Lecture Notes in Computer Science 3348

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Anne Canteaut
Kapaleeswaran Viswanathan (Eds.)

Progress in Cryptology – INDOCRYPT 2004

5th International Conference on Cryptology in India
Chennai, India, December 20-22, 2004
Proceedings

Springer

Volume Editors

Anne Canteaut
Institut National de Recherche en Informatique et Automatique (INRIA)
Projet CODES, Domaine de Voluceau, Rocquencourt
78153 Le Chesnay Cedex, France
E-mail: anne.canteaut@inria.fr

Kapaleeswaran Viswanathan
SETS, 21 Mangadu Swamy Street, Nungambakkam
Chennai 600 034, India
E-mail: kapali@sets.org.in

Library of Congress Control Number: 2004116723

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

ISSN 0302-9743
ISBN 3-540-24130-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11369165 06/3142 5 4 3 2 1 0

Preface

The INDOCRYPT series of conferences started in 2000. INDOCRYPT 2004 was the fifth one in this series. The popularity of this series is increasing every year. The number of papers submitted to INDOCRYPT 2004 was 181, out of which 147 papers conformed to the specifications in the call for papers and, therefore, were accepted to the review process. Those 147 submissions were spread over 22 countries.

Only 30 papers were accepted to this proceedings. We should note that many of the papers that were not accepted were of good quality but only the top 30 papers were accepted. Each submission received at least three independent reviews. The selection process also included a Web-based discussion phase. We made efforts to compare the submissions with other ongoing conferences around the world in order to ensure detection of double-submissions, which were not allowed by the call for papers. We wish to acknowledge the use of the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens in conducting the review process electronically. The software greatly facilitated the Program Committee in completing the review process on time. We would like to thank Cédric Lauradoux and the team at INRIA for their total support in configuring and managing the Web-based submission and review softwares. We are unable to imagine the outcome of the review process without their participation.

This year the invited talks were presented by Prof. Colin Boyd and Prof. Amit Sahai. Colin provided a talk on the design of key establishment protocols while Amit presented a talk on secure protocols for complex tasks in complex environments. They presented two sides of the same coin so that the audience can gain a more comprehensive view of the analysis and design of cryptographic protocols. We hope that the invited talks contributed their share to promoting such an exciting area in cryptology research in India. At the same time, the invited talks were of great value for international researchers, as well, because Colin and Amit shared the latest results of their research activities.

The smooth and successful progress of INDOCRYPT 2004 was due to the efforts of many individuals. The members of the Program Committee worked hard throughout, and did an excellent job. Many external reviewers contributed their time and expertise to aid our decision-making. The Organizing Committee put its maximal effort into ensuring the successful progress of this conference. We wish to thank Prof. R. Balasubramaniam and Dr. M.S. Vijayaraghavan for being the general co-chairs of this conference. We also thank the Cryptology Research Society of India and ISI, Calcutta.

We hope that the INDOCRYPT series of conferences remains a forum for discussing high-quality results in the area of cryptology and its applications to information security in the years to come.

December 2004

Anne Canteaut
Kapaleeswaran Viswanathan

Organization

The INDOCRYPT Conferences are the annual events of the Cryptology Research Society of India. INDOCRYPT 2004 was organized by IMSc, Chennai, and SETS, Chennai.

General Co-chairs

R. Balasubramanian	Institute for Mathematical Sciences, India
M.S. Vijayaraghavan	SETS, India

Program Co-chairs

Anne Canteaut	INRIA, France
Kapaleeswaran Viswanathan	SETS, India

Program Committee

Michael Backes	IBM, Zurich, Switzerland
Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA, France
Cunsheng Ding	Hong Kong University of Science and Technology, China
Andreas Enge	Ecole Polytechnique, France
Caroline Fontaine	CNRS, France
Henri Gilbert	France Telecom R&D, France
Juanma Gonzalez-Nieto	Queensland University of Technology, Australia
Tor Helleseth	University of Bergen, Norway
Thomas Johansson	Lund University, Sweden
Kwangjo Kim	Information and Communications University, Korea
Tanja Lange	University of Bochum, Germany
Arjen Lenstra	Lucent Technologies, USA and Technische Universiteit Eindhoven, The Netherlands
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
Keith Martin	Royal Holloway University of London, UK
Anish Mathuria	Dhirubhai Ambani, Institute of Information and Communication Technology, India

