Lecture Notes in Computer Science 4450

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

Springer

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

Springer is a part of Springer Science+Business Media

springer.com

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

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

Table of Contents

Signatures I

Invited Talk I

Cryptanalysis

Protocols I

Signatures II

Multivariate Cryptosystems

Encryption

Protocols II

Invited Talk II

Number Theoretic Techniques

Public-Key Infrastructure