Scalable and Secure Row-Swap:
Efficient and Safe Row Hammer Mitigation in Memory Systems

Best Paper Award: HPCA 2023 @ Montreal

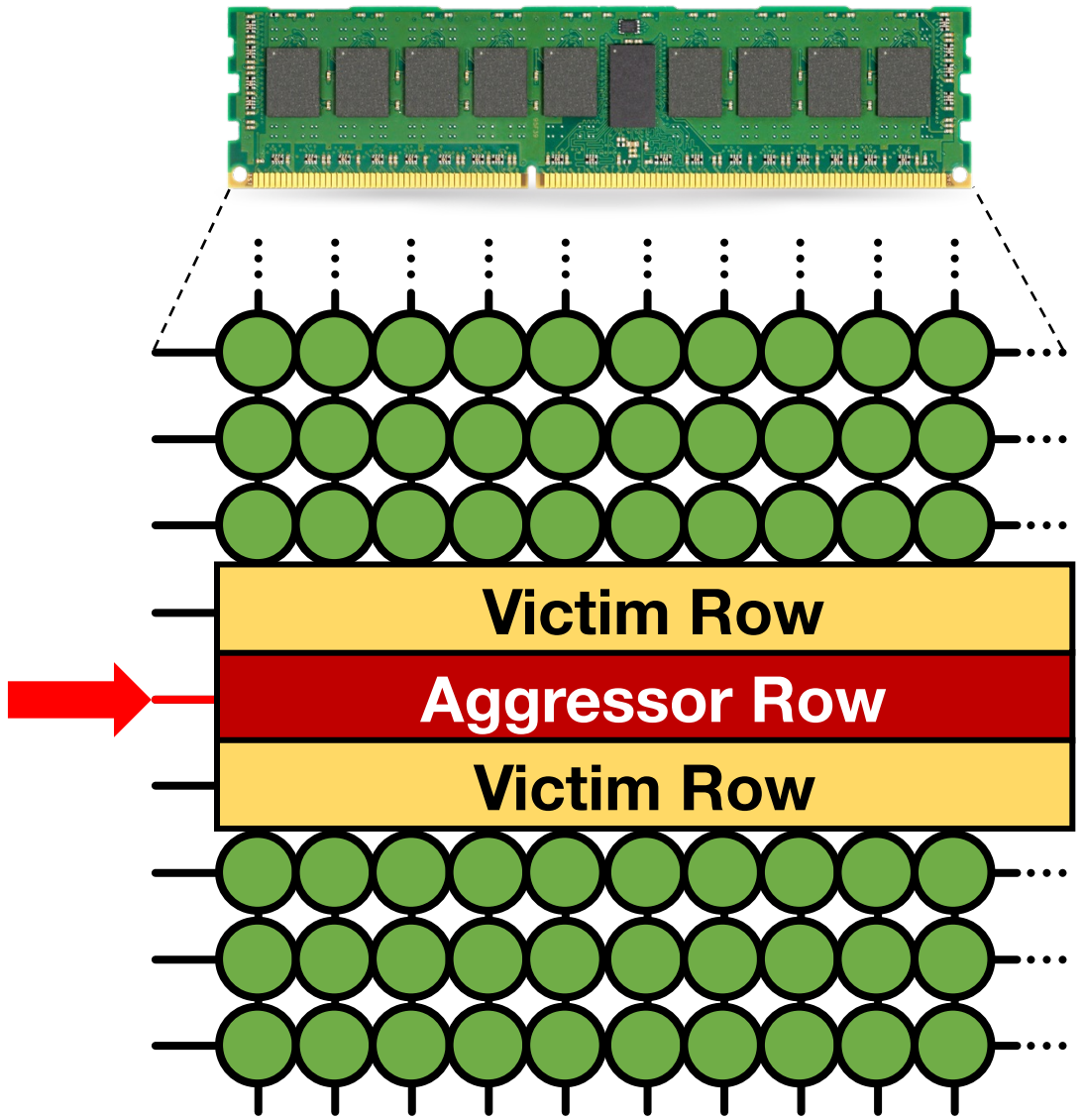
Jeonghyun Woo, Gururaj Saileshwar*, Prashant Nair



* NVIDIA. STAR LAB UBC THE UNIVERSITY OF BRITISH COLUMBIA

Row Hammer

ACCESS
(ACTIVATE)



Row Hammer Attacks

ZDNET

tomorrow
belongs to those who embrace it
today

trending tech innovation business security

/ innovation

Home / Innovation / Security

'Rowhammer' DRAM flaw could widespread, says Google

Google's Project Zero team have found a serious DRAM bug that it's using to encourage computer vendors to cough up more information about hardware flaws.

threatpost

Podcasts / Malware / Vulnerabilities / InfoSec Insiders / Webinars

Mirai-Fueled IoT Botnet Behind DDoS Attacks on DNS Providers

Fake

Rowhammer Vulnerability Comes to Android



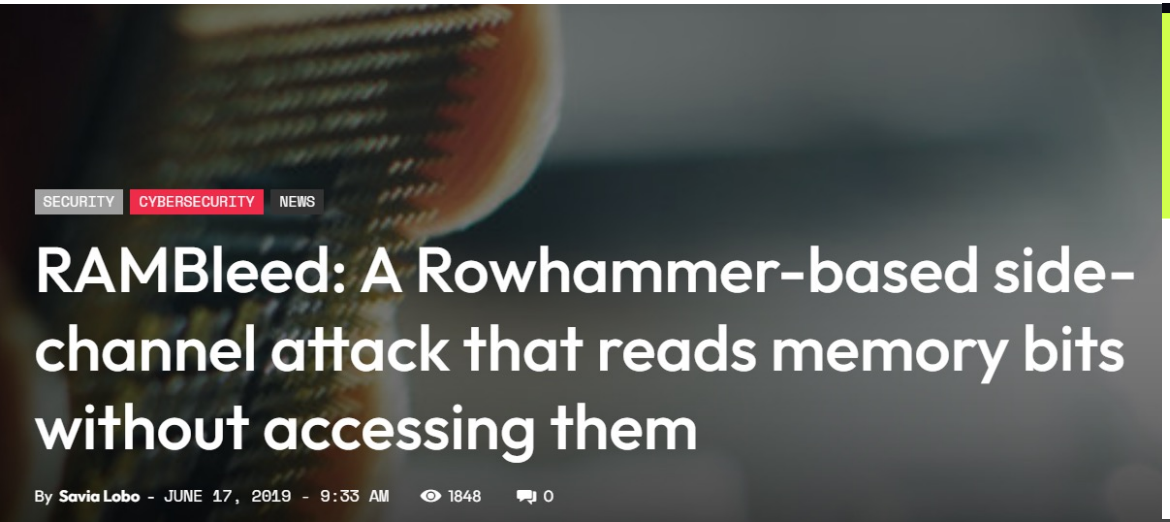
Author:
Tom Spring

October 24, 2016
/ 12:28 pm

2:30 minute read

Share this article:





SECURITY CYBERSECURITY NEWS

RAMBleed: A Rowhammer-based side-channel attack that reads memory bits without accessing them

