Manaar Alam

Modern Microprocessor Architectures Lab – Center for Cyber Security
New York University Abu Dhabi, United Arab Emirates.
☎ +971 568751769 • ✉ alam.manaar@nyu.edu • felu-mittir • Manaar Alam
Manaar Alam • in manaar-alam

Research Interests

My research interests are mainly on:
- Security and Privacy of Machine Learning.
- Application of Machine Learning in Hardware and System Security.

Citation Data (as of Jul 15, 2025)

- **Google Scholar:** Citations – 2117; h-index – 16; i10-index – 21. [Link]

Professional Positions

New York University Abu Dhabi **Abu Dhabi, UAE**
Post-Doctoral Associate *Jan 2022–Present*
Supervisor: *Prof. Michail Maniatakos*
Research Topic: Analyzing different security vulnerabilities of machine learning models in the context of backdoor attacks, exploring the application of large language models in enhancing cybersecurity measures.

Nanyang Technological University **Singapore**
Research Intern *Aug 2017–Jan 2018*
Supervisor: *Prof. Siew-Kei Lam*
Research Topic: Developing a light-weight application to detect and prevent malware for embedded platforms.

Education

Indian Institute of Technology (IIT) Kharagpur **Kharagpur, India**
Ph. D. in Computer Science and Engineering *Jul 2016–Jul 2022*
Thesis: Design and Analysis of Robust Machine Learning in the context of Computer Security
Supervisor: *Prof. Debdeep Mukhopadhyay*

Indian Institute of Technology (IIT) Dhanbad **Dhanbad, India**
Master of Technology in Computer Science and Engineering, GPA - 9.7/10 *Jul 2014–Jun 2016*
Received M. Tech. with *Distinction* and secured *3rd* place from the department.

Institute of Engineering and Management (IEM) Kolkata **Kolkata, India**
Bachelor of Technology in Computer Science and Engineering, GPA - 8.88/10 *Aug 2009–May 2013*

Academic Awards

Fellowships

- Selected for **2023 Postdoc Collaborative Grant**, hosted by New York University Abu Dhabi.
- **IBM PhD Fellowship Award** for the Academic Year 2019-2021.
- Finalist of **Qualcomm Innovation Fellowship** India in 2017 and 2019.
- **National Merit Scholarship** awarded by Government of India for securing position among Top 20 in Higher Secondary Examination (Grades 11-12) in 2009.

Conference Awards

- **3rd Best Poster Award** at International Conference on Security, Privacy, and Applied Cryptographic Engineering (SPACE), Virtual, 2020.
- **Best Student Paper Award** at Smart Card Research and Advanced Application Conference (CARDIS), Prague, Czech Republic, 2019.
- **3rd Best Poster Award** in Young Researcher's Forum at International Conference on Security, Privacy, and Applied Cryptographic Engineering (SPACE), Kanpur, India, 2018.

Research Competitions

- **2nd Best Presentation Award** in Applied Research Competition at Cyber Security Awareness Week (CSAW) 2019, hosted by Indian Institute of Technology (IIT) Kanpur.
- **2nd Best Hardware Demo Award** in Embedded Security Challenge at Cyber Security Awareness Week (CSAW) 2016, hosted by Indian Institute of Technology (IIT) Kanpur.
- **2nd Place** in International Championship for Artificial Intelligence & Networking 2015, hosted by Indian Institute of Technology (IIT) Bombay.

Grant Writing Experience

NYU-KAIST Global Innovation and Research Institute
Robust and private outsourced data processing using cryptographic and hardware guarantees. *Jul 2024–Dec 2025*
Lead PI: Prof. Michail Maniatakos
Grant Amount: USD 150,000 **[Awarded]**.

Conference Proceedings

[c22] Christoforos Vasilatos, Dunia J. Mahboobeh, Hithem Lamri, **Manaar Alam**, and Michail Maniatakos, "*LLMPot: Dynamically Configured LLM-based Honeypot for Industrial Protocol and Physical Process Emulation*". In *10th IEEE European Symposium on Security and Privacy, EuroS&P 2025, Venice, Italy, June 30-July 4, 2025*. **[To Appear]**.

