

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 of Computer Science, Saarbruecken, Germany

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

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

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

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

Table of Contents

Post-Quantum Cryptology

Secure Parameters for SWIFFT.....	1
<i>Johannes Buchmann and Richard Lindner</i>	
FSBday: Implementing Wagner's Generalized Birthday Attack against the SHA-3 Round-1 Candidate FSB	18
<i>Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, Christiane Peters, and Peter Schwabe</i>	

Key Agreement Protocols

Reusing Static Keys in Key Agreement Protocols	39
<i>Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu</i>	
A Study of Two-Party Certificateless Authenticated Key-Agreement Protocols	57
<i>Colleen Swanson and David Jao</i>	

Side Channel Attacks

Fault Analysis of Rabbit: Toward a Secret Key Leakage.....	72
<i>Alexandre Berzati, Cécile Canovas-Dumas, and Louis Goubin</i>	
On Physical Obfuscation of Cryptographic Algorithms	88
<i>Julien Bringer, Hervé Chabanne, and Thomas Icart</i>	
Cache Timing Attacks on Clefia	104
<i>Chester Rebeiro, Debdeep Mukhopadhyay, Junko Takahashi, and Toshinori Fukunaga</i>	

Symmetric Cryptology

Software Oriented Stream Ciphers Based upon FCSRs in Diversified Mode.....	119
<i>Thierry P. Berger, Marine Minier, and Benjamin Pousse</i>	
On the Symmetric Negabent Boolean Functions.....	136
<i>Sumanta Sarkar</i>	
Improved Meet-in-the-Middle Attacks on AES	144
<i>Hüseyin Demirci, İhsan Taşkın, Mustafa Çoban, and Adnan Baysal</i>	

Hash Functions

Related-Key Rectangle Attack of the Full HAS-160 Encryption Mode . . .	157
<i>Orr Dunkelman, Ewan Fleischmann, Michael Gorski, and Stefan Lucks</i>	
Second Preimage Attack on SHAMATA-512	169
<i>Kota Ideguchi and Dai Watanabe</i>	
Towards Secure and Practical MACs for Body Sensor Networks	182
<i>Zheng Gong, Pieter Hartel, Svetla Nikova, and Bo Zhu</i>	
Indifferentiability Characterization of Hash Functions and Optimal Bounds of Popular Domain Extensions	199
<i>Rishiraj Bhattacharyya, Avradip Mandal, and Mridul Nandi</i>	
A Distinguisher for the Compression Function of SIMD-512	219
<i>Florian Mendel and Tomislav Nad</i>	

Number Theoretic Cryptology

Sampling from Signed Quadratic Residues: RSA Group Is Pseudofree . . .	233
<i>Mahabir Prasad Jhanwar and Rana Barua</i>	
Software Implementation of Pairing-Based Cryptography on Sensor Networks Using the MSP430 Microcontroller	248
<i>Conrado Porto Lopes Gouvêa and Julio López</i>	
A New Hard-Core Predicate of Paillier's Trapdoor Function	263
<i>Dong Su and Kewei Lv</i>	

Lightweight Cryptology

Private Interrogation of Devices via Identification Codes	272
<i>Julien Bringer, Hervé Chabanne, Gérard Cohen, and Bruno Kindarji</i>	
RFID Distance Bounding Multistate Enhancement	290
<i>Gildas Avoine, Christian Floerkemeier, and Benjamin Martin</i>	
Two Attacks against the F_f RFID Protocol	308
<i>Olivier Billet and Kaoutar Elkhyaoui</i>	

Signature Protocols

Efficient Constructions of Signcryption Schemes and Signcryption Composability	321
<i>Takahiro Matsuda, Kanta Matsuura, and Jacob C.N. Schuldt</i>	

On Generic Constructions of Designated Confirmer Signatures: The “Encryption of a Signature” Paradigm Revisited	343
<i>Laila El Aimagi</i>	
Verifiably Encrypted Signatures from RSA without NIZKs	363
<i>Markus Rückert</i>	
Identity Based Aggregate Signcryption Schemes	378
<i>S. Sharmila Deva Selvi, S. Sree Vivek, J. Shriram, S. Kalaivani, and C. Pandu Rangan</i>	
Multiparty Computation	
Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience	398
<i>Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i>	
Non-committing Encryptions Based on Oblivious Naor-Pinkas Cryptosystems	418
<i>Huafei Zhu and Feng Bao</i>	
Oblivious Multi-variate Polynomial Evaluation	430
<i>Gérald Gavin and Marine Minier</i>	
Author Index	443