In cooperation with

Call For Papers

Indocrypt 2016

Kolkata, December 11–14, 2016

http://indocrypt2016.iiitd.edu.in/

Proceedings in

Since its introduction in 2000, Indocrypt has been widely acknowledged as the leading Indian venue for cryptography. Additionally, Indocrypt is well known and established around the cryptographic world, attracting cryptographers from all around the world. This year, the conference returns once again to Kolkata (where it was founded).

Original papers on all technical aspects of cryptology are solicited for submission. This includes works on foundational, practical, and industry-related aspects with contributions in various areas including security models, cryptographic primitives, cryptographic protocols, cryptanalysis, hardware and software implementation aspects, and applications. Submissions focusing on cryptographic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing are welcome.

Important dates

Submission deadline:	July 25, 2016 (15:30 GMT/23:00 IST)
Notification of decision:	September 12, 2016
Proceedings version deadline:	October 3, 2016
Conference:	December 11–14, 2016

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published/submitted in a journal or a conference/workshop with proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. The Indocrypt 2016 Chairs reserve the right to share information about submissions with other program committees or journal editors to detect parallel submissions. In addition, the Indocrypt Chairs reserve the right to contact an author's institution/corporation and/or other appropriate organizations if an irregular submission is detected.

Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The length of the submission should be at most 16 pages excluding bibliography and appendices using Springer's LNCS package (see instructions at `http://www.springer.de/comp/lncs/authors.html`), with no changes to the style (i.e., single column with at least 11pt size font with reasonably sized margins). Any number of clearly marked appendices may be supplied following the main body of the paper. However, the committee members are not required to read appendices; the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits. Submitted papers must be in PDF format and should be submitted electronically. A detailed description of the electronic submission procedure is available via `https://indocrypt2016.cs.haifa.ac.il/`.

The proceedings will be published in Springer's Lecture Notes in Computer Science series, and will be available at the conference.

Authors of accepted papers must guarantee that their paper will be presented at the conference.

Program Committee

Diego Aranha	University of Campinas, Brazil
Jean-Philippe Aumasson	Kudelski Security, Switzerland
Steve Babbage	Vodafone Group plc, UK
Rishiraj Bhattacharyya	ISI Kolkata, India
Begül Bilgin	KU Leuven, Belgium
Céline Blondeau	Aalto University, Finland
Andrey Bogdanov	Technical University of Denmark, Denmark
Itai Dinur	Ben-Gurion University of the Negev, Israel
Orr Dunkelman **(chair)**	University of Haifa, Israel
Helena Handschuh	Crytography Research, USA and KU Leuven, Belgium
Carmit Hazay	Bar-Ilan University, Israel
Takanori Isobe	Sony Corporation, Japan
Nathan Keller	Bar-Ilan University, Israel
Tanja Lange	Technische Universiteit Eindhoven, Netherlands
Gaëtan Leurent	INRIA, France
Atefeh Mashatan	Canadian Imperial Bank of Commerce, Canada
Florian Mendel	Graz University of Technology, Austria
Katerina Mitrokotsa	Chalmers University of Technology, Sweden
Amir Moradi	Ruhr-Universität Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
David Naccache	ENS, France
Michael Naehrig	Microsoft Research, USA
Elisabeth Oswald	University of Bristol, UK
Arpita Patra	Indian Institute of Science, Bangalore
Thomas Peyrin	Nanyang Technological University, Singapore
Axel Poschmann	NXP Semiconductors, Germany
Vanishree Rao	PARC, USA
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Bimal Roy	ISI Kolkata, India
Somitra Sanadhya **(chair)**	IIIT Delhi, India
Santanu Sarkar	IIT Madras, India
Jean-Pierre Seifert	Technische Universität Berlin, Germany
Sourav Sen Gupta	ISI Kolkata, India
François-Xavier Standaert	UCL, Belgium
Muthuramakrishnan Venkitasubramaniam	University of Rochester, USA
Xiaoyun Wang	Tsinghua University, China

Contact Information

General Chair: Bimal Roy (bimal@isical.ac.in)
Program Chairs: Orr Dunkelman, Somitra Sanadhya (indocrypt2016@gmail.com)