



*13th International Conference on Security,  
Privacy, and Applied Cryptographic  
Engineering 2023*

# SPACE 2023



**IIT Roorkee,  
Uttarakhand, India**



**14-17 December 2023**



**Springer**

**Lecture Notes in  
Computer Science**

LNCS

LNAI

LNBI



<https://iitr.ac.in/space2023/>



# Organising committee

**Chief Patron**  
**Prof. Kamal Kishore Pant**  
Director of IIT Roorkee

**Organising chair**  
Dr. Manoj Mishra  
IIT Roorkee, CSE dept

## Members

**Dr. R. Balasubramanian**  
*IIT Roorkee, CSE dept*

**Dr. Rahul Thakur**  
*IIT Roorkee, CSE dept*

**Dr. Durga Toshniwal**  
*IIT Roorkee, CSE dept*

**Dr. Sugata Gangopadhyay**  
*IIT Roorkee, CSE dept*

**Dr. Neetesh Kumar**  
*IIT Roorkee, CSE dept*

**Dr. Debiprasanna Sahoo**  
*IIT Roorkee, CSE dept*

**Dr. Aditi Gangopadhyay**  
*IIT Roorkee, Mathematics dept*

**Dr. Rajdeep Niyogi**  
*IIT Roorkee, CSE dept*

**Dr. Raksha Sharma**  
*IIT Roorkee, CSE dept*

**Dr. Sandeep Kumar Garg**  
*IIT Roorkee, CSE dept*

**Dr. Pradumn K. Pandey**  
*IIT Roorkee, CSE dept*

**Dr. Pravendra Singh**  
*IIT Roorkee, CSE dept*

**Dr. Shahbaz Khan**  
*IIT Roorkee, CSE dept*

**Dr. Partha Pratim Roy**  
*IIT Roorkee, CSE dept*

**Dr. Dharmendra Singh**  
*IIT Roorkee, CSE dept*

**Dr. Peddoju Sateesh Kumar**  
*IIT Roorkee, CSE dept*

**Dr. Sudip Roy**  
*IIT Roorkee, CSE dept*

**Dr. Jitin Singla**  
*IIT Roorkee, CSE dept*



# Program committee

## Program chairs

**Dr. Francesco Regazzoni**

*University of Amsterdam,  
(Amsterdam, The Netherlands)  
and Università della Svizzera  
Italiana (Lugano, Switzerland)*

**Dr. Sri Parameswaran**

*School of Computer Science and  
Engineering at the University of  
New South Wales*

