

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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

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.com

© International Association for Cryptologic Research 2010
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
Pierre-Alain Fouque

CNRS and ENS, Paris, France
ENS, Paris, France

Program Chairs

Phong Q. Nguyen
David Pointcheval

INRIA and ENS, Paris, France
CNRS, ENS and INRIA, Paris, France

Program Committee

Alexandra Boldyreva
Xavier Boyen
Dario Catalano
Jung Hee Cheon
Jean-Sébastien Coron
Marc Fischlin
Eiichi Fujisaki
Craig Gentry
Maria Isabel Gonzalez Vasco
Stanislaw Jarecki
Jonathan Katz
Eike Kiltz
Fabien Laguillaumie
Dong Hoon Lee
Reynald Lercier

Georgia Institute of Technology, USA
University of Liege, Belgium
University of Catania, Italy
Seoul National University, South Korea
University of Luxembourg
TU Darmstadt, Germany
NTT Labs, Japan
IBM, USA
Universidad Rey Juan Carlos, Madrid, Spain
UC Irvine, California, USA
University of Maryland, USA
CWI, The Netherlands
University of Caen, France
Korea University, Seoul, South Korea
DGA/CELAR and University of Rennes,
France

Benoît Libert
Vadim Lyubashevsky
Mark Manulis
Alfred Menezes
Kenny Paterson
Duong Hieu Phan
Benny Pinkas
Alon Rosen
Kazue Sako

Université Catholique de Louvain, Belgium
University of Tel-Aviv, Israel
TU Darmstadt and CASED, Germany
University of Waterloo, Canada
Royal Holloway, University of London, UK
University of Paris 8, France
University of Haifa, Israel
IDC Herzliya, Israel
NEC, Japan

VIII Organization

Hovav Shacham
Igor Shparlinski
Martijn Stam
Keisuke Tanaka
Ramarathnam Venkatesan

Damien Vergnaud
Ivan Visconti
Bogdan Warinschi
Brent Waters
Duncan Wong

UC San Diego, California, USA
University of Macquarie, Sydney, Australia
EPFL, Switzerland
Tokyo Institute of Technology, Japan
Microsoft Research, Bangalore and Redmond,
India and USA
ENS, Paris, France
University of Salerno, Italy
Bristol University, UK
University of Texas, USA
City University of Hong Kong, China

External Reviewers

Michel Abdalla
Divesh Aggarwal
Shweta Agrawal
Adi Akavia
Koichiro Akiyama
Frederik Armknecht
Ali Bagherzandi
Aur lie Bauer
Amos Beimei
Daniel J. Bernstein
Raghav Bhaskar
James Birkett
Jens-Matthias Bohli
Joppe Bos
Charles Bouillaguet
John Boxall
Emmanuel Bresson
Jin Wook Byun
David Cash
Guilhem Castagnos
Julien Cathalo
Pierre-Louis Cayrel
Sanjit Chatterjee
C line Chevalier
Kwantae Cho
Kyu Young Choi
Raymond Choo
Ji Young Chun
Cas Cremers
Maria Cristina Onete
 zg r Dagdelen

Vanesa Daza
Sebastiaan de Hoogh
C cile Delerabl e
Olivier de Marneffe
Breno de Medeiros
Alexander W. Dent
Claus Diem
Mario Di Raimondo
Vivien Dubois
Laila El Aïmani
Nadia El Mrabet
Pooya Farshim
Anna Lisa Ferrara
Dario Fiore
Jun Furukawa
David Galindo
Nicolas Gama
Essam Ghadafi
Domingo Gomez Perez
Choudary Gorantla
Vipul Goyal
Robert Granger
Matthew Green
Thomas Gross
Jens Groth
Jaime Gutierrez
Daewan Han
Darrel Hankerson
Carmit Hazay
Brett Hemenway
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
Kwangsue 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 Streffer
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

Encryption I

Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model	1
<i>Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup</i>	
Constant Size Ciphertexts in Threshold Attribute-Based Encryption	19
<i>Javier Herranz, Fabien Laguillaumie, and Carla Ràfols</i>	

