

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

2729

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Dan Boneh (Ed.)

# Advances in Cryptology – CRYPTO 2003

23rd Annual International Cryptology Conference  
Santa Barbara, California, USA, August 17-21, 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

Dan Boneh  
Stanford University  
Computer Science Department  
Gates 475, Stanford, CA, 94305-9045, USA  
E-mail: dabo@cs.stanford.edu

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

ISSN 0302-9743

ISBN 3-540-40674-3 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>

© International Association for Cryptologic Research 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH  
Printed on acid-free paper SPIN: 10929063 06/3142 5 4 3 2 1 0

# Preface

Crypto 2003, the 23rd Annual Crypto Conference, was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara.

The conference received 169 submissions, of which the program committee selected 34 for presentation. These proceedings contain the revised versions of the 34 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. Submissions to the conference represent cutting-edge research in the cryptographic community worldwide and cover all areas of cryptography. Many high-quality works could not be accepted. These works will surely be published elsewhere.

The conference program included two invited lectures. Moni Naor spoke on cryptographic assumptions and challenges. Hugo Krawczyk spoke on the ‘SIGN-and-MAC’ approach to authenticated Diffie-Hellman and its use in the IKE protocols. The conference program also included the traditional rump session, chaired by Stuart Haber, featuring short, informal talks on late-breaking research news.

Assembling the conference program requires the help of many many people. To all those who pitched in, I am forever in your debt.

I would like to first thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto could not exist.

I thank Greg Rose, the general chair, for shielding me from innumerable logistical headaches, and showing great generosity in supporting my efforts.

Selecting from so many submissions is a daunting task. My deepest thanks go to the members of the program committee, for their knowledge, wisdom, and work ethic. We in turn relied heavily on the expertise of the many outside reviewers who assisted us in our deliberations. My thanks to all those listed on the pages below, and my thanks and apologies to any I have missed. Overall, the review process generated over 400 pages of reviews and discussions.

I thank Victor Shoup for hosting the program committee meeting in New York University and for his help with local arrangements. Thanks also to Tal Rabin, my favorite culinary guide, for organizing the postdeliberations dinner. I also thank my assistant, Lynda Harris, for her help in the PC meeting prearrangements.

I am grateful to Hovav Shacham for diligently maintaining the Web system, running both the submission server and the review server. Hovav patched security holes and added many features to both systems. I also thank the people who, by their past and continuing work, have contributed to the submission and review systems. Submissions were processed using a system based on software written by Chanathip Namprempre under the guidance of Mihir Bellare. The

review process was administered using software written by Wim Moreau and Joris Claessens, developed under the guidance of Bart Preneel.

I thank the advisory board, Moti Yung and Matt Franklin, for teaching me my job. They promptly answered any questions and helped with more than one task.

Last, and more importantly, I'd like to thank my wife, Pei, for her patience, support, and love. I thank my new-born daughter, Naomi Boneh, who graciously waited to be born after the review process was completed.

June 2003

Dan Boneh  
Program Chair  
Crypto 2003

# CRYPTO 2003

August 17–21, 2003, Santa Barbara, California, USA

Sponsored by the

*International Association for Cryptologic Research (IACR)*

in cooperation with

*IEEE Computer Society Technical Committee on Security and Privacy,*

*Computer Science Department, University of California, Santa Barbara*

## **General Chair**

Greg Rose, Qualcomm Australia

## **Program Chair**

Dan Boneh, Stanford University, USA

## **Program Committee**

Mihir Bellare	U.C. San Diego, USA
Jan Camenisch	IBM Research, Zurich
Don Coppersmith	IBM Research, Watson, USA
Jean-Sebastien Coron	Gemplus Card International, France
Ronald Cramer	BRICS, Denmark
Antoine Joux	DCSSI Crypto Lab, France
Charanjit Jutla	IBM Research, Watson, USA
Jonathan Katz	University of Maryland, USA
Eyal Kushilevitz	Technion, Israel
Anna Lysyanskaya	Brown University, USA
Phil MacKenzie	Bell Labs, USA
Mitsuru Matsui	Mitsubishi Electric, Japan
Tatsuaki Okamoto	NTT, Japan
Rafail Ostrovsky	Telcordia Technologies, USA
Benny Pinkas	HP Labs, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Tal Rabin	IBM Research, Watson, USA
Kazue Sako	NEC, Japan
Victor Shoup	NYU, USA
Jessica Staddon	PARC, USA
Ramarathnam Venkatesan	Microsoft Research, USA
Michael Wiener	Canada

