Revisiting DRAM Read Disturbance

Identifying Inconsistencies Between Experimental Characterization and Device-Level Studies

Haocong Luo İsmail Emir Yüksel Ataberk Olgun
A. Giray Yağlıkçı Onur Mutlu

ETH Zurich

VTS' 25
28 April 2025

SAFARI

ETH zürich

Executive Summary

- **Goal:** Align and cross-validate the experimental characterization of DRAM read disturbance (RowHammer and RowPress) with the error mechanisms modeled by device-level simulation
  - **Challenge:** Gap between real-chip characterization and device-level mechanisms due to low-level DRAM array layout (i.e., true- and anti-cells)
- **Key Methodology:**
  - Extract key device-level read disturbance mechanisms from prior works
  - Reverse-engineer the true- and anti-cells layout of real DRAM chips
  - Perform real-chip characterization that directly match the access and data patterns studied in device-level works
- **Key Inconsistencies:**
  - For Double-Sided RowHammer, experimental characterization shows bitflips in both directions while device-level mechanisms suggest only 1→0 bitflips will happen
  - For Single-Sided RowPress, experimental characterization shows overwhelmingly 1→0 bitflips while device-level mechanisms suggest both kinds of bitflips will happen

Outline

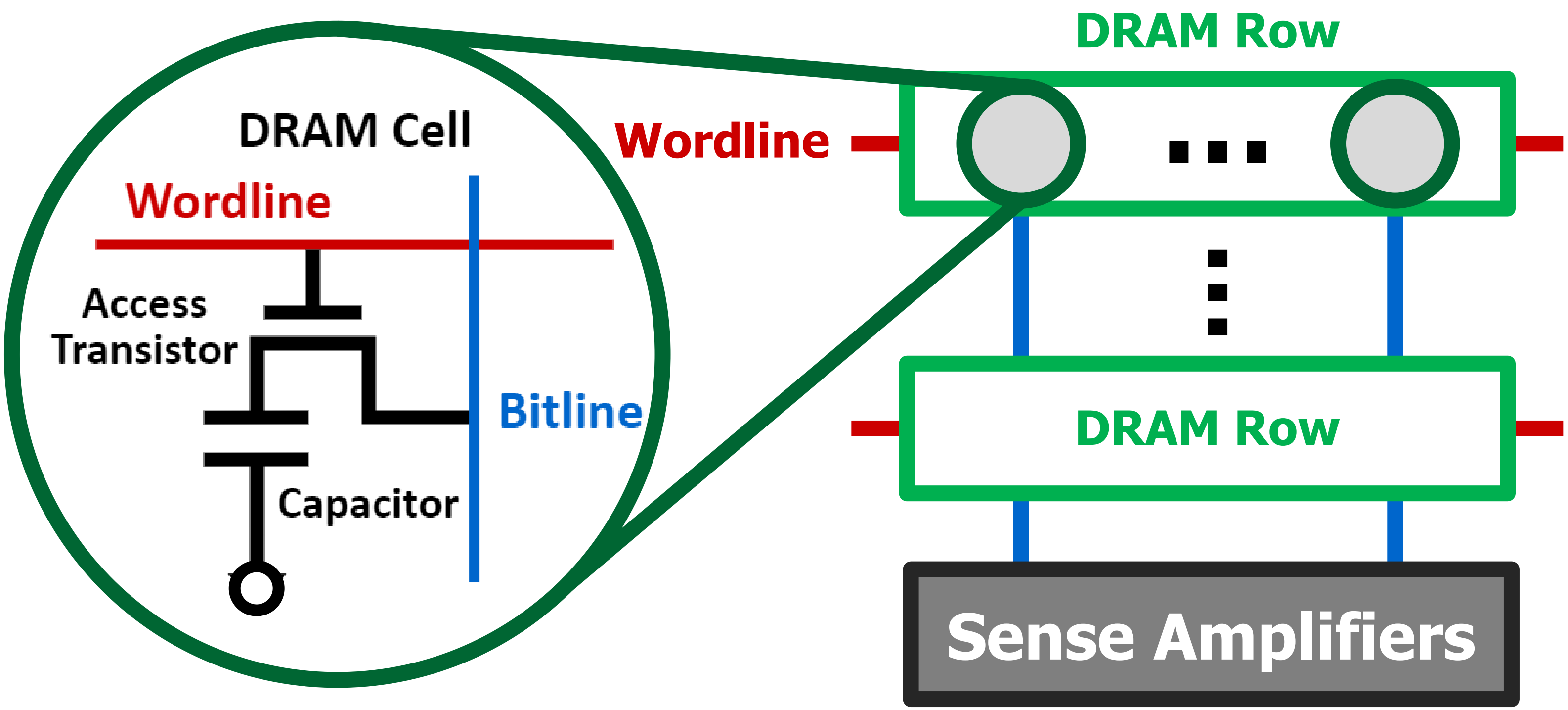
- **Background**
  - Key DRAM Organization & Operation
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

Outline

- **Background**
  - Key DRAM Organization & Operation
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

Background – DRAM Organization I

- **DRAM is the prevalent technology for main memory**
  - A **DRAM cell** stores one bit of information in a leaky capacitor
  - DRAM cells are organized into **DRAM rows**
  - Data are read from DRAM cells at **row-granularity** using **Sense Amplifiers**

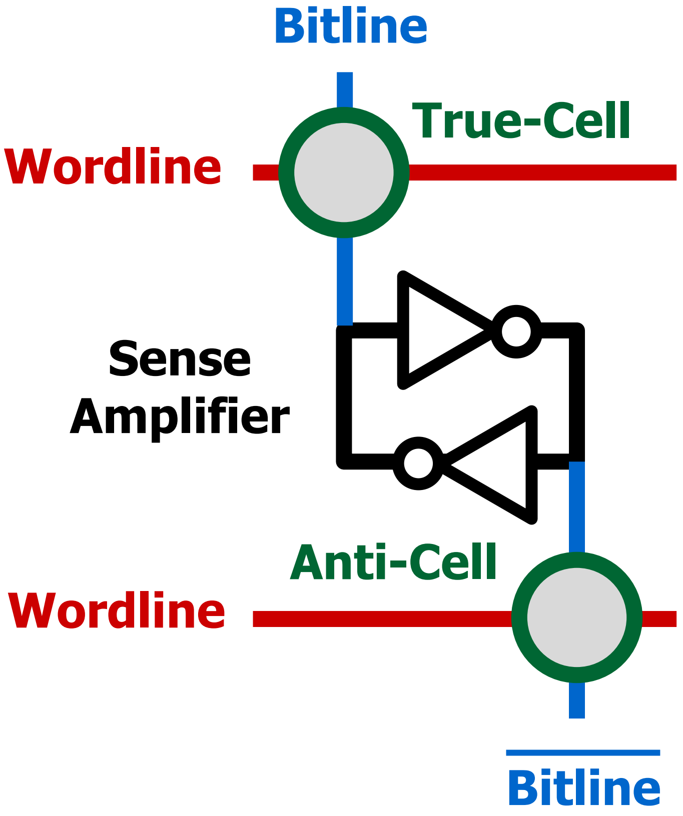


Background – DRAM Organization II

- **True-Cell and Anti-Cell**
  - The sense amplifier is a differential amplifier
  - A DRAM cell can represent a logical 1 by storing either positive or negative charge depending on if it is connected to $\mathbf{Bitline}$ or $\overline{\mathbf{Bitline}}$

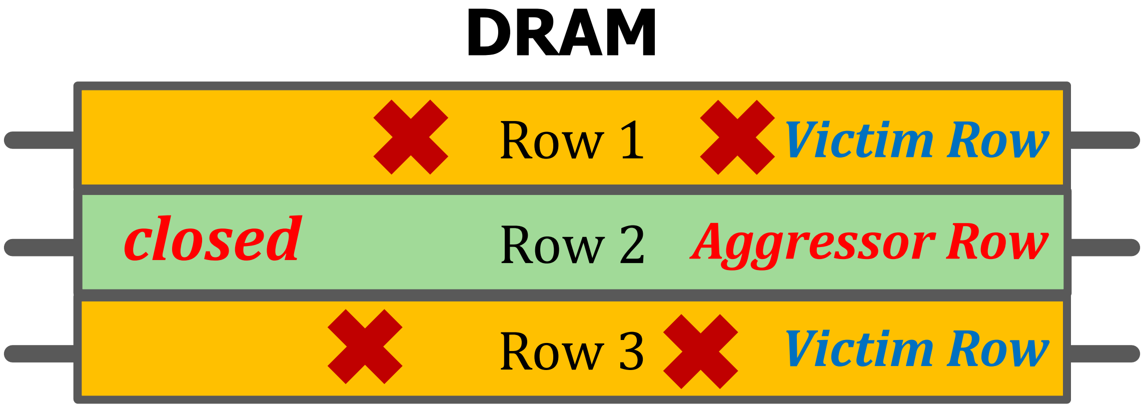
- **True-cell:** Represents a logical 1 by storing positive charge (i.e., $V_{Capacitor} = V_{Core}$)

- **Anti-cell:** Represents a logical 1 by storing negative charge (i.e., $V_{Capacitor} = V_{SS}$)



Background – DRAM Read Disturbance I

- **Read disturbance in DRAM breaks memory isolation**
  - Accessing a DRAM row (aggressor row) disturbs the integrity of data stored in DRAM cells of other **unaccessed** rows (victim rows), causing bitflips
- **Prominent Example I: RowHammer**

