CSI:Rowhammer

Cryptographic Security and Integrity against Rowhammer

Jonas Juffinger, Lukas Lamster, Andreas Kogler, Moritz Lipp, Maria Eichlseder, Daniel Gruss

2023-05-23

IEEE Symposium on Security and Privacy 2023

The Problem with Rowhammer Countermeasures

The Problem with Rowhammer Countermeasures

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
    - Bit Flips are infrequent - ECC, Refresh Rate

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit Flips are infrequent - ECC, Refresh Rate~~ [Kim+14]

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit Flips are infrequent - ECC, Refresh Rate~~ [Kim+14]
  - Detectable with Performance Counters - ANVIL

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit Flips are infrequent - ECC, Refresh Rate~~ [Kim+14]
  - ~~Detectable with Performance Counters - ANVIL~~ [Gru+18]

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit Flips are infrequent - ECC, Refresh Rate~~ [Kim+14]
  - ~~Detectable with Performance Counters - ANVIL~~ [Gru+18]
  - Hammer Distance is 1 - TRR, ZebRAM, B-CATT

The Problem with Rowhammer Countermeasures

- Focusing on **characteristics**
- Which later turn out to be incomplete
  - ~~Bit Flips are infrequent - ECC, Refresh Rate~~ [Kim+14]
  - ~~Detectable with Performance Counters - ANVIL~~ [Gru+18]
  - ~~Hammer Distance is 1 - TRR, ZebRAM, B-CATT~~ [Kog+22]

CSI:Rowhammer

Generic approach to data integrity protection

CSI:Rowhammer – Cryptographic Security and Integrity against Rowhammer

- **Generic** approach to data integrity protection

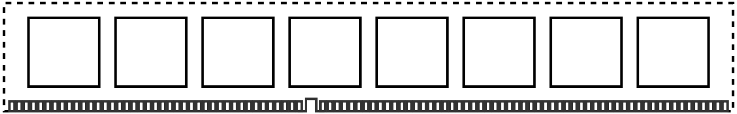
CSI:Rowhammer – Cryptographic Security and Integrity against Rowhammer

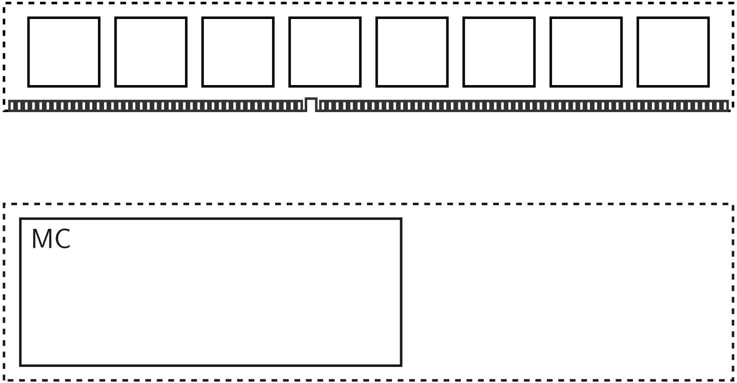
- **Generic** approach to data integrity protection
- Detect all data integrity failures with a MAC

- **Generic** approach to data integrity protection
- Detect all data integrity failures with a MAC
- Best effort correction

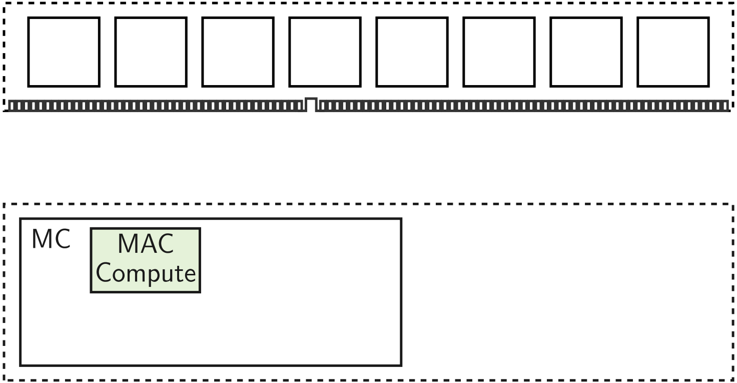
CSI:Rowhammer – Cryptographic Security and Integrity against Rowhammer

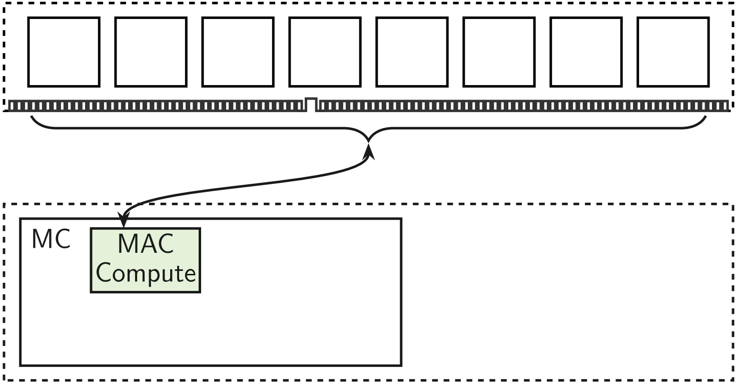
- **Generic** approach to data integrity protection
- Detect all data integrity failures with a MAC
- Best effort correction
- All Rowhammer attacks are DoS in the **worst case**

