

Securing Nano-Circuits Against Optical Probing Attack

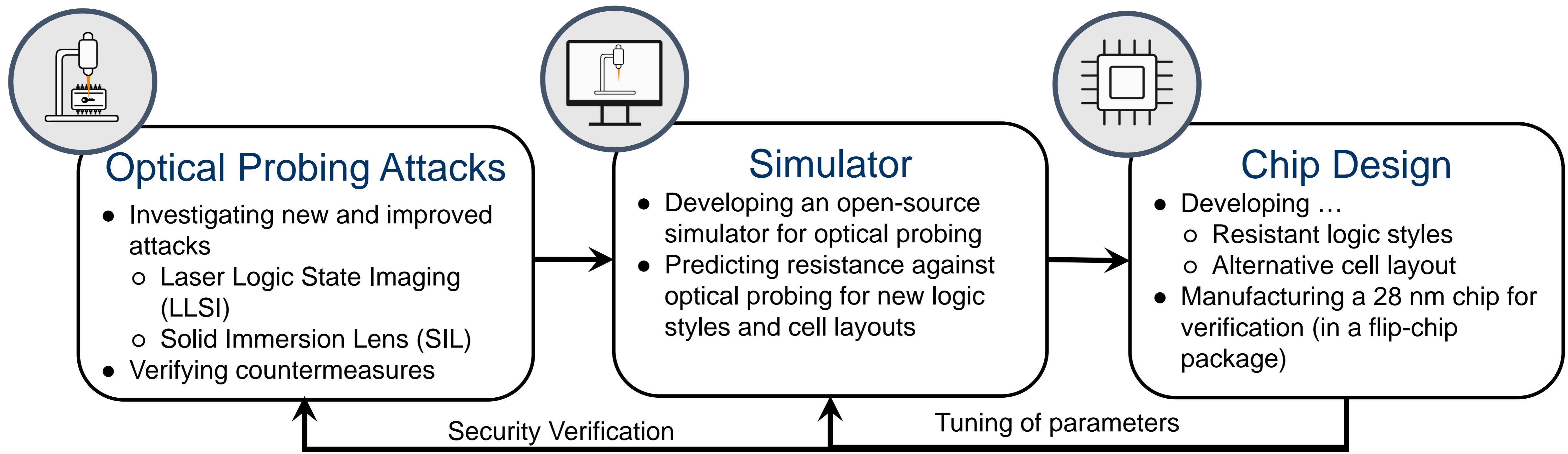
Sajjad Parvin ^U Advisor: Rolf Drechsler ^{U, ‡}

