

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

2274

**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

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 Steingraber 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, Gwenaëlle 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 Bouchier 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.

**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

## Encryption Schemes

New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive	1
<i>Kouichi Sakurai (Kyushu University, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)</i>	
Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages	17
<i>Jean-Sébastien Coron (Gemplus, France), Helena Handschuh (Gemplus, France), Marc Joye (Gemplus, France), Pascal Paillier (Gemplus, France), David Pointcheval (École Normale Supérieure, France), Christophe Tychen (Gemplus, France)</i>	
On Sufficient Randomness for Secure Public-Key Cryptosystems	34
<i>Takeshi Koshihara (Fujitsu Laboratories Ltd, Japan)</i>	
Multi-recipient Public-Key Encryption with Shortened Ciphertext	48
<i>Kaoru Kurosawa (Ibaraki University, Japan)</i>	

## Signature Schemes

Efficient and Unconditionally Secure Digital Signatures and a Security Analysis of a Multireceiver Authentication Code	64
<i>Goichiro Hanaoka (University of Tokyo, Japan), Junji Shikata (University of Tokyo, Japan), Yuliang Zheng (UNC Charlotte, USA), Hideki Imai (University of Tokyo, Japan)</i>	
Formal Proofs for the Security of Signcryption	80
<i>Joonsang Baek (Monash University, Australia), Ron Steinfeld (Monash University, Australia), Yuliang Zheng (UNC Charlotte, USA)</i>	
A Provably Secure Restrictive Partially Blind Signature Scheme	99
<i>Greg Maitland (Queensland University of Technology, Australia), Colin Boyd (Queensland University of Technology, Australia)</i>	

## Protocols I

$M + 1$ -st Price Auction Using Homomorphic Encryption	115
<i>Masayuki Abe (NTT ISP Labs, Japan), Koutarou Suzuki (NTT ISP Labs, Japan)</i>	
Client/Server Tradeoffs for Online Elections	125
<i>Ivan Damgård (Aarhus University, Denmark), Mads Jurik (Aarhus University, Denmark)</i>	

Self-tallying Elections and Perfect Ballot Secrecy . . . . . 141  
*Aggelos Kiayias (Graduate Center, CUNY, USA), Moti Yung (CertCo, USA)*

**Protocols II**

Efficient 1-Out-n Oblivious Transfer Schemes . . . . . 159  
*Wen-Guey Tzeng (National Chiao Tung University, Taiwan)*

Linear Code Implies Public-Key Traitor Tracing . . . . . 172  
*Kaoru Kurosawa (Ibaraki University, Japan), Takuya Yoshida (Tokyo Institute of Technology, Japan)*

Design and Security Analysis  
of Anonymous Group Identification Protocols . . . . . 188  
*Chan H. Lee (City University of Hong Kong, China), Xiaotie Deng (City University of Hong Kong, China), Huafei Zhu (Zhejiang University, China)*

On the Security of the Threshold Scheme  
Based on the Chinese Remainder Theorem . . . . . 199  
*Michaël Quisquater (Katholieke Universiteit Leuven, Belgium), Bart Preneel (Katholieke Universiteit Leuven, Belgium), Joos Vandewalle (Katholieke Universiteit Leuven, Belgium)*

**Cryptanalysis**

Solving Underdefined Systems of Multivariate Quadratic Equations . . . . . 211  
*Nicolas Courtois (SchlumbergerSema, France), Louis Goubin (SchlumbergerSema, France), Willi Meier (FH Aargau, Switzerland), Jean-Daniel Tacier (FH Aargau, Switzerland)*

Selective Forgery of RSA Signatures with Fixed-Pattern Padding . . . . . 228  
*Arjen K. Lenstra (Citibank, USA, and Tech. Univ. Eindhoven, The Netherlands), Igor E. Shparlinski (Macquarie University, Australia)*

New Chosen-Plaintext Attacks on the One-Wayness  
of the Modified McEliece PKC Proposed at Asiacrypt 2000 . . . . . 237  
*Kazukuni Kobara (University of Tokyo, Japan), Hideki Imai (University of Tokyo, Japan)*

**Side Channels**

SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation . . 252  
*Roman Novak (Jozef Stefan Institute, Slovenia)*

A Combined Timing and Power Attack . . . . . 263  
*Werner Schindler (BSI, Germany)*



A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks . . . . .	280
<i>Tetsuya Izu (Fujitsu Labs Ltd, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)</i>	
<b>Invited Talk</b>	
New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report . . . . .	297
<i>Bart Preneel (Katholieke Universiteit Leuven, Belgium)</i>	
<b>ECC Implementations</b>	
An Improved Method of Multiplication on Certain Elliptic Curves . . . . .	310
<i>Young-Ho Park (CIST, Korea University, Korea), Sangho Oh (CIST, Korea University, Korea), Sangjin Lee (CIST, Korea University, Korea), Jongin Lim (CIST, Korea University, Korea), Maenghee Sung (KISA, Korea)</i>	
An Alternate Decomposition of an Integer for Faster Point Multiplication on Certain Elliptic Curves . . . . .	323
<i>Young-Ho Park (CIST, Korea University, Korea), Sangtae Jeong (Seoul National University, Korea), Chang Han Kim (CAMIS, Semyung University, Korea), Jongin Lim (CIST, Korea University, Korea)</i>	
Weierstraß Elliptic Curves and Side-Channel Attacks . . . . .	335
<i>Éric Brier (Gemplus, France), Marc Joye (Gemplus, France)</i>	
<b>Applications</b>	
One-Way Cross-Trees and Their Applications . . . . .	346
<i>Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)</i>	
RSA Key Generation with Verifiable Randomness . . . . .	357
<i>Ari Juels (RSA Laboratories, USA), Jorge Guajardo (Ruhr-Universität Bochum, Germany)</i>	
New Minimal Modified Radix- $r$ Representation with Applications to Smart Cards . . . . .	375
<i>Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)</i>	
<b>Author Index</b> . . . . .	385