Lecture Notes in Computer Science 7107

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

Daniel J. Bernstein Sanjit Chatterjee (Eds.)

Progress in Cryptology – INDOCRYPT 2011

12th International Conference on Cryptology in India
Chennai, India, December 11-14, 2011
Proceedings

Springer

Volume Editors

Daniel J. Bernstein
University of Illinois at Chicago
Department of Computer Science
Chicago, IL 60607–7053, USA
E-mail: djb@math.uic.edu

Sanjit Chatterjee
Indian Institute of Science
Department of Computer Science and Automation
Bangalore 560 012, India
E-mail: sanjit@csa.iisc.ernet.in

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-25577-9 e-ISBN 978-3-642-25578-6
DOI 10.1007/978-3-642-25578-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011941501

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 2011, the 12th International Conference on Cryptology in India, took place December 11–14, 2011. It was co-hosted by the Institute of Mathematical Sciences in Chennai and the Chennai Mathematical Institute. Indocrypt has been held every year since 2000, and has been held under the aegis of the Cryptology Research Society of India since 2003.

We followed the Indocrypt 2006 idea of splitting the submission deadline into two. Authors submitting papers were required to register titles and abstracts by the first deadline, 31 July 2011. A total of 127 submissions had been received by this deadline, although some were withdrawn before review. Authors were allowed to continue working on their papers until the second deadline, August 7.

Submissions were evaluated in three phases over a period of nearly two months. The selection phase started on August 1: Program Committee members began evaluating abstracts and volunteering to handle various papers. We assigned a team of people to each paper. The review phase started on August 9: Program Committee members were given access to the full papers and began in-depth reviews of 98 submissions. Most of the reviews were completed by August 29, the beginning of the discussion phase. Program Committee members were given access to other reviews once they had completed all of their own reviews, and built consensus in their evaluations of the submissions. In the end the discussions included 353 full reports and 219 additional comments. The submissions, reviews, and subsequent discussions were handled smoothly by iChair.

On September 18 we sent out comments from the reviewers, 2 notifications of conditional acceptance, and 20 notifications of unconditional acceptance. The conditionally accepted papers eventually met their acceptance conditions; the final program contains 22 contributed papers, 3 invited talks, and 3 tutorials. The authors prepared final versions of the 22 contributed papers by September 30.

It is our pleasure to thank the other 56 Program Committee members for lending their expertise to Indocrypt 2011 and for putting tremendous effort into detailed reviews and discussions. We would also like to thank Thomas Baignères and Matthieu Finiasz for writing the iChair software; Tanja Lange for modifying the software to handle split submissions and managing the software on her Web server in Europe; the General Chairs, R. Balasubramaniam from the Institute of Mathematical Sciences in Chennai and Rajeeva Laxman Karandikar from the Chennai Mathematical Institute, for smoothly handling all of the local arrangements; 80 external referees who reviewed individual papers upon request from the Program Committee; and, most importantly, all authors for submitting interesting new research papers to Indocrypt 2011.

December 2011

Daniel J. Bernstein and Sanjit Chatterjee
Program Chairs, Indocrypt 2011

Organization

General Chairs

R. Balasubramaniam	Institute of Mathematical Sciences, Chennai, India
Rajeeva Laxman Karandikar	Chennai Mathematical Institute, India

Program Chairs

Daniel J. Bernstein	University of Illinois at Chicago, USA
Sanjit Chatterjee	Indian Institute of Science, Bangalore, India

Program Committee

Roberto Avanzi	Ruhr University Bochum, Germany
Rana Barua	Indian Statistical Institute, India
Lejla Batina	Radboud University Nijmegen, The Netherlands, and KU Leuven, Belgium
Daniel J. Bernstein	University of Illinois at Chicago, USA
Sanjay Burman	Centre for Artificial Intelligence and Robotics, India
Debrup Chakraborty	CINVESTAV-IPN, Mexico
Sanjit Chatterjee	Indian Institute of Science, India
Chen-Mou Cheng	National Taiwan University, Taiwan
Ashish Choudhury	Indian Statistical Institute, India
Sherman S.M. Chow	University of Waterloo, Canada
Christophe De Cannière	Google, Switzerland
Yvo Desmedt	University College London, UK
Christophe Doche	Macquarie University, Australia
Matthieu Finiasz	ENSTA, France
Praveen Gauravaram	Technical University of Denmark, Denmark
Vipul Goyal	Microsoft Research, India
Tim Güneysu	Ruhr University Bochum, Germany
Shay Gueron	University of Haifa, Israel, and Intel Corporation, Israel
Kishan Chand Gupta	Indian Statistical Institute, India
Helena Handschuh	Intrinsic-ID, USA, and KU Leuven, Belgium
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA and Université de Versailles Saint-Quentin-en-Yvelines, France
Koray Karabina	University of Waterloo, Canada

Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Vadim Lyubashevsky	ENS, France
Subhamoy Maitra	Indian Statistical Institute, India
Keith Martin	Royal Holloway, University of London, UK
David McGrew	Cisco, USA
Payman Mohassel	University of Calgary, Canada
Michele Mosca	University of Waterloo, Canada
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India
Michael Naehrig	Technische Universiteit Eindhoven, The Netherlands
Mridul Nandi	Indian Statistical Institute, India
Roger Oyono	Université de la Polynesie Française, French Polynesia
Daniel Page	University of Bristol, UK
Kenny Paterson	Royal Holloway, University of London, UK
Josef Pieprzyk	Macquarie University, Australia
Manoj Prabhakaran	University of Illinois at Urbana-Champaign, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Christian Rechberger	ENS Paris, France
Vincent Rijmen	KU Leuven, Belgium, and TU Graz, Austria
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
P.K. Saxena	DRDO, India
Peter Schwabe	National Taiwan University, Taiwan
Mike Scott	Dublin City University, Ireland
Nicolas Sendrier	INRIA, France
Francesco Sica	
Martijn Stam	University of Bristol, UK
François-Xavier Standaert	Université Catholique de Louvain, Belgium
Damien Stehlé	CNRS and ENS de Lyon, France
Christine Swart	University of Cape Town, South Africa
Michael Szydlo	Akamai, USA
Berkant Ustaoglu	Sabanci University, Turkey
C.E. Veni Madhavan	Indian Institute of Science, India
Huaxiong Wang	Nanyang Technological University, Singapore
Michael J. Wiener	Irdeto, Canada
Bo-Yin Yang	Academia Sinica, Taiwan

Referees

Mohamed Ahmed Abdelraheem	Sk. Subidh Ali
David Adam	Elena Andreeva
Shweta Agrawal	Josep Balasch

Georg T. Becker
S.S. Bedi
Murat Cenk
Yun-An Chang
Jie Chen
Cheng-Kang Chu
Romar dela Cruz
Alex Dent
Jérémie Detrey
Orr Dunkelman
Marc Fischlin
Eduarda Freire
Georg Fuchsbauer
Benoît Gérard
Benedikt Gierlichs
Ian Goldberg
Philipp Grabher
Robert Granger
Jian Guo
Indivar Gupta
Gottfried Herold
Simon Hoerder
Yun-Ju Huang
Seny Kamara
Markus Kasper
Saqib A. Kakvi
Daniel Kraschewski
Virendra Kumar
Meena Kumari
Fabien Laguillaumie
Jooyoung Lee
Allison Bishop Lewko
Hoon Wei Lim
Adriana López-Alt
Shah Mahmood
Ingo von Maurich
Bodhisatwa Mazumdar
Marine Minier
Oliver Mischke
Shahram Mossayebi
Pratyay Mukherjee
Ayan Nandy
Takashi Nishide
Kenji Ohkuma
Adam O'Neill
David Oswald
Omkant Pandey
Sumit Kumar Pandey
Tapas Pandit
Thomas Peters
David Pointcheval
Chester Rebeiro
Francesco Regazzoni
Sujoy Sinha Roy
Antoine Rojat
N.R. Pillai
Subhabrata Samajder
Martin Schläffer
Rich Schroeppel
Y.R. Siddarth
Ron Steinfeld
Doug Stinson
Daehyun Strobel
H.V. Kumar Swamy
Nicolas Thériault
Emmanuel Thomé
Søren S. Thomsen
Stefan Tillich
Tomas Toft
Kerem Varıcı
Ching-Hua Yu
Greg Zaverucha
Liangfeng Zhang
Huafei Zhu

Table of Contents

Secret-Key Cryptography, Part 1

Invited Talk 2

Secret-Key Cryptography, Part 2

Hash Functions

Pairings

Invited Talk 3

Protocols

Tutorial 3