Understanding RowHammer Under Reduced Wordline Voltage

An Experimental Study Using Real DRAM Devices

Abdullah Giray Yağlıkçı

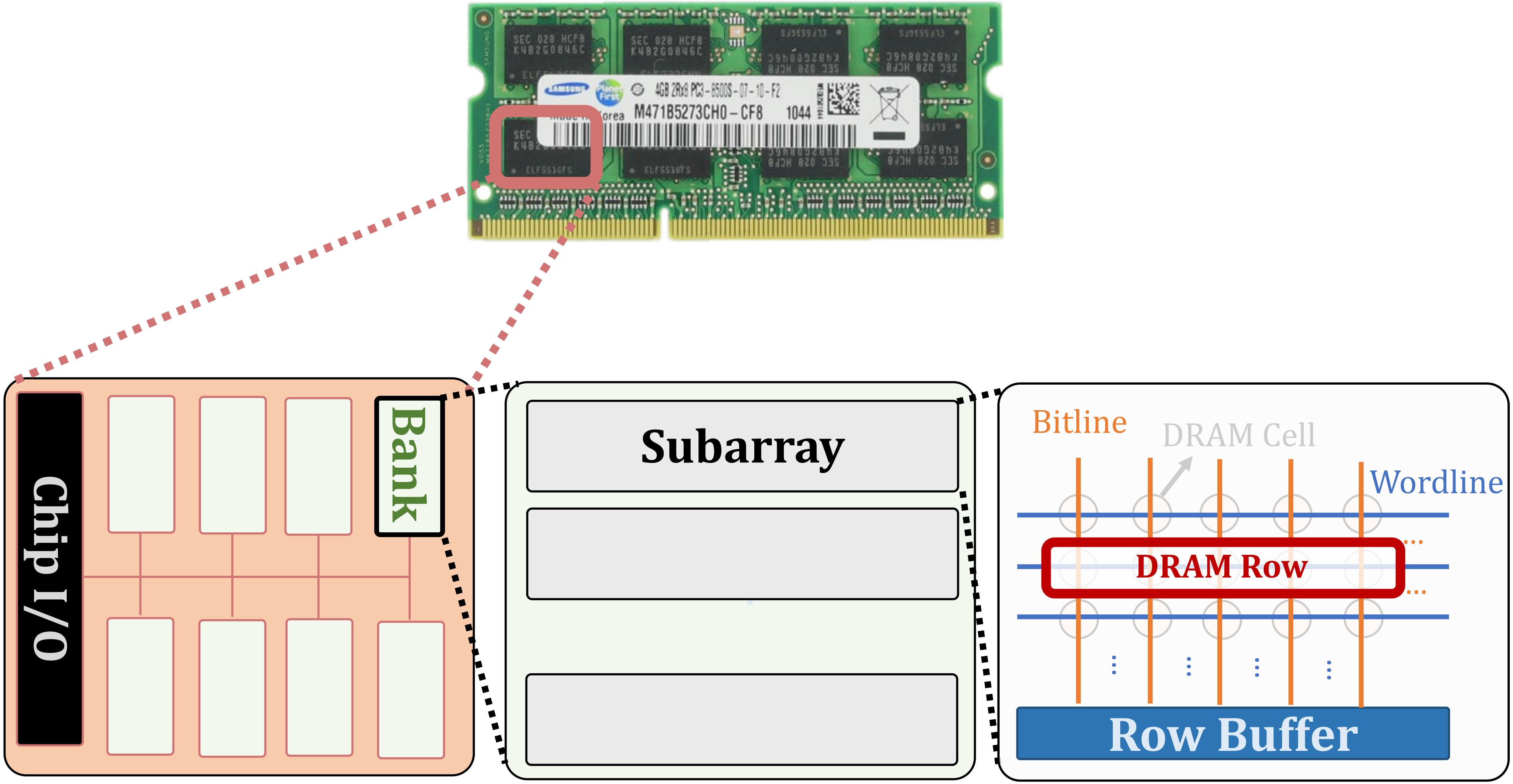
Haocong Luo   Geraldo F. de Oliviera   Ataberk Olgun

Minesh Patel   Jisung Park   Hasan Hassan   Jeremie S. Kim

Lois Orosa   Onur Mutlu

ETH zürich   SAFARI   CESGA Centro de Supercomputación de Galicia

DRAM Organization



Chip I/O

Bank

Subarray

Bitline

DRAM Cell

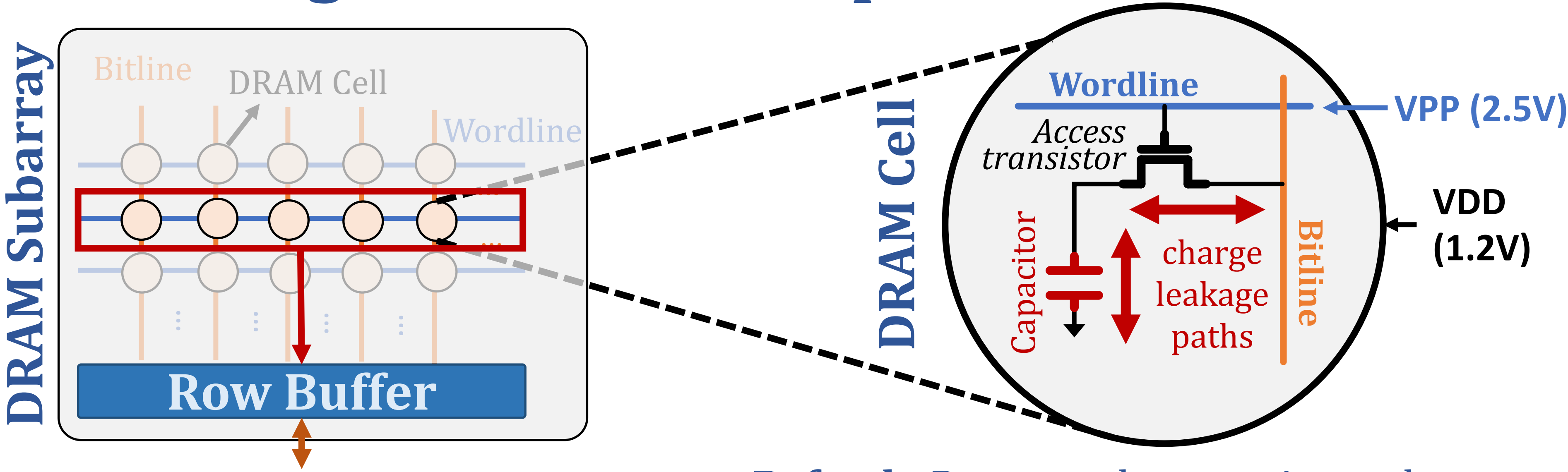
Wordline

DRAM Row

Row Buffer

DRAM Chip **DRAM Bank** **DRAM Subarray**

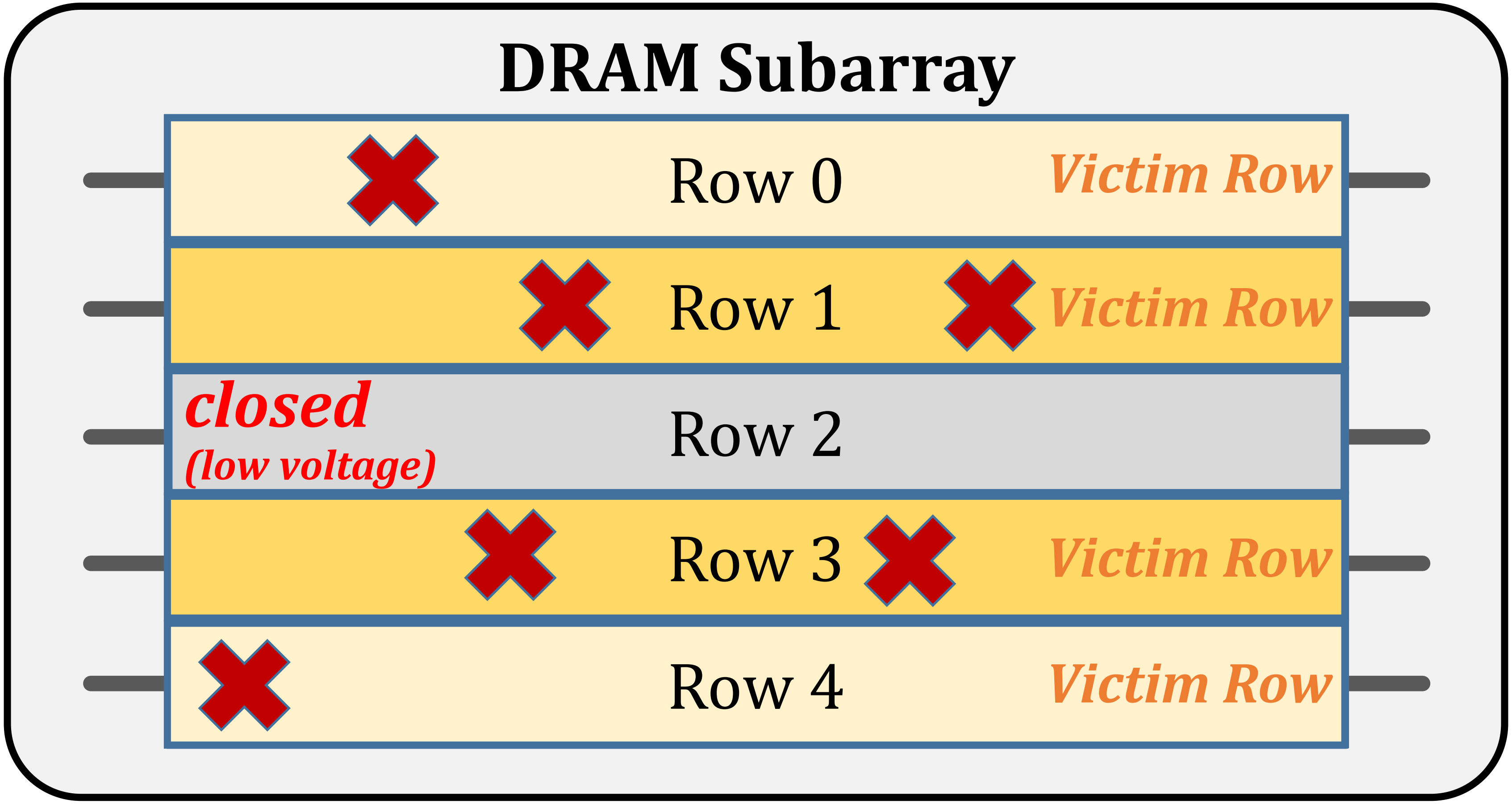
DRAM Organization and Operation



Refresh: Restores the capacitor voltage with a time period called **refresh window**

1. **Row Activation:** Fetch the row's content into the row buffer
2. **Column Access**: Read/Write a column in the row buffer
3. **Precharge**: Disconnect the row from the row buffer

The RowHammer Vulnerability


DRAM Subarray

Row 0 *Victim Row*

Row 1 *Victim Row*

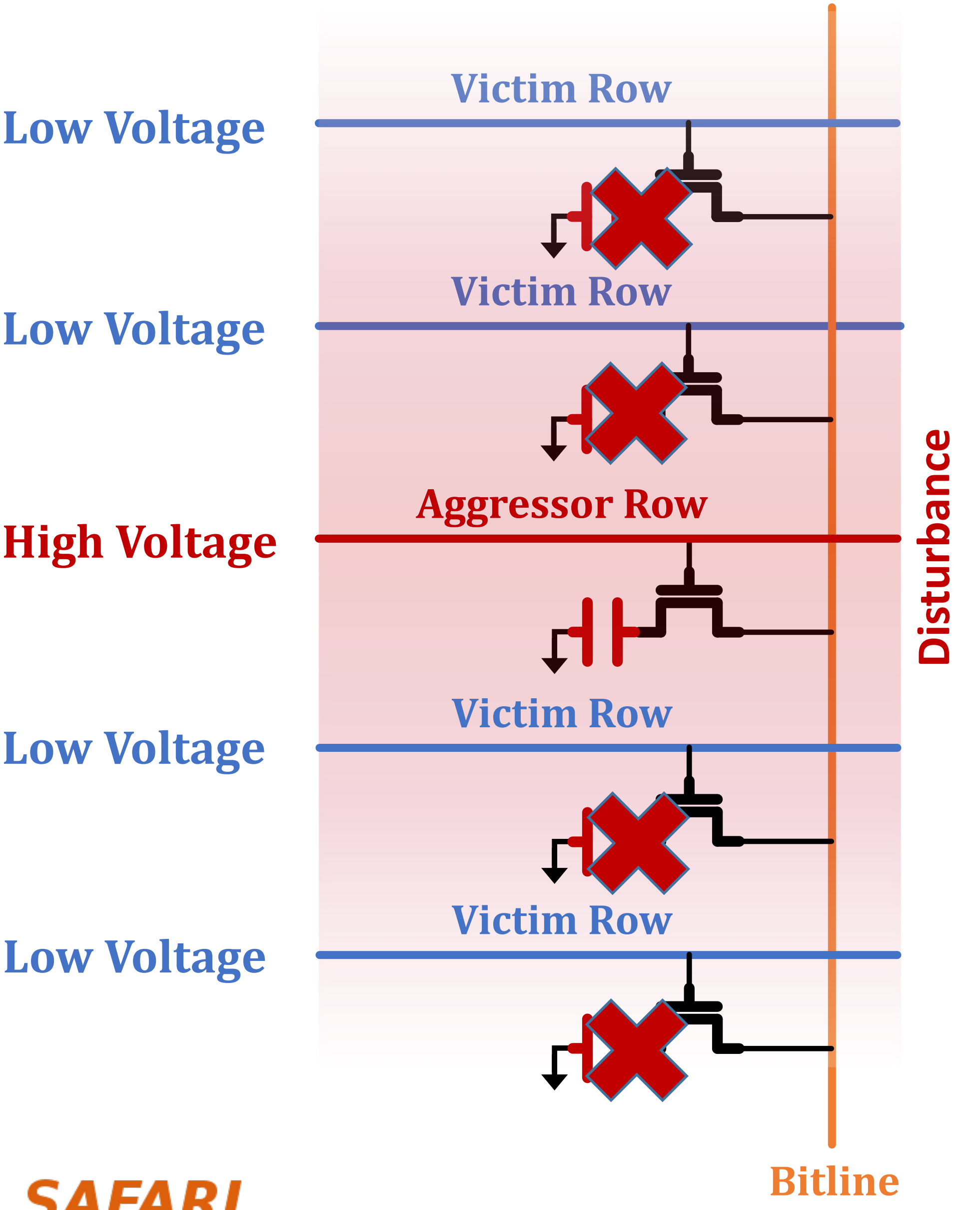
closed
(low voltage)
Row 2

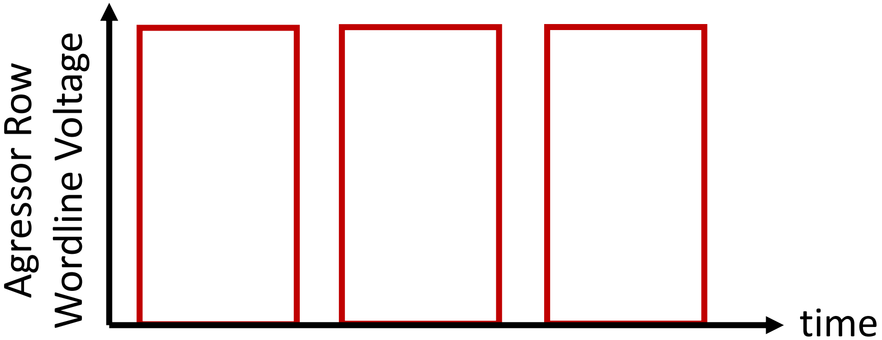
Row 3 *Victim Row*

Row 4 *Victim Row*

Repeatedly **opening** (activating) and **closing** (precharging)
a DRAM row in **real DRAM chips**
causes **RowHammer bit flips** in nearby cells

A Closer Look into RowHammer





Repeatedly toggling wordline voltage is the *key* to inducing **RowHammer bit flips**

Executive Summary

Motivation:

- Repeatedly **toggling a DRAM row's wordline voltage** causes bit flips in nearby rows
- This vulnerability, **RowHammer**, **worsens in denser DRAM chips**
- Understanding RowHammer enables designing **effective and efficient solutions**

Problem: **No study** demonstrates how **wordline voltage (VPP)** affects RowHammer

Goal: Experimentally understand how **VPP affects RowHammer and DRAM operation**

Experimental study: **272 DRAM chips** from **three major DRAM manufacturers**

VPP's effect on RowHammer: *Six observations* show that with reduced VPP,

- **Bit error rate** caused by a RowHammer attack reduces by **15.2% (66.9% max)**
- A row needs to be activated **7.4% more times (85.8% max)** to induce the first bit flip

VPP's effect on DRAM operation: *Nine observations* show that with reduced VPP,

- **208 out of 272** tested DRAM chips **reliably operate** using nominal timing parameters
- Erroneous DRAM chips can reliably operate with
  - **A longer row activation latency,** i.e., 24ns/15ns for 48/16 chips,
  - **Single-error-correcting codes or 2x the refresh rate** *only for* 16.4% of rows

Conclusion: Reducing wordline voltage can **reduce RowHammer vulnerability**
without significantly affecting **reliable DRAM operation**

Outline

Motivation and Goal

Experimental Methodology

RowHammer Under Reduced Wordline Voltage

DRAM Operation Under Reduced Wordline Voltage

Conclusions

Outline

Motivation and Goal

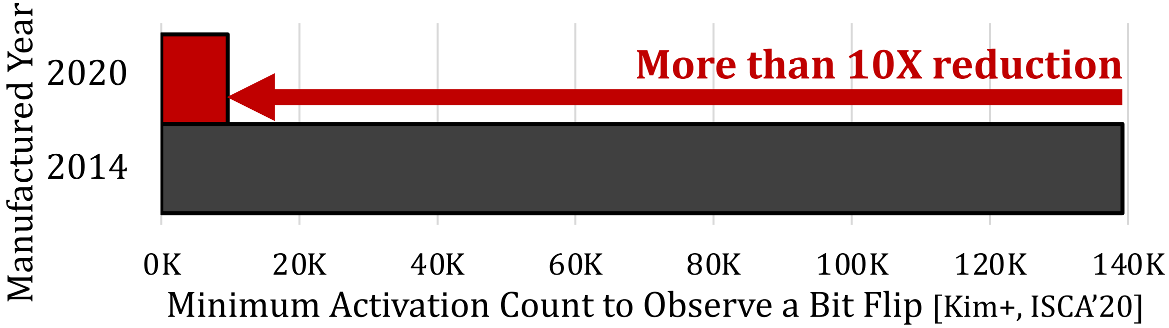
Experimental Methodology

RowHammer Under Reduced Wordline Voltage

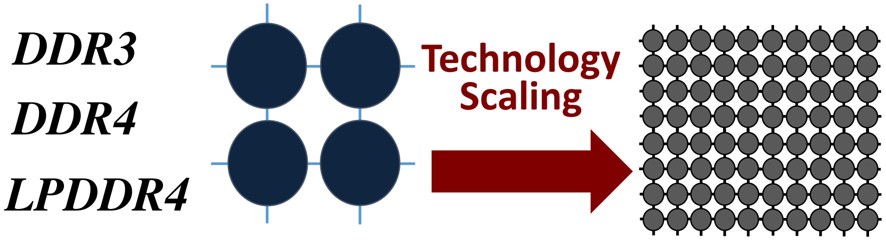
DRAM Operation Under Reduced Wordline Voltage

