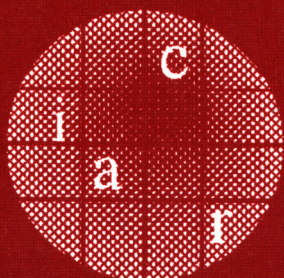


LNCS 2947

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 2004, Proceedings



Springer

Lecture Notes in Computer Science

2947

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

IST 2858

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

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

Series Editors

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

Volume Editors

Feng Bao
 Robert Deng
 Jianying Zhou
 Institute for Infocomm Research
 21 Heng Mui Keng Terrace, Singapore 119613
 E-mail: {fbaofeng,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

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 is a part of Springer Science+Business Media

springeronline.com

© International Association for Cryptologic Research 2004
 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 (I²R), 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, Benoit 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

BIBLIOTHEQUE DU CERIST

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
 Cclin 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

VIII Organization

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

A Generalized Wiener Attack on RSA	1
<i>Johannes Blömer and Alexander May</i>	
Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem	14
<i>Jean-Sébastien Coron</i>	
Faster Scalar Multiplication on Koblitz Curves Combining Point Halving with the Frobenius Endomorphism	28
<i>Roberto Maria Avanzi, Mathieu Ciet, and Francesco Sica</i>	
Application of Montgomery's Trick to Scalar Multiplication for Elliptic and Hyperelliptic Curves Using a Fixed Base Point	41
<i>Pradeep Kumar Mishra and Palash Sarkar</i>	
Fast Arithmetic on Jacobians of Picard Curves	55
<i>Stéphane Flon and Roger Oyono</i>	
Undeniable Signatures Based on Characters: How to Sign with One Bit ..	69
<i>Jean Monnerat and Serge Vaudenay</i>	
Efficient Extension of Standard Schnorr/RSA Signatures into Universal Designated-Verifier Signatures	86
<i>Ron Steinfeld, Huaxiong Wang, and Josef Pieprzyk</i>	
Constructing Committed Signatures from Strong-RSA Assumption in the Standard Complexity Model	101
<i>Huafei Zhu</i>	
Constant Round Authenticated Group Key Agreement via Distributed Computation	115
<i>Emmanuel Bresson and Dario Catalano</i>	
Efficient ID-based Group Key Agreement with Bilinear Maps	130
<i>Kyu Young Choi, Jung Yeon Hwang, and Dong Hoon Lee</i>	
New Security Results on Encrypted Key Exchange	145
<i>Emmanuel Bresson, Olivier Chevassut, and David Pointcheval</i>	
New Results on the Hardness of Diffie-Hellman Bits	159
<i>María Isabel González Vasco, Mats Näslund, and Igor E. Shparlinski</i>	
Short Exponent Diffie-Hellman Problems	173
<i>Takeshi Koshiba and Kaoru Kurosawa</i>	

Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups	187
<i>Benoît Libert and Jean-Jacques Quisquater</i>	
Algebraic Attacks over $GF(2^k)$, Application to HFE Challenge 2 and Sflash-v2	201
<i>Nicolas T. Courtois</i>	
Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$...	218
<i>Alexander May</i>	
General Group Authentication Codes and Their Relation to “Unconditionally-Secure Signatures”	231
<i>Reihaneh Safavi-Naini, Luke McAven, and Moti Yung</i>	
From Digital Signature to ID-based Identification/Signature	248
<i>Kaoru Kurosawa and Swee-Huay Heng</i>	
Identity-Based Threshold Decryption	262
<i>Joonsang Baek and Yuliang Zheng</i>	
An Efficient Signature Scheme from Bilinear Pairings and Its Applications	277
<i>Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo</i>	
An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications	291
<i>Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka</i>	
A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation	305
<i>Jintai Ding</i>	
Efficient, Verifiable Shuffle Decryption and Its Requirement of Unlinkability	319
<i>Jun Furukawa</i>	
A Point Compression Method for Elliptic Curves Defined over $GF(2^n)$...	333
<i>Brian King</i>	
On the Optimal Parameter Choice for Elliptic Curve Cryptosystems Using Isogeny	346
<i>Toru Akishita and Tsuyoshi Takagi</i>	
On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?	360
<i>Rui Zhang, Goichiro Hanaoka, Junji Shikata, and Hideki Imai</i>	
QuasiModo: Efficient Certificate Validation and Revocation	375
<i>Farid F. Elwailly, Craig Gentry, and Zulfikar Ramzan</i>	

A Distributed Online Certificate Status Protocol with a Single Public Key	389
<i>Satoshi Koga and Kouichi Sakurai</i>	
A First Approach to Provide Anonymity in Attribute Certificates	402
<i>Vicente Benjumea, Javier Lopez, Jose A. Montenegro, and Jose M. Troya</i>	
A Nonuniform Algorithm for the Hidden Number Problem in Subgroups	416
<i>Igor E. Shparlinski and Arne Winterhof</i>	
Cryptographic Randomized Response Techniques	425
<i>Andris Ambainis, Markus Jakobsson, and Helger Lipmaa</i>	
A Correct, Private, and Efficient Mix Network	439
<i>Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan</i>	
Author Index	455