FP-RowHammer: DRAM-Based Device Fingerprinting

Hari Venugopalan, **Kaustav Goswami**, Zainul Abi Din, Jason Lowe-Power, Samuel T. King and Zubair Shafiq

UC DAVIS
UNIVERSITY OF CALIFORNIA

Background

Fingerprinting

"*A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification.*"

From Wikipedia

Stateful identifiers

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)

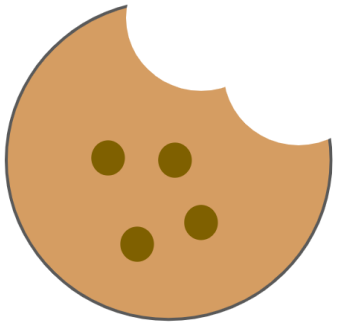
Background

Fingerprinting

"*A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification.*"

From Wikipedia

Stateful identifiers



HTTP Cookie

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)

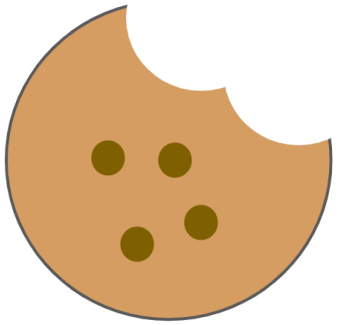
Background

Fingerprinting

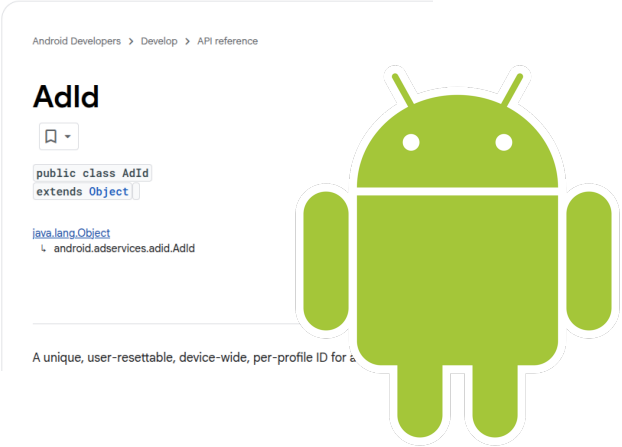
"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateful identifiers



HTTP Cookie



[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)

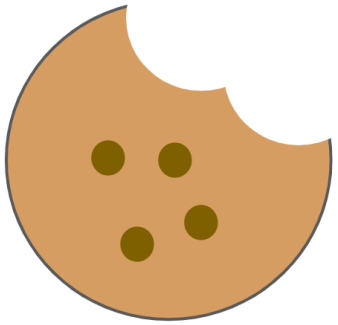
Background

Fingerprinting

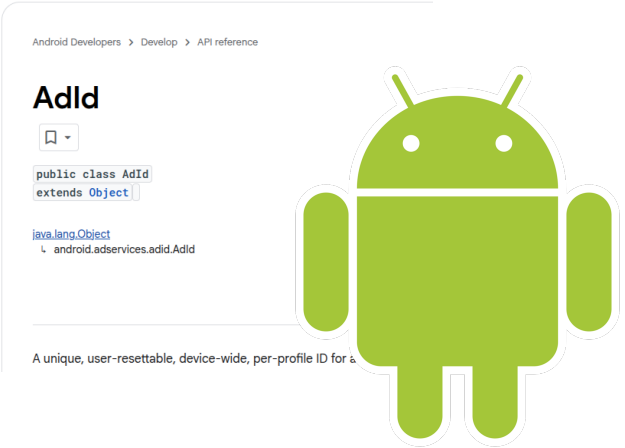
"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateful identifiers



HTTP Cookie



[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)

Background

Fingerprinting

"*A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification.*"

From Wikipedia

Stateless identifiers

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)

Background

Fingerprinting

"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateless identifiers

Fingerprint

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)
[2] https://fingerprint.com/

Background

Fingerprinting

"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateless identifiers

Fingerprint

DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting

Tomer Laor* Ben-Gurion Univ. of the Negev tomerlao@post.bgu.ac.il
Naif Mehanna* Univ. Lille, CNRS, Inria naif.mehanna@univ-lille.fr
Antonin Durey Univ. Lille, CNRS, Inria antonin.durey@univ-lille.fr
Vitaly Dyadyuk Ben-Gurion Univ. of the Negev vitalyd@post.bgu.ac.il
Pierre Laperdrix Univ. Lille, CNRS, Inria pierre.laperdrix@univ-lille.fr
Clémentine Maurice Univ. Lille, CNRS, Inria clementine.maurice@inria.fr
Yossi Oren Ben-Gurion Univ. of the Negev yos@bgu.ac.il
Romain Rouvoy Univ. Lille, CNRS, Inria / IUF romain.rouvoy@univ-lille.fr
Walter Rudametkin Univ. Lille, CNRS, Inria walter.rudametkin@univ-lille.fr
Yuval Yarom Univ. of Adelaide yval@cs.adelaide.edu.au

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)
[2] https://fingerprint.com/
[3] Laor *et al*. DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting, NDSS 2022

Background

Fingerprinting

"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateless identifiers

Fingerprint

DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting

Tomer Laor* Ben-Gurion Univ. of the Negev tomerlao@post.bgu.ac.il
Naif Mehanna* Univ. Lille, CNRS, Inria naif.mehanna@univ-lille.fr
Antonin Durey Univ. Lille, CNRS, Inria antonin.durey@univ-lille.fr
Vitaly Dyadyuk Ben-Gurion Univ. of the Negev vitalyd@post.bgu.ac.il
Pierre Laperdrix Univ. Lille, CNRS, Inria pierre.laperdrix@univ-lille.fr
Clémentine Maurice Univ. Lille, CNRS, Inria clementine.maurice@inria.fr
Yossi Oren Ben-Gurion Univ. of the Negev yos@bgu.ac.il
Romain Rouvoy Univ. Lille, CNRS, Inria / IUF romain.rouvoy@univ-lille.fr
Walter Rudametkin Univ. Lille, CNRS, Inria walter.rudametkin@univ-lille.fr
Yuval Yarom Univ. of Adelaide yval@cs.adelaide.edu.au

DeMiCPU: Device Fingerprinting with Magnetic Signals Radiated by CPU

Yushi Cheng Zhejiang University yushicheng@zju.edu.cn
Xiaoyu Ji* Zhejiang University xji@zju.edu.cn
Juchuan Zhang Zhejiang University juchuanzhang@zju.edu.cn
Wenyuan Xu Zhejiang University wyxu@zju.edu.cn
Yi-Chao Chen University of Texas at Austin yichao@utexas.edu

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)
[2] https://fingerprint.com/
[3] T. Laor *et al.* DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting, NDSS 2022
[4] Y. Cheng *et al.*, DeMiCPU: Devie Fingerprinting with Magnetic Signals Radiated by CPU, ACM CCS 2019

Background

Fingerprinting

"A device fingerprint or machine fingerprint is information collected about the software and hardware of a remote computing device for the purpose of identification."

From Wikipedia

Stateless identifiers

Fingerprint

DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting

Tomer Laor* Ben-Gurion Univ. of the Negev tomerlao@post.bgu.ac.il
Naif Mehanna* Univ. Lille, CNRS, Inria naif.mehanna@univ-lille.fr
Antonin Durey Univ. Lille, CNRS, Inria antonin.durey@univ-lille.fr
Vitaly Dyadyuk Ben-Gurion Univ. of the Negev vitalyd@post.bgu.ac.il
Pierre Laperdrix Univ. Lille, CNRS, Inria pierre.laperdrix@univ-lille.fr
Clémentine Maurice Univ. Lille, CNRS, Inria clementine.maurice@inria.fr
Yossi Oren Ben-Gurion Univ. of the Negev yos@bgu.ac.il
Romain Rouvoy Univ. Lille, CNRS, Inria / IUF romain.rouvoy@univ-lille.fr
Walter Rudametkin Univ. Lille, CNRS, Inria walter.rudametkin@univ-lille.fr
Yuval Yarom Univ. of Adelaide yval@cs.adelaide.edu.au

DeMiCPU: Device Fingerprinting with Magnetic Signals Radiated by CPU

Yushi Cheng Zhejiang University yushicheng@zju.edu.cn
Xiaoyu Ji* Zhejiang University xji@zju.edu.cn
Juchuan Zhang Zhejiang University juchuanzhang@zju.edu.cn
Wenyuan Xu Zhejiang University wyxu@zju.edu.cn
Yi-Chao Chen University of Texas at Austin yichao@utexas.edu

Clock Around the Clock: Time-Based Device Fingerprinting

Iskander Sanchez-Rola Deustotech, University of Deusto iskander.sanchez@deusto.es
Igor Santos Deustotech, University of Deusto isantos@deusto.es
Davide Balzarotti Eurecom davide.balzarotti@eurecom.fr

[1] https://en.wikipedia.org/wiki/Fingerprint_(computing)
[2] https://fingerprint.com/
[3] T. Laor *et al.* DRAWNAPART: A Device Identification Technique based on Remote GPU Fingerprinting, NDSS 2022
[4] Y. Cheng *et al.*, DeMiCPU: Devie Fingerprinting with Magnetic Signals Radiated by CPU, ACM CCS 2019
[5] I. Sanchez-Rola *et al.*, clock Around the clock: Time-Based Device Fingerprinting, ACM CCS 2018

What is a good fingerprint?

Uniqueness

What is a good fingerprint?

Uniqueness: Different users must have different IDs

001	002	003

What is a good fingerprint?

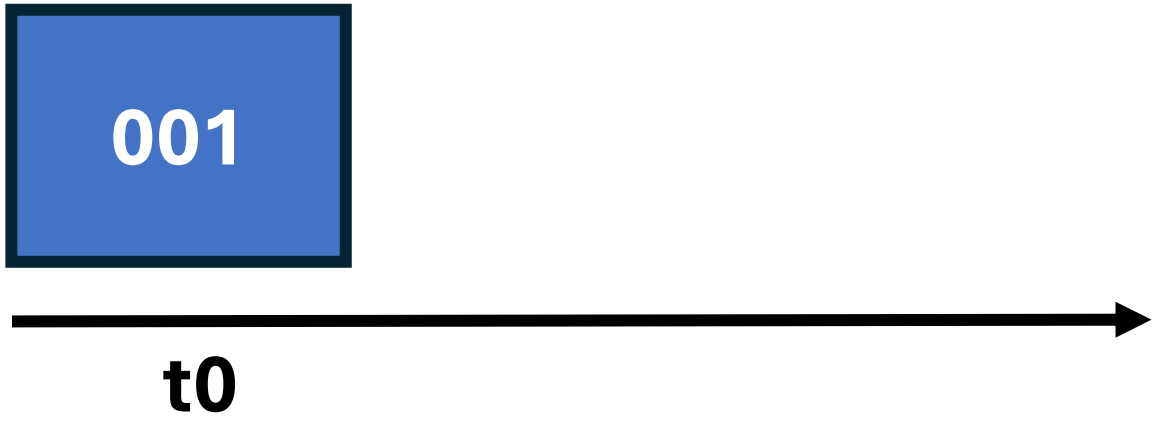
Uniqueness: Different users must have different IDs

Stable

What is a good fingerprint?

