

# *Adnan Siraj Rakin*

Assistant Professor, School of Computing, Binghamton University (SUNY)

Email: [arakin@binghamton.edu](mailto:arakin@binghamton.edu)

[Website](#)

[Google Scholar](#)

[Research Gate](#)

## **Areas of Specialization**

- AI Security (attack & defense algorithms and system design)
- AI system Security (e.g., integrated GPU, Tensorcore, GDDR6 memory)
- Secure AI Agents ( application: LLMs, VLMs & diffusion models)
- Efficient AI Algorithms with strict memory and energy budget (e.g., edge TEEs).

## **Research Interests**

- Designing adversarial attacks & defenses targeting the vulnerability of AI systems and algorithms.
- Efficiently deploying large-scale AI models in a trusted execution environment to protect against memory faults and side channels.
- Exploiting emerging security and privacy challenges for AI Agent and generative applications.
- Optimizing AI algorithms and systems for efficient edge inference.
- Exploring hardware (e.g., Micro-Controller/FPGA/CPU/GPU) vulnerabilities using novel adversarial attacks and securing against them.

## **Education**

2016	B.Sc. in Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology, Bangladesh.
2019-2021	MS in Computer Engineering, Arizona State University, USA.
2019-2022	PH.D. in Computer Engineering, Arizona State University, USA.

## Work History

2016-2017	Lecturer, Bangladesh University, Dhaka, Bangladesh.
2017-2018	Research Assistant, University of Central Florida, Florida, USA.
2018-2019	Teaching Assistant, University of Central Florida, Florida, USA. (Fall-Spring)
2020	Robust Machine Learning Research Intern, Mitsubishi Electric Research Labs, Cambridge, USA.
2019-2022	Research Associate, Arizona State University, Arizona, USA (Fall-Spring).
2022 (Fall) -	Assistant Professor, School of Computing, Binghamton University (SUNY), USA.

## Research Summary

<i>Topic</i>	<i>Publications</i>
Adversarial Weight Attacks	ICCV-19(33);T-PAMI(40); CVPR-24 (12)
Adversarial Weight Defenses	CVPR-20(28);DATE-21(26);DAC-20(31); S&P-24 (17)
Backdoor/Trojan Attack	CVPR-20 (27); ICCV-23 (16); CVPR-26 (2)
Adversarial Input Attacks	ITW-21 (22)
Adversarial Input Example Defenses	CVPR-19(32);GSVLSI-20(30);ISIT-21(25); DAC-21(24)
AI Architecture Stealing Defense	HOST-21(23)
Efficient & Compact NN	DAC-18(37);CVPR-22(19),25(5); WACV-26 (6); DATE-26 (1)
Model Extraction Attack	IEEE S&P 22 (18) (Selected as Top pick for hardware security)
Hardware Vulnerabilities	USENIX-Security 20(29); USENIX-Security 21(21)
Agentic AI Security	(3,4) (Additional works Under-Review)

## Publications

[Google Scholar Profile Link](#)

Students are Highlighted with \*.

### Conferences:

1. Sabbir Ahmed\*, Deniz Najafi, Mohaiminul Al Nahian\*, Navid Khoshavi, Abdullah Al Arafat, Mamshad Nayeem Rizve, Mahdi Nikdast, **Adnan Siraj Rakin**, Shaahin Angizi. "INSPIRE: In-Sensor Compressed Weight Retrieval for Enhancing ViT Efficiency at Edge." Design, Automation Test in Europe Conference, 2026. [Paper Link](#). [Best Paper Award Link](#). (Acceptance rate: 24.9 %)
2. Al Nahian, Mohaiminul\*, Abeer Matar Almalky\*, Sabbir Ahmed\*, Abdullah Al Arafat, Mamshad Nayeem Rizve, and **Adnan Siraj Rakin**. "Eidolon: Unleashing Stealthy Backdoor Pandemic by Infecting a Single Diffusion Model."

