ARCHI–SEC

https://archi-sec.telecom-paristech.fr/

anr® agence nationale de la recherche

Appel : Générique

Année : 2019

Instrument : PRCE

Contact : Loïc Dubois

COORDINATEUR :
Jean-Luc Danger jean-luc.danger@telecom-paris.fr

PARTENAIRES :
Télécom Paris, LIRMM, CRISTAL, LHC, Secure-IC

ABSTRACT

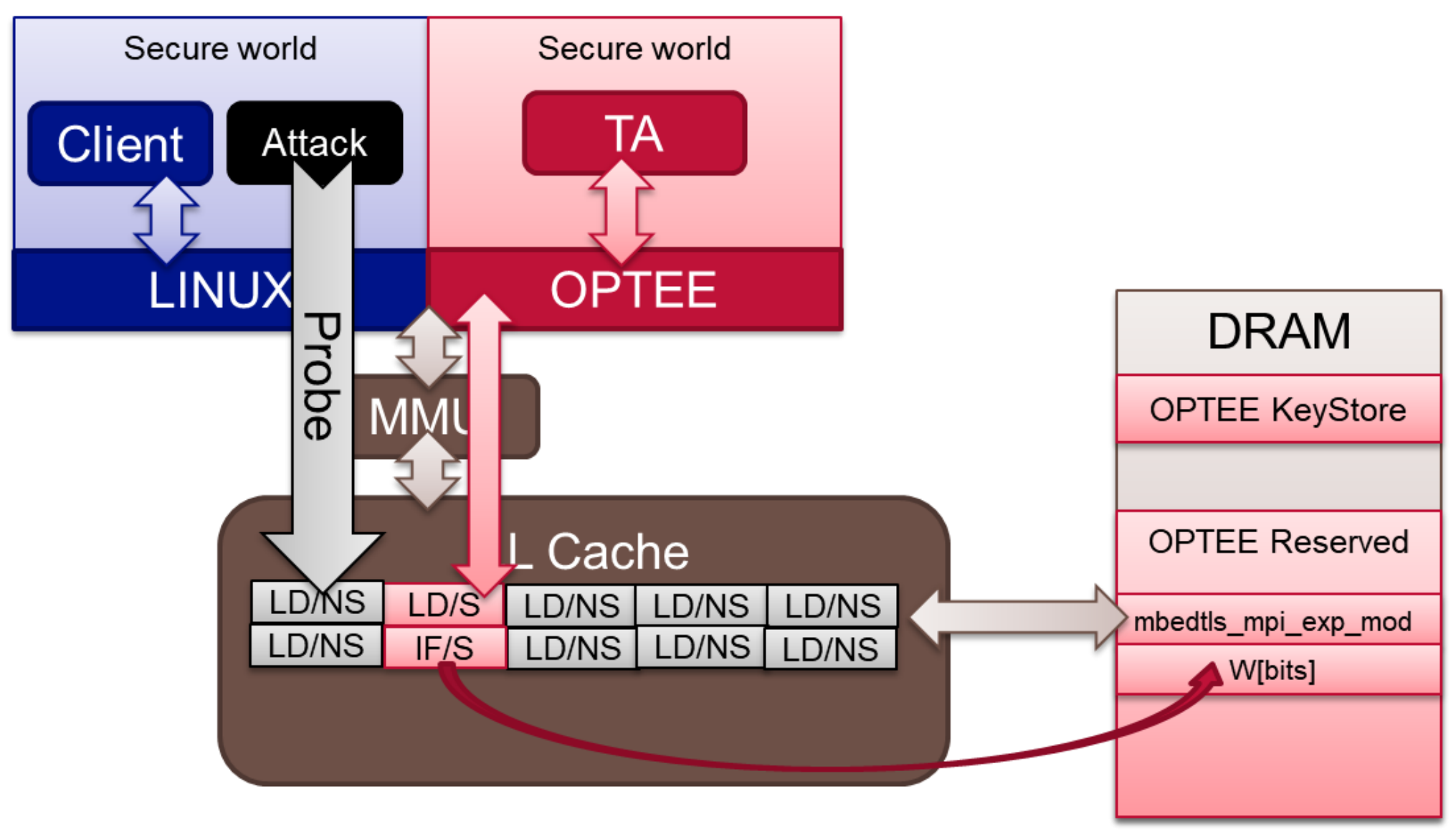
In recent processors (CPUs), **microarchitectural** features can open the door to **security holes** and paves the way to side-channel analysis and transient execution attacks like Meltdown and Spectre. These powerful threats require a thorough analysis and anticipation of potential attacks. The ARCHI-SEC project is to create an open **simulation platform** based on **GEM5** to find microarchitectural vulnerabilities in a system on chip (SoC).

