 Smartphones	Exploitation, Bit Flips	26 Smartphones	17 Smartphones	2016
Dranner: Deterministic Rowhammer Attacks on Mobile Platforms	Double-Sided	LPDDR4	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	0 Smartphones	2016
Flip Feng Shui: Hammering a Needle in the Software Stack	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
One Bit Flips, One Cloud Flips: Cross-VM Row Hammer Attacks and Privilege Escalation	Single-Sided, Double-Sided	DDR3	Unspecified	8 Systems	Exploitation, Bit Flips	8 DIMMs	4 DIMMs (equipment only done on 4)	2018
One Bit Flips, One Cloud Flips: Cross-VM Row Hammer Attacks and Privilege Escalation	Single-Sided, Double-Sided	DDR4	Unspecified	1 Lab System	Exploitation, Bit Flips	1 DIMM	0 DIMMs (equipment not done on DDR4)	2016
Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript	Double-Sided	DDR3	Unspecified	2 Lab Systems	Bit Flips	6 DIMMs	5 DIMMs	2016
Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript	Double-Sided	DDR4	Unspecified	2 Lab Systems	Bit Flips	2 DIMMs	2 DIMMs	2016
SGX-Bomb: Locking Down the Processor via Rowhammer Attack	Double-Sided	DDR4	Unspecified	1 Lab System	Exploitation, Bit Flips	1 DIMM	1 DIMM	2017
When Good Protections Go Bad: Exploiting Anti-DoS Measures to Accelerate Rowhammer Attacks	Single-Sided, Double-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	4 DIMMs	3 DIMMs	2017
Another Flip in the Wall of Rowhammer Defenses	One-Location	DDR4	Unspecified	2 Lab Systems	Exploitation, Bit Flips	4 DIMMs	4 DIMMs	2018
Defeating Software Mitigations Against Rowhammer: A Surgical Precision Hammer	Single-Sided, Double-Sided, Amplified	DDR3	Unspecified	1 Lab System	Exploitation	33 Memory Setups?	14 Memory Setups?	2018
Nethammer: Inducing Rowhammer Faults through Network Requests	Double-Sided	DDR4	Unspecified	3 Lab Systems	Exploitation, Bit Flips	1 DIMM	1 DIMM	2018
Nethammer: Inducing Rowhammer Faults through Network Requests	One-Location	LPDDR2	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2018
Throhammer: Rowhammer Attacks over the Network and Defenses	Double-Sided	DDR3	Unspecified	2 Lab Systems	Bit Flips	4 DIMMs	4 DIMMs	2018
Triggering Rowhammer Hardware Faults on ARM: A PoCist	Double-Sided	LPDDR3	Unspecified	1 Single Board Computer	Bit Flips	1 Single Board	1 Single Board	2018
Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks	Double-Sided	?	Unspecified	?	Exploitation	?	?	2019
Poisonpoint: Suppressing Unwanted Bit Flips on Rowhammer Attacks	Double-Sided	DDR3	Unspecified	1 Lab System	Bit Flips	16 DIMMs	12 DIMMs	2019
RAMBilled: Reading Bits in Memory Without Accessing Them	Single-Sided, Double-Sided	DDR3	Unspecified	1 Lab System	Bit Flips	2 DIMMs	2 DIMMs	2020
TRRepass: Exploiting the Many Sides of Target Row Refresh	Many-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	42 DIMMs	13 DIMMs	2020
TRRepass: Exploiting the Many Sides of Target Row Refresh	Many-Sided	LPDDR4X	Unspecified	13 Mobile Devices	Bit Flips	13 Mobile Devices	5 Mobile Devices	2020