**Dr. Bodhisatwa Mazumdar**

*Computer Science and  
Engineering. Indian Institute of  
Technology Indore*

## General chairs

**Dr. Debdeep Mukhopadhyay**

*Indian Institute of Technology  
Kharagpur, India*

**Dr. Sugata Gangopadhyay**

*Indian Institute of Technology  
Roorkee, India*

## program committee

**Dr. Sugata Gangopadhyay**

*IIT Roorkee, India*

**Dr. Subhadeep Banik**

*University of Lugano, Switzerland*

**Dr. Silvia Mella**

*Radboud University*

**Dr. Marc Stöttinger**

*RheinMain University of Applied  
Science*

**Dr. Nusa Zidaric**

*Leiden University*

**Dr. Dhiman Saha**

*de.ci.phe.red Labs, Indian Institute  
of Technology Bhilai, India*

**Dr. Ruben Niederhagen**

*Academia Sinica, Taiwan, and  
University of Southern Denmark*

**Dr. Diego F. Aranha**

*Aarhus University*

**Dr. Maël Gay**

*University of Stuttgart*

**Dr. Lukasz Chmielewski**

*Masaryk University*

**Dr. Francesco Regazzoni**

*ALaRI - USI (Switzerland)*

**Dr. Marine Minier**

*CITI INSA-Lyon - ARES INRIA  
Project*



# Program committee

**Dr. Jakub Breier**

*Silicon Austria Labs*

**Dr. N. Nalla Anandakumar**

*Continental Automotive,  
Singapore*

**Dr. Kostas Papagiannopoulos**

*Radboud University*

**Dr. Claude Carlet**

*University of Paris 8*

**Dr. Kerstin Lemke-Rust**

*Bonn-Rhein-Sieg University of  
Applied Sciences*

**Dr. Kazuo Sakiyama**

*The University of Electro-  
Communications*

**Dr. Dirmanto Jap**

*Nanyang Technological  
University*

**Dr. Anupam Chattopadhyay**

*Nanyang Technological  
University*

**Dr. Bohan Yang**

*Tsinghua University*

**Dr. Guilherme Perin**

*TU Delft*

**Dr. Debdeep Mukhopadhyay**

*IIT Kharagpur, India*

**Dr. Rajat Subhra Chakraborty**

*IIT Kharagpur, India*

**Dr. Debapriya Basu Roy**

*IIT Kanpur*

**Dr. Sikhar Patranabis**

*IBM Research India*

**Dr. Somitra Sanadhya**

*IIT Jodhpur*

**Dr. Urbi Chatterjee**

*IIT Kanpur*

**Dr. Vishal Saraswat**

*Bosch Global Software  
Technologies*

**Dr. Md Masoom Rabbani**

*KU Leuven*



# Program committee

**Dr. Amr Youssef**

*Concordia University*

**Dr. Sujoy Sinha Roy**

*IIT Kharagpur*

**Dr. Peter Schwabe**

*Radboud University*

**Dr. Bodhisatwa Mazumdar**

*New York University*

**Dr. Reihaneh Safavi-Naini**

*University of Calgary*

**Dr. Subidh Ali**

*Indian Institute of Technology  
Bhilai*

**Dr. Chester Rebeiro**

*Indian Institute of Technology,  
Madras*

**Dr. Utsav Banerjee**

*Indian Institute of Science*

**Dr. Jayaprakash Kar**

*The LNM Institute of  
Information Technology, Jaipur  
(Raj)*

**Dr. Mainack Mondal**

*Indian Institute of Technology,  
Kharagpur*

**Dr. Ulrich Rührmair**

*Ruhr University Bochum*

## **Steering committee**

**Dr. Debdeep Mukhopadhyay**

*Indian Institute of Technology, Kharagpur*

**Dr. Chester Rebeiro**

*Indian Institute of Technology, Madras*

**Dr. Veezinathan Kamakoti**

*Indian Institute of Technology, Madras*

**Dr. Ulrich Rührmair**

*Ludwig Maximilian University of Munich,  
Germany*

# OUR SPEAKERS



**Dr. Elena Dubrova**

*Professor, Department of Electronics  
School of Information and Communication Technology  
Royal Institute of Technology (KTH)  
Stockholm, Sweden.*



**Dr. Debdeep Mukhopadhyay**

*Professor, Department of Computer  
Science and Engineering of the Indian  
Institute of Technology Kharagpur, India.*



**Dr. Arpita Parta**

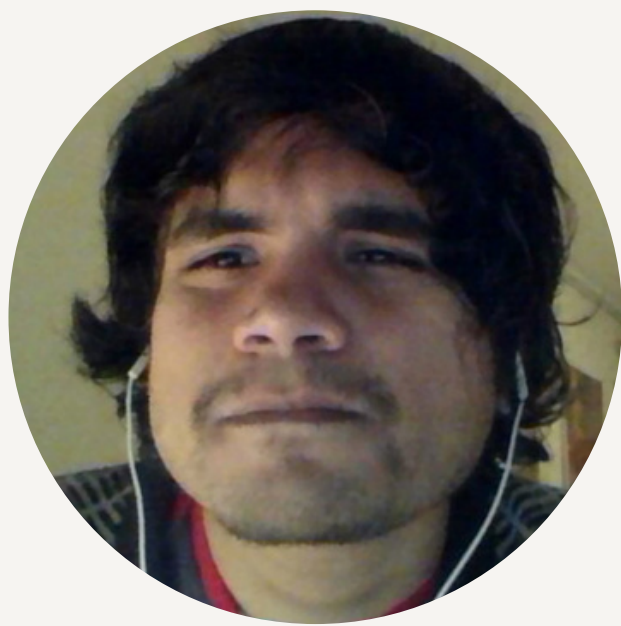
*Associate Professor at Dept. of Computer Science  
& Automation (CSA), EECS Division, Indian  
Institute of Science Bangalore, India.*