Uniqueness

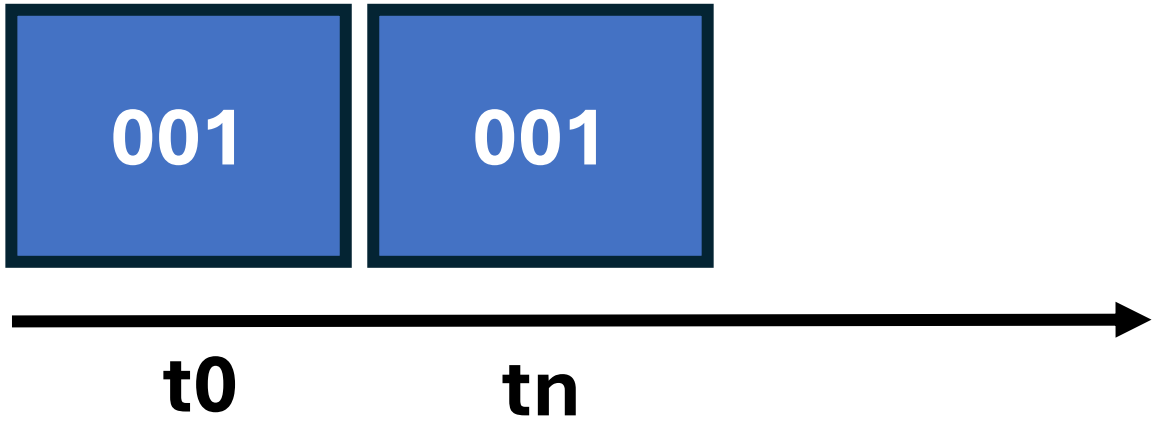
Stable: The fingerprint of a device should never change.



What is a good fingerprint?

Uniqueness

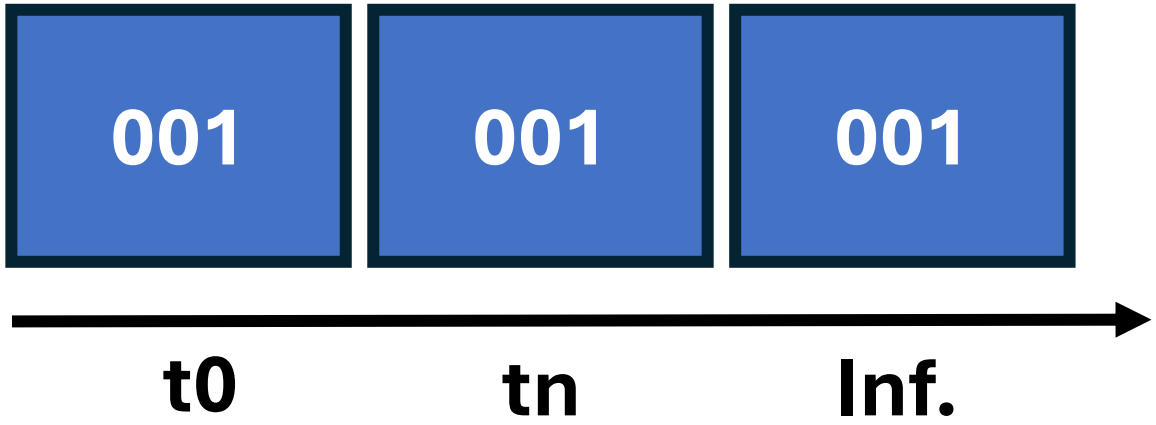
Stable: The fingerprint of a device should never change.



What is a good fingerprint?

Uniqueness

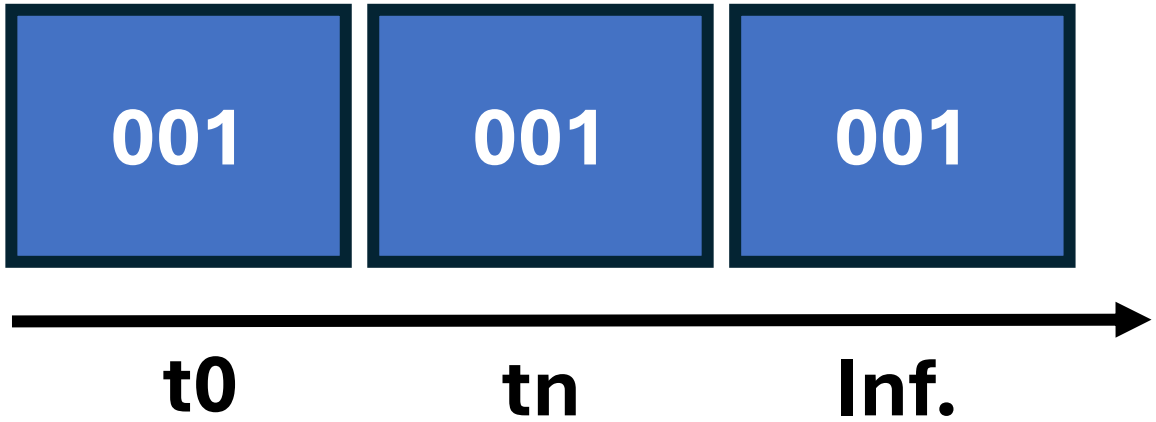
Stable: The fingerprint of a device should never change.



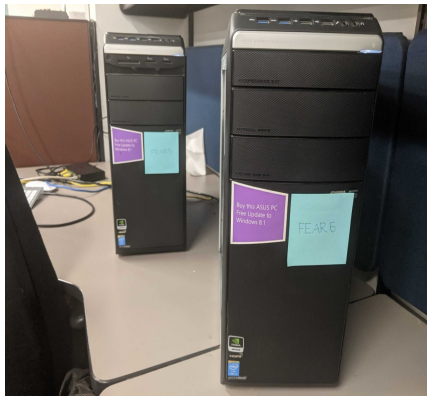
What is a good fingerprint?

Uniqueness

Stable



Test: Homogeneous Devices

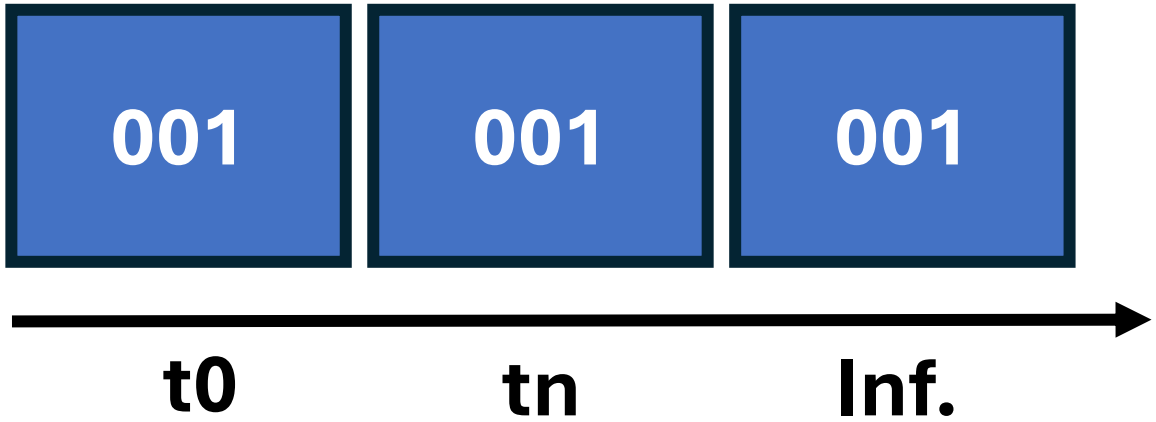


Fingerprint

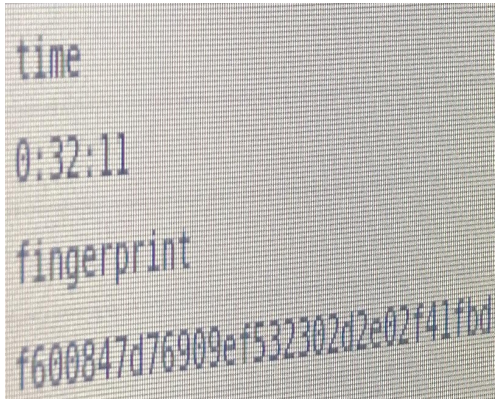
What is a good fingerprint?

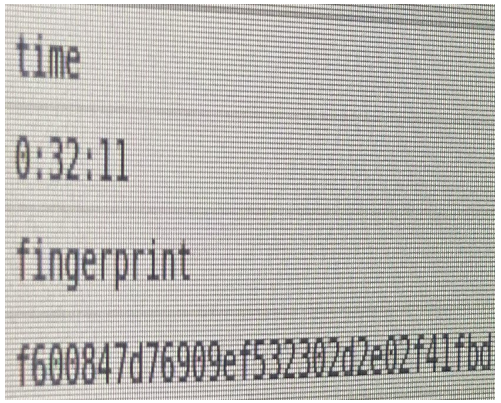
Uniqueness

Stable



Test: Homogeneous Devices

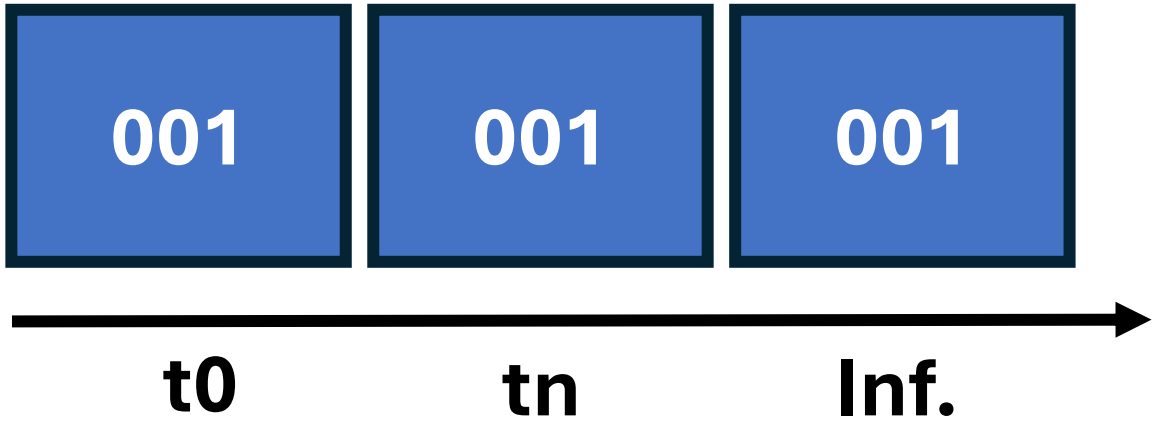




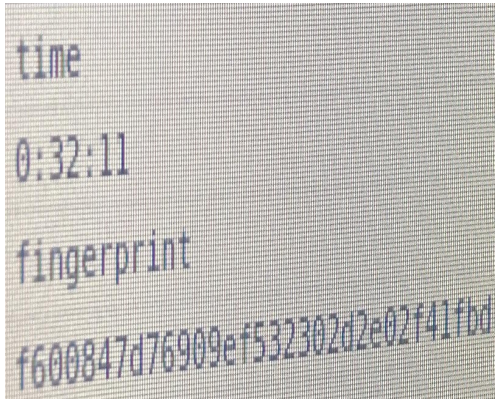
What is a good fingerprint?