SMASH: Synchronized Many-sided Rowhammer Attacks from JavaScript	Many-Sided	DDR4	Unspecified	3 Lab Systems	Bit Flips	5 DIMMs	3 - 5 DIMMs (not clarified)	2021
BLACKSMITH: Scalable Rowhammering in the Frequency Domain	Fuzzed (Blacksmith)	DDR4	Unspecified	10 Lab Systems	Bit Flips	40 DIMMs	40 DIMMs	2022
BLACKSMITH: Scalable Rowhammering in the Frequency Domain	Fuzzed (Blacksmith)	LPDDR4X	Unspecified	JEDEC-compliant developer board	Bit Flips	19 Chips	16 Chips	2022
Half-Double: Hammering from the Next Row Over	Half-Double	DDR4	Unspecified	FPGA	Bit Flips	3 DIMMs	2 DIMMs	2022
Half-Double: Hammering from the Next Row Over	Half-Double	LPDDR4X	Unspecified	7 Mobile Devices	Bit Flips	7 Mobile Devices	5 Mobile Devices	2022
Half-Double: Hammering from the Next Row Over	Half-Double	DDR4	Unspecified	1 Notebook	Bit Flips	1 Notebook	0 Notebooks	2022
Half-Double: Hammering from the Next Row Over	Half-Double	LPDDR4	Unspecified	2 MiniPCs	Bit Flips	2 MiniPCs	0 MiniPCs	2022
SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation, Bit Flips	3 DIMMs	3 DIMMs	2022
SpecHammer: Combining Spectre and Rowhammer for New Speculative Attacks	Many-Sided	DDR4	Unspecified	3 Lab Systems	Exploitation, Bit Flips	3 DIMMs	3 DIMMs	2022
SpyHammer: Understanding and Exploiting Rowhammer Under Fine-Grained Temperature Variations	Single-Sided	DDR4	Temperature	FPGA	Bit Flips	12 DIMMs	12 DIMMs	2022
Understanding Rowhammer Under Reduced Wordline Voltage: An Experimental Study Using Real DRAM Devices	Double-Sided	DDR4	50C	FPGA	Bit Flips	30 DIMMs (272 Chips)	64 Chips	2022
When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	2 DIMMs	1 DIMM	2022
A Rowhammer Reproduction Study Using the Blacksmith Fuzzer	Fuzzed (Blacksmith)	DDR4	Unspecified	4 Lab Systems	Bit Flips	10 DIMMs	8 DIMMs	2023
An Experimental Analysis of Rowhammer in HBM2 DRAM Chips	HBM2	Unspecified	Unspecified	FPGA	Bit Flips	1 Chip	1 Chip	2023
RowPress: Amplifying Read Disturbance in Modern DRAM Chips	Single-Sided	DDR4	Temperature	FPGA	Bit Flips	21 DIMMs	21 DIMMs	2023
RowPress: Amplifying Read Disturbance in Modern DRAM Chips	Single-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	1 DIMM	1 DIMM	2023
Prehammer: Rowhammer and Rowpress Without Physical Address Information	Fuzzed (Blacksmith)	DDR4	Unspecified	Lab Systems	Bit Flips	12 DIMMs	6 DIMMs	2024
Prehammer: Rowhammer and Rowpress Without Physical Address Information	Single-Sided	DDR4	Unspecified	Lab Systems	Bit Flips	12 DIMMs	2 DIMMs	2024
RISC-H: Rowhammer Attacks on RISC-V	Double-Sided	DDR4	ZIC	1 Lab System (RISC-V)	Bit Flips	1 DIMM	1 DIMM	2024
Sidgohammer: Amplifying Rowhammer via Bank-level Parallelism	Many-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	7 DIMMs	7 DIMMs	2024
Sidgohammer: Amplifying Rowhammer via Bank-level Parallelism	Many-Sided	DDR4	Unspecified	1 Lab System	Bit Flips	2 DIMMs	2 DIMMs (not clarified)	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR4	Unspecified	3 Lab Systems	Bit Flips	10 DIMMs	8 DIMMs	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR5	Unspecified	1 Lab System	Bit Flips	10 DIMMs	1 DIMM	2024

