المعهد الهندي للتكنولوجيا دلهي أبوظبي
INDIAN INSTITUTE OF TECHNOLOGY DELHI ABU DHABI

AiSS

Research Symposium on AI, Security & Silicon:

Building Next Generation Intelligent Systems

28th May 2025 | IIT Delhi – Abu Dhabi

AiSS

SYMPOSIUM

About the Symposium

The rapid convergence of artificial intelligence (AI), robust security frameworks, and advanced silicon design is reshaping the technological landscape, paving the way for next-generation intelligent systems. As these fields evolve, they present unprecedented opportunities to create systems that are not only powerful and efficient but also secure and ethically sound. However, this convergence also introduces complex challenges, including ensuring system resilience, scalability, and trustworthiness in an increasingly interconnected world.

Motivated by the need to address these challenges and harness the transformative potential of AI, security, and silicon innovation, this research symposium aims to bring together academics, researchers, industry, and innovators for fruitful interactions at IIT Delhi – Abu Dhabi. The goal of the research symposium is to foster discussion and inspire interdisciplinary collaboration across top technical institutes in the region.

Organized by
IIT Delhi - Abu Dhabi

The Indian Institute of Technology Delhi (IIT Delhi) is one of India's premier institutions for education and research in science, technology, and engineering. IIT Delhi–Abu Dhabi, its international campus, represents a visionary step in extending IIT Delhi's legacy to the dynamic innovation ecosystem of the UAE.

Located in Khalifa City B, Abu Dhabi, this campus is the result of a strategic collaboration between India and the UAE, aimed at advancing excellence in education, research, and innovation. With a focus on cutting-edge fields such as artificial intelligence, sustainable technologies, and advanced computing, IIT Delhi–Abu Dhabi is poised to emerge as a global hub for transformative academic and industry-led initiatives.

Event Schedule

28th May

09:30 – 09:45	**Prof. Shantanu Roy, Exec. Director, IIT Delhi - Abu Dhabi**	Introduction and Opening Remarks
09:45 – 10:15	**Dr. Manan Suri, IIT Delhi**	Technical Talk
10:15 – 10:45	**Dr. Shreekant Thakkar, Technology Innovation Institute**	Keynote
10:45 – 11:00	**TEA/COFFEE BREAK AND GROUP PHOTO**	
11:00 – 11:30	**Dr. Lilas Alrahis, Khalifa University**	Technical Talk
11:30– 12:00	**Dr. Chetan Arora, IIT Delhi**	Technical Talk
12:00 – 12:30	**Dr. Samuel F. Feng, Sorbonne University Abu Dhabi**	Technical Talk
12:30 – 01:30	**LUNCH BREAK**	
13:30 – 14:00	**Dr. Hariprasad Kodamana, IIT Delhi - Abu Dhabi**	Technical Talk
14:00 – 14:30	**Dr. Sandeep Kumar, IIT Delhi**	Technical Talk
14:30 – 15:00	**Dr. Ghada Alsuhli, Khalifa University**	Technical Talk
15:00 – 15:15	**TEA/COFFEE BREAK**	
15:15 – 15:30	**Dr. Akashdeep, New York University Abu Dhabi**	Technical Talk
15:30 – 15:45	**Dr. Rachmad V. W. Putra, New York University Abu Dhabi**	Technical Talk
15:45 - 16:00	**Ms. Esrat Khan, Khalifa University**	Technical Talk
16:00 – 16:15	**Prof. M. Ali Haider, IIT Delhi - Abu Dhabi**	Closing Remarks, Way Forward

10+ Speakers

Speakers

Gain insights from pioneering voices at IIT Delhi, IIT Delhi - Abu Dhabi, New York University Abu Dhabi, Khalifa University, Sorbonne University Abu Dhabi, and Technology Innovation Institute (TII).