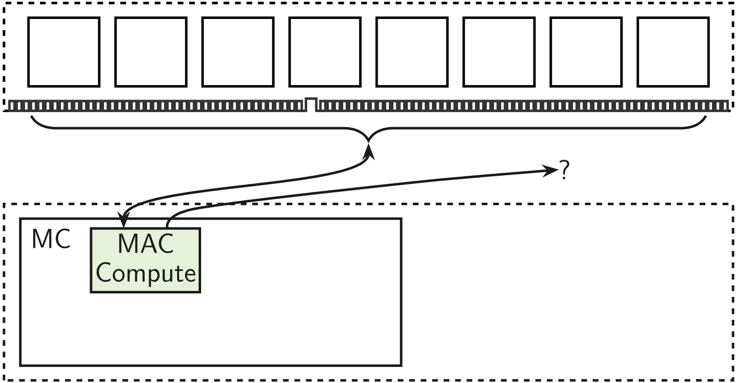


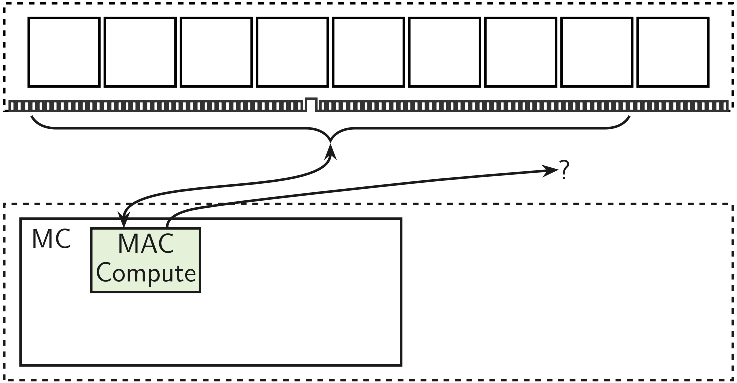


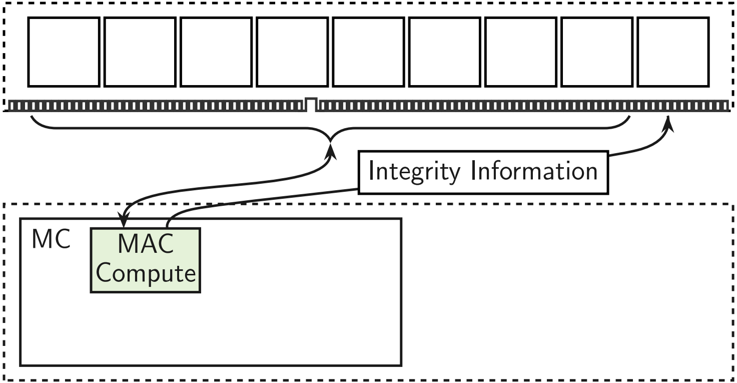
MC

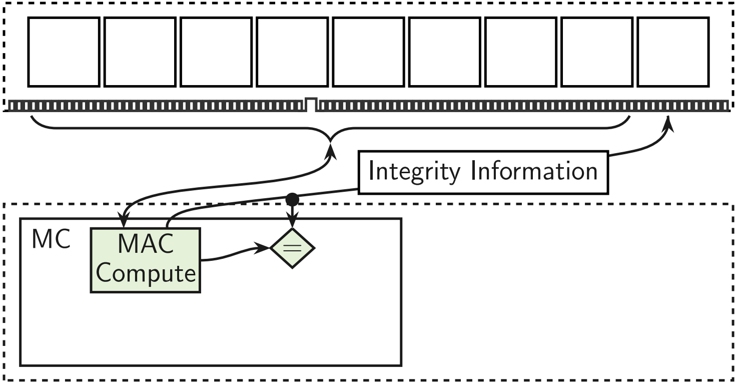

MC
MAC Compute

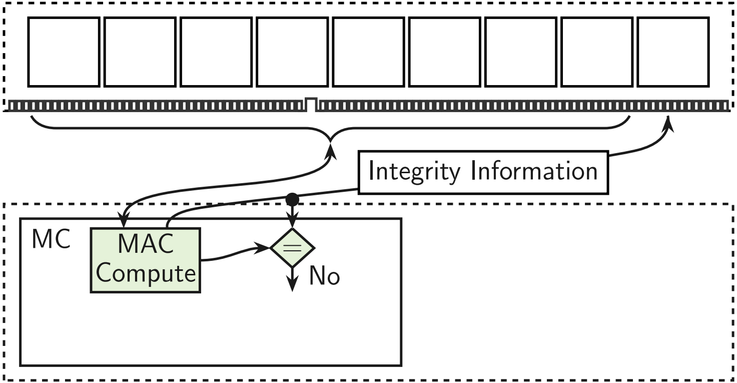

MC
MAC Compute

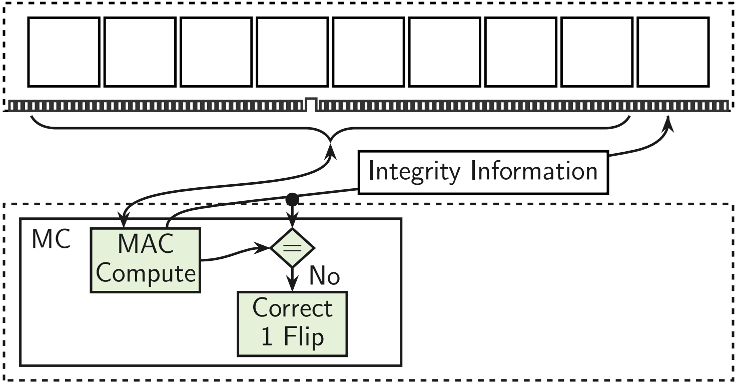

?
MC
MAC
Compute

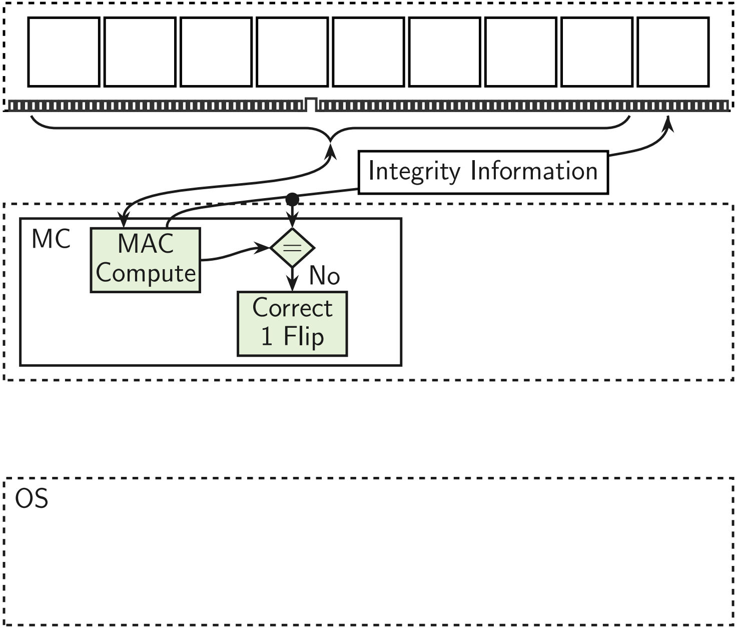

?
MC
MAC
Compute

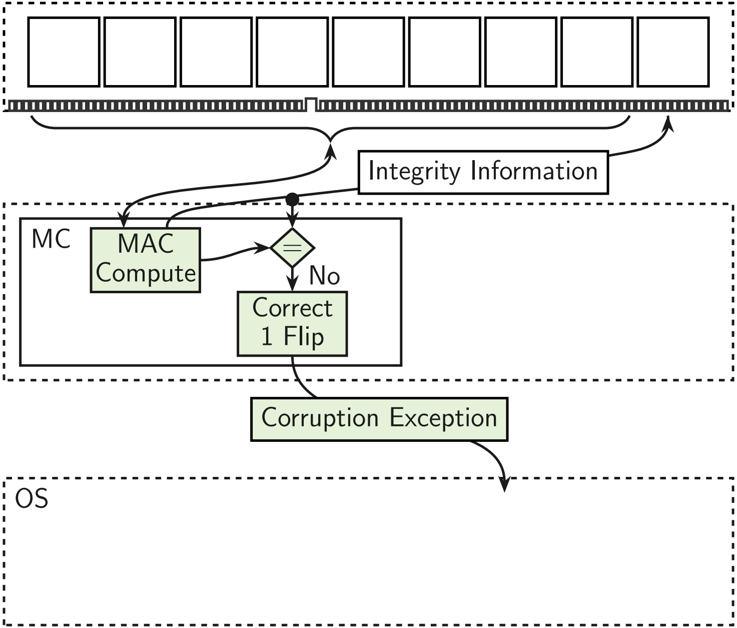

Integrity Information
MC
MAC
Compute

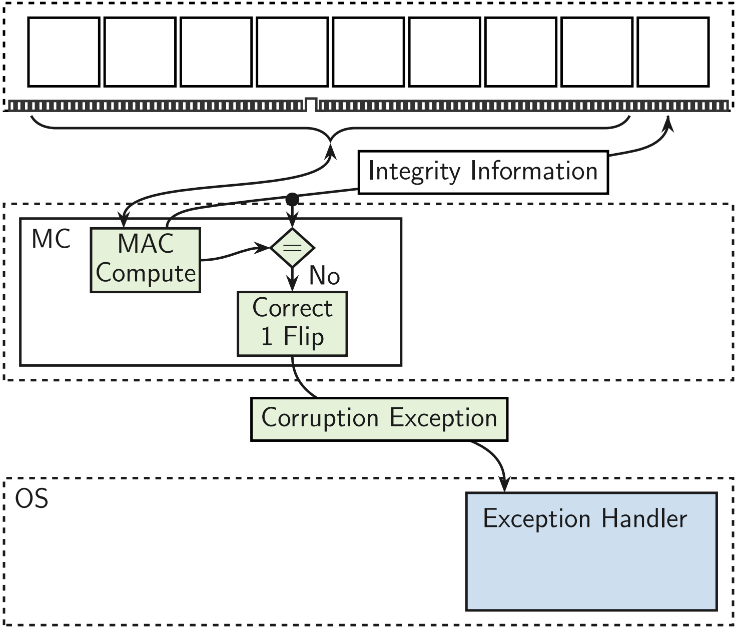

Integrity Information
