Lecture Notes in Computer Science 7668

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

Steven Galbraith Mridul Nandi (Eds.)

Progress in Cryptology - INDOCRYPT 2012

13th International Conference on Cryptology in India
Kolkata, India, December 9-12, 2012
Proceedings

Springer

Volume Editors

Steven Galbraith
University of Auckland
Department of Mathematics
Private Bag 92019
Auckland 1142, New Zealand
E-mail: s.galbraith@math.auckland.ac.nz

Mridul Nandi
Indian Statistical Institute
Applied Statistics Unit
203 B.T. Road
Kolkata 700108, West Bengal, India
E-mail: mridul@isical.ac.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-34930-0 e-ISBN 978-3-642-34931-7
DOI 10.1007/978-3-642-34931-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012951708

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Indocrypt 2012, the 13th International Conference on Cryptology in India, took place during December 9–12, 2012. It was hosted by the Indian Statistical Institute in Kolkata. The Indocrypt series of conferences began in 2000 under the leadership of Bimal Roy. This series is now well established as an international forum for presenting high-quality cryptography research.

This year 99 papers were submitted for consideration. The authors of the submitted papers were from institutions across 25 countries and five continents.

As in previous years, the submission deadline was split into two: authors were required to register titles and abstracts by July 23, 2012, while final versions of papers had to be submitted by July 28. During that week the titles and abstracts were made available to the Program Committee (PC) to enable them to select their preferred articles for review. Most papers were refereed by three committee members, and papers co-authored by a PC member were refereed by five committee members. We thank Tanja Lange for hosting the ichair system, which was used to manage submissions and online discussions, on her Web server.

The review stage was very tight, with only three weeks for reviewing papers and only two weeks (August 20 to September 1) for the online discussions. It was a difficult challenge for the 33 PC members and 86 sub-reviewers to give every paper a fair assessment in such a short time. A total of 313 referee reports were written, and 314 comments were posted on the online discussions. At the end of the discussion process 28 papers were accepted for the proceedings (five of them conditionally accepted subject to successful revision according to referee suggestions). Authors were notified on September 3 and had around 2 weeks to revise their papers according to the suggestions of the referees.

We would like to thank all the authors of submitted papers for supporting the Indocrypt conference. The best way to support a conference is to submit papers to it and attend it. We also wish to thank the members of the PC and their sub-reviewers (a list is given here) for devoting their time and knowledge to the selection of papers.

The proceedings include the revised versions of the 28 selected papers. Revisions were not checked by the PC and the authors bear the full responsibility for the contents of the respective papers. The proceedings also contain invited papers by Nigel Smart and Vinod Vaikuntanathan, as well as a one-page abstract of the invited lecture by Orr Dunkelman.

The organization of the conference involved many individuals. We express our heart-felt gratitude to the General Chair, Bimal Roy, Director of Indian

Statistical Institute, Kolkata, and Subhamoy Maitra for taking care of the actual hosting of the conference. Members of the Cryptology Research Group at the Indian Statistical Institute provided invaluable secretarial support. Finally, we would like to acknowledge Springer for their active cooperation and timely production of the proceedings.

December 2012

Steven Galbraith
Mridul Nandi

Organization

Indocrypt 2012 was organized by the Indian Statistical Institute, Kolkata, in collaboration with the Cryptology Research Society of India.

General Chair

Bimal K. Roy	Indian Statistical Institute, Kolkata, India

Program Co-chairs

Steven Galbraith	University of Auckland, New Zealand
Mridul Nandi	Indian Statistical Institute, Kolkata, India