Keynote

Zero-Trust Robotics

Dr. Shreekant (Ticky) Thakkar

Technology Innovation Institute (TII)

Biosketch

Dr. Shreekant (Ticky) Thakkar is Chief Researcher at the Secure Systems Research Centre, Technology Innovation Institute (TII), UAE, and Adjunct Research Professor at Khalifa University. He leads research on zero-trust end-to-end security, resilience, and safety in cyber-physical and autonomous systems—such as drone swarms -leveraging generative AI and large language models (LLMs).

His team has developed and commercialized integrated systems combining UAVs, UGVs, and human first responders, operating over secure zero-trust mesh and long-range networks. They are also commercializing secure mobile platforms with zero-trust apps for smartphones and laptops.

Dr. Thakkar's work spans embedding zero-trust security into silicon, edge, mobile, and cloud platforms. He actively collaborates with open-source ecosystems including Dronecode, RISC-V, Linux, Apache, and ROS, and with research institutions in the US, Europe, and UAE. Previously, he was Chief Scientist and EVP at a UAE cybersecurity firm, where he helped deliver secure smartphones and VPN appliances. He also held senior roles at Qualcomm, HP, and Intel, including 21 years at Intel as Fellow and Chief Systems Architect for Mobile Systems Technologies.

Dr. Thakkar is a recognized innovator who has launched startups within major tech organizations. He holds a PhD and M.Sc. in Computer Science from the University of Manchester, has authored 45 publications, holds 87 patents, and has over 5,000 Google Scholar citations.

Building an Intelligent Memory-Centric Computing Paradigm

Dr. Manan Suri

Indian Institute of Technology Delhi

Abstract

Research in the field of neuromorphic and cognitive computing has generated a lot of interest in recent years. With potential application in fields such as large-scale data-driven computing, robotics, intelligent autonomous systems, and more bio-inspired computing paradigms are being investigated as the next generation (post-Moore, non-Von Neumann) ultra-low power computing solutions. In this talk we discuss the role that emerging non-volatile resistive memory technology (PCM, CBRAM, OxRAM etc.) can play in dedicated neuromorphic hardware. We focus on novel low-power architectures, programming methodologies, material engineering and optimized synaptic-plasticity emulation. Prototype applications such as complex visual- and auditory pattern extraction is also discussed. We also discuss security use cases based on efficient device-technology co-optimization.

Biosketch

Dr. Manan Suri leads the NVM and Neuromorphic Hardware Research group at IIT Delhi, focusing on Non-Volatile Memory technologies and their applications in AI, neuromorphic computing, and security. Named among MIT Technology Review's Top 35 Innovators (2018), he has received numerous honors, including the IEEE EDS Early Career Award and NASI Young Scientist Award. Dr. Suri has filed multiple patents, published 130+ papers, and led over 25 research projects. He founded CYRAN AI Solutions, an IIT Delhi startup, and advises major tech companies and government bodies.

Graph Neural Networks for Optimized Electronic Design Automation

Dr. Lilas Alrahis

Khalifa University

Abstract

Graph neural networks (GNNs) have demonstrated state-of-the-art results in performing circuit-related tasks across various fields of electronic design automation (EDA). In this talk, I will discuss how GNNs work, how circuits can be represented as graphs, and demonstrate a few examples of hardware security tasks solved using GNNs. Next, I will explore the future of these models and the broader role of machine learning in EDA, including how we can move toward agentic artificial intelligence in this domain. In addition to what GNNs and existing models will need in order to make that shift.

Biosketch

Lilas Alrahis is an Assistant Professor in the Department of Computer and Information Engineering at Khalifa University, Abu Dhabi, UAE. Previously, she was a Postdoctoral Associate at New York University Abu Dhabi (NYUAD), UAE, from March 2021 to August 2024, and a member of the NYUAD Center for Cyber Security. Dr. Alrahis' research focuses on hardware security, design-for-trust, and applied machine learning. She has received the MWSCAS Myril B. Reed Best Paper Award in 2016, the Best Paper Award at the Applied Research Competition during Cyber Security Awareness Week in 2019 and 2021, and the Karlsruhe Institute of Technology (KIT) International Excellence Fellowship in Germany for 2023. Additionally, in July 2023, she was awarded the NYUAD Collaboration Grant. Dr. Alrahis serves as an Associate Editor for the Integration, VLSI Journal and is the Chair of the IEEE Women in Engineering affinity group in the UAE..

