McSee: Evaluating Advanced Rowhammer Attacks and Defenses via Automated DRAM Traffic Analysis

Patrick Jattke Michele Marazzi Flavien Solt

Max Wipfli Stefan Gloor Kaveh Razavi

COMSEC

ETH zürich

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

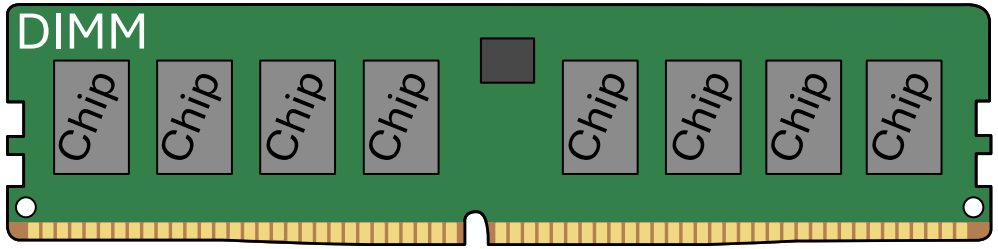
34TH USENIX SECURITY SYMPOSIUM

August 13–15, 2025
Seattle, WA, USA

Track – Hardware Security 3:
Side-Channel and Fault Injection Attacks

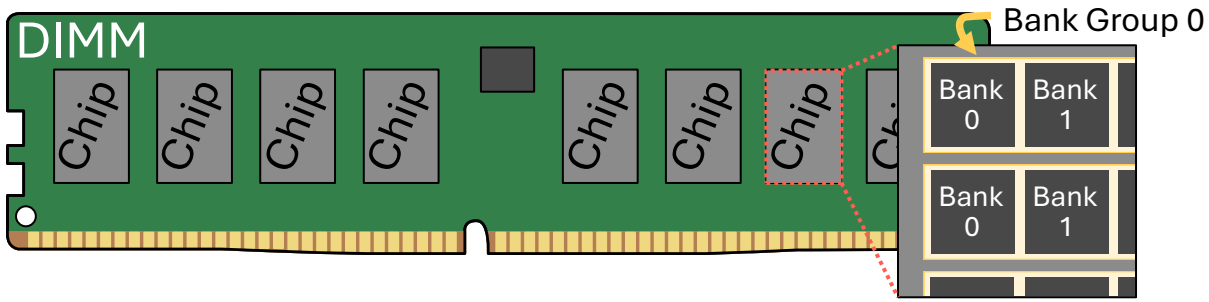
A Primer on DRAM and Rowhammer

DIMM Organization



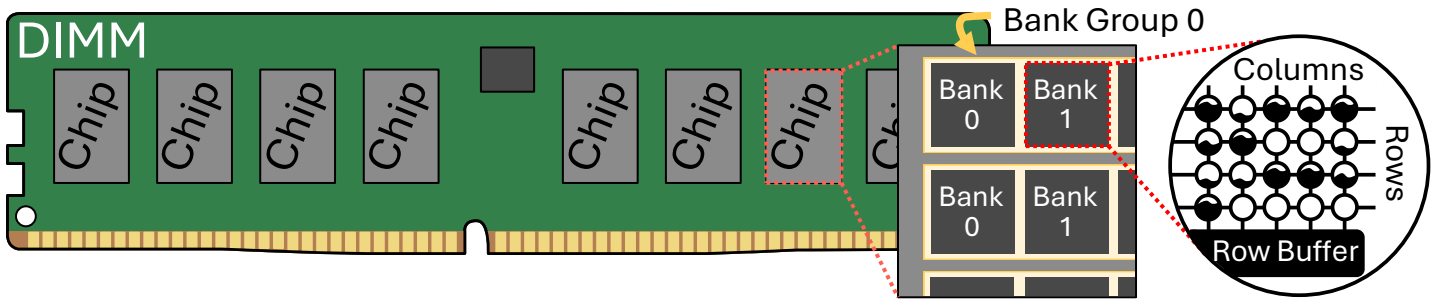
A Primer on DRAM and Rowhammer

DIMM Organization



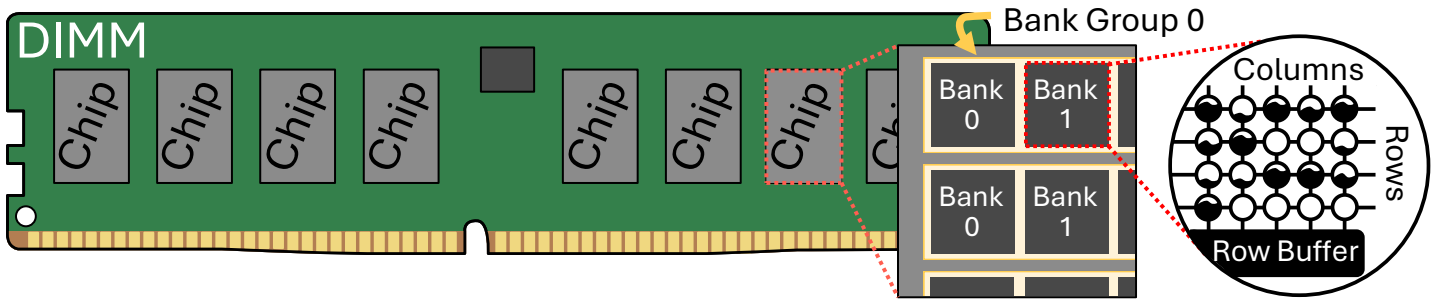
A Primer on DRAM and Rowhammer

DIMM Organization

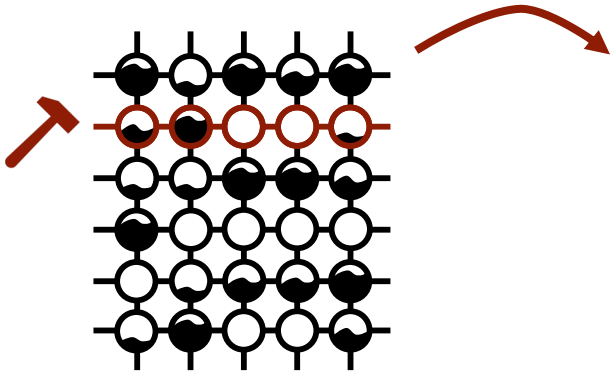


A Primer on DRAM and Rowhammer

DIMM Organization

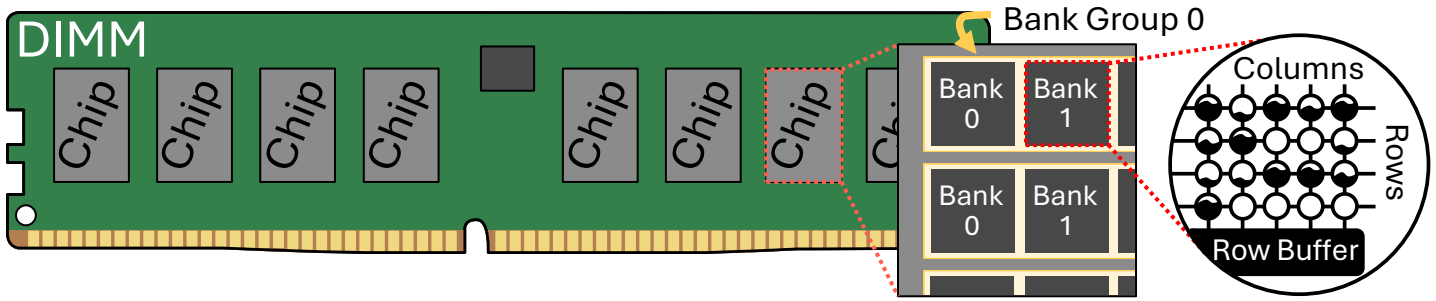


Rowhammer

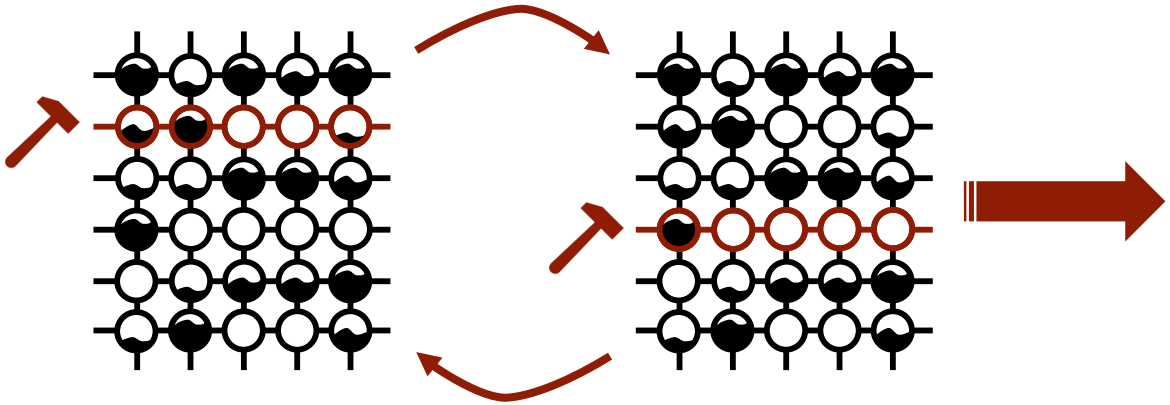


A Primer on DRAM and Rowhammer

DIMM Organization

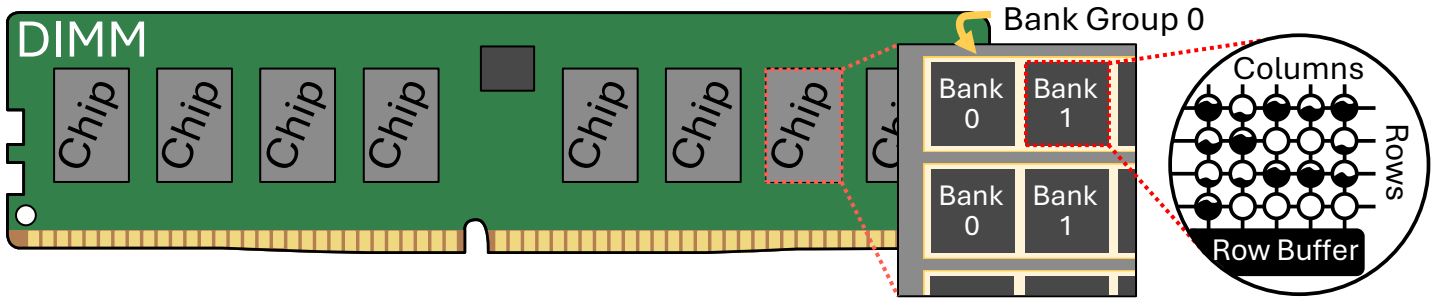


Rowhammer

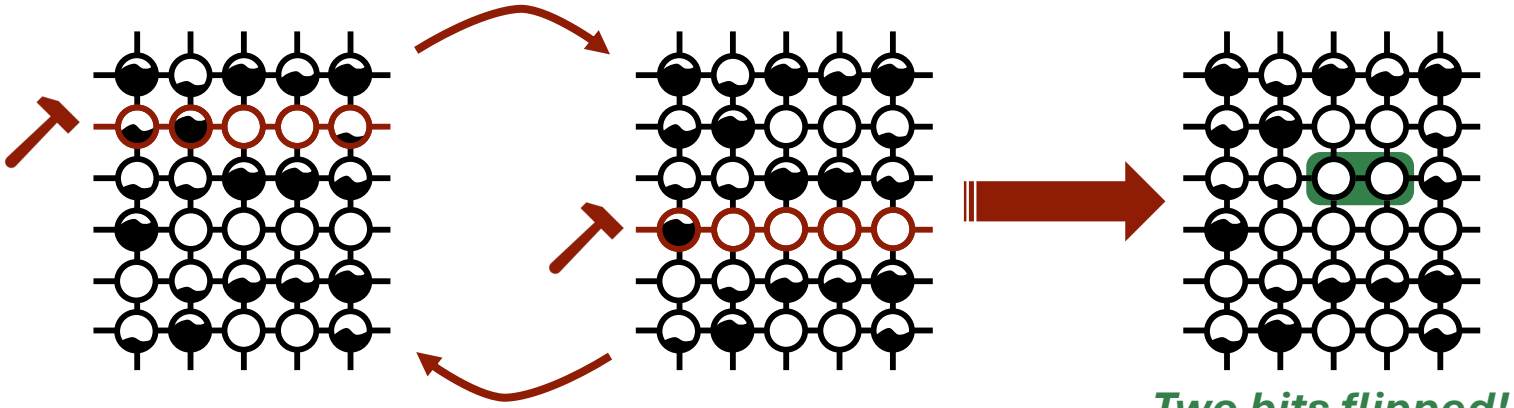


A Primer on DRAM and Rowhammer

DIMM Organization

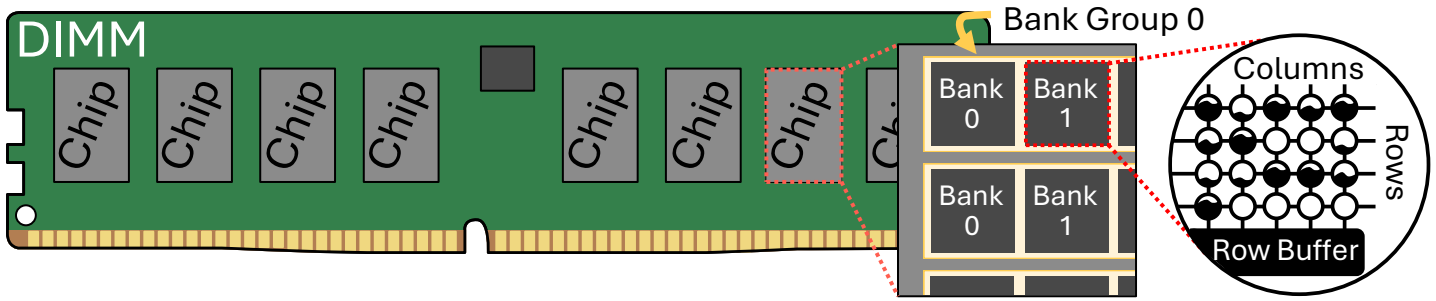


Rowhammer

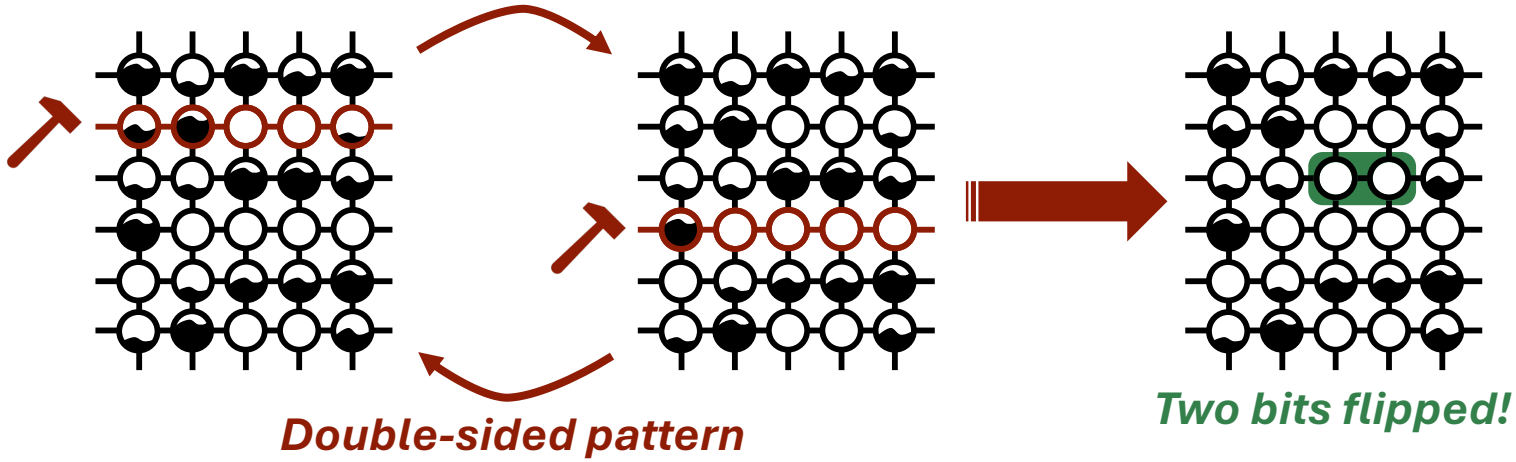


A Primer on DRAM and Rowhammer

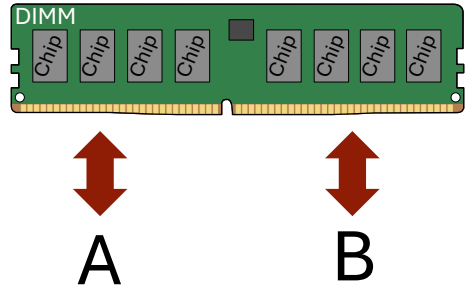
DIMM Organization



Rowhammer

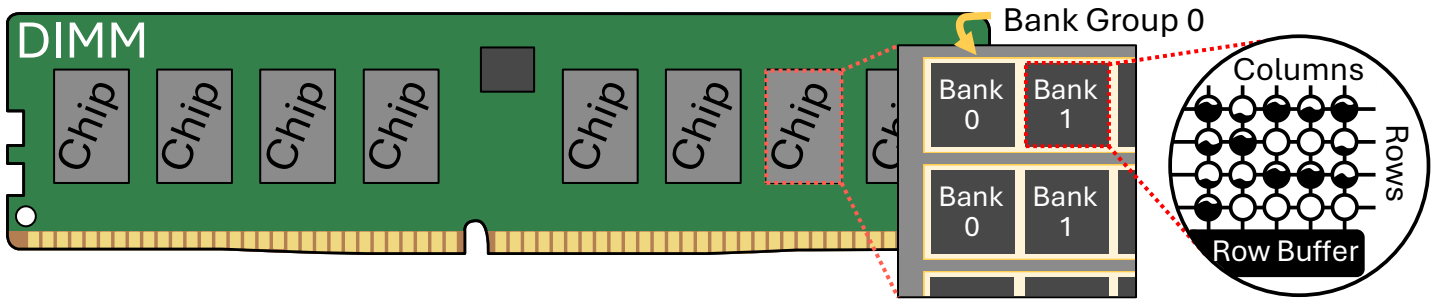


DDR5 Changes

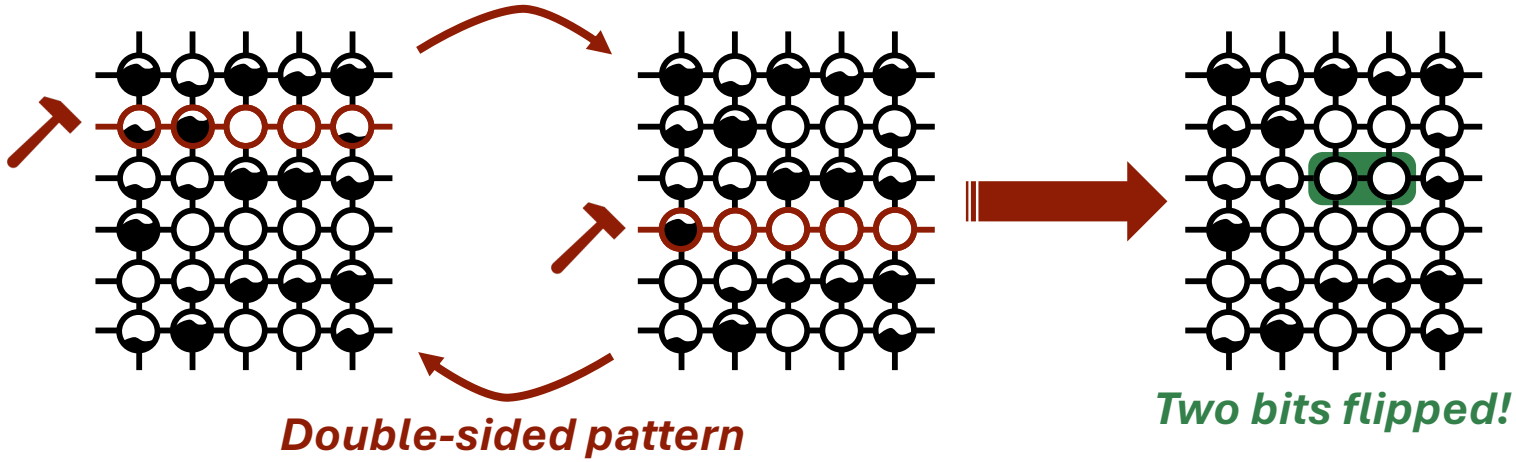


A Primer on DRAM and Rowhammer

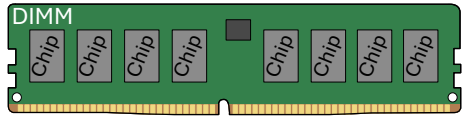
DIMM Organization



Rowhammer



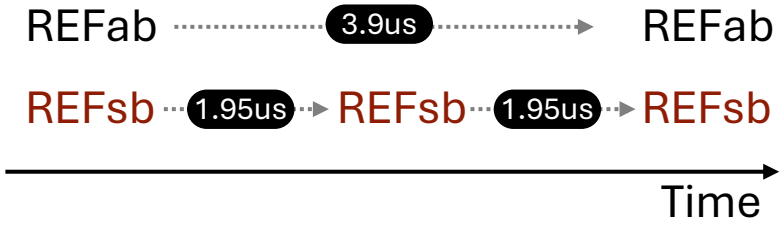
