Wujie Wen

Engineering Building II 2264
Department of Computer Science
North Carolina State University, Raleigh, NC 27606

Phone: (919)5133184
E-mail: wwen2@ncsu.edu
Web: https://wenwujie.github.io/

Research AREAS

Software-Hardware Co-design for Efficient/Reliable Computing, In-Memory Computing, Design Automation;
Secure and Private (e.g. Homomorphic Encryption) AI Computing;
AI-assisted Health, Edge Computing and Cyber-Physical Systems.

Professional Experience

Associate Professor, Department of Computer Science, NC State University, 08/2023–Current

Associate Professor, Department of ECE, Lehigh University, 06/2023-08/2023

Assistant Professor, Department of ECE, Lehigh University, 09/2019-06/2023

Assistant Professor, Department of ECE, Florida International University, 09/2015-08/2019

Visiting Faculty Research Fellow, Air Force Research Laboratory, 06/2017-08/2017

Intern Engineer, Wireless Connectivity Group, Broadcom Corp., 01/2013-04/2013 & 05/2012-08/2012

ASIC Design Engineer, GPU Design Group, Advanced Micro Devices (AMD) Inc., 07/2010-07/2011

Education

Ph.D. in Computer Engineering, University of Pittsburgh, Pittsburgh, PA, USA 09/2011-08/2015
Thesis: "Error Characterization and Correction Techniques for Reliable STT-RAM Designs"
Advisor: Prof. Yiran Chen, Duke University

M.S. in Electronic Engineering, Tsinghua University, Beijing, China 09/2007-07/2010
Best Master Thesis Nomination at Department of Electronic Engineering, Tsinghua University

B.S. in Electronic Engineering*, Beijing Jiaotong University, Beijing, China 09/2002-07/2006
***Honor Class**

Honors and Awards

- **NSF Faculty Early Career Award 2023**.
- **2023 William J. McCalla ICCAD Best Paper Award** at the 42nd ACM/IEEE Conference on Computer-Aided Design (ICCAD), Nov. 2023, San Francisco, CA (**2 out of 750 submissions, ICCAD is a top CSRankings conference in Design Automation, Topic-"Processing-In-Memory Deep Learning Hardware Accelerator"**, **NCSU CSC News:** https://www.csc.ncsu.edu/news/2566)
- MICCAI Society Young Scientist Award Nomination and Shortlist 2020 for paper–"Orchestrating Medical Image Compression and Remote Segmentation Networks", Lima, Peru (First author by Ph.D student–Zihao Liu).
- Best Paper Award Nomination at ASP-DAC 2018, Jeju Island, Korea (First author by Ph.D. student–Qi Liu, **Topic–"Deep Learning Security"**).
- Best Paper Nomination at ICCAD 2018, San Diego, CA (**Topic–"Deep Learning Security"**).
- Best Paper Award Nomination at DATE 2016, Dresden, Germany (First author by me).
- Best Paper Award Nomination at 51st DAC 2014, San Francisco, CA (First author by me).
- Best Paper Nomination from Track–"Hardware for Embedded Systems" at ICCAD 2017, Irvine, CA (First author by Ph.D. student–Tao Liu, **Topic–"Neuromorphic Computing"**).
- Best Paper Nomination from Track–"Hardware for Embedded Systems" at ICCAD 2018, San Diego, CA (**Topic–"Hardware Acceleration of Deep Learning"**).

- Best Ph.D. Forum Poster Presentation at 52nd DAC 2015, San Francisco, CA.
- Feature Paper of Month, IEEE Transactions on Computers, May, 2017.
- Visiting Faculty Research Program Fellowship, Air Force Research Lab, Rome, NY, 2017.
- 49th Design Automation Conference (DAC 2012) A. Richard Newton Graduate Scholarship ($24,000), the only awardee for outstanding research in EDA Domain, San Francisco, CA.
- ACM Special Interest Group on Design Automation (SIGDA) Student Research Competition (SRC) Bronze medal, ICCAD 2014, San Jose, CA.

Research Grants

Awarded Grants

1. **National Science Foundation (NSF) Career Award**, Wujie Wen (PI), *"**CAREER:** Dependable and Secure Machine Learning Acceleration from Untrusted Hardware"*, 10/01/2023-09/30/2028, CNS-2349538, Total amount: $600,000.
2. **National Science Foundation (NSF)**, Wujie Wen (**Lead PI**, Share $400,000) *"Collaborative Research: SaTC: CORE: Medium: Accelerating Privacy-Preserving Machine Learning as a Service: From Algorithm to Hardware"*, CNS-2348733, 07/01/2023-06/30/2027, Total amount: $1,200,000.
3. **National Science Foundation (NSF)**, Wujie Wen (**Lead PI**, Share $355,475), *"SPX: Collaborative Research: Scalable Neural Network Paradigms to Address Variability in Emerging Device based Platforms for Large Scale Neuromorphic Computing"*, SPX-2401544, 11/26/2019-09/30/2024, Total amount: $699,617 ($715,617 with REU Supplemental).
4. **National Science Foundation (NSF)**, Wujie Wen (Co-PI, Share $200,000), *"MRI: Development of Heterogeneous Edge Computing Platform for Real-Time Scientific Machine Learning"*, OAC-2215789, 10/01/2022-09/30/2025, Total amount: $999,600.
5. **National Science Foundation (NSF)**, Wujie Wen (PI, Share $235,000), *"SHF: Small: Collaborative Research: Retraining-free Concurrent Test and Diagnosis in Emerging Neural Network Accelerators"*, CCF-2011236, 10/05/2019-09/30/2023, Total amount: $499,998.
6. **National Science Foundation (NSF)**, Wujie Wen (Single PI), *"EAGER: Invisible Shield: Can Compression Harden Deep Neural Networks Universally Against Adversarial Attacks?"*, CNS-1840813, CNS-2011260, 09/01/2018-08/31/2021, Total amount: $250,000.
7. **The Florida Center for Cybersecurity (FC^2)**, Wujie Wen (PI, Share 50%), *"Towards Robust Deep Learning Systems Against Adversarial Attacks"*, 07/01/2019-06/30/2020, Total: $75,000.
8. **The Florida Center for Cybersecurity (FC^2)**, Wujie Wen (PI, Share 50%), *"Helmet: Deep Neural Network Protection Against Adversarial Attacks"*, 07/01/2017-12/31/2018, Total: $50,000.
9. **Air Force Research Lab (AFRL)**, Wujie Wen (PI), *"Security Analysis of Model Compressed Deep Neural Networks Under Adversarial Attacks"*, 09/15/2017-11/15/2017, $10,000.
10. **Lehigh Collaborative Research Opportunity (CORE) Grant Program**, *"Privacy Implications of Hardware Functionality in Deep Learning"*, Wujie Wen (Co-PI, Share 50%), 09/01/2020-08/31/2022, $60,000.
11. **Lehigh Accelerator Grant Program**, *"Addressing Unreliability in Memristor Crossbars for Deep Neural Network Accelerators"*, Wujie Wen (Co-PI, Share 50%) 01/2022-12/2023, $100,000.

Other Awarded Grants

- **Xilinx University Program Donation**, *"Hardware-software Co-design for Enhancing the Performance and Robustness of Deep Compressed Neural Networks"*, PI, 03/07/2017-03/06/2018, $2,495.

