RowPress

Amplifying Read Disturbance in Modern DRAM Chips

ISCA 2023 Session 2B: Monday 19 June, 2:15 PM EDT

Haocong Luo

Ataberk Olgun *A. Giray Yağlıkçı* *Yahya Can Tuğrul*

Steve Rhyner *Meryem Banu Cavlak* *Joël Lindegger*

Mohammad Sadrosadati *Onur Mutlu*

SAFARI

ETH zürich

High-Level Summary

- We demonstrate and analyze **RowPress, a new read disturbance phenomenon** that causes bitflips in real DRAM chips
- We show that RowPress is **different from the RowHammer vulnerability**
- We demonstrate RowPress **using a user-level program** on a real Intel system with real DRAM chips
- We provide **effective solutions** to RowPress

What is RowPress?

Keeping a DRAM row **open for a long time** causes bitflips in adjacent rows

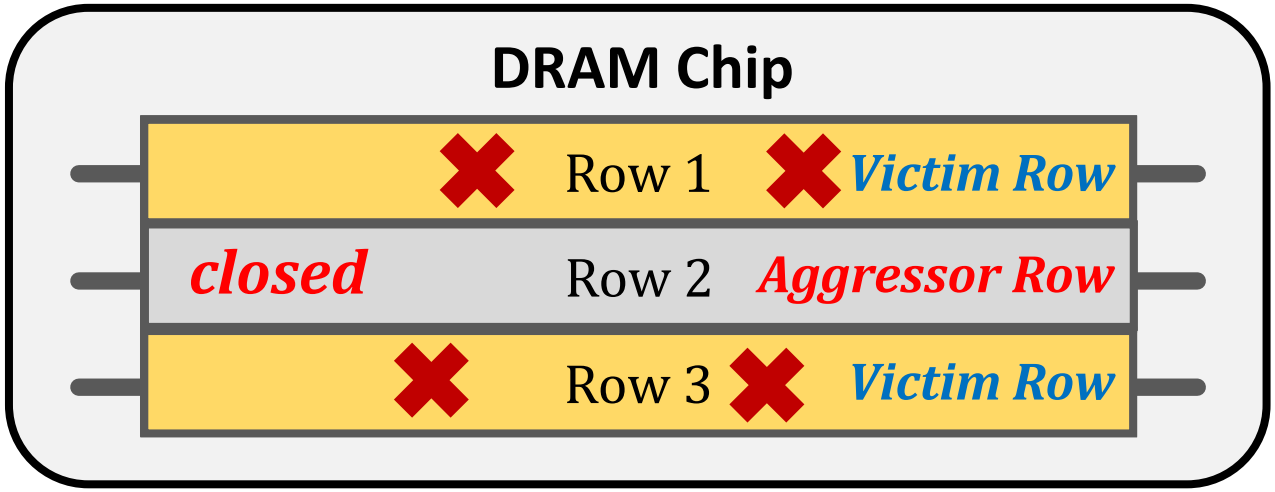
These bitflips do **NOT** require many row activations

Only one activation is enough in some cases!

Now, let's delve into some background and see how this is **different from RowHammer**

Read Disturbance in DRAM

- Read disturbance in DRAM breaks memory isolation
- **Prominent example: RowHammer**



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

Are There Other Read-Disturb Issues in DRAM?

- RowHammer is the only studied read-disturb phenomenon
- Mitigations work by detecting **high row activation count**