OBJECTIVES

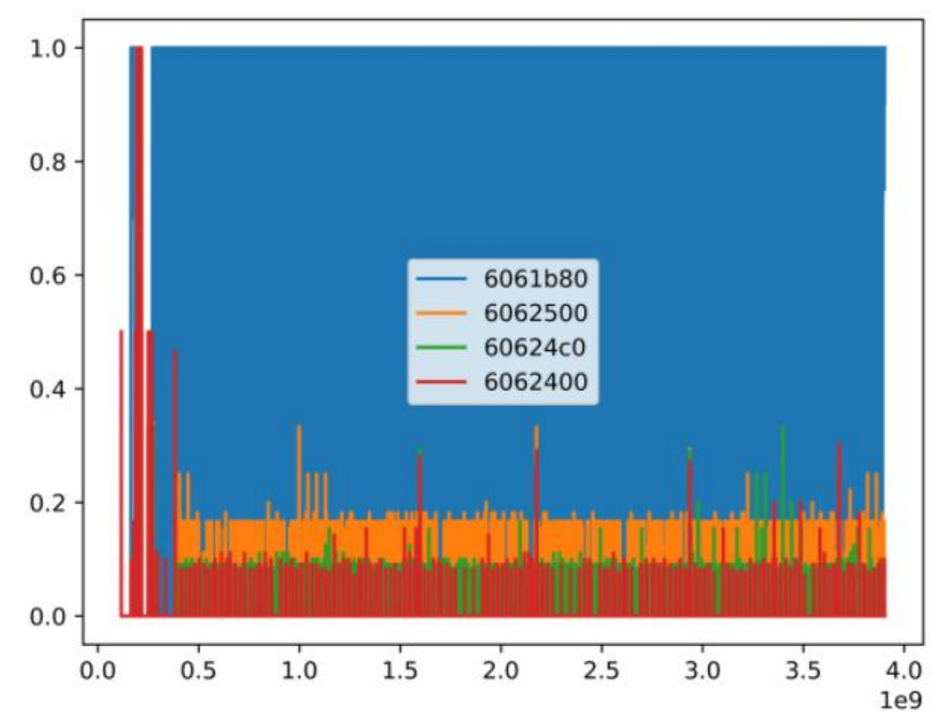
The increase in complexity of modern CPUs and SoCs is mainly driven by the seek of performance rather than security, and most microarchitectural features can open the door to security holes. The ARCHI-SEC project is **to analyze the security of processors and SoC against microarchitectural attacks**. It will create an open virtual platform relying on the gem5 simulator which is a cycle-accurate simulator. GEM5 supports most CPU manufacturers and provides accurate information to observe the microarchitectural behavior and perpetrate attacks. It can simulate components of an heterogeneous SoC architecture. This allows to reproduce the behavior of accelerators or memories and execute fault attacks like Rowhammer on DRAM or Dynamic Voltage and Frequency Scaling (DVFS) in a cryptographic accelerator.