[c21] **Manaar Alam**, Hithem Lamri, and Michail Maniatakos, "*ReVeil: Unconstrained Concealed Backdoor Attack on Deep Neural Networks using Machine Unlearning*". In *62nd ACM/IEEE Design Automation Conference, DAC 2025, San Francisco, United States of America, June 22-25, 2025*. **[To Appear]**.

[c20] Lakshmi Likhitha Mankali, Jitendra Bhandari, **Manaar Alam**, Ramesh Karri, Michail Maniatakos, Ozgur Sinanoglu and Johann Knechtel, "*RTL-Breaker: Assessing the Security of LLMs against Backdoor Attacks on HDL Code Generation*". In *IEEE Design, Automation, and Test in Europe Conference & Exhibition, DATE 2025, Lyon, France, March 31-April 2, 2025*, pages 1–7. DOI: 10.23919/DATE64628.2025.10993260.

[c19] Shubhi Shukla, Subhadeep Dalui, **Manaar Alam**, Shubhajit Datta, Arijit Mondal, Debdeep Mukhopadhyay, and Partha Pratim Chakrabarti, "*Guardian of the Ensembles: Introducing Pairwise Adversarially Robust Loss for Resisting Adversarial Attacks in DNN Ensembles*". In *IEEE/CVF Winter Conference on Applications of Computer Vision, WACV 2025, Arizona, United States of America, February 28-March 4, 2025*, pages 7205–7214. DOI: 10.1109/WACV61041.2025.00700.

[c18] Shubhajit Datta, **Manaar Alam**, Arijit Mondal, Debdeep Mukhopadhyay, and Partha Pratim Chakrabarti, "*Ignorance is not Bliss: A Novel Ensemble Method to Counter Adversarial Attacks on Deep Learning Models*". In *8th International Conference on Data Science and Management of Data, CODS-COMAD Dec'24, Jodhpur, India, December 18-21, 2024*, pages 75–83. DOI: 10.1145/3703323.3703336.

[c17] **Manaar Alam** and Michail Maniatakos, "*AdvHunter: Detecting Adversarial Perturbations in Black-Box Neural Networks through Hardware Performance Counters*". In *61st ACM/IEEE Design Automation Conference, DAC 2024, San Francisco, United States of America, June 23-27, 2024*, pages 184:1–184:6. DOI: 10.1145/3649329.3655682.

[c16] **Manaar Alam**, Yue Wang, and Michail Maniatakos, "*Detecting Backdoor Attacks in Black-Box Neural Networks through Hardware Performance Counters*". In *IEEE Design, Automation, and Test in Europe Conference & Exhibition, DATE 2024, Valencia, Spain, March 25-27, 2024*, pages 1–6. DOI: 10.23919/DATE58400.2024.10546739.

[c15] Soumyadyuti Ghosh, **Manaar Alam**, Soumyajit Dey, and Debdeep Mukhopadhyay, "*'Hello? Is there anybody in there?' Leakage Assessment of Differential Privacy Mechanisms in Smart Metering Infrastructure*". In *22nd International Conference on Applied Cryptography and Network Security, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024*, pages 163–189. DOI: 10.1007/978-3-031-54776-8_7.

[c14] **Manaar Alam**, Esha Sarkar, and Michail Maniatakos, "*PerDoor: Persistent Backdoors in Federated Learning using Adversarial Perturbations*". In *IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2023, Berlin, Germany, July 23-25, 2023*, pages 1–6. DOI: 10.1109/COINS57856.2023.10189281.

[c13] Suvadeep Hajra, Sayandeep Saha, **Manaar Alam**, and Debdeep Mukhopadhyay, "*TransNet: Shift Invariant Transformer Network for Side Channel Analysis*". In *13th International Conference on Cryptology, AfricaCrypt 2022, Fes, Morocco, July 18-20, 2022*, pages 371–396. DOI: 10.1007/978-3-031-17433-9_16.

[c12] Anirban Chakraborty, **Manaar Alam**, and Debdeep Mukhopadhyay, "*A Good Anvil Fears No Hammer: Automated Rowhammer Detection using Unsupervised Deep Learning*". In *2nd Workshop on Artificial Intelligence in Hardware Security, AIHWS@ACNS 2021, Virtual, June 21, 2021*, pages 59–77. DOI: 10.1007/978-3-030-81645-2_5.

