Progress in Cryptology – INDOCRYPT 2003

4th International Conference on Cryptology in India
New Delhi, India, December 8-10, 2003
Proceedings
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 One of the conditionally accepted papers was withdrawn by the authors as they found an error in the paper that could not be repaired in the short time between the notification of the review and the final version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 Tannoy 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
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 NormaleSupérieure, 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 Örs
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. Saarinen
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
VIII Organization

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
Table of Contents

Invited Talks

Linear Complexity and Related Complexity Measures for Sequences .... 1
H. Niederreiter

Forensic Computing .................................................. 18
X. Li and J. Seberry

Stream Cipher

Hiji-bij-bij: A New Stream Cipher with a Self-synchronization Mode of Operation ......................................................... 36
P. Sarkar

Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator ................................................................. 52
S. Paul and B. Preneel

Block Cipher

Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA .......................................................... 68
H.M. Yıldırım

Impossible Differential Cryptanalysis for Block Cipher Structures .... 82
J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung

Impossible Differential Attack on 30-Round SHACAL-2 ................. 97
S. Hong, J. Kim, G. Kim, J. Sung, C. Lee, and S. Lee

Boolean Function

Construction of Perfect Nonlinear and Maximally Nonlinear Multi-output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria ......................................................... 107
K.C. Gupta and P. Sarkar

Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria .................................................. 121
S. Kavut and M.D. Yücel
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret Sharing</td>
<td></td>
</tr>
<tr>
<td>On Multiplicative Linear Secret Sharing Schemes</td>
<td>135</td>
</tr>
<tr>
<td>V. Nikov, S. Nikova, and B. Preneel</td>
<td></td>
</tr>
<tr>
<td>A New $(2, n)$-Visual Threshold Scheme for Color Images</td>
<td>148</td>
</tr>
<tr>
<td>A. Adhikari and S. Sikdar</td>
<td></td>
</tr>
<tr>
<td>On the Power of Computational Secret Sharing</td>
<td>162</td>
</tr>
<tr>
<td>V. Vinod, A. Narayanan, K. Srinathan, C.P. Rangan, and K. Kim</td>
<td></td>
</tr>
<tr>
<td>Bilinear Pairing</td>
<td></td>
</tr>
<tr>
<td>Identity-Based Broadcasting</td>
<td>177</td>
</tr>
<tr>
<td>Y. Mu, W. Susilo, and Y.-X. Lin</td>
<td></td>
</tr>
<tr>
<td>Efficient Verifiably Encrypted Signature and Partially Blind Signature</td>
<td>191</td>
</tr>
<tr>
<td>from Bilinear Pairings</td>
<td></td>
</tr>
<tr>
<td>F. Zhang, R. Safavi-Naini, and W. Susilo</td>
<td></td>
</tr>
<tr>
<td>Extending Joux’s Protocol to Multi Party Key Agreement</td>
<td>205</td>
</tr>
<tr>
<td>R. Barua, R. Dutta, and P. Sarkar</td>
<td></td>
</tr>
<tr>
<td>Public Key</td>
<td></td>
</tr>
<tr>
<td>Public Key Cryptosystems Based on Free Partially Commutative Monoids</td>
<td>218</td>
</tr>
<tr>
<td>and Groups</td>
<td></td>
</tr>
<tr>
<td>P.J. Abisha, D.G. Thomas, and K.G. Subramanian</td>
<td></td>
</tr>
<tr>
<td>Prime Numbers of Diffie-Hellman Groups for IKE-MODP</td>
<td>228</td>
</tr>
<tr>
<td>I. Yie, S. Lim, S. Kim, and D. Kim</td>
<td></td>
</tr>
<tr>
<td>Polynomial Equivalence Problems and Applications to Multivariate</td>
<td>235</td>
</tr>
<tr>
<td>Cryptosystems</td>
<td></td>
</tr>
<tr>
<td>F. Levy-dit-Vehel and L. Perret</td>
<td></td>
</tr>
<tr>
<td>Signature Scheme</td>
<td></td>
</tr>
<tr>
<td>Security Analysis of Several Group Signature Schemes</td>
<td>252</td>
</tr>
<tr>
<td>G. Wang</td>
<td></td>
</tr>
<tr>
<td>Forking Lemmas for Ring Signature Schemes</td>
<td>266</td>
</tr>
<tr>
<td>J. Herranz and G. Sáez</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Practical Mental Poker Without a TTP Based on Homomorphic Encryption</td>
<td>280</td>
</tr>
<tr>
<td>J. Castellà-Roca, J. Domingo-Ferrer, A. Riera, and J. Borrell</td>
<td></td>
</tr>
<tr>
<td>Table of Contents</td>
<td>XI</td>
</tr>
<tr>
<td>-------------------</td>
<td>----</td>
</tr>
<tr>
<td>Lightweight Mobile Credit-Card Payment Protocol</td>
<td>295</td>
</tr>
<tr>
<td>S. Kungpisdan, B. Srinivasan, and P.D. Le</td>
<td></td>
</tr>
<tr>
<td>Elliptic Curve &amp; Algebraic Geometry</td>
<td></td>
</tr>
<tr>
<td>On the Construction of Prime Order Elliptic Curves</td>
<td>309</td>
</tr>
<tr>
<td>E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis</td>
<td></td>
</tr>
<tr>
<td>Counting Points on an Abelian Variety over a Finite Field</td>
<td>323</td>
</tr>
<tr>
<td>F.A. Izadi and V.K. Murty</td>
<td></td>
</tr>
<tr>
<td>Implementation &amp; Digital Watermarking</td>
<td></td>
</tr>
<tr>
<td>Side Channel Attack on Ha-Moon’s Countermeasure of Randomized Signed Scalar Multiplication</td>
<td>334</td>
</tr>
<tr>
<td>K. Okeya and D.-G. Han</td>
<td></td>
</tr>
<tr>
<td>Systolic and Scalable Architectures for Digit-Serial Multiplication in Fields $GF(p^m)$</td>
<td>349</td>
</tr>
<tr>
<td>G. Bertoni, J. Guajardo, and G. Orlando</td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis of Block Based Spatial Domain Watermarking Schemes</td>
<td>363</td>
</tr>
<tr>
<td>T.K. Das</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>More Efficient Password Authenticated Key Exchange Based on RSA</td>
<td>375</td>
</tr>
<tr>
<td>D.S. Wong, A.H. Chan, and F. Zhu</td>
<td></td>
</tr>
<tr>
<td>A Password-Based Authenticator: Security Proof and Applications</td>
<td>388</td>
</tr>
<tr>
<td>Y. Hitchcock, Y.S.T. Tin, J.M. Gonzalez-Nieto, C. Boyd, and P. Montague</td>
<td></td>
</tr>
<tr>
<td>Stronger Security Bounds for OMAC, TMAC, and XCBC</td>
<td>402</td>
</tr>
<tr>
<td>T. Iwata and K. Kurosawa</td>
<td></td>
</tr>
<tr>
<td>Progressive Verification: The Case of Message Authentication</td>
<td>416</td>
</tr>
<tr>
<td>M. Fischlin</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>431</td>
</tr>
</tbody>
</table>