Representative Works

- **NeurIPS'23**,*"Penguin: Parallel-Packed Homomorphic Encryption for Fast Graph Convolutional Network Inference"*, the Thirty-Seventh Annual Conference on Neural Information Processing Systems **(NeurIPS)**, Dec. 2023
- **ICCAD'23**, *"Improving Realistic Worst-Case Performance of NVCiM DNN Accelerators through Training with Right-Censored Gaussian Noise"*, Proc. of the 42nd ACM/IEEE International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2023.
- **MICRO'23**, *"AQ2PNN: Enabling Two-party Privacy-Preserving Deep Neural Network Inference with Adaptive Quantization"*, Proc. of the 56th IEEE/ACM International Symposium on Microarchitecture **(MICRO)**, Nov. 2023.
- **ICML'23**, *"SpENCNN: Orchestrating Encoding and Sparsity for Fast Homomorphically Encrypted Neural Network Inference"*, 40th International Conference on Machine Learning **(ICML)**, July 2023.
- **ICML'23**, *"COLA: Orchestrating Error Coding and Learning for Robust Neural Network Inference Against Hardware Defects"*, 40th International Conference on Machine Learning **(ICML)**, July 2023.
- **Oakland'23**, *"Spectral-DP: Differentially Private Deep Learning through Spectral Perturbation and Filtering"*, the 44th IEEE Symposium on Security and Privacy **(IEEE S&P, Oakland)**, May, 2023.
- **DAC'23**, *"Neurogenesis Dynamics-inspired Spiking Neural Network Training Acceleration"*, ACM/IEEE 60th Design Automation Conference **(DAC)**, July 2023.
- **USENIX Security'23**, *"NeuroPots: Realtime Proactive Defense against Bit-Flip Attacks in Neural Networks"*, the 32nd USENIX Security Symposium **(USENIX Security)**, Aug. 2023
- **NeurIPS'22**, *"CryptoGCN: Fast and Scalable Homomorphically Encrypted Graph Convolutional Network Inference"*, Thirty-Sixth Annual Conference on Neural Information Processing Systems **(NeurIPS)**, Nov. 2022.
- **ACSAC'22**, *"NeuGuard: Lightweight Neuron-Guided Defense against Membership Inference Attacks"*, Proc. ACM 38th Annual Computer Security Application Conference **(ACSAC)**, Dec. 2022.
- **DAC'21**, *"Neural Pruning Search for Real-Time Object Detection of Autonomous Vehicles",* Proc. ACM/IEEE 58th Design Automation Conference **(DAC)**, June 2021.
- **DAC'20**, *"Stealing Your Data from Compressed Machine Learning Models"*, 57th ACM/IEEE Design Automation Conference **(DAC)**, June 2018.
- **DAC'20**, *"Monitoring the Health of Emerging Neural Network Accelerators with Cost-effective Concurrent Test",* Proc. ACM/IEEE 57th Design Automation Conference **(DAC)**, June 2020.
- **CVPR'19**, *"Machine Vision Guided 3D Medical Image Compression for Efficient Transmission and Accurate Segmentation in the Clouds"*, IEEE Computer Society Conference on Computer Vision and Pattern Recognition (**CVPR**), June 2019.
- **CVPR'19**, *"Feature Distillation: DNN-Oriented JPEG Compression Against Adversarial Examples,"* IEEE Computer Society Conference on Computer Vision and Pattern Recognition (**CVPR**), June 2019.

- **DAC'19**, *"A Fault-Tolerant Neural Network Architecture",* Proc. ACM/IEEE Design Automation Conference **(DAC)**, June 2019.
- **DAC'18**, *"DeepN-JPEG: A Deep Neural Network Favorable JPEG-based Image Compression Framework"*, 55th ACM/IEEE Design Automation Conference **(DAC)**, June 2018.

Publications

Conference Publications: Total **81**, CSRankings Conference–**45**, **Computing**–DAC(**18**), ICCAD(**12**), MICRO, HPCA, ICPP; **Security**–Oakland, USENIX Security, ACSAC, HOST; **AI**–NeurIPS, ICML, CVPR, AAAI, ICCV, ECCV.
**Supervised PhD students are underscored.*

81. **NeurIPS2023**: R. Ran, X. Luo, T. Liu, Wei Wang, Gang Quan and **W. Wen**, "Penguin: Parallel-Packed Homomorphic Encryption for Fast Graph Convolutional Network Inference", Thirty-Seventh Annual Conference on Neural Information Processing Systems **(NeurIPS)**, Dec. 2023, pp 1-13.
80. **NeurIPS2023**: H. Peng*, R. Ran*, Y. Luo, J. Zhao, S. Huang, K. Thorat, T. Geng, C. Wang, X. Xu, **W. Wen**, C. Ding, "LinGCN: Structural Linearized Graph Convolutional Network for Homomorphically Encrypted Inference", Thirty-Seventh Annual Conference on Neural Information Processing Systems **(NeurIPS)**, Dec. 2023, pp 1-13. (* denotes equal contribution)
79. **ICCAD2023**: Z. Yan, Y. Qin, **W. Wen**, X. Hu, Y. Shi, "Improving Realistic Worst-Case Performance of NVCiM DNN Accelerators through Training with Right-Censored Gaussian Noise", Proc. ACM/IEEE 42nd International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2023, pp. 1-9. **(William J. McCalla ICCAD Best Paper Award, 2 out of 750 submissions)** (Acceptance Rate: 172/750=22.9%)
78. **ICCV2023**: H. Peng, S. Huang, T. Zhou, Y. Luo, C. Wang, Z. Wang, J. Zhao, X. Xie, A. Li, T. Geng, K. Mahmood, **W. Wen**, X. Xu, C. Ding, "AutoReP: Automatic ReLU Replacement for Fast Private Network Inference", Proc. of the IEEE/CVF International Conference on Computer Vision **(ICCV)**, Oct. 2023, pp. 5178-5188.
77. **MICRO2023**: Y. Luo, N. Xu, H. Peng, C. Wang, S. Duan, K. Mahmood, **W. Wen**, C. Ding, X. Xu, "AQ2PNN: Enabling Two-party Privacy-Preserving Deep Neural Network Inference with Adaptive Quantization", 56th IEEE/ACM International Symposium on Microarchitecture **(MICRO)**, Nov. 2023, pp. 1-13. (Acceptance Rate: 101/424=23.8%)
76. **ICML2023**: R. Ran, X. Luo, W. Wang, T. Liu, G. Quan and **W. Wen**, "SpENCNN: Orchestrating Encoding and Sparsity for Fast Homomorphically Encrypted Neural Network Inference", the 40th International Conference on Machine Learning **(ICML)**, Aug. 2023, pp. 202:28718-28728.
75. **ICML2023**: A. Yu, N. Lyn, J. Yin, Z. Yan and **W. Wen**, "COLA: Orchestrating Error Coding and Learning for Robust Neural Network Inference Against Hardware Defects", the 40th International Conference on Machine Learning **(ICML)**, Aug. 2023, pp. 202:40277-40289.
74. **Oakland 2023**: C. Feng*, N. Xu*, **W. Wen**, P. Venkitasubramaniam, and C. Ding, "Spectral-DP: Differentially Private Deep Learning through Spectral Perturbation and Filtering", the 44th IEEE Symposium on Security and Privacy **(IEEE S&P 2023 (Cycle 3))**, pp. 1–17. May 2023, pp. 1944–1960. (* denotes equal contribution).
73. **USENIX Security 2023**: Q. Liu, J. Yin, **W. Wen**, C. Yang and S. Sha, "NeuroPots: Realtime Proactive Defense against Bit-Flip Attacks in Neural Networks", the 32nd USENIX Security Symposium **(USENIX Security)**, Aug 2023, pp. 1-19 (Acceptance Rate typically 15%∼18%).

72. **NeurIPS2022**: R. Ran, W. Wang, G. Quan, J. Yin, N. Xu and **W. Wen**, "CryptoGCN: Fast and Scalable Homomorphically Encrypted Graph Convolutional Network Inference", Thirty-Sixth Annual Conference on Neural Information Processing Systems **(NeurIPS)**, Nov. 2022, pp 1-10.