[c11] Dhruv Thapar, **Manaar Alam**, and Debdeep Mukhopadhyay, “*Deep Learning assisted Cross-Family Profiled Side-Channel Attacks using Transfer Learning*”. In *22nd International Symposium on Quality Electronic Design, ISQED 2021, Virtual, April 7-9, 2021*, pages 178–185. DOI: 10.1109/ISQED51717.2021.9424254.

[c10] Sai Praveen Kadiyala, Mohit Garg, **Manaar Alam**, Hau Ngo, Debdeep Mukhopadhyay and Thambipillai Srikanthan, “*HARDY: Hardware Based Analysis for malwaRe Detection in Embedded sYstems*”. In *33rd IEEE International System-on-Chip Conference, SOCC 2020, Virtual, September 8-11, 2020*, pages 1–6. DOI: 10.1109/SOCC49529.2020.9524727.

[c9] Anirban Chakraborty, **Manaar Alam**, and Debdeep Mukhopadhyay, “*Deep Learning based Diagnostics for Rowhammer Protection of DRAM Chips*”. In *28th IEEE Asian Test Symposium, ATS 2019, Kolkata, India, December 10-13, 2019*, pages 86–91. DOI: 10.1109/ATS47505.2019.00016.

[c8] **Manaar Alam**, Astikey Singh, Sarani Bhattacharya, Kuheli Pratihar and Debdeep Mukhopadhyay, “*In-situ Extraction of Randomness from Computer Architecture through Hardware Performance Counters*”. In *18th Smart Card Research and Advanced Application Conference, CARDIS 2019, Prague, Czech Republic, November 11-13, 2019*, pages 3–19. DOI: 10.1007/978-3-030-42068-0_1. **[Best Student Paper Award]**

[c7] **Manaar Alam** and Debdeep Mukhopadhyay, “*How Secure are Deep Learning Algorithms from Side-Channel based Reverse Engineering?*”. In *56th ACM/IEEE Design Automation Conference, DAC 2019, Las Vegas, United States of America, June 2-6, 2019*, pages 226. DOI: 10.1145/3316781.3322465.

[c6] **Manaar Alam**, Sarani Bhattacharya, Swastika Dutta, Sayan Sinha, Debdeep Mukhopadhyay, and Anupam Chattopadhyay, “*RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders*”. In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2019, McLean, United States of America, May 6-10, 2019*, pages 218–227. DOI: 10.1109/HST.2019.8740837.

[c5] Nimesh Kirit Shah, **Manaar Alam**, Durga Prasad Sahoo, Debdeep Mukhopadhyay, and Arindam Basu, “*A 0.16pJ/bit Recurrent Neural Network Based PUF for Enhanced Machine Learning Attack Resistance*”. In *24th ACM Asia and South Pacific Design Automation Conference, ASP-DAC 2019, Tokyo, Japan, January 21-24, 2019*, pages 627–632. DOI: 10.1145/3287624.3287696.

[c4] **Manaar Alam**, Debdeep Mukhopadhyay, Sai Praveen Kadiyala, Siew-Kei Lam, and Thambipillai Srikanthan, “*Side-Channel Assisted Malware Classifier with Gradient Descent Correction for Embedded Platforms*”. In *7th International Workshop on Security Proofs for Embedded Systems, PROOFS@CHES 2018, Amsterdam, Netherlands, September 13, 2018*, pages 1–15. DOI: 10.29007/5sdj.

[c3] **Manaar Alam**, Sarani Bhattacharya, and Debdeep Mukhopadhyay, “*Tackling the Time-Defence: An Instruction Count Based Micro-architectural Side-Channel Attack on Block Ciphers*”. In *7th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2017, Goa, India, December 13-17, 2017*, pages 30–52. DOI: 10.1007/978-3-319-71501-8_3.

[c2] **Manaar Alam**, Debapriya Basu Roy, Sarani Bhattacharya, Vidya Govindan, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay, “*SmashClean: A hardware level mitigation to stack smashing attacks in OpenRISC*”. In *14th ACM/IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE 2016, Kanpur, India, November 18-20, 2016*, pages 1–4. DOI: 10.1109/MEMCOD.2016.7797764.