Translating Clinical Insights to AI Models for Cancer Detection

Dr. Chetan Arora

Indian Institute of Technology Delhi

Abstract

In the era of foundational models, researchers are increasingly focussed on developing generalist AI models which may help with various tasks from pathology to radiology, for diagnosing malaria to cancer. When lives are at stake, anything but the highest achievable accuracy is unacceptable. In our group, we wish to leverage the strengths of foundational models, but would also like to specialise them for specific medical imaging tasks, which makes them more accurate, explainable, and robust. In this talk, I will illustrate through examples from some of our recent works in detection of breast cancer detection from mammograms, and gall bladder cancer detection from ultrasound images, how we took inspiration from clinical workflow, and translated them to develop state-of-the-art AI models for cancer detection.

Biosketch

Prof. Chetan Arora is a Microsoft Chair Professor in the CS department at IIT Delhi, Director of the Computer Vision group, and leads the AI in Healthcare lab. He also holds a joint appointment with the School of AI at IIT Delhi and is adjunct faculty at IIIT Delhi. An internationally recognized expert in computer vision and AI, he has over 100 publications in top-tier venues, including 13+ papers at CVPR and several in MICCAI. He has filed 13+ patents and supervised 23 PhD students. With global research collaborations and a decade of industry leadership, he bridges academia and applied innovation.

Interpretable Energy-Based Models for Trustworthy Biomedical AI

Dr. Samuel F. Feng

Sorbonne University Abu Dhabi

Abstract

Medical-AI systems must be understandable to clinicians, verifiable by regulators, and securely deployable on whatever silicon their end-users control-from compact edge devices to private data centers. I will present recent progress in an interpretability-first framework built on energy-based models (EBMs) whose learned energy landscapes act as intuitive decision maps that physicians and auditors can inspect in real time. We'll describe research progress on a few fronts, including a geometry-aware case study in cardiac-ablation guidance shows how embedding anatomical and temporal structure yields calibrated predictions and interactive heat-maps, all while supporting tamper-resistant, end-user execution. We also discuss a reproducibility suite that benchmarks EBM calibration, conformal uncertainty, and energy-map interpretability across a variety of medical imaging datasets. The talk traces the full pipeline-from mathematical insight to secure deployment—highlighting open challenges in robustness, identifiability, and hardware co-design, and inviting collaboration across AI, security engineering, and silicon research communities.

Biosketch

Dr. Samuel F. Feng holds a PhD in Applied & Computational Mathematics from Princeton University and is currently an assistant professor at Sorbonne University Abu Dhabi and affiliated faculty at the Sorbonne Center for Artificial Intelligence (SCAI). His research focuses on interpretable, uncertainty-aware AI systems, with recent work on energy-based models for biomedical applications. He has published 20+ peer-reviewed papers and serves on editorial boards of several international journals.

Generative AI as a Multi-Scale Enabler in Guiding the Energy Transition

Dr. Hariprasad Kodamana

Indian Institute of Technology Delhi - Abu Dhabi

Abstract

The global shift towards sustainable and renewable energy systems presents one of the most critical challenges of our time, necessitating innovative approaches that span multiple scales-from atomic to grid-level dynamics. This talk explores how generative AI serves as a transformative tool in this transition by leveraging its capacity to model complex, interconnected systems. This talk explores applications of generative models in accelerating the discovery of innovative materials for energy applications, identifying novel process routes, and helping process integration while addressing process-environment interactions.

Biosketch

Hariprasad Kodamana is an Associate Professor in the Department of Chemical Engineering and the Yardi School of Artificial Intelligence at IIT Delhi. He joined IIT Delhi in 2018, following a brief tenure at IIT Kharagpur. Prof. Kodamana was a post-doctoral fellow at the University of Alberta, Canada. His research interests encompass various interdisciplinary fields, including AI/ML, optimization and control, and sustainable and net-zero systems within the broader scope of process systems engineering. His work has been focused on advancing computational methods and AI-driven tools to enhance the efficiency, sustainability, and optimization of chemical processes. With over a decade of experience, he has developed innovative algorithms that integrate computational models and machine learning to drive the efficiency and sustainability of complex chemical processes. He has made significant research contributions, with over 90 original research publications, two patents, and a book. He is serving as a subject editor for two prestigious international journals.

