

# Investigating Recent CPU Frontends

Advisor: **Stefan Gast**

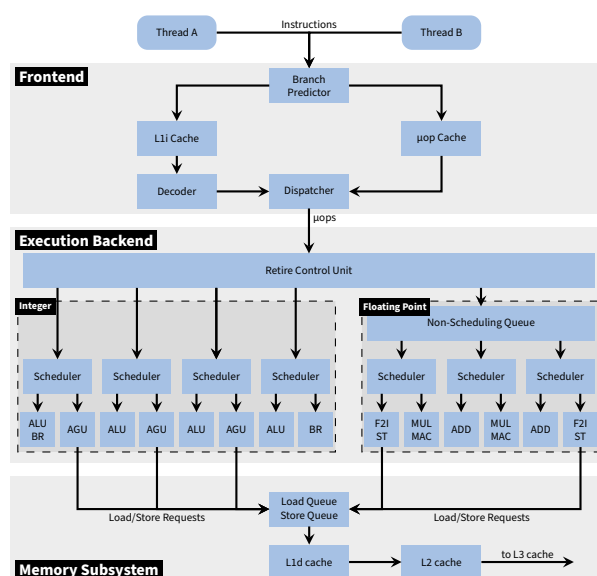
## Motivation

In modern CPUs, the frontend decodes machine code into simpler  $\mu$ ops, which are then executed out-of-order by the CPU backend. Multiple prior attacks have been shown on the frontends of prior CPU generations, including side channel and transient execution attacks. However, CPU vendors frequently update their microarchitectural designs, including the CPU frontend, with unclear security implications.

In this project or thesis, you will investigate the frontend of recent processors for side-channels and transient execution attacks. This topic is scalable, so you can decide on whether you want to do a project, a thesis or both.

## Goals and Tasks

-  Get familiar with modern CPU microarchitectures and attacks on the frontend
-  Think about possible side-channel leakage
-  Exploit and evaluate possible attacks



Simplified execution pipeline of an AMD Zen 4 CPU core.

## Literature

- > [O. Aciğmez, J.-P. Seifert, and Ç. K. Koç](#)  
Predicting Secret Keys via Branch Prediction  
[CT-RSA](#)
- > [P. Kocher et al.](#)  
Spectre Attacks: Exploiting Speculative Execution  
[S&P](#)
- > [Z. Zhang et al.](#)  
BunnyHop: Exploiting the Instruction Prefetcher  
[USENIX Security](#)

## Courses & Deliverables

- ☒ **Introduction to Scientific Working**  
Short report on background  
Short presentation
- ☒ **Bachelor Project**  
Project code and documentation
- ☒ **Bachelor's Thesis**  
Project code  
Thesis  
Final presentation

## Recommended if you're studying

- ☒ CS
- ☒ ICE
- ☒ SEM

## Prerequisites

- > Interest in CPU side channels
- > C, Python, basic x86 assembly

## Advisor Contact

[stefan.gast@tugraz.at](mailto:stefan.gast@tugraz.at)