DDR5 Changes



2 Sub-channels

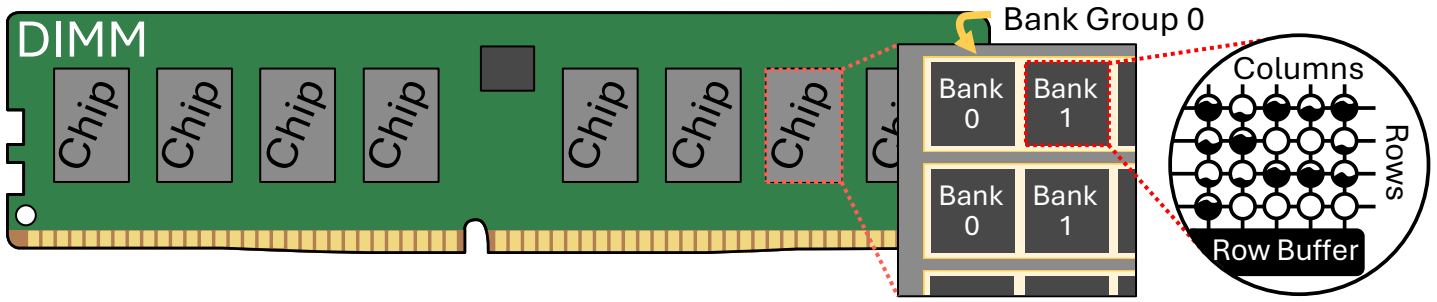
A B

Fine Granularity Refresh

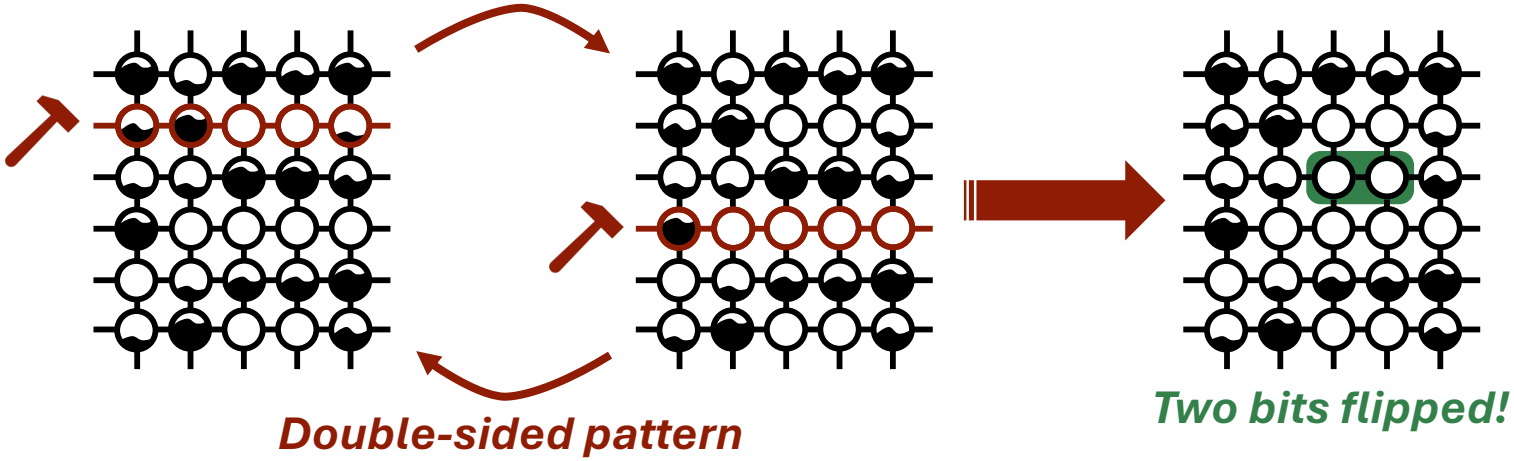


A Primer on DRAM and Rowhammer

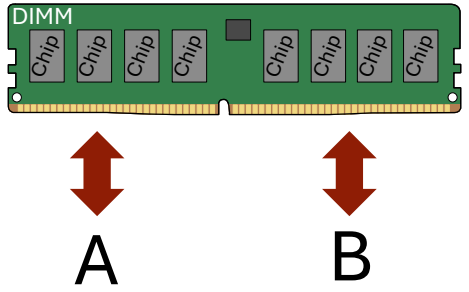
DIMM Organization



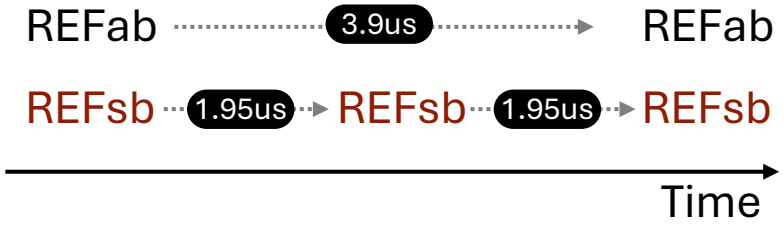
Rowhammer



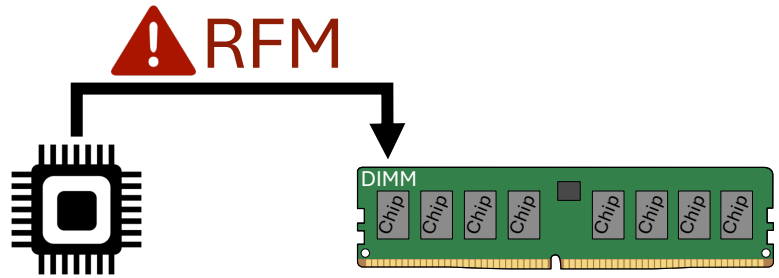
DDR5 Changes



Fine Granularity Refresh

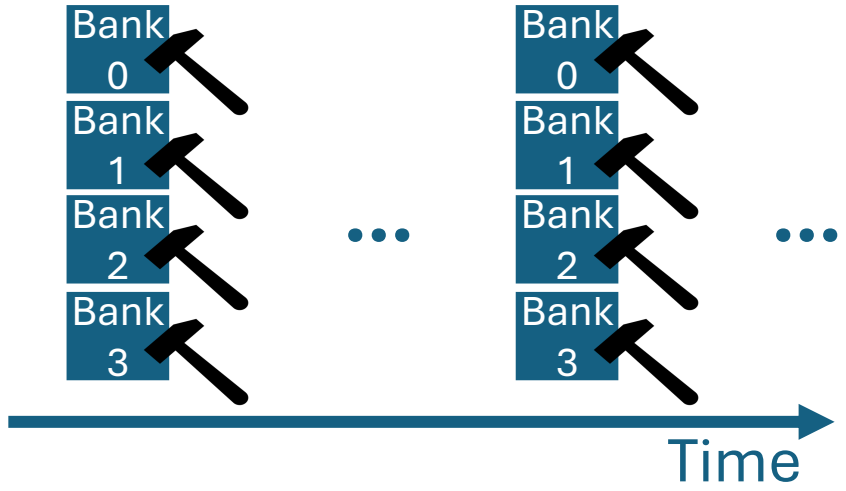


Refresh Management



Rowhammer: An Arms Race in the Dark
Attacks

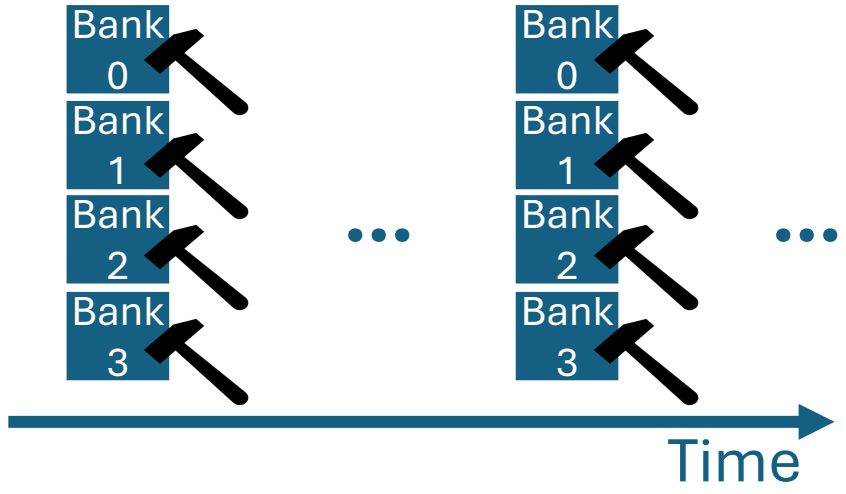
- Sledgehammer hammers **multiple banks** in parallel.
- More bitflips → easier attacks



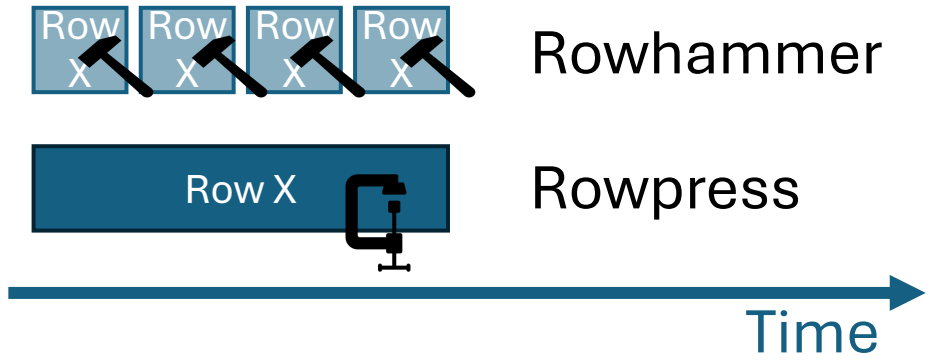
Rowhammer: An Arms Race in the Dark

Attacks

- Sledgehammer hammers **multiple banks** in parallel.
- More bitflips → easier attacks



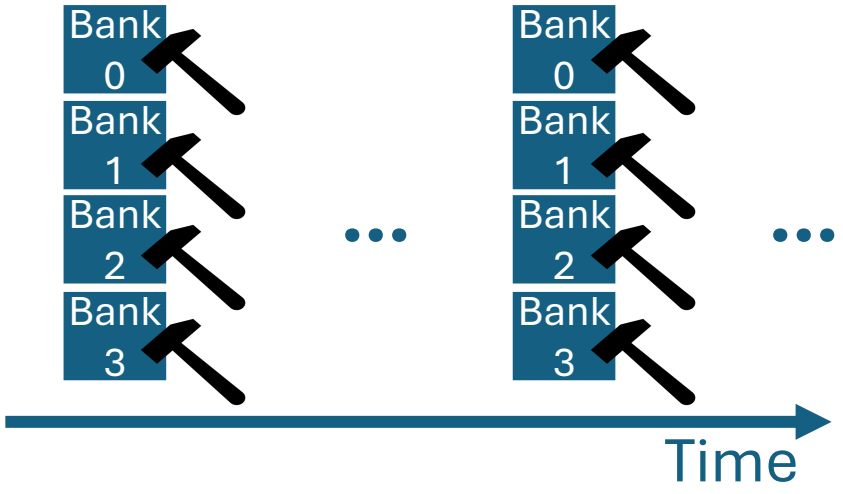
- Rowpress is a new memory disturbance effect.
- Instead of hammering, Rowpress keeps **rows open** for longer.



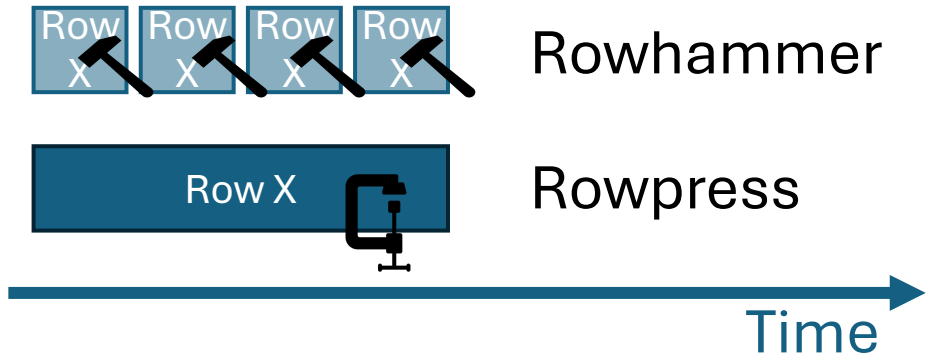
Rowhammer: An Arms Race in the Dark

Attacks

- Sledgehammer hammers **multiple banks** in parallel.
- More bitflips → easier attacks



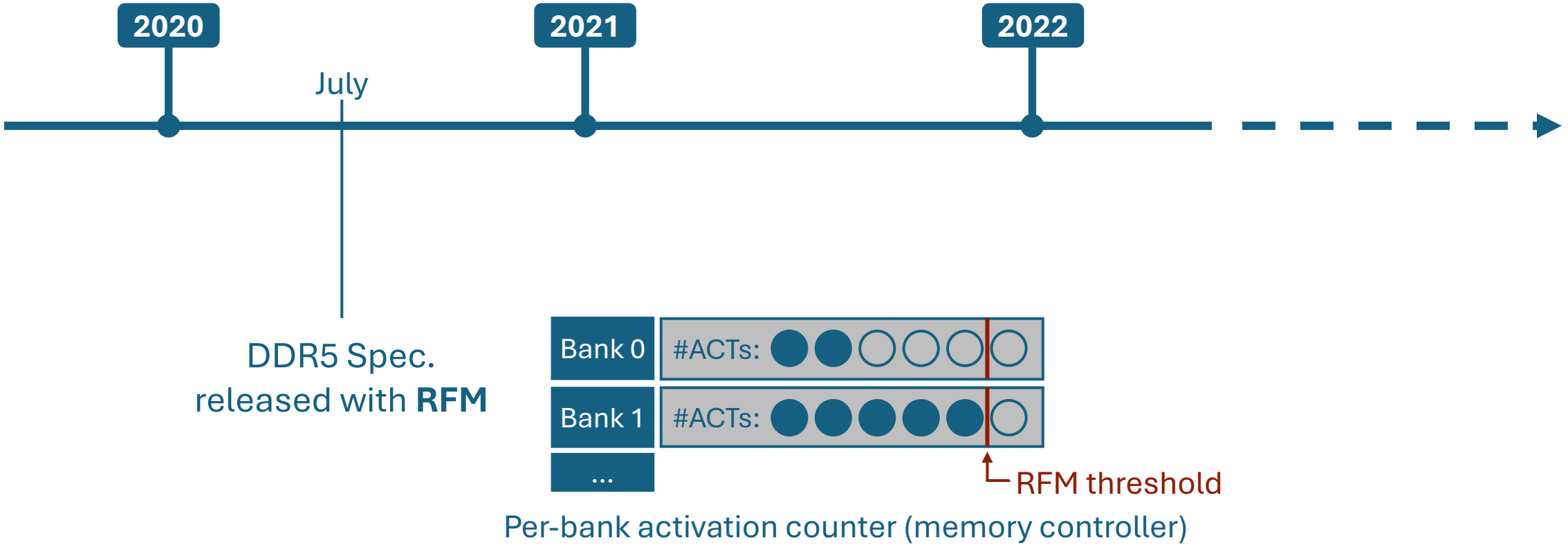
- Rowpress is a new memory disturbance effect.
- Instead of hammering, Rowpress keeps **rows open** for longer.



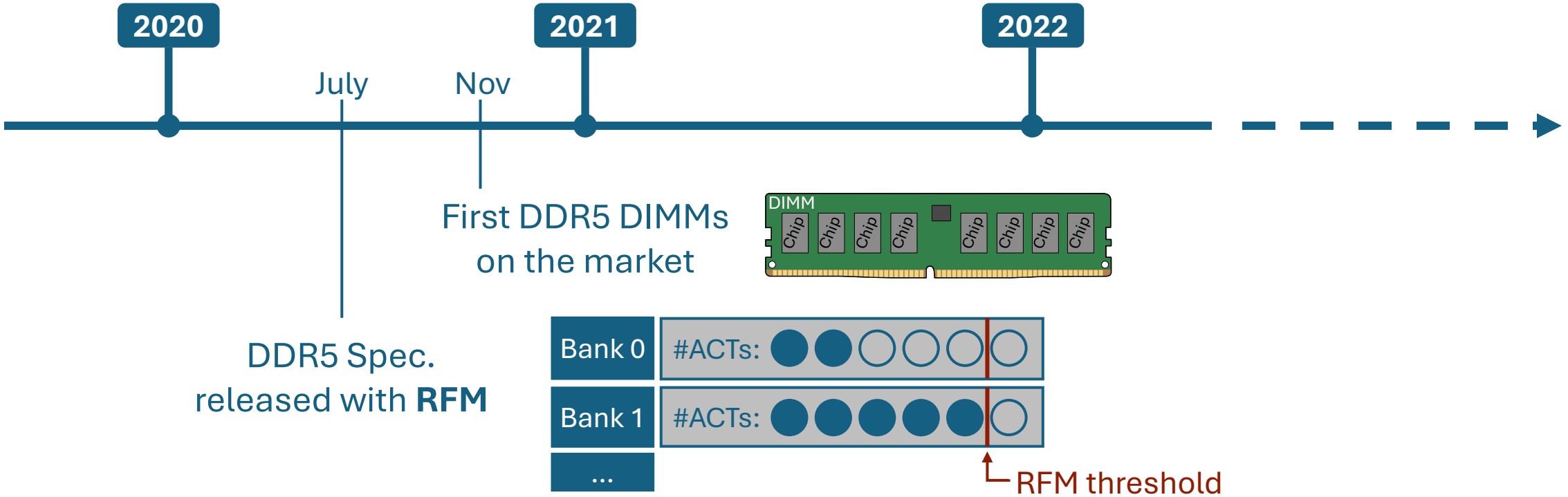
Are advanced attacks exploiting the DRAM device as intended?

Rowhammer: An Arms Race in the Dark
Defenses

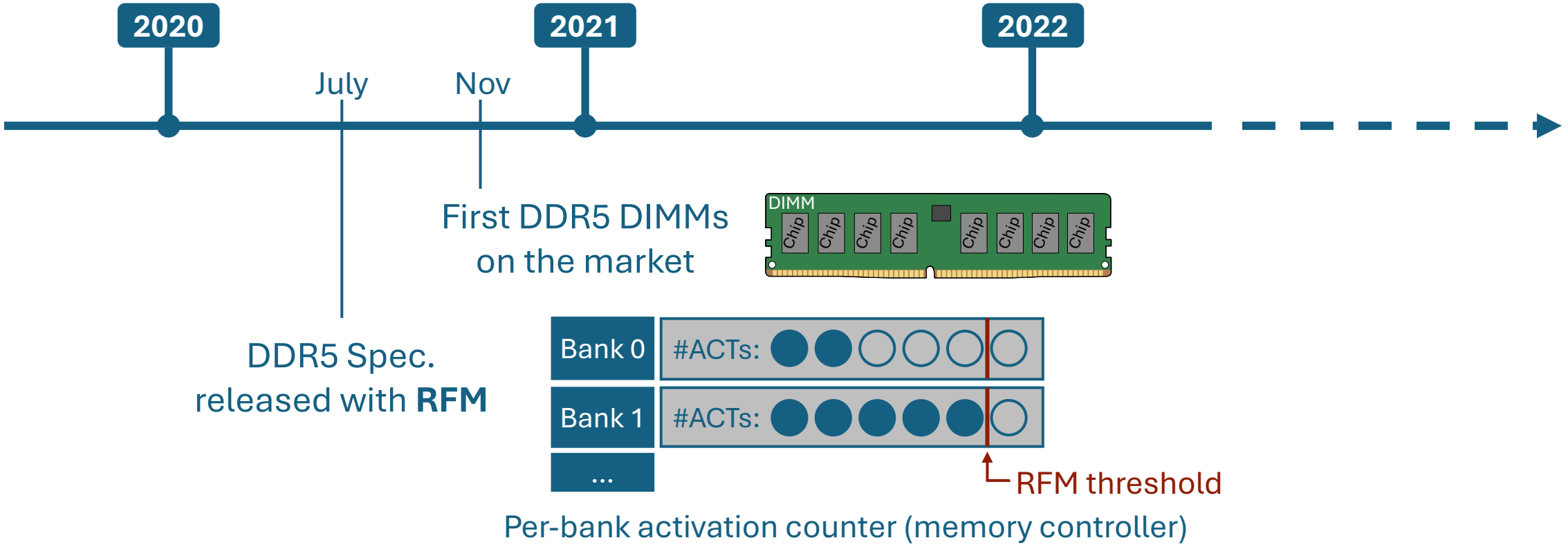
Rowhammer: An Arms Race in the Dark
Defenses



