

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

Bimal Roy (Ed.)

Advances in Cryptology – ASIACRYPT 2005

11th International Conference on the Theory
and Application of Cryptology and Information Security
Chennai, India, December 4-8, 2005
Proceedings



Springer

Volume Editor

Bimal Roy

Indian Statistical Institute, Applied Statistics Unit

203 B.T. Road, Kolkata 700 108, India

E-mail: bimal@isical.ac.in

Library of Congress Control Number: 2005936460

CR Subject Classification (1998): E.3, D.4.6, F.2.1-2, K.6.5, C.2, J.1, G.2

ISSN 0302-9743

ISBN-10 3-540-30684-6 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-30684-9 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 is a part of Springer Science+Business Media

springeronline.com

© International Association for Cryptologic Research 2005

Printed in Germany

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

Printed on acid-free paper SPIN: 11593447 06/3142 5 4 3 2 1 0

Preface

Asiacrypt, the annual conference of cryptology sponsored by IACR is now 11 years old. Asiacrypt 2005 was held during December 4–8, 2005, at Hotel Taj Coromandel, Chennai, India. This conference was organized by the International Association for Cryptologic Research (IACR) in cooperation with the Indian Institute of Technology (IIT), Chennai.

This year a total of 237 papers were submitted to Asiacrypt 2005. The submissions covered all areas of cryptographic research representing the current state of work in the crypto community worldwide. Each paper was blind reviewed by at least three members of the Program Committee and papers co-authored by the PC members were reviewed by at least six members. This first phase of review by the PC members was followed by a detailed discussion on the papers. At the end of the reviewing process 37 papers were accepted and were presented at the conference. The proceedings contain the revised versions of the accepted papers. In addition we were fortunate to have Prof. Andrew Yao and Prof. Bart Preneel as invited speakers.

Based on a discussion and subsequent voting among the PC members, the Best Paper Award for this year's Asiacrypt was conferred to Pascal Paillier and Damien Vergnaud for the paper entitled "Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log."

I would like to thank the following people. First, the General Chair, Prof. Pandu Rangan. Next, Springer for publishing the proceedings in the *Lecture Notes in Computer Science* series. I would also like to thank the submitting authors, the Program Committee members, the external reviewers, and the local Organizing Committee consisting of Mr. Veeraraghavan and Mr. E. Boopal. I acknowledge the partial financial support provided by Microsoft Research Labs, India. I thank Dr. Debrup Chakraborty for his help in managing the submissions and the final preparation of the proceedings. Thanks also goes to Mr. Sanjit Chatterjee for his assistance in the process.

December 2005

Bimal Roy

Asiacrypt 2005

December 3–7, 2005, Chennai, India

Sponsored by the
International Association for Cryptologic Research

in cooperation with
Indian Institute of Technology, Chennai, India

General Chair

C. Pandu Rangan, Indian Institute of Technology, Chennai, India

Program Chair

Bimal Roy, Indian Statistical Institute, Kolkata, India

Program Committee

Manindra Agarwal	Indian Institute of Technology, Kanpur, India, and National University of Singapore, Singapore
Feng Bao	Institute for Infocomm Research, Singapore
Rana Barua	Indian Statistical Institute, India
P.S.L.M. Barreto	University of São Paulo, Brazil
Alex Biryukov	Katholieke Universiteit, Leuven, Belgium
Simon R. Blackburn	Royal Holloway College, University of London, UK
Colin Boyd	Queensland University of Technology, Australia
Nicolas T. Courtois	Axalto Smart Cards, France
Cunsheng Ding	Hong Kong University of Science and Technology, Hong Kong, China
Orr Dunkelman	Technion, Israel
Jovan Golic	Telecom Italia, Italy
Lai Xue Jia	Shanghai Jiaotong University, China
Thomas Johansson	Lund University, Sweden
Chi Sung Laih	National Cheng Kung University, Taiwan
Tanja Lange	Ruhr University Bochum, Germany
Pil Joong Lee	Pohang University of Science & Technology, Korea
Arjen K. Lenstra	Lucent Technologies, USA, and Technische Universiteit Eindhoven, Netherlands
Chae Hoon Lim	Sejong University, Korea
C.E. Veni Madhavan	Indian Institute of Science, India
Alfred Menezes	University of Waterloo, Canada
Phong Q. Nguyen	CNRS/École Normale Supérieure, France
Kapil Paranjape	Institute of Mathematical Sciences, India
David Pointcheval	CNRS/École Normale Supérieure, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
C. Pandu Rangan	Indian Institute of Technology, Madras, India
Vincent Rijmen	Technical University of Graz, Austria
Rei Safavi-Naini	University of Wollongong, Australia
Amit Sahai	University of California, Los Angeles, USA
Kouichi Sakurai	Kyushu University, Japan
P.K. Saxena	SAG, India
Nicolas Sendrier	INRIA, France
Hovav Shacham	Stanford University, USA
Nigel Smart	University of Bristol, UK
Douglas R. Stinson	University of Waterloo, Canada
Xiaoyun Wang	Shandong University, China
Hugh Williams	University of Calgary, Canada

