Preface

The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research. It also marks the coming of age of cryptology research in India.

The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT. In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference. Thus INDOCRYPT is well set on the path to achieving two main objectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India.

The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor. Way back in 1998, the scientific analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR. On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT. It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference series. Of course, the form, character, and execution of the conference series was the combined effort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

There were 75 submissions to INDOCRYPT 2002, out of which one was withdrawn and 31 were accepted. The invited talks were especially strong. Vincent Rijmen of AES fame gave a lecture on the design strategy for the recently accepted AES standard. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena recently achieved a breakthrough by obtaining a polynomial time deterministic algorithm for primality testing. This was presented at an invited talk by the authors. GuoZhen Xiao, an eminent researcher in the theory of sequences and Boolean functions, presented a lecture on efficient algorithms for computing the linear complexity of sequences.

The reviewing process for INDOCRYPT was very stringent and the schedule was very tight. The program committee did an excellent job in reviewing the papers and selecting the final papers for presentation. These proceedings include the revised versions of the selected papers. Revisions were not checked and the authors bear the full responsibility for the contents of the respective papers.

Program committee members were assisted in the review process by external reviewers. The list of external reviewers is included in the proceedings. Our thanks go to all the program committee members and the external reviewers who put in their valuable time and effort in providing important feedback to the authors.

Organizing the conference involved many individuals. We would like to thank the general chairs V.P. Gulati and M. Vidyasagar for taking care of the actual hosting of the conference. They were ably assisted by the organizing committee, whose names are included in the proceedings. Additionally, we would like to thank Kishan Chand Gupta, Sandeepan Chowdhury, Subhasis Pal, and Amiya Kumar Das for substantial help on different aspects of putting together this proceedings in its final form. Finally we would like to thank Springer-Verlag for active cooperation and timely production of the proceedings.

December 2002

Alfred Menezes
Palash Sarkar

INDOCRYPT 2002 was organized by the Institute for Development and Research in Banking Technology (IDRBT) and is an annual event of the Cryptology Research Society of India.

General Co-chairs

Ved Prakash Gulati	IDRBT, Hyderabad, India
M. Vidyasagar	Tata Consultancy Services, Hyderabad, India

Program Co-chairs

Alfred Menezes	University of Waterloo, Canada
Palash Sarkar	Indian Statistical Institute, India

Program Committee

Akshai Aggarwal	University of Windsor, Canada
Manindra Agrawal	Indian Institute of Technology, India
V. Arvind	Institute of Mathematical Sciences, India
Simon Blackburn	Royal Holloway, University of London, UK
Colin Boyd	Queensland University of Technology, Australia
ZongDuo Dai	Academia Sinica, China
Anand Desai	NTT MCL, USA
Ved Prakash Gulati	IDRBT, India
Anwar Hasan	University of Waterloo, Canada
Sushil Jajodia	George Mason University, USA
Charanjit Jutla	IBM, USA
Andrew Klapper	University of Kentucky, USA
Neal Koblitz	University of Washington, USA
Kaoru Kurosawa	Ibaraki University, Japan
Chae Hoon Lim	Sejong University, Korea
Subhamoy Maitra	Indian Statistical Institute, India
C.E. Veni Madhavan	Indian Institute of Science, India
Alfred Menezes	University of Waterloo, Canada
Rei Safavi-Naini	University of Wollongong, Australia
David Pointcheval	ENS Paris, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
A.K. Pujari	University of Hyderabad, India
Jaikumar Radhakrishnan	Tata Institute of Fundamental Research, India
Bimal Roy	Indian Statistical Institute, India
Palash Sarkar	Indian Statistical Institute, India
Vijay Varadharajan	Macquarie University, Australia
Stefan Wolf	University of Montreal, Canada
Chaoping Xing	National University of Singapore, Singapore
Amr Youssef	Cairo University, Egypt

Organizing Committee

S. Sankara Subramanian	IDRBT, India
Rajesh Nambiar	TCS, India
V. Visweswar	IDRBT, India
Ashutosh Saxena	IDRBT, India
V. Ravi Sankar	IDRBT, India
B. Kishore	TCS, India

External Referees

Kazumaro Aoki
Alexandra Boldyreva
Shiping Chen
Olivier Chevassut
Sandeepan Choudhury
Tanmoy K. Das
Matthias Fitzi
Steven Galbraith
Sugata Gangopadhyaya
Craig Gentry
Indivar Gupta
Alejandro Hevia
Michael Jacobs
Rahul Jain
Shaoquan Jiang
Meena Kumari
Yingjiu Li
Sin'ichiro Matsuo
Mridul Nandi
Laxmi Narain
Satomi Okazaki
Kapil Hari Paranjape
Rajesh Pillai
Matt Robshaw
Selwyn Russell
Takeshi Shimoyama
M.C. Shrivastava
Jason Smith
Alain Tapp
Ayineedi Venkateswarlu
Lingyu Wang
Bogdan Warinschi
Yiqun Lisa Yin
Sencun Zhu

Sponsoring Institutions

Acer India Pvt. Ltd., Bangalore
Cisco Systems India Pvt. Ltd., New Delhi
e-commerce magazine, New Delhi
HP India, New Delhi
IBM India Ltd., Bangalore
Infosys Technologies Ltd., Bangalore
Rainbow Information Technologies Pvt. Ltd. New Delhi
Society for Electronic Transactions and Security, New Delhi
Tata Consultancy Services, Mumbai

Table of Contents

Invited Talks

Symmetric Ciphers

New Public-Key Schemes

Foundations

Public-Key Infrastructures

Fingerprinting and Watermarking

Public-Key Protocols

Boolean Functions

Efficient and Secure Implementations

Applications

Anonymity

Secret Sharing and Oblivious Transfer

Author Index