IndoCrypt 2025 – Conference Schedule

December 14 – Tutorials

Time	Session	Details
10:15 AM – 11:15 PM	Tutorial 1	Title: From theory to practice: Inner c-differential cryptanalysis on modern block ciphers Speaker: Pantelimon Stanica (Professor and Manager of Secure Communication program, Applied Mathematics Department, Naval Postgraduate School, USA) **Session Chair: Prof. Bimal Kumar Roy**
11:15 AM – 11:30 AM	**High Tea**	
11:30 AM – 01:00 PM	Tutorial 2	Title: Generalising the NTRU Family: A Unified Perspective Speaker: Sugata Gangopadhyay (Professor, IIT Roorkee) **Session Chair: Pantelimon Stanica**
01:00 PM – 2:30 PM	**Lunch**	
02.30 PM – 5.00 PM	Tutorial 3	Title: Isogeny-based Cryptography Speaker: Luca De Feo (IBM Research Europe) **Session Chair: Prof. Sugata Gangopadhyay**

December 15 – Conference Day 1

Time	Session	Details
09:30 AM – 10:30 AM	**Inauguration**	
10:30 AM – 11:00 AM	**High Tea**	
11:00 AM – 12:00 PM	Invited Talk	Title: Every Contact Leaves a Trace: Microarchitecture Leakages in Modern Computing Systems

		Speaker: Debdeep Mukhopadhyay (Professor, IIT Kharagpur, India) **Session Chair: Prof. Ratna Dutta**
12:00 PM – 01:00 PM	Symmetric Cryptanalysis (2 papers)	1. Refined Linear Approximations for ARX Ciphers and Their Application to ChaCha. Yurie Okada (The University of Osaka), Atsuki Nagai (KDDI CORPORATION) and Atsuko Miyaji (The University of Osaka). 2. Improved Modeling for Substitution Boxes with Negative Samples and Beyond Debranjan Pal (Indian Institute of Technology Kanpur), Anubhab Baksi (Lund University, Sweden), Surajit Mandal (Indian Institute of Technology Madras) and Santanu Sarkar (Indian Institute of Technology Madras). **Session Chair: Prof. Sourav Mukhopadhyay**
01:00 PM – 02:00 PM	**Lunch Break**	
02:00 PM – 03:30 PM	Lattice-based Cryptography (3 papers)	1. Module Lattice based constant-size group signature with Verifier Local Revocation and Backward Unlinkability Komal Pursharthi (Maulana Azad National Institute of Technology, Bhopal) and Dheerendra Mishra (Maulana Azad National Institute of Technology, Bhopal) 2. Efficient Identity-Based Inner Product Functional Encryption from RLWE Anushree Belel (ROVIRA I VIRGILI UNIVERSITY) and Junji Shikata(YOKOHAMA NATIONAL UNIVERSITY) 3. COMPASS: A Compact PASS-lineage Accumulator with Succinct Proofs Tao-Hsiang Chang (National Chengchi University), Jen Chieh Hsu (NationalChengchi University), Hao-Yi Hsu (National Chengchi University), Raylin Tso(National Chengchi University) and Masahiro Mambo (Kanazawa University). **Session Chair: Prof. Sudhakar Sahoo**
03:30 PM – 04:30 PM	Zero-Knowledge and Interactive proofs (2 papers)	1. BOIL: Proof-Carrying Data from Accumulation of Correlated Holographic IOPs

		Maksim Nikolaev , Tohru Kohrita and Javier Silva. 2. Rejection-Free Framework of Zero-Knowledge Proof based on Hint-MLWE Antoine Douteau (Université Caen Normandie) and Adeline Roux-Langlois (Université Caen Normandie). **Session Chair: Deepak Kumar Dalai**
04:30 PM – 05:00 PM	**Tea**	
05:00 PM – 6:00 PM	Industry Talks (1)	Industry Side Story of Cryptology and Security with current global data security threat and vulnerability Speaker: Alok Tiwari (CEO & Co-Founder, AIVOT) **Session Chair: Prof. Susmita Ghosh**
06:00 PM – 07:00 PM	**AGM CRSI**	

