Lecture Notes in Computer Science 3788

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

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

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

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

DoCoMo USA Labs

Table of Contents

Algebra and Number Theory

Multiparty Computation

Zero Knowledge and Secret Sharing

Information and Quantum Theory

Privacy and Anonymity

Cryptanalytic Techniques

Stream Cipher Cryptanalysis

Block Ciphers and Hash Functions

Bilinear Maps

Key Agreement

Provable Security

Signatures