Lecture Notes in Computer Science 3494

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Ronald Cramer (Ed.)

Advances in Cryptology – EUROCRYPT 2005

24th Annual International Conference on the Theory and Applications of Cryptographic Techniques
Aarhus, Denmark, May 22-26, 2005
Proceedings

Springer

Volume Editor

Ronald Cramer
CWI, Amsterdam
and Mathematical Institute, Leiden University
Kruislaan 413, P.O. Box 94079
1090GB Amsterdam, The Netherlands
E-mail: cramer@cwi.nl, cramer@math.leidenuniv.nl

Library of Congress Control Number: 2005926095

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-10 3-540-25910-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25910-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11426639 06/3142 5 4 3 2 1 0

Table of Contents

Cryptanalysis I

Theory I

Encryption I

Signatures and Authentication

Algebra and Number Theory I

Quantum Cryptography

Secure Protocols

Algebra and Number Theory II

Theory II

Encryption II

Cryptanalysis II

Broadcast Encryption and Traitor Tracing

Preface

These are the proceedings of the 24th Annual IACR Eurocrypt Conference. The conference was sponsored by the International Association for Cryptologic Research (IACR; see `www.iacr.org`), this year in cooperation with the Computer Science Department of the University of Aarhus, Denmark. As General Chair, Ivan Damgård was responsible for local organization.

The Eurocrypt 2005 Program Committee (PC) consisted of 30 internationally renowned experts. Their names and affiliations are listed on pages VII and VIII of these proceedings. By the November 15, 2004 submission deadline the PC had received a total of 190 submissions via the IACR Electronic Submission Server. The subsequent selection process was divided into two phases, as usual. In the review phase each submission was carefully scrutinized by at least three independent reviewers, and the review reports, often extensive, were committed to the IACR Web Review System. These were taken as the starting point for the PC-wide Web-based discussion phase. During this phase, additional reports were provided as needed, and the PC eventually had some 700 reports at its disposal. In addition, the discussions generated more than 850 messages, all posted in the system. During the entire PC phase, which started in August 2003 with my earliest invitations to PC members and which continued until March 2005, more than 1000 email messages were communicated. Moreover, the PC received much appreciated assistance from a large body of external reviewers. Their names are listed on page VIII of these proceedings.

The selection process for Eurocrypt 2005 was finalized by the end of January 2005 with a one-day PC meeting held in Amsterdam, The Netherlands. This meeting was attended by most of the PC members. The PC ultimately selected 33 papers for publication in these proceedings and presentation at the conference. After notification of acceptance the authors were provided with the review comments and were granted one month to prepare the final versions, which were due by February 28, 2005. These final versions were not subjected to further scrutiny by the PC and their authors bear full responsibility.

It was a great pleasure to work with this PC, and I thank all members for contributing so much of their scientific expertise, advice, opinions, preferences and devotion, and for their very hard work in the relatively short time frame that a PC has to operate in.

The Eurocrypt 2005 "Best Paper Award" was shared by Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen and Xiuyuan Yu for their paper "Cryptanalysis of the Hash Functions MD4 and RIPEMD" and by Xiaoyun Wang and Hongbo Yu for their paper "How to Break MD5 and Other Hash Functions."

Besides the above-mentioned 33 regular presentations, the Eurocrypt 2005 scientific program featured two invited speakers: *René Schoof* (University of Rome, Italy), with a survey talk on algebraic geometry algorithms in cryptology,

in particular on point counting algorithms for algebraic varieties over finite fields, and *Joe Kilian* (Yianilos Labs, Princeton, USA), with a talk on "Confusion, Quagmire and Irrelevancy: an Optimist's View of the Future of Cryptographic Research."

Many others have, in one way or another, helped the PC, contributed to these proceedings or the Eurocrypt conference as such, thereby also serving the international cryptology community as a whole, directly or indirectly.

The Eurocrypt conference continues to attract many very high-quality submissions from all over the world; so many in fact that not all good papers could be selected. All authors who submitted their work for consideration by the PC are hereby acknowledged for their contributions.

CWI[1] in Amsterdam and the Mathematical Institute at Leiden University, my employers, are gratefully acknowledged for their support.

