Lecture Notes in Computer Science 1992

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Kwangjo Kim (Ed.)

Public Key Cryptography

4th International Workshop on Practice and Theory
in Public Key Cryptosystems, PKC 2001
Cheju Island, Korea, February 13-15, 2001
Proceedings

Springer

Series Editors

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

Volume Editor

Kwangjo Kim
Information and Communications University, Information Security Group
58-4 Hwaam-dong, Yusong-gu, Taejon 305-732, Korea
E-mail: kkj@icu.ac.kr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Public key cryptography : proceedings / 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Cheju Island, Korea, February 13 - 15, 2001. Kwangjo Kim (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 1992)
ISBN 3-540-41658-7

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 3-540-41658-7 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingräber Satztechnik GmbH, Heidelberg
Printed on acid-free paper SPIN: 10782094 06/3142 5 4 3 2 1 0

Preface

The PKC 2001 conference was held at Shilla Hotel, Cheju Island, Korea, 13–15 February 2001. Continuing the first conference PKC 1988 in Yokohama, Japan, PKC 1999 in Kamakura, Japan, and PKC 2000 in Melbourne, Australia, PKC 2001, the fourth conference in the international workshop series was dedicated to practice and theory in public key cryptography.

The program committee of the conference received 67 submissions from 14 countries and regions (Australia, Austria, China, Denmark, Esponia, France, Germany, Greece, Korea, Singapore, Spain, Taiwan, UK, and USA), of which 30 were selected for presentation. All submissions were anonymously reviewed by at least 3 experts in the relevant areas. Revisions were not checked, and the authors bear full responsibility for the contents of their papers. In addition, there were three invited talks by Jun-Cheol Yang of the Ministry of Information and Communication, Korea; Mihir Bellare of the University of California at San Diego, USA; and Ko Itoh of the Organization for Road System Enhancement, Japan.

The program committee consisted of 20 experts in cryptography and data security drawn from the international research community: Kwangjo Kim (Chair, Information and Communications University, Korea), Claude Crepeau (McGill University, Canada), Ed Dawson (Queensland University of Technology, Australia), Yvo Desmedt (Florida State University, USA), Chi Sung Laih (National Cheng Kung University, Taiwan), Pil Joong Lee (POSTECH, 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), Choonsik Park (ETRI, Korea), Sung Jun Park (BCQRE, Korea), Josef Pieprzyk (University of Wollongong, Australia), Claus Schnorr (Frankfurt University, Germany), Nigel Smart (University of Bristol, UK), Jacques Stern (ENS, France), Susanne Wetzel (Bell Labs, USA), Moti Yung (CertCo, USA), and Yuliang Zheng (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 the expert advice of many of their colleagues, including: Ingrid Biehl, Colin Boyd, Marco Bucci, Gary Carter, Seong Taek Chee, Jean-Sébastien Coron, Nora Dabbous, Jean-François Dhem, Marc Fischlin, Roger Fischlin, Pierre Girard, Jaeseung Go, Juanma Gonzalez-Nieto, Helena Handschuh, Marie Henderson, Markus Jakobsson, Marc Joye, Jinho Kim, Seungjoo Kim, Ju Seung Kang, Tri V. Le, Byoungcheon Lee, Hyejoo Lee, Phil MacKenzie, David M'Raïhi, Renato Menicocci, Bernd Meyer, Pascal Paillier, Sang Joon Park, Béatrice Peirani, Jason Reid, Hein Roehrig, Amin Shokrollahi, Igor Shparlinski, Jessica Staddon, Ron Steinfeld, Christophe Tymen, and Kapali Viswanathan. We apologize for any omission in this list.

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.

Our appreciation also goes to members of C&IS Lab. (Cryptology and Information Security Laboratory), including Gookwhan Ahn, Jaeseung Go, Jinho Kim, Heesun Kim, Myungsun Kim, Manho Lee, Byoungcheon Lee, Jaegwan Park, Hyuncheol Park, and Boyeon Song for their skillful and professional assistance in organizing this conference. Choyoung Kim deserves special thanks for her help with preparation of the various tasks of the conference. We are also grateful to all the organizing committee members for their volunteer work.