MC
MAC
Compute
=

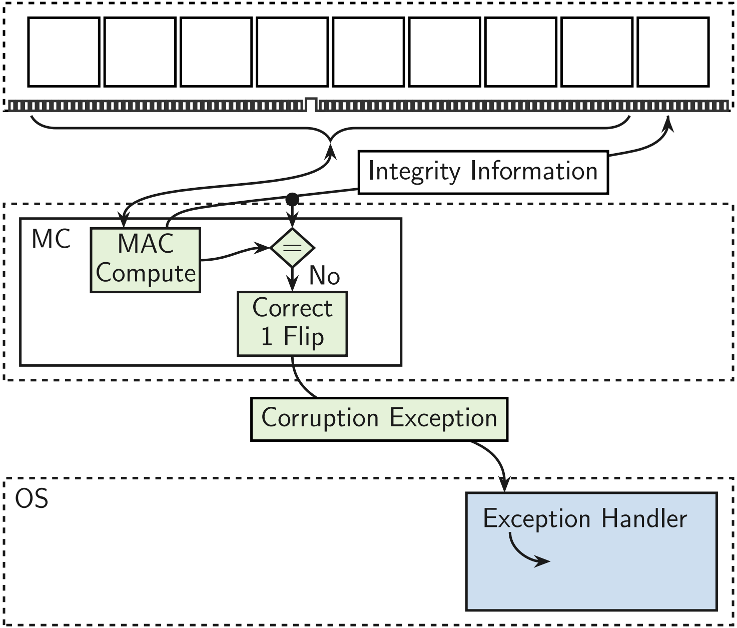

Integrity Information
MC
MAC
Compute
=
No

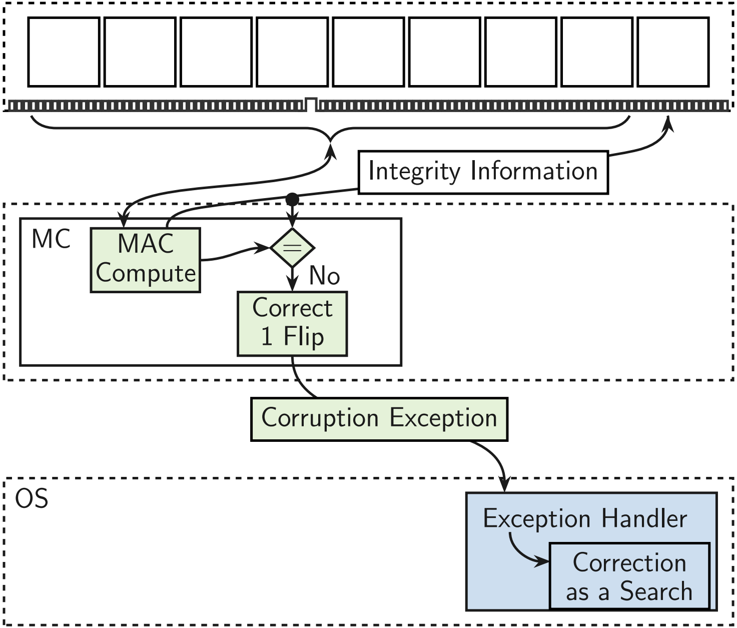

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip

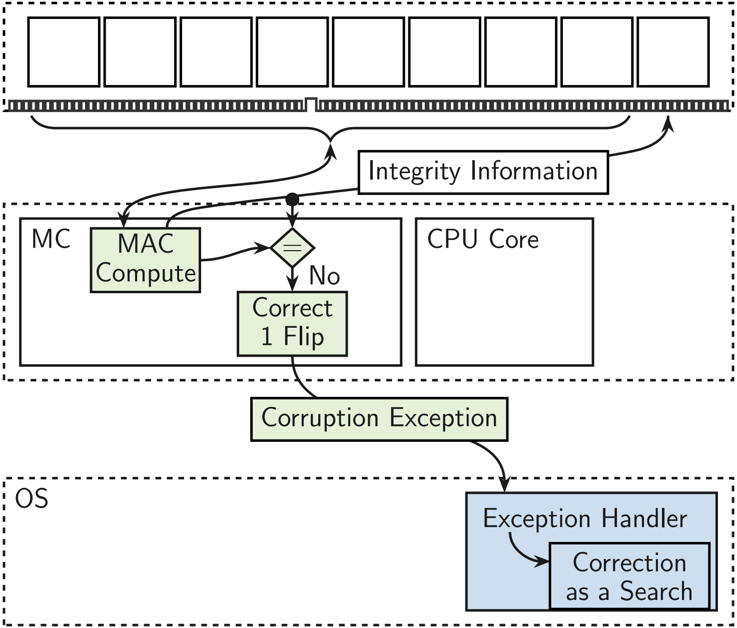

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
OS

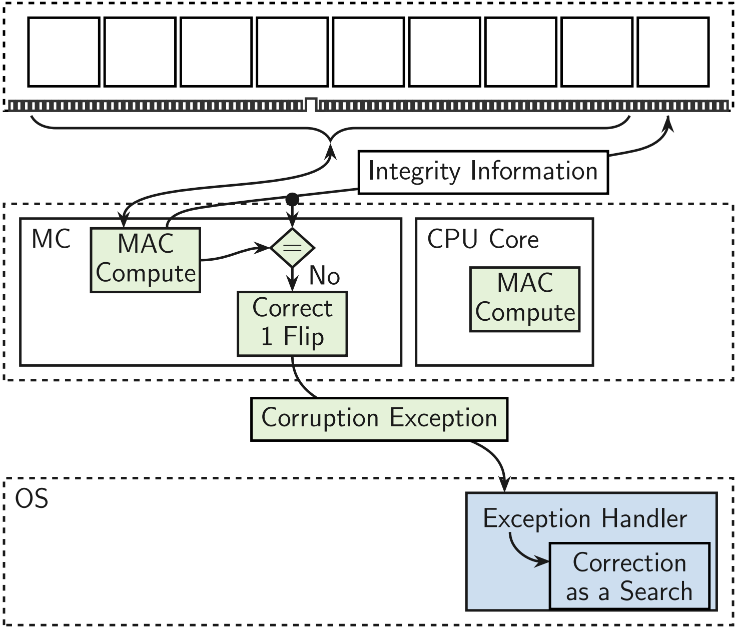

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
Corruption Exception
OS

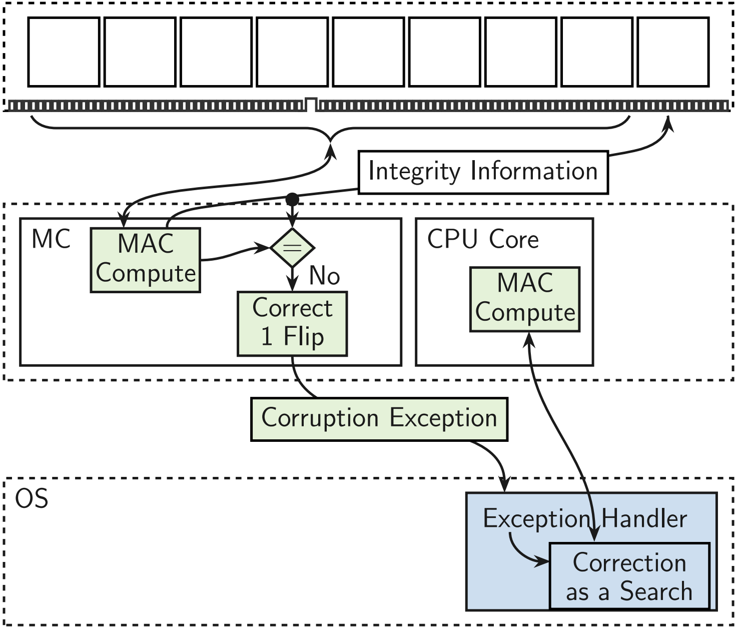

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