Alfred Menezes	University of Waterloo, Canada
Shiho Moriai	Sony Computer Entertainment Inc., Japan
Kenneth Paterson	Royal Holloway University of London, UK
Kapil H. Paranjape	IMSc, Chennai, India
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Bimal Roy	ISI Kolkata, India
Amit Sahai	Princeton University, USA
Palash Sarkar	ISI Kolkata, India
Henk van Tilborg	Technische Universiteit Eindhoven, The Netherlands
D.G. Thomas	Madras Christian College, India
Kapaleeswaran Viswanathan	SETS, Chennai, India
Adam Young	Cigital Labs, USA
Moti Yung	Columbia University, USA

Organizing Committee

Dr. A.K. Chakravarthy	Dept. of IT, MICT, Govt. of India
Mr. Cédric Lauradoux	INRIA, France
Dr. K. Srinivas	IMSc, India
Dr. N.Vijayarangan	SETS, India

Organizing Sub-committee

Mr. G. Aswin	SETS, India
Mr. C. Stephen Balasundaram	SETS, India
Mr. Manish Chauhan	SETS, India
Ms. R. Indra	IMSc, India
Ms. K. Jayasri	SETS, India
Mr. R. Harish Kumar	SETS, India
Mr. Ramakrishna Manja	IMSc, India
Dr. Paul Pandian	IMSc, India
Mr. Vishnu Prasath	IMSc, India
Ms. A. Suganya	SETS, India
Mr. R. Vijayasarathy	SETS, India

External Referees

P.J. Abisha	Sattam Al-Riyami	Florent Bersani
Avishek Adhikari	Lejla Batina	Alex Biryukov
Riza Aditya	Côme Berbain	Simon Blackburn
Toru Akishita	Thierry Berger	Emmanuel Bresson

Jan Camenisch
Liqun Chen
Olivier Chevassut
Matthijs Coster
Deepak Kumar Dalai
V. Rajkumar Dare
Christophe De Cannière
Alex Dent
Jeroen Doumen
Dang Nguyen Duc
Sylvain Duquesne
Håkan Englund
Steven Galbraith
Pierrick Gaudry
Daniel Gottesman
Robert Granger
Kishan Chand Gupta
Darrel Hankerson
Guillaume Hanrot
Martin Hell
Clemens Heuberger
Shoichi Hirose
Yvonne Hitchcock
Dennis Hofheinz
Tetsu Iwata
Cees Jansen
Ellen Jochemsz
Stefan Katzenbeisser
Alexander Kholosha
Caroline Kudla
Joseph Lano
Hyunrok Lee
Kerstin Lemke
Benoît Libert
Vo Duc Liem
Phil MacKenzie
John Malone-Lee
Alexander Maximov
Nele Mentens
Chris Mitchell
Suman K. Mitra
François Morain
Sumio Morioka
Joern Mueller-Quade
James Muir
Svetla Nikova
Luke O'Connor
Siddika Berna Ors
Daniel Page
Matthew Parker
Olivier Pereira
Håvard Raddum
Zulfikar Ramzan
K. Rangarajan
François Recher
Akashi Satoh
Werner Schindler
Takeshi Shimoyama
Taizo Shirai
Jamshid Shokrollahi
Hervé Sibert
Francesco Sica
Andrey Sidorenko
Martijn Stam
Tsuyoshi Takagi
Gerard Tel
Yuuki Tokunaga
Ludo Tolhuizen
Emmanuel Thomé
Pim Tuyls
M.K. Viswanath
Brent Waters
Benne de Weger
Annegret Weng
Arne Winterhof
Christopher Wolf
Robbie Ye
Feng Zhu

Sponsoring Institutions

Bharat Electronics Limited
BRNS Secretariat, Bhabha Atomic Research Centre
Department of Information Technology, Government of India
Department of Science and Technology, Government of India
Electronics Corporation of India Limited
Hewlett Packard India Private Limited
Institute for Development and Research in Banking Technology
NASSCOM
SLN Technologies Private Limited
Sun Microsystems India Private Limited

Table of Contents

Cryptographic Boolean Functions

Foundations

Block Ciphers

Public Key Encryption

Efficient Representations

Public Key Cryptanalysis

Modes of Operation

Signatures

Traitor Tracing and Visual Cryptography