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.

February 2001

Kwangjo Kim

PKC 2001

2001 International Workshop on Practice and Theory in Public Key Cryptography

Shilla Hotel, Cheju Island, Korea
13–15 February 2001

Sponsored by

Cryptology and Information Security Laboratory (C&IS Lab.)
of Information and Communications University
(caislab.icu.ac.kr)

In cooperation with

Korea Institute of Information Security and Cryptology (KIISC)
(www.kiisc.or.kr)

Under the Patronage of

Ministry of Information and Communication (MIC), Korea

Financially Supported by

Electronic and Telecommunications Research Institute (ETRI),
SAMSUNG SECUi.COM, STI (SECURITY Technologies Inc.),
BCQRE, KSIGN, SECUVE, and SOFTFORUM

General Co-chair

Hideki Imai	(University of Tokyo, Japan)
Kil-Hyun Nam	(Korea National Defense University, Korea)

Program Committee

Kwangjo Kim, Chair	(Information and Communications University, Korea)
Claude Crepeau	(McGill University, Canada)
Ed Dawson	(Queensland University of Technology, Australia)
Yvo Desmedt	(Florida State University, USA)
Chi Sung Laih	(National Cheng Kung University, Taiwan)
Pil Joong Lee	(POSTECH, 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)
Choonsik Park	(ETRI, Korea)
Sung Jun Park	(BCQRE, Korea)
Josef Pieprzyk	(University of Wollongong, Australia)
Claus Schnorr	(Frankfurt University, Germany)
Nigel Smart	(University of Bristol, UK)
Jacques Stern	(ENS, France)
Susanne Wetzel	(Bell Labs, USA)
Moti Yung	(CertCo, USA)
Yuliang Zheng	(Monash University, Australia)

Organizing Committee

Kyung Hyune Rhee, Chair	(Pukyong National University, Korea)
Donnie Choi	(STI, Korea)
Hyon Cheol Chung	(SOFTFORUM, Korea)
Ki-Yoong Hong	(KSIGN, Korea)
Kwangjo Kim	(Information and Communications University, Korea)
Kyong-Soo Oh	(SAMSUNG SECUi.COM, Korea)
Ji-Hwan Park	(Pukyong National University, Korea)
Dae Hyun Ryu	(Hansei University, Korea)

Table of Contents

On the Security of a Williams Based Public Key Encryption Scheme 1
Siguna Müller (Univ. of Klagenfurt, Austria)

Semantically Secure McEliece Public-Key Cryptosystems – Conversions for McEliece PKC – 19
Kazukuni Kobara and Hideki Imai (Univ. of Tokyo, Japan)

IND-CCA Public Key Schemes Equivalent to Factoring $n = pq$ 36
Kaoru Kurosawa, Wakaha Ogata, Toshihiko Matsuo, and Shuichi Makishima, (Tokyo Inst. of Tech., Japan)

Identification, Signature and Signcryption Using High Order Residues Modulo an RSA Composite 48
Yuliang Zheng (Monash Univ., Australia)

On the Security of Lenstra's Variant of DSA without Long Inversions 64
Arjen K. Lenstra (Citibank, USA) and Igor E. Shparlinski (Macquarie Univ., Australia)

Fast Irreducibility and Subgroup Membership Testing in XTR 73
Arjen K. Lenstra (Citibank, USA) and Eric R.Verheul (PricewarterhouseCoopers, Netherlands)

A New Aspect for Security Notions: Secure Randomness in Public-Key Encryption Schemes 87
Takeshi Koshiba (Fujitsu, Japan)

The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes 104
Tatsuaki Okamoto (NTT, Japan) and David Pointcheval (ENS, France)

A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System 119
Ivan Damgård and Mads Jurik (Univ. of Aarhus, Denmark)