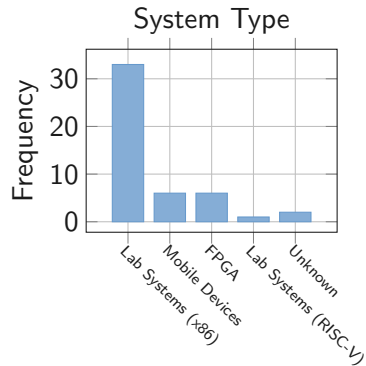
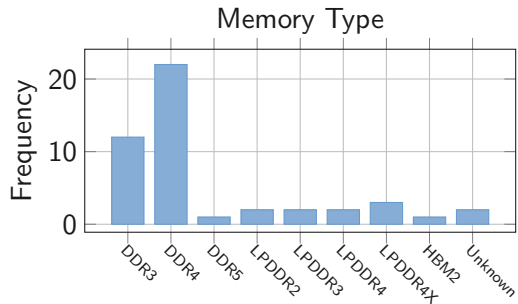
Table 1: Overview of Rowhammer Studies

Comprehensive Review of Rowhammer Papers

Paper	Pattern	Memory Type	Environment	Test Setup	Focus	Sample size	Flips observed on	Year
A New Approach for Rowhammer Attacks	?	?	Unspecified	Unspecified	?	?	?	2016
Dadup Est Machine: Memory Deduplication as an Advanced Exploitation Vector	Double-Sided	DDR3	Unspecified	1 Lab System	Exploitation	1 DIMM	1 DIMM	2016
Drammer: Systematic Rowhammer Attacks on Mobile Platforms	Double-Sided	1 DRDRAM	Unspecified	1 Smartphone	Exploitation, Bit Flips	1 Smartphone	1 Smartphone	2016
Drammer: Systematic Rowhammer Attacks on Mobile Platforms							phones	2016
Drammer: Systematic Rowhammer Attacks on Mobile Platforms							phones	2016
Drammer: Systematic Rowhammer Attacks on Mobile Platforms							phones	2016
One Bit Flips, One Bit Flips							not only done on 4)	2016
One Bit Flips, One Bit Flips							not done on DOR4)	2016
Rowhammer							bits	2016
Rowhammer							bits	2016
SGX-Bomb							bits	2017
When Good Protections Go Bad							bits	2017
When Good Protections Go Bad							bits	2018
Defeating Software							Setups?	2018
Nethammer							bits	2018
Nethammer							phone	2018
Throwhammer							bits	2018
Triggering							board	2018
Exploiting Correcting Codes							bits	2019
Pinpoint Rowhammer							bits	2019
RAMBle							bits	2020
TRReap							bits	2020
TRReap							Devices	2020
SMASH: Synthesizing Rowhammer Attacks							not clarified)	2021
BLACKSMITH							bits	2022
BLACKSMITH							bits	2022
Hammer							bits	2022
Hammer							Devices	2022
Hammer							bits	2022
Hammer							bits	2022
SpecHammer: Characterizing Rowhammer Attacks							bits	2022
SpecHammer: Characterizing Rowhammer Attacks							bits	2022
SpyHammer: Understanding Rowhammer Attacks							bits	2022
Understanding Rowhammer Attacks							bits	2022
When Frodo Fails							bits	2022
A Rowhammer Attack on ARM							bits	2023
An Exploitable Rowhammer Attack on ARM							bits	2023
RowPress							bits	2023
RowPress							bits	2023
FreeHammer: Rowhammer Attacks on ARM							bits	2024
FreeHammer: Rowhammer Attacks on ARM							bits	2024
Sledgehammer							bits	2024
Sledgehammer							bits	2024
ZENHAMMER							not clarified)	2024
ZENHAMMER: Rowhammer Attacks on AMD Zen-based Platforms	Fuzzed (Blacksmith)	DDR3	Unspecified	1 Lab System	Bit Flips	10 DIMMs	1 DIMM	2024

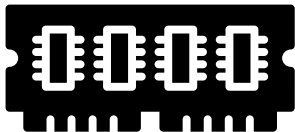
Table 1: Overview of Rowhammer Studies

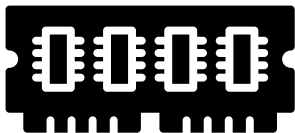




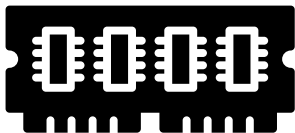
So, does it really matter?