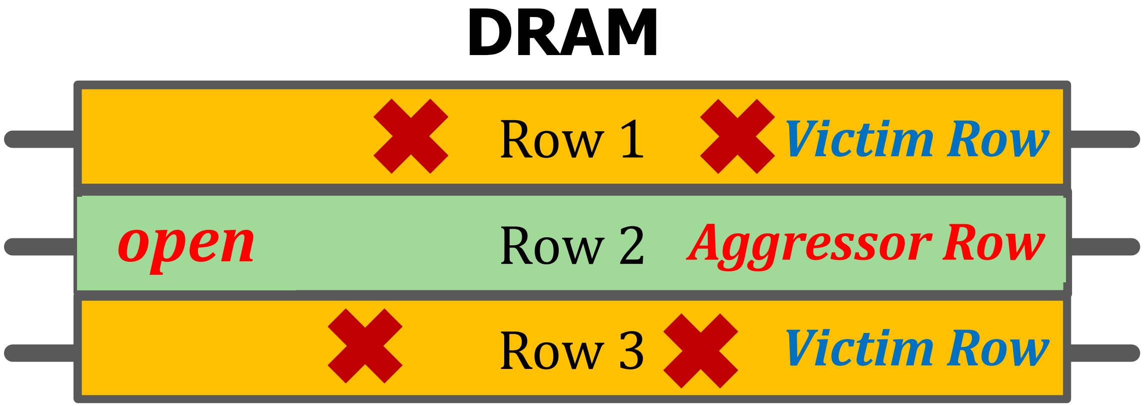


Repeatedly **opening (activating)** and **closing** a DRAM row **many times** causes **RowHammer bitflips** in adjacent rows

[Kim et al., "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors,“ in ISCA’14]

Background – DRAM Read Disturbance II

- **Read disturbance in DRAM breaks memory isolation**
  - Accessing a DRAM row (aggressor row) disturbs the integrity of data stored in DRAM cells of other **unaccessed** rows (victim rows), causing bitflips
- **Prominent Example II: RowPress**



Keeping a DRAM row **open for a long time**
causes bitflips in adjacent rows **without** requiring
as many row activations as RowHammer

[Luo et al., "RowPress: Amplifying Read Disturbance in Modern DRAM Chips," in ISCA'23]

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

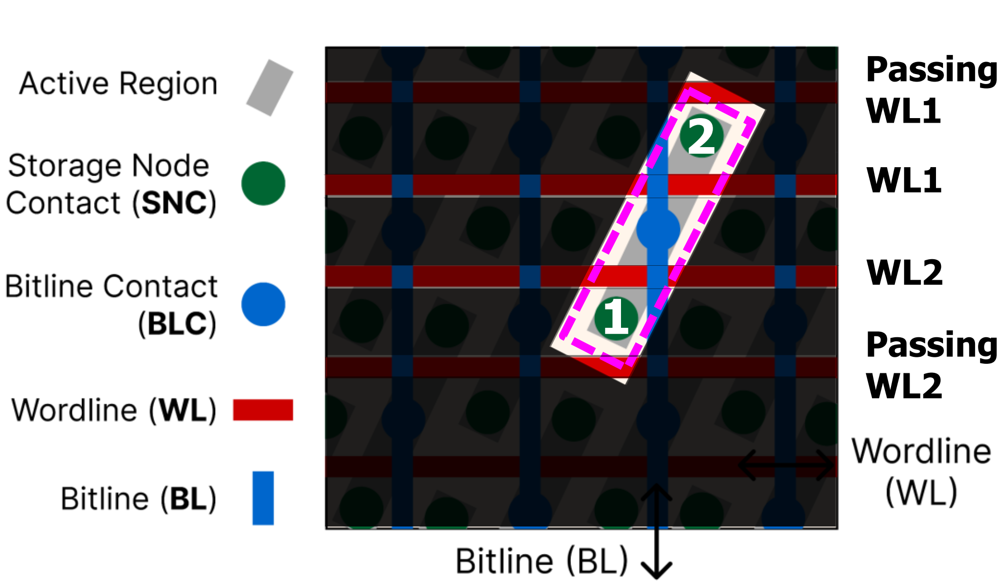
Device-Level Read Disturbance Mechanisms

Key Device-Level Characteristic 1:
Double-Sided RowHammer should only induce 1→0 bitflips

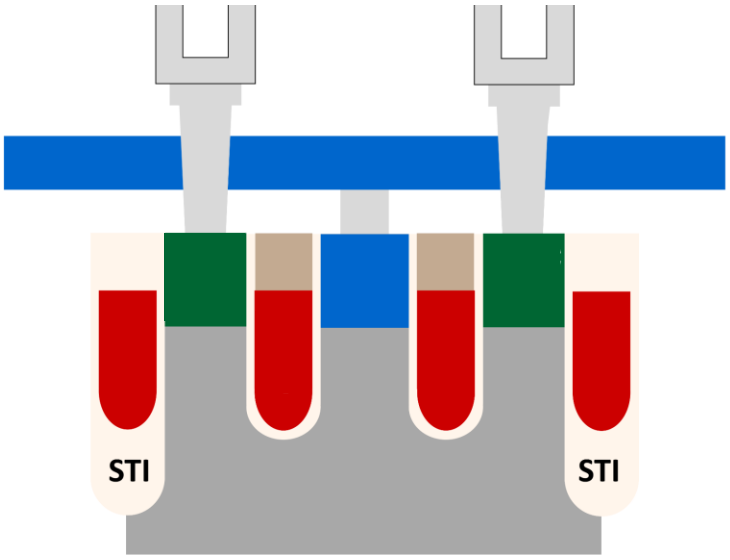
Key Device-Level Characteristic 2:
Single-Sided RowPress should induce both
1→0 and 0→1 bitflips

Device-Level Mechanisms – Physical Layout

- **Modern 6F^2 DRAM cell array layout**



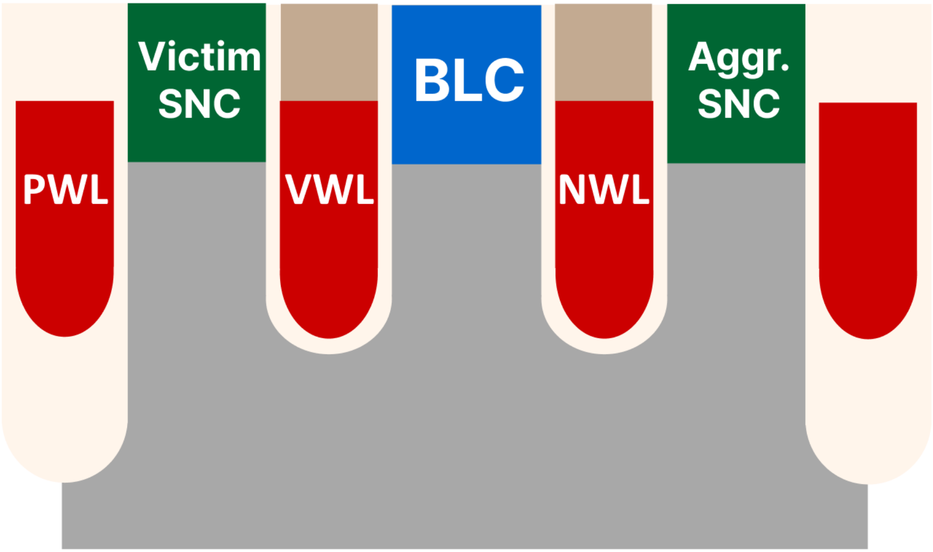
a) Physical Layout of 6F^2 DRAM (Top View)



b) Cross-section of an Active Region (Side View, 2 Cells)

Device-Level Mechanism – RowHammer I

- **Key Error Mechanisms of RowHammer**
  - Trap-assisted Electron Migration [Yang+, EDL’19] [Walker+, TED’21] [Zhou+, IRPS’23]

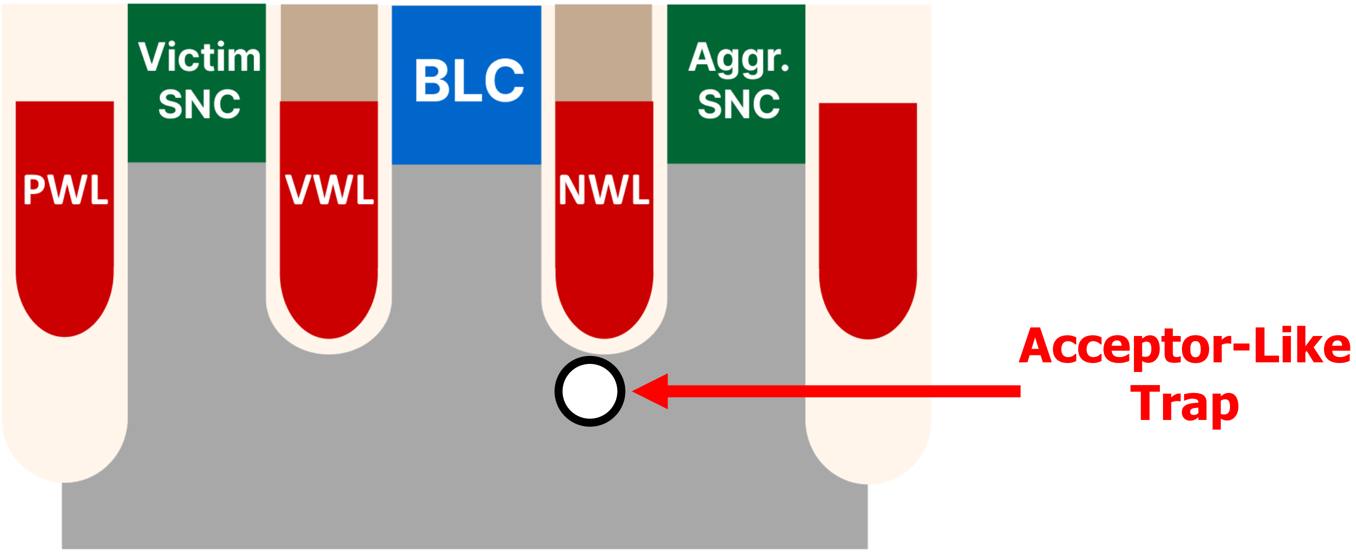


PWL: Passing Wordline **VWL:** Victim Wordline

NWL: Neighboring Wordline (Aggressor)

