Adnan Siraj Rakin

Assistant Professor, School of Computing, Binghamton University (SUNY)
Email: arakin@binghamton.edu
Website
Google Scholar
Research Gate

Areas of Specialization

- AI Security
- Deep Learning
- Computer Vision
- Efficient & Compact AI Algorithms
- Machine Learning
- Computer Engineering (Hardware & Software Co-Design)
- Embedded System

Research Interests

- Security of deep learning algorithms
- Adversarial input attacks & defenses
- Adversarial weight attacks & defenses
- Model inversion attacks on Federated/Split Learning
- Model stealing attack using memory side channel
- Efficient implementation of machine learning framework
- Computer vision algorithms for efficient on-device learning
- Exploring hardware (e.g., FPGA/CPU/GPU) vulnerabilities using novel adversarial attacks

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

Topic	*Publications*
Adversarial Weight Attacks	ICCV-19(23);T-PAMI(28)
Adversarial Weight Defenses	CVPR-20(18);DATE-21(16);DAC-20(21); S&P-24 (7)
Backdoor/Trojan Attack	CVPR-20 (17); ICCV-23 (6)
Adversarial Input Attacks	ITW-21 (12)
Adversarial Input Example Defenses	CVPR-19(22);GSVLSI-20(20);ISIT-21(15); DAC-21(14)
Neural Network (NN) Architecture Stealing Defense	HOST-21(13)
Efficient & Compact NN	ICCD-18(??);DAC-18(27);JETC-20(30);CVPR-22(9)
Model Extraction Attack	IEEE S&P 22 (8)
Hardware Vulnerabilities using NN Adversarial Attack	USENIX-Security 20(19); USENIX-Security 21(11)

Publications

Google Scholar Profile Link

Conferences:

1. 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 %)

2. 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 %)

3. Karim, Nazmul, A. A. Arafat, **Adnan Siraj Rakin**, Zhishan Guo, and Nazanin Rahnavard. "Fisher information guided purification against backdoor attacks." In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS). 2024. (23 %)

4. 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 %)

5. 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 %)

6. 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) (Accepted). (25 %)

7. Mohammad Jobayer Hossain, David Reitano*, **Adnan Siraj Rakin** "Inverse Design of Silicon Photonics Components: A Study from Deep Learning Perspective" 2023 IEEE Photonic Conference (Accepted).

8. **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.

9. 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.

10. 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.

11. **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.

12. **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.

13. 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.

14. 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 %)

15. 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.

16. 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 %)

17. **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%)

18. **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%)

19. Yao, Fan, **Adnan Siraj Rakin**, and Deliang Fan. "Deephammer: 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 %)

20. **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.

21. 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 %)

22. **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 %)

23. **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 %)

24. **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.

25. **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.

26. 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.

27. 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:

28. **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.

29. Cherupally, Sai Kiran; Meng, Jian; **Adnan Siraj Rakin**; Yin, Shihui; Yeo, Injune; 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)

30. He, Zhezhi, Li Yang, Shaahin Angizi, **Adnan Siraj Rakin**, and Deliang Fan. "Sparse BD-Net: a multiplication-less DNN with sparse binarized depth-wise 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 as a Reviewer

1. Neural Information Processing Systems (NeuRIPS 2023,2024)

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)

6. IEEE/CVF International Conference on Computer Vision (ICCV 2021 & 2023)
7. AAAI Conference on Artificial Intelligence (AAAI 2021, 2022 & 2023)
8. IEEE Transactions on Information Forensics & Security
9. Journal on Emerging Technologies and Computing Systems (JETC)
10. IEEE Transactions on Neural Networks and Learning Systems (T-NNLS)
11. IEEE Transactions on Very Large Scale Integration (VLSI) Systems
12. IEEE Network
13. IEEE Journal on Selected Areas in Information theory (JSAIT)
14. Journal of Supercomputing

Served in Technical Program Committee (TPC)

1. International Conference on Computer-Aided Design (ICCAD 2023)

Served as a Session Chair:

1. International Conference on Supercomputing, Orlando, 2023.

Awards

1. I have received the **Educator of the Year award** from the CS department at Binghamton University for the 2022-23 academic year.
2. 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".
3. Received University **Graduate Fellowship** for Summer 2022 by Arizona State University (ECE).
4. IEEE Computer Society Annual Symposium on VLSI (ISVLSI) 2018 **Best Paper Award** Link
5. Received a non-compensatory award for continued customer discovery efforts by successfully completing the **ASU NSF I-Corps** Spring 2021 Five-Week Invitational.