- In Proceedings of the Computer Vision and Pattern Recognition Conference, 2026. [Paper Link](#). (Acceptance rate: 25.42 %)
3. Altaweel, Zainab, Mohaiminul Al Nahian\*, Isaac Lehrer, **Adnan Siraj Rakin**, and Shiqi Zhang. "Safety First: a Dataset of Harmful Task Plans for Robots." In Workshop on Datasets and Evaluators of AI Safety. [Paper Link](#).
  4. Al Nahian, Mohaiminul\*, Zainab Altaweel, David Reitano\*, Sabbir Ahmed\*, Shiqi Zhang, and **Adnan Siraj Rakin**. "Attacking LLM-based Robot Intelligence for Long-horizon Tasks." In RSS 2025 Workshop on Reliable Robotics: Safety and Security in the Face of Generative AI. [Paper Link](#).
  5. Ahmed, Sabbir\*, Abdullah Al Arafat, Deniz Najafi, Akhlak Mahmood, Mamshad Nayeem Rizve, Mohaiminul Al Nahian\*, Ranyang Zhou, Shaahin Angizi, and **Adnan Siraj Rakin**. "Deepcompress-vit: Rethinking model compression to enhance efficiency of vision transformers at the edge." In Proceedings of the Computer Vision and Pattern Recognition Conference, pp. 30147-30156. 2025. [Paper Link](#). (Acceptance rate: 22.12 %)
  6. Ahmed, Sabbir\*, Mamshad Nayeem Rizve, Abdullah Al Arafat, Jacqueline Tiffany Liu, Rahim Hossain, Mohaiminul Al Nahian\*, and **Adnan Siraj Rakin**. "Unified Alignment Protocol: Making Sense of the Unlabeled Data in New Domains." In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pp. 2974-2983. 2026. [Paper Link](#). (Acceptance rate: 33.7 %)
  7. Almalky, Abeer Matar A.\*, Ranyang Zhou, Shaahin Angizi, and **Adnan Siraj Rakin**. "How vulnerable are large language models (llms) against adversarial bit-flip attacks?." In Proceedings of the Great Lakes Symposium on VLSI 2025, pp. 534-539. 2025. [Paper Link](#). (Acceptance rate: 27 %)
  8. Almalky, Abeer\*, Sabbir Ahmed\*, Ranyang Zhou, Mohaiminul Al Nahian\*, Abdullah Al Arafat, Shaahin Angizi, and **Adnan Siraj Rakin**. "LLWRA: Large Language Models Weight Replacement Attack." In 2025 International Conference on Control, Automation and Diagnosis (ICCAD), pp. 1-6. IEEE, 2025. [Paper Link](#).
  9. Zhang, Yunxiang, Sabbir Ahmed\*, Abeer Matar A. Almalky\*, **Adnan Siraj Rakin**, and Wenfeng Zhao. "Non-Negative AdderNet: Algorithm-Hardware Co-design for Lightweight Defense of Adversarial Bit-Flip Attacks." In 2025 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 1-8. IEEE, 2025. [Paper Link](#). (16.9 %) (Acceptance rate: 24.68 %)
  10. Sabbir Ahmed\*, Ranyang Zhou, **Adnan Siraj Rakin**, and Shaahin Angizi. "DNN-Defender: A Victim-Focused In-DRAM Defense Mechanism for Taming Adversarial Weight Attack on DNNs." In Proceedings of the 61st ACM/IEEE

- Design Automation Conference, pp. 1-6. 2024. [Paper Link](#). (16.9 %) (26.4 %)
11. Karim, Nazmul, Abdullah Al Arafat, **Adnan Siraj Rakin**, Zhishan Guo, and Nazanin Rahnavard. "Fisher information guided purification against back-door attacks." In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, pp. 4435-4449. 2024. [Paper Link](#). (16.9 %)
  12. Sabbir Ahmed\*, Ranyang Zhou, Shaahin Angizi, and **Adnan Siraj Rakin**. "Deep-TROJ: An Inference Stage Trojan Insertion Algorithm through Efficient Weight Replacement Attack." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 24810-24819. 2024. (23.6 %) [Paper Link](#).
  13. Zhou, Ranyang, Sabbir Ahmed\*, Arman Roohi, **Adnan Siraj Rakin**, and Shaahin Angizi. "DRAM-Locker: A General-Purpose DRAM Protection Mechanism against Adversarial DNN Weight Attacks." In 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1-6. IEEE, 2024.. 2024. (25 %) [Paper Link](#).
  14. Li, Jingtao, Xing Chen, Li Yang, **Adnan Siraj Rakin**, Deliang Fan, and Chaitali Chakrabarti. "EMGAN: Early-Mix-GAN on Extracting Server-Side Model in Split Federated Learning." In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 38, no. 12, pp. 13545-13553. 2024. (23.75 %) [Paper Link](#).
  15. Yukui Luo, **Adnan Siraj Rakin**, Deliang Fan, and Xiaolin Xu. "DeepShuffle: A Lightweight Defense Framework against Adversarial Fault Injection Attacks on Deep Neural Networks in Multi-Tenant Cloud-FPGA" 2024 IEEE Symposium on Security and Privacy (Accepted). (20 %) [Paper Link](#).
  16. Sabbir Ahmed\*, Abdullah Al Arafat, Mamshad Nayeem Rizve, Rahim Hossain\*, Zhishan Guo, **Adnan Siraj Rakin**. "SSDA: Secure Source-Free Domain Adaptation" International Conference on Computer Vision and Pattern Recognition (ICCV-2023). (25 %) [Paper Link](#).
  17. Mohammad Jobayer Hossain, David Reitano\*, **Adnan Siraj Rakin** "Inverse Design of Silicon Photonics Components: A Study from Deep Learning Perspective" 2023 IEEE Photonic Conference. [Paper Link](#).
  18. **Adnan Siraj Rakin**, M Hafizul Islam Chowdhuryy, F Yao, D Fan. "DeepSteal: Advanced Model Extractions Leveraging Efficient Weight Stealing in Memories" 2022 IEEE Symposium on Security and Privacy. (15 %) [Paper Link](#).

