	830 AM - 900 AM	9 AM - 10 AM	10 AM - 1030 AM	1030 AM - 12 NOON	12 - 130 PM	130 PM - 3 PM	3 PM - 330 PM	330 PM - 530 PM	6PM - 8PM	8PM - 9PM
16.12.2025	Registration	Tutorial 1 (Hardware Enhancements for Software Security) Chester Rebeiro, and Deepanjali S, IIT Madras		Tutorial 1 (Hardware Enhancements for Software Security) Chester Rebeiro, and Deepanjali S, IIT Madras		Tutorial 2 (Firmware Reverse engineering of IoT devices) Santosh Sam Koshy, CDAC		Tutorial 2 (Firmware Reverse engineering of IoT devices) Santosh Sam Koshy, CDAC		
17.12.2025	Campus Tour & Sports			Tutorial 3 (Rust Programming Language) Yashwanth Singh M, Bosch		Tutorial 3 (Rust Programming Language) Yashwanth Singh M, Bosch		ISEA Workshop on Quantum-Era Security Workshop Chair - Anupam Chattopadhyay	Networking Dinner	
18.12.2025	General Chairs' Introduction TPC Chairs' Introduction	Keynote: Sandeep Shukla IIIT Hyderabad Session Chair - Chandan Karfa		Session I: 4 Research Papers Session Chair - Chandan Karfa Paper ID: 15 - Analyzing Non-linear Shift Register Transformations in the Design and Cryptanalysis of Espresso - Anirban Ghatak, Anupam Chattopadhyay, Ambrish Awasthi and Indivar Gupta (ISI, Kolkata; SAG, DRDO, India; NTU, Singapore) Paper ID: 29 - A keystream generator inspired by the experiment of drawing balls with replacement** - Ganesh Yellapu (Bharat Electronics Limited, Bangalore, India) Paper ID: 82 - A new perspective on the decomposition in the Jacobian of small genus hyperelliptic curve - Deepak Bhati and Shashank Singh (CISPA Helmholtz; IISER Bhopal, India) Paper ID: 66 - A Custom Entropy Harvester for Consistent Entropy Supply to the /dev/random** - Kunal Abhishek and Anuyog Chauhan (CDAC, Patna, India)		Industry Demo Poster Session		Session II: 5 Research Papers Session Chair - Urbi Chatterjee Paper ID: 62 - High throughput 64-bit implementation of SNOW-V stream cipher** - Kakumani Kushalram, Majji Harsha Vardhan and Raghvendra Rohit (IIT Roorkee, India) Paper ID: 99 - A Multi-View Contrastive Graph Neural Network Framework for Binary Malware Detection in IoMT environments** - Bhagyasri Bora, Saunav Barman, Rahul Bardhan, Dharitri Brahma and Amitava Nag (Central Institute of Technology, Kokrajhar, India) Paper ID: 58 - Sample Similarity based Incremental Clustering: An Effective Methodology for Anomaly Detection in Networks - Arun K, Ardra V S and Aji S (University of Kerala, India) Paper ID: 37 - Breaking PCB-Chain: A Side Channel Assisted Attack on IoT-Friendly Blockchain Mining - Shubhankar Gambhir, Vishesh Mishra, Urbi Chatterjee and Debapriya Basu Roy (IIT Kanpur, India) Paper ID: 84 - Addressing Cache Side-Channel Attacks using Taint-guided Fine-grained Computation Offloading in Near-Memory Processing** - Simran Preet Kaur, Asutosh Kumar Sarma, Satanu Maity and Manojit Ghose (IIIT Guwahati, India)	Cultural Program & Prize distribution	Gala Dinner
19.12.2025	Registration	Keynote: Sikhar Patranabis IBM Session Chair - Debdeep Mukhopadhyay	Tea Break	Session III: 4 Research Papers Session Chair - Subhadeep Banik Paper ID: 107 - PAC-Guided Design Strategies for Resilient Priority Arbiter PUFs - Durba Chatterjee, Simranjeet Singh, Debdeep Mukhopadhyay, Farhad Merchant and Anupam Chattopadhyay (Radboud University, Netherlands; Forschungszentrum Jülich, Germany; IIT Kharagpur, India; University of Groningen, Netherlands; NTU, Singapore) Paper ID: 96 - Enhanced Hardware Trojan Detection with XGBoost Graph Learning: A Glass Box Approach - C Sneha and M Nirmala Devi (PES University, India) Paper ID: 38 - MLP is better than ResNet on ANSSI's Protected AES Implementation on ARM - Surya Prakash Mishra, Akash Gupta and Atul Prakash (SAG, DRDO, India; Ministry of Defense, India) Paper ID: 90 - Hard-to-Find Bugs in Public-Key Cryptographic Software: Classification and Test Methodologies - Matteo Steinbach, Johann Groszschaedl and Peter Roenne (University of Luxembourg, Luxembourg)	Lunch Break	Session IV: 4 Research Papers Session Chair - Chester Rebeiro Paper ID: 78 - Quantum Synthesis of Large S-Boxes: Heuristic and MILP-Based Transpiled-Depth Optimization - Tarun Yadav, Shweta Singh and Sudha Yadav (DRDO, India) Paper ID: 76 - Toward Crypto Agility: Automated Analysis of Quantum-Vulnerable TLS via Packet Inspection - Subeen Cho, Yulim Hyoung, Hagyeong Kim, Minjoo Sim, Anupam Chattopadhyay, Hwajeong Seo and Hyunji Kim (Hansung University, S. Korea; NTU, Singapore) Paper ID: 49 - Efficient Time Share Masking of AES - Subhadeep Banik and Francesco Regazzoni (University of Lugano, Switzerland; University of Amsterdam, Netherlands) Paper ID: 21 - Secure Secret Sharing Protocol Against Network Data Remanence Side Channel Attacks - Prajwal Thakare, Akash Om Trivedi and Urbi Chatterjee (IIT Kanpur, India)	Tea Break	Session V: 5 Research Papers Session Chair - Debapriya Basu Roy Paper ID: 70 - Investigation on the Impact of Practical Fault Model for Commercial Edge Machine Learning Devices - Shivam Bhasin, Dirmanto Jap, Marina Krček and Stjepan Picek (NTU, Singapore; Radboud University, Netherlands) Paper ID: 53 - A Security Analysis of CNN Partitioning Strategies for Distributed Inference at the Edge - Fatemeh Mehrafrooz, Roozbeh Siyadatzadeh, Nele Mentens and Todor Stefanov (Leiden University, Netherlands; KU Leuven, Belgium) Paper ID: 13 - GhostWriter: Exploiting GPU-Cache Contention to Steal and Steer Multi-Tenant Large-Language-Model Inference - Satyajit Das and Sreenath Vijayakumar (IIT Palakkad, India) Paper ID: 80 - Gradient-Guided Adversarial Patch Attack for Deep Neural Networks - Rishav Kumar, Umesh Kashyap and Sk. Subidh Ali (IIT Bhilai, India) Paper ID: 26 - VulScan-LT: A Lightweight Transformer-based Software Vulnerability Scanning Tool for Resource-Constrained Edge Devices - Dev Saini, Vivek Chaturvedi and Muhammad Shafique (IIT Palakkad, India; NYU Abu Dhabi, UAE)		
20.12.2025	Sight Seeing Tour									