Zain Ul Abideen, Ph.D

CONTACT INFORMATION

Researcher, Electrical and Computer Engineering (ECE) 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 am a dedicated researcher with nearly six years of experience in trustworthy IC design, hardware security, and chip design. I strongly focus on secure ASICs, PUFs, TRNGs, obfuscation, fault injection, side-channel, wire-probing, and post-quantum cryptography. I have authored a book with Springer Nature on Hardware security and designed multiple **silicon-proven chips**, showcasing advanced security countermeasures against side-channel attacks and obfuscation techniques. My work is supported by NSF and leading European funding agencies, with impactful collaborations with industrial leaders like Intrinsic-ID (now Synopsys Inc.). By bridging academia and industry, I specialize in secure chip design, hardware accelerators, and reliable systems, driving innovation in secure and resilient hardware solutions.

RESEARCH INTERESTS

Trustworthy IC design; Hardware security; Hardware obfuscation; Secure-ASIC design; FPGA implementations; Hardware accelerators; Post-Quantum Cryptography (PQC); Multi-party Computation for Blockchain; Secure AI/ML architectures; Reliable and fault-tolerant systems; Embedded systems; Physical Unclonable Functions (PUFs); True Random Number Generators (TRNGs); Security-aware NN; ML/AI-assisted chip design; Cryptographic hardware; Side-channel attack mitigation; Large integer multipliers; Fault injection analysis; Hardware-based ML accelerators.

EDUCATION

1- Tallinn University of Technology (TalTech), Tallinn, Estonia
Ph.D., Information and Communication Technology, 2020-2024
Dissertation: Leveraging FPGA Reconfigurability as an Obfuscation Asset
2- Grenoble Institute of Technology (Grenoble INP-ESISAR), Valence, France
M.Sc., Computer Engineering (Integration, Security and Trust in Embedded System), 2018-2019
Dissertation: Development of an FPGA Emulation-based Fault Injection Tool for RTL designs
3- University of Management and Technology (UMT), Lahore, Pakistan
B.Sc., Electrical Engineering 2014-2018
Thesis: Design and Development of Tele-presence Robot

EXPERIENCE

1- Carnegie Mellon University (CMU), PA, USA Mar, 2024 - continued
Postdoctoral Research Associate
2- Tallinn University of Technology (TalTech), Tallinn, Estonia Mar, 2020-Mar, 2024
Early stage researcher
3- Laboratory of Systems and Communication Engineering (LCIS), Valence, France Jan, 2019-Aug, 2019
Research Assistant
4- 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, Siemens 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, C++, SystemVerilog, MATLAB, Javascript, Intel Assembly, MIPS Assembly, Latex, Visual Basic

RESEARCH PROPOSALS EXPERIENCE

1- CCSS: Protecting IP with Universal Circuit-Based Techniques. (Submitted to NSF)
2- CBI Bosch Fellowship in Collaboration with CMU
3- CHIPS NAPMP NOFO: 2025-NIST-CHIPS-NAPMP-01 (R&D Area 5: Super-scaling Multi-chip Packages Leveraging Application-Architecture-EDA Co-design)
4- Midwest Microelectronics Consortium (MMEC) - Next-gen Chip Security and Reliability with Robust Reconfigurable ASICs
5- Cylab CMU - Hardware Realization of Secure Multi-Party Computation for Blockchain
6- Semiconductor Research Corporation - Structural Attack Methods for Reconfigurable-based Obfuscation
7- MOBERC35 (Estonia) - Security, protection, and privacy in hardware-implemented neural networks
8- SMART4ALL Horizon 2020 - Joint Project on SRAM-PUFs with Intrinsic-ID (now Synopsis)
9- IT Doctoral Award/Fellowship - TalTech Funding for Hardware Security

Teaching Experience

1- Introduction to Hardware Security + Lab, co-teaching at CMU, Spring 2025
2- Introduction to Hardware Security + Lab, co-teaching at TalTech, Spring 2023
3- Digital Logic Design Lab at Grenoble-INP, Spring 2019
4- TA for Digital Logic Design at University of Management and Technology (UMT), Fall 2017
5- TA for Linear Algebra at University of Management and Technology (UMT), Spring 2016
6- TA for Control System, at the University of Management and Technology (UMT), Fall 2015

Research Projects

1- EAGER: IMPRESS-U: Hardware-Efficient Realization of UA Cryptographic Standards (Funded by NSF)
2- Secure and Assured Hardware: Facilitating ESTonia's Digital Society (Funded by EU under Horizon 2020 Programme)
3- Research measure of IT Academy programme for 2018-2022: Riistvara turvalisus (Funded by Euroopa Sotsiaalfond (ESF) under Horizon 2020 Programme)
4- Novel and competent solutions for synthesizing trusted hardware. (Funded by Estonian Research Council under Mobilitas Plus support for applying for an ERC grant (MOBERC))

Funded Research Contributions

1- Tuneable Design Obfuscation -Technique using hybrid-ASIC **(Tape-out)**
- ✧ Developed a specialized CAD tool to obfuscate a design 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.

