An Interdisciplinary Workshop on

Machine Learning for Cryptology

(November 8 – 10, 2023)

INDIAN STATISTICAL INSTITUTE
203, B. T. ROAD, KOLKATA – 700108

Organised by:
Centre for Artificial Intelligence and Machine Learning (CAIML), ISI Kolkata
and
Scientific Analysis Group (SAG), DRDO, Ministry of Defence, Government of India

Program Details

Day 1: November 8, 2023		
10:30 – 11:30	Registration	
11:30 – 12:00	Inaugural Session	Background Details and Welcoming to the Workshop
12:00 – 12:30	High Tea/Coffee Break	
12:30 – 13:30	Technical Session I	Traversing Generative Deep Models: From VAE to LLMs - Foundations, Bias, Responsible Usage, and Future Frontiers Swagatam Das Indian Statistical Institute, Kolkata / TCG CREST
13:30 – 14:30	Lunch Break	
14:30 – 15:30	Technical Session II	Application of Machine Learning in Cryptanalysis Santanu Sarkar Indian Institute of Technology, Madras
15:30 – 16:00	Tea/Coffee Break	
16:00 – 17:00	Technical Session III	Generative AI and ML Models in Cryptology Saibal K. Pal Defence Research and Development Organisation, India
17:00 – 18:00	Technical Session IV	Explainable AI for Cybersecurity Prabhat Mishra University of Florida, USA
Day 2: November 9, 2023		
11:00 – 12:00	Technical Session V	Differential-ML Distinguisher: Extending Classical Differential Distinguishers using Machine Learning Tarun Yadav Defence Research and Development Organisation, India
12:00 – 12:30	High Tea/Coffee Break	
12:30 – 13:30	Technical Session VI	Convergence of Hardware Cryptography and ML for Enhanced Security Amlan Chakrabarti Calcutta University / Indraprastha Institute of Information Technology, Delhi
13:30 – 14:30	Lunch Break	
14:30 – 15:30	Technical Session VII	Challenges to Trustworthy AI Pooja Yadav Defence Research and Development Organisation, India
15:30 – 16:00	Tea/Coffee Break	
16:00 – 17:00	Data Science Challenge Session	Presentations by the best performing team(s)
17:00 – 18:00	Visit to the Geology Museum	
19:00 – 20:30	Banquet	
Day 3: November 10, 2023		

11:00 – 12:00	Valedictory Session	Offering of Certificates
12:00 – 12:30	Tea/Coffee Break	
12:30 – 13:30	Networking Session	Discussing the Next Steps
13:30 – 14:30	Lunch Break	
14:30 – 15:30	Photo Session	

VENUE for Different Sessions: CVPRU Seminar Room, 8th Floor, Library Building, ISI, Kolkata
VENUE for Lunch: Guest House, ISI, Kolkata
VENUE for Banquet: Guest House, ISI, Kolkata
GEOLOGY MUSEUM: Ground Floor, PJA Building, ISI, Kolkata

Details of Technical Talks

Traversing Generative Deep Models: From VAE to LLMs - Foundations, Bias, Responsible Usage, and Future Frontiers

Swagatam Das

Indian Statistical Institute, Kolkata / TCG CREST

Abstract: This talk embarks on a comprehensive journey through the landscape of Generative Deep Models, commencing from the foundational principles underlying models like Variational Autoencoders (VAEs) and advancing to the state-of-the-art Large Language Models (LLMs). Delving into the intricate nuances of inherent biases, it delves deep into ethical considerations and the importance of responsible model deployment. Furthermore, the discussion extends to explore the emerging challenges and future horizons in the realm of generative deep learning, paving the way for a more informed and ethically-conscious adoption of these transformative technologies.