GCX: Graph Learning for Scalable, Label-Efficient Analog Circuit Automation

Dr. Sandeep Kumar

Indian Institute of Technology Delhi

Abstract

Graph learning is redefining structured optimization by enabling data-efficient, topology-aware modeling of complex systems. We begin with a primer on Graph Machine Learning fundamentals and then demonstrate its transformative application to analog circuit design - a domain marked by vast design spaces and simulation bottlenecks. We present Graph of Circuits Explorer (GCX), a semi-supervised framework that learns circuit similarity via Dirichlet energy minimization and propagates performance labels using Graph Neural Networks and kernelized regressors. Integrated with domain-specific optimizers (EASCO and ASTROG), GCX enables scalable, transferable, and simulation-efficient analog sizing. This work positions graph learning as a powerful enabler of intelligent hardware design and structured decision-making.

Biosketch

Sandeep Kumar is an assistant professor in the Department of Electrical Engineering and School of Artificial Intelligence (ScAI) at the Indian Institute of Technology Delhi (IIT Delhi). He heads the Machine Intelligence Signals and Networks (MISN) lab at IIT Delhi. His current research focuses on graphical models, manifolds, semi-supervised learning, and large-scale optimization. He received his M.Tech and PhD degrees from the Indian Institute of Technology (IIT), Kanpur, and completed his postdoc from the Hong Kong University of Science and Technology.

Efficient Hardware Acceleration of FALCON for Post-Quantum Cryptography

Dr. Ghada Alsuhli

Khalifa University

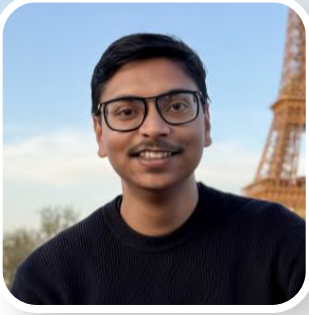
Abstract

The emergence of quantum computing threatens to break widely used public-key cryptosystems such as RSA and ECC, prompting the development and standardization of Post-Quantum Cryptography (PQC) schemes. Among these, FALCON—a lattice-based digital signature algorithm—offers strong security guarantees but imposes heavy computational demands, particularly in its reliance on FFT, NTT, and complex sampling operations. This talk presents our recent work from the System-on-Chip (SoC) Center at Khalifa University, where we design and implement high-performance, resource-efficient hardware accelerators tailored for FALCON. We introduce specialized FFT/IFFT, NTT, and dual-sampling engines optimized for the algorithm's unique structure and security parameters. Our architectures explore the trade-offs between throughput, area, and configurability, making them well-suited for constrained platforms such as edge devices. The proposed designs achieve notable improvements in speed and resource utilization, contributing to the broader goal of building quantum-resilient digital systems.

Biosketch

Dr. Ghada Alsuhli is a postdoctoral fellow at Khalifa University, specializing in hardware acceleration for cryptography, AI, and secure embedded systems. Her research focuses on energy-efficient hardware for post-quantum cryptography, especially the FALCON signature scheme. She leads projects on generative AI, deep learning hardware, and secure quantum-resilient systems. With a PhD in Electrical and Computer Engineering, she integrates hardware design, AI, and networks.

