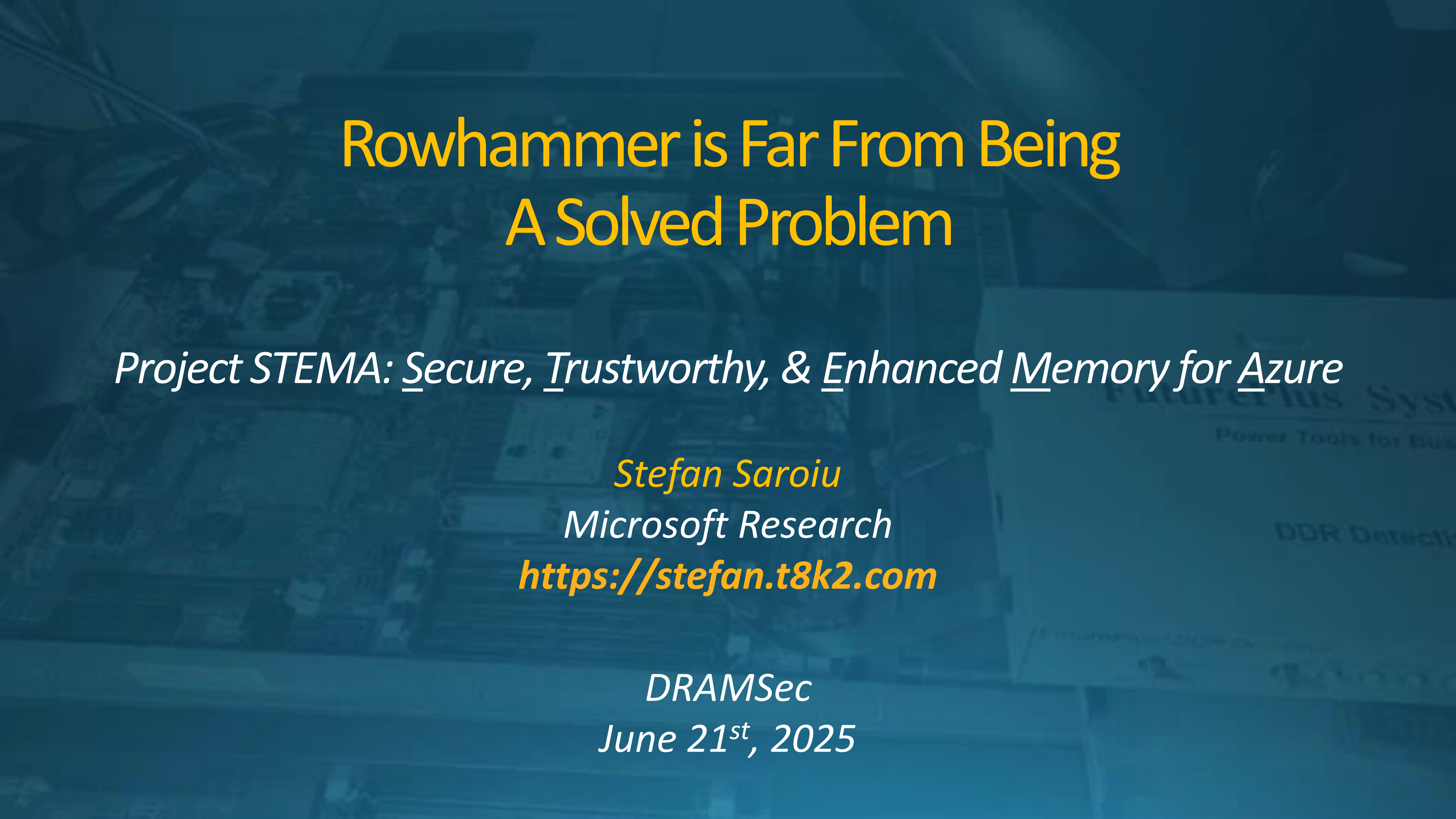


Rowhammer is Far From Being A Solved Problem

Project STEMA: Secure, Trustworthy, & Enhanced Memory for Azure

Stefan Saroiu
Microsoft Research
https://stefan.t8k2.com

DRAMSec
June 21st, 2025

Message #1: To Researchers

Many PRAC Challenges Remain!