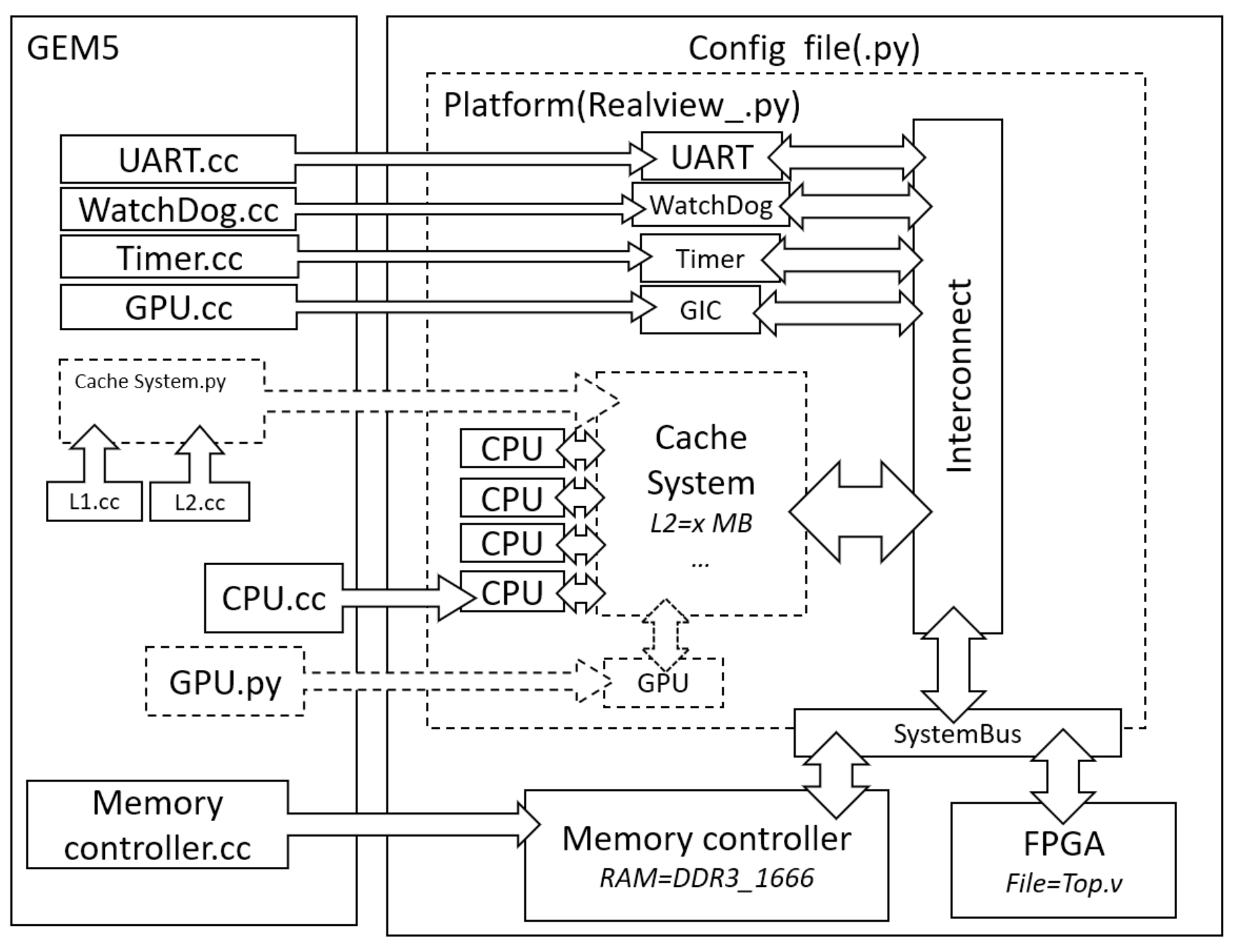
METHOD and FIRST RESULTS

The project is split in parts corresponding to a SoC architecture