Device-Level Mechanism – RowHammer I

- **Key Error Mechanisms of RowHammer**
  - Trap-assisted Electron Migration [Yang+, EDL’19] [Walker+, TED’21] [Zhou+, IRPS’23]

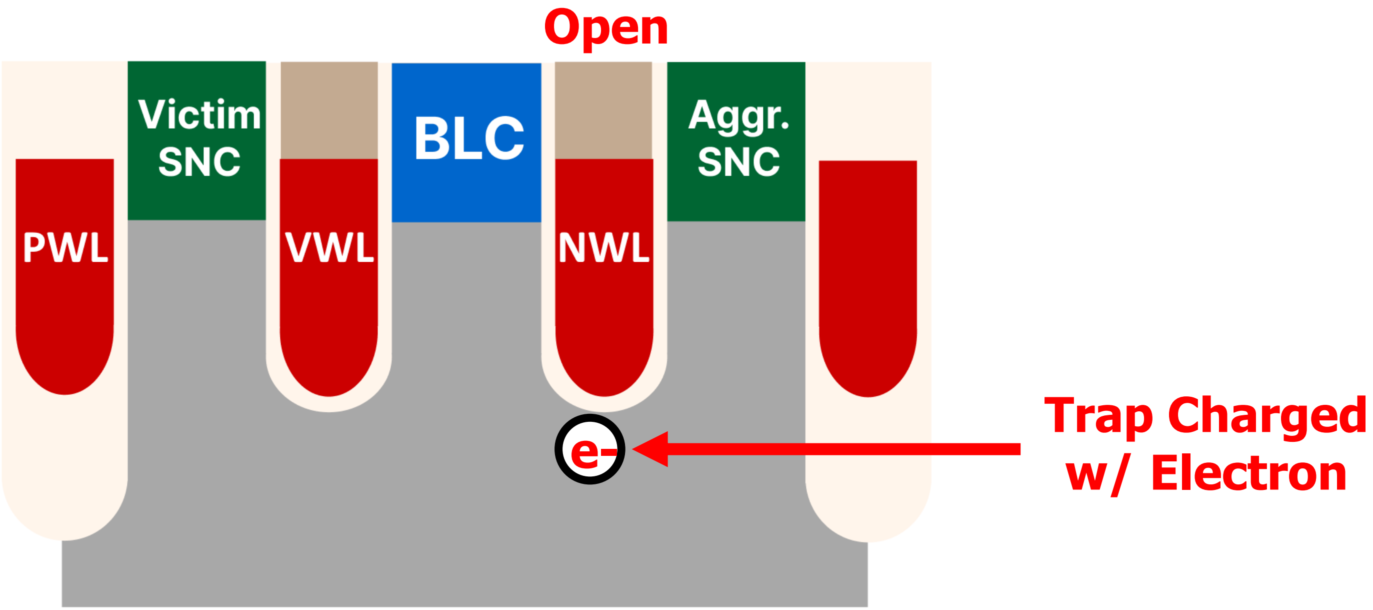


PWL: Passing Wordline **VWL:** Victim Wordline

NWL: Neighboring Wordline (Aggressor)

Device-Level Mechanism – RowHammer I

- **Key Error Mechanisms of RowHammer**
  - Trap-assisted Electron Migration [Yang+, EDL'19] [Walker+, TED'21] [Zhou+, IRPS'23]
    1. When NWL (aggressor) is open, acceptor-like traps are charged with electrons

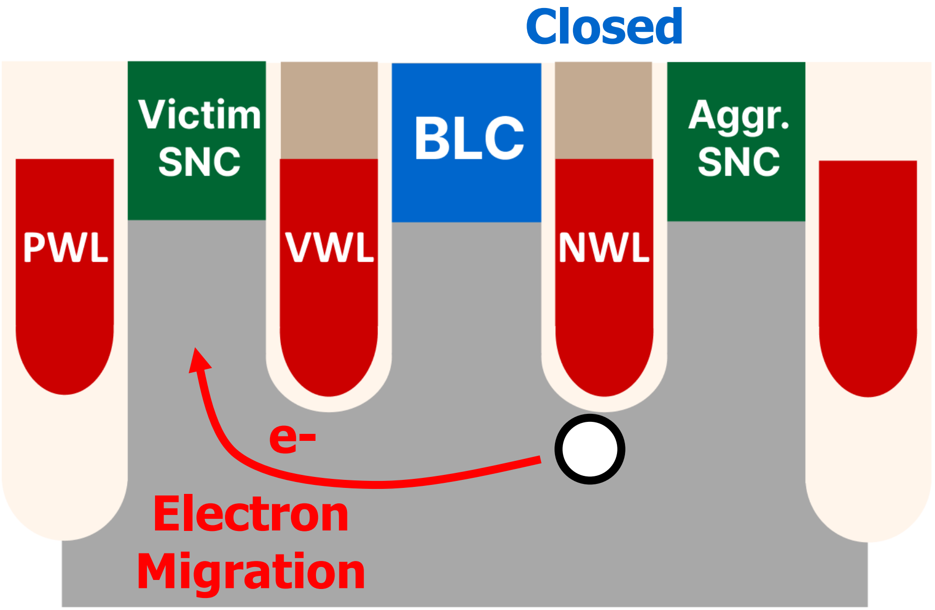


PWL: Passing Wordline **VWL:** Victim Wordline

NWL: Neighboring Wordline (Aggressor)

Device-Level Mechanism – RowHammer I

- **Key Error Mechanisms of RowHammer**
  - Trap-assisted Electron Migration [Yang+, EDL'19] [Walker+, TED'21] [Zhou+, IRPS'23]
    1. When NWL (aggressor) is open, acceptor-like traps are charged with electrons
    2. When NWL (aggressor) is closed, electrons are emitted from traps and migrate towards the victim cell

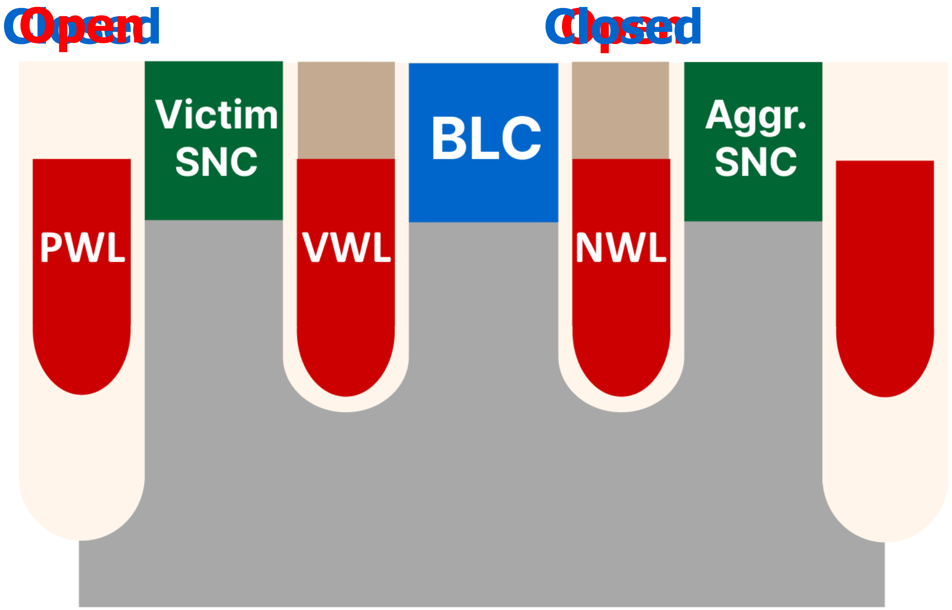


PWL: Passing Wordline **VWL:** Victim Wordline

NWL: Neighboring Wordline (Aggressor)

Device-Level Mechanism – RowHammer II

- **Key Error Mechanisms of RowHammer (Cont'd)**
  - **Double-Sided RowHammer** is **much more effective** than Single-Sided at inducing bitflips (i.e., require **much fewer aggressor row activations**)
  - Both NWL and PWL are aggressors, being opened and closed in an alternating manner, "sandwiching" the victim

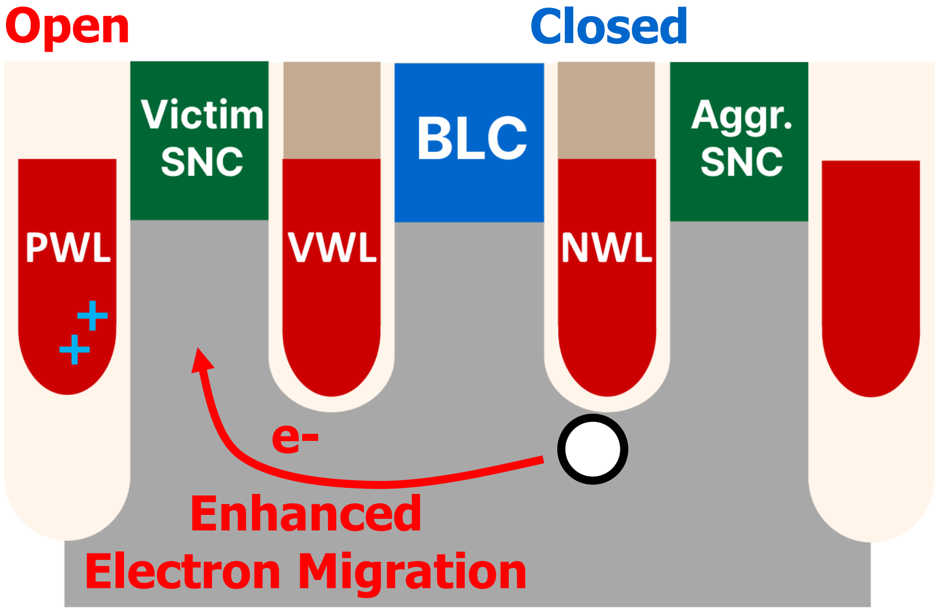


PWL: Passing Wordline (Aggressor) **VWL:** Victim Wordline

NWL: Neighboring Wordline (Aggressor)

