Manaar Alam

Modern Microprocessor Architectures Lab – Center for Cyber Security
New York University, Abu Dhabi, United Arab Emirates.

 +971 568751769   •   ✉ alam.manaar@nyu.edu   •   🌐 manaaralam.github.io
  Manaar Alam   •   manaaralam   •   manaar.alam

Current Position

New York University Abu Dhabi   **Abu Dhabi**
Post-Doctoral Associate   *January 2022–Present*

I am presently working with *Michail Maniatakos* in the Modern Microprocessor Architectures Lab - Center for Cyber Security. My primary research interests mainly lie in the confluence of Deep Learning and Security. I have recently been working with infamous Backdoor Attacks in collaborative Federated Learning environments. I have previously worked in employing state-of-the-art Deep Learning techniques in Hardware and System Security and designing robust countermeasures against different attacks on Deep Learning implementations. I am also interested in various security aspects of Deep Learning techniques like fault-resistance, privacy leakages, adversarial attacks, model-extraction, etc. My other research interests include analyzing physical side-channel leakages from secured cryptographic implementations through micro-architectures, power consumption, etc.

Education

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

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

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

Internship Experience

Nanyang Technological University, Singapore

Title: *Lightweight Assessment of Malware for Embedded Architectures.*

Supervisor: Dr. Siew-Kei Lam.

Description: Worked in a team and developed a light-weight application to detect and prevent Malware for embedded platforms based on statistical $t - test$. The prototype of the application are implemented for both x86 and ARM processors.

Duration: August 2017 - January 2018.

Industrial Collaboration

IBM Research India

Title: *Security Analysis of Containerized Environment*

Description: Analyze the security vulnerabilities in a containerized environment through micro-architectural footprints. The objective is to investigate different possibilities and designing efficient countermeasures.

Duration: August 2019 - June 2021.

TCG Digital Solutions Private Limited

Title: *De-anonymization of Tor Communication*

Description: Design of an efficient and low-cost solution for building traffic correlation attacks on anonymized Tor network to de-anonymize Tor users and clients.

Duration: September 2018 - April 2019.

Achievements

- **3rd Best Poster Award** at SPACE 2020.
- **2nd Best Presentation Award** in Applied Research Competition at CSAW 2019.
- **Best Student Paper Award** at CARDIS 2019.

- **IBM PhD Fellowship Award** for the Academic Year 2019-2021.
- DSCI Excellence Award as a team - felicitated by Bharat Chamber of Commerce.
- **3rd Best Poster Award** in Young Researcher's Forum at SPACE 2018.
- Finalist of Qualcomm Innovation Fellowship India 2017 and 2019.
- **2nd Best Hardware Demo Award** in Embedded Security Challenge at CSAW 2016.
- **National Merit-cum-Means Scholarship** awarded by WBMDFC from 2009 to 2013.
- **National Merit Scholarship** awarded by Govt. of India for securing position among Top 20 in Higher Secondary (10+2) Board Examination in 2009.

Invited Talks and Tutorials

- **Artificial Intelligence in Security: Potential to Make and Break a Secure Connected World**
  - 35th International Conference on VLSI Design, Virtual, February 2022.
  - Co-Speaker: 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.

Professional/Academic Services

- **Reviewer of Journals**: *IEEE ESL, IEEE TIFS, IEEE TVLSI, ACM TECS, ACM JETC, IACR TCHES, IET TRIT*
- **Reviewer of Conferences**: *CARDIS, CCS, DAC, DATE, ICCAD, Indocrypt, NDSS, NeurIPS, S&P, SPACE, TrustCom, Usenix Security, VLSI-SoC*
- **Reviewer of Workshops**: *COSADE, CPSS, TopinHES, WOOT*
- **Organization of National and International Events**:
  - 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.

Technical Skills

- Relevant Software Skills:
  - **Programming Languages:** Python, C, C++, JAVA
  - **Deep Learning Libraries:** PyTorch, Tensorflow, Keras
  - **Micro-architectural Performance Analysis Tools:** perf, PAPI
- Relevant Instrumentation Skills:
  - **Deep Learning Edge Devices:** Google Coral Dev Board, Intel Movidius Neural Compute Stick
  - **High Resolution Imaging:** Carl Zeiss Crossbeam 340 High-resolution Scanning Electron Microscope

Competitions

Cyber Security Awareness Week - Applied Research Competition in India 2019
Indian Institute of Technology Kanpur *Kanpur*
Presented a hardware activity based monitoring approach to evaluate privacy leakages in Deep Learning Algorithms. Secured 2nd place in the competition from all over India.

