Lecture Notes in Computer Science 4117

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

Editorial Board

Cynthia Dwork (Ed.)

Advances in Cryptology - CRYPTO 2006

26th Annual International Cryptology Conference
Santa Barbara, California, USA, August 20-24, 2006
Proceedings

Volume Editor

Cynthia Dwork
Microsoft Research
1065 La Avenida, Mountain View, CA 94043, USA
E-mail: dwork@microsoft.com

Library of Congress Control Number: 2006930607

CR Subject Classification (1998): E.3, G.2.1, F.2.1-2, D.4.6, K.6.5, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-37432-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-37432-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11818175 06/3142 5 4 3 2 1 0

Preface

These are the proceedings of Crypto 2006, the 26th Annual International Cryptology Conference. The conference was sponsored by the International Association of Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California, Santa Barbara. The conference was held in Santa Barbara, California, August 20–24, 2006.

The conference received 220 submissions, out of which the Program Committee selected 34 for presentation. Submission and selection of papers was done using the IChair sofware, developed at the École Polytechnique Fédérale de Lausanne (EPFL) by Thomas Baignères and Matthieu Finiasz. Aided in part by comments from the committee and external reviewers, the authors of accepted papers had roughly six weeks in which to prepare final versions for these proceedings. These were not subject to editorial review.

The committee chose "On the Power of the Randomized Iterate," by Iftach Haitner, Danny Harnik, and Omer Reingold, to receive the Best Paper award.

The committee also invited Oded Regev and David Wagner to speak on topics of their choice. Their talks were entitled, respectively, "Lattice-Based Cryptography" and "Cryptographic Protocols for Electronic Voting."

We continued the tradition of a "Rump Session" of very brief presentations.

The cryptology community provides a collaborative and supportive environment for exciting research, and the success of previous Crypto conferences fosters enthusiasm for participation in subsequent ones. I am deeply grateful to all the authors who submitted papers, not only for their contribution to this conference but also for maintaining this tradition.

I thank Thomas Baignères and Matthieu Finiasz for kindly hosting the server – and for writing IChair in the first place. David Fuchs provided invaluable assistance in assembling the final papers into this volume. Josh Benaloh was everything one could possibly hope for in a General Chair. I thank him for his good judgement and gracious assistance at all times.

In a departure from recent tradition, submissions were not anonymous. I am grateful to Andy Clark and Kevin McCurley for their counsel regarding this course of action, and to the Program Committee for being open to change. I also warmly thank the members of the Program Committee for their energy, intelligence, wisdom, and the maturity with which they approached their task.

Finally, I thank Moni Naor, who for the past nineteen years has taught me cryptography.

June 2006

Cynthia Dwork
Program Chair

CRYPTO 2006

August 20–24, 2006, 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
Josh Benaloh, Microsoft, USA

Program Chair
Cynthia Dwork, Microsoft, USA

Program Committee

Boaz Barak ..... Princeton University, USA
Eli Biham ..... Technion, Israel
Ivan Damgård ..... University of Aarhus, Denmark
Yuval Ishai ..... Technion, Israel
Jonathan Katz ..... University of Maryland, USA
Arjen Lenstra ..... EPFL, Switzerland
Yehuda Lindell ..... Bar-Ilan University, Israel
Tal Malkin ..... Columbia University, USA
Mitsuru Matsui ..... Mitsubishi Electric, Japan
Daniele Micciancio ..... University of California, San Diego, USA
Moni Naor ..... Weizmann Institute of Science, Israel
Phong Nguyen ..... CNRS/École Normale Supérieure, France
Kobbi Nissim ..... Ben-Gurion University, Israel
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Hovav Shacham ..... Weizmann Institute of Science, Israel
Vitaly Shmatikov ..... University of Texas, Austin, USA
Edlyn Teske ..... University of Waterloo, Canada
Salil Vadhan ..... Harvard University, USA
Yiqun Lisa Yin ..... Independent Consultant, USA

Advisory Members

Victor Shoup (Crypto 2005 Program Chair) ..... New York University, USA
Alfred Menezes (Crypto 2007 Program Chair) University of Waterloo, Canada

