2nd International Conference on Security & Privacy
(ICSP 2021)

www.icsp.co.in

November 16-17, 2021
Organized by
Department of Mathematics, National Institute of Technology Jamshedpur, India

Meeting through **Google Meet**
Join on your computer or mobile app
Link: https://meet.google.com/jgy-eymu-jpi

SCHEDULE

NOTE: The mentioned time is in Indian Standard Time (IST) format i.e., (UTC+05:30).

DAY1 (November 16, 2021)	
8:00-8:45	**Inaugural**
Keynote Talks	
8:50-9:45	**Speaker: Pantelimon Stanica,** Naval Postgraduate School, USA. **Title:** Cryptographic Boolean functions and multiplicative differentials
9.55-10.50	**Speaker: Mridul Nandi,** Indian Statistical Institute, Kolkata, India. **Title:** Sponge based Authenticated Cipher
11.00-11.55	**Speaker: Elette Boyle**, Director FACT Research Center and head of RRIS International Program, Efi Arazi School of Computer Science IDC Herzliya, Israel **Title:** Zero-Knowledge Proofs on Distributed Data and Applications to Secure Computation
Paper Presentations	
12:00-13.00	**Title:** A Method of Integer Factorization **Authors:** Zhizhong Pan and Xiao Li
	Title: Secure Multi-Party Computation Using Pre-distributed Information from an Initializer **Authors:** Amirreza Hamidi and Hossein Ghodosi
	Title: Evolving Secret Sharing in Almost Semi-honest Model **Authors:** Jyotirmoy Pramanik and Avishek Adhikari
13.00-13.55	Break
14.00-14.55 (To be confirmed)	**Speaker: Ronald Cramer,** Head of the Cryptology Group, CWI, Mathematical Institute, Leiden University, The Netherlands. **Title:** To be updated
Paper Presentations	
15:00-17.20	**Title:** First-Order Side-Channel Leakage Analysis of Masked but Asynchronous AES **Authors:** Antoine Bouvet, Sylvain Guilley, and Lukas Vlasak
	Title: Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure **Authors:** Meziane Hamoudi, Amina Bel Korchi, Sylvain Guilley, Sofiane Takarabt, Khaled Karray, and Youssef Souissi
	Title: A Suitable Proposal of S-Boxes (Inverse-Like) for the AES, Their Analysis and Performances **Authors:** Said Eddahmani and Sihem Mesnager

2nd International Conference on Security & Privacy
(ICSP 2021)

www.icsp.co.in

November 16-17, 2021
Organized by
Department of Mathematics, National Institute of Technology Jamshedpur, India

Meeting through **Google Meet**
Join on your computer or mobile app
Link: https://meet.google.com/jgy-eymu-jpi

15:00-17.20	**Title:** Towards a Black-Box Security Evaluation Framework **Authors:** Mosabbah Mushir Ahmed, Youssef Souissi, Oualid Trabelsi, Sylvain Guilley, Antoine Bouvet, and Sofiane Takarabt
	Title: Multi-source Fault Injection Detection Using Machine Learning and Sensor Fusion **Authors:** Ritu-Ranjan Shrivastwa, Sylvain Guilley, and Jean-Luc Danger
	Title: Traceable and Verifier-Local Revocable Attribute-Based Signature with Constant Length **Authors:** Syed Taqi Ali
Keynote Talks	
17.30-18.25	**Speaker: Delaram Kahrobaei**, University Dean for Research, City University of New York, CUNY Central, USA. **Title:** Mathematics of Cryptography in the Quantum Era

DAY 2 (November 17, 2021)	
Keynote Talks	
9:00-9:55	**Speaker: Craig Costello**, Microsoft Research, USA. **Title:** The Case for SIKE – a Decade of the Supersingular Isogeny Problem
10.00-10.55	**Speaker: Carmit Hazay**, Bar-IlanUniversity,Israel. **Title:** ZK-PCPs from Leakage-Resilient Secret Sharing
Paper Presentations	
11.00-11.20	**Title:** Higher Order c-Differentials **Authors:** Aaron Geary, Marco Calderini, Constanza Riera, and Pantelimon Stănică
11:30-12:00	**Valedictory**