Mona Hashemi, Ph.D. (she/her)

mona.hashemi67@gmail.com, monah@nus.edu.sg
Google Scholar, LinkedIn, GitHub, ORCID
+65 98 911 537, +98 912 602 82 55
COM3-02-17, Systems and Networking Research Lab, School of Computing, NUS, Singapore

ACADEMIC EXPERIENCE

2025 - now **Postdoctoral Fellow,** National University of Singapore, Singapore
Supervisor: Dr. Trevor E. Carlson

2017 - 2025 **Ph.D. Researcher**, University of Tehran, Iran
Supervisor: Dr. Siamak Mohammadi

2023 - 2024 **Visiting Ph.D. Researcher**, National University of Singapore, Singapore
Supervisor: Dr. Trevor E. Carlson

2021 - 2023 **Remotely Ph.D. Researcher**, National University of Singapore, Singapore
Supervisor: Dr. Trevor E. Carlson

2021 - 2022 **Remotely Ph.D. Researcher**, University of California, San Diego, USA
Supervisor: Dr. Ryan Kastner

EDUCATION

2017 - 2025 **Ph.D. in Computer Architecture**, University of Tehran, Tehran, Iran
Thesis Title: Detecting and Preventing Counterfeit Hardware by Scalable and Reliable Logic Locking
Supervisor: Dr. Siamak Mohammadi

2014 - 2016 **M.S. in Computer Architecture**, Sharif University of Technology, Tehran, Iran
Thesis Title: A Scheme for Counterfeit Chip Detection Using Scan Chain
Supervisor: Dr. Shaahin Hessabi

2008 - 2012 **B.S. in Computer Engineering**, K.N.Toosi University of Technology, Tehran, Iran
Thesis Title: Design and Implementation of a Heliostat System Based on A Solar Tracker
Supervisor: Dr. Amir Mousavinia

TEACHING EXPERIENCE

2021 - 2022 Hardware Security and Trust, Postgraduate Course, 3 Semesters - University of Tehran
2019 - 2022 Functional Verification, Postgraduate Course, 3 Semesters - University of Tehran
2021 Microprocessor and Assembly Language, Undergraduate Course - Invited Teacher, University of Tehran
2019 Asynchronous Circuit Design, Postgraduate Course, 1 Semester - University of Tehran
2016 Digital Electronics, Undergraduate Course, 1 Semester - Sharif University of Technology
2015 VLSI Design, Undergraduate Course, 1 Semester - Sharif University of Technology

RESEARCH EXPERIENCE

2023 - now Research Assistant, CompArch Research Group, National University of Singapore
2017 - 2025 Research Assistant, Dependable System Design Lab, University of Tehran
2014 - 2017 Research Assistant, Very Large-Scale Integration (VLSI) Lab, Sharif University of Technology

WORK EXPERIENCE

2014 - Now Meter Data Collection System Admin, Iran Grid Management Co., Tehran, Iran
2013 - 2014 E-learning Implementation Specialist, Young Talents Pub. Co., Tehran, Iran
2011 - 2012 Computer Technician, Mehan Payesh Afzar Co., Tehran, Iran
2011 - 2012 Tajhizat Pishrafteh Darman Co. (Internship), Tehran, Iran

HONORS AND SPECIAL RECOGNITIONS

2025 **Outstanding PhD Thesis Award** (Granted to only two PhD students)
International ISC Conference on Information Security and Cryptology (ISCISC 2025), Tehran, Iran

2023 **Research Funding** to join NUS as a visiting Ph.D. researcher
School of Computing, National University of Singapore, Singapore

2019 **Research Scholarship** by Ministry of Science, Research, and Technology (Granted to only two students)
Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran

2016 **Ranked 5th** among all M.Sc. students (in Computer Architecture)
Computer Engineering Department, Sharif University of Technology, Tehran, Iran

