INDOCRYPT 2012 is the 13th International Conference on Cryptology in India.

The conference will take place during 9-12 December 2012 at Indian Statistical Institute, Kolkata. Indocrypt 2012 is part of the Indocrypt series organized under the aegis of the Cryptology Research Society of India.

General chair:
Bimal K. Roy, Indian Statistical Institute

Program chairs:
Steven Galbraith, Univ. of Auckland, New Zealand
Mridul Nandi, Indian Statistical Institute, Kolkata

Submission deadline: 23 July 2012
Notification to authors: 3 September 2012
Final version of accepted papers: 17 September 2012

Tutorials: 9 December 2012
Conference: 10-12 December 2012

Call for Papers

Original papers on all technical aspects of cryptology are solicited for submission. The conference seeks original contributions in cryptology. We welcome submissions about new cryptographic primitive proposals, cryptanalysis, security models, hardware and software implementation aspects, cryptographic protocols, and applications. We also consider submissions about cryptographic aspects of network security, complexity theory, information theory, coding theory, number theory, and quantum computing.

Papers must be submitted electronically at the conference server (will be posted on the website). No new submissions will be accepted after 23 July 2012, but it is still possible to modify the submissions until 27th July 2012. Authors of accepted papers must guarantee that their paper will be presented at the conference. The accepted papers will be published by Springer-Verlag in a Lecture Notes in Computer Science volume.

Program Committee

Daniel Bernstein, Univ. of Illinois at Chicago, USA
Sanjit Chatterjee, Indian Institute of Science, India
Chen-Mou Cheng, National Taiwan Univ., Taiwan
Joan Daemen, STMicroelectronics
Philippe Gaborit, Universite de Limoges, France
Steven Galbraith, Univ. of Auckland, New Zealand
Vipul Goyal, Microsoft Research India, India
Shay Gueron, University of Haifa, Israel
Goichiro Hanaoka, National Institute of AIST, Japan
Tetsu Iwata, University of Nagoya, Japan
Tanja Lange, TU Eindhoven, The Netherlands
Kristin Lauter, Microsoft, USA
Keith Martin, Royal Holloway, Univ. of London, UK
Willi Meier, FHNW Switzerland
David Naccache, ENS Paris, France
Mridul Nandi, Indian Statistical Institute, Kolkata
Jesper Buus Nielsen, Aarhus University, Denmark
Elisabeth Oswald, University of Bristol, UK
Carles Padro, NTU, Singapore
Arpita Patra, ETH Zurich, Switzerland
Goutam Paul, Jadavpur University, India
Manoj M. Prabhakaran, UIUC, USA
Bart Preneel, KU Leuven, Belgium
C. Pandu Rangan, Indian Statistical Inst., Chennai
Christian Rechberger, DTU, Denmark
Phillip Rogaway, Univ. of California, Davis, USA
Dipanwita Roy Chowdhury, IIT Kharagpur, India
Palash Sarkar, Indian Statistical Institute, Kolkata
Nicolas Sendrier, INRIA Rocquencourt, France
Damien Stehle, ENS de Lyon, France
Dominique Unruh, University of Tartu, Estonia
Fre Vercauteren, KU Leuven, Belgium

Email ID: indocrypt2012@gmail.com
Website: http://www.isical.ac.in/~indocrypt/ or http://www.math.auckland.ac.nz/~sgal018/indocrypt2012/