Preface

The field of Cryptology witnessed a revolution in the late seventies. Since then it has been expanded into an important and exciting area of research. Over the last two decades, India neither participated actively nor did it contribute significantly towards the development in this field. However, recently a number of active research groups engaged in important research and developmental work have crystalized in different parts of India. As a result, their interaction with the international crypto community has become necessary. With this backdrop, it was proposed that a conference on cryptology – INDOCRYPT, be organized for the first time in India. The Indian Statistical Institute was instrumental in hosting this conference. INDOCRYPT has generated a large amount of enthusiasm amongst the Indians as well as the International crypto communities. An INDOCRYPT steering committee has been formed and the committee has plans to make INDOCRYPT an annual event.

For INDOCRYPT 2000, the program committee considered a total of 54 papers and out of these 25 were selected for presentation. The conference program also included two invited lectures by Prof. Adi Shamir and Prof. Eli Biham.

These proceedings include the revised versions of the 25 papers accepted by the program committee. These papers were selected from all the submissions based on originality, quality and relevance to the field of Cryptology. Revisions were not checked and the authors bear the full responsibility for the contents of the papers in these proceedings.

The selection of the papers was a very difficult and challenging task. I wish to thank all the Program Committee members who did an excellent job in reviewing the papers and providing valuable feedback to the authors. Each submission was reviewed by at least three (only a few by two) reviewers. The program committee was assisted by many colleagues who reviewed submissions in their areas of expertise. The list of external reviewers has been provided separately. My thanks go to them all.

My sincere thanks goes to Springer-Verlag, in particular to Mr. Alfred Hofmann, for the inclusion of the seminar proceedings in their prestigious series Lecture Notes in Computer Science. I am also indebted to Prof. Jacques Stern, Prof. Jennifer Seberry, and Prof. Cunsheng Ding for giving their valuable advise and suggestions towards making the publication of the proceedings of INDOCRYPT 2000 possible.

I gratefully acknowledge financial support from diffferent organizations towards making INDOCRYPT 2000 a success. The contributors were AgniRoth (California, USA), Tata Conusltancy Service (Calcutta, India), CMC Limited (New Delhi, India), Cognizant Technology Solutions (Calcutta, India), Gemplus (Bangalore, India), Ministry of Information Technology (Govt. of India), and IDRBT (Hyderabad, India). I once again thank them all.

In organizing the scientific program and putting together these proceedings I have been assisted by many people. In particular I would like to thank Subhamoy Maitra, Sarbani Palit, Arindom De, Kishan Chand Gupta, and Sandeepan Chowdhury.

Finally I wish to thank all the authors who submitted papers, making this conference possible, and the authors of successful papers for updating their papers in a timely fashion, making the production of these proceedings possible.

December 2000   Bimal Roy

Program Co-chairs

Bimal Roy	Indian Statistical Institute, India
Eiji Okamoto	University of Wisconsin-Milwaukee, USA

General Co-chairs

Cunsheng Ding	Hong Kong University of Science & Technology, Hong Kong
R. Balasubramaniam	Institute of Mathematical Sciences, India

Organizing Committee Chair

Rajeev L. Karandikar	Indian Statistical Institute, India

Program Committee

R. Balasubramaniam	Institute of Mathematical Sciences, India
Rana Barua	Indian Statistical Institute, India
Don Beaver	Certco, USA
Thomas A. Berson	Anagram Laboratories, USA
Paul Camion	CNRS, France
Cunsheng Ding	Hong Kong University of Science & Tecnology, Hong Kong
K. Gopalakrishnan	East Carolina University, USA
Tor Helleseth	University of Bergen, Norway
Thomas Johansson	University of Lund, Sweden
Charanjit S. Jutla	IBM, T. J. Watson Lab, USA
Rajeev L. Karandikar	Indian Statistical Institute, India
Kwang Jo Kim	Information & Communications University, Korea
Andrew M. Klapper	University of Kentucky, USA
Arjen Lenstra	Citibank, USA
Tsutomu Matsumoto	Yokohama National University, Japan
Alfred Menezes	University of Waterloo, Canada
Ron Mullin	University of Waterloo, Canada
Phong Nguyen	ENS, France
Eiji Okamoto	University of Wisconsin-Milwaukee, USA
Tatsuaki Okamoto	NTT Labs, Japan
Dingyi Pei	Chinese Academy of Science, China
Radha Poovendran	University of Maryland, USA
Bart Preneel	COSIC, Belgium
Bimal Roy	Indian Statistical Institute, India
Palash Sarkar	Indian Statistical Institute, India
P. K. Saxena	SAG, India
Jennifer Seberry	University of Wollongong, Australia
K. Sikdar	Indian Statistical Institute, India
Jacques Stern	ENS, France
C. E. Veni Madhavan	Indian Institute of Sciences, India
M. Vidyasagar	Tata Consultancy Services, India
Michael Wiener	Entrust Technologies, Canada

Organizing Committee

Aditya Bagchi	Indian Statistical Institute, India
V. P. Gulati	IDRBT, India
Rajeev L. Karandikar	Indian Statistical Institute, India
Subhamoy Maitra	Indian Statistical Institute, India
Mandar Mitra	Indian Statistical Institute, India
Sarbani Palit	Indian Statistical Institute, India
Bimal Roy	Indian Statistical Institute, India
M. Vidyasagar	Tata Consultancy Services, India
K. S. Vijayan	Indian Statistical Institute, India

List of External Reviewers

Aditya Bagchi	Indian Statistical Institute, India
S S Bedi	SAG,India
A K Bhateja	SAG, India
Carlo Blundo	Universita di Salerno, Italy.
Johan Borst	Katholieke Universiteit Leuven, Belgium
Antoon Bosselaers	Katholieke Universiteit Leuven, Belgium
Dr Chris Charnes	University of Melbourne, Australia
Suresh Chari	IBM, T. J. Watson Lab, USA
Patrik Ekdahl	Lund University,Lund, Sweden
Shai Halevi	IBM, T. J. Watson Lab, USA
Fredrik Jnsson	Lund University,Lund, Sweden
Mike Just	Entrust Technologies, Canada
Meena Kumari	SAG, India
Subhamoy Maitra	Indian Statistical Institute, India
Nasir D. Memon	Polytechnic University, New York, USA.
Serge Mister	Entrust Technologies, Canada
Mandar Mitra	Indian Statistical Institute, India
Anish Ch. Mukherjee	Indian Statistical Institute, India
Pinakpani Pal	Indian Statistical Institute, India
Sarbani Palit	Indian Statistical Institute, India
Matthew Parker	University of Bergen, Norway
Enes Pasalic	Lund University,Lund, Sweden
Rajesh Pillai	SAG, India
David Pointcheval	ENS, France
Havard Raddum	University of Bergen, Norway
Pankaj Rohatgi	IBM, T. J. Watson Lab, USA
Reihaneh Safavi-Naini	University of Wollongong, Australia
Yuriy Tarannikov	Moscow State University, Russia
Serge Vaudenay	EPFL, France
Frederik Vercauteren	Katholieke Universiteit Leuven, Belgium
Robert Zuccherato	Entrust Technologies, Canada