External Reviewers

Michel Abdalla
Masayuki Abe
Adi Akavia
Elena Andreeva
Spyridon Antonakopoulos
Kazumaro Aoki
Frederik Armknecht
Joonsang Baek
Elad Barkan
Lejla Batina
Peter Beelen
Amos Beimel
Mihir Bellare
Josh Benaloh
Daniel Bernstein
Alex Biryukov
Daniel Bleichenbacher
Xavier Boyen
An Braeken
Emmanuel Bresson
Justin Brickell
Jan Camenisch
Ran Canetti
Christophe De Cannière
Dario Catalano
Melissa Chase
Lily Chen
Rafi Chen
Yongxi Cheng
Seung Geol Choi
Scott Contini
Ronald Cramer
Anupam Datta
Cécile Delerablée
Anand Desai
Claus Diem
Jingtai Ding
Yan Zhong Ding
Yevgenyi Dodis
Orr Dunkelman
Phil Eisen
Ariel Elbaz
Serge Fehr
Matthias Fitzi
Lance Fortnow
Pierre-Alain Fouque
Soichi Furuya
Steven Galbraith
Juan Garay
Rosario Gennaro
Henri Gilbert
Eu-Jin Goh
Ronen Gradwohl
Louis Granboulan
Prateek Gupta
Iftach Haitner
Shai Halevi
Renen Hallak
Safuat Hamdy
Helena Handschuh
Danny Harnik
Anwar Hasan
Carmit Hazay
Alex Healy
Javier Herranz
Jonathan Herzog
Jason Hinek
Dennis Hofheinz
Nick Howgrave-Graham
Tetsu Iwata
Stas Jarecki
Ellen Jochemsz
Antoine Joux
Pascal Junod
Charanjit Jutla
Marcelo Kaihara
Yael Tauman Kalai
Alexander Kholosha
Joe Kilian
Eike Kiltz
Jongsung Kim
Vlastimil Klima
Vlad Kolesnikov
Chiu-Yuen Koo
Simon Kramer
Steve Kremer
Sebastien Kunz-Jacques
Eyal Kushilevitz
Tanja Lange
Joseph Lano
Kristin Lauter
Homin Lee
Stephane Lemieux
Matt Lepinski
Gatan Leurent
Benoit Libert
Stefan Lucks
Christoph Ludwig
Anna Lysyanskaya
Vadim Lyubashevsky
Phil MacKenzie
Mohammad Mahmoody
John Malone-Lee
Mark Manasse
Alexander May
Frank McSherry
Willi Meier
Daniele Micciancio
John Mitchell
Anton Mityagin
Peter Montgomery
Tal Moran
Ruggero Morselli
Siguna Müller
Sean Murphy
David Naccache
Arvind Narayanan
Andrew Neff
Gregory Neven
Jesper Buus Nielsen
Tatsuaki Okamoto
Michael Østergaard
Rafi Ostrovsky
Saurabh Panjwani
Souradyuti Paul
Raphael C.-W. Phan
Krzysztof Pietrzak
Benny Pinkas

David Pointcheval
Tal Rabin
Oded Regev
Omer Reingold
Leo Reyzin
Tom Ristenpart
Phil Rogaway
Alon Rosen
Amit Sahai
Yasuyuki Sakai
Louis Salvail
Christian Schaffner
Claus Schnorr
Berry Schoenmakers
Gil Segev
Jean-Pierre Seifert
Ronen Shaltiel
Taizo Shirai
Victor Shoup
Igor Shparlinski
Tom Shrimpton
Andrey Sidorenko
Alice Silverberg
Robert Silverman
Adam Smith
Martijn Stam
François-Xavier Standaert
Ron Steinfeld
Daisuke Suzuki
Mike Szydlo
Katsuyuki Takashima
Tamir Tassa
Tomas Toft
Eran Tromer
Toyohiro Tsurumaru
Andrew Wan
Shuhong Wang
Dai Watanabe
Brent Waters
John Watrous
Benne de Weger
Stephanie Wehner
Enav Weinreb
Susanne Wetzel
Udi Wieder
Douglas Wikström
Christopher Wolf
Duncan Wong
David Woodruff
David Xiao
Guomin Yang
Kan Yasuda
Feng Zhu

Table of Contents