Lecture Notes in Computer Science 6056

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

Phong Q. Nguyen David Pointcheval (Eds.)

Public Key Cryptography – PKC 2010

13th International Conference
on Practice and Theory in Public Key Cryptography
Paris, France, May 26-28, 2010
Proceedings

Springer

Volume Editors

Phong Q. Nguyen
David Pointcheval
École Normale Supérieure
Département d'Informatique
45 rue d'Ulm, 75230 Paris Cedex 05, France
E-mail: {phong.nguyen, david.pointcheval}@ens.fr

Library of Congress Control Number: 2010926287

CR Subject Classification (1998): E.3, K.6.5, C.2, D.4.6, K.4.4, E.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-13012-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13012-0 Springer Berlin Heidelberg New York

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010) was held May 26–28, 2010, at the École Normale Supérieure (ENS) in Paris, France. PKC 2010 was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the *École Normale Supérieure* (ENS) and the *Institut National de Recherche en Informatique et en Automatique* (INRIA). The General Chairs of the conference were Michel Abdalla and Pierre-Alain Fouque.

The conference received a record number of 145 submissions and each submission was assigned to at least 3 committee members. Submissions co-authored by members of the Program Committee were assigned to at least five committee members. Due to the large number of high-quality submissions, the review process was challenging and we are deeply grateful to the 34 committee members and the 163 external reviewers for their outstanding work. After extensive discussions, the Program Committee selected 29 submissions for presentation during the conference and these are the articles that are included in this volume. The best paper was awarded to Petros Mol and Scott Yilek for their paper "Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions." The review process was run using the iChair software, written by Thomas Baignères and Matthieu Finiasz from EPFL, LASEC, Switzerland, and we are indebted to them for letting us use their software.

The program also included two invited talks: it was a great honor to have Daniele Micciancio and Jacques Stern as invited speakers. Their talks were entitled, respectively, "Duality in Lattice Based Cryptography" and "Mathematics, Cryptography, Security." We would like to genuinely thank them for accepting our invitation and for contributing to the success of PKC 2010.

Finally, we would like to thank our sponsors Google, Ingenico, and Technicolor for their financial support and all the people involved in the organization of this conference. In particular, we would like to thank the Office for Courses and Colloquiums (*Bureau des Cours-Colloques*) from INRIA and Gaëlle Dorkeld, as well as Jacques Beigbeder and Joëlle Isnard from ENS, for their diligent work and for making this conference possible. We also wish to thank Springer for publishing the proceedings in the *Lecture Notes in Computer Science* series.

May 2010

Phong Q. Nguyen
David Pointcheval

PKC 2010

13th International Conference on
Practice and Theory in Public Key Cryptography

Paris, France, May 26–28, 2010

General Chairs

Michel Abdalla	CNRS and ENS, Paris, France
Pierre-Alain Fouque	ENS, Paris, France

Program Chairs

Phong Q. Nguyen	INRIA and ENS, Paris, France
David Pointcheval	CNRS, ENS and INRIA, Paris, France

Program Committee

Alexandra Boldyreva	Georgia Institute of Technology, USA
Xavier Boyen	University of Liege, Belgium
Dario Catalano	University of Catania, Italy
Jung Hee Cheon	Seoul National University, South Korea
Jean-Sébastien Coron	University of Luxembourg
Marc Fischlin	TU Darmstadt, Germany
Eiichiro Fujisaki	NTT Labs, Japan
Craig Gentry	IBM, USA
Maria Isabel Gonzalez Vasco	Universidad Rey Juan Carlos, Madrid, Spain
Stanislaw Jarecki	UC Irvine, California, USA
Jonathan Katz	University of Maryland, USA
Eike Kiltz	CWI, The Netherlands
Fabien Laguillaumie	University of Caen, France
Dong Hoon Lee	Korea University, Seoul, South Korea
Reynald Lercier	DGA/CELAR and University of Rennes, France
Benoît Libert	Université Catholique de Louvain, Belgium
Vadim Lyubashevsky	University of Tel-Aviv, Israel
Mark Manulis	TU Darmstadt and CASED, Germany
Alfred Menezes	University of Waterloo, Canada
Kenny Paterson	Royal Holloway, University of London, UK
Duong Hieu Phan	University of Paris 8, France
Benny Pinkas	University of Haifa, Israel
Alon Rosen	IDC Herzliya, Israel
Kazue Sako	NEC, Japan