By Savia Lobo - JUNE 17, 2019 - 9:33 AM 1848 0

ZDNET

tomorrow
belongs to those who embrace it
today

trending tech innovation business security advice buying guides

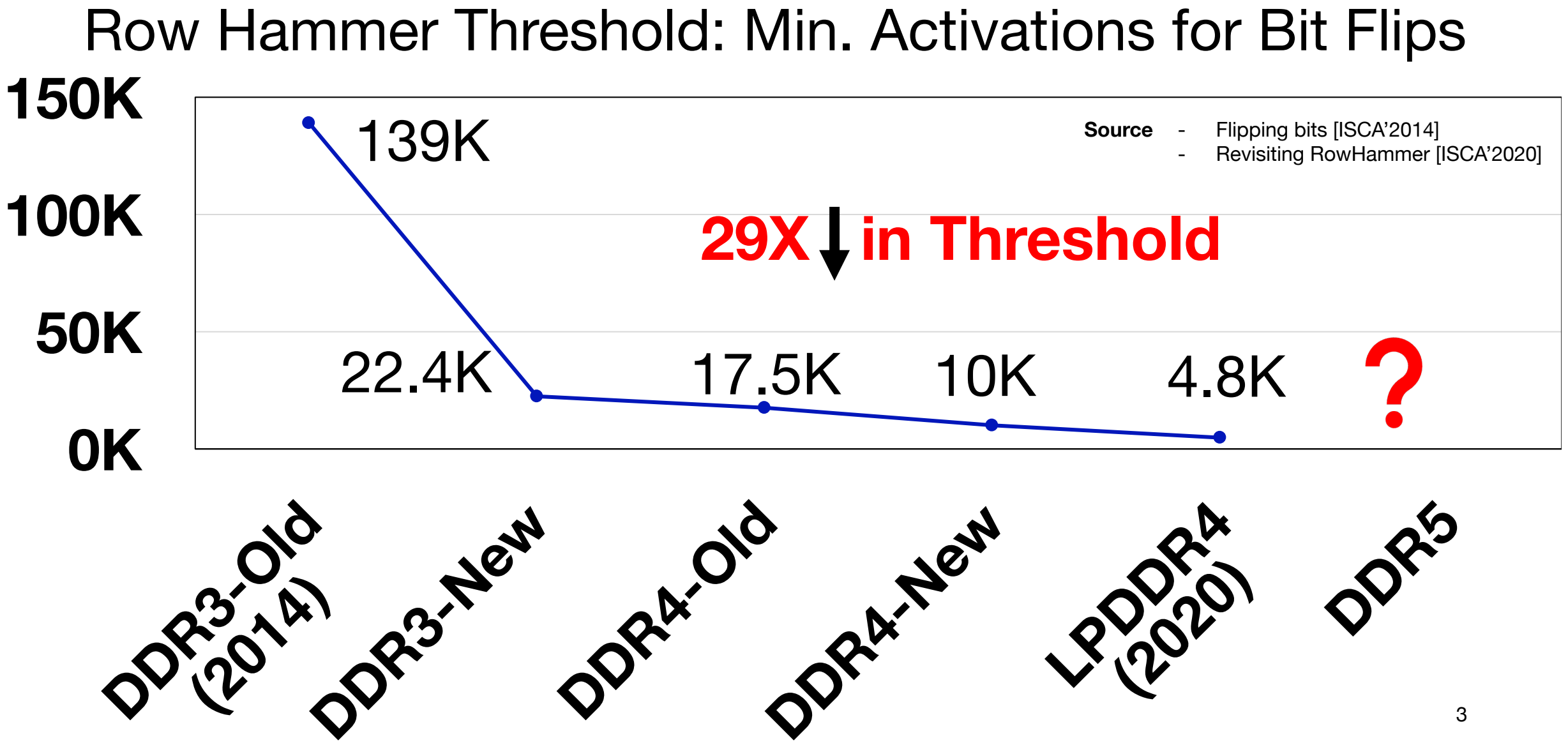
/ innovation

Home / Innovation / Security

This new attack bypasses Rowhammer defenses in most DRAM, say researchers

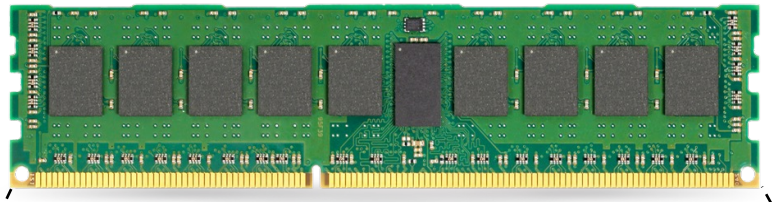
New technique targets industry-wide mitigations implemented in response to the first Rowhammer attack.

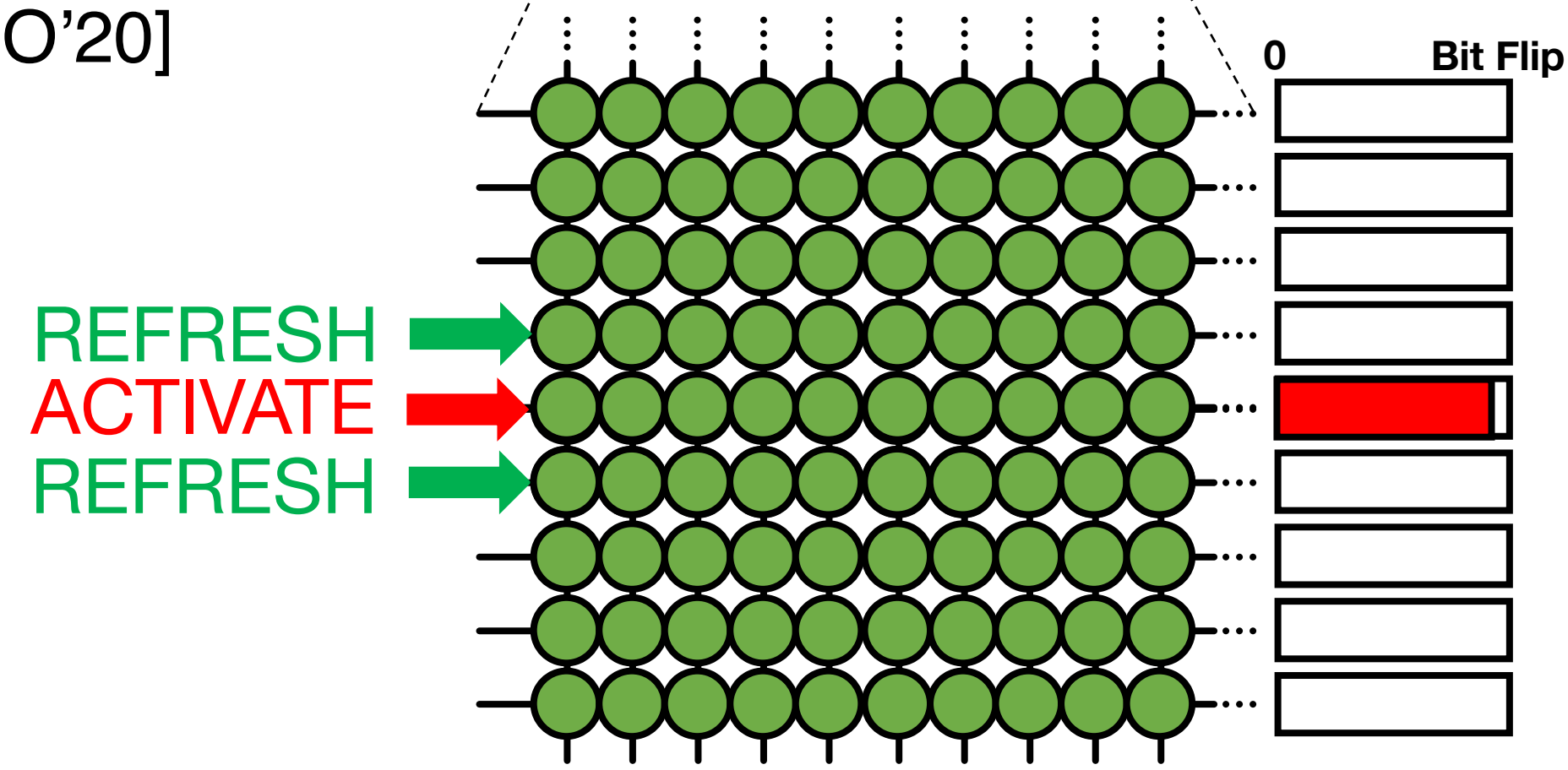
Row Hammer is Getting Worse



Victim-Focused Mitigations (VFM)