Is Rowhammer relevant?

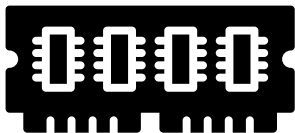




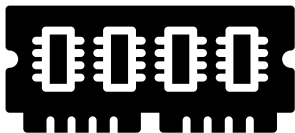
- Reliability? Yes, but...



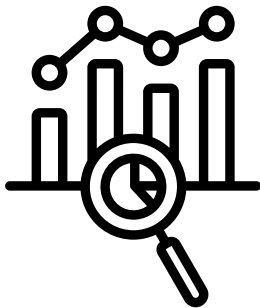
- Reliability? Yes, but...
- Exploits? Yes, but..

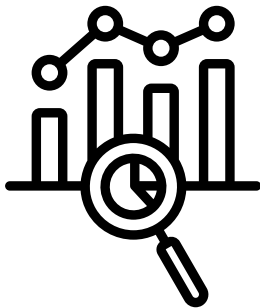


- Reliability? Yes, but...
- Exploits? Yes, but..
- Prevalence? Are even that many system affected?

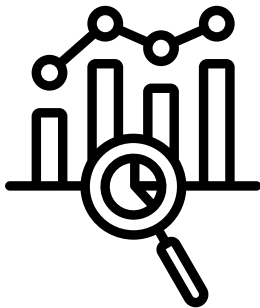


- Reliability? Yes, but...
 - Exploits? Yes, but..
 - Prevalence? Are even that many system affected?
- **We don't know!**

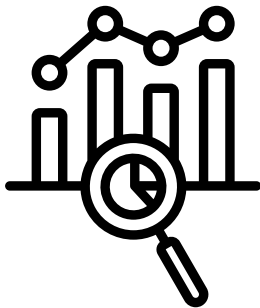




- Overall 378 DIMMs tested

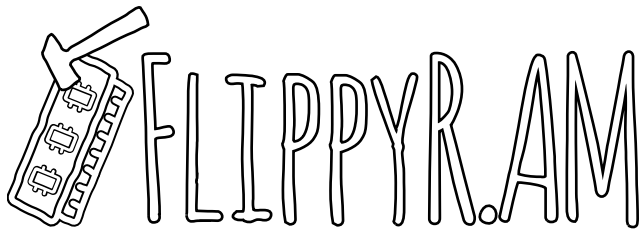


- Overall 378 DIMMs tested
- Overall 296 DIMMs (78.3 %) affected



What do we need?

A Large-Scale Prevalence Study







- Real-world conditions on real systems



- Real-world conditions on real systems
- Large-scale prevalence observations

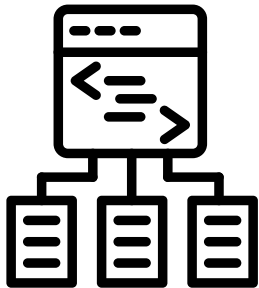


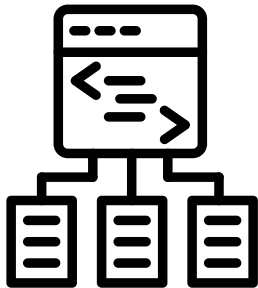
- Real-world conditions on real systems
- Large-scale prevalence observations
- Reproducibility of bit flips



- Real-world conditions on real systems
- Large-scale prevalence observations
- Reproducibility of bit flips (→ are Rowhammer PUFs even practical?)

