Lecture Notes in Computer Science 2612
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

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

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 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 Koshiba, 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 Szydlo, 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 Brouchier 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 Joye ..... Gemplus, France

Program Committee

Giuseppe Ateniese ..... The Johns Hopkins University, USA
John Black ..... University of Colorado at Boulder, USA
Daniel Bleichenbacher ..... Bell Laboratories, USA
Rosario Gennaro ..... IBM T.J. Watson Research Center, USA
Stuart Haber ..... Hewlett-Packard Laboratories, USA
Helena Handschuh ..... Gemplus, France
Markus Jakobsson ..... RSA Laboratories, USA
Antoine Joux ..... DCSSI, France
Kwangjo Kim ..... Information and Communications University, Korea
Seungjoo Kim ..... Korea Information Security Agency, Korea
Chi-Sung Laih ..... National Cheng Kung University, Taiwan
Tatsuaki Okamoto ..... NTT Labs, Japan
David Pointcheval ..... Ecole Normale Supérieure, France
Bart Preneel ..... Katholieke 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 Yung ..... Columbia University, USA
Yuliang Zheng ..... UNC Charlotte, USA

Table of Contents

Cryptographic Architectures

New RSA-based Cryptosystems

Invited Talk I

Chosen-Ciphertext Security

Broadcast Encryption and PRF Sharing

Authentication Structures

Invited Talk II

Elliptic Curves and Pairings

Threshold Cryptography

Implementation Issues