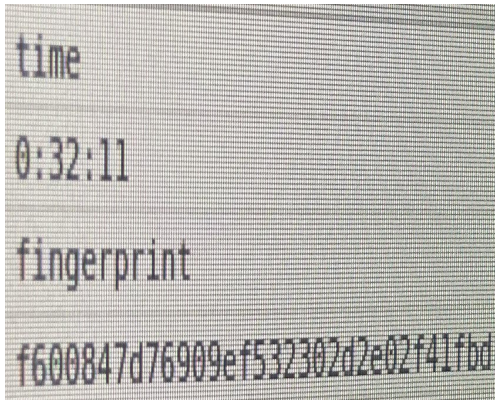
Uniqueness

Stable



Test: Homogeneous Devices





Visitor identifier:
783bb985d9842721b9b5ffee2f537616

Visitor identifier:
b3e10f441fcf3d0ba2d92b19ab6f64ea

Enter FP-RowHammer

Double **D**ata **R**ate **4** **D**ual
In-Line **M**emory **M**odule

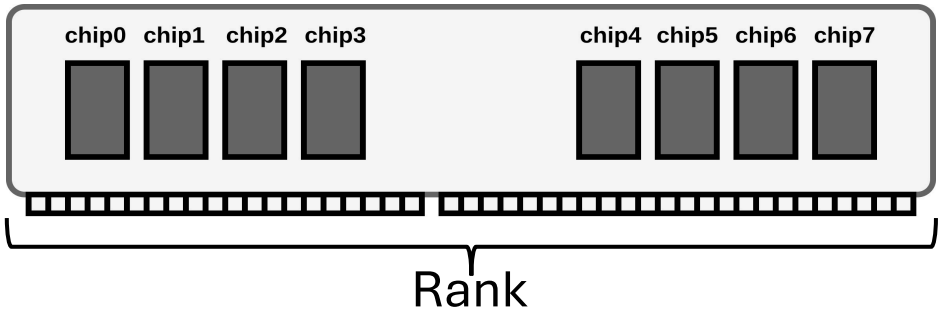
Enter FP-RowHammer

Double **D**ata **R**ate **4** **D**ual
In-Line **M**emory **M**odule

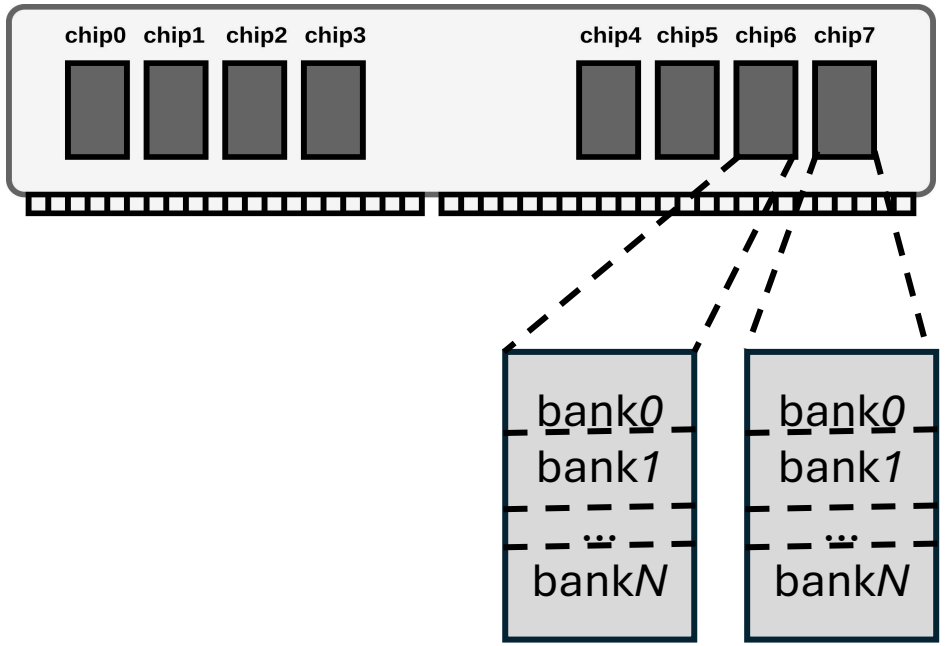
Enter FP-RowHammer

DDR4 DIMM

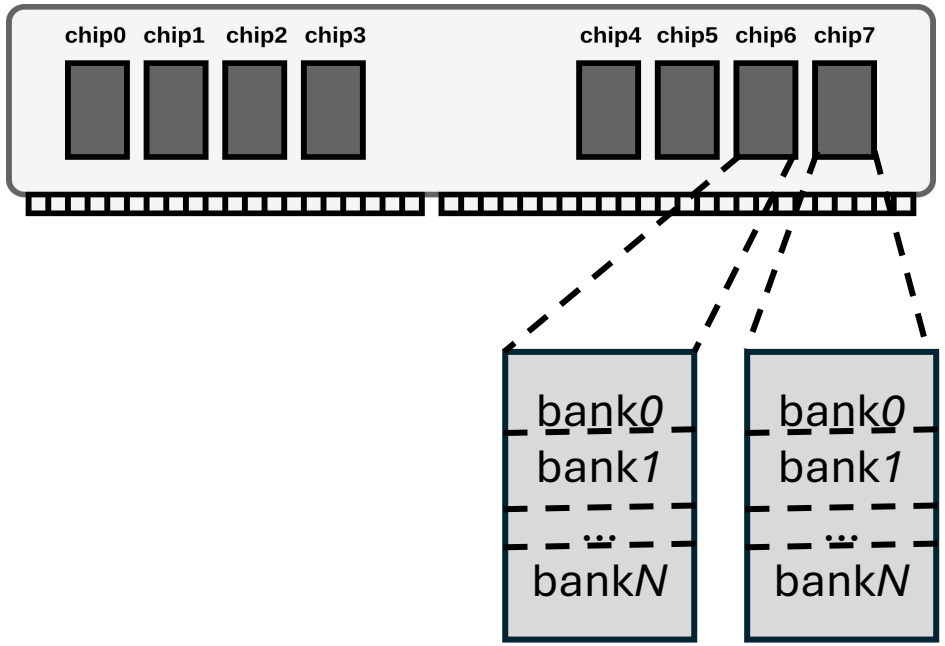
