

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

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

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Anne Canteaut
Kapaleeswaran Viswanathan (Eds.)

Progress in Cryptology – INDOCRYPT 2004

5th International Conference on Cryptology in India
Chennai, India, December 20-22, 2004
Proceedings

Volume Editors

Anne Canteaut

Institut National de Recherche en Informatique et Automatique (INRIA)

Projet CODES, Domaine de Voluceau, Rocquencourt

78153 Le Chesnay Cedex, France

E-mail: anne.canteaut@inria.fr

Kapaleeswaran Viswanathan

SETS, 21 Mangadu Swamy Street, Nungambakkam

Chennai 600 034, India

E-mail: kapali@sets.org.in

Library of Congress Control Number: 2004116723

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

ISSN 0302-9743

ISBN 3-540-24130-2 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

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

Printed on acid-free paper SPIN: 11369165 06/3142 5 4 3 2 1 0

Preface

The INDOCRYPT series of conferences started in 2000. INDOCRYPT 2004 was the fifth one in this series. The popularity of this series is increasing every year. The number of papers submitted to INDOCRYPT 2004 was 181, out of which 147 papers conformed to the specifications in the call for papers and, therefore, were accepted to the review process. Those 147 submissions were spread over 22 countries.

Only 30 papers were accepted to this proceedings. We should note that many of the papers that were not accepted were of good quality but only the top 30 papers were accepted. Each submission received at least three independent reviews. The selection process also included a Web-based discussion phase. We made efforts to compare the submissions with other ongoing conferences around the world in order to ensure detection of double-submissions, which were not allowed by the call for papers. We wish to acknowledge the use of the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens in conducting the review process electronically. The software greatly facilitated the Program Committee in completing the review process on time. We would like to thank Cédric Lauradoux and the team at INRIA for their total support in configuring and managing the Web-based submission and review softwares. We are unable to imagine the outcome of the review process without their participation.

This year the invited talks were presented by Prof. Colin Boyd and Prof. Amit Sahai. Colin provided a talk on the design of key establishment protocols while Amit presented a talk on secure protocols for complex tasks in complex environments. They presented two sides of the same coin so that the audience can gain a more comprehensive view of the analysis and design of cryptographic protocols. We hope that the invited talks contributed their share to promoting such an exciting area in cryptology research in India. At the same time, the invited talks were of great value for international researchers, as well, because Colin and Amit shared the latest results of their research activities.

The smooth and successful progress of INDOCRYPT 2004 was due to the efforts of many individuals. The members of the Program Committee worked hard throughout, and did an excellent job. Many external reviewers contributed their time and expertise to aid our decision-making. The Organizing Committee put its maximal effort into ensuring the successful progress of this conference. We wish to thank Prof. R. Balasubramaniam and Dr. M.S. Vijayaraghavan for being the general co-chairs of this conference. We also thank the Cryptology Research Society of India and ISI, Calcutta.

We hope that the INDOCRYPT series of conferences remains a forum for discussing high-quality results in the area of cryptology and its applications to information security in the years to come.

December 2004

Anne Canteaut
Kapaleeswaran Viswanathan

Organization

The INDOCRYPT Conferences are the annual events of the Cryptology Research Society of India. INDOCRYPT 2004 was organized by IMSc, Chennai, and SETS, Chennai.

General Co-chairs

R. Balasubramanian	Institute for Mathematical Sciences, India
M.S. Vijayaraghavan	SETS, India

Program Co-chairs

Anne Canteaut	INRIA, France
Kapaleeswaran Viswanathan	SETS, India

Program Committee

Michael Backes	IBM, Zurich, Switzerland
Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA, France
Cunsheng Ding	Hong Kong University of Science and Technology, China
Andreas Enge	Ecole Polytechnique, France
Caroline Fontaine	CNRS, France
Henri Gilbert	France Telecom R&D, France
Juanma Gonzalez-Nieto	Queensland University of Technology, Australia
Tor Helleseeth	University of Bergen, Norway
Thomas Johansson	Lund University, Sweden
Kwangjo Kim	Information and Communications University, Korea
Tanja Lange	University of Bochum, Germany
Arjen Lenstra	Lucent Technologies, USA and Technische Universiteit Eindhoven, The Netherlands
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
Keith Martin	Royal Holloway University of London, UK
Anish Mathuria	Dhirubhai Ambani, Institute of Information and Communication Technology, India

