

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

1431

Hideki Imai Yuliang Zheng (Eds.)

Public Key Cryptography

First International Workshop on Practice and
Theory in Public Key Cryptography, PKC'98
Pacifico Yokohama, Japan, February 5-6, 1998
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
The University of Tokyo, Institute of Industrial Science
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 / First International
Workshop on Practice and Theory in Public Key Cryptography, PKC
'98, Pacifico Yokohama, Japan, February 1998. Hideki Imai ; Yuliang
Zheng (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest
; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ;
Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1431)
ISBN 3-540-64693-0**

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1,
E.4

ISSN 0302-9743

ISBN 3-540-64693-0 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10637613 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

The PKC'98 conference, held at Pacifico Yokohama, Japan, 5-6 February, 1998, is the first conference in a new international workshop series dedicated to both practice and theory in public key cryptography.

With the widespread use of public key cryptography in electronic commerce, good practice in applying public key and related supporting technologies, together with prudent assessment and comparison of the technologies, has become more important than ever. The new workshop series provides a unique avenue for both practitioners and theoreticians who are working on public key encryption, digital signature, one-way hashing, and their applications to share their experience and research outcomes.

Exactly 20 years ago, in 1978 Rivest, Shamir, and Adleman published what is now commonly called the RSA cryptosystem (see R. L. Rivest, A. Shamir, and L. Adleman: "A method for obtaining digital signatures and public-key cryptosystems," in *Communications of the ACM*, pp. 120-128, no. 2, vol. 21, 1978.) RSA is the first public key cryptosystem that fulfills both the functions of secure public key encryption and digital signature, and hence arguably the most significant discovery in cryptography. While the mathematical foundation of RSA rests on the intractability of factoring large composite integers, in the same year and the same journal Merkle demonstrated that certain computational puzzles could also be used in constructing public key cryptography (see R. Merkle: "Secure communication over insecure channels," in *Communications of the ACM*, pp. 294-299, no. 4, vol. 21, 1978.) Therefore, it is indeed very timely to hold PKC'98 at a time we are celebrating the 20th anniversary of the discovery of the RSA public key cryptosystem and Merkle's computational puzzles.

The program committee of the conference consisted of Hideki Imai of University of Tokyo, Japan, Arjen Lenstra of Citibank, USA, Tatsuaki Okamoto of NTT, Japan, Jacques Stern of ENS, France, and Yuliang Zheng of Monash University, Australia. Hideki Imai and Yuliang Zheng also served as the co-chairs of the committee. There were in total 30 submissions representing 12 countries and regions, these being Australia, Belgium, France, Germany, Japan, Korea, Singapore, Spain, Taiwan, Tunisia, UK, and USA. From among these submissions 15 were selected for presentation at the conference. In addition, there were 3 invited talks (by Yair Frankel and Moti Yung of CertCo, USA, Jean-Francois Misarsky of France Telecom, and Kiyomichi Araki of Tokyo Institute of Technology, Takakazu Satoh of Saitama University, and Shinji Miura of Sony Corporation, Japan) and a special talk (by Jacques Stern of ENS, France). The last session (Recent Results) of the conference was allocated to short talks on latest research results. There were 6 short talks, 3 of which were selected for inclusion into the final proceedings. Taking this opportunity, we would like to thank all the members of the program committee for putting together such an excellent technical program.

This conference was kindly sponsored by Information-Technology Promotion Agency (IPA) of Japan, Mitsubishi Electric Corporation, and Institute of Industrial Science, the University of Tokyo. It was held in cooperation with the Technical Group on Information Security, the Institute of Electronics, Information, and Communication Engineers (IEICE). We appreciate all these organizations for their generous support and cooperation.

Successfully organizing such a relatively large international conference would not have been possible without the assistance from the secretaries (especially Y. Umemura, M. Morimoto, and Y. Nejime), students, research assistants, and associates from the Imai Laboratory at Institute of Industrial Science.

Our thanks also go to the following colleagues who kindly offered help with chairing sessions at the conference: Kiyomichi Araki (Tokyo Institute of Technology, Japan), Chin-Chen Chang (National Chung Cheng University, Taiwan), Arjen Lenstra (Citibank, USA), Tsutomu Matsumoto (Yokohama National University, Japan), Jean-Francois Misarsky (France Telecom), Eiji Okamoto (JAIST, Japan), Tatsuaki Okamoto (NTT, Japan), Jacques Stern (ENS, France), and Moti Yung (CertCo, USA).

Finally we would like to thank all the people who submitted their papers to the conference (including those whose submissions were not successful), and all the 145 delegates from around the world who attended the conference. Without their support the conference would not have been possible.

