Lecture Notes in Computer Science 2247
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

C. Pandu Rangan Cunsheng Ding (Eds.)

Progress in Cryptology – INDOCRYPT 2001

Second International Conference on Cryptology in India
Chennai, India, December 16-20, 2001
Proceedings

Springer

Volume Editors

C. Pandu Rangan
Indian Institute of Technology, Madras
Department of Computer Science and Engineering
Chennai, India
E-mail: rangan@iitm.ernet.in

Cunsheng Ding
Hong Kong University of Science and Technology
Department of Computer Science
Hong Kong
E-mail: cding@cs.ust.hk

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Progress in cryptology : proceedings / INDOCRYPT 2001, Second International
Conference on Cryptology in India, Chennai, India, December 16 - 20, 2001.
C. Pandu Rangan ; Cunsheng Ding (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2247)
ISBN 3-540-43010-5

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2

ISSN 0302-9743
ISBN 3-540-43010-5 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Steingräber Satztechnik GmbH Heidelberg
Printed on acid-free paper SPIN 10845931 06/3142 5 4 3 2 1 0

Preface

INDOCRYPT 2001, the Second Annual Crypto Conference, is proof of the significant amount of enthusiasm generated among Indian as well as International crypto communities. INDOCRYPT 2001 was organized by the Indian Institute of Technology, Madras and the Institute of Mathematical Sciences, also located in Madras (now Chennai). This event was enthusiastically co-sponsored by eAlcatraz Consulting Private Ltd, Chennai, Odyssey Technologies Ltd, Chennai, and Shanmuga Arts Science Technology and Research Academy (SASTRA), Thanjavur. The Program Committee Co-chair, Prof.C.Pandu Rangan was responsible for local organization and registration.

The Program Committee considered 77 papers and selected 31 papers for presentation. These papers were selected on the basis of perceived originality, quality, and relevance to the field of cryptography. The proceedings include the revised version of the accepted papers. Revisions were not checked as to their contents and authors bear full responsibility for the contents of their submissions.

The selection of papers is a very challenging and demanding task. We wish to thank the Program Committee members who did an excellent job in reviewing the submissions in spite of severe time constraints imposed by the tight processing schedule. Each submission was reviewed by at least three referees (only a few by two). The Program Committee was ably assisted by a large number of reviewers in their area of expertise. The list of reviewers has been provided separately. Our thanks go to all of them.

The conference program included three invited lectures by Prof. Andrew Klapper, University of Kentucky, USA, Dr. Anne Canteaut, INRIA, France, and Dr. Tatsuaki Okamoto, NTT Labs, Japan. In addition to these three invited lectures, pre-conference and post-conference tutorials were conducted by Ramarathnam Venkatesan, Microsoft, Redmond, USA on Random Number Generators: Theory and Practice and by Dipankar Dasgupta, The University of Memphis, USA on a Bio-Inspired Approach to Computer Security. Industrial presentations on the best practices were also scheduled during these days.

Our sincere thanks goes to Springer-Verlag, in particular to Mr. Alfred Hofmann, for publishing the proceedings of INDOCRYPT 2001 as a volume in their prestigious LNCS series. We are also indebted to Prof. Bimal Roy and Prof. C.E.Veni Madhavan and to all the members of the Steering Committee for their valuable advice and suggestions. We gratefully acknowledge the financial support extended by our co-sponsors and 'Golden' sponsors. We wish to make a special mention of the enthusiastic financial support extended by IIT Madras Alumni Association in North America, (IITMAANA) enabling a large number of students and faculty members from various universities in India to attend the conference.

This conference handled all the submissions as well as refereeing in electronic form. The ERNET centre located at IIT Madras, coordinated by Prof. S.V. Raghavan, provided excellent internet services at every stage of this conference.

We wish to place on record our sincere thanks to Prof. R. Natarajan, Director, IIT, Madras, Prof. C.R. Muthukrishnan, Deputy Director, IIT, Madras and Prof. Srinivasa Murthy, Dean, IC&SR, IIT, Madras for encouraging and supporting the conference in every possible way.

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

December 2001

Pandu Rangan C
Cunsheng Ding

INDOCRYPT 2001

December 16-20, 2001, Indian Institute of Technology,
Madras, India

Organized by
Indian Institute of Technology, Madras, India
The Institute of Mathematical Sciences, Chennai, India

Co-sponsored by
eAlcatraz Consulting Private Ltd, Chennai
Odyssey Technologies Ltd, Chennai
Shanmuga Arts Science Technology and Research Academy (SASTRA),
Thanjavur

General Chair

Balasubramaniam R	The Institute of Mathematical Sciences, India

Program Co-chairs

Pandu Rangan C	Indian Institute of Technology, Madras, India
Cunsheng Ding	Hong Kong University of Science, Hong Kong