Many PRAC Challenges Remain (1/4)

- PRAC needs correct config of MANY params

Many PRAC Challenges Remain (1/4)

- PRAC needs correct config of MANY params
  - Example 1: spec is silent on when ALERTn is raised
  - Example 2: spec is silent on how to configure counter thresholds

- Correct configurations often require very conservative values
- Conservative values come with performance penalties

- Will DRAM vendors configure PRAC to eliminate all forms of Rowhammer?

Many PRAC Challenges Remain (2/4)

- PRAC resets row counters

Many PRAC Challenges Remain (2/4)

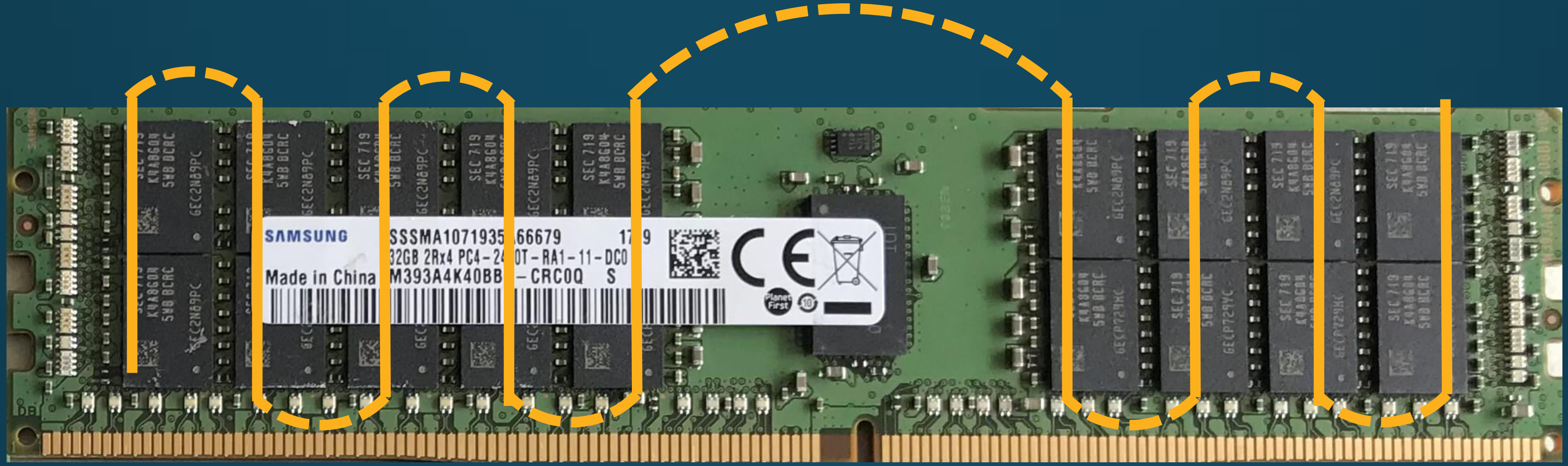
- PRAC resets row counters

- Ideally, reset a row’s counter when all its potential victims are refreshed
- DRAM cannot guarantee that all potential victims are refreshed atomically

- Counters will either be reset too early, or too late

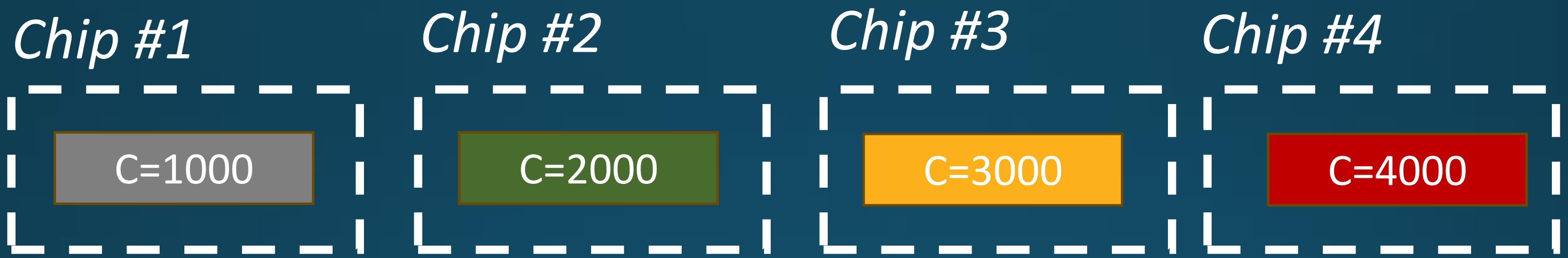
- Is there a principled way to handle counter resets securely?