Target Row Refresh [2015]
TWiCe [ISCA'19]
Graphene [MICRO'20]
and others …



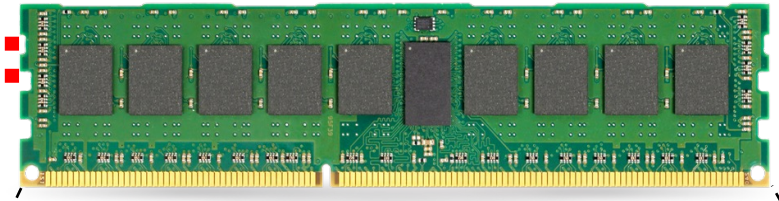


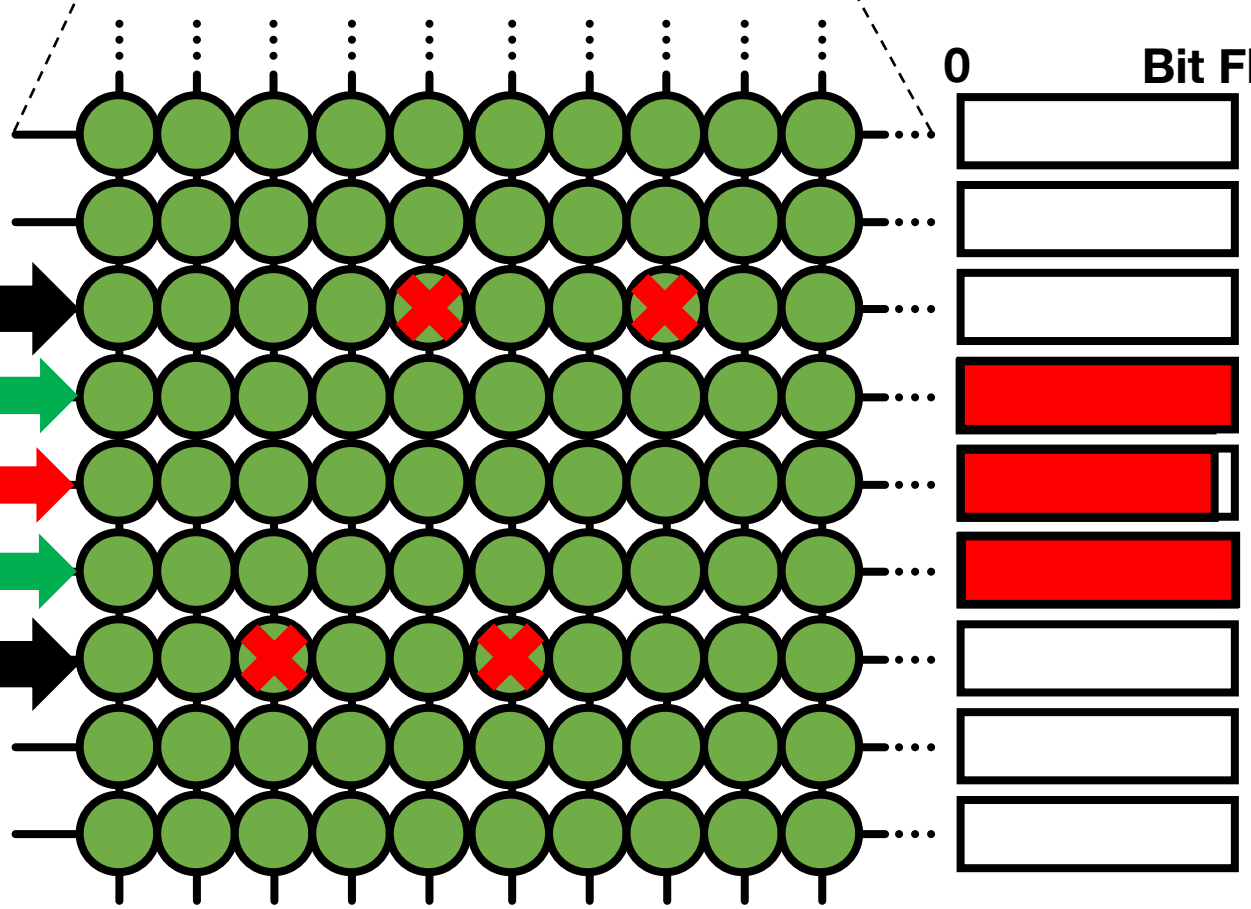
Half-Double Attack on VFM

Google's Half-Double Attack: Exploits Mitigative Refresh*

As Chips Shrink, Rowhammer Attacks Get Harder to Stop

A full fix for the "Half-Double" technique will require rethinking how memory semiconductors are designed.

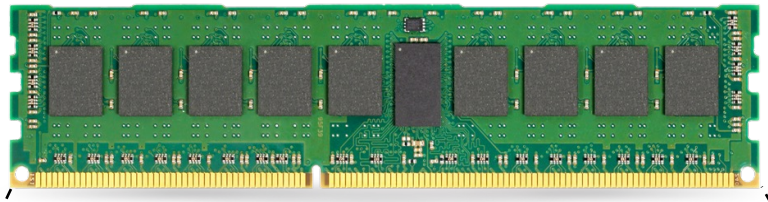




Mitigation → Break Defense

Source*: Half-Double [USENIX SECURITY'2022]

Randomized Row-Swap [ASPLOS'22]