Enter FP-RowHammer



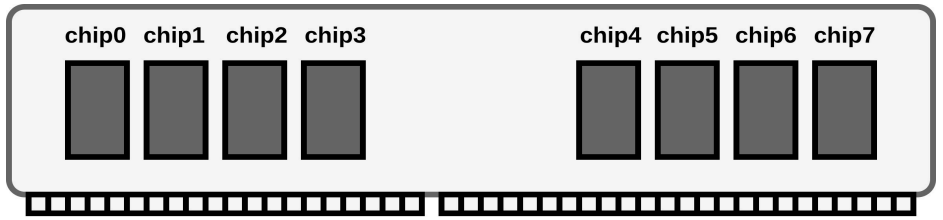
Enter FP-RowHammer



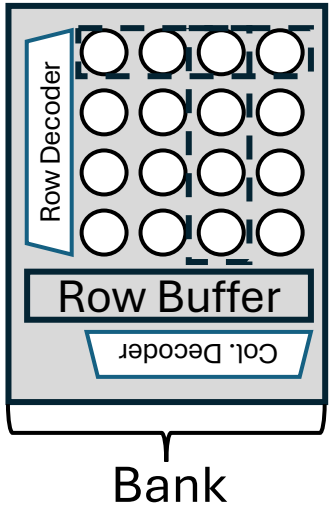
Enter FP-RowHammer



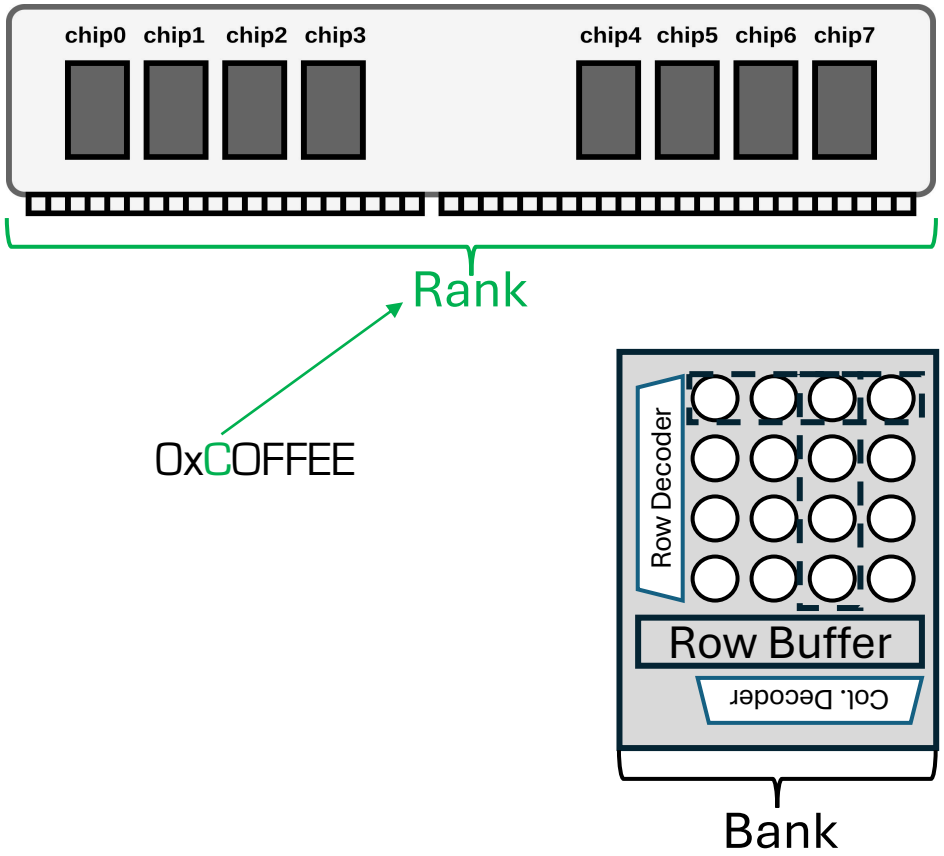
Enter FP-RowHammer



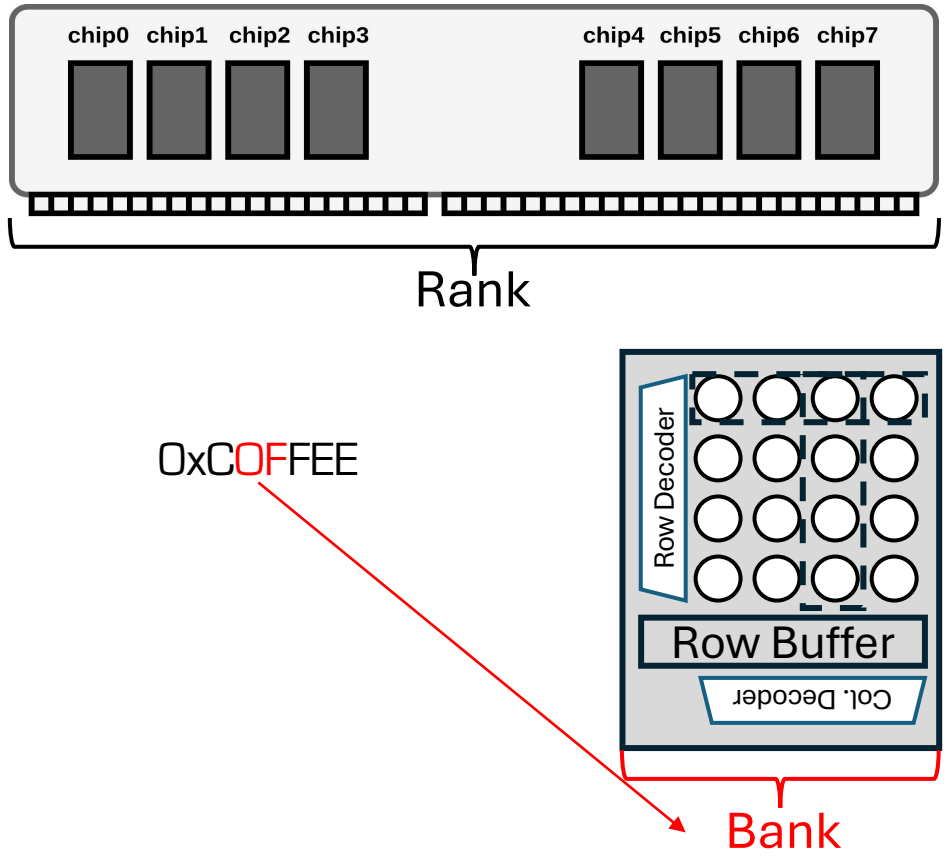
0xCOFFEE



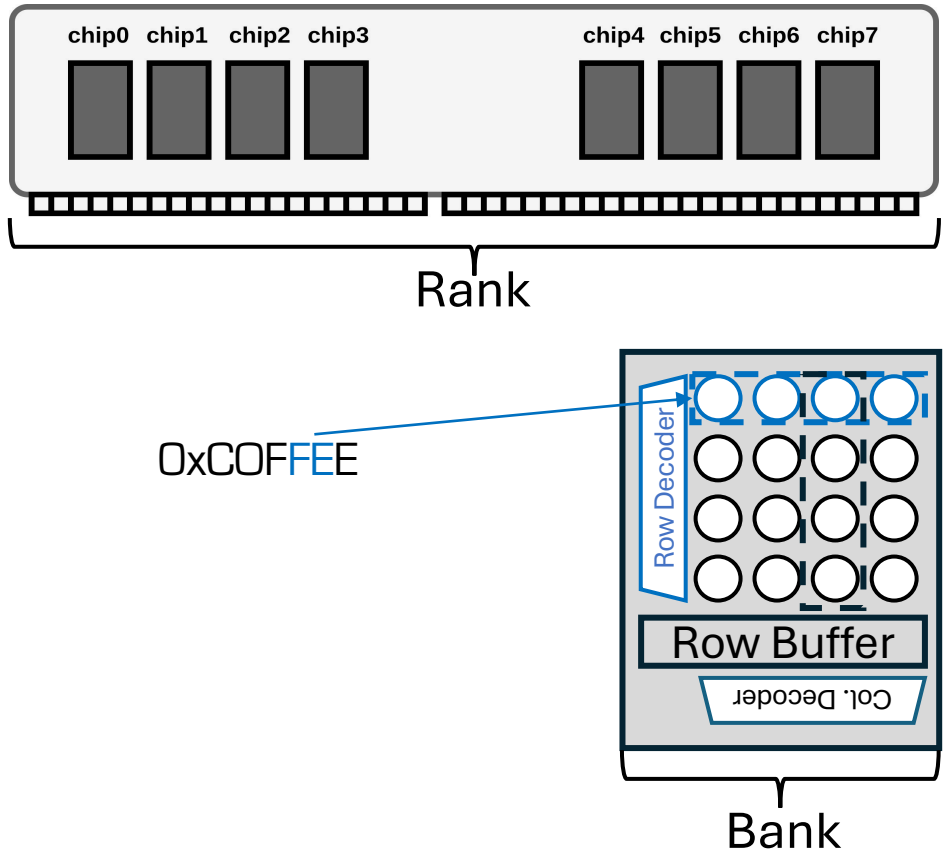
Enter FP-RowHammer



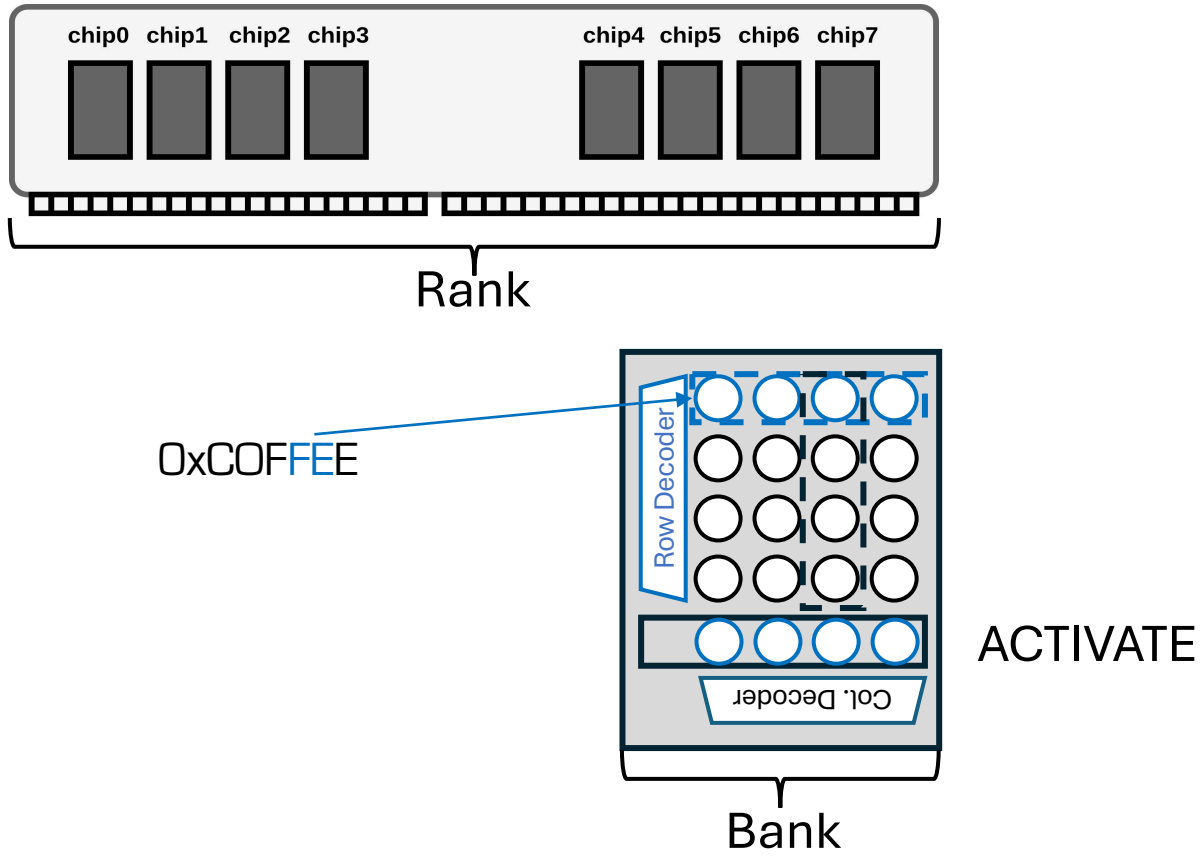
Enter FP-RowHammer



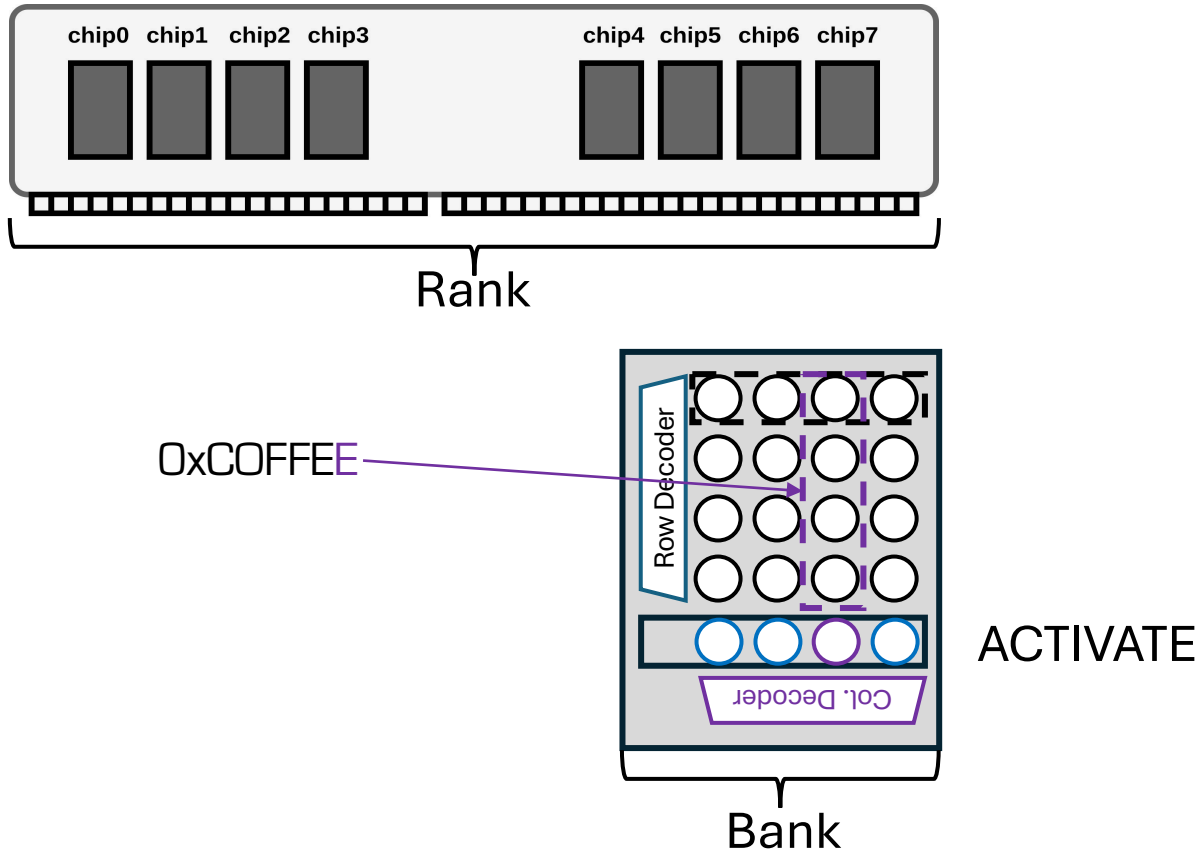
Enter FP-RowHammer



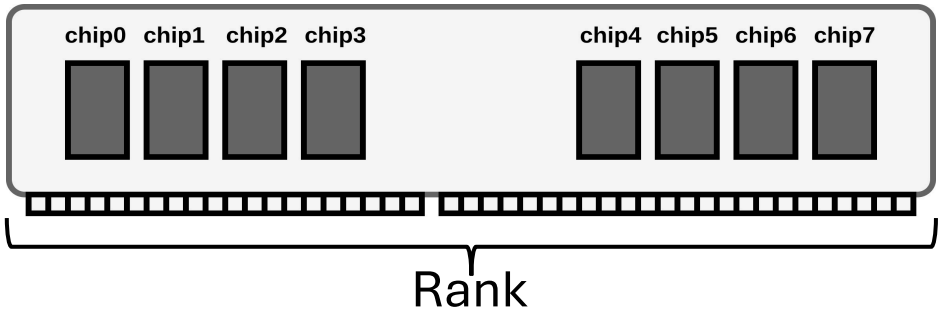
Enter FP-RowHammer



Enter FP-RowHammer

