Lecture Notes in Computer Science 1431
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

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 — Hideki Imai
Monash University, Melbourne, Australia — Yuliang Zheng

PKC'98

1998 International Workshop on Practice and Theory in Public Key Cryptography

Pacifico 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

Special Talk

Regular Contributions

Recent Results