## **Advisory Members**

Moti Yung (Crypto 2002 Program Chair)	Columbia University, USA
Matthew Franklin (Crypto 2004 Program Chair)	U.C. Davis, USA

## External Reviewers

Masayuki Abe	Ted Krovetz	Phillip Rogaway
Amos Beimel	Joe Lano	Pankaj Rohatgi
Alexandra Boldyreva	Gregor Leander	Ludovic Rousseau
Jesper Buus Nielsen	Arjen Lenstra	Atri Rudra
Christian Cachin	Matt Lepinski	Taiichi Saitoh
Ran Canetti	Yehuda Lindell	Louis Salvail
Matt Cary	Moses Liskov	Jasper Scholten
Suresh Chari	Tal Malkin	Hovav Shacham
Henry Cohn	Jean Marc Couveignes	Dan Simon
Nicolas Courtois	Gwenaëlle Martinet	Nigel Smart
Christophe De Canniere	Alexei Miasnikov	Diana Smetters
David DiVincenzo	Daniele Micciancio	Martijn Stam
Yevgeniy Dodis	Kazuhiko Minematsu	Doug Stinson
Pierre-Alain Fouque	Sara Miner	Reto Strobl
Atsushi Fujioka	Michel Mitton	Koutarou Suzuki
Eiichiro Fujisaki	Brian Monahan	Amnon Ta Shma
Jun Furukawa	Frédéric Muller	Yael Tauman
Rosario Gennaro	David Naccache	Stafford Tavares
Philippe Golle	Kobbi Nissim	Vanessa Teague
Stuart Haber	Kaisa Nyberg	Isamu Teranishi
Shai Halevi	Satoshi Obana	Yuki Tokunaga
Helena Handschuh	Pascal Paillier	Nikos Triandopoulos
Susan Hohenberger	Adriana Palacio	Shigenori Uchiyama
Yuval Ishai	Sarvar Patel	Frédéric Valette
Mariusz Jakubowski	Jacques Patarin	Bogdan Warinschi
Rob Johnson	Chris Peikert	Lawrence Washington
Mads Jurik	Krzysztof Pietrzak	Ruizhong Wei
Aviad Kipnis	Jonathan Poritz	Steve Weis
Lars Knudsen	Michael Quisquater	Stefan Wolf
Tadayoshi Kohno	Omer Reingold	Yacov Yacobi
Hugo Krawczyk	Vincent Rijmen	Go Yamamoto



# Table of Contents

## Public Key Cryptanalysis I

Factoring Large Numbers with the TWIRL Device .....	1
<i>Adi Shamir, Eran Tromer</i>	
New Partial Key Exposure Attacks on RSA .....	27
<i>Johannes Blömer, Alexander May</i>	
Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases .....	44
<i>Jean-Charles Faugère, Antoine Joux</i>	

## Alternate Adversary Models

On Constructing Locally Computable Extractors and Cryptosystems in the Bounded Storage Model .....	61
<i>Salil P. Vadhan</i>	
Unconditional Authenticity and Privacy from an Arbitrarily Weak Secret .....	78
<i>Renato Renner, Stefan Wolf</i>	

## Invited Talk I

On Cryptographic Assumptions and Challenges .....	96
<i>Moni Naor</i>	

## Protocols

Scalable Protocols for Authenticated Group Key Exchange .....	110
<i>Jonathan Katz, Moti Yung</i>	
Practical Verifiable Encryption and Decryption of Discrete Logarithms .....	126
<i>Jan Camenisch, Victor Shoup</i>	
Extending Oblivious Transfers Efficiently .....	145
<i>Yuval Ishai, Joe Kilian, Kobbi Nissim, Erez Petrank</i>	

## Symmetric Key Cryptanalysis I

Algebraic Attacks on Combiners with Memory .....	162
<i>Frederik Armknecht, Matthias Krause</i>	

