Bita Rouhani

Contact Information

14865 NE 36th St, Redmond, WA 98052
+1(281)-795-9094
bita.rouhani@microsoft.com

Research Interests

Deep Learning, Real-time Streaming Machine Learning, Algorithm Design for Emerging Computing Platforms and Constrained Devices, Computer Architecture, Design Automation, HW/SW Co-design, Distributed Optimization, Low-Power Computing, Causal Data Analysis, and Safe and Reliable Machine Learning.

Education

University of California San Diego, CA, USA — Jan 2016-Aug 2018

*Ph.D. in Electrical and Computer Engineering- **GPA (4.00/4.00)***
Advisor: Prof. Farinaz Koushanfar

Rice University, Houston, TX, USA — Aug 2013-Dec 2015

*M.Sc. in Electrical and Computer Engineering - **GPA (4.12/4.00)***
Advisor: Prof. Farinaz Koushanfar

Sharif University of Technology, Tehran, IR — Sep 2009-May 2013

*B.Sc. in Electrical Engineering- **GPA (18.35/20.00)***

Professional Experiences

Senior Researcher, Microsoft, Redmond, WA — July 2019-Present

Researcher, Microsoft, Redmond, WA — Sep 2018-July 2019

Research Intern, Microsoft, Redmond, WA

- Computer Architecture Research Group — Summer 2017
- Sensing and Energy Research Group — Summer 2016

Graduate Research Assistant — Aug 2013-Aug 2018

- University of California, San Diego
- Rice University

Teaching Assistant

- University of California, San Diego
  - Security of IoT Systems, Winter 2017
  - Advanced Digital Design, Fall 2016
  - Security of Hardware Embedded Systems, Spring 2016
- Rice University
  - Advanced Digital Hardware Design, Implementation, and Optimization, Fall 2015
  - Design and Analysis of Secure Embedded Systems for IoT era, Spring 2015
- Sharif University
  - Discrete time Signal Processing (DSP), Fall 2012
  - Principle of Electrical Engineering, Fall 2012
  - Signals and Systems, Fall 2011
  - Logic Circuits and Lab, Fall 2011
  - Electronic Principles and Lab, Spring 2011

Lecturer

- Teaching Physics, Mathematics, and C++ to high school students, Tehran

Honors and Awards

- **Best Ph.D. Dissertation Award, UC San Diego**, 2019
- **EECS Rising Star, MIT**, 2018
- **Microsoft Ph.D. Fellowship**, 2017
- **Computing Research Association Woman Grad Cohort Scholarship**, 2016
- **Rice University Honors Student**, GPA: 4.12/4.00
- **DAC Richard Newton Young Student Scholarship**, 2014
- **ECE Department Fellowship**, Rice University, 2013
- **Adaptive Computing & Embedded Systems Fellowship**, Rice University, 2013
- **Exempted from Nationwide M.Sc. Entrance Exam as an Exceptionally Talented Undergraduate**, Sharif University, 2013
- **Best Electrical Engineering B.Sc. Thesis Award**, Sharif University, 2013
- **Ranked 4^{th} among 200^{+} EE Students**, Sharif University, 2013
- **Ranked 69^{th} among $400,000^{+}$ Participants in the Nationwide University Entrance Exam for B.Sc. Degree**, 2009

Selected Publications

[1] **B. Rouhani**, H. Chen, and F. Koushanfar. "DeepSigns: An End-to-End Watermarking Framework for Protecting the Ownership of Deep Neural Networks", in 24rd ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2019

[2] H. Chen, **B. Rouhani**, C. Fu, J. Zhao, and F. Koushanfar. "DeepMarks: A Secure Fingerprinting Framework for Digital Rights Management of Deep Learning Models", in ACM International Conference on Multimedia Retrieval (ICMR), 2019

[3] H. Chen, C. Fu, **B. Rouhani**, J. Zhao, and F. Koushanfar. "DeepAttest: An End-to-End Attestation Framework for Deep Neural Networks", in The 46th International Symposium on Computer Architecture (ISCA), 2019

[4] **B. Rouhani,** M. Ghasemzadeh, and Farinaz Koushanfar, "Automated Scalable Framework for Streaming-based Causal Bayesian Learning Using FPGAs," in 26th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA), 2018

[5] **B. Rouhani,** M. Samragh, T. Javidi, and F. Koushanfar. "Safe Machine Learning and Defeating Adversarial Attacks", IEEE Security and Privacy (S&P) magazine, 2018

