Lecture Notes in Computer Science 2656
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Eli Biham (Ed.)

Advances in Cryptology – EUROCRYPT 2003

International Conference on the Theory
and Applications of Cryptographic Techniques
Warsaw, Poland, May 4-8, 2003
Proceedings

Springer

Volume Editor

Eli Biham
Technion - Israel Institute of Technology
Computer Science Department
Haifa 32000, Israel
E-mail: biham@cs.technion.ac.il

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

ISSN 0302-9743
ISBN 3-540-14039-5 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: 10928608 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of EUROCRYPT 2003, the 22nd annual EUROCRYPT conference. The conference was sponsored by the IACR, the International Association for Cryptologic Research, `www.iacr.org`, this year in cooperation with the Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland. The General Chair, Jerzy Gawinecki, was responsible for the local organization, and the conference registration was handled by the IACR secretariat at the University of California, Santa Barbara, USA.

A total of 37 papers were accepted for presentation at the conference, out of 156 papers submitted (of which one was withdrawn by the authors shortly after the submission deadline). These proceedings contain revised versions of the accepted papers. In addition two invited talks were given: the first was given by Kris Gaj and Arkadiusz Orlowski, entitled "Facts and Myths of Enigma: Breaking Stereotypes." The second invited talk was given by Jacques Stern entitled "Why Provable Security Matters?" The conference program also included a rump session, chaired by Stanisław Jarecki, which featured short informal talks on recent results.

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed by at least three members of the program committee, and papers co-authored by a member of the program committee were reviewed by at least six (other) members. The reviews were then followed by deep discussions on the papers, which contributed a lot to the quality of the final selection. In most cases, extensive comments were sent to the authors. It was a pleasure for me to work with the program committee, whose members worked very hard over several months. I am also very grateful to the external referees who contributed with their special expertise to the selection process. Their work is highly appreciated.

The submission of papers was done using an electronic submission software written by Chanathip Namprempre for CRYPTO 2000 with modifications developed by Andre Adelsbach for EUROCRYPT 2001. All but two papers were submitted using this software, while the two others were submitted on paper and then scanned and entered into the software. During the review process, the program committee was mainly communicating using a review software written by Bart Preneel, Wim Moreau, and Joris Claessens for EUROCRYPT 2000. I would like to thank Orr Dunkelman and Julia Stolin for their help in installing, solving problems, and adding features to the software. I am also very grateful to Wim Moreau for his great help in solving some of the problems we had with the software. The final decisions were made during a committee meeting in Paris. I would like to thank Helena Handschuh and Gemplus for organizing and hosting the meeting. I would also like to acknowledge Elad Barkan and Pnina Cohen for their help whenever it was required.

On behalf of the General Chair I would like to acknowledge the members of the local organizing committee in Warsaw. For financial support of the conference we are very grateful to this year's sponsors.

It is my pleasure to thank the General Chair, Prof. Jerzy Gawinecki, for all his work in organizing the conference, and for the pleasant collaboration and various pieces of advice. I know he spent a lot of effort, during a period of over two years, organizing the conference.

Finally, but most importantly, I would like to thank all the authors from all over the world who submitted papers to the conference, and all the participants at the conference.

February 2003 Eli Biham

EUROCRYPT 2003

May 4–8, 2003, Warsaw, Poland

Sponsored by the
International Association for Cryptologic Research (*IACR*)

in cooperation with the
Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Warsaw

General Chair

Jerzy Gawinecki, Institute of Mathematics and Cryptology, Faculty of Cybernetics, Military University of Technology, Kaliskiego Str. 2, 00-908 Warsaw, Poland

Program Chair

Eli Biham, Computer Science Department, Technion, Israel Institute of Technology, Technion City, Haifa 32000, Israel

Program Committee

Johannes Buchmann ..... TU Darmstadt, Germany
Christian Cachin ..... IBM Research, Switzerland
Don Coppersmith ..... IBM Research, USA
Ronald Cramer ..... Aarhus, Denmark
Joan Daemen ..... Protonworld, Belgium
Yevgeniy Dodis ..... New York University, USA
Cynthia Dwork ..... Microsoft, USA
Juan Garay ..... Bell Labs, USA
Helena Handschuh ..... Gemplus, France
Stanisław Jarecki ..... Stanford, USA
Kwangjo Kim ..... ICU, Korea
Lars R. Knudsen ..... Technical University of Denmark
Shiho Moriai ..... NTT, Japan
Moni Naor ..... Weizmann Institute of Science, Israel
Paul Van Oorschot ..... Carleton University, Canada
Josef Pieprzyk ..... Macquarie University, Australia
David Pointcheval ..... CNRS–ENS, France
Matt Robshaw ..... Royal Holloway, UK
Berry Schoenmakers ..... TU Eindhoven, The Netherlands
Nigel Smart ..... University of Bristol, UK
Douglas R. Stinson ..... Waterloo, Canada
Serge Vaudenay ..... EPFL, Switzerland