Rowhammer: An Arms Race in the Dark
Defenses

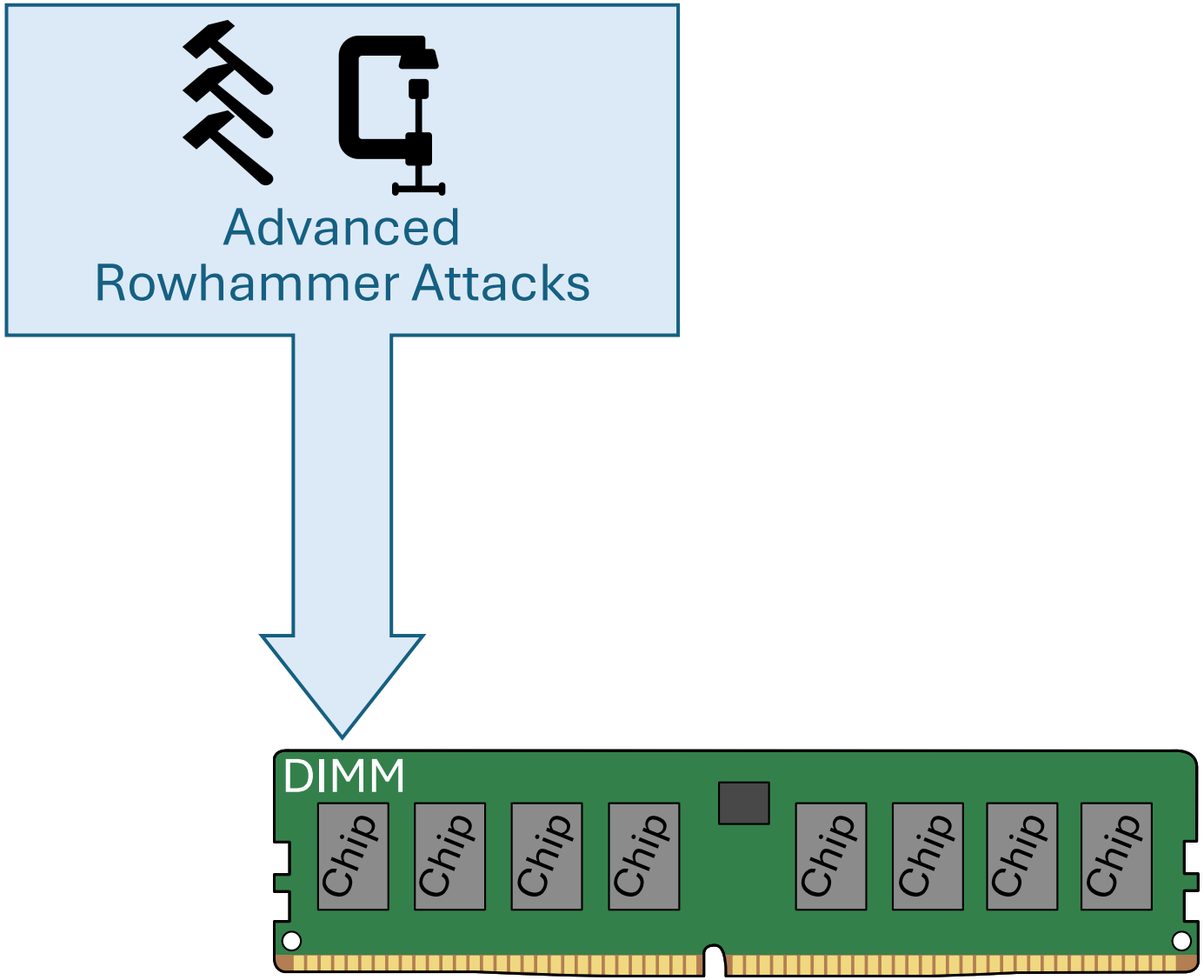


Rowhammer: An Arms Race in the Dark
Defenses

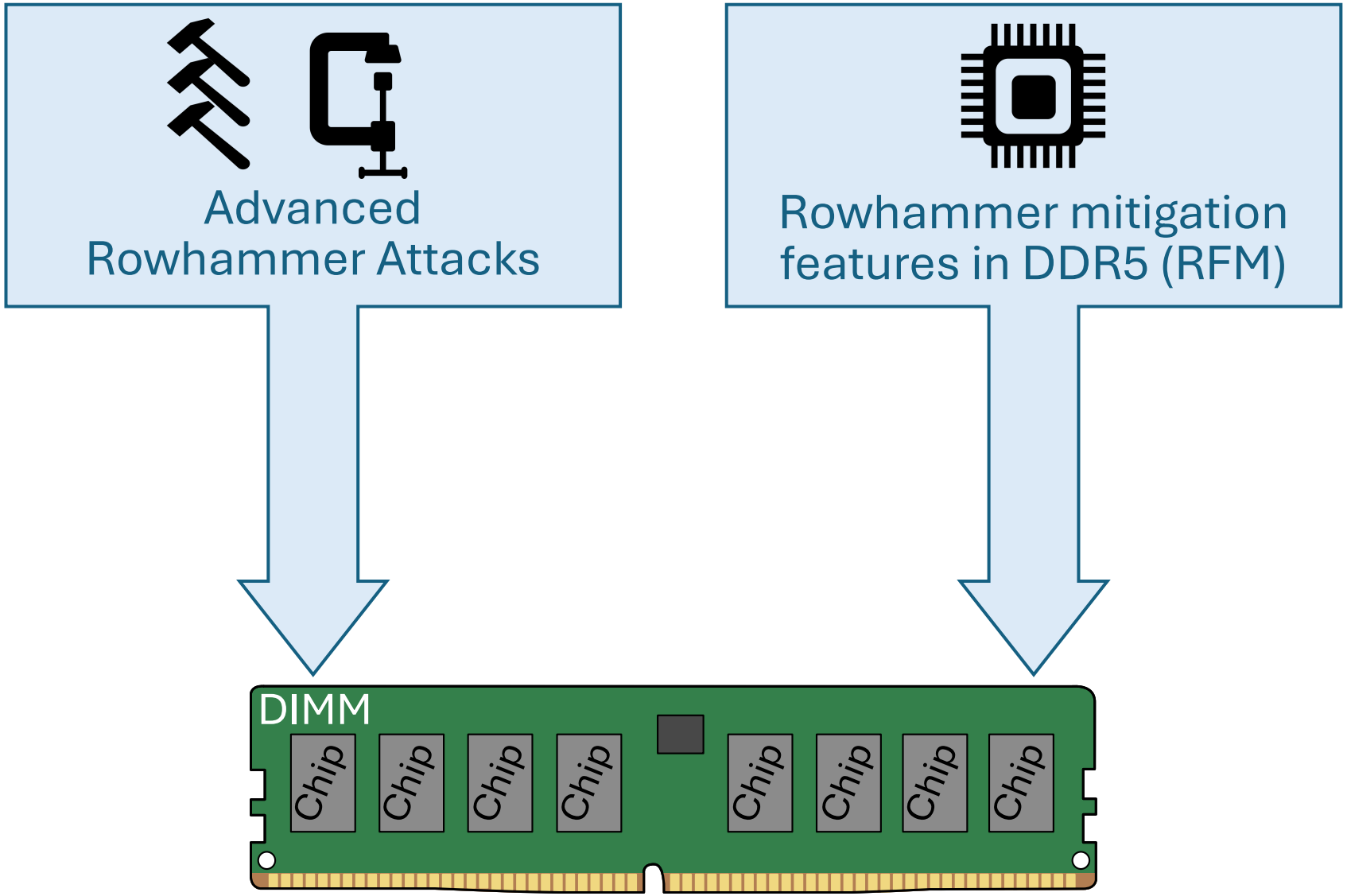


Are CPUs using *optional* DDR5 features to protect against Rowhammer?

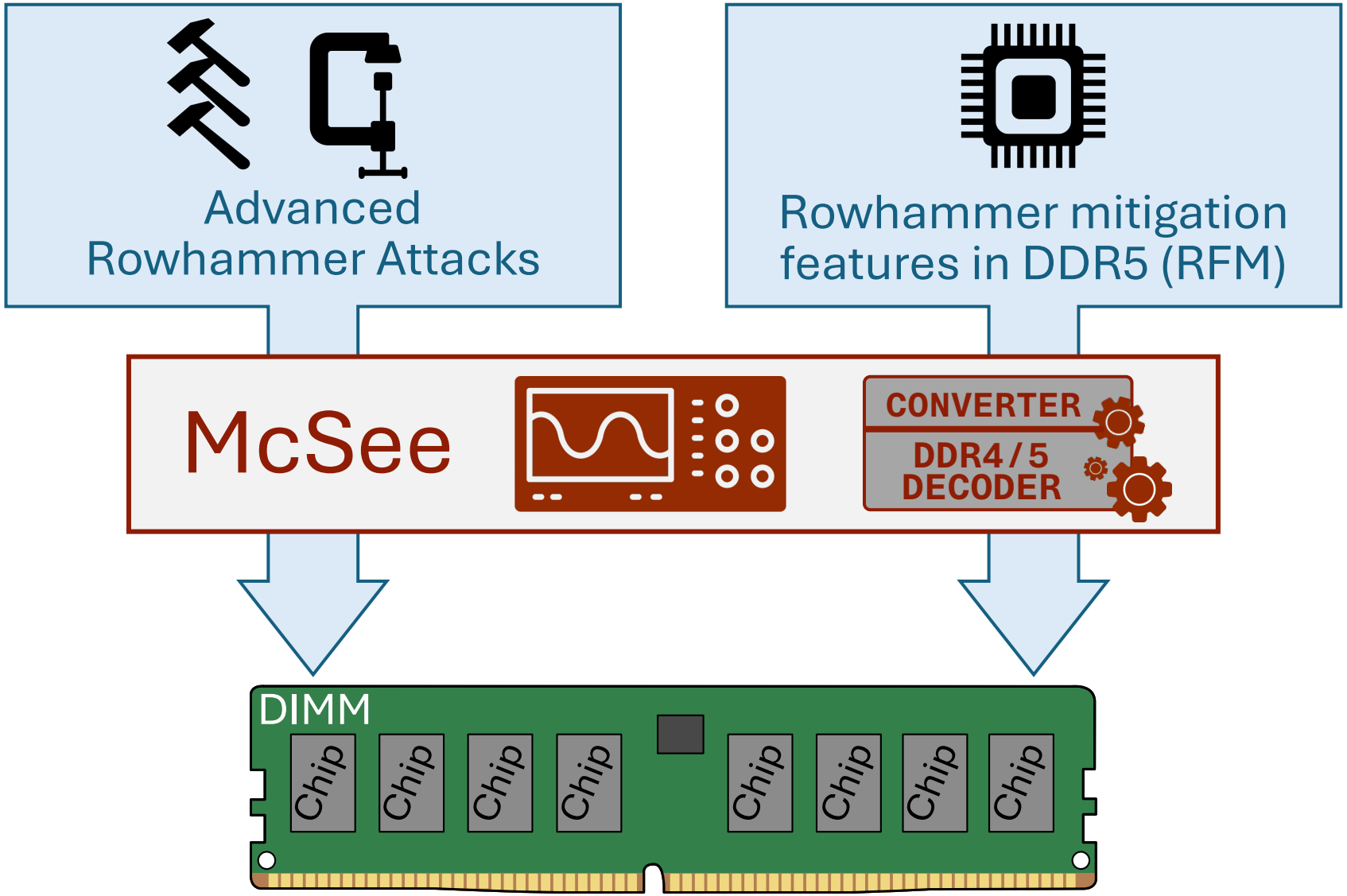
McSee


Advanced
Rowhammer Attacks
DIMM
Chip
Chip
Chip
Chip
Chip
Chip
Chip
Chip

McSee


Advanced
Rowhammer Attacks
Rowhammer mitigation
features in DDR5 (RFM)
DIMM
Chip
Chip
Chip
Chip
Chip
Chip
Chip
Chip

McSee


Advanced
Rowhammer Attacks
Rowhammer mitigation
features in DDR5 (RFM)
McSee
CONVERTER
DDR4/5
DECODER
DIMM
Chip
Chip
Chip
Chip
Chip
Chip
Chip
Chip

Our Solution: The McSee Platform

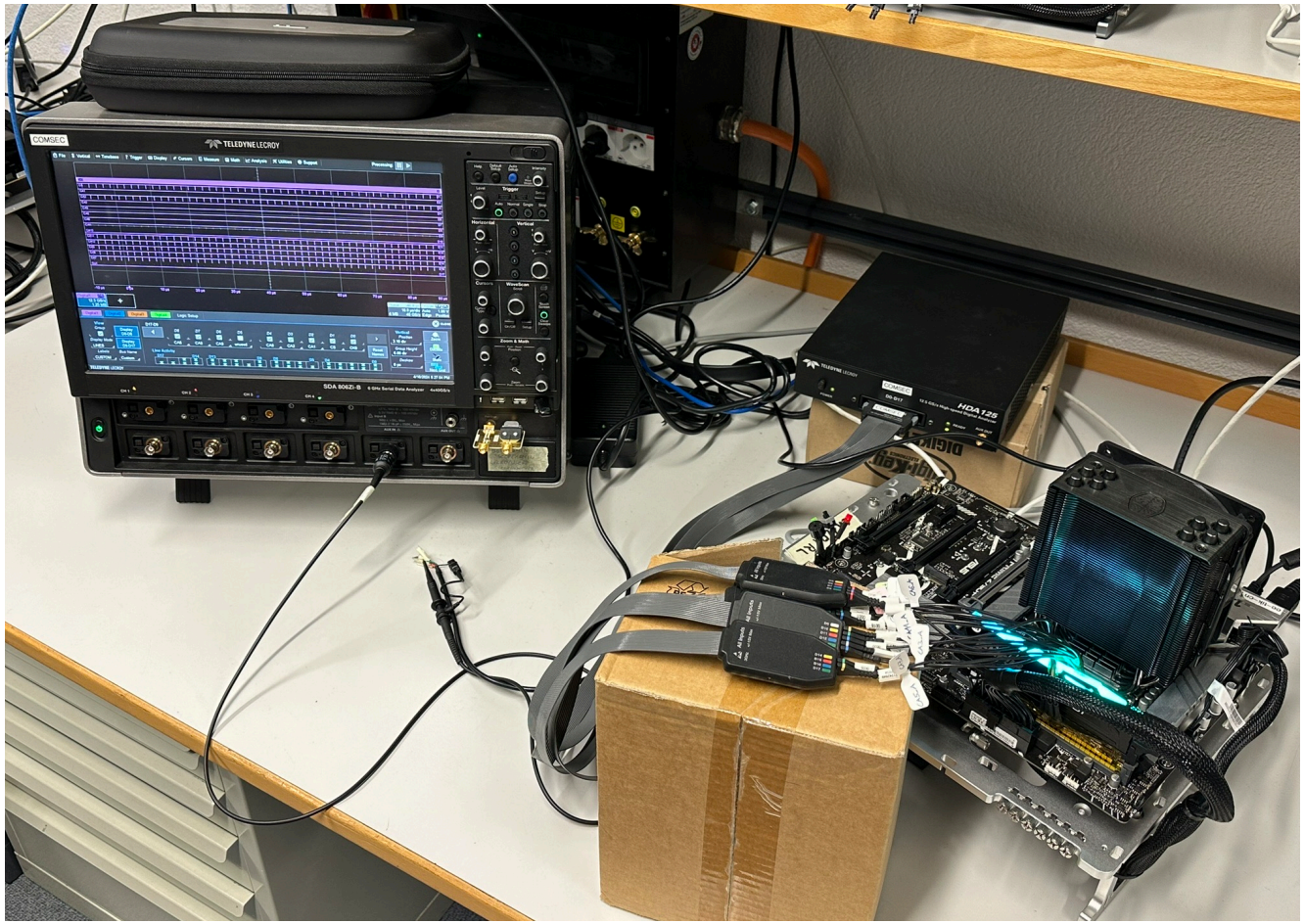
Our Solution: The McSee Platform

Our Solution: The McSee Platform

Our Solution: The McSee Platform

Our Solution: The McSee Platform

Our Solution: The McSee Platform



Goals

Requirements
- ≥ 2.4 GHz
- ≥ 16 chs.
- scriptable

Suitable

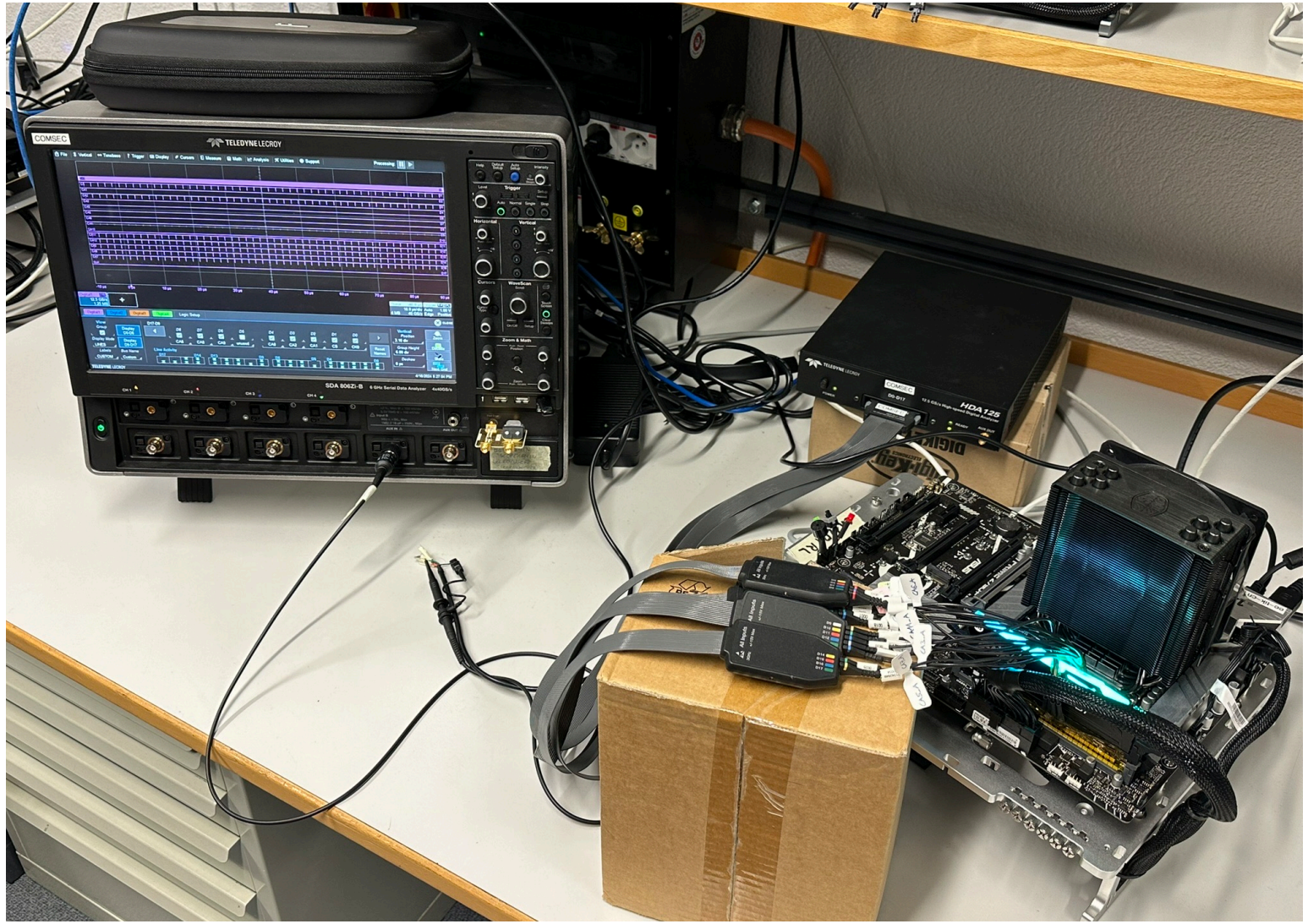
U R SO DIMM DDR 4 5

Flexible

Accessible

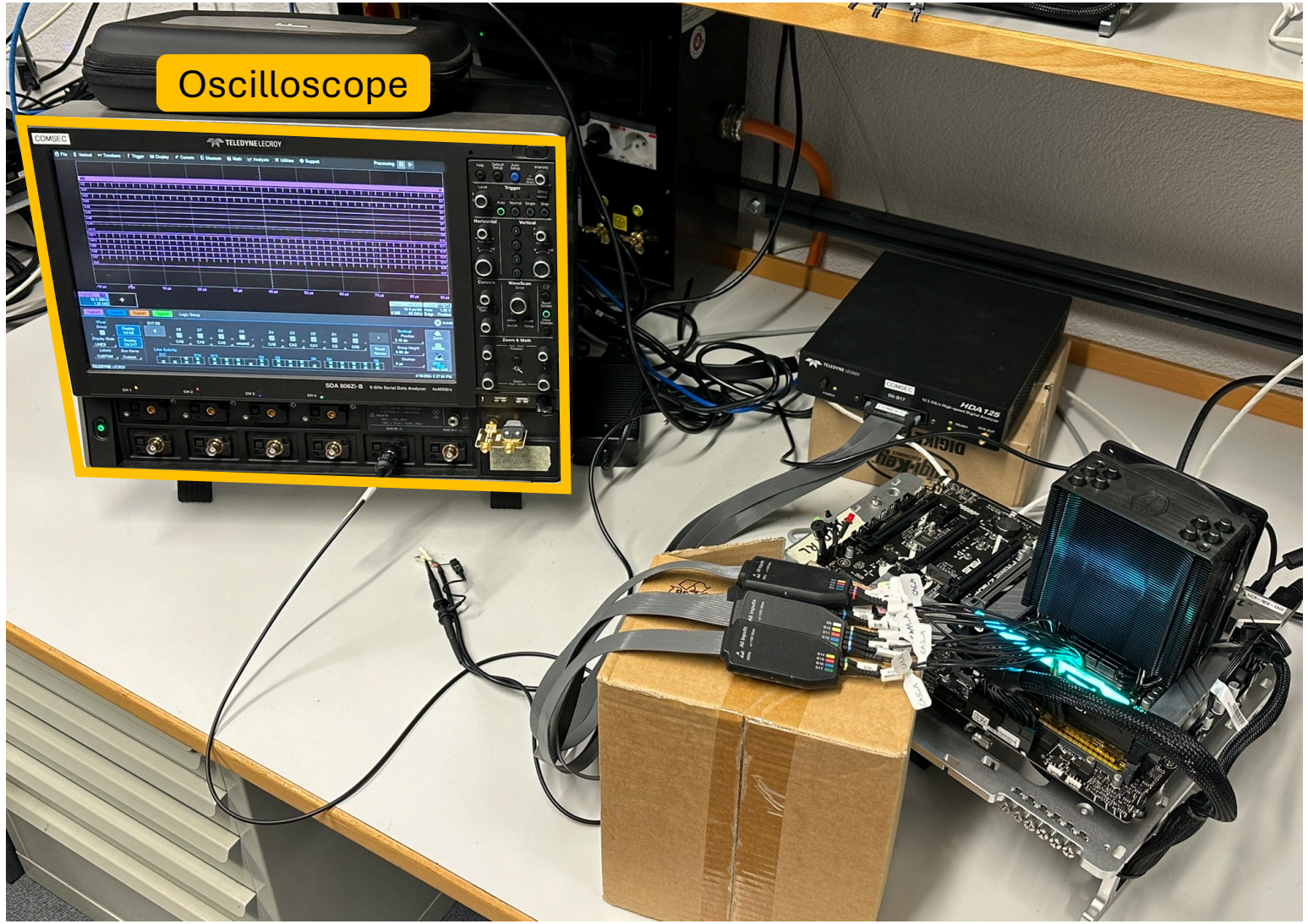
- Enables us to **observe** the DRAM **C/A bus** traffic.
- Supports **18 digital signals.**
- Powered by a custom data **processing pipeline**.