External Reviewers

Michel Abdalla	Decio Luiz Gazzoni Filho	Sandeep Kumar
Raju Agarwal	Gerhard Frey	Meena Kumari
Omran Ahmadi	Pierre-Alain Fouque	Sébastien Kunz-Jacques
Sattam Al-Riyami	Navneet Gaba	Kaoru Kurosawa
Daniel Augot	Fabien Galand	Hidekazu Kuwakado
Roberto Avanzi	Steven Galbraith	Yann Laigle-Chapuy
Steve Babbage	David Galindo	Joseph Lano
Joonsang Baek	Juan Garay	Cedric Lauradoux
Vittorio Bagini	Pierrick Gaudry	Dong Hoon Lee
Boaz Barak	Craig Gentry	Jooyoung Lee
Mark Bauer	Eu-Jin Goh	Jung Wook Lee
S.S. Bedi	Louis Goubin	Wei-Bin Lee
Daniel J. Bernstein	Rob Granger	Stephane Lemieux
Amnon Besser	Jens Groth	Manuel Leone
Raghav Bhaskar	D.J. Guan	Francois Levy-dit-Vehel
A.K. Bhateja	Indivar Gupta	Benoit Libert
Dan Boneh	Saoshi Hada	Yehuda Lindell
Xavier Boyen	Darrel Hankerson	Yu Long
An Braeken	Yong-Sork Her	Chi-Jen Lu
Emmanuel Bresson	Julio Cesar L. Hernández	Ling Lu
Christophe De Canniere	Jason Hinek	Stefan Lucks
Anne Canteaut	Yvonne Hitchcock	Subhomay Maitra
Dario Catalano	Andreas Hirt	John Malone-Lee
Juyoung Cha	Martin Hirt	Stephane Manuel
Sucheta Chakraborty	Susan Hohenberger	Keith Martin
Pascale Charpin	Yoshiaki Hori	Atefeh Mashatan
Sanjit Chatterjee	Wang Chih Hung	Luke McAvan
Liquan Chen	Yong Ho Hwang	Renato Menicocci
Jung Hee Cheon	Kenji Imamoto	Miodrag Mihaljevic
Benoit Chevallier-Mames	Yuval Ishai	Marine Minier
Kookrae Cho	Mike Jacobson	Pradeep Mishra
Kim-Kwang R. Choo	Rahul Jain	P.R. Mishra
Sherman Chow	Devendra Jha	Chris Mitchell
Carlos Cid	Shaoquan Jiang	Bodo Moeller
Ricardo Dahab	Ari Juels	Guglielmo Morgari
Blandine Debraize	Pascal Junod	Bernard Mourrain
Alex Dent	Guruprasad Kar	Yi Mu
Claus Diem	Jonathan Katz	Siguna Mueller
Ratna Dutta	Chong Hee Kim	Frédéric Muller
Andreas Enge	Seung Joo Kim	Mats Naeslund
Chun-I Fan	Shinsaku Kiyomoto	Mridul Nandi
Nelly Fazio	Yuichi Komano	Anderson Nascimento
Serge Fehr	Caroline Kudla	Gregory Neven

X Organization

Antonio Nicolosi	Gal Rouvroy	Dongvu Tonien
Juan Gonzalez Nieto	Yasuyuki Sakai	Wen-Guey Tzeng
Ryuzou Nishi	Palash Sarkar	Shinegori Uchiyama
Takeshi Okamoto	Reg Sawilla	Yoshifumi Ueshige
Tatsuaki Okamoto	Ruediger Schack	Damien Vergnaud
Harold Ollivier	Renate Scheidler	Eric Verheul
Rafi Ostrovsky	Werner Schindler	Neelam Verma
Haruki Ota	Alice Silverberg	Guilin Wang
S.K. Pal	Jae Woo Seo	Huaxiong Wang
Dan Page	Nicholas Sheppard	Dai Watanabe
Pascal Pallier	Jong Hoon Shin	Brent Waters
Dong Jin Park	Tom Shrimpton	Benne de Weger
Jung Hyung Park	M.C. Shrivastava	William Whyte
Young Ho Park	Andrey Sidorenko	Peter Wild
Raphael Pass	Sanjeet Singh	Christopher Wolf
Kenny Paterson	Martijn Stam	Kjell Wooding
Kun Peng	Hung-Min Sun	Yongdong Wu
Slobodan Petrovic	Jae Chul Sung	Tianbing Xia
Duong Hieu Phan	Krishna Suri	Pratibha Yadav
N. Rajesh Pillai	Willy Susilo	Bo-Yin Yang
Benny Pinkas	Gelareh Taban	Yeon Hyeong Yang
Norbert Pramstaller	Keisuke Tanaka	Jeong Il Yoon
J. Radhakrishnan	Edlyn Teske	Young Tae Youn
Christian Rechberger	Jean-Pierre Tillich	Yuliang Zheng
Eric Rescorla	Rajeev Thamman	Huafei Zhu
Leo Reyzin	Nicolas Theriault	