Steering Committee

Balakrishnan N	Indian Institute of Science, Bangalore, India
Balasubramaniam R	The Institute of Mathematical Sciences, India
Bimal Roy	Indian Statistical Institute, Calcutta, India
Gulati V P	IDRBT, Hyderabad, India
Kapil H Paranjape J	The Institute of Mathematical Sciences, India
Karandikar R L	Indian Statistical Institute, Delhi, India
Manindar Agrawal	Indian Institute of Technology, Kanpur, India
Palash Sarkar	University of Waterloo, Canada
Pandu Rangan C	Indian Institute of Technology, Madras
Saxena P K	SAG, New Delhi, India
Sitaram N	CAIR, Bangalore, India
Vidyasagar M	Tata Consultancy Services, Hyderabad, India

Program Committee

Alfred John Menezes	University of Waterloo, Canada
Arjen K Lenstra	Citibank, USA
Balasubramaniam R	The Institute of Mathematical Sciences, India
Bimal Roy	Indian Statistical Institute, Calcutta, India
Claude Carlet	University of Caen, France

Cunsheng Ding	Hong Kong University of Science, Hong Kong
Dingyi Pei	Academia Sinica, China
Eiji Okamoto	University of Wisconsin, USA
Harald Niederreiter	National University of Singapore, Singapore
Jennifer Seberry	University of Wollongong, Australia
Kwangjo Kim	Information and Communications University, Korea
Lam Kwok Yan	National University of Singapore, Singapore
Neal Koblitz	University of Washington, USA
Palash Sarkar	University of Waterloo, Canada
Pandu Rangan C	Indian Institute of Technology, Madras, India
Rei Safavi-Naini	University of Wollongong, Australia
Thomas Johansson	Lund University, Sweden
Tom Berson	Anagram Laboratories, USA
Tsutomu Matsumoto	Japan
Veni Madhavan C E	SAG, India

Organizing Committee

Boopal E	Indian Institute of Technology, Madras, India
Kamakoti V	Indian Institute of Technology, Madras, India
Veeraraghavan V	Indian Institute of Technology, Madras, India

List of External Reviewers

Alfred John Menezes
Amr Youssef
Andreas Westfeld
Antoine Valembois
Arash Reyhani-Masoleh
Arjen K Lenstra
Ashwin Kumar M V N
Bedi S S
Berry Schoenmakers
Bhatiga A K
Bimal Roy
Byoungcheon Lee
Caroline Fontaine
Claude Carlet
Cunsheng Ding
Ding Yi Pei
Eiji Okamoto
Enes Pasalic
Eric Filiol
Eugene P Xavier
Evelyne Lutton
Fredrik Jonsson
Gambhir R K
Guillaume Poupard
Harald Niederreiter
Huapeng Wu
Indivar Gupta
Kaisa Nyberg
Khanna R K
Kishan C. Gupta
Kwangjo Kim
Laxmi Narayan
Marc Girault
Martijn Stam
Masahiro Mambo
Meena Kumari
Miodrag Mihaljevic
Neal Koblitz
Nicolas Sendrier
Pabitra Pali Chowdhury
Palash Sarkar
Pandu Rangan C
Paul J. Schellenberg
Pierrick Gaudry

Prabhu B
Pranava Raja Goundan
Pratibha Yadav
Raghavan S V
Rana Barua
Reihanah Safavi-Naini
Samik Sengupta
Sandeepan Chowdhury
Sanjeev K. Mishra
Sarbani Palit
Sexena P K
Sikdar K
Srinathan K
Srivastava M C
Subhamoy Maitra
Supratik Mukhopadhyay
Tharani Rajan
Thomas Johansson
Veni Madhavan C E

Sponsors

Arunai Charitable Trust, Tiruvannamalai
Cyberspace, Chennai
Dharma Naidu Educational and Charitable Trust, Chennai
HSMAK Charitable Trust, Gulbarga
Jai Barath Charitable Trust, Vaniyambadi
Jaya Educational Trust, Chennai
IITMAANA, USA
Lalitha Educational Trust, Hyderabad
Mauritius Research Council, Mauritius
MESCO, Hyderabad
Microsoft Corporation India Pvt. Ltd, Chennai
Nalini Suresh, Chennai
Ponniamman Educational Society, Chennai
Prince Venkateswara Education Society, Chennai
Rajalakshmi Educational Trust, Chennai
Sapthagiri Engineering College, Dharmapuri
Satyabama Institute of Science and Technology (Deemed University)
Sri Nandanam Educational and Social Welfare Trust, Thiruppathur
SUN Microsystem, India
Vasista Education Soceity, Narsapur, AP
Velammal Engineering College, Chennai

Table of Contents

Invited Lecture

Hashing

Algebraic Schemes

Elliptic Curves

Coding Theory

Applications – I

Cryptanalysis

Distributed Cryptography

Boolean Functions

Digital Signatures

Shift Registers

Applications – II