Lecture Notes in Computer Science 3797

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

Subhamoy Maitra C.E. Veni Madhavan
Ramarathnam Venkatesan (Eds.)

Progress in Cryptology – INDOCRYPT 2005

6th International Conference on Cryptology in India
Bangalore, India, December 10-12, 2005
Proceedings

Springer

Volume Editors

Subhamoy Maitra
Indian Statistical Institute, Applied Statistics Unit
203 B T Road, Kolkata 700 108, India
E-mail: subho@isical.ac.in

C.E. Veni Madhavan
Indian Institute of Science (IISc)
Department of Computer Science and Automation (CSA)
Bangalore 560 012, India
E-mail: cevm@csa.iisc.ernet.in

Ramarathnam Venkatesan
Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA
E-mail: venkie@microsoft.com

Library of Congress Control Number: 2005936804

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

ISSN 0302-9743
ISBN-10 3-540-30805-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30805-8 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11596219 06/3142 5 4 3 2 1 0

Preface

Indocrypt began in the year 2000 under the leadership of Bimal Roy and Indocrypt 2005 was the sixth conference in this series. This series has been well accepted by the international research community as a forum for presenting high-quality cryptography research. This year a total of 148 papers were submitted for consideration to the Program Committee and after a careful review process, 31 were accepted for presentation. We would like to thank the authors of all submitted papers, including those that were accepted and those which, unfortunately, could not be accommodated.

The reviewing process for Indocrypt was very stringent and the schedule was extremely tight. The Program Committee members did an excellent job in reviewing and selecting the papers for presentation. During the review process, the Program Committee members were communicating using a review software developed by Bart Preneel, Wim Moreau and Joris Claessens. We acknowledge them for providing the software. The software was hosted at I2R, Singapore and we are grateful to Feng Bao and Jianying Zhou for allowing that. This year's conference was deeply indebted to Qiu Ying of I2R, Singapore, who took the responsibility of maintaining the review software and the server. Without his great cooperation Indocrypt 2005 could not have been possible. In this regard I would like to acknowledge the support of Tanmoy Kanti Das, Dibyendu Chakrabarti, Mridul Nandi, Deepak Kumar Dalai, Sumanta Sarkar and Sourav Mukhopadhyay for handling important administrative issues in the submission and review processes as well as for putting together these proceedings in their final form. We are also grateful to Palash Sarkar for his cooperation and guidance in Indocrypt 2005.

The proceedings include the revised versions of the 31 selected papers. Revisions were not checked by the Program Committee and the authors bear the full responsibility for the contents of the respective papers. Our thanks go to all the Program members and the external reviewers (a list of them is included in the proceedings) who put in their valuable time and effort in providing important feedback to the authors. We thank V. Kumar Murty of the University of Toronto for kindly agreeing to present the invited talk. The talk has been included in the proceedings.

The organization of the conference involved many individuals. We express our heartfelt gratitude to the general Co-chairs K. Gopinath and Soumyendu Raha for taking care of the actual hosting of the conference. They were ably assisted by Kumar Swamy H.V. and the members of the Organizing Committee. There was also invaluable secretarial support from CAS Laboratory, Informatics Laboratory (CSA department) and IMI at the Indian Institute of Science, Bangalore. Finally, we would like to acknowledge Springer for active cooperation and timely production of the proceedings.

December 2005

Subhamoy Maitra
C. E. Veni Madhavan
Ramarathnam Venkatesan

Organization

Indocrypt 2005 was organized by the Indian Institute of Science, Bangalore, in collaboration with the Cryptology Research Society of India.

General Co-chairs

K. Gopinath	Indian Institute of Science, Bangalore
Soumyendu Raha	Indian Institute of Science, Bangalore

Program Co-chairs

Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
C. E. Veni Madhavan	Indian Institute of Science, Bangalore, India
Ramarathnam Venkatesan	Microsoft Corporation, Redmond, USA

Program Committee

V. Arvind	Institute of Mathematical Sciences Chennai, India
R. Balasubramanian	Institute of Mathematical Sciences Chennai, India
Feng Bao	Institute for Infocomm Research, Singapore
Alex Biryukov	K. U. Leuven (ESAT, COSIC group), Belgium
Xavier Boyen	Voltage Security, USA
Mathieu Ciet	Gemplus International, SA, France
Abhijit Das	Indian Institute of Technology, Kharagpur, India
Anand Desai	NTT, MCL, USA
Josep Domingo-Ferrer	Rovira i Virgili University of Tarragona, Catalonia
Orr Dunkelman	Technion, Israel
Caroline Fontaine	Universitè des Sciences et Technologies de Lille - CNRS, France
Sugata Gangopadhyay	Indian Institute of Technology, Roorkee, India
Guang Gong	University of Waterloo, Canada

