

Side-Channel Attacks on Modern GPUs

Advisor: **Mathias Oberhuber**

Motivation

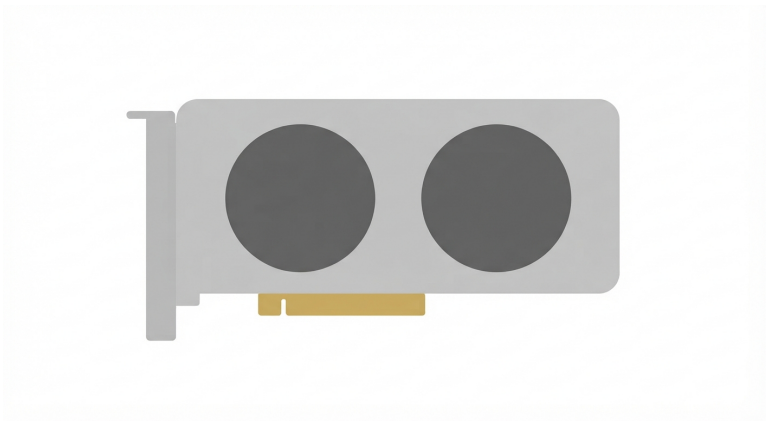
Recent advances in artificial intelligence, particularly Large Language Models (LLMs), have significantly increased the demand for Graphics Processing Units (GPUs) to accelerate computationally intensive workloads. As GPUs become increasingly important, their security also becomes a growing concern. In particular, side-channel attacks can expose sensitive information by exploiting unintended information leakage during GPU execution.

This Project

In this thesis, we review and analyze existing research on side-channel vulnerabilities in modern GPUs. The goal is to identify potential information leakage sources, examine existing attack techniques, and discuss their security implications for GPU-accelerated AI workloads.

Goals and Tasks

- Review existing research on side-channel attacks targeting modern GPUs.
- Analyze known attack techniques and their relevance to LLM workloads.
- Reproduce, evaluate, and extend selected attack techniques from existing literature.
- Discuss the findings, limitations, and security implications for GPU-accelerated AI applications.



Literature

- H. Kim et al.
  TIMESLICE-SANDWICH: A GPU Side-Channel Attack Exploiting Time-Sliced Scheduling
  USENIX Security Symposium

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 low-level programming C/C++
- Programming (Python)
- Familiarity with GPU programming

Advisor Contact

mathias.oberhuber@tugraz.at