

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Marc Joye (Ed.)

Topics in Cryptology – CT-RSA 2003

The Cryptographers' Track at the RSA Conference 2003
San Francisco, CA, USA, April 13-17, 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

Marc Joye
Gemplus, Card Security Group
La Vigie, Avenue du Jujubier, ZI Athélia IV
13705 La Ciotat Cedex
France
E-mail: marc.joye@gemplus.com

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, G.2.1, D.4.6, K.6.5, K.4.4, F.2.1-2, C.2, J.1

ISSN 0302-9743

ISBN 3-540-00847-0 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 Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10872873 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of CT-RSA 2003, the Cryptographers' Track at RSA Conference 2003. The proceedings of CT-RSA 2001 and CT-RSA 2002 were published in Springer-Verlag's Lecture Notes in Computer Science series as LNCS 2020 and LNCS 2271, respectively.

The Cryptographers' Track is one of the many parallel tracks of the RSA Conference. With many thousands of participants, the RSA Conference is the largest security and cryptography event of the year.

There were 97 submitted contributions this year, of which 26, or 27%, were selected for presentation. The program also included two invited talks by Tom Berson ("Cryptography After the Bubble: How to Make an Impact on the World") and by Adi Shamir ("RSA Shortcuts").

All submissions were reviewed by at least three members of the program committee. I am very grateful to the 21 members of the program committee for their hard and efficient work in assembling the program. My thanks also go to the 78 external referees who helped in the review process in their area of expertise: Gail-Joon Ahn, Toru Akishita, Kazumaro Aoki, Gildas Avoine, Joonsang Baek, Olivier Benoit, Alex Biryukov, Alexandra Boldyreva, Antoon Bosselaers, Emmanuel Bresson, Eric Brier, Brice Canvel, Dario Catalano, Chien Yuan Chen, Donghyeon Cheon, Jung Hee Cheon, Olivier Chevassut, Kilsoo Chun, Mathieu Ciet, Christophe Clavier, Jean-Sébastien Coron, Reza Curtmola, Christophe De Cannière, Jean-François Dhem, Xuhua Ding, Pierre-Alain Fouque, Jacques Fournier, Fabien Germain, Jovan Dj. Golić, Philippe Golle, Louis Granboulan, Jorge Guajardo, D.J. Guan, Jinsu Hyun, Eliane Jaulmes, Pascal Junod, Sungwoo Kang, Jonathan Katz, Dongryeol Kim, Tetsutaro Kobayashi, Yoshi Kohno, Takeshi Koshihara, Hyun-jo Kwon, Byoungcheon Lee, Y.C. Lee, Arjen Lenstra, Seongan Lim, Phil MacKenzie, Gwenaëlle Martinet, Jean Monnerat, Maithili Narasimha, Hanae Nozaki, Katsuyuki Okeya, Francis Olivier, Siddika Berna Ors, Elisabeth Oswald, Pascal Paillier, Benny Pinkas, Guillaume Poupard, Pankaj Rohatgi, Ludovic Rousseau, Tomas Sander, Marius Schilder, Jasper Scholten, Stefaan Seys, Hung-Min Sun, Jaechul Sung, Mike Szydło, Mårten Trolin, Christophe Tymen, Frédéric Valette, Holger Vogt, Bodgan Warinschi, Susanne Wetzel, Karel Wouters, Shouhuai Xu, Jeong Yi, and Fangguo Zhang. I apologize for possible omissions. Finally, I would like to thank Julien Bouchier for hosting and maintaining the review website. The excellent web-based software, maintained by the COSIC group at K.U. Leuven, was used for the review process.

In addition to those mentioned above, many people contributed to the success of CT-RSA 2003, and I thank them: Ari Juels and Burt Kaliski for interfacing with the conference organizers; Marseille Burton and Kurt Stammberger for handling issues not directly related to the scientific program; and Bart Preneel, the Program Chair for CT-RSA 2002, for giving me good advice. Last, but not

least, I would like to thank all the authors who submitted papers, making the conference possible, and the authors of accepted papers for their cooperation.

It is our sincere hope that the Cryptographers' Track will remain a premium forum of intellectual exchange in the broad area of the application and theory of cryptography.

November 2002

Marc Joye

RSA Conference 2003, Cryptographers' Track

April 13–17, 2003, San Francisco, USA

RSA Conference 2003 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track at RSA Conference 2003 was organized by RSA Laboratories (<http://www.rsasecurity.com>).

