

CryptArchi 2023 • June 13<sup>th</sup>, 2023

# Simulating cold boot attacks in the gem5 simulator

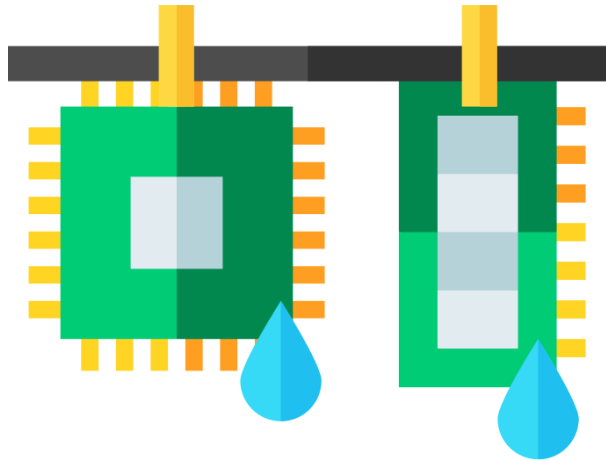
Loïc FRANCE

Supervised by Pascal BENOIT & Florent BRUGUIER



# The ARCHISEC project

---



## ARCHI-SEC

micro-ARCHItectural SECurity

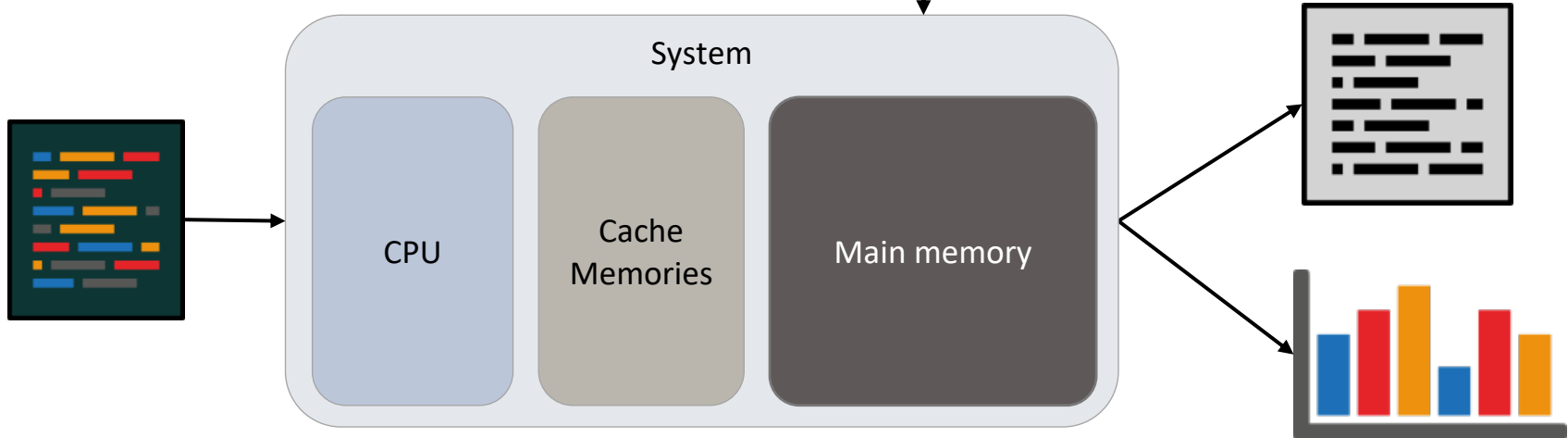
Goal:

Simulate microarchitecture to find weaknesses and develop appropriate protections.