Speaker's Bio: Swagatam Das earned his B.E. in Electronics and Telecommunications Engineering, M.E. with a specialization in Control Engineering, and Ph.D.(Engineering) degrees from Jadavpur University, India, in the years 2003, 2005, and 2009, respectively. Currently a Professor at the Indian Statistical Institute (ISI), Kolkata, India, he previously served as the Head of the Electronics and Communication Sciences Unit at ISI Kolkata from 2021 to 2023. Presently, he also holds the position of Professor and Deputy Director at the Institute for Advancing Intelligence (IAI), TCG CREST, Kolkata, India. His research interests encompass deep learning and non-convex optimization, and he published over 400 research articles in reputed venues. Dr. Das is the founding Co-Editor-in-Chief of Swarm and Evolutionary Computation, an international journal by Elsevier. He has served or is currently serving as an Associate Editor for several prominent journals, including the IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Cybernetics, IEEE Transactions on Evolutionary Computation, Pattern Recognition (Elsevier), Neurocomputing (Elsevier), Information Sciences (Elsevier), IEEE Trans. on Systems, Man, and Cybernetics: Systems, among others. He is a member of the editorial board of Information Fusion (Elsevier), Progress in Artificial Intelligence (Springer), Applied Soft Computing (Elsevier), Engineering Applications of Artificial Intelligence (Elsevier), and so on. Dr. Das has received over 30,000 Google Scholar citations and an H-index of 82 till date. He has actively participated in the program committees and organizing committees of renowned international conferences such as NeurIPS, AAAI, ICML, AISTATS, CVPR, IEEE CEC, GECCO, and more. He currently serves as an ACM Distinguished Speaker. He is the recipient of the 2012 Young Engineer Award from the Indian National Academy of Engineering (INAE) and the 2015 Thomson Reuters Research Excellence India Citation Award for being the highest-cited researcher in Engineering and Computer Science in India between 2010 and 2014.

Application of Machine Learning in Cryptanalysis

Santanu Sarkar

Indian Institute of Technology, Madras

Abstract: In this talk, first we will discuss some optimization techniques inspired from nature and also Bayesian optimization. Then, we present how one can use machine learning techniques to analyse ciphers.

Speaker's Bio: Santanu Sarkar received the Ph.D. degree in Mathematics from the Indian Statistical Institute, Kolkata, India, in 2011. He was a Guest Researcher at the National Institute of Standards and Technology (NIST). He is currently a professor at the Indian Institute of Technology, Madras, India. His main research interests include cryptology and number theory.

Generative AI & ML Models in Cryptology

Saibal K. Pal

Defence Research and Development Organisation, India

Abstract: This talk will introduce different AI & ML based generative models and discuss their potential usages in the area of cryptology in particular.

Speaker's Bio: Dr. Saibal K. Pal is a Senior Scientist at Scientific Analysis Group, Defence Research & Development Organization (DRDO), Delhi. He has served as the Director of Information Technology and Cyber Security in the Ministry last year. He received his PhD in Computer Science from University of Delhi and is an Invited Faculty & Research Guide at a number of national institutions. He has more than 2 decades of experience of working in public sector and has closely worked on the policy formulation and implementation for various types of communities in India. His areas of

interest are E-Governance, Information & Network Security, Computational Intelligence and Information Systems. He has more than 200 publications in books, journals & international conference proceedings.

Explainable AI for Cybersecurity

Prabhat Mishra

University of Florida, USA

Abstract: This talk provides a comprehensive overview of security vulnerabilities and state-of-the-art countermeasures using explainable AI. Specifically, it will cover how explainable AI can be effectively used for detection and mitigation of hardware as well as software vulnerabilities. It also provides insights into the security threats towards machine learning models and presents effective countermeasures. The attendees will be able to get a complete picture of cybersecurity challenges and how to detect them using machine learning techniques for designing secure and trustworthy systems.

Speaker's Bio: Prabhat Mishra is a Professor in the Department of Computer and Information Science and Engineering and a UF Research Foundation Professor at the University of Florida. His research interests include embedded systems, hardware security, system-on-chip validation, explainable AI, and quantum computing. He currently serves as an Associate Editor of ACM Transactions on Embedded Computing Systems. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), a Fellow of the American Association for the Advancement of Science (AAAS), and a Distinguished Scientist of the Association for Computing Machinery (ACM).

Differential-ML Distinguisher: Extending Classical Differential Distinguishers using Machine Learning

Tarun Yadav

Defence Research and Development Organisation, India

Abstract: The differential attack is a basic cryptanalytic technique for block ciphers. Application of machine learning shows promising results for the differential cryptanalysis. In this talk, the author will present a novel approach to extend the classical differential distinguisher using machine learning. The application of the approach on three lightweight block ciphers SPECK32, SIMON32, and GIFT64 will be discussed and results will be presented.