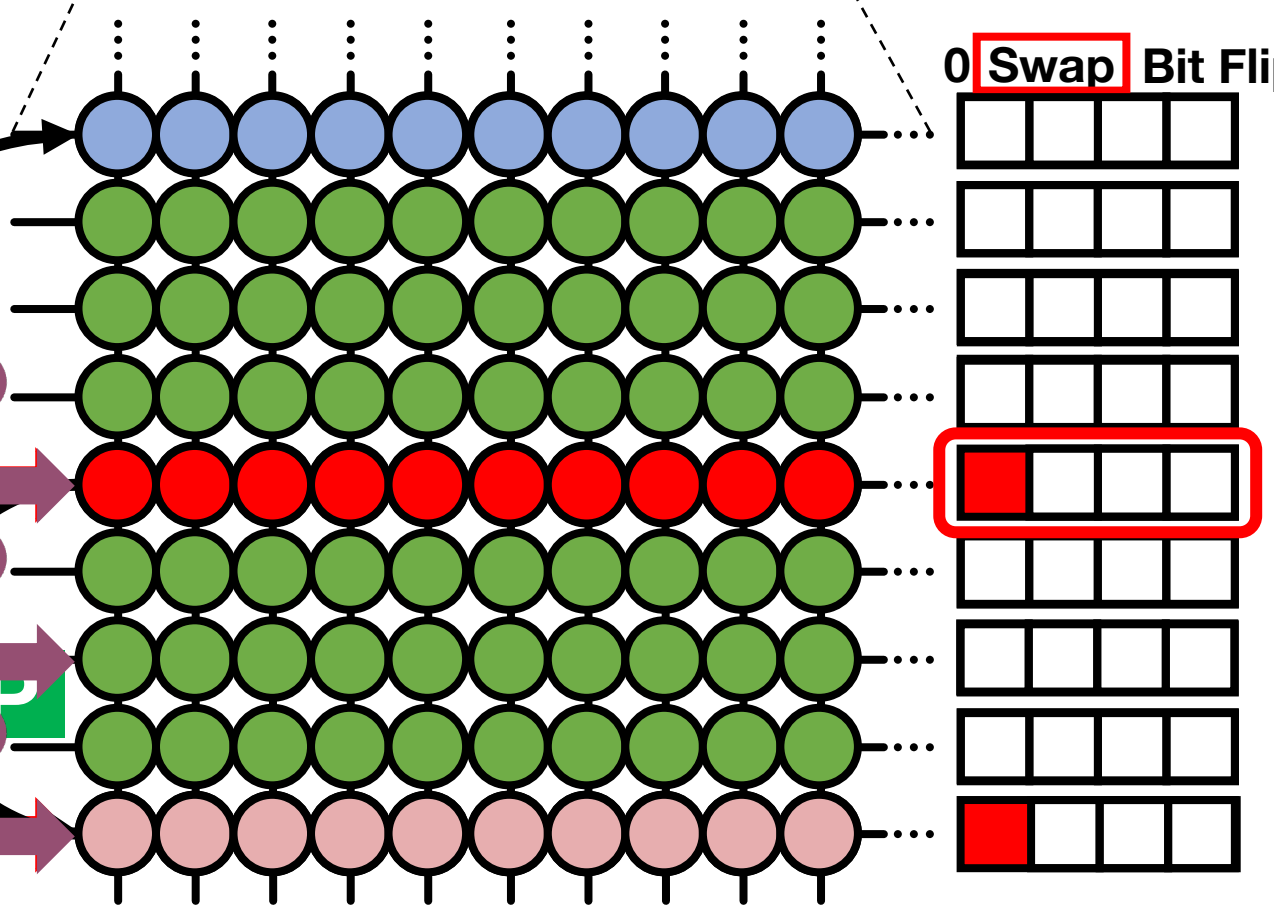
Spatial correlation

Defend Half-Double

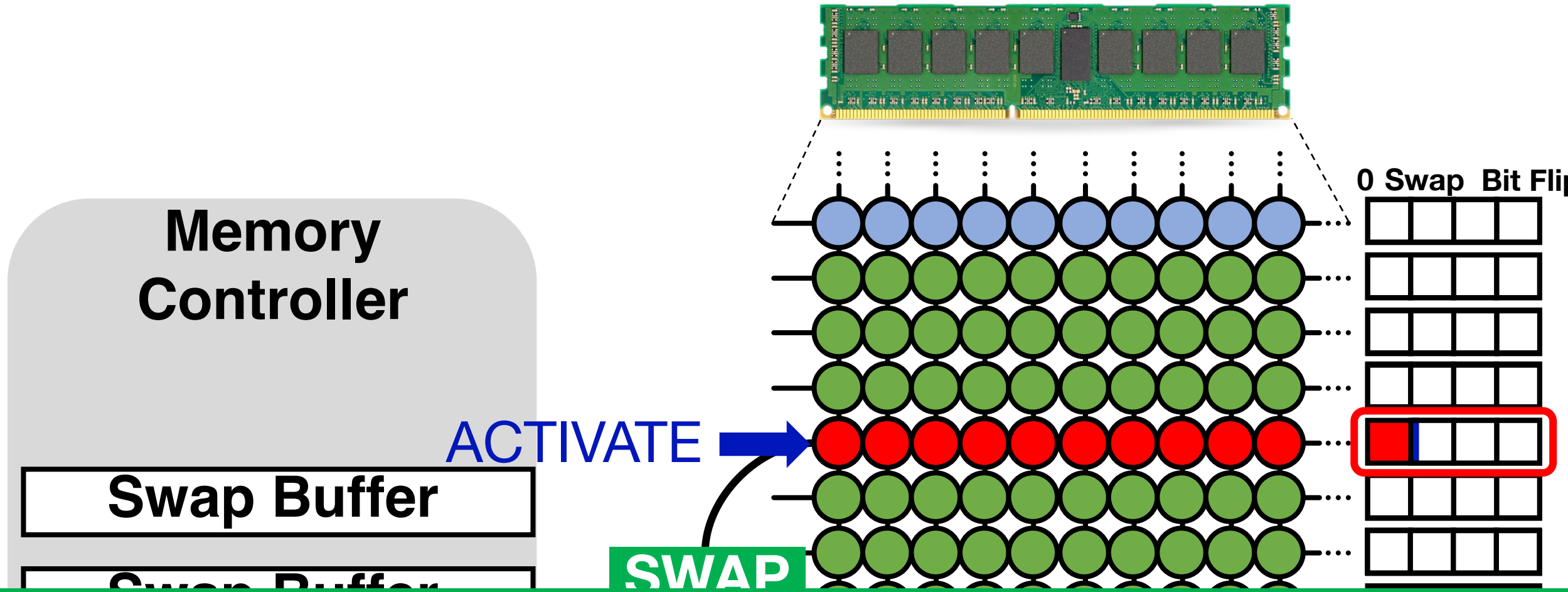
Swap Threshold

Security ↑ Performance ↓

3+ Years of Security

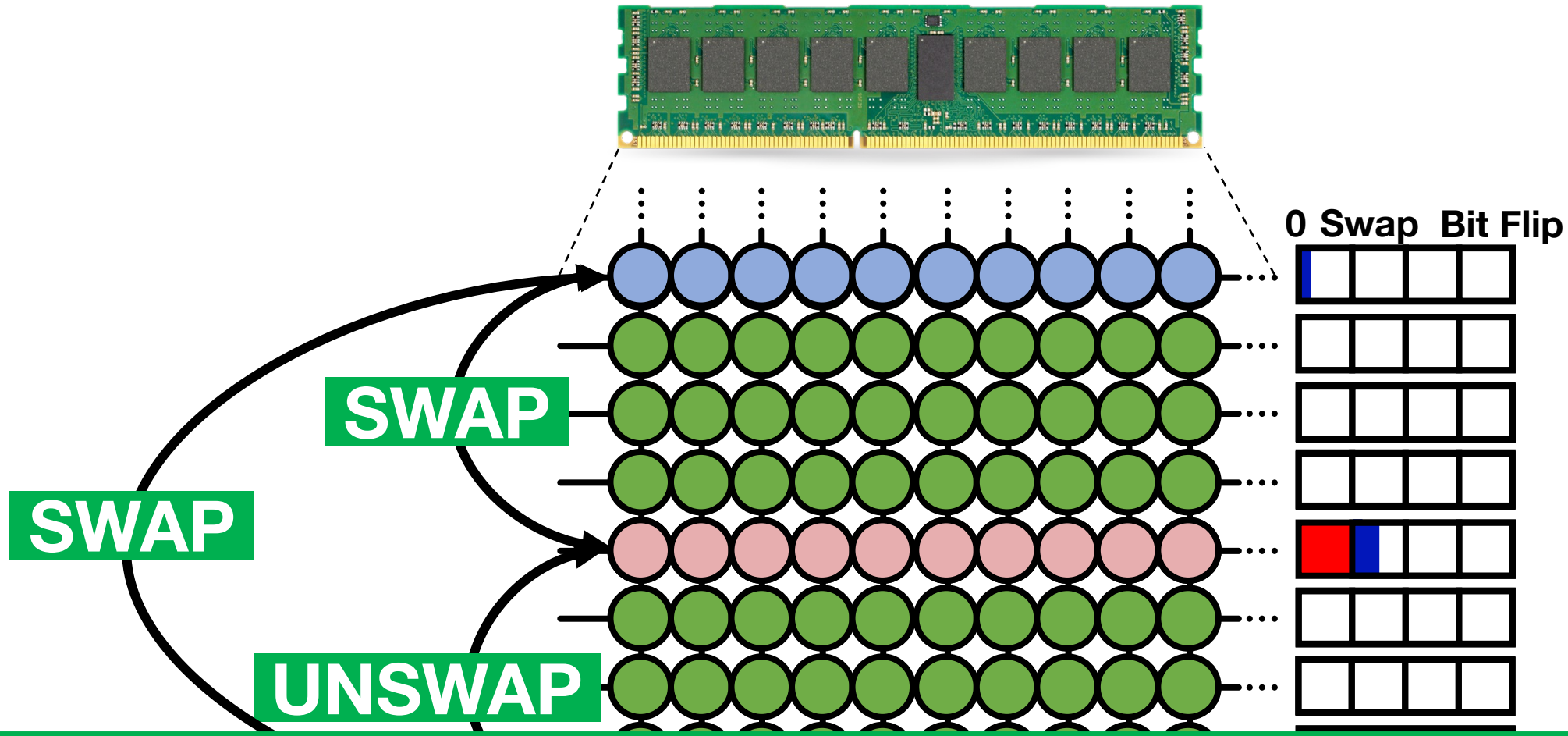


RRS Security Pitfall: Latent Activations



Swap Operation → 1 Latent Activation

RRS Security Pitfall: Latent Activations



Unswap-Swap Operation → 2 Latent Activations

Juggernaut Attack

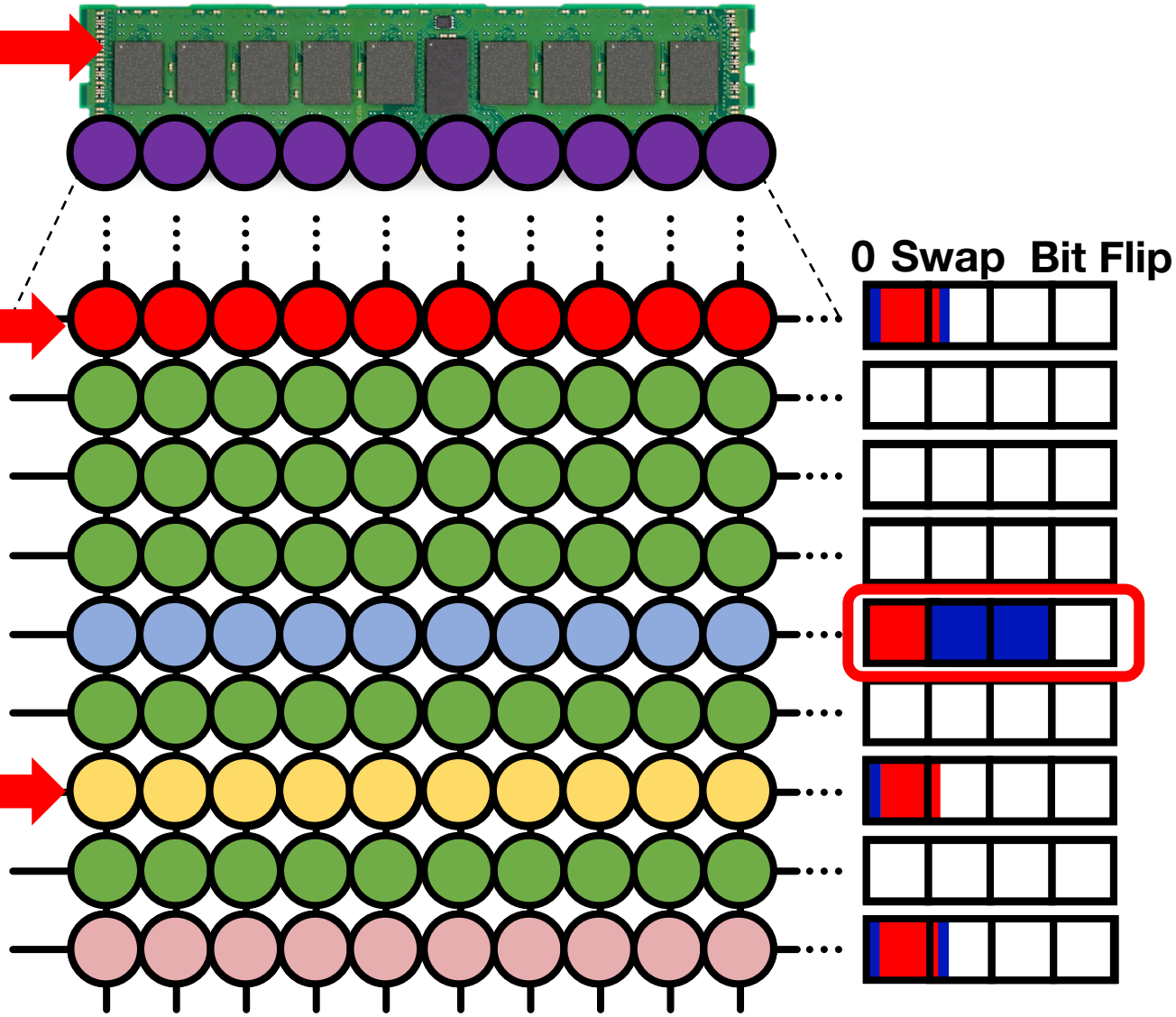