Our Solution: The McSee Platform



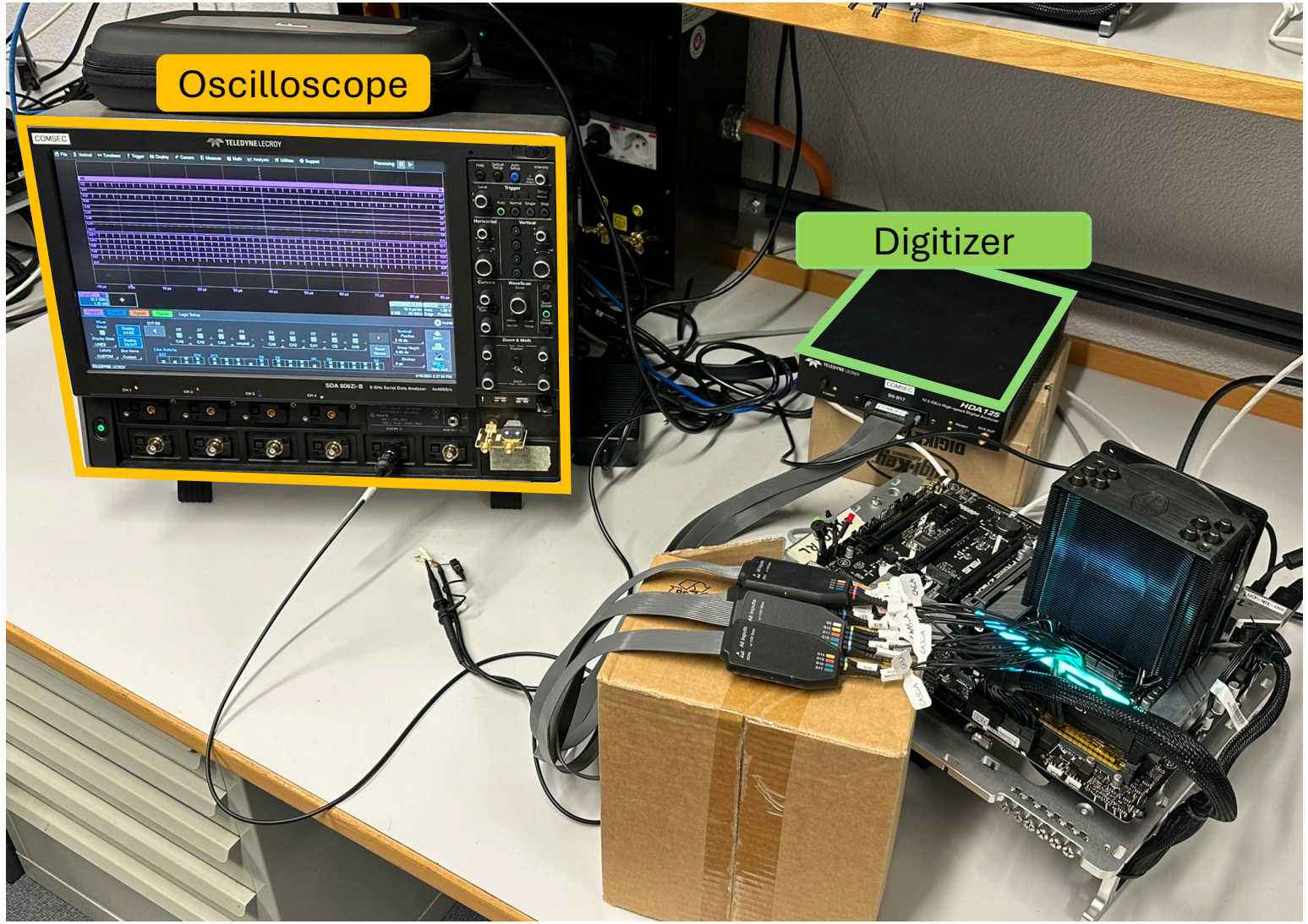
Component	Model TELEDYNE Name

Our Solution: The McSee Platform



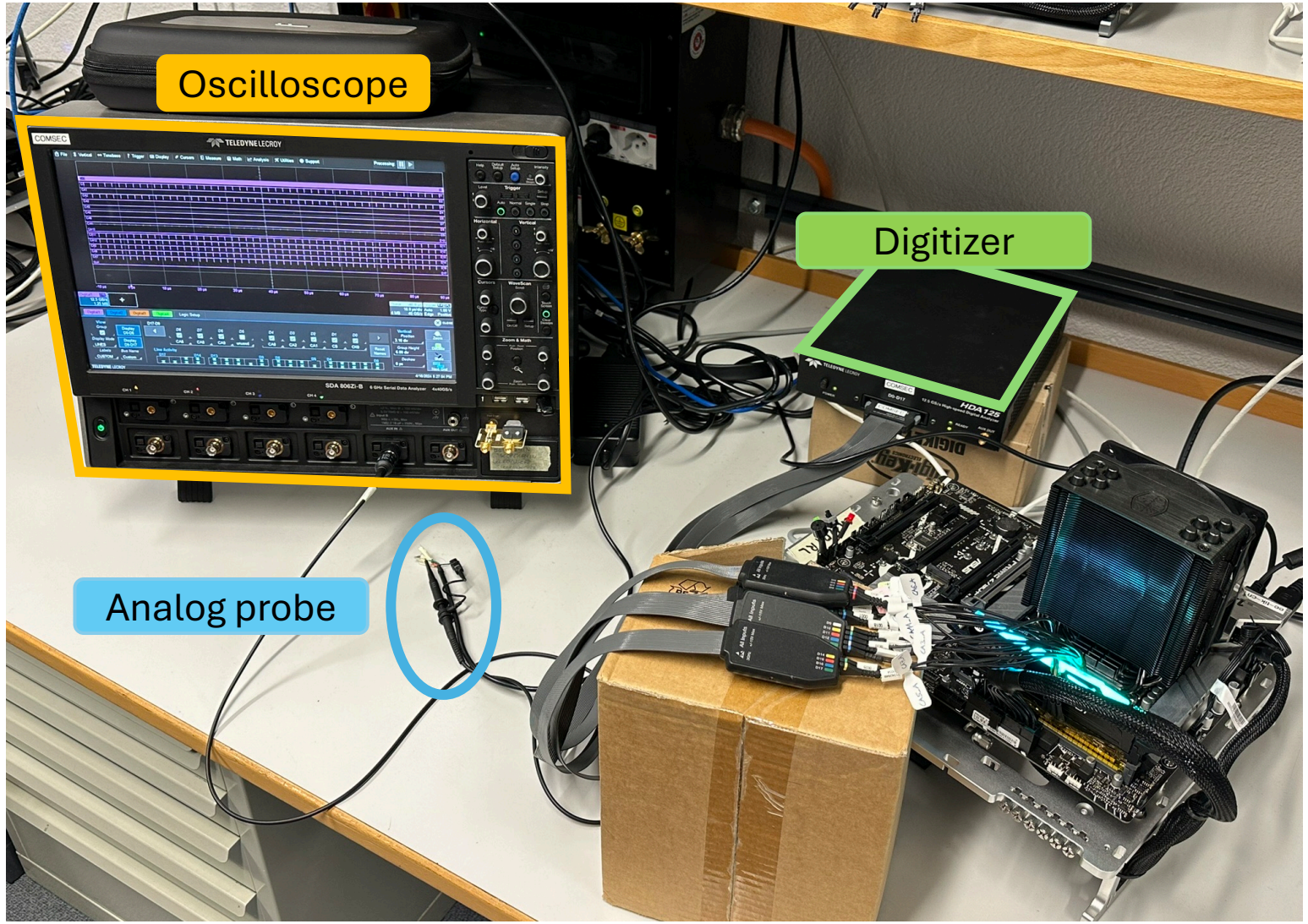
Component	Model TELEDYNE Name
Oscilloscope	SDA 806Zi-B

Our Solution: The McSee Platform



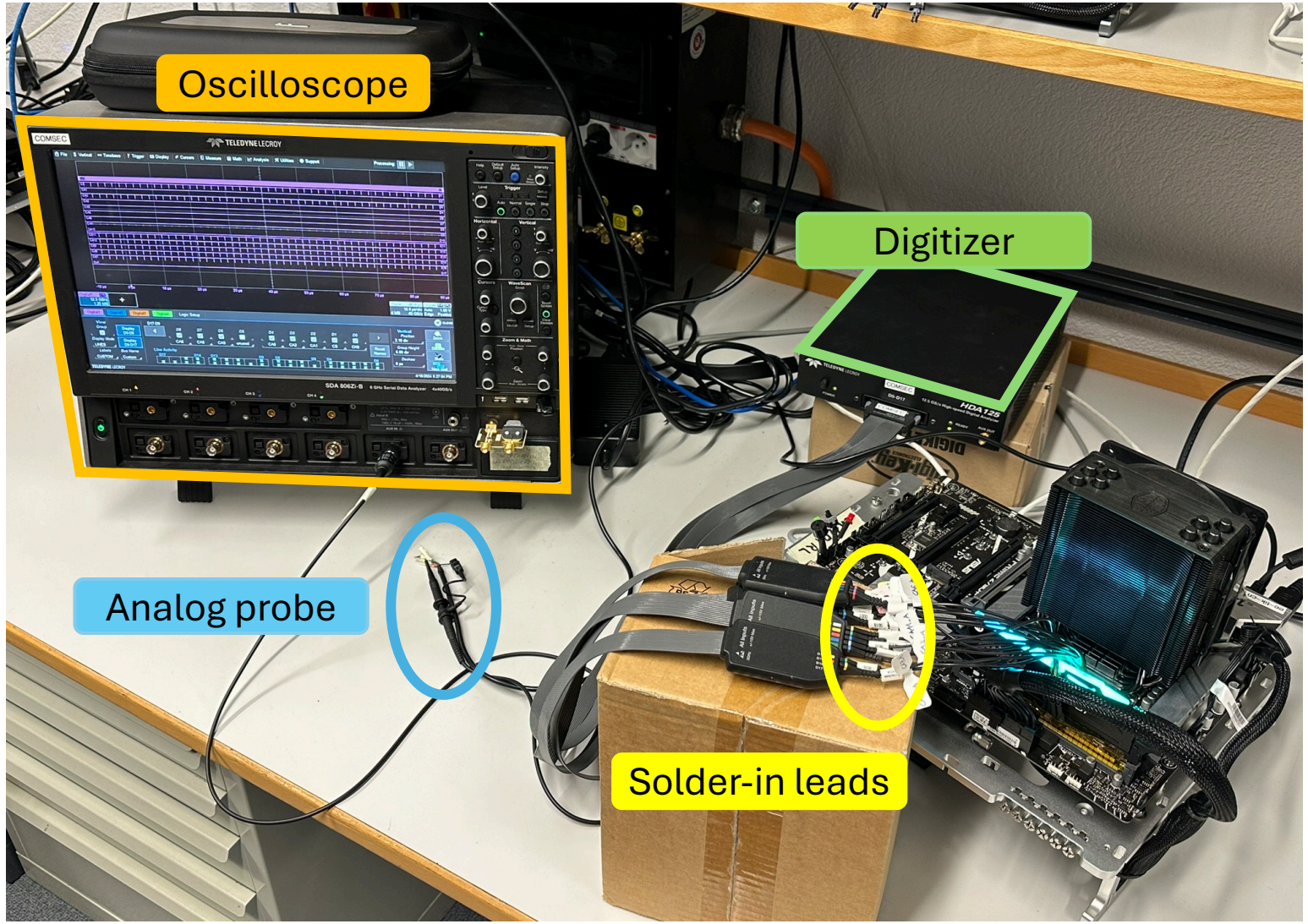
Component	Model TELEDYNE Name
Oscilloscope	SDA 806Zi-B
Digitizer	HDA125-18-LBUS

Our Solution: The McSee Platform



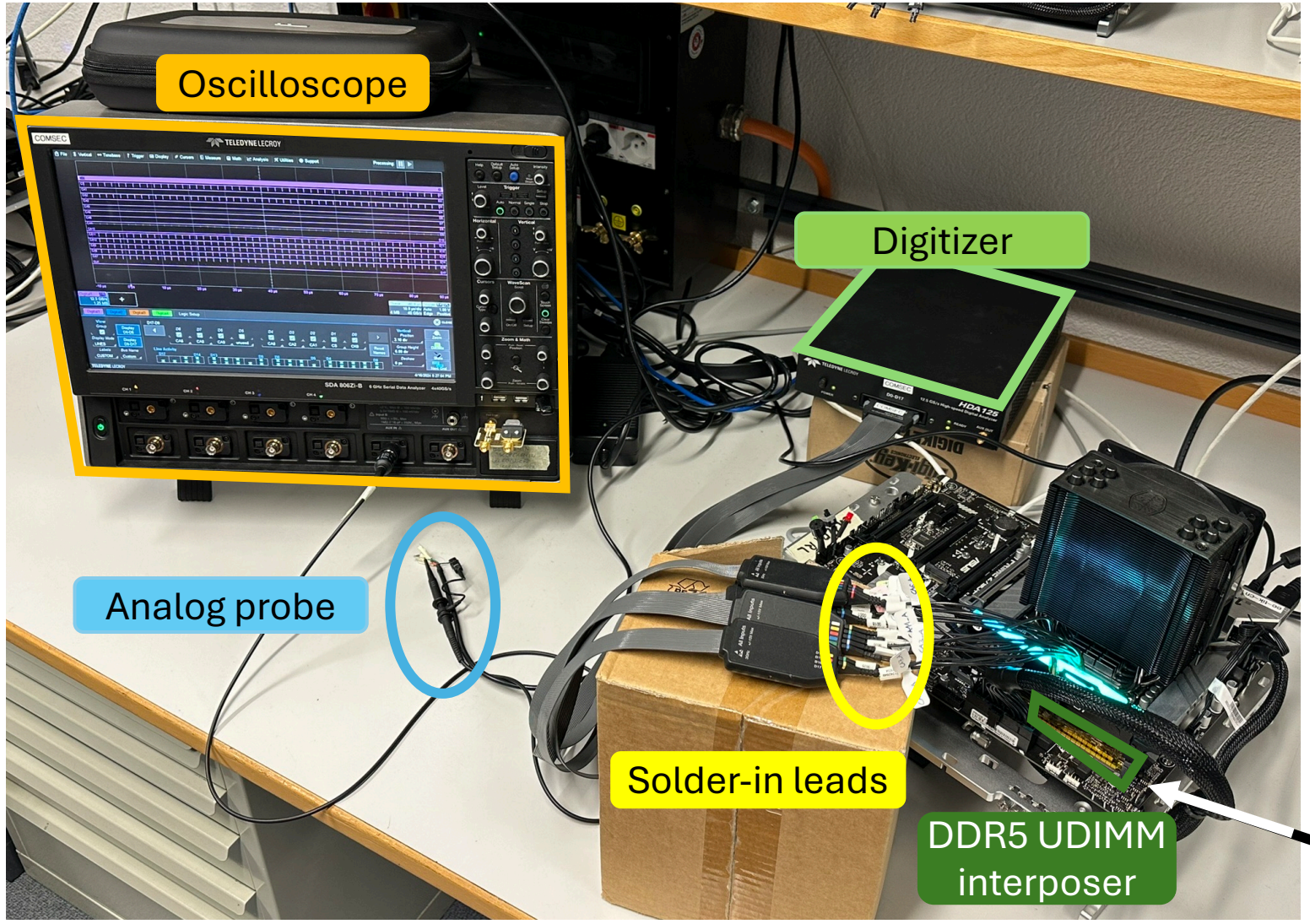
Component	Model TELEDYNE Name
Oscilloscope	SDA 806Zi-B
Digitizer	HDA125-18-LBUS
Analog probe	PP021

Our Solution: The McSee Platform

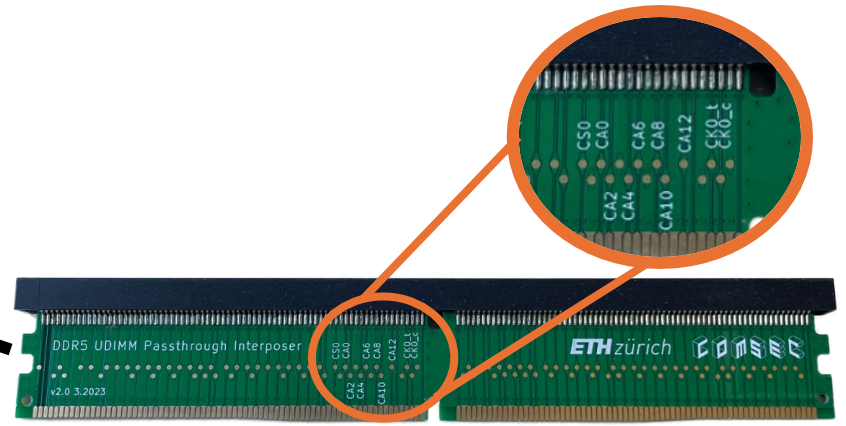


Component	Model TELEDYNE Name
Oscilloscope	SDA 806Zi-B
Digitizer	HDA125-18-LBUS
Analog probe	PP021
Solder-in leads	HAD-DLS-18QL

Our Solution: The McSee Platform

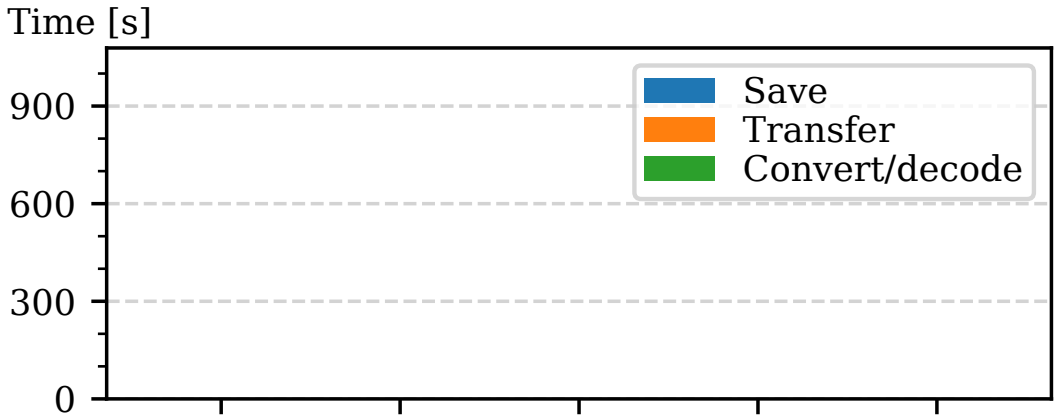


Component	Model TELEDYNE Name
Oscilloscope	SDA 806Zi-B
Digitizer	HDA125-18-LBUS
Analog probe	PP021
Solder-in leads	HAD-DLS-18QL
DDR5 UDIMM interposer	*n/a (custom PCB)*