Cryptanalysis

Algebraic Cryptanalysis of the PKC'2009 Algebraic Surface Cryptosystem	35
<i>Jean-Charles Faugère and Pierre-Jean Spaenlehauer</i>	
Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA	53
<i>Mathias Herrmann and Alexander May</i>	
Implicit Factoring with Shared Most Significant and Middle Bits	70
<i>Jean-Charles Faugère, Raphaël Marinier, and Guénaél Renault</i>	

Protocols I

On the Feasibility of Consistent Computations	88
<i>Sven Laur and Helger Lipmaa</i>	
Multi-query Computationally-Private Information Retrieval with Constant Communication Rate	107
<i>Jens Groth, Aggelos Kiayias, and Helger Lipmaa</i>	
Further Observations on Optimistic Fair Exchange Protocols in the Multi-user Setting	124
<i>Xinyi Huang, Yi Mu, Willy Susilo, Wei Wu, and Yang Xiang</i>	

Network Coding

Secure Network Coding over the Integers	142
<i>Rosario Gennaro, Jonathan Katz, Hugo Krawczyk, and Tal Rabin</i>	
Preventing Pollution Attacks in Multi-source Network Coding	161
<i>Shweta Agrawal, Dan Boneh, Xavier Boyen, and David Mandell Freeman</i>	

Tools

Groth-Sahai Proofs Revisited	177
<i>Essam Ghadafi, Nigel P. Smart, and Bogdan Warinschi</i>	
Constant-Round Concurrent Non-Malleable Statistically Binding Commitments and Decommitments.....	193
<i>Zhenfu Cao, Ivan Visconti, and Zongyang Zhang</i>	

Elliptic Curves

Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions	209
<i>Robert Granger and Michael Scott</i>	
Faster Pairing Computations on Curves with High-Degree Twists	224
<i>Craig Costello, Tanja Lange, and Michael Naehrig</i>	
Efficient Arithmetic on Hessian Curves	243
<i>Reza R. Farashahi and Marc Joye</i>	

Lossy Trapdoor Functions

CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model	261
<i>Toshihide Matsuda, Ryo Nishimaki, and Keisuke Tanaka</i>	
More Constructions of Lossy and Correlation-Secure Trapdoor Functions	279
<i>David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev</i>	
Chosen-Ciphertext Security from Slightly Lossy Trapdoor Functions	296
<i>Petros Mol and Scott Yilek</i>	

Protocols II

Efficient Set Operations in the Presence of Malicious Adversaries.....	312
<i>Carmit Hazay and Kobbi Nissim</i>	
Text Search Protocols with Simulation Based Security	332
<i>Rosario Gennaro, Carmit Hazay, and Jeffrey S. Sorensen</i>	

Discrete Logarithm

Solving a 676-Bit Discrete Logarithm Problem in $\text{GF}(3^{6n})$	351
<i>Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, and Tsuyoshi Takagi</i>	

Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval	368
<i>Steven D. Galbraith and Raminder S. Ruprai</i>	

Encryption II

Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation	384
<i>Nuttapong Attrapadung and Benoît Libert</i>	

Security of Encryption Schemes in Weakened Random Oracle Models (Extended Abstract)	403
<i>Akinori Kawachi, Akira Numayama, Keisuke Tanaka, and Keita Xagawa</i>	

Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes	420
<i>Nigel P. Smart and Frederik Vercauteren</i>	

Signatures

Unlinkability of Sanitizable Signatures	444
<i>Christina Brzuska, Marc Fischlin, Anja Lehmann, and Dominique Schröder</i>	

Confidential Signatures and Deterministic Signcryption	462
<i>Alexander W. Dent, Marc Fischlin, Mark Manulis, Martijn Stam, and Dominique Schröder</i>	

Identity-Based Aggregate and Multi-signature Schemes Based on RSA	480
<i>Ali Bagherzandi and Stanisław Jarecki</i>	

Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More	499
<i>Xavier Boyen</i>	

Author Index	519
---------------------------	-----