March 1998
University of Tokyo, Japan
Monash University, Melbourne, Australia

Hideki Imai
Yuliang Zheng

PKC'98

1998 International Workshop on Practice and Theory in Public Key Cryptography Pacifco Yokohama, Japan, 5-6 February, 1998

Sponsored by

Information-Technology Promotion Agency (IPA), Japan
Mitsubishi Electric Corporation
Institute of Industrial Science, the University of Tokyo

In cooperation with

The Technical Group on Information Security, the Institute of
Electronics, Information and Communication Engineers (IEICE)

Organizing Committee

Hideki Imai, Co-chair	(University of Tokyo, Japan)
Yuliang Zheng, Co-chair	(Monash University, Australia)
Members of Imai Lab	(University of Tokyo, Japan)

Program Committee

Hideki Imai, Co-chair	(University of Tokyo, Japan)
Arjen Lenstra	(Citibank, USA)
Tatsuaki Okamoto	(NTT, Japan)
Jacques Stern	(ENS, France)
Yuliang Zheng, Co-chair	(Monash University, Australia)

Contents

Invited Talks

Distributed public key cryptosystems	1
<i>Yair Frankel and Moti Yung (CertCo, USA)</i>	
How (not) to design RSA signature schemes	14
<i>Jean-François Misarsky (France Telecom)</i>	
Overview of elliptic curve cryptography	29
<i>Kiyomichi Araki (Tokyo Inst of Tech, Japan), Takakazu Satoh (Saitama Uni, Japan) and Shinji Miura (Sony, Japan)</i>	

Special Talk

Lattices and cryptography: An overview	50
<i>Jacques Stern (ENS, France)</i>	

Regular Contributions

A signcryption scheme with signature directly verifiable by public key	55
<i>Feng Bao and Robert H. Deng (Nat Uni of Singapore)</i>	
Guaranteed correct sharing of integer factorization with off-line shareholders	60
<i>Wenbo Mao (HP Labs Bristol, UK)</i>	
Lower bounds on term-based divisible cash systems	72
<i>Tatsuaki Okamoto (NTT, Japan) and Moti Yung (CertCo, USA)</i>	
Certifying trust	83
<i>Ilari Lehti and Pekka Nikander (Helsinki Uni of Tech, Finland)</i>	
On the security of server-aided RSA protocols	99
<i>Johannes Merkle and Ralph Werchner (Uni of Frankfurt, Germany)</i>	

On the security of ElGamal-based encryption	117
<i>Yiannis Tsiounis (GTE Labs, USA) and Moti Yung (CertCo, USA)</i>	
An authenticated Diffie-Hellman key agreement protocol secure against active attacks	135
<i>Shouichi Hirose and Susumu Yoshida (Kyoto Uni, Japan)</i>	
On the security of Girault's identification scheme	149
<i>Shahrokh Saeednia (Uni Libre de Bruxelles, Belgium) and Rei Safavi-Naini (Uni of Wollongong, Australia)</i>	
A scheme for obtaining a message from the digital multisignature	154
<i>Chin-Chen Chang, Jyh-Jong Leu, Pai-Cheng Huang and Wei-Bin Lee (Nat Chung Cheng Uni, Taiwan)</i>	
Secure hyperelliptic cryptosystems and their performance	164
<i>Yasuyuki Sakai (MELCO, Japan), Kouichi Sakurai (Kyushu Uni, Japan) and Hirokazu Ishizuka (MELCO, Japan)</i>	
A practical implementation of elliptic curve cryptosystems over GF(p) on a 16 bit microcomputer	182
<i>Toshio Hasegawa, Junko Nakajima and Mitsuru Matsui (MELCO, Japan)</i>	
Two efficient algorithms for arithmetic of elliptic curves using Frobenius map	195
<i>Jung Hee Cheon, Sungmo Park, Sangwook Park and Daeho Kim (ETRI, Korea)</i>	
Public-key cryptosystems using the modular group	203
<i>Akihiro Yamamura (TAO, Japan)</i>	
A cellular automaton based fast one-way hash function suitable for hardware implementation	217
<i>Miodrag Mihajević (Acad of Sci and Arts, Yugoslavia), Yuliang Zheng (Monash Uni, Australia) and Hideki Imai (Uni of Tokyo, Japan)</i>	
A new hash function based on MDx-family and its application to MAC	234
<i>Sang Uk Shin, Kyung Hyune Rhee (Pukyong Nat Uni, Korea), Dae Hyun Ryu and Sang Jin Lee (Elect and Telec Res Inst, Korea)</i>	

Recent Results

Security issues for contactless smart cards	247
<i>Michael W. David (CUBIC, USA) and Kouichi Sakurai (Kyushu Uni, Japan)</i>	
Parameters for secure elliptic curve cryptosystem – improvements on Schoof’s algorithm	253
<i>Tetsuya Izu, Jun Kogure, Masayuki Noro and Kazuhiro Yokoyama (Fujitsu, Japan)</i>	
A note on the complexity of breaking Okamoto-Tanaka ID-based key exchange scheme	258
<i>Masahiro Mambo and Hiroki Shizuya (Tohoku Uni, Japan)</i>	
Author Index	263