Zain Ul Abideen, Ph.D

Contact Information

Researcher, Electrical and Computer Engineering — abideen@cmu.edu
Carnegie Mellon University, Pittsburgh, PA, USA — xaainulabideen@gmail.com
Skype: xaainulabiden LinkedIn Orcid Google scholar +1 (412) 608 3400

Short bio

I have gained significant expertise in the trustworthiness of ICs, chip design, and reliable embedded systems during my almost five years of research experience. While pursuing my master's degree, I worked with the Cybersecurity Institute at the University of Grenoble Alpes, where I focused on developing trustworthy hardware and side-channel algorithms. During my doctoral studies, I created a tool that is compatible with the CAD flow and utilizes a reconfigurable fabric (an FPGA fabric) to obscure the design intent during fabrication. This leaves the task of programming a portion of the circuit later in a trusted environment. My proposed CAD flow explores the FPGA-ASIC design space and generates heavily obscured designs, where only small portions of the logic resemble an ASIC.

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, 2020-2024
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
Dissertation: Development of a 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

Experience

Carnegie Mellon University (CMU), PA, USA Mar, 2024 - continued
Postdoctoral Research Associate (Hardware obfuscation, PQC, PUF, TRNG, Secure Neural Networks)

Tallinn University of Technology (TalTech), Tallinn, Estonia Mar, 2020-Mar, 2024
Early stage researcher (Hardware obfuscation, PQC, Large multipliers, PUF, TRNG, chip designing)

Institut polytechnique de Grenoble – ESISAR, Valence, France Jan, 2019-Aug, 2019
Research Assistant (Reliability, Fault emulation)

University of Management and Technology (UMT), Lahore, Pakistan 2017-2018
Teacher and Research Assistant (Linear Algebra, Digital Logic Design, Control System, Embedded System & Robotics)

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, Journal of Circuits, Systems, and Computers and ScienceDirect Machine Learning with Applications
Volunteer in the organizing committee of CSAW'18 Europe Cybersecurity competition in 2019
Received the Rector's medal upon completing B.Sc. in 2018, in addition to five semesters of continuous Rector/Dean Merit awards.

First position during my master studies at Grenoble-INP ESISAR
Received 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
Runner up in ACM SIGBED Student Research Competition 2023
Awarded with Keevalikku IT doctoral scholarship 2023

Publications

Journals

1. **Z. U. Abideen**, S. Gokulanathan, Muayad J. Aljafar, 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. "Impact of Orientation on the Bias of SRAM-based PUFs," in *IEEE Design & Test* vol. X, no. X. pp. X, 2023. doi: 10.1109/MDAT.2023.3322621
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 Polynomialsm" in *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.
7. M. A. Hafeez, M. Rashid, H. Tariq, **Z. U. Abideen**, S. S. Alotaibi, and M. H. Sinky. "Performance Improvement of Decision Tree: A Robust Classifier Using Tabu Search Algorithm," in Applied Sciences, vol. 11, no. 15. pp. 6728, 2021. doi: 10.3390/app11156728
8. **Z. U. Abideen** and M. Rashid. EFIC-ME: "A Fast Emulation Based Fault Injection Control and Monitoring Enhancement," in *IEEE Access*, vol. 8, pp. 207705-207716, 2020. doi: 10.1109/ACCESS.2020.3038198

Conferences

9. 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.
10. **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.
11. 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.
11. **Z. U. Abideen**, M. B. Anwar and H. Tariq, "Dual Purpose Cartesian Infrared Sensor Array Based PID Controlled Line Follower Robot for Medical Applications," 2018 International Conference on Electrical Engineering (ICEE), 2018, pp. 1-7, doi: 10.1109/ICEE.2018.8566871.
12. Z. U. Abideen, H. Tariq, M. A. Hafeez and Z. M. Subhani, "An Improved Implementation of Shift Displacement Method on Hardware – Comprehensive Evaluation of Emerging Bipedal Techniques," 2020 4th International Conference on Automation, Control and Robots (ICACR), Rome, Italy, 2020, pp. 7-12, doi: 10.1109/ICACR51161.2020.9265496.

Preprints

13. 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.

Research Projects

Project Title: *Secure and Assured Hardware: Facilitating ESTonia's Digital Society.*
PIs: Samuel Nascimento Pagliarini
Source: Horizon 2020 Programme
Funder: European Comission
Period funded: Jan-2021 - Dec-2023

Project Title: *Research measure of IT Academy programme for 2018-2022: Riistvara turvalisus.*
PIs: Samuel Nascimento Pagliarini
Source: Horizon 2020 Programme
Funder: Euroopa Sotsiaalfond (ESF)
Period funded: Jan-2018 - Aug-2023

Project Title: *Novel and competent solutions towards synthesizing trusted hardware.*
PIs: Samuel Nascimento Pagliarini
Source: Mobilitas Plus support for applying for an ERC grant (MOBERC)
Funder: Estonian Research Council)
Period funded: Jan-2018 - Aug-2023

Seminars, Workshops, and Conferences

Doctoral Seminar
Department of Computer Systems, Tallinn University of Technology (TalTech), Estonia
Apr 2020 - Jan 2022.

FDOME: Flexible Design Obfuscation Method for Embedded-ASIC (workshop)
IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Kolkata, India
Dec 15-17, 2020.

SAFEST workshop
Tallinn University of Technology (TalTech), Estonia
March 26, 2021.