[6] **B. Rouhani,** M. Samragh, M. Javaheripi, F. Koushanfar, and T. Javadi, "DeepFense: Online Accelerated Defense Against Adversarial Deep Learning", International Conference on Computer-Aided Design (ICCAD), 2018

[7] **B. Rouhani,** S. Hussain, K. Lauter, and F. Koushanfar. "ReDCrypt: RealTime Privacy Preserving Deep Learning Using FPGAs", ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2018

[8] **B. Rouhani,** M. Sadegh Riazi, and F. Koushanfar. "DeepSecure: Scalable Provably-Secure Deep Learning", In Proceedings of Design Automation Conference (DAC), 2018

[9] S. Hussain**, B. Rouhani,** M. Ghasemzadeh, and F. Koushanfar. "MAXelerator: FPGA Accelerator for Privacy Preserving Multiply-Accumulate (MAC) on Cloud Servers", In Proceedings of Design Automation Conference (DAC), 2018

[10] S. Riazi, **B. Rouhani,** and F. Koushanfar. "Privacy Concerns in Deep Learning", IEEE Security and Privacy (S&P) magazine, 2018.

[11] **B. Rouhani,** A. Mirhoseini, and F. Koushanfar. "Deep^{3}: Leveraging Three Levels of Parallelism for Efficient Deep Learning", In Proceedings of Design Automation Conference (DAC), 2017

[12] **B. Rouhani,** A. Mirhoseini, and F. Koushanfar. "RISE: An Automated Framework for Real-Time Intelligent Video Surveillance on FPGA", ACM Transactions on Embedded Computing Systems (TECS), 2017

[13] **B. Rouhani,** M. Ghasemzadeh, and F. Koushanfar. "Real-time Causal Internet Log Analytics by HW/SW/Projection Co-design", Hardware Demo in Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017

[14] **B. Rouhani,** A. Mirhoseini, and F. Koushanfar. “TinyDL: Just-in-Time Deep Learning Solution for Constrained Embedded Systems”, In Proceedings of International Symposium on Circuits & Systems (ISCAS), 2017

[15] **B. Rouhani,** A. Mirhoseini, E. Songhori, and F. Koushanfar. “Automated Real-Time Analysis of Streaming Big and Dense Data on Reconfigurable Platforms”, ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2016 **(Selected as one of the notable books and articles of 2016 by Computing Reviews)**

[16] **B. Rouhani,** A. Mirhoseini, and F. Koushanfar. “DeLight: Adding Energy Dimension To Deep Neural Networks”, In Proceedings of International Symposium on Low Power Electronics and Design (ISLPED), 2016

[17] A. Mirhoseini, **B. Rouhani,** E. Songhori, and F. Koushanfar. “Chime: Checkpointing Long Computations on Intermittently Energized IoT Device”, IEEE Transactions on Multi-Scale Computing Systems (TMSCS), 2016

[18] A. Mirhoseini, **B. Rouhani,** E. Songhori, and F. Koushanfar. “PerformML: Performance Optimized Machine Learning by Platform and Content Aware Customization”, In Proceedings of Design Automation Conference (DAC), 2016

[19] **B. Rouhani,** A. Mirhoseini, and F. Koushanfar. “Going Deeper than Deep Learning for Massive Data Analytics under Physical Constraints”, In proceedings of International Conference on Hardware/Software Co-design and System Synthesis (CODES+ISSS), 2016

[20] **B. Rouhani,** E. Songhori, A. Mirhoseini, and F. Koushanfar. “SSketch: An Automated Framework for Streaming Sketch-based Analysis of Big Data on FPGA”, Field-Programmable Custom Computing Machines (FCCM), 2015

[21] A. Mirhoseini, E. Songhori, **B. Rouhani,** and F. Koushanfar. “Flexible Transformations For Learning Big Data”, Short Paper, ACM Special Interest Group for the Computer Systems Performance Evaluation Conference, (SIGMETRICS), 2015

Preprints

[22] M. Javaheripi, **B. Rouhani**, and F. Koushanfar. “SWNet: Small-World Neural Networks and Rapid Convergence”, arXiv preprint arXiv:1904.04862, 2019

[23] M. Ghasemzadeh, F. Lin, **B. Rouhani**, F. Koushanfar, and K. Huang. “AgileNet: Lightweight Dictionary-based Few-shot Learning.” ArXiv Preprint 1805.08311, 2018

Patents

[1] **B. Rouhani**, Douglas C Burger, and Eric S Chung. “Neural entropy enhanced machine learning”. U.S. patent, Application No. 15853458, 2019

