Lecture Notes in Computer Science 2274
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

David Naccache Pascal Paillier (Eds.)

Public Key Cryptography

5th International Workshop on Practice and Theory
in Public Key Cryptosystems, PKC 2002
Paris, France, February 12-14, 2002
Proceedings

Springer

Series Editors

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

Volume Editors

David Naccache
Pascal Paillier
Gemplus International, Cryptography and Security Group
34 Rue Guynemer, 92447 Issy-le-Moulineaux, France
E-mail: {David.Naccache/Pascal.Paillier}@gemplus.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Public key cryptography : proceedings / 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12 - 14, 2002. David Naccache ; Pascal Paillier (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2274)
ISBN 3-540-43168-3

CR Subject Classification (1998): E.3, F.2.0, C.2.0

ISSN 0302-9743
ISBN 3-540-43168-3 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Steingräber Satztechnik GmbH, Heidelberg
Printed on acid-free paper SPIN 10846181 06/3142 5 4 3 2 1 0

Preface

The International Workshop on Practice and Theory in Public Key Cryptography PKC 2002 was held at the Maison de la Chimie, situated in the very center of Paris, France from February 12 to 14, 2002. The PKC series of conferences yearly represents international research and the latest achievements in the area of public key cryptography, covering a wide spectrum of topics, from cryptosystems to protocols, implementation techniques or cryptanalysis. After being held in four successive years in pacific-asian countries, PKC 2002 experienced for the first time a European location, thus showing its ability to reach an ever wider audience from both the industrial community and academia.

We are very grateful to the 19 members of the Program Committee for their hard and efficient work in producing such a high quality program. In response to the call for papers of PKC 2002, 69 papers were electronically received from 13 different countries throughout Europe, America, and the Far East. All submissions were reviewed by at least three members of the program committee, who eventually selected the 26 papers that appear in these proceedings. In addition to this program, we were honored to welcome Prof. Bart Preneel who kindly accepted to give this year's invited talk. The program committee gratefully acknowledges the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, Seigo Arita, Olivier Baudron, Mihir Bellare, Emmanuel Bresson, Eric Brier, Mathieu Ciet, Alessandro Conflitti, Jean-Sébastien Coron, Roger Fischlin, Pierre-Alain Fouque, Matt Franklin, Rosario Genarro, Marc Girault, Louis Granboulan, Goichiro Hanaoka, Darrel Hankerson, Eliane Jaulmes, Ari Juels, Jinho Kim, Marcos Kiwi, Kazukuni Kobara, Francois Koeune, Byoungcheon Lee, A. K. Lenstra, Pierre Loidreau, Wenbo Mao, Gwenaelle Martinet, Yi Mu, Phong Nguyen, Satoshi Obana, Guillaume Poupard, Yasuyuki Sakai, Hideo Shimizu, Tom Shrimpton, Ron Steinfeld, Katsuyuki Takashima, Huaxiong Wang, and Yuji Watanabe. Julien Brouchier deserves special thanks for skillfully maintaining the program committee's website and patiently helping out during the refereeing process.

Finally, we wish to thank all the authors who committed their time by submitting papers (including those whose submissions were not successful), thus making this conference possible, as well as the participants, organizers, and contributors from around the world for their kind support.

December 2001 David Naccache, Pascal Paillier

PKC 2002

Fifth International Workshop on Practice and Theory in Public Key Cryptography

Maison de la Chimie, Paris, France
February 12–14, 2002

Program Committee

David Naccache (Program Chair) ..... Gemplus, France

Daniel Bleichenbacher ..... Bell Labs, Lucent Technologies, USA
Yvo Desmedt ..... Florida State University, USA
Marc Fischlin ..... Goethe-University of Frankfurt, Germany
Shai Halevi ..... IBM T. J. Watson Research Center, USA
Markus Jakobsson ..... RSA Laboratories, USA
Antoine Joux ..... DCSSI, France
Burt Kaliski ..... RSA Laboratories, USA
Kwangjo Kim ..... Information and Communications University, Korea
Eyal Kushilevitz ..... Technion, Israel
Pascal Paillier ..... Gemplus, France
David Pointcheval ..... École Normale Supérieure, France
Jean-Jacques Quisquater ..... Université Catholique de Louvain, Belgium
Phillip Rogaway ..... UC Davis, USA
Kazue Sako ..... NEC Corporation, Japan
Bruce Schneier ..... Counterpane Internet Security, USA
Junji Shikata ..... University of Tokyo, Japan
Igor Shparlinski ..... Macquarie University, Australia
Moti Yung ..... Certco, USA
Jianying Zhou ..... Oracle Corporation, USA

Table of Contents

Protocols II

Cryptanalysis

Side Channels

Invited Talk

ECC Implementations

Applications