Lecture Notes in Computer Science 3621

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

Victor Shoup (Ed.)

Advances in Cryptology – CRYPTO 2005

25th Annual International Cryptology Conference
Santa Barbara, California, USA, August 14-18, 2005
Proceedings

Springer

Volume Editor

Victor Shoup
New York University, Department of Computer Science
251 Mercer Street, New York, NY 10012, USA
E-mail: shoup@cs.nyu.edu

Library of Congress Control Number: Applied for

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-10 3-540-28114-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28114-6 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11535218 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of Crypto 2005, the 25th Annual International Cryptology Conference. The conference was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Science Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference was held in Santa Barbara, California, August 14–18, 2005.

The conference received 178 submissions, out of which the program committee selected 33 for presentation. The selection process was carried out by the program committee via an "online" meeting. The authors of selected papers had a few weeks to prepare final versions of their papers, aided by comments from the reviewers. However, most of these revisions were not subject to any editorial review.

This year, a "Best Paper Award" was given to Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, for their paper "Finding Collisions in the Full SHA-1."

The conference program included two invited lectures. Ralph Merkle delivered an IACR Distinguished Lecture, entitled "The Development of Public Key Cryptography: a Personal View; and Thoughts on Nanotechnology." Dan Boneh gave an invited talk, entitled "Bilinear Maps in Cryptography."

We continued the tradition of a "rump session," featuring short, informal presentations (usually serious, sometimes entertaining, and occasionally both). The rump session was chaired this year by Phong Q. Nguyễn.

I would like to thank everyone who contributed to the success of this conference. First, thanks to all the authors who submitted papers: a conference program is no better than the quality of the submissions (and hopefully, no worse). Second, thanks to all the members of the program committee: it was truly an honor to work with a group of such talented and hard working individuals. Third, thanks to all the external reviewers (listed below) for assisting the program committee: their expertise was invaluable. Fourth, thanks to Matt Franklin, Dan Boneh, Jan Camenisch, and Christian Cachin for sharing with me their experiences as previous Crypto and Eurocrypt program chairs. Finally, thanks to my wife, Miriam, and my children, Alec and Nicol, for their love and support, and for putting up with all of this.

June 2005 Victor Shoup

CRYPTO 2005

August 14–18, 2005, 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

Stuart Haber, HP Labs, USA

Program Chair

Victor Shoup, New York University, USA

Program Committee

Masayuki Abe	NTT Information Sharing Platform Laboratories, Japan
Boaz Barak	Institute for Advanced Study & Princeton University, USA
Amos Beimel	Ben-Gurion University, Israel
Alex Biryukov	Katholieke Universiteit Leuven, Belgium
John Black	University of Colorado at Boulder, USA
Alexandra Boldyreva	Georgia Institute of Technology, USA
Jan Camenisch	IBM Zurich Research Laboratory, Switzerland
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Craig Gentry	DoCoMo USA Labs, USA
Shai Halevi	IBM T. J. Watson Research Center, USA
Stanislaw Jarecki	University of California at Irvine, USA
Antoine Joux	DGA & Univ. Versailles St-Quentin, France
Jonathan Katz	University of Maryland, USA
Arjen Lenstra	Lucent Technologies, USA & TU Eindhoven, The Netherlands
Yehuda Lindell	Bar-Ilan University, Israel
Tal Malkin	Columbia University, USA
Ilya Mironov	Microsoft Research, USA
David Naccache	Gemplus, France & Royal Holloway, UK
Moni Naor	Weizmann Institute of Science, Israel
Leonid Reyzin	Boston University, USA
Louis Salvail	Aarhus Universitet, Denmark
Alice Silverberg	University of California at Irvine, USA
Adam Smith	Weizmann Institute of Science, Israel
Rebecca Wright	Stevens Institute of Technology, USA

Advisory Members

Matt Franklin (Crypto 2004 Program Chair)	UC Davis, USA
Cynthia Dwork (Crypto 2006 Program Chair)	Microsoft Research, USA

External Reviewers

Luis von Ahn
Jesus F. Almansa
Michael Anshel
Frederik Armknecht
Michael Backes
Endre Bangerter
Paulo Barreto
Donald Beaver
Mihir Bellare
Daniel J. Bernstein
Bhargav Bhatt
Ian F. Blake
Daniel Bleichenbacher
Dan Boneh
Xavier Boyen
An Braeken
Eric Brier
Christian Cachin
Ran Canetti
Pascale Charpin
Melissa Chase
Benoit Chevallier-Mames
Martin Cochran
Nicolas Courtois
Ivan Damgård
Christophe De Cannière
Nenad Dedić
Michael de Mare
Claudia Diaz
Xuhua Ding
Hans Dobbertin
Yevgeniy Dodis
Iwan Duursma
Ariel Elbaz
Michael Engling
Marc Fischlin
Matthias Fitzi
Gerhard Frey
Eiichiro Fujisaki
Steven Galbraith
Juan Garay
Rosario Gennaro
Daniel Gottesman
Louis Goubin
Prateek Gupta
Helena Handschuh
Jonathan Herzog
Susan Hohenberger
Omer Horvitz
Nick Howgrave-Graham
Jim Hughes
Dae Hyun Yum
Yuval Ishai
Geetha Jagannathan
Marc Joye
Charanjit Jutla
Yael Tauman Kalai
Alexander Kholosha
Chiu-Yuen Koo
Hugo Krawczyk
Kaoru Kurosawa
Eyal Kushilevitz
Tanja Lange
Joseph Lano
Gregor Leander
Homin Lee
Wen-Ching Winnie Li
Anna Lysyanskaya
David M'Raihi
Phil Mackenzie
John Malone-Lee
Alexander May
Daniele Micciancio
Sara Miner More
Tal Moran
Shiho Moriai
Ryan Moriarty
Frédéric Muller
Kumar Murty
Steven Myers
Anderson Nascimento
Antonio Nicolosi
Jesper Buus Nielsen
Kobbi Nissim
Kazuo Ohta
Tatsuaki Okamoto
Siddika Berna Örs
Pascal Paillier
Matthew Parker
Rafael Pass
Thomas B. Pedersen
Krzysztof Pietrzak
Benny Pinkas
David Pointcheval
Joern-Mueller Quade
Tal Rabin
Zulfikar Ramzan
Omer Reingold
Pankaj Rohatgi
Guy Rothblum
Karl Rubin
Andreas Ruttor
Christian Schaffner
Berry Schoenmakers
Hovav Shacham
abhi shelat
Vitaly Shmatikov
Thomas Shrimpton
Hervé Sibert
Andrey Sidorenko
Nigel Smart
Dieter Sommer
Martijn Stam
Douglas R. Stinson
Koutarou Suzuki
Emmanuel Thomé
Eran Tromer
Fréderik Vercauteren
Eric Verheul
Emanuele Viola
Andrew Wan
Bogdan Warinschi
Hoeteck Wee
Benne de Weger
Enav Weinreb
Stephen Weis
Susanne Wetzel
Claire Whelan
Christopher Wolf
Nikolai Yakovenko
Shoko Yonezawa
Moti Yung
Sheng Zhong

Table of Contents