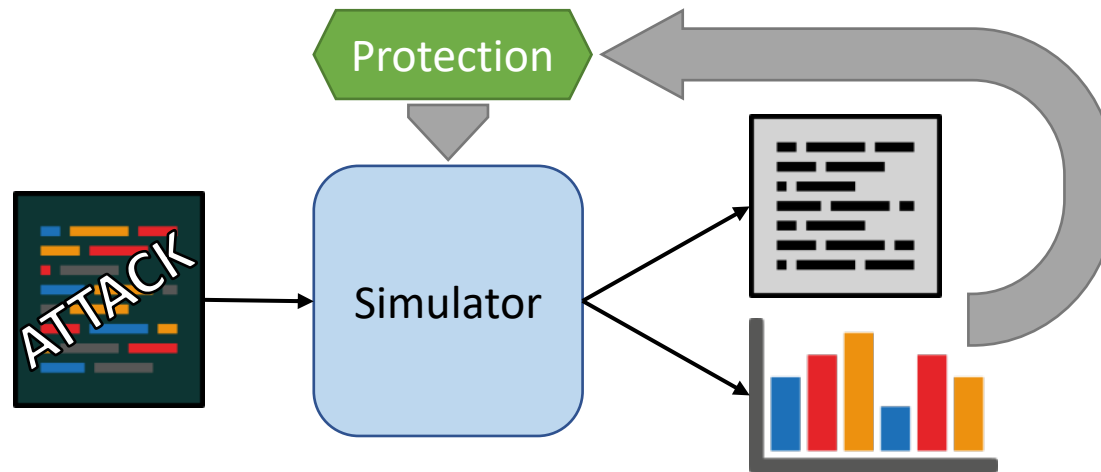
# gem5: Architecture simulator

- CPU type
- Number of cores
- Cache levels and sizes
- Main memory size
- Other modules
- ...