Program Chair

Marc JoyeGemplus, France

Program Committee

Giuseppe Ateniese The Johns Hopkins University, USA
John BlackUniversity of Colorado at Boulder, USA
Daniel Bleichenbacher Bell Laboratories, USA
Rosario GennaroIBM T.J. Watson Research Center, USA
Stuart HaberHewlett-Packard Laboratories, USA
Helena Handschuh Gemplus, France
Markus Jakobsson RSA Laboratories, USA
Antoine JouxDCSSI, France
Kwangjo Kim Information and Communications University, Korea
Seungjoo Kim Korea Information Security Agency, Korea
Chi-Sung Lai National Cheng Kung University, Taiwan
Tatsuaki Okamoto NTT Labs, Japan
David PointchevalEcole Normale Supérieure, France
Bart PreneelKatholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater Université Catholique de Louvain, Belgium
Tsuyoshi Takagi Technische Universität Darmstadt, Germany
Gene Tsudik University of California at Irvine, USA
Serge Vaudenay ... Swiss Federal Institute of Technology (EPFL), Switzerland
Sung-Ming Yen National Central University, Taiwan
Moti YungColumbia University, USA
Yuliang Zheng UNC Charlotte, USA

Table of Contents

Key Self-protection

Forward-Security in Private-Key Cryptography	1
<i>Mihir Bellare and Bennet Yee</i>	
Intrusion-Resilient Public-Key Encryption	19
<i>Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, and Moti Yung</i>	

Message Authentication

TMAC: Two-Key CBC MAC	33
<i>Kaoru Kurosawa and Tetsu Iwata</i>	
Montgomery Prime Hashing for Message Authentication	50
<i>Douglas L. Whiting and Michael J. Sabin</i>	

Digital Signatures

An Analysis of Proxy Signatures: Is a Secure Channel Necessary?	68
<i>Jung-Yeun Lee, Jung Hee Cheon, and Seungjoo Kim</i>	
Invisibility and Anonymity of Undeniable and Confirmer Signatures	80
<i>Steven D. Galbraith and Wenbo Mao</i>	

Pairing Based Cryptography

A Secure Signature Scheme from Bilinear Maps	98
<i>Dan Boneh, Ilya Mironov, and Victor Shoup</i>	
Access Control Using Pairing Based Cryptography	111
<i>Nigel P. Smart</i>	

Multivariate and Lattice Problems

NTRUSIGN: Digital Signatures Using the NTRU Lattice	122
<i>Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte</i>	
About the XL Algorithm over $GF(2)$	141
<i>Nicolas T. Courtois and Jacques Patarin</i>	

Cryptographic Architectures

Efficient $GF(p^m)$ Arithmetic Architectures
for Cryptographic Applications 158
*Guido Bertoni, Jorge Guajardo, Sandeep Kumar, Gerardo Orlando,
Christof Paar, and Thomas Wollinger*

Hardware Performance Characterization of Block Cipher Structures 176
Lu Xiao and Howard M. Heys

New RSA-based Cryptosystems

Simple Identity-Based Cryptography with Mediated RSA 193
Xuhua Ding and Gene Tsudik

Two Birds One Stone: Signcryption Using RSA 211
John Malone-Lee and Wenbo Mao

Invited Talk I

Cryptography after the Bubble: How to Make an Impact on the World 226
Tom Berson

Chosen-Ciphertext Security

Rethinking Chosen-Ciphertext Security under Kerckhoffs' Assumption 227
Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng

Provably Secure Public-Key Encryption
for Length-Preserving Chaumian Mixes 244
Bodo Möller

Broadcast Encryption and PRF Sharing

Fault Tolerant and Distributed Broadcast Encryption 263
Paolo D'Arco and Douglas R. Stinson

Shared Generation of Pseudo-Random Functions with Cumulative Maps .. 281
Huaxiong Wang and Josef Pieprzyk

Authentication Structures

Authenticated Data Structures for Graph and Geometric Searching 295
*Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos,
and Robert Cohen*

Fractal Merkle Tree Representation and Traversal 314
Markus Jakobsson, Tom Leighton, Silvio Micali, and Michael Szydlo

Invited Talk II

RSA Shortcuts	327
<i>Adi Shamir</i>	

Elliptic Curves and Pairings

The Width- w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks	328
<i>Katsuyuki Okeya and Tsuyoshi Takagi</i>	
Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation	343
<i>Kirsten Eisenträger, Kristin Lauter, and Peter L. Montgomery</i>	

Threshold Cryptography

Two Efficient and Provably Secure Schemes for Server-Assisted Threshold Signatures	355
<i>Shouhuai Xu and Ravi Sandhu</i>	
Secure Applications of Pedersen's Distributed Key Generation Protocol ...	373
<i>Rosario Gennaro, Stanisław Jarecki, Hugo Krawczyk, and Tal Rabin</i>	

Implementation Issues

Seeing through MIST Given a Small Fraction of an RSA Private Key	391
<i>Colin D. Walter</i>	
Simple Backdoors for RSA Key Generation	403
<i>Claude Crépeau and Alain Slakmon</i>	
Author Index	417