TU Graz
SCIENCE
PASSION
TECHNOLOGY

Topics for Seminar Talks

Barbara Gigerl, Rishub Nagpal

October 4th, 2023

Registration Process

1. Find a group
2. Register your group: sip-team@iaik.tugraz.at
3. Wait for the confirmation mail to get your group number
4. Choose a seminar topic
5. Register for a seminar topic: https://www.termino.gv.at/meet/b/96af1b7b54cbfe4fbfbcdb4a2bb94788-256179
6. Receive your git repositories (by email)

Deadline: Monday, 9.10., 23:59

Organizational Information

- Select a topic from the catalogue or *send us your own ideas*!
  - SoC Basics
  - SoC Security
  - SoC Environment
- By choosing a topic you agree on presenting on one of the possible dates
- Length of presentation: 20 min + 10 min
- Optional: use the template
- Submit your slides until Monday evening - we will review your presentation and send you feedback.

Preliminary Timetable

SoC Basics	8.11., 15.11., 22.11.
SoC Security	22.11., 29.11., 6.12., 13.12.
SoC Environment	13.12., 10.1., 17.1., 24.1.

SoC Basics

Topic #1

Topic #1: ASIC vs FPGAs
Hardware designs can be implemented either on an ASIC, or on an FPGA. Both techniques have specific advantages and disadvantages depending on the use case.

- What is an ASIC?
- What is an FPGA?
- How do these platforms differ?

Topic #2

Topic #2: Architecture of FPGAs
FPGAs consist of configurable logic blocks (CLBs), connected by programmable interconnects. Depending on the manufacturer, these CLBs can further be divided into logic blocks.

- What is a CLB and what role do interconnects play?
- How and when are CLBs configured?
- What are IOBs (Input Output Blocks)?

Topic #3

Topic #3: The FPGA design process
Hardware written in a HDL like Verilog needs to be translated to a netlist before it can be used on an FPGA. This translation involves amongst others synthesis, implementation and place & route.

- Describe the FPGA design process and give an overview of the involved steps.
- How can the path from a Verilog HDL design to a real FPGA implementation be described?
- What is the purpose of each step? Which things need to be considered?

Topic #4

Topic #4: SoC Bus Interconnections
Efficient communication between the components of a SoC is critical for the overall system performance.

- Which strategies to interconnect hardware modules of a SoC exist?
- Describe the basic architecture of a bus.
- Which types of bus topologies exist?
- What are the most popular bus protocols?

Topic #5

Topic #5: ARM AXI Interface
SoCs frequently use the ARM AXI interface for on-chip communication.

- What is the purpose of the AXI interface?
- Describe the AXI handshake mechanism.
- Which channels are described by the AXI specification?
- What is the purpose of AXI stream?
- Explain example usage scenarios of the AXI protocol. Choose one meaningful example.

Topic #6

Topic #6: Network-on-Chip (NoC) designs
Network-on-Chip (NoC) can be seen as an alternative over traditional bus-based architectures.

- How is the network-on-chip design paradigm characerized?
- What are the differences/advantages to bus-based architectures?
- How could a sketch of a NoC look like?

SoC Security

SoC Security

Topic #7

Topic #7: Weak point bitstream?
Security concerns for FPGAs typically evolve around the bitstream file which is used to configure the FPGA. One class of vulnerabilities are bitstream replay attacks.

- Give an overview of the bitstream lifecycle.
- Which vulnerabilities are possible in which stage of the lifecycle?
- What are bitstream replay attacks? How can they be counteracted?
- Duncan et. al, *FPGA Bitstream Security: A Day in the Life.*, In: ITC 2019 (2019).

Topic #8

Topic #8: FPGA Bitstream Encryption
Most FPGAs provide a mechanism to encrypt bitstreams. This feature protects designs from being copied, altered or reverse engineered. However, bitstream encryption isn't perfect. Research has shown that some schemes can be broken in various ways.

- Why is bitstream encryption needed on FPGAs?
- How does bitstream encryption work?
- Give an overview of existing attacks on bitstream encryption.
- Ender et. al, *The Unpatchable Silicon: A Full Break of the Bitstream Encrypton on Xilinx 7-Series FPGAs*, In: USENIX'20 (2020).

Topic #9

Topic #9: Remote Power Attacks on FPGAs
There is an increasing interest in sharing FPGAs across multiple users simultaneously in the cloud, enabling remote power analysis attacks. In these attacks, an adversary, that shares the FPGA with the victim, can instantiate sensors to monitor voltage fluctuations of the shared power distribution networks.

- What is remote power analysis?
- Which techniques to implement on-chip voltage sensors exist?
- What are possible countermeasures?
- Martinez-Rodriguez et. al, *SoK: Remote Power Analysis*, In: ARES 2021 (2021)
- Moini et. al, *Voltage Sensor Implementations for Remote Power Attacks on FPGAs*, In: ACM Trans. Reconfigurable Technol. Syst. 2023 (2023)

Topic #10

Topic #10: Fault attacks on FPGAs
FPGAs are vulnerable to fault attacks. In this attacks, incorrect system behavior is, for example, triggered by voltage drops.

- Explain the basics of fault attacks.
- Which attack scenarios for fault attacks on FPGAs exist?
- Krautter et. al, *Remote and Stealthy Fault Attacks on Virtualized FPGAs*, In: DATE 2021 (2021)
- Lohrke et. al, *Key Extraction Using Thermal Laser Stimulation*, In: CHES 2018 (2018)
- What are possible countermeasures?

Topic #11

Topic #11: EM Side-Channel Attacks on SoCs
SoCs are vulnerable to ElectroMagnetic (EM) side-channels. In this attacks, the electromagnetic radiation of a device is measured during its computation, which reveals side-channel information that ca nbe exploited in SCA.

- Explain the basics of EM side-channel attacks.
- Longo et. al, *SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip*, In: CHES 2015 (2015).
- What are possible countermeasures?

Topic #12

Topic #12: Security by Obfuscation for FPGAs
Obfuscation methods are often applied by vendors to protect FPGAs from reverse engineering.

- What is security by obfuscation?
- How can it be achieved?
- Labafniya et. al, *An Obfuscation Method Based on CFGLUTs for Security of FPGAs*, In: ISeCure 2021 (2021).
- Karam et. al, *Robust Bitstream Protection in FPGA-based Systems through Low-Overhead Obfuscation*, In: ReConFig 2017 (2017)

Topic #13

Topic #13: Hardware Trojan Attacks in FPGAs
Hardware trojans pose serious security concerns. In recent years, researchers showed that FPGAs are vulnerable to such attacks.

- What is a hardware trojan and to what extent are they dangerous?
- Wang et. al, *Hardware Trojan Attack in Embedded Memory*, In: JETC, Volume 17, Issue 1 (2021).
- Which countermeasures exist?

Topic #14

Topic #14: Reverse Engineering ICs
Vendors of ICs invest significant effort to counteract attempts to reverse engineer their product. Still, there exist several approaches to reverse engineer ICs.

- What are the general steps when reverse engineering an IC?
- Which methods exist?
- Azriel et. al, *A survey of algorithmic methods in IC reverse engineering*, In: JCE 2021 (2021).
- What are their limitations?
- Which methods exist specifically for FPGAs and ASICs?

Topic #15

Topic #15: Security Co-Processors
Sometimes it's necessary to keep things separate to get both security and performance. Security co-processor can do that.

- When to use a security co-processor?
- How do they communicate?
- How do they perform in comparison?
- Which guarantees can they give?
- Steinegger et. al, *A Fast and Compact RISC-V Accelerator for Ascon and Friends*, In: CARDIS 2020 (2020).
- Which other use cases are there besides security for co-processors?

SoC Environment

SoC Environment

Topic #16

Topic #16: Alternative HDLs
Today, most applications are still traditionally written in Verilog, System Verilog or VHDL. However, there exist many more alternative HDLs, including Bluespec and Chisel.

- What alternatives to traditional HDLs exist?
- Using code snippets, what are their characteristics?
- What are the major road blocks of replacing traditional HDLs?

Topic #17

Topic #17: Assertion-based Hardware Verification
Functional validation has long been a major difficulty in digital design. Assertion-based verification (ABV) is a technique which is often applied to tackle this challenge.

- What is the main principle ABV?
- What is the advantage/disadvantage?
- Give an example.
- Witharana et. al, *A Survey on Assertion-based Hardware Verification* ACM Computing Surveys (2022).

Topic #18

Topic #18: Formal Verification in Hardware Design

The correct design of complex hardware represents a serious challenge. In recent years, formal methods have emerged as an alternative approach to ensure the quality of hardware designs.

- What are formal methods? What are the challenges of applying a formal verification approach to a hardware design?
- What is the advantage of formally verifying a hardware design compared to traditional techniques?
- Give an example.
- Chauhan et. al, *Verifying IP-Core based System-On-Chip Designs* Twelfth Annual IEEE International ASIC/SOC Conference (1999).
- Kern et. al, *Formal Verification in Hardware Design: A Survey* ACM Trans. Design Autom. Electr. Syst. (1999).

Topic #19

Topic #19: High Level Synthesis
The traditional way of developing hardware is often cumbersome, error-prone and requires the usage of HDLs. High-level synthesis (HLS) aims at generating synthesizable designs from high-level specifications directly.

- What is high-level synthesis?
- Which toolchains exist for high-level synthesis of hardware?
- Ye et al., *ScaleHLS: A New Scalable High-Level Synthesis Framework on Multi-Level Intermediate Representation*, In: HPCA 2022 (2022)

Topic #20

Topic #20: FPGAs in Space
FPGAs have been used in space for more than a decade. In order to be feasible for space applications, FPGAs need to fulfill a row of requirements, including radio tolerance.

- To which extent are FPGAs suitable for space?
- What are the main challenges when using FPGAs in space?
- Which manufacturers provide such technologies?

Topic #21

Topic #21: Open-Source Hardware
Industry relies mostly on proprietary tools to handle hardware designs, which can be cumbersome and very expensive. Recently, there has been several initiatives to make hardware design more open-source.

- What are the problems of proprietary/closed-source tools for hardware development? Which of these problems could be solved with open-source?
- Give examples of areas related to hardware where open-source concepts are already applied.
- Yosys / SymbiYosys represent powerful open-source synthesis tools. What are their limitations? How to use them? Give a short demo!

Topic #22

Topic #22: FaaS - FPGA-as-a-Service
FPGAs are increasingly being used in cloud infrastructures allowing users to remotely access and use FPGAs, which is often called FPGA-as-a-Service (FaaS).

- What is the idea behind FaaS? How is a typical FaaS architecture structured?
- How is security in FaaS provided?
- Pundir et. al, *What is All the FaaS About? - Remote Exploitation of FPGA-as-a-Service Platforms* HPCA 2022 (2022).

Topic #23

Topic #23: Soft Cores and ARM/RISC-V Processors
In a SoC, processors are often placed as a standalone unit, but can also be delivered as a HDL design which is then synthesized and used as an FPGA configuration.

- What are soft cores and what is the difference to hard cores?
- Which ARM soft-cores exist?
- Which RISC-V soft-cores exist?

Topic #24

Topic #24: Booting Linux
You press a button and suddenly there's a shell. How did the device get there?

- How does Linux boot on ARM/RISC-V/x86?
- Which role plays the BIOS/UEFI?
- What is Secureboot and what can it do?
- What is a bootloader and why is there one called the Berkeley Bootloader (BBL)?

Topic #25

Topic #25: FPGAs for Medical Applications
Many medical use cases require real-time analysis of data. FPGAs provide a convenient way to accelerate this.

- Give a few examples of use cases of FPGAs in medicine.
- What is the big advantage of using FPGAs for processing medical data?
- Pick a specific use case and describe it in more detail.
- Kulkarni et al., *Reconfigurable Probabilistic AI Architecture for Personalized Cancer Treatment*, ICRC 2019 (2019).
- Arefeen et al., *Real-time, data-driven system to learn parameters for multisite pacemaker beat detection*, ACSSC 2017 (2017).

Topic #26

Topic #26: FPGAs and Neural Networks / ZynqNet
FPGAs and SoCs are often used for neural computing, for example ZynqNet, which is based on the Zynq SoC.

- Why are neural networks on FPGAs and SoCs so popular?
- What is the application area?
- Describe ZynqNet.
- Gschwend, *ZynqNet: An FPGA-Accelerated Embedded Convolutional Neural Network* (2016).

Topic #27

Topic #27: Energy Efficient SoCs
FPGAs and SoCs are often used for high-performance computing, but also in restricted areas requiring low power, including mobile and IoT.

- In which areas is it critical to have an energy efficient SoC?
- How can energy efficiency be achieved?
- Which methods exist to estimate the power consumption of a SoC?
- Gschwend, *Energy Efficient Power Distribution on Many-Core SoC* VLSID 2019 (2019).