Device-Level Mechanism – RowHammer II

- **Key Error Mechanisms of RowHammer (Cont'd)**
  - **Double-Sided RowHammer** is **much more effective** than Single-Sided at inducing bitflips (i.e., require **much fewer aggressor row activations**)
    - When NWL is closed, PWL is open: Enhancing electron migration
    - NWL is closed for a longer period: More time for electron emission from traps



PWL: Passing Wordline (Aggressor) **VWL:** Victim Wordline
NWL: Neighboring Wordline (Aggressor)

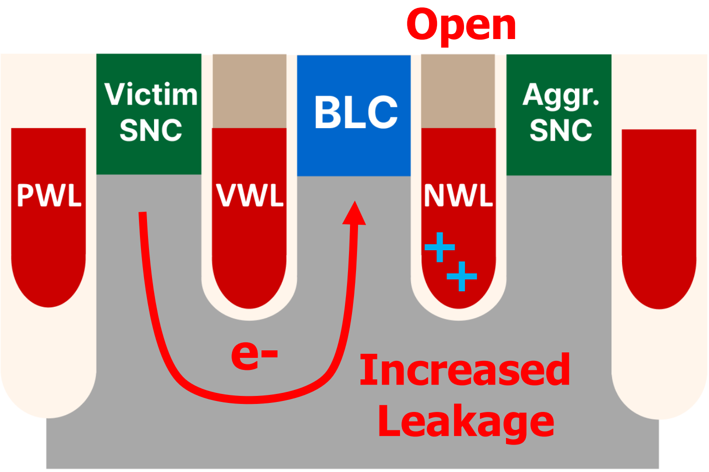
Device-Level Mechanism – RowHammer III

- **Key Error Mechanisms of RowHammer (Cont'd)**
  - **Double-Sided RowHammer** is **much more effective** than Single-Sided at inducing bitflips (i.e., require **much fewer aggressor row activations**)
  - Electron migration is significantly enhanced by the alternating opening-closing of the NWL and the PWL -> **Enhances 1→0 bitflips**
    - State-of-the-art device-level study claim 0→1 bitflips are "eliminated completely" [Zhou+, IRPS'23]

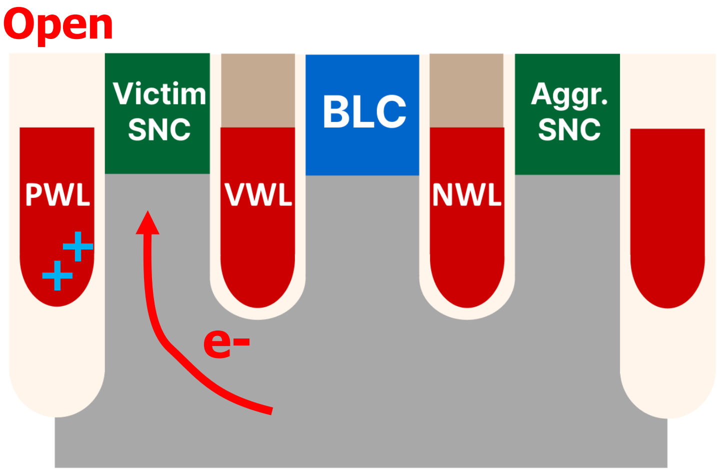
Key Device-Level Characteristic 1:
Double-Sided RowHammer should only induce 1→0 bitflips

Device-Level Mechanism – RowPress I

- **Key Error Mechanisms of RowPress**
  - **NWL RowPress:** When NWL is kept open for a long period, its strong electric field increases the leakage from the victim to the BLC, **causing 0→1 bitflips** [Zhou+, TED'24] [Zhou+, IRPS'24]
  - **PWL RowPress:** When PWL is kept open for a long period, its strong electric field draws electrons towards the victim, **causing 1→0 bitflips** [Zhou+, TED'24] [Zhou+, IRPS'24]



NWL RowPress



PWL RowPress

Device-Level Mechanism – RowPress II

- **Key Error Mechanisms of RowPress**
  - **NWL RowPress:** When NWL is kept open for a long period, its strong electric field increases the leakage from the victim to the BLC, **causing 0→1 bitflips** [Zhou+, TED'24] [Zhou+, IRPS'24]
  - **PWL RowPress:** When PWL is kept open for a long period, its strong electric field draws electrons towards the victim, **causing 1→0 bitflips** [Zhou+, TED'24] [Zhou+, IRPS'24]

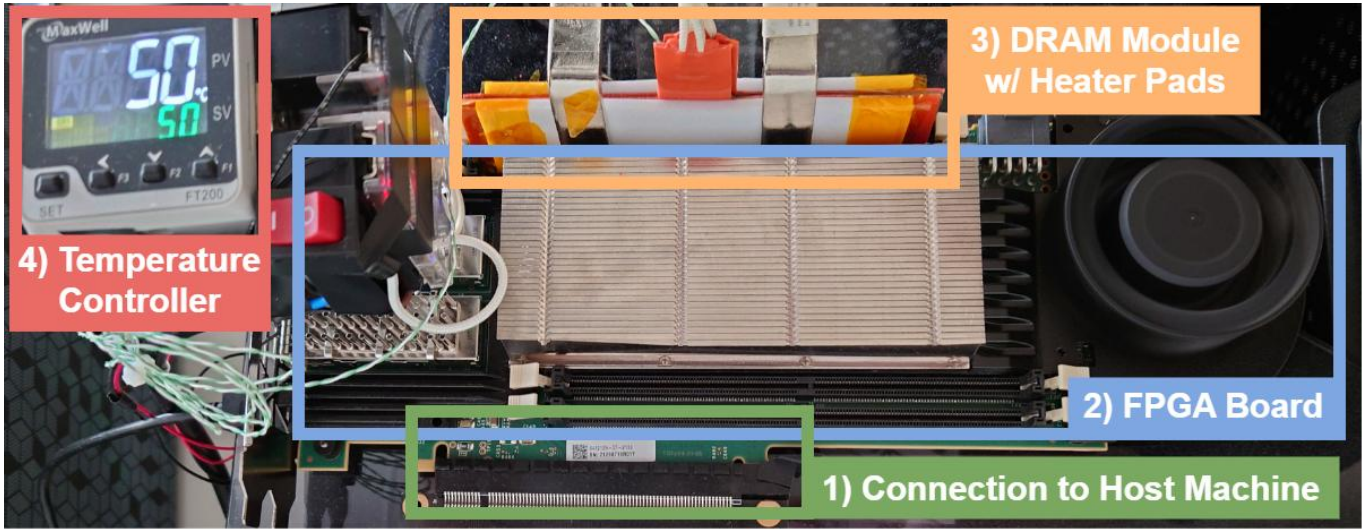
Key Device-Level Characteristic 2:
Single-Sided RowPress should induce both
1→0 and 0→1 bitflips

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

Real-Chip Characterization Methodology I

- **DRAM Bender**
  - Commodity-off-the-shelf (COTS) DDR4 DRAM testing infrastructure


MaxWell
50
PV
50
SV
FT200
SET
3) DRAM Module w/ Heater Pads
4) Temperature Controller
2) FPGA Board
1) Connection to Host Machine

Fine-grained control over
DRAM commands and timings (1.5ns granularity)

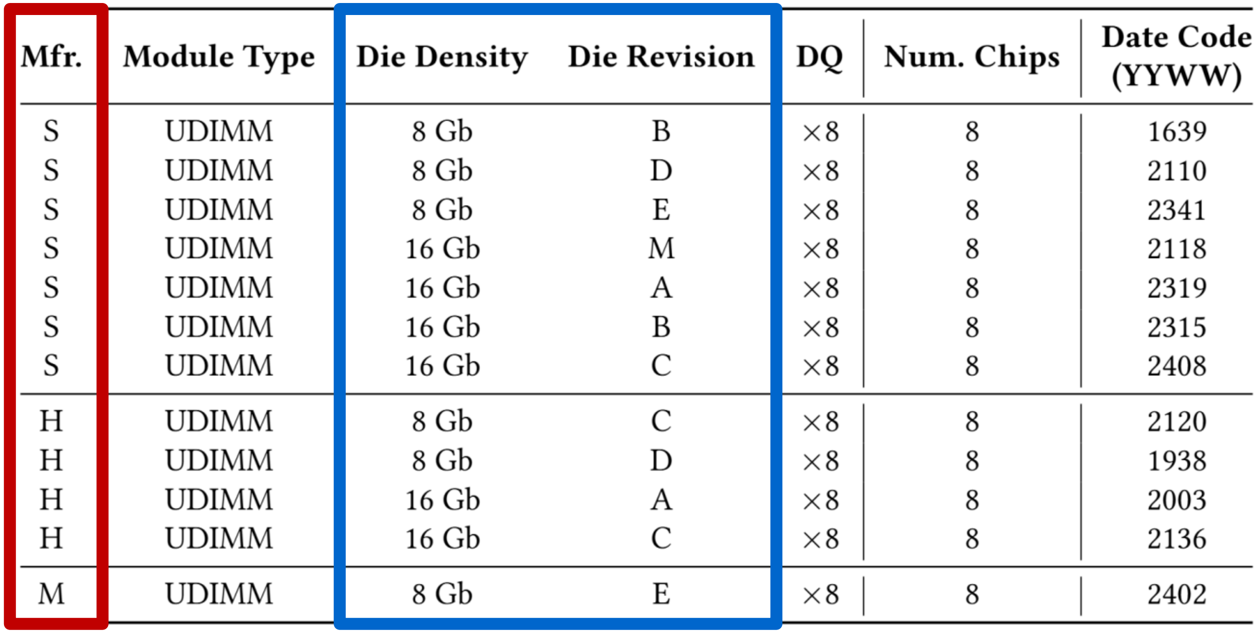
https://github.com/CMU-SAFARI/DRAM-Bender

Olgun et al., "DRAM Bender: An Extensible and Versatile FPGA-based Infrastructure to Easily Test State-of-the-art DRAM Chips," in TCAD, 2023.