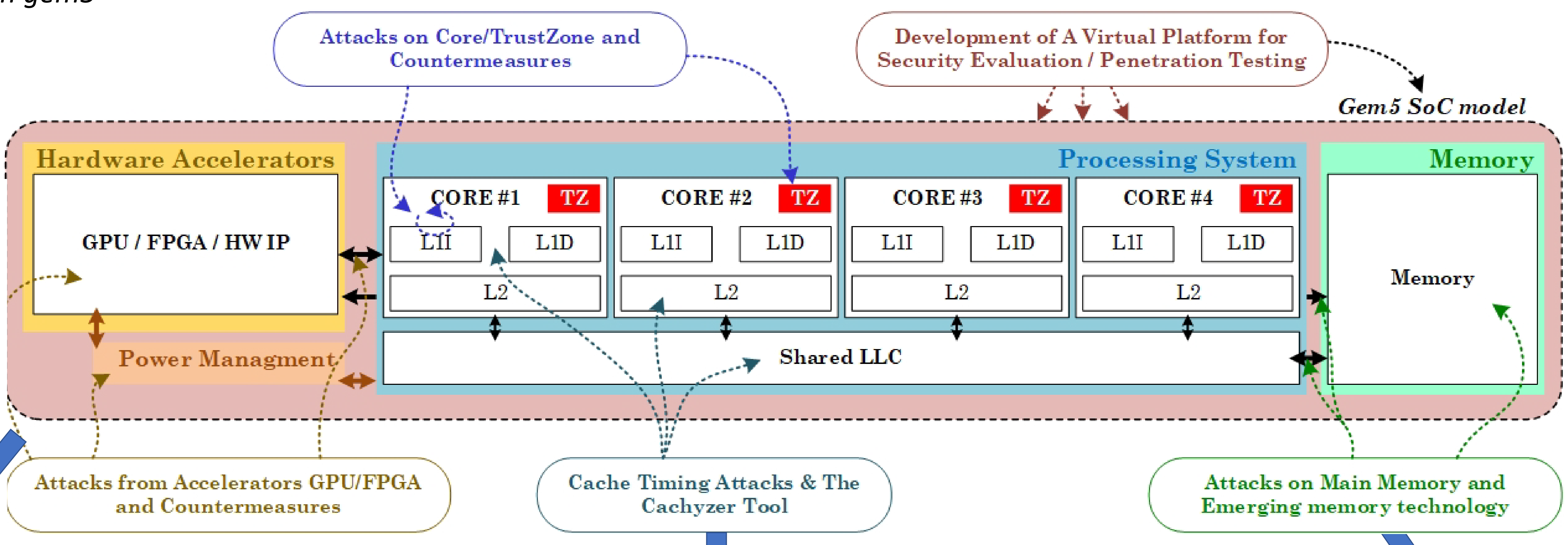


Prime-Probing OPTEE with gem5

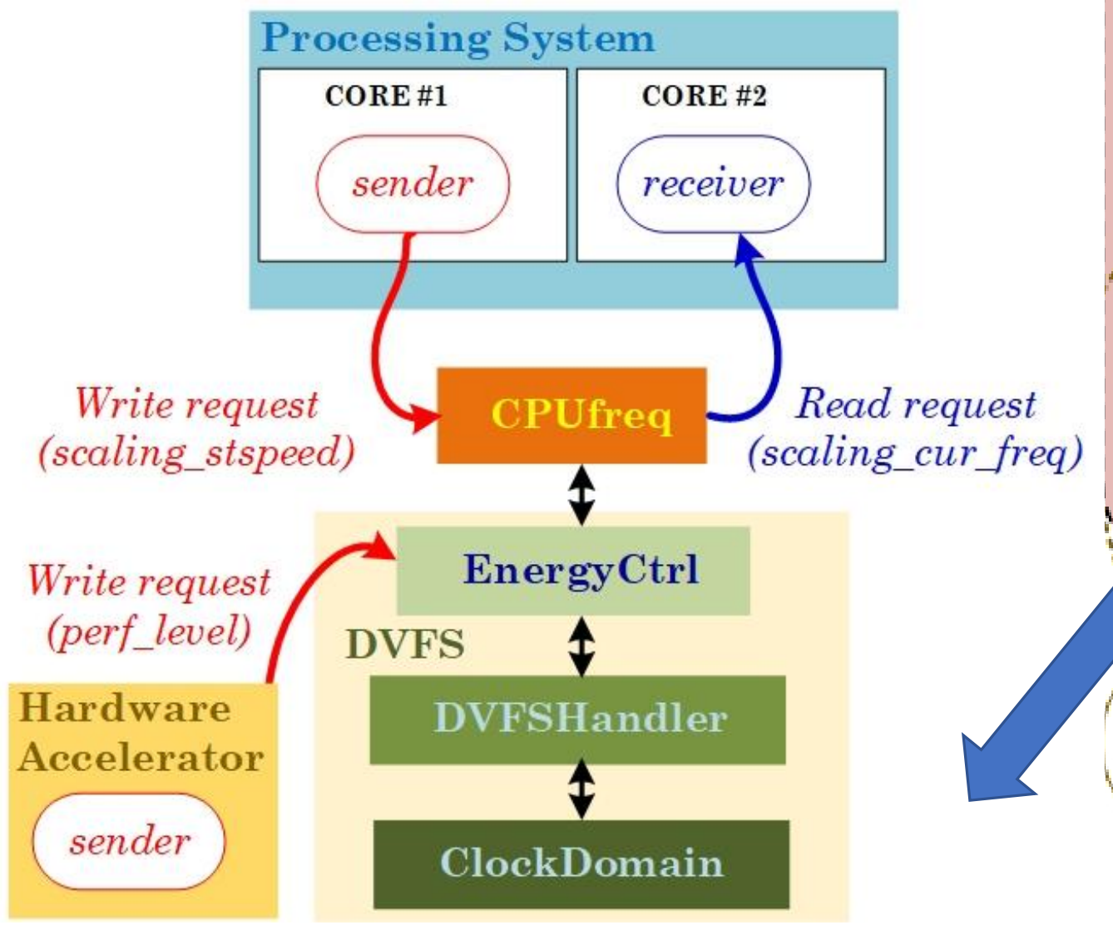


