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\textsuperscript{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 Ministry of Education and Science, and UPC.

January 2008

Ronald Cramer

\textsuperscript{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 I: Algebraic and Number Theoretical Cryptanalysis (I)

Total Break of the \( \ell \)-IC Signature Scheme .......................... 1  
*Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, and Jacques Stern*

Recovering NTRU Secret Key from Inversion Oracles .................. 18  
*Petros Mol and Moti Yung*

Solving Systems of Modular Equations in One Variable: How Many RSA-Encrypted Messages Does Eve Need to Know? .................. 37  
*Alexander May and Maike Ritzenhofen*

## Session II: Theory of Public Key Encryption

Relations Among Notions of Plaintext Awareness ..................... 47  
*James Birkett and Alexander W. Dent*

Completely Non-malleable Encryption Revisited ..................... 65  
*Carmine Ventre and Ivan Visconti*

## Invited Talk I

Cryptographic Test Correction............................................ 85  
*Eric Levieil and David Naccache*

## Session III: Digital Signatures (I)

Off-Line/On-Line Signatures: Theoretical Aspects and Experimental Results .......................................................... 101  
*Dario Catalano, Mario Di Raimondo, Dario Fiore, and Rosario Gennaro*

Construction of Universal Designated-Verifier Signatures and Identity-Based Signatures from Standard Signatures ................ 121  
*Siamak F. Shahandashti and Reihaneh Safavi-Naini*

Proxy Signatures Secure Against Proxy Key Exposure ................. 141  
*Jacob C.N. Schuldt, Kanta Matsuura, and Kenneth G. Paterson*
Session IV: Identification, Broadcast and Key Agreement

Lattice-Based Identification Schemes Secure Under Active Attacks ...... 162
    Vadim Lyubashevsky

Efficient Simultaneous Broadcast........................................... 180
    Sebastian Faust, Emilia Käsper, and Stefan Lucks

SAS-Based Group Authentication and Key Agreement Protocols ...... 197
    Sven Laur and Sylvain Pasini

Session V: Implementation of Fast Arithmetic

An Optimized Hardware Architecture for the Montgomery Multiplication Algorithm ........................................ 214
    Miaoqing Huang, Kris Gaj, Soonhak Kwon, and Tarek El-Ghazawi

New Composite Operations and Precomputation Scheme for Elliptic Curve Cryptosystems over Prime Fields.................. 229
    Patrick Longa and Ali Miri

Session VI: Digital Signatures (II)

Online-Untransferable Signatures ........................................... 248
    Moses Liskov and Silvio Micali

Security of Digital Signature Schemes in Weakened Random Oracle Models ............................................... 268
    Akira Numayama, Toshiyuki Isshiki, and Keisuke Tanaka

A Digital Signature Scheme Based on $CVP_{\infty}$........................ 288
    Thomas Plantard, Willy Susilo, and Khin Than Win

Session VII: Algebraic and Number Theoretical Cryptanalysis (II)

An Analysis of the Vector Decomposition Problem ...................... 308
    Steven D. Galbraith and Eric R. Verheul

A Parameterized Splitting System and Its Application to the Discrete Logarithm Problem with Low Hamming Weight Product Exponents .... 328
    Sungwook Kim and Jung Hee Cheon
## Session VIII: Public Key Encryption

Certificateless Encryption Schemes Strongly Secure in the Standard Model .......................... 344
   *Alexander W. Dent, Benoît Libert, and Kenneth G. Paterson*

Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption .......... 360
   *Benoît Libert and Damien Vergnaud*

Public Key Broadcast Encryption with Low Number of Keys and Constant Decryption Time ........... 380
   *Yi-Ru Liu and Wen-Guey Tzeng*

**Author Index** ................................................................. 397