2014 **Ranked 6th** among more than 4000 applicants
Nationwide University Entrance Exam for Graduate Students in Computer Engineering, Iran

2013 **Ranked 1st** among all Computer Science and Engineering applicants
Competitive Recruitment Exam of the Ministry of Energy, Iran

2012 **Ranked 6th** among all B.Sc. students
Computer Engineering Department, K. N. T. University of Technology, Tehran, Iran

2008 **Top 0.5%** among more than 150000 applicants
Nationwide University Entrance Exam for Undergraduate Students in Mathematics, Iran

2007 **Ranked 1st** among all the students in high school
Tehran, Iran

PUBLICATION

- Published:

TOP: A Combined Logical and Physical Obfuscation Method for Securing the Networks-on-Chip Against Reverse Engineering Attacks
M. Hashemi, S. Mohammadi, and T.E. Carlson
IEEE Access, 2025

PARS: A Layered Hardware Obfuscation Platform for Resilience and Secure Collaborative Multi-Module Designs
M. Hashemi, S. Mohammadi, and T.E. Carlson
Proceedings of the ACM SIGCOMM Posters and Demos, 2025

SRLL: Improving Security and Reliability with User-Defined Constraint-Aware Logic Locking
M. Hashemi, S. Mohammadi, and T.E. Carlson
ACM Journal on Emerging Technologies in Computing Systems, 2025

LOTUS: A Scalable Framework to Lock Multi-Module Designs with One-Time Key and Self-Destructing Approaches
M. Hashemi, S. Mohammadi, and T.E. Carlson
IEEE Embedded Systems Letters, 2024

FAST-GO: Fast, Accurate, and Scalable Hardware Trojan Detection using Graph Convolutional Networks
A. Imangholi*, M. Hashemi*, A. Momeni, S. Mohammadi, and T.E. Carlson
International Symposium on Quality Electronic Design (ISQED), 2024

Graph Centrality Algorithms for Hardware Trojan Detection at Gate-Level Netlists
M. Hashemi*, A. Momeni*, A. Pashrashid, and S. Mohammadi
International Journal of Engineering, 2022

Hardware Trojan Detection Based on Graph Centrality Features (In Persian)
A. Momeni, M. Hashemi, and S. Mohammadi
International Conference on Electrical, Computer and Mechanical Engineering, 2022

Fast and Energy-Efficient CNFET Adders with CDM and Sensitivity-based Device-Circuit Co-Optimization
K. Haghshenas, M. Hashemi, and T. Nikoubin
IEEE Transactions on Nanotechnology, 2018

CNTFET Full-Adders for Energy-Efficient Arithmetic Applications
M. Grailoo, M. Hashemi, K. Haghshenas, S. Rezaee, S. Rapolu, and T. Nikoubin
International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2015

Design and Implementation of a Heliostat System with Solar Tracker (In Persian)
K. Haghshenas and M. Hashemi
International Conference on Emerging Trends in Energy Conservation (ETEC), 2015

- Accepted and presented (to be published):

Securing Deep Learning Hardware: A Survey of Side-Channel Vulnerabilities and Countermeasures
Z. Mohammadi, M. Hashemi, and S. Mohammadi
The ISC International Journal of Information Security (ISeCure), 2025

- Accepted to be presented as demo:

PARS: A Layered Hardware Obfuscation Platform for Resilience and Secure Collaborative Multi-Module Designs
M. Hashemi, S. Mohammadi, and T.E. Carlson
IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2025

- Submitted:

Energy aware DNN Training using Space Sharing and Early Feedback
K. Haghshenas and M. Hashemi

Remote Power Side-Channel Attack of PQC-based KEMs on Modern x86 Processors: A Case Study of Kyber
M. Hashemi, Q. Wu, F. Zhang, Sh. Bhasin, and T. E. Carlson

- In-preparation:

SoK: All You Need to Know About Side Channel and Fault Injection Attacks on Standardized PQC Algorithms
M. Hashemi and T.E. Carlson