Program Committee

Daniel Bernstein	University of Illinois at Chicago, USA
Sanjit Chatterjee	Indian Institute of Science, India
Chen-Mou Cheng	National Taiwan University, Taiwan
Joan Daemen	STMicroelectronics
Philippe Gaborit	Universite de Limoges, France
Steven Galbraith	University of Auckland, New Zealand
Vipul Goyal	Microsoft Research India, India
Shay Gueron	University of Haifa, Israel
Goichiro Hanaoka	National Institute of AIST, Japan
Tetsu Iwata	University of Nagoya, Japan
Stanislaw Jarecki	UC Irvine, USA
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Kristin Lauter	Microsoft, USA
Keith Martin	Royal Holloway, University of London, UK
Willi Meier	FHNW Switzerland
David Naccache	Ecole Normale Superieure, Paris, France
Mridul Nandi	Indian Statistical Institute, Kolkata, India
Jesper Buus Nielsen	Aarhus University, Denmark
Elisabeth Oswald	University of Bristol, UK
Carles Padro	Nanyang Technological University, Singapore
Arpita Patra	ETH Zurich, Switzerland
Goutam Paul	Jadavpur University, India

Manoj M. Prabhakaran	University of Illinois, Urbana-Champaign, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
C. Pandu Rangan	Indian Statistical Institute, Chennai, India
Christian Rechberger	Danish Technical University, Denmark
Phillip Rogaway	University of California, Davis, USA
Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Palash Sarkar	Indian Statistical Institute, Kolkata, India
Nicolas Sendrier	INRIA Rocquencourt, France
Damien Stehle	Ecole Normale Superieure de Lyon, France
Dominique Unruh	University of Tartu, Estonia
Fre Vercauteren	Katholieke Universiteit Leuven, Belgium

External Referees

Mohamed Ahmed Abdelraheem
Elena Andreeva
Diego F. Aranha
Subhadeep Banik
Guido Bertoni
Rishiraj Bhattacharyya
Zeeshan Bilal
Begül Bilgin
Praloy Biswas
Julia Borghoff
Joppe Bos
Charles Bouillaguet
Christina Boura
Stanislav Bulygin
Donghoon Chang
Yun-An Chang
Melissa Chase
Anupam Chattopadhyay
Ashish Choudhury
Sherman S.M. Chow
Craig Costello
Abhijit Das
Christophe Doche
Keita Emura
Reza Rezaeian Farashahi
Thomas Fuhr
David Galindo
Sugata Gangopadhyay
Gerhard Hancke
Carmit Hazay
Javier Herranz
Huseyin Hisil
Chethan Kamath
Ferhat Karakoc
Sandip Karmakar
Kouhei Kasamatsu
Simon Knellwolf
Ozgul Kucuk
Fabien Laguillaumie
Gregory Landais
Cédric Lauradoux
Anh Le
Gregor Leander
Benoit Libert
Changshe Ma
Subhamoy Maitra
Preetha Mathews
Takahiro Matsuda
Filippo Melzani
Miodrag Mihaljevic
Nicky Mouha
Sean Murphy
Michael Naehrig
Souradyuti Paul
Roel Peeters
Albrecht Petzoldt
Maria Naya Plasencia
Sukhendu Quila
Dhiman Saha
Yusuke Sakai
Subhabrata Samajdar
Somitra Sanadhya
Yu Sasaki
Jacob C.N. Schuldt
Gautham Sekar
Sharmila Deva Selvi
Sourav Sengupta
Jae Hong Seo
Kyoji Shibutani
Francesco Sica
Alice Silverberg
Shashank Singh
Ben Smith
Valentin Suder
Enrico Thomae
Michael Tunstall
Berkant Ustaoglu
Vinod Vaikuntanathan
Ayineedi Venkateswarlu
Sree Vivek
Colin Walter
Carolyn Whitnall
Christopher Wolf
Marcin Wójcik
Shota Yamada
Naoto Yanai
Bo-Yin Yang
Wei Zhang

Sponsoring Institutions

Defence Research and Developement Organization (D.R.D.O.), India
Google Inc., India
Microsoft Research, Bangalore
National Board of Higher Mathematics (N.B.H.M.), Mumbai
Reserve Bank of India (R.B.I.), Kolkata
Tata Consultancy Services (T.C.S.), Kolkata

Table of Contents

Invited Papers

Protocol

Side Channel

Hash Functions and Stream Cipher

Cryptanalysis of Block Ciphers

Time Memory Trade-Off

Hardware

Elliptic Curve

Digital Signature

Symmetric Key Design and Provable Security