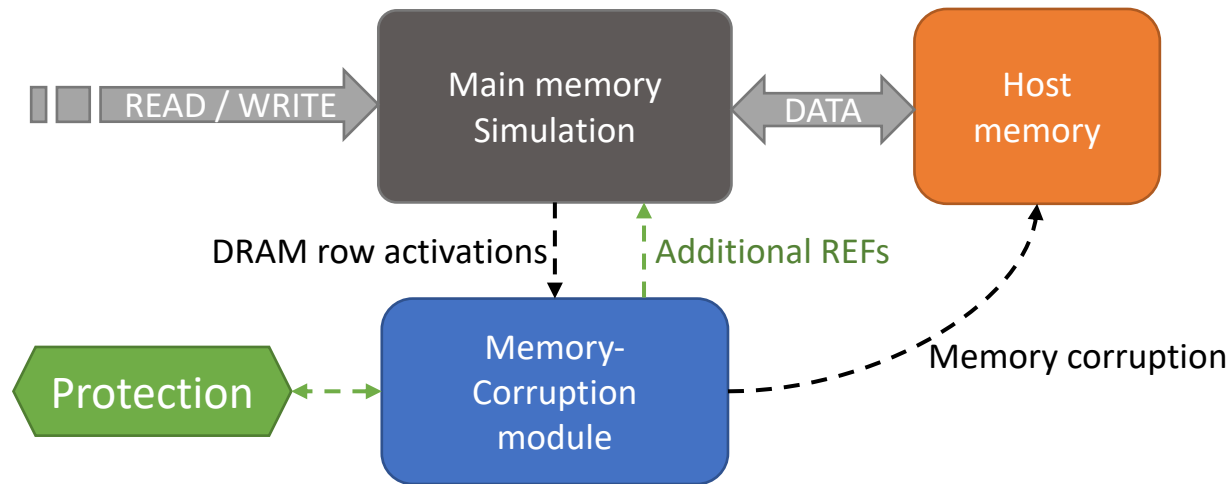
# Use simulators to create protections

---

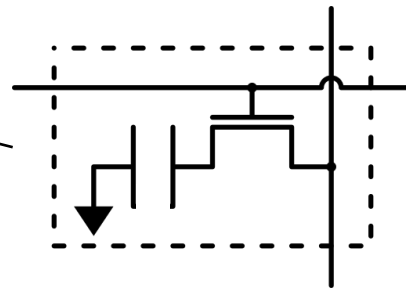
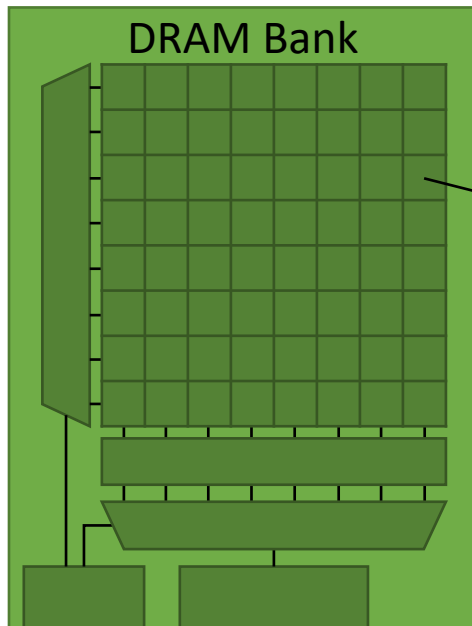


# Previous work: Rowhammer

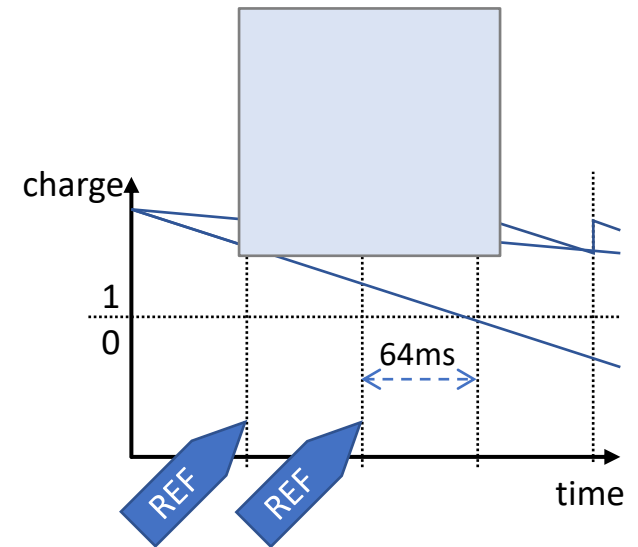
Integration of memory corruption from **Rowhammer** attacks (corruption of the memory induced by memory accesses)



# DRAM data persistence



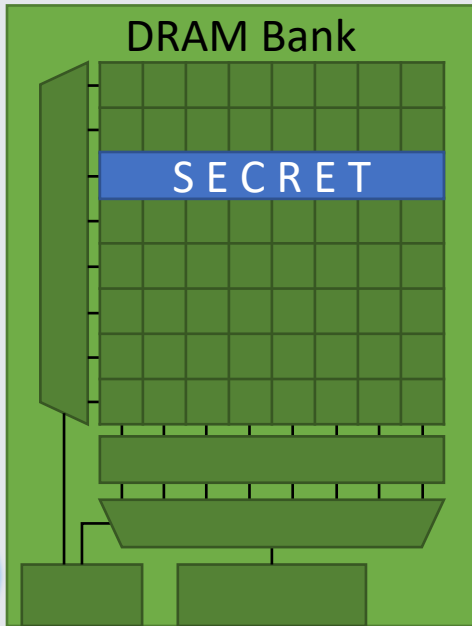
Charged capacitor: 1  
Empty capacitor: 0



# Cold-Boot attack

Principle: recover persistent information from the memory after turning off the victim system

