A COQ FRAMEWORK FOR MORE TRUSTWORTHY DRAM CONTROLLERS

Felipe Lisboa Malaquias[1], Mihail Asavoae[2], Lirida Naviner[1], and Florian Brandner[1]

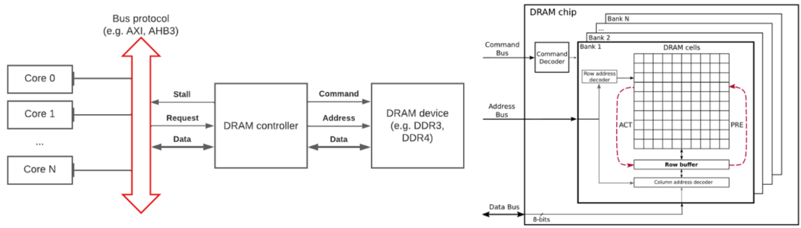
[1]LTCI, Télécom Paris, Institut Polytechnique de Paris
[2]CEA List, Université Paris-Saclay

1. Summary

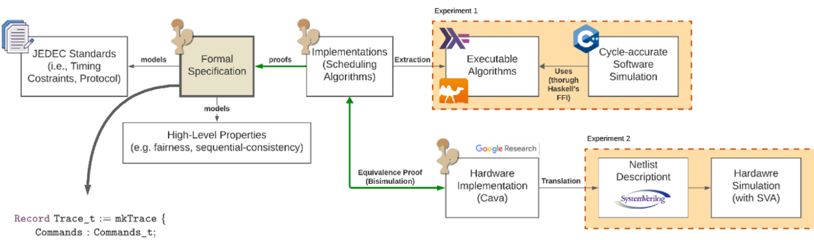
- Recently proposed Real-Time **DRAM controllers** lack trustworthiness.
- We propose a **Coq** framework to aid design and exploration of **new DRAM scheduling algorithms**, in a **reliable** way.
- We use our framework to model two basic scheduling algorithms and propose a new one.
- Algorithms modelled according to the framework are provably compliant with the JEDEC standards [1] and obey other high-level properties, such as fairness [2, 3].
- Algorithms can be proven to be equivalent to a **hardware implementations** written in Cava, a Coq DSL [4]. Cava implementations can then be **translated to SystemVerilog**.

2. Motivation

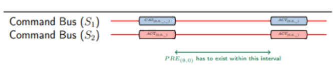
- Memory controllers connect **memory requests coming from processing units** (e.g., CPUs, GPUs, DMA-mapped devices) to the **main memory**.
- The controller needs to implement a scheduling algorithm to decide the **order** in which requests are serviced.
- **Difficult** to balance **predictability** and **performance**. While trying to balance both, algorithms can **get complex** really fast.



3. The Framework (plus Experiments)




```
Record Trace_t := mkTrace {
    Commands : Commands_t;
    ...
    Cmds_T_RRD_ok : forall a b, a \in Commands → b \in Commands →
          isACT a → isACT b → ~~ Same_Bank a b → Before a b → a.(CDate)
          + T_RRD <= b.(CDate);
    ...
    Cmds_ACT_ok: forall a b, a \in Commands → b \in Commands → isACT a
          ∨ isCAS a → isACT b → (Same_Bank a b) → Before a b → exists c
          , (c \in Commands) && (isPRE c) && Same_Bank b c && Same_Bank
           a c && (After c a) && (Before c b);
    ...
}.
```



[1] Joint Electron Device Engineering Council (JEDEC). Ddr4 sdram standard, 2021.

[2] Felipe Lisboa, Mihail Asavoae, and Florian Brandner. A coq framework for more trustworthy dram controllers. In *Proceedings of the 30th International Conference on Real-Time Networks and Systems (RTNS '22)*, RTNS'22. ACM, 2022.

[3] Felipe Lisboa Malaquias, Mihail Asavoae, and Florian Brandner. A formal framework to design and prove trustworthy memory controllers. *Real-Time Systems*, 59(4):664–704, 2023.

[4] Felipe Lisboa Malaquias, Mihail Asavoae, and Florian Brandner. From the standards to silicon: Formally proved memory controllers. In *NASA Formal Methods Symposium*, pages 295–311. Springer, 2023.

This research was supported by Labex DigiCosme (project ANR11LABEX0045DIGICOSME) operated by ANR as part of the program «Investissement d'Avenir» Idex ParisSaclay (ANR11IDEX000302).