Lecture Notes in Computer Science 4939

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

Ronald Cramer (Ed.)

Public Key Cryptography – PKC 2008

11th International Workshop
on Practice and Theory in Public Key Cryptography
Barcelona, Spain, March 9-12, 2008
Proceedings

Volume Editor

Ronald Cramer
CWI Amsterdam and
Leiden University
The Netherlands
E-mail: ronald.cramer@cwi.nl

Library of Congress Control Number: 2008921494

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 3-540-78439-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-78439-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12234431 06/3180 5 4 3 2 1 0

Preface

These are the Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography – PKC 2008. The workshop was held in Barcelona, Spain, March 9–12, 2008.

It was sponsored by the International Association for Cryptologic Research (IACR; see `www.iacr.org`), this year in cooperation with MAK, the Research Group on Mathematics Applied to Cryptography at UPC, the Polytechnical University of Catalonia. The General Chair, Carles Padró, was responsible for chairing the Local Organization Committee, for handling publicity and for University attracting funding from sponsors.

The PKC 2008 Program Committee (PC) consisted of 30 internationally renowned experts. Their names and affiliations are listed further on in these proceedings. By the September 7, 2007 submission deadline the PC had received 71 submissions via the IACR Electronic Submission Server. The subsequent selection process was divided into two phases, as usual. In the review phase each submission was carefully scrutinized by at least three independent reviewers, and the review reports, often extensive, were committed to the IACR Web Review System. These were taken as the starting point for the PC-wide Web-based discussion phase. During this phase, additional reports were provided as needed, and the PC eventually had some 258 reports at its disposal. In addition, the discussions generated more than 650 messages, all posted in the system. During the entire PC phase, which started on April 12, 2006 with the invitation by the PKC Steering Committee, and which continued until March 2008, more than 500 e-mail messages were communicated. Moreover, the PC received much appreciated assistance by a large body of external reviewers. Their names are also listed in these proceedings.

The selection process for PKC 2008 was finalized by the end of November 2007. After notification of acceptance, the authors were provided with the review comments and were granted three weeks to prepare the final versions, which were due by December 14, 2007. These final versions were not subjected to further scrutiny by the PC and their authors bear full responsibility. The Program Committee worked hard to select a balanced, solid and interesting scientific program, and I thank them very much for their efforts.

After consultation with the PC, I decided to grant the PKC 2008 "Best Paper Award" to Vadim Lyubashevsky (University of California at San Diego), for his paper "Lattice-Based Identification Schemes Secure Under Active Attacks". Besides the above-mentioned 21 regular presentations, the PKC 2008 scientific program featured three invited speakers: David Naccache (ENS, Paris) on "Cryptographic Test Correction", Jean-Jacques Quisquater (Université Catholique de Louvain) on "How to Secretly Extract Hidden Secret Keys: A State of the Attacks", and Victor Shoup (New York University) on "The Role of Discrete

Logarithms in Designing Secure Crypto-Systems". David Naccache also contributed (unrefereed) notes for his lecture, which are also included in this volume.

CWI[1] in Amsterdam and the Mathematical Institute at Leiden University, my employers, are gratefully acknowledged for their support. Also many thanks to Springer for their collaboration. Thanks to Shai Halevi for his IACR Web-handling system.

Eike Kiltz from the CWI group, besides serving as a member of the PC, provided lots of general assistance to the Chair, particularly when setting up and running the Web system and when preparing this volume. I thank Carles Padró, PKC 2008 General Chair, for our smooth and very pleasant collaboration. Finally, we thank our sponsors the Spanish Ministery of Education and Science, and UPC.

