

Preface

INDOCRYPT 2017, the 18th International Conference on Cryptology in India, was held at Institute of Mathematical Sciences, Chennai, India, during December 10–13, 2017. The INDOCRYPT series of conferences began in 2000 under the leadership of Prof. Bimal Roy of the Indian Statistical Institute and is organized under the aegis of the Cryptology Research Society of India (CRSI). The conference focused on all technical aspects of cryptology.

The submissions for INDOCRYPT 2017 were due on August 27, 2017. In response to the call for papers, we received 75 submissions from around 20 countries, out of which 19 were chosen for inclusion in the program. The review process was conducted in two stages. In the first stage, each paper was reviewed by at least three independent reviewers, with papers from Program Committee members receiving at least five reviews. This was followed by a week-long rigorous and detailed discussion phase to decide on the acceptance of the submissions. Reviewers with potential conflicts of interest for specific papers were excluded from all discussions about those papers. The 43 members of the Program Committee were aided in this tedious and time-consuming task by many external reviewers. We would like to thank them all for their service, their expert opinions, and their spirited contributions to the review process. The authors had to revise their papers according to the suggestions of the referees and submit the camera-ready versions by October 15.

The submission and review process was done using Shai Halevi's Web Submission and Review Software. We wish to express our sincere gratitude to Shai Halevi for the software, which facilitated a smooth and easy submission and review process.

INDOCRYPT 2017 had three invited speakers with two from academia and one from the Government of India. Elette Boyle (Israel) enlightened the audience on "Recent Advances in Function and Homomorphic Secret Sharing". Tancrède Lepoint (USA) spoke on the interesting topic of "Post-Quantum Cryptography Using Module Lattices". The speech of Saikat Datta (Policy Director, Centre for Internet & Society, India) covered policy-making in India on Cryptography.

Finally, we would like to thank the general chairs, Prof. C. Pandu Rangan (Indian Institute of Technology Madras) and Prof. R. Balasubramanian (Institute of Mathematical Sciences); the team at the Indian Institute of Science who maintained the conference website; and the local organizing team at the Indian Institute of Technology, Madras, for their sincere hard work and for the local organization matters for the conference. We are especially grateful to our sponsors for their generous support of the conference. We would also like to express our appreciation to Springer for their active cooperation and timely production of the proceedings.

Finally, we would like to thank all the authors who submitted their work to INDOCRYPT 2017, and all the attendees. Without your spirited participation, the conference would not be a success. We hope you enjoy the proceedings of this year's INDOCRYPT conference.

December 2017

Nigel P. Smart
Arpita Patra

Progress in Cryptology – INDOCRYPT 2017

18th International Conference on Cryptology in India,
Chennai, India, December 10–13, 2017, Proceedings

Patra, A.; Smart, N.P. (Eds.)

2017, XII, 403 p. 68 illus., Softcover

ISBN: 978-3-319-71666-4