Lecture Notes in Computer Science 3958

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

Editorial Board

Moti Yung Yevgeniy Dodis
Aggelos Kiayias Tal Malkin (Eds.)

Public Key Cryptography – PKC 2006

9th International Conference
on Theory and Practice of Public-Key Cryptography
New York, NY, USA, April 24-26, 2006
Proceedings

Springer

Volume Editors

Moti Yung
RSA Laboratories
and
Columbia University
Computer Science Department
1214 Amsterdam Avenue, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Yevgeniy Dodis
New York University
Department of Computer Science
251 Mercer Street, New York, NY 10012, USA
E-mail: dodis@cs.nyu.edu

Aggelos Kiayias
University of Connecticut
Department of Computer Science and Engineering Storrs
CT 06269-2155, USA
E-mail: aggelos@cse.uconn.edu

Tal Malkin
Columbia University
Department of Computer Science
1214 Amsterdam Avenue, New York, NY 10027, USA
E-mail: tal@cs.columbia.edu

Library of Congress Control Number: 2006924182

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-33851-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33851-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11745853 06/3142 5 4 3 2 1 0

Preface

The 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2006) took place in New York City. PKC is the premier international conference dedicated to cryptology focusing on all aspects of public-key cryptography. The event is sponsored by the International Association of Cryptologic Research (IACR), and this year it was also sponsored by the Columbia University Computer Science Department as well as a number of sponsors from industry, among them: EADS and Morgan Stanley, which were golden sponsors, as well as Gemplus, NTT DoCoMo, Google, Microsoft and RSA Security, which were silver sponsors. We acknowledge the generous support of our industrial sponsors; their support was a major contributing factor to the success of this year's PKC.

PKC 2006 followed a series of very successful conferences that started in 1998 in Yokohama, Japan. Further meetings were held successively in Kamakura (Japan), Melbourne (Australia), Jeju Island (Korea), Paris (France), Miami (USA), Singapore and Les Diablerets (Switzerland). The conference became an IACR sponsored event (officially designated as an IACR workshop) in 2003 and has been sponsored by IACR continuously since then. The year 2006 found us all in New York City where the undertone of the conference was hummed in the relentless rhythm of the city that never sleeps.

This year's conference was the result of a collaborative effort by four of us: Moti Yung served as the conference and program chair. Moti orchestrated the whole project and led the Program Committee's efforts in the careful selection of the 34 papers that you will find in this volume. Yevgeniy Dodis served as the general and sponsorship chair, coordinating the sponsorship efforts. Aggelos Kiayias served as the publicity and publication chair, tending to the conference's publicity aspects, Web-site, submission and reviewing site as well as the editorial preparation of the present volume. Tal Malkin served as the general and local arrangements chair and was responsible for the very critical job of hosting PKC 2006 at Columbia University.

The selection of papers for this year's program was a delicate and laborious task. PKC 2006 had received a total of 124 submissions by the day of the submission deadline, November 15, 2005. Each paper was refereed by at least four committee members who were frequently assisted by external reviewers. The online discussions together with the reviews that were posted on the online reviewing site, if printed, would require more than 450 pages of densely printed text. The present proceedings volume contains the revised versions of the accepted extended abstracts as submitted by the authors after an alloted three week revision period based on the Program Committee's comments. The PKC 2006 Program Committee had the pleasure of according this year's *PKC Best Paper Award* to Daniel Bleichenbacher and Alexander May for their advancement

of RSA cryptanalysis in their paper entitled "New Attacks on RSA with Small Secret CRT-Exponents."

We would like to thank the Program Committee members as well as the external reviewers for their volunteered hard work invested in selecting the program. We thank the PKC Steering Committee for their support. We also wish to thank the following individuals: Shai Halevi for providing his Web-review and submission system to be used for the conference and for providing technical support; the submission and reviewing-site administrator David Walluck as well as the other students of the CryptoDRM Lab at the University of Connecticut for providing technical support; and Michael Locasto for Web-site administration support at Columbia University. Finally big thanks are due to all authors of submitted papers whose quality contributions make this research area a pleasure to work in, and made this conference a possibility.