From FPGAs to Obfuscated eASICs: Design and Security Trade-offs (Conference presentation)
International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation, Samos, Greece
Dec 16-18, 2021.

SAFEST Summer school
LIRMM - Laboratoire d'informatique, de robotique et de microélectronique de Montpellier, France
June 8-10, 2022.

Obfuscating the Hierarchy of a Digital IP (Conference presentation)
IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Shanghai, P.R. China
Jul 3-7, 2022.

Attending the conference and staff exchange through SAFEST
2022 Workshop on Cryptographic Hardware and Embedded Systems (CHES), Leuven, Belgium
Sep 18-21, 2022.

Attending conference and workshops
hardwear.io Netherlands 2022, The Hague, Netherlands
Oct 23-27, 2022.

Attending conference and workshops
Constructive Side-Channel Analysis and Secure Design: 14th International Workshop, COSADE, Munich, Germany
April 3-4, 2023.

Attending the Ph.D. Young People Programme.
Design Automation and Test in Europe (DATE), Antwerp, Belgium

April 235-27, 2022.

Attending the Ph.D. Young Fellow Program to present my poster
60th Design Automation Conference (DAC), San Francisco, United States
July 7-13, 2023.

Attending the Ph.D. forum to present my poster
SUMMER SCHOOL and Security Week at Technical University of Graz (TU Graz), Graz, Austria
September 4-8, 2023.

Presenting my thesis at the ACM SIGBED Student Research Competition
Embedded System Week (ESWEEK), Hamburg, Germany
September 17-22, 2023.

Thesis Committees

Former
Giorgi Basiashvili (M.Sc. candidate, Computer and System Engineer, qualified 2022)

Designed Chips

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, and spice simulation for the 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, and spice simulation for the final GDS file

Open-source developments

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

Collaborations

Collaboration with KU Leaven under the SAFEST project to design a chip for validating ring oscillators.
Collaboration with Intrinsic ID (now part of Synopsys, Inc.) to validate the characteristics of SRAM-based PUF

Educational Projects

Design and Implementation of Omni-Directional Telepresence Robot [Robotics: May'17-Apr'18]
Innovation Project at ESISAR – Analyzing intensity and high precision localization of acoustic signal using BlueCoin [Embedded System: Sep'18-Jan'19]
Reducing the execution time (Performance optimization) of the application using NEON on ARM processor[Computer Architecture: Nov'18-Dec'18]
Optimization and simulation of RISC processor using VHDL in Vivado [Computer Architecture: Nov'18-Dec'18]
Hardware Software co-verification of UART using QuestaSim [Verification: Dec'17-Jan'18]
Analysis of side channel Attacks on STM32 running AES-128 [Security: Feb'18-Aug'18]
Integration of Custom IP for speed controller, Implementation on SOC (Zynq + Artix 7) [Embedded System: Nov'18-Dec'18]
Design and Modelling of Fast Line Tracer [Embedded System: May'15-Jun'17]
APT (Automatic Picture Transmission) from NOAA Satellite using NI USRP-2900 [Embedded System: May'18-Dec'18]
Implementation of High-speed synchronous communication using Opal Kelly XEM 6001 [Embedded System: Jan'19-feb'19]
Implementation of systolic architecture using deep learning (CNN) [Embedded System: Jan'19-Feb'19]
Solar-Piezo Energy Harvester-based Mobile Charger for Tourists [Hobby Project: Mar'15-Apr'15]
Designing and Simulation MIPS (CISC) Processor in Xilinx [Computer Architecture: Jan'16-June'16]
GSM-Based LPG (Gas Level) Management System with LCD [Embedded System: Aug'17-Nov'17]
Mini Portable Vacuum Cleaner [Course Project: Jan'17-Aug'17]
Design of Mini Radar using Arduino and Visual Studio [Course Project: Jun'17-Jul'17]
PLC-based Direction and Speed Controlled object counting system on conveyor belt [Instruments & Measurements: Dec'17-Jan'18]
Implementation of High-speed synchronous communication using Opal Kelly XEM 6001 [Embedded System: Jan'19-Feb'19]
Implementation of systolic architecture using deep learning (CNN) [Embedded System: Jan'19-Feb'19]

Extracurricular Activities

Winner Mic Geek, Circuit Debugging, Logic Design in IST Youth Carnival 2018 held in Institute of Space Technology Islamabad (National level competition, more than 48 universities participated in this competition) 2016-17-18
Winner Logic Design All Pakistan Engineering TRIO (National level competition at University of Lahore) 2017
Winner Robo Tech, IETEC, held in University of Engineering and Technology KSK Campus 2018
Winner Logic Master and Circuit Designing in University of Central Punjab Engineering Olympiad 2018
Winner Robo Race IEEE-WEEK FAST-NUCES Lahore 2017
2nd Position in Wiring Guru KONTESTO DEBRAIN KLASH'16 UMT
Runner up AZEEM HAYAT Speed Soldering Competition, Line Following Robot Competition IEEE-WEEK FAST-NUCES Lahore 2017
Participated in regional research projects Exhibition hosted by Higher Education Commission (HEC) at LUMS, 2017

News Coverage

The latest development following the victory in the International Security Competition was reported on national news in Estonia.
The news coverage in research in Estonia after winning the International Security Competition.
News coverage about my competitions at the University of Management and Technology in Lahore.