Lecture Notes in Computer Science 2729

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

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

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

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 pre-arrangements.

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

Table of Contents

Public Key Cryptanalysis II

Universal Composability

Zero-Knowledge

Algebraic Geometry

Public Key Constructions

Invited Talk II

New Problems

Symmetric Key Constructions

New Models

Symmetric Key Cryptanalysis II