Conclusions

Motivation



- Defenses are becoming **prohibitively expensive** **[Kim et al., ISCA'20]**
- A **deeper understanding** is needed **[Orosa and Yaglikci et al., MICRO'21]**
- Prior works investigate **how RowHammer changes** across



[Kim et al., ISCA'20]

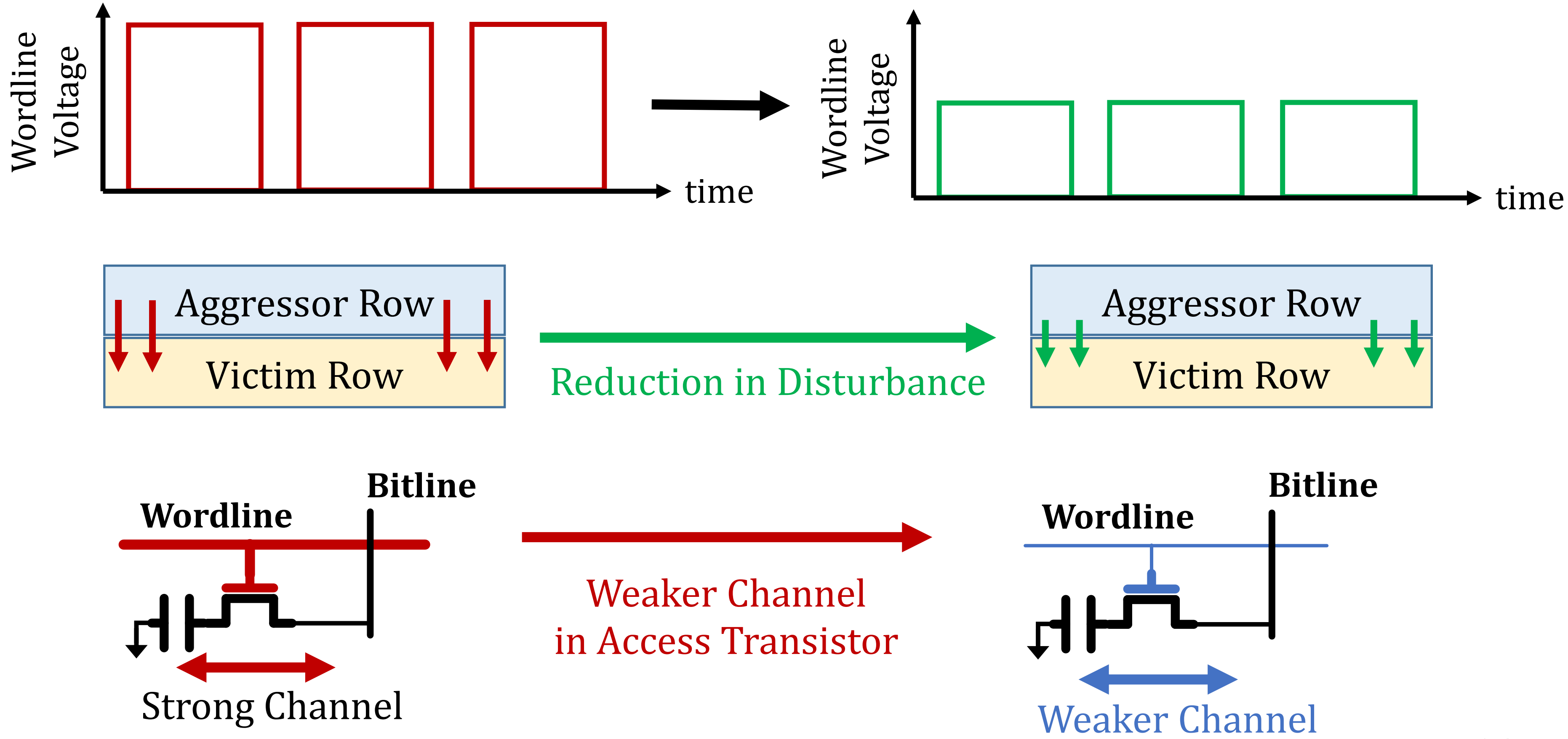
[Orosa and Yaglikci et al., MICRO'21]

Repeatedly toggling **wordline voltage** causes RowHammer

No rigorous experimental study demonstrates how the **magnitude of wordline voltage** affects the **RowHammer vulnerability of real DRAM chips**

Our Hypothesis

Reducing **wordline voltage**
can **reduce RowHammer vulnerability**
without significantly affecting **reliable DRAM operation**



Wordline Voltage

time

Wordline Voltage

time

Aggressor Row

Victim Row

Reduction in Disturbance

Aggressor Row

Victim Row

Wordline

Bitline

Strong Channel

Weaker Channel
in Access Transistor

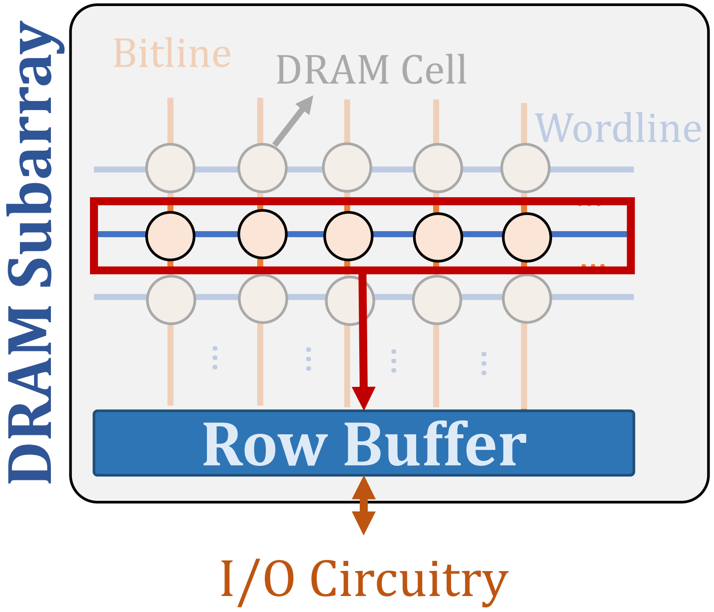
Wordline

Bitline

Weaker Channel

Our Goal

Understand how the **wordline voltage (VPP)** affects **RowHammer vulnerability** and **reliable DRAM operation** on real DRAM chips



Outline

Motivation and Goal

Experimental Methodology

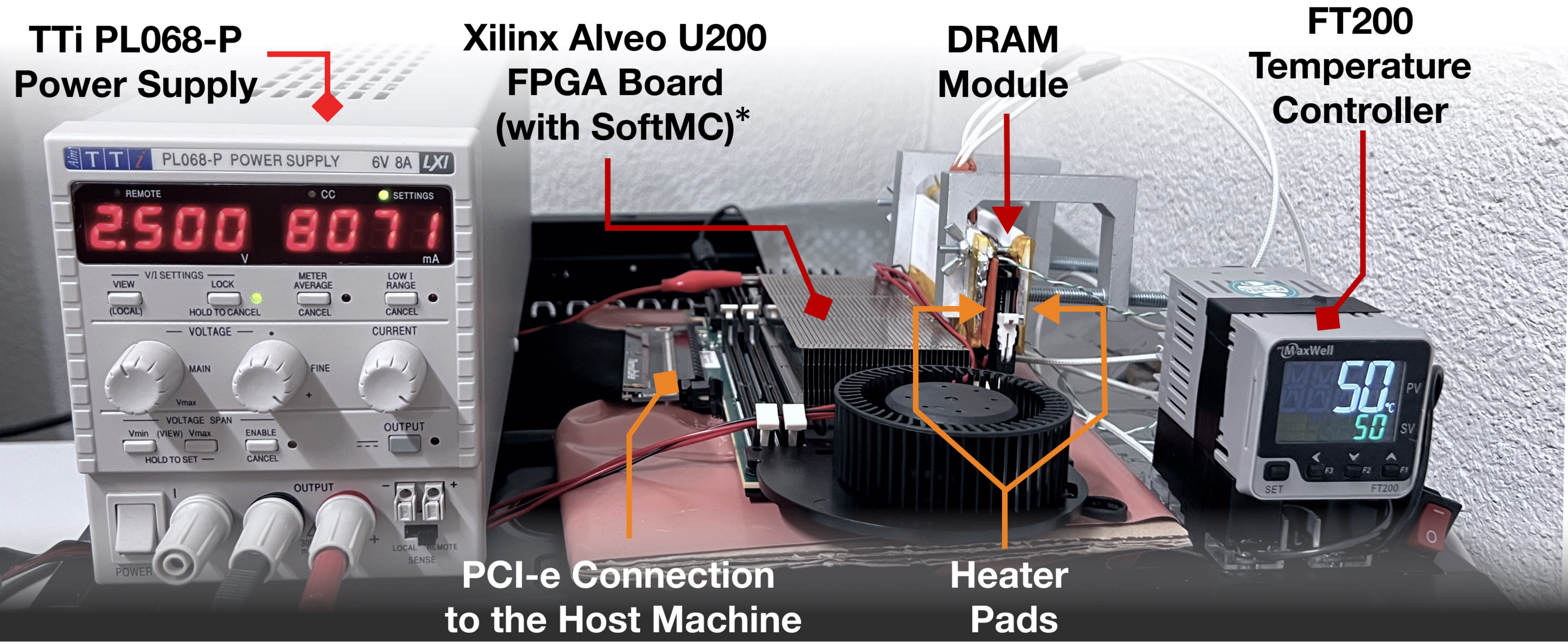
RowHammer Under Reduced Wordline Voltage

DRAM Operation Under Reduced Wordline Voltage

Conclusions

DRAM Testing Infrastructure

FPGA-based SoftMC (Xilinx Virtex UltraScale+ XCU200)



Fine-grained control over **DRAM commands**, **timing parameters (±1.5ns)**, **temperature (±0.1°C)**, and **wordline voltage (±1mV)**

*Hassan et al., "SoftMC: A Flexible and Practical Open-Source Infrastructure for Enabling Experimental DRAM Studies," in HPCA, 2017. [Available on GitHub: https://github.com/CMU-SAFARI/SoftMC]

DRAM Testing Methodology

To characterize our DRAM chips at **worst-case** conditions:

1. **Prevent sources of interference during core test loop**
   - **No DRAM refresh**: to avoid refreshing victim row
   - **No DRAM calibration events**: to minimize variation in test timing
   - **No RowHammer mitigation mechanisms**: to observe circuit-level effects
   - Test for **less than a refresh window (32ms)** to avoid retention failures
   - **Repeat tests** for ten times
2. **Worst-case access sequence**
   - We use **worst-case** access sequence based on prior works' observations
   - For each row, **repeatedly access the two physically-adjacent rows as fast as possible**

DRAM Chips Tested

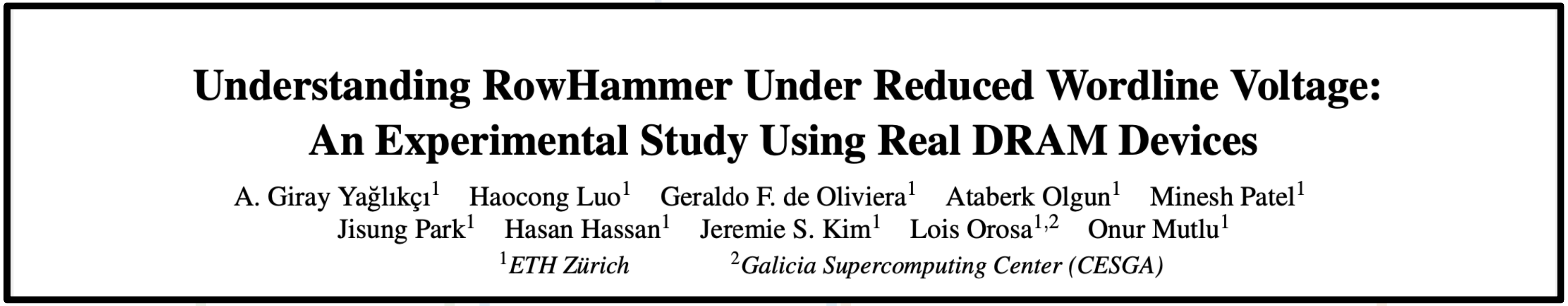
272 DDR4 DRAM Chips

Mfr.	# DIMMs	# Chips	Density	Die	Org.	Date
A (Micron)	1	8	4Gb	-	x8	48-16
	4	64	8Gb	B	x4	11-19
	3	24	4Gb	F	x8	07-21
	2	16	4Gb	-	x8	
B (Samsung)	2	16	8Gb	B	x8	52-20
	1	8	8Gb	C	x8	19-19
	3	24	8Gb	D	x8	10-21
	1	8	4Gb	E	x8	08-17
	1	8	4Gb	F	x8	02-21
	2	16	8Gb		x8	
C (SK Hynix)	2	16	16Gb	A	x8	51-20
	3	24	4Gb	B	x8	02-21
	2	16	4Gb	C	x8	
	3	24	8Gb	D	x8	48-20

3 Major Manufacturers

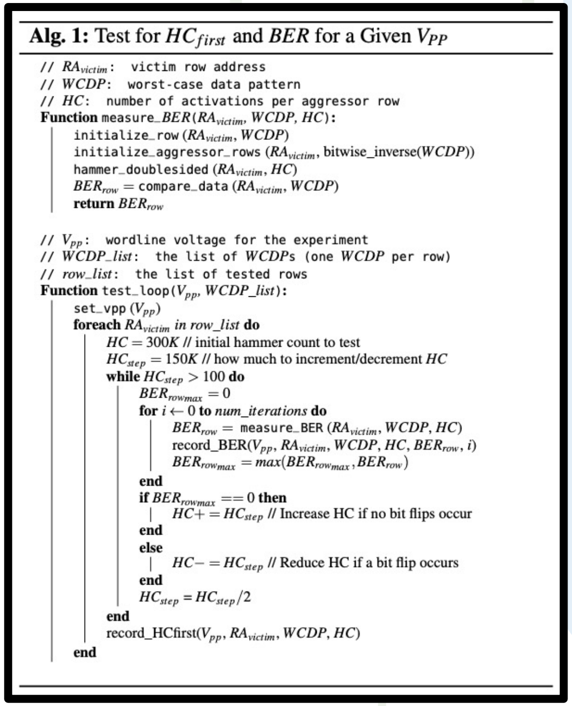
More Details in the Paper

272 DDR4 DRAM Chips



Understanding RowHammer Under Reduced Wordline Voltage: An Experimental Study Using Real DRAM Devices

A. Giray Yağlıkçı[1] Haocong Luo[1] Geraldo F. de Oliviera[1] Ataberk Olgun[1] Minesh Patel[1]
Jisung Park[1] Hasan Hassan[1] Jeremie S. Kim[1] Lois Orosa[1,2] Onur Mutlu[1]
[1]*ETH Zürich* [2]*Galicia Supercomputing Center (CESGA)*



Alg. 1: Test for HC_{first} and BER for a Given V_{PP}

```
// $RA_{victim}$:  victim row address
// $WCDP$:  worst-case data pattern
// $HC$:  number of activations per aggressor row
Function measure_$BER$($RA_{victim}$, $WCDP$, $HC$):
    initialize_row ($RA_{victim}$, $WCDP$)
    initialize_aggressor_rows ($RA_{victim}$, bitwise_inverse($WCDP$))
    hammer_doublesided ($RA_{victim}$, $HC$)
    $BER_{row}$ = compare_data ($RA_{victim}$, $WCDP$)
    return $BER_{row}$

// $V_{pp}$:  wordline voltage for the experiment
// $WCDP\_list$:  the list of $WCDP$s (one $WCDP$ per row)
// $row\_list$:  the list of tested rows
Function test_loop($V_{pp}$, $WCDP\_list$):
    set_vpp ($V_{pp}$)
    foreach $RA_{victim}$ in $row\_list$ do
        $HC = 300K$ // initial hammer count to test
        $HC_{step} = 150K$ // how much to increment/decrement $HC$
        while $HC_{step} > 100$ do
            $BER_{rowmax} = 0$
            for $i \leftarrow 0$ to $num\_iterations$ do
                $BER_{row}$ = measure_BER ($RA_{victim}$, $WCDP$, $HC$)
                record_BER($V_{pp}$, $RA_{victim}$, $WCDP$, $HC$, $BER_{row}$, $i$)
                $BER_{rowmax} = max(BER_{rowmax}, BER_{row})$
            end
            if $BER_{rowmax} == 0$ then
                $HC+ = HC_{step}$ // Increase HC if no bit flips occur
            end
            else
                $HC- = HC_{step}$ // Reduce HC if a bit flip occurs
            end
            $HC_{step} = HC_{step}/2$
        end
        record_HCfirst($V_{pp}$, $RA_{victim}$, $WCDP$, $HC$)
    end
```

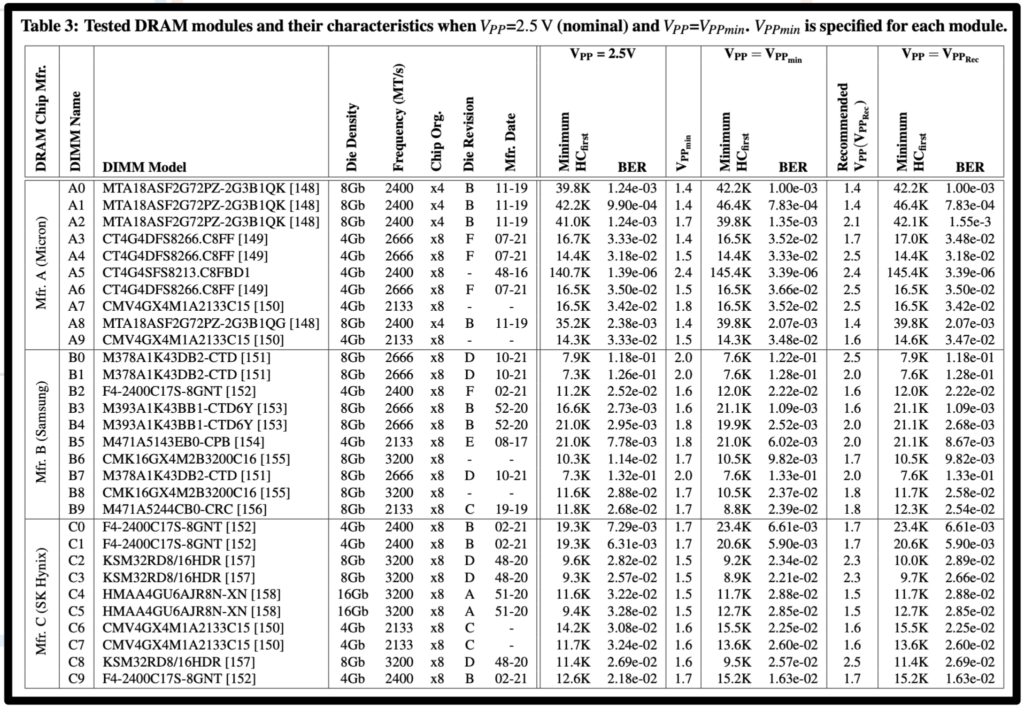


Table 3: Tested DRAM modules and their characteristics when V_{PP}=2.5 V (nominal) and $V_{PP}=V_{PPmin}$. V_{PPmin} is specified for each module.

