

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

New York University, NY, 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

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

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

springeronline.com

© International Association for Cryptologic Research 2005
Printed in Germany

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. Nguyen.

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.

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

Table of Contents

Efficient Collision Search Attacks on SHA-0 <i>Xiaoyun Wang, Hongbo Yu, Yiqun Lisa Yin</i>	1
Finding Collisions in the Full SHA-1 <i>Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu</i>	17
Pebbling and Proofs of Work <i>Cynthia Dwork, Moni Naor, Hoeteck Wee</i>	37
Composition Does Not Imply Adaptive Security <i>Krzysztof Pietrzak</i>	55
On the Discrete Logarithm Problem on Algebraic Tori <i>Robert Granger, Frederik Vercauteren</i>	66
A Practical Attack on a Braid Group Based Cryptographic Protocol <i>Alexei Myasnikov, Vladimir Shpilrain, Alexander Ushakov</i>	86
The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption <i>Yi Lu, Willi Meier, Serge Vaudenay</i>	97
Unconditional Characterizations of Non-interactive Zero-Knowledge <i>Rafael Pass, abhi shelat</i>	118
Impossibility and Feasibility Results for Zero Knowledge with Public Keys <i>Joël Alwen, Giuseppe Persiano, Ivan Visconti</i>	135
Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors <i>Marc Fischlin</i>	152
A Formal Treatment of Onion Routing <i>Jan Camenisch, Anna Lysyanskaya</i>	169
Simple and Efficient Shuffling with Provable Correctness and ZK Privacy <i>Kun Peng, Colin Boyd, Ed Dawson</i>	188

Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions <i>Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, Haixia Shi</i>	205
Private Searching on Streaming Data <i>Rafail Ostrovsky, William E. Skeith III</i>	223
Privacy-Preserving Set Operations <i>Lea Kissner, Dawn Song</i>	241
Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys <i>Dan Boneh, Craig Gentry, Brent Waters</i>	258
Generic Transformation for Scalable Broadcast Encryption Schemes <i>Jung Yeon Hwang, Dong Hoon Lee, Jongin Lim</i>	276
Authenticating Pervasive Devices with Human Protocols <i>Ari Juels, Stephen A. Weis</i>	293
Secure Communications over Insecure Channels Based on Short Authenticated Strings <i>Serge Vaudenay</i>	309
On Codes, Matroids and Secure Multi-party Computation from Linear Secret Sharing Schemes <i>Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, Carles Padró</i>	327
Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields <i>Ronald Cramer, Serge Fehr, Martijn Stam</i>	344
Secure Computation Without Authentication <i>Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, Tal Rabin</i> ...	361
Constant-Round Multiparty Computation Using a Black-Box Pseudorandom Generator <i>Ivan Damgård, Yuval Ishai</i>	378
Secure Computation of Constant-Depth Circuits with Applications to Database Search Problems <i>Omer Barkol, Yuval Ishai</i>	395

Analysis of Random Oracle Instantiation Scenarios for OAEP and Other Practical Schemes <i>Alexandra Boldyreva, Marc Fischlin</i>	412
Merkle-Damgård Revisited: How to Construct a Hash Function <i>Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, Prashant Puniya</i>	430
On the Generic Insecurity of the Full Domain Hash <i>Yevgeniy Dodis, Roberto Oliveira, Krzysztof Pietrzak</i>	449
New Monotones and Lower Bounds in Unconditional Two-Party Computation <i>Stefan Wolf, Jürg Wullschleger</i>	467
One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption <i>Thomas Holenstein, Renato Renner</i>	478
A Quantum Cipher with Near Optimal Key-Recycling <i>Ivan Damgård, Thomas Brochmann Pedersen, Louis Salvail</i>	494
An Efficient CDH-Based Signature Scheme with a Tight Security Reduction <i>Benoît Chevallier-Mames</i>	511
Improved Security Analyses for CBC MACs <i>Mihir Bellare, Krzysztof Pietrzak, Phillip Rogaway</i>	527
HMQR: A High-Performance Secure Diffie-Hellman Protocol <i>Hugo Krawczyk</i>	546
Author Index	567