

# Overview of Practical Sessions

October 2, 2023  
Ahmet Can Mert  
[ahmet.mert@iaik.tugraz.at](mailto:ahmet.mert@iaik.tugraz.at)



## A High-level Overview

- We have one-hour practical session every week (Tuesday, 10:00-11:00). We will use it for ...
  - Tutorials
    - Verilog, Software tool, FPGA
  - Explaining assignments
  - Office hour and Q&A

# Course webpage/Discord Channel

- All course materials (lecture slides, tutorials, assignments...) will be available in course webpage.
  - <https://www.iaik.tugraz.at/chw>

**SELECTED TOPICS OF INFORMATION SECURITY -  
CRYPTOGRAPHY ON HARDWARE PLATFORMS (WS  
2023/24)**

[Course Number 705221](#) | Wintersemester 2023/24

**Content**

This course teaches how to implement cryptographic algorithms efficiently on hardware platforms. It covers hardware implementation aspects of symmetric-key, asymmetric-key cryptographic primitives, true and pseudo random number generation, physically unclonable functions, as well as basics of homomorphic encryption. The content offered in the lectures is accompanied by practical assignments. In the practical assignments, you will be given reference proof-of-concept software implementations and you will build hardware-software codesign architectures for them.

Learning goals:

**Lecturers**

- ✉ [Sujoy Sinha Roy](#)
- ✉ [Ahmet Can Mert](#)

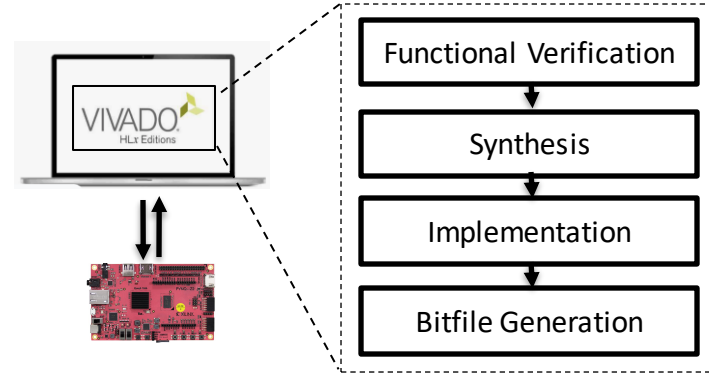
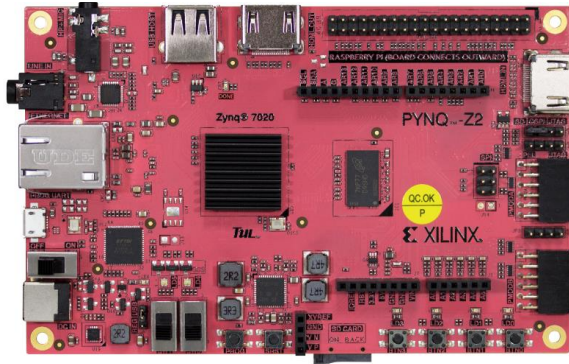
**Table of Content**

- > [Content](#)
- > [Material](#)
- > [Administrative Information](#)
- > [Lecture Dates and Exams](#)
- > [Lecturers and Teaching Assistants](#)

- **Discord Channel**
  - Announcements, Q&A, ...
  - Link (also in the course webpage): <https://discord.gg/hNe9mjeZH>

# Tools: FPGA Board

- For some parts of the assignments, we will use the PYNQ-Z2 FPGA board for implementing the cryptographic primitives.
  - Artix-7 FPGA equipped with ARM Cortex-A9 FPGA



- Collect your board from our office (room IF02024) once you form your group
  - One FPGA per group

## Tools: Software

- In the assignments, we will use Xilinx tools for RTL simulation and FPGA programming.
  - Xilinx Vivado 2019.1 Webpack -> Xilinx Vitis
  - For RTL simulation, you are free to use other tools (i.e., Modelsim).  
(We recommend Xilinx Vivado/Vitis)
- Installation guide will be available in course webpage.
  - Windows and Ubuntu
  - No support for MACOS  
(We recommend Windows OS)

## Tools: Hardware Description Languages (HDLs)

- In this course, we will use Verilog for assignments.
  - SystemVerilog is also fine
  - VHDL?
- Tomorrow, we will continue with a quick Verilog recap.

# Assignments

- There will be two assignments.
  - HW design and writing its Verilog code
  - RTL-level simulation/verification
  - Verification on actual FPGA
  
- **100% of your grade is from assignments.**