								V_{PP} = 2.5V			$V_{PP} = V_{PP_{min}}$			$V_{PP} = V_{PP_{Rec}}$	
DRAM Chip Mfr.	DIMM Name	DIMM Model	Die Density	Frequency (MT/s)	Chip Org.	Die Revision	Mfr. Date	Minimum HC_{first}	BER	$V_{PP_{min}}$	Minimum HC_{first}	BER	Recommended $V_{PP}(V_{PP_{Rec}})$	Minimum HC_{first}	BER
Mfr. A (Micron)	A0	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	39.8K	1.24e-03	1.4	42.2K	1.00e-03	1.4	42.2K	1.00e-03
	A1	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	42.2K	9.90e-04	1.4	46.4K	7.83e-04	1.4	46.4K	7.83e-04
	A2	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	41.0K	1.24e-03	1.7	39.8K	1.35e-03	2.1	42.1K	1.55e-3
	A3	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	16.7K	3.33e-02	1.4	16.5K	3.52e-02	1.7	17.0K	3.48e-02
	A4	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	14.4K	3.18e-02	1.5	14.4K	3.33e-02	2.5	14.4K	3.18e-02
	A5	CT4G4SFS8213.C8FBD1	4Gb	2400	x8	-	48-16	140.7K	1.39e-06	2.4	145.4K	3.39e-06	2.4	145.4K	3.39e-06
	A6	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	16.5K	3.50e-02	1.5	16.5K	3.66e-02	2.5	16.5K	3.50e-02
	A7	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	-	-	16.5K	3.42e-02	1.8	16.5K	3.52e-02	2.5	16.5K	3.42e-02
	A8	MTA18ASF2G72PZ-2G3B1QG [148]	8Gb	2400	x4	B	11-19	35.2K	2.38e-03	1.4	39.8K	2.07e-03	1.4	39.8K	2.07e-03
	A9	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	-	-	14.3K	3.33e-02	1.5	14.3K	3.48e-02	1.6	14.6K	3.47e-02
Mfr. B (Samsung)	B0	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.9K	1.18e-01	2.0	7.6K	1.22e-01	2.5	7.9K	1.18e-01
	B1	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.3K	1.26e-01	2.0	7.6K	1.28e-01	2.0	7.6K	1.28e-01
	B2	F4-2400C17S-8GNT [152]	4Gb	2400	x8	F	02-21	11.2K	2.52e-02	1.6	12.0K	2.22e-02	1.6	12.0K	2.22e-02
	B3	M393A1K43BB1-CTD6Y [153]	8Gb	2666	x8	B	52-20	16.6K	2.73e-03	1.6	21.1K	1.09e-03	1.6	21.1K	1.09e-03
	B4	M393A1K43BB1-CTD6Y [153]	8Gb	2666	x8	B	52-20	21.0K	2.95e-03	1.8	19.9K	2.52e-03	2.0	21.1K	2.68e-03
	B5	M471A5143EB0-CPB [154]	4Gb	2133	x8	E	08-17	21.0K	7.78e-03	1.8	21.0K	6.02e-03	2.0	21.1K	8.67e-03
	B6	CMK16GX4M2B3200C16 [155]	8Gb	3200	x8	-	-	10.3K	1.14e-02	1.7	10.5K	9.82e-03	1.7	10.5K	9.82e-03
	B7	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.3K	1.32e-01	2.0	7.6K	1.33e-01	2.0	7.6K	1.33e-01
	B8	CMK16GX4M2B3200C16 [155]	8Gb	3200	x8	-	-	11.6K	2.88e-02	1.7	10.5K	2.37e-02	1.8	11.7K	2.58e-02
	B9	M471A5244CB0-CRC [156]	8Gb	2133	x8	C	19-19	11.8K	2.68e-02	1.7	8.8K	2.39e-02	1.8	12.3K	2.54e-02
Mfr. C (SK Hynix)	C0	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	19.3K	7.29e-03	1.7	23.4K	6.61e-03	1.7	23.4K	6.61e-03
	C1	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	19.3K	6.31e-03	1.7	20.6K	5.90e-03	1.7	20.6K	5.90e-03
	C2	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	9.6K	2.82e-02	1.5	9.2K	2.34e-02	2.3	10.0K	2.89e-02
	C3	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	9.3K	2.57e-02	1.5	8.9K	2.21e-02	2.3	9.7K	2.66e-02
	C4	HMAA4GU6AJR8N-XN [158]	16Gb	3200	x8	A	51-20	11.6K	3.22e-02	1.5	11.7K	2.88e-02	1.5	11.7K	2.88e-02
	C5	HMAA4GU6AJR8N-XN [158]	16Gb	3200	x8	A	51-20	9.4K	3.28e-02	1.5	12.7K	2.85e-02	1.5	12.7K	2.85e-02
	C6	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	C	-	14.2K	3.08e-02	1.6	15.5K	2.25e-02	1.6	15.5K	2.25e-02
	C7	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	C	-	11.7K	3.24e-02	1.6	13.6K	2.60e-02	1.6	13.6K	2.60e-02
	C8	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	11.4K	2.69e-02	1.6	9.5K	2.57e-02	2.5	11.4K	2.69e-02
	C9	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	12.6K	2.18e-02	1.7	15.2K	1.63e-02	1.7	15.2K	1.63e-02

Full paper on arXiv: https://arxiv.org/abs/2206.09999

Outline

Motivation and Goal

Experimental Methodology

RowHammer Under Reduced Wordline Voltage

DRAM Operation Under Reduced Wordline Voltage

Conclusions

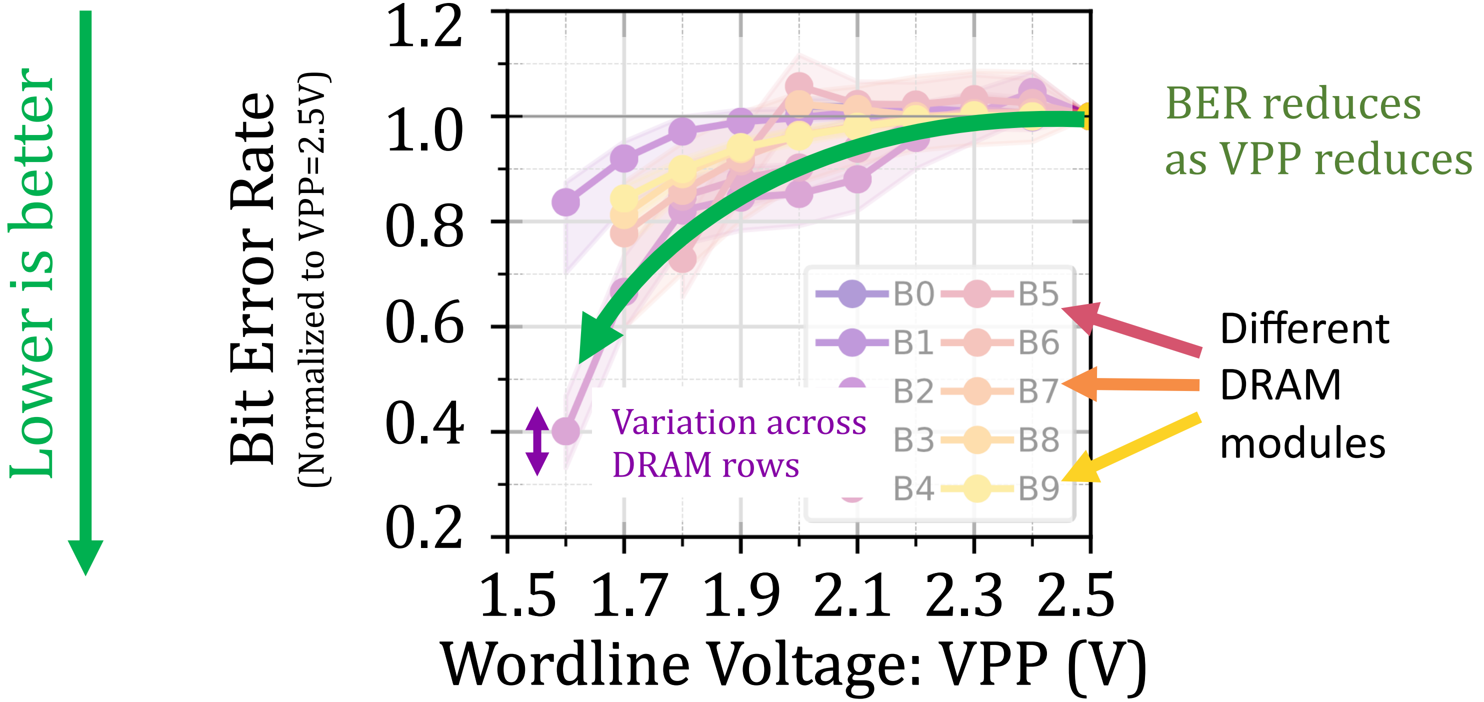
Key Takeaway from RowHammer Analysis

Takeaway 1

Reducing wordline voltage **reduces RowHammer vulnerability**

- **15.2%** (66.9% max) **fewer bit flips** occur
- **Activation count** at which *the first bit flip* occurs **increases** by **7.4%** (85.8% max)

Wordline Voltage's Effect on RowHammer

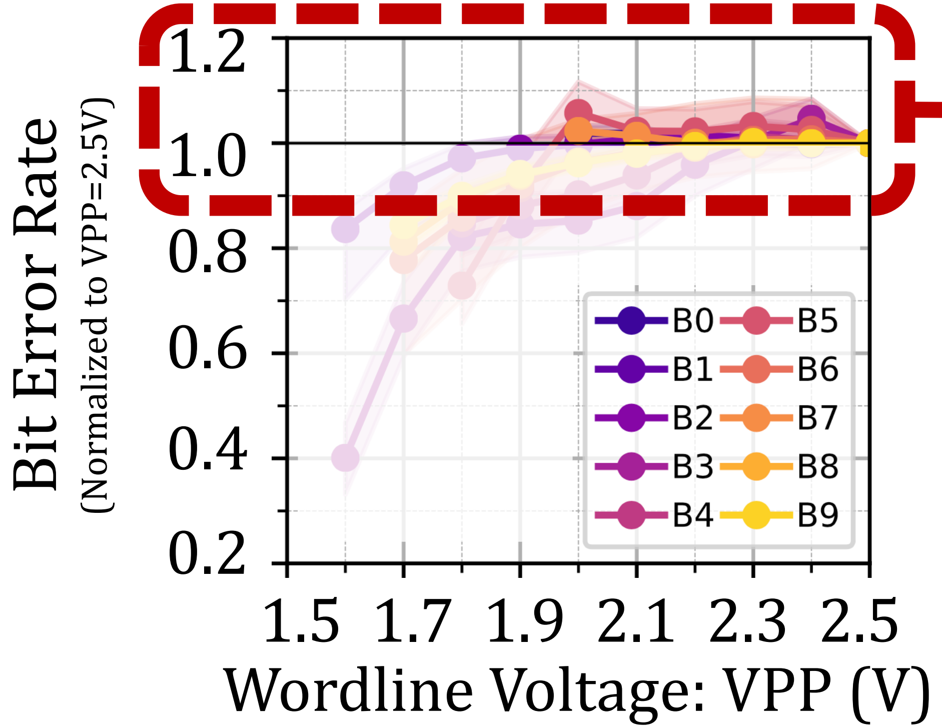


OBSERVATION 1

Fewer DRAM cells experience RowHammer bit flips under **reduced wordline voltage**

Wordline Voltage's Effect on RowHammer

Lower is better

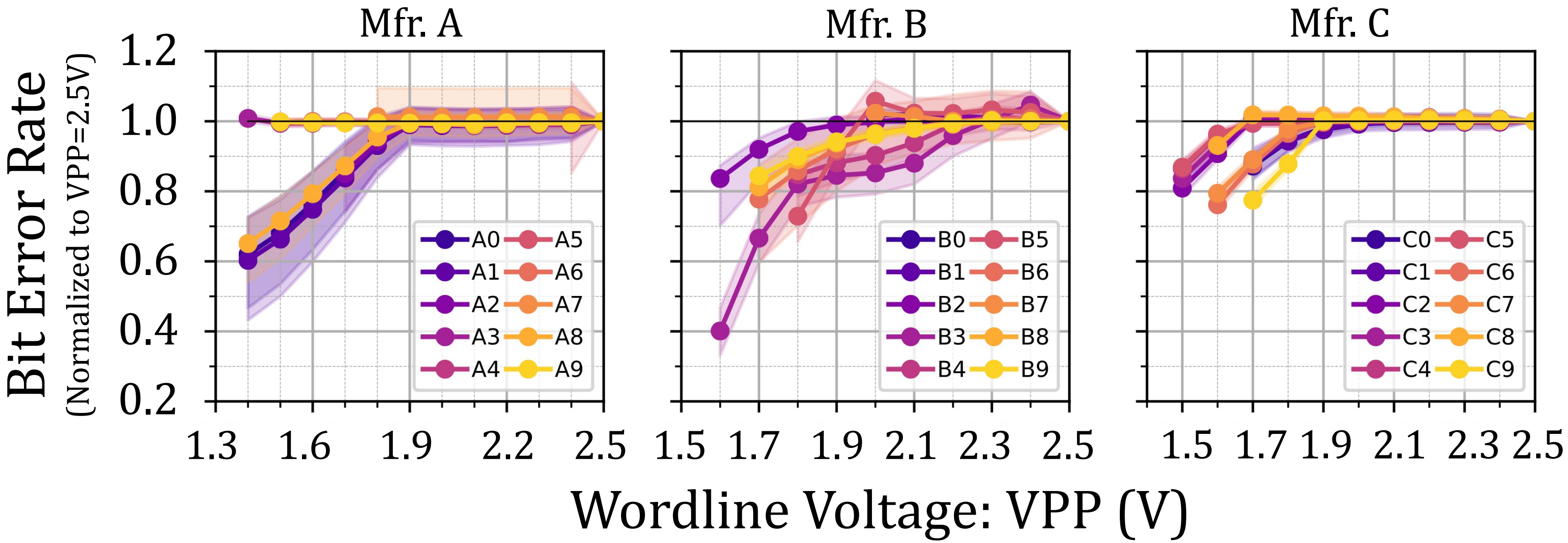


Bit error rate increases

OBSERVATION 2

Reducing wordline voltage can cause **more DRAM cells** to experience bit flips in **a small fraction of rows (15.4%)**

Wordline Voltage's Effect on RowHammer



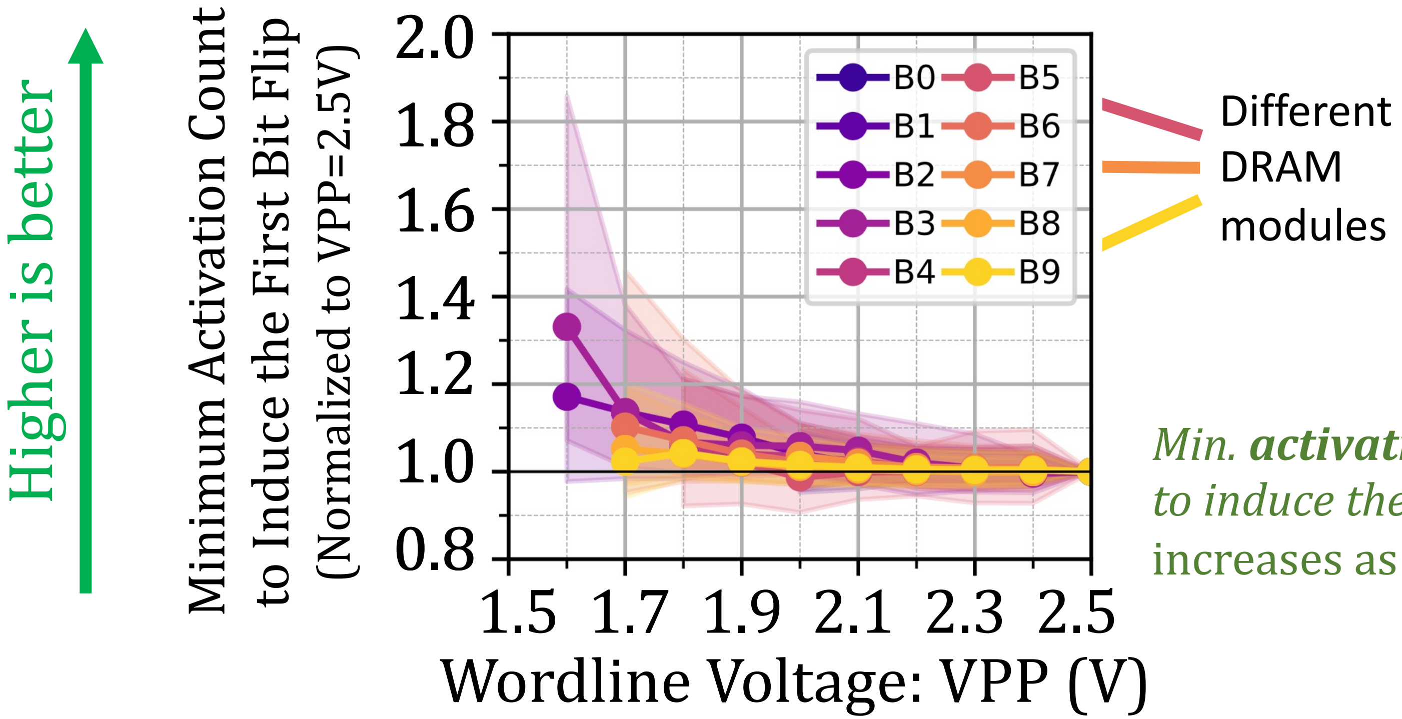
OBSERVATION 1

Fewer DRAM cells experience RowHammer bit flips under **reduced wordline voltage**

OBSERVATION 2

Reducing wordline voltage can cause **more DRAM cells** to experience bit flips in **a small fraction of rows (15.4%)**