[2] **B. Rouhani**, H. Chen, and F. Koushanfar. “Intellectual property protection for deep neural networks”. Provisional U.S. patent, Application No. 62649926, 2018

[3] **B. Rouhani**, M. Javaheripi, and F. Koushanfar. “Small-World Nets for fast DNN training/execution”. Provisional U.S. patent, Application No. 62749609, 2018

[4] **B. Rouhani**, M. Samragh, T. Javidi, and F. Koushanfar, “Characterizing and Thwarting Adversarial Deep Learning”. Provisional U.S. patent, Application No. 62531816, 2017

[5] **B. Rouhani**, M. Ghasemzadeh, and F. Koushanfar. “Automated Scalable Framework for Dynamic Causal Bayesian Learning on FPGA”. Provisional U.S. patent, Application No. 62452880, 2017

[6] **B. Rouhani**, A. Mirhoseini, and F. Koushanfar. “MobiDeep: Making Sense of Mobile Context by Deep Learning”. Provisional U.S. patent, Application No. 62294215, 2016

Workshops

[1] “ExtDict: Extensible Dictionaries for Data- and Platform-Aware Large-Scale Learning”, International Parallel & Distributed Processing Symposium (IPDPS) ParLearning workshop, 2017 (**Best paper award**)

[2] “Data- and Platform-Aware Large Scale Machine Learning”, Annual Data Science Meet-up, Rice University, 2015

[3] “Automated Sketch-based Analysis of Big Data on FPGA”, International Conference on Computational Photography (ICCP), 2015

[4] ”HW/SW Co-design Approach for Large Matrix Computation”, Richard Newton Young Student forum in Design Automation Conference (DAC), 2014

[5] “Design and Implementation of Automatic License-Plate Recognition”, Sharif University, 2013 (**Best B.Sc. Thesis Award**)

Computer Skills

- **Programming skill:** Python, C, C++, Verilog (HDL), Java, MATLAB, R
- **Parallel programming:** MPI, OpenMP, OpenCL, CUDA
- **Machine Learning Libraries:** PyTorch, TensorFlow, Theano, Caffe, Keras
- **Design Tools:** Xilinx Design Tools (ISE, Vivado HLS, Vivado), Modelsim, System Generator, Code Composer Studio, Codevision AVR, Hspice, ADS, Altium Protel 99 SE
- **Hardware:** Xilinx Virtex/Spartan FPGAs, WARP

Professional Services

- **Executive Committee Member**, Diversity and Inclusion Council, Microsoft Corporation, 2018-present
- **President and Executive Committee Member**, Women ExCEL (Electrical and Computer Engineering Leaders), Rice University, 2013-2015
- **Research Mentor**, 2014-present
  - *PhD Students.*
    - Mohammad Samragh (4th year PhD student at UCSD)
    - Huili Chen (3rd year PhD student at UCSD)
    - Mojan Javaheripi (2nd year PhD student at UCSD)
    - Fang Lin (2nd year PhD student at UCSD)
    - Shehzeen Hussain (2nd year PhD student at UCSD)
  - *Master Students.*
    - Cihan Kilinc (2nd year M.Sc. student at UCSD)
    - Mohammad Ghasemzadeh (now working as a hardware engineer at Apple)
  - *Undergraduate Students.*
    - Keith Chao-Kun Yu (now pursuing his M.Sc. degree at Cornell University)
    - Xinwei Fan (Applying for PhD programs)
  - *High-School Students.*
    - Kasra Sadeghi (now pursuing his B.Sc. degree at UT Austin)
    - Arta Kasaeian (now pursuing his B.Sc. degree at UCLA)
- **External Reviewer:**
  - IEEE International Symposium on High-Performance Computer Architecture (HPCA), 2019
  - ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2019
  - Design, Automation, and Test in Europe Conference (DATE), 2019
  - IEEE Micro Journal, 2019
  - ACM Transactions on Privacy and Security, 2018
  - Computing Surveys, 2018
  - ACM Transactions on Design Automation of Electronic Systems (TODAES), 2018
  - Design Automation Conference (DAC), 2018
  - Applied Cryptography and Network Security Conference (ACNS), 2016
  - The Network and Distributed System Security Symposium (NDSS), 2016
  - IEEE Symposium on Security and Privacy (SP), 2015
  - IEEE Symposium on Hardware-Oriented Security and Trust (HOST), 2015
  - Field-programmable Logic and Applications Conference (FPL), 2015