Real-Chip Characterization Methodology II

- **DRAM Chips Tested**
  - COTS DDR4 from all **three major DRAM manufacturers**
  - 12 different modules with **different DRAM die revisions and densities**
  - 96 DRAM chips in total
  - We test 2048 randomly chosen victim rows from each module

Table 1: DRAM Chips Tested



Mfr.	Module Type	Die Density	Die Revision	DQ	Num. Chips	Date Code (YYWW)
S	UDIMM	8 Gb	B	×8	8	1639
S	UDIMM	8 Gb	D	×8	8	2110
S	UDIMM	8 Gb	E	×8	8	2341
S	UDIMM	16 Gb	M	×8	8	2118
S	UDIMM	16 Gb	A	×8	8	2319
S	UDIMM	16 Gb	B	×8	8	2315
S	UDIMM	16 Gb	C	×8	8	2408
H	UDIMM	8 Gb	C	×8	8	2120
H	UDIMM	8 Gb	D	×8	8	1938
H	UDIMM	16 Gb	A	×8	8	2003
H	UDIMM	16 Gb	C	×8	8	2136
M	UDIMM	8 Gb	E	×8	8	2402

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

True- and Anti-Cell Layout Reverse Engineering

- **Motivation**
  - DRAM internal architecture and layout is opaque to the memory controller
  - The observed bitflip direction in real-chip characterization results does not always correspond to the real bitflip direction that happens in the DRAM cells (i.e., due to true- and anti-cells)
- **Retention Failure Based Reverse Engineering**
  - Major DRAM retention leakage paths (junction leakage and GIDL) are towards the access transistor substrate, which are usually negatively biased [Saino+, IEDM'00] [Yang+, EDL'13] [Park+, IMW'15] [Lee+, JSSC'11]
  - Prior works on experimental characterization of DRAM retention failures assume DRAM retention failure only contain 1→0 bitflips, and leverages this to reverse engineer the true- and anti-cell layout of DRAM chips [Liu+, ISCA'13] [Nam+, ISCA'24]

➢ **We find consistent true- and anti-cell layouts as in prior works**

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

Summary of Inconsistencies Found

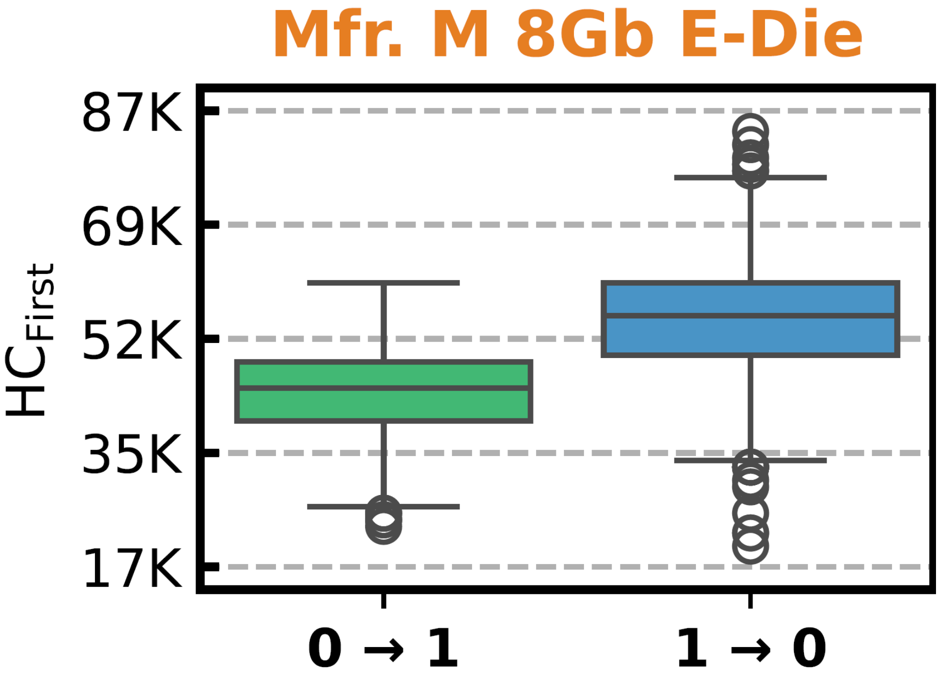
- **Inconsistency I – Double-Sided RowHammer Bitflip Direction**
  - Real-Chip Characterization: Observed both 0→1 and 1→0 bitflips; 0→1 bitflips are initially easier to induce than 1→0 bitflips
  - Device-Level Mechanism: Double-Sided RowHammer significantly enhances 1→0 leakage that it should only induce 1→0 bitflips
- **Inconsistency II – Double-Sided RowHammer Bitflip Count**
  - Real-Chip Characterization: Only with a sufficiently large hammer count does the number of 1→0 bitflips exceed that of 0→1 bitflips
  - Device-Level Mechanism: Double-Sided RowHammer significantly enhances 1→0 leakage that it should only induce 1→0 bitflips
- **Inconsistency III – Single-Sided RowPress Bitflip Direction**
  - Real-Chip Characterization: Observed overwhelmingly 1→0 bitflips
  - Device-Level Mechanism: Single-Sided RowPress should induce both 0→1 and 1→0 bitflips

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

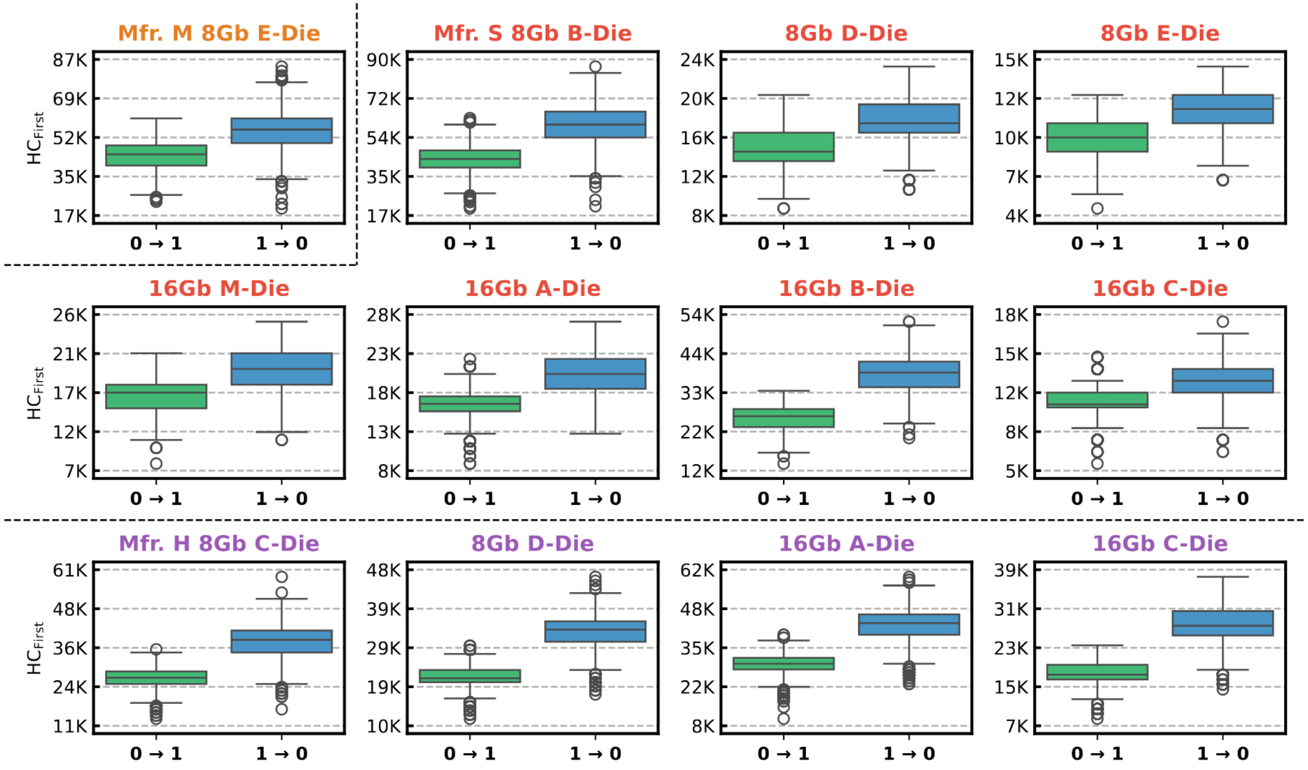
Initial Bitflip Direction of Double-Sided RowHammer I

- **Access Pattern:** Double-Sided RowHammer
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: HC_{First}**, the minimum aggressor row activation (hammer) count to induce at least one bitflip in the victim row