Many PRAC Challenges Remain (3/4)



- One row spans many DRAM chips
  with counter values that are out-of-sync

Same Row Has Different Counters



Chip #1

C=1000

Chip #2

C=2000

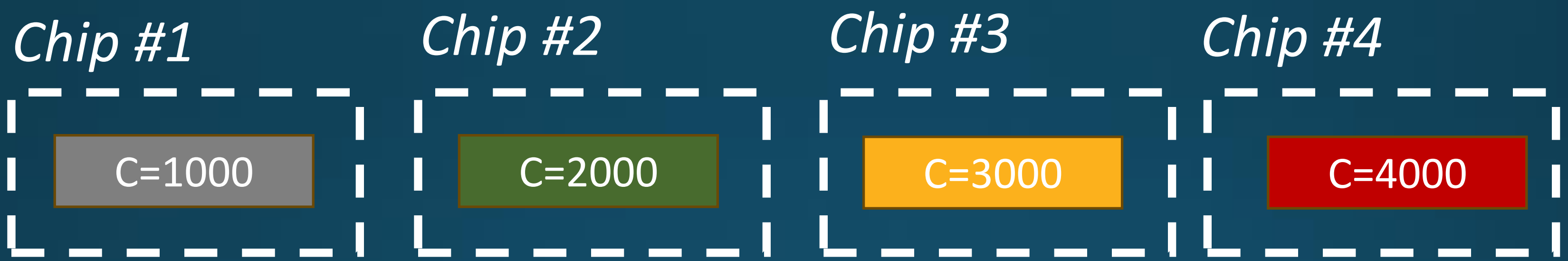
Chip #3

C=3000

Chip #4

C=4000

Chip #4 Requires Mitigation



Chip #1

C=1000

Chip #2

C=2000

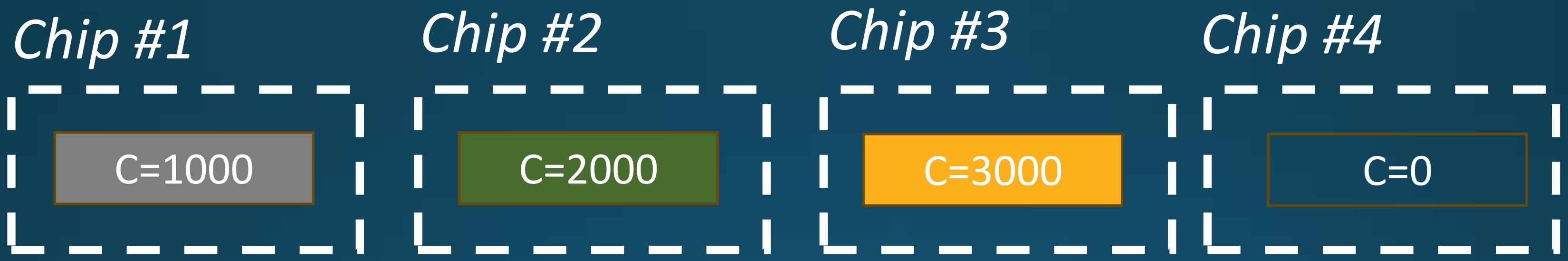
Chip #3

C=3000

Chip #4

C=4000

Chip #4 Requires Mitigation



Chip #1

C=1000

Chip #2

C=2000

Chip #3

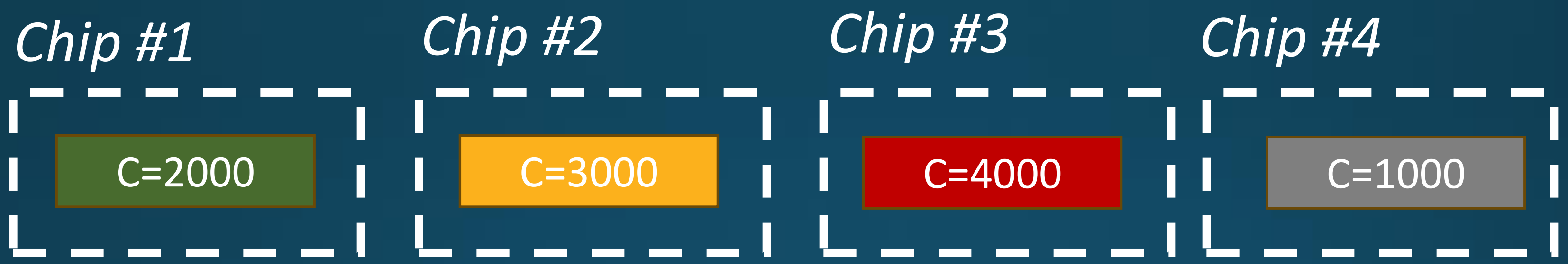
