

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

Alfred Kobsa

University of California, Irvine, CA, 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

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

ISBN-10 0302-9743

ISBN-13 3-540-85173-9 Springer Berlin Heidelberg New York
978-3-540-85173-8 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.com
Springer is a part of Springer Science+Business Media

© International Association for Cryptologic Research 2008
Printed in Germany

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.

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

Table of Contents

Random Oracles

The Random Oracle Model and the Ideal Cipher Model Are Equivalent	1
<i>Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin</i>	
Programmable Hash Functions and Their Applications.....	21
<i>Dennis Hofheinz and Eike Kiltz</i>	

Applications

One-Time Programs	39
<i>Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum</i>	
Adaptive One-Way Functions and Applications	57
<i>Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan</i>	

Public-Key Crypto I

Bits Security of the Elliptic Curve Diffie-Hellman Secret Keys	75
<i>Dimitar Jetchev and Ramarathnam Venkatesan</i>	
Improved Bounds on Security Reductions for Discrete Log Based Signatures	93
<i>Sanjam Garg, Raghav Bhaskar, and Satyanarayana V. Lokam</i>	
Circular-Secure Encryption from Decision Diffie-Hellman	108
<i>Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky</i>	
Public-Key Locally-Decodable Codes	126
<i>Brett Hemenway and Rafail Ostrovsky</i>	

Hash Functions I

Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms	144
<i>Helena Handschuh and Bart Preneel</i>	
Cryptanalysis of the GOST Hash Function	162
<i>Florian Mendel, Norbert Pramstaller, Christian Rechberger, Marcin Kontak, and Janusz Szmidt</i>	

Preimages for Reduced SHA-0 and SHA-1	179
<i>Christophe De Cannière and Christian Rechberger</i>	

Cryptanalysis I

On the Power of Power Analysis in the Real World: A Complete Break of the KEELOQ Code Hopping Scheme	203
<i>Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani</i>	
Bug Attacks	221
<i>Eli Biham, Yaniv Carmeli, and Adi Shamir</i>	

Multiparty Computation I

Scalable Multiparty Computation with Nearly Optimal Work and Resilience	241
<i>Ivan Damgård, Yuval Ishai, Mikkel Krøigaard, Jesper Buus Nielsen, and Adam Smith</i>	
Cryptographic Complexity of Multi-Party Computation Problems: Classifications and Separations	262
<i>Manoj Prabhakaran and Mike Rosulek</i>	

Cryptanalysis II

Cryptanalysis of MinRank	280
<i>Jean-Charles Faugère, Françoise Levy-dit-Vehel, and Ludovic Perret</i>	
New State Recovery Attack on RC4	297
<i>Alexander Maximov and Dmitry Khovratovich</i>	

Public-Key Crypto II

Dynamic Threshold Public-Key Encryption	317
<i>Cécile Delerablée and David Pointcheval</i>	
On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles	335
<i>Alexandra Boldyreva, Serge Fehr, and Adam O'Neill</i>	
Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles	360
<i>Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart</i>	
Communication Complexity in Algebraic Two-Party Protocols	379
<i>Rafail Ostrovsky and William E. Skeith III</i>	

Hash Functions II

Beyond Uniformity: Better Security/Efficiency Tradeoffs for Compression Functions	397
<i>Martijn Stam</i>	
Compression from Collisions, or Why CRHF Combiners Have a Long Output	413
<i>Krzysztof Pietrzak</i>	
Constructing Cryptographic Hash Functions from Fixed-Key Blockciphers.....	433
<i>Phillip Rogaway and John Steinberger</i>	

Privacy

Distributed Private Data Analysis: Simultaneously Solving How and What	451
<i>Amos Beimel, Kobbi Nissim, and Eran Omri</i>	
New Efficient Attacks on Statistical Disclosure Control Mechanisms	469
<i>Cynthia Dwork and Sergey Yekhanin</i>	

Multiparty Computation II

Efficient Secure Linear Algebra in the Presence of Covert or Computationally Unbounded Adversaries	481
<i>Payman Mohassel and Eran Weinreb</i>	
Collusion-Free Protocols in the Mediated Model	497
<i>Joël Alwen, Abhi Shelat, and Ivan Visconti</i>	

Zero Knowledge

Efficient Constructions of Composable Commitments and Zero-Knowledge Proofs	515
<i>Yevgeniy Dodis, Victor Shoup, and Shabsi Walfish</i>	
Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems	536
<i>Chris Peikert and Vinod Vaikuntanathan</i>	

Oblivious Transfer

A Framework for Efficient and Composable Oblivious Transfer	554
<i>Chris Peikert, Vinod Vaikuntanathan, and Brent Waters</i>	

Founding Cryptography on Oblivious Transfer – Efficiently	572
<i>Yuval Ishai, Manoj Prabhakaran, and Amit Sahai</i>	
Author Index	593