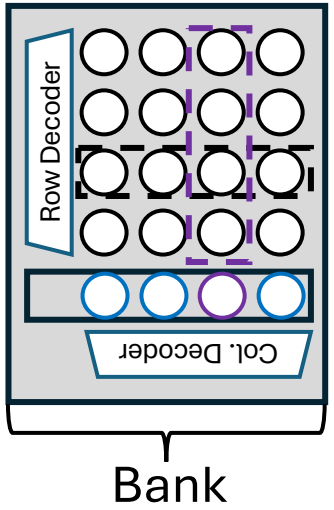


Enter FP-RowHammer



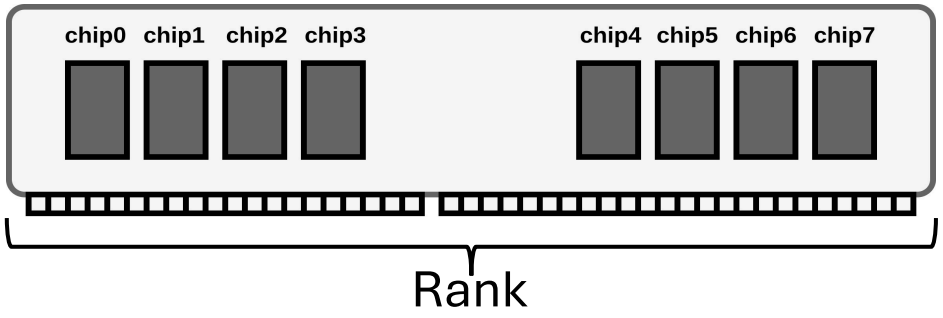
0xCOFFEE

0xCOF00E



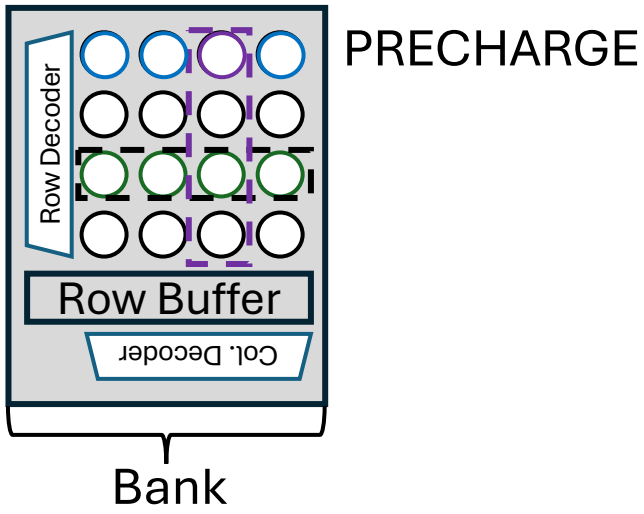
ACTIVATE

Enter FP-RowHammer



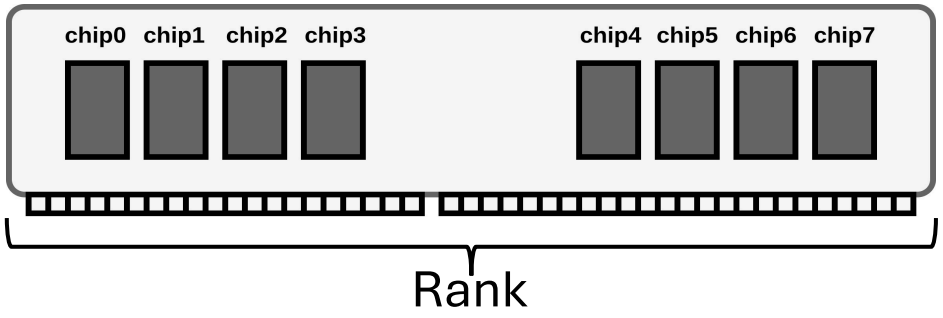
0xCOFFEE

0xCOF00E



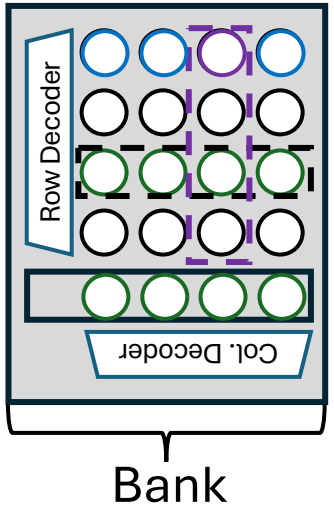
PRECHARGE

Enter FP-RowHammer



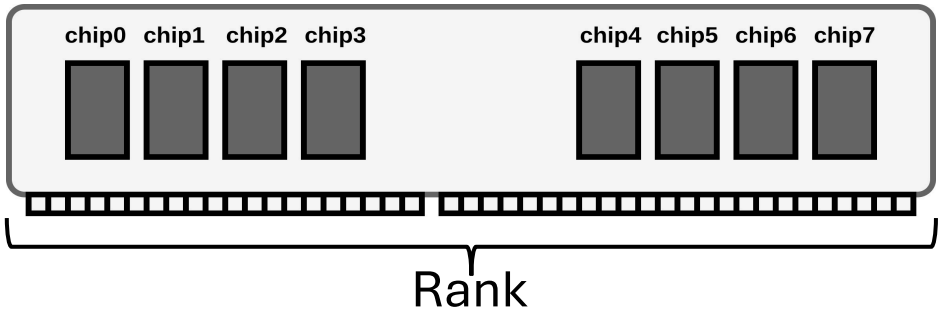
0xCOFFEE

0xCOF00E



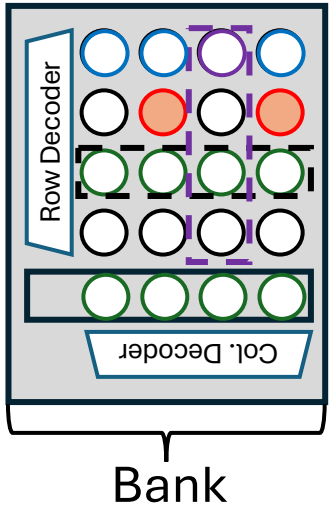
ACTIVATE

Enter FP-RowHammer

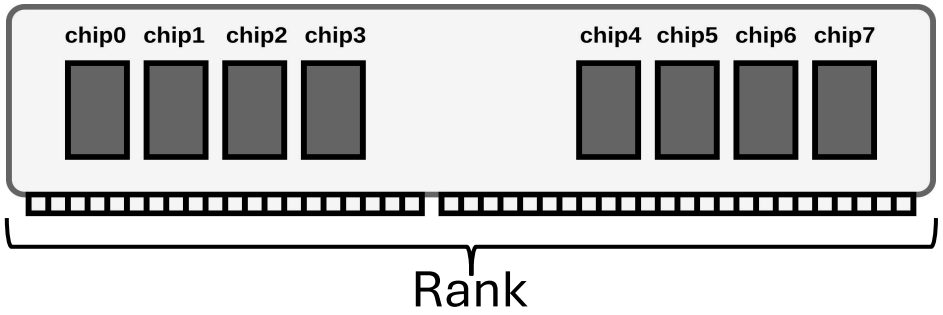


Bitflips!