Wordline Voltage's Effect on RowHammer

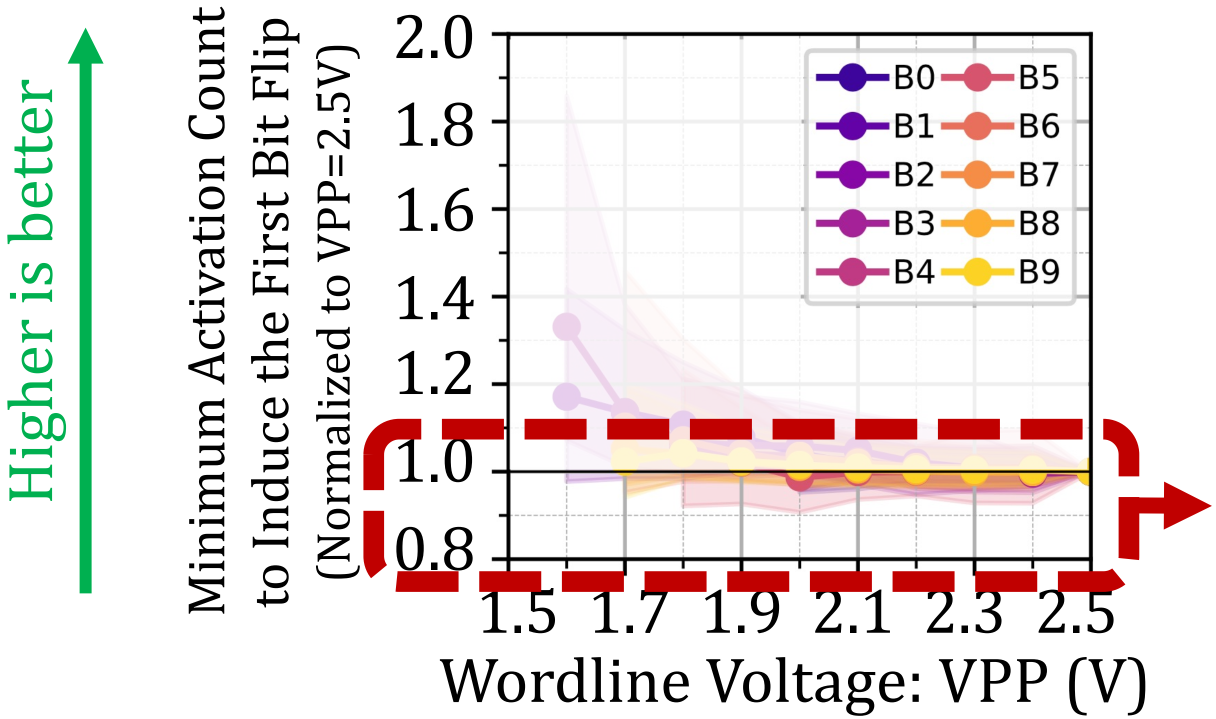


Min. ***activation count*** *to induce the first bit flip* increases as VPP reduces

OBSERVATION 4

The first bit flip occurs at **higher activation counts** as **wordline voltage reduces**

Wordline Voltage’s Effect on RowHammer

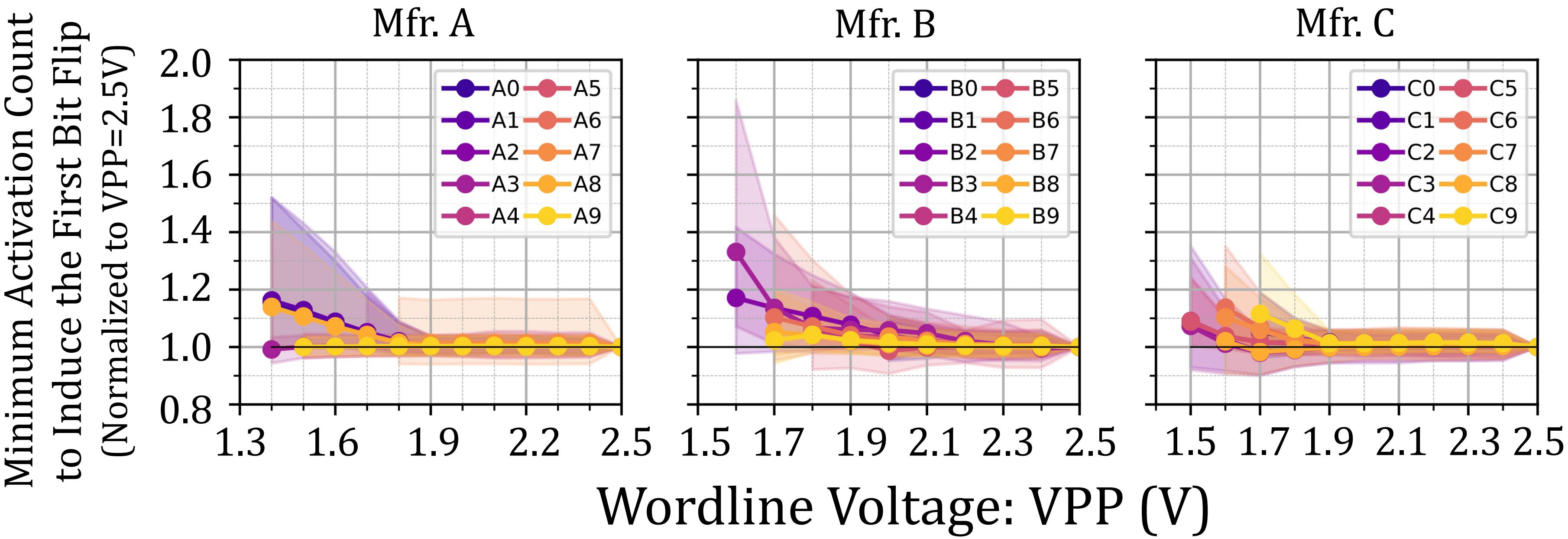


Min. ***activation count*** *to induce the first bit flip* ***reduces***

OBSERVATION 5

For a **small fraction of rows (14.2%)**, the first bit flip occurs at a **smaller activation count** as **wordline voltage reduces**

Wordline Voltage's Effect on RowHammer



OBSERVATION 4

The first bit flip occurs at **higher activation counts** as **wordline voltage reduces**

OBSERVATION 5

For a **small fraction of rows (14.2%)**, the first bit flip occurs at a **smaller activation count** as **wordline voltage reduces**

Also in the Paper

Wordline voltage's effect on *RowHammer vulnerability*
varies across different **DRAM rows** and **manufacturers**

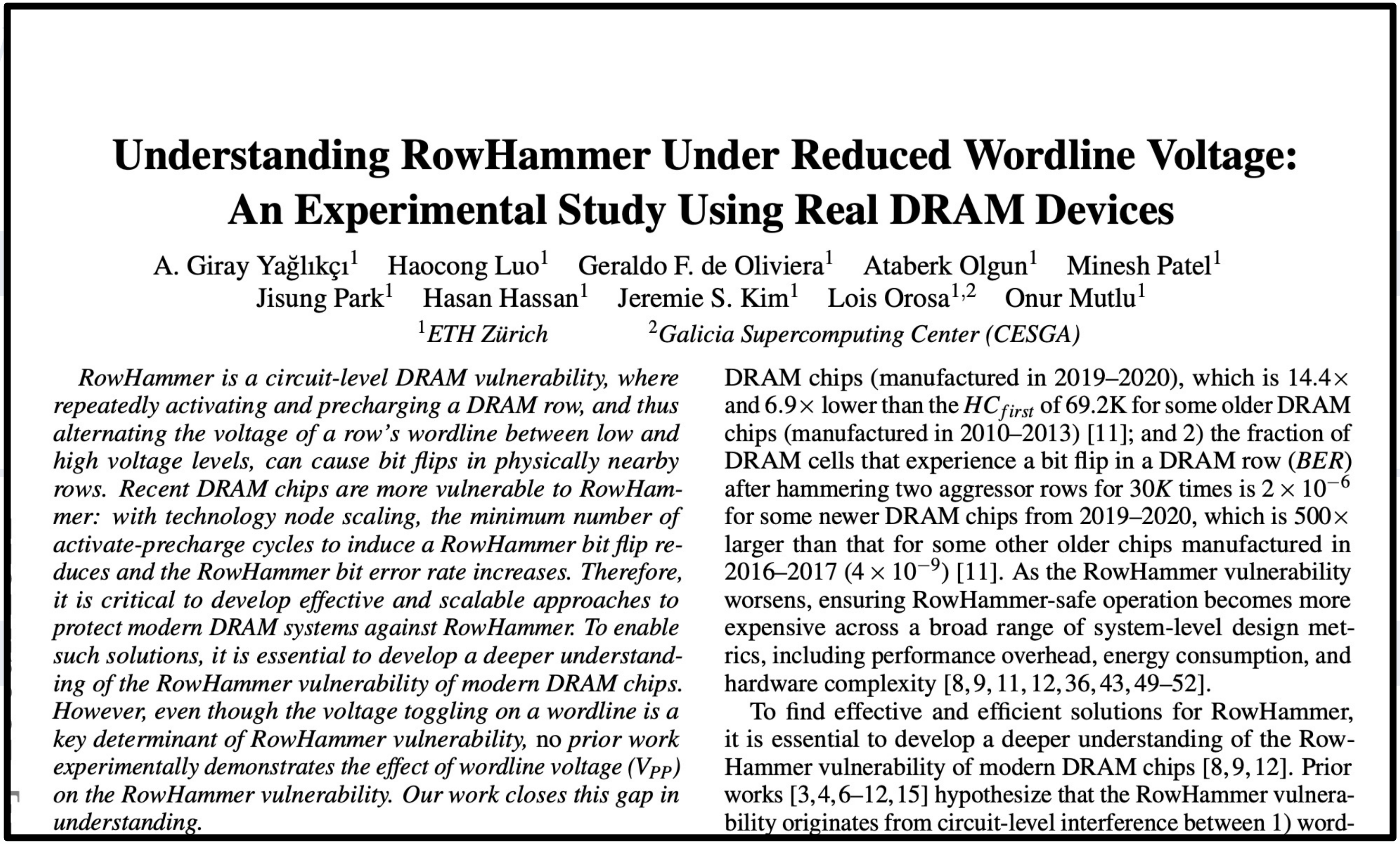
OBSERVATION 3

Change in *bit error rate*
varies across different **DRAM rows** and **manufacturers**

OBSERVATION 6

Change in *the activation count at which the first bit flip occurs*
varies across different **DRAM rows** and **manufacturers**

Also in the Paper



Understanding RowHammer Under Reduced Wordline Voltage: An Experimental Study Using Real DRAM Devices

A. Giray Yağlıkçı[1] Haocong Luo[1] Geraldo F. de Oliviera[1] Ataberk Olgun[1] Minesh Patel[1]
Jisung Park[1] Hasan Hassan[1] Jeremie S. Kim[1] Lois Orosa[1,2] Onur Mutlu[1]
[1]*ETH Zürich* [2]*Galicia Supercomputing Center (CESGA)*

RowHammer is a circuit-level DRAM vulnerability, where repeatedly activating and precharging a DRAM row, and thus alternating the voltage of a row's wordline between low and high voltage levels, can cause bit flips in physically nearby rows. Recent DRAM chips are more vulnerable to RowHammer: with technology node scaling, the minimum number of activate-precharge cycles to induce a RowHammer bit flip reduces and the RowHammer bit error rate increases. Therefore, it is critical to develop effective and scalable approaches to protect modern DRAM systems against RowHammer. To enable such solutions, it is essential to develop a deeper understanding of the RowHammer vulnerability of modern DRAM chips. However, even though the voltage toggling on a wordline is a key determinant of RowHammer vulnerability, no *prior work experimentally demonstrates the effect of wordline voltage* (V_{PP}) *on the RowHammer vulnerability. Our work closes this gap in understanding.*

DRAM chips (manufactured in 2019–2020), which is 14.4× and 6.9× lower than the HC_{first} of 69.2K for some older DRAM chips (manufactured in 2010–2013) [11]; and 2) the fraction of DRAM cells that experience a bit flip in a DRAM row (*BER*) after hammering two aggressor rows for 30*K* times is 2×10^{-6} for some newer DRAM chips from 2019–2020, which is 500× larger than that for some other older chips manufactured in 2016–2017 (4×10^{-9}) [11]. As the RowHammer vulnerability worsens, ensuring RowHammer-safe operation becomes more expensive across a broad range of system-level design metrics, including performance overhead, energy consumption, and hardware complexity [8,9,11,12,36,43,49–52].

To find effective and efficient solutions for RowHammer, it is essential to develop a deeper understanding of the RowHammer vulnerability of modern DRAM chips [8,9,12]. Prior works [3,4,6–12,15] hypothesize that the RowHammer vulnerability originates from circuit-level interference between 1) word-

Full paper on arXiv: https://arxiv.org/abs/2206.09999

Key Takeaway from RowHammer Analysis

Takeaway 1

Reducing wordline voltage **reduces RowHammer vulnerability**

- **15.2%** (66.9% max) **fewer bit flips** occur
- **Activation count** at which *the first bit flip* occurs **increases** by **7.4%** (85.8% max)

Outline

Motivation and Goal

Experimental Methodology

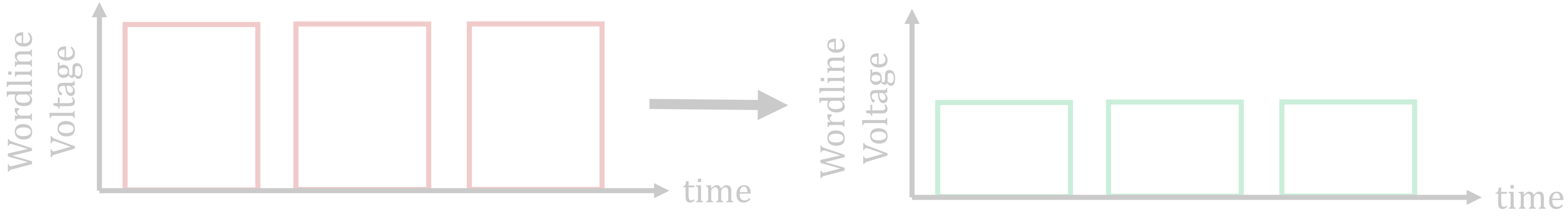
RowHammer Under Reduced Wordline Voltage

DRAM Operation Under Reduced Wordline Voltage

Conclusions

Our Hypothesis

Reducing **wordline voltage**
can **reduce RowHammer vulnerability**
without significantly affecting **reliable DRAM operation**



Reduction in Disturbance

Weaker Channel
in Access Transistor

Key Takeaways from DRAM Operation Analysis

Takeaway 2

208/272 tested DRAM chips **reliably operate** using **nominal timing parameters** due to the **built-in safety margins** (guardbands)

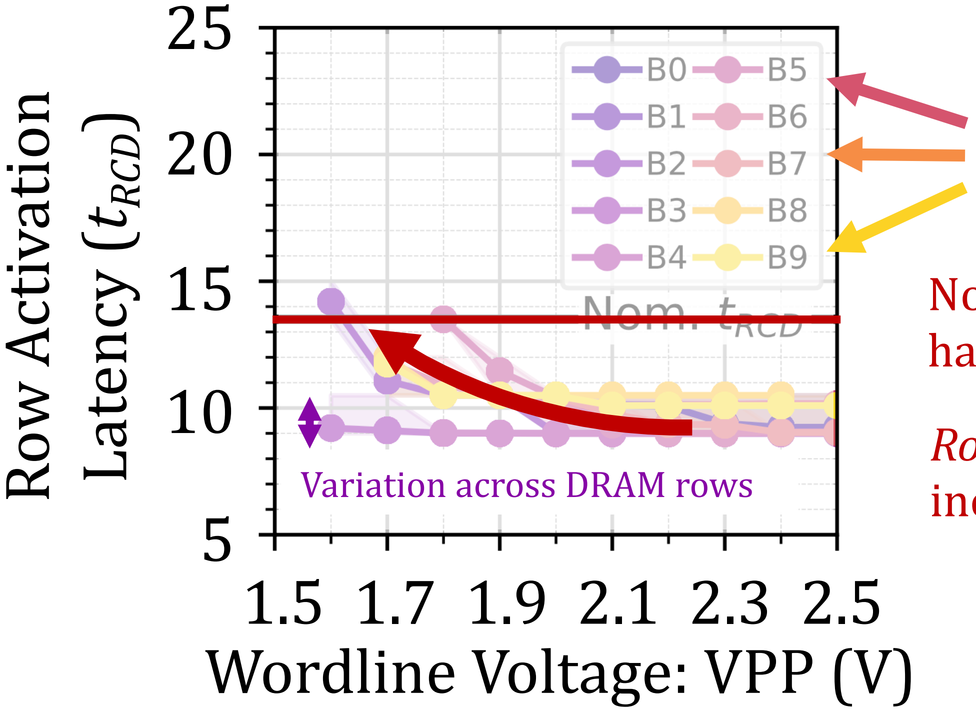
64/272 tested DRAM chips can **reliably operate** with **longer row activation latency** (24ns/15ns for 48/16 chips)

Takeaway 3

216/272 tested DRAM chips **reliably operate** using **nominal refresh rate** due to the **built-in safety margins** (guardbands)

56/272 tested DRAM chips can **reliably operate** using **single-error-correction ECC** *or* **2x the refresh rate** for ***only*** **16.4% of rows**

Wordline Voltage's Effect on Row Activation Latency



Different DRAM modules

Nominal activation latency has a significant guardband

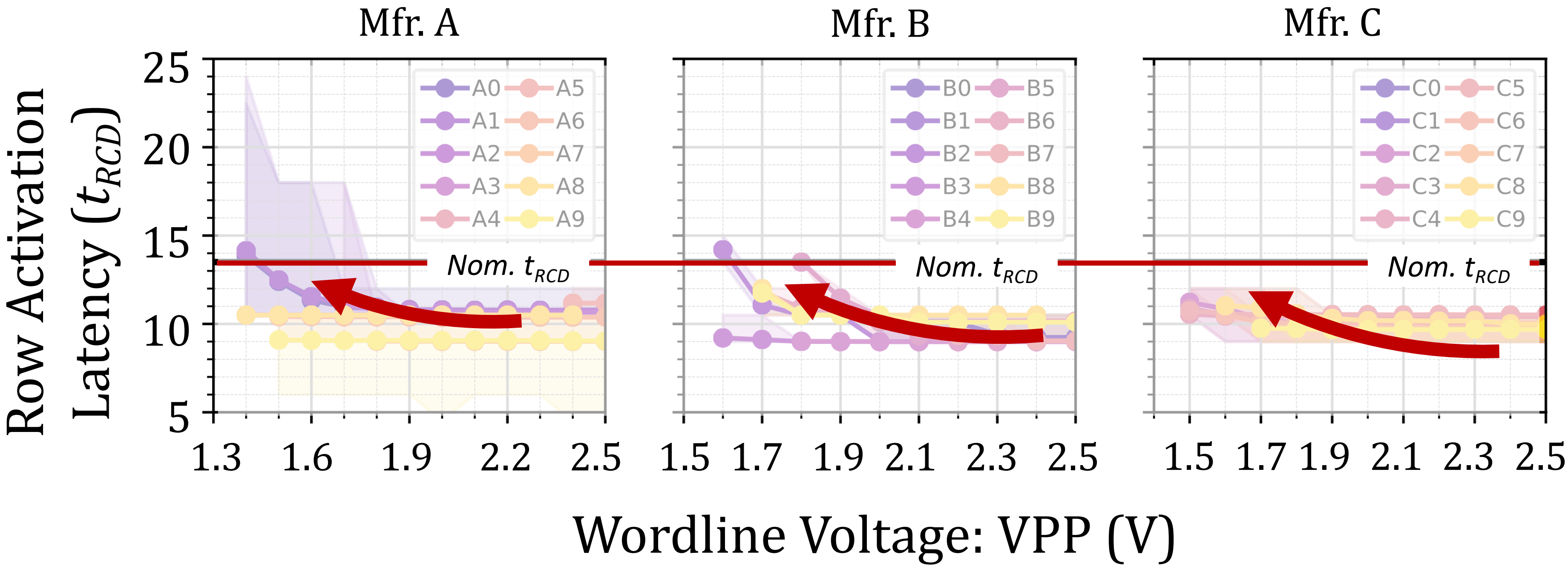
Row activation latency increases as V_{PP} reduces

