

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

2247

**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

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingraber 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 accepted 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

## VIII

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



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

### Sponsors

Arunai Charitable Trust, Tiruvannamalai  
 Cyberspace, Chennai  
 Dharma Naidu Educational and Charitable Trust, Chennai  
 HSMAC 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  
 Ponnamman 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 Socety, Narsapur, AP  
 Velammal Engineering College, Chennai

## Table of Contents

### Invited Lecture

Cryptographic Functions and Design Criteria for Block Ciphers .....	1
<i>A. Canteaut</i>	

### Hashing

Mobile Agent Route Protection through Hash-Based Mechanisms .....	17
<i>J. Domingo-Ferrer</i>	

A New Anonymous Fingerprinting Scheme with High Enciphering Rate ....	30
<i>M. Kuribayashi and H. Tanaka</i>	

A Parallel Algorithm for Extending Cryptographic Hash Functions .....	40
<i>P. Sarkar and P.J. Schellenberg</i>	

Incremental Hash Function Based on Pair Chaining & Modular Arithmetic Combining .....	50
<i>B.-M. Goi, M.U. Siddiqi, and H.-T. Chuah</i>	

### Algebraic Schemes

Multiples of Primitive Polynomials over $GF(2)$ .....	62
<i>K.C. Gupta and S. Maitra</i>	

Fast Generation of Cubic Irreducible Polynomials for XTR .....	73
<i>J.M. Kim, I. Yie, S.I. Oh, H.D. Kim, and J. Ryu</i>	

Cheating Prevention in Secret Sharing over $GF(p^t)$ .....	79
<i>J. Pieprzyk and X.-M. Zhang</i>	

### Elliptic Curves

An Application of Sieve Methods to Elliptic Curves .....	91
<i>S.A. Miri and V.K. Murty</i>	

Elliptic Curves of Prime Order over Optimal Extension Fields for Use in Cryptography .....	99
<i>H. Baier</i>	

A Secure Family of Composite Finite Fields Suitable for Fast Implementation of Elliptic Curve Cryptography .....	108
<i>M. Ciet, J.-J. Quisquater, and F. Sica</i>	

**Coding Theory**

Frameproof and IPP Codes .....	117
<i>P. Sarkar and D.R. Stinson</i>	

Linear Authentication Codes: Bounds and Constructions .....	127
<i>R. Safavi-Naini, H. Wang and C. Xing</i>	

**Applications – I**

Selective Receipt in Certified E-Mail .....	136
<i>S. Kremer and O. Markowitch</i>	

Spatial Domain Digital Watermarking with Buyer Authentication .....	149
<i>S. Maitra and D.P. Mukherjee</i>	

Efficient Public Auction with One-Time Registration and Public Verifiability .....	162
<i>B. Lee, K. Kim, and J. Ma</i>	

An Analysis of Integrity Services in Protocols .....	175
<i>K. Viswanathan, C. Boyd, and E. Dawson</i>	

**Cryptanalysis**

Cryptanalysis of the Nonlinear FeedForward Generator .....	188
<i>S.S. Bedi and N.R. Pillai</i>	

Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree .....	195
<i>M. Maurer, A. Menezes, and E. Teske</i>	

Cryptanalysis of Imai and Matsumoto Scheme B Asymmetric Cryptosystem .....	214
<i>A. Youssef and G. Gong</i>	

**Distributed Cryptography**

Robust and Secure Broadcasting .....	223
<i>Y. Mu and V. Varadharajan</i>	

Toward Optimal Player Weights in Secure Distributed Protocols .....	232
<i>K. Srinathan, C.P. Rangan, and V. Kamakoti</i>	

**Boolean Functions**

Autocorrelation Properties of Correlation Immune Boolean Functions .....	242
<i>S. Maitra</i>	

On the Constructing of Highly Nonlinear Resilient Boolean Functions by Means of Special Matrices .....	254
<i>M. Fedorova and Y. Tarannikov</i>	

### Digital Signatures

A Twin Algorithm for Efficient Generation of Digital Signatures .....	267
<i>D. Ramesh</i>	
Efficient “on the Fly” Signature Schemes Based on Integer Factoring .....	275
<i>T. Okamoto, M. Tada, and A. Miyaji</i>	

### Shift Registers

Clock-Controlled Shift Registers and Generalized Geffe Key-Stream Generator .....	287
<i>A. Kholosha</i>	
Efficient Software Implementation of Linear Feedback Shift Registers .....	297
<i>S. Chowdhury and S. Maitra</i>	
Comments on a Signature Scheme Based on the Third Order LFSR Proposed at ACISP2001 .....	308
<i>S. Lim, S. Kim, I. Yie, and J. Kim</i>	

### Applications – II

Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography .....	316
<i>L. Shujun, M. Xuanqin, and C. Yuanlong</i>	
Re-dividing Complexity between Algorithms and Keys (Key Scripts) .....	330
<i>G. Samid</i>	
A Tool Box of Cryptographic Functions Related to the Diffie-Hellman Function .....	339
<i>E. Kiltz</i>	
Author Index .....	351