ACTIVATE AGGRESSOR

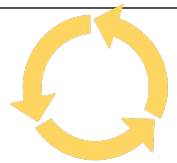
1 Exploit latent activations

ACTIVATE

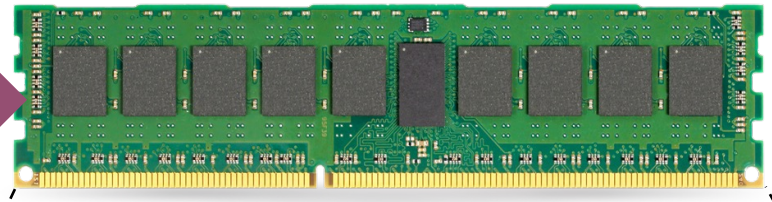
ACTIVATE



Juggernaut Attack



Random Guess

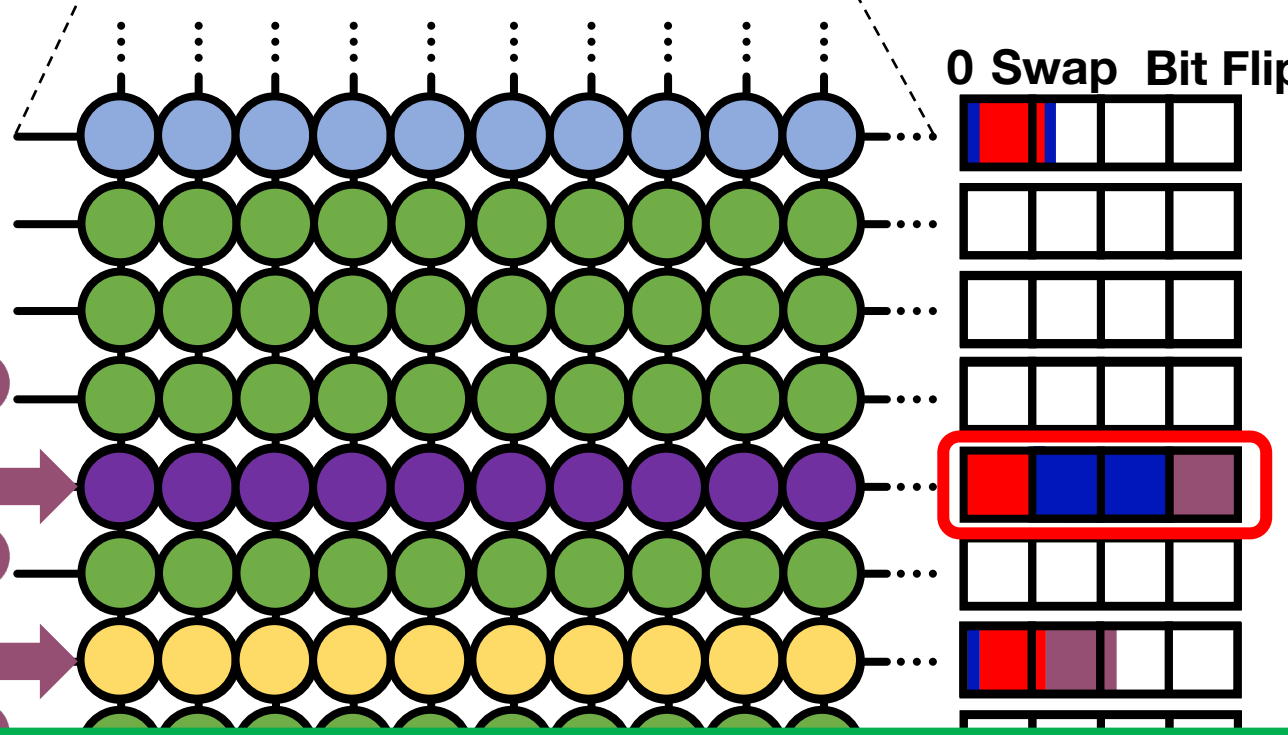


1 Exploit latent activations

2 Guess Aggressor



Break RRS in < 4 hours

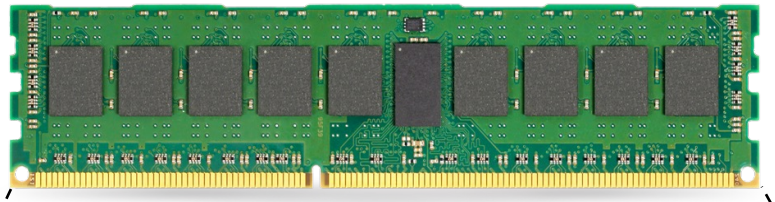


Random Guess

Random Guess

Please see the paper for a detailed security analysis

Secure Row-Swap (SRS)