Hovav Shacham	UC San Diego, California, USA
Igor Shparlinski	University of Macquarie, Sydney, Australia
Martijn Stam	EPFL, Switzerland
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Ramarathnam Venkatesan	Microsoft Research, Bangalore and Redmond, India and USA
Damien Vergnaud	ENS, Paris, France
Ivan Visconti	University of Salerno, Italy
Bogdan Warinschi	Bristol University, UK
Brent Waters	University of Texas, USA
Duncan Wong	City University of Hong Kong, China

External Reviewers

Michel Abdalla	Vanesa Daza
Divesh Aggarwal	Sebastiaan de Hoogh
Shweta Agrawal	Cécile Delerablée
Adi Akavia	Olivier de Marneffe
Koichiro Akiyama	Breno de Medeiros
Frederik Armknecht	Alexander W. Dent
Ali Bagherzandi	Claus Diem
Aurélie Bauer	Mario Di Raimondo
Amos Beimei	Vivien Dubois
Daniel J. Bernstein	Laila El Aimani
Raghav Bhaskar	Nadia El Mrabet
James Birkett	Pooya Farshim
Jens-Matthias Bohli	Anna Lisa Ferrara
Joppe Bos	Dario Fiore
Charles Bouillaguet	Jun Furukawa
John Boxall	David Galindo
Emmanuel Bresson	Nicolas Gama
Jin Wook Byun	Essam Ghadafi
David Cash	Domingo Gomez Perez
Guilhem Castagnos	Choudary Gorantla
Julien Cathalo	Vipul Goyal
Pierre-Louis Cayrel	Robert Granger
Sanjit Chatterjee	Matthew Green
Céline Chevalier	Thomas Gross
Kwantae Cho	Jens Groth
Kyu Young Choi	Jaime Gutierrez
Raymond Choo	Daewan Han
Ji Young Chun	Darrel Hankerson
Cas Cremers	Carmit Hazay
Maria Cristina Onete	Brett Hemenway
Özgür Dagdelen	Javier Herranz

Mathias Herrmann
Dennis Hofheinz
Thomas Holenstein
Jeongdae Hong
Qiong Huang
Jung Yeon Hwang
Thomas Icart
Toshiyuki Isshiki
Malika Izabachène
Tibor Jager
Ayman Jarrous
Haimin Jin
Seny Kamara
Koray Karabina
Akinori Kawachi
Yutaka Kawai
Mitsuru Kawazoe
Jihye Kim
Kitak Kim
Minkyu Kim
Myungsun Kim
Woo Kwon Koo
Takeshi Koshiba
Hugo Krawczyk
Virendra Kumar
Robin Künzler
Benoît Larroque
Hyung Tae Lee
Ji-Seon Lee
Kwangsu Lee
Munkyu Lee
Anja Lehmann
Arjen K. Lenstra
Allison Lewko
Yehuda Lindell
Xiaomin Liu
Satya Lokam
Julio Lopez
Xizhao Luo
Lior Malka
Toshihide Matsuda
Payman Mohassel
Tal Moran
Michael Naehrig
Toru Nakanishi
Gregory Neven
Ryo Nishimaki
Yasuyuki Nogami
Tatsuaki Okamoto
Josh Olsen
Adam O'Neill
Claudio Orlandi
Alina Ostafe
Adriana Palacio
Omkant Pandey
C. Pandu Rangan
Hyun-A Park
Jehong Park
Jong Hwan Park
Sylvain Pasini
Chris Peikert
Olivier Pereira
Angel L. Perez del Pozo
Bertram Poettering
Hyun Sook Rhee
Maike Ritzenhofen
Ben Riva
Francisco Rodriguez-Henriquez
Yannis Rouselakis
Ahmad-Reza Sadeghi
Alessandra Scafuro
Thomas Schneider
Berry Schoenmakers
Dominique Schröder
Michael Scott
Jae Hong Seo
Elaine Shi
Thomas Sirvent
William Skeith
Damien Stehlé
Mario Strefler
Willy Susilo
Koutarou Suzuki
Tamir Tassa
Edlyn Teske-Wilson
Berkant Ustaoglu
Vinod Vaikuntanathan
Carmine Ventre
Jorge L. Villar
Panagiotis Voulgaris

Christian Wachsmann
Christopher Wolf
Keita Xagawa
Xiaokang Xiong
Guomin Yang
Scott Yilek
Kazuki Yoneyama
Tsz Hon Yuen
Aaram Yun
Zongyang Zhang
Vassilis Zikas

Sponsors

Financial support by the following sponsors is gratefully acknowledged:

- ENS
- Google
- Ingenico
- Technicolor

Table of Contents

Tools

Elliptic Curves

Lossy Trapdoor Functions

Protocols II

Discrete Logarithm

Encryption II

Signatures