Seminar „Hardware-oriented Computer Science“, Winter Semester 2025/26.

Ilia Polian & Maël Gay, Institute of Computer Architecture and Computer Engineering

Seminar date: TBA

Further optional date: TBA

Hardware-oriented computer science is a wide field of research. In this seminar, we will focus on two aspects of it: emerging architectures and hardware security, as they are both extremely relevant nowadays. This seminar will discuss those two aspects of hardware-oriented computer science.

First of all, many novel computing paradigms that differ from traditional architectures have emerged. They cover a wide range of possible applications and technologies, such as new memory elements, new computing paradigms and entirely new forms of data processing. Some of these new approaches intend to deal with hardware limitations of traditional architectures, such as area and energy usage, while others focus on possible future applications, like large scale neural networks and high performance computing.

In terms of hardware security, our second research focus for this seminar, a large variety of encryption schemes, attacks and counter-measures have been proposed over the year. On the encryption side, schemes range from well studied ciphers, such as the AES, to new quantum safe ones in the area Post-Quantum Cryptography. Attacks themselves can of course be theoretical. What is called cryptanalysis, but they can also make use of passive side-channels, such as the power consumption of a device, or active attacks, such as the injection of faults during the encryption process, to recover secret information. These are called hardware-based attacks. Due to those attacks, many counter-measures have been proposed, with new ones surfacing shortly after new attacks are found.

The seminar topics will cover some of the new computing architectures among others: stochastic computing, approximate computing, neural network accelerators and emerging memory devices, as well as hardware cryptography: post-quantum schemes, side-channel attacks, fault attacks and their respective counter-measures.

The **seminar description,** which includes a list of topics, summarizes requirements, and organization, and provides hints on how to prepare the written report and the oral presentation, is uploaded in ILIAS. Please read it carefully. The Latex sources of this summary, to be used as a template for your written report, are also uploaded in ILIAS.

The topics will be briefly introduced in the **first meeting** on **TBA** in room **TBA**. The actual presentations will be organized in a block at the end of the semester, so you have enough time to understand your topic, and prepare your report and your presentation. The exact dates of the seminar will be determined during the first meeting. No requests to change the dates will be accommodated after this meeting. It is **compulsory to attend all presentations** of the seminar to get credits, so do bring your calendar to the first meeting.

In the **second meeting** on **TBA**, the topics will be assigned. Please look at the papers and come to the meeting with a list of at least three favorites. All participants have one week to select the topics. We will ignore all emails during the first week asking to reserve a certain topic; all participants present during the second meeting will have equal chances of getting a topic of their interest. Please do attend the second meeting as well, since all topics which have been assigned during that meeting will not be available.

After the second meeting, the list of topics that are still available (were not assigned) will be published in ILIAS. If you did not attend the second meeting or want to replace your topic, write an email (after the second meeting), with a ranked list of at least three, preferably more, topics from the list of available topics. The topics will be assigned on a first-come, first-serve basis; if you did not specify enough topics, you will be assigned the topic with the lowest number still available.