

*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

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, 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*

Dipanwita Roy Chowdhury Vincent Rijmen  
Abhijit Das (Eds.)

# Progress in Cryptology – INDOCRYPT 2008

9th International Conference on Cryptology in India  
Kharagpur, India, December 14-17, 2008  
Proceedings

## Volume Editors

Dipanwita Roy Chowdhury

Abhijit Das

Dept. of Computer Science and Engineering

Indian Institute of Technology, Kharagpur 721 302, India,

E-mail: {drc, abhij@cse.iitkgp.ernet.in}

Vincent Rijmen

K.U. Leuven, ESAT/COSIC

Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium

E-mail: Vincent.Rijmen@esat.kuleuven.be

Library of Congress Control Number: 2008940079

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4, F.2.1-2, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-89753-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-89753-8 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 is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008

Printed in Germany

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

Printed on acid-free paper SPIN: 12572953 06/3180 5 4 3 2 1 0

# Message from the General Chairs

The 2008 International Conference on Cryptology in India (INDOCRYPT 2008) was the ninth event in this series. It was organized by the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, in co-operation with the Cryptology Research Society of India (CRSI). Over the years, INDOCRYPT has become a leading forum for disseminating the latest research results in cryptology. This year's conference brought together leading and eminent researchers worldwide in Kharagpur (India), during December 14–17, 2008, to present and discuss a wide variety of aspects on cryptology and security.

The program of the conference spanned over four days and included, in addition to a high-quality technical program, two tutorials delivered by the very best in the field, giving young researchers and students an excellent opportunity to learn about the latest trends in cryptography and cryptanalysis.

A conference of this magnitude would not have been possible without the hard and excellent work of all the members of the Organizing Committee. Our special thanks are due to Dipanwita Roy Chowdhury and Vincent Rijmen (Program Co-chairs) for coordinating and leading the effort of the Program Committee, culminating in an excellent technical program. We are grateful to the Tutorial Chair, Debdeep Mukhopadhyay, for arranging two high-quality tutorial talks by eminent leaders in the field.

We are indebted to all other members of the Organizing Committee for their excellent work. Dilip Kumar Nanda (Organizing Chair) along with his team coordinated all the local arrangements with elan. Abhijit Das (Publication Chair) managed the publication of the conference proceedings through his tireless efforts. We also take this opportunity to acknowledge the contributions of the Publicity Chair (Soumen Maity) and of the Finance Chair (Raja Datta) to the success of the conference. No amount of thanks is sufficient for the omnipresent team of enthusiastic volunteers who did their best for the smooth sailing of the conference.

Last but not the least, we extend our heartfelt thanks to the authors, the reviewers, the participants, and the sponsors of the conference, for their vital contributions to the success of the event.

December 2008

Indranil Sen Gupta  
Bimal K. Roy

# Message from the Technical Program Chairs

Welcome to the Proceedings of the 9th International Conference on Cryptology, INDOCRYPT 2008. This annual event started off eight 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 111 papers from all over the world. After a rigorous review process, the Program Committee selected 33 papers out of the 111 submissions. Most of the papers received at least three independent reviews made by the Program Committee members and also by additional external experts. The papers along with the reviews were scrutinized by the Program Committee members during a two-week 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 the external reviewers who gave their precious time in reviewing and selecting the best set of papers.

We are fortunate to have several eminent researchers as keynote and invited speakers. The main conference program was preceded by a day of tutorial presentations. We would like to thank Debdeep Mukhopadhyay, the Tutorial Chair, for his active initiation and enthusiasm to make the tutorial sessions a success. We would like to express our thanks to Abhijit Das, the Publication Chair, who gave his precious time to compile the conference proceedings. Further, we thank Anirban Sarkar, who helped with the setting up and maintenance of the conference Web server.

We hope that you will find the INDOCRYPT 2008 proceedings technically rewarding.

December 2008

Dipanwita Roy Chowdhury  
Vincent Rijmen

# Organization

## General Chairs

Indranil Sen Gupta	Indian Institute of Technology, Kharagpur, India
Bimal K. Roy	Indian Statistical Institute, Kolkata, India

## Program Chairs

Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Vincent Rijmen	KU Leuven, Belgium and Graz University of Technology, Austria

## Tutorial Chair

Debdeep Mukhopadhyay	Indian Institute of Technology, Kharagpur, India
----------------------	--

## Publication Chair

Abhijit Das	Indian Institute of Technology, Kharagpur, India
-------------	--

## Organizing Chair

Dilip K. Nanda	Indian Institute of Technology, Kharagpur, India
----------------	--