[c1] **Manaar Alam**, Soumyajit Chatterjee, and Haider Banka, “*A novel parallel search technique for optimization*”. In *3rd IEEE International Conference on Recent Advances in Information Technology, RAIT 2016, Dhanbad, India, March 3-5, 2016*, pages 259–263. DOI: 10.1109/RAIT.2016.7507912.

Journal Publications

[j18] Shubhajit Datta, **Manaar Alam**, Arijit Mondal, Debdeep Mukhopadhyay, and Partha Pratim Chakrabarti, “*Decision Guided Robust DL Classification of Adversarial Images Combining Weaker Defenses*”. In *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS), Volume: 14, Issue: 4, December 2024*, pages 758–772. DOI: 10.1109/JETCAS.2024.3497295.

[j17] Shubhi Shukla, **Manaar Alam**, Pabitra Mitra, and Debdeep Mukhopadhyay, “*Stealing the Invisible: Unveiling Pre-Trained CNN Models through Adversarial Examples and Timing Side-Channels*”. In *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS), Volume: 14, Issue: 4, December 2024*, pages 634–646. DOI: 10.1109/JETCAS.2024.3485133.

[j16] **Manaar Alam**, Hithem Lamri, and Michail Maniatakos, “*Get Rid Of Your Trail: Remotely Erasing Backdoors in Federated Learning*”. In *IEEE Transactions on Artificial Intelligence (TAI), Volume: 5, Issue: 12, December 2024*, pages 6683–6698. DOI: 10.1109/TAI.2024.3465441.

[j15] Yue Wang, Wenqing Li, **Manaar Alam**, Michail Maniatakos, and Saif Eddin Jabari, “*Backdozer: A Backdoor Detection Methodology for DRL-based Traffic Controllers*”. In *ACM Journal on Autonomous Transportation Systems (JATS), Volume: 1, Issue: 4, August 2024*, pages 1–22. DOI: 10.1145/3639828.

[j14] Suvadeep Hajra, **Manaar Alam**, Sayandeep Saha, Stjepan Picek, and Debdeep Mukhopadhyay, “*On the Instability of Softmax Attention-based Deep Learning Models in Side-channel Analysis*”. In *IEEE Transactions on Information Forensics & Security (TIFS), Volume: 19, October 2023*, pages 514–528. DOI: 10.1109/TIFS.2023.3326667.

[j13] Sayandeep Saha, **Manaar Alam**, Arnab Bag, Debdeep Mukhopadhyay, and Pallab Dasgupta, “*Learn from Your Faults: Leakage Assessment in Fault Attacks using Deep Learning*”. In *Springer Journal of Cryptology (JoC), Volume: 36, Issue: 3, July 2023*, Article Number: 19. DOI: 10.1007/s00145-023-09462-6.

[j12] Kuheli Pratihar, Urbi Chatterjee, **Manaar Alam**, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty, “*Birds of the Same Feather Flock Together: A Dual Mode Circuit for Strong PUF-TRNG Functionalities*”. In *IEEE Transactions on Computers (TC), Volume: 72, Issue: 6, June 2023*, pages 1636–1651. DOI: 10.1109/TC.2022.3218986.

[j11] Shubhi Shukla, **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Pabitra Mitra, “*Whispering MLaaS: Exploiting Timing Channels to Compromise User Privacy in Deep Neural Networks*”. In *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume: 2023, Issue: 2, March 2023*, pages 587—–613. DOI: 10.46586/tches.v2023.i2.587-613

[j10] Soumik Sinha, Sayandeep Saha, **Manaar Alam**, Varun Agarwal, Ayantika Chatterjee, Anoop Mishra, Deepak Khazanchi, and Debdeep Mukhopadhyay, “*Exploring Bitslicing Architectures for Enabling FHE-assisted Machine Learning*”. In *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), Volume: 41, Issue: 11, November 2022*, pages 4004–4015. DOI: 10.1109/TCAD.2022.3204909.

[j9] **Manaar Alam**, Sayandeep Saha, Debdeep Mukhopadhyay, and Sandip Kundu, “*NN-Lock: A Lightweight Authorization to Prevent IP Threats of Deep Learning Models*”. In *ACM Journal on Emerging Technologies in Computing Systems (JETC), Volume: 18, Issue: 3, July 2022*, pages 51:1–51:19. DOI: 10.1145/3505634.