January 2008 Ronald Cramer

[1] CWI is the National Research Institute for Mathematics and Computer Science in the Netherlands

PKC 2008

The 11th International Workshop on Practice and Theory in Public Key Cryptography

Universitat Politècnica de Catalunya, Barcelona, Spain
March 9–12, 2008

Sponsored by the *International Association for Cryptologic Research (IACR)*

Organized in cooperation with the
Research Group on Mathematics Applied to Cryptography at UPC

General Chair

Carles Padró, UPC, Spain

Program Chair

Ronald Cramer, CWI Amsterdam and Leiden University, The Netherlands

Local Organizing Committee

Javier López, Ignacio Gracia, Jaume Martí, Sebastià Martín, Carles Padró and Jorge L. Villar

PKC Steering Committee

Ronald Cramer	CWI and Leiden University, The Netherlands
Yvo Desmedt	UCL, UK
Hideki Imai	University of Tokyo, Japan
David Naccache	ENS, France
Tatsuaki Okamoto	NTT, Japan
Jacques Stern	ENS, France
Moti Yung	Columbia University and Google, USA
Yuliang Zheng	University of North Carolina, USA

Program Committee

Michel Abdalla	ENS, France
Masayuki Abe	NTT, Japan
Alexandra Boldyreva	Georgia Tech, USA
Jung Hee Cheon	Seoul National University, South Korea
Ronald Cramer	CWI and Leiden University, The Netherlands
Matthias Fitzi	ETH, Switzerland
Matthew Franklin	UC Davis, USA
Steven Galbraith	Royal Holloway, UK
Juan A. Garay	Bell Labs, USA
Rosario Gennaro	IBM Research, USA
Craig Gentry	Stanford University, USA
Kristian Gjøsteen	NTNU, Norway
Maria I. González Vasco	University Rey Juan Carlos, Spain
Jens Groth	UCL, UK
Yuval Ishai	Technion, Israel and UCLA, USA
Eike Kiltz	CWI, The Netherlands
Kaoru Kurosawa	Ibaraki University, Japan
Wenbo Mao	HP Labs, China
Alexander May	University of Bochum, Germany
Jesper Buus Nielsen	Aarhus University, Denmark
Berry Schoenmakers	TU Eindhoven, The Netherlands
abhi shelat	University of Virginia, USA
Victor Shoup	New York University, USA
Martijn Stam	EPFL, Switzerland
Rainer Steinwandt	Florida Atlantic University, USA
Tsuyoshi Takagi	Future University of Hakodate, Japan
Edlyn Teske	University Waterloo, Canada
Ramarathnam Venkatesan	Microsoft, USA & India
Jorge Villar Santos	UPC, Spain
Moti Yung	Columbia University and Google, USA

External Reviewers

Toru Akishita	Pierre-Alain Fouque	Sang Geun Hahn
Jean-Luc Beuchat	Jun Furukawa	Daewan Han
Raghav Bhaskar	Phong Nguyen	Goichiro Hanaoka
Johannes Blömer	Nicolas Gama	Darrel Hankerson
David Cash	Willi Geiselmann	Anwar Hasan
Nishanth Chandran	Kenneth Giuliani	Swee-Huay Heng
Carlos Cid	Jason Gower	Nick Howgrave-Graham
Iwan Duursma	Nishanth Chandran	David Jao
Serge Fehr	Vipul Goyal	Marc Joye
Marc Fischlin	Matt Green	Waldyr Benits Jr.

Pascal Junod
Charanjit Jutla
Marcelo Kaihara
Alexandre Karlov
Kil-Chan Ha
Noboru Kunihiro
Tanja Lange
Mun-Kyu Lee
Arjen K. Lenstra
Jun Li
Alptekin Küpçü
Anna Lysyanskaya
Daniele Micciancio
David Mireles
Peter Montgomery
Gregory Neven
Dan Page
Omkant Pandey
Jehong Park
Sylvain Pasini
Kenny Paterson
John Proos
Mike Scott
Masaaki Shirase
Igor E. Shparlinski
Martin Simka
Soonhak Kwon
Eberhard Stickel
Douglas Stinson
Isamu Teranishi
Dominique Unruh
José Villegas
Camille Vuillaume
Douglas Wikström
Christopher Wolf
Go Yamamoto

Table of Contents

Session IV: Identification, Broadcast and Key Agreement

Session V: Implementation of Fast Arithmetic

Session VI: Digital Signatures (II)

Session VII: Algebraic and Number Theoretical Cryptanalysis (II)

Session VIII: Public Key Encryption