

Program Committee

- **Diego Aranha**, University of Campinas, Brazil & Aarhus University Denmark
- **Shi Bai**, Florida Atlantic University, USA
- **Subhadeep Banik**, EPFL, Switzerland
- **Lejla Batina**, Radboud University, The Netherlands
- **Rishiraj Bhattacharyya**, NISER, India
- **Christina Boura**, University of Versailles and Inria, France
- **Debrup Chakraborty**, ISI, Kolkata, (Co-chair), India
- **Sanjit Chatterjee**, IISc, Bangalore, India
- **Geoffroy Couteau**, Karlsruhe Institute of Technology
- **Pooya Farshim**, CNRS and ENS, France
- **Shay Gueron**, University of Haifa, Israel
- **Divya Gupta**, Microsoft Research India
- **Indivar Gupta**, SAG-DRDO, Delhi, India
- **Gottfried Herold**, Ruhr University Bochum, Germany
- **Viet Tung Hoang**, Florida State University, USA
- **Takanorilsoe**, University of Hyogo, Japan
- **Tetsu Iwata**, Nagoya University, Japan (Co-chair)
- **Elena Kirshanova**, ENS Lyon, France
- **Shanta Laishram**, ISI, Delhi, India
- **Patrick Longa**, Microsoft Research Redmond, USA
- **Atul Luykx**, Visa Research, USA
- **Subhamoy Maitra**, ISI, Kolkata, India
- **Hemanta K. Maji**, Purdue University, USA
- **Bart Mennink**, Radboud University, The Netherlands
- **Kazuhiko Minematsu**, NEC Corporation, Japan
- **Debdeep Mukhopadhyay**, IIT, Kharagpur, India
- **Mridul Nandi**, ISI, Kolkata, India
- **Khoa Nguyen**, NTU, Singapore
- **Ryo Nishimaki**, NTT, Japan
- **Raphael Phan**, Multimedia University, Malaysia
- **Manoj Prabhakar**, IIT, Bombay, India
- **Somindu C. Ramanna**, IIT, Kharagpur, India
- **Francisco Rodriguez-Henriquez**, CINVESTAV-IPN, Mexico
- **Adeline Roux-Langlois**, Univ Rennes, CNRS, IRISA, France
- **Jacob Schuldt**, AIST, Japan
- **Peter Schwabe**, Radboud University, The Netherlands
- **Francois-Xavier Standaert**, UCL, Belgium
- **Siwei Sun**, Chinese Academy of Sciences, China
- **Atsushi Takayasu**, University of Tokyo, Japan
- **Srinivas Vivek**, IIIT, Bangalore, India
- **Shota Yamada**, AIST, Japan
- **Kazuki Yoneyama**, Ibaraki University, Japan
- **Yu Yu**, Shanghai Jiao Tong University, China
- **Vassilis Zikas**, University of Edinburgh, UK

Invited Speakers

- **Takahiro Matsuda**, National Institute of Advanced Industrial Science and Technology (AIST), Japan
- **Gilles Van Assche**, STMicroelectronics, Diegem, Belgium
- **Mridul Nandi**, Indian Statistical Institute, Kolkata, India

CALL FOR PAPERS

Important Dates

- Submission deadline: 30 August, 2018; 11:59 AM, GMT
- Notification to authors: 12 October, 2018
- Final versions of accepted papers: 22 October, 2018
- Tutorials: 9 December, 2018
- Conference: 10-12 December, 2018

For details Visit <https://www.isical.ac.in/~indocrypt/>

Contact Persons

Prof. Shri Kant

Organizing Chair
Research & Technology Development Centre
Sharda University, 32, 34 Knowledge Park-III
Greater Noida-201306, India

Phone: +91-8368753003, +91-9868251170

Email: indocrypt-2018@sharda.ac.in

Dr. Indivar Gupta

Organizing Co-Chair
Scientific Analysis Group, DRDO,
Ministry of Defence,
Metcalfe House, Delhi-110054

Phone: +91-11-23812651, +91-9868247233

Email: indivar_gupta@yahoo.com

View of the ultra-modern Sharda University
campus spread over 63 acres.



