

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

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

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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.

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 Polynésie 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 Szydło	Akamai, USA
Berkant Ustaoglu	Sabancı 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
J  r  mie Detrey
Orr Dunkelman
Marc Fischlin
Eduarda Freire
Georg Fuchsbauer
Beno  t G  rard
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 L  pez-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 Schl  ffer
Rich Schroepel
Y.R. Siddarth
Ron Steinfeld
Doug Stinson
Daehyun Strobel
H.V. Kumar Swamy
Nicolas Th  riault
Emmanuel Thom  
S  ren S. Thomsen
Stefan Tillich
Tomas Toft
Kerem Varıcı
Ching-Hua Yu
Greg Zaverucha
Liangfeng Zhang
Huafei Zhu

Table of Contents

Tutorial 1

Tor and the Censorship Arms Race: Lessons Learned (Abstract)	1
<i>Roger Dingledine</i>	

Tutorial 2

Elliptic Curves for Applications (Abstract)	2
<i>Tanja Lange</i>	

Side-Channel Attacks

PKDPA: An Enhanced Probabilistic Differential Power Attack Methodology	3
<i>Dhiman Saha, Debdeep Mukhopadhyay, and Dipanwita RoyChowdhury</i>	

Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks	22
<i>Maxime Nassar, Sylvain Guilley, and Jean-Luc Danger</i>	

Square Always Exponentiation	40
<i>Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, and Vincent Verneuil</i>	

An Enhanced Differential Cache Attack on CLEFIA for Large Cache Lines	58
<i>Chester Rebeiro, Rishabh Poddar, Amit Datta, and Debdeep Mukhopadhyay</i>	

Partial Key Exposure: Generalized Framework to Attack RSA	76
<i>Santanu Sarkar</i>	

Invited Talk 1

The Yin and Yang Sides of Embedded Security (Abstract)	93
<i>Christof Paar</i>	

Secret-Key Cryptography, Part 1

Mars Attacks! Revisited: Differential Attack on 12 Rounds of the MARS Core and Defeating the Complex MARS Key-Schedule	94
<i>Michael Gorski, Thomas Knapke, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
Linear Cryptanalysis of PRINTCIPHER–Trails and Samples Everywhere	114
<i>Martin Ågren and Thomas Johansson</i>	
Practical Attack on 8 Rounds of the Lightweight Block Cipher KLEIN	134
<i>Jean-Philippe Aumasson, María Naya-Plasencia, and Markku-Juhani O. Saarinen</i>	
On Related-Key Attacks and KASUMI: The Case of A5/3	146
<i>Phuong Ha Nguyen, Matthew J.B. Robshaw, and Huaxiong Wang</i>	

Invited Talk 2

Cryptology: Where Is the New Frontier? (Abstract)	160
<i>Ross Anderson</i>	

Secret-Key Cryptography, Part 2

Analysis of the Parallel Distinguished Point Tradeoff	161
<i>Jin Hong, Ga Won Lee, and Daegun Ma</i>	
On the Evolution of GGHN Cipher	181
<i>Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar</i>	
HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers	196
<i>Sourav Sen Gupta, Anupam Chattopadhyay, and Ayesha Khalid</i>	
Addressing Flaws in RFID Authentication Protocols	216
<i>Mohammad Hassan Habibi, Mohammad Reza Aref, and Di Ma</i>	

Hash Functions

Practical Analysis of Reduced-Round KECCAK	236
<i>María Naya-Plasencia, Andrea Röck, and Willi Meier</i>	
Boomerang Distinguisher for the SIMD-512 Compression Function	255
<i>Florian Mendel and Tomislav Nad</i>	

Lightweight Implementations of SHA-3 Candidates on FPGAs	270
<i>Jens-Peter Kaps, Panasayya Yalla, Kishore Kumar Surapathi, Bilal Habib, Susheel Vadlamudi, Smriti Gurung, and John Pham</i>	

Pairings

Publicly Verifiable Secret Sharing for Cloud-Based Key Management . . .	290
<i>Roy D'Souza, David Jao, Ilya Mironov, and Omkant Pandey</i>	
On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant	310
<i>Robert Drylo</i>	
Attractive Subfamilies of BLS Curves for Implementing High-Security Pairings	320
<i>Craig Costello, Kristin Lauter, and Michael Naehrig</i>	

Invited Talk 3

Stone Knives and Bear Skins: Why Does the Internet Run on Pre-historic Cryptography? (Abstract)	343
<i>Eric Rescorla</i>	

Protocols

The Limits of Common Coins: Further Results	344
<i>Hemanta K. Maji and Manoj Prabhakaran</i>	
Secure Message Transmission in Asynchronous Directed Graphs	359
<i>Shashank Agrawal, Abhinav Mehta, and Kannan Srinathan</i>	
Towards a Provably Secure DoS-Resilient Key Exchange Protocol with Perfect Forward Secrecy	379
<i>Lakshmi Kuppusamy, Jothi Rangasamy, Douglas Stebila, Colin Boyd, and Juan Gonzalez Nieto</i>	

Tutorial 3

Software Optimizations for Cryptographic Primitives on General Purpose x86_64 Platforms	399
<i>Shay Gueron</i>	

Author Index	401
-------------------------------	-----