Corruption Exception
OS
Exception Handler

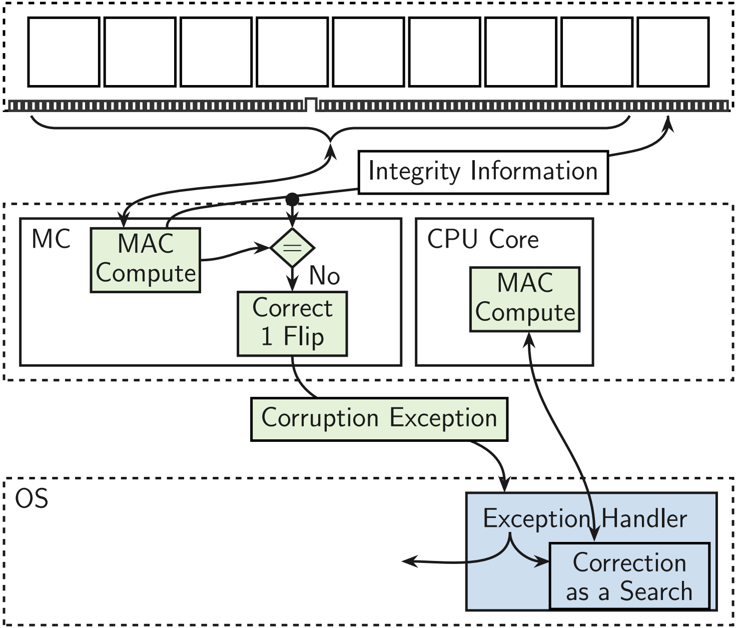

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
Corruption Exception
OS
Exception Handler

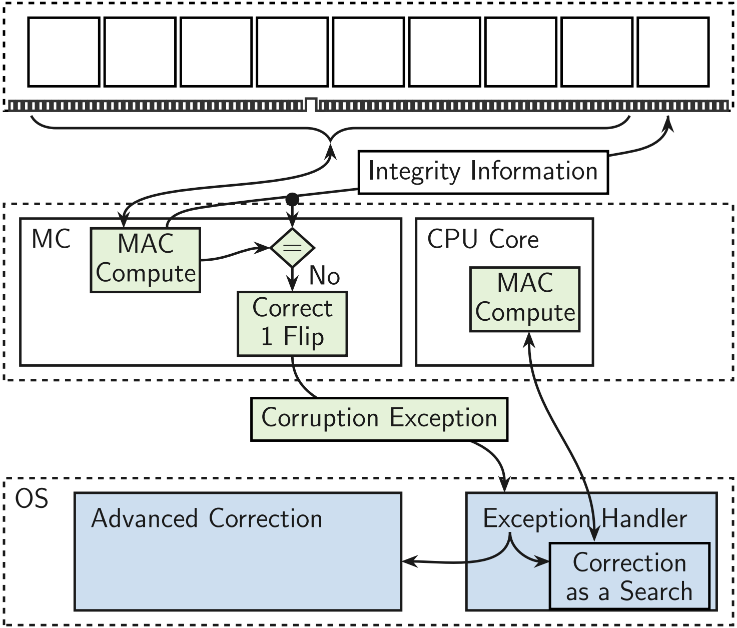

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
Corruption Exception
OS
Exception Handler
Correction as a Search

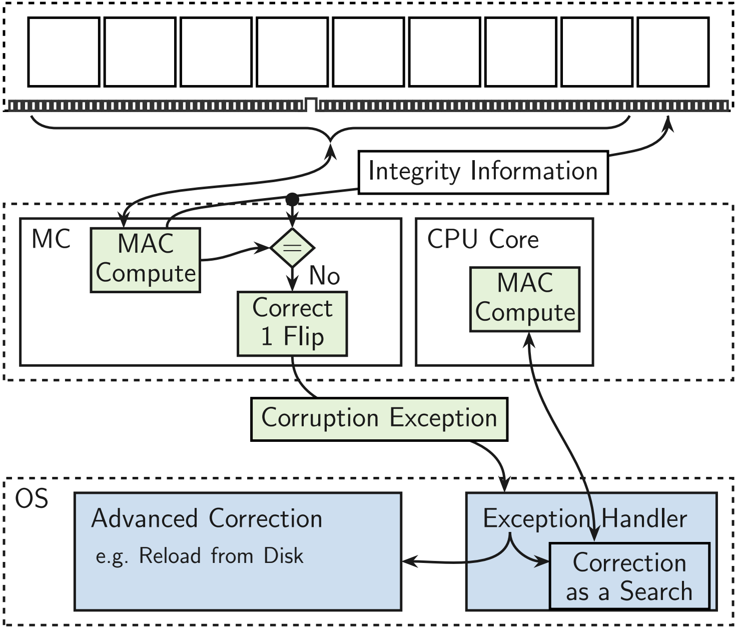

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
Corruption Exception
OS
Exception Handler
Correction as a Search