Victim system



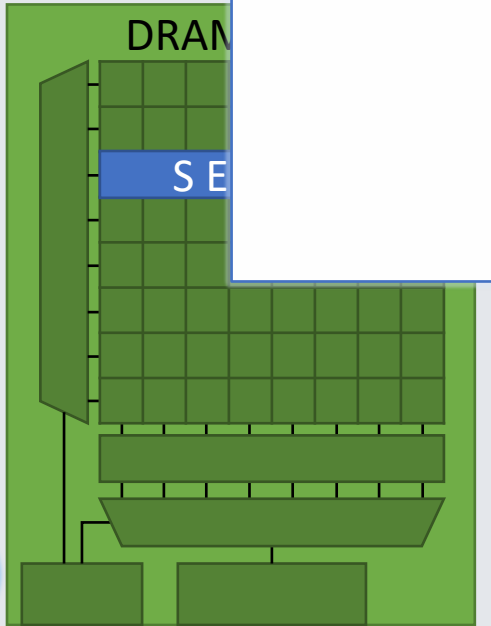
Aggressor system



# Cold-Boot attack

Principle: recover persistent information from the memory after turning off

Victim system



Aggressor system





# Cold-Boot protections

---

- Detect temperature changes and wipe memory
  - Not always possible
- Store sensitive data outside RAM
  - Usually only for encryption keys, not for all sensitive data
- Gluing the memory on the motherboard
  - Limits the system, does not prevent booting aggressor OS on victim device
- Full-memory encryption
  - Performance issues, need modifications on the OS and/or the hardware
- Memory Scrambling
  - Only makes extracting data slower

# Cold-Boot protections

---

- Detect temperature changes and wipe memory

P. McGregor et al., "Braving the cold: New methods for preventing cold boot attacks on encryption keys," Black Hat Security Conference, 2008

- Store sensitive data outside RAM

T. Müller et al., "TRESOR Runs Encryption Securely Outside RAM," USENIX Security 2011.

- Gluing the memory on the motherboard

J. A. Halderman et al., "Lest we remember: cold-boot attacks on encryption keys," ACM SS 2008

- Full-memory encryption

J. Götzfried et al., "RamCrypt: Kernel-based Address Space Encryption for User-mode Processes," ASIA CCS 2016

- Memory Scrambling

S.F. Yitbarek et al., "Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors," HPCA 2017