VIII Organization

Alfred Menezes	University of Waterloo, Canada
Shiho Moriai	Sony Computer Entertainment Inc., Japan
Kenneth Paterson	Royal Holloway University of London, UK
Kapil H. Paranjape	IMSc, Chennai, India
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Bimal Roy	ISI Kolkata, India
Amit Sahai	Princeton University, USA
Palash Sarkar	ISI Kolkata, India
Henk van Tilborg	Technische Universiteit Eindhoven, The Netherlands
D.G. Thomas	Madras Christian College, India
Kapaleeswaran Viswanathan	SETS, Chennai, India
Adam Young	Cigital Labs, USA
Moti Yung	Columbia University, USA

Organizing Committee

Dr. A.K. Chakravarthy	Dept. of IT, MICT, Govt. of India
Mr. Cédric Lauradoux	INRIA, France
Dr. K. Srinivas	IMSc, India
Dr. N.Vijayarangan	SETS, India

Organizing Sub-committee

Mr. G. Aswin	SETS, India
Mr. C. Stephen Balasundaram	SETS, India
Mr. Manish Chauhan	SETS, India
Ms. R. Indra	IMSc, India
Ms. K. Jayasri	SETS, India
Mr. R. Harish Kumar	SETS, India
Mr. Ramakrishna Manja	IMSc, India
Dr. Paul Pandian	IMSc, India
Mr. Vishnu Prasath	IMSc, India
Ms. A. Suganya	SETS, India
Mr. R. Vijayasathy	SETS, India

External Referees

P.J. Abisha	Sattam Al-Riyami	Florent Bersani
Avishek Adhikari	Lejla Batina	Alex Biryukov
Riza Aditya	Côme Berbain	Simon Blackburn
Toru Akishita	Thierry Berger	Emmanuel Bresson

Jan Camenisch	Ellen Jochemsz	Zulfikar Ramzan
Liqun Chen	Stefan Katzenbeisser	K. Rangarajan
Olivier Chevassut	Alexander Kholosha	François Recher
Matthijs Coster	Caroline Kudla	Akashi Satoh
Deepak Kumar Dalai	Joseph Lano	Werner Schindler
V. Rajkumar Dare	Hyunrok Lee	Takeshi Shimoyama
Christophe De Cannière	Kerstin Lemke	Taizo Shirai
Alex Dent	Benoît Libert	Jamshid Shokrollahi
Jeroen Doumen	Vo Duc Liem	Hervé Sibert
Dang Nguyen Duc	Phil MacKenzie	Francesco Sica
Sylvain Duquesne	John Malone-Lee	Andrey Sidorenko
Håkan Englund	Alexander Maximov	Martijn Stam
Steven Galbraith	Nele Mentens	Tsuyoshi Takagi
Pierrick Gaudry	Chris Mitchell	Gerard Tel
Daniel Gottesman	Suman K. Mitra	Yuuki Tokunaga
Robert Granger	François Morain	Ludo Tolhuizen
Kishan Chand Gupta	Sumio Morioka	Emmanuel Thomé
Darrel Hankerson	Joern Mueller-Quade	Pim Tuyls
Guillaume Hanrot	James Muir	M.K. Viswanath
Martin Hell	Svetla Nikova	Brent Waters
Clemens Heuberger	Luke O'Connor	Benne de Weger
Shoichi Hirose	Siddika Berna Ors	Annegret Weng
Yvonne Hitchcock	Daniel Page	Arne Winterhof
Dennis Hofheinz	Matthew Parker	Christopher Wolf
Tetsu Iwata	Olivier Pereira	Robbie Ye
Cees Jansen	Håvard Raddum	Feng Zhu

Sponsoring Institutions

Bharat Electronics Limited
 BRNS Secretariat, Bhabha Atomic Research Centre
 Department of Information Technology, Government of India
 Department of Science and Technology, Government of India
 Electronics Corporation of India Limited
 Hewlett Packard India Private Limited
 Institute for Development and Research in Banking Technology
 NASSCOM
 SLN Technologies Private Limited
 Sun Microsystems India Private Limited

Table of Contents

Invited Talks

Design of Secure Key Establishment Protocols: Successes, Failures and Prospects <i>Colin Boyd</i>	1
Secure Protocols for Complex Tasks in Complex Environments <i>Amit Sahai</i>	14

