Lecture Notes in Computer Science 5922

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

Bimal Roy Nicolas Sendrier (Eds.)

Progress in Cryptology - INDOCRYPT 2009

10th International Conference on Cryptology in India
New Delhi, India, December 13-16, 2009
Proceedings

Springer

Volume Editors

Bimal Roy
Indian Statistical Institute, Applied Statistics Unit
203 B.T. Road, Kolkata 700108, India
E-mail: bimal@isical.ac.in

Nicolas Sendrier
Centre de Recherche INRIA Paris-Rocquencourt, Projet-Team SECRET
B.P. 105, 78153 Le Chesnay Cedex, France
E-mail: Nicolas.Sendrier@inria.fr

Library of Congress Control Number: 2009939328

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-10627-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-10627-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12802036 06/3180 5 4 3 2 1 0

Message from the General Chair

Starting with organizing the first International Conference on Cryptology in India (INDOCRYPT) in 2000, Cryptology Research Society of India (CRSI) has been spearheading these conferences in India every year in December at different places within the country. This year, the tenth conference in this series - INDOCRYPT 2009 was held in Delhi. The event was organized jointly by Scientific Analysis Group (SAG), Defense Research and Development Organization (DRDO) and Delhi University (DU) under the aegis of CRSI.

As is apparent, INDOCRYPT has been emerging as a powerful forum for researchers to interact, share their thoughts and their work with others for the overall growth of cryptology research in the world, more specifically in India. The overwhelming response in quality submissions to the conference and transparent open review mechanism helped in keeping the standards high and also in inducing researchers to participate in the conference and take up serious interest in the subject and R&D in this area. The response from within the country as well as from abroad was overwhelming, even from those participants who did not have contributory papers.

The complete INDOCRYPT 2009 event spanned over four days from 13 to 16 December 2009. The very first day was totally dedicated to two tutorials, whereas the main conference was held on the remaining three days with three invited talks and presentation of 20 papers. The tutorials were delivered by two eminent speakers—Willi Meier and Nicolas Sendrier provided insight of the subject to young researchers and also stimulated the thinking of others. The three invited talks were delivered by Dan Bernstein, Marc Girault and Thomas Johansson. I am thankful to all these speakers.

A conference of this kind would not have been possible to organize without full support from different people across different committees. While all logistic and general organizational aspects were looked after by the Organizing Committee teams, the coordination and selection of technical papers required dedicated and time-bound efforts by the Program Chairs. I am thankful to Nicolas Sendrier and Bimal Roy for their efforts in bringing out such an excellent technical program for the participants.

I am indebted to my fellow Organizing Chairs, Neelima Gupta (DU) and S.S. Bedi (SAG), and all other members of the organizing team from SAG and DU, who worked hard in making all the arrangements. Special thanks are due to the Organizing Secretary, S.K. Pal, for working tirelessly, shoulder to shoulder with volunteers and other team members from SAG and DU to make the stay of participants comfortable and the event enjoyable.

I express my heartfelt thanks to DRDO and DU for supporting us in all possible manners and also to MCIT (DIT), MSRI, BEL and ITI for sponsoring the event.

Last but not the least, I extend my sincere thanks to all those who contributed to INDOCRYPT 2009 and especially to the lucky ones who are now "authors" in this prestigious LNCS series of conference proceedings.

December 2009 P.K. Saxena

Message from the Technical Program Chairs

We are glad to present the proceedings of the 10th International Conference on Cryptology, INDOCRYPT 2009. This annual event started off nine years ago in the year 2000 by the Cryptology Research Society of India and has gradually matured into one of the topmost international cryptology conferences. This year we received 104 proposals of contributed talks from all over the world. After a rigorous review process, the Program Committee selected 28 papers out of those submissions. Each paper was thoroughly examined by several independent experts from the Program Committee or from the scientific community. The papers along with the reviews were then scrutinized by the Program Committee members during a discussion phase. We would like to thank the authors of all the papers for submitting their quality research work to the conference. Special thanks go to the Program Committee members and to the external reviewers for the time and energy they spent throughout the selection process so as to offer a conference and a volume of high scientific quality.

In addition to the contributed talks, we were fortunate to hear several keynote speakers who presented two very instructive tutorials:

Willi Meier	Analysis of Certain Stream Ciphers and Hash Functions
Nicolas Sendrier	The Design of Code-Based Cryptosystems

There were also three insightful survey talks:

Daniel J. Bernstein	High-speed Cryptography
Marc Girault	Cryptology and Elliptic Curves: A 25-Year Love (?) Story
Thomas Johansson	Coding Theory as a Tool in Cryptology

Finally, let us say that we are greatly indebted to Matthieu Finasz for setting up and running the submission and review server and for his help in the handling of the camera-ready versions of the published papers. We wish you a pleasant reading.