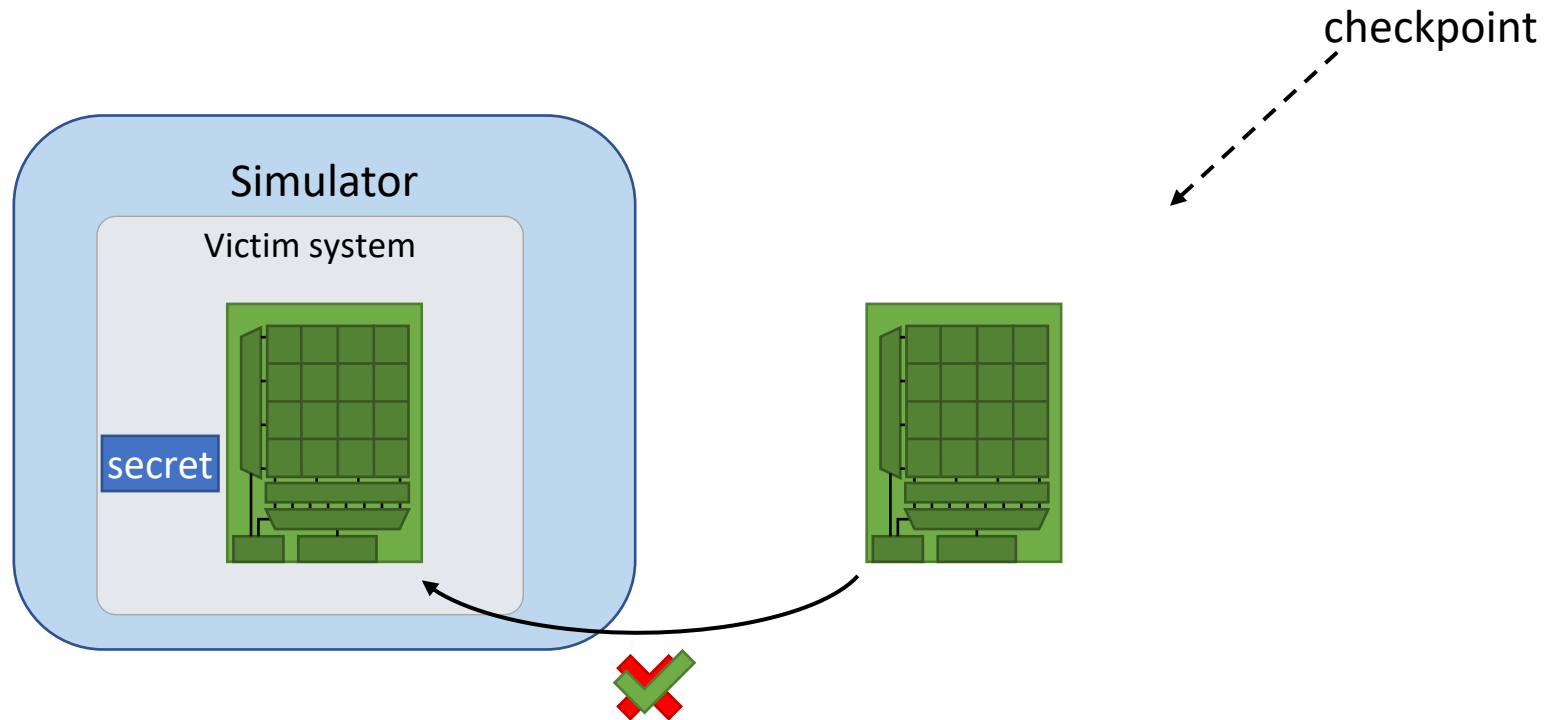
# Cold-Boot attacks on NV RAM

---

Non-volatile → does not need cooling, data persist for a very long time after shut down

⇒ make attacks easier to execute

# Cold-Boot simulation



# Demo

checkpoint

RAM

```
int main() {
    char buffer[] = "secret: cryptarchi2023";
    // ...
    return 0;
}
```

```
$>gem5.opt [...]
--kernel=victim.elf
--checkpoint-at-end
```

RAM2

Aggressor system

RAM1

RAM2

```
int main() {
    int index = find(RAM2, "secret", RAM2_SIZE);
    if (index >= 0) {
        printf("found @ 0x%x\n", index);
        dump(&(RAM2[index-64]), 128);
    }
    else {
        puts("not found\n");
    }
    return 0;
}
```

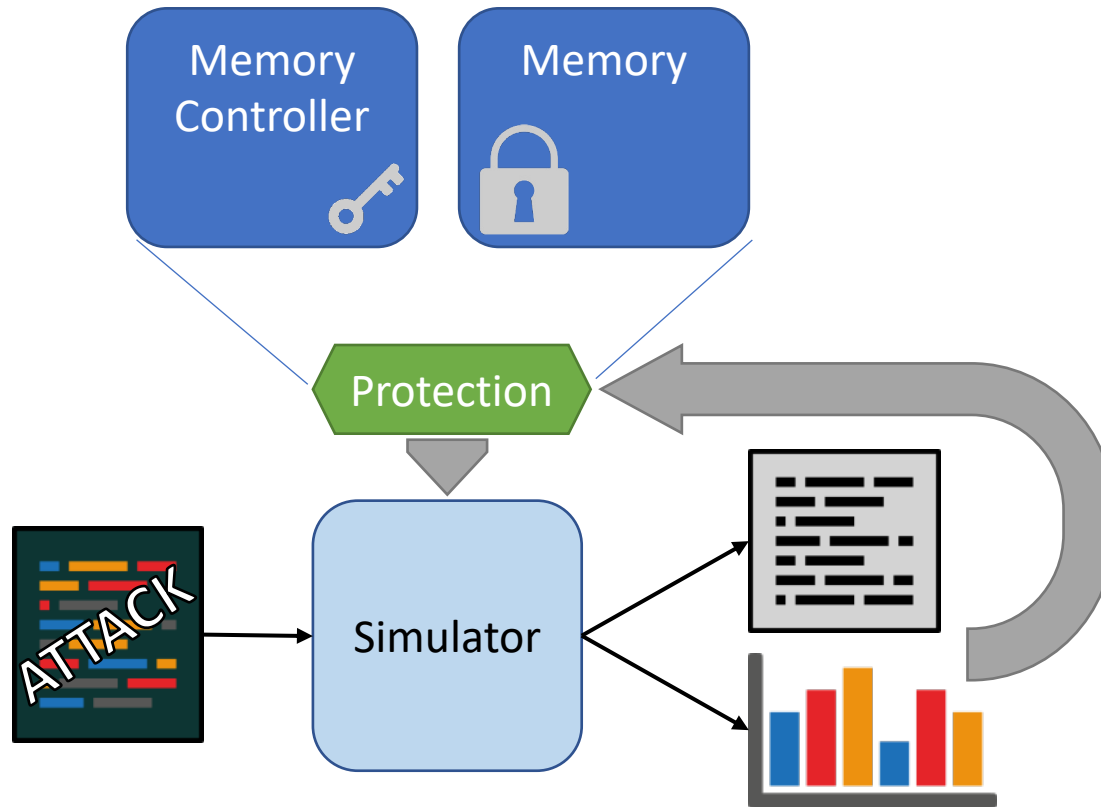
```
$>gem5.opt [...]
--kernel=aggressor.elf
--memory-init-storeids=8
--memory-init-pmems=cpt/system.physmem.store7.pmem
```