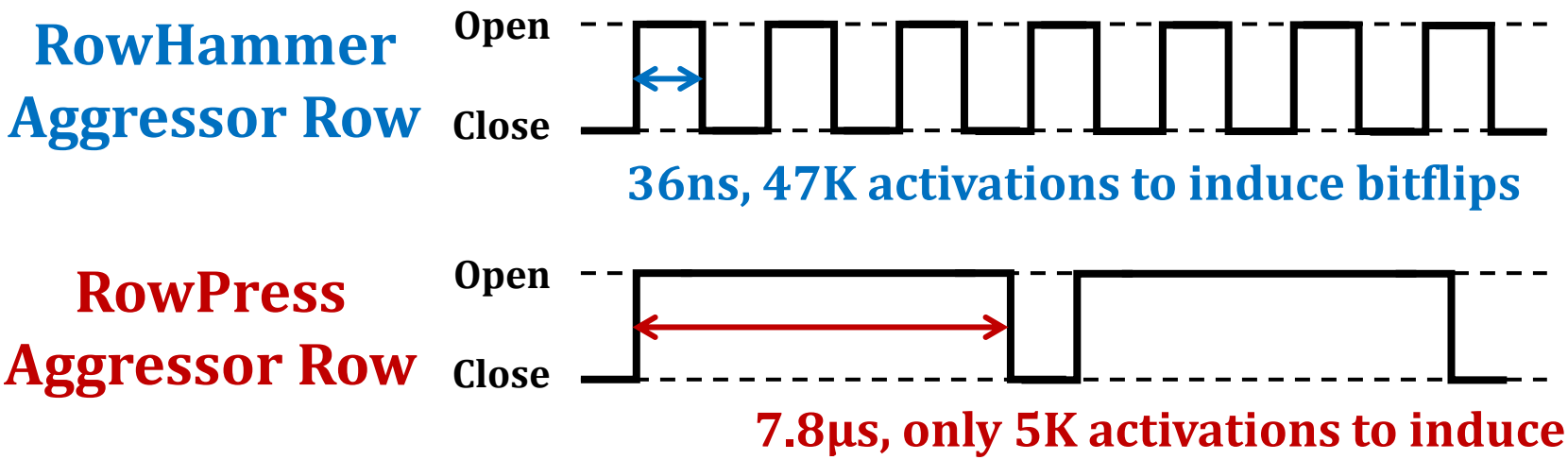
What if there is another read-disturb phenomenon that **does NOT rely on high row activation count**?

https://www.reddit.com/r/CrappyDesign/comments/arw0q8/now_this_this_is_poor_fencing/

RowPress vs. RowHammer

Instead of using a high activation count,

☞ increase the time that the aggressor row stays open

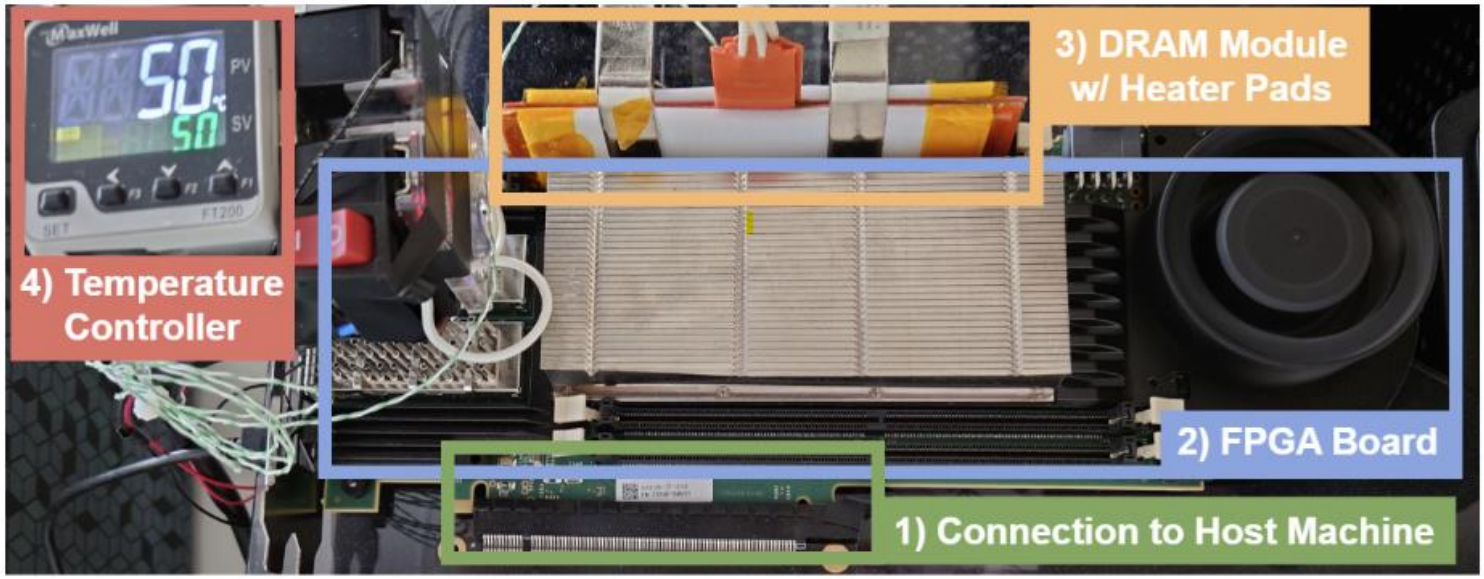


We observe bitflips even with **ONLY ONE activation** in extreme cases where the row stays open for 30ms