Reference Paper for the talk: Yadav, T., Kumar, M. (2021). Differential-ML Distinguisher: Machine Learning Based Generic Extension for Differential Cryptanalysis. In: Longa, P., Ràfols, C. (eds) Progress in Cryptology – LATINCRYPT 2021. LATINCRYPT 2021. Lecture Notes in Computer Science (LNCS), vol. 12912. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-88238-9_10

Speaker's Bio: Tarun Yadav completed his B.Tech in Computer Science and Engineering from IIT Ropar in 2012. He is currently working as a Scientist in the Scientific Analysis Group, DRDO. His research area includes cryptanalysis of block ciphers and protocol analysis. He has published various research papers related to differential cryptanalysis of block ciphers.

Convergence of Hardware Cryptography and ML for Enhanced Security

Amlan Chakrabarti

Calcutta University / Indraprastha Institute of Information Technology, Delhi

Abstract: Security in the digital age is an ever-evolving challenge, and organizations are continually seeking innovative ways to safeguard their sensitive data and systems. The convergence of hardware cryptography and machine learning (ML) presents a promising frontier for achieving enhanced security. This talk explores the seamless integration of hardware-based encryption techniques with the power of ML algorithms, enabling more robust protection against modern cyber threats.

Speaker's Bio: Dr. Amlan Chakrabarti is a Full Professor at the A.K. Choudhury School of Information Technology, University of Calcutta, with over 20 years of experience in Engineering Education and Research. He is also the former Dean of the Faculty of Engineering & Technology of his University (2016-2019). He was a Post-Doctoral fellow at the Princeton University, USA, in 2011-2012. Dr. Chakrabarti has received numerous prestigious awards, including the DST BOYSCAST fellowship in Engineering Science, the INSA Visiting Faculty Fellowship, and the JSPS Invitation Research Award. He is recognized for his contributions to academia, winning the Erasmus Mundus Leaders Award, the Hamied Visiting Professorship at the University of Cambridge, Siksha Ratna Award from the Dept. of Higher Education, Govt. of

West Bengal, and being the Fellow of West Bengal Academy of Science and Technology. He actively leads the University's participation in the ALICE-India Collaboration at CERN Geneva and heads the IT and Technology Innovation Cell for the Department of Higher Education, Govt. of West Bengal. He has lead 15+ funded research projects funded by Government agencies as well as industries till date. Dr. Chakrabarti's research focuses on various areas, including Machine Learning, Computer Vision, Reconfigurable Computing, VLSI CAD, and Quantum Computing. He has supervised 20+ Ph.D. students, published over 200 research papers, and served as an editor for esteemed journals and book series published by Elsevier and Springer Nature. His extensive contributions to both national and international research make him a respected figure in the field.

Challenges to Trustworthy AI

Pooja Yadav

Defence Research and Development Organisation, India

Abstract: AI has shown wide applicability in human life which also raises relevant concerns regarding its safety, security, privacy and ethics. The answer to these issues is not straight forward and thus need to be dealt in a unified way. To address these concerns, the concept of “Trustworthy AI” has emerged. AI systems raise the bar in terms of the set of properties for “Trustworthy AI”. For an AI system to be trustworthy, following characteristics should be considered collectively in the overall lifecycle of an AI system, starting from the design and development phase to the deployment and operational phase of an AI system: Fairness, Transparency, Accountability, Robustness and Reliability, Privacy, Safety and Security. Trustworthiness is a prerequisite for people and societies to develop, deploy and use AI systems. Striving towards Trustworthy AI concerns not only the trustworthiness of the AI system itself, but requires a holistic and systemic approach, encompassing the trustworthiness of all actors and processes that are part of the system’s socio-technical context throughout its entire life cycle. Various countries and technology giants are working on technical controls, regulations and standardization front to make these properties realizable.

Speaker’s Bio: Pooja Yadav is a Scientist ‘F’ at Scientific Analysis Group, Defence Research & Development Organization (DRDO), Delhi. She completed her postgraduate degree from IISc Banglore with specialization in Machine Learning. She has received DRDO strategic contribution award and many team awards for various activities. She has more than 20 years of work experience with DRDO. She worked in many security critical projects and evaluated security of many IT products which are being utilised by security agencies. Since the last 10 years, she developed state-of-the-art cryptanalysis tools to uncover messages which were encrypted using the same key and text completion tools for various Indian regional languages. Currently her team is working on developing a framework to evaluate Trustworthiness of AI systems.