Lecture Notes in Computer Science 1751
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Hideki Imai   Yuliang Zheng (Eds.)

Public Key Cryptography

Third International Workshop
on Practice and Theory in
Public Key Cryptosystems, PKC 2000
Melbourne, Victoria, Australia, January 18-20, 2000
Proceedings

Springer

Volume Editors

Hideki Imai
University of Tokyo, Institute of Industrial Science, The Third Department
7-22-1, Roppongi, Minato-ku, Tokyo, 106-8558, Japan
E-mail: imai@iis.u-tokyo.ac.jp

Yuliang Zheng
Monash University, School of Computing and Information Technology
McMahons Road, Frankston, Melbourne, VIC 3199, Australia
E-mail: yzheng@fcit.monash.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Public key cryptography : proceedings / Third International Workshop on
Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne,
Victoria, Australia, January 18 - 20, 2000. Hideki Imai ; Yuliang Zheng (ed.).
- Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1751)
ISBN 3-540-66967-1

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-66967-1 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10719554 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The PKC2000 conference was held at the Melbourne Exhibition Centre, Victoria, Australia, January 18-20, 2000. It was the third conference in the international workshop series dedicated to practice and theory in public key cryptography.

The program committee of the conference received 70 full submissions from around the world, of which 31 were selected for presentation. All submissions were reviewed by experts in the relevant areas.

The program committee consisted of 19 experts in cryptography and data security drawn from the international research community, these being Chin-Chen Chang (National Chung Cheng University, Taiwan), Claude Crépeau (McGill University, Canada), Ed Dawson (Queensland University of Technology, Australia), Yvo Desmedt (Florida State University, USA), Hideki Imai (Co-chair, University of Tokyo, Japan), Markus Jakobsson (Bell Labs, USA), Kwangjo Kim (Information and Communications University, Korea), Arjen Lenstra (Citibank, USA), Tsutomu Matsumoto (Yokohama National University, Japan), David Naccache (Gemplus, France), Eiji Okamoto (University of Wisconsin-Milwaukee, USA), Tatsuaki Okamoto (NTT Labs, Japan), Josef Pieprzyk (University of Wollongong, Australia), Jean-Jacques Quisquater (Université Catholique de Louvain, Belgium), Nigel Smart (HP Labs Bristol, UK), Vijay Varadharajan (University of Western Sydney, Australia), Serge Vaudenay (Ecole Polytechnique Fédérale de Lausanne, Switzerland), Moti Yung (CertCo, USA), and Yuliang Zheng (Co-chair, Monash University, Australia). Members of the committee spent numerous hours in reviewing the submissions and providing advice and comments on the selection of papers.

The program committee also asked expert advice of many of their colleagues, including: Masayuki Abe, Kazumaro Aoki, Paul Ashley, Joonsang Baek, Olivier Baudron, Christophe Bidan, Dan Boneh, Colin Boyd, Chris Charnes, Jean-Sébastien Coron, Ed Dawson, Paul Dumais, Kenneth Finlayson, Pierre-Alain Fouque, Atsushi Fujioka, Chandana Gamage, Juan Garay, Hossein Ghodosi, Pierre Girard, Jean-Luc Giraud, Louis Granboulan, Marc Gysin, Stuart Haber, Helena Handschuh, Ari Juels, Tetsutaro Kobayashi, Byongcheon Lee, Wei-Bin Lee, Phil MacKenzie, Wenbo Mao, William Millan, David M'Raïhi, Yi Mu, Shinichi Nakahara, Kenny Nguyen, Phong Nguyen, David Pointcheval, Pascal Paillier, Ludovic Rousseau, Selwyn Russell, David Soldera, Stuart Stubblebine, Koutarou Suzuki, Christophe Tymen, Shigenori Uchiyama, Susanne Wetzel, Stefan Wolf, and Chuan-Kun Wu.

We would like to take this opportunity to thank all the program committee members and external experts for their invaluable help in producing such a high quality program. We are especially indebted to Chin-Chen Chang who made sure all the submissions assigned to him were properly reviewed in spite of the devastating earthquake and its countless aftershocks that rocked Taiwan in late September 1999.

The conference would not have been successful without the financial support from both Imai Laboratory (imailab-www.iis.u-tokyo.ac.jp) of the Institute of Industrial Science, University of Tokyo, and LINKS – Laboratory for Information and Network Security (www.pscit.monash.edu.au/links/) of the Faculty of Information Technology, Monash University. Our appreciation also goes to members of LINKS, including Jerald Chong, Chandana Gamage, Lionnel Heng, Khaled Khan, Jussi Leiwo, Patrik Mihailescu, and E-Yang Tang for their skillful and professional assistance in organizing this conference. Chandana Gamage deserves special thanks for helping out during the entire refereeing and editing process.

Last, but not least, we would like to thank all the authors who submitted their papers to the conference (including those whose submissions were not successful), as well as the conference participants from around the world, for their support which made this conference possible.

January 2000 Hideki Imai
Yuliang Zheng

PKC2000

2000 International Workshop on Practice and Theory in Public Key Cryptography

Melbourne Exhibition Centre, Australia
January 18-20, 2000

Sponsored by

Imai Laboratory of the Institute of Industrial Science,
University of Tokyo, Japan (imailab-www.iis.u-tokyo.ac.jp)
and
LINKS – Laboratory for Information and Network Security
of Monash University, Australia (www.pscit.monash.edu.au/links/)

Program Committee

Hideki Imai, Co-chair	(University of Tokyo, Japan)
Yuliang Zheng, Co-chair	(Monash University, Australia)
Chin-Chen Chang	(National Chung Cheng University, Taiwan)
Claude Crepeau	(McGill University, Canada)
Ed Dawson	(Queensland University of Technology, Australia)
Yvo Desmedt	(Florida State University, USA)
Markus Jakobsson	(Bell Labs, USA)
Kwangjo Kim	(Information and Communications University, Korea)
Arjen Lenstra	(Citibank, USA)
Tsutomu Matsumoto	(Yokohama National University, Japan)
David Naccache	(Gemplus, France)
Eiji Okamoto	(University of Wisconsin-Milwaukee, USA)
Tatsuaki Okamoto	(NTT Labs, Japan)
Josef Pieprzyk	(University of Wollongong, Australia)
Jean-Jacques Quisquater	(Université Catholique de Louvain, Belgium)
Nigel Smart	(HP Labs Bristol, UK)
Vijay Varadharajan	(University of Western Sydney, Australia)
Serge Vaudenay	(EPFL, Switzerland)
Moti Yung	(CertCo, USA)

Contents