

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Cynthia Dwork (Ed.)

Advances in Cryptology - CRYPTO 2006

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



Springer

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

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

Table of Contents

Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs <i>Elad Barkan, Eli Biham, Adi Shamir</i>	1
On the Power of the Randomized Iterate <i>Iftach Haitner, Danny Harnik, Omer Reingold</i>	22
Strengthening Digital Signatures Via Randomized Hashing <i>Shai Halevi, Hugo Krawczyk</i>	41
Round-Optimal Composable Blind Signatures in the Common Reference String Model <i>Marc Fischlin</i>	60
On Signatures of Knowledge <i>Melissa Chase, Anna Lysyanskaya</i>	78
Non-interactive Zaps and New Techniques for NIZK <i>Jens Groth, Rafail Ostrovsky, Amit Sahai</i>	97
Rankin's Constant and Blockwise Lattice Reduction <i>Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, Phong Q. Nguyen</i>	112
Lattice-Based Cryptography <i>Oded Regev</i>	131
A Method for Making Password-Based Key Exchange Resilient to Server Compromise <i>Craig Gentry, Philip MacKenzie, Zulfikar Ramzan</i>	142
Mitigating Dictionary Attacks on Password-Protected Local Storage <i>Ran Canetti, Shai Halevi, Michael Steiner</i>	160
Rationality and Adversarial Behavior in Multi-party Computation <i>Anna Lysyanskaya, Nikos Triandopoulos</i>	180
When Random Sampling Preserves Privacy <i>Kamalika Chaudhuri, Nina Mishra</i>	198

Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models <i>Moni Naor, Gil Segev, Adam Smith</i>	214
Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets <i>Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin, Adam Smith</i>	232
On Forward-Secure Storage <i>Stefan Dziembowski</i>	251
Construction of a Non-malleable Encryption Scheme from Any Semantically Secure One <i>Rafael Pass, abhi shelat, Vinod Vaikuntanathan</i>	271
Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles) <i>Xavier Boyen, Brent Waters</i>	290
Fast Algorithms for the Free Riders Problem in Broadcast Encryption <i>Zulfikar Ramzan, David P. Woodruff</i>	308
The Number Field Sieve in the Medium Prime Case <i>Antoine Joux, Reynald Lercier, Nigel Smart, Frederik Vercauteren</i> ...	326
Inverting HFE Is Quasipolynomial <i>Louis Granboulan, Antoine Joux, Jacques Stern</i>	345
Cryptanalysis of $2R^-$ Schemes <i>Jean-Charles Faugère, Ludovic Perret</i>	357
Receipt-Free Universally-Verifiable Voting with Everlasting Privacy <i>Tal Moran, Moni Naor</i>	373
Cryptographic Protocols for Electronic Voting <i>David Wagner</i>	393
Asymptotically Optimal Two-Round Perfectly Secure Message Transmission <i>Saurabh Agarwal, Ronald Cramer, Robbert de Haan</i>	394
Random Selection with an Adversarial Majority <i>Ronen Gradwohl, Salil Vadhan, David Zuckerman</i>	409
Oblivious Transfer and Linear Functions <i>Ivan B. Damgård, Serge Fehr, Louis Salvail, Christian Schaffner</i>	427

On Expected Constant-Round Protocols for Byzantine Agreement <i>Jonathan Katz, Chiu-Yuen Koo</i>	445
Robust Multiparty Computation with Linear Communication Complexity <i>Martin Hirt, Jesper Buus Nielsen</i>	463
On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation <i>Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell, Erez Petrank</i>	483
Scalable Secure Multiparty Computation <i>Ivan Damgård, Yuval Ishai</i>	501
Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields <i>Hao Chen, Ronald Cramer</i>	521
Automated Security Proofs with Sequences of Games <i>Bruno Blanchet, David Pointcheval</i>	537
On Robust Combiners for Private Information Retrieval and Other Primitives <i>Remo Meier, Bartosz Przydatek</i>	555
On the Impossibility of Efficiently Combining Collision Resistant Hash Functions <i>Dan Boneh, Xavier Boyen</i>	570
On the Higher Order Nonlinearities of Algebraic Immune Functions <i>Claude Carlet</i>	584
New Proofs for NMAC and HMAC: Security without Collision-Resistance <i>Mihir Bellare</i>	602
Author Index	621