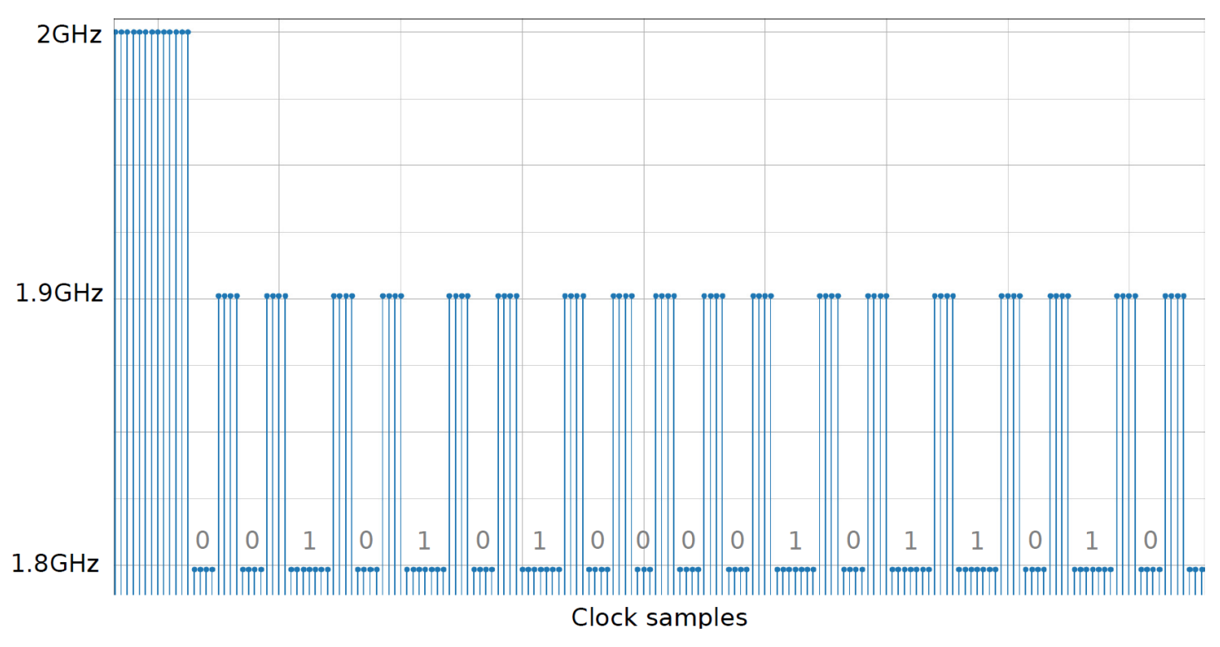


How a gem5 simulation model is laid out between C++ files and Python files.