2- Robustness Evaluation via Design-time Decisions of SRAM-based PUFs **(Tape-out)**
- ✧ A collaboration with Intrinsic ID to design a Chip that 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.

3- Local Layout Effect-based Ring Oscillators for Hardware Security Applications **(Tape-out)**
- ✧ As a part of the European Union's Horizon 2020 SAFEST project with KU Leuven, a chip was designed that comprises more than 200 macros of Ring Oscillators (ROs). The ROs were finely tuned for hardware security and can cover frequency ranges of tens of kHz.

5- Open-source Library of Very Large Integer Multipliers
- ✧ A comprehensive framework was created to design different multiplier architectures suitable for post-quantum cryptography. Additionally, numerous variants were assessed with PPA overheads on both FPGA and ASIC platforms.

6- Preventing Distillation-based Attacks on Neural Network IP
- ✧ Developed a novel obfuscation method to secure hardware-implemented neural network intellectual property (IP) from distillation-based attacks.
- ✧ Proposed a key-less obfuscation approach that poisons predictions, preventing attackers from accurately replicating the neural network model.
- ✧ Designed a secure NN obfuscation framework that maintains model accuracy while reducing stolen model effectiveness across multiple datasets.

7- Systematic Evaluation of the Building blocks of Post-Quantum Cryptography Algorithms
- ✧ A comprehensive evaluation of all the algorithm building blocks finalized in the 3rd round of the PQC competition.

8- High-speed Hardware Accelerator for the SABER: LWR-based KEM PQC **(Tape-out)**
- ✧ An ASIC accelerator was successfully taped out to implement the SABER PQC algorithm. The SABER algorithm was a part of NIST's PQC standards, emphasizing lattice-based security. This custom design achieves optimal performance and power efficiency, addressing real-world challenges in post-quantum cryptography.

9- DPA-based Side-Channel Attack on AES at Hardware Abstract Level
- ✧ Designed and implemented a Differential Power Analysis (DPA) attack on AES encryption to extract cryptographic keys at the hardware abstraction level, showcasing vulnerabilities in power side-channel leakage.

10- Emulation-based Fault Injection Tool for RTL Designs
- ✧ Developed a fault injection tool for RTL designs using emulation to analyze fault tolerance and evaluate the resilience of hardware against injected faults.

11- ML-Driven Framework for Detecting Microarchitectural Vulnerabilities

- ✧ Developed a flexible and reconfigurable framework using gem5, data mining, and machine learning to assess and detect emerging microarchitectural vulnerabilities, including high-resolution Cache Side-Channel Attacks like Prime+Scope.

12- Winner of HeLLO CTF: Hardware Security Competition

- ✧ Secured first place in the prestigious HeLLO CTF competition by demonstrating vulnerability analysis in hardware IP security evaluation, including key recovery, reverse engineering, and countermeasure bypassing.

13- Performance Optimization Using NEON on ARM Processors

- ✧ Optimized application execution time on ARM processors by leveraging the NEON SIMD architecture and designing efficient constant multiplier architectures.
- ✧ Reduced computation time by implementing vectorized operations and parallel processing tailored for constant multiplier performance enhancement.

Academic Service

1- IEEE Day Ambassador (2016-18)
2- IEEE member (2014-Present)
3- ACM member (2020-present)
4- Reviewer for IEEE TCAD, IEEE TIFS, IET Electronics, IEEE TVLSI, IEEE Access, EPICS in IEEE, Journal of Circuits, Systems and Computers, DATE, IEEE/ACM ICCAD, IEEE MDTS and Computers and Science Direct Machine Learning with Applications
5- TPC member for IEEE MDTS, IEEE ETS, IEEE/ACM ICCAD 5- Volunteer in the organizing committee of the CSAW'18 Europe Cybersecurity competition in 2019
6- Organized Special Session on Hardware Security at 34th Microelectronics Design and Test Symposium
7- Member Master Thesis Committee
8- Reviewing the Undergraduate and graduate theses at CMU and TalTech 9- Special Session on Hardware Security at the 34th Microelectronics Design and Test Symposium

Invited Talks

1-CMOS Digital Logic: Principles and Applications, University of Massachusetts Dartmouth (February, 2025)
2- Emerging Topics in Hardware Security: Innovations in Chiplet Security, Obfuscation, Security Primitives and Post-Quantum Cryptography (February, 2025)
3- Security Robustness of SRAM PUFs, Intrinsic-ID (June, 2023)
4- Leveraging FPGA Reconfigurability for Obfuscation, Technical University of Munich (TUM), (April, 2023)
5- Countermeasure for IC Supply Chain Threats, Grenoble-INP (January, 2022)
6- Overview of Hello:CTF Competition, Summer SAFEST Workshop (March 2021)