Microsoft®
Research



DoCoMo USA Labs

Table of Contents

Algebra and Number Theory

Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log <i>Pascal Paillier, Damien Vergnaud</i>	1
Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log? <i>David Jao, Stephen D. Miller, Ramarathnam Venkatesan</i>	21
Adapting Density Attacks to Low-Weight Knapsacks <i>Phong Q. Nguyễn, Jacques Stern</i>	41
Efficient and Secure Elliptic Curve Point Multiplication Using Double-Base Chains <i>Vassil Dimitrov, Laurent Imbert, Pradeep Kumar Mishra</i>	59

Multiparty Computation

Upper Bounds on the Communication Complexity of Optimally Resilient Cryptographic Multiparty Computation <i>Martin Hirt, Jesper Buus Nielsen</i>	79
Graph-Decomposition-Based Frameworks for Subset-Cover Broadcast Encryption and Efficient Instantiations <i>Nuttapong Attrapadung, Hideki Imai</i>	100
Revealing Additional Information in Two-Party Computations <i>Andreas Jakoby, Maciej Liśkiewicz</i>	121

Zero Knowledge and Secret Sharing

Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation <i>Vladimir Kolesnikov</i>	136
Parallel Multi-party Computation from Linear Multi-secret Sharing Schemes <i>Zhifang Zhang, Mulan Liu, Liangliang Xiao</i>	156

Updatable Zero-Knowledge Databases	
<i>Moses Liskov</i>	174

Information and Quantum Theory

Simple and Tight Bounds for Information Reconciliation and Privacy Amplification	
<i>Renato Renner, Stefan Wolf</i>	199
Quantum Anonymous Transmissions	
<i>Matthias Christandl, Stephanie Wehner</i>	217

Privacy and Anonymity

Privacy-Preserving Graph Algorithms in the Semi-honest Model	
<i>Justin Brickell, Vitaly Shmatikov</i>	236
Spreading Alerts Quietly and the Subgroup Escape Problem	
<i>James Aspnes, Zoë Diamadi, Kristian Gjøsteen, René Peralta, Aleksandr Yampolskiy</i>	253
A Sender Verifiable Mix-Net and a New Proof of a Shuffle	
<i>Douglas Wikström</i>	273
Universally Anonymizable Public-Key Encryption	
<i>Ryotaro Hayashi, Keisuke Tanaka</i>	293

Cryptanalytic Techniques

Fast Computation of Large Distributions and Its Cryptographic Applications	
<i>Alexander Maximov, Thomas Johansson</i>	313
An Analysis of the XSL Algorithm	
<i>Carlos Cid, Gaëtan Leurent</i>	333

Stream Cipher Cryptanalysis

New Applications of Time Memory Data Tradeoffs	
<i>Jin Hong, Palash Sarkar</i>	353
Linear Cryptanalysis of the TSC Family of Stream Ciphers	
<i>Frédéric Muller, Thomas Peyrin</i>	373

A Practical Attack on the Fixed RC4 in the WEP Mode <i>I. Mantin</i>	395
A Near-Practical Attack Against B Mode of HBB <i>Joydip Mitra</i>	412

Block Ciphers and Hash Functions

New Improvements of Davies-Murphy Cryptanalysis <i>Sébastien Kunz-Jacques, Frédéric Muller</i>	425
A Related-Key Rectangle Attack on the Full KASUMI <i>Eli Biham, Orr Dunkelman, Nathan Keller</i>	443
Some Attacks Against a Double Length Hash Proposal <i>Lars R. Knudsen, Frédéric Muller</i>	462
A Failure-Friendly Design Principle for Hash Functions <i>Stefan Lucks</i>	474

Bilinear Maps

Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application <i>Yumiko Hanaoka, Goichiro Hanaoka, Junji Shikata, Hideki Imai</i>	495
Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps <i>Paulo S.L.M. Barreto, Benoît Libert, Noel McCullagh, Jean-Jacques Quisquater</i>	515
Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps <i>Toru Nakanishi, Nobuo Funabiki</i>	533

Key Agreement

Modular Security Proofs for Key Agreement Protocols <i>Caroline Kudla, Kenneth G. Paterson</i>	549
A Simple Threshold Authenticated Key Exchange from Short Secrets <i>Michel Abdalla, Olivier Chevassut, Pierre-Alain Fouque, David Pointcheval</i>	566

Examining Indistinguishability-Based Proof Models for Key
Establishment Protocols
Kim-Kwang Raymond Choo, Colin Boyd, Yvonne Hitchcock 585

Provable Security

Server-Aided Verification: Theory and Practice
Marc Girault, David Lefranc 605

Errors in Computational Complexity Proofs for Protocols
Kim-Kwang Raymond Choo, Colin Boyd, Yvonne Hitchcock 624

Signatures

Universal Designated Verifier Signature Proof (or How to Efficiently
Prove Knowledge of a Signature)
Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo 644

Efficient Designated Confirmer Signatures Without Random Oracles or
General Zero-Knowledge Proofs
Craig Gentry, David Molnar, Zulfikar Ramzan 662

Universally Convertible Directed Signatures
Fabien Laguillaumie, Pascal Paillier, Damien Vergnaud 682

Author Index 703