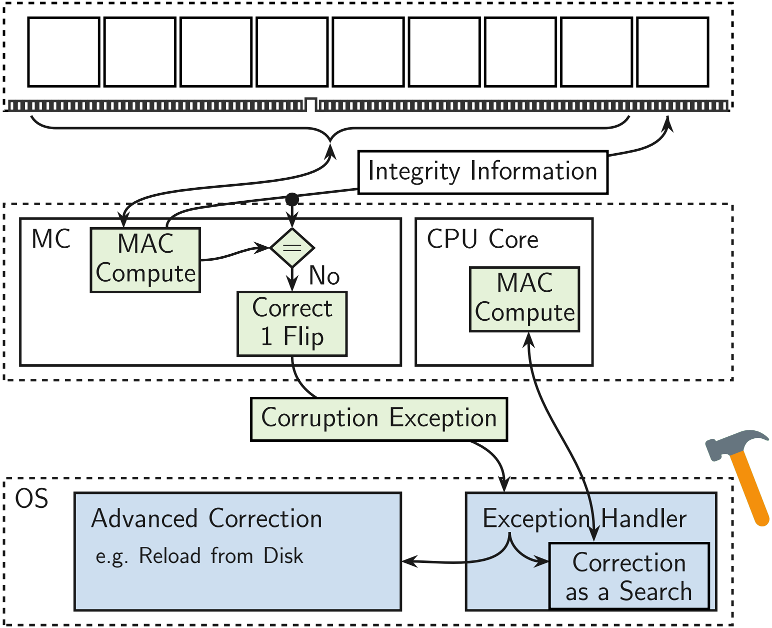

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Exception Handler
Correction as a Search

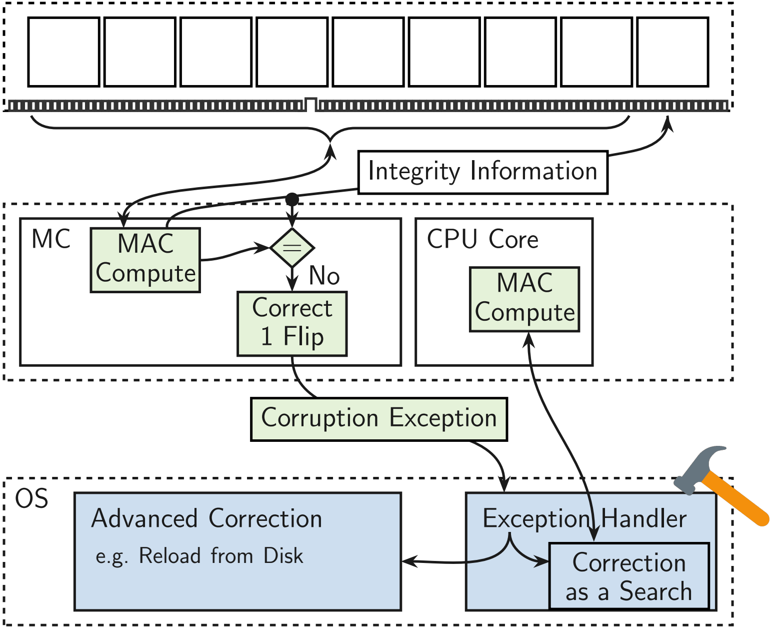

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Exception Handler
Correction as a Search

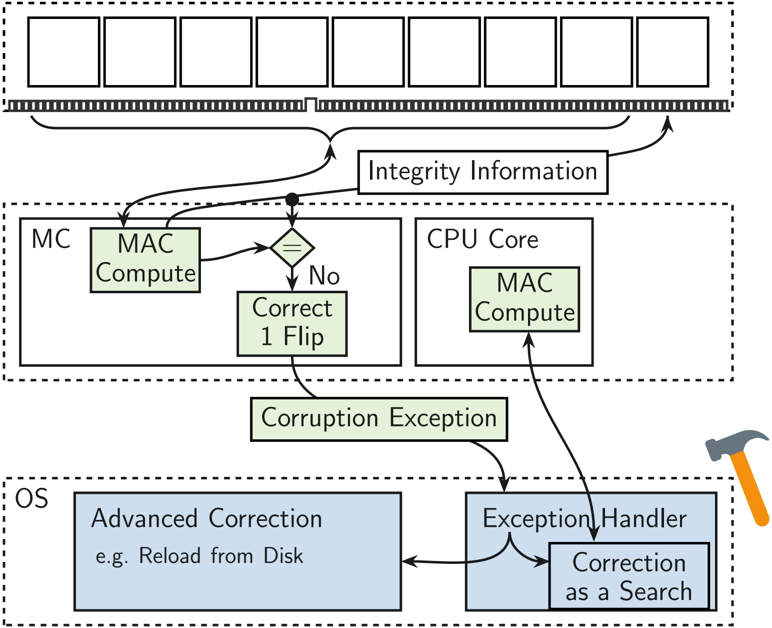

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Exception Handler
Correction as a Search

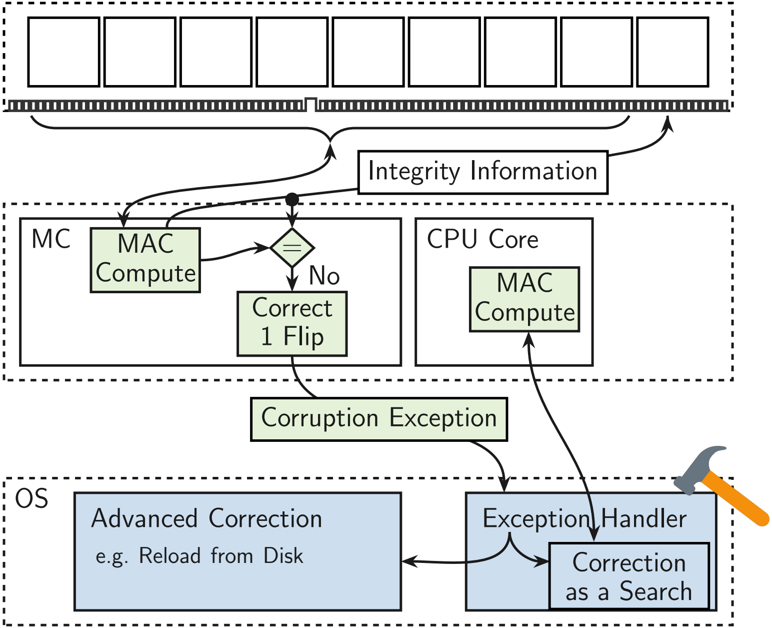

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
Exception Handler
Correction as a Search