71. **ACSAC2022**: N. Xu, B. Wang, R. Ran, **W. Wen** and P. Venkitasubramaniam, "NeuGuard: Lightweight Neuron-Guided Defense against Membership Inference Attacks", Proc. ACM 38th Annual Computer Security Application Conference **(ACSAC)**, Dec. 2022, pp. 1-15. (Acceptance Rate: 73/303=24.3%)

70. **DAC2023**: S. Huang, H. Fang, K. Mahmood, B. Lei, N. Xu, B. Lei, Y. Sun, D. Xu, **W. Wen** and C. Ding, "Neurogenesis Dynamics-inspired Spiking Neural Network Training Acceleration", the 60th ACM/IEEE Design Automation Conference **(DAC)**, July 2023, pp. 1-6. (Acceptance Rate: 263/1156= 22.7%)

69. **DAC2023**: H. Peng, S. Zhou, Y. Luo, N. Xu, S. Duan, R. Ran, J. Zhao, C. Wang, T. Geng, **W. Wen**, X. Xu and C. Ding, "PASNet: Polynomial Architecture Search Framework for Two-party Computation-based Secure Neural Network Deployment", the 60th ACM/IEEE Design Automation Conference **(DAC)**, July 2023, pp. 1-6. (Acceptance Rate: 263/1156= 22.7%)

68. **DAC2022**: H. Peng, S. Huang, S. Chen, B. Li, W. Jiang, **W. Wen**, J. Bi, H. Liu, and C. Ding, "A Length Adaptive Algorithm-Hardware Co-design of Transformer on FPGA Through Sparse Attention and Dynamic Pipelining", Proc. ACM/IEEE 59th Design Automation Conference **(DAC)**, July 2022, pp. 1-6. (Acceptance Rate: 223/987= 23%, **Top Ranked, Selected as Publicity Paper**)

67. **ICCAD2022**: S. Islam, S. Zhou, R. Ran, Y. Jin, W. Wen, C. Ding and M. Xie, "EVE: Environmental Adaptive Neural Network Models for Low-power Energy Harvesting System", Proc. ACM/IEEE 41st International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2022, pp. 1-9. (Acceptance Rate: 132/586=22.5%)

66. **ASPDAC2022**: A. Yu, N. Lyu, **W. Wen** and Z. Yan, "Reliable Memristive Neural Network Accelerators Based on Early Denoising and Sparsity Induction", Proc. ACM/IEEE 27th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2022, pp. 598-603.

65. **HOST2021**: F. Hosseini, Q. Liu, F. Meng, C. Yang, and **W. Wen**, "Safeguarding the Intelligence of Neural Networks with Built-in Light-weight Integrity MArks (LIMA)", IEEE International Symposium on Hardware Oriented Security and Trust **(HOST)**, Dec. 2021 (Virtual), pp. 1-12.

64. **EMSOFT2021**: F. Hosseini, F. Meng, C. Yang, **W. Wen**, and R. Cammarota, "Tolerating Defects in Low-power Neural Network Accelerators via Retraining-free Weight Approximation", the 21st ACM SIGBED International Conference on Embedded Software **(EMSOFT)**, Oct 2021, pp. 1-21 (Acceptance rate $\sim$ 23%, published in ACM Transactions on Embedded Computing Systems–ACM TECS).

63. **DAC2021**: J. Xie, P. He and **W. Wen**, "Efficient Implementation of Finite Field Arithmetic for Binary Ring-LWE Post-Quantum Cryptography Through a Novel Lookup-Table-Like Method", Proc. ACM/IEEE 58th Design Automation Conference **(DAC)**, June 2021, pp. 1-6 (Acceptance Rate: 23%)

62. **DAC2021**: P. Zhao, G. Yuan, Y. Cai, W. Niu, Q. Liu, **W. Wen**, B. Ren, Y. Wang and X. Lin, "Neural Pruning Search for Real-Time Object Detection of Autonomous Vehicles", Proc. ACM/IEEE 58th Design Automation Conference **(DAC)**, June 2021, pp. 1-6. (Acceptance Rate: 23%)

61. **BIBM2020**: S. Wen, Y. Chen, Z. Liu, **W. Wen**, X. Xu, Y. Shi, T. Ho, Q. Jia M. Huang and J. Zhuang, "Do Noises Bother Human and Neural Networks In the Same Way? A Medical Image

Analysis Perspective", Proc. IEEE International Conference on Bioinformatics and Biomedicine 2020 **(BIBM)**, Dec. 2020, pp. 1166-1170.

60. **ACSAC2020**: T. Liu, Z. Liu, Q. Liu, **W. Wen**, W. Xu and M. Li, "StegoNet: Turn Deep Neural Network into a Stegomalware", Proc. ACM 36th Annual Computer Security Application Conference **(ACSAC)**, Austin, TX, Dec. 2020, pp. 928-938. (Acceptance Rate: 70/302=23%)

59. **ICCAD2020**: Q. Liu, **W. Wen** and Y. Wang, "Concurrent Weight Encoding-based Detection for Bit-Flip Attack on Neural Network Architecture", Proc. ACM/IEEE 39th International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2020, pp. 1-8. (Acceptance Rate: 127/470=27%)

58. **ICCAD2020**: C. Zhang, K. Abdelaal, A. Chen, X. Zhao, **W. Wen** and X. Guo, "ECC Cache: A Lightweight Error Detection for Phase-Change Memory Stuck at Faults", Proc. ACM/IEEE 39th International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2020, pp. 1-9. (Acceptance Rate: 127/470=27%)

57. **ECCV2020**: X. Ma, W. Niu, T. Zhang, S. Liu, S. Lin, H. Li, **W. Wen**, X. Chen, J. Tang, K. Ma, B. Ren, and Y. Wang, "An Image Enhancing Pattern-based Sparsity for Real-time Inference on Mobile Devices", Proc. of the 16th European Conference on Computer Vision **(ECCV)**, Sep. 2020, pp. 1-16. (Acceptance Rate: 1361/5025=27%)

56. **MICCAI2020**: Q. Liu, H. Jiang, T. Liu, Z. Liu, S. Li, **W. Wen** and Y. Shi, "Defending Deep Learning-based Biomedical Image Segmentation from Adversarial Attacks: A Low-cost Frequency Refinement Approach", the 23rd International Conference on Medical Image Computing and Computer Assisted Intervention **(MICCAI)**, Lima, Peru, Oct 2020, pp. 342-351. (Early Accept)

55. **MICCAI2020**: Z. Liu, S. Li, Y. Chen, T. Liu, Q. Liu, X. Xu, Y. Shi, and **W. Wen**, "Orchestrating Medical Image Compression and Remote Segmentation Networks", the 23rd International Conference on Medical Image Computing and Computer Assisted Intervention **(MICCAI)**, Lima, Peru, Oct 2020, pp. 406-416. (Early Accept, **Nominated and Shortlisted for 2020 MICCAI Society Young Scientist Award**)

54. **DAC2020**: N. Xu, Q. Liu, T. Liu, Z. Liu, X. Guo and **W. Wen**, "Stealing Your Data from Compressed Machine Learning Models", Proc. ACM/IEEE 57th Design Automation Conference **(DAC)**, San Francisco, CA, 2020, pp. 1-6. (Acceptance Rate: 228/984=23.0%)

53. **DAC2020**: Q. Liu, T. Liu, Z. Liu, **W. Wen** and C. Yang, "Monitoring the Health of Emerging Neural Network Accelerators with Cost-effective Concurrent Test", Proc. ACM/IEEE 57th Design Automation Conference **(DAC)**, San Francisco, CA, 2020, pp. 1-6. (Acceptance Rate: 228/984=23.0%)

52. **ASPDAC2020**: X. Ma, G. Yuan, S. Lin, C. Ding, F. Yu, T. Liu, **W. Wen**, X. Chen and Y. Wang, "Tiny but Accurate: A Pruned, Quantized and Optimized Memristor Crossbar Framework for Ultra Efficient DNN Implementation," Proc. ACM/IEEE 25th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2020, pp. 301-306. (Acceptance Rate: 86/279=30%)

51. **ICCAD2019**: T. Liu and **W. Wen**, "Making the Fault-Tolerance of Emerging Neural Network Accelerators Scalable", Proc. ACM/IEEE 38th International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2019, pp. 1-5. (Invited Tutorial)

50. **CVPR2019**: Z. Liu, X. Xu, T. Liu, Q. Liu, Y. Wang, Y. Shi, **W. Wen**, M. Huang, H. Yuan and J. Zhuang, "Machine Vision Guided 3D Medical Image Compression for Efficient Transmission and Accurate Segmentation in the Clouds," IEEE Computer Society Conference on Computer Vision and Pattern Recognition (**CVPR**), Long Beach, CA, 2019, pp. 12687-12696.