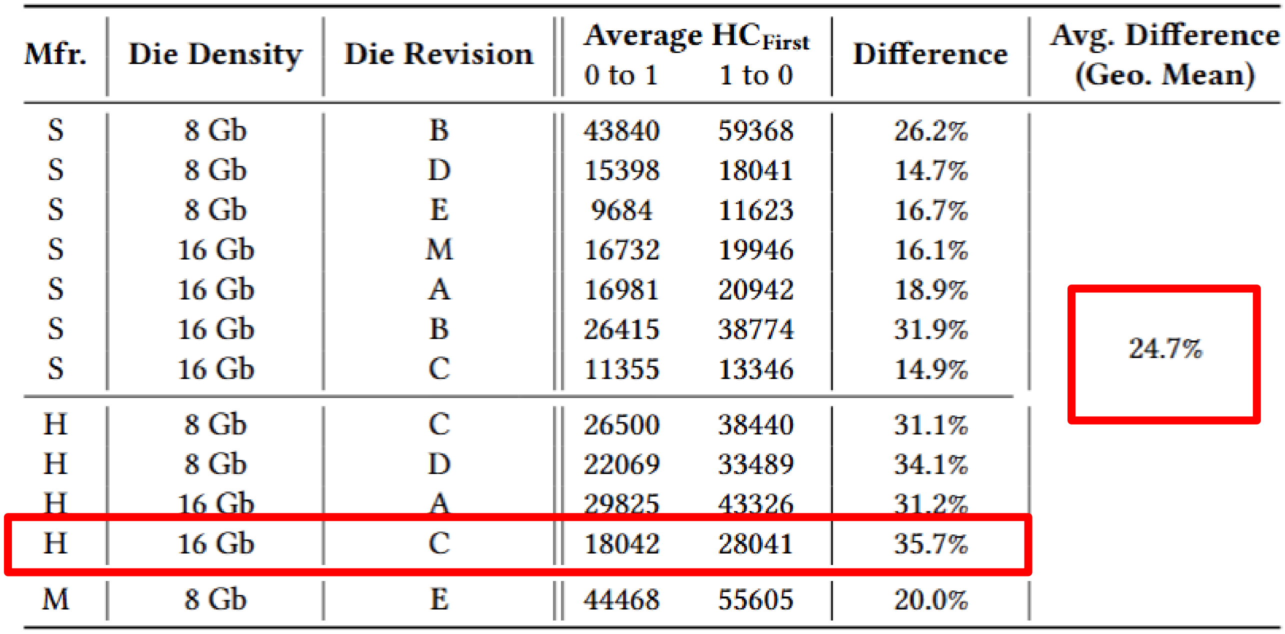
Initial Bitflip Direction of Double-Sided RowHammer I

- **Access Pattern:** Double-Sided RowHammer
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: $\mathbf{HC_{First}}$** , the minimum aggressor row activation (hammer) count to induce at least one bitflip in the victim row



Initial Bitflip Direction of Double-Sided RowHammer II

- **Average HC_{First} of 0→1 and 1→0 bitflips (Double-Sided RowHammer)**



Mfr.	Die Density	Die Revision	Average HC_{First}		Difference	Avg. Difference (Geo. Mean)
			0 to 1	1 to 0		
S	8 Gb	B	43840	59368	26.2%	24.7%
S	8 Gb	D	15398	18041	14.7%	
S	8 Gb	E	9684	11623	16.7%	
S	16 Gb	M	16732	19946	16.1%	
S	16 Gb	A	16981	20942	18.9%	
S	16 Gb	B	26415	38774	31.9%	
S	16 Gb	C	11355	13346	14.9%	
H	8 Gb	C	26500	38440	31.1%	
H	8 Gb	D	22069	33489	34.1%	
H	16 Gb	A	29825	43326	31.2%	
H	16 Gb	C	18042	28041	35.7%	
M	8 Gb	E	44468	55605	20.0%	

Real-Chip Obsv. 1: Double-Sided RowHammer induces both 0→1 and 1→0 bitflips

Real-Chip Obsv. 2: For Double-Sided RowHammer, it is easier to induce 0→1 bitflips than 1→0 bitflips

Inconsistency I

- **Takeaways from Real-Chip Characterization Results**
  - Double-Sided RowHammer involves error mechanisms for inducing both 0→1 and 1→0 bitflips
  - For Double-Sided RowHammer, the observed error mechanism for 0→1 bitflips is initially stronger than that of 1→0 bitflips in the most vulnerable DRAM cells (i.e., those requiring the least number of aggressor row activations to experience bitflips)

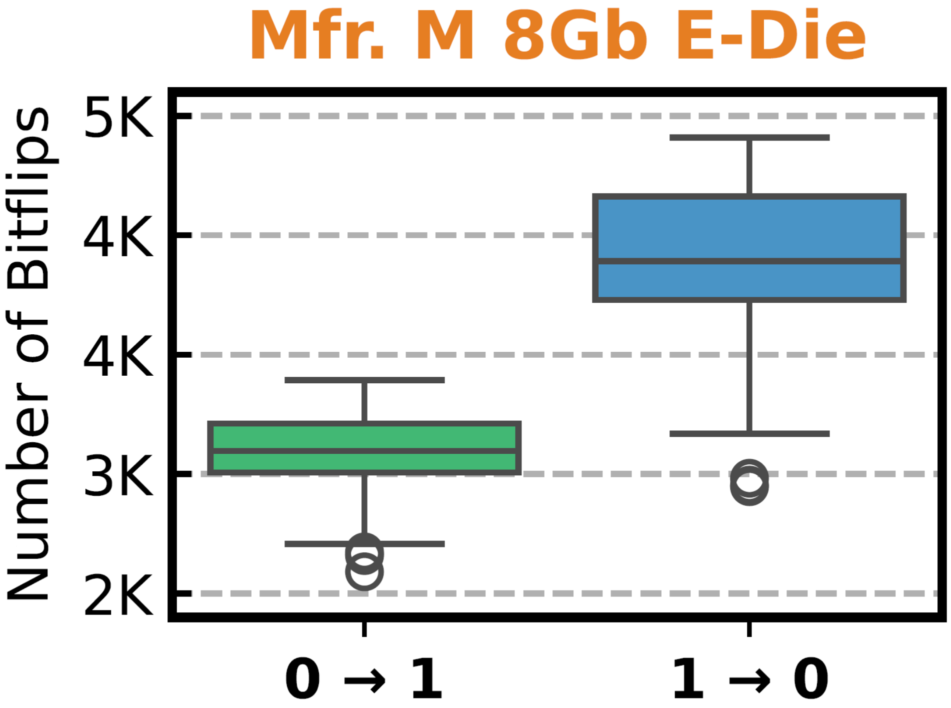
- **Characteristics from Device-Level Mechanisms**
  - Double-Sided RowHammer significantly enhances leakage that causes 1→0 bitflips that it should only induce 1→0 bitflips

Outline

- Background
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- Device-Level DRAM Read Disturbance Mechanisms
- Real-Chip Characterization Methodology
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- Hypotheses
- Conclusion

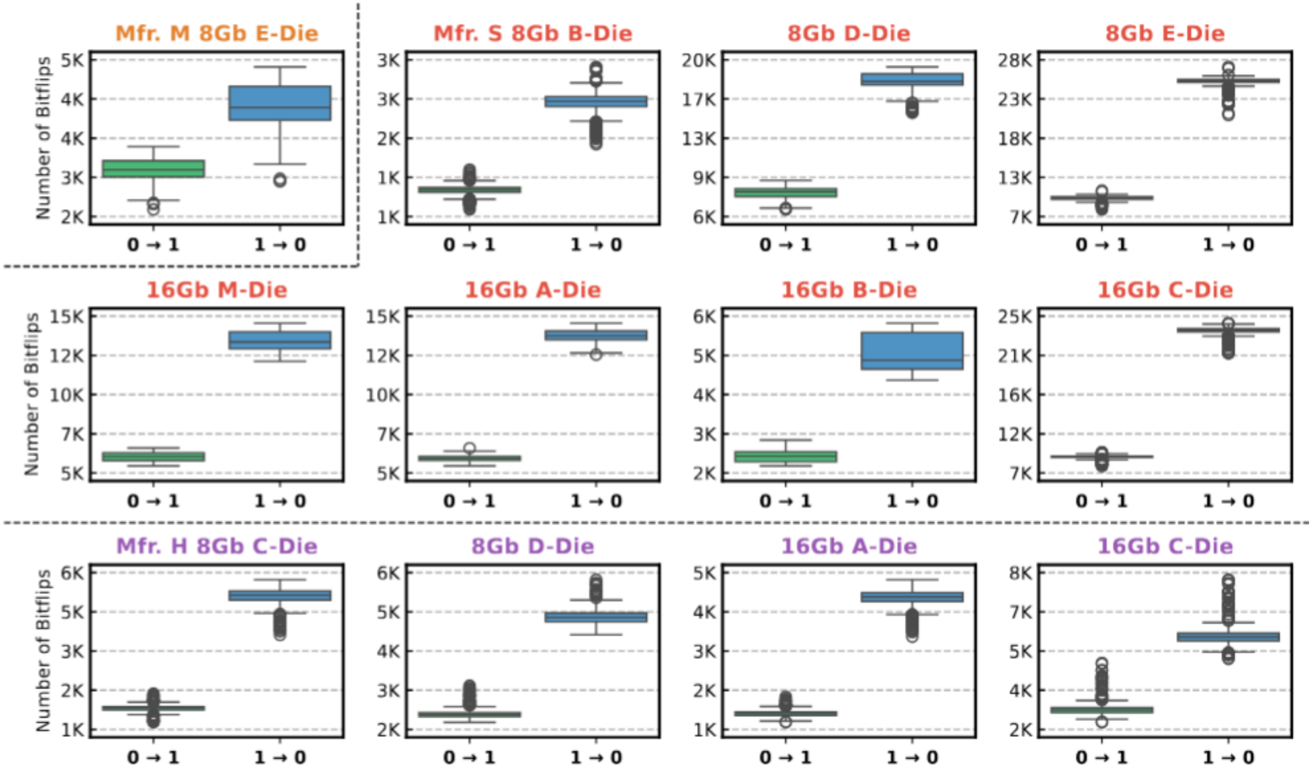
Bitflip Count of Double-Sided RowHammer I

- **Access Pattern:** Double-Sided RowHammer
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: Per-Row Bitflip Count**, after hammering each aggressor row for a sufficiently high number of times (500K)