Honors and Awards

1- Achieved the Rector's medal upon completing B.Sc. in 2018 and five consecutive semesters of Rector/Dean Merit awards.
2- First position during my master's studies at Grenoble-INP ESISAR.
6- Received IDEX Master Scholarship during my master's studies
3- Won first position in the International competition of Hardware Security (HeLLO: CTF) (2022)
4- Young People Programme award from DATE 2023
5- Young Fellows Program award from DAC 2023
6- Runner up in ACM SIGBED Student Research Competition 2023
7- Awarded with Keevalikku IT doctoral Award 2023 (Best thesis award)

Books

Hardware Security

1. **Z. U. Abideen** and S. Pagliarini. "Reconfigurable Obfuscation Techniques for the IC Supply Chain (Using FPGA-like Schemes for Protection of Intellectual Property)," in *Springer Nature.* (Synthesis Lectures on Digital Circuits & Systems, Production Phase).

Selected Publications

Selected Journals

1. **Z. U. Abideen**, S. Gokulanathan, Muayad J. Aljafar, S. Pagliarini. "An Overview of FPGA-inspired Obfuscation Techniques," in *ACM Comput. Surv.* vol. 56, no. 12. pp. 1-38, 2024. doi: 10.1145/3677118 - Impact Factor: 23.8 (2023)
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. 41, no. 3. pp. 14-20, 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," in *IEEE Embedded Systems Letters* vol. X, no. X. pp. X, 2024. doi: 10.1109/LES.2024.3459730
4. M. Imran, **Z. U. Abideen** and S. Pagliarini. "A Versatile and Flexible Multiplier Generator for Large Integer Polynomials" 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.
6. 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
7. **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

Selected Conferences

1. **Z. U. Abideen**, L. Aksoy, S. Pagliarini. "Late Breaking Results: Is Reconfigurable-based Obfuscation Secure?," in *DATE*. Just Accepted (February 2025). doi: Accepted
2. **Z. U. Abideen**, D. Garg, L. Pileggi, S. Pagliarini. "Late Breaking Results: Security Analysis of Universal Circuits," in *DAC*. Just Accepted (February 2025). doi: Submitted
3. 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.
4. **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.
5. 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.
6. **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.
7. 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 Bi-pedal 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.

Seminars, Workshops, and Conferences

1- *Reconfigurable Hardware Obfuscation* (Doctoral Seminar)
Department of Computer Systems, Tallinn University of Technology, Estonia, Apr 2020 - Jan 2022.
2- *FDOME: Flexible Design Obfuscation Method for Embedded-ASIC (workshop)*
IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Kolkata, India, Dec 15-17, 2020.
3- *Overview of Hello:CTF Competition* (SAFEST workshop)
Tallinn University of Technology (TalTech), Estonia, March 26, 2021.
4- *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.
5- *Leveraging SRAM for the PUF* (SAFEST Summer School)
LIRMM - Laboratoire d'informatique, de robotique et de microélectronique de Montpellier, France, June 8-10, 2022.
6- *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.
7- *Attending the conference and staff exchange through SAFEST*
2022 Workshop on Cryptographic Hardware and Embedded Systems (CHES), Leuven, Belgium, Sep 18-21, 2022.
8- *Attending conference and workshops*
hardwear.io Netherlands 2022, The Hague, Netherlands, Oct 23-27, 2022.
9- *Attending conference and workshops*
Constructive Side-Channel Analysis and Secure Design: 14th International Workshop, COSADE, Munich, Germany, April 3-4, 2023.
10- *Attending the Ph.D. Young People Programme.*
Design Automation and Test in Europe (DATE), Antwerp, Belgium, April 235-27, 2022.
11- *Attending the Ph.D. Young Fellow Program to present my poster*
60th Design Automation Conference (DAC), San Francisco, United States, July 7-13, 2023.
12- *Attending the Ph.D. forum to present my poster*
SUMMER SCHOOL and Security Week at the Technical University of Graz (TU Graz), Graz, Austria, September 4-8, 2023.
13- *Presenting my thesis at the ACM SIGBED Student Research Competition*
Embedded System Week (ESWEEK), Hamburg, Germany, September 17-22, 2023.
14- *Presenting my thesis at TTTC's Doctoral Thesis Competition*
42nd IEEE VLSI Test Symposium, Tempe, AZ, USA, April 22-24, 2024.
15- *Attendee & Presenter*
2024 CyLab Partners Conference, Pittsburgh, PA, USA, September 24-25, 2024.

Thesis Committees

Former and Current
1- Muhammad Asfand Hafeez (B.Sc. candidate, Electrical Engineering, qualified 2021)
2- Giorgi Basiashvili (M.Sc. candidate, Computer and System Engineering, qualified 2022)
3- Carlos Gewehr (Phd. candidate, Electrical and Computer Engineering, ongoing)
4- Frances Adiwijaya (B.Sc. candidate, Electrical and Computer Engineering, ongoing)

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)

News Coverage

Security Competition was Featured on National News in Estonia.
News coverage after winning the International Security Competition.