

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

University of California, Los Angeles, CA, 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

Rana Barua Tanja Lange (Eds.)

Progress in Cryptology – INDOCRYPT 2006

7th International Conference on Cryptology in India
Kolkata, India, December 11-13, 2006
Proceedings

Volume Editors

Rana Barua
Indian Statistical Institute
Division of Theoretical Statistics and Mathematics
Kolkata, India
E-mail: rana@isical.ac.in

Tanja Lange
Eindhoven University of Technology
Department of Mathematics and Computer Science
Eindhoven, Netherlands
E-mail: tanja@hyperelliptic.org

Library of Congress Control Number: 2006937160

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 3-540-49767-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49767-7 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 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11941378 06/3142 5 4 3 2 1 0

Preface

Indocrypt 2006, the 7th International Conference on Cryptology in India, took place December 11-13, 2006 in Kolkata, India. As in previous years, it was organized by the Cryptology Research Society of India, and the General Chair Bimal Roy did an excellent job in keeping all strands together by ensuring an excellent collaboration between the local organizers and the Program Committee and making the conference memorable for the talks and the social program.

Two invited lectures were presented at Indocrypt 2006: James L. Massey spoke about *Whither Cryptography?* and Alfred J. Menezes presented *Another Look at "Provable Security". II*, which is a joint work with Neal Koblitz.

The submission deadline for Indocrypt was on August 18 and we received 186 submissions. To give the authors maximal time to modify their papers and at the same time guarantee the maximal review time for the Program Committee, we had separate submission and revision deadlines. After the submission deadline it was no longer possible to submit a new paper and so the PC members could enter the selection phase during which they only got to see the abstracts of the papers. Out of the 186 papers originally submitted, 20 were withdrawn before the revision deadline on August 21 and 81 were revised at least once. Our experience with this approach of separating the deadlines was entirely positive. We would also like to take this opportunity to thank the developers of iChair, Thomas Baignères and Matthieu Finiasz at EPFL, for making iChair available and for answering several questions which allowed us to extend the functionality of iChair to handle separate deadlines. The software was very useful for the submission process, the collection of reviews, and the discussion.

The Program Committee did a remarkable job of finishing refereeing almost all papers by September 8, even though 166 papers marked a new record in submissions. In the following discussion phase many more reports were added and the Program Committee worked intensively to gain confidence in its decisions. The 39 Program Committee members produced 422 comments during the 2 weeks of discussion. It is our pleasure to thank all Program Committee members for their very timely and concentrated effort that allowed us to notify the authors on time on September 22 and even send out the comments the same day.

Finally, we would like to thank all authors for submitting interesting new research papers to Indocrypt, providing us with an embarrassment of riches out of which we could only accept 29 contributed papers, even though many more would have been worth publishing. It is a pleasure to see Indocrypt being a well-accepted cryptography conference where fresh results are submitted.

Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA Rocquencourt, France
Claude Carlet	University of Paris 8, France
Yvo Desmedt	University College London, UK
Orr Dunkelman	Technion - Israel Institute of Technology, Israel
Krishnan Gopalakrishnan	East Carolina University, USA
Kishan C. Gupta	University of Waterloo, Canada
Tom Høholdt	Technical University of Denmark, Denmark
Jin Hong	Seoul National University, Korea
Laurent Imbert	LIRMM, CRNS, France
Tetsu Iwata	Nagoya University, Japan
Antoine Joux	DGA and Université de Versailles Saint-Quentin-en-Yvelines, France
Marc Joye	Thomson R&D France, France
Charanjit Jutla	IBM T.J. Watson Research Center, USA
Chi Sung Lai	National Cheng Kung University, Taiwan
Kerstin Lemke-Rust	Ruhr University Bochum, Germany
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
John Malone-Lee	UK
Pradeep Kumar Mishra	University of Calgary, Canada
Gregory Neven	Katholieke Universiteit Leuven, Belgium and Ecole Normale Supérieure, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
C. Pandu Rangan	Department of Computer Science and Engineering, IIT Madras, India
Bimal Roy	Indian Statistical Institute, Kolkata, India
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Rei Safavi-Naini	University of Wollongong, Australia
Pramod K. Saxena	Scientific Analysis Group, Delhi, India
Jennifer Seberry	University of Wollongong, Australia
Nicolas Sendrier	INRIA Rocquencourt, France
Nigel Smart	University of Bristol, UK
Martijn Stam	EPFL, Switzerland
Bo-Yin Yang	Academia Sinica, Taiwan
Melek D. Yücel	Middle East Technical University, Turkey
Jianying Zhou	Institute for Infocomm Research, Singapore

