

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

Tatsuaki Okamoto Xiaoyun Wang (Eds.)

Public Key Cryptography – PKC 2007

10th International Conference
on Practice and Theory in Public-Key Cryptography
Beijing, China, April 16-20, 2007
Proceedings

Volume Editors

Tatsuaki Okamoto

NTT Laboratories, Nippon Telegraph and Telephone Corporation

Japan

E-mail: okamoto.tatsuaki@lab.ntt.co.jp

Xiaoyun Wang

Shandong University and Tsinghua University

China

E-mail: xywang@sdu.edu.cn

Library of Congress Control Number: 2007923868

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 3-540-71676-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-71676-1 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

©International Association for Cryptologic Research 2007

Printed in Germany

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

Printed on acid-free paper SPIN: 12042999 06/3180 5 4 3 2 1 0

Preface

The 10th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2007) was held at Tsinghua University in Beijing, China, April 16–20, 2007. 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 National Natural Science Foundation of China (NSFC) and Tsinghua University.

The conference received 118 submissions, and the Program Committee selected 29 of these for presentation. The Program Committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to public-key cryptography. Each paper was anonymously reviewed by at least three Program Committee members.

Extended abstracts of the revised versions of the accepted papers are in these proceedings. The program also included three invited lectures by Rafail Ostrovsky with UCLA, USA, Shige Peng with Shandong University, China and Adi Shamir with the Weizmann Institute of Science, Israel. Two papers regarding the invited lectures are included in these proceedings. The PKC 2007 Program Committee had the pleasure of awarding this year's PKC best paper award to Xavier Boyen and Brent Waters for their paper, entitled "Full-Domain Subgroup Hiding and Constant-Size Group Signatures."

We are extremely grateful to the Program Committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection. We gratefully acknowledge the help of a large number of external reviewers who reviewed submissions in their area of expertise. We also thank the PKC Steering Committee for their support.

Electronic submissions were made possible by the Web Review system, iChair, developed by Thomas Baignères and Matthieu Finiasz at EPFL, LASEC. We would like to thank Thomas Baignères and Matthieu Finiasz for their great support.

We deeply thank Andrew C. Yao, the General Chair, for his effort in organizing and making this conference possible. The great scientist was the source of the success of PKC 2007.

We are grateful to all the Organizing Committee members for their volunteer work. In addition, we would like to thank Wei Yu for his enormous support in installing and operating the iChair system in the review process and editing of these proceedings.

We wish to thank all the authors, for submitting papers, and the authors of accepted papers for their cooperation.

February 2007

Tatsuaki Okamoto
Xiaoyun Wang

PKC 2007

The 10th International Conference on Theory and Practice of Public-Key Cryptography

Tsinghua University, Beijing, China, April 16–20, 2007

Sponsored by the *International Association of Cryptologic Research (IACR)*,
National Natural Science Foundation of China and *Tsinghua University*.

General Chair

Andrew C. Yao, Tsinghua University, China

Program Co-chairs

Tatsuaki Okamoto, NTT, Japan

Xiaoyun Wang, Tsinghua University, China

Organizing Committee

Andrew C. Yao Tsinghua University, China
Xiaoyun Wang Tsinghua University, China
Yuexuan Wang Tsinghua University, China
Xiaoming Sun Tsinghua University, China
Hongbo Yu Tsinghua University, China
Qi Feng Tsinghua University, China
Meiqin Wang Shandong University, China

Program Committee

Feng Bao I2R, Singapore
Jung Hee Cheon Seoul National University, Korea
Alfredo De Santis University of Salerno, Italy
Yvo Desmedt UCL, UK
Giovanni Di Crescenzo Telcordia Tech., USA
Steven Galbraith Royal Holloway University of London, UK
Juan Garay Bell labs, USA
Jonathan Katz University of Maryland, USA
Kwangjo Kim ICU, Korea
Hugo Krawczyk IBM, USA
Arjen Lenstra Lucent, USA
Anna Lysyanskaya Brown University, USA
Alfred Menezes University of Waterloo, Canada
Kazuo Ohta University of Electro-Communications, Japan

