

Lecture Notes in Computer Science

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

2567

**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

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002  
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](http://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 Genaro, 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 Koshihara, 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 Strohbl, 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.

VI Preface

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

## Diffie-Hellman Based Schemes

Efficient Construction of (Distributed) Verifiable Random Functions .....1  
*Yevgeniy Dodis*

An Identity-Based Signature from Gap Diffie-Hellman Groups .....18  
*Jae Choon Cha and Jung Hee Cheon*

## Threshold Cryptography

Threshold Signatures, Multisignatures and Blind Signatures Based  
on the Gap-Diffie-Hellman-Group Signature Scheme .....31  
*Alexandra Boldyreva*

An Efficient Two-Party Public Key Cryptosystem Secure  
against Adaptive Chosen Ciphertext Attack .....47  
*Philip MacKenzie*

## Reduction Proofs

On the Bit Security of NTRUEncrypt .....62  
*Mats Näslund, Igor E. Shparlinski, and William Whyte*

Equivalence between Semantic Security and Indistinguishability  
against Chosen Ciphertext Attacks .....71  
*Yodai Watanabe, Junji Shikata, and Hideki Imai*

## Broadcast and Tracing

Randomness Re-use in Multi-recipient Encryption Schemes ..... 85  
*Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon*

Public Key Trace and Revoke Scheme Secure  
against Adaptive Chosen Ciphertext Attack .....100  
*Yevgeniy Dodis and Nelly Fazio*

## Digital Signatures

The Cramer-Shoup Strong-RSA Signature Scheme Revisited ..... 116  
*Marc Fischlin*

Strong Key-Insulated Signature Schemes .....130  
*Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung*

**Specialized Multiparty Cryptography**

A Verifiable Secret Shuffle of Homomorphic Encryptions ..... 145  
*Jens Groth*

Round-Optimal Contributory Conference Key Agreement ..... 161  
*Colin Boyd and Juan Manuel González Nieto*

**Cryptanalysis I**

Security Analysis of the MOR Cryptosystem ..... 175  
*Christian Tobias*

A Practical Attack on Some Braid Group  
Based Cryptographic Primitives ..... 187  
*Dennis Hofheinz and Rainer Steinwandt*

**Elliptic Curves: Implementation Attacks**

A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems ..... 199  
*Louis Goubin*

Validation of Elliptic Curve Public Keys ..... 211  
*Adrian Antipa, Daniel Brown, Alfred Menezes, René Struik,  
and Scott Vanstone*

Exceptional Procedure Attack on Elliptic Curve Cryptosystems ..... 224  
*Tetsuya Izu and Tsuyoshi Takagi*

**Implementation and Hardware Issues**

On Montgomery-Like Representations for Elliptic Curves over  $GF(2^k)$  .... 240  
*Martijn Stam*

A Dedicated Sieving Hardware ..... 254  
*Willi Geiselmann and Rainer Steinwandt*

A Fast and Secure Implementation of Sflash ..... 267  
*Mehdi-Laurent Akkar, Nicolas T. Courtois, Romain Duteuil,  
and Louis Goubin*

**New Public Key Schemes**

A Practical Public Key Cryptosystem from Paillier and Rabin Schemes ... 279  
*David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar*

A Lattice Based Public Key Cryptosystem  
Using Polynomial Representations ..... 292  
*Seong-Hun Paeng, Bae Eun Jung, and Kil-Chan Ha*

**Elliptic Curves: General Issues**

The Security of DSA and ECDSA  
(Bypassing the Standard Elliptic Curve Certification Scheme) .....309  
*Serge Vaudenay*

**Cryptanalysis II**

Side-Channel Attacks on Textbook RSA and ElGamal Encryption ..... 324  
*Ulrich Kühn*

On the Security of HFE, HFEv- and Quartz ..... 337  
*Nicolas T. Courtois, Magnus Daum, and Patrick Felke*

Generic Attacks and the Security of Quartz .....351  
*Nicolas T. Courtois*

**Author Index** .....365