49. **CVPR2019**: Z. Liu, T. Liu, Q. Liu, N. Xu, X. Lin, Y. Wang and **W. Wen**, "Feature Distillation: DNN-Oriented JPEG Compression Against Adversarial Examples," IEEE Computer Society Conference on Computer Vision and Pattern Recognition (**CVPR**), Long Beach, CA, 2019, pp. 860-868.
48. **DAC2019**: T. Liu, **W. Wen**, L. Jiang, Y. Wang, C. Yang and G. Quan, "A Fault-Tolerant Neural Network Architecture", Proc. ACM/IEEE Design Automation Conference **(DAC)**, Las Vegas, NV, 2019, pp. 1-6. (Acceptance Rate: 202/815=24.8%)
47. **HPCA2019**: Z. Li, C. Ding, S. Wang, **W. Wen**, Y. Zhuo, C. Liu, Q. Qiu, W. Xu, X. Lin, X. Qian, Y. Wang, "E-RNN: Design Optimization for Efficient Recurrent Neural Networks in FPGAs," Proc. of the 25th International Symposium on High-Performance Computer Architecture **(HPCA)**, Feb. 2019, pp. 69-80. (Acceptance Rate: 46/233=19.7%)
46. **CCGRID2019**: S. Homsi, G. Quan, **W. Wen**, G. A. Chapparo-Baquero and L. Njilla, "Game Theoretic-Based Approaches for Cybersecurity-Aware Virtual Machine Placement in Public Cloud Clusters", the 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing **(CCGRID)**, May 2019, pp. 272-281. (Acceptance Rate: 47/207=22.7%)
45. **AAAI2019**: Y. Wang, Z. Zhan, J. Tang, B. Yuan, L. Zhao, **W. Wen**, S. Wang, and X. Lin, "Universal Approximation Property and Equivalence of Stochastic Computing-based Neural Networks and Binary Neural Networks," Proc. of the 33rd AAAI Conference on Artificial Intelligence **(AAAI)**, Feb. 2019, pp. 5369-5376. (Acceptance Rate: 1150/7095=16.2%).
44. **WiSec2019**: T. Liu and **W. Wen**, "Deep-evasion: Turn deep neural network into evasive self-contained cyber-physical malware: poster", Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks **(WiSec)**, May 2019, pp. 320-321.
43. **ASP-DAC2019**: T. Liu, N. Xu, Q. Liu, Y. Wang, and **W. Wen**, "A System-level Perspective to Understand the Vulnerability of Deep Learning Systems," Proc. ACM/IEEE 23rd Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2019, pp. 506-511. (Invited Special Session)
42. **ICCAD2018**: S. Wang, X. Wang, P. Zhao, **W. Wen**, D. Kaeli, P. Chin, and X. Lin, "Defensive dropout for hardening deep neural networks under adversarial attacks," IEEE/ACM International Conference On Computer Aided Design **(ICCAD)**, Nov. 2018, pp. 71:1-71:8. (**Best Paper Award Nomination**, Acceptance Rate: 98/396=25%)
41. **ICCAD2018**: Q. Lou, **W. Wen**, and L. Jiang, "3DICT: A Reliable and QoS Capable Mobile Process-In-Memory Architecture for Lookup-based CNNs in 3D XPoint ReRAMs," IEEE/ACM International Conference On Computer Aided Design **(ICCAD)**, Nov. 2018, pp. 53:1-53:8. (**Best Paper Award Nomination** from track–Hardware for Embedded Systems, Acceptance Rate: 98/396=25%)
40. **ECCV2018**: T. Zhang, S. Ye, K. Zhang, J. Tang, **W. Wen**, M. Fardad, and Y. Wang, "A Systematic DNN Weight Pruning Framework using Alternating Direction Method of Multipliers," Proc. of the 15th European Conference on Computer Vision **(ECCV)**, Sep. 2018, pp. 1-16. (Acceptance Rate: 717/2439=29%)
39. **DAC2018**: Z. Liu, T. Liu, **W. Wen**, L. Jiang, J. Xu, Y. Wang and G. Quan, "DeepN-JPEG: A Deep Neural Network Favorable JPEG-based Image Compression Framework," Proc. 55th ACM/IEEE Design Automation Conference **(DAC)**, June 2018, pp. 1-6. (Acceptance Rate: 168/691=24.3%)
38. **HOST2018**: T. Liu, **W. Wen** and Y. Jin, "SIN^2: Stealth Infection on Neural Network–A Low-cost Agile Neural Trojan Attack Methodology," Proc. IEEE International Symposium on Hardware Oriented Security and Trust **(HOST)**, Washington, DC, May 2018, pp. 227-230. (Acceptance Rate: 22/84=26.2%)

37. **ASP-DAC2018**: Q. Liu, T. Liu, Z. Liu, Y. Wang, Y. Jin and **W. Wen**, "Security Analysis and Enhancement of Model Compressed Deep Learning Systems under Adversarial Attacks," Proc. ACM/IEEE 23rd Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2018, pp. 721-726. **(Best Paper Award Nomination)**

36. **ASP-DAC2018**: T. Liu, L. Jiang, Y. Jin, G. Quan and **W. Wen**, "PT-Spike: A Precise-Time-Dependent Single Spike Neuromorphic Architecture with Efficient Supervised Learning," Proc. IEEE 23rd Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2018, pp. 568-573.

35. **ISVLSI2018**: Z. Liu, T. Liu, J. Guo, N. Wu and **W. Wen**, "An ECC-Free MLC STT-RAM Based Approximate Memory Design for Multimedia Applications," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Jul. 2018, pp. 142-147. (Oral Acceptance Rate: 57/192=29%)

34. **ISVLSI2018**: T. Liu, Z. Liu, Q. Liu and **W. Wen**, "Enhancing the Robustness of Deep Neural Networks from "Smart" Compression," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Jul. 2018, pp. 528-532. (Invited Special Session)

33. **ICC2018**: H. Wu, L. Chen, C. Shen, **W. Wen** and J. Xu, "Online Geographical Load Balancing for Energy-Harvesting Mobile Edge Computing," IEEE International Conference on Communications (ICC) 2018 Green Communications Systems and Networks Symposium, May. 2018, pp. 1-6.

