Preface

The INDOCRYPT conference series started in 2000, and INDOCRYPT 2003 was the fourth one in this series. This series has been accepted by the international research community as a forum for presenting high-quality crypto research, as is evident from the 101 submissions this year, spread over 21 countries and all five continents. The accepted papers were written by authors from 16 countries, covering four continents.

A total of 101 papers were submitted for consideration to the program committee, and after a careful reviewing process 30 were accepted for presentation. One of the conditionally accepted papers was withdrawn by the authors as they found an error in the paper that could not be repaired in the short time between the notification of the review and the final version submission. Thus the final list contains 29 accepted papers. We would like to thank the authors of all submitted papers, including both those that were accepted and those which, unfortunately, could not be accommodated.

The reviewing process for INDOCRYPT was very stringent and the schedule was extremely tight. The program committee members did an excellent job in reviewing and selecting the papers for presentation. During the review process, the program committee members communicated using a review software package developed by Bart Preneel, Wim Moreau and Joris Claessens. We acknowledge them for providing this software. These proceedings include the revised versions of the 29 selected papers. Revisions were not checked by the program committee and the authors bear the full responsibility for the contents of the respective papers. Our thanks go to all the program committee members and the external reviewers (a list of them is included in the proceedings) who put in their valuable time and effort in providing important feedback to the authors.

This year the invited talks were presented by Prof. Harald Niederreiter and Prof. Jennifer Seberry. They do not need any introduction. Prof. Niederreiter presented a talk on "Linear Complexity and Related Complexity Measures for Sequences" and the talk of Prof. Seberry was on "Forensic Computing." Both talks have been included in these proceedings.

The organization of the conference involved many individuals. We would like to thank the general co-chairs Prof. Rajeeva L. Karandikar and Dr. P.K. Saxena 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 Tanmoy Kanti Das for handling all the submissions, and Avishek Adhikari and Madhusudan Karan for putting together this proceedings in its final form. Finally we would like to acknowledge Springer-Verlag for active cooperation and timely production of the proceedings.

December 2003   Thomas Johansson
                                                        Subhamoy Maitra

Organization

Indocrypt 2003 was organized by the Indian Statistical Institute, Delhi and the Scientific Analysis Group, Delhi.

General Co-chairs

Rajeeva L. Karandikar	Indian Statistical Institute, Delhi, India
Dr. P.K. Saxena	Scientific Analysis Group, New Delhi, India

Program Co-chairs

Thomas Johansson	Department of Information Technology, Lund University, Sweden
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India

Program Committee

R. Balasubramanian	Institute of Mathematical Sciences, India
Rana Barua	Indian Statistical Institute, Kolkata, India
Simon R. Blackburn	University of London, UK
Anne Canteaut	INRIA-Rocquencourt, France
John Clark	University of York, UK
Cunsheng Ding	Hong Kong University of Science and Technology, China
Yvo Desmedt	Florida State University, USA
Tor Helleseth	University of Bergen, Norway
Charanjit Singh Jutla	IBM Watson, USA
Thomas Johansson	Lund University, Sweden
Kaoru Kurosawa	Ibaraki University, Japan
Andrew Klapper	University of Kentucky, USA
Arjen K. Lenstra	Citibank, USA
Helger Lipmaa	Helsinki University of Technology, Finland
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
Alfred John Menezes	University of Waterloo, Canada
Phong Nguyen	École Normale Supérieure, France
C. Pandu Rangan	Indian Institute of Technology, Chennai, India
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Bimal Roy	Indian Statistical Institute, Kolkata, India
Vincent Rijmen	Cryptomathic, Belgium
P.K. Saxena	Scientific Analysis Group, Delhi, India
Jennifer Seberry	University of Wollongong, Australia

Pantelimon Stanica   Auburn University, Montgomery, USA
Kapaleeswaran Viswanathan   Queensland University of Technology, Australia
Moti Yung   Columbia University, USA

Organizing Committee

Dr. K.K. Bajaj   Office of the Controller of CA, MIT, Delhi
Prof. B.K. Dass   University of Delhi
Dr. B.K. Gairola   NIC, Delhi
Dr. Arup Pal   ISI, Delhi
Dr. Anish Sarkar   ISI, Delhi
Dr. Ashutosh Saxena   IDRBT, Hyderabad
Dr. Meena Kumari   SAG, Delhi
Mr. Jagdish Prasad   SAG, Delhi
Dr. Shri Kant   SAG, Delhi
Mr. G.S. Gupta   SAG, Delhi
Mr. Parimal Kumar   SAG, Delhi
Mr. Rajeev Thaman   SAG, Delhi
Mr. N. Rajesh Pillai   SAG, Delhi
Ms. Sarvjeet Kaur   SAG, Delhi
Ms. Roopika Chaudhary   SAG, Delhi
Ms. Noopur Shrotriya   SAG, Delhi

External Referees

Daniel Augot
S.S. Bedi
Siddika Berna Őrs
Sanjay Burman
Sucheta Chakrabarti
Suresh Chari
Thomas W. Cusick
Amites Dasgupta
Alex Dent
Vu Dong To
Ratna Dutta
Caroline Fontaine
Steven Galbraith
Gagan Garg
Indivar Gupta
Helena Handschuh
Darrel Hankerson
Florian Hess
Kouichi Itoh
Tetsu Iwata

Goce Jakimoski
Pascal Junod
Tanmoy Kanti Das
Meena Kumari
Pradeep Kumar Mishra
Françoise Levy-dit-Vehel
Keith Martin
Shin'ichiro Matsuo
Yi Mu
Partha Mukhopadhyay
Hirofumi Muratani
Sean Murphy
Jorge Nakahara, Jr.
Mridul Nandi
Laxmi Narain
Wakaha Ogata
Yasuhiro Ohtaki
Markku-Juhani O. Saari-nen
Elisabeth Oswald

Saibal K. Pal
Matthew Parker
Kenny Paterson
N. Rajesh Pillai
David Pointcheval
Michaël Quisquater
Malapati Raja Sekhar
Matt Robshaw
Pankaj Rohatgi
Atri Rudra
Kouichi Sakurai
Palash Sarkar
Hervé Sibert
Nigel Smart
Martijn Stam
Michael Steiner
H.V. Kumar Swamy
Jacques Traoré
Frederik Vercauteren
Johan Wallén

Yejing Wang	Tianbing Xia	Xianmo Zhang
Peter Wild	Pratibha Yadav	Weiliang Zhao

Sponsoring Institutions

DRDO, Government of India
Shoghi Communications Ltd., New Delhi, India
Technocab India Ltd., Bangalore, India