Eurocrypt 2004 PC Co-chairs Christian Cachin and Jan Camenisch (IBM Research), as well as Crypto 2004 PC Chair Matt Franklin (UC Davis), gave useful advice on a number of occasions. Also many thanks to Springer for its collaboration. Peter Landrock (Cryptomathic) is kindly acknowledged for agreeing to organize and chair the Eurocrypt 2005 rump session, a traditional, entertaining Tuesday evening session with brief research announcements and "any other business."

Hats off to John Tromp (Quantum Computing and Advanced Systems Research Group, CWI), who reallocated, from the summer of 2004 until February 2005, substantial amounts of his precious research time to expertly manage the technical infrastructure for electronic submissions and Web review. The software was run on the network of CWI's INS Department. I hereby acknowledge the support of INS head Martin Kersten and his system manager Matthijs Mourits. Also many thanks to Harry Buhrman and Paul Vitányi! Thomas Herlea from KU Leuven's IACR submission server and webreview system development team offered prompt technical assistance to John whenever needed. Michael Smeding (Computer Support Team, CWI) provided prompt service to me and my group.

Serge Fehr of my Cryptology and Information Security Research Group at CWI was in charge of "General Affairs." In particular, he assisted me during the very busy week following the submission deadline, organized the PC meeting in collaboration with Wilmy van Ojik (Conference Organization, CWI), helped the PC by logging the entire decision process during the meeting, and provided instrumental assistance when I edited this volume. Serge, thanks a lot!

Finally, I thank Ivan Damgård, Eurocrypt 2005 General Chair, for our very pleasant collaboration during the organization of Eurocrypt 2005, a memorable addition to our many joint scientific endeavors (and friendship!)

March 2005 Ronald Cramer

[1] CWI is the National Research Institute for Mathematics and Computer Science in The Netherlands.

EUROCRYPT 2005

May 22–26, 2005, Aarhus, Denmark

Sponsored by the
International Association for Cryptologic Research (IACR)
in cooperation with the
Computer Science Department, Faculty of Science,
University of Aarhus, Denmark

General Chair

Ivan Damgård, Department of Computer Science,
University of Aarhus, Denmark

Program Chair

Ronald Cramer, CWI, Amsterdam & Mathematical Institute,
Leiden University, The Netherlands

Program Committee

Michael Backes ..... IBM Zürich Research Laboratory, Switzerland
Daniel Bleichenbacher ..... Lucent Bell Labs, USA
Don Beaver ..... Syntechnica, LLC, USA
Don Coppersmith ..... IBM T. J. Watson Research Center, USA
Hans Dobbertin ..... University of Bochum, Germany
Yevgeniy Dodis ..... New York University, USA
Marc Fischlin ..... ETH Zürich, Switzerland
Steven Galbraith ..... Royal Holloway, University of London, UK
Shafi Goldwasser ..... MIT, USA & Weizmann Institute of Science, Israel
Shai Halevi ..... IBM T. J. Watson Research Center, USA
Johan Håstad ..... Royal Institute of Technology, UK
Marc Joye ..... Gemplus, France
Aggelos Kiayias ..... University of Connecticut, USA
Eyal Kushilevitz ..... Technion, Israel
Arjen Lenstra ..... Lucent Bell Labs, USA & TU Eindhoven, The Netherlands
Phong Q. Nguyễn ..... CNRS & École Normale Supérieure, France
Kaisa Nyberg ..... Nokia, Finland
Tatsuaki Okamoto ..... NTT, Japan
Rafail Ostrovsky ..... U.C.L.A., USA
Carles Padró ..... Universitat Politècnica de Catalunya, Spain
Benny Pinkas ..... Hewlett-Packard Labs, Israel

..... *(continued on the next page)* .....

Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Louis Salvail ..... University of Aarhus, Denmark
Palash Sarkar ..... Indian Statistical Institute, India
Berry Schoenmakers ..... TU Eindhoven, The Netherlands
Igor Shparlinski ..... Macquarie University, Australia
Douglas Stinson ..... University of Waterloo, Canada
Salil Vadhan ..... Harvard University, USA
Moti Yung ..... Columbia University, USA

External Referees

Michel Abdalla
Masayuki Abe
Saurabh Aggarwal
Roberto Avanzi
Joonsang Baek
Paulo Barreto
Amos Beimel
Eli Biham
Alex Biryukov
Alexandra Boldyreva
Emmanuel Bresson
Éric Brier
Christian Cachin
Jan Camenisch
Ran Canetti
Christophe De Cannière
Dario Catalano
Debrup Chakraborty
Yan-Cheng Chang
Denis Charles
Sanjit Chatterjee
Benoît Chevallier-Mames
Olivier Chevassut
Scott Contini
Giovanni Di Crescenzo
Ivan Damgård
Drew Dean
Jean-François Dhem
Iwan Duursma
Stefan Dziembowski
Kirsten Eisentraeger
Nelly Fazio
Matthias Fitzi
Pierre-Alain Fouque
Matt Franklin
Michael H. Freedman
Atsushi Fujioka
David Galindo
Juan Garay
Rosario Gennaro
Guang Gong
Maribel González Vasco
Ignacio Gracia
Louis Granboulan
Stuart Haber
Helena Handschuh
Alex Healy
Javier Herranz
Florian Hess
Jason Hinek
Martin Hirt
Susan Hohenberger
Thomas Holenstein
Nick Howgrave-Graham
Yuval Ishai
Markus Jakobsson
Stanislaw Jarecki
Antoine Joux
Ari Juels
Jonathan Katz
Alexander Kholosha
Eike Kiltz
Tetsutaro Kobayashi
Tadayoshi Kohno
Yuichi Komano
Hugo Krawczyk
Gunnar Kreitz
Caroline Kudla
Noboru Kunihiro
Jeff Lagarias
Tanja Lange
Joseph Lano
Kristin Lauter
Yehuda Lindell
Helger Lipmaa
Moses Liskov
Phil MacKenzie
Subhamoy Maitra
Tal Malkin
John Malone-Lee
Stefan Mangard
Keith Martin
Alexander May
Mira Meyerovich
Silvio Micali
Anton Mityagin
Paz Morillo
Siguna Mueller
Sourav Mukhopadhyay
Enric Nart
Kenny Nguyen
Minh-Huyen Nguyen
Antonio Nicolosi
Jesper Nielsen
Kobbi Nissim
Satoshi Obana
Miyako Ohkubo
Kazuo Ohta
Elisabeth Oswald
Pascal Paillier
Rafael Pass
Kenny Paterson

Maura Paterson
Souradyuti Paul
Thomas Pedersen
Jan Pelzl
Giuseppe Persiano
Erez Petrank
Birgit Pfitzmann
Duong Hieu Phan
Krzysztof Pietrzak
David Pointcheval
Manoj Prabhakaran
Bartosz Przydatek
Jordi Pujolàs
Tal Rabin
Omer Reingold
Rennato Renner
Leonid Reyzin
Vincent Rijmen
Pankaj Rohatgi
Alon Rosen
Germán Sáez
Kazue Sako
Takakazu Satoh
Christian Schaffner
Werner Schindler
Mike Scott
Hovav Shacham
Ronen Shaltiel
Peter Shor
Victor Shoup
Tom Shrimpton
Alice Silverberg
Nigel Smart
Martijn Stam
François-Xavier Standaert
Allan Steel
Damien Stehlé
Ron Steinfeld
Koutarou Suzuki
Mike Szydlo
Keisuke Tanaka
Tamir Tassa
Yael Tauman
Isamu Teranishi
Edlyn Teske
Mårten Trolin
Yiannis Tsiounis
Pim Tuyls
Shigenori Uchiyama
Vinod Vaikuntanathan
Ingrid Verbauwhede
Frederik Vercauteren
Eric Verheul
Jorge Luis Villar
Michael Waidner
Shabsi Walfish
Huaxiong Wang
Xiaoyun Wang
Mark Watkins
Benne de Weger
Steve Weis
Annegret Weng
Mike Wiener
Douglas Wikström
Christopher Wolf
Stefan Wolf
Go Yamamoto
Aleksandr Yampolskiy
Yuliang Zheng
Hong-Sheng Zhou