Manaar Alam

Secured Embedded Architecture Laboratory
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur, West Bengal, India.

+91 9073202113 • alam.manaar@iitkgp.ac.in • manaaralam.github.io
manaaralam • manaar.alam

Current Position

Indian Institute of Technology, Kharagpur **Kharagpur**
Ph. D. in Computer Science and Engineering, *July 2016–Present*

I am working under the supervision of *Prof. Debdeep Mukhopadhyay*. My research interest mainly lies in the application of machine learning techniques in the field of hardware and software security. I have interest on designing robust machine learning based countermeasure for against side-channel attacks, malwares, and ransomwares. I am also interested in different security aspects of machine learning like fault-resistance, privacy leakages, adversarial attacks, etc. I have also worked on analyzing side-channel leakages from secured embedded devices using machine leaning to retrieve the secret key.

Education

Indian Institute of Technology (Indian School of Mines), Dhanbad **Dhanbad**
M. Tech. in Computer Science and Engineering, OGPA - 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**
B. Tech. in Computer Science and Engineering, DGPA - 8.88/10 *August 2009–May 2013*

Hindu School (under WBCHSE) **Kolkata**
Higher Secondary Examination (10+2), Overall - 92.6% *July 2007–May 2009*
Secured *13th* place in all over West Bengal. Scored 100% in Mathematics.

Modern School (under WBBSE) **Kolkata**
Secondary Examination (10), Overall - 89.37% *May 2007*

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.

Academic Projects

M. Tech. Thesis

Title: *A Novel Parallel Search Technique for Multi-Objective Optimization.*

Supervisor: Dr. Haider Banka.

Description: Developed a new Parallel Search Technique to deal with various Multi-Objective Optimization Problems. With binary encoding scheme this novel technique performs better than most of the existing multi-objective optimization algorithms like NSGA-II, and MOPS.

Duration: July 2015 - April 2016.

B. Tech. Dissertation

Title: *Web Sentiment Analysis.*

Supervisor: Dr. Satyajit Chakraborty.

Description: Designed a web tool which allows visitors to assess the web sentiment on any subject. For each topic a pie chart expresses the current real-time sentiment along with a list of the latest news headlines associated with the subject. The pie chart and the headlines allow seeing what issues or events drive the sentiment in a positive or negative way.

Duration: August 2012 - July 2013.

Other Projects

Industrial Collaboration

Title: *Security Analysis of Kubernetes Container-Orchestration System*

Collaborator: IBM Research India

Description: Analyze the security guarantee provided by Kubernetes container-orchestration system. The main objective is to find out possible vulnerabilities and design efficient countermeasures.

Duration: August 2019 - Present.

Title: *De-anonymization of TOR Network*

Collaborator: The Chatterjee Group

Description: Design of an efficient and low-cost solution to build traffic correlation attack on anonymized TOR network in order to de-anonymize TOR user and clients.

Duration: September 2018 - April 2019.

Vocational Training

Title: *Online Job Portal using PHP and MySQL.*

Organizer: NIVT India.

Description: Designed an online job portal which helps both the job seekers and the recruiters to find the right organization and the employees respectively.

Duration: June 2012 - July 2012.

Title: *Online Photo Gallery using J2EE and MySQL*

Organizer: NIVT India.

Description: Developed an online photo gallery allowing every user to create online albums, organize digital photos and to share with other users.

Duration: December 2011 - January 2012.

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.

Invited Talks

- Workshop on Cyber Physical System Security, Indian Institute of Technology Kharagpur, December 2019.
- Workshop on Advanced Side Channel Evaluation of Hardware Security, Indian Institute of Technology Kharagpur, July 2018.

Achievements

- 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 2019-20.
- 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.
- National Merit-cum-Means Scholarship awarded by WBMDFC from 2009 to 2013.
- Certificate of Excellence on ERP – Essentials from Research Software Solutions (P) Ltd. (Microsoft Gold Certified Partner), April 2010.
- National Merit Scholarship awarded by Govt. of India for securing position among Top 20 in Higher Secondary Board Examination in 2009.

Professional Services

- **Reviewer of Journals**: *IEEE TVLSI*, *ACM TECS*, *Springer Sādhanā*
- **Sub-Reviewer of Conferences**: *COSADE '18,'20. DAC '18,'19,'20. TCHES '19,'20*
- **Sub-Reviewer of Workshops**: *TopinHES '18*

Teaching Assistance

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

Extra-Curricular Activities

- Awards and Positions in inter-school sit-and-draw competitions.
- Participated and secured 3rd Prize in a Mathematics Competition at FESTRONIX 2011 held at Institute of Engineering and Management, Kolkata, February 2011.

Personal Details

Date of Birth: 11th February, 1991.
Gender: Male.
Languages Known: English, Bengali, Hindi.
Nationality: Indian.