Unswap

ACTIVATE

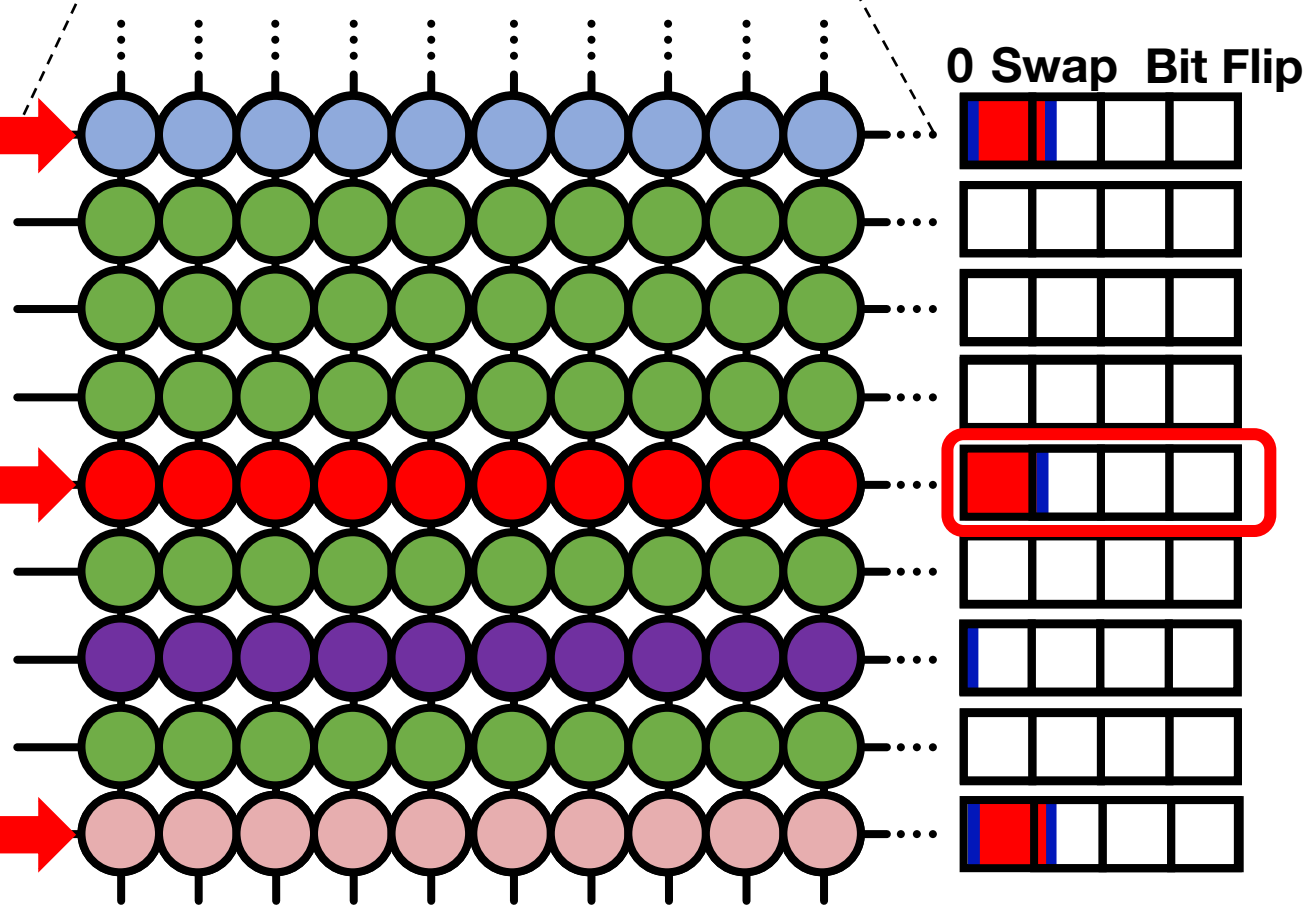
Swap-Only

Latent Activations

ACTIVATE

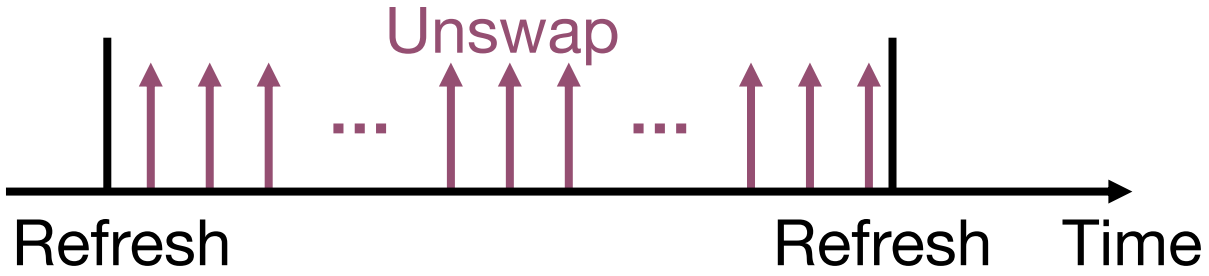
2+ Years of Security

ACTIVATE

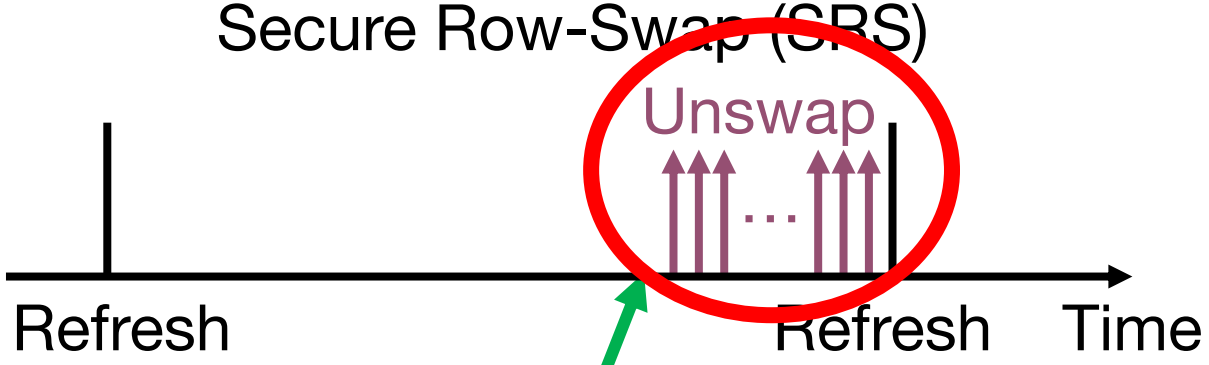


Secure Row-Swap (SRS)

Randomized Row-Swap (RRS)

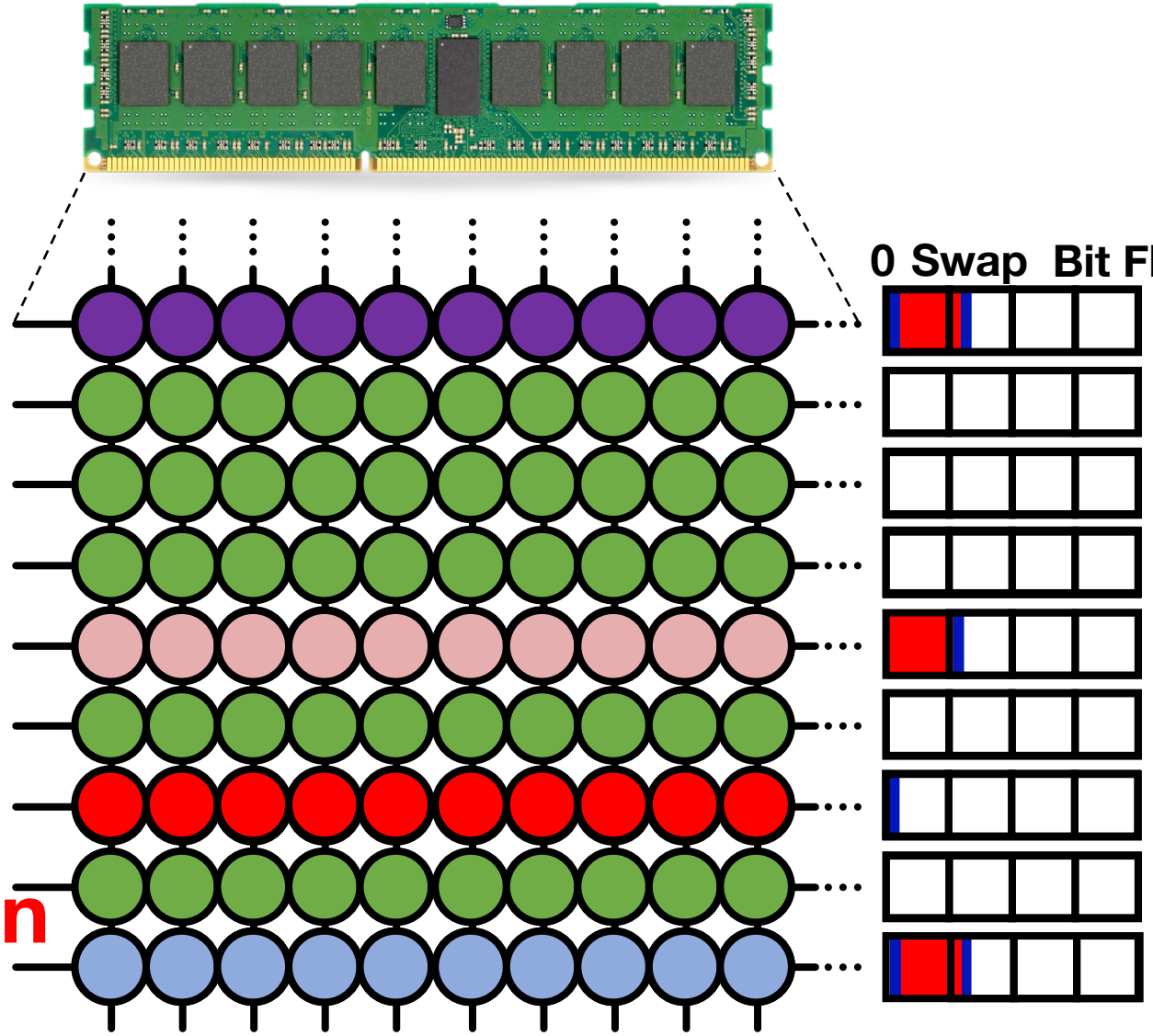


Secure Row-Swap (SRS)