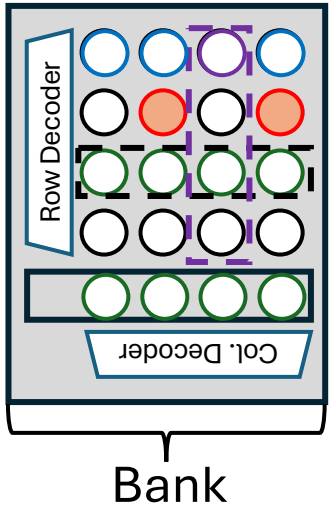
0xCOFFEE
0xCOFFFE
0xCOF00E



Enter FP-RowHammer

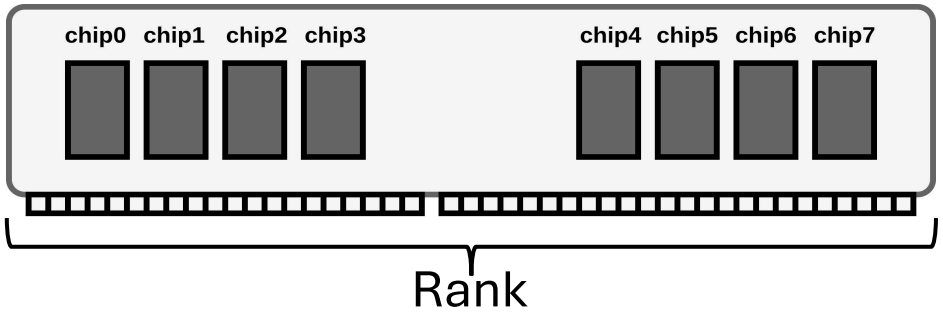


0xCOFFEE
0xCOFFFE
0xCOF00E

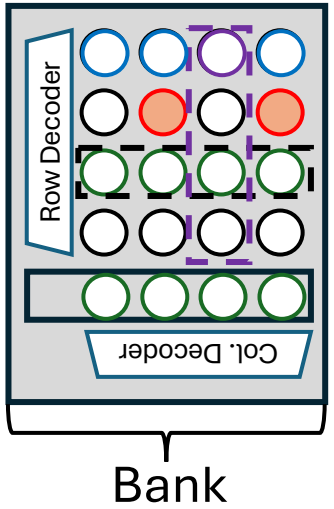


RowHammer

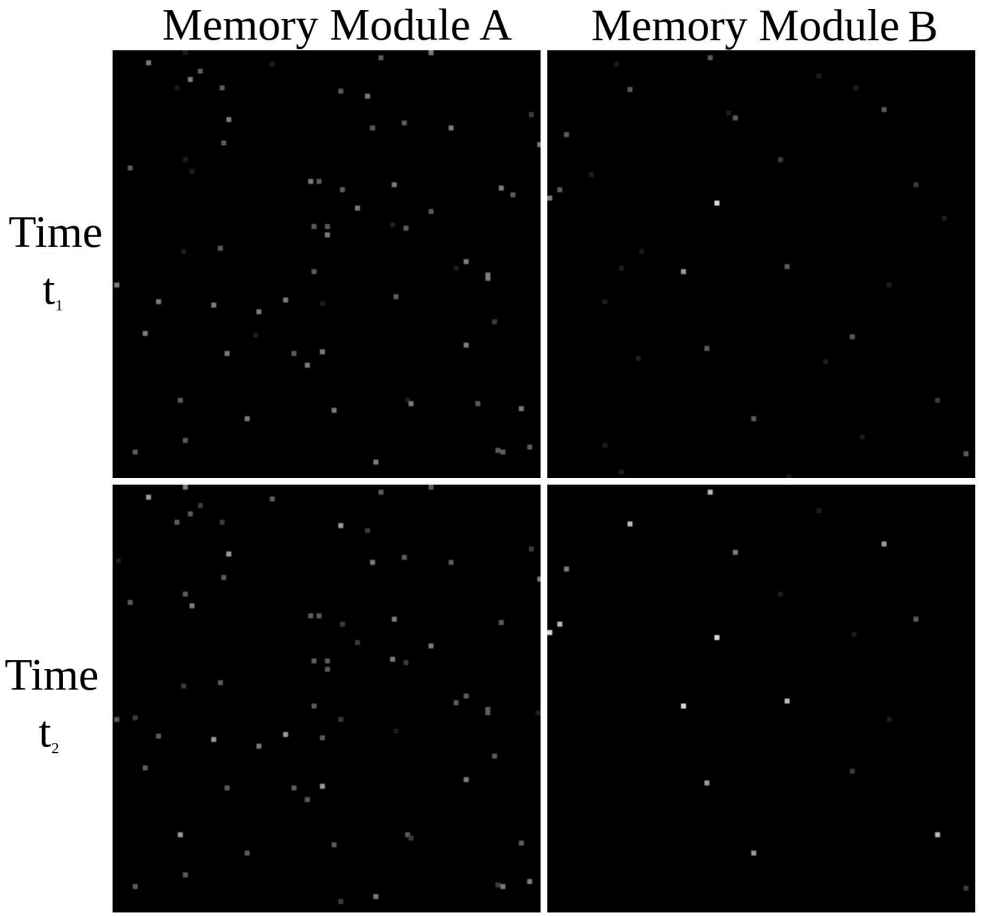
Enter FP-RowHammer



0xCOFFEE
0xCOFFFE
0xCOF00E



RowHammer



Threat Model

- We consider a host-based fingerprinting model
  - Authentication
  - Cross-application tracking
  - Targeted attacks
  - Anti-cheat techniques
- Assumptions
  - Unprivileged attacks
- Challenges
  - Bitflip non-determinism
  - Overcome OS memory abstractions
  - RowHammer defenses

Test bed

We used 98 DIMMs from two DRAM manufacturers.

Dimension	Manufacturer A	Manufacturer B
1Rx8	35	10
1Rx16	11	2
2Rx8	36	4
Total	**82**	**16**

We used 8 Intel Kaby Lakes, 2 Sky Lakes and 1 Coffee Lake machines.

Getting around non-determinism

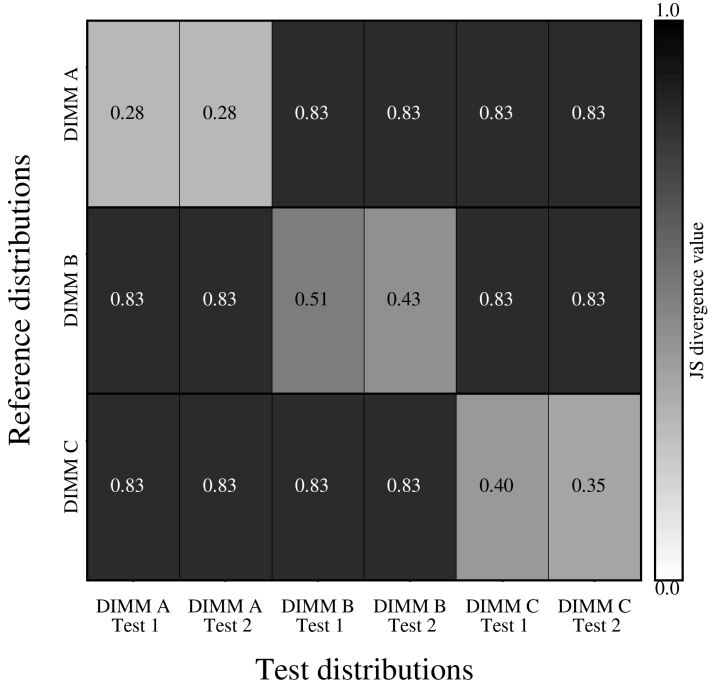
- Bitflips are **arbitrary**.
- We used JS divergence to match fingerprints on a 2 MiB page.
- We used the birthday paradox to quickly find the same region.

Getting around OS abstraction

- Bitflips are **arbitrary**.
- We used JS divergence to match fingerprints on a 2 MiB page.
- We used the birthday paradox to quickly find the same region.

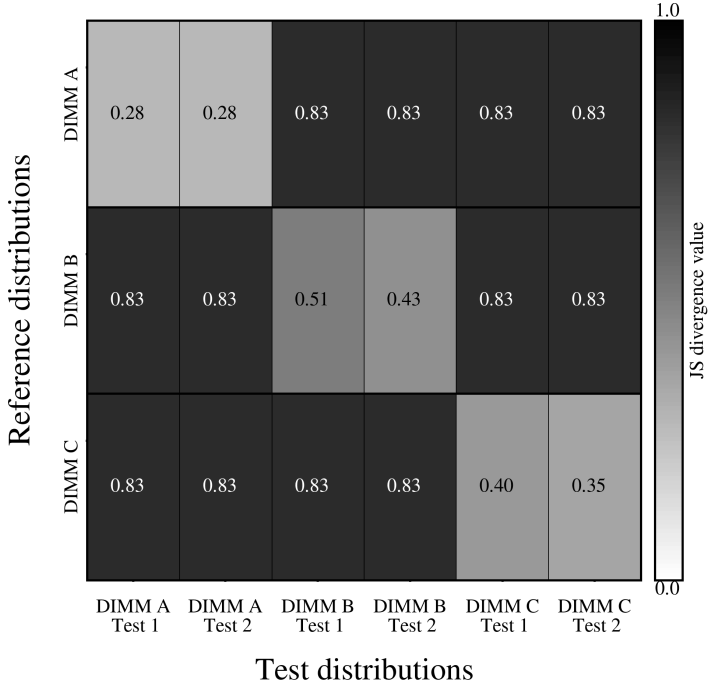
Uniqueness

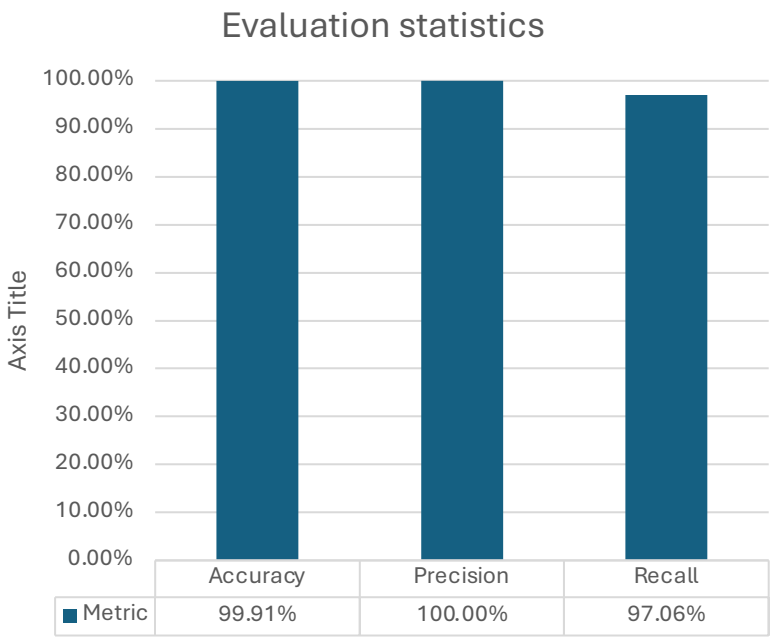
- Bitflips are **arbitrary**.
- We used JS divergence to match fingerprints on a 2 MiB page.
- We used the birthday paradox to quickly find the same region.



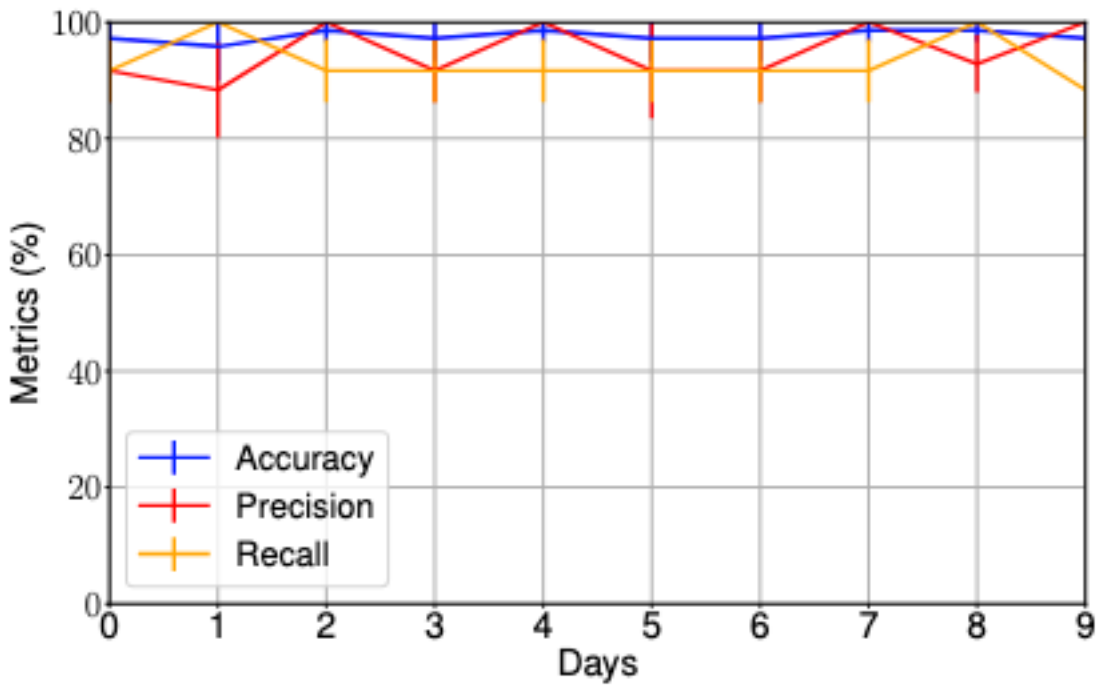
Uniqueness

- Bitflips are **arbitrary**.
- We used JS divergence to match fingerprints on a 2 MiB page.
- We used the birthday paradox to quickly find the same region.