INDOCRYPT 2018

December 9 - 12, 2018

19TH INTERNATIONAL CONFERENCE
ON **CRYPTOLOGY** IN INDIA

Jointly organised by

Scientific Analysis
Group, DRDO



UNDER THE AEGIS
OF **CRSI & IACR**

Cryptography
Research
Society of India



International
Association for
Cryptography Research



Venue India Habitat Centre, New Delhi, India

UNLOCK NEW AVENUES IN CRYPTOLOGY



AIM OF THE CONFERENCE

In the digital age, management and security of the information in the cyber space is quite critical. The multifarious dimension of cryptology plays an important role in dissemination of information securely. Through the 19th edition of INDOCRYPT, well known cryptologists of the globe will come together on the same platform to discuss the advances in the current cryptographic technology and will deliberate on current and post quantum cryptographic scenarios.

ABOUT CRYPTOLOGICAL RESEARCH SOCIETY OF INDIA

Set up in 2001, Cryptology Research Society of India is a scientific assembly made up of academicians, researchers, specialists, students and institutions who are interested in promoting the science and technology of Cryptology and Data Security and related theory and applications in India. The CRSI has been founded for:

- Supporting and promoting research activities in cryptology and information security in India.
- To arrange lectures, discussions, workshops, seminars, conferences etc. for motivating and guiding young Indian researchers in the field of cryptology.
- Organizing the annual events INDOCRYPT, National Instructional Workshop (NIWC) and the National Workshop on Cryptology.

ABOUT SCIENTIFIC ANALYSIS GROUP, DRDO

Scientific Analysis Group (SAG) is one of the premier labs of DRDO and was established in 1963 for carrying out R&D activities in the area of design, development and analysis of communication systems. It is a self-accounting unit of DRDO and a member of the cluster of computational system of DRDO. SAG has been undertaking different projects apart from carrying out the research and development activities in the field of cryptology and information security. Presently SAG is located at Metcalfe House complex, M.G. Road, Delhi with more than hundred scientists and supporting staff.

ABOUT SHARDA UNIVERSITY

Sharda University is a venture of the renowned SGI group and has been established in 2009 in Greater Noida, Delhi-NCR. The University's goal is to nurture brilliant brains who will go on to become leaders in their chosen field. The University established the Research and Technology Development Centre (RTDC), in 2009 with the sole aim of offering cutting-edge research facilities on-campus. It is awarded as the **Best Private University In India by National Education Excellence Awards 2018.**

RTDC is an ISO certified centre (ISO 9001: 2008 & ISO 9001: 2001 and ISO 9000:2015). It is equipped with state-of-the-art facilities for working in multi-disciplinary areas with the collaboration of various institutions/industries of repute. It also looks after the Ph.D. program of the University and plays an important role in ensuring quality research.

REGISTRATION FEE

Designation	Foreign Participants		Indian participants	
	On or Before Oct. 30, 2018	After Oct. 30, 2018	On or Before Oct. 30, 2018	After Oct. 30, 2018
Academia/ R & D Org.	US\$ 700	US\$ 750	INR 8,000	INR 9,000
Students	US\$ 450	US\$ 500	INR 3,000	INR 3,500
Industry	US\$ 850	US\$ 900	INR 10,000	INR 11,000

TUTORIAL FEE

Foreign Participants	Indian participants
US\$ 50	INR 2,000

- Payment may be done through wire transfer or demand draft in favour of INDOCRYPT 2018, Payable at Allahabad Bank, Greater Noida, Gautam Budh Nagar.
- In case of Cheque, Foreign participants are to pay additional 15\$.
- Members of CRSI are offered 25% discount in the registration fees for the conference.
- Those who are registering for conference are exempted from tutorial fee.