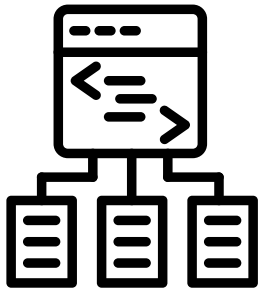
Linux bundled with a set of tools to





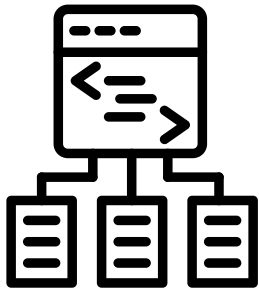
Linux bundled with a set of tools to

- Test and identify DRAM address functions



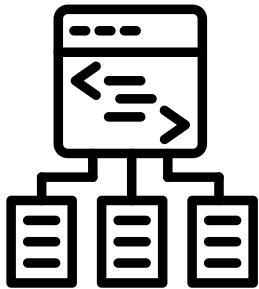
Linux bundled with a set of tools to

- Test and identify DRAM address functions
 - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE



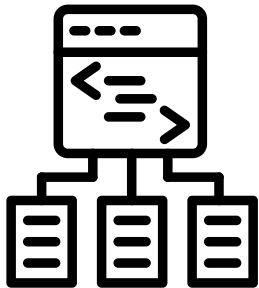
Linux bundled with a set of tools to

- Test and identify DRAM address functions
 - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips



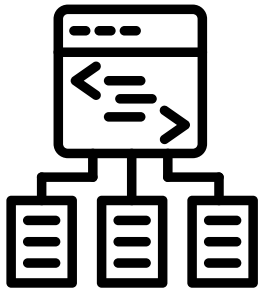
Linux bundled with a set of tools to

- Test and identify DRAM address functions
 - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
 - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool



Linux bundled with a set of tools to

- Test and identify DRAM address functions
 - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
 - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool
- **No** attacks/exploits



Linux bundled with a set of tools to

- Test and identify DRAM address functions
 - Drama, DRAMDig, TRRespass RE, Dare (Zenhammer), AMDRE
- Test Rowhammer patterns and document bit flips
 - Blacksmith, TRRespass, RowhammerJs, Rowhammer-Test, FlipFloyd, RowPress, HammerTool
- **No** attacks/exploits
 - No advantage in testing them on real-world systems

How can I participate?





- Get a free bootable USB stick from us

How can I participate?



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



- Get a free bootable USB stick from us
- or download bootable ISO from <https://FlippyR.am>



- Get a free bootable USB stick from us
 - or download bootable ISO from <https://FlippyR.am>
- Run our tests while you don't need the system (e.g., while sleeping/at work)



- Get a free bootable USB stick from us
 - or download bootable ISO from <https://FlippyR.am>
- Run our tests while you don't need the system (e.g., while sleeping/at work)
- Upload your results → then they contribute to our study





- Everything is open source: <https://FlippyR.am>



- Everything is open source: <https://FlippyR.am>
- Build the ISO and flash it yourself



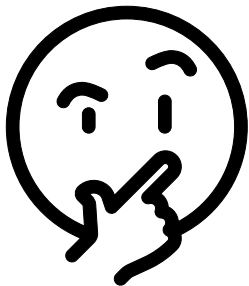
- Everything is open source: <https://FlippyR.am>
- Build the ISO and flash it yourself
- Docker-Image is available as well

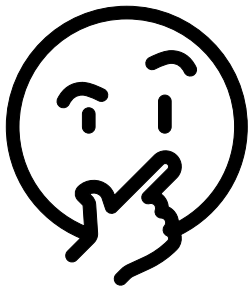


- Everything is open source: <https://FlippyR.am>
- Build the ISO and flash it yourself
- Docker-Image is available as well
- ISO-Image booted via USB is best

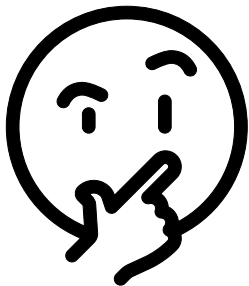


- Everything is open source: <https://FlippyR.am>
- Build the ISO and flash it yourself
- Docker-Image is available as well
- ISO-Image booted via USB is best
 - (your own or ours, doesn't matter for us)

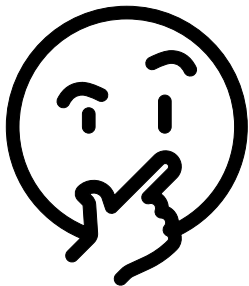


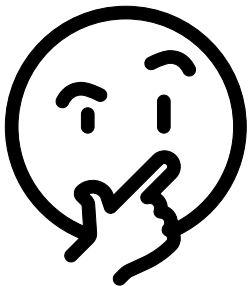


- Got the USB stick from us?

