Lecture Notes in Computer Science 2567
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Yvo G. Desmedt (Ed.)

Public Key Cryptography – PKC 2003

6th International Workshop
on Practice and Theory in Public Key Cryptography
Miami, FL, USA, January 6-8, 2003
Proceedings

Springer

Series Editors

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

Volume Editor

Yvo G. Desmedt
Florida State University
Department of Computer Science
253 Love Building, Tallahassee, FL 32306-4530, USA
E-mail: desmedt@cs.fsu.edu

Cataloging-in-Publication Data applied for

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

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

ISSN 0302-9743
ISBN 3-540-00324-X Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN 10871877 06/3142 5 4 3 2 1 0

Preface

PKC 2003 was the Sixth 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 Department of Computer Science, Florida State University. The General Chair, Mike Burmester was responsible for local organization, registration, etc.

There were 105 submitted papers which were considered by the Program Committee. This is an increase of 52% compared to PKC 2002, which took place in Paris, France, February 2002, and which was incorrectly identified on the cover of the proceedings as being the fourth workshop. Due to the large number of submissions, some papers that contained new ideas had to be rejected. Priority was given to novel papers. Of the 105 submissions, 26 were selected for the proceedings. These contain the revised versions of the accepted papers. Each paper was sent to at least 3 members of the program committee for comments. Revisions were not checked for correctness of their scientific aspects and the authors bear 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 roughly 1 out of 4 of the submitted papers. Submissions to PKC 2003 were required to be anonymous. A Program Committee member could only present one accepted paper, or co-author at most two accepted papers without being allowed to present these. Papers submitted by members of the Program Committee were sent to at least 4 referees (and, of course, no Program Committee member reviewed his or her own paper).

The following external referees helped the Program Committee in reaching its decisions: Mehdi-Laurent Akkar, Joonsang Baek, Endre Bangerter, Régis Bevan, Daniel Bleichenbacher, Emmanuel Bresson, Eric Brier, Jan Camenisch, Matthew Campagna, Dario Catalano, Benoit Chevallier-Mames, Koji Chida, Nicolas Courtois, Annalisa De Bonis, Yevgeniy Dodis, Thomas Dübendorfer, Jacques Fournier, Atsushi Fujioka, Jun Furukawa, Clemente Galdi, Rosario Gennaro, Christophe Giraud, Louis Granboulan, Louis Goubin, Stuart Haber, Thomas Holenstein, Nick Howgrave-Graham, Stanislaw Jarecki, Antoine Joux, Jonathan Katz, Wataru Kishimoto, Erik Woodward Knudsen, Takeshi Koshiba, Hugo Krawczyk, Ben Lynn, Anna Lysyanskaya, Kazuto Matsuo, Patrick McDaniel, Phong Nguyen, Jesper Buus Nielsen, Satoshi Obana, Benny Pinkas, David Pointcheval, Bartosz Przydatek, Hervé Sibert, Francesco Sica, Nigel Smart, Markus Stadler, Martijn Stam, Reto Strobl, Koutarou Suzuki, Mike Szydlo, Tsuyoshi Takagi, Katsuyuki Takashima, Eran Tromer, Christophe Tymen, Salil Vadhan, Stefan Wolf, Jürg Wullschleger, and Akihiro Yamamura. (I apologize for any possible omission.) The Program Committee appreciates their efforts.

Thanks to Hoang Ha, Haizhi Chen, and Wayman E. Luy for secretarial work and for partially maintaining the WWW page of the conference, and to Wayne Sprague for setting up the e-mail addresses for PKC. Several people helped the General Chair with sending out the call for papers, registration, registration at the conference, etc.

Finally, I would like to thank everyone who submitted to PKC 2003, and IACR for its sponsorship.

October 2002 Yvo Desmedt

PKC 2003

Sixth International Workshop on Practice and Theory in Public Key Cryptography

Miami Convention Center, Miami, Florida, USA
January 6–8, 2003

Sponsored by the

International Association for Cryptologic Research
in cooperation with the
Department of Computer Science, Florida State University

General Chair

Mike Burmester, Florida State University, USA

Program Chair

Yvo Desmedt, Florida State University, USA

Program Committee

Masayuki Abe	NTT Laboratories, Japan
Feng Bao	Laboratories for Information Technology, Singapore
Giovanni Di Crescenzo	Telcordia, USA
Marc Joye	Gemplus, France
Kaoru Kurosawa	Ibaraki University, Japan
Arjen Lenstra	Citicorp, USA
Tal Malkin	AT&T Research, USA
Ueli Maurer	ETH, Zurich, Switzerland
Moni Naor	Weizmann Institute of Science, Israel
Tatsuaki Okamoto	NTT Laboratories, Japan
Jacques Patarin	Université de Versailles, France
Tal Rabin	IBM Research Lab., USA
Kazue Sako	NEC, Japan
Jacques Stern	École Normale Supérieure, France
Serge Vaudenay	ETH, Lausanne, Switzerland
Yongge Wang	University of North Carolina, USA
Michael Wiener	Canada
Moti Yung	Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

Table of Contents

Specialized Multiparty Cryptography

Cryptanalysis I

Elliptic Curves: Implementation Attacks

Implementation and Hardware Issues

New Public Key Schemes

Elliptic Curves: General Issues

Cryptanalysis II