[j8] Anirban Chakraborty, **Manaar Alam**, Vishal Dey, Anupam Chattopadhyay, and Debdeep Mukhopadhyay, “*A Survey on Adversarial Attacks and Defences*”. In *IET CAAI Transactions on Intelligence Technology (TRIT), Volume: 6, Issue: 1, March 2021*, pages 25–45. DOI: 10.1049/cit2.12028. **[Honorable Mention for Most Downloaded Paper of the Year]**

[j7] Anirban Chakraborty, Sarani Bhattacharya, **Manaar Alam**, Sikhar Patranabis, and Debdeep Mukhopadhyay, “*RASSLE: Return Address Stack based Side-channel LEakage*”. In *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume: 2021, Issue: 2, February 2021*, pages 275–303. DOI: 10.46586/tches.v2021.i2.275-303

[j6] **Manaar Alam**, Sarani Bhattacharya, and Debdeep Mukhopadhyay, “*Victims can be Saviors: A Machine Learning based detection for Micro-Architectural Side-Channel Attacks*”. In *ACM Journal on Emerging Technologies in Computing Systems (JETC), Volume: 17, Issue: 2, January 2021*, pages 14:1–14:31. DOI: 10.1145/3439189.

[j5] **Manaar Alam**, Debdeep Mukhopadhyay, Sai Praveen Kadiyala, Siew-Kei Lam, and Thambipillai Srikanthan, “*Improving Accuracy of HPC-based Malware Classification for Embedded Platforms using Gradient Descent Optimization*”. In *Springer Journal of Cryptographic Engineering (JCEN), Volume: 10, Issue: 4, November 2020*, pages 289–303. DOI: 10.1007/s13389-020-00232-9.

[j4] **Manaar Alam**, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay, “*Neural Network-based Inherently Fault-tolerant Hardware Cryptographic Primitives without Explicit Redundancy Checks*”. In *ACM Journal on Emerging Technologies in Computing Systems (JETC), Volume: 17, Issue: 1, September 2020*, pages 3:1–3:30. DOI: 10.1145/3409594.

[j3] Sai Praveen Kadiyala, **Manaar Alam**, Yash Shrivastava, Sikhar Patranabis, Muhamed Fauzi Bin Abbas, Arnab Biswas, Debdeep Mukhopadhyay, and Thambipillai Srikanthan. “*LAMBDA: Lightweight Assessment of Malware for emBeddeD Architectures*”. In *ACM Transactions on Embedded Computing Systems (TECS), Volume: 19, Issue: 4, June 2020*, pages 23:1–23:31. DOI: 10.1145/3390855.

[j2] **Manaar Alam**, Sarani Bhattacharya, Sayan Sinha, Chester Rebeiro, and Debdeep Mukhopadhyay, “*IPA: An Instruction Profiling based Micro-Architectural Side-Channel Attack on Block Ciphers*”. In *Springer Journal of Hardware and Systems Security (HASS), Volume: 3, Issue: 1, March 2019*, pages 26–44. DOI: 10.1007/s41635-018-0060-3

[j1] Debapriya Basu Roy, **Manaar Alam**, Sarani Bhattacharya, Vidya Govindan, Francesco Regazzoni, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay, “*Customized Instructions for Protection Against Memory Integrity Attacks*”. In *IEEE Embedded Systems Letters (ESL), Volume: 10, Issue: 3, September 2018*, pages 91–94. DOI: 10.1109/LES.2018.2828506.

Patents

[p1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay, "*A System for Detecting Ransomware in a Computer System and a Method Thereof*". Patent Application Number: 201831045833, Filed: December 4, 2018. **[Filed]**

Selected Preprints

[w3] Hithem Lamri, **Manaar Alam**, Haiyan Jiang, Michail Maniatakos, "*DRAUN: An Algorithm-Agnostic Data Reconstruction Attack on Federated Unlearning Systems*". In *arXiv, June 2025*. DOI: 10.48550/arXiv.2506.01777.

[w2] Prithwish Basu Roy, Akashdeep Saha, **Manaar Alam**, Johann Knechtel, Michail Maniatakos, Ozgur Sinanoglu, Ramesh Karri "*Veritas: Deterministic Verilog Code Synthesis from LLM-Generated Conjunctive Normal Form*". In *arXiv, May 2025*. DOI: 10.48550/arXiv.2506.00005.