December 16 – Conference Day 2

Time	Session	Details
09:30 AM – 10:30 AM	Invited Talk	Title: Taking Post-Quantum Cryptography from Theory to Practice: A Case Study with Signal Speaker: Shuichi Katsumata (Lead Cryptography Researcher, PQShield & AIST, Japan) **Session Chair: Dr. Indivar Gupta**
10:30 AM – 11:00 AM	**Tea**	
11.00 AM – 12.00 PM	Industry Talk (2)	Title: TBU Speaker: Nilesh Dande (CEO, Fortytwo Labs) **Session Chair: Dr. S.K.Pal**
12:00 PM – 01:00 PM	Isogeny-based Cryptography (2 papers)	1. Smooth twins for cryptographic applications from Pell equations Daniel Berger (DLR). 2.Hardened CTIDH: Dummy-Free and Deterministic CTIDH Gustavo Banegas (Inria and Laboratoire d'Informatique de l'Ecole polytechnique),

		Andreas Hellenbrand (RheinMain University of Applied Sciences Wiesbaden) and Matheus Saldanha (Universidade Federal de Santa Catarina). **Session Chair: Aditi Gangopadhyay**
01:00 PM – 02:00 PM	**Lunch Break**	
02:00 PM – 03:00 PM	Isogeny-based Cryptography (2 papers)	3. Key-Updatable Identity-Based Signature Schemes Tobias Guggemos (Ludwig-Maximilians-Universität Munich) and Farzin Renan (Middle East Technical University) 4. Beyond Sequential Walks: Parallelizing the GA-dlog Problem Sudeshna Karmakar (IIT Madras), Abul Kalam (IIT Madras) and Santanu Sarkar (IIT Madras). **Session Chair: Dr. Jayprakash Kar**
03:00 PM – 4:30 PM	Quantum Security (3 papers)	1. Practically Implementable Minimal Universal Gate Sets for Multi-Qudit Systems with Cryptographic Validation Anisha Dutta (Tata Steel Ltd.), Sayantan Chakraborty (Accenture), Chandan Goswami (Presidency University) and Avishek Adhikari (Presidency University). 2. One-Time Memories Secure against Depth-Bounded Quantum Circuits Kyosuke Sekii (University of Tsukuba) and Takashi Nishide (University of Tsukuba) 3. New Results in Quantum Analysis of LED: Featuring One and Two Oracle Attacks Siyi Wang (Nanyang Technological University), Kyungbae Jang (Hansung University), Anubhab Baksi (Nanyang Technological University), Sumanta Chakraborty (Techno International New Town), Anupam Chattopadhyay (Nanyang Technological University) and Hwajeong Seo (Hansung University). **Session Chair: Ravi Anand**
04:30 PM – 05:30 PM	Secret Sharing, Privacy & Distributed Trust (2 papers)	1.Traceable Bottom-Up Secret Sharing and Law & Order on Community Social Key Recovery Rittwik Hajra (Indian Statistical Institute, Kolkata, India), Subha Kar (Indian Statistical Institute, Kolkata), Pratyay Mukherjee (Supra Research) and Soumit Pal (Indian Statistical Institute, Kolkata).

		2. Beyond Confidentiality: Framing-Resistant Secure Vault Schemes Meghna Sengupta (University of Edinburgh **Session Chair: Shivam Bhasin**
05:30 PM – 06:00 PM	**Tea**	
06:00 PM	**Cultural and Banquet**	

December 17 – Conference Day 3

Time	**Session**	**Details**
09:30 – 10:30 AM	Invited Talk	Title: Cracking Secrets Beyond the Dataset: Revisiting Deep Learning in Side-Channel Analysis Speaker: Shivam Bhasin (Principal Research Scientist, Nanyang Technological University, Singapore) **Session Chair: TBD**
10:30 – 11:00 AM	**Tea**	
11:00 – 12:30 PM	Cryptographic Assumptions & Implementation (3 papers)	1.On the Classical Hardness of the Semidirect Discrete Logarithm Problem in Finite Groups Mohammad Ferry Husnil Arif (Universitas Indonesia) and Muhammad Imran (Universitas Indonesia). 2. Multivariate Encryptions with LL' perturbations - Is it possible to repair HFE in encryption? Pierre Varjabedian (THALES DIS, Université de Versailles Saint-Quentin en Yvelines) and Jacques Patarin (THALES DIS, Université de Versailles Saint-Quentin en Yvelines) 3. High-Performance FPGA Implementation of a Recursive Modular Karatsuba Multiplier over GF(2^m) Ruby Kumari (CEERI, Pilani, India), Sumeet Saurav (CEERI, Pilani, India) and Abhijit Karmakar (CEERI, Pilani, India). **Session Chair: Dr. Ch. A. S. Murty**
12:30 PM – 01:00 PM	**Valedictory**	

01:00 PM – 02:00 PM	**Lunch Break**
02:00 PM onwards	**Excursion**

Each talk is 25 minutes followed by 5 minutes Q&A session.