OBSERVATION 7

Row activation latency **increases** with reduced **wordline voltage**

208 out of 272 DRAM chips complete row activation **before the nominal activation latency**

Wordline Voltage's Effect on Row Activation Latency

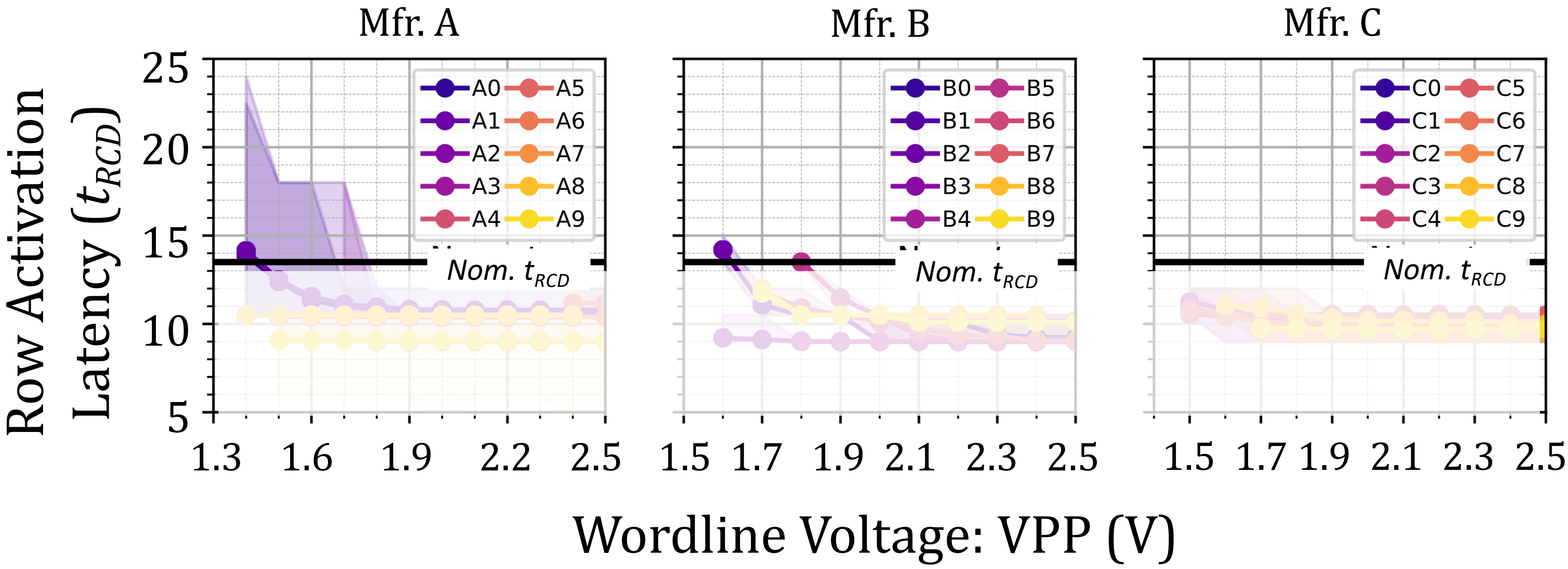


OBSERVATION 7

Row activation latency **increases** with reduced **wordline voltage**

208 out of 272 DRAM chips complete row activation **before the nominal activation latency**

Wordline Voltage's Effect on Row Activation Latency



48 DRAM chips from Mfr A. **reliably work** with a row activation latency of **24 ns**

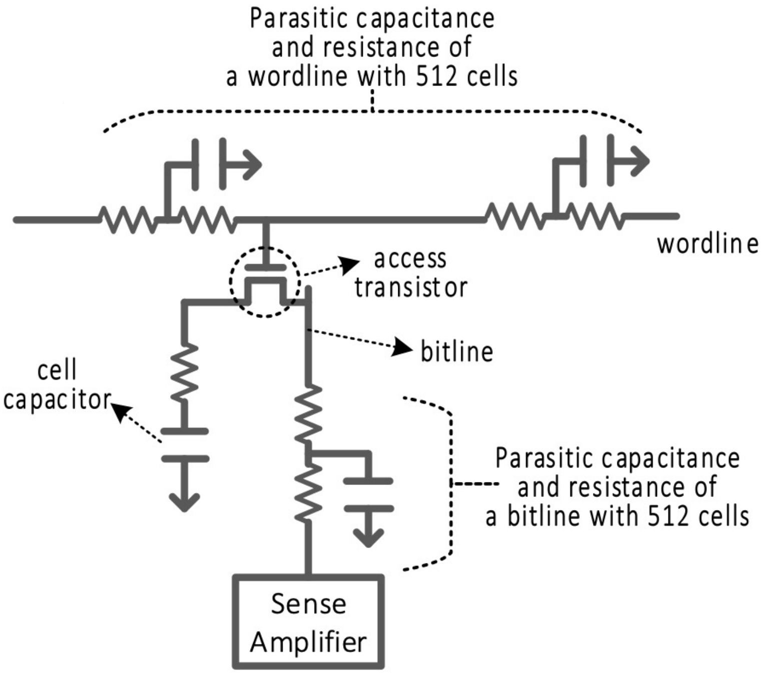
16 DRAM chips from Mfr. B **reliably work** with a row activation latency of **15 ns**

All DRAM chips from Mfr. C **reliably work** using the nominal latency of **13.5ns**

SPICE Simulation Methodology

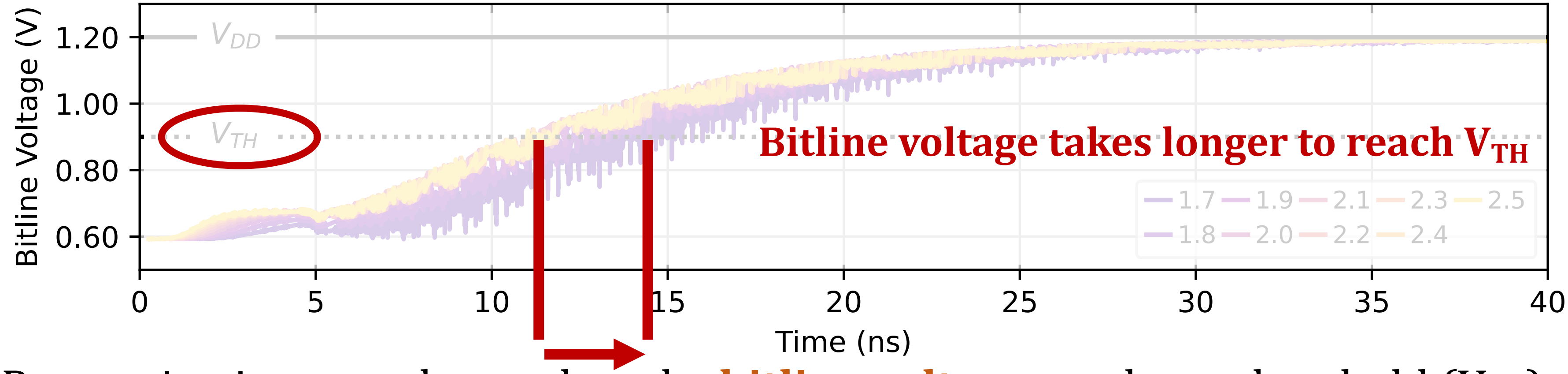
- Insights into **wordline voltage's affect on DRAM operation**
- 22 nm transistor model
- **Monte-Carlo analysis** with 5% variation and **10K iterations**

Component	**Parameters**
DRAM Cell	C: 16.8 fF, R: 698 Ω
Bitline	C: 100.5 fF, R: 6980 Ω
Cell Access NMOS	W: 55 nm, L: 85 nm
Sense Amp. NMOS	W: 1.3 um, L: 0.1 um
Sense Amp. PMOS	W: 0.9 um, L: 0.1 um



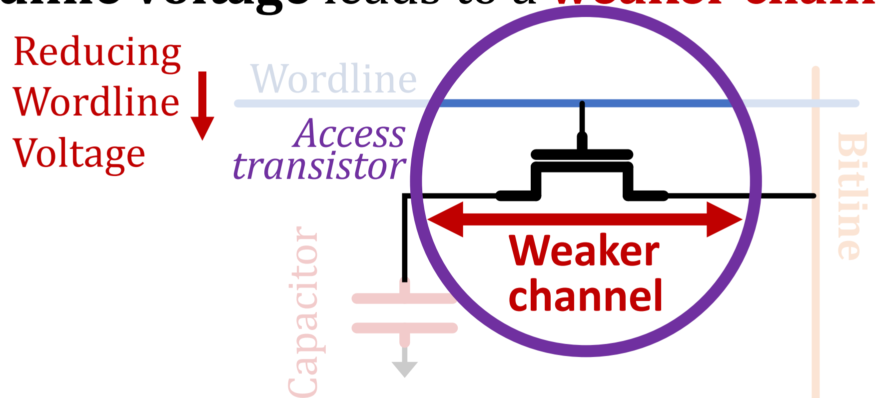
Chang et al., "[Understanding Reduced-Voltage Operation in Modern DRAM Devices: Experimental Characterization, Analysis, and Mechanisms]," SIGMETRICS, 2018. [SPICE Model on GitHub]

A Closer Look into Row Activation Latency



Bitline voltage takes longer to reach V_{TH}

- Row activation completes when the **bitline voltage** reaches a threshold (V_{TH})
- Reduced **wordline voltage** leads to a **weaker channel** in the access transistor



Reducing Wordline Voltage

Weaker channel

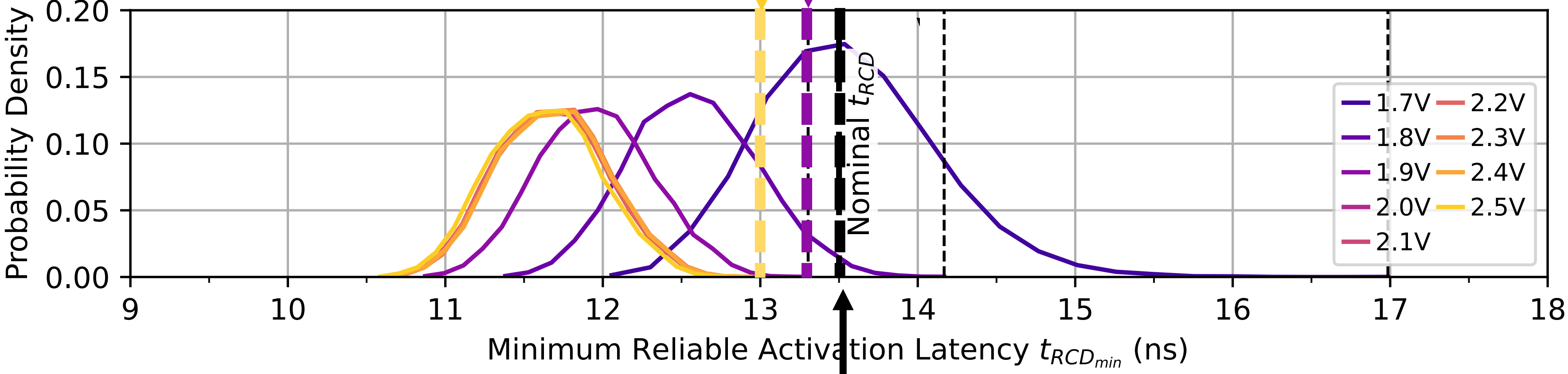
OBSERVATION 8

Row activation latency **increases** with **reduced** wordline voltage

Variation in Row Activation Latency

Worst case $t_{RCD_{min}}$ when VPP = 2.5V

Worst case $t_{RCD_{min}}$ when VPP = 1.9V



Nominal row activation latency

When wordline voltage is reduced from 2.5V to 1.9V:

- The worst-case row activation latency is still lower than nominal value
- The guardband reduces from **4.4%** to **1.5%**
  as the worst-case latency increases from **12.9ns** to **13.3ns**

OBSERVATION 9

SPICE simulation results **agree with** our observations based on experiments **on real chips**

The SPICE simulation results are *not identical* with real chip observations because the SPICE model *cannot* simulate a real DRAM chip's **exact behavior** without **proprietary** design and manufacturing information

Also in the Paper

Wordline voltage's effect on DRAM **charge restoration** process

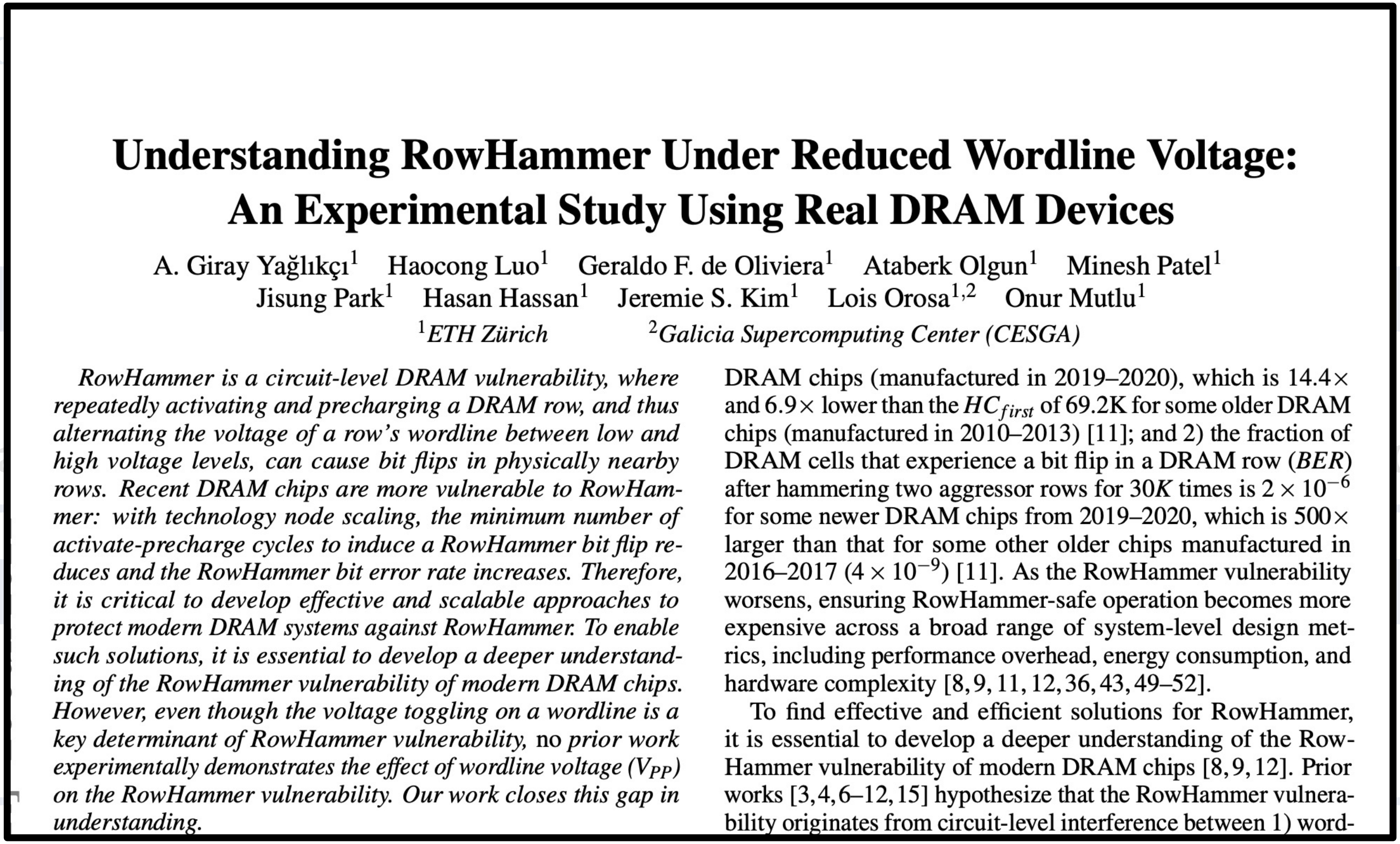
OBSERVATION 10

A DRAM cell's capacitor voltage **can saturate** at a **lower voltage** level **when wordline voltage is reduced**

OBSERVATION 11

A DRAM cell's **charge restoration latency** (t_{RASmin}) **can increase** with **reduced wordline voltage**

Also in the Paper



Understanding RowHammer Under Reduced Wordline Voltage: An Experimental Study Using Real DRAM Devices

A. Giray Yağlıkçı[1] Haocong Luo[1] Geraldo F. de Oliviera[1] Ataberk Olgun[1] Minesh Patel[1]
Jisung Park[1] Hasan Hassan[1] Jeremie S. Kim[1] Lois Orosa[1,2] Onur Mutlu[1]
[1]*ETH Zürich* [2]*Galicia Supercomputing Center (CESGA)*

RowHammer is a circuit-level DRAM vulnerability, where repeatedly activating and precharging a DRAM row, and thus alternating the voltage of a row's wordline between low and high voltage levels, can cause bit flips in physically nearby rows. Recent DRAM chips are more vulnerable to RowHammer: with technology node scaling, the minimum number of activate-precharge cycles to induce a RowHammer bit flip reduces and the RowHammer bit error rate increases. Therefore, it is critical to develop effective and scalable approaches to protect modern DRAM systems against RowHammer. To enable such solutions, it is essential to develop a deeper understanding of the RowHammer vulnerability of modern DRAM chips. However, even though the voltage toggling on a wordline is a key determinant of RowHammer vulnerability, no prior work *experimentally demonstrates the effect of wordline voltage (V_{PP}) on the RowHammer vulnerability. Our work closes this gap in understanding.*

DRAM chips (manufactured in 2019–2020), which is 14.4× and 6.9× lower than the HC_{first} of 69.2K for some older DRAM chips (manufactured in 2010–2013) [11]; and 2) the fraction of DRAM cells that experience a bit flip in a DRAM row (*BER*) after hammering two aggressor rows for 30K times is 2×10^{-6} for some newer DRAM chips from 2019–2020, which is 500× larger than that for some other older chips manufactured in 2016–2017 (4×10^{-9}) [11]. As the RowHammer vulnerability worsens, ensuring RowHammer-safe operation becomes more expensive across a broad range of system-level design metrics, including performance overhead, energy consumption, and hardware complexity [8, 9, 11, 12, 36, 43, 49–52].

