

# Lecture Notes in Computer Science

2271

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

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Bart Preneel (Ed.)

# Topics in Cryptology – CT-RSA 2002

The Cryptographers' Track at the RSA Conference 2002  
San Jose, CA, USA, February 18-22, 2002  
Proceedings



Springer

## Series Editors

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

## Volume Editor

Bart Preneel  
Katholieke Universiteit Leuven, Department of Electrical Engineering  
Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium  
E-mail: bart.preneel@esat.kuleuven.ac.be

## Cataloging-in-Publication Data applied for

### Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Topics in cryptology : the Cryptographers' Track at the RSA Conference 2002 ;  
proceedings / CT-RSA 2002, San José, CA, USA, February 18 - 22, 2002.

Bart Preneel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ;  
London ; Milan ; Paris ; Tokyo : Springer, 2002

(Lecture notes in computer science ; Vol. 2271)

ISBN 3-540-43224-8

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743

ISBN 3-540-43224-8 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 Olgun Computergrafik  
Printed on acid-free paper      SPIN: 10846157      06/3142      5 4 3 2 1 0

# Preface

This volume continues the tradition established in 2001 of publishing the contributions presented at the Cryptographers' Track (CT-RSA) of the yearly RSA Security Conference in Springer-Verlag's Lecture Notes in Computer Science series.

With 14 parallel tracks and many thousands of participants, the RSA Security Conference is the largest e-security and cryptography conference. In this setting, the Cryptographers' Track presents the latest scientific developments.

The program committee considered 49 papers and selected 20 for presentation. One paper was withdrawn by the authors. The program also included two invited talks by Ron Rivest ("Micropayments Revisited" – joint work with Silvio Micali) and by Victor Shoup ("The Bumpy Road from Cryptographic Theory to Practice").

Each paper was reviewed by at least three program committee members; papers written by program committee members received six reviews. The authors of accepted papers made a substantial effort to take into account the comments in the version submitted to these proceedings. In a limited number of cases, these revisions were checked by members of the program committee.

I would like to thank the 20 members of the program committee who helped to maintain the rigorous scientific standards to which the Cryptographers' Track aims to adhere. They wrote thoughtful reviews and contributed to long discussions; more than 400 Kbyte of comments were accumulated. Many of them attended the program committee meeting, while they could have been enjoying the sunny beaches of Santa Barbara.

I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, N. Asokan, Tonnes Brekne, Emmanuel Bresson, Eric Brier, Jan Camenisch, Christian Collberg, Don Coppersmith, Jean-Sébastien Coron, Serge Fehr, Marc Fischlin, Matthias Fitzi, Pierre-Alain Fouque, Anwar Hasan, Clemens Holenstein, Kamal Jain, Marc Joye, Darko Kirovski, Lars Knudsen, Neal Kobnitz, Anna Lysyanskaya, Lennart Meier, David M'Raihi, Phong Nguyen, Pascal Paillier, Adrian Perrig, David Pointcheval, Tal Rabin, Tomas Sander, Berk Sunar, Michael Szydlo, Christophe Tymen, Frederik Vercauteren, Colin Walter, Andre Weimerskirch, and Susanne Wetzels. I apologize for any inadvertent omissions.

Electronic submissions were made possible by a collection of PHP scripts originally written by Chanathip Namprempr and some perl scripts written by Sam Rebelsky and SIGACT's Electronic Publishing Board. For the review procedure, web-based software was used which I designed for Eurocrypt 2000; the code was written by Wim Moreau and Joris Claessens.

I would like to thank Wim Moreau for helping with the electronic processing of the submissions and final versions, Ari Juels and Burt Kaliski for interfacing

with the RSA Security Conference, and Alfred Hofmann and his colleagues at Springer-Verlag for the timely production of this volume.

Finally, I wish to thank all the authors who submitted papers and the authors of accepted papers for the smooth cooperation which enabled us to process these proceedings as a single **LaTeX** document.

We hope that in the coming years the Cryptographers' Track will continue to be a forum for dialogue between researchers and practitioners in information security.

November 2001

Bart Preneel

# RSA Cryptographers' Track 2002

February 18–22, 2002, San Jose, California

The RSA Conference 2002 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track was organized by RSA Laboratories (<http://www.rsasecurity.com>).