Real DRAM Chip Characterization (I)

FPGA-Based DDR4 Testing Infrastructure

- Based on SoftMC [Hassan+, HPCA'17] and DRAM Bender [Olgun+, TCAD'23]
- Fine-grained control over DRAM commands, timings, and temperature



Real DRAM Chip Characterization (II)

DRAM Chips Tested

- 164 DDR4 chips from all 3 major DRAM manufacturers

Mfr.	#DIMMs	#Chips	Density	Die Rev.	Org.	Date
Mfr. S (Samsung)	2	8	8Gb	B	x8	20-53
	1	8	8Gb	C	x8	N/A
	3	8	8Gb	D	x8	21-10
	2	8	4Gb	F	x8	N/A
Mfr. H (SK Hynix)	1	8	4Gb	A	x8	19-46
	1	8	4Gb	X	x8	N/A
	2	8	16Gb	A	x8	20-51
	2	8	16Gb	C	x8	21-36
Mfr. M (Micron)	1	16	8Gb	B	x4	N/A
	2	4	16Gb	B	x16	21-26
	1	16	16Gb	E	x4	20-14
	2	4	16Gb	E	x16	20-46
	1	4	16Gb	F	x16	21-50

Major Takeaways from Real DRAM Chips

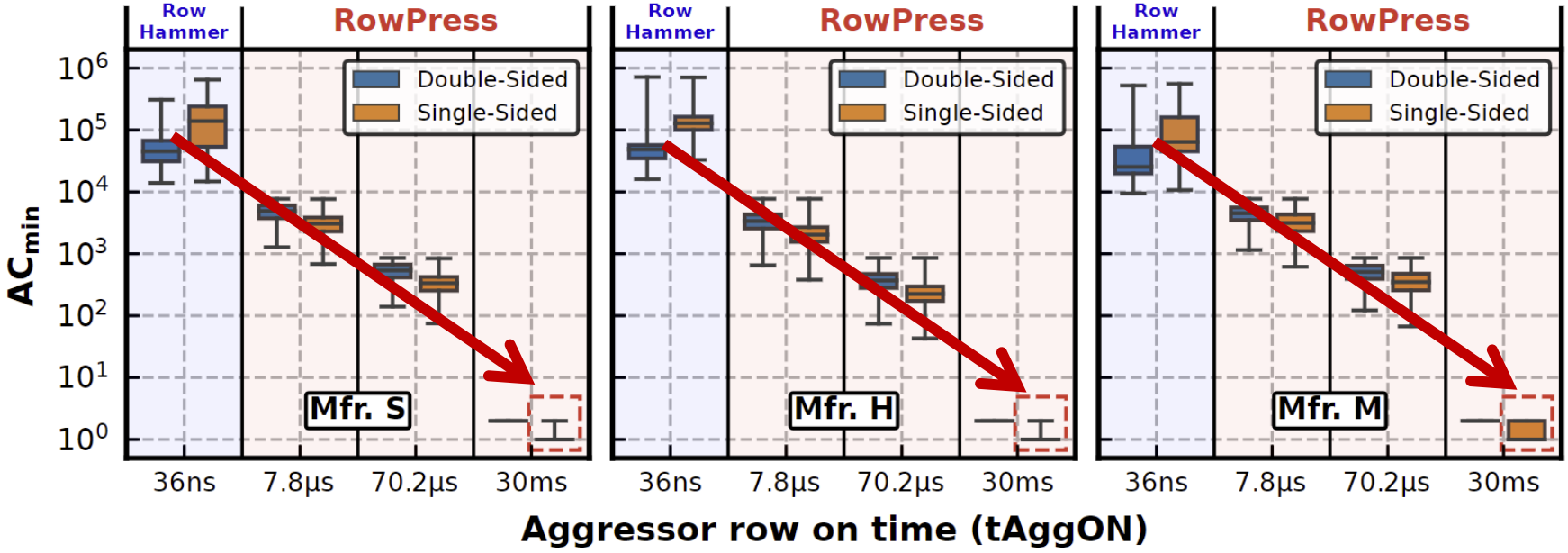
RowPress significantly **amplifies** DRAM's vulnerability to read disturbance

RowPress has a **different** underlying error **mechanism** from RowHammer

Key Characteristics of RowPress (I)

