

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

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

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

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

Table of Contents

Cryptanalysis and Protocol Weaknesses

New Attacks on RSA with Small Secret CRT-Exponents <i>Daniel Bleichenbacher, Alexander May</i>	1
An Attack on a Modified Niederreiter Encryption Scheme <i>Christian Wieschebrink</i>	14
Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm <i>Sébastien Kunz-Jacques, Gwenaëlle Martinet, Guillaume Poupard, Jacques Stern</i>	27

Distributed Crypto-computing

Efficient Polynomial Operations in the Shared-Coefficients Setting <i>Payman Mohassel, Matthew Franklin</i>	44
Generic On-Line/Off-Line Threshold Signatures <i>Chris Crutchfield, David Molnar, David Turner, David Wagner</i>	58
Linear Integer Secret Sharing and Distributed Exponentiation <i>Ivan Damgård, Rune Thorbek</i>	75

Encryption Methods

Encoding-Free ElGamal Encryption Without Random Oracles <i>Benoît Chevallier-Mames, Pascal Paillier, David Pointcheval</i>	91
Parallel Key-Insulated Public Key Encryption <i>Goichiro Hanaoka, Yumiko Hanaoka, Hideki Imai</i>	105
Provably Secure Steganography with Imperfect Sampling <i>Anna Lysyanskaya, Mira Meyerovich</i>	123

Cryptographic Hash and Applications

Collision-Resistant No More: Hash-and-Sign Paradigm Revisited <i>Ilya Mironov</i>	140
--	-----

Higher Order Universal One-Way Hash Functions from the Subset Sum Assumption

Ron Steinfeld, Josef Pieprzyk, Huaxiong Wang 157

Number Theory Algorithms

An Algorithm to Solve the Discrete Logarithm Problem with the Number Field Sieve

An Commeine, Igor Semaev 174

Efficient Scalar Multiplication by Isogeny Decompositions

Christophe Doche, Thomas Icart, David R. Kohel 191

Curve25519: New Diffie-Hellman Speed Records

Daniel J. Bernstein 207

Pairing-Based Cryptography

Strongly Unforgeable Signatures Based on Computational Diffie-Hellman

Dan Boneh, Emily Shen, Brent Waters 229

Generalization of the Selective-ID Security Model for HIBE Protocols

Sanjit Chatterjee, Palash Sarkar 241

Identity-Based Aggregate Signatures

Craig Gentry, Zulfikar Ramzan 257

On the Limitations of the Spread of an IBE-to-PKE Transformation

Eike Kiltz 274

Cryptosystems Design and Analysis

Inoculating Multivariate Schemes Against Differential Attacks

Jintai Ding, Jason E. Gower 290

Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol

Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov 302

High-Order Attacks Against the Exponent Splitting Protection

Frédéric Muller, Frédéric Valette 315

Signature and Identification

New Online/Offline Signature Schemes Without Random Oracles <i>Kaoru Kurosawa, Katja Schmidt-Samoa</i>	330
Anonymous Signature Schemes <i>Guomin Yang, Duncan S. Wong, Xiaotie Deng, Huaxiong Wang</i>	347
The Power of Identification Schemes <i>Kaoru Kurosawa, Swee-Huay Heng</i>	364

Authentication and Key Establishment

Security Analysis of KEA Authenticated Key Exchange Protocol <i>Kristin Lauter, Anton Mityagin</i>	378
SAS-Based Authenticated Key Agreement <i>Sylvain Pasini, Serge Vaudenay</i>	395
The Twist-AUGmented Technique for Key Exchange <i>Olivier Chevassut, Pierre-Alain Fouque, Pierrick Gaudry, David Pointcheval</i>	410
Password-Based Group Key Exchange in a Constant Number of Rounds <i>Michel Abdalla, Emmanuel Bresson, Olivier Chevassut, David Pointcheval</i>	427

Multi-party Computation

Conditional Oblivious Cast <i>Cheng-Kang Chu, Wen-Guey Tzeng</i>	443
Efficiency Tradeoffs for Malicious Two-Party Computation <i>Payman Mohassel, Matthew Franklin</i>	458

PKI Techniques

On Constructing Certificateless Cryptosystems from Identity Based Encryption <i>Benoît Libert, Jean-Jacques Quisquater</i>	474
Building Better Signcryption Schemes with Tag-KEMs <i>Tor E. Bjørstad, Alexander W. Dent</i>	491

Security-Mediated Certificateless Cryptography
 Sherman S.M. Chow, Colin Boyd, Juan Manuel González Nieto 508

k -Times Anonymous Authentication with a Constant Proving Cost
 Isamu Teranishi, Kazue Sako 525

Author Index 543