**Hassan Salmani**
Email: hassan.salmani@howard.edu; Phone: 202-806-7684
https://scholar.google.com/citations?user=Pb8P2lAAAAAJ&hl=en

## Education

- **Postdoc** 2011-2013

Department of Electrical and Computer Engineering, The University of Connecticut, CT
Mentor: Prof. Mohammad Tehranipoor

- **PhD** 2008-2011

Department of Electrical and Computer Engineering, The University of Connecticut, CT
Thesis: Design Methodologies for Improving the Trustworthiness and Quality of Integrated Circuits
Advisor: Prof. Mohammad Tehranipoor

## Employment

- *Associate Professor*, Howard University, Department of Electrical and Computer Engineering 2020-Present
- *Assistant Professor*, Howard University, Department of Electrical and Computer Engineering 2013-2020

## Research Interest

- Hardware security and trust
- Side channel Analyses and Embedded System Security
- Internet of things security
- Memory Forensics
- VLSI design and testing

## Publication

### Books and Book Chapters

1. Hassan Salmani, "Trusted Digital Circuits - Hardware Trojan Vulnerabilities, Prevention and Detection," Springer, ISBN 978-3-319-79081-7, 2018
2. Hassan Salmani, Book chapter entitled "Hardware Trojan Attacks and Countermeasures," for " Fundamentals of IP and SoC Security - Design, Verification, and Debug," Published by Springer, ISBN 978-3-319-50055-3
3. Hassan Salmani, Book chapter entitled "Digital Circuit Vulnerabilities to Hardware Trojans" for "Hardware IP Security and Trust," Published by Springer, ISBN 978-3-319-49024-3
4. Mohammad Tehranipoor, Hassan Salmani, and Xuehui Zhang Integrated Circuit Authentication - Hardware Trojans and Counterfeit Detection, Springer ISBN 978-3-319-00816-5

### Published Peer-reviewed Journals

1. H. Salmani, "Gradual-N-Justification (GNJ) to Reduce False-Positive Hardware Trojan Detection in Gate-Level Netlist," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 4, pp. 515-525, April 2022.
2. Phillips, P., Afolabi, O.R. & Salmani, H. Experimental Data Anomaly Detection at Edge Sensor Nodes Using Physics Laws. J Hardw Syst Secur 5, 19–31 (2021)
3. H. Salmani, T. Hoque, S. Bhunia, M. Yasin, J. J. Rajendran and N. Karimi, "Special Session: Countering IP Security threats in Supply chain," 2019 IEEE 37th VLSI Test Symposium (VTS), 2019, pp. 1-9.
4. Ted Winograd, Gaurav Shenoy, Hassan Salmani, Hamid Mahmoodi, Setareh Rafatirad, and Houman Homayoun, “Programmable Gates Using Hybrid CMOS-STT Design to Prevent IC Reverse Engineering,” Accepted and to be appeared at ACM Transactions on Design Automation of Electronic Systems (TODAES), 2018

   Bicky Shakya, Tony He, Hassan Salmani, Domenic Forte, Swarup Bhunia, Mark Tehranipoor, “Benchmarking of Hardware Trojans and Maliciously Affected Circuits,” Journal of Hardware and Systems Security, 1-18, April 2017

5. Hassan Salmani, “COTD: Reference-free Hardware Trojan Detection and Recovery based on Controllability and Observability in Gate-level Netlist,” TIFS 2017
6. Hassan Salmani and Mark Tehranipoor, “Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion,” TIFS 2016
7. Hassan Salmani and et al. “Reliability Analysis of Spin Transfer Torque based Look up Tables under Process Variations and NBTI Aging,” Elsevier Microelectronics Reliability 2016
8. Hassan Salmani, W. Zhao, M. Tehranipoor, S. Chakravarty, P. Girard, and X. Wen, “Layout-Aware Pattern Evaluation and Analysis for Power-Safe Application of TDF Patterns,” Journal of Low Power Electronics (JOLPE), vol. 8, pp. 248-258, 2012
9. Hassan Salmani and M. Tehranipoor, “Layout-Aware Switching Activity Localization to Enhance Hardware Trojan Detection,” IEEE Transactions on Information Forensics & Security, 2011.
10. Hassan Salmani, M. Tehranipoor, and J. Plusquellic, "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol. PP, no.99, pp.1, 2012
11. Mohammad Tehranipoor, Hassan Salmani, Xuehui Zhang, Xiaoxiao Wang, Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, "Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges," Computer, vol. 44, no. 7, pp. 66-74, July 2011.