19. Yang, Li, **Adnan Siraj Rakin**, and Deliang Fan. "Rep-Net: Efficient On-Device Learning via Feature Reprogramming." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2022) (CVPR 2022) (26%) [Paper Link](#).
20. Jingtao Li, **Adnan Siraj Rakin**, Xing Chen, Zhezhi He, Deliang Fan, Chaitali Chakrabarti. "ResSFL: A Resistance Transfer Framework for Defending Model Inversion Attack in Split Federated Learning." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2022) (CVPR 2022) (26%) [Paper Link](#).
21. **Adnan Siraj Rakin**, Yukui Luo, Xiaolin Xu, and Deliang Fan. "Deep-Dup: An Adversarial Weight Duplication Attack Framework to Crush Deep Neural Network in Multi-Tenant FPGA." 30th USENIX Security Symposium (USENIX Security 21) (18 %) [Paper Link](#).
22. **Adnan Siraj Rakin**, Ye Wang, Shuchin Aeron, Toshiaki Koike-Akino, Pierre Moulin and Kieran Parsons. "Towards Universal Adversarial Examples and Defenses." at Information Theory Workshop, October 2021 [Paper Link](#).
23. Li, Jingtao, Zhezhi He, **Adnan Siraj Rakin**, Deliang Fan, and Chaitali Chakrabarti. "NeurObfuscator: A Full-stack Obfuscation Tool to Mitigate Neural Architecture Stealing." arXiv preprint arXiv:2107.09789 (2021) (HOST 2021) [Paper Link](#).
24. Sai Kiran, **Adnan Siraj Rakin**, Shihui Yin, Mingoo Seok, Deliang Fan, Jaesun Seo "Leveraging Noise and Aggressive Quantization of In-Memory Computing for Robust DNN Hardware Against Adversarial Input and Weight Attacks", DAC-2021 (Accepted). (23 %)
25. Ye Wang, Shuchin Aeron, **Adnan Siraj Rakin**, Toshiaki Koike-Akino, Pierre Moulin and Kieran Parsons. "Robust Machine Learning via Privacy/Rate-Distortion Theory " IEEE International Symposium on Information Theory (ISIT), page: 1320-1325, 2021 [Paper Link](#).
26. Li, Jingtao, **Adnan Siraj Rakin**, Zhezhi He, Deliang Fan, and Chaitali Chakrabarti. "RADAR: Run-time Adversarial Weight Attack Detection and Accuracy Recovery." arXiv preprint arXiv:2101.08254 (2021) (DATE 2021) [Paper Link](#). (35 %)
27. **Adnan Siraj Rakin**, Zhezhi He, and Deliang Fan. "Tbt: Targeted neural network attack with bit trojan." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 13198-13207. 2020 [Paper Link](#). (26%)