Amplifying Read Disturbance in DRAM

- Reduces the minimum number of row activations needed to induce a bitflip (**ACmin**) by **1-2 orders of magnitude**
- In extreme cases, activating a row **only once** induces bitflips



Key Characteristics of RowPress (II)

Amplifying Read Disturbance in DRAM

- Reduces the minimum number of row activations needed to induce a bitflip (**ACmin**) by **1-2 orders of magnitude**
- In extreme cases, activating a row **only once** induces bitflips
- Gets worse as **temperature increases**

Different From RowHammer

- Affects a **different set of cells** compared to RowHammer and retention failures
- **Behaves differently** as access pattern and temperature changes compared to RowHammer

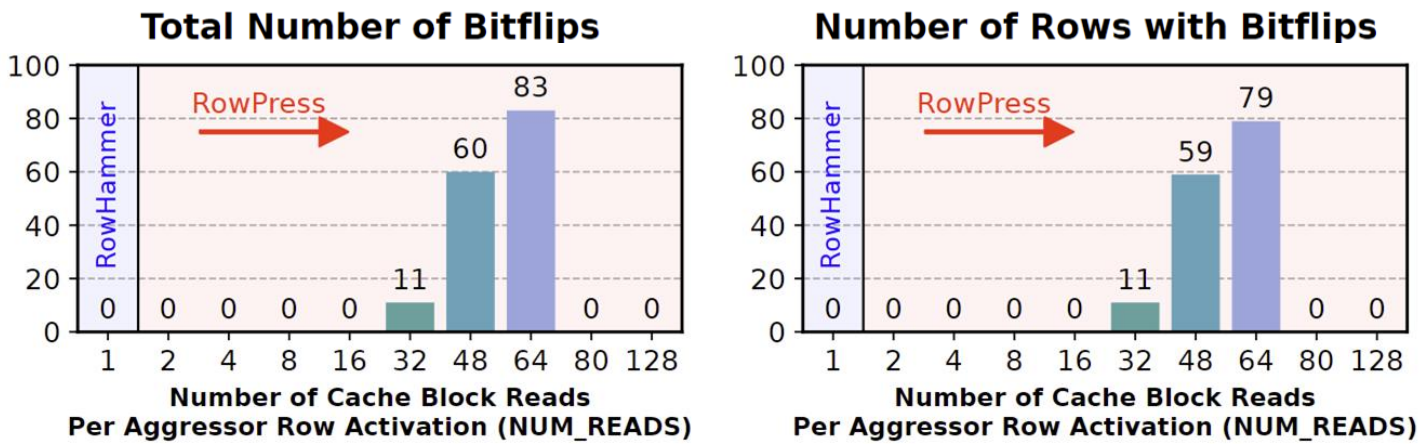
Real-System Demonstration (I)

Intel Core i5-10400
(Comet Lake)

Samsung DDR4 Module
M378A2K43CB1-CTD
(Date Code: 20-10)
w/ TRR RowHammer Mitigation

Key Idea: A proof-of-concept RowPress program keeps a DRAM row open for a longer period by **keeping on accessing different cache blocks in the row**

Real-System Demonstration (II)



Key Idea: A proof-of-concept RowPress program keeps a DRAM row open for a longer period by **keeping on accessing different cache blocks in the row**

Leveraging RowPress, a user-level program
induces bitflips when RowHammer cannot

How to Avoid RowPress Bitflips

We propose a methodology to **adapt existing RowHammer mitigations to also mitigate RowPress**

Key Mechanisms:

1. Limit the maximum time that a row can stay open
2. Configure the RowHammer mitigation to account for the RowPress-induced reduction in the number of activations needed to cause bitflips

Our solutions **mitigate RowPress** at **low additional performance overhead**

More Results

Many more results & analyses in the paper

- 6 major takeaways
- 19 major empirical observations

Fully open source and artifact evaluated

- https://github.com/CMU-SAFARI/RowPress

RowPress

Amplifying Read Disturbance in Modern DRAM Chips

ISCA 2023 Session 2B: Monday 19 June, 2:15 PM EDT

Haocong Luo

Ataberk Olgun *A. Giray Yağlıkçı* *Yahya Can Tuğrul*

Steve Rhyner *Meryem Banu Cavlak* *Joël Lindegger*

Mohammad Sadrosadati *Onur Mutlu*

SAFARI

ETH zürich