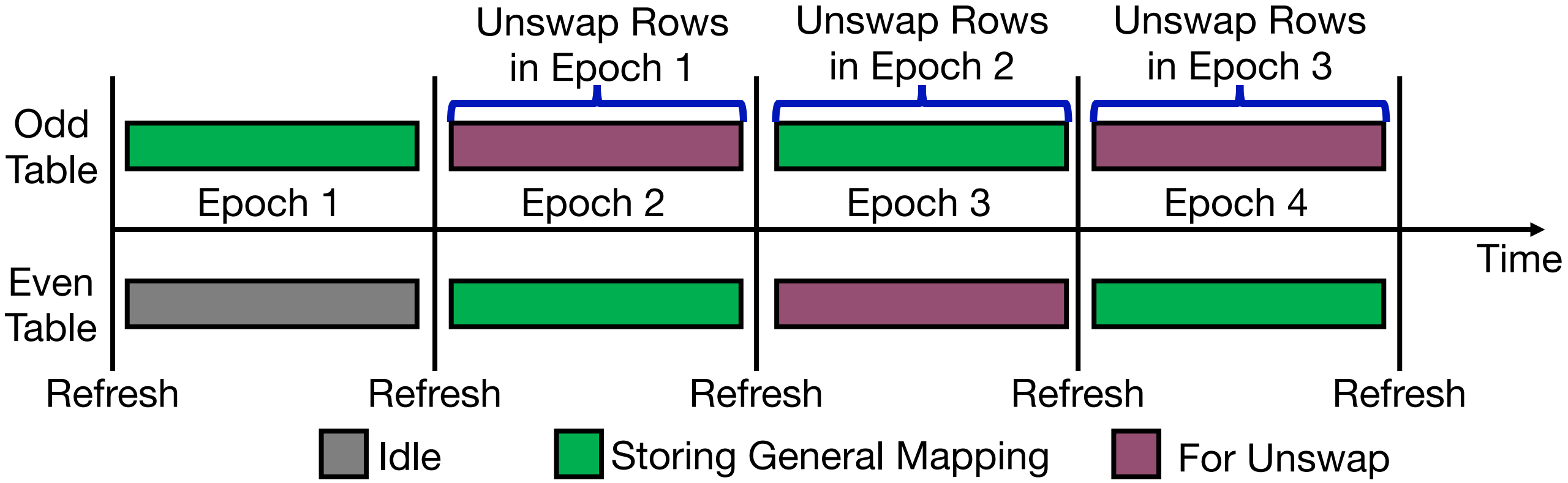
Latency Spike

Performance Degradation



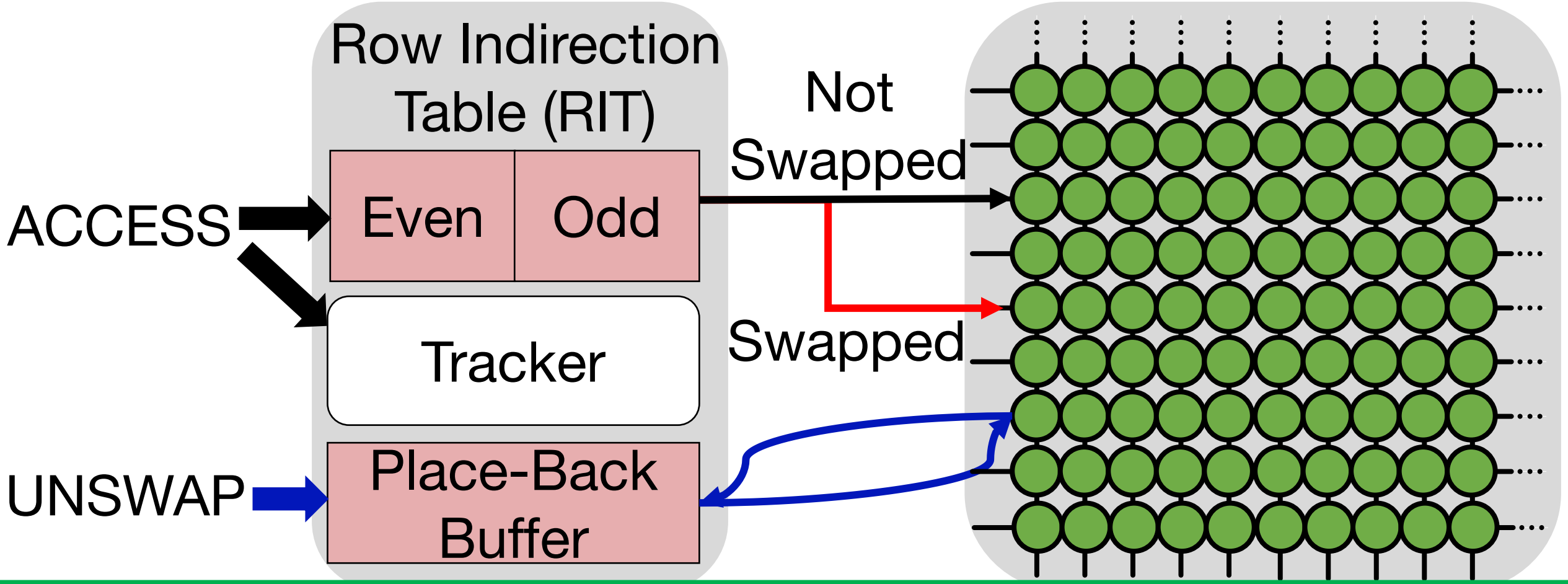
Secure Row-Swap (SRS)

Key Idea: Delay unswaps using two separate tables



No Performance Overhead

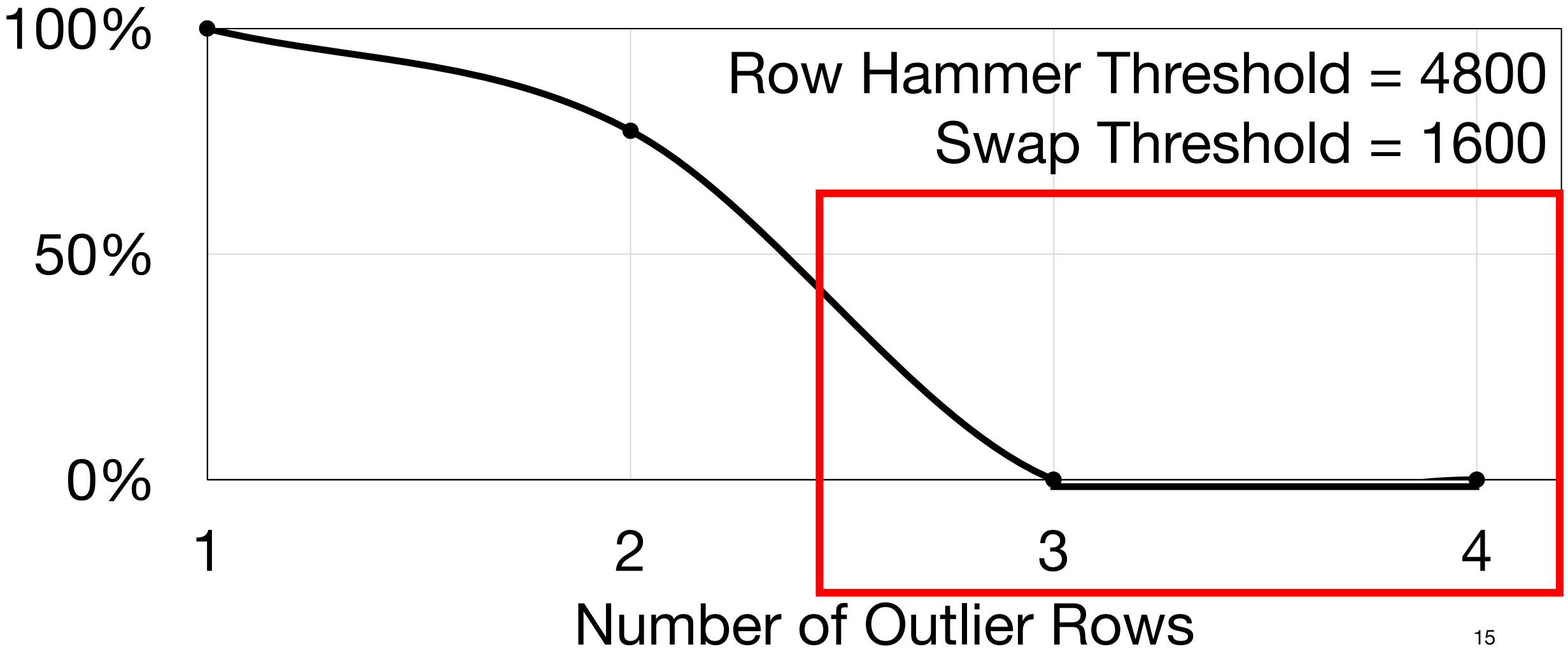
Implementation of Secure Row-Swap



Please see the paper for our detailed implementation

Insight: Scalable & Secure Mitigation

Outlier rows: Bypassing SRS → Cause Bit Flips



Insight: Scalable & Secure Mitigation

Few outliers bypass SRS

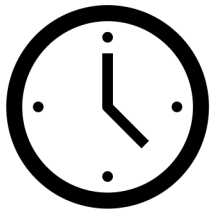
Pin these outliers in LLC!