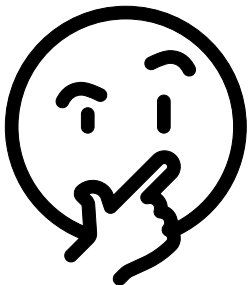


- Got the USB stick from us?

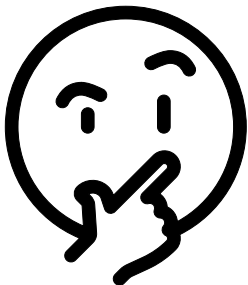




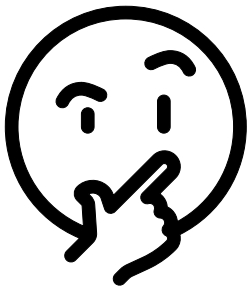
- Got the USB stick from us?
 - You know who we are



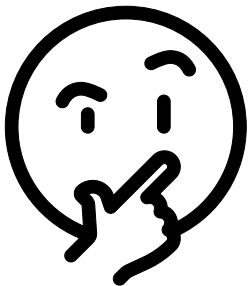
- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project



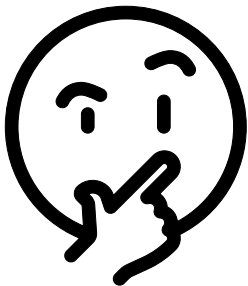
- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project
 - We don't spread malware → We would run into bigger problems if we would



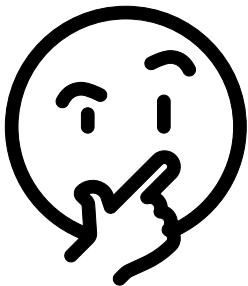
- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project
 - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...



- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project
 - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns



- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project
 - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns
 - Don't participate if you have concerns



- Got the USB stick from us?
 - You know who we are
 - This is a DFG-FWF research project
 - We don't spread malware → We would run into bigger problems if we would
- Should I disconnect all disks and peripherals? If you feel like it...
- Science is important but I still have concerns
 - Don't participate if you have concerns
 - Otherwise: please help us answering a question that we can't answer without you

Why should I participate?



Why should I participate?



Why should I participate?



- How relevant is Rowhammer on real systems?



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know





- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:
 - Keep your flippyram USB stick



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:
 - Keep your flippyram USB stick
 - Get a flippyram t-shirt if you test at least 10 systems (limited stock)



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:
 - Keep your flippyram USB stick
 - Get a flippyram t-shirt if you test at least 10 systems (limited stock)
 - You can win a gift card (see website)



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:
 - Keep your flippyram USB stick
 - Get a flippyram t-shirt if you test at least 10 systems (limited stock)
 - You can win a gift card (see website)
 - Get your name in the acknowledgements of our study



- **How relevant is Rowhammer on real systems?**
- Academics cannot answer this alone
 - we need real users to know
- Other perks, if you want to:
 - Keep your flippyram USB stick
 - Get a flippyram t-shirt if you test at least 10 systems (limited stock)
 - You can win a gift card (see website)
 - Get your name in the acknowledgements of our study
 - Learn if your own hardware is affected







- Rowhammer: reliability issue + exploitable



- Rowhammer: reliability issue + exploitable
- Real-world prevalence still unclear



- Rowhammer: reliability issue + exploitable
- Real-world prevalence still unclear
- Join us: Contribute to the large-scale flippyram study!

Ten Years of Rowhammer

A Retrospect (and Path to the Future)

Martin Heckel^{1,2} (@lunkw1ll)

Daniel Gruss¹ (@lavados)

Florian Adamsky² (@c1t)

¹ Graz University of Technology

² Hof University of Applied Sciences

