Utilizing ASIP Designer for Industry Projects (BMBF), Teaching Activities, and Research

ASIP University Day 2021
17.11.2021

Lennart Reimann, M.Sc
Univ.-Prof. Dr. rer. nat. Rainer Leupers

Lennart.reimann@ice.rwth-aachen.de

Agenda

- Institute Introduction
- Teaching Activities
- BMBF Project
- Research Activities

Agenda

- Institute Introduction
- Teaching Activities
- BMBF Project
- Research Activities

ICE @ RWTH Aachen University

- Institute for Communication Technologies and Embedded Systems
  Chair for Distributed Signal Processing (DSP)
  Chair for Software for Systems on Silicon (SSS)

- Team:
  Jointly managed by two professors:
  Haris Gacanin, Rainer Leupers

  Emeriti: Gerd Ascheid, Heinrich Meyr

  Guest professors: A. Hoffmann, G. Dartmann
  ~20 PhD/Postdoc researchers
  8 non-academic staff




R&D topics in HW/SW design

ICE Spin-off history

- Cadis
  - Design and simulation of DSP algorithms
  -

Agenda

- Institute Introduction
- **Teaching Activities**
- BMBF Project
- Research Activities

Project: Embedded Processor Design and Optimization

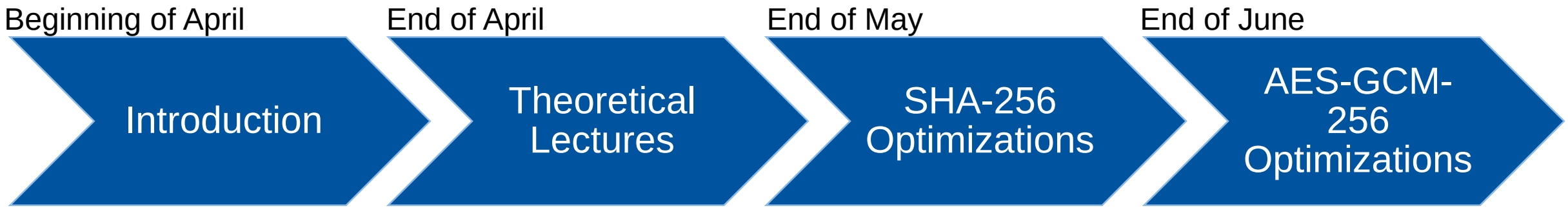
- Teaching project during summer semester
- Average of 10 participants (master course), many students start as student assistants afterwards
- Project starts with theoretical lectures about processor design
  - What is a program counter unit?
  - What is pipelining?
  - What is a register file?
- Goal: Optimize a given RISC-V processor (RV32IE) for two cryptographic algorithms:
  - SHA-256
  - AES-GCM-256
- What do the students learn?
  - How in-order processor architectures work
  - How to do:
    - Profiling and identify hotspots
    - Use ASIP Designer to modify the control flow, add instructions, add memories
    - Use Design Compiler to synthesize the generated RTL code

1. Three theoretical lectures about:
   1.

- Instruction fetch and PC increment 17.111 0 0 1 4 5.nLang (en-GB)>BDC q0.000014305 0 960 540 reWE5.89 0.626

Time Schedule

- Project starts in April and finishes at the end of July
- Project concludes with a short presentation of the individual AES-GCM optimizations and their evaluation

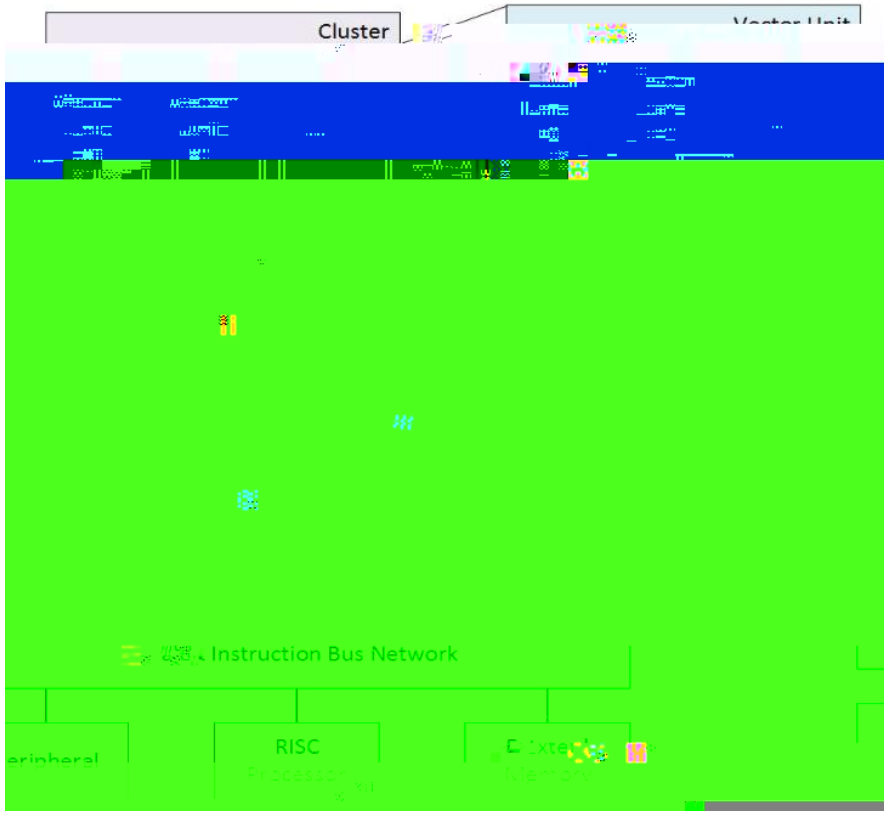


Agenda

- Institute Introduction
- Teaching Activities
- **BMBF Project**
- Research Activities

BMBF Project: ZUSE-KI-AVF

- Project goal: Developing a configurable massively-parallelizable vector co-processor architecture
  - Should run radar, lidar, image processing algorithms
  - Additionally, should speed up convolutional neural networks
- The processor architecture comes from the IMS, Hannover
  - It is controlled by a RISC-V architecture
- The ICE will provide a compiler to program the RISC-V and his co-processor (right)
- ASIP Designer is normally not used to program main & co-processor
  - New challenge
- First approach is going to use intrinsics to communicate with the co-processor
- Following steps? Vector data types? Compiler optimizations for intrinsics?



Software Verification using ASIP Designer as a DE

- Information flow analysis can give you the leakage paths of sensitive signals
  - You can either remove those leakage paths or
  - Verify that those leakages are not used for a given software

- For our elaborations we use the
  - RTL Generator
  - Generated Compiler:
    - Call Graphs
    - Hex Files
    - …
  - Our tool for the information flow analysis: QFlow

- Changes inside the hardware description are easily integrated into the compiler
  - Everything can be automated

Questions

If you have any questions related to any of the three topics, feel free to contact me:

Lennart.Reimann@ice.rwth-aachen.de