Securing Fabless ICs: Automated Cryptographic Logic Locking with LLM-Driven CAD



Dr. Akashdeep Saha

New York University Abu Dhabi

Abstract

Integrated circuits (ICs) are the backbone of modern computing systems. However, escalating design costs and tight time-to-market pressures have driven companies to adopt a fabless model by outsourcing fabrication to offshore foundries. This model introduces security and trust challenges, from IP piracy and hardware trojans to reverse engineering, causing billions of dollars in losses. Logic locking addresses these threats by embedding key-based logic so that only the correct secret key restores functionality. However, successive locking schemes often succumb to new attacks, exposing unforeseen vulnerabilities. We review attacks on advanced techniques such as a cellular automaton–based sequential scheme and the CAS-Lock combinational approach. We then present two cryptographically secure locking primitives that resist all existing threats to logic locking. Next, we analyze optimal locations in a circuit to lock to balance resilience and overhead and introduce an end-to-end framework, MIDAS, to automate diverse locking strategies. Finally, we demonstrate how a large language model (LLM) can accelerate the design and evaluation of secure logic locking with far less manual effort.

Biosketch

Akashdeep Saha received his PhD from the Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Kharagpur, India. Currently, he is a postdoctoral associate at the Centre for Cyber Security, New York University Abu Dhabi. His broad area of research is hardware security and logic obfuscation.

Towards Energy-Efficient and Reliable Spiking Neural Network Systems

Dr. Rachmad Vidya Wicaksana Putra

New York University Abu Dhabi

Abstract

Neuromorphic computing with Spiking Neural Networks (SNNs) offers a promising path to ultra-low power consumption, thanks to their sparse, spike-based operations and bio-inspired learning. This makes them ideal for resource-constrained embedded machine learning systems that aim to enhance human productivity. However, SNNs still face challenges in energy efficiency and reliability due to high memory access energy and hardware faults such as permanent defects and soft errors. In this talk, I will present our research at the eBRAIN Lab (Prof. Shafique, NYU-AD) on enabling energy-efficient and reliable SNN systems through a cross-layer approach. The talk will introduce SNN fundamentals, outline key challenges, and highlight cutting-edge hardware/software optimizations and low-cost fault mitigation strategies for dependable, low-overhead SNN deployment.

Biosketch

Dr. Rachmad earned his PhD in Computer Science from TU Wien, Austria, and holds B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from ITB, Indonesia, with Cum Laude distinction. He has served in academic roles at ITB and TU Wien and worked in industry as an FPGA engineer in Indonesia and Austria. Currently, he is a Research Team Leader at eBRAIN Lab, New York University Abu Dhabi. His research focuses on brain-inspired computing, neuromorphic engineering, computer architecture, VLSI, system-on-chip, emerging devices, and energy-efficient embedded AI.

Secure PLCs: Logic Locking for Structured Text

Ms. Esrat Khan

Khalifa University

Abstract

PLCs are fundamental components in Industrial Control Systems, yet they remain vulnerable to cyber threats, including control logic injection attacks. Existing security measures, such as network encryption and anomaly detection, fail to protect the internal logic of PLCs from unauthorized modifications. This talk introduces a novel PLC security framework based on logic locking that integrates encryption into the widely used Structured Text language of PLC programming. The proposed method is facilitated by the use of the recently developed SPeLL technique for behavioral FSM logic locking and its hardware security toolchain. Unlike FSM state obfuscation methods, SPeLL is based on the concept of FSM transition obfuscation, and its adoption ensures that unauthorized PLC access results in incorrect execution paths of the control program, thereby protecting against reverse engineering attacks. The framework is validated through virtual commissioning using CODESYS and Factory IO, demonstrating its effectiveness in industrial automation environments.

Biosketch

Esrat Khan holds an MSc in Electrical and Computer Engineering from Khalifa University, Abu Dhabi, UAE, and is currently pursuing her PhD in the same field. Her PhD research focuses on Federated Machine Learning for Process Automation. She has contributed to several international conferences. Additionally, her team, KU-TII, secured second place in the HeLLO CTF 2023 competition. She has completed internships at Lockheed Martin and Al Ramz Corporation, working on unmanned systems and financial automation. Esrat is dedicated to advancing technology through research and development.