Kishan Chand Gupta	University of Waterloo, Canada
Tor Helleseth	University of Bergen, Norway
David Jao	Microsoft Research, USA
Andrew Klapper	University of Kentucky, USA
Kaoru Kurosawa	Ibaraki University, Japan
Tanja Lange	Technical University of Denmark, Denmark
John Malone-Lee	University of Bristol, UK
Francoise Levy-dit-Vehel	Ècole Nationale Supérieure des Techniques Avancées, France
Yucel D. Melek	METU Cryptology Institute, Turkey
Pradeep Kumar Mishra	University of Calgary, Canada
François Morain	Laboratoire d'Informatique de l' Ècole Polytechnique, France
Harald Niederreiter	National University of Singapore, Singapore
Rafail Ostrovsky	UCLA, USA
Enes Pasalic	Technical University of Denmark, Denmark
Josef Pieprzyk	Macquarie University, Australia
Zulfikar Ramzan	NTT DoCoMo USA Labs, USA
Pandu Rangan	Indian Institute of Technology Madras, India
Bimal Roy	Indian Statistical Institute, Kolkata, India
Rei Safavi-Naini	University of Wollongong, Australia
Pramod Saxena	SAG, India
Abhi Shelat	IBM, Zurich, Switzerland
Pante Stanica	Auburn University, Montgomery, USA
Berk Sunar	Worcester Polytechnic Institute, USA
Yuriy Tarannikov	Moscow State University, Russia
Moti Yung	Columbia University, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

External Referees

Michel Abdalla
Masayuki Abe
Raju Agarwal
Carlos Aguilar
Mehdi-Laurent Akkar
Ersan Akyildiz
Shirish Altekar
Tomoyuki Asano
Daniel Augot
Joonsang Baek
Selcuk Baktir
Sverine Baudry
S.S. Bedi
Kamel Bentahar
Raghav Bhaskar
Lilian Bohy
Alexandra Boldyreva
Colin Boyd
Eric Brier
Philippe Bulens
Christophe De Canniere
Jordi Castellà-Roca
Julien Cathalo
Liqun Chen
Joe Cho
Scott Contini
Thomas W. Cusick
Tanmoy Kanti Das
Guerric Meurice de Dormale
Ali Doianaksoy
R. Dupont
Sylvain Duquesne
Adam Elbirt
Haining Fan
Matthew J. Fanto
Pooya Farshim
Benot Feix
Eiichiro Fujisaki

Navneet Gaba
Pierrick Gaudry
Indeevar Gupta
Martin Hell
Javier Herranz
Katrin Hoeper
Susan Hohenberger
Laurent Imbert
Tetsu Iwata
Dimitar P. Jetchev
Shaoquan Jiang
Marc Joye
Pascal Junod
Sarvjeet Kaur
Seluk Kavut
Alexander Kholosha
Takeshi Koshiba
Hugo Krawczyk
Meena Kumari
Noboru Kunihiro
F. Laguillaumie
Joseph Lano
Cedric Lauradoux
Benoit Libert
Moses Liskov
Phil MacKenzie
Frederic Magniez
Dahlia Malkhi
C.R. Mandal
Antoni M.-Balleste
John Erik Mathiassen
Matthew McKague
Alfred Menezes
Jonathan Millen
Sara Miner More
Sourav Mukhopadhyay
Yassir Nawaz
Kazuto Ogawa
Alina Oprea
Elisabeth Oswald
Ferruh Özbudak
Daniel Page
S.K. Pal
Kapil Paranjape
Matthew Parker
Maura Paterson
Roger Patterson
Chris Peikert
Ludovic Perret
Rajesh Pillai
Constantin Popescu
Bart Preneel
Duong Quang Viet
Hvard Raddum
Sibabrata Ray
Jeremie Roland
Pieter Rozenhart
Amit Sahai
Erkay Savas
Hovav Schacham
Kai Schramm
Francesc Sebé
Igor Semaev
Rozenhart Seong
Han Shin
Francesco Sica
Adam Smith
Agustí Solanas
M.C. Srivastava
Martijn Stam
Franois-Xavier Standaert
Ron Steinfeld
Makoto Sugita
Keisuke Tanaka
Adrian Tang
Nicolas Theriault
E. Thomé
Dongvu Tonien
Patrick Traynor
Eran Tromer
Gary Walsh
Huaxiong Wang
Bogdan Warinschi
Eric Wegrzynowski
Kjell Wooding
David Woodruff
Pratibha Yadav
Tugrul Yanik
Bulent Yener
Nam Yul Yu
Huafei Zhu