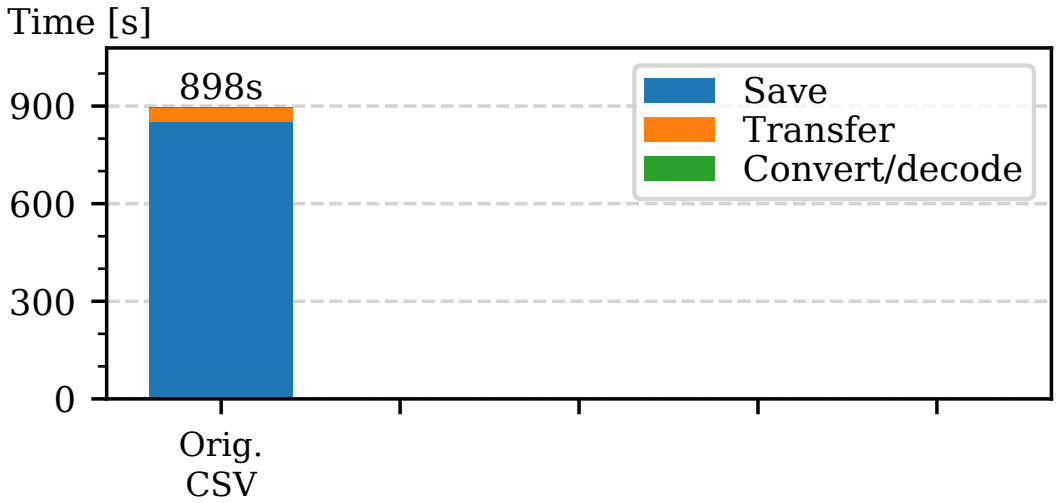
Optimizing McSee

Optimizing McSee



Optimizing McSee

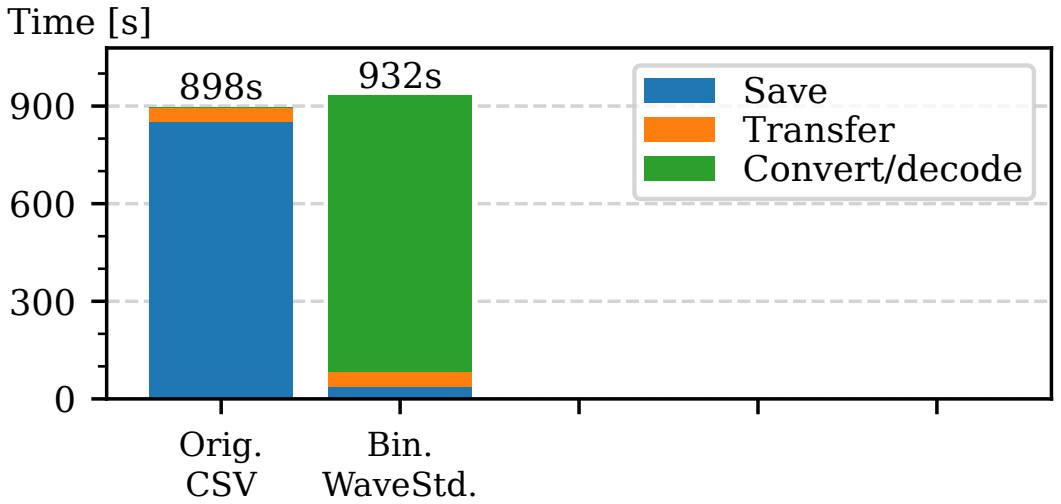
Baseline



Optimizing McSee

Baseline

Bin WaveStudio

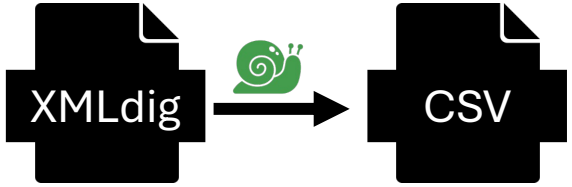


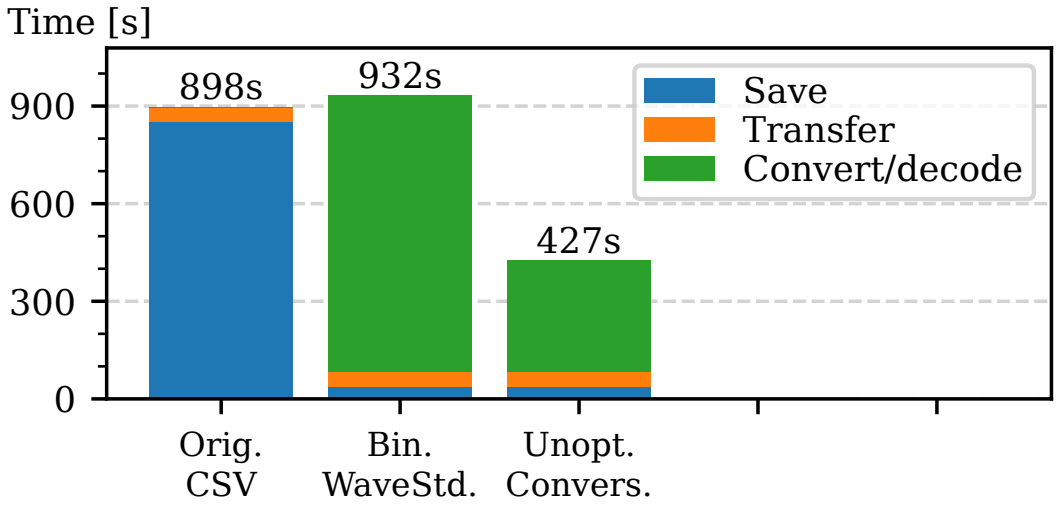
Optimizing McSee

Baseline

Bin WaveStudio

Unoptimized Custom Converter



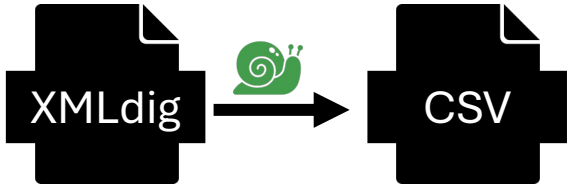


Optimizing McSee

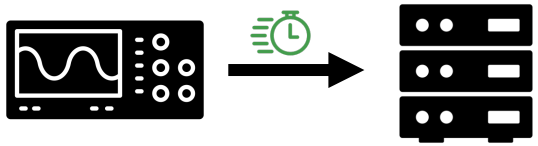
Baseline

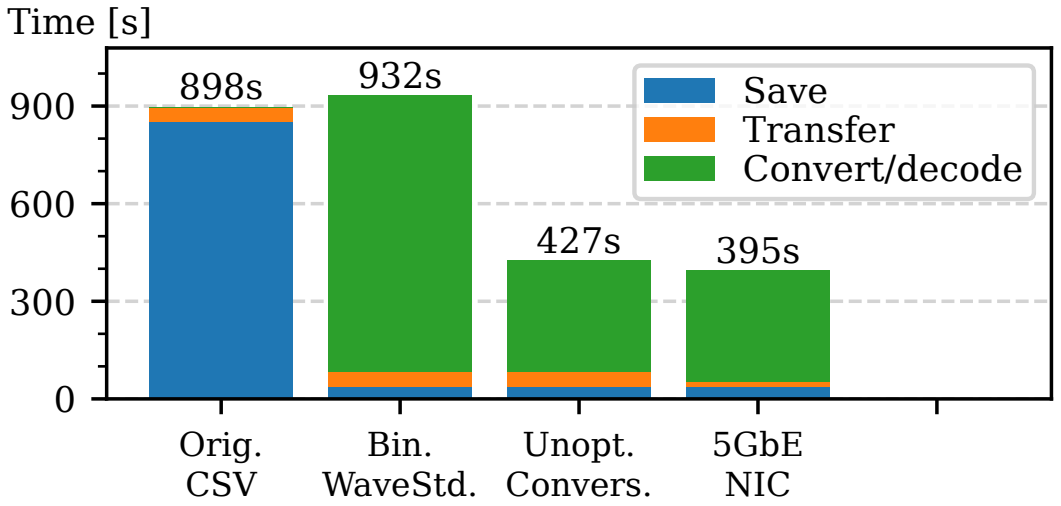
Bin WaveStudio

Unoptimized Custom Converter



5GbE NIC



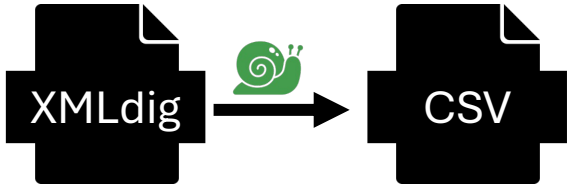


Optimizing McSee

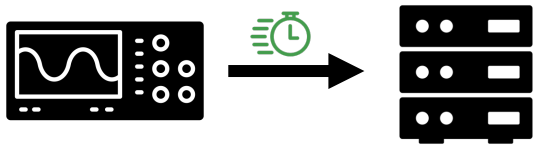
Baseline

Bin WaveStudio

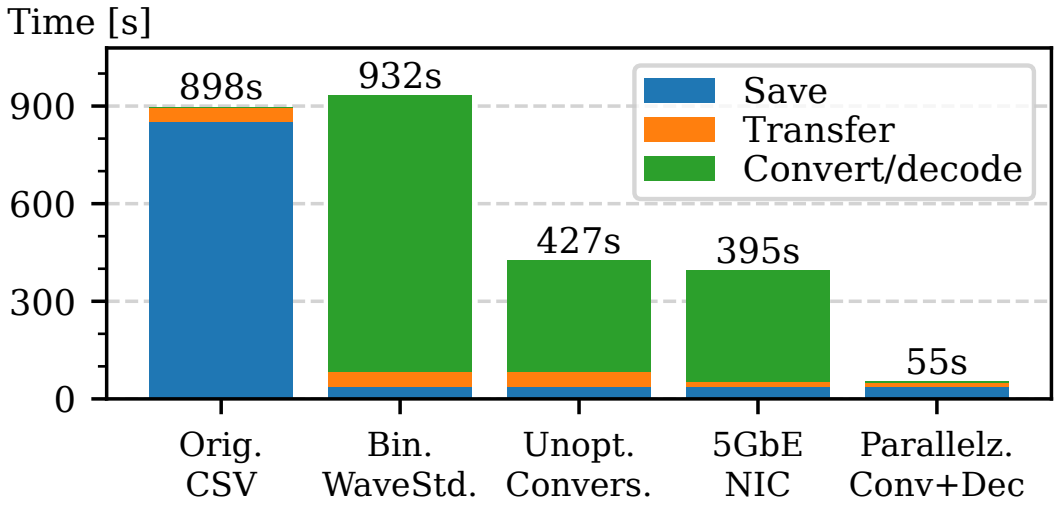
Unoptimized Custom Converter



5GbE NIC



Parallel Conversion & Decoding

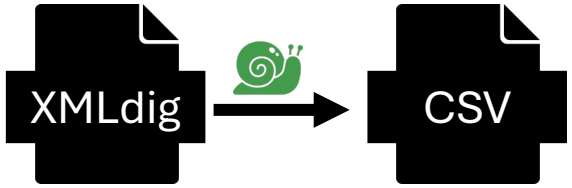


Optimizing McSee

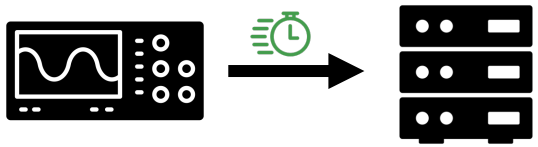
Baseline

Bin WaveStudio

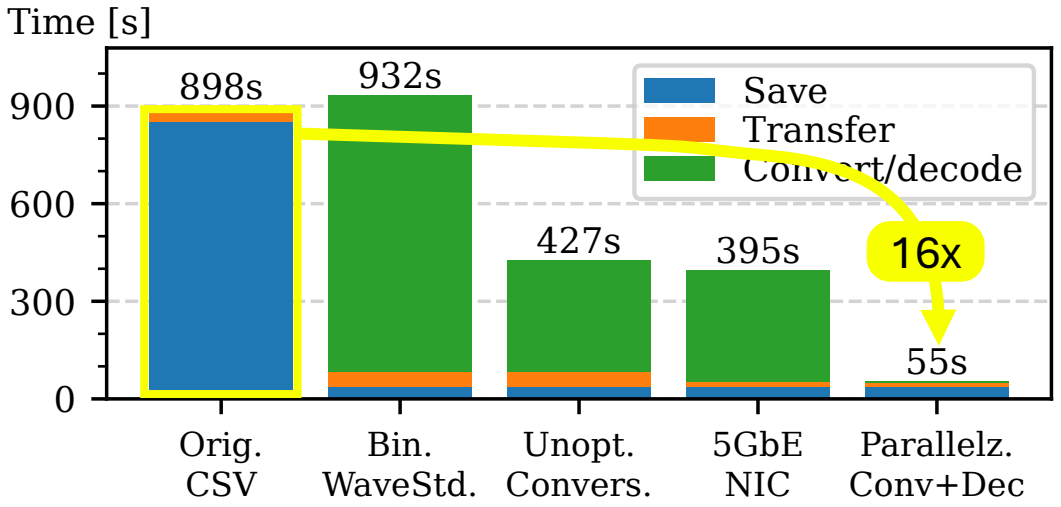
Unoptimized Custom Converter



5GbE NIC



Parallel Conversion & Decoding

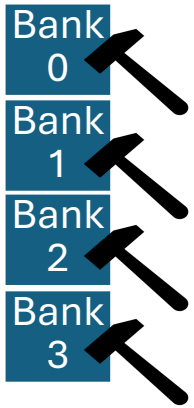


Optimizing the McSee data processing pipeline improved the processing time by 16x.

Analyzing Advanced DRAM Attacks

Analyzing Advanced DRAM Attacks

SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism

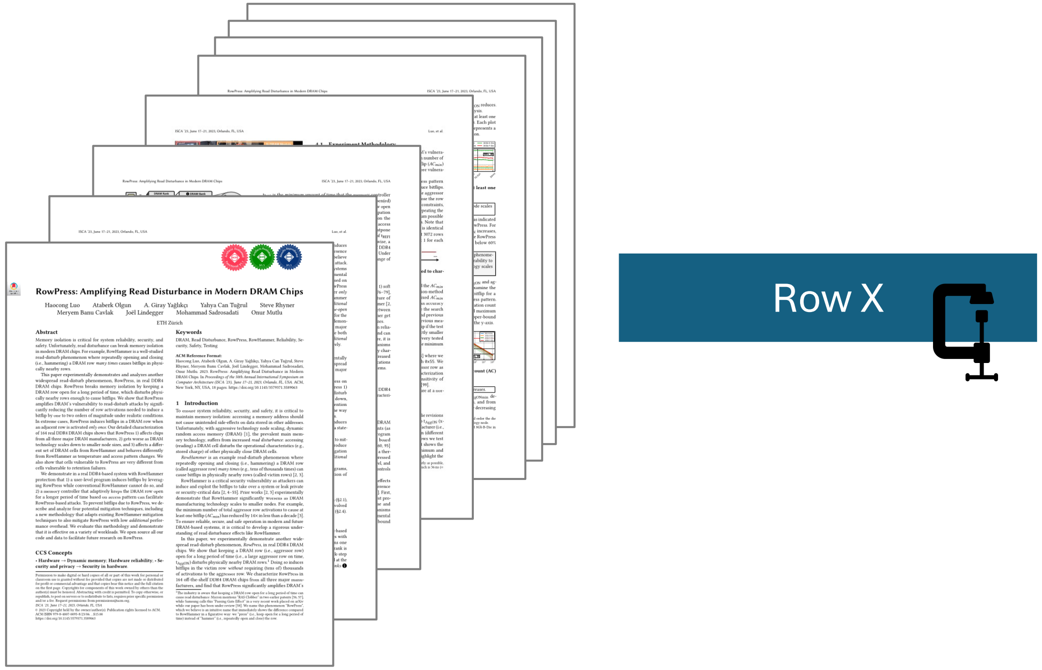


Sledgehammer

(USENIX Security ‘24)

Analyzing Advanced DRAM Attacks

Sledgehammer
(USENIX Security ‘24)

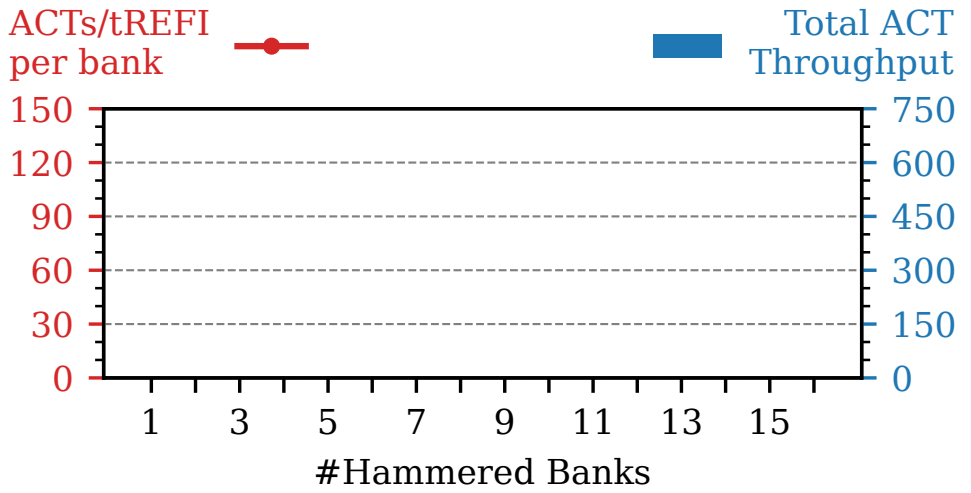


Rowpress
(ISCA ‘24)

Analzying Sledgehammer's ACT Throughput

EXPERIMENT

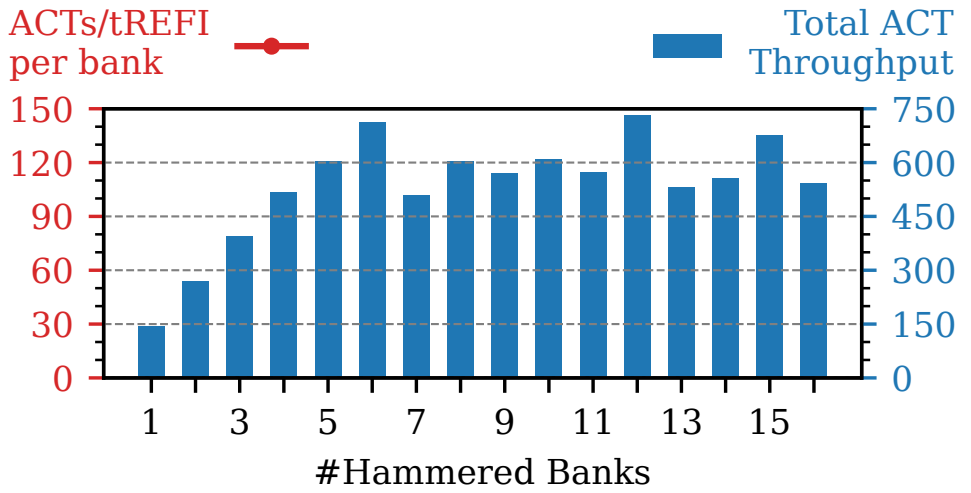
- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



Analzying Sledgehammer's ACT Throughput

EXPERIMENT

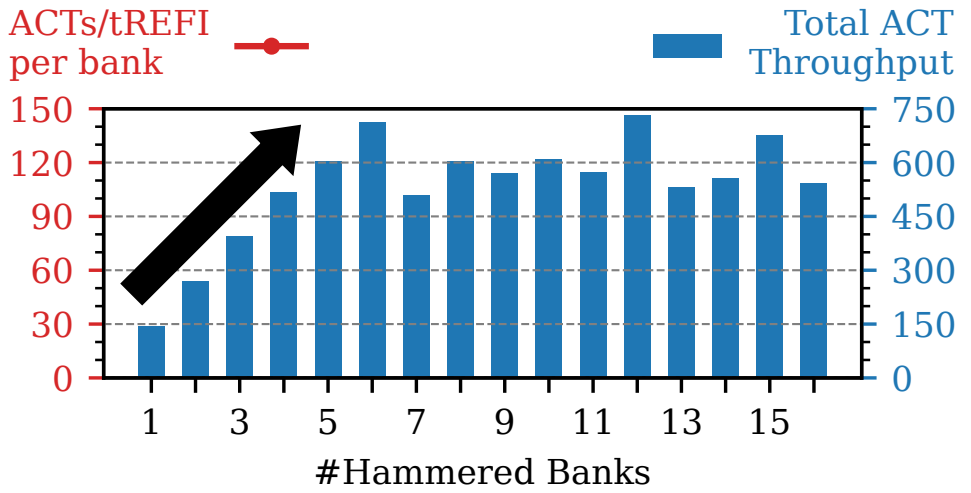
- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



Analzying Sledgehammer's ACT Throughput

EXPERIMENT

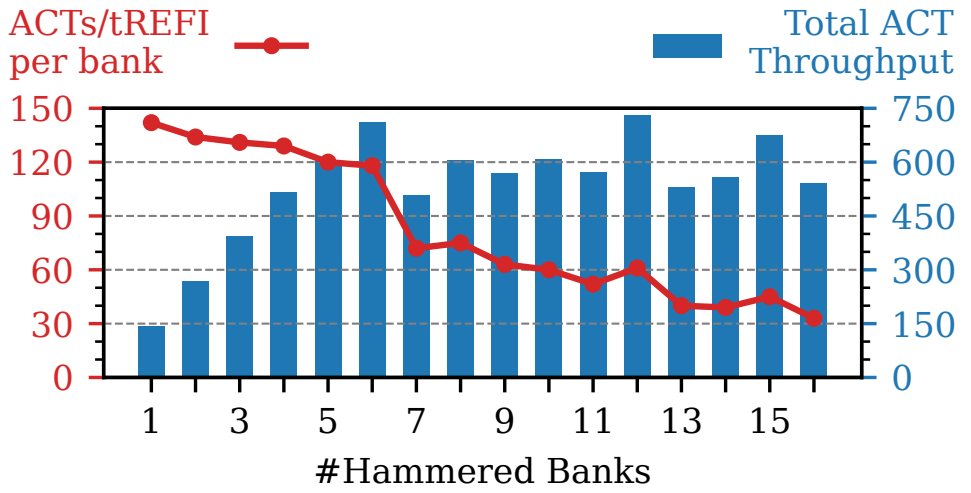
- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



Analzying Sledgehammer's ACT Throughput

EXPERIMENT

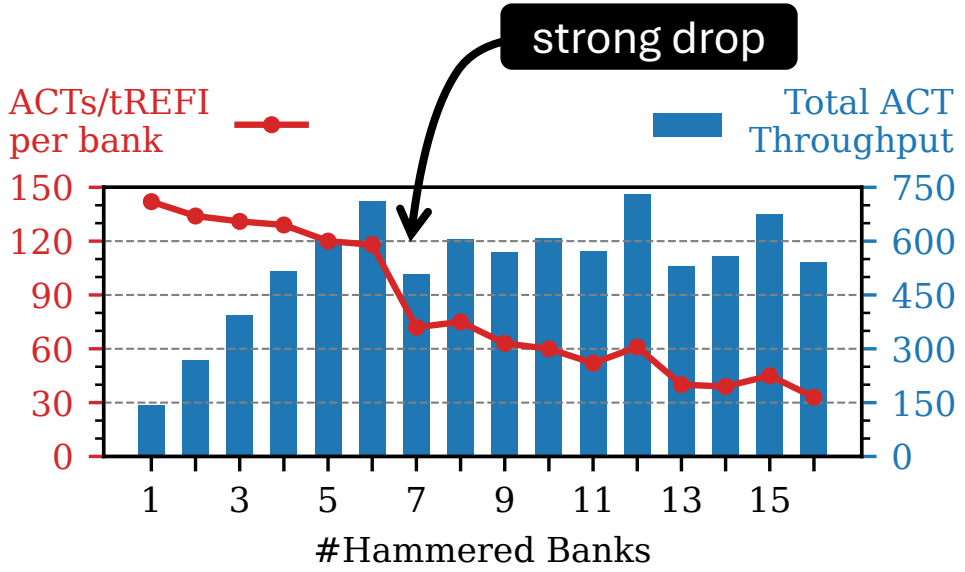
- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



Analzying Sledgehammer's ACT Throughput

EXPERIMENT

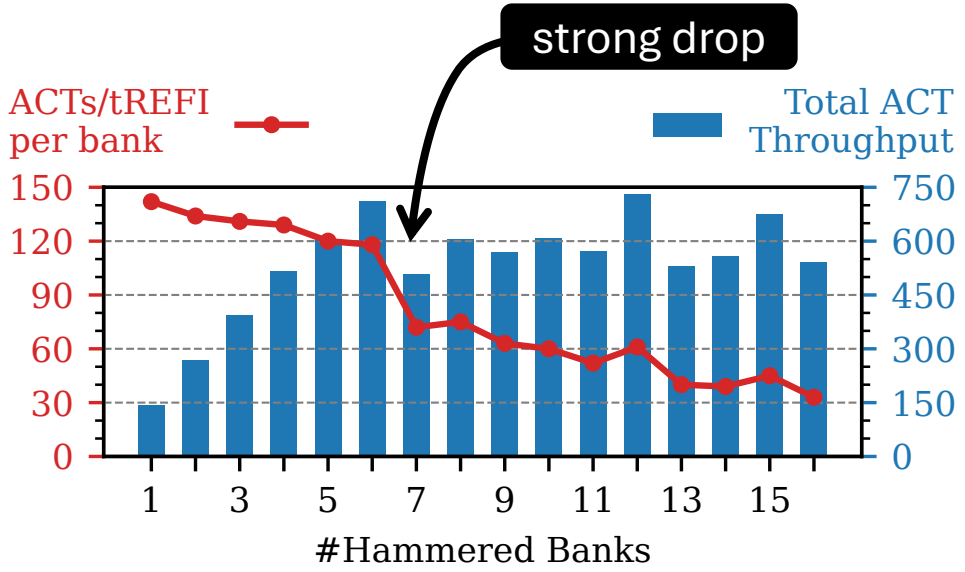
- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



Analzying Sledgehammer's ACT Throughput

EXPERIMENT

- Intel i7-8700K (Coffee Lake)
- Run Sledgehammer while hammering **1-16 banks** in parallel.
- Capture traces using McSee.



O1. Hammering more banks is beneficial for up to six banks, after which the per-bank ACT rate strongly declines.

Analzying Sledgehammer's ACT Reordering

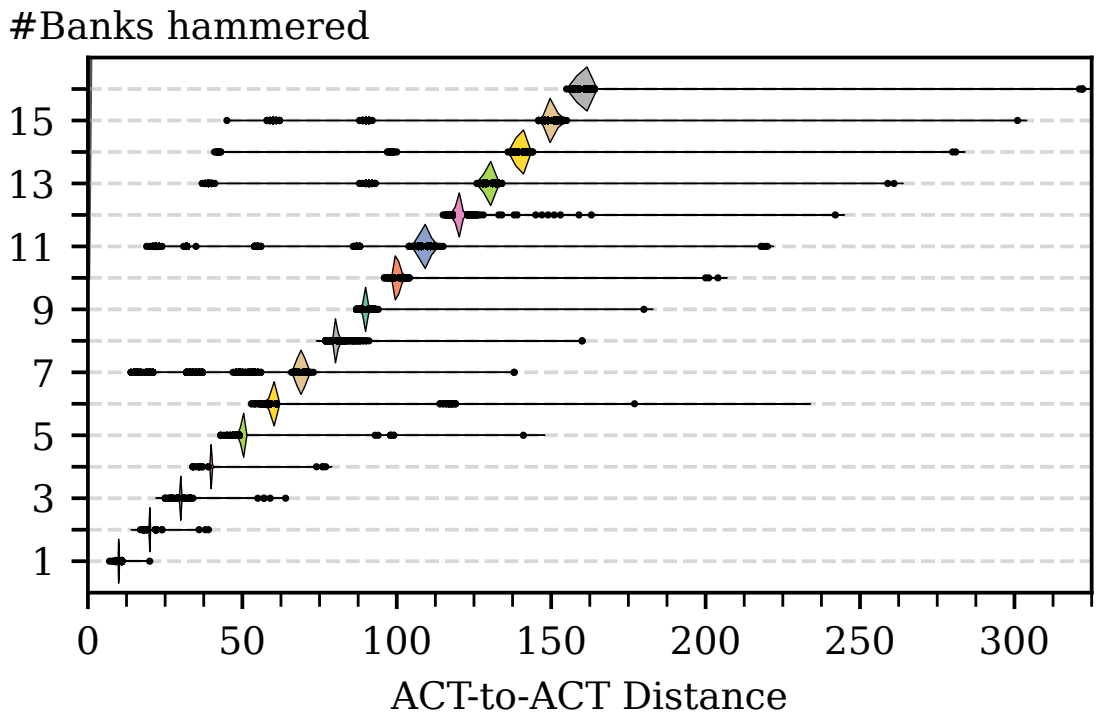
ANALYSIS

- Hypothesis: more banks hammered ⇒ less ACT reordering.
- Analyze the **ACT-to-ACT distance** of aggressor pairs.