Rafail Ostrovsky	UCLA, USA
Dingyi Pei	Guangzhou University, China
David Pointcheval	ENS, France
C. Pandu Rangan	IIT Madras, India
Hovav Shacham	Weizmann Institute, Israel
Igor Shparlinski	Macquarie University, Australia
Serge Vaudenay	EPFL, Switzerland
Frances Yao	City University of Hong Kong, Hong Kong, China
Moti Yung	Columbia University, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

Steering Committee

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

External Reviewers

Michel Abdalla	Yuichiro Esaki	Yutaka Kawai
Patrick Amon	Serge Fehr	Aggelos Kiayias
Paolo D Arco	Anna Lisa Ferrara	Eike Kilt
Joonsang Baek	Matthieu Finiasz	Woo-Hwan Kim
Thomas Baigneres	Pierre-Alain Fouque	Thorsten Kleinjung
Caroline Belrose	Rosario Gennaro	Yuichi Kokubun
Olivier Billet	Nick Howgrave Graham	Vlad Kolesnikov
Colin Boyd	Jens Groth	Yuichi Komano
Dan Brown	Shai Halevi	Takahiro Kondo
Qingjun Cai	Safuat Hamdy	Chiu-Yuen Koo
Sebastien Canard	Yoshikazu Hanatani	Noboru Kunihiro
Melissa Chase	Darrel Hankerson	Kaoru Kurosawa
Carlos Cid	Jason Hinek	Taekyoung Kwon
Scott Contini	Qiong Huang	Rob Lambert
Cecile Delerabelle	James Hughes	Kristin Lauter
Alex Dent	Sebastien Kunz Jacques	Munkyu Lee
Konidala M. Divyan	Ellen Jochemsz	Jin Li
Junwu Dong	Pascal Junod	Yong Li
Dang Nguyen Duc	Marcelo Kaihara	Vo Duc Liem
Ratna Dutta	Alexandre Karlov	Seongan Lim

Perret Ludovic	Sylvain Pasini	Berkant Ustaoglu
Daegun Ma	Kenny Paterson	Jose Villegas
Benoit Chevallier Mames	Manas Patra	Ivan Visconti
Barbara Masucci	Ludovic Perret	Martin Vuagnoux
Alex May	Benny Pinkas	Shabsi Walfish
Alexander May	Tal Rabin	Brent Waters
Maria Meyerovich	Leonid Rayzin	Christopher Wolf
Anton Mityagin	Pankaj Rohatgi	Duncan S. Wong
Satoshi Miyagawa	Bagus Santoso	David Woodruff
Payman Mohassel	Benjamin Smith	Yongdong Wu
David Molnar	Martijn Stam	Guomin Yang
Jean Monnerat	Ron Steinfeld	Jeong Hyun Yi
Siguna Mueller	Rene Struik	Kazuki Yoneyama
Phong Nguyen	Willy Susilo	Hyojin Yoon
Phong Q. Nguyen	Chunming Tang	Xiaolai Zhang
Takashi Nishide	Emmanuel Thome	
Haruki Ota	Xiaojian Tian	
Duong Hieu PHAN	Jacques Traore	

Table of Contents

Signatures I

Full-Domain Subgroup Hiding and Constant-Size Group Signatures	1
<i>Xavier Boyen and Brent Waters</i>	
A Direct Anonymous Attestation Scheme for Embedded Devices	16
<i>He Ge and Stephen R. Tate</i>	
Anonymous Signatures Made Easy	31
<i>Marc Fischlin</i>	
On the Generic and Efficient Constructions of Secure Designated Confirmer Signatures	43
<i>Guilin Wang, Joonsang Baek, Duncan S. Wong, and Feng Bao</i>	

Invited Talk I

Cryptanalysis of Group-Based Key Agreement Protocols Using Subgroup Distance Functions	61
<i>Dima Ruinskiy, Adi Shamir, and Boaz Tsaban</i>	