Referees

Andre Adelsbach	Daniel Augot	Jean-Claude Bajard
Andris Ambainis	Joonsang Baek	Lejla Batina

S.S. Bedi	Tor Helleseth	Michele Mosca
Peter Birkner	Katrin Hoepfer	Mridul Nandi
Carlo Blundo	Susan Hohenberger	Yassir Nawaz
Jean Christian Boileau	Nick Howgrave-Graham	Christophe Negre
Alexandra Boldyreva	Po-Yi Huang	Afonso Araújo Neto
Xavier Boyen	Ulrich Huber	Michael Neve
Emmanuel Bresson	Shaoquan Jiang	Rafail Ostrovsky
Jan Cappaert	Thomas Johansson	Daniel Page
Sanjit Chatterjee	Shri Kant	Pascal Paillier
Liqun Chen	Guruprasad Kar	Saibal K. Pal
Benoit Chevallier-Mames	Stefan Katzenbeisser	Je Hong Park
Jung-Hui Chiu	Jonathan Katz	Kenny Paterson
Yvonne Cliff	John Kelsey	Anindya Patthak
Deepak Kumar Dalai	Dalia Khader	Souradyuti Paul
Ivan Damgaard	Alexander Kholosha	Jan Pelzl
Tanmoy Kanti Das	Eike Kiltz	Kun Peng
Tom St Denis	Lars Ramkilde	Pino Persiano
Alex Dent	Knudsen	Duong Hieu Phan
Vassil Dimitrov	Ulrich Kuehn	N. Rajesh Pillai
Christophe Doche	H.V. Kumar Swamy	Alessandro Piva
Gwenaél Doerr	Meena Kumari	David Pointcheval
Sylvain Duquesne	Sandeep Kumar	Axel Poschmann
Alain Durand	Sébastien Kunz-Jacques	Emmanuel Prouff
Thomas Eisenbarth	Kaoru Kurosawa	Frederic Raynal
Xinxin Fan	Fabien Laguillaumie	Vincent Rijmen
Pooya Farshim	Joseph Lano	Matt Robshaw
Serge Fehr	Cédric Lauradoux	Jörg Rothe
Dacio Luiz Gazzoni Filho	Dong Hoon Lee	Pieter Rozenhart
Caroline Fontaine	Frédéric Lefebvre	Andy Rupp
Pierre-Alain Fouque	Stephane Lemieux	Palash Sarkar
Philippe Gaborit	Arjen K. Lenstra	Berry Schoenmakers
Sebastian Gajek	Pierre-Yvan Liardet	Jörg Schwenk
Fabien Galand	Helger Lipmaa	Siamak Fayyaz
Steven Galbraith	Joseph Liu	Shahandashti
Gagan Garg	Zhijun Li	Nicholas Sheppard
Rosario Gennaro	Pierre Loidreau	Igor Shparlinski
Pascal Giorgi	Spyros Magliveras	Thomas Shrimpton
Philippe Golle	Subhamoy Maitra	Herve Sibert
Louis Goubin	Stéphane Manuel	Francesco Sica
Robert Granger	Mark Manulis	Alice Silverberg
Johannes Groszschädl	Keith Martin	Rainer Steinwandt
Indivar Gupta	Nicolas Meloni	Hung-Min Sun
Robbert de Haan	Sihem Mesnager	V. Suresh
	J. Mohapatra	Michael Szydlo
	Abhradeep Mondal	Adrian Tang

Nicolas Thériault
Soeren S. Thomsen
Dongvu Tonien
Mårten Trolin
Boaz Tsaban
Wen-Guey Tzeng
Damien Vergnaud

Nicolas
Veyrat-Charvillon
Charlotte Vikkelsoe
Ryan Vogt
Melanie Volkamer
Brent Waters
Andreas Westfeld

Kjell Wooding
Hongjun Wu
Brecht Wyseur
Yongjin Yeom
Aaram Yun
Nam Yul Yu
Moti Yung

Sponsoring Institutions

Cranes Software
Microsoft India
Metalogic Systems
Tata Consultancy Services

Table of Contents

Invited Talk

Whither Cryptography?	1
<i>James L. Massey</i>	

Symmetric Cryptography: Attacks

Non-randomness in eSTREAM Candidates Salsa20 and TSC-4.....	2
<i>Simon Fischer, Willi Meier, Côme Berbain, Jean-François Biasse, M.J.B. Robshaw</i>	
Differential and Rectangle Attacks on Reduced-Round SHACAL-1	17
<i>Jiqiang Lu, Jongsung Kim, Nathan Keller, Orr Dunkelman</i>	
Algebraic Attacks on Clock-Controlled Cascade Ciphers.....	32
<i>Kenneth Koon-Ho Wong, Bernard Colbert, Lynn Batten, Sultan Al-Hinai</i>	
An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication.....	48
<i>Marc P.C. Fossorier, Miodrag J. Mihaljević, Hideki Imai, Yang Cui, Kanta Matsuura</i>	

