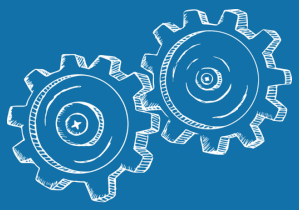

Software-based Fault Attacks

Advisor: **Moritz Lipp**

Motivation

Modern processors are being pushed at their limits in terms of heat and power to achieve fast performance. However, in order to keep the processor running within its specification, voltage and frequency needs to be adjusted accordingly.

With Plundervolt [1], the privileged interface to modify the voltage has been exploited to undermine the system's security. By undervolting the CPU an attacker can fault computations, allowing to leak cryptographic keys from SGX enclaves.

The aim of this thesis is to investigate other unexplored methods to induce faults in a CPUs computations.

Goals and Tasks

- Get familiar with existing fault attacks
- Background research on hardware optimizations
- Perform and evaluate experiments

Logo of the Plundervolt attack

Literature

- K. Murdock et al.
  Plundervolt: Software-based Fault Injection Attacks against Intel SGX
  Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P'20)

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