28. **Adnan Siraj Rakin**, He, Zhezhi, Jingtao Li, Chaitali Chakrabarti, and Deliang Fan. "Defending and harnessing the bit-flip based adversarial weight attack." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 14095-14103. 2020 [Paper Link](#). (26%)
29. Yao, Fan, **Adnan Siraj Rakin**, and Deliang Fan. "Deephhammer: Depleting the intelligence of deep neural networks through targeted chain of bit flips." In 29th USENIX Security Symposium (USENIX Security 20), pp. 1463-1480. 2020 [Paper Link](#). (18 %)
30. **Adnan Siraj Rakin**, Zhezhi He, Li Yang, Yanzhi Wang, Liqiang Wang, and Deliang Fan. "Robust Sparse Regularization: Defending Adversarial Attacks Via Regularized Sparse Network." In Proceedings of the 2020 on Great Lakes Symposium on VLSI, pp. 125-130. 2020 [Paper Link](#).
31. Li, Jingtao, **Adnan Siraj Rakin**, Yan Xiong, Liangliang Chang, Zhezhi He, Deliang Fan, and Chaitali Chakrabarti. "Defending bit-flip attack through DNN weight reconstruction." In 2020 57th ACM/IEEE Design Automation Conference (DAC), pp. 1-6. IEEE, 2020 [Paper Link](#). (23 %)
32. **Adnan Siraj Rakin**, He, Zhezhi and Deliang Fan. "Parametric noise injection: Trainable randomness to improve deep neural network robustness against adversarial attack." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 588-597. 2019 [Paper Link](#). (26 %)
33. **Adnan Siraj Rakin**, Zhezhi He, and Deliang Fan. "Bit-flip attack: Crushing neural network with progressive bit search." In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 1211-1220. 2019 [Paper Link](#). (25 %)
34. **Adnan Siraj Rakin**, and Deliang Fan. "Defense-net: Defend against a wide range of adversarial attacks through adversarial detector." In 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 332-337. IEEE, 2019 [Paper Link](#).
35. **Adnan Siraj Rakin**, Shaahin Angizi, Zhezhi He, and Deliang Fan. "PIM-TGAN: A processing-in-memory accelerator for ternary generative adversarial networks." In 2018 IEEE 36th International Conference on Computer Design (ICCD), pp. 266-273. IEEE, 2018 [Paper Link](#).
36. He, Zhezhi, Shaahin Angizi, **Adnan Siraj Rakin**, and Deliang Fan. "Bd-net: a multiplication-less dnn with binarized depthwise separable convolution." In 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 130-135. IEEE, 2018 [Paper Link](#).

37. Angizi, Shaahin, Zhezhi He, **Adnan Siraj Rakin**, and Deliang Fan. "Cmp-pim: an energy-efficient comparator-based processing-in-memory neural network accelerator." In Proceedings of the 55th Annual Design Automation Conference, pp. 1-6. 2018 [Paper Link](#). (23 %)

### Journals:

38. Zhou, Ranyang, Jacqueline Liu\*, Sabbir Ahmed\*, Nakul Kochar, **Adnan Siraj Rakin**, and Shaahin Angizi. "Assessing the Potential of Escalating RowHammer Attack Distance to Bypass Counter-Based Defenses." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2024).
39. Zhou, Ranyang, Jacqueline Liu\*, Nakul Kochar, Sabbir Ahmed\*, **Adnan Siraj Rakin**, and Shaahin Angizi. "A Novel Insight Into the Vulnerability of DDR4 DRAM Cells Across Multiple Hammering Settings." IEEE Embedded Systems Letters 16, no. 4 (2024): 337-340.
40. **Adnan Siraj Rakin**, Z. He, J. Li, F. Yao, C. Chakrabarti and D. Fan, "T-BFA: Targeted Bit-Flip Adversarial Weight Attack," in IEEE Transactions on Pattern Analysis and Machine Intelligence, doi: 10.1109/TPAMI.2021.3112932. [Paper Link](#).
41. Cherupally, Sai Kiran; Meng, Jian; **Adnan Siraj Rakin**; Yin, Shihui; Yeo, In-june; Yu, Shimeng; Fan, Deliang; Seo, Jae-sun, "Improving the Accuracy and Robustness of RRAM-based In-Memory Computing Against RRAM Hardware Noise and Adversarial Attacks" in Semiconductor Science and Technology. (Accepted 2021)
42. He, Zhezhi, Li Yang, Shaahin Angizi, **Adnan Siraj Rakin**, and Deliang Fan. "Sparse BD-Net: a multiplication-less DNN with sparse binarized depthwise separable convolution." ACM Journal on Emerging Technologies in Computing Systems (JETC) 16, no. 2 (2020): 1-24 [Paper Link](#).

