Feng Bao
Robert Deng
Jianying Zhou (Eds.)

LNCS 2947

Public Key Cryptography – PKC 2004

7th International Workshop
on Theory and Practice in Public Key Cryptography
Singapore, March 2004, Proceedings

c
i
a
r

Springer

Lecture Notes in Computer Science 2947
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Feng Bao Robert Deng
Jianying Zhou (Eds.)

Public Key Cryptography – PKC 2004

7th International Workshop
on Theory and Practice in Public Key Cryptography
Singapore, March 1-4, 2004
Proceedings

Springer

Volume Editors

Feng Bao
Robert Deng
Jianying Zhou
Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
E-mail: {baofeng,deng,jyzhou}@i2r.a-star.edu.sg

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-21018-0 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10987001 06/3142 5 4 3 2 1 0

Preface

PKC 2004 was the 7th International Workshop on Practice and Theory in Public Key Cryptography and was sponsored by IACR, the International Association for Cryptologic Research (www.iacr.org). This year the workshop was organized in cooperation with the Institute for Infocomm Research (I^2R), Singapore.

There were 106 paper submissions from 19 countries to PKC 2004. That is the highest submission number in PKC history. Due to the large number of submissions and the high quality of the submitted papers, not all the papers that contained new ideas were accepted. Of the 106 submissions, 32 were selected for the proceedings. Each paper was sent to at least 3 members of the Program Committee for comments. The revised versions of the accepted papers were not checked for correctness of their scientific aspects and the authors bear the full responsibility for the contents of their papers. Some authors will write final versions of their papers for publication in refereed journals.

I am very grateful to the members of the Program Committee for their hard work in the difficult task of selecting fewer than 1 in 3 of the submitted papers, as well as the following external referees who helped the Program Committee: Nuttapong Attrapadung, Roberto Maria Avanzi, Gildas Avoine, Joonsang Baek, Qingjun Cai, Jae Choon Cha, Chien-Ning Chen, Liqun Chen, Xiaofeng Chen, Koji Chida, Nicolas T. Courtois, Yang Cui, Jean-François Dhem, Louis Goubin, Louis Granboulan, Rob Granger, Jens Groth, Yumiko Hanaoka, Darrel Hankerson, Chao-Chih Hsu, Tetsutaro Kobayashi, Yuichi Komano, Hidenori Kuwakado, Tanja Lange, Peter Leadbitter, Byoungcheon Lee, Chun-Ko Lee, Henry C.J. Lee, John Malone Lee, Yong Li, Benoît Libert, Hsi-Chung Lin, Yi Lu, Jean Monnerat, Anderson C.A. Nascimento, C. Andrew Neff, Akira Otsuka, Daniel Page, Kenny Paterson, Kun Peng, David Pointcheval, Taiichi Saitoh, Junji Shikata, Igor Shparlinksi, Martijn Stam, Ron Steinfeld, Koutarou Suzuki, Shigenori Uchiyama, Frederik Vercauteren, Guilin Wang, Benne de Weger, Guohua Xiong, Go Yamamoto, Shoko Yonezawa, Rui Zhang, and Huafei Zhu. (I apologize for any possible omission.) The Program Committee appreciates their efforts.

Thanks to Patricia Loh for the secretarial work and to Ying Qiu for maintaining the WWW page of the conference. Finally, I would like to thank everyone who submitted to PKC 2004, and IACR for its sponsorship.

December 2003 Feng Bao

PKC 2004

7th International Workshop on Practice and Theory in Public Key Cryptography

Singapore
March 1–4, 2004

Sponsored and organized by

Institute for Infocomm Research, Singapore

In co-operation with

International Association for Cryptologic Research

General Chair

Robert Deng	Institute for Infocomm Research, Singapore

Program Chair

Feng Bao	Institute for Infocomm Research, Singapore

Publication Chair

Jianying Zhou	Institute for Infocomm Research, Singapore

Program Committee

Masayuki Abe	NTT Laboratories, Japan
Feng Bao	Institute for Infocomm Research, Singapore
Colin Boyd	Queensland University of Technology, Australia
Robert Deng	Institute for Infocomm Research, Singapore
Yvo Desmedt	Florida State University, USA
Marc Fischlin	Fraunhofer Institute for Secure Telecooperation, Germany
Eiichiro Fujisaki	NTT Laboratories, Japan
Goichiro Hanaoka	University of Tokyo, Japan
Marc Joye	Gemplus, France
Kwangjo Kim	Information and Communications University, Korea
Arjen Lenstra	Citibank, USA and Tech. Uni. Eindhoven, Netherlands
Wenbo Mao	Hewlett-Packard Labs, UK
Alfred Menezes	University of Waterloo, Canada
Phong Nguyen	CNRS/École Normale Supérieure, France
Dingyi Pei	Chinese Academy of Sciences, China
Claus Schnorr	Frankfurt University, Germany

Nigel Smart	University of Bristol, UK
Renji Tao	Chinese Academy of Sciences, China
Serge Vaudenay	Swiss Federal Institute of Technology, Switzerland
Sung-Ming Yen	National Central University, Taiwan
Moti Yung	Columbia University, USA
Yuliang Zheng	University of North Carolina, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Table of Contents