^UInstitute of Computer Science, University of Bremen, Germany

[‡]Cyber-Physical Systems, DFKI GmbH, Germany

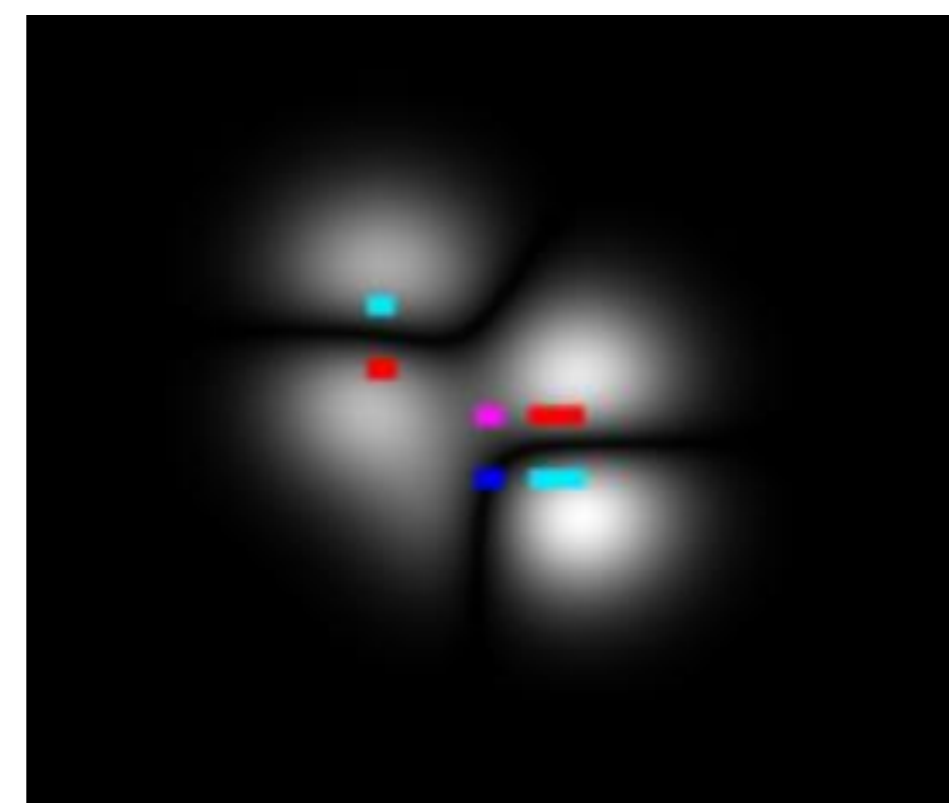
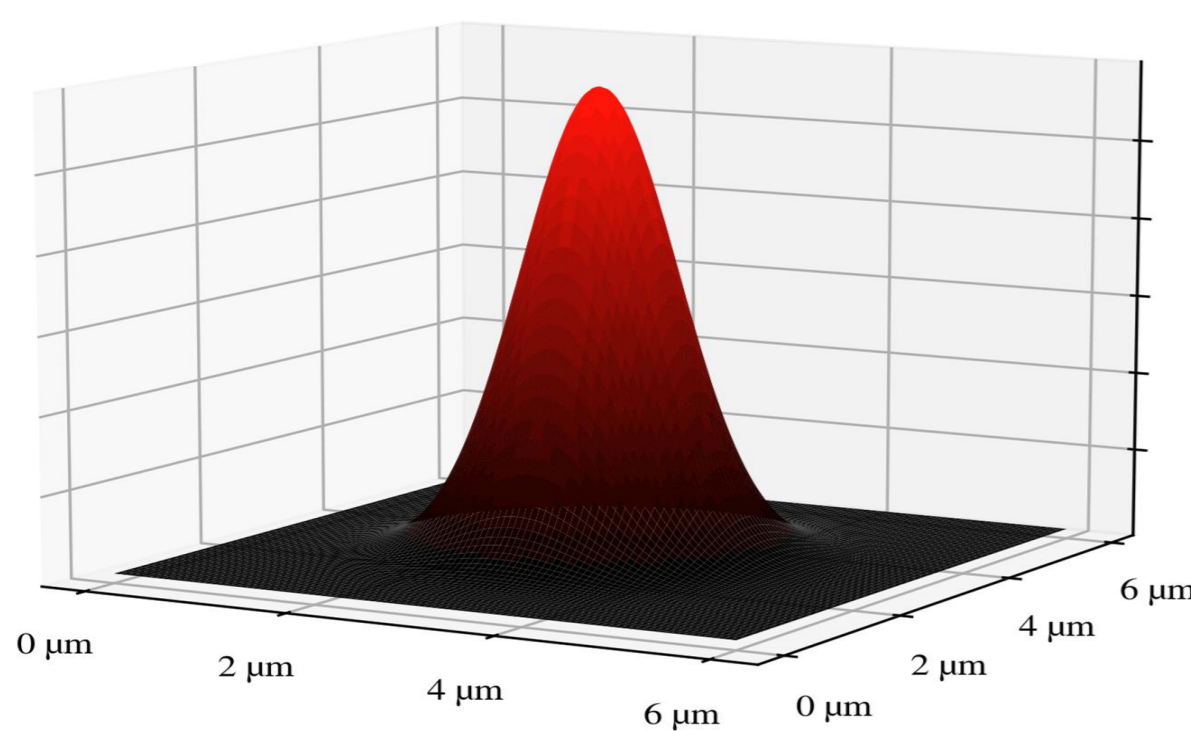
Email: [parvin, drechsler]@uni-bremen.de

PROJECT SUMMARY



OP Simulation

- Model laser beam as Gaussian distribution
 - Width depending on wavelength of the light source and numerical aperture of the lens
- Model chip layout as polygons
 - Modulation capacity depending on voltage, transistor type, etc.
- Calculate 2-D convolution of laser point spread function and layout polygons