December 2009

Bimal K. Roy
Nicolas Sendrier

Organization

General Chair

P.K. Saxena	SAG, Delhi, India

Program Chairs

Bimal Roy	ISI Kolkata, India
Nicolas Sendrier	INRIA, France

Organizing Chairs

Neelima Gupta	Delhi University, India
S.S. Bedi	SAG, Delhi, India

Organizing Secretary

Saibal K. Pal	SAG, Delhi, India

Organizing Committee

S.K. Muttoo	Delhi University, India
Meena Kumari	SAG, Delhi, India
Shrikant	JCB, Delhi, India
Naveen Kumar	Delhi University, India
N. Rajesh Pillai	SAG, Delhi, India
Sarvjeet Kaur	SAG, Delhi, India
Rajeev Thaman	SAG, Delhi, India
P.D. Sharma	Delhi University, India
S.K. Azad	Delhi University, India
Noopur Shrotriya	SAG, Delhi, India
Sanchit Gupta	SAG, Delhi, India
Sandhya Khurana	Delhi University, India
Rahul Johari	Delhi University, India
Ajay Shrivastava	SAG, Delhi, India

Program Committee

Gildas Avoine	Université catholique de Louvain, Belgium
Thierry Berger	Université de Limoges, France
Raghav Bhaskar	Microsoft Research Bangalore, India
Johannes Buchmann	Technische Universität Darmstadt, Germany
Sanjay Burman	CAIR Bangalore, India
Sanjit Chatterjee	University of Waterloo, Canada
Cusheng Ding	Hong Kong University of Science and Technology, China
Jintai Ding	University of Cincinnati, USA
Orr Dunkelman	École Normale Supérieure, France
Bao Feng	Institute for Infocomm Research, Singapore
Matthieu Finiasz	ENSTA, France
Pierrick Gaudry	LORIA, France
Guang Gong	University of Waterloo, Canada
Neelima Gupta	University of Delhi, India
Tor Helleseth	University of Bergen, Norway
Seokhie Hong	Korea University, Korea
Pascal Junod	University of Applied Sciences Western Switzerland, Switzerland
Jens-Peter Kaps	George Mason University, USA
Andrew Klapper	University of Kentucky, USA
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Subhamoy Maitra	ISI Kolkata, India
Keith Martin	Royal Holloway, University of London, UK
Alfred Menezes	University of Waterloo, Canada
Marine Minier	INSA de Lyon, France
S.K. Muttoo	University of Delhi, India
Mridul Nandi	NIST, USA
Kaisa Nyberg	Helsinki University of Technology, Finland
Tatsuaki Okamoto	NTT Corporation, Japan
Dingyi Pei	Guangzhou University, China
Josef Pieprzyk	Macquarie University, Australia
C. Pandu Rangan	IIT Chennai, India
Vincent Rijmen	K.U. Leuven, Belgium and Graz University of Technology, Austria
Matt Robshaw	Orange Labs, France
Dipanwita RoyChaudhury	IIT Kharagpur, India
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	ISI Kolkata, India
P.K. Saxena	SAG, Delhi, India
Jean-Pierre Tillich	INRIA, France
C.E. Veni Madhavan	IISC Bangalore, India

Additional Referees

Avishek Adhikari
Carlos Aguilar Melchor
François Arnault
Daniel J. Bernstein
Rishiraj Bhattacharyya
Jaydeb Bhowmik
Anne Canteaut
Yaniv Carmeli
Donghoon Chang
Qi Chen
Joo Yeon Cho
Abhijit Das
Sharmila Deva Selvi
Yusong Du
Xinxin Fan
Georg Fuchsbauer
Sugata Gangopadhyay
Indivar Gupta
Mohammad Hassanzadeh
Michael Hojsik
Honggang Hu
Thomas Icart
Ellen Jochemz
Ramakanth Kavuluru
John Kelsey
Eike Kiltz
Ki Tak Kim
S. Kiyomoyo
Meena Kumari
Yann Laigle-Chapuy
Cédric Lauradoux
Gaëtan Leurent
Zhijun Li
Alexander May
Seyed Mehdi
S.P. Mishra
Saibal K. Pal
Arpita Patra
Goutam Paul
Kun Peng
Ludovic Perret
N.R. Pillai
Benjamin Pousse
Padmanabhan Raman
Sumanta Sarkar
Berry Schoenmakers
Peter Schwabe
Yannick Seurin
Thomas Shrimpton
Damien Stehlé
C. Su
V. Suresh
Kumar Swamy H.V.
Damien Vergnaud

Table of Contents

Hash Functions

Number Theoretic Cryptology

Lightweight Cryptology

Signature Protocols

Multiparty Computation