### Published Peer-reviewed Conference Paper

12. Hassan Salmani, “WiP: Reference-free Hardware Trojan Detection in Manufactured Integrated Circuits,” The 11th ACM Hardware and Architectural Support for Security and Privacy (HASP) 2023
13. Hassan Salmani, Mohsen Mosleh, and Gloria Washington, “Undergraduate Research Experience Impact on Retention in an Electrical Engineering and Computer Science (EECS) Program”, The IEEE 19th International Conference on Frontiers in Education: Computer Science & Computer Engineering (FECS’23)
14. Mohsen Mosleh, Marcus Alfred, Preethi Chandran, John Harkless, Arlene Maclin, Courtney Robinson, Hassan Salmani, Sonya Smith, Gloria Washington, Hessam Yazdani, “Outcome Assessment and Learned Best Practices of an Undergraduate Research Experience (URE) Program” to appear in ASEE Zone 1 Conference - Spring 2023.
15. Hassan Salmani, Mohsen Mosleh, “Undergraduate Research Experience in Internet of Things and its Impact on Academic Experience”, FECS'22 - The 18th Int'l Conf on Frontiers in Education: Computer Science and Computer Engineering
16. Hassan Salmani, “The Improved COTD Technique for Hardware Trojan Detection in Gate-level Netlist”, In Proceedings of the Great Lakes Symposium on VLSI 2022 (GLSVLSI '22). Association for Computing Machinery, New York, NY, USA, 449–454.
17. Hassan Salmani and et al., “Memory Forensics Tools Quantification and Ranking,” ICARS 2022: 16. International Conference on Availability, Reliability and Security, Accepted
18. Hassan Salmani, “The Improved COTD Technique for Hardware Trojan Detection in gate-level netlist”, GLSVLSI 2022, Accepted
19. Hassan Salmani and Mohsen Mosleh, “Undergraduate research experience in Internet of Things and its impact on academic experience,” FECS'22 - The 18th Int'l Conf on Frontiers in Education: Computer Science and Computer Engineering
20. Braxton Dula, Prudence Phillips, Hassan Salmani, Multi-variate Data Anomaly Detection in Wireless Sensor Networks, SecDev 2019, Poster
21. H Salmani, T Hoque, S Bhunia, M Yasin, JJV Rajendran, N Karimi, "Special Session: Countering IP Security threats in Supply chain," 2019 IEEE 37th VLSI Test Symposium (VTS)
22. Hassan Salmani, "COTD: Reference-free Hardware Trojan Detection in Gate-level Netlist", GOMACTech 2017
23. Raza Shafiqi, Hamid Mahmoodi, Houman Homayoun, and Hassan Salmani, "The ATPG Attack for Reverse Engineering of Combinational Hybrid Custom-Programmable Circuits", GOMACTech 2017
24. Aliyar Attaran, Hassan Salmani, Houman Homayoun, Hamid Mahmoodi, “Dynamic Single and Dual Rail Spin Transfer Torque Look Up Tables with Enhanced Robustness under CMOS and MTJ Process Variations,” ICCD 2016
25. Darya Almasi, Houman Homayoun, Hassan Salmani, and Hamid Mahmoodi, "Comparative Analysis of Hybrid Magnetic Tunnel Junction and CMOS Logic Circuits," SOCC 2016