32. **ICCAD2017**: T. Liu, Z. Liu, F. Lin, Y. Jin, G. Quan, and **W. Wen**, "MT-Spike: A Multilayer Time-based Spiking Neuromorphic Architecture with Temporal Error Backpropagation," Proc. ACM/IEEE International Conference on Computer-Aided Design **(ICCAD)**, Nov. 2017, pp. 1-8. **(Best Paper Award Nomination from track–Hardware for Embedded Systems)**

31. **DATE2016**: **W. Wen**, M. Mao, H. Li, Y. Chen, Y. Pei and N. Ge, "A Holistic Tri-region MLC STT-RAM Design with Combined Performance, Energy, and Reliability Optimizations," Proc. ACM/IEEE Design, Automation & Test in Europe **(DATE)**, Mar. 2016, pp. 1285-1290. **(Best Paper Award Nomination, 13 out of 829, top 1.5%)**

30. **ISLPED2017**: L. Jiang, M. Kim, **W. Wen**, and D. Wang, "XNOR-POP: A Processing-in-Memory Architecture for Binary Convolutional Neural Networks in Wide-IO2 DRAMs," Proc. ACM/IEEE International Symposium on Low Power Electronics and Design **(ISLPED)**, Aug. 2017, pp. 1-6. (Acceptance Rate: 24%)

29. **ASP-DAC2017**: Z. Liu, **W. Wen**, L. Jiang, Y. Jin, and G. Quan, "A Statistical STT-RAM Retention Model for Fast Memory Subsystem Designs," Proc. ACM/IEEE 21th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2017, pp. 720-725. (Acceptance rate: 111/358 = 31%)

28. **ASP-DAC2017**: X. Yang and **W. Wen**, "Design of A Pre-scheduled Data Bus (DBUS) for Advanced Encryption Standard (AES) Encrypted System-on-Chips (SoCs)," Proc. ACM/IEEE 21th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2017, pp. 506-511. (Acceptance rate: 111/358 = 31%)

27. **ASP-DAC2017**: A. Ren, S. Liu, R. Cai, **W. Wen**, P. Varshney and Y. Wang, "Algorithm-Hardware Co-optimization of Memristor-Based Framework for Solving SOCP and Homogeneous QCQP Problems," Proc. ACM/IEEE 21th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2017, pp. 788-793. (Acceptance rate: 111/358 = 31%)

26. **GLSVLSI2017**: L. Jiang, S. Mittal, and **W. Wen**, "Building a Fast and Power Efficient Inductive Charge Pump System for 3D Stacked Phase Change Memories," Proc. ACM Great Lakes Symposium on VLSI (GLSVLSI), May 2017, pp. 275-280.

25. **GLSVLSI2017**: S. Sha, **W. Wen**, S. Ren and G. Quan, "A Thermal-Balanced Variable-Sized-Bin-Packing Approach for Energy Efficient Multi-Core Real-Time Scheduling," Proc. ACM Great Lakes Symposium on VLSI (GLSVLSI), May 2017, pp. 257-262.

24. **ISQED2017**: T. Liu, and **W. Wen**, "A Fast and Ultra Low Power Time-Based Spiking Neuromorphic Architecture for Embedded Applications," Proc. IEEE 18th International Symposium on Quality Electronic Design (ISQED), Mar. 2017, pp. 19-22. (Invited Special Session)

23. **ISQED2017**: G. Chaparro-Baquero, S. Sha, S. Homsi, **W. Wen** and G. Quan, "Processor/Memory Co-scheduling Using Periodic Resource Server for Real-Time System Under Peak Temperature Constraints," Proc. IEEE 18th International Symposium on Quality Electronic Design (ISQED), Mar. 2017, pp. 360-366.

22. **ICCAD2016**: C. Yang, B. Liu, **W. Wen**, M. Barnell, Q. Wu, H. Li, Y. Chen and J. Rajendran, "Security of Neuromorphic Computing: Thwarting Learning Attacks Using Memristor's Obsolescence Effect," Proc. ACM/IEEE International Conference on Computer Aided Design **(ICCAD)**, Nov. 2016, pp. 1-6. (Acceptance rate: 97/408 = 24%)

21. **ICCAD2016**: S. Li, **W. Wen**, Y. Wang, Q. Qiu, Y. Chen and H. Li, "A Data Locality-aware Design Framework for Reconfigurable Sparse Matrix-Vector Multiplication Kernel," Proc. ACM/IEEE International Conference on Computer Aided Design **(ICCAD)**, Nov. 2016, pp. 1-6. (Acceptance rate: 97/408 = 24%)

20. **ICPP2016**: S. Sha, **W. Wen**, M. Fan, S. Ren and G. Quan, "Performance Maximization via Frequency Oscillation on Temperature Constrained Multicore Processors," Proc. ACM/IEEE International Conference on Parallel Processing **(ICPP)**, Aug. 2016, pp. 526-535. (Acceptance rate: 53/251 = 21.1%)

19. **DAC2016**: X. Chen, N. Khoshavi, J. Zhou, D. Huang, R. DeMara, J. Wang, **W. Wen** and Y. Chen,"AOS: Adaptive Overwrite Scheme for Energy-Efficient MLC STT-RAM Cache," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2016, pp. 1-6. (Acceptance rate: 152/878 = 17.3%)

18. **DAC2016**: T. W, Q. Han, S. Sha, **W. Wen**, G. Quan and M. Qiu, "On Harmonic Fixed-Priority Scheduling of Periodic Real-Time Tasks with Constrained Deadlines," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2016, pp. 1-6. (Acceptance rate: 152/878 = 17.3%)

17. **DAC2016**: E. Eken, L. Song, I. Bayram, C. Xu, **W. Wen**, Y. Xie and Y. Chen, "NVSim-VXs: An Improved NVSim for Variation Aware STT-RAM Simulation," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2016, pp. 1-6. (Acceptance rate: 152/878 = 17.3%)

16. **DAC2016**: M. Mao, **W. Wen**, X. Liu, J. Hu, D. Wang, Y. Chen and H. Li, "TEMP: Thread Batch Enabled Memory Partitioning for GPU," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2016, pp. 1-6. (Acceptance rate: 152/878 = 17.3%)

15. **DATE2016**: X. Wang, M. Mao, E. Eken, **W. Wen**, H. Li and Y. Chen, "Sliding Basket: An Adaptive ECC Scheme for Runtime Write Failure Suppression of STT-RAM Cache," Proc. ACM/IEEE Design, Automation & Test in Europe **(DATE)**, Mar. 2016, pp.762-767. (Acceptance rate: 199/824 = 24.0%).

14. **ASP-DAC2016**: L. Jiang, **W. Wen**, D. Wang and L. Duan, "Improving Read Performance of STT-MRAM based Main Memories through Smash Read and Flexible Read," Proc. ACM/IEEE 21th Asia and South Pacific Design Automation Conference (ASP-DAC), Jan. 2016, pp.31-36. (Acceptance rate: 94/274 = 34.3%)