found @ 0x00004FF

78,CD,67,E3,54,69,C4,F0,41,33,7A,1F,F2,D8,DA,41,1C,C7,5C,38,05,0B,0F,51,AD,0B,48,18,97,B9,9B,F0,  
FC,A1,A1,E0,74,05,C9,3A,19,B5,39,AD,EB,49,96,08,2E,73,03,43,5A,4E,4A,06,36,5A,6A,F9,61,34,12,56,  
73,65,63,72,65,74,3A,20,63,72,79,70,74,61,72,63,68,69,32,30,32,33,C3,18,8A,ED,09,8E,7B,B8,04,0C,  
EB,C4,76,AA,A6,24,23,C4,E4,4F,86,81,B0,0D,F2,CE,CC,92,3D,D7,62,91,10,DC,22,2A,BF,4D,9B,41,83,D8,

x.g.Ti..A3z...A..\8...Q..H....  
...t...9..I...s.CZnj.6Zj.a4.V  
**secret: cryptarchi2023**.....{...  
..v..\$#.0.....=.b...".M.A..

# Developing countermeasures



Thank you! Questions?

Loïc France

[[loic.france@lirmm.fr](mailto:loic.france@lirmm.fr)]



# CryptArchi 2023 • June 13<sup>th</sup>, 2023

## References

- [Binkert2011] N. Binkert, et al., "The gem5 simulator," ACM SIGARCH computer architecture news, 2011.
- [Gotzfried2016] J. Götzfried et al., "RamCrypt: Kernel-based Address Space Encryption for User-mode Processes," ASIA CCS 2016
- [Gruhn2013] M. Gruhn, and T. Müller. "On the practicability of cold boot attacks." 2013 International Conference on Availability, Reliability and Security. IEEE, 2013.
- [Halderman2008] J. A. Halderman et al., "Lest we remember: cold-boot attacks on encryption keys," ACM SS 2008
- [McGregor2008] P. McGregor et al., "Braving the cold: New methods for preventing cold boot attacks on encryption keys," Black Hat Security Conference, 2008
- [Muller2011] T. Müller et al., "TRESOR Runs Encryption Securely Outside RAM," USENIX Security 2011
- [Xiang2018] Pan, Xiang, et al. "Nvcool: When non-volatile caches meet cold boot attacks," ICCD 2018
- [Yitbarek2017] S.F. Yitbarek et al., "Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors," HPCA 2017
- [Yu2006] J. Yu, , and A. Koorosh. "Leakage current in dram memory cell." 16th Biennial University/Government/Industry Microelectronics Symposium. IEEE, 2006.

Loïc France

[loic.france@lirmm.fr]

