**10 - 13 December 2017, Chennai, India**
http://events.csa.iisc.ernet.in/indocrypt2017/

Since its introduction in 2000, Indocrypt has been widely acknowledged as the leading venue for cryptography in India. Indocrypt is well known and established around the cryptographic world, attracting a broad international audience, as well as hosting prestigious invited speakers. This year, the conference returns once again to Chennai. 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.**

| | |
|---|---|
| Paper Submission Deadline | ~~Aug 20~~ **Aug 27** (12.00 GMT) |
| Notification of Acceptance | **Oct 5** |
| Final Manuscripts Due | **Oct 15** |

**Program Committee**

| | |
|---|---|
| Adeline Roux-Langlois, | CNRS/IRISA, France |
| Aggelos Kiayias, | University of Edinburgh, UK |
| Alessandra Scafuro, | North Carolina State University, USA |
| Andrey Bogdanov, | Technical University of Denmark, Denmark |
| Anja Lehmann, | IBM Research - Zurich, Switzerland |
| Arpita Patra, **(Co-chair)** | Indian Institute of Science, India |
| Bart Preneel, | KU Leuven, Belgium |
| Benny Pinkas, | Bar-Ilan University, Israel |
| Bhavana Kanukurthi, | Indian Institute of Science, India |
| Carmit Hazay, | Bar-Ilan University, Israel |
| Chris Brzuska, | Hamburg University, Germany |
| Christophe Petit, | Oxford University, UK |
| Debdeep Mukhopadhyay, | Indian Institute of Technology Kharagpur, India |
| Dennis Hofheinz, | Karlsruhe Institute of Technology, Germany |
| Francois-Xavier Standaert, | Catholic University of Louvain (UCL Crypto Group), Belgium |
| Georg Fuchsbauer, | ENS Paris, France |
| Giuseppe Persiano, | University of Salerno, Italy |
| Goutam Paul, | Indian Statistical Institute Kolkata, India |
| Helena Handschuh, | Rambus Cryptography Research and KU Leuven, Belgium |
| Itai Dinur, | Ben-Gurion University, Israel |
| Jesper Buus Nielsen, | Aarhus University, Denmark |
| Jonathan Katz, | University of Maryland Park, USA |
| Joppe W. Bos, | NXP Semiconductors, Belgium |
| Kaoru Kurosawa, | Ibaraki University, Japan |
| Kenny Paterson, | Royal Holloway, University of London, UK |
| Krzysztof Pietrzak, | IST Austria, Austria |
| Manoj Prabhakaran, | Indian Institute of Technology Bombay, India |
| Marc Fischlin, | Darmstadt University of Technology, Germany |
| Martin Albrecht, | Royal Holloway, University of London, UK |
| Mike Rosulek, | Oregon State, USA |
| Nigel P. Smart, **(Co-chair)** | University of Bristol, UK |
| Nishanth Chandran, | Microsoft Research Bangalore, India |
| C. Pandu Rangan, | Indian Institute of Technology Madras, India |
| Ranjit Kumerasan, | Microsoft Research Redmond, USA |
| Rosario Gennaro, | City University New York, USA |
| Shweta Agrawal, | Indian Institute of Technology Madras, India |
| Somitra Kr Sanadhya, | Ashoka university, India |
| Takahiro Matsuda, | AIST, Japan |
| Tancrede Lepoint, | SRI, USA |
| Thomas Johansson, | Lund University, Sweden |
| Thomas Schneider, | Darmstadt University of Technology, Germany |
| Vipul Goyal, | Carnegie Mellon University, USA |
| Yu Sasaki, | NTT Secure Platform Laboratories, Japan |