March 2006

Moti Yung
Yevgeniy Dodis
Aggelos Kiayias
Tal Malkin

Organization

PKC Steering Committee

Ronald Cramer	CWI and Leiden University, The Netherlands
Yvo Desmedt	University College London, UK
Hideki Imai (Chair)	University of Tokyo, Japan
Kwangjo Kim	Information and Communications University, Korea
David Naccache	École Normale Supérieure, France
Tatsuaki Okamoto	NTT Labs, Japan
Jacques Stern	École Normale Supérieure, France
Moti Yung	RSA Laboratories and Columbia University, USA
Yuliang Zheng (Secretary)	University of North Carolina at Charlotte, USA

Organizing Committee

Conference and Program Chair	Moti Yung
General and Sponsorship Chair	Yevgeniy Dodis
Publicity and Publication Chair	Aggelos Kiayias
General and Local Arrangements Chair	Tal Malkin

Industrial Sponsors

EADS
Morgan Stanley
Gemplus
NTT DoCoMo
Google
Microsoft
RSA Security

Program Committee

Masayuki Abe	NTT Japan
Feng Bao	I2R, Singapore
Paulo S.L.M. Barreto	University of São Paulo, Brazil
Amos Beimel	Ben Gurion University, Israel
Xavier Boyen	Voltage Technology, USA
Serge Fehr	CWI, The Netherlands
Pierre-Alain Fouque	ENS Paris, France
Juan Garay	Bell Labs, USA
Rosario Gennaro	IBM Research, USA
Nick Howgrave-Graham	NTRU Cryptosystems, USA
Dong Hoon Lee	Korea University, Korea
Wenbo Mao	HP Labs, China
Alexander May	Paderborn University, Germany
David Naccache	ENS, France
Rafail Ostrovsky	UCLA, USA
Kenny Paterson	Royal Holloway, U. of London, UK
Giuseppe Persiano	University of Salerno, Italy
Benny Pinkas	Haifa University, Israel
Leonid Reyzin	Boston University, USA
Kazue Sako	NEC Japan
Jean-Sébastien Coron	University of Luxembourg
Alice Silverberg	U. C. Irvine, USA
Jessica Staddon	PARC, USA
Ron Steinfeld	Macquarie University, Australia
Edlyn Teske	University of Waterloo, Canada
Wen-Guey Tzeng	NCTU, Taiwan
Susanne Wetzel	Stevens Institute, USA
Yiqun Lisa Yin	Independent Consultant, USA
Adam Young	MITRE, USA
Moti Yung	RSA Labs and Columbia U., USA

External Reviewers

Michel Abdalla	Ran Canetti	Yang Cui
Ben Adida	Melissa Chase	Martin Döring
Luis von Ahn	Lily Chen	Paolo D'Arco
Giuseppe Ateniese	Liqun Chen	Michael De Mare
Joonsang Baek	Benoît Chevallier-Mames	Breno de Medeiros
Paulo Barreto	Chen-Kang Chu	Nenad Dedić
Daniel Brown	Mathieu Ciet	Alex Dent
Jan Camenisch	Scott Contini	Glenn Durfee

Pooya Farshim
Marc Fischlin
Jun Furukawa
Steven Galbraith
Clemente Galdi
David Galindo
Decio Gazzoni
Kristian Gjøsteen
Dorian Goldfeld
Philippe Golle
Vanessa Gratzer
Shai Halevi
Wei Han
Darrel Hankerson
Anwar Hasan
Javier Herranz
Jason Hinek
Dennis Hofheinz
Nicholas Hopper
Toshiyuki Isshiki
Stanislaw Jarecki
Markus Kaiser
Jonathan Katz
Tim Kerins
Eike Kiltz
Hugo Krawczyk
Sebastien Kunz-Jacques
Kaoru Kurosawa
Eonkyung Lee
Xiangxue Li
Benoît Libert
Shia-Yin Lin
Yehuda Lindell
Pierre Loidreau
Anna Lysyanskaya
John Malone-Lee
Gwenaëlle Martinet
Barbara Masucci
Bernd Meyer
Ulrike Meyer
Peter Montgomery
Kengo Mori
Volker Müller
James Muir
Chanathip Namprempre
Phong Nguyen
Jesper Buus Nielsen
Satoshi Obana
Daniel Page
Adriana Palacio
Josef Pieprzyk
David Pointcheval
Geraint Price
Karl Rubin
Tomas Sander
Oliver Schirokauer
Katja Schmidt-Samoa
Michael Scott
Hovav Shacham
Junji Shikata
Nigel Smart
Diana Smetters
Jerry Solinas
Rainer Steinwandt
Willy Susilo
Koutaro Suzuki
Isamu Teranishi
Nicholas Theriault
Richard M. Thomas
Xiaojian Tian
Ivan Visconti
Guilin Wang
Huaxiong Wang
Brent Waters
Ralf-Philipp Weinmann
Enav Weinreb
Kai Wirt
Duncan Wong
David Woodruff
Rui Zhang
Yunlei Zhao
Sheng Zhong
Huafei Zhu
Sebastien Zimmer

Table of Contents

Number Theory Algorithms

Pairing-Based Cryptography

Cryptosystems Design and Analysis

Signature and Identification

Authentication and Key Establishment

Multi-party Computation

PKI Techniques