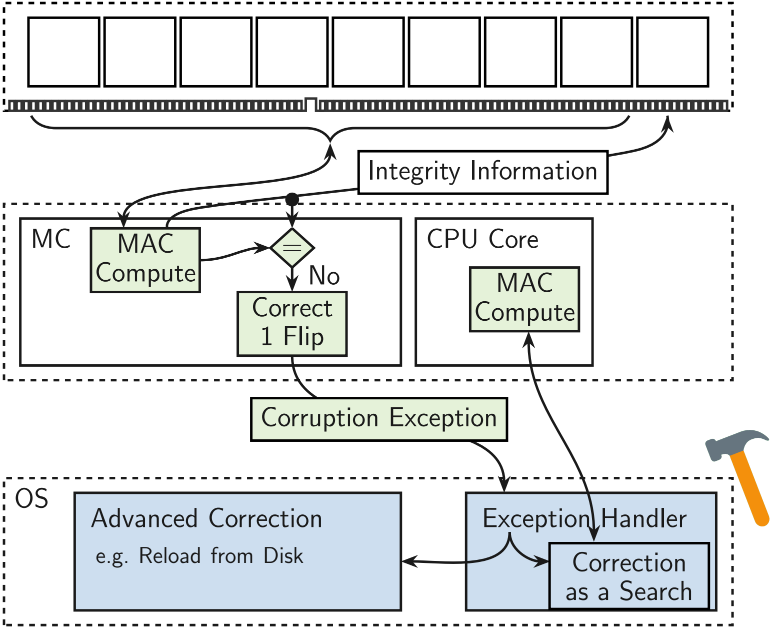

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

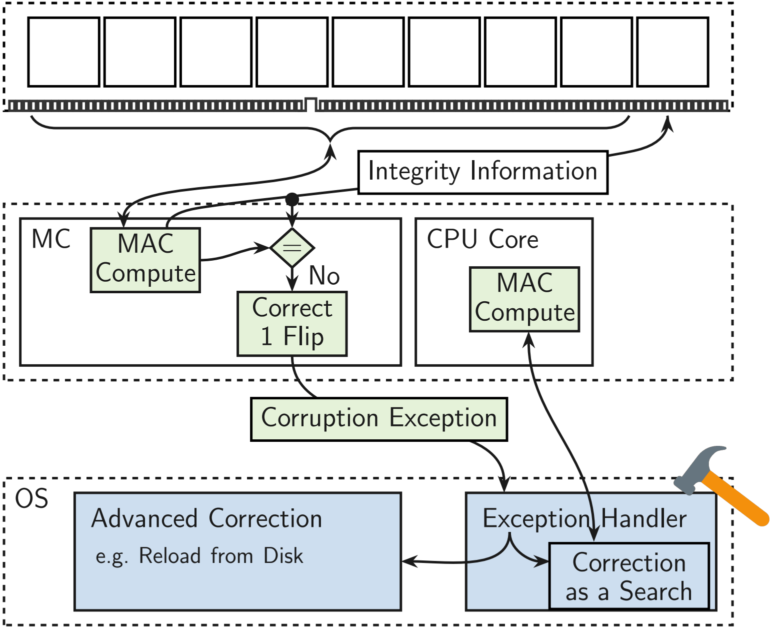

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

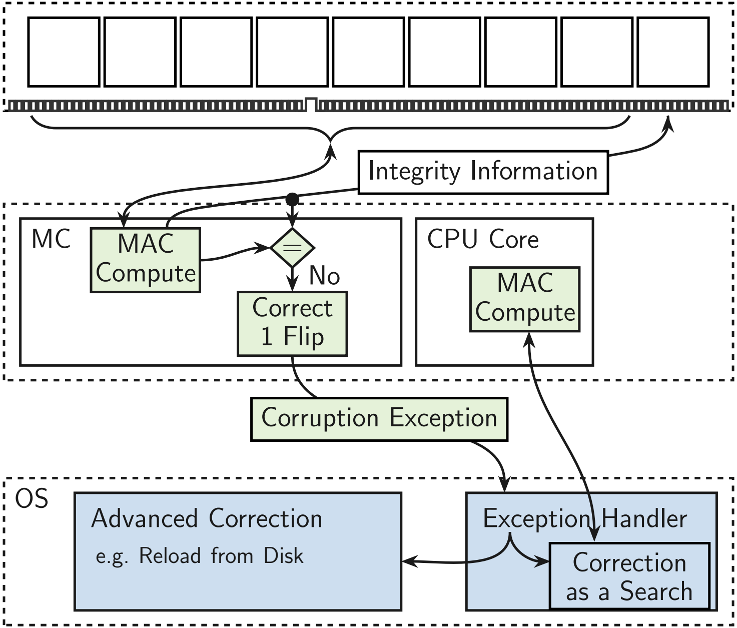

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

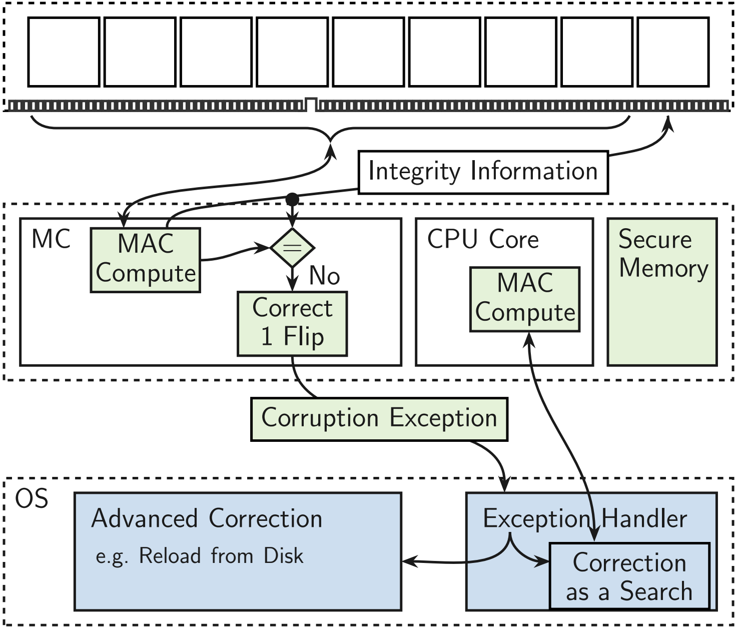

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

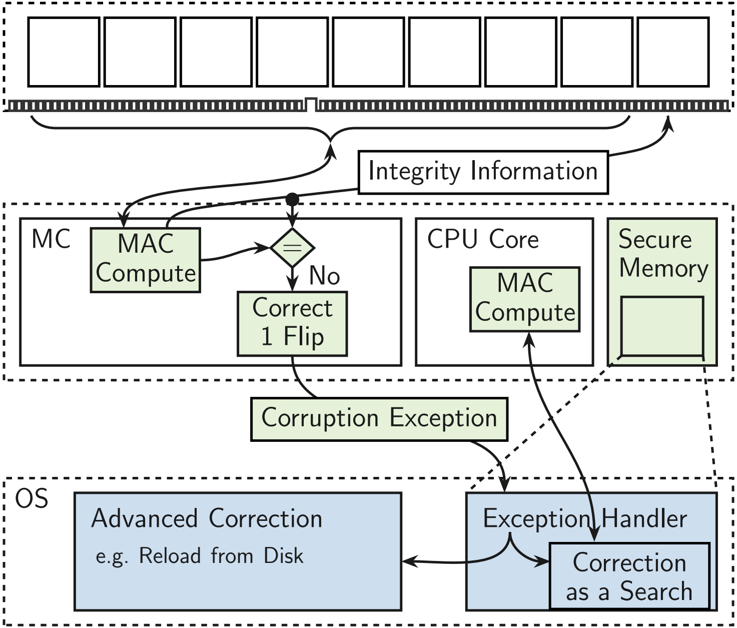

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search


Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

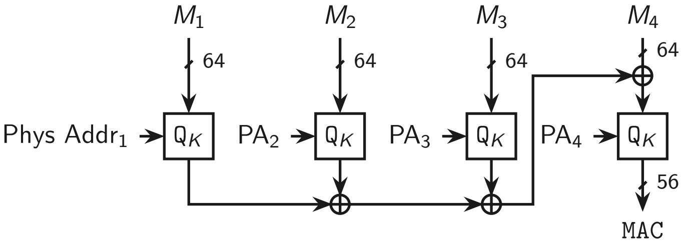

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search


Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

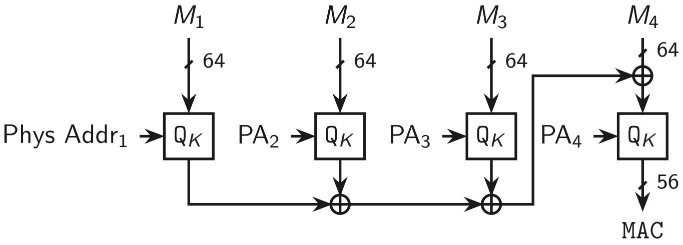

Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Secure Memory
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search


