Lecture Notes in Computer Science 5157

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

David Wagner (Ed.)

Advances in Cryptology – CRYPTO 2008

28th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 17-21, 2008
Proceedings

Volume Editor

David Wagner
University of California, Berkeley
Berkeley CA 94720-1776, USA
E-mail: daw@cs.berkeley.edu

Library of Congress Control Number: 2008932556

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 3-540-85173-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85173-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12453214 06/3180 5 4 3 2 1 0

Preface

CRYPTO 2008, the 28th Annual International Cryptology Conference, was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society 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 17–21, 2008. Susan Langford served as the General Chair of CRYPTO 2008, and I had the privilege of serving as the Program Chair.

The conference received 184 submissions, and all were reviewed by the Program Committee. Each paper was assigned at least three reviewers, while submissions co-authored by Program Committee members were reviewed by at least five people. All submissions were anonymous, and the identity of the authors were not revealed to committee members. During the first phase of the review process, the Program Committee, aided by reports from 142 external reviewers, produced a total of 611 reviews in all. Then, committee members discussed these papers in depth over a period of 8 weeks using an electronic messaging system, in the process writing 1,400 discussion messages. After careful deliberation, the Program Committee selected 32 papers for presentation. The authors of accepted papers were given 5 weeks to prepare final versions for these proceedings. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

Gilles Brassard delivered the 2008 IACR Distinguished Lecture. The Best Paper Award was announced at the conference. Dan Bernstein served as the chair of the Rump Session, a forum for short and entertaining presentations on recent work of both a technical and non-technical nature.

I would like to thank everyone who contributed to the success of CRYPTO 2008. Shai Halevi provided software for facilitating the reviewing process that was of great help throughout the Program Committee's work, and I am especially grateful for his assistance. Alfred Menezes and Shai Halevi served as advisory members of the Program Committee, and I am grateful to them, and Arjen Lenstra and Bart Preneel, for their cogent advice. Susan Langford and others played a vital role in organizing the conference. Also, I am deeply grateful to the Program Committee for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review. Thanks also to the external reviewers, listed on the following pages, for contributing their time and expertise. Finally, I would like to thank all the authors who submitted papers to CRYPTO 2008 for submitting their best research.

August 2008 David Wagner

CRYPTO 2008

August 17–21, 2008, 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

Susan Langford, Hewlett-Packard Company

Program Chair

David Wagner, UC Berkeley

Program Committee

Boaz Barak	Princeton University
John Black	University of Colorado at Boulder
Xavier Boyen	Voltage Security
Melissa Chase	Brown University
Jean-Sebastien Coron	University of Luxembourg
Yevgeniy Dodis	New York University
Orr Dunkelman	KU Leuven
Matt Franklin	UC Davis
Craig Gentry	Stanford University
Henri Gilbert	Orange Labs
Kristian Gjosteen	Norwegian University of Science and Technology
Louis Granboulan	European Aeronautic Defence and Space Company
Danny Harnik	IBM Haifa Research Lab
Susan Hohenberger	Johns Hopkins University
Nick Hopper	University of Minnesota
Yuval Ishai	Technion Institute and UCLA
Thomas Johansson	Lund University
Ari Juels	RSA Laboratories

Lars Knudsen	DTU Mathematics
Kristin Lauter	Microsoft Research
Yehuda Lindell	Bar Ilan University
Tal Malkin	Columbia University
Manoj Prabhakaran	University of Illinois, Urbana-Champaign
Zulfikar Ramzan	Symantec
Renato Renner	ETH Zurich
Matt Robshaw	Orange Labs
Alon Rosen	Herzliya Interdisciplinary Center
Amit Sahai	UCLA
Hovav Shacham	UC San Diego
Tom Shrimpton	Portland State University and University of Lugano
Adam Smith	Pennsylvania State University
Serge Vaudenay	EPFL
Brent Waters	SRI International
Lisa Yin	Independent Consultant

Advisory Members

Alfred Menezes (CRYPTO 2007 Program Chair)	University of Waterloo
Shai Halevi (CRYPTO 2009 Program Chair)	IBM Research

External Reviewers

Michel Abdalla	Denis Charles	Marc Girault
Tolga Acar	Seung Geol Choi	Sharon Goldberg
Joel Alwen	Carlos Cid	Mark Gondree
Thomas Baignères	Martin Cochran	Vipul Goyal
Zuzana Beerliova	Roger Colbeck	Matthew Green
Amos Beimel	Scott Contini	Jens Groth
Mihir Bellare	Scott Coull	Venkatesan Guruswami
Josh Benaloh	Dána Dachman-Soled	Shai Halevi
Come Berbain	Oscar Dahlsten	Michael Hamburg
Olivier Billet	Jintai Ding	Carmit Hazay
Alexandra Boldyreva	Glenn Durfee	Martin Hirt
Dan Boneh	Ariel Elbaz	Thomas Holenstein
Colin Boyd	Jean-Charles Faugère	Mariusz Jakubowski
Emmanuel Bresson	Serge Fehr	Stas Jarecki
Reinier Broker	Marc Fischlin	Antoine Joux
Lennart Brynielsson	Pierre-Alain Fouque	Jonathan Katz
Ran Canetti	Martin Gagne	John Kelsey
Yaniv Carmeli	Juan Garay	Aggelos Kiayias
Rafik Chaabouni	Praveen Gauravaram	Yongdae Kim

Markulf Kohlweiss
Gillat Kol
Hugo Krawczyk
Alptekin Küpçü
Eyal Kushilevitz
Homin Lee
Matt Lepinski
Huijia Lin
Satya Lokam
Steve Lu
Vadim Lyubashevsky
Philip Mackenzie
Mohammad Mahmoody-Ghidary
Krystian Matusiewicz
Daniele Micciancio
Ilya Mironov
Payman Mohassel
David Molnar
Tal Moran
Volker Muller
Sean Murphy
Yusuke Naito
Yassir Nawaz
Phong Nguyen
Jesper Buus Nielsen
Kobbi Nissim
Alina Oprea
Kazu Ota
Khaled Ouafi
Raphael Overbeck
Carles Padro
Pascal Paillier
Sylvain Pasini
Jacques Patarin
Chris Peikert
Christophe Petit
Thomas Peyrin
Duong Hieu Phan
David Pointcheval
Prashant Puniya
Tal Rabin
Mario Di Raimondo
Dominic Raub
Oded Regev
Omer Reingold
Renato Renner
Leonid Reyzin
Thomas Ristenpart
Matthieu Rivain
Phillip Rogaway
Guy Rothblum
Peter Ryan
Kazuo Sakiyama
Yu Sasaki
Michael Scott
Gil Segev
Yannick Seurin
abhi shelat
Igor Shparlinski
Nigel Smart
John Steinberger
Ron Steinfeld
Mike Szydlo
Stefano Tessaro
Soren Thomsen
Nikos Triandopoulos
Eran Tromer
Salil Vadhan
Vinod Vaikuntanathan
Martin Vuagnoux
Shabsi Walfish
Andrew Wan
Lei Wang
Hoeteck Wee
Enav Weinreb
Steve Weis
Daniel Wichs
Stefan Wolf
Duncan Wong
Juerg Wullschleger
Aaram Yun
Gideon Yuval
Erik Zenner
Yunlei Zhao
Vassilis Zikas

Table of Contents

Random Oracles

Applications

Public-Key Crypto I

Hash Functions I

Cryptanalysis I

Multiparty Computation I

Cryptanalysis II

Public-Key Crypto II

Hash Functions II

Privacy

Multiparty Computation II

Zero Knowledge

Oblivious Transfer