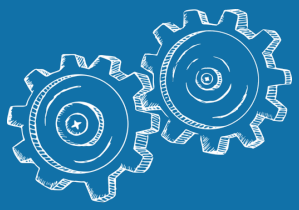

A Trusted Execution Environment for the Vortex GPU

Advisor: **Paul Gollob**

Motivation

Trusted execution environments (TEEs) such as Intel TDX or AMD SEV-SNP protect workloads even from a compromised OS or hypervisor. However, many sensitive workloads, especially machine learning, run on GPUs. Research designs like *Graviton* showed how GPUs can isolate kernels such that the untrusted driver still manages resources but cannot access protected memory.

Vortex is an open-source, RISC-V based GPU, and its newest version supports **virtual memory**. This makes it a good basis for isolation mechanisms similar to modern CPU TEEs.

In this master project or thesis, you will design and implement a **TEE architecture** for Vortex that protects GPU kernels and their memory from the untrusted driver. You will prototype the design and evaluate its security and overhead.

Goals and Tasks

- Get familiar with GPU TEE designs (e.g., Graviton) and CPU TEEs.
- Understand the Vortex architecture and its virtual memory subsystem.
- Design a TEE architecture for Vortex, including a threat model.
- Implement the design in the Vortex RTL and adapt the driver/runtime.
- Evaluate the security guarantees as well as the performance and area overhead.

Literature

- S. Volos, K. Vaswani, and R. Bruno
  Graviton: Trusted Execution Environments on GPUs
  OSDI 2018
  https://www.usenix.org/conference/osdi18/presentation/volos
- B. Tine et al.
  Vortex: Open-Source RISC-V GPU
  MICRO 2021
  https://github.com/vortexgpgpu/vortex

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Computer architecture, virtual memory, SystemVerilog
- C/C++, interest in TEEs

Advisor Contact

paul.gollob@tugraz.at