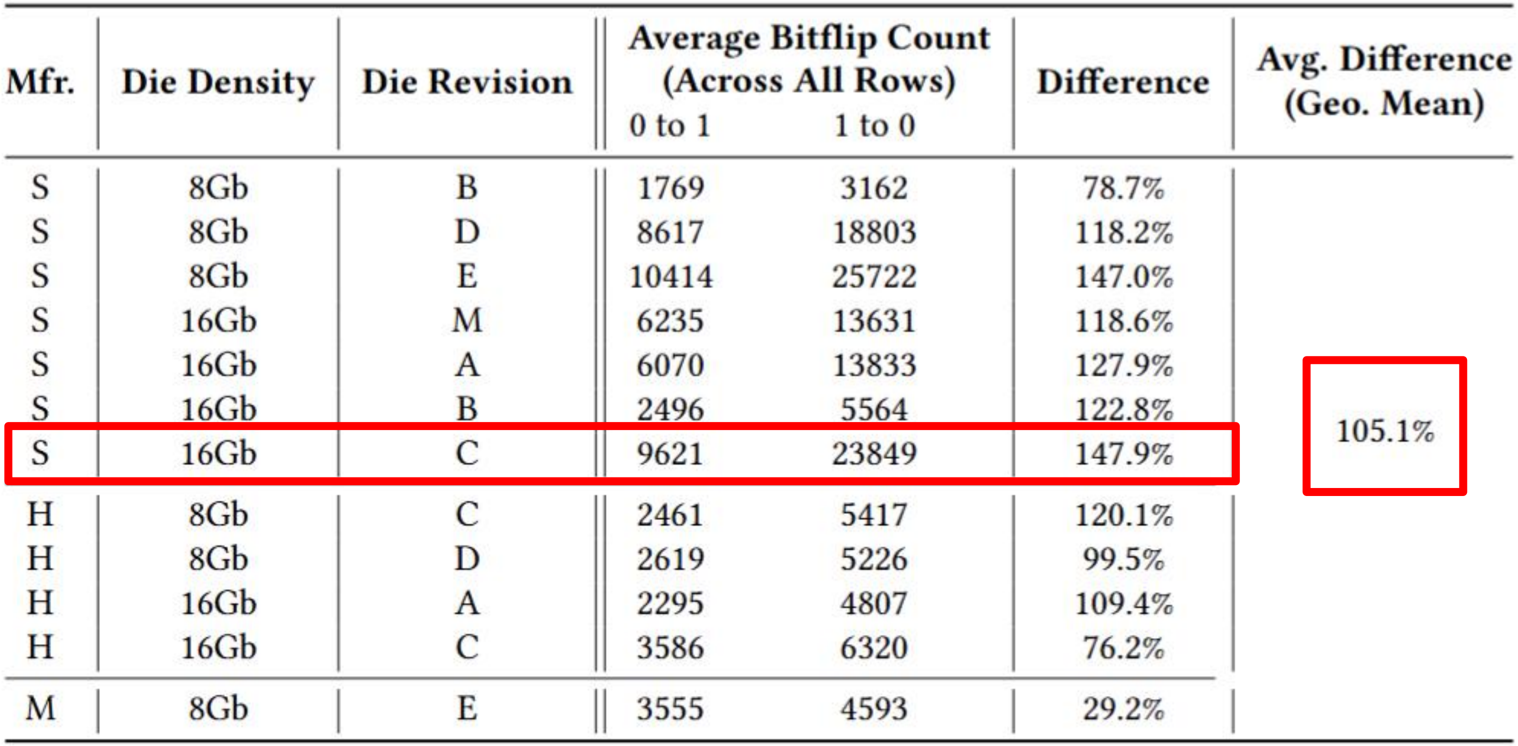
Bitflip Count of Double-Sided RowHammer I

- **Access Pattern:** Double-Sided RowHammer
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: Per-Row Bitflip Count**, after hammering each aggressor row for a sufficiently high number of times (500K)



Bitflip Count of Double-Sided RowHammer II

- **Average bitflip count (across all victim rows) of 0→1 and 1→0 bitflips (Double-Sided RowHammer)**

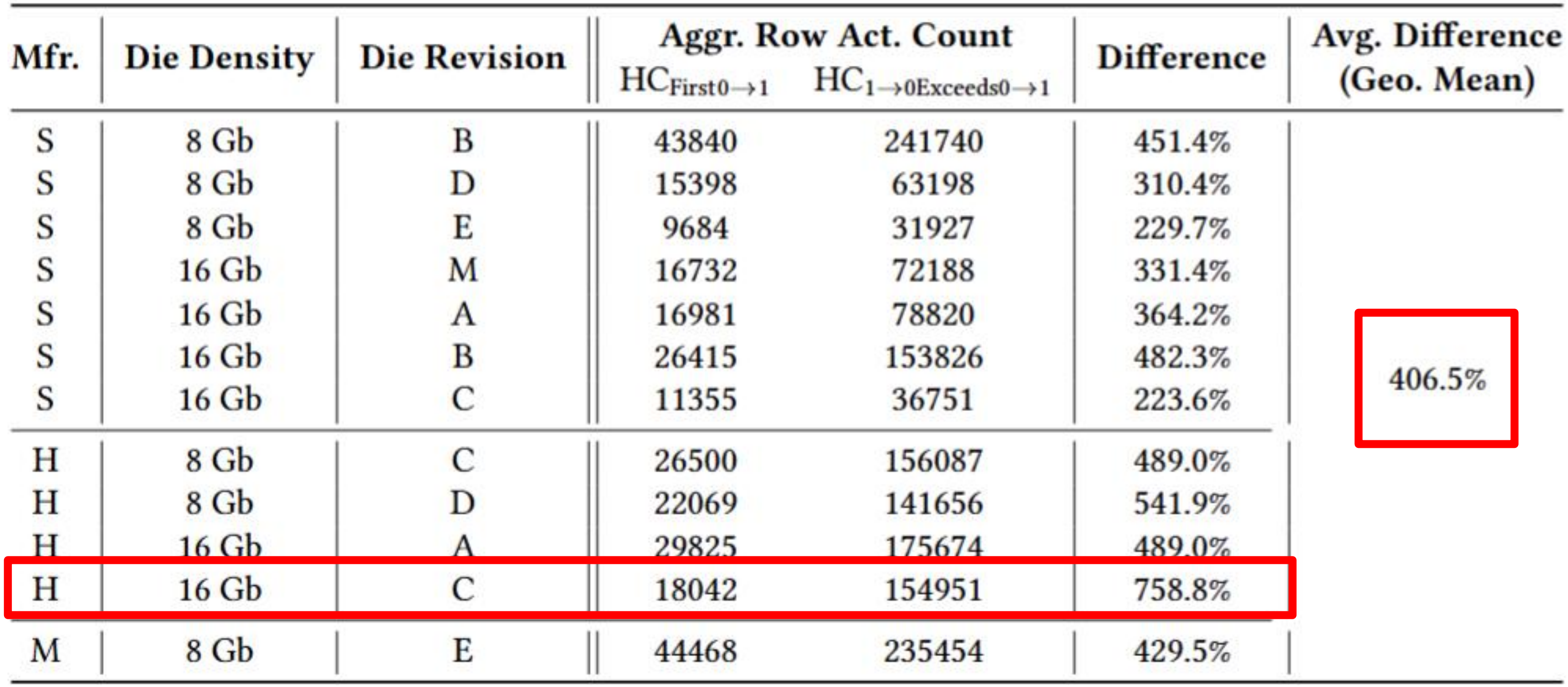


Mfr.	Die Density	Die Revision	Average Bitflip Count (Across All Rows)		Difference	Avg. Difference (Geo. Mean)
			0 to 1	1 to 0		
S	8Gb	B	1769	3162	78.7%	105.1%
S	8Gb	D	8617	18803	118.2%	
S	8Gb	E	10414	25722	147.0%	
S	16Gb	M	6235	13631	118.6%	
S	16Gb	A	6070	13833	127.9%	
S	16Gb	B	2496	5564	122.8%	
S	16Gb	C	9621	23849	147.9%	
H	8Gb	C	2461	5417	120.1%	
H	8Gb	D	2619	5226	99.5%	
H	16Gb	A	2295	4807	109.4%	
H	16Gb	C	3586	6320	76.2%	
M	8Gb	E	3555	4593	29.2%	

Real-Chip Obsv. 3: With sufficiently many hammers, Double-Sided RowHammer induces more 1→0 than 0→1 bitflips

Bitflip Count of Double-Sided RowHammer III

- **When does the number of 1→0 bitflips start to exceed the number of 0→1 bitflips?**
  - **$HC_{1\rightarrow0Exceeds0\rightarrow1}$:** The minimum hammer count that the number of 1→0 bitflips exceed the number of 0→1 bitflips



Mfr.	Die Density	Die Revision	Aggr. Row Act. Count		Difference	Avg. Difference (Geo. Mean)
			$HC_{First0\rightarrow1}$	$HC_{1\rightarrow0Exceeds0\rightarrow1}$		
S	8 Gb	B	43840	241740	451.4%	406.5%
S	8 Gb	D	15398	63198	310.4%	
S	8 Gb	E	9684	31927	229.7%	
S	16 Gb	M	16732	72188	331.4%	
S	16 Gb	A	16981	78820	364.2%	
S	16 Gb	B	26415	153826	482.3%	
S	16 Gb	C	11355	36751	223.6%	
H	8 Gb	C	26500	156087	489.0%	
H	8 Gb	D	22069	141656	541.9%	
H	16 Gb	A	29825	175674	489.0%	
H	16 Gb	C	18042	154951	758.8%	
M	8 Gb	E	44468	235454	429.5%	

Inconsistency II

- **Takeaways from Real-Chip Characterization Results**
  - For Double-Sided RowHammer, the observed error mechanism for 1→0 bitflips are only stronger than that of 0→1 bitflips with a sufficiently high hammer count