Marking: A Privacy Protecting Approach Against Blackmailing 137
Dennis Kügler and Holger Vogt (Darmstadt Univ. of Tech., Germany)

Cryptanalysis of Two Sparse Polynomial Based Public Key Cryptosystems 153
Feng Bao, Robert H. Deng (Kent Ridge Digital Labs, Singapore), Willi Geiselmann (Univ. of Karlsruhe, Germany), Claus Schnorr (Frankfurt Univ., Germany), Rainer Steinwandt (Univ. of Karlsruhe, Germany), and Hongjun Wu (Kent Ridge Digital Labs, Singapore)

Cryptanalysis of PKP: A New Approach 165
Éliane Jaulmes and Antoine Joux (DCSSI, France)

Cryptanalysis of a Digital Signature Scheme
on ID-Based Key-Sharing Infrastructures 173
Hongjun Wu, Feng Bao,
and Robert H. Deng (Kent Ridge Digital Labs, Singapore)

Loopholes in Two Public Key Cryptosystems
Using the Modular Group 180
Rainer Steinwandt (Univ. of Karlsruhe, Germany)

Efficient Revocation in Group Signatures 190
Emmanuel Bresson and Jacques Stern (ENS, France)

A Public-Key Traitor Tracing Scheme with Revocation
Using Dynamic Shares 207
Wen-Guey Tzeng
and Zhi-Jia Tzeng (Nat. Chiao Tung Univ., Taiwan)

Efficient Asymmetric Self-Enforcement Scheme
with Public Traceability 225
Hirotaka Komaki, Yuji Watanabe, Goichiro Hanaoka,
and Hideki Imai (Univ. of Tokyo, Japan)

Adaptive Security for the Additive-Sharing
Based Proactive RSA 240
Yair Frankel (Ecash Tech., USA),
Philip D. MacKenzie (Bell Labs, USA),
and Moti Yung (CertCo, USA)

Robust Forward-Secure Signature Schemes with Proactive Security 264
Wen-Guey Tzeng
and Zhi-Jia Tzeng (Nat. Chiao Tung Univ., Taiwan)

Equitability in Retroactive Data Confiscation
versus Proactive Key Escrow 277
Yvo Desmedt (Florida State Univ., USA),
Mike Burmester (Royal Holloway Univ. of London, UK),
and Jennifer Seberry (Univ. of Wollongong, Australia)

A PVSS as Hard as Discrete Log and Shareholder Separability 287
Adam Young (Columbia Univ., USA) and Moti Yung (CertCo, USA)

One Round Threshold Discrete-Log Key Generation
without Private Channels 300
Pierre-Alain Fouque and Jacques Stern (ENS, France)

Remarks on Mix-Network Based on Permutation Networks 317
Masayuki Abe and Fumitaka Hoshino (NTT, Japan)

New Key Recovery in WAKE Protocol 325
Chong Hee Kim and Pil Joong Lee (POSTECH, Korea)

Redundant Representation of Finite Fields 339
Willi Geiselmann
and Harald Lukhaub (Univ. of Karlsruhe, Germany)

Compact Encoding of Non-adjacent Forms
with Applications to Elliptic Curve Cryptography 353
Marc Joye and Christophe Tymen (Gemplus, France)

Efficient Implementation of Elliptic Curve Cryptosystems
on the TI MSP430x33x Family of Microcontrollers 365
Jorge Guajardo (WPI, USA), Rainer Blümel,
Uwe Krieger (Cryptovision, Germany), and Christof Paar (WPI, USA)

Secure Server-Aided Signature Generation 383
Markus Jakobsson and Susanne Wetzel (Bell Labs, USA)

Efficient Long-Term Validation of Digital Signatures 402
Arne Ansper, Ahto Buldas,
Meelis Roos, and Jan Willemson (Cybernetica, Estonia)

A Novel Systolic Architecture for an Efficient RSA Implementation 416
Nikos K. Moshopoulos
and K. Z. Pekmestzi (Nat. Tech. Univ. of Athens, Greece)

Author Index 423