Wire Transfer Details

Account Name: INDOCRYPT 2018 | **Account No:** 50440591180

Branch: Greater Noida, Gautam Budh Nagar | **IFSC Code:** ALLA0213270

MICR Code: 110010150 | **Swift Code:** ALLAINBBRPN

Accommodation & Transport

Zahid Ali
Tel.: 011-43663600, Mob: 9654013065
broadway@oldworldhospitality.com

Prateek Parashar
Tel: 011-47165500
prateek.parashar@indebo.com

Accommodation:
(Student Delegates)

Email: indocrypt-2018@sharda.ac.in

Accommodation:
(Official Delegates)

Email: indivar_gupta@yahoo.com

Chief Patron

Mr. G. Athithan, DS&DG
(MED, Cos & CS), DRDO

Mr. P. K. Gupta, Chancellor
Sharda University

Co-Patron

Mr. Y. K. Gupta, Pro-Chancellor
Sharda University

Mr. Prashant Gupta
Executive Director, Sharda University

General Chairs

Anu Khosla, Director, Scientific
Analysis Group, DRDO, Delhi

Brishbhan Singh Panwar
Dean Academics, Sharda University

Program Chairs

Debrup Chakraborty,
ISI, Kolkata, India

Testu Iwata
Nagoya University, Nagoya, Japan

Organizing Chair

Shri Kant, RTDC, SU, (Chair)

Indivar Gupta, SAG, DRDO, (Co-Chair)

Organizing Committee

Dhananjay Dey, SAG, DRDO

Bhartendu Nandan, SAG, DRDO

Girish Mishra, SAG, DRDO

Manoj Kumar, SAG, DRDO

Ajit Kumar, Jt. Reg., SU

A. K. Sahoo, SET, SU

Rajiv Kumar, SET, SU

Sandeep Singh, SET, SU

Diwakar Gautam, SET, SU

P. K. Singh, SBSR, SU

Vinay Verma, SBSR, SU

K. K. Pande, SBSR, SU

Suman, SBSR, SU

Prem Shankar Jha, SBSR, SU

Shruti Singh, SBSR, SU

Kumar Gautam Anand, SOLC, SU

Amit Kumar Shrivastav, DDM, SU

Sandeep Teotia, DDM, SU

Priya Verma, DDM, SU

Vineet Ruhela, DDM, SU

Organizing Secretary

Rajesh Kumar, SBSR, SU
(Organizing Secretary)

Khursheed Alam, SBSR, SU
(Treasurer)

Advisory Board

Ajay Prakash Sawhney, Secretary
MeitY, New Delhi

R. Balasubramanian, IMSc., Chennai

Bimal Kumar Roy, ISI, Kolkata

C. E. Veni Madhavan, IISc, Bangalore

Pandu Rangan Chandrasekaran, IIT
Chennai

G. R. C. Reddy, Vice Chancellor, SU

R. P. Agarwal, Chief Advisor, SU

Vijay Gupta, Prof. Emeritus, SU

Neelam Verma, SAG-DRDO, Delhi

Pratibha Yadav, SAG-DRDO, Delhi

N. Rajesh Pillai, SAG-DRDO, Delhi

R. M. Mehra, Prof. Emeritus, SU

N. B. Singh, Prof. Emeritus, SU

A. H. Siddiqi, Prof. Emeritus, SU

Surya Prakash Rao, Dean Res., SU

R. C. Singh, COE, SU

H.S. Gaur, Dean, SBSR, SU

Parma Nand, Dean, SET, SU

DL N Shastri, Director, Corp Affair, SU

Vikram Singh, Director (T&P), SU

Student Organizing Committee

Ramesh Kumar, SBSR, SU

Atar Singh, SBSR, SU

Himanshu Chaudhary, SBSR, SU

Suryya Adobala, SET, SU

Ezéchiél Kituta Katembo, SET, SU

Rachna Kumari, SBSR, SU

Monika Srivastava, SBSR, SU

Karan Surana, SBSR, SU

Pawan Dhapola, SBSR, SU

Sai Kiran Dommeti, SBSR, SU

Martin Thomson Pazhoom, SBSR, SU