## Program Chair

Bart Preneel, Katholieke Universiteit Leuven, Belgium

## Program Committee

Dan Boneh	Stanford University, USA
Yvo Desmedt	Florida State University, USA
Dieter Gollmann	Microsoft Research, USA
Stuart Haber	Intertrust, USA
Shai Halevi	IBM Research, USA
Helena Handschuh	Gemplus, France
Martin Hirt	ETH, Switzerland
Markus Jakobsson	RSA Laboratories, USA
Ari Juels	RSA Laboratories, USA
Pil Jong Lee	Postech, Korea
Alfred Menezes	University of Waterloo, Canada
Kaisa Nyberg	Nokia, Finland
Tatsuaki Okamoto	NTT Labs, Japan
Christof Paar	Worcester Polytechnique Institute, USA
Jean-Jacques Quisquater	Univ. Cath. de Louvain, Belgium
Jacques Stern	Ecole Normale Supérieure, France
Michael Wiener	Canada
Yacov Yacobi	Microsoft Research, USA
Moti Yung	Certco, USA
Yuliang Zheng	Monash University, Australia

# Table of Contents

## Public Key Cryptography

- On Hash Function Firewalls in Signature Schemes . . . . . 1  
*Burton S. Kaliski Jr.*
- Observability Analysis – Detecting When Improved Cryptosystems Fail . . . 17  
*Marc Joye, Jean-Jacques Quisquater, Sung-Ming Yen, and Moti Yung*

## Efficient Hardware Implementations

- Precise Bounds for Montgomery Modular Multiplication  
and Some Potentially Insecure RSA Moduli . . . . . 30  
*Colin D. Walter*
- Montgomery in Practice: How to Do It More Efficiently in Hardware . . . . 40  
*Lejla Batina and Geeke Muurling*
- MIST: An Efficient, Randomized Exponentiation Algorithm  
for Resisting Power Analysis . . . . . 53  
*Colin D. Walter*
- An ASIC Implementation of the AES SBoxes . . . . . 67  
*Johannes Wolkerstorfer, Elisabeth Oswald, and Mario Lamberger*

## Public Key Cryptography: Theory

- On the Impossibility of Constructing Non-interactive Statistically-Secret  
Protocols from Any Trapdoor One-Way Function . . . . . 79  
*Marc Fischlin*
- The Representation Problem Based on Factoring . . . . . 96  
*Marc Fischlin and Roger Fischlin*

## Symmetric Ciphers

- Ciphers with Arbitrary Finite Domains . . . . . 114  
*John Black and Phillip Rogaway*
- Known Plaintext Correlation Attack against RC5 . . . . . 131  
*Atsuko Miyaji, Masao Nonaka, and Yoshinori Takii*

## E-Commerce and Applications

- Micropayments Revisited . . . . . 149  
*Silvio Micali and Ronald L. Rivest*



Proprietary Certificates .....	164
<i>Markus Jakobsson, Ari Juels, and Phong Q. Nguyen</i>	

Stateless-Recipient Certified E-Mail System Based on Verifiable Encryption .....	182
<i>Giuseppe Ateniese and Cristina Nita-Rotaru</i>	

## Digital Signatures

RSA-Based Undeniable Signatures for General Moduli .....	200
<i>Steven D. Galbraith, Wenbo Mao, and Kenneth G. Paterson</i>	

Co-operatively Formed Group Signatures .....	218
<i>Greg Maitland and Colin Boyd</i>	

Transitive Signature Schemes .....	236
<i>Silvio Micali and Ronald L. Rivest</i>	

Homomorphic Signature Schemes .....	244
<i>Robert Johnson, David Molnar, Dawn Song, and David Wagner</i>	

## Public Key Encryption

GEM: A <u>G</u> eneric Chosen-Ciphertext Secure <u>E</u> ncryption <u>M</u> ethod .....	263
<i>Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen</i>	

Securing “Encryption + Proof of Knowledge” in the Random Oracle Model .....	277
<i>Masayuki Abe</i>	

## Discrete Logarithm

Nonuniform Polynomial Time Algorithm to Solve Decisional Diffie-Hellman Problem in Finite Fields under Conjecture .....	290
<i>Qi Cheng and Shigenori Uchiyama</i>	

Secure Key-Evolving Protocols for Discrete Logarithm Schemes .....	300
<i>Cheng-Fen Lu and Shiuh-Pyng Winston Shieh</i>	

Author Index .....	311
--------------------	-----