Cryptanalysis

Length Based Attack and Braid Groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key Exchange Protocol	76
<i>Alex D. Myasnikov and Alexander Ushakov</i>	
New Chosen-Ciphertext Attacks on NTRU	89
<i>Nicolas Gama and Phong Q. Nguyen</i>	
Cryptanalysis of the Paeng-Jung-Ha Cryptosystem from PKC 2003	107
<i>Daewan Han, Myung-Hwan Kim, and Yongjin Yeom</i>	

Protocols I

Optimistic Fair Exchange in a Multi-user Setting	118
<i>Yevgeniy Dodis, Pil Joong Lee, and Dae Hyun Yum</i>	
Multi-party Stand-Alone and Setup-Free Verifiably Committed Signatures	134
<i>Huafei Zhu, Willy Susilo, and Yi Mu</i>	
Knowledge-Binding Commitments with Applications in Time-Stamping	150
<i>Ahto Buldas and Sven Laur</i>	

Signatures II

Efficient Ring Signatures Without Random Oracles	166
<i>Hovav Shacham and Brent Waters</i>	
Traceable Ring Signature	181
<i>Hiichiro Fujisaki and Koutarou Suzuki</i>	
Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir Without Random Oracles	201
<i>Mihir Bellare and Sarah Shoup</i>	
Improved On-Line/Off-Line Threshold Signatures	217
<i>Emmanuel Bresson, Dario Catalano, and Rosario Gennaro</i>	

Multivariate Cryptosystems

High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems	233
<i>Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li, and John Wagner</i>	
Cryptanalysis of HFE with Internal Perturbation	249
<i>Vivien Dubois, Louis Granboulan, and Jacques Stern</i>	
ℓ -Invertible Cycles for Multivariate Quadratic (MQ) Public Key Cryptography	266
<i>Jintai Ding, Christopher Wolf, and Bo-Yin Yang</i>	

Encryption

Chosen-Ciphertext Secure Key-Encapsulation Based on Gap Hashed Diffie-Hellman	282
<i>Eike Kiltz</i>	
Parallel Key-Insulated Public Key Encryption Without Random Oracles	298
<i>Benoît Libert, Jean-Jacques Quisquater, and Moti Yung</i>	
Multi-bit Cryptosystems Based on Lattice Problems	315
<i>Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa</i>	

Protocols II

Practical and Secure Solutions for Integer Comparison	330
<i>Juan Garay, Berry Schoenmakers, and José Villegas</i>	
Multiparty Computation for Interval, Equality, and Comparison Without Bit-Decomposition Protocol	343
<i>Takashi Nishide and Kazuo Ohta</i>	

Identity-Based Traitor Tracing	361
<i>Michel Abdalla, Alexander W. Dent, John Malone-Lee, Gregory Neven, Duong Hieu Phan, and Nigel P. Smart</i>	
Verifiable Shuffle of Large Size Ciphertexts	377
<i>Jens Groth and Steve Lu</i>	

Invited Talk II

A Survey of Single-Database Private Information Retrieval: Techniques and Applications	393
<i>Rafail Ostrovsky and William E. Skeith III</i>	

Number Theoretic Techniques

Deterministic Polynomial Time Equivalence Between Factoring and Key-Recovery Attack on Takagi's RSA	412
<i>Noboru Kunihiro and Kaoru Kurosawa</i>	
Efficient Pseudorandom Generators Based on the DDH Assumption	426
<i>Reza Rezaeian Farashahi, Berry Schoenmakers, and Andrey Sidorenko</i>	
Fast Batch Verification of Multiple Signatures	442
<i>Jung Hee Cheon and Jeong Hyun Yi</i>	

Public-Key Infrastructure

A Closer Look at PKI: Security and Efficiency	458
<i>Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, and Bogdan Warinschi</i>	
Self-Generated-Certificate Public Key Encryption Without Pairing	476
<i>Junzuo Lai and Weidong Kou</i>	

Author Index	491
-------------------------------	-----