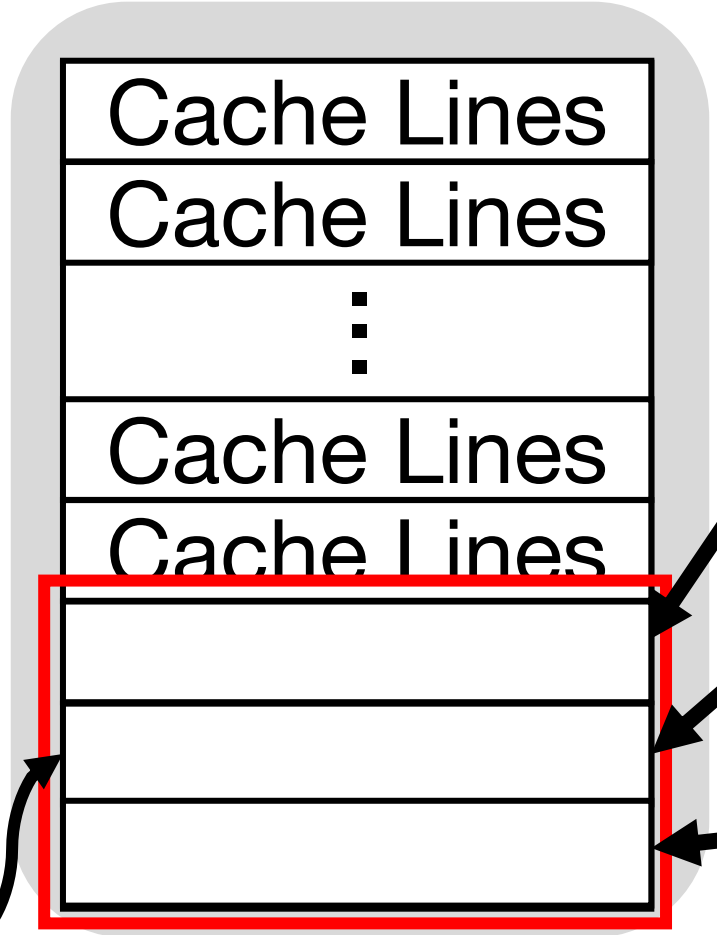
Better Scalability

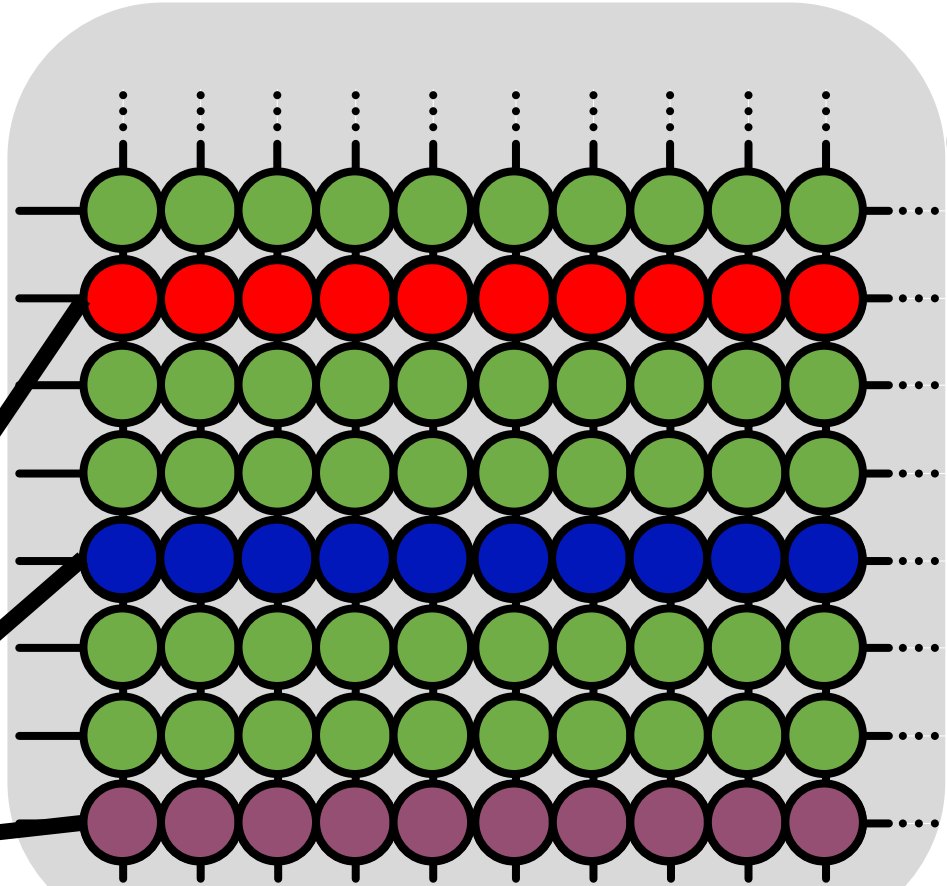
Number of Outlier Rows	Attack Time
1	12 Secs
2	1.3 Hours
3	30.7 Days
4	64 Years

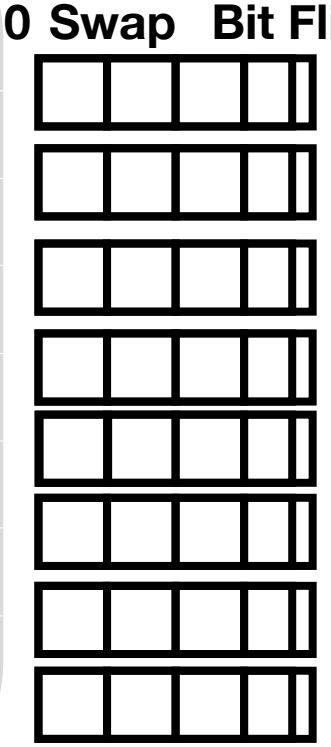
Scalable and Secure Row-Swap



Every
31 days





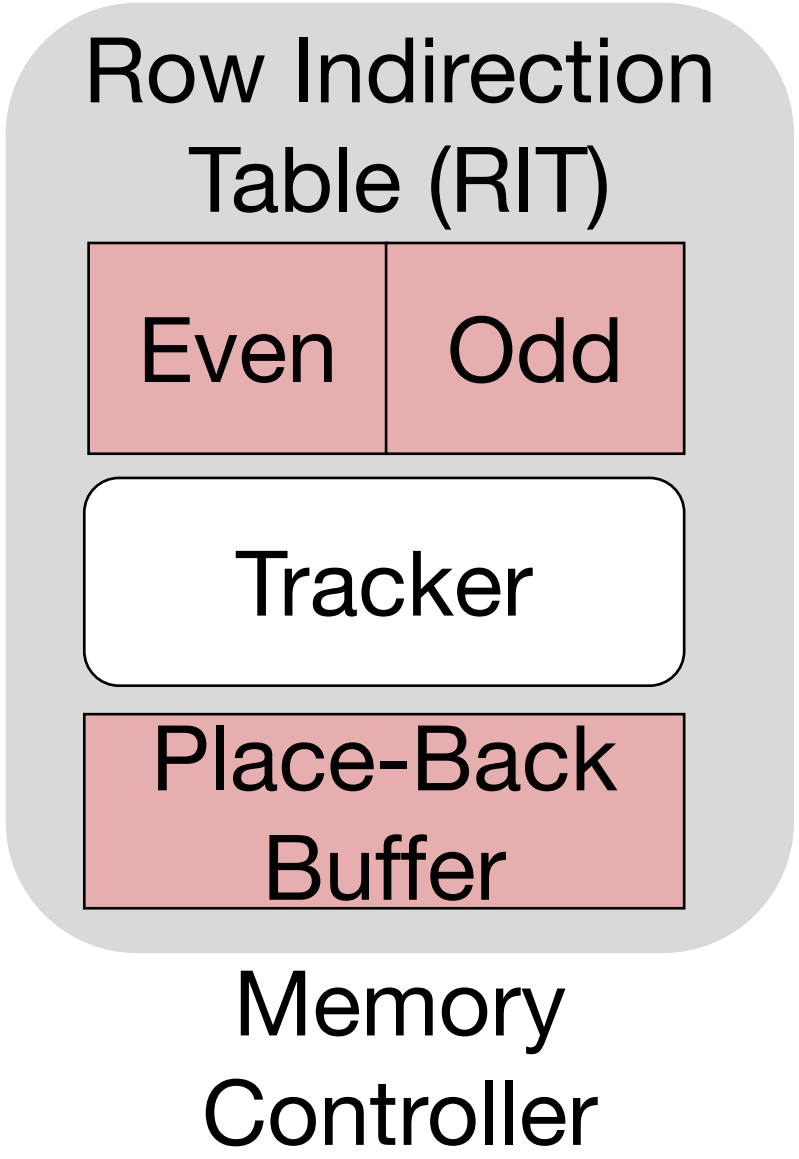


Pinning Region

Last Level Cache

DRAM

Scale-SRS: SRAM Overhead

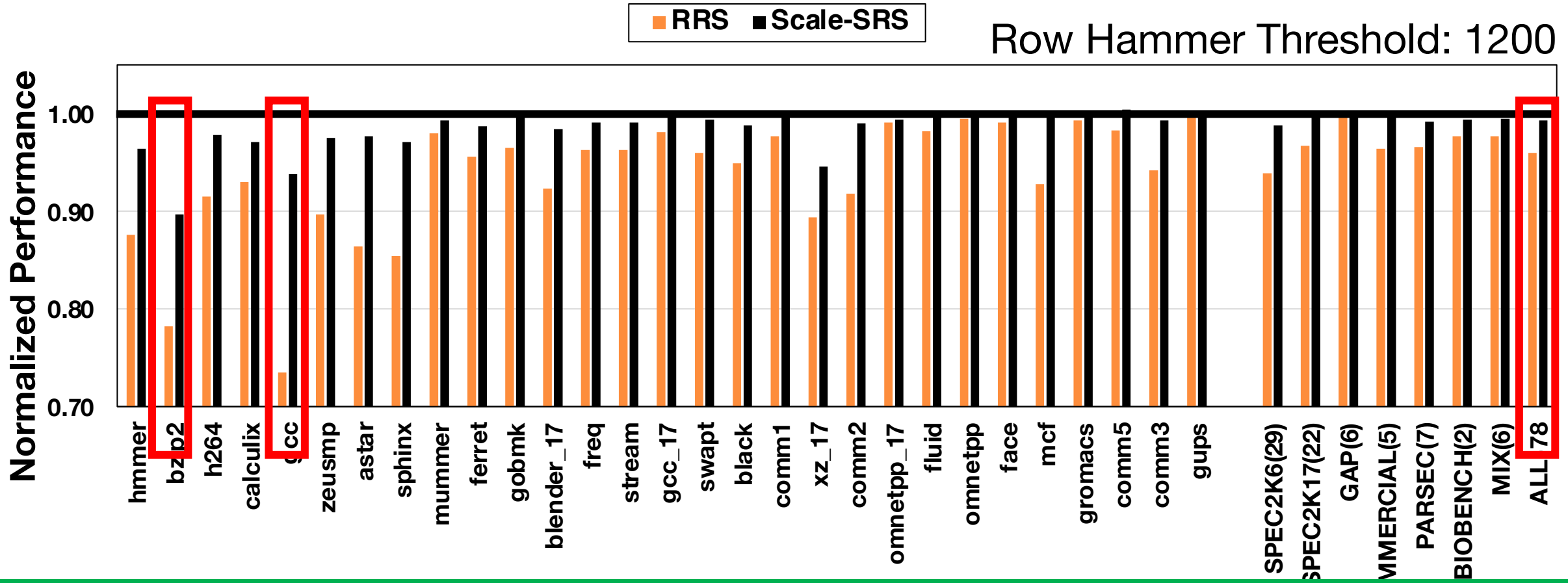


Overhead Per Bank

Row Hammer Threshold	RRS	Scale-SRS
4800	36 KB	18.7 KB
2400	131 KB	44.4 KB
1200	251 KB	76.9 KB

3.3X lower SRAM Overhead

Scale-SRS: Performance



Less than 1% performance overhead

Summary

Juggernaut → Breaks Randomized Row-Swap (RRS) in **< 4 hours**

Secure Row-Swap: Secure against **2+ years** of continuous attacks

Scalable & Secure Row-Swap → **Scalable and Low-Cost Mitigation**

Thank You!

jhwoo36@ece.ubc.ca

JeonghyunW

jeonghyunwoo0306.github.io



RRS versus Scale-SRS