26. Ted Winograd, Hassan Salmani, Hamid Mahmoodi, and Houman Homayoun, Kris Gaj, “Preventing Design Reverse engineering with Reconfigurable Spin Transfer Torque Look Up Tables,” DAC 2016
27. Ragh Kuttappa, Hamid Mahmoodi, Hassan Salmani, and Houman Homayoun, “Reliability Analysis of Spin Transfer Torque based Look up Tables under Process Variations,” ISCAS 2016
28. Ted Winograd, Hassan Salmani, Hamid Mahmoodi, Houman Homayoun, “Preventing Design Reverse engineering with Reconfigurable Spin Transfer Torque LUT Gates,” ISQED 2016
29. Ted Winograd, Hassan Salmani, Hamid Mahmoodi, and Houman Homayoun, "STT-CMOS Hybrid Designs for Reverse-engineering Prevention," GOMACTech 2016.
30. Jonnetta Bratcher, Naja Green, Jonathan Lopera, Justin Powell, Candace Ross, and Hassan Salmani, “Hardware Trojan Prevention for Protection of Medical Devices and Personal Health Records,” Undergraduate student poster presentation, IEEE Sarnoff Symposium 2015.
31. Hassan Salmani, Hamid Mahmoodi, and Houman Homayoun “Logical Vanishability for Counterfeit Prevention,” SMTA/CALCE Counterfeit Electronic Parts and Electronic Supply Chain Symposium, 2015.
32. Hassan Salmani, Mohammad Tehranipoor, and Ramesh Karri, “Trust Benchmarks and Design Vulnerability Analysis,” IEEE International Conference on Computer Design (ICCD 2013)
33. Hassan Salmani and Mohammad Tehranipoor, “Analyzing Circuit Vulnerability to Hardware Trojan Insertion at the Behavioral Level,” IEEE Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT 2013)
34. Hassan Salmani, W. Zhao, M. Tehranipoor, S. Chacravarty, and X. Wen, "Layout-Aware Pattern Evaluation and Analysis for Power-Safe Application of TDF Patterns," Proc. IEEE International Workshop on Impact of Low-Power design on Test and Reliability, pp. 20-21, Trodheim, Norway, May 23-27, 2011.
35. Hassan Salmani, M. Tehranipoor, and J. Plusquellic, "A layout-aware approach for improving localized switching to detect hardware Trojans in integrated circuits," Information Forensics and Security (WIFS), 2010 IEEE International Workshop on , pp.1-6, Dec. 2010
36. Hassan Salmani, M. Tehranipoor, and J. Plusquellic, “New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time,” Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on, pp.66-73, July 2009
37. X. Wang, Hassan Salmani, M. Tehranipoor, and J. Plusquellic, “Hardware Trojan Detection and Isolation using Current Integration and Localized Current Analysis,” Defect and Fault Tolerance of VLSI Systems, 2008. DFTVS '08. IEEE International Symposium on, pp.87-95, Oct. 2008.
38. Hassan Salmani, Seyed Chassem Miremadi, “Assessment of Message Missing Failures in CAN-based Systems,” Proc. of the 23rd IASTED International Multi-conferences Parallel and Distributed Computing and Networks (PDCN), pp. 387-392, Innsburck, Austria, February 15-17, 2005.
39. Hassan Salmani, Seyed Chassem Miremadi, “Contribution of Controller Area Networks Controllers to Masquerade Failures,” Proc. IEEE Pacific Rim International Symposium on Dependable Computing, pp.310-316, 12-14 Dec. 2005.

## Teaching Experience

- Computer Systems Architect, Spring 2022, 2023, 2024, 2025
- Adv. Computer Sys. Architect, Spring 2022, 2023, 2024, 2025
- Introduction to Computer Networking, Spring 2019, 2020, 2021
- Introduction to VLSI Design, Fall 2018, 2019, 2020, 2021, 2022, 2023, 2024
- Intro. to VLSI Design Lab, Fall 2021, 2022, 2023, 2024
- VLSI Design, Fall 2021, 2022, 2023, 2024
- VLSI Design Lab, Fall 2021, 2022, 2023, 2024
- Embedded Systems Design Lab, Spring 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025
- Microcomputer Design, Fall 2014, 2017, 2018

- Research in Undergraduate Experience, Spring 2017, 2018, 2019, 2020, 2021
- Introduction to Engineering, Fall 2017, 2018, 2019, 2020, 2021, 2022
- Fundamentals of Digital Systems Design, Spring 2014, 2015, 2016, 2017
- Fundamentals of Digital Systems Design Lab, Spring 2014, 2015, 2016, 2017
- Advanced Digital Systems Design, Fall 2013, 2014, 2015, 2016
- Advanced Digital Systems Design Lab, Fall 2013, 2014, 2015, 2016
- Operating System for Engineering, Spring 2015, 2016