

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

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

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'Raihi, 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

A Practical and Secure Fault-Tolerant Conference-Key Agreement Protocol	1
<i>Wen-Guey Tzeng (Nat Chiao Tung Uni, Taiwan)</i>	
An Efficient NICE-Schnorr-Type Signature Scheme	14
<i>Detlef Hühnlein, and Johannes Merkle (secunet, Germany)</i>	
Identification of Bad Signatures in Batches	28
<i>Jarosław Pastuszak, Dariusz Michalek (Polish Acad of Sci, Poland), Josef Pieprzyk, and Jennifer Seberry (Uni of Wollongong, Australia)</i>	
Some Remarks on a Fair Exchange Protocol	46
<i>Jianying Zhou, Robert Deng, and Feng Bao (Kent Ridge Digital Labs, Singapore)</i>	
Gaudry's Variant against C_{ab} Curves	58
<i>Seigo Arita (NEC, Japan)</i>	
An Identification Scheme Based on Sparse Polynomials	68
<i>William D. Banks, Daniel Lieman (Uni of Missouri, USA), and Igor E. Shparlinski (Macquarie Uni, Australia)</i>	
A State-Based Model for Certificate Management Systems	75
<i>Chuchang Liu, Maris A. Ozols, Marie Henderson, and Tony Cant (DSTO, Australia)</i>	
Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence	93
<i>Reto Kohlas, and Ueli Maurer (ETH, Switzerland)</i>	
The Composite Discrete Logarithm and Secure Authentication	113
<i>David Pointcheval (ENS, France)</i>	
Chosen-Ciphertext Security for Any One-Way Cryptosystem	129
<i>David Pointcheval (ENS, France)</i>	
Short Proofs of Knowledge for Factoring	147
<i>Guillaume Poupard, and Jacques Stern (ENS, France)</i>	
Secure and Practical Tree-Structure Signature Schemes Based on Discrete Logarithms	167
<i>X.Y.Wang (Uni of Hong Kong, and Shandong Uni, China), L.C.Hui, K.P.Chow, W.W.Tsang, C.F.Chong, and H.W.Chan (Uni of Hong Kong, China)</i>	

All-or-Nothing Transform and Remotely Keyed Encryption Protocols	178
<i>Sang Uk Shin, Weon Shin, and Kyung Hyune Rhee (PuKyong Nat Uni, Korea)</i>	
Security of Public Key Certificate Based Authentication Protocols	196
<i>Wu Wen, Takamichi Saito, and Fumio Mizoguchi (Sci Uni of Tokyo, Japan)</i>	
Efficient Implementation of Schoof's Algorithm in Case of Characteristic 2	210
<i>Tetsuya Izu, Jun Kogure, and Kazuhiro Yokoyama (Fujitsu Labs, Japan)</i>	
Key Recovery in Third Generation Wireless Communication Systems	223
<i>Juanma González Nieto (QUT, Australia), DongGook Park (QUT, Australia, and Korea Telecom), Colin Boyd, and Ed Dawson (QUT, Australia)</i>	
Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications	238
<i>Katsuyuki Okeya, Hiroyuki Kurumatani (Hitachi, Japan), and Kouichi Sakurai (Kyushu Uni, Japan)</i>	
Certificates of Recoverability with Scalable Recovery Agent Security	258
<i>Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)</i>	
Design Validations for Discrete Logarithm Based Signature Schemes	276
<i>Ernest Brickell (Intel, USA), David Pointcheval (ENS, France), Serge Vaudenay (EPFL, Switzerland), and Moti Yung (Certco, USA)</i>	
Optimally Efficient Accountable Time-Stamping	293
<i>Ahto Buldas, Helger Lipmaa (Küberneetika AS, Estonia), and Berry Schoenmakers (Eindhoven Uni of Tech, The Netherlands)</i>	
"Pseudorandom Intermixing": A Tool for Shared Cryptography	306
<i>Yair Frankel (CertCo, USA), Philip MacKenzie (Bell Labs, USA), and Moti Yung (CertCo, USA)</i>	
RSA-Based Auto-recoverable Cryptosystems	326
<i>Adam Young (Columbia Uni, USA), and Moti Yung (CertCo, USA)</i>	
Efficient and Fresh Certification	342
<i>Irene Gassko (Bell Labs, USA), Peter S. Gemmell (Uni of New Mexico, USA), and Philip MacKenzie (Bell Labs, USA)</i>	

Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions	354
<i>Ronald Cramer (ETH, Switzerland), Ivan Damgård (Aarhus Uni, Denmark), and Philip MacKenzie (Bell Labs, USA)</i>	
Cryptographic Approaches to Privacy in Forensic DNA Databases	373
<i>Philip Bohannon, Markus Jakobsson (Bell Labs, USA), and Sukamol Srikwan (Chulalongkorn Uni, Thailand)</i>	
Making Hash Functions from Block Ciphers Secure and Efficient by Using Convolutional Codes	391
<i>Toru Inoue (AMSL, Japan), and Kouichi Sakurai (Kyushu Uni, Japan)</i>	
Fast Implementation of Elliptic Curve Arithmetic in $GF(p^n)$	405
<i>Chae Hoon Lim, and Hyo Sun Hwang (Future Systems, Korea)</i>	
An Auction Protocol Which Hides Bids of Losers	422
<i>Kazue Sako (NEC, Japan)</i>	
Forward Secrecy and Its Application to Future Mobile Communications Security	433
<i>DongGook Park (QUT, Australia, and Korea Telecom), Colin Boyd (QUT, Australia), and Sang-Jae Moon (Kyungpook Nat Uni, Korea)</i>	
Selecting Cryptographic Key Sizes	446
<i>Arjen K. Lenstra (Citibank, USA), and Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)</i>	
A Structured ElGamal-Type Multisignature Scheme	466
<i>Mike Burmester (Royal Holloway, Uni of London, UK), Yvo Desmedt (Florida State Uni, USA), Hiroshi Doi (Okayama Uni, Japan), Masahiro Mambo (Tohoku Uni, Japan), Eiji Okamoto (Uni of Wisconsin, Milwaukee, USA), Mitsuru Tada, and Yuko Yoshifuji (JAIST, Japan)</i>	
Author Index	485