## Publicity Chair

Soumen Maity	Indian Institute of Technology, Kharagpur, India
--------------	--

## Finance Chair

Raja Datta	Indian Institute of Technology, Kharagpur, India
------------	--

## Program Committee

Abhijit Das	IIT Kharagpur, India
Alex Biryukov	Univ. du Luxembourg, Luxembourg
Alfred Menezes	University of Waterloo, Canada
Anne Canteaut	INRIA, France
Arjen K. Lenstra	EPFL, Switzerland and Alcatel-Lucent Bell Laboratories, USA
Bimal K. Roy	ISI Kolkata, India

C. Pandu Rangan	IIT Madras, India
C.E. Veni Madhavan	IISC Bangalore, India
Çetin Kaya Koç	Oregon State University, USA
Chandan Mazumdar	Jadavpur University, Kolkata, India
Charanjit S. Jutla	IBM T.J. Watson Research Center, USA
Christian Rechberger	Graz University of Technology, Austria
Dan Page	University of Bristol, UK
Debdeep Mukhopadhyay	IIT Kharagpur, India
Dipanwita Roy Chowdhury	IIT Kharagpur, India
Helger Lipmaa	Cybernetica AS, Estonia
Indranil Sen Gupta	IIT Kharagpur, India
Ingrid Verbauwhede	ESAT, KU Leuven, Belgium
Jennifer Seberry	University of Wollongong, Australia
Joan Daemen	ST Microelectronics, Belgium
Josef Pieprzyk	Macquarie University, Australia
Jovan Golic	Security Innovation, Telecom Italia, Turin, Italy
Keith Martin	University of London, UK
Kolin Paul	IIT Delhi, India
Matt Robshaw	Orange Labs, France
Matthew Parker	University of Bergen, Norway
Paulo Barreto	University of Sao Paulo, Brazil
Pramod K. Saxena	SAG, New Delhi, India
R. Balasubramaniam	IMSc, Chennai, India
Ramarathnam Venkatesan	Microsoft, Redmond, USA
Rei Safavi-Naini	University of Wollongong, Australia
Sanjay Barman	CAIR, Bangalore, India
Shiho Moriai	Sony Computer Entertainment Inc., Japan
Soumen Maity	IIT Kharagpur, India
Subhamoy Maitra	ISI Kolkata, India
Svetla Nikova	KU Leuven, Belgium
Tanja Lange	Technische Universiteit Eindhoven, The Netherlands
Tor Helleseeth	University of Bergen, Norway
Vincent Rijmen	KU Leuven, Belgium and Graz University of Technology, Austria
Willi Meier	FHNW, Switzerland

## Additional Referees

Andrey Bogdanov	Benoit Libert	Goutam Paul
Angela Piper	Berry Schoenmakers	Håvard Raddum
Arpita Patra	Christophe Clavier	Jaydeb Bhowmik
Arun K. Majumdar	Christian Kraetzer	Jeff Hoffstein
Ashish Choudhary	Florian Mendel	Jean-Philippe Aumasson
Avishek Adhikari	Geong Sen Poh	Joonsang Baek

Juraj Sarinay	Nathan Keller	Sourav Mukhopadhyay
Kanta Matsuura	Nele Mentens	Shahram Khazaei
Kazue Sako	Nicolas Sendrier	Takashi Satoh
Kenny Paterson	Nicolas Gama	Thomas Popp
Kristian Gjøsteen	Nick Howgrave-Graham	Tomislav Nad
Lejla Batina	Noboru Kunihiro	Tomoyuki Asano
Mahabir Prasad Jhanwar	Onur Ozen	Toshihiro Ohigashi
Marc Stevens	Pim Tuyls	Tor Erling Bjørstad
Matrin Gagné	Sanjit Chatterjee	Vipul Goyal
Martin Schläffer	Safuat Hamdy	Yannick Seurin
Maura Paterson	Sébastien Canard	Yong Ki Lee
Miroslav Knežević	Sebastiaan Faust	Yunlei Zhao
Mridul Nandy	Somitra Kumar	
Michael Naehrig	Sanadhya	



# Table of Contents

## Stream Ciphers

Slid Pairs in Salsa20 and Trivium .....	1
<i>Deike Priemuth-Schmid and Alex Biryukov</i>	
New Directions in Cryptanalysis of Self-synchronizing Stream Ciphers .....	15
<i>Shahram Khazaei and Willi Meier</i>	
Analysis of RC4 and Proposal of Additional Layers for Better Security Margin .....	27
<i>Subhamoy Maitra and Goutam Paul</i>	
New Results on the Key Scheduling Algorithm of RC4 .....	40
<i>Mete Akgün, Pınar Kavak, and Hüseyin Demirci</i>	