13. **ASP-DAC2016**: X. Zhang, G. Sun, Y. Zhang, **W. Wen**, Y. Chen, H. Li, "A Novel PUF based on Cell Error Rate Distribution of STT-RAM," Proc. ACM/IEEE 21th Asia and South Pacific Design Automation Conference (ASP-DAC), Jan. 2016, pp.342-347. (Acceptance rate: 94/274 = 34.3%)
12. **ISVLSI2016**: K. Shamsi, Y. Jin and **W. Wen**, "Hardware Security Challenges Beyond CMOS: Attacks and Remedies," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Jul. 2016, pp. 200-205 (Invited Special Session).
11. **ISVLSI2016**: B. Li, Y. Pei and **W. Wen**, "Efficient Low-Density Parity-Check (LDPC) Code Decoding for Combating Asymmetric Errors in STT-RAM," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Jul. 2016, pp. 266-271.
10. **DAC2015**: J. Guo, **W. Wen**, J. Hu, D. Wang, H. Li and Y. Chen, "FlexLevel: a Novel NAND Flash Storage System Design for LDPC Latency Reduction," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2015, pp. 1-6. (Acceptance rate: 162/789=20.5%)
9. **DAC2014**: **W. Wen**, Y. Zhang, M. Mao and Y. Chen, "State-Restrict MLC STT-RAM Designs for High-Reliable High-Performance Memory System," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2014, pp. 1-6. **(Best Paper Award Nomination, 7 out of 787, 0.9%)**
8. **DAC2014**: M. Mao, **W. Wen**, Y. Zhang, H. Li and Y. Chen, "Exploration of GPGPU Register File Architecture Using Domain-wall-shift-write based Racetrack Memory," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2014, pp. 1-6. (Acceptance rate: 174/787 = 22.1%)
7. **DAC2014**: E. Eken, Y. Zhang, **W. Wen**, R. Joshi, H. Li and Y. Chen, "A New Field-Assisted Access Scheme of STT-RAM with Self-Reference Capability,", Design Automation Conference **(DAC)**, Jun. 2014, pp. 1-6. (Acceptance rate: 174/787 = 22.1%)
6. **ISCE2014**: **W. Wen**, Y. Zhang, M. Mao and Y. Chen, "STT-RAM Reliability Enhancement through ECC and Access Scheme Optimization", International Symposium on Consumer Electronics, Jun. 2014, pp. 1-2.
5. **ICCAD2013**: **W. Wen**, M. Mao, X. Zhu, S. Kang, D. Wang and Y. Chen, "CD-ECC: Content-Dependent Error Correction Codes for Combating Asymmetric Nonvolatile Memory Operation Errors," Proc. ACM/IEEE International Conference on Computer Aided Design **(ICCAD)**, Nov. 2013, pp. 1-8. (Acceptance rate: 92/354 = 26%)
4. **DAC2012**: **W. Wen**, Y. Zhang, Y. Chen, Y. Wang and Y. Xie, "PS3-RAM: A Fast Portable and Scalable Statistical STT-RAM Reliability Analysis Method," Proc. ACM/IEEE Design Automation Conference **(DAC)**, Jun. 2012, pp. 1191-1196. (Acceptance rate: 168/741 = 23%)
3. **DATE2013**: J. Guo, **W. Wen**, and Y. Chen, "DA-RAID-5: A Disturb Aware Data Protection Technique for NAND Flash Storage Systems," Proc. ACM/IEEE Design, Automation & Test in Europe **(DATE)**, Mar. 2013, pp. 380-385. (Acceptance rate: 92/354 = 26.0%)
2. **ASP-DAC2013**: **W. Wen**, Y. Zhang, L. Zhang and Y. Chen, "Loadsa: A Yield-Driven Top-Down Design Method for STT-RAM Array," Proc. ACM/IEEE 18th Asia and South Pacific Design Automation Conference **(ASP-DAC)**, Jan. 2013, pp. 291-296. (Acceptance rate ∼31.2%)
1. **ICCAD2012**: Y. Zhang, L. Zhang, **W. Wen**, G. Sun and Y. Chen, "Multi-level Cell STT-RAM: Is It Realistic or Just a Dream?" Proc. ACM/IEEE International Conference on Computer Aided Design **(ICCAD)**, Nov. 2012, pp. 526-532. (Acceptance rate: 82/338 = 24.3%)

Journal Publications: Total **20**

20. **TNNLS2021**: Q. Liu and **W. Wen**, "Model Compression Hardens Deep Neural Networks: A New Perspective to Prevent Adversarial Attacks", IEEE Transactions on Neural Networks and Learning Systems (TNNLS), June 2021, pp. 1–12.
19. **TODES2020**: S. Sha, A. Bankar, **W. Wen** and G. Quan, "On Fundamental Principles for Thermal-Aware Design on Periodic Real-Time Multi-Core Systems", ACM Transactions on Design Automation of Electronic Systems **(TODAES)**, 2020, vol. 25, no. 2, pp. 23:1–23:23.
18. **TCAD2020**: C. Yang, B. Liu, H. Li, Y. Chen, M. Barnell, Q. Wu, **W. Wen** and J. Rajendran, "Thwarting Replication Attack against Memristor-based Neuromorphic Computing System," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, Oct. 2020, vol. 39, no. 10, pp. 2192-2205.
17. **CCF-Trans2020**: T. Liu, G. Quan and **W. Wen**, "FPT-spike: a Flexible Precise-time-dependent Single-spike Neuromorphic Computing Architecture", CCF Transactions on High Performance Computing (HPC), June 2020, pp. 1-16.
16. **JETC2019**: B. Li, M. Mao, X. Liu, T. Liu, Z. Liu, **W. Wen**, Y. Chen and H. Li, "Thread Batching for High-performance Energy-efficient GPU Memory Design", ACM Journal on Emerging Technologies in Computing Systems **(JETC)**, Dec. 2019, vol. 15, no. 4, pp. 39:1-39:21.
15. **PARCO2019**: S. Sha, **W. Wen**, G. Chaparro-Baquero and G. Quan, "Thermal-Constrained Energy Efficient Real-Time Scheduling on Multi-Core Platforms," Parallel Computing (PARCO), vol. 85, 2019, pp. 231-242, ISSN 0167-8191, https://doi.org/10.1016/j.parco.2019.01.003.
14. **TPDS2018**: S. Sha, **W. Wen**, S. Ren and G. Quan, "M-Oscillating: Performance Maximization on Temperature-Constrained Multi-Core Processors," IEEE Transactions on Parallel and Distributed Systems **(TPDS)**, Nov. 2018, vol. 29, no. 11, pp. 2528-2539.
13. **TCAD2018**: Z. Liu, M. Mao, T. Liu, X. Wang, **W. Wen**, Y. Chen, H. Li, D. Wang, Y. Pei and N. Ge, "TriZone: A Design of MLC STT-RAM Cache for Combined Performance, Energy, and Reliability Optimizations," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, Oct. 2018, vol. 37, no. 10, pp. 1985-1998.
12. **JETC2018**: B. Li, Y. Pei and **W. Wen**, "Efficient LDPC Code Design for Combating Asymmetric Errors in STT-RAM," ACM Journal on Emerging Technologies in Computing Systems **(JETC)**, Mar. 2018, vol. 14, no. 1, pp. 10:1-10:20.
11. **TC2017**: M. Mao, **W. Wen**, Y. Zhang, Y. Chen and H. Li, "An Energy-Efficient GPGPU Register File Architecture Using Racetrack Memory," IEEE Transactions on Computers **(TC)**, Apr. 2017, vol. 66, no. 9, pp. 1478-1490.
10. **JETC2017**: X. Yang, **W. Wen** and F. Ming, "Improving AES Core Performance via An Advanced ASBUS Protocol," ACM Journal on Emerging Technologies in Computing Systems **(JETC)**, Dec. 2017, vol. 14, no. 1, pp. 6:1-6:23.
9. **TC2016**: X. Chen, N. Khoshavi, R. DeMara, J. Wang, J. Zhou, D. Huang, **W. Wen**, Y. Chen, "Energy-Aware Adaptive Restore Schemes for MLC STT-RAM Cache," IEEE Transactions on Computers **(TC)**, Nov. 2016, vol. 66, no. 5, pp. 786-798. **(Feature Paper of Month–May, 2017)**
8. **TCAD2016**: J. Guo, **W. Wen**, J. Hu, D. Wang, H. Li and Y. Chen, "FlexLevel NAND Flash Storage System Design to Reduce LDPC Latency," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, Oct. 2016, vol. 36, no. 7, pp. 1167-1180.

