

## Preface

We are pleased to present the proceedings of INDOCRYPT 2015, held during December 6–9, 2015, in Bangalore, India. This was the 16th edition of the INDOCRYPT series organized under the aegis of the Cryptology Research Society of India (CRSI).

The INDOCRYPT series of conferences began in 2000 under the leadership of Prof. Bimal Roy of Indian Statistical Institute.

The submissions for INDOCRYPT 2015 were due on July 20, 2015. We received 60 submissions from which, after a careful review and discussion process, 19 were selected for the conference proceedings.

The review process was conducted in two stages: In the first stage, most papers were reviewed by at least three committee members. In the second phase, which lasted for about two weeks, online discussion took place in order to decide on the acceptance of the submissions.

During the review process the Program Committee was helped by a team of 65 external reviewers.

We would like to thank the Program Committee members and the external reviewers for sharing their expertise and giving every paper a fair assessment. The review process was done with EasyChair, which greatly simplified the process.

We were delighted that Itai Dinur, Sanjam Garg, Seny Kamara, Alon Rosen, and Palash Sarkar agreed to deliver invited talks on several interesting topics of relevance to INDOCRYPT.

We were also pleased to have Yevgeniy Dodis and Manoj Prabhakaran deliver two tutorials as part of the conference.

We thank the General Chairs Satya Lokam and Sanjay Burman as well as the teams DRDO and the National Mathematics Initiative at the Indian Institute of Science, Bangalore, for their hard work and taking care of all the local organization matters for the conference. We are especially grateful to our sponsors for their generous support of the conference.

We acknowledge Springer for their active cooperation and timely production of the proceedings. Finally we thank all the authors who submitted papers to the INDOCRYPT 2015, and all the attendees. We hope you enjoy the proceedings of this year's INDOCRYPT conference.

December 2015

Alex Biryukov  
Vipul Goyal

Progress in Cryptology -- INDOCRYPT 2015  
16th International Conference on Cryptology in India,  
Bangalore, India, December 6-9, 2015, Proceedings  
Biryukov, A.; Goyal, V. (Eds.)  
2015, XX, 371 p. 53 illus. in color., Softcover  
ISBN: 978-3-319-26616-9