Zain Ul Abideen

Contact Information

Department of Computer Systems, Tallinn University of Technology (TalTech), Estonia
Address: Akadeemia tee 7/2-314, Tallinn, Estonia (12616)
Contact: +372 53783637, zain.abideen@taltech.ee, xaainulabideen@gmail.com
LinkedIn Orcid Google scholar Website Skype: xaainulabideen

Research Interests

Trustworthy integrated circuit (IC) design, Hardware security; Hardware obfuscation; Secure-ASIC design; Chip design (front-end/back-end); FPGA implementations; Hardware accelerators; Cryptography; Embedded systems.

Education

Tallinn University of Technology (TalTech), Tallinn, Estonia
Ph.D., Information and Communication Technology, 2020-(Expected Fall 2023)
Dissertation: Leveraging FPGA Re-configurability as an Obfuscation Asset

Institut polytechnique de Grenoble – ESISAR, Valence, France
M.Sc., Computer Engineering (Integration, Security and Trust in Embedded System), 2018-2019
Thesis: Development of an FPGA Emulation-based Fault Injection Tool for RTL designs

University of Management and Technology (UMT), Lahore, Pakistan
B.Sc., Electrical Engineering, 2014-2018
Thesis: Design and Development of Tele-presence Robot

Projects

Tuneable Design Obfuscation Technique using hybrid-ASIC

- ✧ I developed a specialized CAD tool that utilizes a standard-cell based physical synthesis flow and explores the FPGA-ASIC design space, allowing for flexibility and compatibility with contemporary design practices. Its main purpose is to obfuscate the design.
- ✧ Executing RTL to GDS flow (Placement, power planning, CTS, routing, STA, etc.) for different designs, demonstrating the attained obfuscation quantitatively.

A Robustness Evaluation of SRAM-based PUFs on 65nm CMOS Technology from TSMC

- ✧ We collaborated with Intrinsic ID to design a chip using 65nm LP Technology from TSMC. This Chip design explores various memory and chip-level parameters to analyze the impact of different chip-level decisions for each SRAM macro, such as location, rotation, and power delivery strategy.
- ✧ Writing Verilog code and logic synthesis (front-end), RTL & gate-level Simulation
- ✧ Executing RTL to GDS flow (Placement, power planning, CTS, routing, STA, etc.)
- ✧ (RTL to GDS) Executing DRC, LVS, IR drop analysis, spice simulation for final GDS file

Local Layout Effect-based Ring Oscillators on 65nm CMOS Technology from TSMC

- ✧ As a part of the European Union's Horizon 2020 SAFEST project, We collaborated with KU Leuven to design a chip that comprises more than 200 macros of Ring Oscillators (ROs). The ROs are finely tuned for hardware security purposes and can cover a frequency range of a few tens of KHz.
- ✧ Writing Verilog code for front-end logic synthesis and conducting RTL and gate-level simulation
- ✧ Executing RTL to GDS flow (Placement, power planning, CTS, routing, STA, etc.)
- ✧ (RTL to GDS) Executing DRC, LVS, IR drop analysis, spice simulation for final GDS file

Professional Skills

Tools: Cadence Genus, Cadence Innovus, Siemes EDA Calibre, Cadence Xcelium Logic Simulator, Siemes EDA ModelSim, Xilinx Vivado IDE, LTSpice, Proteous, NI Multisim, KiCAD EDA, STM32Cube.
Languages: Verilog, TCL, VHDL, Python, C, SystemVerilog, MATLAB, Javascript, Intel Assembly, MIPS Assembly, Latex, Visual Basic.

Service, Honors and Awards

IEEE Day Ambassador (2016-18), student member (2018-Present)
Reviewer for IET Electronics, IEEE Access

Volunteer, Organizing committee of CSAW'18 Europe Cybersecurity competition (2019)

Received continuous Rector/Dean Merit awards for five semesters and the prestigious Rector's medal upon completing B.Sc. in 2018
First position during my master studies at Grenoble-INP ESISAR

IDEX Master Scholarship during my master studies

Won first position in the International competition of Hardware Security (HeLLO: CTF) (2022)
Young People Programme funding for DATE 2023
Young Fellows Program funding for DAC 2023

Open-source Developments

TOTe (Tuneable Design Obfuscation Technique using eASIC)
TTech-LIB (An Open-source Library of Large Integer Polynomial Multipliers)

Supervision

Co-supervisor, Giorgi Basiashvili (M.Sc. candidate, Computer Engineering, qualified 2022)

Publications

Journals

1. **Z. U. Abideen**, S. Gokulanathan, Muayad J. Aljafa, S. Pagliarini. "An Overview of FPGA-inspired Obfuscation Techniques," 2023. (Submitted to ACM Computing Surveys).
2. **Z. U. Abideen**, R. Wang, T. D. Perez, G. J. Schrijen and S. Pagliarini. "Investigating the Impact of Design-Time Decisions on the characteristics of SRAM-Based PUFs," 2023. (Submitted to IEEE Design & Test)
3. Muayad J. Aljafa, **Z. U. Abideen**, A. Peetermans, B. Gierlichs and S. Pagliarini, "SCALLER: **S**tandard **C**ell **A**ssembled and **L**ocal **L**ayout **E**ffect-based **R**ing Oscillators," 2023. (Submitted to IEEE Solid-State Circuits Letters).
4. M. Imran, **Z. U. Abideen** and S. Pagliarini. "A Versatile and Flexible Multiplier Generator for Large Integer Polynomials. Journal of Hardware and Systems Security," 2023. doi: 10.1007/s41635-023-00134-2.
5. **Z. U. Abideen**, T. D. Perez, M. Martins and S. Pagliarini, "A Security-aware and LUT-based CAD Flow for the Physical Synthesis of hASICs," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023. doi: 10.1109/TCAD.2023.3244879.
6. M. Imran, **Z. U. Abideen** and S. Pagliarini. An Experimental Study of Building Blocks of Lattice-Based NIST Post-Quantum Cryptographic Algorithms in *Electronics*, vol. 41, no. 10. pp. 1953, 2020. doi:10.3390/electronics9111953.

Conferences

7. G. Basiashvili, **Z. U. Abideen** and S. Pagliarini, "Obfuscating the Hierarchy of a Digital IP," 2022. In: A. Orailoglu, M. Reichenbach, M. Jung (eds) Embedded Computer Systems: Architectures, Modeling, and Simulation. SAMOS 2022. Lecture Notes in Computer Science, vol 13511. Springer, Cham, doi:10.1007/978-3-031-15074-6_19.
8. **Z. U. Abideen**, T. D. Perez and S. Pagliarini. From FPGAs to Obfuscated eASICs: Design and Security Trade-offs," 2021 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2021, pp. 1-4, doi: 10.1109/AsianHOST53231.2021.9699758.
9. M. Imran, **Z. U. Abideen** and S. Pagliarini, "An Open-source Library of Large Integer Polynomial Multipliers," 2021 24th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2021, pp. 145-150, doi: 10.1109/DDECS52668.2021.9417065.

Preprints

10. M. Grailoo, **Z. U. Abideen**, M. Leier and S. Pagliarini. Preventing Distillation-based Attacks on Neural Network IP. *arxiv*, doi:10.48550/arXiv.2204.00292.