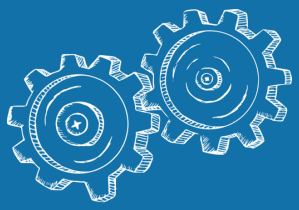


New Forms of Speculation

Advisor: **Moritz Lipp**

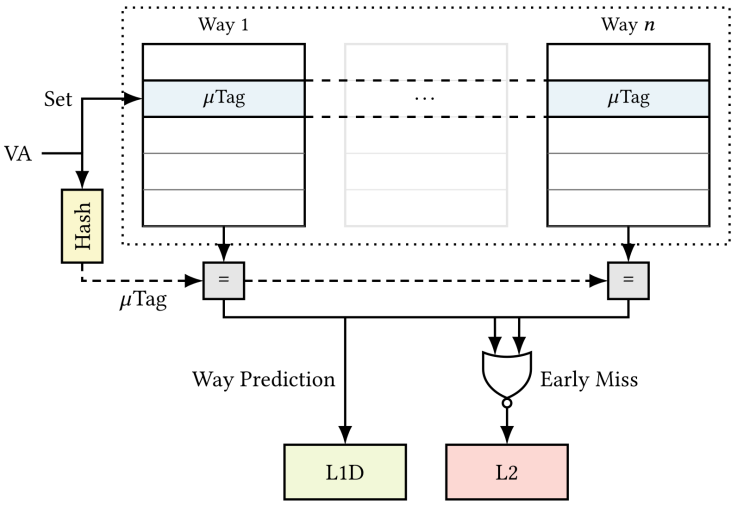
Motivation

With Spectre [1], speculative execution in out-of-order processors has been exploited to leak sensitive data. However, speculation in any form plays a key role to increase the performance of processors. Thus, there are optimizations at all levels of the CPU that may leak information, e.g. the cache way predictor of AMD CPUs [2].

The aim of this thesis is to investigate unexplored speculation mechanisms and performance optimizations in microarchitectures.

Goals and Tasks

- Get familiar with existing side channel and transient execution attacks
- Background research on hardware optimizations
- Perform and evaluate experiments



Simplified Version of AMD's Way Predictor

Literature

- P. Kocher et al.
  Spectre Attacks: Exploiting Speculative Execution
  S&P
- M. Lipp et al.
  Take a Way: Exploring the Security Implications of AMD's Cache Way Predictors
  AsiaCCS

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

- C/C++
- Basic Assembly programming
- Prior knowledge of CPU architecture is useful, but not essential!

Advisor / Contact

moritz.lipp@iaik.tugraz.at