C=3000

Chip #4

C=0

After Another 1000 row activations

After Another 1000 row activations



Chip #1

C=2000

Chip #2

C=3000

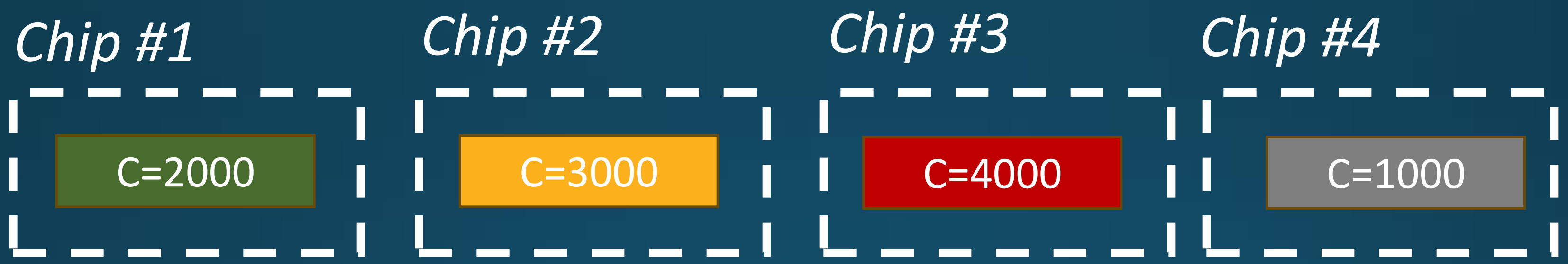
Chip #3

C=4000

Chip #4

C=1000

Chip #3 Requires Mitigation



Chip #1

C=2000

Chip #2

C=3000

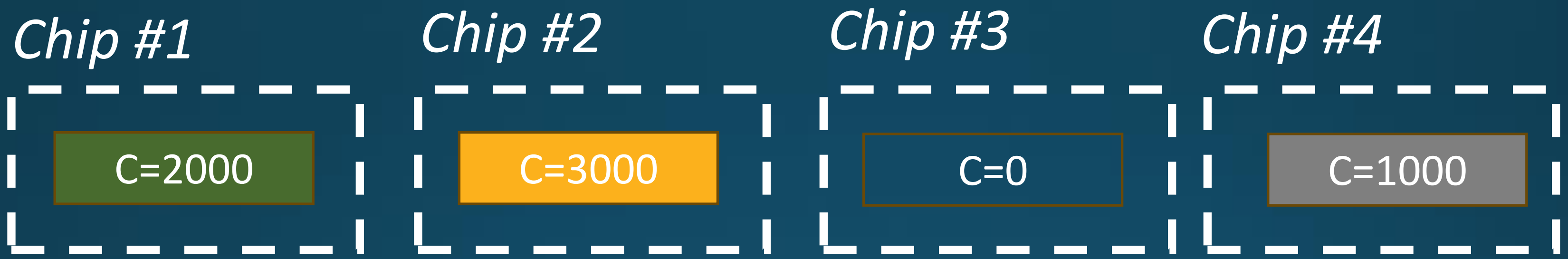
Chip #3

C=4000

Chip #4

C=1000

Chip #3 Requires Mitigation



Chip #1

C=2000

Chip #2

C=3000

Chip #3

C=0

Chip #4

C=1000

Many PRAC Challenges Remain (4/4)