Fast Algebraic Attacks on Stream Ciphers with Linear Feedback . . . . . 176  
*Nicolas T. Courtois*

Cryptanalysis of SAFER++ . . . . . 195  
*Alex Biryukov, Christophe De Cannière, Gustaf Dellkrantz*

## Public Key Cryptanalysis II

A Polynomial Time Algorithm for the Braid Diffie-Hellman  
 Conjugacy Problem . . . . . 212  
*Jung Hee Cheon, Byungheup Jun*

The Impact of Decryption Failures on the Security of  
 NTRU Encryption . . . . . 226  
*Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval,  
 John Proos, Joseph H. Silverman, Ari Singer, William Whyte*

## Universal Composability

Universally Composable Efficient Multiparty Computation from  
 Threshold Homomorphic Encryption . . . . . 247  
*Ivan Damgård, Jesper Buus Nielsen*

Universal Composition with Joint State . . . . . 265  
*Ran Canetti, Tal Rabin*

## Zero-Knowledge

Statistical Zero-Knowledge Proofs with Efficient Provers:  
 Lattice Problems and More . . . . . 282  
*Daniele Micciancio, Salil P. Vadhan*

Derandomization in Cryptography . . . . . 299  
*Boaz Barak, Shien Jin Ong, Salil P. Vadhan*

On Deniability in the Common Reference String and Random Oracle  
 Model . . . . . 316  
*Rafael Pass*

## Algebraic Geometry

Primality Proving via One Round in ECPP and One Iteration  
 in AKS . . . . . 338  
*Qi Cheng*

Torus-Based Cryptography . . . . . 349  
*Karl Rubin, Alice Silverberg*

## Public Key Constructions

Efficient Universal Padding Techniques for Multiplicative Trapdoor One-Way Permutation . . . . .	366
<i>Yuichi Komano, Kazuo Ohta</i>	
Multipurpose Identity-Based Signcryption (A Swiss Army Knife for Identity-Based Cryptography) . . . . .	383
<i>Xavier Boyen</i>	

## Invited Talk II

SIGMA: The ‘SIGn-and-MAc’ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols . . . . .	400
<i>Hugo Krawczyk</i>	

## New Problems

On Memory-Bound Functions for Fighting Spam . . . . .	426
<i>Cynthia Dwork, Andrew Goldberg, Moni Naor</i>	
Lower and Upper Bounds on Obtaining History Independence . . . . .	445
<i>Niv Buchbinder, Erez Petrank</i>	
Private Circuits: Securing Hardware against Probing Attacks . . . . .	463
<i>Yuval Ishai, Amit Sahai, David Wagner</i>	

## Symmetric Key Constructions

A Tweakable Enciphering Mode . . . . .	482
<i>Shai Halevi, Phillip Rogaway</i>	
A Message Authentication Code Based on Unimodular Matrix Groups . . .	500
<i>Matthew Cary, Ramarathnam Venkatesan</i>	
Luby-Rackoff: 7 Rounds Are Enough for $2^{n(1-\varepsilon)}$ Security . . . . .	513
<i>Jacques Patarin</i>	

## New Models

Weak Key Authenticity and the Computational Completeness of Formal Encryption . . . . .	530
<i>Omer Horvitz, Virgil Gligor</i>	
Plaintext Awareness via Key Registration . . . . .	548
<i>Jonathan Herzog, Moses Liskov, Silvio Micali</i>	
Relaxing Chosen-Ciphertext Security . . . . .	565
<i>Ran Canetti, Hugo Krawczyk, Jesper Buus Nielsen</i>	

## **Symmetric Key Cryptanalysis II**

Password Interception in a SSL/TLS Channel .....	583
<i>Brice Canvel, Alain Hiltgen, Serge Vaudenay, Martin Vuagnoux</i>	
Instant Ciphertext-Only Cryptanalysis of GSM	
Encrypted Communication .....	600
<i>Elad Barkan, Eli Biham, Nathan Keller</i>	
Making a Faster Cryptanalytic Time-Memory Trade-Off .....	617
<i>Philippe Oechslin</i>	
<b>Author Index</b> .....	631