Analzying Sledgehammer's ACT Reordering

ANALYSIS

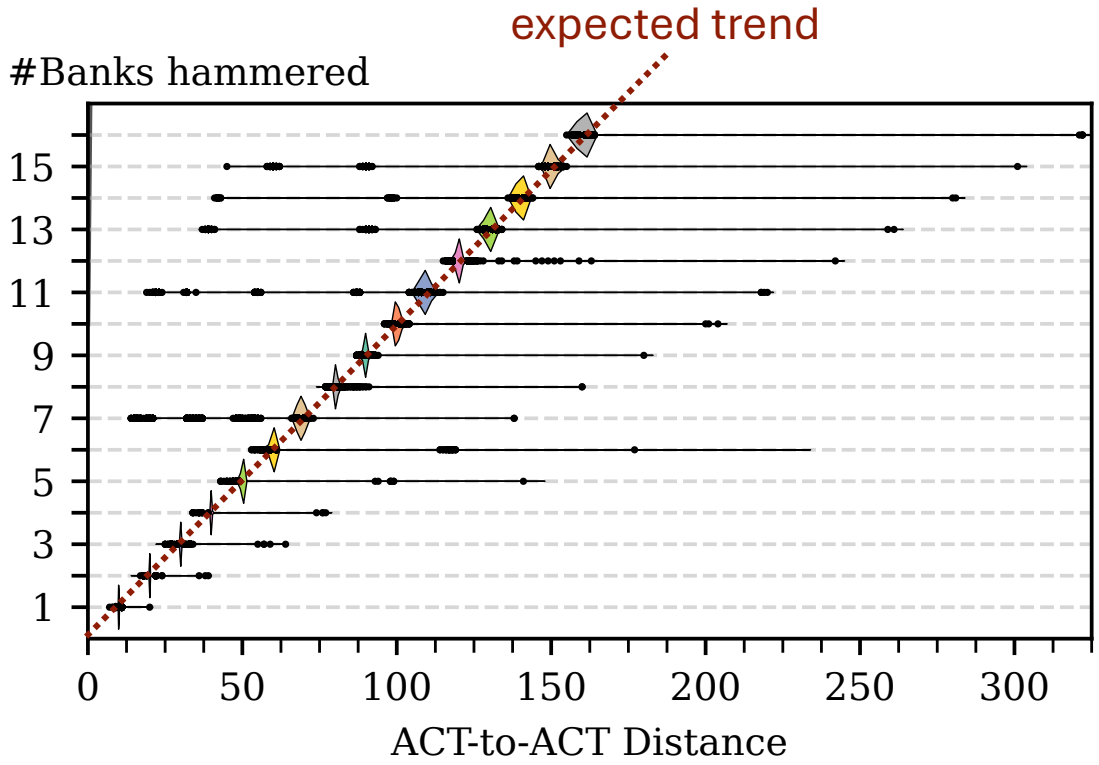
- Hypothesis: more banks hammered ⇒ less ACT reordering.
- Analyze the **ACT-to-ACT distance** of aggressor pairs.



Analzying Sledgehammer's ACT Reordering

ANALYSIS

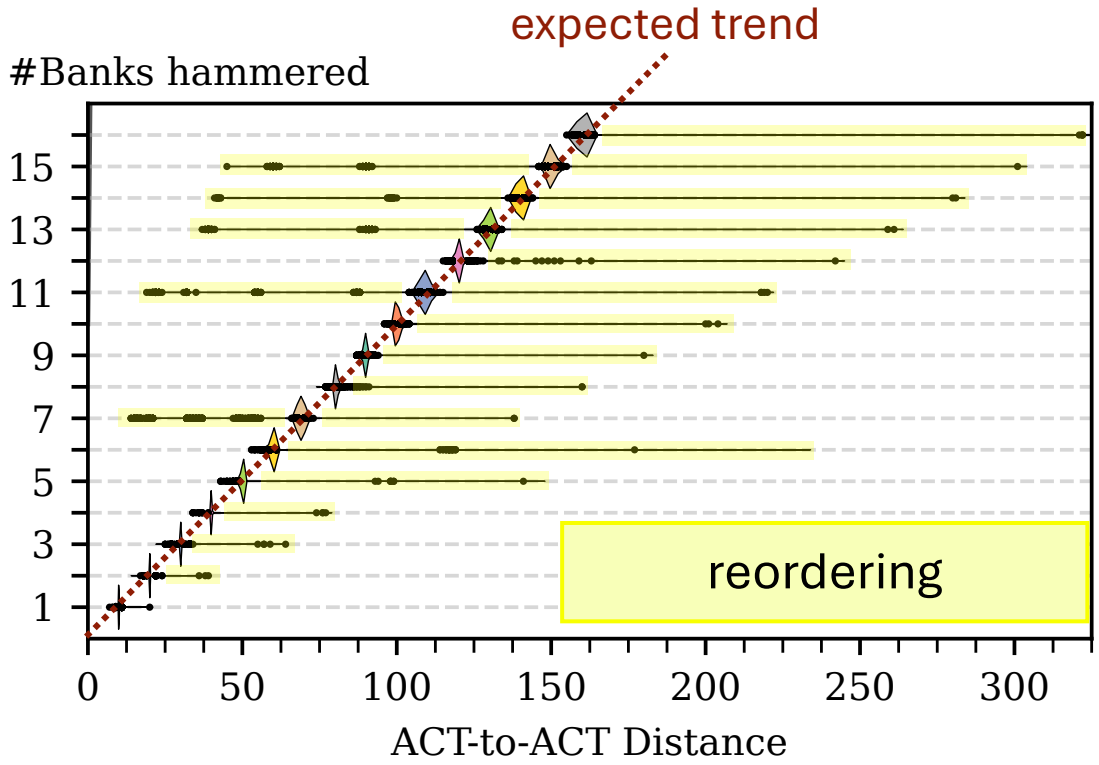
- Hypothesis: more banks hammered ⇒ less ACT reordering.
- Analyze the **ACT-to-ACT distance** of aggressor pairs.



Analzying Sledgehammer's ACT Reordering

ANALYSIS

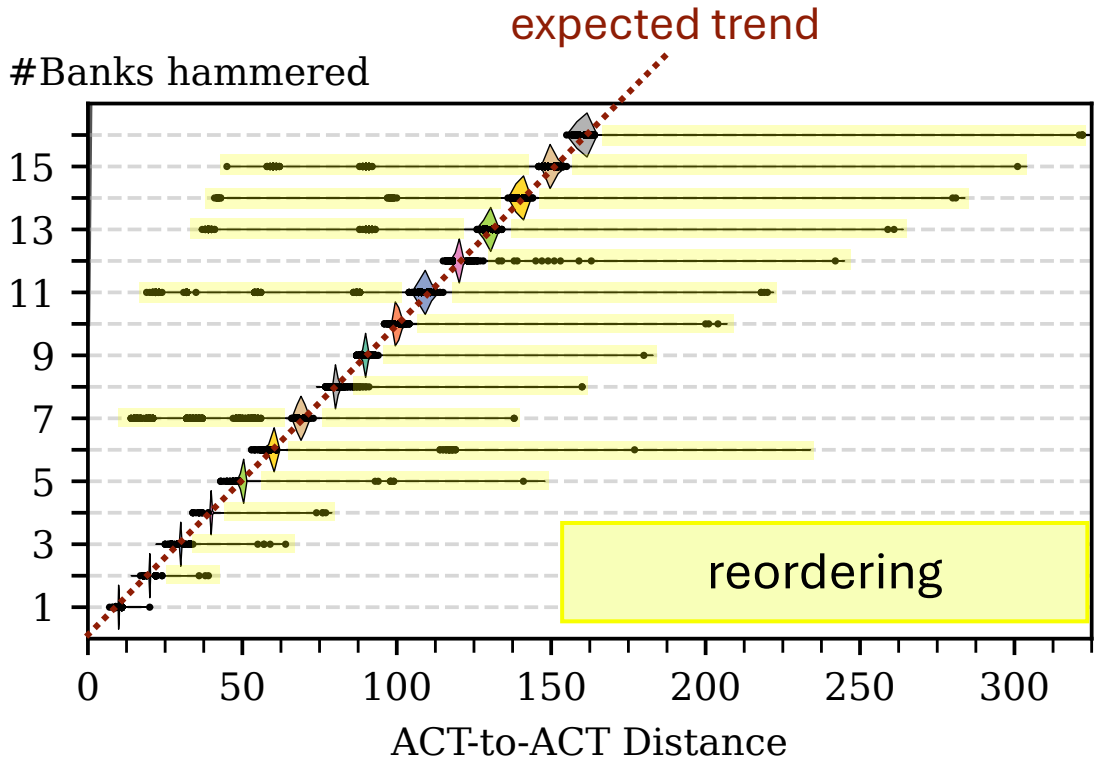
- Hypothesis: more banks hammered ⇒ less ACT reordering.
- Analyze the **ACT-to-ACT distance** of aggressor pairs.



Analzying Sledgehammer's ACT Reordering

ANALYSIS

- Hypothesis: more banks hammered ⇒ less ACT reordering.
- Analyze the **ACT-to-ACT distance** of aggressor pairs.



O2. Increasing the number of hammered banks from one to seven causes, on average, 6.7x more reordering of ACTs.

Analzying Rowpress' Row-Open Time

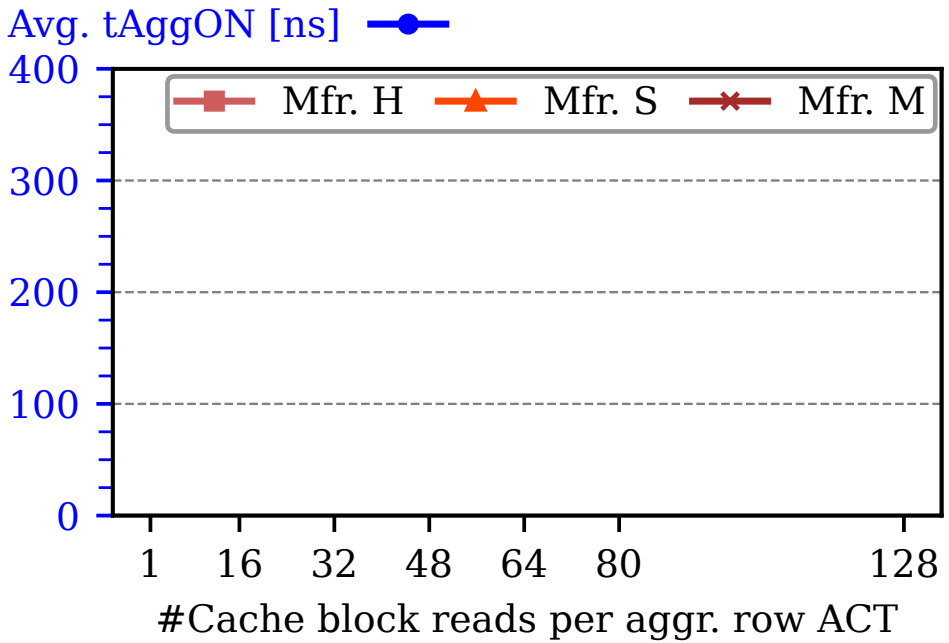
EXPERIMENT

- Intel i7-8700K (Coffee Lake) with same DIMM as org. work.
- Original results reproduced.
- Capture traces while fixing #cache block reads.

Analzying Rowpress' Row-Open Time

EXPERIMENT

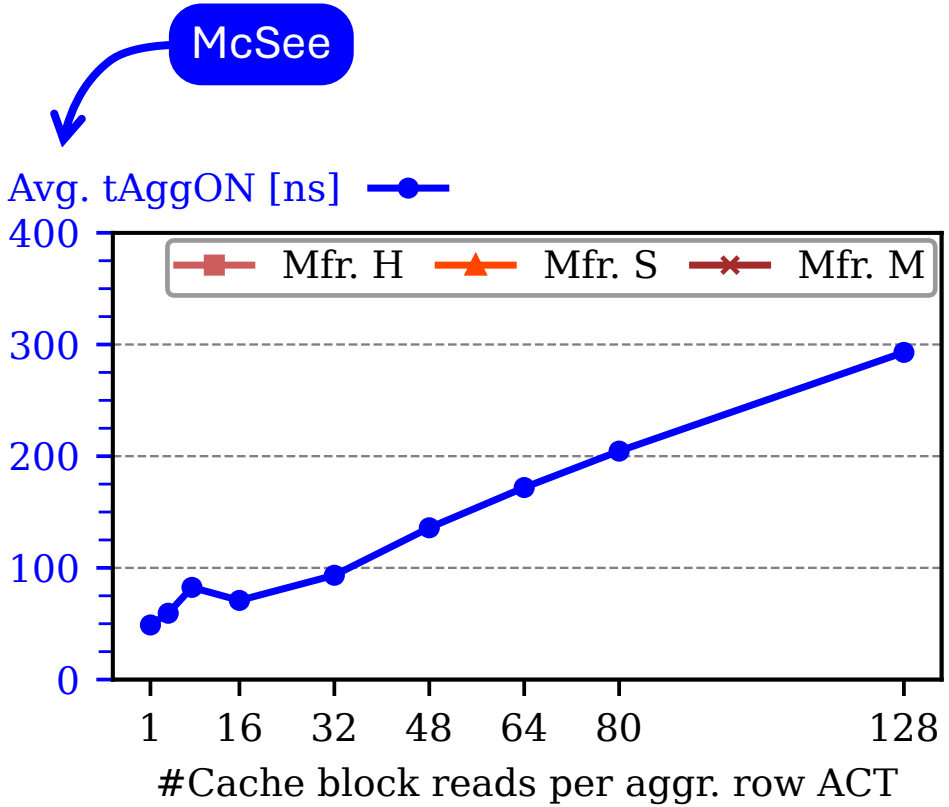
- Intel i7-8700K (Coffee Lake) with same DIMM as org. work.
- Original results reproduced.
- Capture traces while fixing #cache block reads.



Analzying Rowpress' Row-Open Time

EXPERIMENT

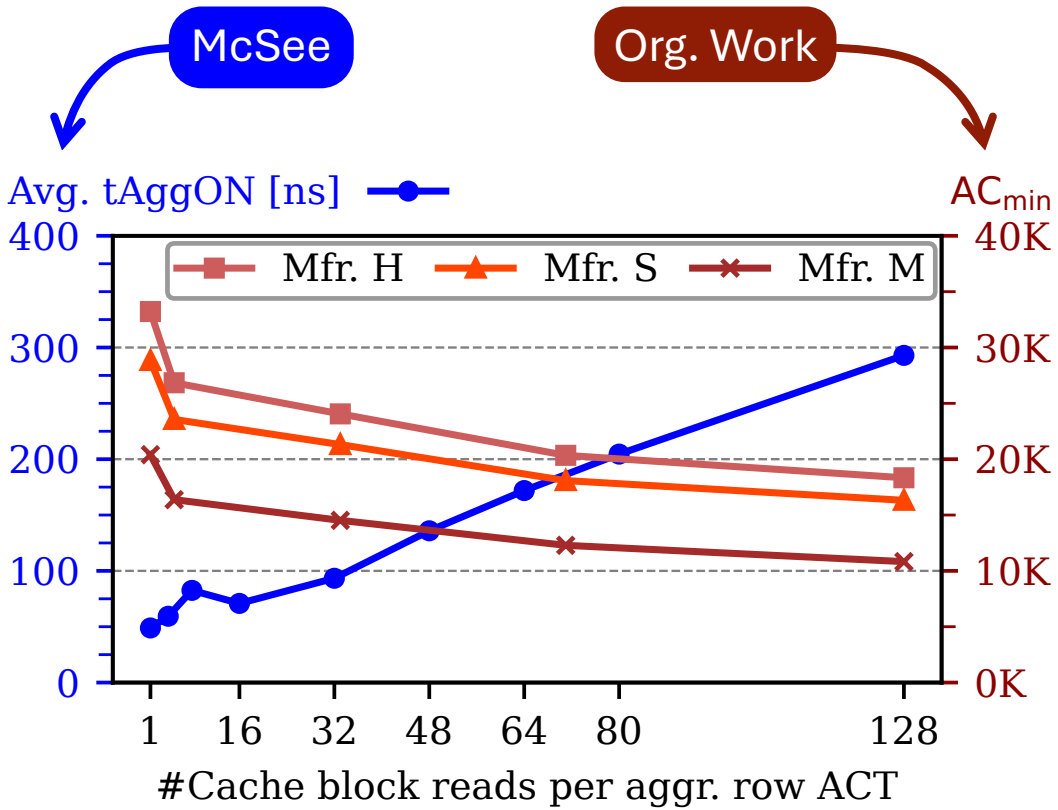
- Intel i7-8700K (Coffee Lake) with same DIMM as org. work.
- Original results reproduced.
- Capture traces while fixing #cache block reads.



Analzying Rowpress' Row-Open Time

EXPERIMENT

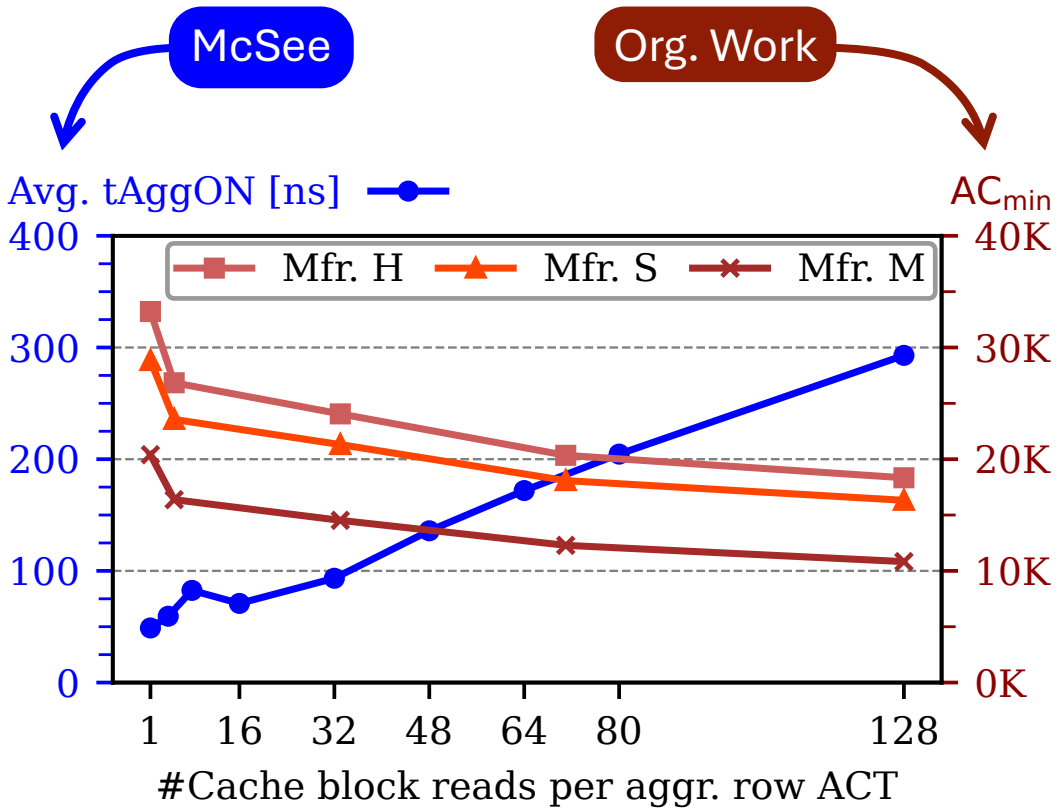
- Intel i7-8700K (Coffee Lake) with same DIMM as org. work.
- Original results reproduced.
- Capture traces while fixing #cache block reads.



Analzying Rowpress' Row-Open Time

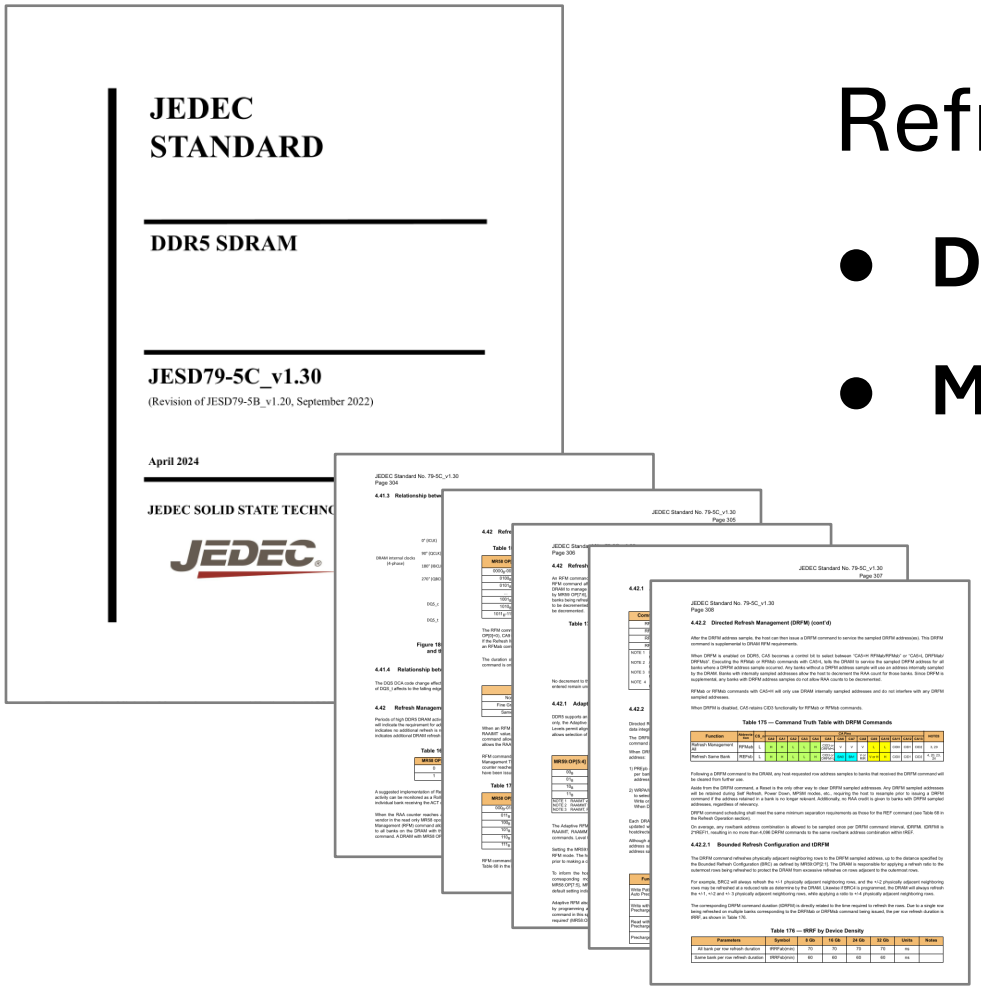
EXPERIMENT

- Intel i7-8700K (Coffee Lake) with same DIMM as org. work.
- Original results reproduced.
- Capture traces while fixing #cache block reads.



O3. Rowpress' ability to reduce ACmin on commodity systems is significantly lower (2x) than for the most effective pattern (17.6x) in the original work.