Deep Learning-Based Generic Side-Channel Attack of ML-KEM on Modern Cortex-A72 Processors
Q. Wu, M. Hashemi, D. Jap, F. Zhang, T. E. Carlson, and Sh. Bhasin

Metastable Failure Predicting in Distributed Systems using ML
M. Hashemi and K. Haghshenas

Multi-Layered Security for DNNs: Integrated Strategies against Side-Channel and Neural Architecture Stealing Attacks
M. Hashemi and S. Kazemi Abharian

Evaluating the Impact of Active Wire Fence Placement on Remote Power Side-Channel Attacks in Multi-Tenant FPGAs
S. Ojaghi, A. Ghorbani Bargani, S. Babaian, M. Hashemi, S. Mohammadi, and A. Khonsari

Correlation Power Attack Benchmark Suite for AES: An Open-Source Pre-Silicon Power Analysis Tool
M. Hashemi and T.E. Carlson

SERVICES

1. **Artifact Evaluator:** IEEE Symposium on Security and Privacy (SP), 2026.
2. **Reviewer:** International Conference on VLSI Design (VLSID), 2026.
3. **Co-Reviewer:** The International Conference on Computer-Aided Design (ICCAD), 2025.
4. **Workshop Organizer:** Post-Quantum Cryptography: Resilience, Verification, and Secure Design Automation (Co-located with ICCAD 2025).
5. **Committee Member:** RoboCup Iran Open, Qazvin Islamic Azad University, Qazvin, Iran.

INTEREST

HW Security	Hardware Security Verification, Reliable VLSI Design, Secure Hardware Architectures, Secure Design for Heterogeneous Systems, Secure Hardware using Reconfigurable Designs, Security using Post-CMOS Approaches, Security-Aware Custom Computing, Security Critical System-on-Chips, Hardware Security in GPU
Distributed Systems	Privacy Preserving in Distributed Systems, Security-Aware Distributed Systems, Anomaly and Failure Detection in Distributed Systems, Reliable Distributed Systems, Metastable Failure in Distributed Systems
AI/ML	Security-Aware Hardware Design for NN Architectures, Hardware Security in Deep Learning Models, Hardware Trojan in NN Architectures and Transformers, Machine Learning in IoT Security, Machine Learning in Security of Distributed Systems, Applications of AI in CAD and HW Security, Energy-Aware Training, Fault Resiliency in QNN
PQC	Side-Channel Analysis of Post Quantum Cryptography Schemes, Fault Attacks in Post Quantum Cryptography
In-Memory Computing	Hardware Security in Processing-In-Memory (PIM), Hardware Security in Processing-Near-Memory (PNM), Side-Channel Attacks on PIM and PNM, Secure Space Sharing for IMC, Hardware Security in Data-Centric AI Workloads in the Era of Data Gravity Centric Computing

MENTORING AND ADVISING

1. Mentoring **Ph.D. thesis** on "Hardware Side-Channel Vulnerabilities and Countermeasures in Deep Learning Models"
   By: Zahra Mohammadi, University of Tehran, 2025
2. Mentoring **B.sc. thesis** on "PUFClk: Reconfigurable PUFs for Robust Clock Locking in Device Identification and Authorization"
   By: Atefe Rabiei, University of Tehran, 2024
3. Mentoring **B.sc. thesis** on "Hardware Trojan Localization at Gate-Level Netlists using Graph Convolutional Networks"
   By: Ali Imangholi, University of Tehran, 2023
4. Mentoring **Ph.D. thesis** on "Power Side Channel Attacks on Spiking Neural Networks"
   By: Sina Ojaghi, University of Tehran, 2023
5. Mentoring **M.sc. thesis** on "Feature Extraction/Selection for Hardware Trojan Detection using Machine Learning Methods"
   By: Amir Abbas Momeni, University of Tehran, 2022
6. Mentoring **M.sc. thesis** on "Simulation of Efficient Statistical Methods to Detect Hardware Trojan"
   By: Mostafa Roustaei, University of Tehran, 2021
7. Mentoring **M.sc. thesis** on "Decreasing Process Variation Impact on Hardware Trojan Detection in Nanotechnology"
   By: Mostafa Abbasmollaei, University of Tehran, 2018