Organiser

IIT Delhi - Abu Dhabi, Office of the Vice Provost for Research and External Engagement

Symposium Coordinators

Prof. Manan Suri
(IIT Delhi)

Prof. Lilas Alrahis
(Khalifa University)

المعهد الهندي للتكنولوجيا دلهي أبوظبي
INDIAN INSTITUTE OF TECHNOLOGY DELHI ABU DHABI

TĀQA-AI BOOTCAMP

Energy and AI Summer Bootcamp

*Exclusively designed for **Class 11** and **12***

4th- 8th August, 2025 | IIT Delhi – Abu Dhabi

Organised by
Office of the Vice Provost for
Research and External Engagement

Email: vp.research@iitdabudhabi.ac.ae

Phone: (+971) 50 355 9173

Mark your Calendar...

International Conference on

AI and Materials for Sustainability

Water – Energy – Climate

15th - **17**th December, 2025

Organised by
IIT Delhi – Abu Dhabi

المعهد الهنـدي للتكنولوجيـــا دلهي
أبـــوظبي
INDIAN INSTITUTE OF TECHNOLOGY DELHI
ABU DHABI

AIMS 2025
AI & MATERIALS FOR SUSTAINABILITY

Mark your Calendar...

www.aims2025.com
info@aims2025.com

UiT Norges arktiske universitetsmuseum

University of Inland Norway

المعهد الهندي للتكنولوجيا دلهي أبوظبي
INDIAN INSTITUTE OF TECHNOLOGY DELHI ABU DHABI

Workshop on

Photonics, Genomics and AI for Health

18-19 December 2025

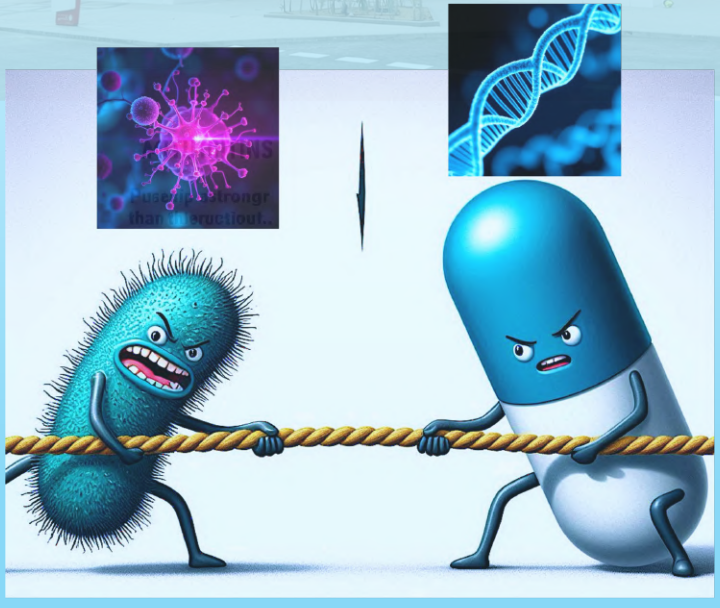
Indian Institute of Technology Delhi – Abu Dhabi

Key Themes:

- Novel Photonics Tools for Health
- Anti-Microbial Resistance & Genomics
- AI and Photonics for Health
- Health-Tech Innovations

Special Highlights:

Panel Discussions with Global Experts
Industry Connect Sessions
Poster Presentations
Networking Opportunities



Be Part of Transforming Healthcare with Cutting-Edge Research!

Contact

Prof. Joby Joseph
Provost, IITD-Abu Dhabi
Email: joby@iitdabudhabi.ac.ae

IITD-AD

المعهد الهندي للتكنولوجيا دلهي أبوظبي
INDIAN INSTITUTE OF TECHNOLOGY DELHI ABU DHABI

Location

Khalifa city B, Abu Dhabi UAE

Mark your Calendar...

Notes

Notes

AiSS

المعهد الهندي للتكنولوجيا دلهي
أبوظبي

INDIAN INSTITUTE OF TECHNOLOGY DELHI
ABU DHABI

Location

IIT Delhi - Abu Dhabi, Khalifa City B, Abu Dhabi, UAE

Contact

Office of the Vice Provost for Research and External Engagement
(+971) 50 355 9173
vp.research@iitdabudhabi.ac.ae