Cryptographic Protocols

Tripartite Key Exchange in the Canetti-Krawczyk Proof Model <i>Yvonne Hitchcock, Colin Boyd, Juan Manuel González Nieto</i>	17
The Marriage Proposals Problem: Fair and Efficient Solution for Two-Party Computations <i>Audrey Montreuil, Jacques Patarin</i>	33

Applications

On the Security of a Certified E-Mail Scheme <i>Guilin Wang, Feng Bao, Jianying Zhou</i>	48
Multiplicative Homomorphic E-Voting <i>Kun Peng, Riza Aditya, Colin Boyd, Ed Dawson, Byoungcheon Lee</i>	61

Stream Ciphers

Chosen Ciphertext Attack on a New Class of Self-Synchronizing Stream Ciphers <i>Bin Zhang, Hongjun Wu, Dengguo Feng, Feng Bao</i>	73
Algebraic Attacks Over $GF(q)$ <i>Lynn Margaret Batten</i>	84

Cryptographic Boolean Functions

Results on Algebraic Immunity for Cryptographically Significant Boolean Functions

Deepak Kumar Dalai, Kishan Chand Gupta, Subhamoy Maitra 92

Generalized Boolean Bent Functions

Laurent Poinot, Sami Harari 107

On Boolean Functions with Generalized Cryptographic Properties

An Braeken, Ventzislav Nikov, Svetla Nikova, Bart Preneel 120

Foundations

Information Theory and the Security of Binary Data Perturbation

Poorvi L. Vora 136

Symmetric Authentication Codes with Secrecy and Unconditionally Secure Authenticated Encryption

Luke McAven, Reihaneh Safavi-Naini, Moti Yung 148

Block Ciphers

Faster Variants of the MESH Block Ciphers

Jorge Nakahara Júnior 162

Related-Key Attacks on Reduced Rounds of SHACAL-2

Jongsung Kim, Guil Kim, Sangjin Lee, Jongin Lim, Junghwan Song 175

Related-Key Attacks on DDP Based Ciphers: CIKS-128 and CIKS-128H

Youngdai Ko, Changhoon Lee, Seokhie Hong, Jaechul Sung, Sangjin Lee 191

Cryptanalysis of Ake98

Jorge Nakahara Júnior, Daniel Santana de Freitas 206

Public Key Encryption

Designing an Efficient and Secure Public-Key Cryptosystem Based on Reducible Rank Codes

Thierry Berger, Pierre Loidreau 218

HEAD: Hybrid Encryption with Delegated Decryption Capability <i>Palash Sarkar</i>	230
A Provably Secure Elliptic Curve Scheme with Fast Encryption <i>David Galindo, Sebastià Martín, Tsuyoshi Takagi,</i> <i>Jorge L. Villar</i>	245

Efficient Representations

Advances in Alternative Non-adjacent Form Representations <i>Gildas Avoine, Jean Monnerat, Thomas Peyrin</i>	260
---	-----

Public Key Cryptanalysis

Attacks on Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups <i>Françoise Levy-dit-Vehel, Ludovic Perret</i>	275
Exact Analysis of Montgomery Multiplication <i>Hisayoshi Sato, Daniel Schepers, Tsuyoshi Takagi</i>	290
Cryptography, Connections, Cocycles and Crystals: A p-Adic Exploration of the Discrete Logarithm Problem <i>H. Gopalkrishna Gadiyar, KM Sangeeta Maini, R. Padma</i>	305

Modes of Operation

EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data <i>Shai Halevi</i>	315
Impossibility of Construction of OWHF and UOWHF from PGV Model Based on Block Cipher Secure Against ACPA <i>Donghoon Chang, Wonil Lee, Seokhie Hong, Jaechul Sung,</i> <i>Sangjin Lee, Soohak Sung</i>	328
The Security and Performance of the Galois/Counter Mode (GCM) of Operation <i>David A. McGrew, John Viega</i>	343

Signatures

Revisiting Fully Distributed Proxy Signature Schemes
Javier Herranz, Germán Sáez 356

New ID-Based Threshold Signature Scheme from Bilinear Pairings
Xiaofeng Chen, Fangguo Zhang, Divyan M. Konidala, Kwangjo Kim 371

Separable Linkable Threshold Ring Signatures
Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, Duncan S. Wong 384

Traitor Tracing and Visual Cryptography

A New Black and White Visual Cryptographic Scheme for General Access Structures
Avishek Adhikari, Tridib Kumar Dutta, Bimal Roy 399

Identification Algorithms for Sequential Traitor Tracing
Marcel Fernandez, Miguel Soriano 414

Author Index 431