SELECTED PROJECTS

1. **Hardware Security & Logic Locking:** Robust hardware by introducing a scalable IP-level logic locking solution, a framework for multi-module systems, and a network topology obfuscation architecture to prevent reverse engineering or deobfuscation attacks.
2. **Hardware Trojan Detection Using Machine Learning & Graph-Based Analysis:** Explore Hardware Trojan detection using graph-based network analysis (Graph Convolutional Networks and graph centrality features).
3. **Counterfeit Chip Detection Using Scan Chain:** An IP protection mechanism based on the scan chain to restrict IP execution only on specific FPGA devices to efficiently protect IPs from being cloned, over-product, or used with unauthorized integration.
4. **Side-Channel Analysis of Post Quantum Cryptography:** Developed the first generic remote power side-channel attack against the NIST-standardized ML-KEM PQC scheme on out-of-order processors and verified the vulnerability of constant-time PQC in virtualized/containerized cloud environments.
5. **Open-Source Pre-Silicon Power Analysis Tool:** Develop an open-source pre-silicon power analysis tool using Standard Cell Library (PDK) for logic gates to model and calculate power dissipation.
6. **Meter Data Collection System:** MDC software collects various hardware and software information on devices. Meter data can be used to support billing, as well as analytics use cases, such as load profiling, consumption tracking, forecasting, asset loading and revenue protection, including the detection of tampering, theft or leakage.
7. **Design and Implementation of a Heliostat System Based on a Solar Tracker:** Control a microcontroller attached to two stacked stepper motors to track the sun and reflect its light toward a target utilizing a mirror (PCB designed via Altium Designer).
8. A designed PCB in Altium Designer software to control a microcontroller attached to two stacked stepper motors. The motors were connected to a mirror to track the sun and then reflect its light toward a target.
9. **Nanoelectronics & CNTFET-based Circuit Optimization:** By employing Device-Circuit Co-Design Optimization, Carbon Nanotube Field-Effect Transistors (CNFET) adders were developed to achieve superior power efficiency and computational performance. These techniques are promising for next-generation low-power computing architectures.

SKILLS

Programming	C, C++, Microsoft Visual Studio pack (VC#, VC++), Java, X86 Assembly, Python
HDL	VHDL, VerilogHDL, SystemVerilog, Xilinx (ISE, Vivado, Vivado HLS, SDK), Intel FPGA (Modelsim)
CAD Tools	Synopsys (Design Compiler, DFT compiler, HSIM, HSPICE), Cadence (SoC/IC Encounter), CodeVisionAVR, Altium Designer (PCB), MaxPlus, Tanner Tools Pro (L-edit)
Other Tools	SQL, Oracle, Git and Version Control, MATLAB (M-file, GUI)

SELECTED COURSES

Hardware Security and Trust
Advanced Computer Architecture
Advanced VLSI Design
Functional Verification
Asynchronous Circuit Design
System on Chip Design
Network on Chip
Low Power Design
Embedded Systems
Green Computing
Computer Methods for Modeling of High Frequency Circuits

REFERENCES

Dr. Siamak Mohammadi
Associate Professor
University of Tehran
Google Scholar
smohamadi@ut.ac.ir

Dr. Kawsar Haghshenas
Assistant Professor
University of Groningen
Google Scholar
k.haghshenas@rug.nl

Dr. Trevor E. Carlson
Associate Professor
National University of Singapore
Google Scholar
tcarlson@comp.nus.edu.sg

Dr. Shaahin Hessabi
Associate Professor
Sharif University of Technology
Google Scholar
hessabi@sharif.edu