To find effective and efficient solutions for RowHammer, it is essential to develop a deeper understanding of the RowHammer vulnerability of modern DRAM chips [8, 9, 12]. Prior works [3, 4, 6–12, 15] hypothesize that the RowHammer vulnerability originates from circuit-level interference between 1) word-

Full paper on arXiv: https://arxiv.org/abs/2206.09999

Key Takeaways from DRAM Operation Analysis

Takeaway 2

208/272 tested DRAM chips **reliably operate** using **nominal timing parameters** due to the **built-in safety margins** (guardbands)

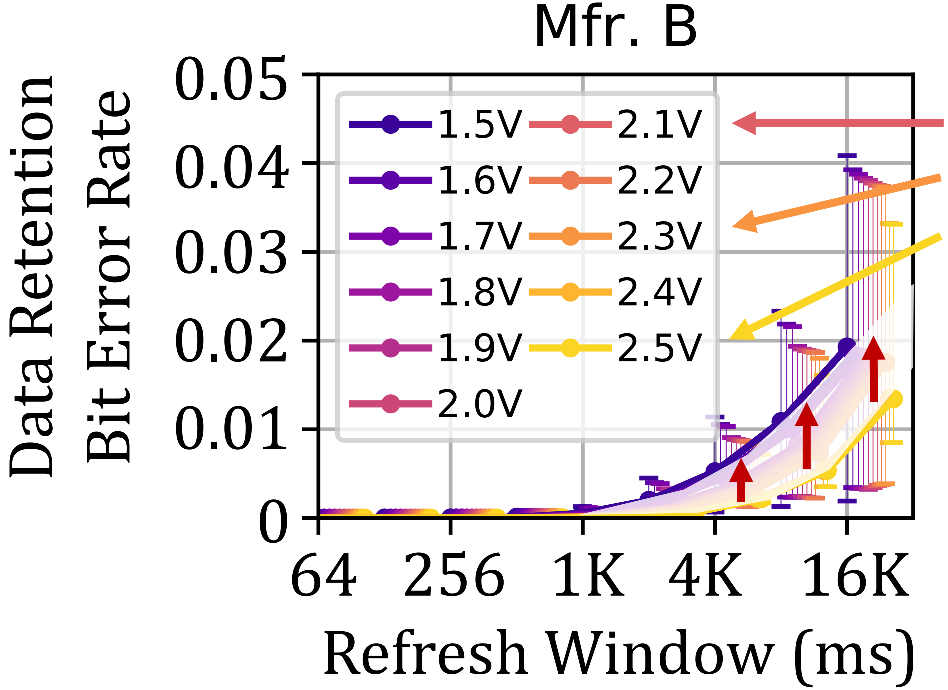
64/272 tested DRAM chips can **reliably operate** with **longer row activation latency** (24ns/15ns for 48/16 chips)

Takeaway 3

216/272 tested DRAM chips **reliably operate** using **nominal refresh rate** due to the **built-in safety margins** (guardbands)

56/272 tested DRAM chips can **reliably operate** using **single-error-correction ECC** *or* **2x the refresh rate** for ***only*** **16.4% of rows**

Wordline Voltage's Effect on DRAM Refresh



Different colors represent different wordline voltage levels

Data retention BER increases as wordline voltage reduces

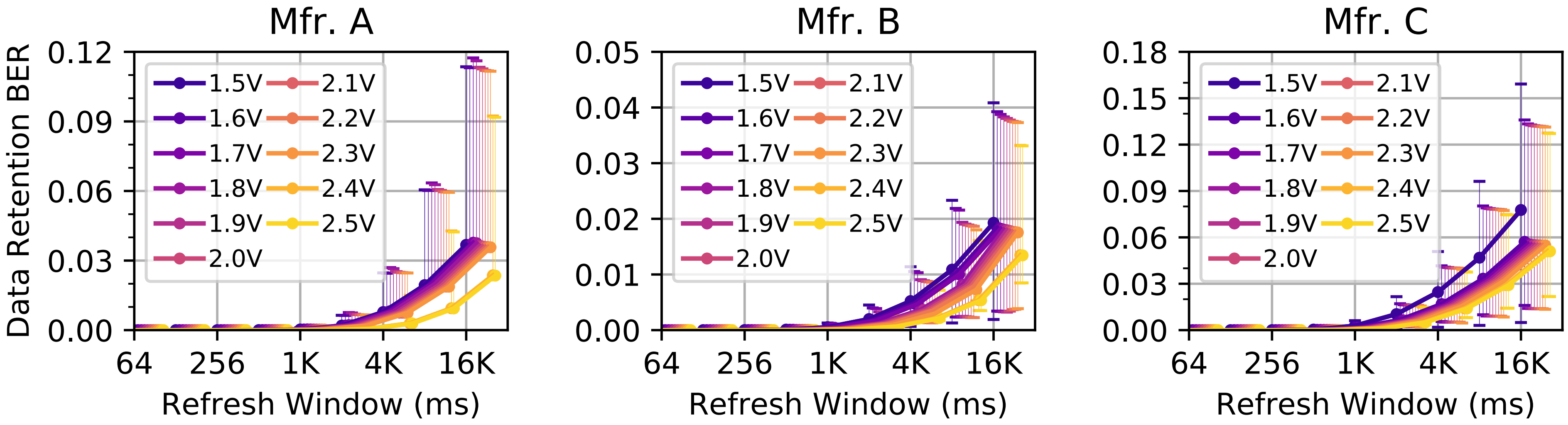
OBSERVATION 12

More DRAM cells tend to experience **data retention bit flips** when **wordline voltage is reduced**

OBSERVATION 13

216 out of 272 DRAM chips **reliably operate** using **nominal refresh rate** due to the **built-in safety margins** (guardbands)

Wordline Voltage's Effect on DRAM Refresh



OBSERVATION 12

More DRAM cells tend to experience **data retention bit flips** when **wordline voltage is reduced**

OBSERVATION 13

216 out of 272 DRAM chips **reliably operate** using **nominal refresh rate** due to the **built-in safety margins** (guardbands)

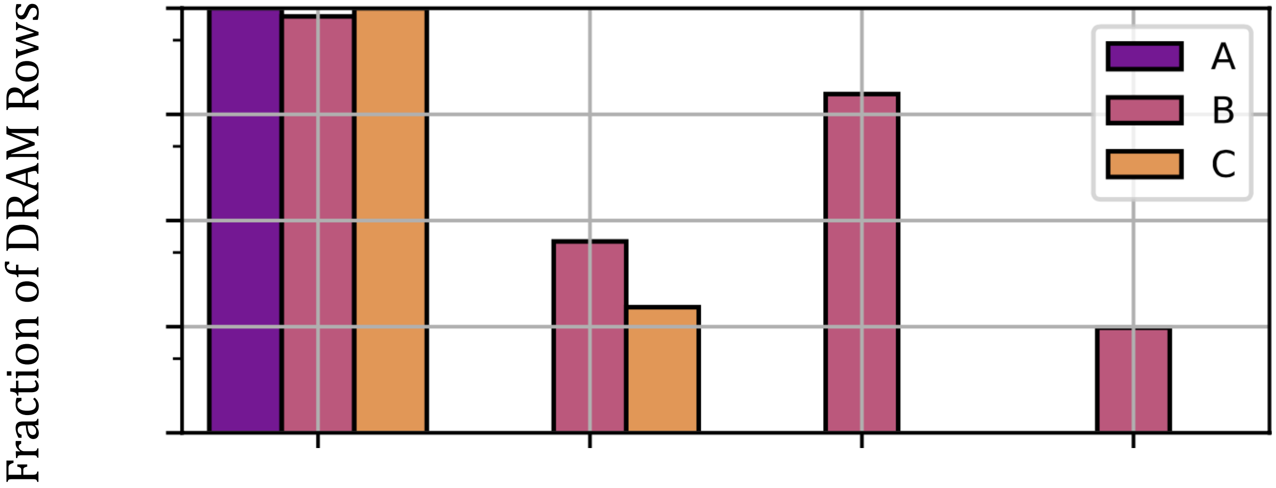
Spatial Distribution of Data Retention Bit Flips

- There are **no 64-bit words** with **more than one bit flip**

OBSERVATION 14

Data retention errors **can be avoided** using **single error correcting codes** at the smallest refresh window that yields *non-zero* bit error rate

- A **small fraction** of DRAM rows contain **erroneous words**



Number of 64-bit data words with one bit flip

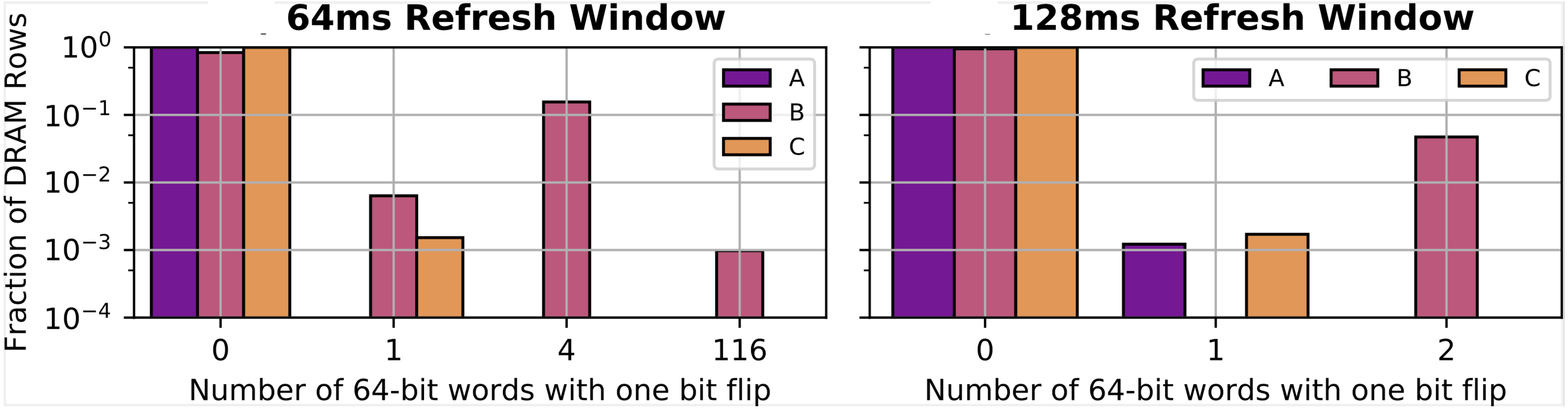
Spatial Distribution of Data Retention Bit Flips

- There are **no 64-bit words** with **more than one bit flip**

OBSERVATION 14

Data retention errors **can be avoided** using **single error correcting codes** at the smallest refresh window that yields *non-zero* bit error rate

- A **small fraction** of DRAM rows contain **erroneous words**



OBSERVATION 15

Only a small fraction (16.4%/5.0%) of DRAM rows have **erroneous words** at the smallest refresh rate (64ms/128ms) that yields *non-zero* bit error rate

Key Takeaways from DRAM Operation Analysis

Takeaway 2

208/272 tested DRAM chips **reliably operate** using **nominal timing parameters** due to the **built-in safety margins** (guardbands)

64/272 tested DRAM chips can **reliably operate** with **longer row activation latency** (24ns/15ns for 48/16 chips)

Takeaway 3

216/272 tested DRAM chips **reliably operate** using **nominal refresh rate** due to the **built-in safety margins** (guardbands)

56/272 tested DRAM chips can **reliably operate** using **single-error-correction ECC** *or* **2x the refresh rate** for ***only*** **16.4% of rows**

Outline

Motivation and Goal

Experimental Methodology

RowHammer Under Reduced Wordline Voltage

DRAM Operation Under Reduced Wordline Voltage

Conclusions

Conclusion

We provide *the first* RowHammer characterization **under reduced wordline voltage**

Experimental results with *272 real DRAM chips* show that **reducing wordline voltage:**

1. **Reduces RowHammer vulnerability**
   - **Bit error rate** caused by a RowHammer attack reduces by **15.2% (66.9% max)**
   - A row needs to be activated **7.4% more times (85.8% max)** to induce *the first* bit flip
2. **Increases row activation latency**
   - More than **76%** of the tested DRAM chips **reliably operate** using **nominal** timing parameters
   - Remaining **24%** **reliably operate** with **increased** (up to 24ns) row activation latency
3. **Reduces data retention time**
   - **80%** of the tested DRAM chips **reliably operate using nominal refresh rate**
   - Remaining **20%** **reliably operate** by
     - Using **single error correcting codes**
     - **Doubling the refresh rate** for **a small fraction (16.4%) of DRAM rows**

Reducing wordline voltage can **reduce RowHammer vulnerability**
without significantly affecting **reliable DRAM operation**

Understanding RowHammer Under Reduced Wordline Voltage

An Experimental Study Using Real DRAM Devices

Abdullah Giray Yağlıkçı
Haocong Luo   Geraldo F. de Oliviera   Ataberk Olgun
Minesh Patel   Jisung Park   Hasan Hassan   Jeremie S. Kim
Lois Orosa   Onur Mutlu

ETH zürich   SAFARI   CESGA Centro de Supercomputación de Galicia

Understanding RowHammer Under Reduced Wordline Voltage

An Experimental Study Using Real DRAM Devices

Abdullah Giray Yağlıkçı

Haocong Luo Geraldo F. de Oliviera Ataberk Olgun

Minesh Patel Jisung Park Hasan Hassan Jeremie S. Kim

Lois Orosa Onur Mutlu

ETH zürich SAFARI CESGA

Centro de Supercomputación de Galicia

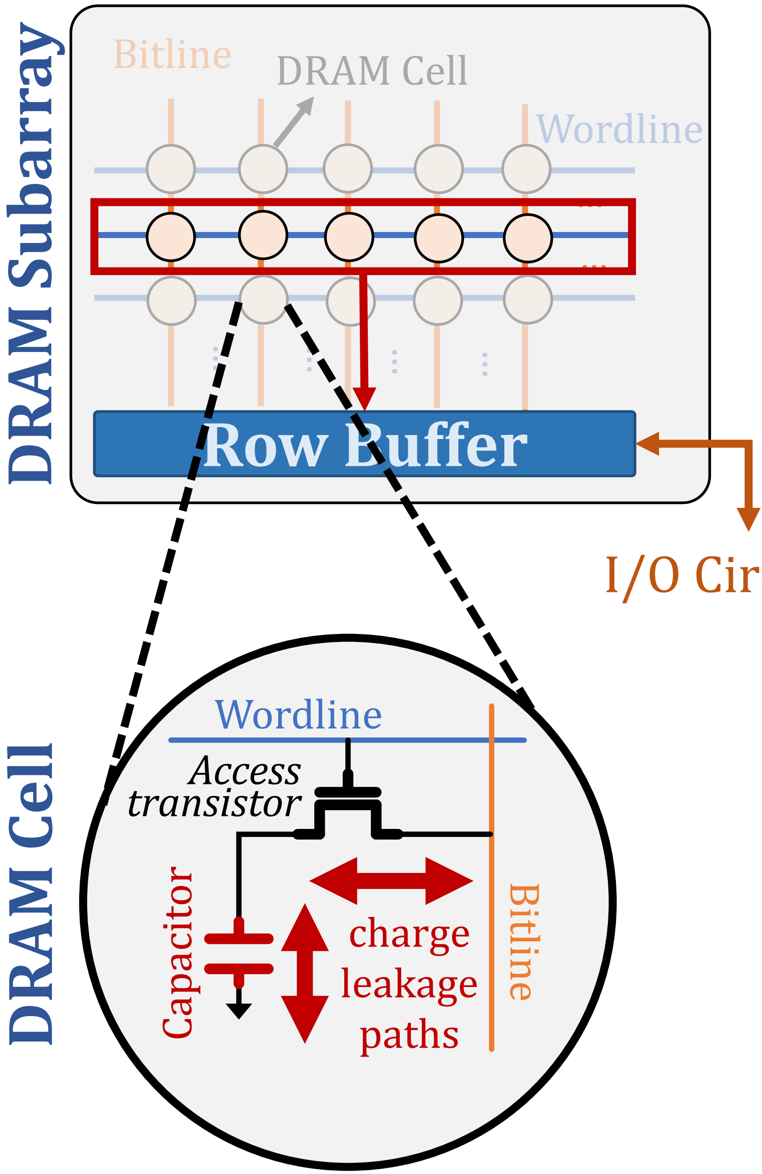
Understanding RowHammer Under Reduced Wordline Voltage

An Experimental Study Using Real DRAM Devices

BACKUP SLIDES

Abdullah Giray Yağlıkçı
Haocong Luo Geraldo F. de Oliviera Ataberk Olgun
Minesh Patel Jisung Park Hasan Hassan Jeremie S. Kim
Lois Orosa Onur Mutlu