## Cryptographic Hash Functions

Two Attacks on RadioGatún .....	53
<i>Dmitry Khovratovich</i>	
Faster Multicollisions .....	67
<i>Jean-Philippe Aumasson</i>	
A New Type of 2-Block Collisions in MD5 .....	78
<i>Jiří Vábek, Daniel Jošćák, Milan Boháček, and Jiří Tůma</i>	
New Collision Attacks against Up to 24-Step SHA-2 (Extended Abstract) .....	91
<i>Somitra Kumar Sanadhya and Palash Sarkar</i>	

## Public-Key Cryptography – I

Secure Hierarchical Identity Based Encryption Scheme in the Standard Model .....	104
<i>Yanli Ren and Dawu Gu</i>	
A Fuzzy ID-Based Encryption Efficient When Error Rate Is Low .....	116
<i>Jun Furukawa, Nuttapong Attrapadung, Ryuichi Sakai, and Goichiro Hanaoka</i>	
Type-Based Proxy Re-encryption and Its Construction .....	130
<i>Qiang Tang</i>	

Toward a Generic Construction of Universally Convertible Undeniable Signatures from Pairing-Based Signatures .....	145
<i>Laila El Aimagi</i>	

## Security Protocols

Concrete Security for Entity Recognition: The Jane Doe Protocol .....	158
<i>Stefan Lucks, Erik Zenner, André Weimerskirch, and Dirk Westhoff</i>	
Efficient and Strongly Secure Password-Based Server Aided Key Exchange (Extended Abstract) .....	172
<i>Kazuki Yoneyama</i>	
Round Efficient Unconditionally Secure Multiparty Computation Protocol .....	185
<i>Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i>	
A New Anonymous Password-Based Authenticated Key Exchange Protocol .....	200
<i>Jing Yang and Zhenfeng Zhang</i>	
Group Key Management: From a Non-hierarchical to a Hierarchical Structure .....	213
<i>Sébastien Canard and Amandine Jambert</i>	

## Hardware Attacks

Scan Based Side Channel Attacks on Stream Ciphers and Their Counter-Measures .....	226
<i>Mukesh Agrawal, Sandip Karmakar, Dhiman Saha, and Debdeep Mukhopadhyay</i>	
Floating Fault Analysis of Trivium .....	239
<i>Michal Hojsík and Bohuslav Rudolf</i>	
Algebraic Methods in Side-Channel Collision Attacks and Practical Collision Detection .....	251
<i>Andrey Bogdanov, Ilya Kizhvatov, and Andrey Pyshkin</i>	

## Block Ciphers

New Related-Key Boomerang Attacks on AES .....	266
<i>Michael Gorski and Stefan Lucks</i>	
New Impossible Differential Attacks on AES .....	279
<i>Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim</i>	

Reflection Cryptanalysis of Some Ciphers .....	294
<i>Orhun Kara</i>	
A Differential-Linear Attack on 12-Round Serpent.....	308
<i>Orr Dunkelman, Sebastiaan Indestege, and Nathan Keller</i>	
New AES Software Speed Records .....	322
<i>Daniel J. Bernstein and Peter Schwabe</i>	

## Public-Key Cryptography – II

A New Class of Weak Encryption Exponents in RSA .....	337
<i>Subhamoy Maitra and Santanu Sarkar</i>	
Two New Efficient CCA-Secure Online Ciphers: MHCBC and MCBC...	350
<i>Mridul Nandi</i>	

## Cryptographic Hardware

Chai-Tea, Cryptographic Hardware Implementations of xTEA .....	363
<i>Jens-Peter Kaps</i>	
High Speed Compact Elliptic Curve Cryptoprocessor for FPGA Platforms .....	376
<i>Chester Rebeiro and Debdeep Mukhopadhyay</i>	

## Elliptic Curve Cryptography

More Discriminants with the Brezing-Weng Method .....	389
<i>Gaetan Bisson and Takakazu Satoh</i>	
Another Approach to Pairing Computation in Edwards Coordinates ....	400
<i>Sorina Ionica and Antoine Joux</i>	

## Threshold Cryptography

A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem .....	414
<i>Kamer Kaya and Ali Aydın Selçuk</i>	
Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority .....	426
<i>Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao</i>	

<b>Author Index</b> .....	437
---------------------------	-----