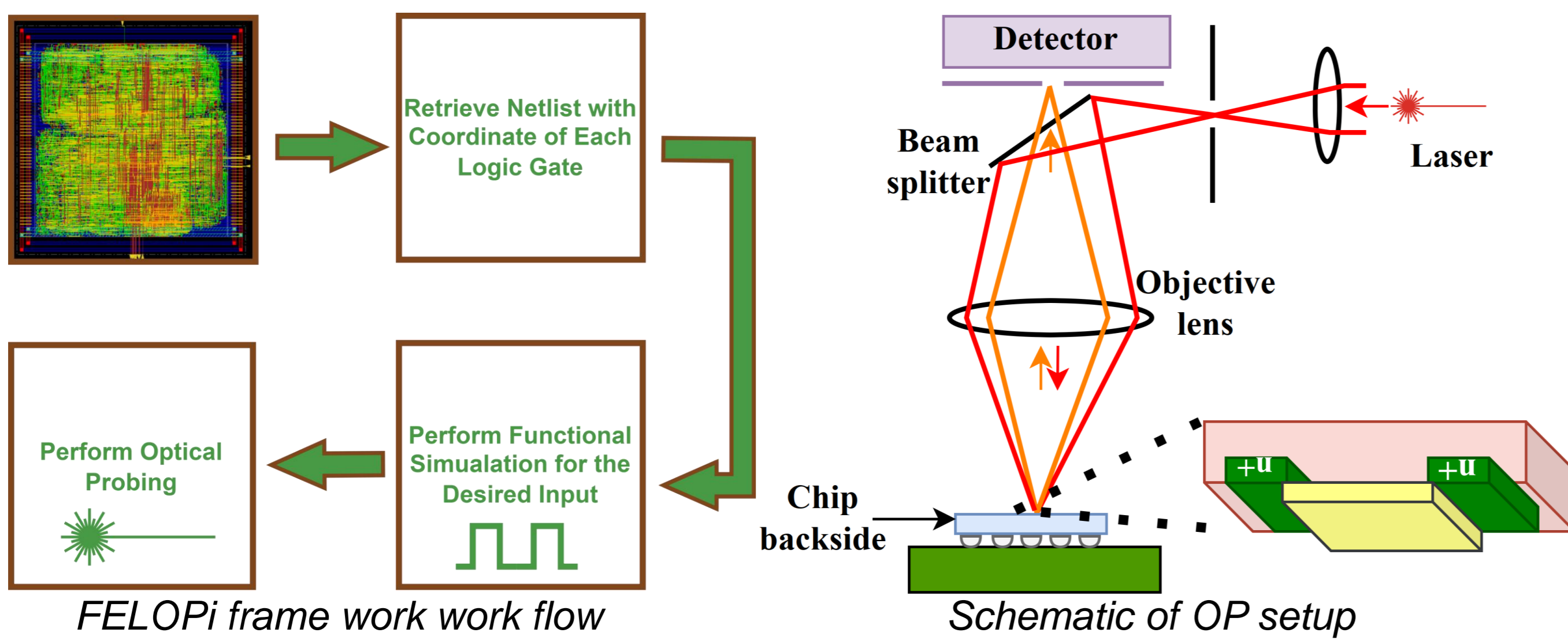


Laser point spread function for $\lambda=1320$ nm, $NA=0.71$

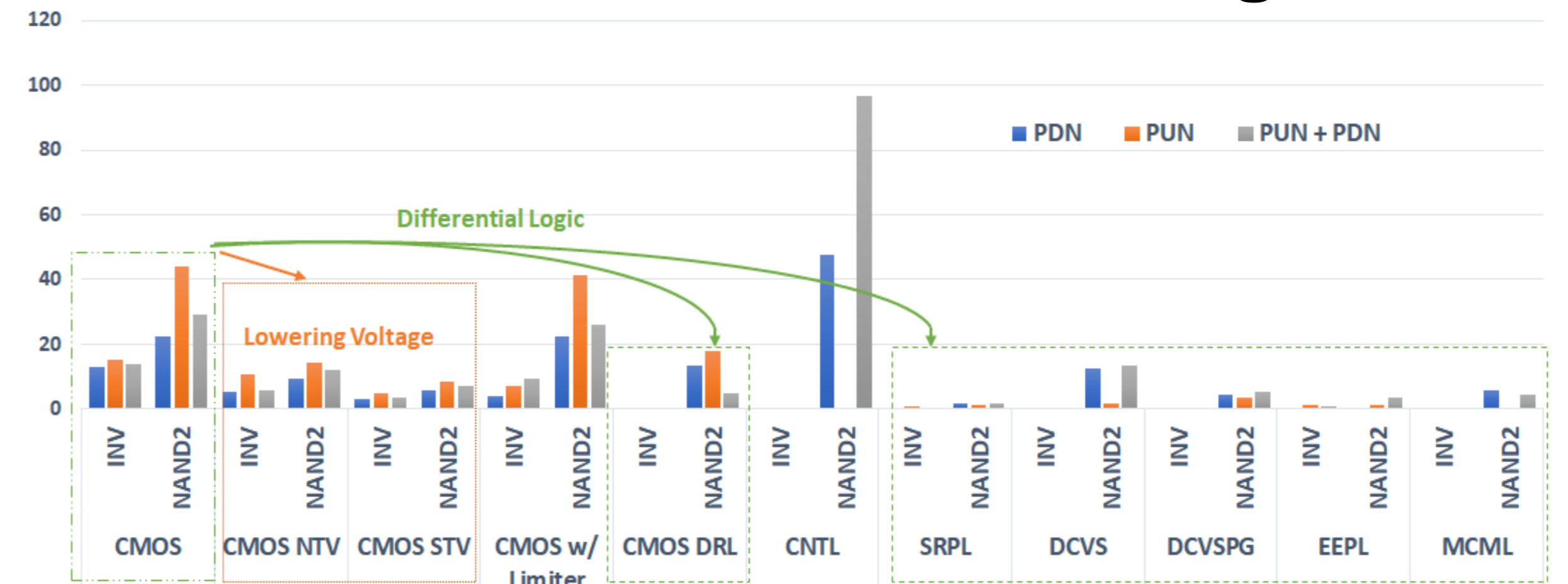
Simulated EOFM image with layout overlay at $\lambda=1320$ nm, $NA=3.3$