Hash Functions

Update on Tiger	63
<i>Florian Mendel, Bart Preneel, Vincent Rijmen, Hirotaka Yoshida, Dai Watanabe</i>	
RC4-Hash: A New Hash Function Based on RC4.....	80
<i>Donghoon Chang, Kishan Chand Gupta, Mridul Nandi</i>	
Security of VSH in the Real World	95
<i>Markku-Juhani O. Saarinen</i>	

Provable Security: Key Agreement

Cryptanalysis of Two Provably Secure Cross-Realm C2C-PAKE Protocols	104
<i>Raphael C.-W. Phan, Bok-Min Goi</i>	
Efficient and Provably Secure Generic Construction of Three-Party Password-Based Authenticated Key Exchange Protocols	118
<i>Weijia Wang, Lei Hu</i>	
On the Importance of Public-Key Validation in the MQV and HMQV Key Agreement Protocols	133
<i>Alfred Menezes, Berkant Ustaoglu</i>	

Invited Talk

Another Look at “Provable Security”. II	148
<i>Neal Koblitz, Alfred Menezes</i>	

Provable Security: Public Key Cryptography

Efficient CCA-Secure Public-Key Encryption Schemes from RSA-Related Assumptions	176
<i>Jaimee Brown, Juan Manuel González Nieto, Colin Boyd</i>	
General Conversion for Obtaining Strongly Existentially Unforgeable Signatures	191
<i>Isamu Teranishi, Takuro Oyama, Wakaha Ogata</i>	
Conditionally Verifiable Signature	206
<i>Ian F. Blake, Aldar C-F. Chan</i>	
Constant Phase Bit Optimal Protocols for Perfectly Reliable and Secure Message Transmission	221
<i>Arpita Patra, Ashish Choudhary, Kannan Srinathan, Chandrasekaran Pandu Rangan</i>	

Symmetric Cryptography: Design

Using Wiedemann’s Algorithm to Compute the Immunity Against Algebraic and Fast Algebraic Attacks	236
<i>Frédéric Didier</i>	

Enciphering with Arbitrary Small Finite Domains	251
<i>Valery Pryamíkov</i>	
Enumeration of 9-Variable Rotation Symmetric Boolean Functions Having Nonlinearity > 240	266
<i>Selçuk Kavut, Subhamoy Maitra, Sumanta Sarkar, Melek D. Yücel</i>	

Modes of Operation and Message Authentication Codes

Symmetric Nonce Respecting Security Model and the MEM Mode of Operation	280
<i>Peng Wang, Dengguo Feng, Wenling Wu</i>	
HCH: A New Tweakable Enciphering Scheme Using the Hash-Encrypt-Hash Approach	287
<i>Debrup Chakraborty, Palash Sarkar</i>	
Efficient Shared-Key Authentication Scheme from Any Weak Pseudorandom Function	303
<i>Ryo Nojima, Kazukuni Kobara, Hideki Imai</i>	
A Simple and Unified Method of Proving Indistinguishability	317
<i>Mridul Nandi</i>	

Fast Implementation of Public Key Cryptography

Extended Double-Base Number System with Applications to Elliptic Curve Cryptography	335
<i>Christophe Doche, Laurent Imbert</i>	
CMSS – An Improved Merkle Signature Scheme	349
<i>Johannes Buchmann, Luis Carlos Coronado García, Erik Dahmen, Martin Döring, Elena Klintsevich</i>	

ID-Based Cryptography

Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature	364
<i>Man Ho Au, Joseph K. Liu, Willy Susilo, T.H. Yuen</i>	
Secure Cryptographic Workflow in the Standard Model	379
<i>Manuel Barbosa, Pooya Farshim</i>	

Multi-receiver Identity-Based Key Encapsulation with Shortened
Ciphertext 394
Sanjit Chatterjee, Palash Sarkar

Identity-Based Parallel Key-Insulated Encryption Without Random
Oracles: Security Notions and Construction 409
Jian Weng, Shengli Liu, Kefei Chen, Changshe Ma

Embedded System and Side Channel Attacks

AES Software Implementations on ARM7TDMI 424
Matthew Darnall, Doug Kuhlman

Galois LFSR, Embedded Devices and Side Channel Weaknesses 436
Antoine Joux, Pascal Delaunay

Author Index 453