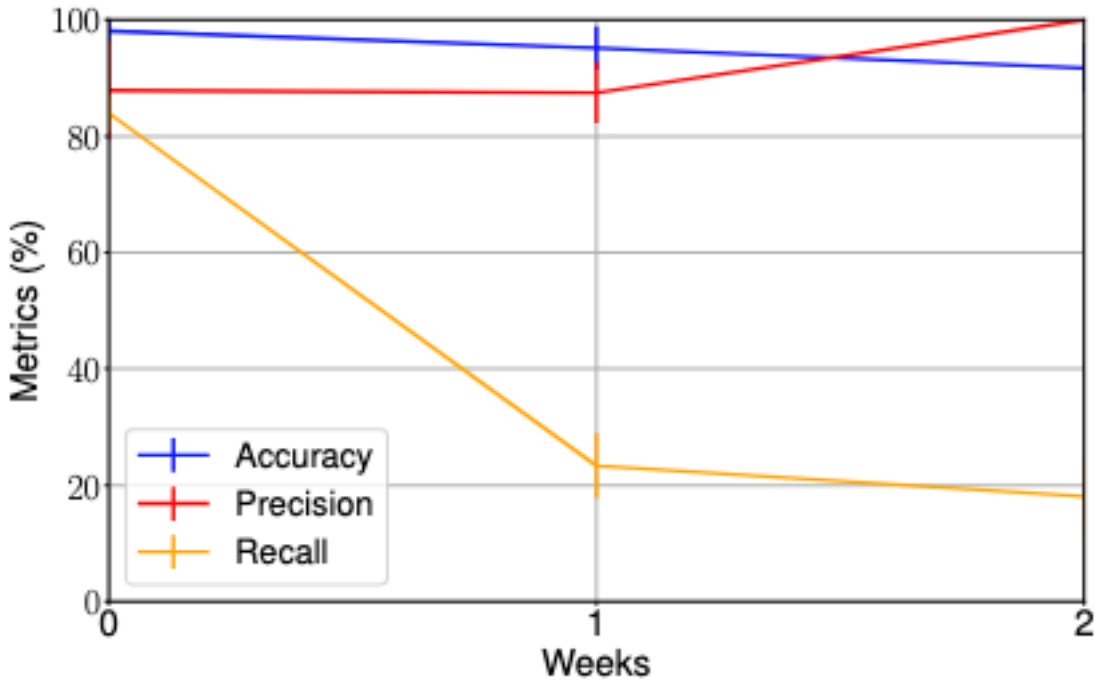




Stability

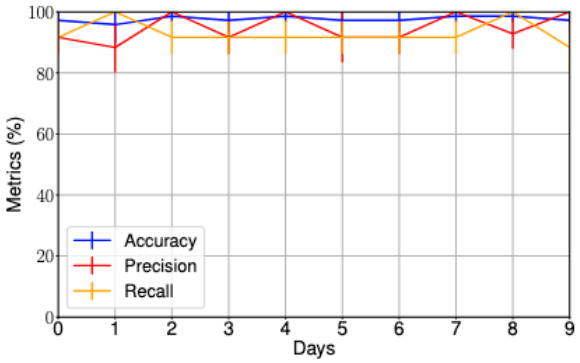


Fingerprint metrics across **days**

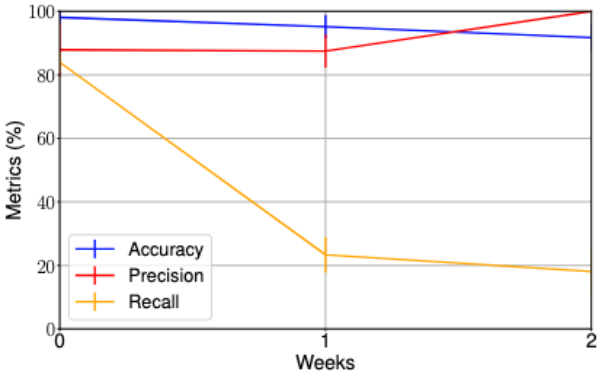


Fingerprint metrics across **weeks**

Stability



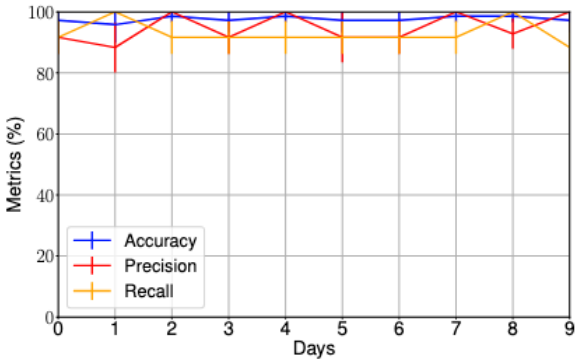
Fingerprint metrics across **days**



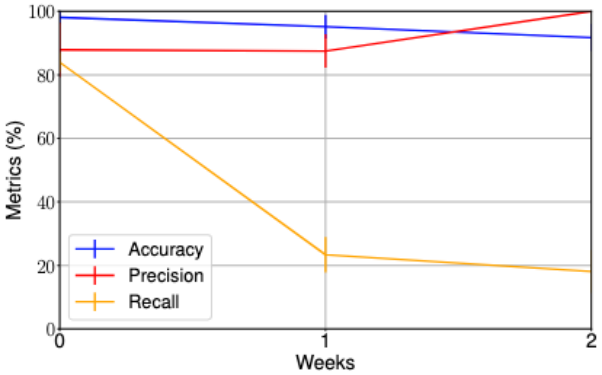
Fingerprint metrics across **weeks**

Why is there a drop in performance?

Stability



Fingerprint metrics across **days**

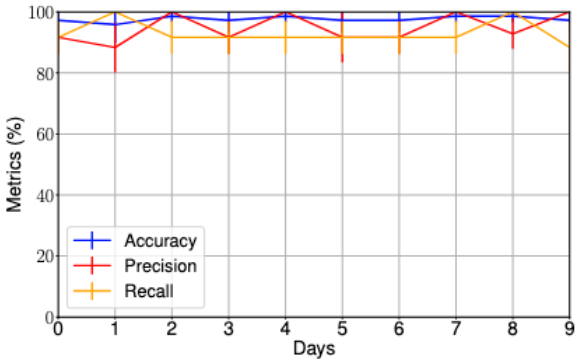


Fingerprint metrics across **weeks**

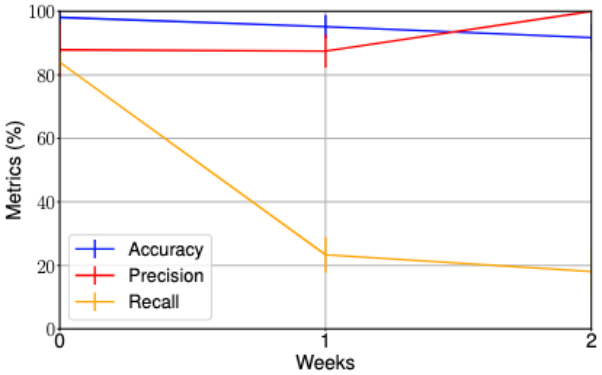
Why is there a drop in performance?

Re-seating

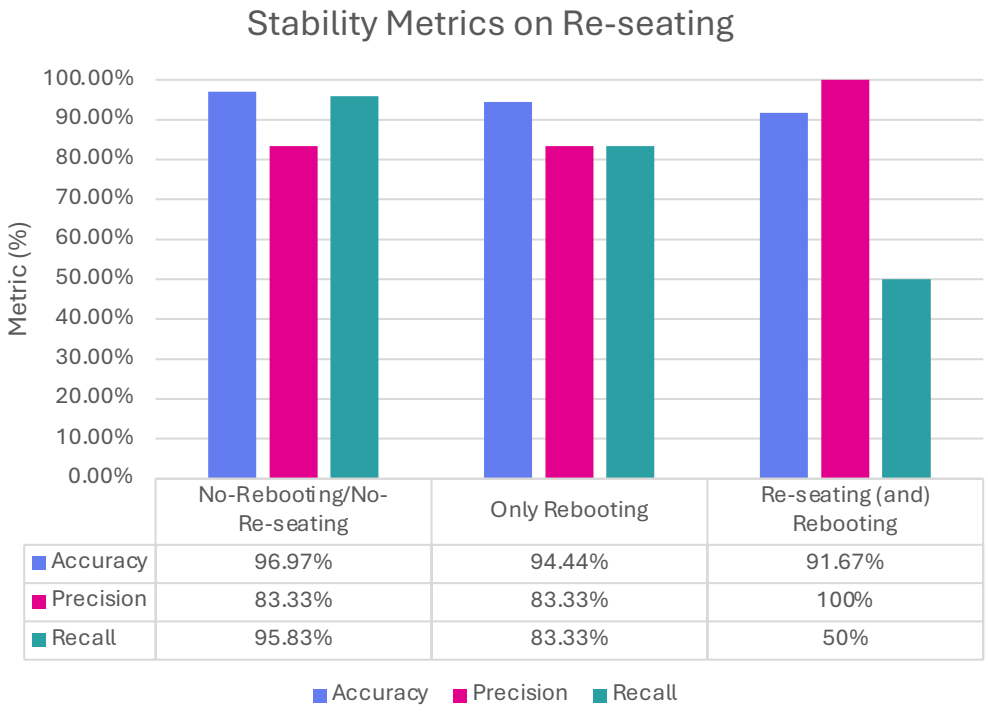
Stability



Fingerprint metrics across **days**



Fingerprint metrics across **weeks**



	No-Rebooting/No-Re-seating	Only Rebooting	Re-seating (and) Rebooting
Accuracy	96.97%	94.44%	91.67%
Precision	83.33%	83.33%	100%
Recall	95.83%	83.33%	50%

Why is there a drop in performance?