7. **TCAD2014**: **W. Wen**, Y. Zhang, Y. Chen, Y. Wang and Y. Xie, "PS3-RAM: A Fast Portable and Scalable Statistical STT-RAM Reliability/Energy Analysis Method," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, Nov. 2014, vol. 33, no. 11, pp. 1644-1656.
6. **TMAG2014**: E. Eken, Y. Zhang, **W. Wen**, R. Joshi, H. Li, and Y. Chen, "A Novel Self-reference Technique for STT-RAM Read and Write Reliability Enhancement," IEEE Transaction on Magnetics **(TMAG)**, Nov. 2014, vol. 50, no. 11, 3401404.
5. **TMAG2012**: Y. Zhang, **W. Wen**, and Y. Chen, "The Prospect of STT-RAM Scaling from Read ability Perspective," IEEE Transaction on Magnetics **(TMAG)**, vol. 48, no. 1, Nov. 2012, pp. 3035-3038.
4. **SPIN2013**: Y. Zhang, **W. Wen**, and Y. Chen, "STT-RAM Cell Design Considering MTJ Asymmetric Switching," SPIN, vol. 2, no. 3, Nov. 2013, 1240007.
3. **JETC2013**: Y. Chen, W. Wong, H. Li, C.-K. Koh, Y. Zhang, and **W. Wen**, "On-chip Caches built on Multi-Level Spin-Transfer Torque RAM Cells and Its Optimizations," ACM Journal on Emerging Technologies in Computing Systems **(JETC)**, vol. 9, no 2, article 16, May 2013.
2. **IET2011**: C. Geng, Y. Pei, **W. Wen**, Z. Luan, N. Ge, "ASIC implementation of fractionally spaced Rake receiver for high data rate UWB," IET Electronic Letters, vol. 47, no. 3, 2011, pp. 215-217.
1. **W. Wen**, Y. Pei and N. Ge, "ASIC design optimization of a decision feedback equalizer at Single-Carrier Ultra-wideband," Journal of Tsinghua University (Science and Technology), vol. 50, no. 4, 2010, pp. 577-580.

Book Chapters:

1. Y. Zhang, **W. Wen**, and Y. Chen, "Asymmetry in STT-RAM Cell Operations," (in Emerging Memory Technologies: Design, Architecture, and Applications, Editor: Yuan Xie), Springer, Aug. 31, 2013, ISBN: 978-14-419-9550-6.
2. **W. Wen**, Y. Zhang, and Y. Chen, "Statistical Reliability/Energy Characterization in STT-RAM Cell Designs," (in Spintronics Based Computing, Editors: Weisheng Zhao and Guillaume Prenat), Springer, Jun. 14, 2015. ISBN:978-3-319-15179-3.
3. Y. Zhang, **W. Wen**, H. Li, and Y. Chen, "The Prospect of STT-RAM Scaling, (in Metallic Spintronic Devices," Editor: Xiaobin Wang), CRC Press, Aug. 4, 2014. ISBN: 978-14-665-8844-8.

Patents Granted

- **W. Wen**, E. Eken, H. Li, X. Bi, and Y. Chen, "Spin-transfer Torque Memory Magnetic-assisted Nondestructive Self-reference Sensing Method," US Provisional Patent Application (US9627024 B2), Apr 18, 2017.

Teaching & Research Advising

Courses*: Total 8 (1 at NCSU, 4 at Lehigh and 3 at FIU)

- NCSU-Graduate: CSC591/791/ECE591 "Software-Hardware Co-design for Intelligent Systems", FL23 (Enrollment: 12)
- Lehigh-Graduate: ECE450 "Software-Hardware Co-design of Deep Learning Systems" (new course created by me), FL19/FL20/SP22/FL22 (Enrollment: 9/5/15/11, Average Score: 4.9/4.9/4.4 of 5);

- Lehigh-Undergraduate/Graduate Core: ECE319 "Digital System Design", FL21 (Enrollment: 7, Average Score: 4.92 of 5);
- Lehigh-Undergraduate Core: ECE201 "Computer Architecture", SP22 (Enrollment: 33 undergraduates, Average Score: 3.8 of 5);
- Lehigh-Undergraduate/Graduate: ECE350/450 "Computer-Aided Design of Digital Systems", SP20/SP21 (COVID-19) (new course created by me), Enrollment: 5/3;
- FIU-Undergraduate Core: EEL3712 "Logic Design", Fall 2017/2018, Spring 2018/2019, Average Enrollment 55, SP19 (Enrollment: 55, Average Score: 4.2 of 5)
- FIU-Graduate: EEL6167 "VLSI Design", FL 2015/2016/2017/2018, Average Enrollment 7, FL18 (Enrollment: 7, Average Evaluation Score: 4.8 of 5)
- FIU-Graduate level: EEL6726 "Advanced VLSI Design", SP 2016/2017/2018/2019, Average Enrollment 6, SP19 (Enrollment 7, Average Score: 4.5 of 5).

**Teaching load at Lehigh is 1+1 from FL19 to SP20 (the first 2 years), then 1+2 (1 in FL21 and 2 in SP22)*

**Teaching load at FIU is 1+1 in the first 2 years), then 2+2 in year 3 and 4.*

Research Advising

PhD/Master Students–5 PhDs, 2 Masters

- Ran Ran, *Ph.D. at NCSU*, Since 08/2023. Topic: Algorithm-Hardware Co-Design for Accelerating Encrypted Machine Learning; (Passed Written Prelim Exam), Expected Graduate Date: 05/2025. (Research Intern at VISA, Summer'24)
- Nuo Xu, *Ph.D. at Lehigh ECE*, Since 09/2019, Topic: "Tackling Emerging Data Privacy Risks in Machine Learning", Expected Graduate Date: 05/2024. (Research Intern at Oak Ridge National Lab, Summer'24)
- Anlan Yu, *Female Ph.D. at Lehigh ECE*, Co-advise with Prof. Zhiyuan Yan, Since 09/2021, Topic: Orchestrating Coding and Learning for Reliable and Secure Neural Network Processing. Expected Graduate Date: 12/2024. (Intern at Google Youtube Group, Fall'23)
- Qiying Li, *Female Ph.D. at Lehigh ECE*, Since 08/2023, Co-advise with Prof. Zhiyuan Yan and Prof. YaLin Liu (Lehigh Bioengineering/Mechanical Engineering), funded by NSF MRI project.
- Xinwei Luo, *Ph.D. at Lehigh ECE*, 06/2022-08/2023, Now PhD at Lehigh CSE Department
- Alex Schiffman, *Master at Lehigh ECE*, Since 05/2021, Thesis: "Practical 6D Object Pose Estimation with Deep Learning", Graduate Date: 12/2021. **First Employment:** Software R&D Engineering at Medtronic, North Haven, Connecticut.
- Han Jiang, *Master at Lehigh ECE*, 12/2019-05/2020, Topic: "AI-Assisted Medical Imaging" (One second-author paper at top medical AI conference-MICCAI2021), Graduate Date: 05/2021.
  First Employment: Software Engineer at U.S. Bancorp, Concord CA.

Graduated PhDs: 3

- Qi Liu, *Ph.D. at Lehigh University*, 09/2019-06/2022;
  Ph.D. Thesis: "Enhancing the Security and Reliability of Deep Learning Systems under Attacks and Hardware Faults".
  First Employment: Amazon Applied Research Scientist.

- Zihao Liu, *Ph.D. at FIU, Visiting Ph.D. at Lehigh*, 01/2016-07/2020;
  Ph.D. Thesis: "Machine vision, NOT Human Vision, Guided Compression towards Low-Latency and Robust Deep Learning Systems".
  First Employment: Research Scientist at Alibaba DAMO Academy.
- Tao Liu, *Ph.D. at FIU, Visiting Ph.D. at Lehigh*, 09/2016–07/2020;
  Ph.D. Thesis: "A System-level Perspective Towards Efficient, Reliable and Secured Neural Network Computing".
  First Employment: Tenure-Track Assistant Professor at Lawrence Technological University.