### Presentations

1. Presented our attack "DeepSteal" at IEEE Security and Privacy, Oakland 2022. [Youtube Link](#)
2. Presented a conference paper titled "Tbt: Targeted neural network attack with bit trojan" in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition in 2020. [Youtube Link](#)
3. Presented a conference paper titled "Robust Sparse Regularization: Defending Adversarial Attacks Via Regularized Sparse Network" in GLSVLSI 2020: Proceedings of 2020 on Great Lakes Symposium on VLSI. [Video Link](#)

4. Presented a conference paper titled "Deep-Dup: An Adversarial Weight Duplication Attack Framework to Crush Deep Neural Network in Multi-Tenant FPGA" in USENIX Security Symposium 2021. [Youtube Link](#)
5. Presented my internship work "Towards Universal Adversarial Examples and Defenses" at Information Theory Workshop, October 2021. [Youtube Link](#)

## Served in Technical Program Committee (TPC)

1. International Conference on Computer-Aided Design (ICCAD 2023)
2. Workshop on Dependable and Secure Machine Learning (DSML 2024)
3. Design and Automation Conference (DAC 2025 & 2026)

## Served as a Session Chair:

1. International Conference on Supercomputing, Large-Scale Applications Track, Orlando, 2023.
2. Design and Automation Conference, AI-Security Track (Co-Chair), San Francisco, 2025.
3. Design and Automation Conference, Hidden in Plain Sight: Designing Systems for Private Intelligence (co-Chair), LA, 2026.

## Awards

1. Best paper award in DATE 2026, [Best Paper Award Link](#).
2. Outstanding reviewer award from CVPR 2026.
3. Received the Outstanding Research Achievement Award from the School of Computing in 2024-2025 academic year.
4. Outstanding TPC member award from DAC 2025.
5. Our paper "DeepSteal" has been selected as the Picks in Hardware and Embedded Security in 2024.
6. I have received the **Educator of the Year award** from the CS department at Binghamton University for the 2022-23 academic year.

7. Received the **dean's dissertation award 2022** for the college of engineering (Fulton School) at Arizona State University. My dissertation topic was "Exploration of Security and Privacy Challenges through Adversarial Weight Perturbation in Deep Learning Models".
8. Received University **Graduate Fellowship** for Summer 2022 by Arizona State University (ECE).

## Served as a Reviewer

1. Neural Information Processing Systems (NeurIPS 2023,2024 & 2025)
2. International Conference on Learning Representations (ICLR 2024)
3. International Conference on Computer-Aided Design (ICCAD 2023)
4. European Conference on Computer Vision (ECCV 2022)
5. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2021, 2022, 2023, 2024 & 2025)
6. IEEE/CVF International Conference on Computer Vision (ICCV 2021 , 2023 & 2025)
7. AAI Conference on Artificial Intelligence (AAAI 2021, 2022 & 2023)
8. Design and Automation Conference (DAC 2025)
9. International Conference on Machine Learning (ICML 2025)
10. Transactions on Dependable and Secure Computing (TDSC)
11. IEEE Transactions on Information Forensics & Security
12. Journal on Emerging Technologies and Computing Systems (JETC)
13. IEEE Transactions on Neural Networks and Learning Systems (T-NNLS)
14. IEEE Transactions on Very Large Scale Integration (VLSI) Systems
15. IEEE Network
16. IEEE Journal on Selected Areas in Information theory (JSAIT)
17. Journal of Supercomputing

## Grants

1. Data Science Transdisciplinary Area of Excellence (TAE): Dual Optimization of Efficiency and Security of Modern Deep Learning Framework Running on FPGA Platform. (PI \$13,809)
2. The Center for Information Assurance and Cybersecurity (CIAC): Towards Secured Generalized Semi-supervised Federated Learning (SSFL) (PI \$4000)
3. Binghamton University Projects for New Undergraduate Researchers (BUP-NUR) program (PI \$12,500).

## Teaching

1. Embedded systems (Fall-18, TA).
2. Introduction to Machine Learning (CS 436/536) (Fall 22,23,24,25,26 & Spring 23)
3. Computer Architecture from a Programmer's Perspective (CS 220) (Fall 23)
4. AI security (CS 680A) (Spring 25)
5. Research Methodology (CS 601) (Fall-26)
6. Developed an online course: [Demo Lecture](#).

## Student Mentoring.

1. **PhD Students:** Sabbir Ahmed (awarded the Soc Excellence in Computer Science Research, PhD), Abeer Al Malky (Third-year, seven publications), Mohaiminul Al Nahian (Third-year, seven publications)
2. **MS Students:** David Reitano (graduated with Outstanding Academic Achievement Award)

## Outreach and Community Activities

1. Arranged workshop with Girls Who Code at Binghamton on Introduction to ML.
2. Arranged workshop for New York State Masters Teachers Program (NYSMTP) to introduce AI security Challenges to Upstate New York State Teachers.
3. Invited Elementary School Kids from Tioga County for a LAB tour.

4. Invited talk/seminar at Get to Know Your Fellow CAE-R.
5. Invited talk/seminar at NJIT, VIT, and Sastra University.