**Dr. Benedikt Gierlich**

*Research Expert, COSIC  
Department of Electrical Engineering  
Katholieke Universiteit Leuven  
Belgium.*

# OUR SPEAKERS



**DR. SUBHADEEP BANIK**

*Senior Scientist  
Swiss Federal Institute of Technology  
Lausanne, Switzerland.*



**Dr. Mainack Mondal**

*Assistant Professor, Department of  
Computer Science and Engineering of the  
Indian Institute of Technology  
Kharagpur, India.*

# Program Schedule

## SPACE 2023

**Day 1**

**December 14, 2023**

**9:00 to 18:30 hrs**

09:00 - 09:30 hrs

Welcome note

09:30-11:00 hrs

Tutorial 1: Dr. Mainack Mondal, IIT Kharagpur

11:00-11:30 hrs

Tea Break

11:30-13:00 hrs

Tutorial 1 (Continued): Dr. Mainack Mondal,  
IIT Kharagpur

13:00-14:30 hrs

Lunch

14:30-16:00 hrs

Tutorial 2: Dr. Subhadeep Banik, Swiss Federal  
Institute of Technology in Lausanne

16:00-16:30 hrs

Tea Break

16:30 - 18 hrs

Tutorial 2 (Continued): Dr. Subhadeep Banik,  
Swiss Federal Institute of Technology in Lausanne

18:00 -18:30 hrs

High Tea

# Program Schedule

SPACE 2023

**Day 2**

**December 15, 2023**

**9:00 to 18:30 hrs**

09:00- 10:00 hrs      Conference Opening Session

10:00-11:00 hrs      Keynote Talk 1: Prof. Elena Dubrova, Royal Institute of Technology (KTH), Stockholm, Sweden

11:00-11:30 hrs      Tea Break

11:30-13:00 hrs      Paper Session 1: Symmetric and Public Key Cryptography

13:00-14:00 hrs      Lunch Break

14:00-15:00 hrs      Keynote Talk 2: Dr. Arpita Parta, IISC Bangalore.

15:00-16:00 hrs      Paper Session 2: Network Security

16:00 - 16:30 hrs      Tea Break

16:30 -18:00 hrs      Paper Session 3: Hardware Security and Physical Attacks

118:00 -18:30 hrs      High Tea

# Program Schedule

SPACE 2023

**Day 3**

**December 16, 2023**

**9:00 to 18:30 hrs**

09:00- 10:00 hrs

Paper Session 4: Symmetric Key Cryptography

10:00-11:00 hrs

Keynote Talk 3: Dr. Benedikt Gierlichs, KU Leuven

11:00-11:30 hrs

Tea Break

11:30-13:00 hrs

Paper Session 5: Public Key Cryptography and Post Quantum Cryptography

13:00-14:00 hrs

Lunch Break

14:00-15:00 hrs

Keynote Talk 4: TBD

15:00-16:00 hrs

Paper Session 6: Security and Privacy

16:00 - 16:30 hrs

Tea Break

16:30 -17:00 hrs

Poster Session

17:00-18:00 hrs

Paper Session 7: Side-Channel Analysis, Adversarial ML

18:00-18:30 hrs

High tea

19:00 hrs onwards

Banquet Dinner

# Program Schedule

## SPACE 2023

**Day 4**

**December 17, 2023**

**9:30 to 18:30 hrs**

09:30 -11:00 hrs	Post Quantum Cryptography (PQC) Workshop from KU Leuven (Dr. Benedikt Gierlichs and team) and IIT Kharagpur (Prof. Debdeep Mukhopadhyay and team)
11:00-11:30 hrs	Tea Break
11:30-13:00 hrs	PQC Workshop (Continued)
13:00-14:00 hrs	Lunch Break
14:00-15:30 hrs	PQC Workshop (Continued)
15:30-16:00 hrs	Tea Break
16:00-17:30 hrs	PQC Workshop (Continued)
17:30-18:00 hrs	Concluding session
18:00 -18:30 hrs	High Tea