Analyzing Rowhammer Defenses



Refresh Management (RFM)

- **DIMM's SPD**: RFM values
- **Memory Controller**: RFM commands

RFM Values

ID	Mf. Date [yy-mm]	Size [GiB]	Wd. [bits]	Geom. #[RK,BK,BA,R]
M1	22-05	16	x8	1,8,4,16
M2	22-08	16	x8	1,8,4,16
M3	22-01	16	x8	1,8,4,16
M4	21-10	16	x8	1,8,4,16
see the results for M5-M11 in the paper				
H1	22-01	8	x16	1,4,4,16
H2	22-12	8	x16	1,4,4,16
H3	22-07	16	x8	1,8,4,16
see the results for H4-H10 in the paper				
H11	21-12	8	X16	1,4,4,16
S1	22-02	8	x16	1,4,4,16
S2	21-12	8	x16	1,4,4,16
S3	22-01	16	x8	1,8,4,16
S4	21-10	16	x8	1,8,4,16
see the results for S5-S7 in the paper				
U1	22-05	8	x16	1,4,4,16

RFM Values

- Custom **DDR5 SPD decoder** to read RFM values:
  - RFM Required
  - RAAIMT
  - RAAMMT

ID	Mf. Date [yy-mm]	Size [GiB]	Wd. [bits]	Geom. #[RK,BK,BA,R]
M1	22-05	16	x8	1,8,4,16
M2	22-08	16	x8	1,8,4,16
M3	22-01	16	x8	1,8,4,16
M4	21-10	16	x8	1,8,4,16
see the results for M5-M11 in the paper				
H1	22-01	8	x16	1,4,4,16
H2	22-12	8	x16	1,4,4,16
H3	22-07	16	x8	1,8,4,16
see the results for H4-H10 in the paper				
H11	21-12	8	X16	1,4,4,16
S1	22-02	8	x16	1,4,4,16
S2	21-12	8	x16	1,4,4,16
S3	22-01	16	x8	1,8,4,16
S4	21-10	16	x8	1,8,4,16
see the results for S5-S7 in the paper				
U1	22-05	8	x16	1,4,4,16

RFM Values

- Custom **DDR5 SPD decoder** to read RFM values:
  - RFM Required
  - RAAIMT
  - RAAMMT

ID	Mf. Date [yy-mm]	Size [GiB]	Wd. [bits]	Geom. #[RK,BK,BA,R]	RFM [REQ, RAAIMT/-MMT]
M1	22-05	16	x8	1,8,4,16	0, 80, 6x
M2	22-08	16	x8	1,8,4,16	0, RFU, RFU
M3	22-01	16	x8	1,8,4,16	0, 80, 6x
M4	21-10	16	x8	1,8,4,16	0, 80, 4x
see the results for M5-M11 in the paper					
H1	22-01	8	x16	1,4,4,16	0, RFU, RFU
H2	22-12	8	x16	1,4,4,16	0, 80, 6x
H3	22-07	16	x8	1,8,4,16	0, 80, 6x
see the results for H4-H10 in the paper					
H11	21-12	8	X16	1,4,4,16	**1**, 56, 3x
S1	22-02	8	x16	1,4,4,16	0, 80, 6x
S2	21-12	8	x16	1,4,4,16	0, RFU, RFU
S3	22-01	16	x8	1,8,4,16	0, RFU, RFU
S4	21-10	16	x8	1,8,4,16	0, RFU, RFU
see the results for S5-S7 in the paper					
U1	22-05	8	x16	1,4,4,16	0, 80, 6x

RFM Values

- Custom **DDR5 SPD decoder** to read RFM values:
  - RFM Required
  - RAAIMT
  - RAAMMT

O5. The majority DDR5 devices report valid RFM values, but only one DIMM requires RFM.

ID	Mf. Date [yy-mm]	Size [GiB]	Wd. [bits]	Geom. #[RK,BK,BA,R]	RFM [REQ, RAAIMT/-MMT]
M1	22-05	16	x8	1,8,4,16	0, 80, 6x
M2	22-08	16	x8	1,8,4,16	0, RFU, RFU
M3	22-01	16	x8	1,8,4,16	0, 80, 6x
M4	21-10	16	x8	1,8,4,16	0, 80, 4x
see the results for M5-M11 in the paper					
H1	22-01	8	x16	1,4,4,16	0, RFU, RFU
H2	22-12	8	x16	1,4,4,16	0, 80, 6x
H3	22-07	16	x8	1,8,4,16	0, 80, 6x
see the results for H4-H10 in the paper					
H11	21-12	8	X16	1,4,4,16	**1**, 56, 3x ⚠
S1	22-02	8	x16	1,4,4,16	0, 80, 6x
S2	21-12	8	x16	1,4,4,16	0, RFU, RFU
S3	22-01	16	x8	1,8,4,16	0, RFU, RFU
S4	21-10	16	x8	1,8,4,16	0, RFU, RFU
see the results for S5-S7 in the paper					
U1	22-05	8	x16	1,4,4,16	0, 80, 6x

DDR5 Systems

	Microarchitecture	Release Date	Model
★	Intel **Alder Lake** (AL)	Nov. 2021	i7-12700K
	Intel **Raptor Lake** (RL)	Oct. 2022	i7-13700K
★	AMD **Zen 4** (Z4)	Sept. 2022	R7 7700X

★ First Intel and AMD CPUs with DDR5 support.

RFM in DDR5 Memory Controllers

EXPERIMENT

- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)

RFM in DDR5 Memory Controllers

EXPERIMENT

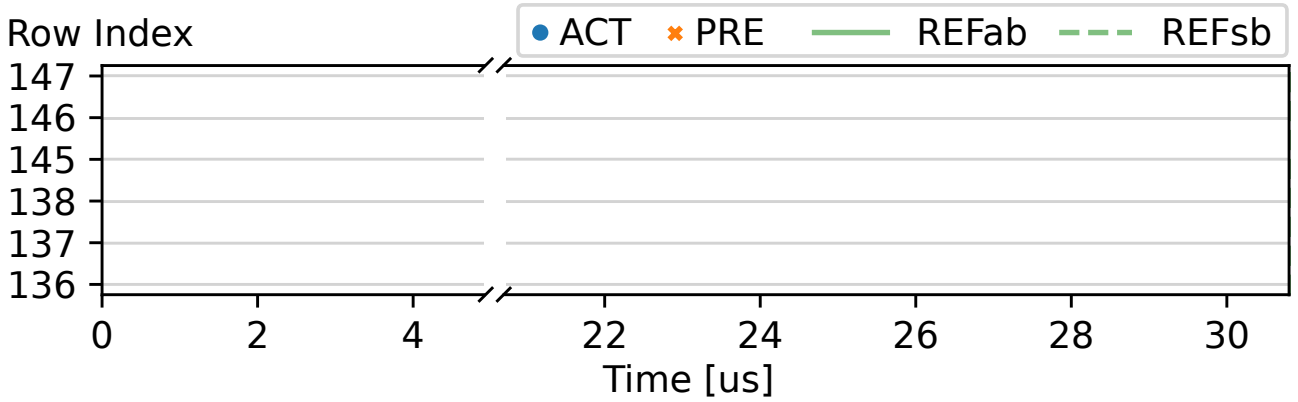
- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)

O7. Intel Alder/Raptor Lake and AMD Zen 4 do not issue RFMs.

RFM in DDR5 Memory Controllers

EXPERIMENT

- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)

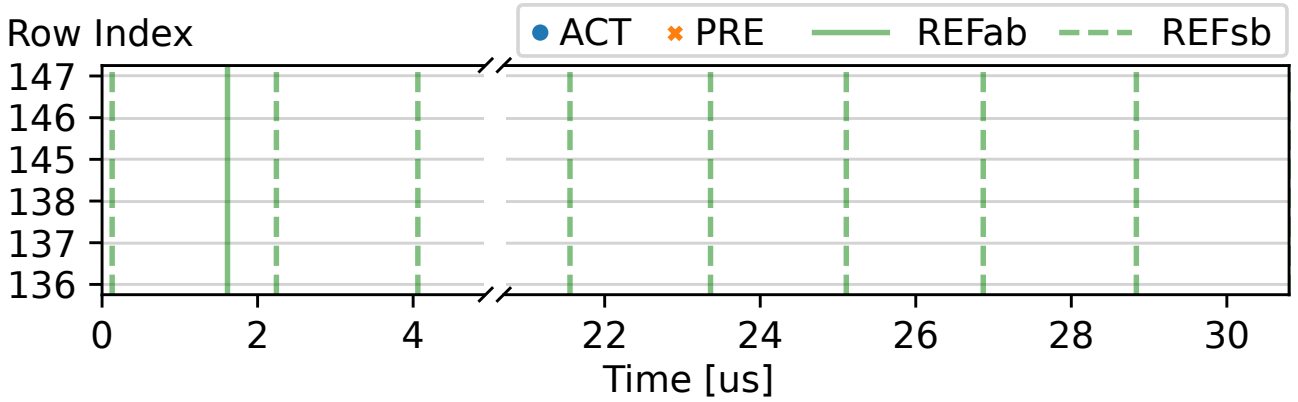


O7. Intel Alder/Raptor Lake and AMD Zen 4 do not issue RFMs.

RFM in DDR5 Memory Controllers

EXPERIMENT

- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)



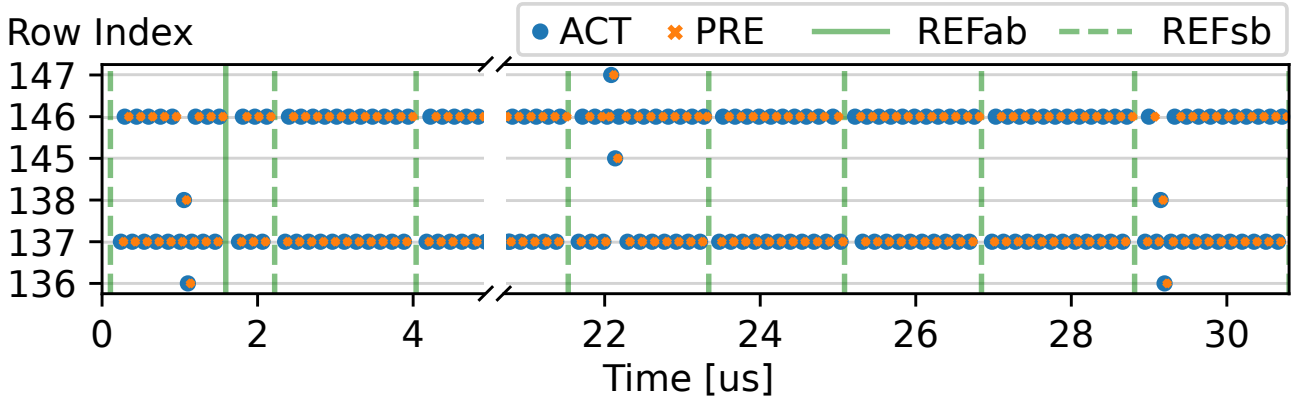
O7. Intel Alder/Raptor Lake and AMD Zen 4 do not issue RFMs.

O8. Intel Alder/Raptor Lake use FGR mode by default.
AMD Zen 4 systems do not use FGR mode.

RFM in DDR5 Memory Controllers

EXPERIMENT

- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)



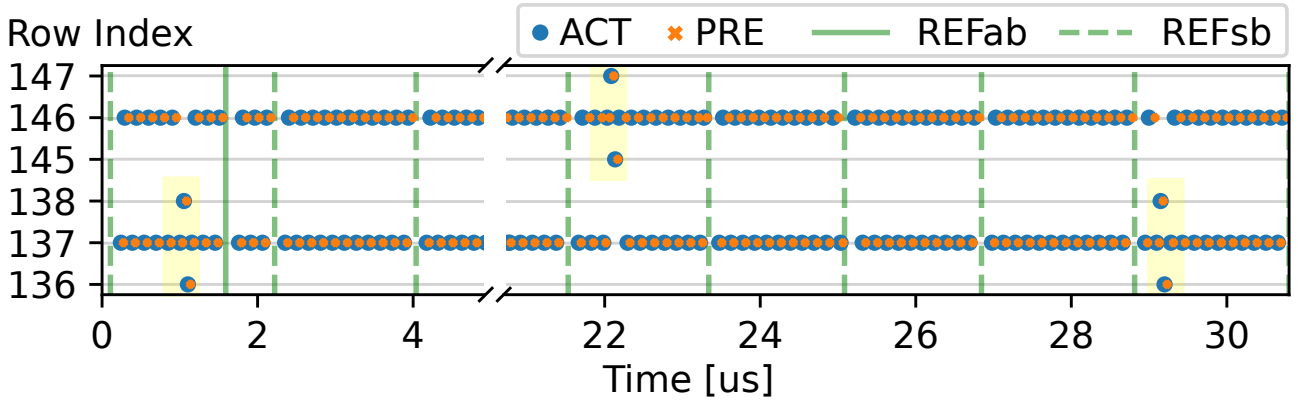
O7. Intel Alder/Raptor Lake and AMD Zen 4 do not issue RFMs.

O8. Intel Alder/Raptor Lake use FGR mode by default.
AMD Zen 4 systems do not use FGR mode.

RFM in DDR5 Memory Controllers

EXPERIMENT

- Double-sided Rowhammer.
- Tested DIMMs:
  - H5 (SKH, RFM required: No)
  - H11 (SKH, RFM required: Yes)



O7. Intel Alder/Raptor Lake and AMD Zen 4 do not issue RFMs.

O8. Intel Alder/Raptor Lake use FGR mode by default.
AMD Zen 4 systems do not use FGR mode.

O9. Intel Raptor Lake CPUs employ pseudo-TRR (pTRR).

Intel’s pseudo-TRR Mitigation

How likely is it that a row gets refreshed by pTRR?

Intel’s pseudo-TRR Mitigation

How likely is it that a row gets refreshed by pTRR?

EXPERIMENT

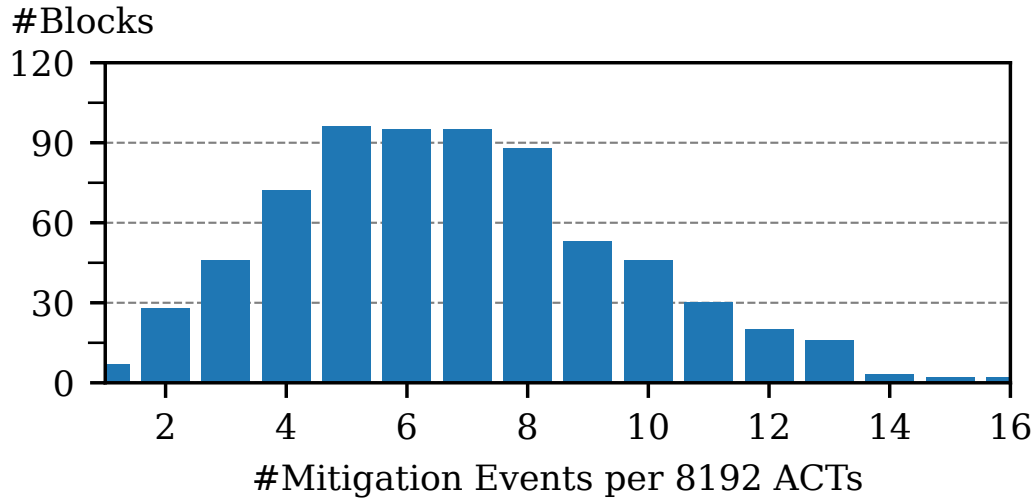
- Hammer two aggressors for 8192 ACTs.
- `clflush` and `mfence` between hammers.
- Repeat experiment for 512 times.

Intel’s pseudo-TRR Mitigation

How likely is it that a row gets refreshed by pTRR?

EXPERIMENT

- Hammer two aggressors for 8192 ACTs.
- `clflush` and `mfence` between hammers.
- Repeat experiment for 512 times.

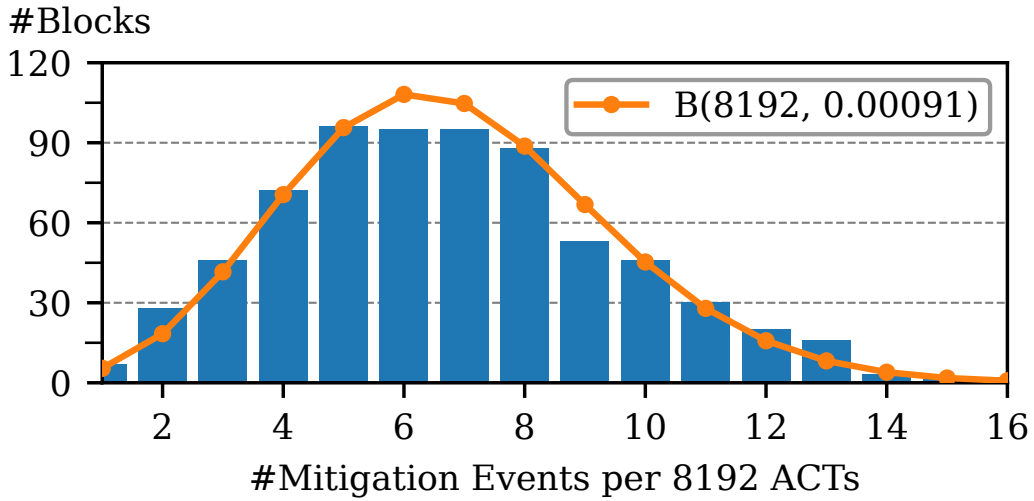


Intel’s pseudo-TRR Mitigation

How likely is it that a row gets refreshed by pTRR?

EXPERIMENT

- Hammer two aggressors for 8192 ACTs.
- `clflush` and `mfence` between hammers.
- Repeat experiment for 512 times.

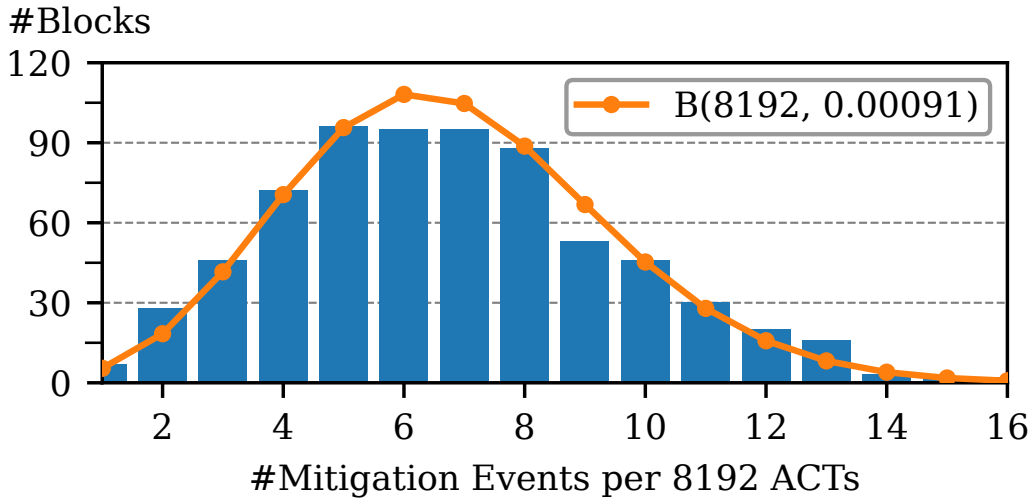


Intel's pseudo-TRR Mitigation

How likely is it that a row gets refreshed by pTRR?

EXPERIMENT

- Hammer two aggressors for 8192 ACTs.
- `clflush` and `mfence` between hammers.
- Repeat experiment for 512 times.



pTRR refreshes aggressor-adjacent rows with a probability of 0.091%.

Intel’s pseudo-TRR Mitigation

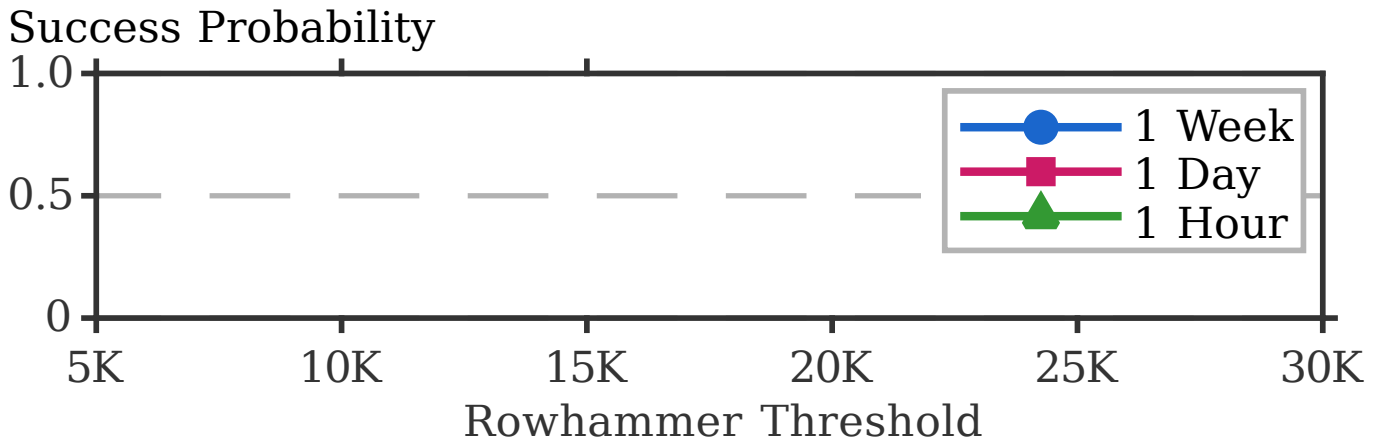
How long does it take to naively bypass pTRR?

[1] A. G. Yağlikçi *et al.*, “HiRA: Hidden Row Activation for Reducing Refresh Latency of Off-the-Shelf DRAM Chips,” in *MICRO ’22*, 2022.

Intel's pseudo-TRR Mitigation

How long does it take to naively bypass pTRR?

- PARA model from previous work [1]
- **50%** attack success probability after

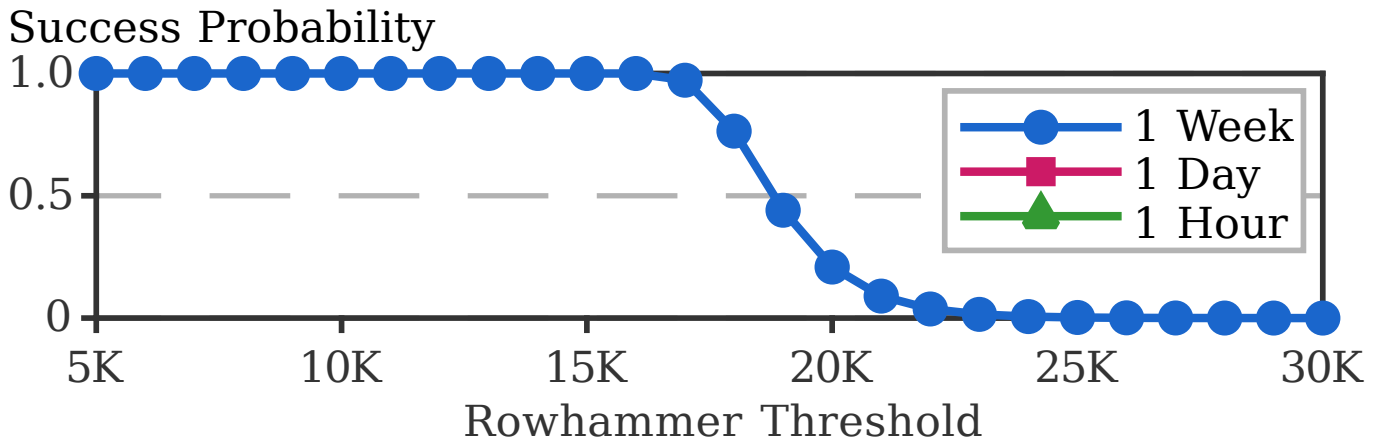


[1] A. G. Yağlikçi *et al.*, "HiRA: Hidden Row Activation for Reducing Refresh Latency of Off-the-Shelf DRAM Chips," in *MICRO '22*, 2022.

