Mona
HASHEMI

Postdoctoral Fellow | National University of Singapore

Singapore
+65 98 911537
monah@nus.edu.sg
mona.hashemi67@gmail.com

Research Statement

Nov. 06, 2025

My research focuses on intersection of hardware security, machine learning for trusted computing, and system-level design for secure and reliable architectures. As integrated circuit (IC) supply chains have become increasingly globalized, they are now more exposed to threats such as counterfeiting, overproduction, IP piracy, and hardware Trojans. Over the past several years, my work has centered on developing design-for-security methodologies that provide end-to-end protection of hardware systems, spanning from device-level design to cloud deployment, within the Zero Trust era. I believe that future computing platforms must embed security as a design primitive rather than an afterthought. Accordingly, my research focuses on building secure hardware systems through the co-optimization of performance, reliability, and security across multiple layers of the design stack, including logic, architecture, and system integration.

Doctoral Research: Hardware Security and Trust

During my Ph.D. at the University of Tehran (UT) under the supervision of Dr. Siamak Mohammadi, and at the National University of Singapore (NUS) as a visiting student in collaboration with Dr. Trevor E. Carlson, I developed scalable and reliable hardware security frameworks to defend against supply chain threats. My dissertation, "Detecting and Preventing Counterfeit Hardware by Scalable and Reliable Logic Locking," introduced the SRLL framework [1], a constraint-aware logic locking mechanism that protects high-performance designs against oracle-based, machine learning, and propagation attacks with minimal overhead. This work established a new direction in security-aware design automation, where obfuscation is dynamically optimized to user-defined performance and area constraints. Building upon this foundation, I led several projects that extended logic locking to complex multi-module systems and networks-on-chip, including:

- LOTUS [2]: A scalable multi-module locking framework with one-time key and self-destructing mechanisms
- TOP [3]: A combined logical and physical obfuscation framework for NoCs
- PARS [4]: A layered hardware obfuscation platform for collaborative multi-IP systems

Expanding Toward ML-Driven Hardware Security

The increasing sophistication of hardware threats inspired my recent exploration of machine learning (ML) for Trojan detection and anomaly identification in integrated circuits. In collaboration with students in our research groups at UT and NUS, we proposed graph-based ML frameworks that exploit circuit structural features for Trojan localization and classification [5-7]. Our proposed models achieve scalable and accurate detection using graph convolutional networks (GCNs) and Graph Centrality Algorithms, significantly outperforming existing feature-based approaches.

Current Postdoctoral Research: Side-Channel Analysis of Post Quantum Cryptography

As a postdoctoral fellow at the National University of Singapore, my research extends hardware security to encompass post-quantum cryptography (PQC) and microarchitectural vulnerabilities. I developed one of the first remote power side-channel attacks on Kyber (ML-KEM) executing on modern x86 processors, uncovering critical weaknesses in supposedly constant-time PQC implementations under cloud virtualization environments [8]. This work, together with my ongoing studies on side-channel and fault-injection resilience in PQC systems, contributes to the development of holistic frameworks for secure, high-performance, and trustworthy computing architectures.

Future Research Directions

My long-term vision is to build intelligent, secure, and energy-aware [9-12] hardware platforms. I plan to pursue the following interrelated research directions:

- **Secure and Explainable ML in Hardware Systems:** Explore privacy-preserving and interpretable ML frameworks that protect sensitive data and model integrity in hardware contexts. Techniques such as federated learning and secure multi-party computation will enable collaborative hardware intelligence without compromising privacy or security. Moreover, model security involves techniques such as model watermarking or model locking, which can help to detect unauthorized use or modification of a machine learning model [13].
- **ML for Hardware Threat Detection:** Leveraging ML to detect side-channel leaks, Trojans, and malware in ICs and embedded systems, developing self-adaptive defenses that evolve against new attack surfaces, including heterogeneous and cloud-integrated architectures.
- **Hardware Security for Distributed and Cloud Systems:** System security involves protecting the overall system in which machine learning models are deployed. This includes techniques such as secure multi-party computation, which can enable multiple parties to jointly compute a machine learning model without revealing their individual data to each other. I plan to study secure virtualization and power-aware resource management in multi-tenant cloud infrastructures. By integrating hardware-enforced isolation with AI-driven anomaly detection, I aim to enhance cloud reliability and protect data across distributed architectures.
- **Secure Near Memory Computing:** Exploring security-by-design strategies for in-memory and near-memory computing, addressing vulnerabilities in emerging paradigms such as PIM/PNM accelerators and data-centric AI workloads.