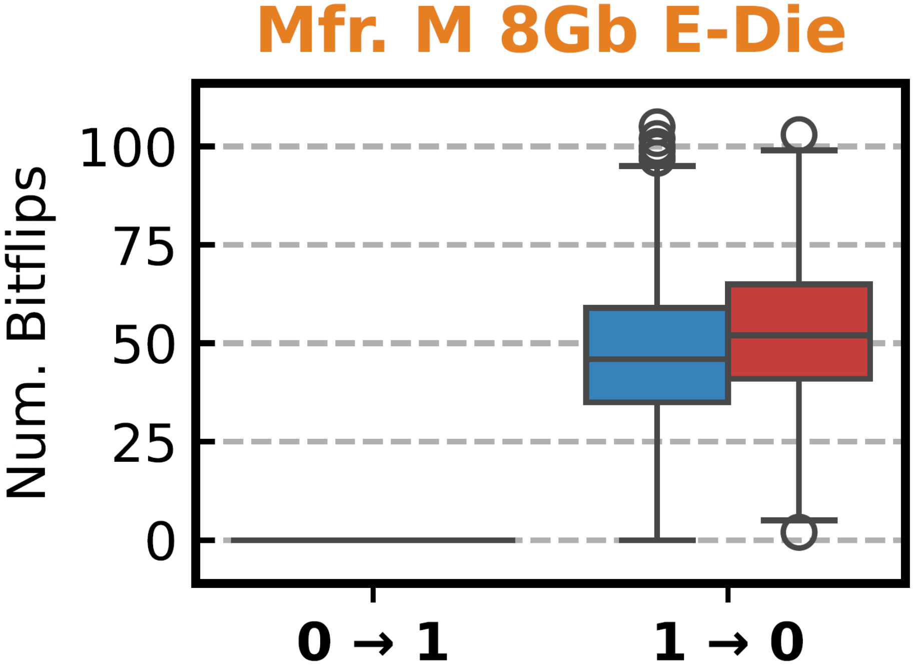
- **Characteristics from Device-Level Mechanisms**
  - Double-Sided RowHammer significantly enhances leakage that causes 1→0 bitflips that it should only induce 1→0 bitflips

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

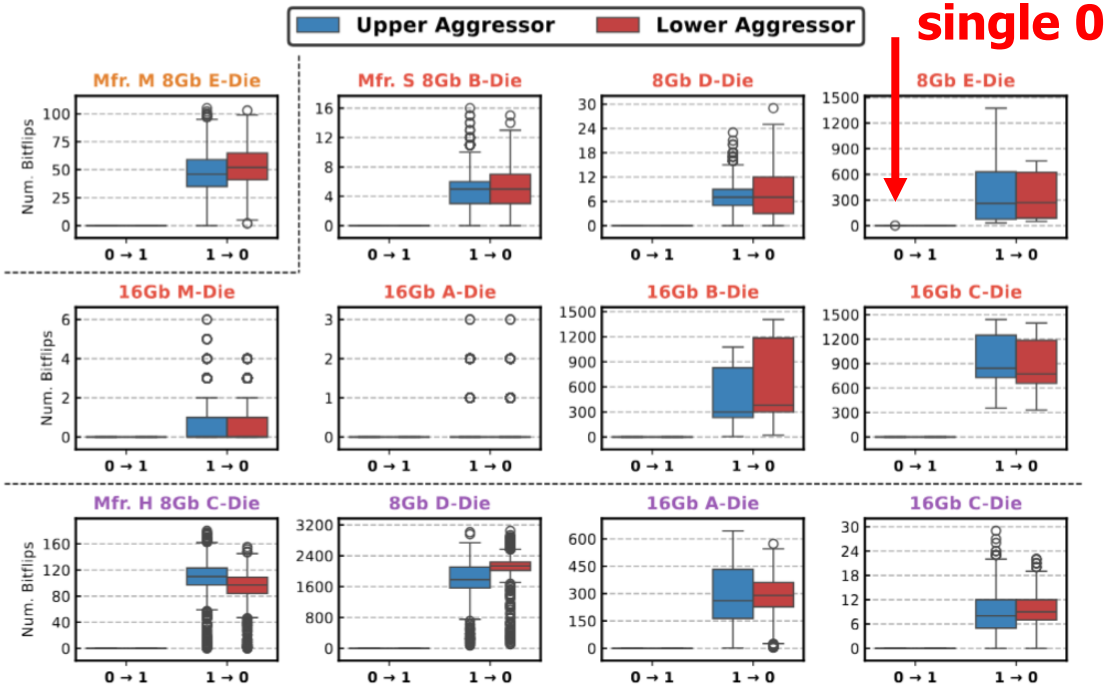
Bitflip Direction of Single-Sided RowPress

- **Access Pattern:** Single-Sided RowPress at both the upper and lower aggressor row; kept open for 7.8µs per activation
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: Per-Row Bitflip Count**, after activating each aggressor row for a sufficiently high number of times (7500)



Bitflip Direction of Single-Sided RowPress

- **Access Pattern:** Single-Sided RowPress at both the upper and lower aggressor row; kept open for 7.8µs per activation
- **Data Pattern:** All physical 1 (or 0) in the victim rows, All physical 0 (or 1) in the aggressor rows
- **Key Metric: Per-Row Bitflip Count**, after activating each aggressor row for a sufficiently high number of times (7500)



Only observed a single 0→1 bitflip

Inconsistency III

- **Takeaways from Real-Chip Characterization Results**
  - For Single-sided RowPress, for both NWL and PWL, the observed error mechanism for inducing 1→0 bitflips is much stronger than that of 0→1 bitflips that we observe overwhelmingly 1→0 bitflips within the refresh window

- **Characteristics from Device-Level Mechanisms**
  - NWL Single-Sided RowPress should induce 0→1 bitflips
  - PWL Single-Sided RowPress should induce 1→0 bitflips

Summary of Inconsistencies Found

- **Inconsistency I – Double-Sided RowHammer Bitflip Direction**
  - Real-Chip Characterization: Observed both 0→1 and 1→0 bitflips; 0→1 bitflips are initially easier to induce than 1→0 bitflips
  - Device-Level Mechanism: Double-Sided RowHammer significantly enhances 1→0 leakage that it should only induce 1→0 bitflips

- **Inconsistency II – Double-Sided RowHammer Bitflip Count**
  - Real-Chip Characterization: Only with a sufficiently large hammer count does the number of 1→0 bitflips exceed that of 0→1 bitflips
  - Device-Level Mechanism: Double-Sided RowHammer significantly enhances 1→0 leakage that it should only induce 1→0 bitflips

- **Inconsistency III – Single-Sided RowPress Bitflip Direction**
  - Real-Chip Characterization: Observed overwhelmingly 1→0 bitflips
  - Device-Level Mechanism: Single-Sided RowPress should induce both 0→1 and 1→0 bitflips

Outline

- **Background**
  - Key DRAM Organization
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- **Device-Level DRAM Read Disturbance Mechanisms**
- **Real-Chip Characterization Methodology**
  - Reverse Engineering of True- and Anti-Cell Layout
- **Real-Chip Characterization Results**
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- **Hypotheses**
- **Conclusion**

Hypotheses I

- **Two Possibilities**
  - The retention failure based true- and anti-cell reverse engineering methodology is not always applicable in modern DRAM chips
  - Current device-level explanations of DRAM read disturbance is not comprehensive enough
- **Other major retention leakage paths that does NOT leak towards the substrate**
  - Dielectric leakage that leaks towards BLC?
  - More pronounced in modern DRAM as process keeps shrinking [Yu+, ICET'22]

Hypotheses II

- **Existing device-level works make oversimplified assumptions during simulation**
  - Prior works that study the trap-assisted electron migration leakage mechanism only focus on acceptor-like trap
    [Yang+, EDL'19] [Walker+, TED'21] [Zhou+, IRPS'23] [Zhou+, TED'24]
  - Are donor-like traps really not causing any read disturbance leakage?
- **Device-level simulations focus on a few isolated structures and components**
  - Maybe the modeled read disturbance mechanisms are no longer first-order when put in the context of a full DRAM array
  - Other coupling mechanisms between multiple devices and/or process variation might dominate real-chip characterization results
- **Real-chip characterization results are heavily skewed**
  - There could be asymmetry between the signal margins of reading a 1 and a 0, as a result of sense amplifier design and operation

Hypotheses III

- **There could be two different sets of read disturbance leakage mechanisms that affects different sets of DRAM cells**
  - For example, the error mechanism of 1→0 bitflips could be the major mechanism of Double-Sided RowHammer as prior works study for the majority of the cells
  - However, the error mechanism behind the 0→1 bitflips determines the tail distribution of the HC_{First} (i.e., it affects the most vulnerable DRAM cells)

Outline

- Background
  - Key DRAM Organization & Operation
  - DRAM Read Disturbance Phenomena: RowHammer & RowPress
- Device-Level DRAM Read Disturbance Mechanisms
- Real-Chip Characterization Methodology
  - Reverse Engineering of True- and Anti-Cell Layout
- Real-Chip Characterization Results
  - Inconsistency I: Initial Bitflip Direction of Double-Sided RowHammer
  - Inconsistency II: Bitflip Count of Double-Sided RowHammer
  - Inconsistency III: Bitflip Direction of Single-Sided RowPress
- Hypotheses
- **Conclusion**

Conclusion

- **Goal:** Align and cross-validate the experimental characterization of read disturbance (RowHammer and RowPress) with the error mechanisms modeled by device-level simulation
  - **Challenge:** Gap between real-chip characterization and device-level mechanisms due to low-level DRAM array layout (i.e., true- and anti-cells)
- **Key Methodology:**
  - Extract key device-level read disturbance mechanisms from prior works
  - Reverse-engineer the true- and anti-cells layout of real DRAM chips
  - Perform real-chip characterization that directly match the access and data patterns studied in device-level works
- **Key Inconsistencies:**
  - For Double-Sided RowHammer, experimental characterization shows bitflips in both directions while device-level mechanisms suggest only 1→0 bitflips will happen
  - For Single-Sided RowPress, experimental characterization shows overwhelmingly 1→0 bitflips while device-level mechanisms suggest both kinds of bitflips will happen

Revisiting DRAM Read Disturbance

Identifying Inconsistencies Between Experimental Characterization and Device-Level Studies

Haocong Luo İsmail Emir Yüksel Ataberk Olgun
A. Giray Yağlıkçı Onur Mutlu

ETH Zurich

VTS' 25
28 April 2025

arXiv

Data & Code

SAFARI

ETHzürich