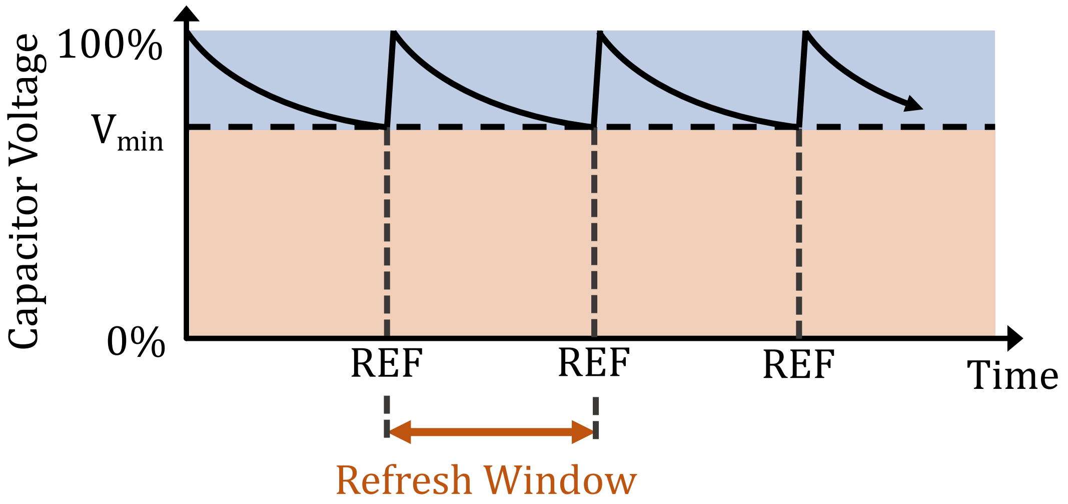
DRAM Operation



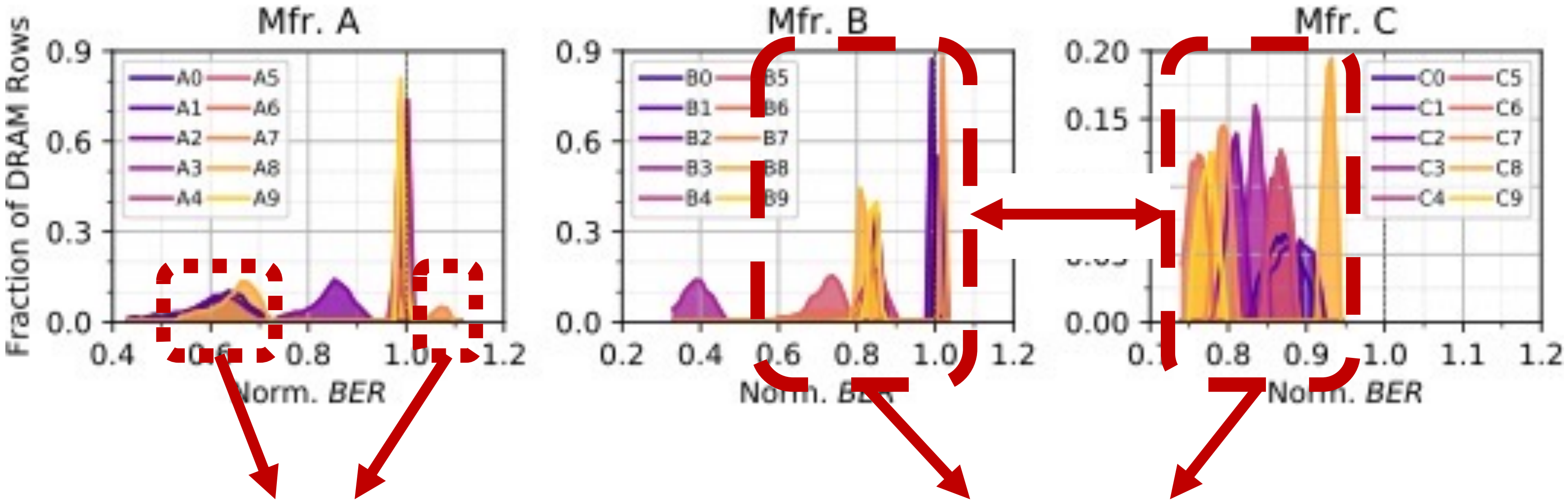
1 **Row Activation:** Fetching the row's content into the **row buffer**

2 **Column Access:** Read/Write a column in the row buffer

3 **Precharge:** Disconnect the row from the row buffer



Distribution of Bit Flips across DRAM Rows



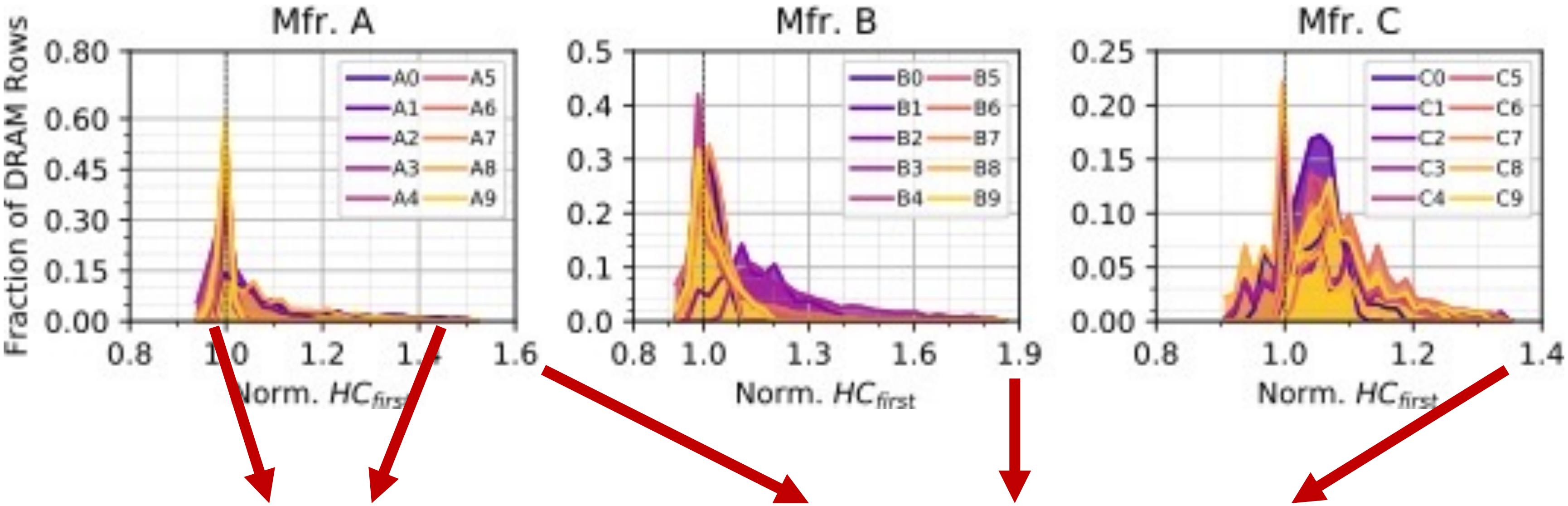
Across **rows**

Across **manufacturers**

OBSERVATION 3

***BER* reduction** with reduced wordline voltage varies across different **DRAM rows** and **manufacturers**

Distribution of HC_{first} across DRAM Rows



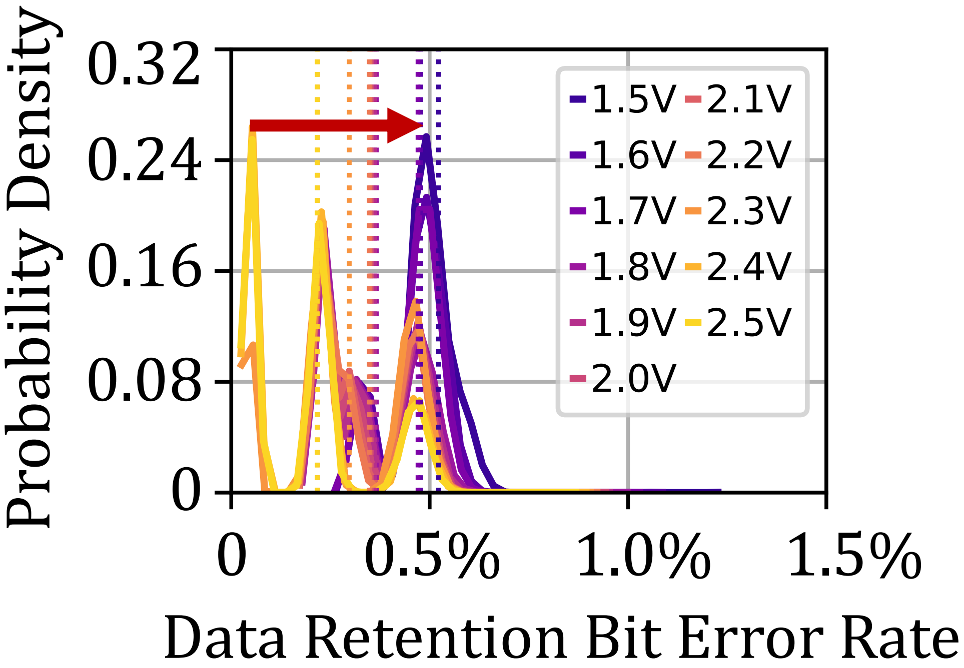
Across **rows**

Across **manufacturers**

OBSERVATION 3

HC_{first} reduction with reduced wordline voltage varies across different **DRAM rows** and **manufacturers**

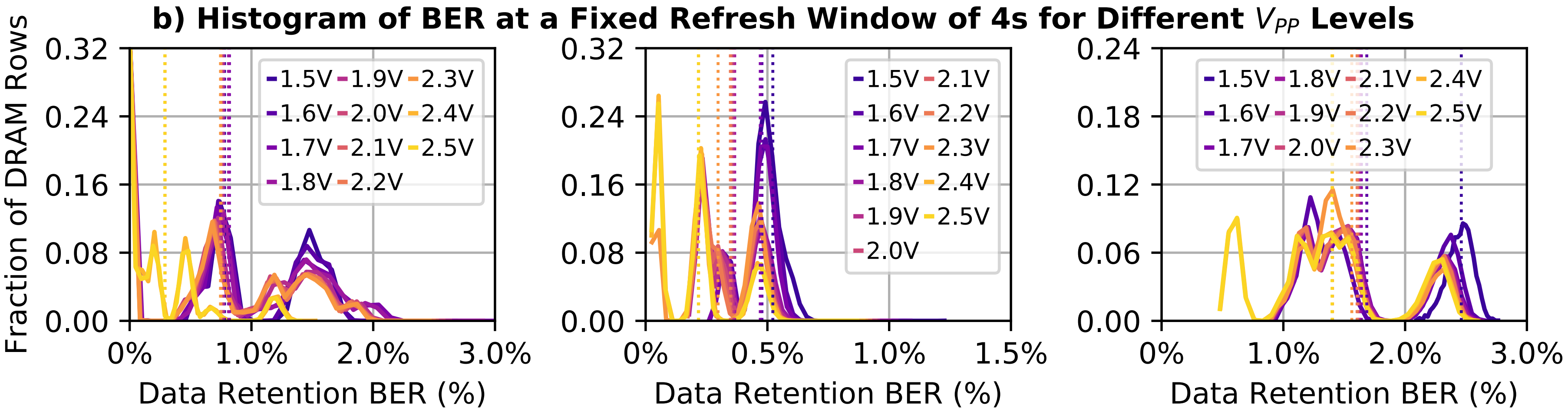
Wordline Voltage's Effect on DRAM Refresh



OBSERVATION 12

More DRAM cells tend to experience **data retention bit flips** when **wordline voltage is reduced**

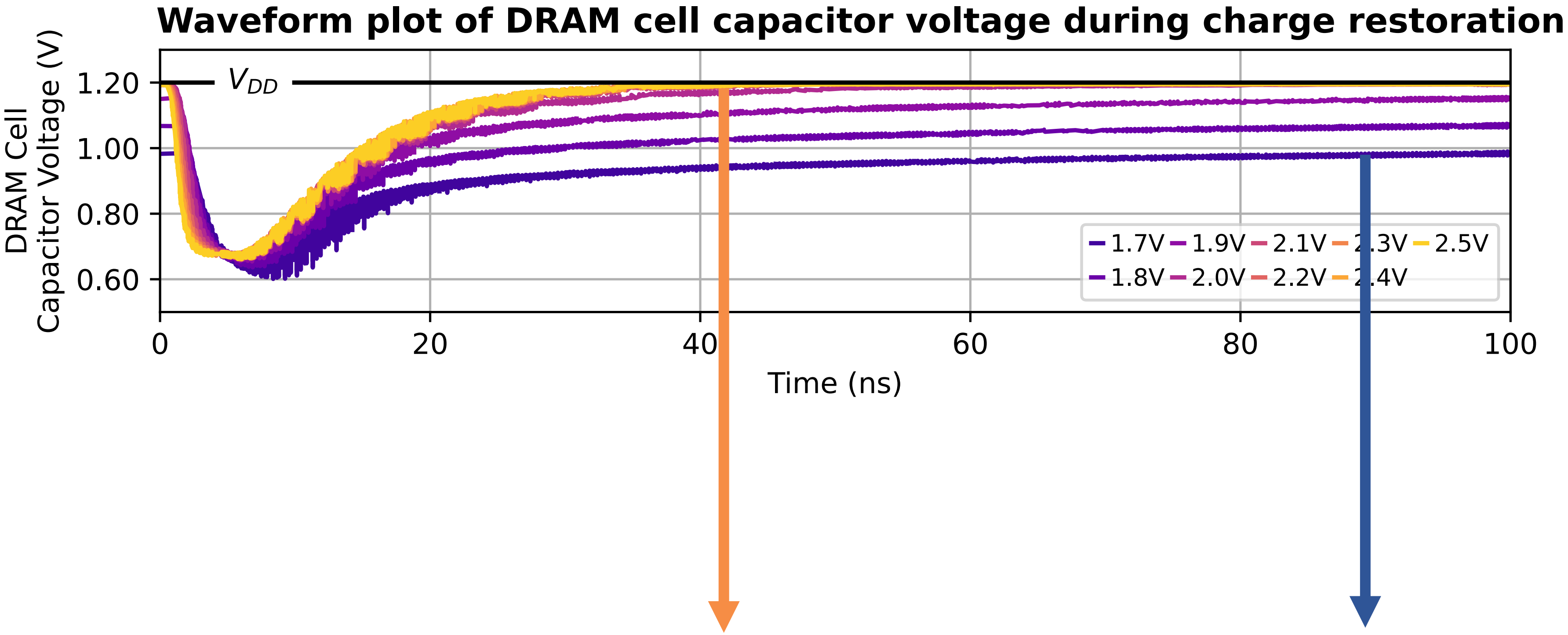
Wordline Voltage’s Effect on DRAM Refresh



OBSERVATION 12

More DRAM cells tend to experience **data retention bit flips** when **wordline voltage is reduced**

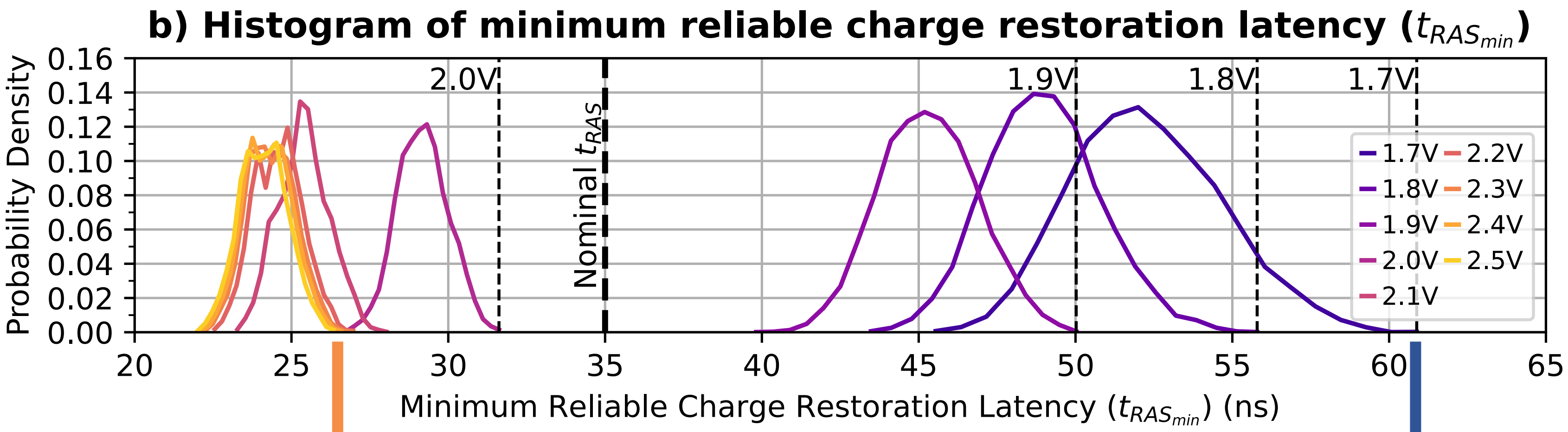
Charge Restoration Process



OBSERVATION 10

A DRAM cell's capacitor voltage **can saturate** at a **lower voltage** level **when wordline voltage is reduced**

Also in the Paper



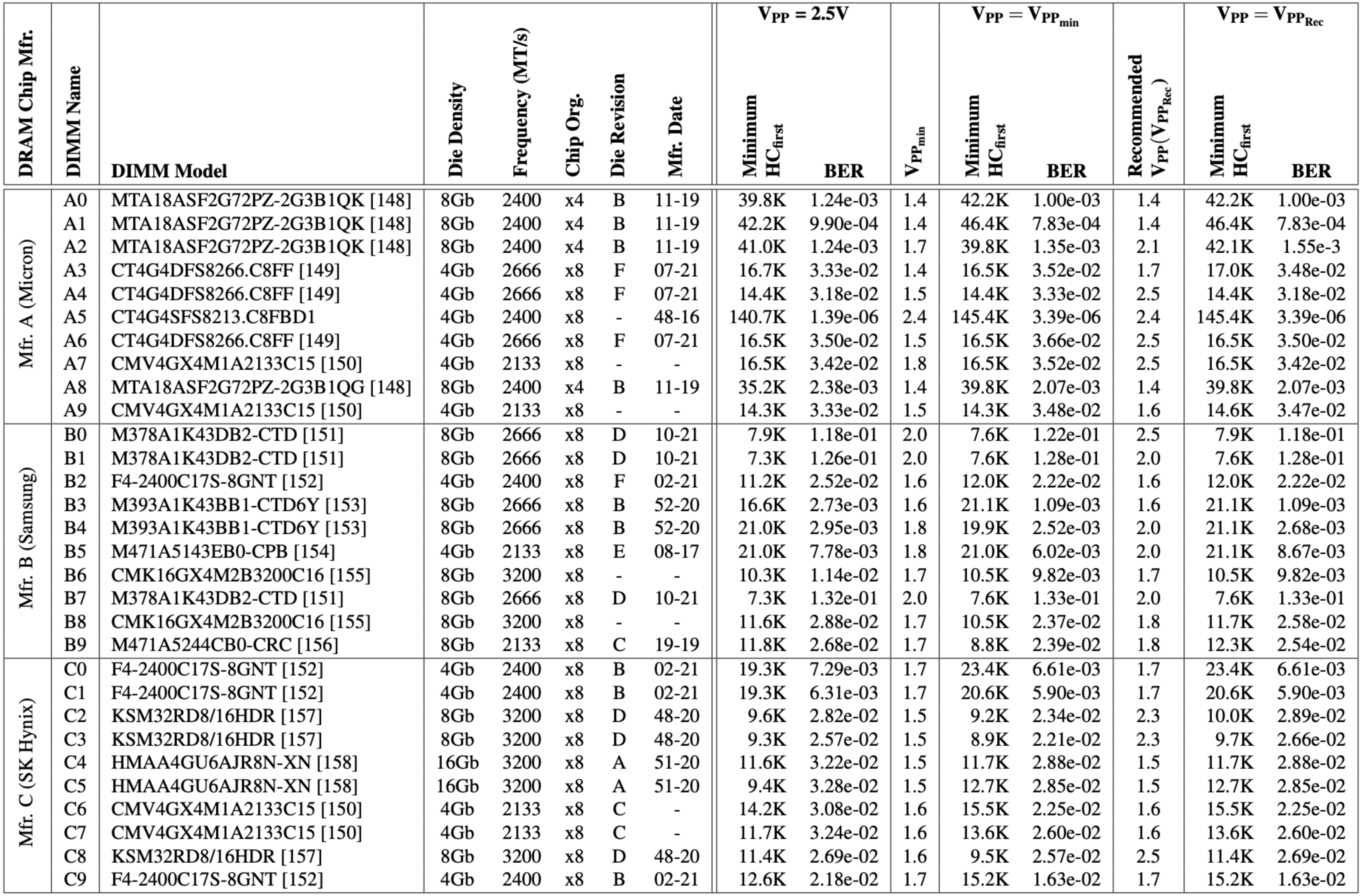
b) Histogram of minimum reliable charge restoration latency ($t_{RAS_{min}}$)