Intel’s pseudo-TRR Mitigation

How long does it take to naively bypass pTRR?

- PARA model from previous work [1]
- **50%** attack success probability after
  - **1 week:** for RH threshold **18 800**

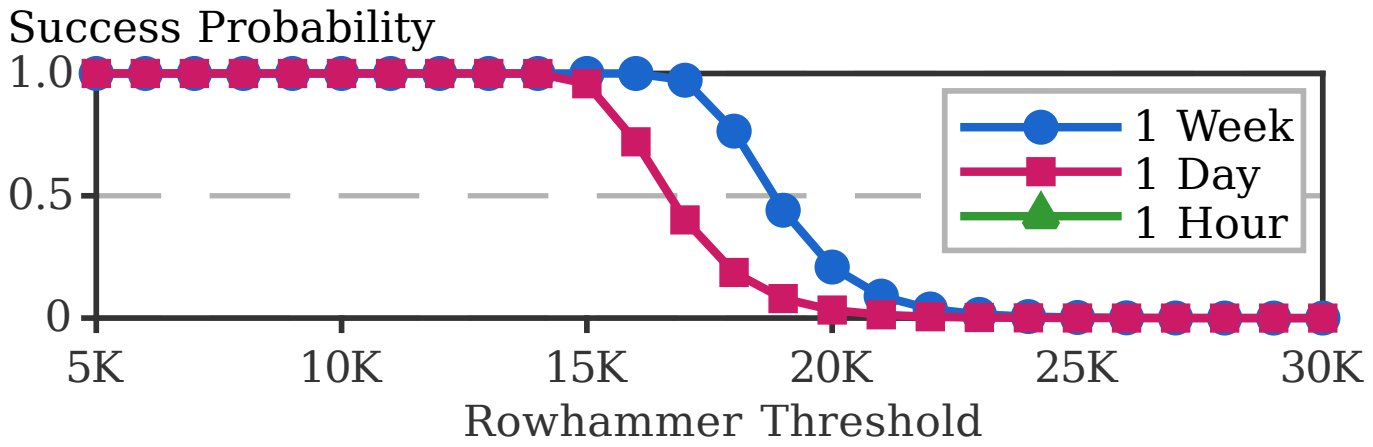


[1] A. G. Yağlikçi *et al.*, “HiRA: Hidden Row Activation for Reducing Refresh Latency of Off-the-Shelf DRAM Chips,” in *MICRO ’22*, 2022.

Intel's pseudo-TRR Mitigation

How long does it take to naively bypass pTRR?

- PARA model from previous work [1]
- **50%** attack success probability after
  - **1 week:** for RH threshold **18 800**
  - **1 day**: for RH threshold of **16 700**

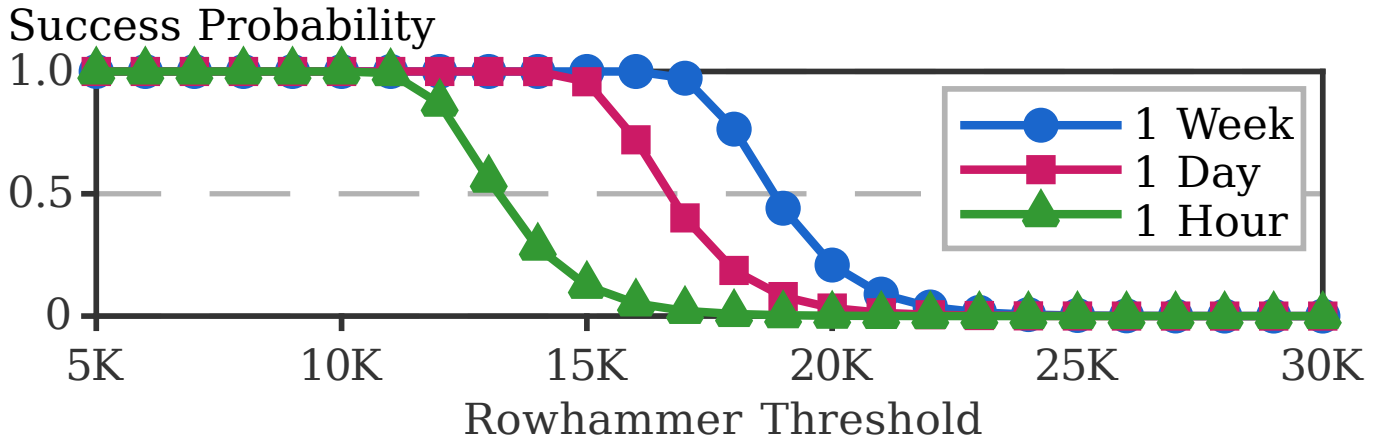


[1] A. G. Yağlikçi *et al.*, "HiRA: Hidden Row Activation for Reducing Refresh Latency of Off-the-Shelf DRAM Chips," in *MICRO '22*, 2022.

Intel's pseudo-TRR Mitigation

How long does it take to naively bypass pTRR?

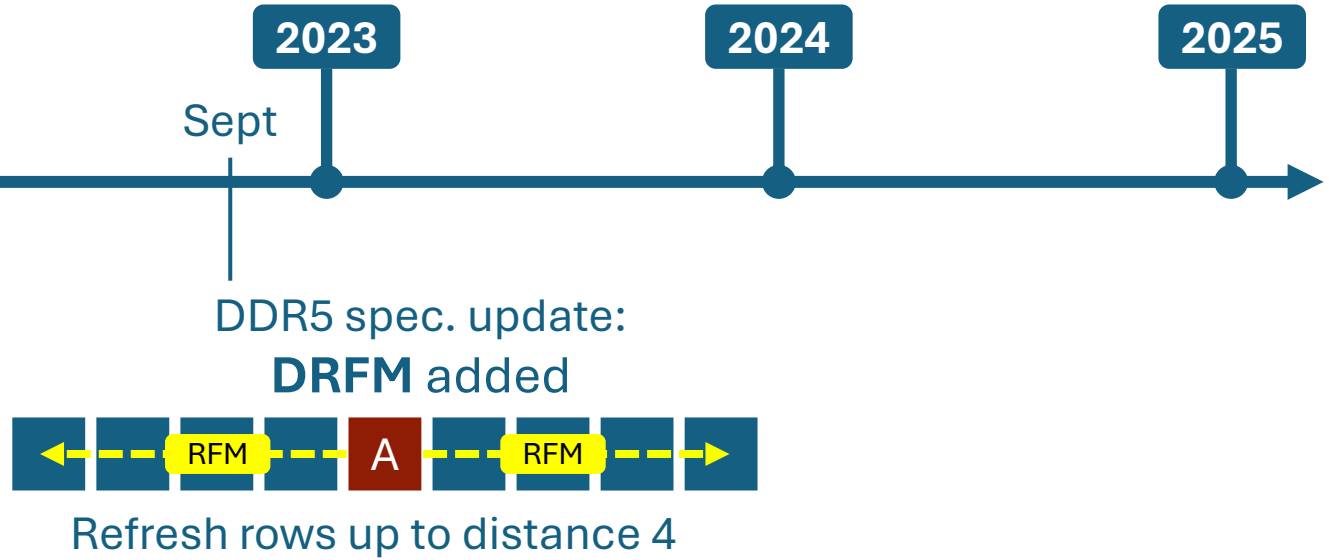
- PARA model from previous work [1]
- **50%** attack success probability after
  - **1 week:** for RH threshold **18 800**
  - **1 day**: for RH threshold of **16 700**
  - **1 hour:** for RH threshold of **13 200**



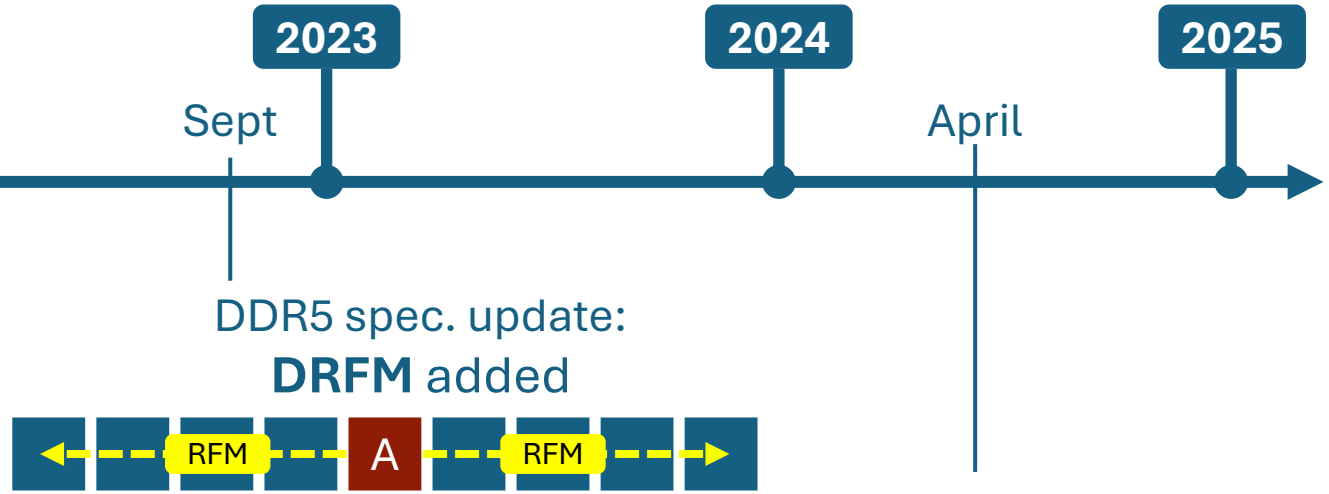
[1] A. G. Yağlikçi *et al.*, "HiRA: Hidden Row Activation for Reducing Refresh Latency of Off-the-Shelf DRAM Chips," in *MICRO '22*, 2022.

Future Work

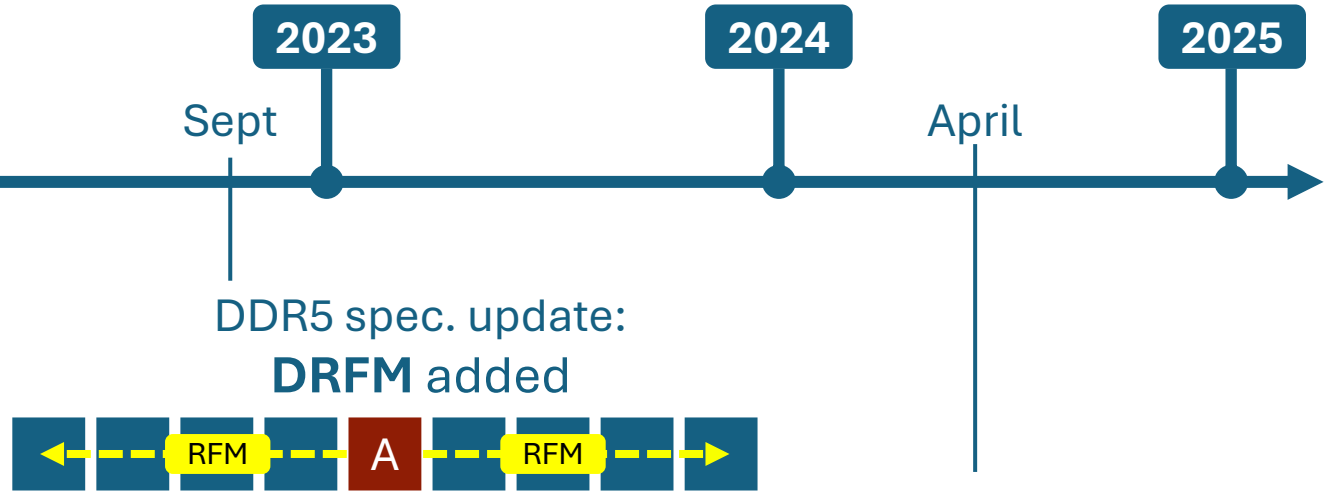
Future Work


2023
2024
2025
Sept
DDR5 spec. update:
DRFM added
RFM
A
RFM
Refresh rows up to distance 4

Future Work

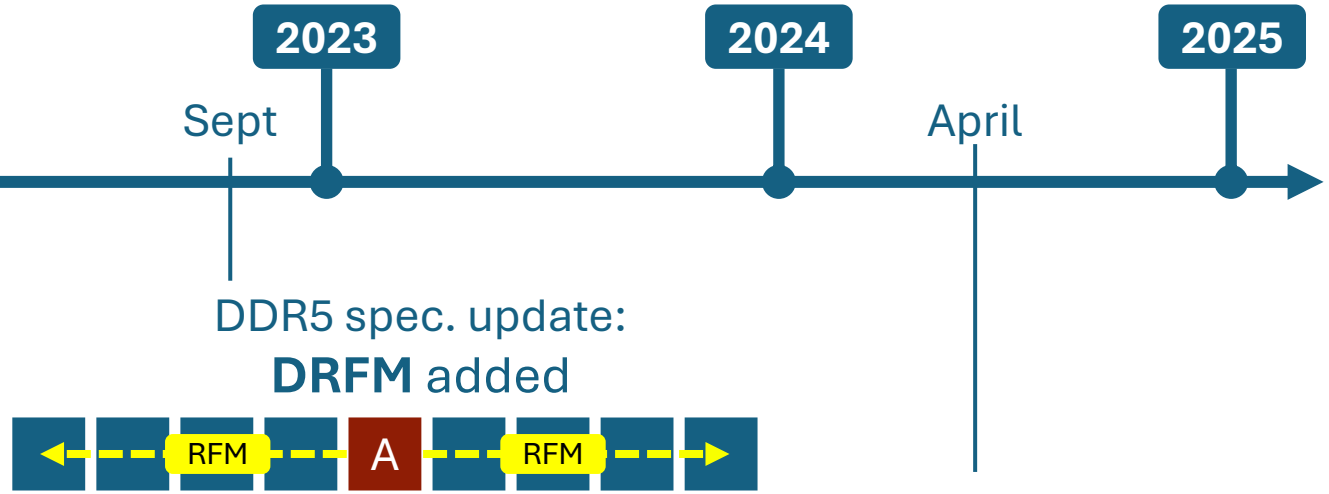

2023
2024
2025
Sept
April
DDR5 spec. update:
DRFM added
RFM
A
RFM
Refresh rows up to distance 4
DDR5 spec. update:
PRAC added
Row 0
#ACTs:
Row 1
#ACTs:
...
Per-row activation counter (DRAM)

Future Work



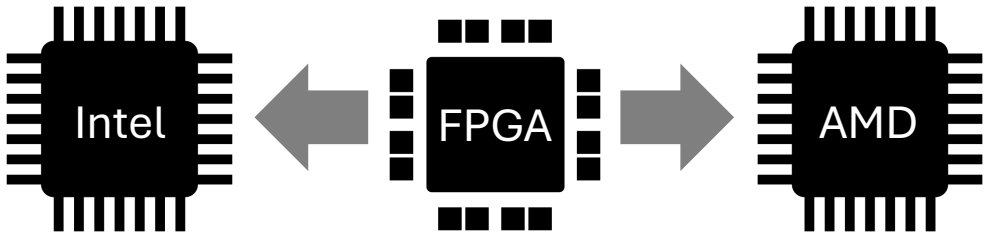
Improved system-level Rowpress attacks

Future Work



Improved system-level Rowpress attacks

Rowhammer pattern execution



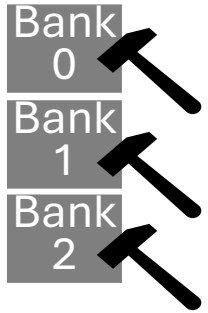
Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.

Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.

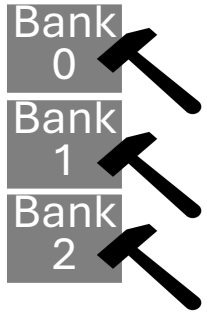


Sledgehammer is most effective on six banks.

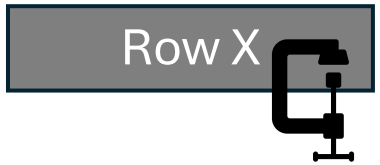
Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.



Sledgehammer
is most effective on six banks.

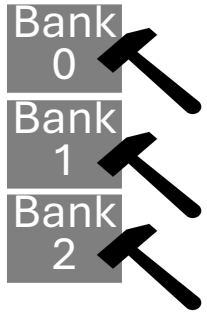


Rowpress
has limited effect on ACmin (2x) on a real system.

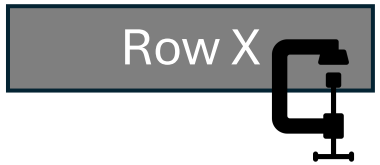
Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.



Sledgehammer
is most effective on six banks.



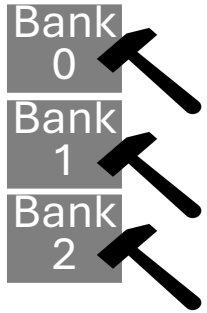
Rowpress
has limited effect on ACmin (2x) on a real system.

No RFM cmds
on Intel AL/RL and AMD Z4.

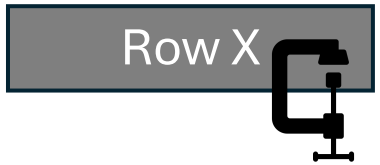
Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.

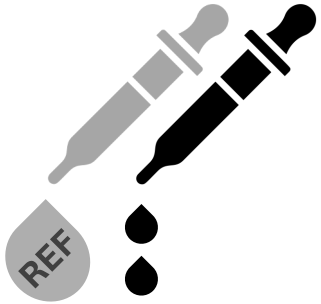


Sledgehammer
is most effective on six banks.



Rowpress
has limited effect on ACmin (2x) on a real system.

No RFM cmds
on Intel AL/RL and AMD Z4.

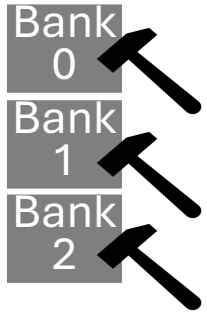


FGR Mode
is used by Intel AL/RL CPUs.

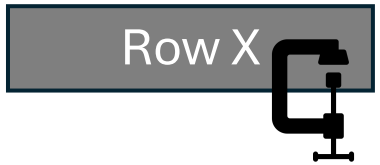
Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.

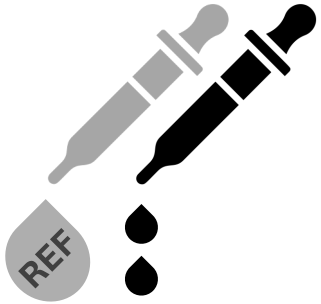


Sledgehammer
is most effective on six banks.

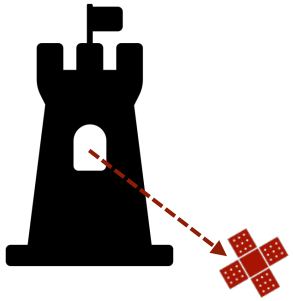


Rowpress
has limited effect on ACmin (2x) on a real system.

No RFM cmds
on Intel AL/RL and AMD Z4.



FGR Mode
is used by Intel AL/RL CPUs.

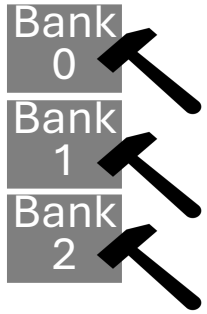


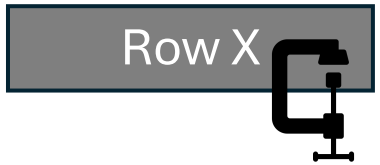
Intel pTRR
is a Rowhammer mitigation in the RL memory controller.

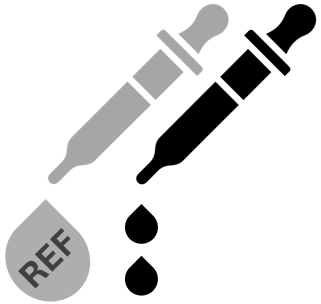
Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich

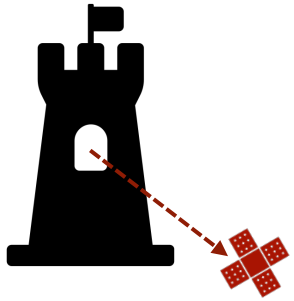
Conclusion

McSee enables for the first time *precise* insights into DRAM Attacks and Defenses on DDR4/DDR5 DRAM.

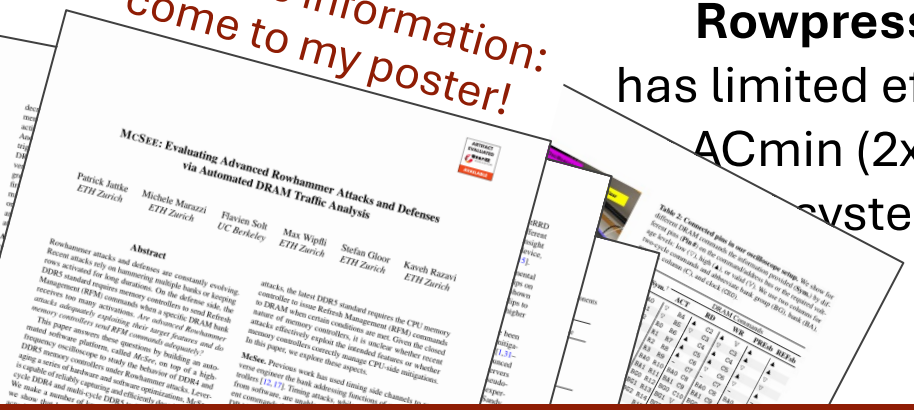








For more information: come to my poster!



Rowpress has limited effect ACmin (2x) on ystem.

No RFM cmds on Intel AL/RL and AMD Z4.

FGR Mode is used by Intel AL/RL CPUs.

Intel pTRR is a Rowhammer mitigation in the RL memory controller.

Patrick Jattke pjattke@ethz.ch pjattke linkedin.com/in/pjattke COMSEC ETH zürich