Patents

[pt1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. A System for Detecting Ransomware in a Computer System and a Method Thereof. [**Filed Indian Patent**. Patent Application No.: TEMP/E-1/49892/2018-KOL]

Journals

[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

Journals Under Review

[sj6] **Manaar Alam**, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. Neural Network-based Inherently Fault-Tolerant Cryptographic Primitives without Explicit Redundancy Checks. In *ACM Journal on Emerging Technologies in Computing Systems (JETC)*. [**Under Review**]

[sj5] Sayandeep Saha, **Manaar Alam**, Arnab Bag, Debdeep Mukhopadhyay, and Pallab Dasgupta. Leakage Assessment in Fault Attacks: A Deep Learning Perspective. In *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*. [**Under Review**]

[sj4] Anirban Chakraborty, **Manaar Alam**, and Debdeep Mukhopadhyay. A Good Anvil Fears No Hammer: Automated Rowhammer Detection using Unsupervised Deep Learning. In *IEEE Transactions on Computer (TC)*. [**Under Review**]

[sj3] **Manaar Alam**, Sarani Bhattacharya, Sourangshu 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)*. [**Under Review**]

[sj2] Sai Praveen Kadiyala, **Manaar Alam**, Yash Shrivastava, Sikhar Patranabis, Muhamed Fauzi Bin Abbas, Arnab Biswas, Debdeep Mukhopadhyay, Siew-Kei Lam, and Thambipillai Srikanthan. LAMBDA: Lightweight Assessment of Malware for emBeddeD Architectures. In *ACM Transactions on Embedded Computing Systems (TECS)*. [**First Revision Submitted**]

[sj1] **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)*. [**First Revision Submitted**]

Conferences

[c10] 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.

[c9] **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*. [**Accepted**] [**Best Paper Award**]

[c8] **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.

[c7] **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.

[c6] 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.

[c5] **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 2018, Adelaide, Australia, December 7–8, 2018*.

[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 *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.

Poster Presentations

[p6] **Manaar Alam** and Debdeep Mukhopadhyay. How Secure are Deep Learning Algorithms from Side-Channel based Reverse Engineering? *POSTER: ACM/IEEE Design and Automation Conference (DAC)*, Las Vegas, United States of America, June 2019.

[p5] **Manaar Alam**, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. Enhancing Fault Tolerance of Neural Networks for Security-Critical Applications. *POSTER: ACM/IEEE Design and Automation Conference (DAC)*, Las Vegas, United States of America, June 2019.

[p4] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. Detecting Malware and Ransomware using Hardware Performance Counters. *POSTER: Security, Privacy, and Applied Cryptography Engineering (SPACE)*, Kanpur, India, December 2018. **[Third Best Poster Award]**

[p3] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. Detecting Malware and Ransomware using Hardware Performance Counters. *POSTER: IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington DC, United States of America, May 2018.

[p2] Sai Praveen Kadiyala, Muhamed Fauzi Bin Abbas, Yash Shrivastava, Sikhar Patranabis, **Manaar Alam**, Debdeep Mukhopadhyay, Siew-Kei Lam, and Thambipillai Srikanthan. LAMBDA: Lightweight Assesment of Malware for emBeddeD Architectures. *POSTER: Singapore International Cyber Week (SICW)*, Singapore, September 2017.

[p1] **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. *POSTER: Cyber Security Awareness Week (CSAW)*, Kanpur, India, November 2016.

arXiv/ePrint Papers

[i6] **Manaar Alam**, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. Enhancing Fault Tolerance of Neural Networks for Security-Critical Applications In *arXiv, CoRR, abs/1902.04560*, February 2019. **[Accepted as Work-in-Progress in DAC 2019]**

[i5] Nimesh Shah, **Manaar Alam**, Durga Prasad Sahoo, Debdeep Mukhopadhyay, and Arindam Basu. A 0.16pJ/bit Recurrent Neural Network Based PUF for Enhanced Machine Learning Atack Resistance In *arXiv, CoRR, abs/1812.05347*, December 2018. **[Accepted in ASP-DAC 2019]**

[i4] **Manaar Alam** and Debdeep Mukhopadhyay. How Secure are Deep Learning Algorithms from Side-Channel based Reverse Engineering? In *arXiv, CoRR, abs/1811.05259*, November 2018. **[Accepted as Late-Breaking-Results in DAC 2019]**

[i3] Anirban Chakraborty, **Manaar Alam**, Vishal Dey, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. Adversarial Attacks and Defences: A Survey. In *arXiv, CoRR, abs/1810.00069*, September 2018.

[i2] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. RAPPER: Ransomware Prevention via Performance Counters. In *arXiv, CoRR, abs/1802.03909*, February 2018. **[Modified Version Accepted in Kangacrypt 2018]**

[i1] **Manaar Alam**, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Sourangshu Bhattacharya. Performance Counters to Rescue: A Machine Learning based safeguard against Micro-architectural Side-Channel-Attacks. In *Cryptology ePrint Archive, Report 2017/564*, July 2017.

References

- **Dr. Debdeep Mukhopadhyay**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, debdeep@cse.iitkgp.ac.in
- **Dr. Haider Banka**, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, banka.h.cse@ismdhanbad.ac.in