[w1] Christoforos Vasilatos, **Manaar Alam**, Talal Rahwan, Yasir Zaki, and Michail Maniatakos, "*HowkGPT: Investigating the Detection of ChatGPT-generated University Student Homework through Context-Aware Perplexity Analysis*". In *arXiv, June 2023*. DOI: 10.48550/arXiv.2305.18226.

GitHub Repositories

- ReVeil: Unconstrained Concealed Backdoor Attack on Deep Neural Networks using Machine Unlearning (DAC'25). https://github.com/felu-mittir/ReVeil
- Get Rid Of Your Trail: Remotely Erasing Backdoors in Federated Learning (TAI'24). https://github.com/felu-mittir/federated_backdoor_unlearning
- AdvHunter: Detecting Adversarial Perturbations in Black-Box Neural Networks through Hardware Performance Counters (DAC'24). https://github.com/felu-mittir/AdvHunter
- Detecting Backdoor Attacks in Black-Box Neural Networks through Hardware Performance Counters (DATE'24). https://github.com/felu-mittir/dnn-backdoor-detection-DATE24
- PerDoor: Persistent Backdoors in Federated Learning using Adversarial Perturbations (COINS'23). https://github.com/felu-mittir/PerDoor
- Learn from Your Faults: Leakage Assessment in Fault Attacks Using Deep Learning (JoC'23). https://github.com/felu-mittir/DL_FALAT

Industrial Collaborations

IBM Research **Bangalore, India**
Microarchitecture-based side-channel security analysis of containerized environments. *Aug 2019–Jun 2021*

TCG Digital Solutions Private Limited **Kolkata, India**
De-anonymization of Tor communication using timing side-channel. *Aug 2017–Jan 2018*

Invited Talks

- **Trust is an Illusion: When Backdoors Turn AI Against You**
  - Workshop on Machine Learning and Hardware Security, Indian Institute of Technology Kharagpur, India, March 2025.
- **Double-Edged Sword of Backdoor Attacks in Federated Learning: Persistent Injection and Stealthy Removal**
  - Middle East and North Africa Cyber Security Seminar Series, New York University Abu Dhabi, UAE, October 2023.
  - The Grove School of Engineering, City University of New York, New York, USA, July 2023.
- **Artificial Intelligence in Security: Potential to Make and Break a Secure Connected World**
  - 35th International Conference on VLSI Design (VLSID), Virtual, February 2022.
  - Co-Speaker: Prof. Debdeep Mukhopadhyay
- **In-situ Extraction of Randomness from Computer Architecture**
  - Workshop on Cyber Physical System Security, Indian Institute of Technology Kharagpur, India, December 2019.
- **Early Detection of Anomaly using Side-Channel: Statistics and Learning**
  - Workshop on Advanced Side Channel Evaluation of Hardware Security, Indian Institute of Technology Kharagpur, India, July 2018.

Community Service and Outreach

Organization of National and International Events

- BioHack 3D workshop and hackathon in the Cyber Security Awareness Week (CSAW) 2024 at NYU Abu Dhabi, in collaboration with the Computer Science and Engineering Departments at IIT Kanpur, IIT Kharagpur, and IIT Guwahati, November 2024.

- Middle East and North Africa Cyber Security Seminar Series, New York University Abu Dhabi, UAE, September 2023 to May 2024.
- International Conference on Applied Cryptography and Network Security (ACNS), Abu Dhabi, UAE, March 2024.
- Workshop on Cyber Physical System Security, Indian Institute of Technology Kharagpur, India, December 2019.
- Workshop on Advanced Side-Channel Evaluation of Hardware Security, Indian Institute of Technology Kharagpur, India, July 2018.