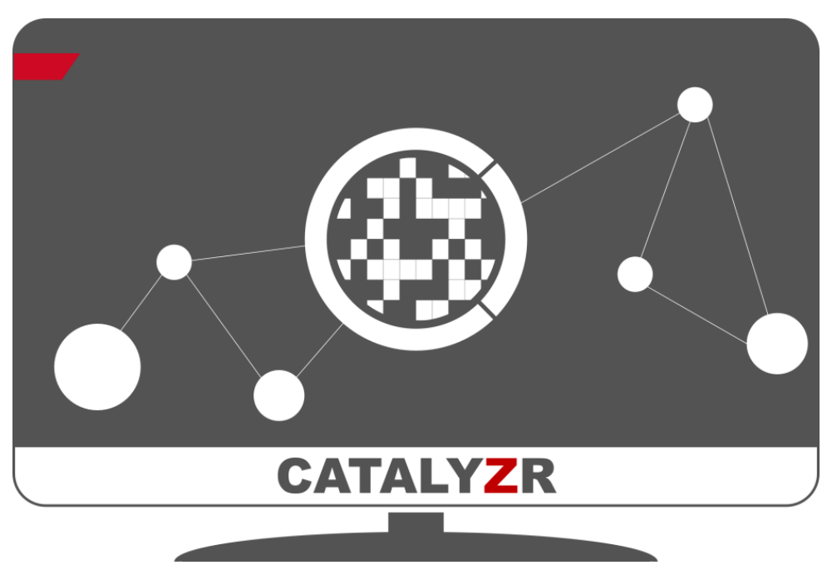

Attacks on Core/TrustZone and Countermeasures
Development of A Virtual Platform for Security Evaluation / Penetration Testing
Gem5 SoC model
Hardware Accelerators
GPU / FPGA / HW IP
Power Managment
Processing System
CORE #1
CORE #2
CORE #3
CORE #4
TZ
L1I
L1D
L2
Shared LLC
Memory
Memory
Attacks from Accelerators GPU/FPGA and Countermeasures
Cache Timing Attacks & The Cachyzer Tool
Attacks on Main Memory and Emerging memory technology