HOST: Hardware Demo 2018
IEEE International Symposium on Hardware Oriented Security and Trust (HOST) *Washington DC*
Designed a lightweight malware detection methodology for embedded platforms along with a fast ransomware detection techniques using Hardware Performance Counters. Reached Final round in the competition from all over the world.

Cyber Security Awareness Week - Embedded Security Challenge in India 2016
Indian Institute of Technology Kanpur *Kanpur*
Designed a novel hardware mitigation technique for memory corruption and control flow integrity attacks in embedded systems. Secured 2nd place in the competition from all over India.

International Championship for Artificial Intelligence & Networking 2015
Indian Institute of Technology Bombay *Mumbai*
Designed a cost effective prototype of a carom playing bot from scrap materials. Secured 2nd place in the competition from all over India. Demonstration can be found on the following link. (https://www.youtube.com/watch?v=18IkxVzs_Zk).

National Round of Indo-US Robo League   **2015**
Indian Institute of Technology Bombay   *Mumbai*
Reached Pre-Final round for designing a cost effective Line Follower Robot.

Teaching Assistance

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

Peer-Reviewed Journal Publications

[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)*. **[To Appear]**.

[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**, 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

[j4] **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, June 2020*, pages 289–303. DOI: 10.1007/s13389-020-00232-9

[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

Peer-Reviewed Conference Publications

[c11] 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*. **[Accepted]**

[c10] 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.

[c9] 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.

[c8] 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.

[c7] **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 Paper Award]**

[c6] **Manaar Alam** and Debdeep Mukhopadhyay, "*How Secure are Deep Learning Algorithms from Side-Channel based Reverse Engineering?*". In *ACM/IEEE Design Automation Conference, DAC 2019, Las Vegas, United States of America, June 2-6, 2019*, pages 226. DOI: 10.1145/3316781.3322465.

[c5] **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.

[c4] 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 Asia and South Pacific Design Automation Conference, ASP-DAC 2019, Tokyo, Japan, January 21-24, 2019*, pages 627–632. DOI: 10.1145/3287624.3287696.

[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 *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 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.

Peer-Reviewed Workshop Publications

[w3] 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.

[w2] **Manaar Alam**, Sayan Sinha, Sarani Bhattacharya, Swastika Dutta, Debdeep Mukhopadhyay, and Anupam Chattopadhyay, "*RAPPER: Ransomware Prevention via Performance Counters*". In *Australian Workshop on Offensive Cryptography, Kangacrypt@AsiaCrypt 2018, Adelaide, Australia, December 7–8, 2018*.

[w1] **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.

Patents

[1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay, "*A System for Detecting Ransomware in a Computer System and a Method Thereof*". Patent No.: IN201831045833A, Filed: December 4, 2018, Published: June 12, 2020.

Manuscripts Under Submission

[8] Suvadeep Hajra, **Manaar Alam**, Sayandeep Saha, Stjepan Picek, and Debdeep Mukhopadhyay, "*More Heads are Better than One: On Softmax Attention for Automatic Selection of Points-of-Interest from Long Traces*".

[7] Shubhi Shukla, **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Pabitra Mitra, "*Whispering MLaaS: Exploiting Timing Channels to Compromise User Privacy in Deep Neural Networks*".

[6] **Manaar Alam**, Esha Sarkar, and Michail Maniatakos, "*PerDoor: Persistent Non-Uniform Backdoors in Federated Learning using Adversarial Perturbation*".

[5] Shubhajit Datta, **Manaar Alam**, Arijit Mondal, Debdeep Mukhopadhyay, and Partha Pratim Chakrabarti, "*A Precise Decision-guided Adversarially Robust Classification Methodology using Traditional Individually Weaker Defences*".

[4] 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*".

[3] Sayandeep Saha, **Manaar Alam**, Arnab Bag, Debdeep Mukhopadhyay, and Pallab Dasgupta, "*Learn from Your Faults: Leakage Assessment in Fault Attacks using Deep Learning*".

[2] **Manaar Alam**, Shubhajit Datta, Debdeep Mukhopadhyay, Arijit Mondal, and Partha Pratim Chakrabarti, "*PARL: Diversity of Ensemble Network to thwart Adversarial Attacks via Pairwise Adversarially Robust Loss Function*".

[1] **Manaar Alam**, Shubhajit Datta, Debdeep Mukhopadhyay, Arijit Mondal, and Partha Pratim Chakrabarti, "*Resisting Adversarial Attacks in Deep Neural Networks using Diverse Decision Boundaries*".

References

o **Debdeep Mukhopadhyay**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, debdeep.mukhopadhyay@gmail.com

o **Partha Pratim Chakraborti**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, ppchak@cse.iitkgp.ac.in

o **Michail Maniatakos**, Associate Professor, Computer Engineering Division, New York University Abu Dhabi, michail.maniatakos@nyu.edu