Integrity Information
MC
MAC Compute
=
No
Correct 1 Flip
CPU Core
MAC Compute
Secure Memory
Corruption Exception
OS
Advanced Correction
e.g. Reload from Disk
Exception Handler
Correction as a Search

CSI:Rowhammer – MAC Design

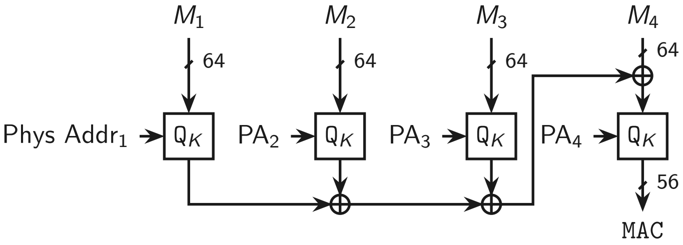


CSI:Rowhammer – MAC Design



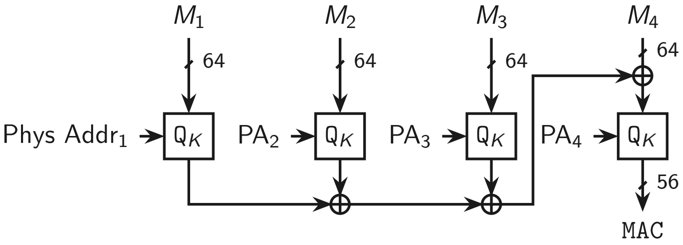
- PMAC construction

CSI:Rowhammer – MAC Design



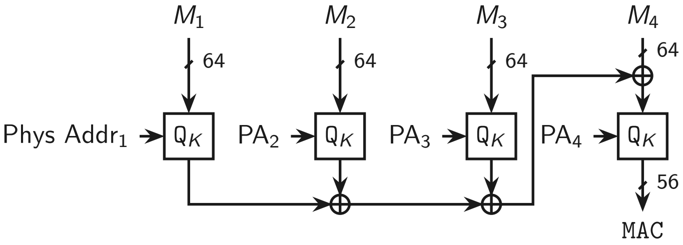
- PMAC construction
- QARMA$_5$-64-σ_0 block cipher [Ava17]

CSI:Rowhammer – MAC Design



- PMAC construction
- QARMA$_5$-64-σ_0 block cipher [Ava17]
- Physical address as tag

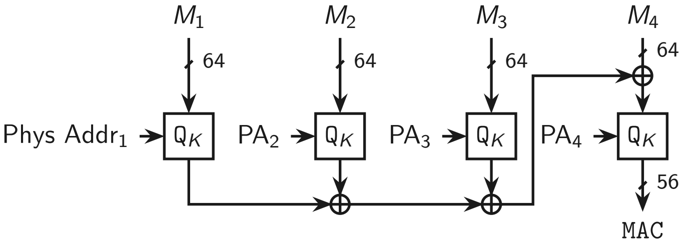
CSI:Rowhammer – MAC Design



- PMAC construction
- QARMA_5-64-σ_0 block cipher [Ava17]
- Physical address as tag

- 5.13 ns 256-bit

CSI:Rowhammer – MAC Design



- PMAC construction
- QARMA$_5$-64-σ_0 block cipher [Ava17]
- Physical address as tag
- 5.13 ns 256-bit
- 6.60 ns 512-bit

Data Correction

CSI:Rowhammer – Correction as a Search

- MACs **cannot** correct bit flips

CSI:Rowhammer – Correction as a Search

- MACs **cannot** correct bit flips
- Brute force search with **approximate equality**

CSI:Rowhammer – Correction as a Search

- MACs **cannot** correct bit flips
- Brute force search with **approximate equality**

$$0010110100101101 \xrightarrow{\text{MAC}} 01011010$$

CSI:Rowhammer – Correction as a Search

- MACs **cannot** correct bit flips
- Brute force search with **approximate equality**

$$0010110100101101 \xrightarrow{\text{MAC}} 01011010$$

$$\texttt{MAC from DRAM} \longrightarrow 01010010 \ \checkmark$$

CSI:Rowhammer – Correction as a Search

- MACs **cannot** correct bit flips
- Brute force search with **approximate equality**

$$\texttt{0010110100101101} \xrightarrow{\text{MAC}} \texttt{01011010}$$

$$\texttt{MAC from DRAM} \longrightarrow \texttt{01010010} \checkmark$$

CSI:Rowhammer – Correction as a Search

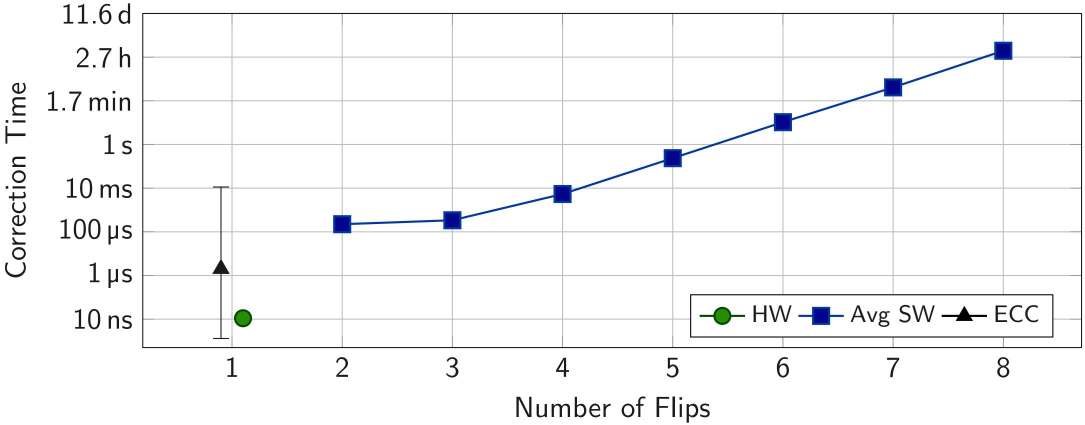
- MACs **cannot** correct bit flips
- Brute force search with **approximate equality**

$$\texttt{0010110100101101} \xrightarrow{\text{MAC}} \texttt{01011010}$$

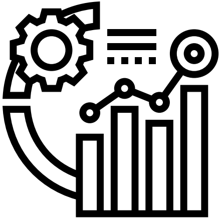
$$\texttt{MAC from DRAM} \longrightarrow \texttt{01010010} \checkmark$$

