

Preface

We are glad to present the proceedings of INDOCRYPT 2014, held during 14–17 December in New Delhi, India. INDOCRYPT 2014 is the 15th edition of the INDOCRYPT series organized under the aegis of the Cryptology Research Society of India (CRSI). The conference has been organized by the Scientific Analysis Group (SAG), DRDO, New Delhi, India. The INDOCRYPT series of conferences began in 2000 under the leadership of Prof. Bimal Roy of Indian Statistical Institute.

In response to the call for papers, we received 101 submissions from around 30 countries around the globe. The submission deadline was July 28, 2014. The review process was conducted in two stages: In the first stage, most papers were reviewed by at least four committee members, while papers from Program Committee members received at least five reviews. This was followed by a week-long online discussion phase to decide on the acceptance of the submissions. The Program Committee was also suitably aided in this tedious task by 94 external reviewers to be able to complete this as per schedule, which was on September 7. Finally, 25 submissions were selected for presentation at the conference.

We would like to thank the Program Committee members and the external reviewers for giving every paper a fair assessment in such a short time. The refereeing process resulted in 367 reviews, along with several comments during the discussion phase. The authors had to revise their papers according to the suggestions of the referees and submit the camera-ready versions by September 22.

We were delighted that Phillip Rogaway, Marc Joye, and María Naya-Plasencia agreed to deliver invited talks on several interesting topics of relevance to INDOCRYPT. The program was also enriched to have Claude Carlet and Florian Mendel as Tutorial speakers on important areas of Cryptography, to make the conference program complete.

We would like to thank the General Chairs, Dr. G. Athithan and Dr. P.K. Saxena, for their advice and for being a prime motivator. We would also like to specially thank the Organizing Chair Saibal K. Pal and the Organizing Secretary Sucheta Chakrabarty for developing the layout of the program and in managing the financial support required for such a conference. Our job as Program Chairs was indeed made much easier by the software, easychair. We also say our thanks to Durga Prasad for maintaining the webpage for the conference. We would also acknowledge Springer for their active cooperation and timely production of the proceedings.

Last but certainly not least, our thanks go to all the authors, who submitted papers to INDOCRYPT 2014, and all the attendees. Without your support the conference would not be a success.



<http://www.springer.com/978-3-319-13038-5>

Progress in Cryptology -- INDOCRYPT 2014
15th International Conference on Cryptology in India,
New Delhi, India, December 14-17, 2014, Proceedings
Meier, W.; Mukhopadhyay, D. (Eds.)
2014, XXVI, 444 p. 80 illus., Softcover
ISBN: 978-3-319-13038-5