Local Organizing Committee

Andrzej Ameljańczyk
Grażyna Biernacka
Bogdan Bojarski
Piotr Bora
Marek Dukaczewski
Anna Gajownik
Stanisław Janeczko
Tomasz Kijko
Tomasz Korza
Zenon Kosowski
Ryszard Kossowski
Krzysztof Mańk
Maciej Mączyński
Dobrosław Mąka
Bogdan Miszczak
Michał Misztal
Marek Niezgótka
Roman Oziębała
Jacek Papaj
Janusz Szmidt
Arkadiusz Szymaniec
Aleksander Wittlin

Sponsors

Gold Sponsors

Comp S.A., Warsaw, Poland
Microsoft Corporation, Redmond, WA, USA

Silver Sponsors

Radomska Wytwórnia Telefonów, "Telefony Polskie" S.A., Radom, Poland

Bronze Sponsors

Military Communication Institute, Zegrze, Poland
Telecommunications Research Institute, Warsaw, Poland
Enigma Systemy Ochrony Informacji Sp. z o.o., Warsaw, Poland

External Referees

Masayuki Abe
Kazumaro Aoki
Gildas Avoine
Michael Backes
Harad Baier
Boaz Barak
Alexander Barg
Elad Barkan
Josh Benaloh
Simon Blackburn
Daniel Bleichenbacher
Dan Boneh
Emmanuel Bresson
Jan Camenisch
Ran Canetti
Brice Canvel
Dario Catalano
Olivier Chevassut
Jean-Sébastien Coron
Alex Dent
Jean-François Dhem
David Divincenzo
Jeroen Doumen
Orr Dunkelman
Nelly Fazio
Matthias Fitzi
Pierre-Alain Fouque
Eiichiro Fujisaki
Steven Galbraith
David Gamarnik
Katherina Geissler
Rosario Gennaro
Yael Gertner
Henri Gilbert
Bobi Gilburd
Eu-Jin Goh
Jovan Golić
Philippe Golle
Louis Granboulan
Jens Groth
Stuart Haber
Shai Halevi
Danny Harnik
Birgit Henhapl
Florian Hess
Deukjo Hong
Fumitaka Hoshino
Nick Howgrave-Graham
Yuval Ishai
Oleg Izmerly
Antoine Joux
Pascal Junod
Mads Jurik
Mike Just
Masayuki Kanda
Nathan Keller
Svein Knapskog
Tetsutaro Kobayashi
Evangelos Kranakis
Hugo Krawczyk
Michiharu Kudo
Byoungcheon Lee
Yehuda Lindell

Yi Lu
Christof Ludwig
Phil MacKenzie
Tal Malkin
John Malone-Lee
Wenbo Mao
Keith Martin
Gwenaëlle Martinet
Willi Meier
Marine Minier
Ilya Mironov
Bodo Moeller
Jean Monnerat
Tal Mor
Sean Murphy
Phong Nguyen
Antonio Nicolosi
Roberto Oliveira
Francis Olivier
Dan Page
Pascal Paillier
Matthew Parker
Kenny Paterson
Benny Pinkas
Guillaume Poupard
Bart Preneel
Haavard Raddum
Omer Reingold
Leonid Reyzin
Alon Rosen
Louis Salvail
Arthur Schmidt
Hovav Shaham
Igor Shparlinski
Hervé Sibert
Adam Smith
Gregory Sorkin
Jessica Staddon
Martijn Stam
Michael Steiner
Jacques Stern
Koutarou Suzuki
Tsuyoshi Takagi
Barbara Terhal
Yuuki Tokunaga
Pim Tuyls
Christophe Tymen
Frederik Vercauteren
Ullrich Vollmer
Huaxiong Wang
Michael Wiener
Fangguo Zhang
Xianmo Zhang

Table of Contents

Foundations and Complexity Theoretic Security

Public Key Encryption

New Primitives

Cryptanalysis II

Elliptic Curves Cryptography

Digital Signatures

Invited Talk II

Cryptanalysis III

Key Exchange

Information Theoretic Cryptography

Secure Multi-party Computation II

Group Signatures