- PRAC lacks rigorous security analysis!
  - No reference implementation

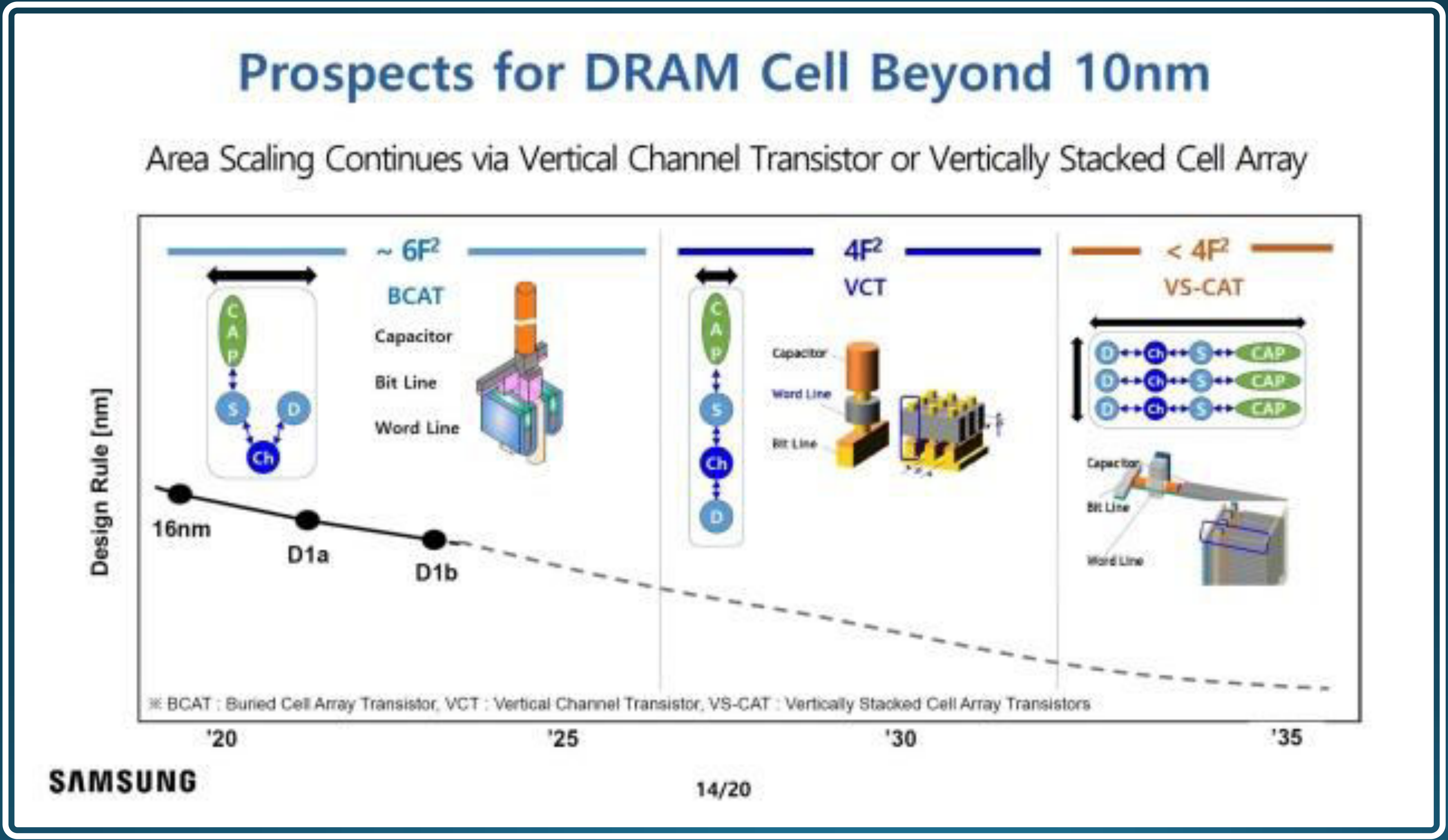
Rowhammer is far from being solved

- Will PRAC be configured correctly?
- Counter Resets?!
- How to handle out-of-sync counters?
- Principled security analysis
- Lightweight ALERTs
- Per-row Rowhammer thresholds

Message #2: To Industry

Stop making unsubstantiated promises
Be skeptical

No More Surprises!



Prospects for DRAM Cell Beyond 10nm

Area Scaling Continues via Vertical Channel Transistor or Vertically Stacked Cell Array

※ BCAT : Buried Cell Array Transistor, VCT : Vertical Channel Transistor, VS-CAT : Vertically Stacked Cell Array Transistors

SAMSUNG

Slide from IMW 2024

Current Prevalent Attitude in Industry

- VCT architecture eliminates Rowhammer at the root

My take:

- You can’t scale DRAM further without experiencing significant data integrity problems

I’m worried