Table of Contents

Invited Talk

Abelian Varieties and Cryptography
V. Kumar Murty 1

Sequences

Proof of a Conjecture on the Joint Linear Complexity Profile of Multisequences
Harald Niederreiter, Li-Ping Wang 13

Period of Streamcipher *Edon80*
Jin Hong 23

Boolean Function and S-Box

On the Algebraic Immunity of Symmetric Boolean Functions
An Braeken, Bart Preneel 35

On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks
Claude Carlet 49

Hash Functions

How to Construct Universal One-Way Hash Functions of Order r
Deukjo Hong, Jaechul Sung, Seokhie Hong, Sangjin Lee 63

Towards Optimal Double-Length Hash Functions
Mridul Nandi 77

Design Principles

Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries
Souradyuti Paul, Bart Preneel 90

Design Principles for Combiners with Memory
Frederik Armknecht, Matthias Krause, Dirk Stegemann 104

Cryptanalysis I

Cryptanalysis of the Quadratic Generator
Domingo Gomez, Jaime Gutierrez, Alvar Ibeas 118

Attack the Dragon
Håkan Englund, Alexander Maximov 130

Two Algebraic Attacks Against the F-FCSRs Using the IV Mode
Thierry P. Berger, Marine Minier 143

Cryptanalysis of Keystream Generator by Decimated Sample Based Algebraic and Fast Correlation Attacks
Miodrag J. Mihaljević, Marc P.C. Fossorier, Hideki Imai 155

Time Memory Trade-Off

TMD-Tradeoff and State Entropy Loss Considerations of Streamcipher MICKEY
Jin Hong, Woo-Hwan Kim 169

Time-Memory Trade-Offs: False Alarm Detection Using Checkpoints
Gildas Avoine, Pascal Junod, Philippe Oechslin 183

Cryptanalysis II

Cryptanalysis of Barni et al. Watermarking Scheme
Tanmoy Kanti Das, Jianying Zhou 197

Completion Attacks and Weak Keys of Oleshchuk's Public Key Cryptosystem
Heiko Stamer 209

New Constructions

An Optimal Subset Cover for Broadcast Encryption
Sarang Aravamuthan, Sachin Lodha 221

MaTRU: A New NTRU-Based Cryptosystem
Michael Coglianese, Bok-Min Goi 232

Anonymous Password-Based Authenticated Key Exchange
Duong Quang Viet, Akihiro Yamamura, Hidema Tanaka 244

Pairings

Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism
Michael Scott 258

Reconsideration on the Security of the Boneh-Franklin Identity-Based Encryption Scheme
Mototsugu Nishioka 270

Signatures

Short Undeniable Signatures Without Random Oracles: The Missing Link
Fabien Laguillaumie, Damien Vergnaud 283

Short Threshold Signature Schemes Without Random Oracles
Hong Wang, Yuqing Zhang, Dengguo Feng 297

Applications

Attacking an Asynchronous Multi-party Contract Signing Protocol
Jose A. Onieva, Jianying Zhou, Javier Lopez 311

Fairness and Correctness in Case of a Premature Abort
Jens-Matthias Bohli, Jörn Müller-Quade, Stefan Röhrich 322

E-Cash

Short E-Cash
Man Ho Au, Sherman S.M. Chow, Willy Susilo 332

A Universally Composable Scheme for Electronic Cash
Mårten Trolin 347

Implementations

Energy-Privacy Trade-Offs in VLSI Computations
Akhilesh Tyagi 361

Modified Serial Multipliers for Type-IV Gaussian Normal Bases
Chang Han Kim, Yongtae Kim, Nam Su Chang, IlWhan Park 375

Scalar Multiplication on Elliptic Curves Defined over Fields of Small Odd Characteristic
Christophe Negre 389

SCA Resistant Parallel Explicit Formula for Addition and Doubling of Divisors in the Jacobian of Hyperelliptic Curves of Genus 2
Tanja Lange, Pradeep Kumar Mishra 403

Author Index 417