Undergraduate Students

- Lehigh ECE (3)-George Huang, Xinchen Ma, and Colin Li;
  Senior Design Project Title: "Body Controlled UAV", 09/2020-05/2021;
- Lehigh ECE (2)-Casper Coleman (Female), Daniel Onyemelukwe;
  Senior Design Project Title: "What's My Food? The Fridge Food Tracker", 09/2019-05/2020.
- FIU ECE (4)-Antonio Rubio (Hispanic), Geovanys Garcia (Hispanic), Thony Yan, Nicky Yan Liang;
  Project Title: "IMay, Machine Learning for the Everyday User", 09/2018-08/2019.

Achievements of Advised Students

- Ran Ran: Travel Award ($1,000), College of Engineering, NCSU.
- Tao Liu: 1) Best Paper Nomination at ASP-DAC2018; 2) A. Richard Newton Young Student Fellow Award at DAC2017; 3) ACM Student Research Competition (SRC) Travel Award at ICCAD2017; 4) Graduate Travel Grants (twice) at HOST2017/HOST2018.
- Zihao Liu: 1) 2020 MICCAI Society Young Scientist Award Nomination and Shortlist; 2) Travel Grant for Non-volatile Memories Workshop 2016, UCSD.
- Qi Liu: 1) Best Paper Nomination at ASP-DAC2018; 2) Young Student Fellow Award at DAC2020.
- Nuo Xu, Young Student Fellow Award at DAC2020;
- Ruoyu Wang, Lehigh University Presidential Fellowship, 09/2020-08/2021.

SERVICE

University

- ECE Department, Lehigh: Faculty Search Committee, 2020, 2022.
- ECE Department, Lehigh: Computer Engineering Curriculum Committee, 09/2019–Current.
- ECE Department, Lehigh: Colloquium Chair, 09/2021–Current.
- RCEAS (College), Lehigh: Library Technology Services (LTS) Faculty Committee, 09/2020–Current.

Professional
Conference Service-Leadership

- **General Chair**, the 18th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Miami, Florida, 2019;
- **General Co-Chair/Organizer**, the 1st **T**rustworthy and **R**eliable **AI** accelerator desig**N (TRAIN)** Workshop at Embedded Systems Week (ESWEEK), Oct, 2021. web: `https://sites.google.com/view/trainworkshop2021`.

- **Organizing Committee**, NSF Computer System Research (CSR) PI Meeting, Oct. 2023.
- **Lead Organizing Committee Member**, ACM/IEEE Design Automation Conference (DAC) Early Career Workshop (Virtual), 2020.
- **Technical Program Committee (TPC) Co-Chair**, the 17th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Hong Kong SAR, China, 2018.
- **Technical Area Co-Chair**, **AI/ML Security/Privacy Track** for ACM/IEEE Design Automation Conference (DAC), 2022.
- **Technical Area Co-Chair**, "VLSI for Machine Learning and Artificial Intelligence", ACM Great Lakes Symposium on VLSI (GLSVLSI), 2020, 2021.
- **Technical Area Chair**, "Embedded System Architecture and Design", ACM/IEEE Asia and South Pacific Design Automation Conference (ASPDAC), Tokyo, Japan, 2019.
- **Technical Area Chair**, "Emerging and Evolutionary Design", 30th IEEE International System-on-Chip Conference (SOCC), Munich Germany, 2017.
- **Financial Chair**, 15th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh PA, 2016.
- **Publication Chair**, IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems (AICAS), 2021.
- **Poster Session Chair/Organizing Committee**, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington DC, 2017.
- Special Session Organizer and Contributor of "Emerging Trends in Energy Efficient and Secure Neural Network Acceleration", 17th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Hong Kong SAR, China, 2018.
- Special Session Organizer and Contributor of "Emerging Devices for Hardware Security: Fiction or Future", 15th IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh PA, 2016.
- Embedded Tutorial Contributor of "When Neural Networks Meet Hardware: The Princess, The Knight, and the Very Bad Dragon", 38th ACM/IEEE International Conference on Computer-Aided Design (ICCAD), Westminster CO, 2019.
- Session Chair, ACM/IEEE International Conference on Computer-Aided Design (ICCAD), Nov. 2020.
- Session Chair, ACM/IEEE Design Automation Conference (DAC) 2018.
- Session Chair, IEEE International Conference on Computer-Aided Design (ICCAD) 2015, 2017, 2018.
- Session Chair, IEEE Asia and South Pacific Design Automation Conference (ASP-DAC), 2017, 2018.

Technical Program Committee Member

- Embedded Systems Week (ESWEEK), IEEE International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), 2023;
- ACM/IEEE Design Automation Conference (DAC), 2019, 2020, 2021, 2022;
- IEEE International Symposium on High-Performance Computer Architecture (HPCA)-External Review Committee, 2023;
- ACM/IEEE Design, Automation & Test in Europe (DATE), 2020;

- ACM/IEEE International Conference on Computer Aided Design (ICCAD), 2017, 2018, 2019;
- IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2019, 2020, 2021;
- IEEE Asia and South Pacific Design Automation Conference (ASP-DAC), 2017, 2018, 2019, 2021, 2023;
- IEEE International Conference on Computer Design (ICCD), 2017;
- ACM Great Lakes Symposium on VLSI (GLSVLSI), 2017, 2018, 2019, 2020;
- IEEE International Conference on VLSI Design and 15th International Conference on Embedded Systems Design (VLSID), 2015-2017;
- IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016-2018;
- IEEE International Conference on Network, Storage and Architecture (NAS), 2016;
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2016-2017.

Editorship

- Associate Editor, IEEE Circuits and Systems (CAS) Magazine, 2020-Present;
- Associate Editor, Neurocomputing, 2018-Present;
- Guest Editor, IEEE Transactions on Circuits and Systems I: Regular Papers, Special Issue, 2022;
- Guest Editor, IEEE Transactions on Circuits and Systems II (TCAS): Express Briefs, Special Issue, 2020-2021;
- Guest Editor, ACM Journal on Emerging Technologies in Computing (JETC) Special Issue on New Trends in Nanoelectronic Device, Circuit and Architecture Design, 2019-2020.

Selected Reviewer/Panelist

- Panelist, NSF CISE **(Career)** Program, 2023;
- Panelist, NSF CISE Program **(Medium)**, 2021;
- Panelist, U.S. Department of Energy (DOE) Office of Science, 2016, 2018, 2019;
- Reviewer, Army Research Office (ARO) Grant, 2017;
- Reviewer, Hong Kong Research Grant Council (RCG), 2020, 2021, 2023;
- IEEE Transactions on Pattern Analysis and Machine Intelligence (**TPAMI**);
- IEEE Transactions on Neural Networks and Learning Systems (**TNNLS**);
- IEEE Transactions on Very Large Scale Integration (**TVLSI**) Systems;
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**);
- IEEE Transactions on Multi-Scale Computing Systems (**TMSCS**);
- IEEE Transactions on Electron Devices (**TED**);
- ACM Transactions on Privacy and Security (**TOPS**);
- ACM Journal on Emerging and Selected Topics in Circuits and Systems (**JETC**);
- ACM Transactions on Design Automation of Electronic Systems (**TODAES**);

- ACM Transactions on Embedded Computing Systems (**TECS**);
- IEEE Transactions on Computers (**TC**);
- IEEE Transactions on Communications (**TCOM**);
- IEEE Journal on Emerging and Selected Topics in Circuits and Systems (**JETCAS**);
- IEEE Transactions on Circuit and Systems II (**TCAS-II**);
- IEEE Transactions on Nanotechnology (**TNANO**);
- IEEE Design & Test of Computers (**D&T**);
- IEEE Transactions on Cyber-Physical Systems (**TCPS**);
- IEEE Embedded Systems Letters (**ESL**);
- IEEE Transactions on Sustainable Computing (**TSUSC**);
- IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (**RTCSA**);
- IEEE International Test Conference (**ITC**);
- IEEE International Symposium on Circuits and Systems (**ISCAS**).