

Preface

Since its introduction in 2000, INDOCRYPT has been widely acknowledged as the leading Indian venue for cryptography. As part of this tradition, INDOCRYPT 2016 was held during December 11–14, in Kolkata. This was the fourth time the conference was hosted Kolkata since its introduction by Prof. Bimal Roy. Past venues were held throughout India: Kolkata (2000, 2006, 2012, 2016), Chennai (2001, 2004, 2007, 2011), Hyderabad (2002, 2010), New Delhi (2003, 2009, 2014), Bangalore (2005, 2015), Kharagpur (2008), and Mumbai (2013).

INDOCRYPT 2016 attracted 84 submissions from 20 different countries, out of which 23 were selected at the end of a long review process: Most papers were reviewed by at least three committee members, whereas papers co-authored by Program Committee members were reviewed by at least five reviewers. In addition to the 283 reviews (produced with the aid of 91 additional reviewers), the Program Committee generated 223 comments during the discussion phase. We would like to express our sincere gratitude to all the members of the Program Committee, as well as all the external reviewers who helped in the challenging reviewing process.

The submission and review process was done using the iChair software package. We wish to express our sincere gratitude to Thomas Baignères and Matthieu Finiasz for the iChair software, which facilitated a smooth and easy submission and review process.

In addition to the 23 presentations of accepted papers, the attendees of INDOCRYPT also enjoyed three invited talks given by leading experts. Claudio Orlandi (Denmark) spoke about “Faster Zero-Knowledge Protocols for General Circuits and Applications”; the talk by François-Xavier Standaert (Belgium) covered “Leakage-Resilient Symmetric Cryptography”; and Tetsu Iwata (Japan) discussed “Breaking and Repairing Security Proofs of Authenticated Encryption Schemes.”

Finally, we would like to thank the general chair, Prof. Bimal Roy, and the local organizing team comprising members from the Applied Statistics Unit, the R.C. Bose Center for Cryptology and Security at ISI Kolkata, and the Cryptology Research Society of India.

December 2016

Orr Dunkelman
Somitra Sanadhya

Progress in Cryptology – INDOCRYPT 2016
17th International Conference on Cryptology in India,
Kolkata, India, December 11–14, 2016, Proceedings
Dunkelman, O.; Sanadhya, S. (Eds.)
2016, XVII, 429 p. 66 illus., Softcover
ISBN: 978-3-319-49889-8