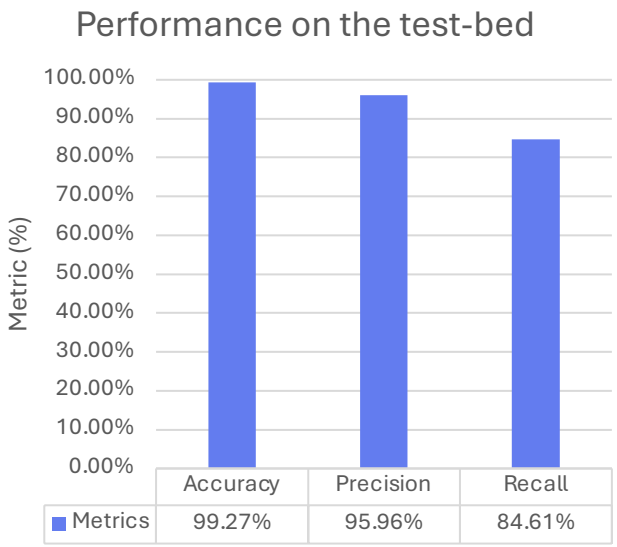
Re-seating

Performance and Robustness

100,000 accesses

Repeating twice

9.9 seconds



Performance and Robustness

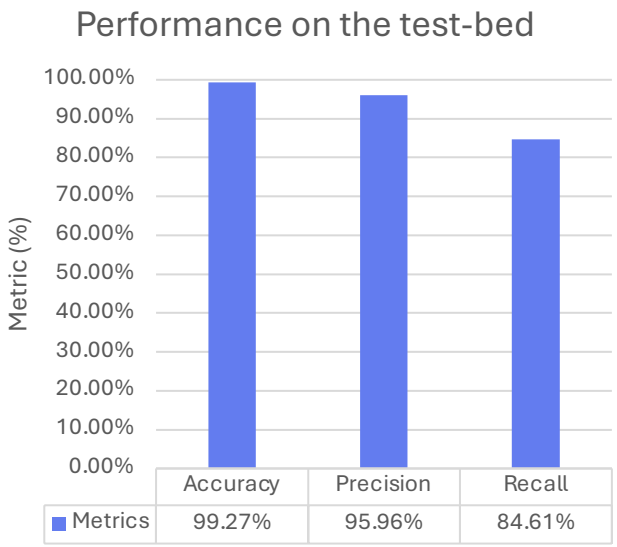
100,000 accesses

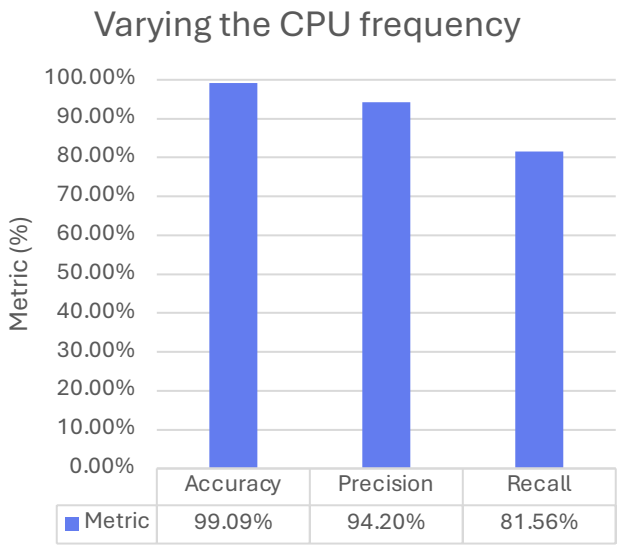
Repeating twice

9.9 seconds

Running YouTube

No crashes.





Performance and Robustness

100,000 accesses

Repeating twice

9.9 seconds

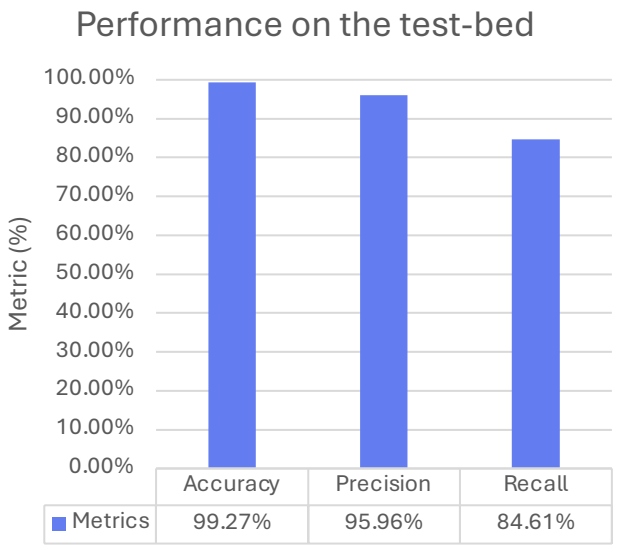
Running YouTube

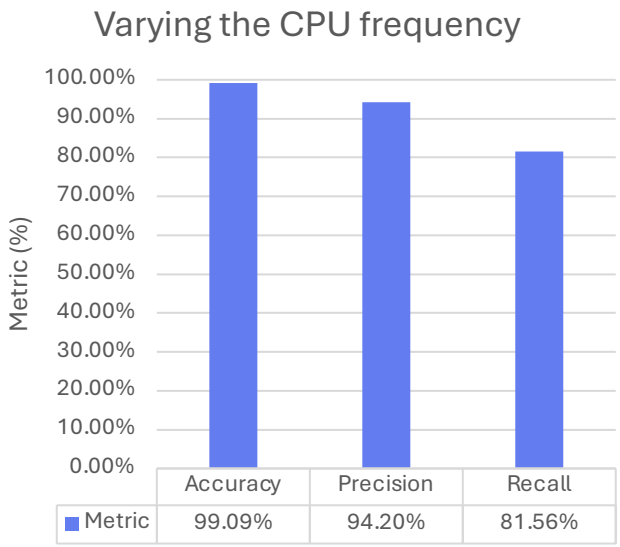
No crashes.

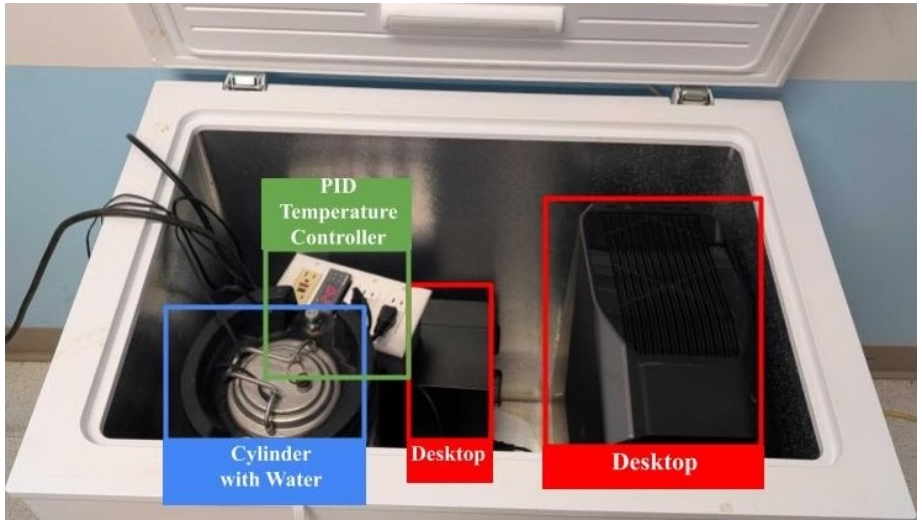
Varying the temperature.

Reference at 15° C

Testing at 40° C







Performance and Robustness

100,000 accesses

Repeating twice

9.9 seconds

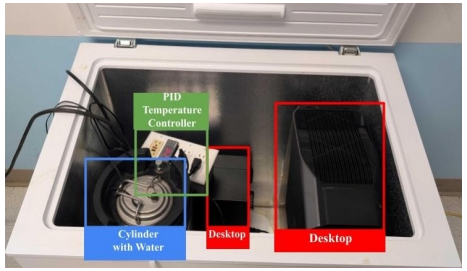
Running YouTube

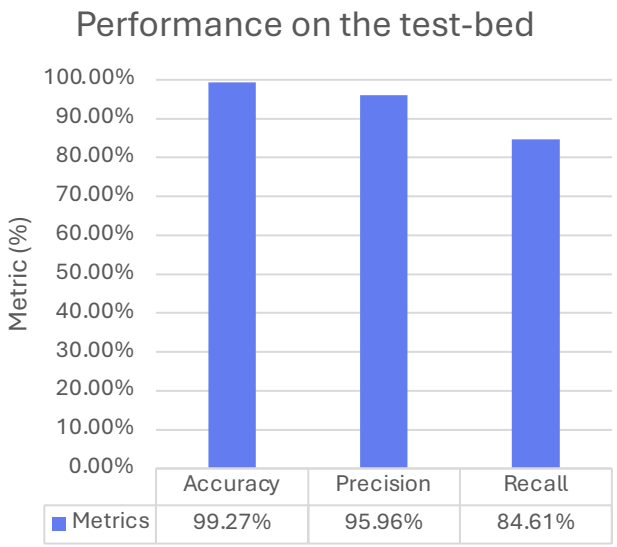
No crashes.

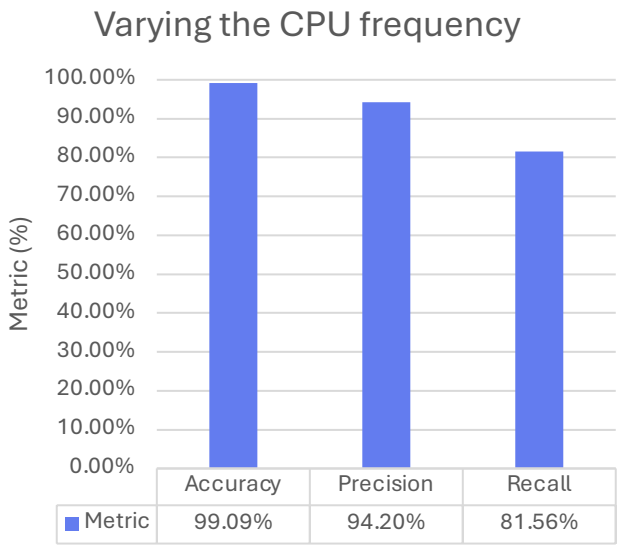
Varying the temperature.

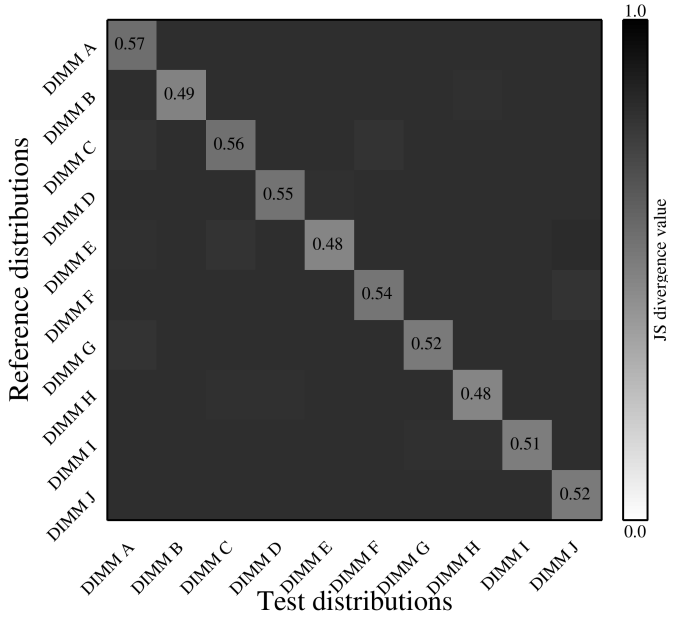
Reference at 15° C

Testing at 40° C









Conclusion

- In this work, we presented FP-RowHammer.
  - A RowHammer based fingerprinting technique.
  - First large-scale RowHammer fingerprinting technique on 98 DDR4 DIMMs
  - High uniqueness and stability
- Risky for apps to use FP-Rowhammer for authentication, but OS/hardware vendors can safely implement FP-Rowhammer.
- **FP-RowHammer cannot be trivially mitigated without fixing the RowHammer vulnerability.**
- Extend our findings to simulation models.

Thank You

Questions?

Read the full paper at: