Universität Stuttgart

Our Research Foci and Your Opportunities

Ilia Polian
Hardware-oriented Computer Science

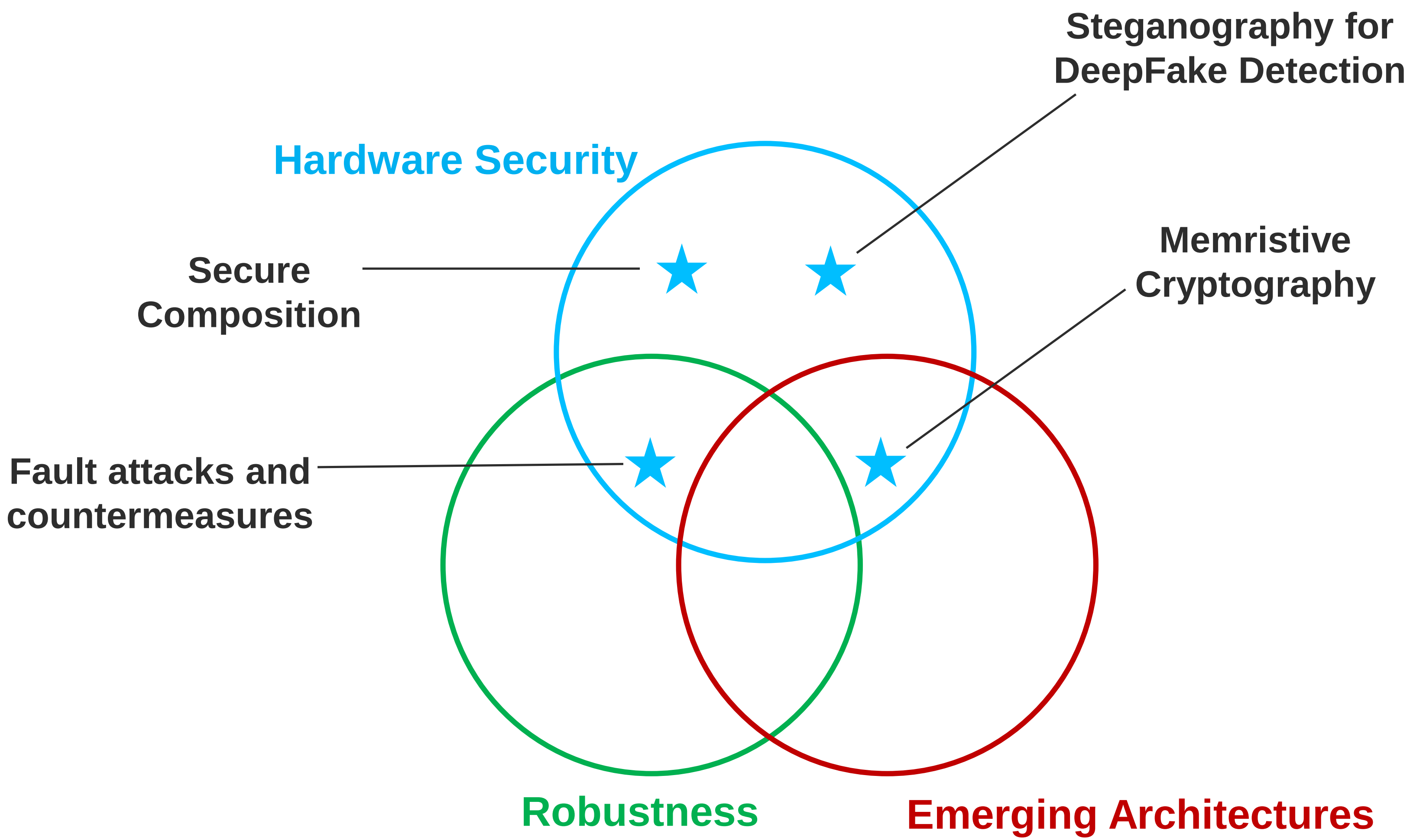
June 2020

Why This Presentation?

- Lectures must cover (somewhat) well-established knowledge; new research results often lack maturity to be included into regular teaching.
- We want to show you what we are working on now.
  - The topics change over time; this material is from 2020.
- Useful especially for those of you who are planning to focus in our area, write a thesis with us, etc.
- Brief sketches rather than fully-fledged coverage, but providing references to further probe yourself.

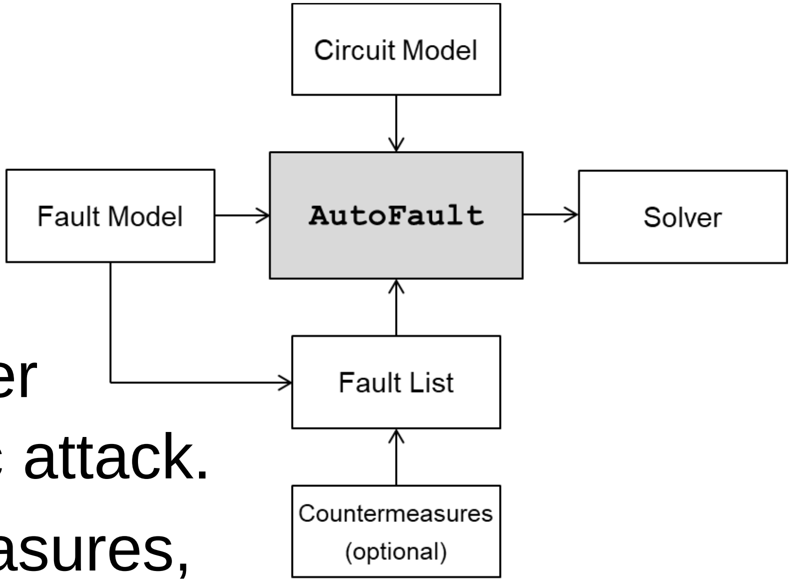
Outline

1. **Topics related to hardware-oriented security**
2. Topics related to emerging technologies
3. Topics related to robustness
4. Connection to our teaching program



hocos
hardware-oriented computer science

Fault Attacks

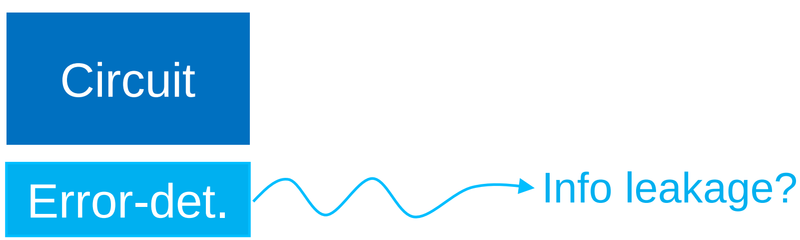


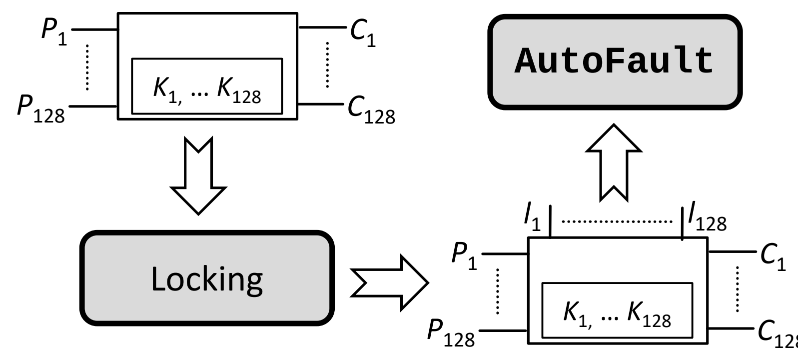
- Automatic construction of fault attacks.
  - Tool **`AutoFault`:** Reads cipher description, produces algebraic attack.
  - Future: Incorporate countermeasures, protection against other attacks.
- Security-oriented error-detecting codes.
  - Compact protection codes, Rabii-Keren codes (with correction), codes incorporating randomness.
- New attacks: Statistical Impossible Fault Attack.

hocos
hardware-oriented computer science

Secure Composition

- How to protect circuits against fault attacks, side-channel attacks, counterfeiting, at the same time?
  – Does error-detecting circuitry leak information?
  – Do fault attacks work on circuits with masking, locking, or further countermeasures against other threats?

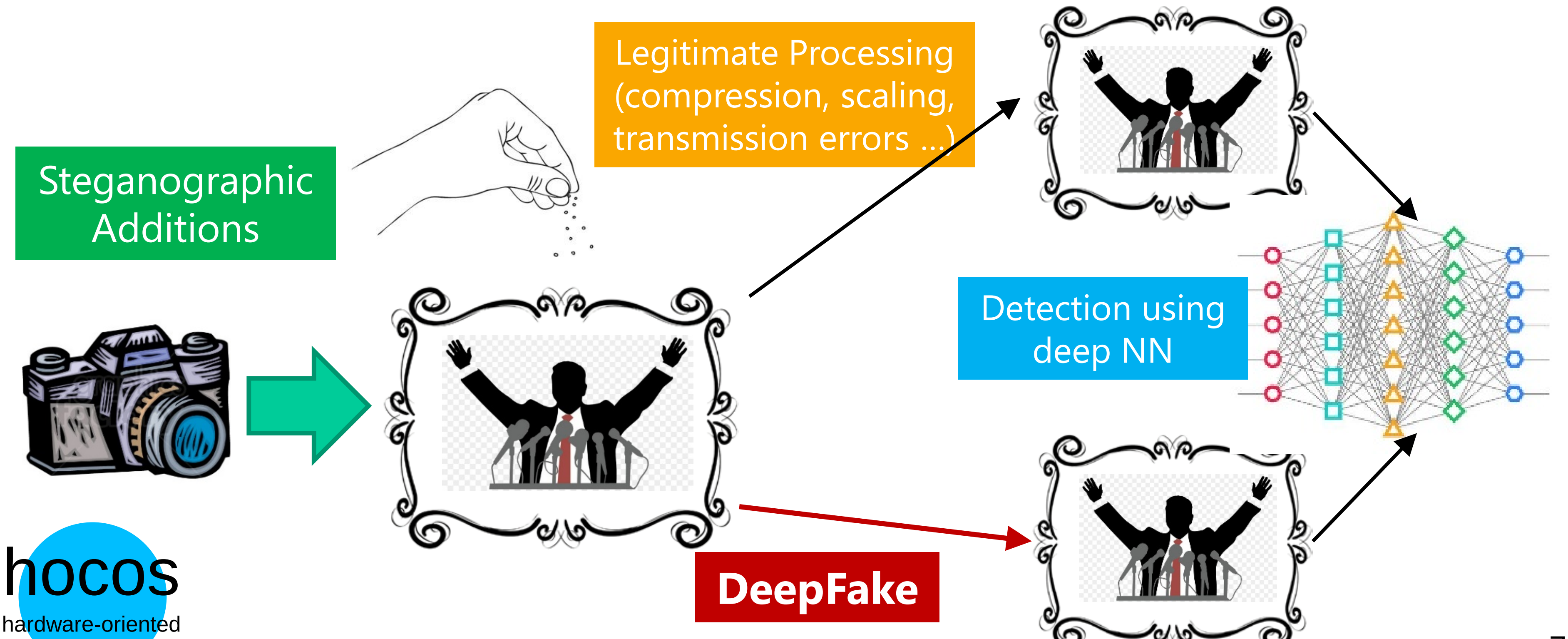




hocos
hardware-oriented computer science

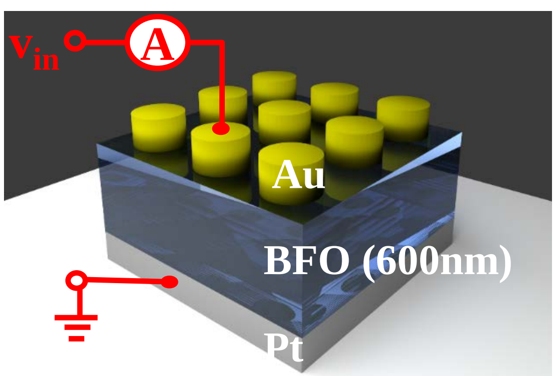
DeepFake Detection

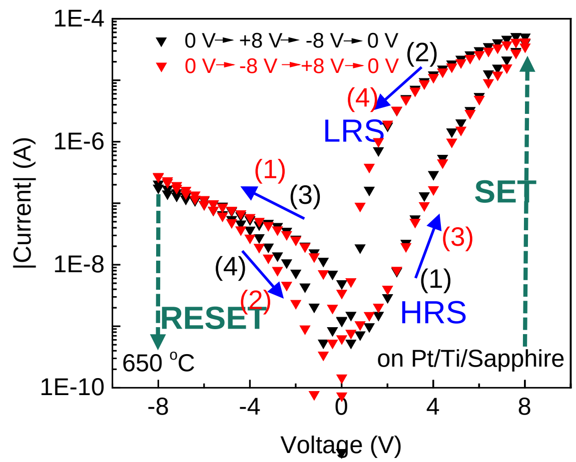
- DeepFake: Authentically looking fake video.
  - E.g., face-swap, lip-synchronization, puppet-master.
- Detect, combining deep-learning + steganography.
  - Challenge: Video can be modified in legitimate ways!



Memristive Cryptography

- How to implement crypto functions using memristors (emerging nano-devices)?
  - Focus on novel electroforming-free BFO memristors.
  - Also investigate physical attacks + countermeasures.





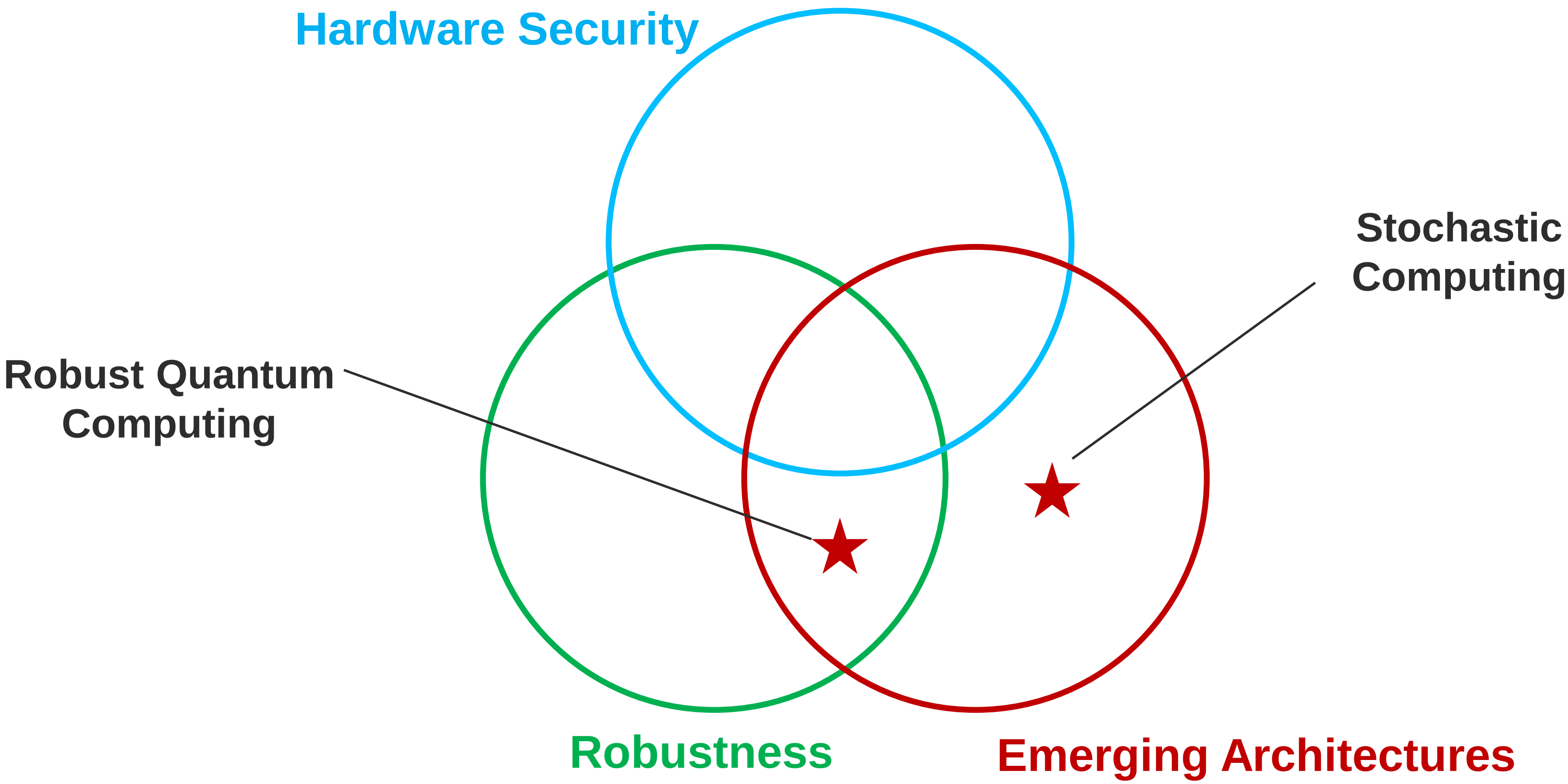
hocos
hardware-oriented
computer science

To Probe Further…

- AutoFault: https://www.doi.org/10.1109/FDTC.2019.00012
- Error-detecting codes: https://doi.org/10.29007/w37p
- SIFA: https://www.doi.org/10.13154/tches.v2018.i3.547-572
- Information leakage: http://www.proofs-workshop.org/2019/doc/PROOFS2019-Paper1.pdf
- Camouflaging, locking, obfuscation:
  https://dl.acm.org/doi/10.1145/2508859.2516656
  https://ieeexplore.ieee.org/document/8203496
  https://link.springer.com/article/10.1007/s10836-019-05800-4
  https://ieeexplore.ieee.org/document/7546854
- Steganography: https://doi.org/10.2352/ISSN.2470-1173.2020.4.MWSF-076
- DeepFake: https://doi.org/10.1109/AVSS.2018.8639163
- Memristors: https://doi.org/10.1109/IVSW.2019.8854394

Outline

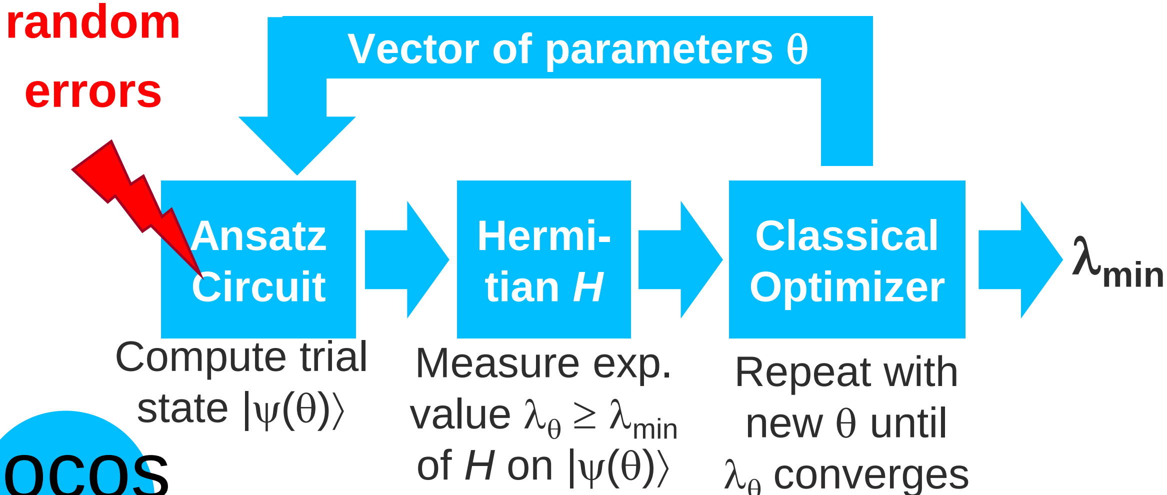
1. Topics related to hardware-oriented security
2. **Topics related to emerging technologies**
3. Topics related to robustness
4. Connection to our teaching program

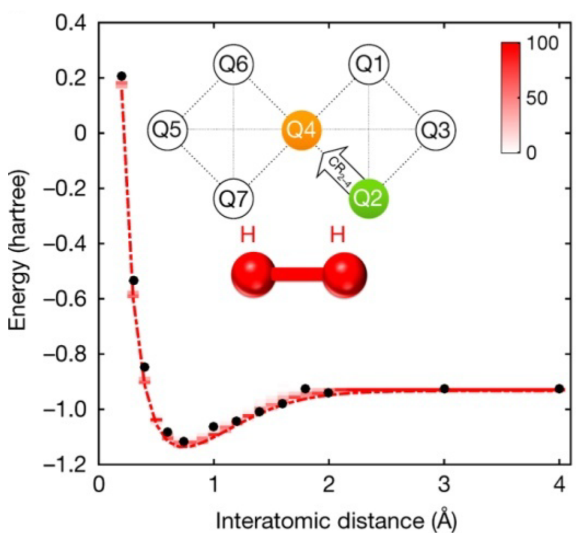


hocos
hardware-oriented computer science

Robust Quantum Computing

- Transpilation of quantum circuits: map a circuit to a quantum architecture with known noise levels.
- Investigate and improve robustness of “noisy intermediate-scale quantum” (NISQ) circuits.
  - E.g., Variational Quantum Eigensolver.

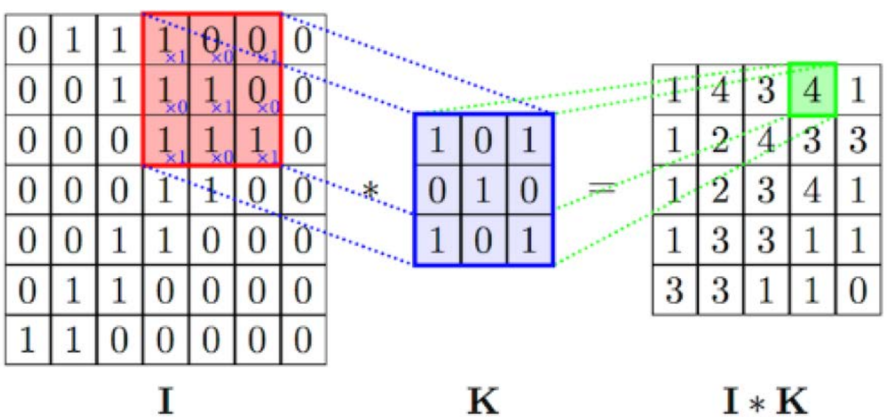


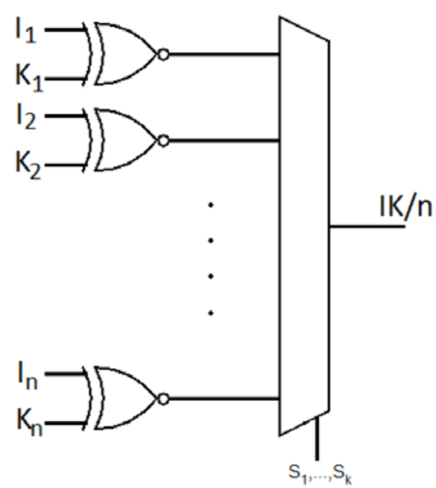


hocos
hardware-oriented computer science

Stochastic Computing

- Stochastic computing for multimodal tasks, e.g., image/video classification.
- Robustness of stochastic circuits under errors.
- Biomedical systems using stochastic computing
  – E.g., X-ray image segmentation by convolutional NNs.





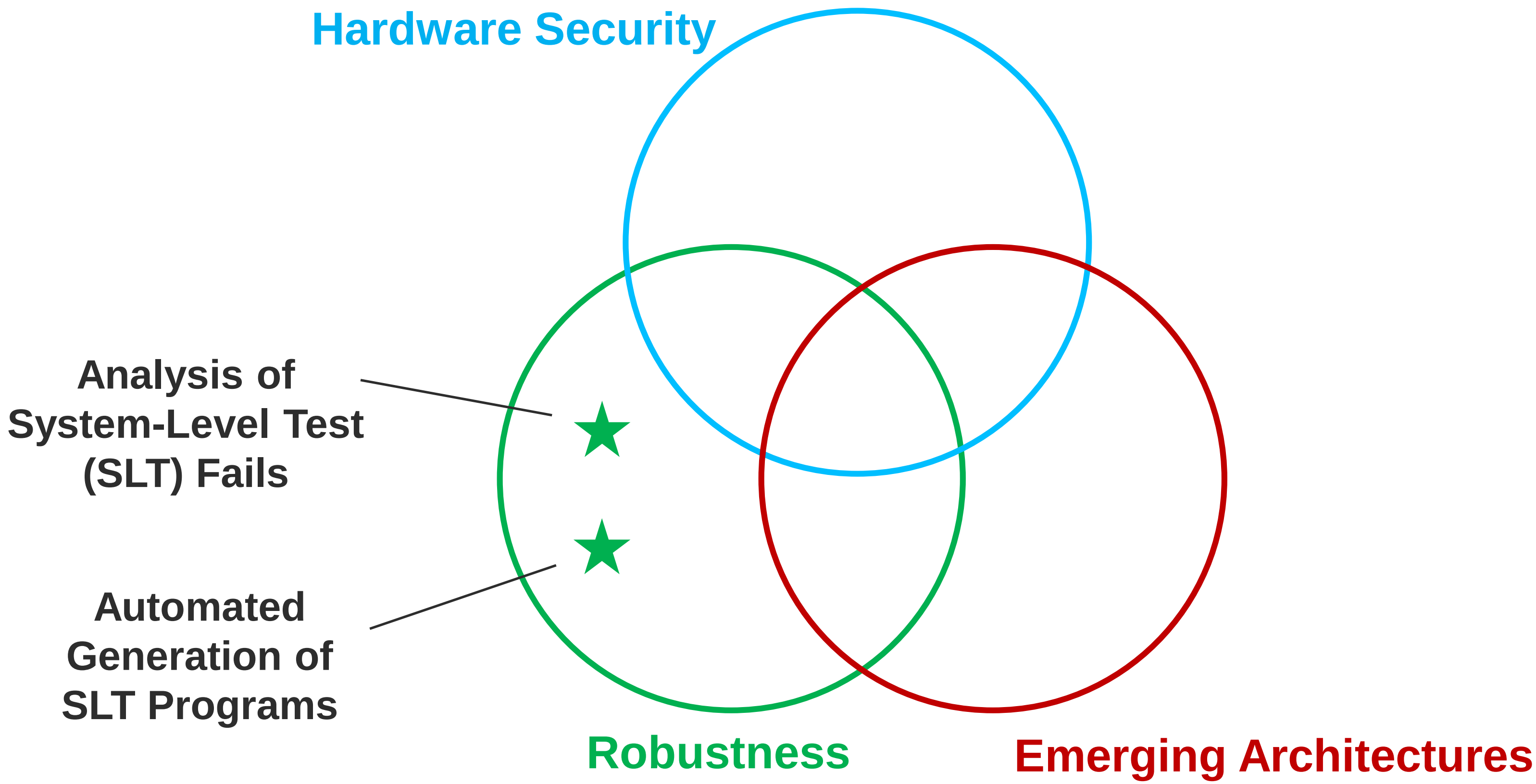
hocos
hardware-oriented computer science

To Probe Further:

- QC transpilation: https://arxiv.org/pdf/2002.09783.pdf , https://arxiv.org/pdf/1809.02573.pdf , https://arxiv.org/pdf/1712.04722.pdf
- QC robustness: https://doi.org/10.1038/nature23879 , https://doi.org/10.1038/ncomms5213
- SC basics: https://doi.org/10.1109/TCAD.2017.2778107
- SC under errors: https://doi.org/10.1145/2990503
- SC-based NNs: 10.1109/ICRC.2019.8914706
- Multimodal NNs: https://cs.stanford.edu/people/karpathy/cvpr2015.pdf
- X-ray segment.: https://doi.org/10.1109/CHASE.2017.59

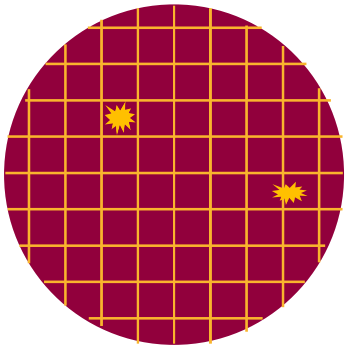
Outline

1. Topics related to hardware-oriented security
2. Topics related to emerging technologies
3. **Topics related to robustness**
4. Connection to our teaching program



hocos
hardware-oriented
computer science

System-Level Test (SLT)



Manufactured circuit with defects

Post-manufacturing test

System-level test
SLT-unique fails reported

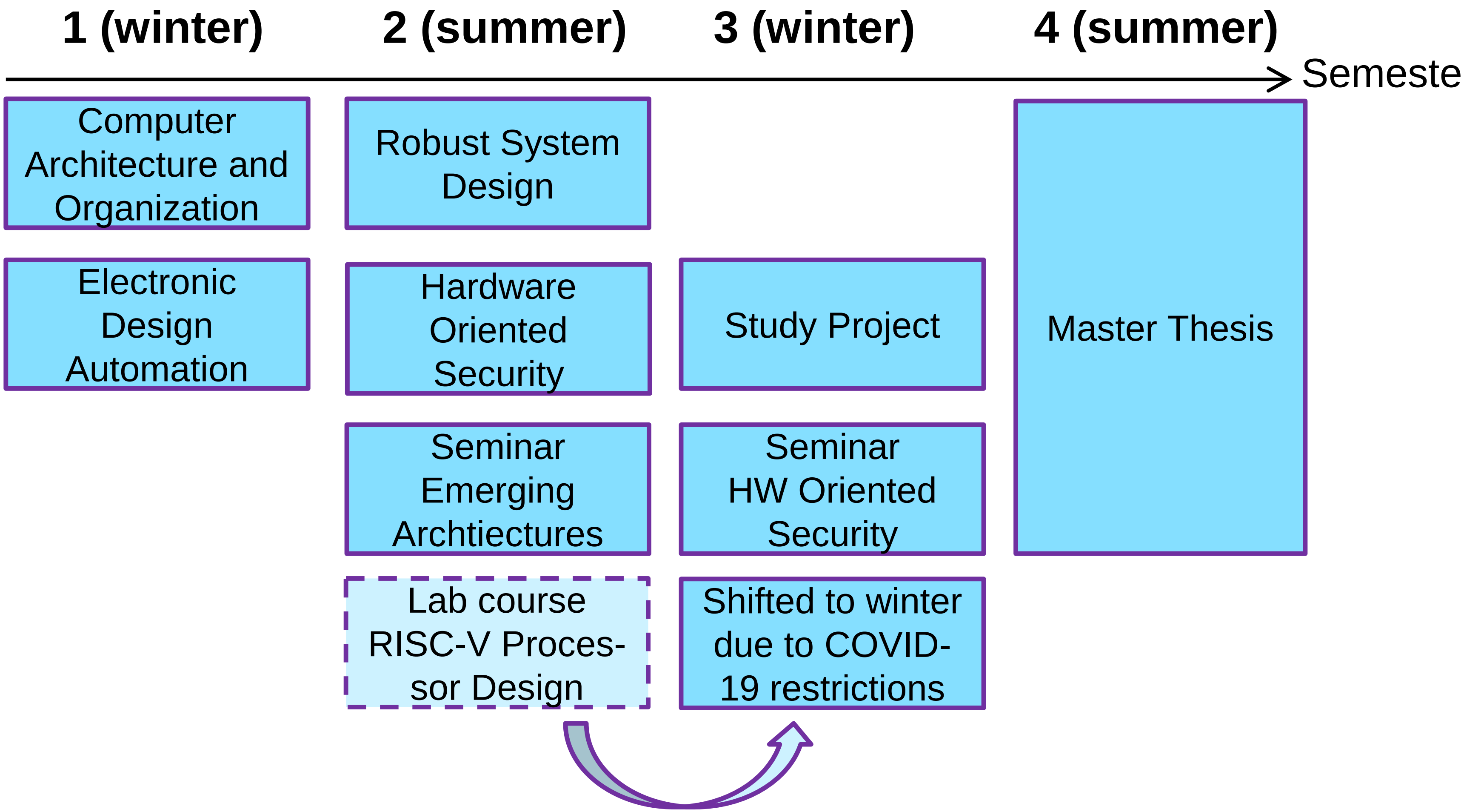
- Why are there SLT-unique fails, and how to prevent them?
  - Complex defects? Coverage holes? System-level interactions?
- How to generate SLT programs with desired characteristics?
  - E.g., software-based stress test from high-level architecture models.
- How to incorporate self-awareness of SoC-under-test?

Outline

1. Topics related to hardware-oriented security
2. Topics related to emerging technologies
3. Topics related to robustness
4. **Connection to our teaching program**

hocos
hardware-oriented
computer science

Our Teaching Offer



hocos
hardware-oriented
computer science

Teaching Offer Details

- This is a generic plan; we cannot guarantee it for each semester (we may have to skip some courses).
- We can also offer new courses, e.g., other seminars.
- CAO and EDA are more general-interest lectures; HOS and RSD are closer to our own research.
- RISC-V Processor Design is a new lab course. It requires CAO. Other courses have no prerequisites.
- If you have to choose between a seminar and a project, we recommend taking a seminar.
- Take some of our courses before asking for a project.

Thesis, Projects & Co

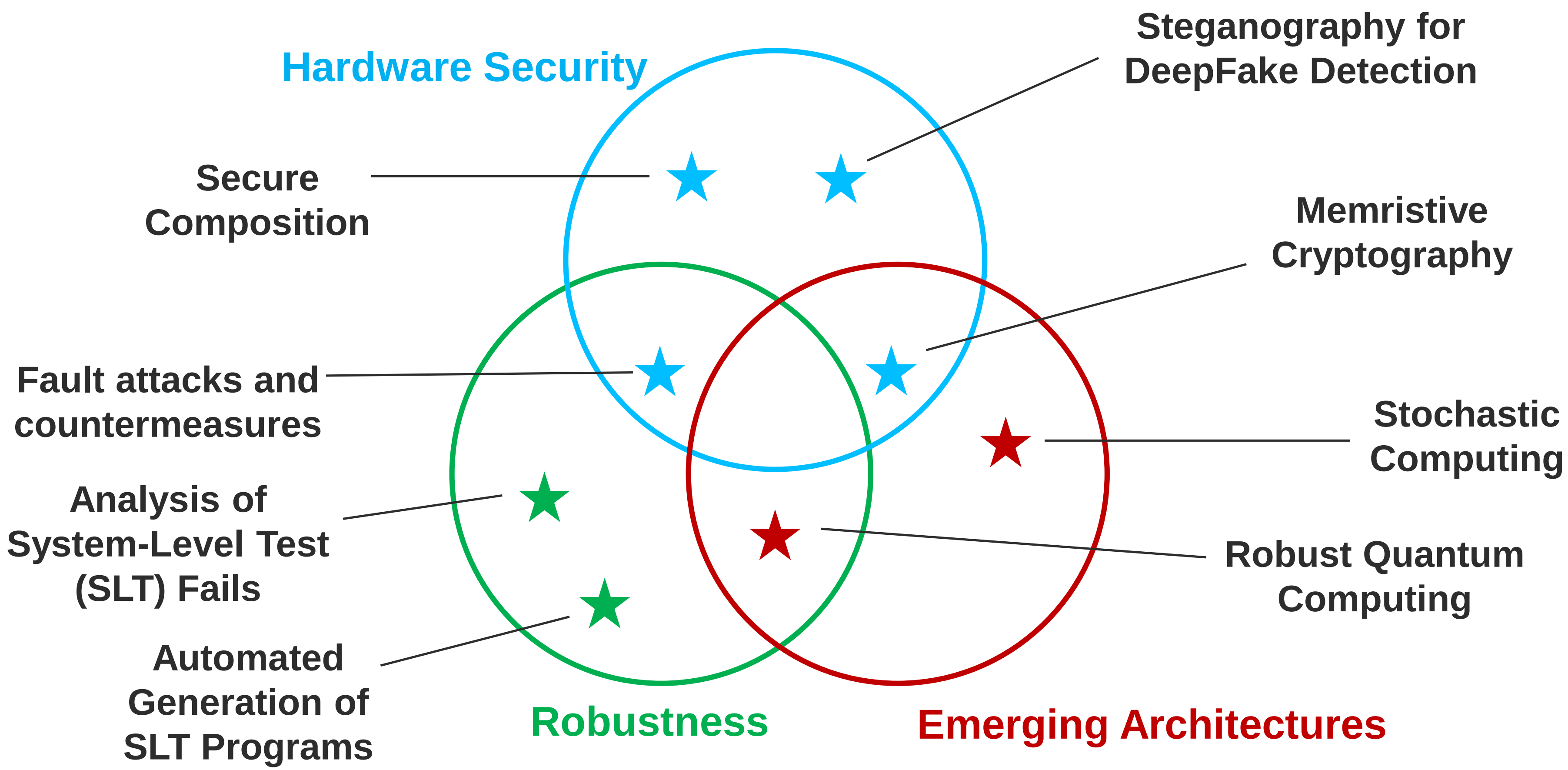
- We do not have a list of pre-defined topics.
  - We want to define your dream topic (and no, we cannot supervise a topic that we do not understand ourselves).
  - Fill out the questionnaire on the HOCOS website and send it with your transcript of records.
- You are encouraged to talk to group members if a topic is of interest to you (see list on next slide).
  - We expect some pre-existing knowledge on that topic, e.g., HOS for security, Prof. Leymann's / Prof. Barz's lecture for quantum, deep-learning lecture for DeepFake.
  - We prefer people who did a seminar with us (your thesis topic can but doesn't have to extend your seminar topic).

Your Main Contacts

- Mael Gay: AutoFault, Error-detecting codes, fault vs. side-channel attacks, masking.
- Devanshi Upadhyaya: AutoFault, locking/obfusc.
- Swaroop Shankar Prasad: Stego, DeepFake.
- N.N. (we are currently hiring): Memristors.
- Sebastian Brandhofer: Quantum circuits.
- Florian Neugebauer: Robust stochastic circuits.
- Roshwin Sengupta: Stochastic multimodal NNs.
- Nourhan Elhamawy: System-level test.

Recent Master Thesis Topics

- Preliminary Hazard Analysis and Fault Handling Methods in Solar Thermal Power Plant Control Systems.
- Hardware Optimization of Code-based Post-quantum Cryptosystem based on Quasi-dyadic Goppa Codes.
- Framework for mapping a given neural network onto a stochastic circuit.
- FPGA-Based Elliptic Curve Fault Attacks.
- Detection of Malicious Spatial-Domain Steganography over Noisy Channels Using Convolutional Neural Networks.
- Implementation and Analysis of Stochastic Convolutional Neural Network (LeNet-5) on FPGA.
- Evaluating Robustness of Stochastic Neural Networks against Adversarial Learning Attacks.



hocos
hardware-oriented
computer science