Professional Service

Program Committee Member

- IACR Conference on Cryptographic Hardware and Embedded Systems (CHES): 2026
- AAAI Conference on Artificial Intelligence (AAAI): 2023, 2024, 2025, 2026
- ACM ASIA Conference on Computer and Communications Security (AsiaCCS): 2025
- International Conference on VLSI Design (VLSID): 2024, 2025

Session Chair

- International Conference on Applied Cryptography and Network Security (ACNS): 2024

Journal Reviewer

- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
- IEEE Transactions on Computers (TC)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- IEEE Embedded System Letters (ESL)
- IEEE Transactions on Artificial Intelligence (TAI)
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- Springer Journal of Cryptographic Engineering (JCEN)
- Springer Journal of Hardware and Systems Security (HASS)

External Conference Reviewer

- International Conference on Learning Representations (ICLR): 2024, 2025
- International Conference on Machine Learning (ICML): 2024, 2025
- Conference on Neural Information Processing Systems (NeurIPS): 2022, 2023, 2024, 2025
- ACM Conference on Computer and Communications Security (CCS): 2022, 2023, 2024
- The Network and Distributed System Security Symposium (NDSS): 2023, 2024, 2025, 2026
- IEEE Symposium on Security and Privacy (S&P): 2023, 2024
- USENIX Security Symposium (USENIX Security): 2023, 2024, 2025
- IACR Conference on Cryptographic Hardware and Embedded Systems (CHES): 2025
- IEEE International Symposium on High-Performance Computer Architecture (HPCA): 2024
- ACM/IEEE Design Automation Conference (DAC): 2019, 2020, 2021, 2022, 2023
- ACM/IEEE International Conference on Computer-Aided Design (ICCAD): 2022, 2023
- IEEE Design, Automation and Test in Europe Conference (DATE): 2022, 2024
- IEEE/IFIP Conference on Very Large Scale Integration (VLSI-SoC): 2020
- Smart Card Research and Advanced Application Conference (CARDIS): 2021
- IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom): 2019
- International Conference on Security, Privacy, and Applied Cryptographic Engineering (SPACE): 2021
- Asian Hardware Oriented Security and Trust Symposium (AsianHOST): 2022
- International Conference on Cryptology in India (Indocrypt): 2020

External Workshop Reviewer

- International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE): 2018
- ACM Cyber-Physical System Security Workshop (CPSS): 2022

- IEEE Workshop on Offensive Technologies (WOOT): 2020
- EMNLP Workshop on NLP for Positive Impact (NLP4PI): 2024

Membership of Professional Bodies

- **IEEE Member**, Mar 2023 – Present.

Teaching Experience

Guest Lecture

- Postgraduate Course
  - **Hardware Security (IIT Kharagpur)**: Spring 2021
    - Lecture on "Security of Machine Learning"
    - Lecture on "Application of Machine Learning on Security"
- Undergraduate Course
  - **Cyberwarfare (NYU Abu Dhabi)**: Fall 2024
    - Lecture on "Can We Trust Deep Learning?"
  - **Computer Organization and Architectures (NYU Abu Dhabi)**: Fall 2024
    - Lecture on "Microarchitectural Attacks"

Teaching Assistant

- Postgraduate Course
  - **High Performance Computer Architecture (IIT Kharagpur)**: Spring 2019 and Spring 2020
  - **Cryptography and Network Security (IIT Kharagpur)**: Autumn 2018 and Autumn 2019
- Undergraduate Course
  - **Programming and Data Structures Theory (IIT Kharagpur)**: Autumn 2020
  - **Foundation of Algorithm Design and Machine Learning (IIT Kharagpur)**: Spring 2018
  - **Programming and Data Structures Lab (IIT Kharagpur)**: Spring 2017
  - **Algorithm Design & Analysis Lab (IIT Dhanbad)**: Spring 2016
  - **Data Structures Lab (IIT Dhanbad)**: Autumn 2015
  - **Computer Programming Lab (IIT Dhanbad)**: Autumn 2015 and Spring 2016

Student Research Project Mentorship

- New York University Abu Dhabi
  - Undergraduate Students: 3
- Indian Institute of Technology Kharagpur
  - Postgraduate Students: 3 [one publication in ISQED 2021].
  - Undergraduate Students: 4 [one publication in CARDIS 2019 (Best Paper Award), one publication in HOST 2019].

References

- **Debdeep Mukhopadhyay**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, debdeep.mukhopadhyay@gmail.com
- **Michail Maniatakos**, Associate Professor, Computer Engineering Division, New York University Abu Dhabi, michail.maniatakos@nyu.edu
- **Ramesh Karri**, Professor, Electrical and Computer Engineering, New York University, rkarri@nyu.edu
- **Partha Pratim Chakrabarti**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, ppchak@cse.iitkgp.ac.in