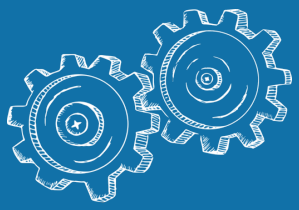


Preventing Side-Channel Leakage with Randomized Hardware Designs

Advisor: **Lukas Giner**

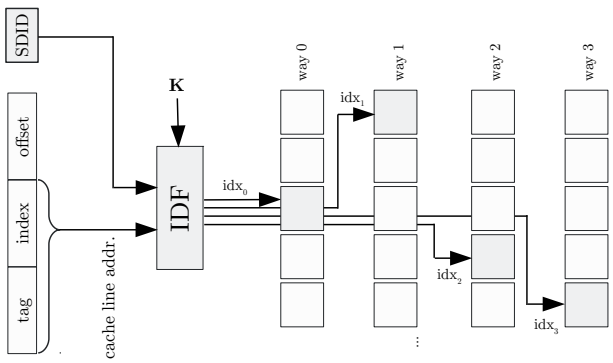
Motivation

Side-channel attacks are a pervasive threat to security-critical systems. They can exist wherever hardware elements are shared between different security domains. One example is the CPU's cache, which has been used extensively as a building block for side-channel attacks in recent years. By increasing the complexity of the mapping between memory addresses and locations in the cache, randomized cache designs try to make using this channel too tedious to be practical. One example of such a design is ScatterCache [1]. However, more recent work [2] has brought into question how much security these designs provide in practice.

We want to design and evaluate hardware components with stronger security guarantees, and we need you to do it! You will help with the design of a new system and write simulation software to test any hypotheses we generate.

Goals and Tasks

- Research background [1, 2] on existing randomized cache designs
- Help with developing a new and much better design!
- Implement & evaluate the design in a software simulator



Mapping of addresses to cache sets in ScatterCache.

Literature

- M. Werner et al.
  ScatterCache: Thwarting Cache Attacks via Cache Set Randomization
  https://www.usenix.org/system/files/sec19-werner.pdf
- A. Purnal et al.
  Systematic Analysis of Randomization-based Protected Cache Architectures
  https://www.esat.kuleuven.be/cosic/publications/article-3194.pdf

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 ☑ MATH

Prerequisites

- Solid foundation in probability theory
- Programming (C/C++/Rust)

Advisor / Contact

lginer@iaik.tugraz.at