Broader Impact and Collaboration

My research is inherently interdisciplinary, bridging hardware design, security verification, and machine learning–based analytics. I have collaborated with leading research groups at the National University of Singapore (NUS) and the University of California, San Diego (UCSD), mentored several Ph.D., M.Sc., and B.Sc. students, organized an international workshop, and contributed as a reviewer, co-reviewer, and artifact evaluator for top-tier international conferences in hardware security.

At IPM, I am eager to contribute to ongoing research in secure hardware modeling, embedded AI, and system verification, while fostering cross-disciplinary collaboration among hardware, cryptography, and AI research teams. I envision leading initiatives that drive the development of next-generation secure and intelligent computing architectures.

In summary, my research integrates design-for-security principles, machine learning intelligence, and system-level co-design to tackle the evolving challenges of hardware security. At IPM, I aim to extend this foundation toward building trustworthy computing frameworks that deliver security, reliability, and efficiency from transistor to cloud.

References

[1] **M. Hashemi**, S. Mohammadi, and T.E. Carlson, “SRLL: Thwarting Counterfeit Hardware with User-Defined Constraints-Aware Scalable and Reliable Logic Locking”, *ACM Journal on Emerging Technologies in Computing Systems*, vol. 21, no. 1, pp. 1-27, 2025.

[2] **M. Hashemi**, S. Mohammadi, and T. E. Carlson, "LOTUS: A Scalable Framework to Lock Multimodule Designs with One-Time Self-Destructing Key," *IEEE Embedded Systems Letters*, vol. 16, no. 4, pp. 413-416, 2024.

[3] **M. Hashemi**, S. Mohammadi, and T. E. Carlson, "TOP: A Combined Logical and Physical Obfuscation Method for Securing Network-on-Chip Against Reverse Engineering Attacks," *IEEE Access*, 2025.

[4] **M. Hashemi**, S. Mohammadi, and T. E. Carlson, "PARS: A Layered Hardware Obfuscation Platform for Resilience and Secure Collaborative Multi-Module Designs," Proceedings of the ACM SIGCOMM Posters and Demos, pp. 115-117, 2025.

[5] A. Imangholi*, **M. Hashemi***, A. Momeni, S. Mohammadi, and T.E. Carlson, “FAST-GO: Fast, Accurate, and Scalable Hardware Trojan Detection using Graph Convolutional Networks”, *25th International Symposium on Quality Electronic Design (ISQED)*, pp. 1-8, 2024.

[6] **M. Hashemi***, A. Momeni*, A. Pashrashid, and S Mohammadi, “Graph Centrality Algorithms for Hardware Trojan Detection at Gate-Level Netlists”, *International Journal of Engineering*, vol. 35, no. 7, pp. 1375-1387, 2022.

[7] A Momeni, **M. Hashemi**, and S Mohammadi, “Hardware Trojan Detection Based on Graph Centrality Features”, *5th International Conference on Electrical, Computer and Mechanical Engineering*, 2022, Tehran, Iran (In Persian).

[8] **M. Hashemi**, Q. Wu, F. Zhang, Sh. Bhasin, and T. E. Carlson, “Remote Power Side-Channel Attack of PQC-based KEMs on Modern x86 Processors: A Case Study of Kyber” (Submitted).

[9] K. Haghshenas, **M. Hashemi**, and T. Nikoubin, “Fast and Energy-Efficient CNFET Adders with CDM and Sensitivity-based Device-Circuit Co-Optimization”, *IEEE Transactions on Nanotechnology,* vol. 17, no. 4, pp. 783-794, 2018.

[10] Z M. Grailoo, **M. Hashemi**, K. Haghshenas, S. Rezaee, S. Rapolu, and T. Nikoubin, “CNTFET Full-Adders for Energy-Efficient Arithmetic Applications”, *International Conference on Computing, Communication and Networking Technologies (ICCCNT),* pp. 1-6, 2015.

[11] K. Haghshenas and **M. Hashemi**, “Design and Implementation of a Heliostat System with Solar Tracker”, *International Conference on Emerging Trends in Energy Conservation (ETEC),* 2015 (In persian).

[12] K. Haghshenas and **M. Hashemi**, “Energy aware DNN Training using Space Sharing and Early Feedback”, (Submitted).

[13] Z. Mohammadi, **M. Hashemi**, and S Mohammadi, “Securing Deep Learning Hardware: A Survey of Side-Channel Vulnerabilities and Countermeasures”, *The ISC International Journal of Information Security (ISeCure), 2025*, (To be published).