- Parity bits to shrink search space

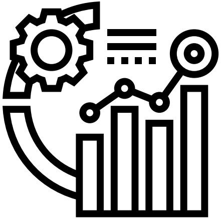
CSI:Rowhammer – Correction Time



CSI:Rowhammer – Advanced Error Correction

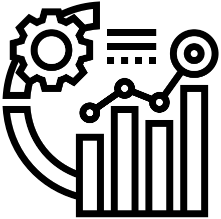


CSI:Rowhammer – Advanced Error Correction



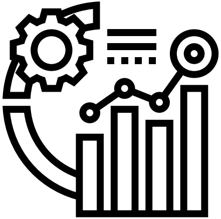
- OS has some **knowledge** about the corrupted data

CSI:Rowhammer – Advanced Error Correction



- OS has some **knowledge** about the corrupted data
- Reload disk backed data instead of correcting

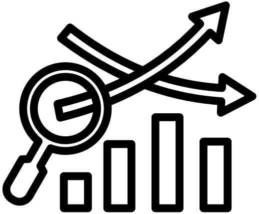
CSI:Rowhammer – Advanced Error Correction



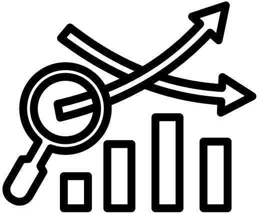
- OS has some **knowledge** about the corrupted data
- Reload disk backed data instead of correcting
- Recompute data (page tables)

Evaluation

CSI:Rowhammer – Evaluation

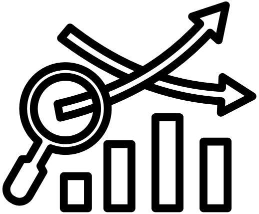


CSI:Rowhammer – Evaluation



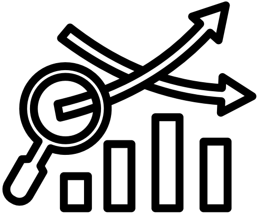
- Implemented CSI:Rowhammer in **gem5**

CSI:Rowhammer – Evaluation



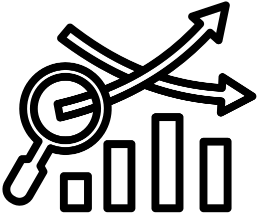
- Implemented CSI:Rowhammer in **gem5**
- Modified **Linux** kernel

CSI:Rowhammer – Evaluation



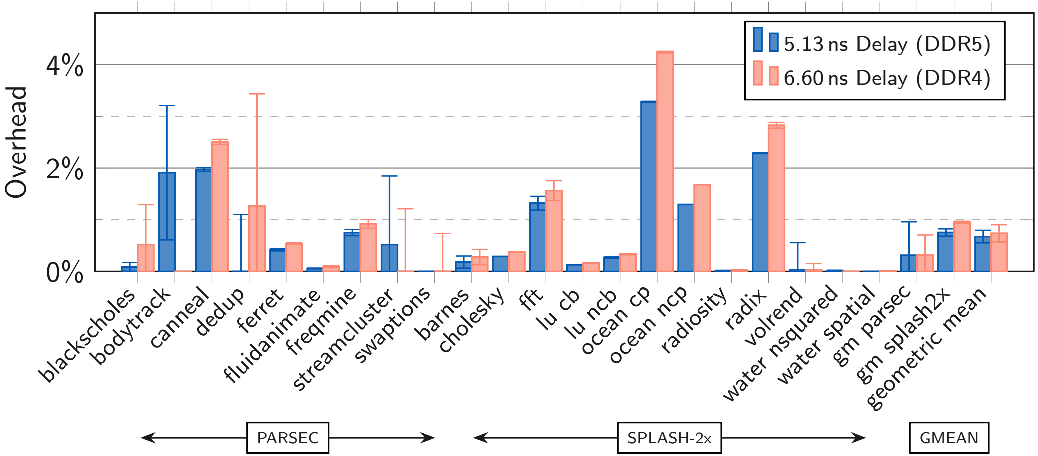
- Implemented CSI:Rowhammer in **gem5**
- Modified **Linux** kernel
- Evaluated correct functionality

CSI:Rowhammer – Evaluation



- Implemented CSI:Rowhammer in **gem5**
- Modified **Linux** kernel
- Evaluated correct functionality
- Evaluated performance overhead

CSI:Rowhammer – Performance Overhead



CSI:Rowhammer – Security Evaluation

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**
- Rowhammer can induce bit flips in MAC

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**
- Rowhammer can induce bit flips in MAC
- Decreases MAC strength from initial 56 bit

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**
- Rowhammer can induce bit flips in MAC
- Decreases MAC strength from initial 56 bit

Data Flips	$\log_2(\#$ Correction Tries$)$	Ignored Flips	MAC Strength
5	26.0	3	41.2
6	31.5	2	45.4
7	38.8	1	50.2
8	42.4	0	56.0

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**

Data Flips	$\log_2(\#$ Correction Tries$)$	Ignored Flips	MAC Strength
5	26.0	3	41.2
6	31.5	2	45.4
7	38.8	1	50.2
8	42.4	0	56.0

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**
- Silent Data Corruption rate less than once per 10^9 billion years.

Data Flips	$\log_2$(# Correction Tries)	Ignored Flips	MAC Strength
5	26.0	3	41.2
6	31.5	2	45.4
7	38.8	1	50.2
8	42.4	0	56.0

CSI:Rowhammer – Security Evaluation

- **Approximate Equality**
- Silent Data Corruption rate less than once per 10^9 billion years.
- Rowhammer second preimage after one year: $9.75 \cdot 10^{-5}\,\%$

Data Flips	$\log_2(\#$ Correction Tries$)$	Ignored Flips	MAC Strength
5	26.0	3	41.2
6	31.5	2	45.4
7	38.8	1	50.2
8	42.4	0	56.0

Read the Paper:

Read the Paper:

- Corruption exception **nesting detection**

Read the Paper:

- Corruption exception nesting detection
- **Virtualization** with or without guest support

Read the Paper:

- Corruption exception nesting detection
- **Virtualization** with or without guest support
- Many more interesting **implementation details**

Read the Paper:

- Corruption exception nesting detection
- **Virtualization** with or without guest support
- Many more interesting **implementation details**
- Detailed security evaluation

CSI:Rowhammer

Cryptographic Security and Integrity against Rowhammer

Jonas Juffinger, Lukas Lamster, Andreas Kogler, Moritz Lipp, Maria Eichlseder, Daniel Gruss

2023-05-23

IEEE Symposium on Security and Privacy 2023

✉ jonas.juffinger@iaik.tugraz.at 🐦 @notimaginary_ 🌐 www.jonasjuffinger.com

PoC: github.com/CSIRowhammer/CSIRowhammerPoC

References i

[Ava17] Roberto Avanzi. The QARMA Block Cipher Family: Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes. In: IACR Transactions on Symmetric Cryptology 2017.1 (2017), pp. 4–44.

[Gru+18] Daniel Gruss et al. Another Flip in the Wall of Rowhammer Defenses. In: S&P. 2018.

[Kim+14] Yoongu Kim et al. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. In: ACM SIGARCH Computer Architecture News 42.3 (2014), pp. 361–372.

[Kog+22] Andreas Kogler et al. Half-Double: Hammering From the Next Row Over. In: USENIX Security Symposium. 2022.