OBSERVATION 11

A DRAM cell's **charge restoration latency** (t_{RASmin})
can increase with **reduced wordline voltage**

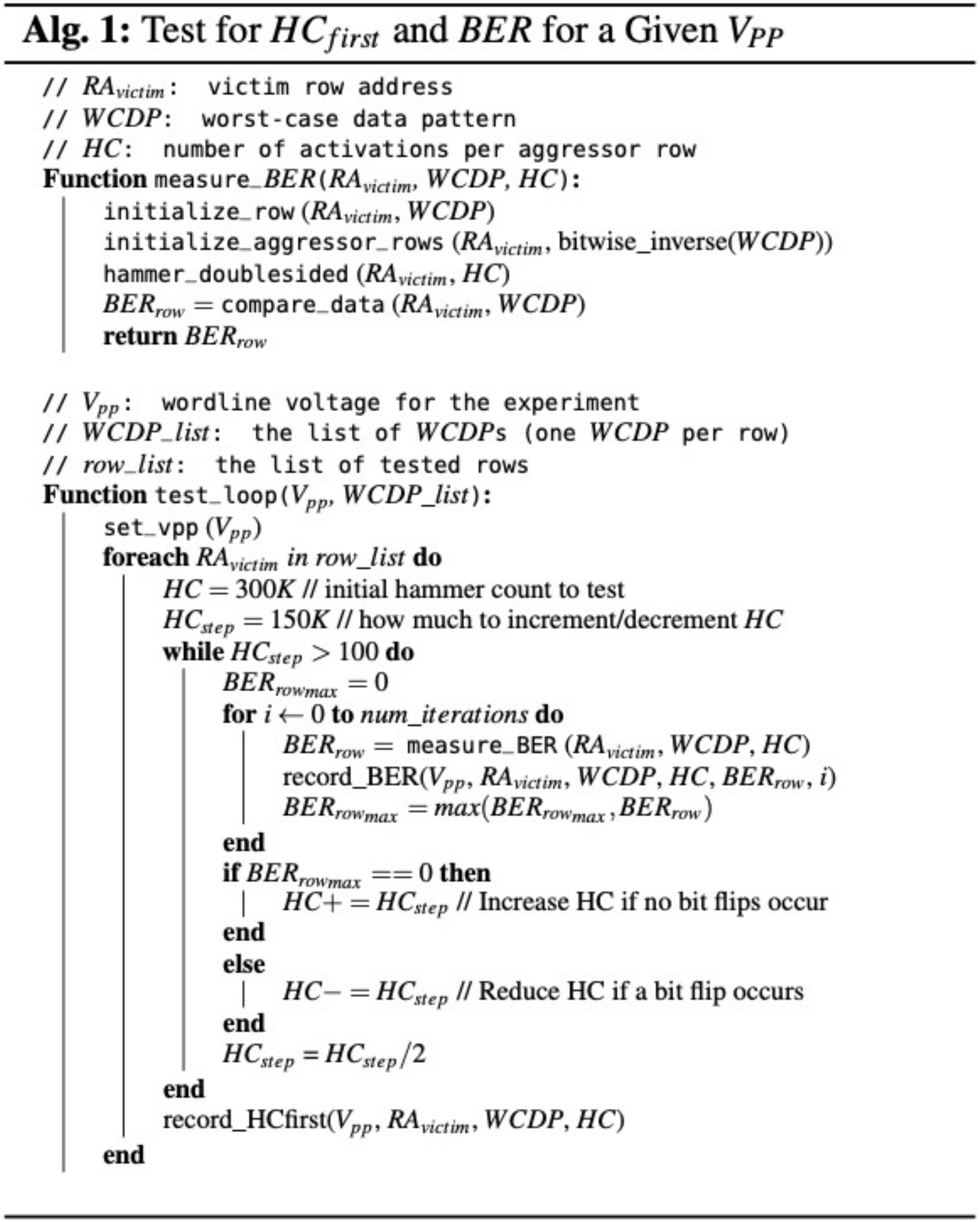
DRAM Chips Tested

Table 3: Tested DRAM modules and their characteristics when V_{PP}=2.5 V (nominal) and V_{PP}=V_{PPmin}. V_{PPmin} is specified for each module.



DRAM Chip Mfr.	DIMM Name	DIMM Model	Die Density	Frequency (MT/s)	Chip Org.	Die Revision	Mfr. Date	V_{PP} = 2.5V		$V_{PP_{min}}$	$V_{PP} = V_{PP_{min}}$		Recommended V_{PP} ($V_{PP_{Rec}}$)	$V_{PP} = V_{PP_{Rec}}$	
								Minimum HC_{first}	BER		Minimum HC_{first}	BER		Minimum HC_{first}	BER
Mfr. A (Micron)	A0	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	39.8K	1.24e-03	1.4	42.2K	1.00e-03	1.4	42.2K	1.00e-03
	A1	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	42.2K	9.90e-04	1.4	46.4K	7.83e-04	1.4	46.4K	7.83e-04
	A2	MTA18ASF2G72PZ-2G3B1QK [148]	8Gb	2400	x4	B	11-19	41.0K	1.24e-03	1.7	39.8K	1.35e-03	2.1	42.1K	1.55e-3
	A3	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	16.7K	3.33e-02	1.4	16.5K	3.52e-02	1.7	17.0K	3.48e-02
	A4	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	14.4K	3.18e-02	1.5	14.4K	3.33e-02	2.5	14.4K	3.18e-02
	A5	CT4G4SFS8213.C8FBD1	4Gb	2400	x8	-	48-16	140.7K	1.39e-06	2.4	145.4K	3.39e-06	2.4	145.4K	3.39e-06
	A6	CT4G4DFS8266.C8FF [149]	4Gb	2666	x8	F	07-21	16.5K	3.50e-02	1.5	16.5K	3.66e-02	2.5	16.5K	3.50e-02
	A7	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	-	-	16.5K	3.42e-02	1.8	16.5K	3.52e-02	2.5	16.5K	3.42e-02
	A8	MTA18ASF2G72PZ-2G3B1QG [148]	8Gb	2400	x4	B	11-19	35.2K	2.38e-03	1.4	39.8K	2.07e-03	1.4	39.8K	2.07e-03
	A9	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	-	-	14.3K	3.33e-02	1.5	14.3K	3.48e-02	1.6	14.6K	3.47e-02
Mfr. B (Samsung)	B0	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.9K	1.18e-01	2.0	7.6K	1.22e-01	2.5	7.9K	1.18e-01
	B1	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.3K	1.26e-01	2.0	7.6K	1.28e-01	2.0	7.6K	1.28e-01
	B2	F4-2400C17S-8GNT [152]	4Gb	2400	x8	F	02-21	11.2K	2.52e-02	1.6	12.0K	2.22e-02	1.6	12.0K	2.22e-02
	B3	M393A1K43BB1-CTD6Y [153]	8Gb	2666	x8	B	52-20	16.6K	2.73e-03	1.6	21.1K	1.09e-03	1.6	21.1K	1.09e-03
	B4	M393A1K43BB1-CTD6Y [153]	8Gb	2666	x8	B	52-20	21.0K	2.95e-03	1.8	19.9K	2.52e-03	2.0	21.1K	2.68e-03
	B5	M471A5143EB0-CPB [154]	4Gb	2133	x8	E	08-17	21.0K	7.78e-03	1.8	21.0K	6.02e-03	2.0	21.1K	8.67e-03
	B6	CMK16GX4M2B3200C16 [155]	8Gb	3200	x8	-	-	10.3K	1.14e-02	1.7	10.5K	9.82e-03	1.7	10.5K	9.82e-03
	B7	M378A1K43DB2-CTD [151]	8Gb	2666	x8	D	10-21	7.3K	1.32e-01	2.0	7.6K	1.33e-01	2.0	7.6K	1.33e-01
	B8	CMK16GX4M2B3200C16 [155]	8Gb	3200	x8	-	-	11.6K	2.88e-02	1.7	10.5K	2.37e-02	1.8	11.7K	2.58e-02
	B9	M471A5244CB0-CRC [156]	8Gb	2133	x8	C	19-19	11.8K	2.68e-02	1.7	8.8K	2.39e-02	1.8	12.3K	2.54e-02
Mfr. C (SK Hynix)	C0	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	19.3K	7.29e-03	1.7	23.4K	6.61e-03	1.7	23.4K	6.61e-03
	C1	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	19.3K	6.31e-03	1.7	20.6K	5.90e-03	1.7	20.6K	5.90e-03
	C2	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	9.6K	2.82e-02	1.5	9.2K	2.34e-02	2.3	10.0K	2.89e-02
	C3	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	9.3K	2.57e-02	1.5	8.9K	2.21e-02	2.3	9.7K	2.66e-02
	C4	HMAA4GU6AJR8N-XN [158]	16Gb	3200	x8	A	51-20	11.6K	3.22e-02	1.5	11.7K	2.88e-02	1.5	11.7K	2.88e-02
	C5	HMAA4GU6AJR8N-XN [158]	16Gb	3200	x8	A	51-20	9.4K	3.28e-02	1.5	12.7K	2.85e-02	1.5	12.7K	2.85e-02
	C6	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	C	-	14.2K	3.08e-02	1.6	15.5K	2.25e-02	1.6	15.5K	2.25e-02
	C7	CMV4GX4M1A2133C15 [150]	4Gb	2133	x8	C	-	11.7K	3.24e-02	1.6	13.6K	2.60e-02	1.6	13.6K	2.60e-02
	C8	KSM32RD8/16HDR [157]	8Gb	3200	x8	D	48-20	11.4K	2.69e-02	1.6	9.5K	2.57e-02	2.5	11.4K	2.69e-02
	C9	F4-2400C17S-8GNT [152]	4Gb	2400	x8	B	02-21	12.6K	2.18e-02	1.7	15.2K	1.63e-02	1.7	15.2K	1.63e-02

RowHammer Test



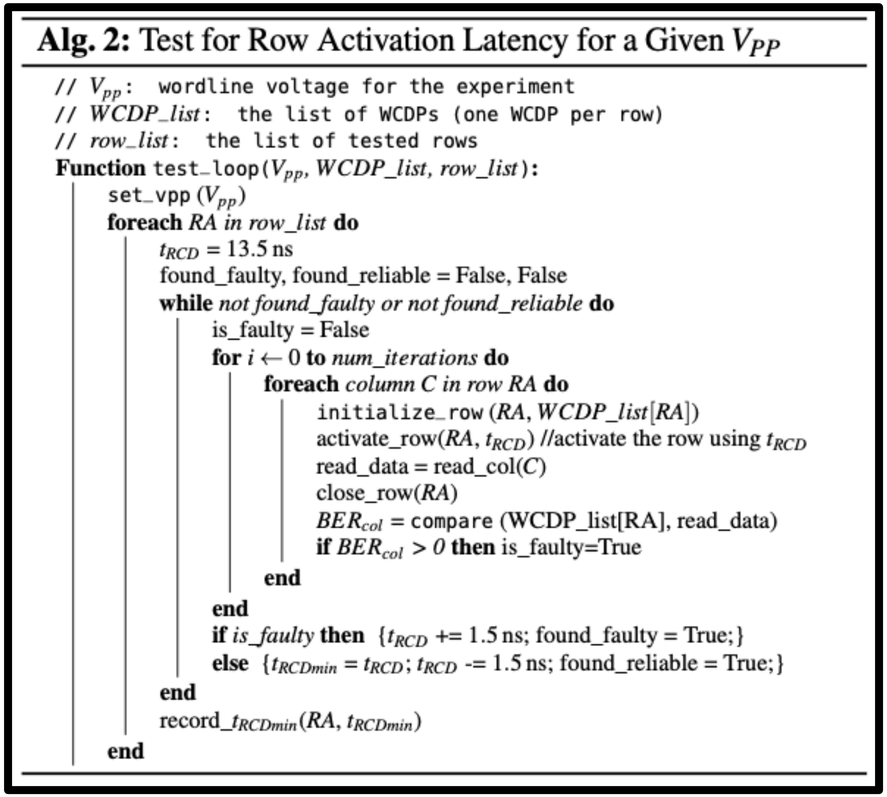
Alg. 1: Test for HC_{first} and BER for a Given V_{PP}

```
// $RA_{victim}$:  victim row address
// $WCDP$:  worst-case data pattern
// $HC$:  number of activations per aggressor row
Function measure_BER($RA_{victim}$, $WCDP$, $HC$):
    initialize_row ($RA_{victim}$, $WCDP$)
    initialize_aggressor_rows ($RA_{victim}$, bitwise_inverse($WCDP$))
    hammer_doublesided ($RA_{victim}$, $HC$)
    $BER_{row}$ = compare_data ($RA_{victim}$, $WCDP$)
    return $BER_{row}$

// $V_{pp}$:  wordline voltage for the experiment
// $WCDP\_list$:  the list of $WCDP$s (one $WCDP$ per row)
// $row\_list$:  the list of tested rows
Function test_loop($V_{pp}$, $WCDP\_list$):
    set_vpp ($V_{pp}$)
    foreach $RA_{victim}$ in $row\_list$ do
        $HC = 300K$ // initial hammer count to test
        $HC_{step} = 150K$ // how much to increment/decrement $HC$
        while $HC_{step} > 100$ do
            $BER_{rowmax} = 0$
            for $i \leftarrow 0$ to $num\_iterations$ do
                $BER_{row}$ = measure_BER ($RA_{victim}$, $WCDP$, $HC$)
                record_BER($V_{pp}$, $RA_{victim}$, $WCDP$, $HC$, $BER_{row}$, $i$)
                $BER_{rowmax} = max(BER_{rowmax}, BER_{row})$
            end
            if $BER_{rowmax} == 0$ then
                $HC += HC_{step}$ // Increase HC if no bit flips occur
            end
            else
                $HC -= HC_{step}$ // Reduce HC if a bit flip occurs
            end
            $HC_{step} = HC_{step}/2$
        end
        record_HCfirst($V_{pp}$, $RA_{victim}$, $WCDP$, $HC$)
    end
```

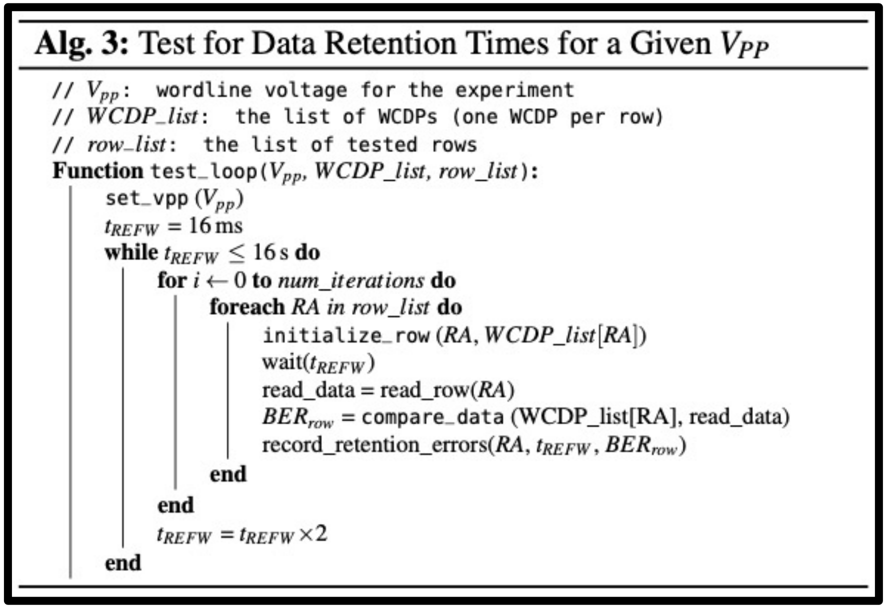
SAFARI

Row Activation and Refresh Rate Tests



Alg. 2: Test for Row Activation Latency for a Given V_{PP}

```
// $V_{pp}$: wordline voltage for the experiment
// $WCDP\_list$: the list of WCDPs (one WCDP per row)
// $row\_list$: the list of tested rows
Function test_loop($V_{pp}$, $WCDP\_list$, $row\_list$):
    set_vpp ($V_{pp}$)
    foreach $RA$ in $row\_list$ do
        $t_{RCD}$ = 13.5 ns
        found_faulty, found_reliable = False, False
        while not found_faulty or not found_reliable do
            is_faulty = False
            for $i \leftarrow 0$ to $num\_iterations$ do
                foreach column $C$ in row $RA$ do
                    initialize_row ($RA$, $WCDP\_list[RA]$)
                    activate_row($RA$, $t_{RCD}$) //activate the row using $t_{RCD}$
                    read_data = read_col($C$)
                    close_row($RA$)
                    $BER_{col}$ = compare (WCDP_list[RA], read_data)
                    if $BER_{col} > 0$ then is_faulty=True
                end
            end
            if is_faulty then {$t_{RCD}$ += 1.5 ns; found_faulty = True;}
            else {$t_{RCDmin} = t_{RCD}$; $t_{RCD}$ -= 1.5 ns; found_reliable = True;}
        end
        record_$t_{RCDmin}$($RA$, $t_{RCDmin}$)
    end
```



Alg. 3: Test for Data Retention Times for a Given V_{PP}

```
// $V_{pp}$: wordline voltage for the experiment
// $WCDP\_list$: the list of WCDPs (one WCDP per row)
// $row\_list$: the list of tested rows
Function test_loop($V_{pp}$, $WCDP\_list$, $row\_list$):
    set_vpp ($V_{pp}$)
    $t_{REFW}$ = 16 ms
    while $t_{REFW} \leq$ 16 s do
        for $i \leftarrow 0$ to $num\_iterations$ do
            foreach $RA$ in $row\_list$ do
                initialize_row ($RA$, $WCDP\_list[RA]$)
                wait($t_{REFW}$)
                read_data = read_row($RA$)
                $BER_{row}$ = compare_data (WCDP_list[RA], read_data)
                record_retention_errors($RA$, $t_{REFW}$, $BER_{row}$)
            end
        end
        $t_{REFW} = t_{REFW} \times 2$
    end
```

Understanding RowHammer Under Reduced Wordline Voltage

An Experimental Study Using Real DRAM Devices

BACKUP SLIDES

Abdullah Giray Yağlıkçı

Haocong Luo   Geraldo F. de Oliviera   Ataberk Olgun

Minesh Patel Jisung Park   Hasan Hassan   Jeremie S. Kim

Lois Orosa   Onur Mutlu

ETH zürich   SAFARI   CESGA Centro de Supercomputación de Galicia