System on Chip



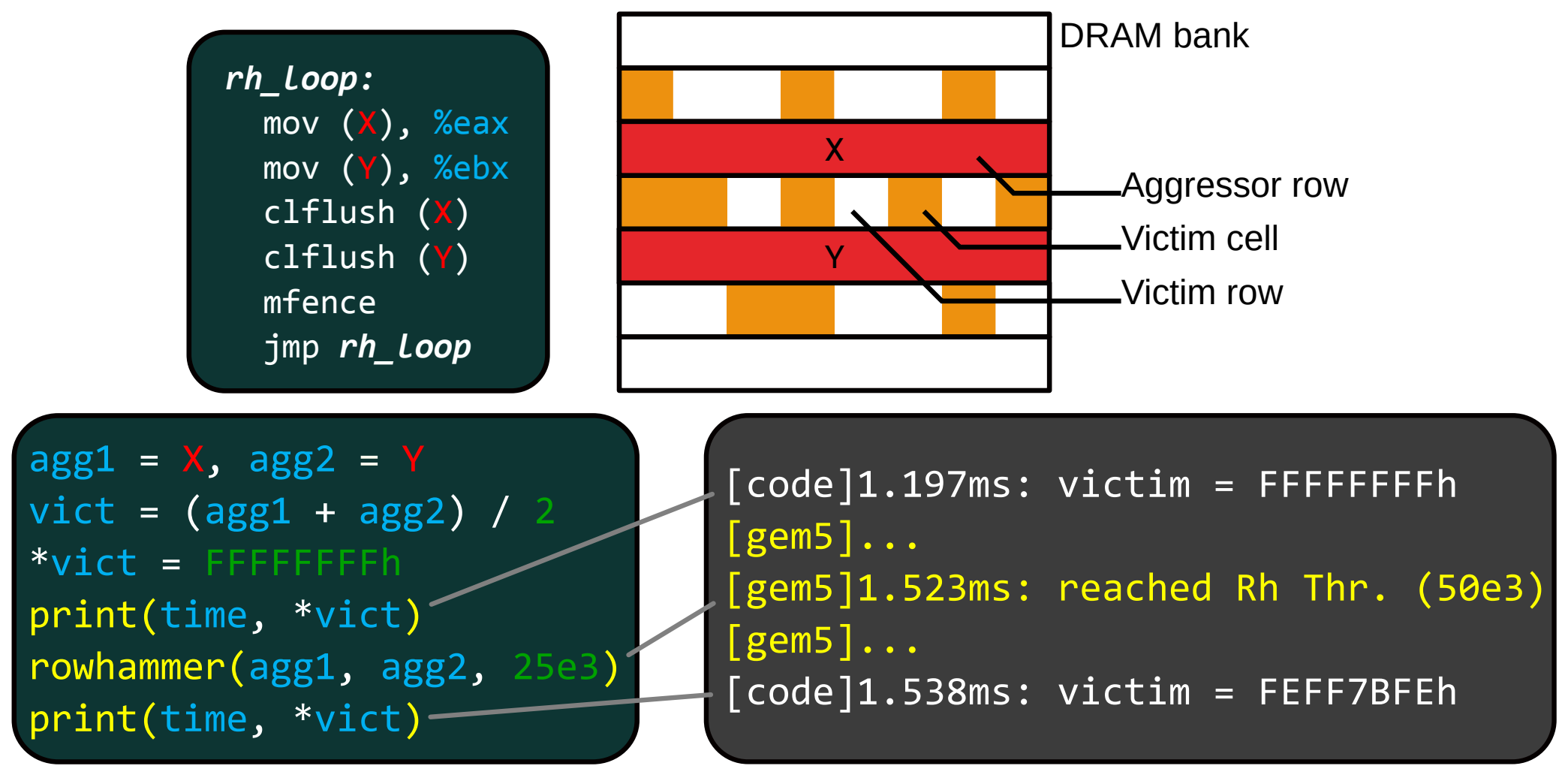


A malicous process uses the DVFS of the SoC as a covert channel to send confidential data to a malicious receiver discretly by frequency scaling.



Tools to assess cache vunerabilities

Post-Quantum Cryptographic Algorithms versus Constant-Timeness, 18-19 feb. 2021, ETSI: https://etsi.eventsair.com/etsi-iqc-quantum-safe-cryptography-technical-event/speakers



```
rh_Loop:
  mov (X), %eax
  mov (Y), %ebx
  clflush (X)
  clflush (Y)
  mfence
  jmp rh_Loop
```

```
agg1 = X, agg2 = Y
vict = (agg1 + agg2) / 2
*vict = FFFFFFFFh
print(time, *vict)
rowhammer(agg1, agg2, 25e3)
print(time, *vict)
```

```
[code]1.197ms: victim = FFFFFFFFh
[gem5]...
[gem5]1.523ms: reached Rh Thr. (50e3)
[gem5]...
[code]1.538ms: victim = FEFF7BFEh
```

Implementing Rowhammer Memory Corruption in the gem5 Simulator
https://hal.umontpellier.fr/hal-03418858/document

TELECOM Paris
IP PARIS
LABORATOIRE HUBERT CURIEN UMR • CNRS • 5516 • SAINT-ETIENNE
SECURE-IC THE SECURITY SCIENCE COMPANY
LIRMM
CRIStAL Centre de Recherche en Informatique, Signal et Automatique de Lille

25 et 26 JANVIER
2022
WISG22 WORKSHOP INTERDISCIPLINAIRE SUR LA SÉCURITÉ GLOBALE
UNIVERSITÉ DE BORDEAUX