SIMULATOR

Scaling Up OP Simulation

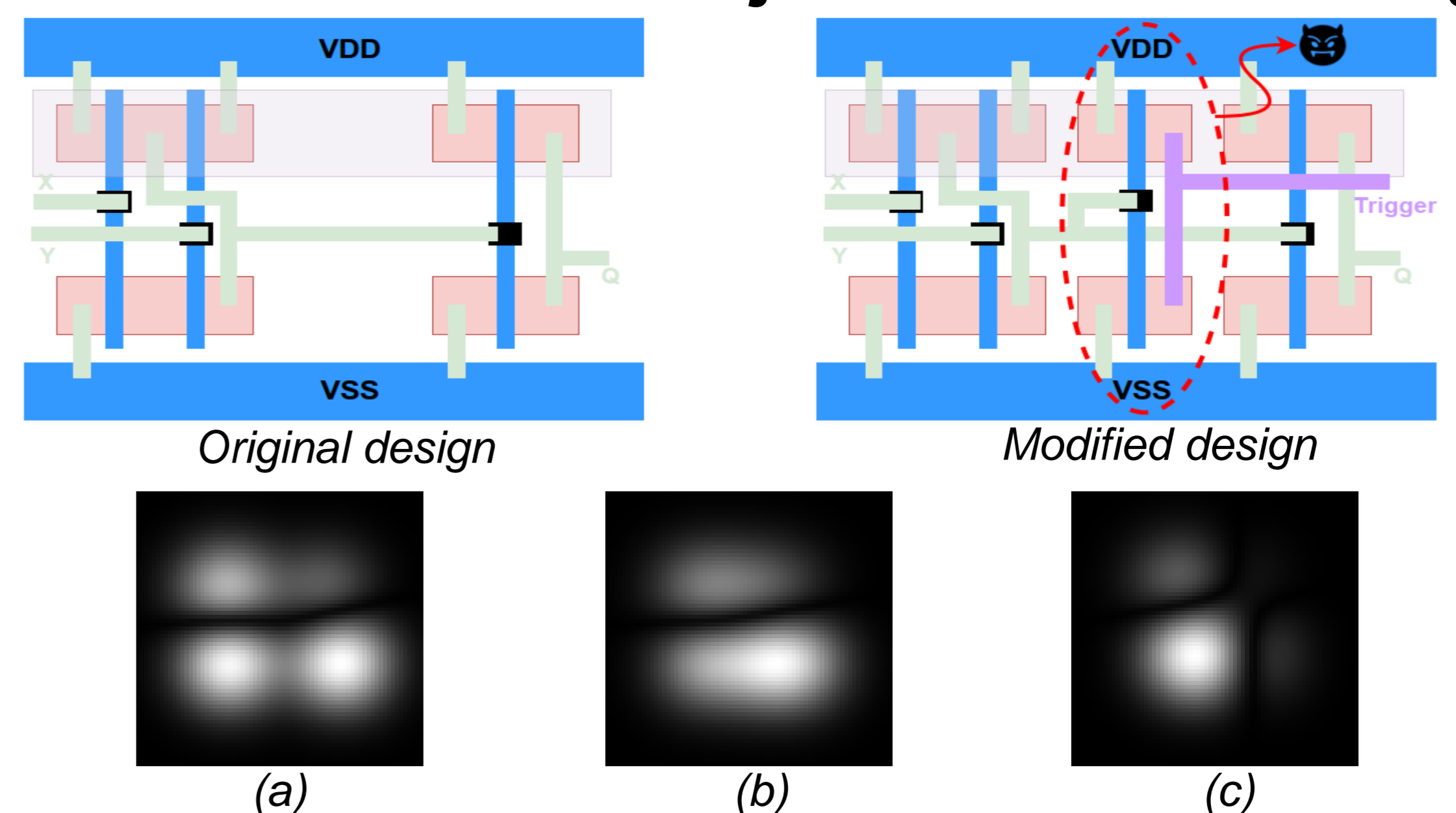


Use Case: OP Robust Circuit Design



- Simulation of static optical probing on different logic styles
 - A circuit can become more robust toward optical probing by using dual-rail logic (DRL) gates
 - Other design techniques like supply voltage reduction can also help to reduce the SNR

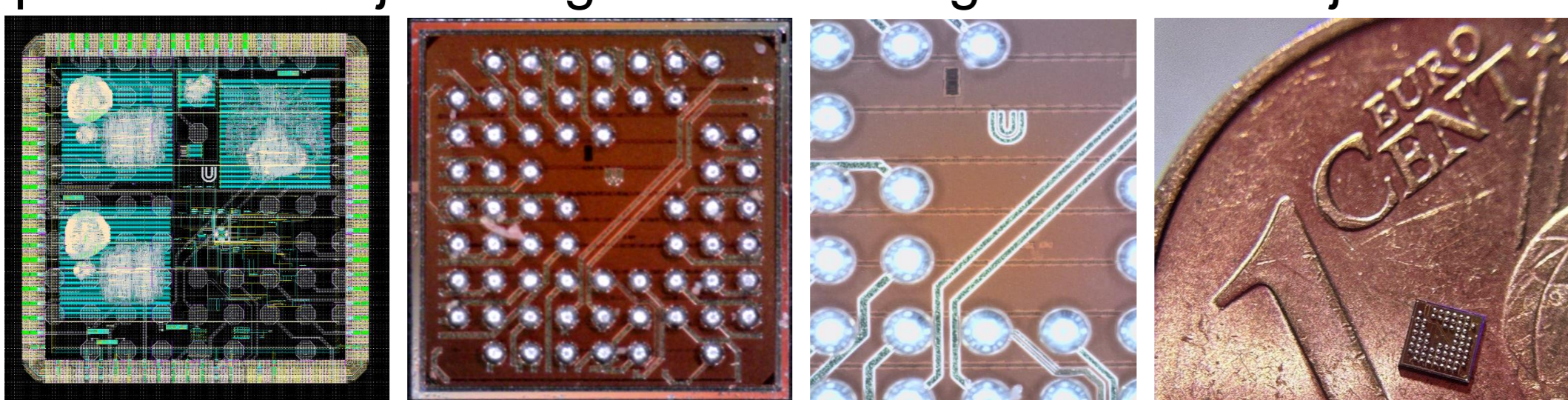
Use Case: Hardware Trojan Detection Using OP



a) OP simulation of original design, b) OP simulation of modified design, c) difference between modified and original design OP simulation results

CHIP DESIGN

- More than 300 individual test structures
 - Single transistors, single logic gates, etc.
- Several RISC-V cores + part of AES core + SRAM block
 - Designed with our secure logic gates and standard cell library.
- Implemented trojans: digital and analog hardware trojans



OP ATTACK

- The designed chip will be used to perform OP attack on the chip.
- To verify our developed simulator results
 - Accuracy of our simulator
 - Evaluate our proposed OP countermeasures
 - Hardware trojan detection using OP setup
- Perform novel OP attacks
 - LLSI analysis
 - OP attack with the aid of Solid Immersion Lens
- Investigate the effect of metal layers on OP reflection



PUBLICATION

- Published 7** conference papers
 - DATE, ASP-DAC, ISVLSI, etc.
- Best paper award at ISVLSI 2023**
- Under review publications
 - 2X Journals
 - 1X Conference paper
- Parvin, Sajjad**, et al. "Toward optical probing resistant circuits: A comparison of logic styles and circuit design techniques." *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2022.
- Parvin, Sajjad**, et al. "FELOPi: A Framework for Simulation and Evaluation of Post-Layout File Against Optical Probing." *2023 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2023.
- Parvin, Sajjad**, et al. "LAT-UP: Exposing Layout-Level Analog Hardware Trojans Using Contactless Optical Probing." *2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2023.